# Cisco MDS 9000 ファミリ NX-OS セキュリティ設定ガイド

初版：16/01/28



シスコシステムズ合同会社
http://www.cisco.com/jp

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices をご覧ください。

Text Part Number:

**【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、米国シスコシステムズ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 MDS 9000 ファミリ NX-OS セキュリティ設定ガイド*

# CONTENTS

# 新機能および変更された機能に関する情報

表 1 に、このガイドで追加および変更された機能を示します

*表 1　　新機能および変更された機能*

| 機能 | リリース | 参照先 |
|---|---|---|
| セキュア ログインの機能拡張 | 7.3(1)DY(1) | 第 3 章「セキュア ログインの機能拡張」 |
| Cisco MDS 9700 シリーズ スイッチでの SHA2 の IPSec および IKEv2 のサポート | 7.3(1)DY(1) | 第 7 章「IPSec ネットワーク セキュリティの設定」 |
| SHA2 の IPSec および IKEv2 のサポート | 7.3(0)D1(1) | 第 7 章「IPSec ネットワーク セキュリティの設定」 |

# はじめに

ここでは、『*Cisco MDS 9000 ファミリ NX-OS セキュリティ コンフィギュレーション ガイド*』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

## 対象読者

このマニュアルは、マルチレイヤ ディレクタおよびファブリック スイッチの Cisco MDS 9000 ファミリの設定および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

## マニュアルの構成

このマニュアルの構成は、次のとおりです。

| | タイトル | 説明 |
|---|---|---|
| 第 1 章 | セキュリティの概要 | Cisco MDS 9000 ファミリ NX-OS ソフトウェアがサポートするセキュリティ機能の概要を示します。 |
| 第 2 章 | FIPS の設定 | FIPS 設定の注意事項について説明し、FIPS モードをイネーブルにする方法および FIPS のセルフテストを実行する方法についても説明します。 |
| 第 5 章 | ユーザ ロールおよび共通ロールの設定 | ユーザ ロールおよび共通ロールの設定方法を説明します。 |
| 第 3 章 | 外部 AAA サーバでのセキュリティ機能の設定 | Cisco MDS 9000 ファミリのすべてのスイッチで提供される AAA パラメータ、ユーザ プロファイル、Remote Authentication Dial-In User Service（RADIUS）認証のセキュリティ オプションについて説明し、これらのオプションの設定情報を示します。 |
| 第 4 章 | IPv4 および IPv6 のアクセス コントロール リストの設定 | IPv4 のスタティック ルーティング機能と、この機能を使用した VSAN 間のトラフィック ルーティングについて説明します。 |
| 第 6 章 | 認証局およびデジタル証明書の設定 | 認証局（CA）との連携方法およびセキュアかつスケーラブルな通信を実現するためのデジタル認証の使用方法について説明します。 |

| | タイトル | 説明 |
|---|---|---|
| 第 7 章 | IPSec ネットワーク セキュリティの設定 | プロトコルおよびアルゴリズムのネゴシエーションの処理に使用されるデジタル証明書、IP Security Protocol（IPSec）オープン スタンダード、およびインターネット キー交換（IKE）プロトコルについて詳述します。 |
| 第 8 章 | FC-SP および DHCHAP の設定 | DHCHAP プロトコルについて説明します。DHCHAP は、Cisco MDS 9000 ファミリ スイッチと他のデバイスの間で認証を提供する FC-SP プロトコルです。 |
| 第 9 章 | ポート セキュリティの設定 | Cisco MDS 9000 ファミリ スイッチのポートへの不正アクセスを防止するポート セキュリティ機能について詳細に説明します。 |
| 第 10 章 | Fibre Channel Common Transport 管理セキュリティの設定 | ネットワーク管理者だけがスイッチにクエリーを送信して、情報にアクセスできるように、ファイバ チャネル トランスポート管理サーバ クエリーを設定する方法の詳細について説明します。 |
| 第 11 章 | ファブリック バインディングの設定 | VSAN のファブリック バインディング セキュリティ機能（特定のスイッチ間だけで ISL をイネーブルにする機能）について説明します。 |
| 第 12 章 | Cisco TrustSec ファイバ チャネル リンク暗号化の設定 | IP ホストが iSCSI プロトコルを使用してファイバ チャネル ストレージにアクセスできるようにするためのスイッチの設定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。 |
| **[ ]** | 角カッコの中の要素は、省略可能です。 |
| **[ x \| y \| z ]** | どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。 |

出力例では、次の表記法を使用しています。

| | |
|---|---|
| `screen フォント` | スイッチが表示する端末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、次の表記法を使用しています。

(注) 「*注釈*」を意味します。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

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

Cisco MDS 9000 ファミリのマニュアル セットには次のマニュアルが含まれます。オンラインでドキュメントを検索するには、次の Web サイトにある Cisco MDS NX-OS Documentation Locator を使用してください。

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.htm

## リリース ノート

- 『*Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*』
- 『*Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*』
- 『*Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*』
- 『*Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*』
- 『*Release Notes for Cisco MDS 9000 Family Fabric Manager*』

## 法規制の遵守および安全性情報

- 『*Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*』

## 互換性に関する情報

- 『*Cisco Data Center Interoperability Support Matrix*』
- 『*Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*』
- 『*Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*』

- 『*Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*』
- 『*Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*』
- 『*Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*』

## ハードウェアの設置

- 『*Cisco MDS 9710 Series Hardware Installation Guide*』
- 『*Cisco MDS 9500 Series Hardware Installation Guide*』
- 『*Cisco MDS 9250i Series Hardware Installation Guide*』
- 『*Cisco MDS 9200 Series Hardware Installation Guide*』
- 『*Cisco MDS 9100 Series Hardware Installation Guide*』
- 『*Cisco MDS 9148S Series Hardware Installation Guide*』
- 『*Cisco MDS 9148S Multilayer Fabric Switch Quick Start Guide*』
- 『*Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*』

## ソフトウェアのインストールおよびアップグレード

- 『*Cisco MDS 9000 NX-OS Release 4.1(x)*』および『*SAN-OS 3(x) Software Upgrade and Downgrade Guide*』
- 『*Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*』
- 『*Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*』

## Cisco NX-OS

- 『*Cisco MDS 9000 Family NX-OS Licensing Guide*』
- 『*Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*』
- 『*Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*』
- 『*Cisco MDS 9000 ファミリ NX-OS Inter-VSAN ルーティング コンフィギュレーション ガイド*』

## Cisco Fabric Manager

- 『*Cisco Fabric Manager Fundamentals Configuration Guide*』
- 『*Cisco Fabric Manager System Management Configuration Guide*』
- 『*Cisco Fabric Manager Interfaces Configuration Guide*』
- 『*Cisco Fabric Manager Fabric Configuration Guide*』
- 『*Cisco Fabric Manager Quality of Service Configuration Guide*』
- 『*Cisco Fabric Manager Security Configuration Guide*』
- 『*Cisco Fabric Manager IP Services Configuration Guide*』
- 『*Cisco Fabric Manager Intelligent Storage Services Configuration Guide*』
- 『*Cisco Fabric Manager High Availability and Redundancy Configuration Guide*』
- 『*Cisco Fabric Manager Inter-VSAN Routing Configuration Guide*』
- *Cisco Fabric Manager オンライン ヘルプ*
- *Cisco Fabric Manager Web Services オンライン ヘルプ*

## コマンドライン インターフェイス

- 『*Cisco MDS 9000 Family Command Reference*』

## インテリジェント ストレージ ネットワーキング サービス コンフィギュレーション ガイド

- 『*Cisco MDS 9000 I/O Acceleration Configuration Guide*』
- 『*Cisco MDS 9000 Family SANTap Deployment Guide*』
- 『*Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*』
- 『*Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*』
- 『*Cisco MDS 9000 Family Secure Erase Configuration Guide*』
- 『*Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*』

## トラブルシューティングおよび参考資料

- 『*Cisco NX-OS System Messages Reference*』
- 『*Cisco MDS 9000 Family NX-OS Troubleshooting Guide*』
- 『*Cisco MDS 9000 Family NX-OS MIB Quick Reference*』
- 『*Cisco MDS 9000 Family NX-OS SMI-S Programming Reference*』
- 『*Cisco MDS 9000 Family Fabric Manager Server Database Schema*』

# 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

Cisco MDS 9000 NX-OS ソフトウェアは、ストレージ エリア ネットワーク（SAN）内にセキュリティを提供する高度なセキュリティ機能をサポートしています。これらの機能は、故意か故意でないかにかかわらず、内部や外部の脅威からネットワークを保護します。

この章は、次の項で構成されています。



## FIPS

連邦情報処理標準規格（FIPS）140-2、*暗号モジュール セキュリティ要件は*、暗号モジュールに対する米国政府の要求条件を定義しています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

FIPS の設定については、第 2 章「FIPS の設定」を参照してください。

# ユーザ ロールおよび共通ロール

ロールベースの許可は、ユーザにロールを割り当てることによってスイッチへのアクセスを制限します。Cisco MDS 9000 ファミリ内のすべての管理アクセスは、ロールに基づきます。ユーザは、ユーザが属するロールによって明示的に許可されている管理操作の実行に制限されます。

ユーザ ロールおよび共通ロールの設定については、第 3 章「共通ロールの設定」を参照してください。

# RADIUS および TACACS+

認証、許可、アカウンティング（AAA）機能は、スイッチを管理するユーザの ID 確認、アクセス権付与、およびアクション追跡を実行します。リモート AAA サーバを利用するソリューションを提供するため、すべての Cisco MDS 9000 ファミリ スイッチで Remote Authentication Dial-In User Service（RADIUS）プロトコルおよび Terminal Access Controller Access Control System Plus（TACACS+）プロトコルが使用されています。このセキュリティ機能は、AAA サーバでの中央集中型のユーザ アカウント管理機能を実現します。

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。ルータまたはアクセス サーバをネットワーク アクセス サーバとして使用している場合、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 サーバは AAA を介して通信します。

このマニュアルの各章では、次の機能について説明します。

- スイッチ管理：コマンドライン インターフェイス（CLI）や Simple Network Management Protocol（SNMP）などのすべての管理アクセス手段にセキュリティを提供する管理セキュリティ システム。
- スイッチの AAA 機能：Cisco MDS 9000 ファミリの任意のスイッチで、コマンドライン インターフェイス（CLI）または簡易ネットワーク管理プロトコル（SNMP）を使用して AAA スイッチ機能を設定する機能。
- RADIUS：不正なアクセスからネットワークを保護する、AAA を介して実装された分散型クライアント/サーバ システム。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。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。
- TACACS+：AAA を介して実装されるセキュリティ アプリケーション。ルータまたはネットワーク アクセス サーバへのアクセスを取得しようとするユーザの中央集中型検証を実現します。TACACS+ サービスは、一般に UNIX または Windows NT ワークステーションで稼働する TACACS+ デーモン上のデータベースに保持されます。TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。

RADIUS および TACACS+ の設定方法については、第 4 章「外部 AAA サーバでのセキュリティ機能の設定」を参照してください。

# IP ACL

IP アクセス コントロール リスト（ACL）は、帯域外管理イーサネット インターフェイスおよび帯域内 IP 管理インターフェイスでの基本的なネットワーク セキュリティを実現します。Cisco MDS 9000 ファミリ スイッチでは、IP ACL を使用して不明や送信元や信頼できない送信元からのトラフィックを制限し、ユーザ ID またはデバイス タイプに基づいてネットワークの使用を制限します。

IP ACL の設定手順については、第 5 章「IPv4 および IPv6 のアクセス コントロール リストの設定」を参照してください。

# PKI

公開キー インフラストラクチャ（PKI）は、MDS 9000 スイッチがネットワーク内のセキュアな通信を実現するためにデジタル証明書を取得し、使用することを可能にします。PKI のサポートにより、デジタル証明書をサポートする IP セキュリティ プロトコル（IPSec）、インターネット キー交換（IKE）、およびセキュア シェル（SSH）などのアプリケーションの管理機能およびスケーラビリティが実現します。

PKI の設定については、第 6 章「認証局およびデジタル証明書の設定」を参照してください。

# IPSec

IP Security（IPSec）プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供する、Internet Engineering Task Force（IETF）によるオープン規格のフレームワークです。IPSec は、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つまたは複数のデータ フローの保護など、IP レイヤにセキュリティ サービスを提供します。

IPSec の設定については、第 7 章「IPSec ネットワーク セキュリティの設定」を参照してください。

# FC-SP および DHCHAP

Fibre Channel Security Protocol（FC-SP）機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）は、Cisco MDS 9000 ファミリ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

FC-SP の使用により、スイッチ、ストレージ デバイス、およびホストは信頼性の高い管理可能な認証メカニズムを使ってそれぞれのアイデンティティを証明できます。FC-SP の使用により、ファイバ チャネル トラフィックをフレーム単位で保護することで、信頼できないリンクであってもスヌーピングやハイジャックを防止できます。ポリシーと管理アクションの一貫した組み合わせがファブリックを介して伝播されて、ファブリック全体での均一なレベルのセキュリティが実現します。

FS-SP および DHCHAP の詳細については、第 8 章「FC-SP および DHCHAP の設定」を参照してください。

# ポート セキュリティ

ポート セキュリティ機能は、1 つ以上の所定のスイッチ ポートへのアクセス権を持つ特定の World-Wide Name（WWN）をバインドすることによって、スイッチ ポートへの不正なアクセスを防止します。

スイッチ ポートでポート セキュリティをイネーブルにしている場合は、そのポートに接続するすべてのデバイスがポート セキュリティ データベースになければならず、所定のポートにバインドされているものとしてデータベースに記されている必要があります。これらの両方の基準を満たしていないと、ポートは動作上アクティブな状態にならず、ポートに接続しているデバイスは SAN へのアクセスを拒否されます。

ポート セキュリティの設定については、第 9 章「ポート セキュリティの設定」を参照してください。

# Fibre Channel Common Transport 管理サーバ クエリー

FC-CT クエリー管理機能により、管理者はストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログイン デバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーン セットの追加と削除の権限、ファブリックに接続するすべてのホストのホスト バス アダプタ（HBA）の詳細などがあります。

ファブリック バインディングの設定については、第 10 章「Fibre Channel Common Transport 管理セキュリティの設定」を参照してください。

# ファブリック バインディング

ファブリック バインディング機能では、ファブリック バインディング設定で指定したスイッチ間だけでスイッチ間リンク（ISL）をイネーブルにできます。この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されたりすることがなくなります。この機能では、Exchange Fabric Membership Data（EEMD）プロトコルを使用することによって、許可されたスイッチのリストがファブリック内の全スイッチで同一になります。

ファブリック バインディングの設定については、第 11 章「ファブリック バインディングの設定」を参照してください。

# TrustSec ファイバ チャネル リンク暗号化

Cisco TrustSec ファイバ チャネル リンク暗号化は、Fibre Channel-Security Protocol（FC-SP）の拡張機能であり、既存の FC-SP アーキテクチャを使用してトランザクションの整合性と機密保持を実現します。暗号化をピア認証に追加することにより、セキュリティを確保し、望ましくないトラフィック傍受を防止します。ピア認証は、Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）プロトコルを使用した FC-SP 標準に従って実装されます。

TrustSec ファイバ チャネル リンク暗号化については、第 12 章「Cisco TrustSec ファイバ チャネル リンク暗号化の設定」を参照してください。

# Cisco MDS 9000 シリーズ プラットフォームのオープン IP ポート

Cisco MDS 9000 シリーズ プラットフォームのデフォルト設定には、外部管理インターフェイスに開かれている IP ポートがあります。以下の表にオープン ポートと対応するサービスを示します。

*表 1-1　Cisco MDS 9000 シリーズ プラットフォームのオープン IP ポート*

| ポート番号 | IP プロトコル（UDP/TCP） | プラットフォーム | 機能/サービス名 | ランダム ポートかどうか |
|---|---|---|---|---|
| なし | UDP | すべて | — | — |
| 600 ～ 1024 | TCP | すべて | NFS | はい |
| 2002 | TCP | すべて | リモート パケット キャプチャ | いいえ |
| 7546 | TCP | すべて | IPv4 を介した CFS | いいえ |
| 9333 | TCP | すべて | クラスタ | いいえ |
| 32768 ～ 32769 | TCP | HP c-Class Blade System 用 Cisco MDS 8GB ファブリック スイッチ<br>Cisco MDS 9148<br>Cisco MDS 9222i<br>Cisco MDS 9506<br>Cisco MDS 9509<br>Cisco MDS 9513 | ライセンス マネージャ | はい |
| 44583 ～ 59121 | TCP | Cisco MDS 9148S<br>Cisco MDS 9250i<br>Cisco MDS 9706<br>Cisco MDS 9710 | ライセンス マネージャ | はい |

**NFS**：この範囲のポートがスイッチの NFS サービスで使用されます。これはスイッチ内でのみ使用されます。これらのポートとの間に外部アクセスを提供する必要はありません。この機能をディセーブルにできません。このサービスへのアクセスをブロックするには、ポートの範囲へのアクセスを拒否するように IP アクセス リストを設定します。詳細については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』の「Configuring IPv4 and IPv6 Access Control Lists」のセクションを参照してください。

**リモート パケット キャプチャ**：このポートはリモート キャプチャ プロトコル（RPCAP）を使用して、ホストの Ethereal プロトコル アナライザのクライアントとの通信に、スイッチのファイバ チャネル アナライザ サービスで使用されます。このサービスはトラブルシューティングに使用され、スイッチの通常の動作のオプションです。この機能をディセーブルにできません。このサービスへのアクセスをブロックするには、ポートの範囲へのアクセスを拒否するように IP アクセス リストを設定します。詳細については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』の「Configuring IPv4 and IPv6 Access Control Lists」のセクションを参照してください。

**IPv4 を介した CFS**：このポートは IPv4 サービスを介した CFS により使用され、ファブリック内のピア スイッチにスイッチ設定情報を配信します。CFS はスイッチがピアと通信するための重要なサービスですが、複数のトランスポート オプションが使用可能です。正しいトランスポートは、ファブリックの実装によって異なります。このポートは IPv4 サービスを介した CFS をディセーブルにすることによりクローズすることができます。詳細については、『Cisco MDS 9000 Family CLI Configuration Guide』の「Enabling CFS Over IP」のセクションを参照してください。

**クラスタ**：このポートはクラスタ内のピア スイッチと通信するクラスタ サービスにより使用されます。IOA および SME といった機能がこのサービスに依存しています。このような機能が使用されていない場合、クラスタ サービスはスイッチの動作に必要ではありません。このポートはクラスタ サービスをディセーブルにすることによりクローズすることができます。詳細については、『Cisco MDS 9000 Family Storage Media Encryption Configuration Guide』の「Enabling and Disabling Clustering」のセクションを参照してください。

**ライセンス マネージャ**：これらのポートは、License Manager サービスにより使用されます。これはスイッチ内でのみ使用されます。これらのポートとの間に外部アクセスを提供する必要はありません。この機能をディセーブルにできません。このサービスへのアクセスをブロックするには、ポートの範囲へのアクセスを拒否するように IP アクセス リストを設定します。詳細については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』の「Configuring IPv4 and IPv6 Access Control Lists」のセクションを参照してください。


# FIPS の設定

連邦情報処理標準規格（FIPS）140-2、*暗号モジュール セキュリティ要件*は、暗号モジュールに対する米国政府の要求条件を定義しています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

（注） Cisco MDS SAN-OS Release 3.1(1) および NX-OS Release 4.1(1b) 以降は FIPS に準拠して実装しており、現在のところ米国政府による認定途中にありますが、現時点では FIPS 準拠ではありません。

この章は、次の項で構成されています。



## 設定時の注意事項

FIPS モードをイネーブルにする前に次の注意事項を守ってください。

- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。ユーザのログインは SSH だけで行ってください。
- RADIUS/TACACS+ によるリモート認証をディセーブルにしてください。スイッチに対してローカルのユーザだけが認証可能です。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、スイッチ上の既存ユーザ アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- VRRP をディセーブルにしてください。
- 認証用 MD5 または暗号用 DES のいずれかを含む、すべての IKE ポリシーを削除してください。認証に SHA、暗号用に 3DES/AES を使用するようにポリシーを修正してください。
- SSH サーバの RSA1 キー ペアすべてを削除してください。

# FIPS モードのイネーブル化

FIPS モードを有効にするには、次の手順に従ってください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | コンフィギュレーション モードに入ります。 |
| ステップ 2 | `switch(config)# fips mode enable` | FIPS モードをイネーブルにします。 |
| | `switch(config)# no fips mode enable` | FIPS モードをディセーブルにします。 |

# FIPS ステータスの表示

FIPS のステータスを表示するには **show fips status** コマンドを入力します。

# FIPS セルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。

(注)　FIPS の電源投入時セルフテストは、**fips mode enable** コマンドを入力して FIPS モードがイネーブルにされていると自動的に実行されます。スイッチが FIPS モードに入るのは、すべてのセルフテストが正しく完了したときだけです。セルフテストのいずれかが失敗すると、スイッチは再起動します。

電源投入時セルフテストは、FIPS モードのイネーブル後、即時に実行されます。既知の解を使用する暗号アルゴリズム テストは、Cisco MDS 9000 ファミリ製品に実装されている FIPS 140-2 認定暗号アルゴリズムのそれぞれに対して、すべての暗号機能で実行されなければなりません。

既知解テスト(KAT)を利用すると、暗号アルゴリズムは正しい出力があらかじめわかってるデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト: このテストは公開キー/秘密キー ペアが生成されたときに実行されます。
- 乱数連続生成テスト: このテストは乱数が生成されたときに実行されます。

以上の両方はスイッチが FIPS モードに入っていると自動的に実行されます。


# ユーザ ロールおよび共通ロールの設定

CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して作成したロールは CLI を使用して変更でき、その逆も可能です。

CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、Fabric Manager や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章は、次の項で構成されています。



## 機能情報

このセクションには、リリースの新機能と更新機能が一時的にについて説明します。

*表 3-1　新機能および変更された機能*

| 機能 | リリース | 説明 |
|---|---|---|
| セキュア ログインの機能拡張 | 7.3(1)DY(1) | この機能により、サービス拒絶（DoS）攻撃と思われる攻撃が検出された場合、ログイン試行を自動的にブロックすることで、Cisco MDS スイッチのセキュリティを強化できます。 |

# ロール ベースの認証

Cisco MDS 9000 ファミリ スイッチはロールに基づいた認証を行います。ロールベースの認証は、ユーザをロール（役割）に割り当てることによってスイッチ操作へのアクセスを制限します。この種類の認証では、ユーザに割り当てられたロールに基づいて管理操作が制限されます。

ユーザがコマンドの実行、コマンドの完了、またはコンテキスト ヘルプの取得を行った場合、ユーザにそのコマンドへのアクセス権があると、スイッチ ソフトウェアによって処理の続行が許可されます。

この項では、次のトピックについて取り上げます。



## ロールの概要

ロールごとに複数のユーザを含めることができ、各ユーザは複数のロールに所属できます。たとえば、role1 ユーザにはコンフィギュレーション コマンドへのアクセスだけが、role2 ユーザには **debug** コマンドへのアクセスだけが許可されているとします。この場合、role1 と role2 の両方に所属しているユーザは、コンフィギュレーション コマンドと **debug** コマンドの両方にアクセスできます。

（注）　ユーザが複数のロールに所属している場合、各ロールで許可されているすべてのコマンドを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、TechDocs グループに属しているユーザが、コンフィギュレーション コマンドへのアクセスを拒否されているとします。ただし、このユーザはエンジニアリング グループにも属しており、コンフィギュレーション コマンドへのアクセス権を持っています。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

ヒント　ロールを作成した時点で、必要なコマンドへのアクセスが即時に許可されるわけではありません。管理者が各ロールに適切なルールを設定して、必要なコマンドへのアクセスを許可する必要があります。

## ロールとプロファイルの設定

追加ロールの作成または既存ロールのプロファイル修正を行うには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# role name techdocs`<br>`switch(config-role)#` | 指定したロール（techdocs）のモードを開始します。<br>(注)　ロール サブモード プロンプトは、ロールのサブモードを開始したことを示します。このサブモードは techdocs グループに固有です。 |
| | `switch(config)# no role name techdocs` | ロール techdocs を削除します。 |
| ステップ 3 | `switch(config-role)# description Entire Tech Docs group` | 新しいロールに記述を割り当てます。記述は 1 行に制限され、スペースを含めることができます。 |
| | `switch(config-role)# no description` | Tech Docs グループの記述をリセットします。 |

(注)　network-admin ロールに属するユーザだけがロールを作成できます。

# 各ロールのルールと機能の設定

各ロールに、最大 16 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。たとえば、ルール 1 のあとにルール 2 が適用され、ルール 3 以降が順に適用されます。network-admin ロールに属さないユーザは、ロールに関連したコマンドを実行できません。

たとえば、ユーザ A にすべての **show** コマンドの実行を許可されていても、ユーザ A が network-admin ロールに所属していないかぎり、ユーザ A は **show role** コマンドの出力を表示できません。

**rule** コマンドでは特定のロールで実行できる動作を指定します。ルールを構成する要素は、ルール番号、ルール タイプ（許可または拒否）、コマンド タイプ（**config**、**clear**、**show**、**exec**、**debug** など）、および任意の機能名（FSPF、ゾーン、VSAN、fcping、インターフェイスなど）です。

(注)　この場合、**exec** コマンドでは、**show**、**debug** および **clear** の各コマンドのカテゴリに含まれない、EXEC モード内のすべてのコマンドが対象になります。

デフォルトのロールがすべてのユーザに適用でき、設定済みロールが特定のユーザに適用できる場合、次のシナリオについて検討します。

- 同じルール タイプ（許可または拒否）：デフォルト ロールと特定のユーザに設定されているロールで同じルール タイプを使用する場合、特定のユーザはデフォルトと設定済みの両方のロールのすべてのルールにアクセスできます。

  デフォルト ロール **A** の場合、次のルールがあります。

  ```
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit config feature ssh
  rule 2 permit config feature ntp
  rule 1 permit config feature tacacs+
  ```

  特定のユーザにはロール **B** が割り当てられ、ルールは 1 つあります。

  ```
  rule 1 permit config feature dpvm
  ```

  特定のユーザは、**A** と **B** の両方のルールにアクセスできます。

- 異なるルール タイプ:デフォルト ロールと特定のユーザに設定されているロールで特定のルールのルール タイプが異なる場合、デフォルト ロールによって設定済みロールの競合するルール ステートメントが上書きされます。

  デフォルト ロール **A** の場合、次のルールがあります。

```
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp
rule 1 permit config feature tacacs+
```

  特定のユーザにはロール **B** が割り当てられ、ルールは 2 つあります。

```
rule 6 permit config feature dpvm
rule 2 deny config feature ntp
```

  **A** と **B** のルール 2 が競合します。この場合、**A** は **B** の競合するルールを上書きし、ユーザには、上書きルールを含む、**A** と **B** の残りのルールが割り当てられます。

```
rule 6 permit config feature dpvm
rule 5 permit show feature environment
rule 4 permit show feature hardware
rule 3 permit config feature ssh
rule 2 permit config feature ntp ----------> Overridden rule
rule 1 permit config feature tacacs+
```

## SAN-OS リリース 3.3(1c) および NX-OS リリース 4.2(1a) 間のルール変更によるロールの動作への影響

ロールに設定可能なルールは、SAN-OS リリース 3.3(1c) と NX-OS リリース 4.2(1a) 間で修正されています。その結果、SAN-OS リリース 3.3(1c) から NX-OS リリース 4.2(1a) にアップグレード後は、ロールが期待どおりに動作しません。必要な動作を復元するには手動での設定変更が必要です。

***ルール 4 およびルール 3***:アップグレード後、**exec** と **feature** が削除されます。次のようにルール 4 およびルール 3 を変更します。

| **SAN-OS リリース 3.3(1c) のルール** | **NX-OS リリース 4.2(1a) では、ルールを次のように設定します。** |
|---|---|
| rule 4 permit exec feature debug | rule 4 permit debug |
| rule 3 permit exec feature clear | rule 3 permit clear |

***ルール 2***:アップグレード後、**exec feature license** は廃止されます。

| **SAN-OS リリース 3.3(1c) のルール** | **NX-OS リリース 4.2(1a) のルール** |
|---|---|
| rule 2 permit exec feature debug | リリース 4.2(1) では使用できません。 |

***ルール 9、ルール 8 およびルール 7***:アップグレード後、設定するには、機能を有効にする必要があります。SAN-OS リリース 3.3(1c) では、有効にしなくてもこの機能を設定できます。

| SAN-OS リリース 3.3(1c) のルール | NX-OS リリース 4.2(1a) では、ルールを維持するには次のようにします。 |
|---|---|
| rule 9 deny config feature telnet | リリース 4.2(1) では使用できません。 |
| rule 8 deny config feature tacacs-server | アップグレード中に、機能を有効化してルールを維持します。そうしないと、ルールが消失します。 |
| rule 7 deny config feature tacacs+ | アップグレード中に、機能を有効化してルールを維持します。そうしないと、ルールが消失します。 |

## プロファイルの変更

既存ロールのプロファイルを変更するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# role name sangroup`<br>`switch(config-role)#` | 既存のロール sangroup のロール コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config-role)# rule 1 permit config`<br>`switch(config-role)# rule 2 deny config feature fspf`<br>`switch(config-role)# rule 3 permit debug feature zone`<br>`switch(config-role)# rule 4 permit exec feature fcping` | sangroup ロールに属すユーザが、**fspf config** コマンドを除くすべてのコンフィギュレーション コマンドを実行できるようにします。これらのユーザは、**zone debug** コマンドおよび **fcping** EXEC モード コマンドも実行できます。 |
| ステップ 4 | `switch(config-role)# no rule 4` | ルール 4 を削除し、sangroup が **fcping** コマンドを実行できないようにします。 |

ステップ 3 で、ルール 1 が最初に適用され、sangroup ユーザがすべての **config** コマンドにアクセスすることが許可されます。次にルール 2 が適用され、sangroup ユーザには FSPF 設定が拒否されます。結果として、sangroup ユーザは **fspf** コンフィギュレーション コマンドを除く、他のすべての **config** コマンドを実行できます。

**(注)** ルールは適用する順序が重要です。これらの 2 つのルールを入れ替え、**deny config feature fspf** ルールを最初に置き、次に **permit config** ルールを置いた場合は、2 番めのルールがグローバルに効果を持って最初のルールに優先するため、sangroup ユーザの全員にすべてのコンフィギュレーション コマンドの実行を許可することになります。

# VSAN ポリシーの設定

VSAN ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください）。

選択した VSAN セットだけにタスクの実行が許可されるように、ロールを設定できます。デフォルトでは、どのロールの VSAN ポリシーも許可に設定されているため、すべての VSAN に対してタスクが実行されます。選択した VSAN セットだけにタスクの実行が許可されるロールを設定できます。1 つのロールに対して選択的に VSAN を許可するには、VSAN ポリシーを拒否に設定し、あとでその設定を許可に設定するか、または適切な VSAN を設定します。

（注）　VSAN ポリシーが拒否に設定されているロールに設定されているユーザは、E ポートの設定を変更できません。これらのユーザが変更できるのは、（ルールの内容に応じて）F ポートまたは FL ポートの設定だけです。これにより、これらのユーザは、ファブリックのコア トポロジに影響する可能性のある設定を変更できなくなります。

ヒント　ロールを使用して、VSAN 管理者を作成できます。設定したルールに応じて、これらの VSAN 管理者は他の VSAN に影響を与えることなく、VSAN に MDS 機能（ゾーン、fcdomain、VSAN プロパティなど）を設定できます。また、ロールが複数の VSAN での処理を許可している場合、VSAN 管理者はこれらの VSAN 間で F ポートまたは FL ポートのメンバーシップを変更できます。

VSAN ポリシーが拒否に設定されているロールに属すユーザのことを、VSAN 制限付きユーザと呼びます。

## VSAN ポリシーの変更

（注）　NX-OS リリース 4.x 以降では、VSAN の適用は、非 show コマンドに対してのみ実行されます。show コマンドは除外されます。

（注）　SAN-OS リリース 3.x 以前では、VSAN の適用は非 show コマンドに対して実行されますが、すべての show コマンドが適用されるわけではありません。

既存ロールの VSAN ポリシーを変更するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# role name sangroup`<br>`switch(config-role)#` | sangroup ロールのロール コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config)# vsan policy deny`<br>`switch(config-role-vsan)` | このロールの VSAN ポリシーを **deny** に変更し、VSAN を選択的に許可できるサブモードを開始します。 |
| | `switch(config-role)# no vsan policy deny` | 設定されている VSAN ロール ポリシーを削除し、工場出荷時のデフォルト（**permit**）に戻します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | `switch(config-role-vsan)# permit vsan 10-30` | このロールが、VSAN 10 ～ 30 に許可されたコマンドを実行できるようにします。 |
| | `switch(config-role-vsan)# no permit vsan 15-20` | このロールの権限を、VSAN 15 ～ 20 のコマンドの実行について除外します。したがって、このロールは、VSAN 10 ～ 14、および 21 ～ 30 でコマンドを実行できることになります。 |

# ロールの配信

ロールベース設定は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的なデータベース管理を可能にし、ファブリック全体に対するシングル ポイントでの設定を提供します。

次の設定が配信されます。

- ロール名と説明
- ロールに対するルールのリスト
- VSAN ポリシーと許可されている VSAN のリスト

この項では、次のトピックについて取り上げます。


- ロール データベースの概要（3-37 ページ）
- ファブリックのロック（3-38 ページ）
- ロールベース設定変更のコミット（3-38 ページ）
- ロールベース設定変更の廃棄（3-38 ページ）
- ロールベース設定の配布のイネーブル化（3-39 ページ）
- セッションのクリア（3-39 ページ）
- データベース マージに関する注意事項（3-39 ページ）
- ロールベース情報の表示（3-39 ページ）
- 配信がイネーブルの場合のロールの表示（3-42 ページ）


## ロール データベースの概要

ロールベース設定は 2 つのデータベースを利用して設定内容の受け取りと実装を行います。

- コンフィギュレーション データベース：ファブリックで現在実行されているデータベースです。
- 保留中のデータベース：以降の設定変更は保留中のデータベースに保存されます。設定を修正した場合は、保留中のデータベースの変更内容をコンフィギュレーション データベースにコミットするかまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、その変更をコミットするまでコンフィギュレーション データベースに反映されません。

（注）　お客様に「syslog"%VSHD-4-VSHD_ROLE_DATABASE_OUT_OF_SYNC"」が発生するとすぐに、ロール コンフィギュレーション データベースがマージ時にスイッチ間で異なることが検出されます。ファブリック内のすべてのスイッチで、ロール コンフィギュレーション データベースを一致させることを推奨します。いずれかのスイッチで設定を編集し、目的のロール コンフィギュレーション データベースを取得してからコミットします。

# ファブリックのロック

データベースを修正する最初のアクションで保留中のデータベースが作成され、ファブリック全体の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースの複製が、最初の変更とともに保留中のデータベースになります。

# ロールベース設定変更のコミット

保留中のデータベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、保留中のデータベースは消去されます。

ロールベースの設定変更をコミットするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# role commit vsan 3` | ロールベースの設定変更をコミットします。 |

# ロールベース設定変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

ロールベースの設定変更を廃棄するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# role abort` | ロールベースの設定変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。 |

# ロールベース設定の配布のイネーブル化

ロールベース設定の配信をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# role distribute` | ロールベース設定の配信をイネーブルにします。 |
| | `switch(config)# no role distribute` | ロールベース設定の配信をディセーブルにします(デフォルト)。 |

# セッションのクリア

ファブリック内の既存のロール セッションを強制的にクリアするには、開始されたセッションに参加中のスイッチから **clear role session** コマンドを発行します。

**注意**　このコマンドを発行すると、保留中のデータベース内のすべての変更が失われます。

```
switch# clear role session
```

# データベース マージに関する注意事項

ファブリックのマージではスイッチ上のロール データベースは変更されません。2 つのファブリックをマージし、それらのファブリックが異なるロール データベースを持つ場合は、ソフトウェアがアラート メッセージを発します。

- ファブリック全体のすべてのスイッチでロール データベースが同一であることを確認してください。
- 必ず目的のデータベースになるように任意のスイッチのロール データベースを編集してから、コミットしてください。これによりファブリック内のすべてのスイッチ上のロール データベースの同期が保たれます。

# ロールベース情報の表示

スイッチに設定されたルールを表示するには、**show role** コマンドを使用します。ルールはルール番号別、およびそれぞれのロールに基づいて表示されます。ロール名を指定しなかった場合はすべてのロールが表示されます。例 3-1 を参照してください。

***例 3-1　すべてのロールに関する情報の表示***

```
switch# show role
Role: network-admin
  Description: Predefined Network Admin group. This role cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  clear           *
```

```
  2       permit  config          *
  3       permit  debug           *
  4       permit  exec            *
  5       permit  show            *

Role: network-operator
  Description: Predefined Network Operator group. This role cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *(excluding show running-config, show startup-config)
  2       permit  exec            copy licenses
  3       permit  exec            dir
  4       permit  exec            ssh
  5       permit  exec            terminal
  6       permit  config          username

Role: server-admin
  Description: Predefined system role for server administrators. This role
  cannot be modified.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  exec            install

Role: priv-15
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  config          *
  3       permit  clear           *
  4       permit  debug           *
  5       permit  exec            *

Role: priv-14
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-13
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-12
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-11
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-10
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-9
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
```

```
Role: priv-8
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-7
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-6
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-5
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-4
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-3
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-2
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-1
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)

Role: priv-0
  Description: This is a system defined privilege role.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            *
  2       permit  exec            enable
  3       permit  exec            ssh
  4       permit  exec            ping
  5       permit  exec            telnet
  6       permit  exec            traceroute

Role: default-role
  Description: This is a system defined role and applies to all users.
  Vsan policy: permit (default)
  ----------------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------------
  1       permit  show            system
  2       permit  show            snmp
  3       permit  show            module
  4       permit  show            hardware
  5       permit  show            environment
```

# 配信がイネーブルの場合のロールの表示

コンフィギュレーション データベースを表示するには、**show role** コマンドを使用します。

配信がロール設定に対してイネーブルかどうか、現在のファブリック ステータス（ロックまたはロック解除）、および最後に実行された動作を表示するには、**show role status** コマンドを使用します。例 3-2 を参照してください。

***例 3-2　ロール ステータス情報の表示***

```
switch# show role status
Distribution: Enabled
Session State: Locked

Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

保留中のロール データベースを表示するには、**show role pending** コマンドを使用します。

例 3-3 は、この手順に従って **show role pending** コマンドを実行した出力を示しています。

1. **role name myrole** コマンドを使用して `myrole` というロールを作成します。
2. **rule 1 permit config feature fspf** コマンドを入力します。
3. **show role pending** コマンドを入力して、出力を表示します。

***例 3-3　保留中のロール データベース情報の表示***

```
switch# show role pending
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands

Role: TechDocs
  vsan policy: permit (default)

Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule     Type    Command-type      Feature
  ----------------------------------------------
    1.   permit     config                  *
    2.     deny     config               fspf
    3.   permit      debug               zone
    4.   permit       exec             fcping
```

```
Role: myrole
  vsan policy: permit (default)
  ----------------------------------------------
  Rule     Type     Command-type       Feature
  ----------------------------------------------
    1.    permit     config                 fspf
```

保留中のロール データベースとコンフィギュレーションのロール データベースの相違を表示するには、**show role pending-diff** コマンドを使用します。例 3-4 を参照してください。

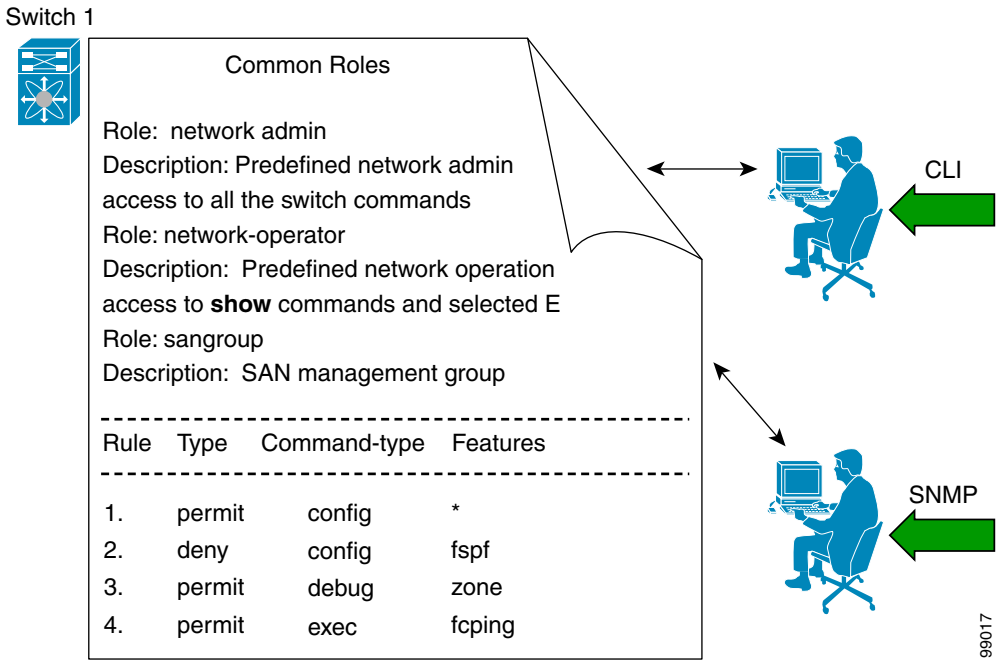
*例 3-4　2 つのデータベースの相違の表示*

```
switch# show role pending-diff
    +Role: myrole
    +  vsan policy: permit (default)
    +  ----------------------------------------------
    +  Rule     Type     Command-type       Feature
    +  ----------------------------------------------
    +    1.    permit     config                 fspf
```

# 共通ロールの設定

Cisco MDS 9000 ファミリのすべてのスイッチで、CLI と SNMP は共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます（図 3-1 を参照）。

*図 3-1　　共通ロール*



ネットワーク管理者権限を持つカスタム ロールのユーザは、他のユーザのアカウントの変更に制限されます。ただし、管理者だけはすべてのユーザ アカウントを変更できます。

ユーザ権限を変更するには、次のタスクを実行します。

1. コンソール認証を使用してロールを変更します。

コンソール認証を 'local' に設定している場合は、ローカル管理者ユーザでログオンし、ユーザを変更します。

2. リモート認証を使用してロールを変更します。

リモート認証をオフにします。ローカル管理者権限でログオンし、ユーザを変更します。リモート認証をオンにします。

3. LDAP/AAA を使用してロールを変更します。

LDAP/AAA でグループを作成し、このグループの名前をネットワーク管理者に変更します。必要なユーザをこのグループに追加します。このグループのユーザに完全なネットワーク管理者権限が付与されました。

SNMP の各ロールは、CLI を通じて作成または変更されたロールと同じです（「ロール ベースの認証」セクション（3-32 ページ）を参照）。

各ロールは、必要に応じて 1 つ以上の VSAN に制限できます。

SNMP または CLI を使用して、新しいロールの作成、または既存のロールの変更を実行できます。

- SNMP：CISCO-COMMON-ROLES-MIB を使用してロールを設定または変更します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。
- CLI：**role name** コマンドを使用します。

# CLI オペレーションから SNMP へのマッピング

SNMP では、GET、SET、および NOTIFY の 3 つの操作だけを行うことができます。CLI では、DEBUG、SHOW、CONFIG、CLEAR、および EXEC の 5 つの操作を行うことができます。

（注）　NOTIFY には、CLI の syslog メッセージのような制限はありません。

表 3-2 は、CLI オペレーションが SNMP オペレーションにどのようにマッピングされるかを示します。

***表 3-2　CLI オペレーションから SNMP オペレーションへのマッピング***

| CLI オペレーション | SNMP オペレーション |
|---|---|
| DEBUG | Ignored |
| SHOW | GET |
| CONFIG | SET |
| CLEAR | SET |
| EXEC | SET |

例 3-5 に、my_role という名前のロールの CLI 操作を SNMP 操作へマッピングする特権およびルールを示します。

*例 3-5　CLI 操作から SNMP 操作へのマッピングの表示*

```
switch# show role name my_role
Role:my_role
  vsan policy:permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit     clear                *
    2.     deny     clear              ntp
    3.   permit    config               *
    4.     deny    config              ntp
    5.   permit     debug                *
    6.     deny     debug              ntp
    7.   permit      show                *
    8.     deny      show              ntp
    9.   permit      exec                *
```

（注）　ルール 4 では、CONFIG は NTP では拒否されますが、ルール 9 によって、NTP MIB オブジェクトに対する SET は許可されます。これは、EXEC も SNMP SET 操作にマッピングされているためです。

# ユーザ アカウントの設定

Cisco MDS 9000 ファミリ スイッチでは、すべてのユーザのアカウント情報がシステムに保管されます。ユーザの認証情報、ユーザ名、ユーザ パスワード、パスワードの有効期限、およびロール メンバーシップが、そのユーザのユーザ プロファイルに保存されます。

ここで説明するタスクを利用すると、ユーザの作成および既存ユーザのプロファイルの修正を実行できます。これらのタスクは管理者によって定義されている特権ユーザに制限されます。

この項では、次のトピックについて取り上げます。

- ユーザの作成に関する注意事項（3-45 ページ）
- ユーザの設定（3-47 ページ）
- ユーザのログアウト（3-48 ページ）
- ユーザ アカウント情報の表示（3-48 ページ）

## ユーザの作成に関する注意事項

**snmp-server user** オプションで指定したパスフレーズと **username** オプションで指定したパスワードは同期されます。

デフォルトでは、明示的に期限を指定しないかぎり、ユーザ アカウントは無期限に有効です。**expire** オプションを使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。日付は YYYY-MM-DD 形式で指定します。

ユーザを作成する際、次の点に注意してください。

- 1 つのスイッチには、最大 256 ユーザを設定できます。
- bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、sys は予約語で、ユーザの設定には使用できません。
- ユーザ パスワードはスイッチ コンフィギュレーション ファイルに表示されません。
- パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。「admin」は Cisco MDS 9000 ファミリ スイッチのデフォルト パスワードではなくなりました。強力なパスワードを明確に設定する必要があります。
- トラブルシューティングのために **internal** キーワードを指定してコマンドを発行するには、network-admin グループのメンバーであるアカウントが必要です。

**注意**　Cisco MDS NX-OS では、ユーザ名がアルファベットで始まる限り、リモートで作成するか（TACACS+ または RADIUS を使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+ [プラス]、= [等号]、_ [下線]、- [ハイフン]、\ [バックスラッシュ]、および . [ピリオド]）を使って作成したユーザ名がサポートされます。特殊文字（指定された特殊文字を除く）を使用してローカル ユーザ名を作成することはできません。サポートされていない特殊文字によるユーザ名が AAA サーバに存在し、ログイン時に入力されると、そのユーザはアクセスを拒否されます。

## パスワード強度の確認

設定したパスワードの強度を確認できます。

パスワードのチェックをイネーブルにした場合、Cisco NX-OS ソフトウェアで作成できるのは強力なパスワードだけです。

パスワードの強度の確認をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# password strength-check` | パスワード チェックをイネーブルにします（デフォルト）。 |
| ステップ 3 | `switch(config)# no password strength-check` | パスワード チェックをディセーブルにします。 |

## 強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（"abcd" など）を含んでいない
- 複数の同じ文字の繰り返し（"aaabbb" など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字と小文字の両方を含んでいない。
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

# ユーザの設定

新規ユーザの設定または既存ユーザのプロファイル修正を行うには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# username usam password abcd123AAA expire 2003-05-31` | ユーザ アカウント（usam）を作成または更新し、パスワード（abcd123AAA）および有効期限 2003-05-31 を設定します。 |
| | `switch(config)# username msam password 0 abcd12AAA role network-operator` | ユーザ アカウント（msam）を作成または更新し、クリア テキスト（0 で示される）のパスワード（abcd12AAA）を指定します。パスワードの長さは 64 文字に制限されています。 |
| | `switch(config)# username user1 password 5 $1$UgOR6Xqb$z.HZlMk.ZGr9VH67a` | ユーザ アカウント（user1）に暗号化（5 で指定される）パスワード（!@*asdsfsdfjh!@df）を指定します。<br>(注)　ユーザが暗号化パスワード オプションを指定して作成された場合、対応する SNMP ユーザは作成されません。 |
| ステップ 3 | `switch(config)# username usam role network-admin` | network-admin ロールに指定のユーザ（usam）を追加します。 |
| | `switch(config)# no username usam role vsan-admin` | vsan-admin ロールから指定のユーザ（usam）を削除します。 |
| ステップ 4 | `switch(config)# username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSI YZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8d veqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=` | 既存のユーザ アカウント（admin）の SSH キーを指定します。 |
| | `switch(config)# no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSI YZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8d veqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=` | ユーザ アカウント（admin）の SSH キーを削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | `switch(config)# username usam ssh-cert-dn usam-dn dsa` | 既存のユーザ アカウント（usam）の認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。 |
| | `switch(config)# username user1 ssh-cert-dn user1-dn rsa` | 既存のユーザ アカウント（user1）の認証に使用する SSH X.509 証明書の識別名と RSA アルゴリズムを指定します。 |
| | `switch(config)# no username admin ssh-cert-dn admin-dn dsa` | ユーザ アカウント（admin）の SSH X.509 証明書の識別名を削除します。 |

# ユーザのログアウト

スイッチの他のユーザをログアウトするには、**clear user** コマンドを使用します。

次の例では、vsam という名前のユーザが、スイッチからログアウトされます。

```
switch# clear user vsam
```

ログインしているユーザのリストを表示するには、**show users** コマンドを使用します（例 3-6 を参照）。

***例 3-6　ログインしているすべてのユーザの表示***

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (user.example.com)
admin    pts/10       Jan 13 03:05 (dhcp-10-10-1-1.example.com)
admin    pts/11       Jan 13 01:53 (dhcp-10-10-2-2.example.com)
```

# ユーザ アカウント情報の表示

ユーザ アカウントに関して設定されている情報を表示するには、**show user-account** コマンドを使用します。例 3-7 ～ 3-8 を参照してください。

***例 3-7　指定したユーザに関する情報の表示***

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

***例 3-8　すべてのユーザに関する情報の表示***

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
```

```
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

# セキュア ログインの機能拡張

Cisco MDS 9000 シリーズ スイッチでは、次の安全なログイン拡張機能がサポートされています。

- ログイン パラメータの設定（3-49 ページ）
- ユーザごとのログイン ブロックの設定（3-51 ページ）
- ユーザ 1 人あたりのセッション数の制限（ユーザ 1 人あたり、ログイン 1 回あたり）（3-52 ページ）
- パスフレーズの設定とユーザ アカウントのロック（3-53 ページ）
- ユーザ名のパスワード プロンプトの有効化（3-54 ページ）
- OS の整合性を確認するための SHA-256 アルゴリズムのサポート（3-55 ページ）
- RADIUS/TACACS+ を使用するための共有キー値の設定（3-55 ページ）

## ログイン パラメータの設定

Cisco MDS 9000 デバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

すべてのログイン パラメータは、デフォルトではディセーブルです。他のログイン コマンドを使用する前に **login block-for** コマンドを入力してデフォルトのログイン機能をイネーブルにする必要があります。**login block-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**login quiet-mode access-class** コマンドが入力されるまで、ACL はログイン時間から除外されません。

ログイン パラメータを設定するには、次の手順を実行します。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　Cisco MDS 9000 デバイスで DoS の検出に役立つログイン パラメータを設定します。

```
switch(config)# system login block-for seconds attempts tries within seconds
```

（注）　このコマンドは、その他のログイン コマンドの前に発行する必要があります。

**ステップ 3**　(任意) このコマンドはオプションですが、デバイスが静音モードに切り替わるときにデバイスに適用される ACL を指定するように設定することを推奨します。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。

```
switch(config)# system login quiet-mode access-class {acl-name | acl-number}
```

**ステップ 4**　特権 EXEC モードに戻ります。

```
switch(config)# exit
```

**ステップ 5**　ログイン パラメータを表示します。

```
switch# show system login
```

**ステップ 6**　失敗したログイン試行に関連する情報のみを表示します。

```
switch# show system login failures
```

---

*例 3-9　ログイン パラメータの設定*

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
switch(config)# system login block-for 100 attempts 15 within 100
switch(config)# system login quiet-mode access-class myacl
```

*例 3-10　デフォルトの ACL を表示*

以下は、**show ip access-list sl_def_acl** コマンドの出力例であり、デフォルトの ACL を表示します。

```
switch(config)# show ip access-list sl_def_acl
ip access-list sl_def_acl
permit tcp any any established (0 matches)
deny tcp any any eq port telnet (0 matches)
deny tcp any any eq port www (0 matches)
deny tcp any any eq port ssh (0 matches)
permit ip any any (0 matches)
```

*例 3-11　ログイン パラメータなしの確認*

**show system login** コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
switch# show system login
No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
 If more than 2 login failures occur in 20 seconds or less,
logins will be disabled for 60 seconds.

Switch presently in Quiet-Mode.

Will remain in Quiet-Mode for 43 seconds.

Denying logins from all sources.
```

*例 3-12 失敗したログイン試行に関する情報の表示*

**show system login failures** コマンドからの次のサンプル出力は、スイッチ上で失敗したすべてのログイン試行を表示します。

```
switch# show system login failures
Information about last 20 login failure's with the device.
--------------------------------------------------------------------------------
---------------
-
Username                                Line     Source          Appname         TimeStamp
--------------------------------------------------------------------------------
---------------
-
--------------------------------------------------------------------------------
---------------
-
lock4                                   pts/1    192.0.2.2  login           Thu Feb 16
14:36:12 2017
as                                      pts/1    192.0.2.2   login           Thu Feb 16
14:36:16 2017
as                                      pts/1    192.0.2.2  login           Thu Feb 16
14:36:20 2017
```

# ユーザごとのログイン ブロックの設定

ユーザごとのログイン ブロック機能を使用すると、Denial of Service（DoS）攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカル ユーザのみに適用されます。ログインに失敗したユーザをブロックするようにログイン パラメータを設定するには、ここに示す手順を実行します。

ユーザごとのログイン ブロックを設定するには、次の手順を実行します。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　ユーザをブロックするようにログイン パラメータを設定します。

```
switch(config)# aaa authentication rejected attempts in seconds ban seconds
```

**（注）**　デフォルトのログイン パラメータに戻すには **no aaa authentication rejected** コマンドを使用します。

**ステップ 3**　特権 EXEC モードに戻ります。

```
switch(config)# exit
```

**ステップ 4**　ログイン パラメータを表示します。

```
switch# show system login
```

**ステップ 5**　ブロックされたローカル ユーザを表示します。

```
switch# show aaa local user blocked
```

**ステップ 6**　ブロック済みローカル ユーザのクリア:

```
switch# clear aaa local user blocked {username user | all}
```

*例 3-13　ユーザごとのログイン ブロックの設定*

次に、60 秒の間に 5 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch# aaa authentication rejected 5 in 60 ban 3
```

*例 3-14　ログイン パラメータの表示*

次に、スイッチで設定されているログイン パラメータを表示する例を示します。

```
switch# show run | i rejected
aaa authentication rejected 5 in 60 ban 300
```

*例 3-15　ブロックされたローカル ユーザの表示*

次に、ブロック済みローカル ユーザを表示する例を示します。

```
switch# show aaa local user blocked
Local-user                  State

testuser                    Watched (till 11:34:42 IST Feb 5 2015)
```

*例 3-16　ブロック済みローカル ユーザのクリア*

次に、ブロック済みローカル ユーザ testuser をクリアする例を示します。

```
switch# clear aaa local user blocked username testuser
```

# ユーザ 1 人あたりのセッション数の制限（ユーザ 1 人あたり、ログイン 1 回あたり）

ユーザごとの最大セッション数を制限するには、次の手順に従います。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　ユーザごとの最大セッション数を制限します。指定できる範囲は 1 ～ 7 です。最大ログイン制限を 1 に設定すると、ユーザ 1 人あたりのセッション数（telnet/SSH）が 1 つに制限されます。

```
switch(config)# user max-logins max-logins
```

**ステップ 3**　特権 EXEC モードに戻ります。

```
switch(config)# exit
```

*例 3-17　ユーザごとのセッション数を制限します*

次に、単一のユーザのログインの最大回数を 1 セッションに設定する例を示します。

```
switch# user max-logins 1
```

# パスフレーズの設定とユーザ アカウントのロック

パスフレーズの長さ、有効期間、およびユーザ アカウント ロック機能を設定するには、ここに示す手順を実行します。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　パスフレーズの最小長または最大長のいずれかを設定します。

```
switch(config)# userpassphrase {min-length min_value | max-length max_value}
```

**ステップ 3**　最小、最大、または完全パスフレーズ長の設定が表示されます。

```
switch# show userpassphrase {min-length | max-length | length}
```

**ステップ 4**　任意のユーザに対してパスフレーズの有効期間を設定できます。

```
switch(config)# username user passphrase {lifetime | warntime | gracetime}
```

**ステップ 5**　(オプション)デフォルトの設定を更新します。

```
switch(config)# userpassphrase {default-lifetime | default-warntime | default-gracetime |
min-length min_value | max-length max_value}
```

**ステップ 6**　任意のユーザのパスフレーズの有効期間を表示します。

```
switch# show username user passphrase timevalues
```

**ステップ 7**　任意のユーザ アカウントをロックします。

```
switch(config)# username user lock-user-account
```

**ステップ 8**　任意のユーザ パスフレーズの有効期限を設定します。

```
switch(config)# username user expire-userpassphrase
```

**ステップ 9**　すべてのロックされたユーザを表示します。

```
switch(config)# show locked-users
```

*例 3-18　最大および最小パスフレーズ長の設定*

次の例では、最小パスフレーズ長を 8、最大パスフレーズ長を 80 として設定する方法を示します。

```
switch(config)# userpassphrase min-length 8 max-length 80
```

*例 3-19　最小パスフレーズ長の表示*

次の例では、最小パスフレーズ長を示します。

```
switch(config)# show userpassphrase min-length
Minimum passphrase length : 8
```

*例 3-20　ユーザのパスフレーズの有効期間を設定します。*

次の例では、ユーザのパスフレーズの有効期間を設定する方法を示しています。

```
switch(config)# username user1 passphrase lifetime 10
```

*例 3-21　ユーザのパスフレーズの有効期間を表示します。*

次の例では、ユーザのパスフレーズの有効期間を設定する方法を示しています。

```
switch(config)# show username user1 passphrase timevalues
Last passphrase change(Y-M-D):  2017-02-06
Passphrase lifetime:            99999 days after last passphrase change
Passphrase warning time starts: 7 days before passphrase lifetime
Passphrase Gracetime ends:      never
```

*例 3-22　ユーザ アカウントのロック*

次の例では、ユーザ アカウントをロックする方法を示します。

```
switch(config)# username user1 lock-user-account
```

*例 3-23　ユーザ パスフレーズの有効期限の設定*

次の例では、ユーザ アカウントをロックする方法を示します。

```
switch(config)# username user1 expire-userpassphrase
```

*例 3-24　ロックされたユーザを表示します。*

次の例では、ロックされているすべてのユーザを示します。

```
switch(config)# show locked-users
```

# ユーザ名のパスワード プロンプトの有効化

ユーザ名のパスワード プロンプトを有効にするには、次の手順を実行します。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　ログイン パスワード入力要求をイネーブルにします。このコマンドがイネーブルになっている場合、ユーザが **username** コマンドを *password* オプションなしで入力すると、パスワードを入力するよう求められます。パスワードの入力には隠し文字を使用できます。ログイン パスワード入力要求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。

```
switch(config)# password prompt username
```

**ステップ 3**　特権 EXEC モードに戻ります。

```
switch(config)# exit
```

# OS の整合性を確認するための SHA-256 アルゴリズムのサポート

**show file bootflash:/ sha256sum** コマンドを使用して、ファイルの sha256sum を表示します。このコマンドのサンプル出力を次に示します。

```
switch# show file bootflash:/ sha256sum

abd9d40020538acc363df3d1bae7d1df16841e4903fca2c07c7898bf4f549ef5
```

# RADIUS/TACACS+ を使用するための共有キー値の設定

リモート認証およびアカウンティング用に設定する共有秘密は非表示にする必要があります。**radius-server key** および **tacacs-server key** コマンドでは、別のコマンドを使用して暗号化された共有秘密を使用できます。

RADIUS/TACACS+ を使用するための共有キー値を設定するには、次の手順を実行します。

**ステップ 1**　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。

```
switch# configure terminal
```

**ステップ 2**　キー タイプ 7 で RADIUS および TACACS の共有秘密を設定します。暗号化された共有秘密を生成する間はユーザ入力が非表示になります。

```
switch(config)# generate type7_encrypted_secret
```

**（注）**　プレーン テキストから暗号化された文字列を別個に生成して、暗号化された共有秘密を後から設定することもできます。

**ステップ 3**　特権 EXEC モードに戻ります。

```
switch(config)# exit
```

# SSH の設定

RSA キーによるセキュア SSH 接続は、Cisco MDS 9000 ファミリのすべてのスイッチでデフォルトで使用できます。DSA キーによるセキュア SSH 接続が必要な場合は、デフォルトの SSH 接続をディセーブルにし、DSA キーを生成して、SSH 接続をイネーブルにする必要があります（「SSH サーバ キー ペアの生成」セクション（3-56 ページ）を参照）。

サーバ キーを生成するには、**ssh key** コマンドを使用します。

**注意**　SSH でスイッチにログインし、**aaa authentication login default none** コマンドを発行した場合、ログインするために 1 つ以上のキーストロークを入力する必要があります。少なくとも 1 つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

ここで説明する内容は、次のとおりです。



# SSH の概要

SSH は Cisco NX-OS CLI にセキュアなコミュニケーションを提供します。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, Adelman（RSA）を使用する SSH2
- DSA を使用する SSH2

# SSH サーバ キー ペアの生成

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用中の SSH クライアント バージョンに従って、SSH サーバ キー ペアを生成します。各キー ペアに指定するビット数は、768 ～ 2048 です。

SSH サービスは、SSH バージョン 2 で使用する 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。

**注意**　SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

SSH サーバ キー ペアを生成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ssh key dsa 1024`<br>`generating dsa key.....`<br>`generated dsa key` | DSA サーバ キー ペアを生成します。 |
| | `switch(config)# ssh key rsa 1024`<br>`generating rsa key.....`<br>`generated rsa key` | RSA サーバ キー ペアを生成します。 |
| | `switch(config)# no ssh key rsa 1024`<br>`cleared RSA keys` | RSA サーバ キーペアの設定をクリアします。 |

# SSH キーの指定

SSH キーを指定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH キーは次の 3 種類の形式で指定できます。

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

指定したユーザの OpenSSH 形式の SSH キーを指定または削除するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ315RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=` | ユーザ アカウント（admin）の SSH キーを指定します。 |
| | `switch(config)# no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ315RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=` | ユーザ アカウント（admin）の SSH キーを削除します。 |

指定したユーザの IETF SECSH 形式の SSH キーを指定または削除するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub` | IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。 |
| ステップ 2 | `switch# config t`<br>`switch(config)#` | コンフィギュレーション モードに入ります。 |
| ステップ 3 | `switch(config)# username admin sshkey file bootflash:secsh_file.pub` | ユーザ アカウント（admin）の SSH キーを指定します。 |
| | `switch(config)# no username admin sshkey file bootflash:secsh_file.pub` | ユーザ アカウント（admin）の SSH キーを削除します。 |

指定したユーザの PEM フォーマット化された公開キー証明書形式の SSH キーを指定または削除するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem` | PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。 |
| ステップ 2 | `switch# config t`<br>`switch(config)#` | コンフィギュレーション モードに入ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | `switch(config)# username admin sshkey file bootflash:cert.pem` | ユーザ アカウント(usam)の SSH キーを指定します。 |
| | `switch(config)# no username admin sshkey file bootflash:cert.pem` | ユーザ アカウント(usam)の SSH キーを削除します。 |

# 生成したキー ペアの上書き

必要なバージョンの SSH キー ペア オプションがすでに生成されている場合は、前回生成されたキー ペアをスイッチに上書きさせることができます。

前回生成されたキー ペアを上書きする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ssh key dsa 768`<br>`ssh key dsa 512`<br>`dsa keys already present, use force`<br>`option to overwrite them`<br>`switch(config)# ssh key dsa 512 force`<br>`deleting old dsa key.....`<br>`generating dsa key.....`<br>`generated dsa key` | サーバ キー ペアの設定を試みます。必要なサーバ キー ペアがすでに設定されている場合は、**force** オプションを使用して、そのサーバ キーペアを上書きします。<br>古い DSA キーを削除し、新しく指定されたビットを使用してサーバ キー ペアを設定します。 |

# SSH ホストのクリア

**clear ssh hosts** コマンドは、信頼できる SSH ホストの既存のリストをクリアし、SCP/SFTP を特定のホストの **copy** コマンドとともに使用することを再許可します。

SCP/SFTP を **copy** コマンドとともに使用する場合は、信頼できる SSH ホストのリストが作成され、スイッチ内に保存されます(例 3-25 を参照)。

***例 3-25　SCP/SFTP を使用したファイルのコピー***

```
switch# copy scp://abcd@10.10.1.1/users/abcd/abc
bootflash:abc The authenticity of host '10.10.1.1 (10.10.1.1)'
can't be established.
RSA1 key fingerprint is 01:29:62:16:33:ff:f7:dc:cc:af:aa:20:f8:20:a2:db.
Are you sure you want to continue connecting (yes/no)? yes
Added the host to the list of known hosts
(/var/home/admin/.ssh/known_hosts). [SSH key information about the host is
stored on the switch]
abcd@10.10.1.1's password:
switch#
```

**copy** コマンドとともに SCP/SFTP を使用する前にホストの SSH キーが変更された場合は、エラーが表示されます(例 3-26 を参照)。

***例 3-26　SCP/SFTP を使用したファイルのコピー(SSH キーの変更によるエラーの発生)***

```
switch# copy scp://apn@10.10.1.1/isan-104
bootflash:isan-ram-1.0.4
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
36:96:ca:d7:29:99:79:74:aa:4d:97:49:81:fb:23:2f.
Please contact your system administrator.
Add correct host key in /mnt/pss/.ssh/known_hosts to get rid of this
message.
Offending key in /mnt/pss/.ssh/known_hosts:2
RSA1 host key for 10.10.1.1 has changed and you have requested strict
checking.
```

# SSH または Telnet サービスのイネーブル化

デフォルトでは、SSH サービスは、RSA キーによってイネーブルになっています。

SSH または Telnet サービス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。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature ssh`<br>`updated` | SSH サービスの使用を有効にします。 |
| | `switch(config)# no feature ssh`<br>`updated` | SSH サービスの使用をディセーブルにします(デフォルト)。 |
| | `switch(config)# feature telnet`<br>`updated` | Telnet サービスの使用をイネーブルにします。 |
| | `switch(config)# no feature telnet`<br>`updated` | Telnet サービスの使用をディセーブルにします(デフォルト)。 |

# SSH プロトコル ステータスの表示

SSH プロトコルのステータス(イネーブルまたはディセーブル)、およびそのスイッチでイネーブルになっているバージョンを表示するには、**show ssh server** コマンドを使用します(例 3-27 を参照)。

***例 3-27　SSH プロトコルのステータスの表示***

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

指定されたキーまたはすべてのキーのサーバ キーペアの詳細を表示するには、**show ssh key** コマンドを使用します(例 3-28 を参照)。

***例 3-28　サーバ キーペアの詳細の表示***

```
switch# show ssh key
rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
```

```
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss
AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaWcMMYsEgxc9ada1NElp
8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAOi/Cti84qFb3kTqXlS9mEhdQUo0lH
cH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsAAABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9F
NipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/QwI4q68/eaw=
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

（注）　SSH でスイッチにログインし、**aaa authentication login default none** CLI　コマンドを発行した場合、ログインするために 1 つ以上のキーストロークを入力する必要があります。少なくとも 1 つのキーストロークを入力せずに **Enter** キーを押すと、ログインは拒否されます。

# デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリ スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出処と完全性を保証する 1 つのデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局（CA）によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書インフラストラクチャは Secure Socket Layer（SSL）をサポートする最初の証明書を使用し、セキュリティ インフラストラクチャにより照会または通知の形で返信を受け取ります。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

スイッチは、X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかに設定できますが、両方に設定することはできません。いずれかに設定されている場合は、その認証が失敗すると、パスワードの入力を求められます。

# パスワードのないファイル コピーおよび SSH

セキュア シェル（SSH）公開キー認証は、パスワードのないログインを行うために使用できます。SCP および SFTP は SSH をバックグラウンドで使用するため、これらのコピー プロトコルを使用することにより、公開キー認証によるパスワードのないコピーが可能になります。この NX-OS バージョンは、SCP および STFP クライアント機能だけをサポートしています。

SSH による認証に使用できる RSA および DSA ID を作成できます。この ID は、公開キーと秘密キーという 2 つの部分から構成されています。公開キーおよび秘密キーはスイッチによって生成されますが、外部で生成してスイッチにインポートすることもできます。インポートするためには、キーが OPENSSH 形式であることが必要です。

SSH サーバをホストしているホスト マシン上でキーを使用するには、そのマシンに公開キー ファイルを転送し、サーバの SSH ディレクトリ（たとえば、$HOME/.ssh）にあるファイル authorized_keys に内容を追加します。秘密キーをインポートおよびエクスポートする場合、キーは暗号化によって保護されます。同一のパスフレーズを入力するように求められます。パスフレーズを入力すると、秘密キーは暗号化によって保護されます。パスワード フィールドを空白のままにしておくと、キーは暗号化されません。

キーを別のスイッチにコピーする必要がある場合は、スイッチからホスト マシンにキーをエクスポートし、そのマシンから他のスイッチに同じキーをインポートします。

- キー ファイルは、リブート後も維持されます。

キー ペアをインポートおよびエクスポートするために、次の CLI が提供されます。スイッチで SSH ユーザ キー ペアを生成する CLI コマンドは次のように定義されます。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# username admin keypair generate rsa`<br>`generating rsa key(1024 bits).....`<br>`generated rsa key` | アカウント（admin）の公開および秘密 RSA キーを生成します。その後、指定されたユーザのホーム ディレクトリにキー ファイルを保存します。そのサーバ キー ペアを上書きするには force オプションを使用します。<br>（注）　この例は RSA キーの場合です。DSA キーの場合、rsa を dsa に置き換えます。 |
| | `switch(config)# no username admin keypair generate rsa` | アカウント（admin）の公開および秘密 RSA キーを削除します。 |
| ステップ 3 | `switch# show username admin keypair`<br>`**********`<br>`rsa Keys generated: Thu Jul  9 11:10:29 2009`<br>`ssh-rsa`<br>`AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD`<br>`0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq`<br>`srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ`<br>`bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=`<br>`bitcount:262144`<br>`fingerprint:`<br>`8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d`<br>`**********`<br>`could not retrieve dsa key information`<br>`**********` | アカウント（admin）の公開キーを示します。 |
| | | |
| ステップ 4 | `switch(config)# username admin keypair export bootflash:key_rsa rsa`<br>`Enter Passphrase:`<br>`switch(config)# dir`<br>`951  Jul 09 11:13:59 2009  key_rsa`<br>`221  Jul 09 11:14:00 2009  key_rsa.pub` | ユーザ（admin）のホーム ディレクトリからブートフラッシュ メモリにキー ペアをエクスポートします。<br>キー ペア（公開キーと秘密キー）が指定の場所にエクスポートされます。ユーザは秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは uri で指定したファイル名としてエクスポートされ、公開キーは「.pub」拡張子が後に付く同じファイル名でエクスポートされます。<br>ユーザは任意のスイッチにこのキー ペアをコピーして、さらに SCP サーバのホーム ディレクトリに公開ファイルをコピーできるようになります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | switch(config)# **username admin keypair import bootflash:key_rsa rsa**<br>Enter Passphrase:<br>switch(config)# show username admin keypair<br>**********<br>rsa Keys generated: Thu Jul  9 11:10:29 2009<br>ssh-rsa<br>AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD<br>0P8boZElTfJFx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvq<br>srU9TBypYDPQkR/+Y6cKubyFWVxSBG/NHztQc3+QC1zdkIxGNJ<br>bEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbqS33GZsCAX6v0=<br>bitcount:262144<br>fingerprint:<br>8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d<br>**********<br>could not retrieve dsa key information<br>********** | スイッチのホーム ディレクトリにキーペアをインポートします。<br>ここで示す uri は秘密キー の uri であり、公開キーは「.pub」拡張子が付いて同じ場所に存在する必要があります。ユーザはパスフレーズの入力が求められ、キーの暗号化に使用されたのと同じパスフレーズを入力する必要があります。<br>サーバにパスワードレス コピーをする必要があるスイッチに秘密キーがコピーされ、そのサーバのホーム ディレクトリの authorized_keys ファイルにコピーされた公開キーがある場合、ユーザはスイッチからサーバへのパスワードレス ファイル コピーおよび ssh を実行できます。<br>(注)　サーバの authorized_keys ファイルに公開キーをコピーするのに、ユーザは前述の show コマンドからキーをコピーすることもできます。 |
| ステップ 6 | server# **cat key_rsa.pub >> $HOME/.ssh/authorized_keys** | SCP サーバの authorized_keys ファイルに key_rsa.pub に保存されている公開キーを追加します。標準 ssh と scp コマンドを使用して、スイッチからこのサーバへのパスワードレス ssh および scp が有効になりました。 |

# 管理者パスワードの回復

次の 2 通りの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザ名による CLI の使用
- スイッチの電源再投入

ここでは、次の項目について説明します。

- network admin 権限での CLI の使用（3-63 ページ）
- スイッチの電源の再投入（3-63 ページ）

## network admin 権限での CLI の使用

network-admin 権限を持つユーザ名でスイッチにログインしているか、ログインできる場合に、管理者パスワードを回復するには、次の手順を実行します。

**ステップ 1**　ユーザ名に network-admin 権限があることを確認するには、**show user-accounts** コマンドを使用します。

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:dbgusr
        this user account has no expiry date
        roles:network-admin network-operator
```

**ステップ 2**　ユーザ名に network-admin 権限がある場合は、**username** コマンドを発行して新しい管理者パスワードを割り当てます。

```
switch# config t
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

**ステップ 3**　ソフトウェア設定を保存します。

```
switch# copy running-config startup-config
```

## スイッチの電源の再投入

network-admin 特権を持つスイッチ上でセッションを開始できない場合は、スイッチの電源を再投入して管理者パスワードを回復する必要があります。

**注意**　この手順を実行すると、スイッチ上のすべてのトラフィックが中断されます。スイッチとの接続はすべて 2 ～ 3 分間切断されます。

**（注）**　管理者パスワードは、Telnet または SSH セッションからは回復できません。ローカル コンソール接続を使用できる必要があります。コンソール接続のセットアップの詳細については、『*Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*』を参照してください。

スイッチの電源を再投入して、管理者パスワードを回復するには、次の手順を実行します。

**ステップ 1**　2 つのスーパーバイザ モジュールを搭載した Cisco MDS 9500 シリーズ スイッチの場合は、シャーシのスロット 6 からスーパーバイザ モジュールを取り外します。

**（注）**　Cisco MDS 9500 シリーズでは、パスワード回復手順をアクティブなスーパーバイザ モジュールで実行する必要があります。スロット 6 のスーパーバイザ モジュールを取り外すことで、パスワード回復手順中にスイッチオーバーが発生しないようにします。

**ステップ 2**　スイッチの電源を再投入します。

**ステップ 3**　スイッチが Cisco NX-OS ソフトウェアのブート シーケンスを開始したときに **Ctrl-]** キー シーケンスを押して、`switch(boot)#` プロンプト モードを開始します。

```
Ctrl-]
switch(boot)#
```

**ステップ 4**　コンフィギュレーション モードに切り替えます。

```
switch(boot)# config terminal
```

**ステップ 5**　admin-password コマンドを発行して、管理者パスワードをリセットします。これは、コンソールを使用してログインのリモート認証を無効にします(有効な場合)。これはパスワードを回復した後、新しいパスワードで管理者がコンソールからログインできるようにするために行います。Telnet/SSH の認証は、これにより影響を受けません。

```
switch(boot-config)# admin-password <new password>
WARNING! Remote Authentication for login through console will be disabled#
```

強力なパスワードの詳細については、「パスワード強度の確認」セクション(3-46 ページ)を参照してください。

**ステップ 6**　EXEC モードに切り替えます。

```
switch(boot-config)# admin-password <new password>
```

**ステップ 7**　**load** コマンドを発行して、Cisco NX-OS ソフトウェアをロードします。

```
switch(boot)# load bootflash:m9500-sf1ek9-mz.2.1.1a.bin
```

**注意**　コンフィギュレーションを保存するために使用するイメージより古いシステム イメージをブートし、**install all** コマンドを使用せずにシステムをブートする場合、スイッチはバイナリ コンフィギュレーションを消去し、ASCII コンフィギュレーションを使用します。この場合は、**init system** コマンドを使用してパスワードを回復する必要があります。

**ステップ 8**　新しい管理者パスワードを使用してスイッチにログインします。

```
switch login: admin
Password: <new password>
```

**ステップ 9**　Fabric Manager の SNMP パスワードとしても使用できるようにするために、新しいパスワードをリセットします。

```
switch# config t
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

**ステップ 10**　ソフトウェア設定を保存します。

```
switch# copy running-config startup-config
```

**ステップ 11**　以前に取り外したスーパーバイザ モジュールをシャーシのスロット 6 に挿入します。

# デフォルト設定

表 3-3 に、スイッチのすべてのスイッチ セキュリティ機能のデフォルト設定を示します。

*表 3-3　スイッチ セキュリティのデフォルト設定*

| パラメータ | デフォルト |
|---|---|
| Cisco MDS スイッチでのロール | ネットワーク オペレータ（network-operator） |
| AAA 設定サービス | ローカル |
| 認証ポート | 1821 |
| アカウンティング ポート | 1813 |
| 事前共有キーの送受信 | クリア テキスト |
| RADIUS サーバ タイムアウト | 1 秒 |
| RADIUS サーバ再試行 | 1 回 |
| TACACS+ | ディセーブル |
| TACACS+ サーバ | 未設定 |
| TACACS+ サーバのタイムアウト | 5 秒 |
| AAA サーバへの配信 | ディセーブル |
| ロールに対する VSAN ポリシー | Permit |
| ユーザ アカウント | 有効期限なし（設定されていない場合） |
| パスワード | なし |
| パスワード強度 | イネーブル |
| アカウンティング ログ サイズ | 250 KB |
| SSH サービス | イネーブル |
| Telnet サービス | ディセーブル |

CHAPTER 4

# 外部 AAA サーバでのセキュリティ機能の設定

認証、許可、アカウンティング（AAA）機能は、スイッチを管理するユーザの ID 確認、ユーザへのアクセス権付与、およびユーザ アクションの追跡を実行します。Cisco MDS 9000 ファミリのすべてのスイッチで、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルを使用することで、リモート AAA サーバを使用するソリューションが実現されます。

指定されたユーザ ID およびパスワードの組み合わせに基づいて、スイッチはローカル認証やローカル データベースによる認可、またはリモート認証や AAA サーバによる認可を実行します。スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。この秘密キーはすべての AAA サーバ、または特定の AAA サーバに設定できます。このセキュリティ機能により、AAA サーバを中央で管理できます。

この章は、次の項で構成されています。

# スイッチ管理のセキュリティ

Cisco MDS 9000 ファミリ スイッチの管理セキュリティは、コマンドライン インターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）を含む、すべての管理アクセス方式にセキュリティを提供します。

この項では、次のトピックについて取り上げます。



## CLI セキュリティ オプション

CLI にはコンソール（シリアル接続）、Telnet、またはセキュア シェル（SSH）を使用してアクセスできます。

- リモート セキュリティ制御
  - RADIUS を利用

    「RADIUS サーバ モニタリング パラメータの設定」セクション（4-89 ページ）を参照してください。
  - TACACS+ を利用

    「TACACS+ サーバ モニタリング パラメータの設定」セクション（4-100 ページ）を参照してください。
- ローカル セキュリティ制御

  「ローカル AAA サービス」セクション（4-121 ページ）を参照してください。

これらのセキュリティ機能は、次のシナリオにも設定できます。

- Small Computer Systems Interface over IP（iSCSI）認証

  『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』、『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。
- Fibre Channel Security Protocol（FC-SP）認証

  第 8 章「FC-SP および DHCHAP の設定」を参照してください。

## SNMP セキュリティ オプション

SNMP エージェントは、SNMPv1、SNMPv2c、および SNMPv3 のセキュリティ機能をサポートしています。SNMP を使用するすべてのアプリケーション（Cisco MDS 9000 Fabric Manager など）に、標準 SNMP セキュリティ機能が適用されます。

SNMP セキュリティ オプションは Fabric Manager と Device Manager にも適用できます。

SNMP セキュリティ オプションの詳細については、『*Cisco MDS 9000 NX-OS Family System Management Configuration Guide*』を参照してください。

Fabric Manager と Device Manager の詳細については、『*Cisco Fabric Manager Fundamentals Configuration Guide*』を参照してください。

# スイッチの AAA 機能

CLI または Fabric Manager あるいは SNMP アプリケーションを使用して、すべての Cisco MDS 9000 ファミリ スイッチに AAA スイッチ機能を設定できます。

この項では、次のトピックについて取り上げます。



## 認証

認証は、スイッチにアクセスするユーザまたはデバイスの識別情報を検証するプロセスです。この ID 確認は、スイッチにアクセスしようとするエンティティが提出するユーザ ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリ スイッチでは、ローカル認証（ローカル ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

（注）　Fabric Manager は末尾が空白スペースの AAA パスワードをサポートしません（例「passwordA」）。

## 認可

すべての Cisco MDS スイッチに次の認可ロールがあります。

- ネットワーク オペレータ（network-operator）：設定を表示する権限だけがあります。オペレータは設定内容を変更できません。
- ネットワーク管理者（network-admin）：すべてのコマンドを実行し、設定内容を変更する権限があります。管理者は最大 64 の追加ロールを作成し、カスタマイズできます。
- デフォルトロール：GUI を利用する権限があります（Fabric Manager および Device Manager）。このアクセス権は、GUI にアクセスすることを目的として、すべてのユーザに自動的に与えられます。

これらのロールは変更または削除ができません。追加のロールを作成することで、次のオプションを設定できます。

- ユーザ ロールをローカルに割り当てるか、またはリモート AAA サーバを使用して、ロールベースの認可を設定します。
- ロール情報を格納するように、リモート AAA サーバのユーザ プロファイルを設定します。このロール情報は、リモート AAA サーバを通じてユーザを認証したときに、自動的にダウンロードされ、使用されます。

（注）　ユーザが新しく作成されたロールのうちの 1 つだけに属している場合、このロールが削除されると、ユーザにはただちにデフォルトの network-operator ロールが設定されます。

# アカウンティング

アカウンティング機能はスイッチへのアクセスに使用されるすべての管理設定のログを追跡し、管理します。この情報を利用して、トラブルシューティングや監査に使用するレポートを生成できます。アカウンティング ログはローカルで保存したり、リモート AAA サーバに送信したりできます。

# リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各スイッチに対するユーザ パスワード リストをより簡単に管理できます。
- AAA サーバはすでに企業全体に配置済みであり、簡単に導入できます。
- ファブリック内のすべてのスイッチのアカウンティング ログを集中管理できます。
- ファブリック内の各スイッチに対するユーザ ロール設定をより簡単に管理できます。

# リモート認証に関する注意事項

リモート AAA サーバを使用する場合は、次の注意事項に従ってください。

- 最低 1 つの AAA サーバが IP で到達可能になっている必要があります。
- すべての AAA サーバが到達不能である場合のポリシーとして、適切なローカル AAA ポリシーを必ず設定してください。
- オーバーレイ Ethernet LAN がスイッチに接続している場合、AAA サーバは容易に到達可能です（『*Cisco Fabric Manager IP Services Configuration Guide*』および『*Cisco MDS 9000 Family NX-OS Configuration Guide*』を参照）。この方法を推奨します。
- スイッチに接続された SAN ネットワーク内のゲートウェイ スイッチを 1 つまたは複数、AAA サーバに到達するイーサネット LAN に接続する必要があります。

# サーバ グループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。サーバ グループは、同じ AAA プロトコルを実装するリモート AAA サーバ セットです。サーバ グループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモート サーバで試行が行われます。サーバ グループ内のすべての AAA サーバが応答しなかった場合、そのサーバ グループ オプションは障害が発生しているものと見なされます。必要に応じて、複数のサーバ グループを指定できます。Cisco MDS スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバ グループのサーバが試行されます。

# AAA サービス設定オプション

Cisco MDS 9000 ファミリ スイッチ製品内の AAA 設定は、サービス ベースです。次のサービスごとに、異なる AAA 設定を作成できます。

- Telnet または SSH ログイン（Fabric Manager および Device Manager ログイン）
- コンソール ログイン
- iSCSI 認証（『*Cisco Fabric Manager IP Services Configuration Guide*』および『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』を参照）
- FC-SP 認証（第 8 章「FC-SP および DHCHAP の設定」を参照）
- アカウンティング

一般に、AAA 設定の任意のサービスに対して指定できるオプションは、サーバ グループ、ローカル、および none の 3 つです。各オプションは指定した順序で試行されます。すべてのオプションが失敗した場合、ローカルが試行されます。

**注意**　Cisco MDS NX-OS では、ユーザ名がアルファベットで始まる限り、リモートで作成するか（TACACS+ または RADIUS を使用）ローカルで作成するかに関係なく、英数字または特定の特殊文字（+ [プラス]、= [等号]、_ [下線]、- [ハイフン]、\ [バックスラッシュ]、および . [ピリオド]）を使って作成したユーザ名がサポートされます。リモートで作成するか（TACACS+ または RADIUS を使用）ローカルで作成するかに関係なく、ローカル ユーザ名をすべて数字で作成したり、特殊文字（上記の特殊文字を除く）を使用して作成したりすることはできません。数字だけのユーザ名やサポートされていない特殊文字によるユーザ名が AAA サーバに存在し、ログイン時に入力されると、そのユーザはアクセスを拒否されます。

**（注）**　オプションの 1 つとしてローカルが指定されていない場合でも、認証用に設定されたすべての AAA サーバに到達不能であるかどうかがデフォルトで試行されます。ユーザは、このフォールバックを柔軟にディセーブルにすることができます。

RADIUS がタイムアウトする際は、フォールバック設定に応じてローカル ログインが試行されます。このローカル ログインに成功するには、同一のパスワードを持つそのユーザのローカル アカウントが存在し、かつ RADIUS のタイムアウトと再試行は 40 秒未満でなければなりません。そのユーザが認証されるのは、ローカルの認証設定にそのユーザ名とパスワードが存在する場合です。

表 4-1 に、AAA サービス設定オプションごとに CLI（コマンドライン インターフェイス）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（Cisco Fabric Manager および Device Manager ログイン） | **aaa authentication login default** |
| コンソール ログイン | **aaa authentication login console** |
| Small Computer Systems Interface over IP（iSCSI）認証 | **aaa authentication iscsi default** |

*表 4-1　AAA サービス コンフィギュレーション コマンド(続き)*

| 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 |
|---|---|
| FC-SP 認証 | **aaa authentication dhchap default** |
| アカウンティング | **aaa accounting default** |

(注)　コンソールで認証方法を何も設定しない場合は、コンソールと Telnet または SSH の両方にデフォルトの認証方法が適用されます。

# エラー対応ステータス

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。この場合は、error-enabled 機能をイネーブルにした場合、次のメッセージが画面に表示されます。

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

このメッセージの表示をイネーブルにするには、**aaa authentication login error-enable** コマンドを使用します。

このメッセージの表示をディセーブルにするには、**no aaa authentication login error-enable** コマンドを使用します。

現在の表示ステータスを確認するには、**show aaa authentication login error-enable** コマンドを使用します(例 4-1 を参照)。

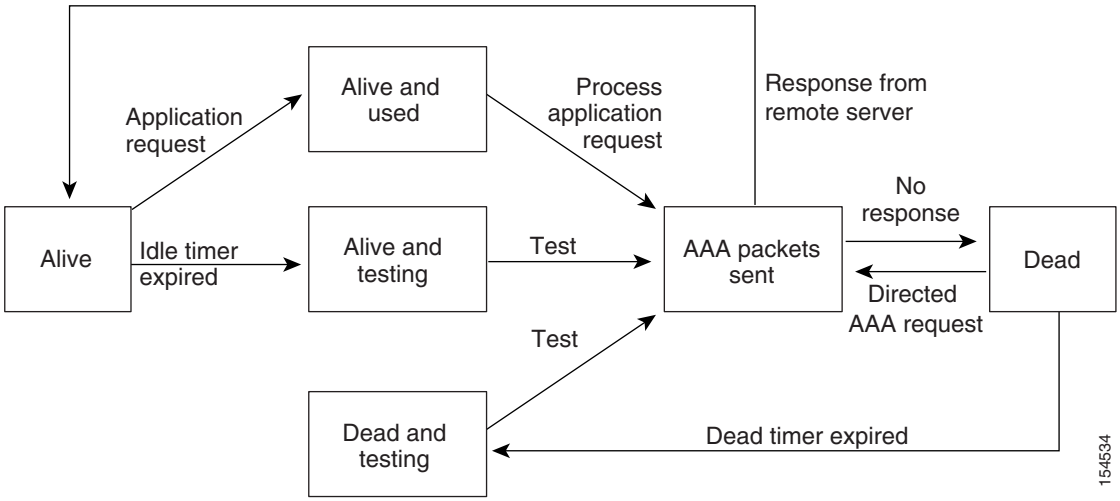
*例 4-1　AAA 認証ログイン情報の表示*

```
switch# show aaa authentication login error-enable
enabled
```

# AAA サーバのモニタリング

応答の途絶えた AAA サーバは AAA 要求の処理に遅延をもたらします。AAA 要求の処理時間を節約するため、MDS スイッチは定期的に AAA サーバをモニタして AAA サーバが応答している(または稼働している)かどうかを確認できます。MDS スイッチは、応答のない AAA サーバを停止中としてマーク付けします。また、停止中のいずれの AAA サーバにも AAA 要求を送りません。MDS スイッチは定期的に停止中の AAA サーバを監視し、応答するようになったら稼働中と認識します。このモニタリング プロセスでは、実際の AAA 要求を送出する前にその AAA サーバが稼働中であることを確認します。AAA サーバのステートが停止中または稼働中に変化すると常に SNMP トラップが生成され、MDS スイッチはパフォーマンスに影響が出る前に、管理者に対して障害が発生していることを警告します。AAA サーバのステートについては、図 4-1 を参照してください。

*図 4-1　AAA サーバのステート*




(注)　稼働中のサーバと停止中のサーバのモニタリング間隔はそれぞれ別で、ユーザが設定できます。AAA サーバのモニタリングはテスト用認証要求を AAA サーバに送信することで行われます。

テスト パケットで使用されるユーザ名とパスワードは設定が可能です。

「RADIUS サーバ モニタリング パラメータの設定」セクション（4-89 ページ）、「RADIUS サーバ モニタリング パラメータの設定」セクション（4-93 ページ）および「RADIUS サーバの詳細の表示」セクション（4-99 ページ）を参照してください。

# 認証と許可のプロセス

認証は、スイッチを管理する人物の ID を確認するプロセスです。この ID 確認は、スイッチを管理しようとする人物が入力したユーザ ID およびパスワードの組み合わせに基づいて行われます。Cisco MDS 9000 ファミリ スイッチでは、ローカル認証（ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

許可は、アクセス コントロールを提供します。これは、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。ユーザは、ユーザ ID とパスワードの組み合わせに基づいて認証および認可され、割り当てられているロールに従ってネットワークにアクセスします。スイッチで TACACS+ プロトコルを使用していれば、ユーザによる不正なアクセスを防ぐことができるパラメータを設定できます。

AAA の許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。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。

認証と認可の手順は次のとおりです。

**ステップ 1**　Cisco MDS 9000 ファミリ内の必要なスイッチへのログインには、Telnet、SSH、Fabric Manager/Device Manager、またはコンソールのログイン オプションを使用します。

**ステップ 2**　サーバ グループ認証方式を使用するサーバ グループを設定した場合は、グループ内の最初の AAA サーバに認証要求が送信されます。

- その AAA サーバが応答に失敗すると次の AAA サーバに送信され、リモート サーバが認証要求に応答するまで繰り返されます。
- サーバ グループ内のすべての AAA サーバが応答に失敗した場合は、次のサーバ グループのサーバに送信が行われます。
- 設定されているすべての方式で応答が得られなかった場合、デフォルトでローカル データベースが認証に使用されます。次の項で、このフォールバックをディセーブルにする方法について説明します。

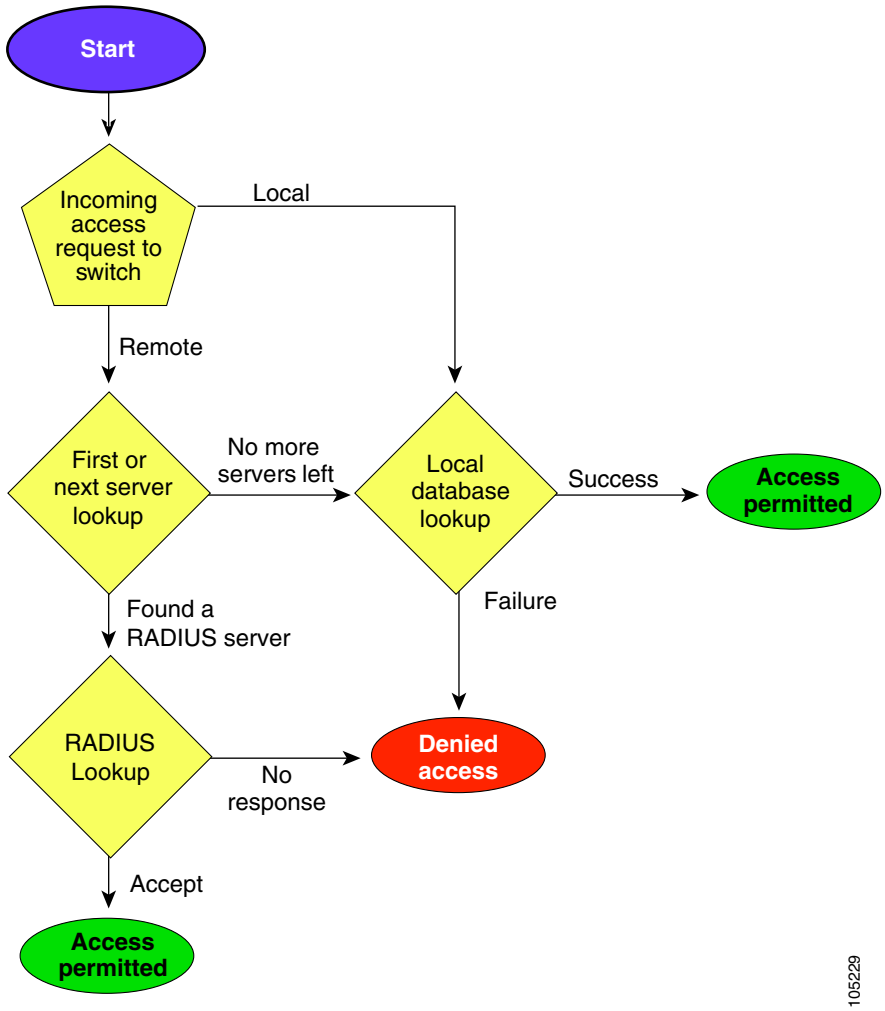
**ステップ 3**　リモートの AAA サーバにより認証に成功すると、場合に応じて次の処理が実行されます。

- AAA サーバのプロトコルが RADIUS の場合は、認証応答に伴って **cisco-av-pair** 属性で指定されたユーザ ロールがダウンロードされます。
- AAA サーバ プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。
- リモート AAA サーバからのユーザ ロールの入手に失敗した場合、**show aaa user default-role** コマンドがイネーブルであれば、ユーザには network-operator ロールが割り当てられます。このコマンドがディセーブルの場合には、アクセスが拒否されます。

**ステップ 4**　ユーザ名とパスワードがローカルで認証に成功した場合は、ログインが許可され、ローカル データベースに設定されているロールが割り当てられます。

図 4-2 に、認可と認証のプロセスのフローチャートを示します。

*図 4-2　スイッチの認可と認証のフロー*




(注)　残りのサーバ グループがないということは、どのサーバ グループのどのサーバからも応答がないということを意味します。
残りのサーバがないということは、このサーバ グループのどのサーバからも応答がないということを意味します。

TACACS+ サーバでロールベースの認証を設定するには、次の手順に従います。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authorization` | 認証方式の設定を有効にします。 |
| ステップ 3 | `switch(config)# aaa authorization config-commands` | config モード Layer2 および Layer3 のすべてのコマンドの認証を有効にします。 |
| ステップ 4 | `switch(config)# aaa authorization config-commands default group tac1` | 指定した TACACS+ サーバ グループの認証を有効にします。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | `switch(config)# aaa authorization commands` | すべての EXEC モード コマンドへの AAA 許可を有効にします。 |
| ステップ 6 | `switch(config)# aaa authorization commands default group tac1` | 指定した TACACS+ サーバ グループの認証を有効にします。 |
| ステップ 7 | `switch(config)# aaa authorization commands default group local` | デフォルトの TACACS+ サーバ グループの認証を有効にします。認証は、ローカル ユーザ データベースに基づいています。 |
| ステップ 8 | `switch(config)# no aaa authorization command default group tac1` | 認証されたユーザに対し指定した機能の認証を削除します。 |

(注)
- 承認の設定は、TACACS+ サーバを使用して実施する認証にのみ提供されます。
- AAA 許可方式の [none] オプションは廃止されました。4.x イメージからアップグレードし、[none] を許可方式の 1 つとして設定した場合、ローカルに置き換えられます。機能は変わりません。
- コマンド許可では、デフォルト ロールを含むユーザのロールベース許可コントロール（RBAC）がディセーブルになります。

AAA 認証に関する情報と、リモート認証に割り当てられたデフォルト ユーザ ロールを表示するには、**show** コマンドを使用できます。（例 4-2 から例 4-3 を参照してください）。

*例 4-2　AAA 許可情報の詳細の表示*

```
switch# show aaa authorization all
AAA command authorization:
         default authorization for config-commands: local
         default authorization for commands: local
         cts: group rad1
```

*例 4-3　リモート認証のデフォルト ユーザ ロールの表示*

```
switch# show aaa user default-role
enabled
```

## 認証のフォールバック メカニズムの設定

リモート認証が設定され、すべての AAA サーバに到達不能（認証エラー）である場合は、ローカル データベースへのフォールバックをイネーブルまたはディセーブルにできます。認証エラーの場合、フォールバックはデフォルトでローカルに設定されています。コンソール ログインと ssh/telnet ログインの両方に対して、このフォールバックをディセーブルにすることもできます。このフォールバックを無効にすると、認証のセキュリティが強化されます。

CLI 構文と動作は次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **show run aaa all**<br>aaa authentication login default fallback error local<br>aaa authentication login console fallback error local | デフォルトのフォールバックの動作が表示されます。 |
| ステップ 3 | switch(config)# **no aaa authentication login default fallback error local**<br>WARNING!!! Disabling fallback can lock your switch. | 認証用のローカル データベースへのフォールバックをディセーブルにします。<br>(注)　コンソールへフォールバックをディセーブルにするには、このコマンドの **default** を **console** で置き換えます。 |

**注意**　デフォルトとコンソールの両方に対してフォールバックがディセーブルである場合は、リモート認証がイネーブルになり、サーバに到達不能であるため、スイッチはロックされます。

## 認可プロファイルの確認

各種コマンドの認可プロファイルを確認できます。イネーブルの場合、すべてのコマンドは、検証用に Access Control Server（ACS）に転送されます。検証が完了すると、検証の詳細が表示されます。

```
switch# terminal verify-only username sikander
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature telnet
% Success
switch(config)# feature ssh
% Success
switch(config)# end
% Success
switch# exit
```

**(注)**　このコマンドは、コマンドを確認するだけで設定をイネーブルにしません。

## 認証のテスト

コマンドの認証設定をテストできます。

コマンドの認証をテストするには、**test aaa authorization command-type** コマンドを使用します。

```
switch(config)# test aaa authorization command-type commands user u1 command "feature
dhcp"
% Success
```

# AAA サーバのモニタリング パラメータをグローバルに設定

AAA サーバ モニタリング パラメータは、すべてのサーバにグローバルに設定、または特定のサーバに対して個別に設定できます。この項では、グローバル コンフィギュレーションの設定方法について説明します。グローバル コンフィギュレーションは、個別のモニタリング パラメータが定義されていないすべてのサーバに適用されます。各サーバで、特定のサーバに対して定義された個々のテスト パラメータは、グローバル設定よりも常に優先されます。

RADIUS サーバのグローバル モニタリング パラメータを設定するには、次のコマンドを使用します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# radius-server deadtime 10` | RADIUS サーバのグローバル デッド タイムを 10 分間に設定します。<br>許容範囲は 0 ～ 1440 分です。 |
| ステップ 3 | `switch(config)# radius-server timeout 20f` | RADIUS サーバのグローバル タイムアウトを 20 分間に設定します。<br>許容範囲は 1 ～ 60 分です。 |
| ステップ 4 | `switch(config)# radius-server retransmit 2` | RADIUS サーバのグローバル再送信回数を 2 に設定します。<br>許容範囲は 0 ～ 5 です。 |
| ステップ 5 | `switch(config)# radius-server test username username password password idle-time time` | RADIUS サーバのテスト パラメータをグローバルに設定します。 |
| | `switch(config)# radius-server test username username password password no` | RADIUS サーバのグローバルなテスト パラメータを無効にします。 |

(注)　TACACS サーバのグローバル テスト パラメータの設定の場合に相当するコマンドを取得するには、上記の手順の radius を tacacs と置き換えます。

グローバル AAA サーバ モニタリング パラメータは次の動作を確認します。

- 新しい AAA サーバを設定すると、その AAA サーバは、グローバル テスト パラメータを使用して監視されます(定義されている場合)。
- グローバル テスト パラメータが追加または変更されると、テスト パラメータが設定されていないすべての AAA サーバは、新しいグローバル テスト パラメータを使用して監視されるようになります。
- サーバのサーバ テスト パラメータを削除した場合、またはアイドル時間を 0(デフォルト値)に設定した場合、そのサーバは、グローバル テスト パラメータを使用して監視されるようになります(定義されている場合)。

- グローバル テスト パラメータを削除したり、グローバル アイドル時間を 0 に設定したりしても、サーバ テスト パラメータが存在するサーバは影響を受けません。ただし、これまではグローバル パラメータを使用して監視されていた他のすべてのサーバのモニタリングが停止します。
- ユーザ指定のサーバ テスト パラメータによってサーバのモニタリングが失敗した場合は、グローバル テスト パラメータにフォールバックしません。

# LDAP の設定

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS 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います。LDAP 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働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 つのアクセス コントロール サーバ（LDAP デーモン）が認証と許可の各サービスを個別に提供できます。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。

LDAP 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に、TCP（TCP ポート 389）を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

（注）　Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

この項では、次のトピックについて取り上げます。

# LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=$userid のデフォルト値です。

（注）　バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザ パスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

# LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
  - OpenLDAP
  - Microsoft Active Directory
- Secure Sockets Layer（SSL）上の LDAP は、SSL バージョン 3 および Transport Layer Security（TLS）バージョン 1.0、バージョン 1.1、およびバージョン 1.2 をサポートします。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- Cisco MDS スイッチは、次のすべての条件を満たし、LDAP がリモート認証プロトコルを使用している場合、ローカル ロールをリモート ユーザに割り当てます。
  - LDAP サーバのリモート ユーザ名は、Cisco MDS スイッチのローカル ユーザと同じ名前です。（たとえば、“test” が AD サーバでのユーザ名の場合は、Cisco MDS スイッチでも同じユーザ名が作成されます）
  - LDAP サーバは、Cisco MDS スイッチで AAA 認証として設定されます。
  - ローカル ユーザとリモート ユーザに割り当てられるロールは異なります。

次の例では、LDAP サーバのユーザ名が "test" で、AD グループ "testgroup" のメンバーである場合について検討します。Cisco MDS スイッチは、名前が "testgroup" に設定されたロールを使用し、このロールには特定の許可ロールが割り当てられています。このロールは Cisco MDS スイッチで作成され、LDAP を使用してスイッチにログインするリモート ユーザ用です。また、Cisco MDS スイッチにはローカル ユーザ名 "test" も使用し、ロールとして "network-admin" が割り当てられています。Cisco MDS スイッチは AAA 認証用に設定され、認証プロトコルとして LDAP を使用します。この場合、ユーザがユーザ名 "test" を使用して Cisco MDS スイッチにログインすると、スイッチは LDAP 認証を使用するユーザを認証します（AD サーバで作成された "test" ユーザのパスワードを使用します）。ただし、ロールは、リモートで認証されたユーザに割り当てられる "testgroup" ロールではなく、ローカル ユーザ "test" に割り当てられる "network-admin" が割り当てられます。

# LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること

# デフォルト設定

表 4-2 は、LDAP パラメータのデフォルト設定の一覧です。

*表 4-2　LDAP パラメータのデフォルト設定*

| パラメータ | デフォルト |
|---|---|
| LDAP | ディセーブル |
| LDAP 認証方式 | 検索してからバインド |
| LDAP 認証メカニズム | プレーン |
| デッド間隔時間 | 0 分 |
| タイムアウト間隔 | 5 秒 |
| アイドル タイマー間隔 | 60 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 | Cisco |

# LDAP のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの LDAP 機能はディセーブルになっています。認証に関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、LDAP 機能を明示的にイネーブルにする必要があります。

LDAP をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **feature ldap** | LDAP をイネーブルにします。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **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。 |

# LDAP サーバ ホストの設定

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上でその LDAP サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の LDAP サーバを設定できます。

(注)　デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバ グループに追加されます。LDAP サーバを別の LDAP サーバ グループに追加することもできます。

LDAP サーバ ホストを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-server host 10.10.2.2 enable-ssl** | LDAP サーバの IPv4 または IPv6 アドレス、あるいはホスト名を指定します。<br>**enable-ssl** キーワードは、LDAP クライアントに Secure Sockets Layer(SSL)セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの整合性と機密保持を保証します。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **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。 |

# LDAP サーバの RootDN の設定

LDAP サーバ データベースのルート指定名(DN)を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

LDAP サーバに RootDN 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 | switch# **configure terminal**<br>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 | switch(config)# **ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60** | LDAP サーバ データベースの rootDN を指定し、ルートのパスワードをバインドします。<br>任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です（グローバル値が設定されていない場合は 389）。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **show ldap-server** | （任意）LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# LDAP サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバはすべて、LDAP を使用するように設定する必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Cisco MDS NX-OS リリース 6.2(1) 以降では、Cisco MDS 9000 シリーズ スイッチがグループ ベースのユーザ ロールをサポートします。また、LDAP サーバにグループを作成し、Cisco MDS スイッチにまったく同じ名前のグループを作成してから、そのグループにユーザを追加できます。ユーザ ロール属性は設定されたグループのユーザに継承されます。これは Microsoft LDAP サーバの内蔵の memberOf 属性を使用して実行できます。memberOf 属性を使用するには、スイッチのロール名を作成していることを確認します。ロール名は LDAP サーバのグループ名と同じである必要があります。

（注）
- ユーザはスイッチで使用可能な 1 つのグループだけに属することができます。
- ユーザは複数のグループに属することができますが、スイッチ ロールに含めることができるのは 1 つのグループのみです。
- グループ名にスペースを含めることはできません。

LDAP サーバ グループを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **aaa group server ldap LDAPServer1**<br>switch(config-ldap)# | LDAP サーバ グループを作成し、そのグループの LDAP 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。 |
| ステップ 3 | switch(config-ldap)# **server 10.10.2.2** | LDAP サーバを、LDAP サーバ グループのメンバとして設定します。<br>指定した LDAP サーバが見つからない場合は、ldap-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 | switch(config-ldap)# **authentication compare password-attribute TyuL8r** | (任意) バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。 |
| ステップ 5 | switch(config-ldap)# **enable user-server-group** | (任意) グループ検証をイネーブルにします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名が LDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。 |
| ステップ 6 | switch(config-ldap)# **enable Cert-DN-matc**h | (任意) ユーザ プロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。 |
| ステップ 7 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 8 | switch# **show ldap-server groups** | (任意) LDAP サーバ グループの設定を表示します。 |
| ステップ 9 | switch# **show run ldap** | (任意) LDAP の設定を表示します。 |
| ステップ 10 | switch# **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。 |

# グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

グローバルな LDAP タイムアウト間隔を設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-server timeout 10** | LDAP 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。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |

| | | |
|---|---|---|
| ステップ 4 | switch# **show ldap-server** | (任意)LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

LDAP サーバにタイムアウト間隔を設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-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。デフォルトはグローバル値です。<br>(注)　特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **show ldap-server** | (任意)LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# グローバル LDAP サーバ ポートの設定

クライアントが TCP 接続を開始するグローバル LDAP サーバ ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

グローバルな LDAP サーバ ポートを設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-server port 2** | サーバへの LDAP メッセージに使用するグローバル TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **show ldap-server** | (任意)LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAP サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

TCP ポートを設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-server host 10.10.1.1 port 200 timeout 5** | サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。<br>（注）　特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **show ldap-server** | （任意）LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# LDAP 検索マップの設定

検索クエリーを LDAP サーバに送信するように LDAP 検索マップを設定できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

LDAP 検索マップを設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap search-map map1**<br>switch(config-ldap-search-map)# | LDAP 検索マップを設定します。 |

| | | |
|---|---|---|
| ステップ 3 | Example 1:<br>switch(config-ldap-search-map)# **userprofile attribute-name description search-filter "(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com**<br>Example 2:<br>switch(config-ldap-search-map)# **userprofile attribute-name "memberOf" search-filter "(&(objectClass=inetOrgPerson)(cn=$userid))" base-DN dc=acme,dc=com** | (任意)ユーザ プロファイル、信頼できる証明書、CRL、証明書 DN 一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベース DN を設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。<br>(注)　LDAP 検索フィルタ文字列は最大 128 文字に制限されています。<br>ユーザがメンバーとして所属しているグループを指定します。 |
| ステップ 4 | switch(config-ldap-search-map)# **exit**<br>switch(config)# | LDAP 検索マップ コンフィギュレーション モードを終了します。 |
| ステップ 5 | switch(config)# **show ldap-search-map** | (任意)設定された LDAP 検索マップを表示します。 |
| ステップ 6 | switch# **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。 |

# LDAP デッド タイム間隔の設定

すべての LDAP サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、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の時間を指定します。

(注)　デッド タイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイム間隔はグループ単位で設定できます。

LDAP 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。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **ldap-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。範囲は 1 ～ 60 分です。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **show ldap-server** | (任意)LDAP サーバの設定を表示します。 |
| ステップ 5 | switch# **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。 |

# LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

LDAP サーバに AAA 許可を設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2** | LDAP サーバのデフォルトの AAA 許可方式を設定します。<br>**ssh-certificate** キーワードは、証明書認証を使用した LDAP 許可またはローカル許可を設定し、ssh-publickey キーワードは、**SSH 公開キー**を使用した LDAP 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。<br>group-list 引数は、スペースで区切られた LDAP サーバ グループ名のリストです。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式では、許可にローカル データベースが使用されます。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch(config)# **show aaa authorization** | (任意)AAA 許可の設定を表示します。all キーワードは、デフォルト値を表示します。 |
| ステップ 5 | 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。 |

# LDAP のディセーブル化

LDAP 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。

LDAP をディセーブルにするには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | switch# **configure terminal**<br>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 | switch(config)# **no feature ldap** | LDAP をディセーブルにします。 |
| ステップ 3 | switch(config)# **exit**<br>switch# | 設定モードを終了します。 |
| ステップ 4 | switch# **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。 |

このコマンドの出力フィールドの詳細については、『*Cisco MDS 9000 Family Command Reference, Release 5.0(1a)*』を参照してください。

# LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
    server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

# RADIUS サーバ モニタリング パラメータの設定

Cisco MDS 9000 ファミリ スイッチは、RADIUS プロトコルを使用してリモート AAA サーバと通信できます。複数の RADIUS サーバおよびサーバ グループを設定し、タイムアウトおよび再試行回数を設定できます。

RADIUS はネットワークへの不正なアクセスを防ぐ分散型クライアント/サーバ プロトコルです。Cisco の実装では、RADIUS クライアントは Cisco MDS 9000 ファミリ スイッチで実行され、ユーザ認証およびネットワーク サービス アクセス情報がすべて含まれる RADIUS 中央サーバに認証要求が送信されます。

ここでは、RADIUS の動作の定義、ネットワーク環境の特定、および設定可能な内容について説明します。

- ログイン時にユーザによる RADIUS サーバの指定を許可（4-97 ページ）

# RADIUS サーバのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定するどの RADIUS サーバにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- タイムアウトの値
- 送信試行回数
- ユーザによるログイン時の RADIUS サーバ指定の許可

# RADIUS サーバのアドレスの設定

最大 64 台の RADIUS サーバを追加できます。RADIUS のキーは永続性ストレージに必ず暗号化して保存されます。実行コンフィギュレーションにも、暗号化されたキーが表示されます。

ホスト RADIUS サーバの IPv4 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server host 10.10.0.0 key HostKey` | 選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 10.10.0.0 で、キーは HostKey です。 |
| ステップ 3 | `switch(config)# radius-server host 10.10.0.0 auth-port 2003` | RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 10.10.0.0 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。 |
| ステップ 4 | `switch(config)# radius-server host 10.10.0.0 acct-port 2004` | RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。 |
| ステップ 5 | `switch(config)# radius-server host 10.10.0.0 accounting` | アカウンティングの目的のみに使用されるこのサーバを指定します。<br>（注）　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。 |
| ステップ 6 | `switch(config)# radius-server host 10.10.0.0 key 0 abcd` | 指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。 |
| | `switch(config)# radius-server host 10.10.0.0 key 4 da3Asda2ioyuoiuH` | 指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。 |

ホスト RADIUS サーバの IPv6 アドレスおよびその他のオプションを指定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server host 2001:0DB8:800:200C::417A Key HostKey` | 選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは 2001:0DB8:800:200C::417A で、キーは HostKey です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | `switch(config)# radius-server host 2001:0DB8:800:200C::417A auth-port 2003` | RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは 2001:0DB8:800:200C::417A で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。 |
| ステップ 4 | `switch(config)# radius-server host 2001:0DB8:800:200C::417A acct-port 2004` | RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。 |
| ステップ 5 | `switch(config)# radius-server host 2001:0DB8:800:200C::417A accounting` | アカウンティングの目的のみに使用されるこのサーバを指定します。<br>（注）　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。 |
| ステップ 6 | `switch(config)# radius-server host 2001:0DB8:800:200C::417A key 0 abcd` | 指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。 |
| | `switch(config)# radius-server host 2001:0DB8:800:200C::417A key 4 da3Asda2ioyuoiuH` | 指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。 |

ホスト RADIUS サーバの DNS 名およびその他のオプションを指定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server host radius2 key HostKey` | 選択した RADIUS サーバの事前共有キーを指定します。このキーは **radius-server key** コマンドを使用して割り当てたキーを上書きします。この例では、ホストは radius2 で、キーは HostKey です。 |
| ステップ 3 | `switch(config)# radius-server host radius2 auth-port 2003` | RADIUS 認証メッセージを送信する宛先 UDP ポート番号を指定します。この例では、ホストは radius2 で、認証ポートは 2003 です。デフォルトの認証ポートは 1812 で、有効な範囲は 0 ～ 65366 です。 |
| ステップ 4 | `switch(config)# radius-server host radius2 acct-port 2004` | RADIUS アカウンティング メッセージを送信する宛先 UDP ポート番号を指定します。デフォルトのアカウンティング ポートは 1813 で、有効な範囲は 0 ～ 65366 です。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 5 | `switch(config)# radius-server host radius2 accounting` | アカウンティングの目的のみに使用されるこのサーバを指定します。<br>(注)　**authentication** と **accounting** オプションのどちらも指定しないと、サーバは認証およびアカウンティングの両方の目的に使用されます。 |
| ステップ 6 | `switch(config)# radius-server host radius2 key 0 abcd` | 指定したサーバのクリア テキスト キーを指定します。キーの長さは 64 文字に制限されています。 |
| | `switch(config)# radius-server host radius2 key 4 da3Asda2ioyuoiuH` | 指定したサーバの暗号化キーを指定します。キーの長さは 64 文字に制限されています。 |

# RADIUS サーバにおける暗号の種類と事前共有キーのデフォルト値の概要

スイッチを RADIUS サーバに対して認証するには、RADIUS 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、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）。グローバル鍵は、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。

グローバル キーの割り当てを上書きするには、**radius-server host** コマンドで個々の RADIUS サーバの設定時に **key** オプションを明示的に使用する必要があります。

# RADIUS サーバにおける暗号の種類と事前共有キーのデフォルト値の設定

RADIUS 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 | `switch# config t` | 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 | `switch(config)# radius-server key AnyWord` | RADIUS クライアントおよびサーバ間の通信を認証する事前共有キー（AnyWord）を設定します。デフォルトはクリア テキストです。 |
| | `switch(config)# radius-server key 0 AnyWord` | RADIUS クライアントとサーバ間の通信を認証する、クリア テキスト（0 で指定）で記述された事前共有キー（AnyWord）を設定します。 |
| | `switch(config)# radius-server key 7 abe4DFeeweo00o` | RADIUS クライアントとサーバ間の通信を認証する、暗号化テキスト（7 で指定）で指定された事前共有キー（暗号化テキストで指定）を設定します。 |

# RADIUS サーバのタイムアウト間隔の設定

すべての RADIUS サーバに対して送信間のグローバル タイムアウト値を設定できます。

(注)　タイムアウト値が個々のサーバに設定されている場合は、グローバル設定された値よりもそれらの値が優先されます。

RADIUS サーバへの再送信間のタイムアウト値を指定するには、次の手順を実行してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server timeout 30` | スイッチがタイムアウト障害を宣言する前に、すべての RADIUS+ サーバからの応答を待機する、スイッチのグローバル タイムアウト期間（秒）を設定します。指定できる範囲は 1 ～ 1440 秒です。 |
| | `switch(config)# no radius-server timeout 30` | 送信時間をデフォルト値（1 秒）に戻します。 |

# RADIUS サーバのタイムアウト間隔および再送信のデフォルト値の設定

デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。RADIUS サーバに対してタイムアウトの値を設定することもできます。

RADIUS サーバがユーザを認証する試行回数を指定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server retransmit 3` | ローカル認証に戻る前に、スイッチが RADIUS サーバへの接続を試行する回数（3）を設定します。 |
| | `switch(config)# no radius-server retransmit` | デフォルトの試行回数（1）に戻します。 |

# RADIUS サーバ モニタリング パラメータの設定

RADIUS サーバをモニタするためのパラメータを設定できます。サーバを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

この項では、次のトピックについて取り上げます。


- テスト アイドル タイマーの設定（4-94 ページ）
- テスト ユーザ名の設定（4-94 ページ）
- デッド タイマーの設定（4-95 ページ）

## テスト アイドル タイマーの設定

テスト アイドル タイマーには、MDS スイッチがテスト パケットを送るまで RADIUS サーバが要求を受信しないでいる時間間隔を指定します。

(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 タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

アイドル タイマーを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server host 10.1.1.1 test idle-time 20` | テスト用のアイドル間隔の値を分で設定します。有効な範囲は 1 ～ 1440 分です。 |
| ステップ 3 | `switch(config)# no radius-server host 10.1.1.1 test idle-time 20` | デフォルト値(0 分)に戻します。 |

## テスト ユーザ名の設定

定期的な RADIUS サーバのステータス テストに使用するユーザ名とパスワードを設定できます。RADIUS サーバを監視するテスト メッセージを発行するために、テスト ユーザ名とパスワードを設定する必要はありません。デフォルトのテスト ユーザ名(test)とデフォルトのパスワード(test)を利用できます。

(注)　セキュリティ上の理由から、テスト ユーザ名を RADIUS データベースに存在する既存のユーザ名と同一にしないことを推奨します。

定期的な RADIUS サーバのステータス テストに使用するオプションのユーザ名とパスワードを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server host 10.1.1.1 test username testuser` | テスト ユーザ(testuser)にデフォルトのパスワード(test)を設定します。デフォルトのユーザ名は test です。 |
| | `switch(config)# no radius-server host 10.1.1.1 test username testuser` | テスト ユーザ名(testuser)を削除します。 |
| | `switch(config)# radius-server host 10.1.1.1 test username testuser password Ur2Gd2BH` | テスト ユーザ(testuser)を設定し、強力なパスワードを割り当てます。 |

## デッド タイマーの設定

デッド タイマーには、MDS スイッチが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻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の間隔を指定します。

(注)　デフォルトのデッド タイマー値は 0 分です。デッド タイマーの間隔が 0 分の場合、RADIUS サーバがサーバ グループの一部でグループのデッド タイム インターバルが 0 分を超えていないかぎり、RADIUS サーバ モニタリングは実行されません。(「サーバ グループ」セクション(4-70 ページ)を参照してください)。

(注)　デッド RADIUS サーバに RADIUS テスト メッセージが送信される前に、同サーバのデッド タイマーの期限が切れた場合、同サーバがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッド タイマーの時間よりも短いアイドル時間でテスト ユーザを設定します。

デッド タイマーを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server deadtime 30` | デッド タイマー間隔値を分で設定します。有効な範囲は 1 ～ 1440 分です。 |
| ステップ 3 | `switch(config)# no radius-server deadtime 30` | デフォルト値(0 分)に戻します。 |

# RADIUS サーバの概要

最大 64 台の RADIUS サーバを追加できます。RADIUS のキーは永続性ストレージに必ず暗号化して保存されます。実行コンフィギュレーションにも、暗号化されたキーが表示されます。新しい RADIUS サーバを設定する際は、デフォルト設定を利用することも、パラメータのいずれかを修正してデフォルトの RADIUS サーバ設定を上書きすることもできます。

## テスト アイドル タイマーの設定

テスト アイドル タイマーには、MDS スイッチがテスト パケットを送るまで RADIUS サーバが要求を受信しないでいる時間間隔を指定します。

(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 タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

テスト アイドル タイマーを設定するには、RADIUS サーバ モニタリング パラメータの設定(4-89 ページ)を参照してください。

## テスト ユーザ名の設定

定期的な RADIUS サーバのステータス テストに使用するユーザ名とパスワードを設定できます。RADIUS サーバを監視するテスト メッセージを発行するために、テスト ユーザ名とパスワードを設定する必要はありません。デフォルトのテスト ユーザ名（test）とデフォルトのパスワード（test）を利用できます。

（注）　セキュリティ上の理由から、テスト ユーザ名を RADIUS データベースに存在する既存のユーザ名と同一にしないことを推奨します。

定期的な RADIUS サーバのステータス テストに使用するオプションのユーザ名とパスワードの設定については、RADIUS サーバ モニタリング パラメータの設定（4-89 ページ）を参照してください。

# RADIUS サーバの検証の概要

Cisco SAN-OS リリース 3.0(1) では、RADIUS サーバを定期的に検証できます。スイッチは、設定されたユーザ名とパスワードを使用してテスト用認証をサーバに送信します。このテスト認証にサーバが応答しない場合、サーバは応答能力がないものと見なされます。

（注）　セキュリティ上の理由から、RADIUS サーバで設定されたユーザ名をテスト ユーザ名として使用しないことを推奨します。

サーバを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

# モニタリング用 RADIUS テスト メッセージの送信

RADIUS サーバをモニタするテスト メッセージを手動で送信できます。

RADIUS サーバにテスト メッセージを送信するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# test aaa server radius 10.10.1.1 test test` | デフォルトのユーザ名（test）とパスワード（test）を使用して RADIUS サーバにテスト メッセージを送信します。 |
| | `switch# test aaa server radius 10.10.1.1 testuser Ur2Gd2BH` | 設定されたテスト ユーザ名（testuser）とパスワード（Ur2Gd2BH）を使用して RADIUS サーバにテスト メッセージを送信します。<br>（注）　設定済みのユーザ名およびパスワードはオプションです（「テスト ユーザ名の設定」セクション（4-94 ページ）を参照）。 |

# ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、MDS スイッチは認証要求を RADIUS サーバ グループの最初のサーバに転送します。誘導要求オプションをイネーブルにすると、どの RADIUS サーバに認証要求を送信するかをユーザが指定できるようにスイッチを設定できます。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。*hostname* は設定した 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。

MDS スイッチにログインしているユーザが認証用の RADIUS サーバを選択できるようにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius-server directed-request` | ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。 |
| | `switch(config)# no radius-server directed-request` | サーバ グループの最初のサーバに認証要求を送信するように戻します(デフォルト)。 |

RADIUS への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show radius-server directed-request
disabled
```

# ベンダー固有属性の概要

Internet Engineering Task Force(IETF)ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバ間での ベンダー固有属性(VSA)の通信方式が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さ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-avpair** です。値は次の形式のストリングです。

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

**protocol** は、特定の認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 =(等号記号)、省略可能な属性の場合は *(アスタリスク)です。

Cisco MDS 9000 ファミリ スイッチに対するユーザ認証に RADIUS サーバを使用した場合、RADIUS プロトコルは、認証結果とともに認可情報などのユーザ属性を戻すように RADIUS サーバに指示します。この許可情報は、VSA で指定されます。

## VSA の形式

Cisco NX-OS ソフトウェアでは、次の VSA プロトコル オプションがサポートされています。

- **Shell** プロトコル：ユーザ プロファイル情報を提供するために Access-Accept パケットで使用されます。
- **Accounting** プロトコル：Accounting-Request パケットで使用されます。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。

次の属性が Cisco NX-OS ソフトウェアでサポートされています。

- **roles**：この属性は、ユーザが属すすべてのロールをリストします。値フィールドは、グループ名のスペース区切りリストを含む文字列です。たとえば、ユーザが **vsan-admin** および **storage-admin** ロールに属している場合、値フィールドは **vsan-admin storage-admin** になります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する 2 つの例を示します。

  ```
  shell:roles="network-admin vsan-admin"
  shell:roles*"network-admin vsan-admin"
  ```

  VSA が **shell:roles*"network-admin vsan-admin"** として指定されている場合は、この VSA がオプション属性としてフラグ設定されます。その他のシスコ デバイスはこの属性を無視します。

- **accountinginfo**：この属性は、標準の RADIUS アカウンティング プロトコルに含まれる属性を補足する追加的なアカウンティング情報を表します。この属性が送信されるのは、Account-Request フレームの VSA 部分に保管され、スイッチ上の RADIUS クライアントから送信される場合だけです。この属性を併用できるのは、アカウンティング プロトコル関連の PDU だけです。

## AAA サーバでの SNMPv3 の指定

ベンダー/カスタム属性 **cisco-av-pair** は、次のフォーマットを使用してユーザのロール マッピングを指定する場合に使用できます。

```
shell:roles="roleA roleB …"
```

（注）　Telnet または SSH により Fabric Manager または Device Manager を利用して Cisco MDS スイッチに正常にログインした場合、スイッチに AAA サーバベースの認証が設定されていると、1 日の有効期限で一時的な SNMP ユーザ エントリが自動的に作成されます。スイッチは、使用している Telnet または SSH ログイン名を SNMPv3 ユーザ名として SNMPv3 プロトコル データ ユニット（PDU）を認証します。管理ステーションは Telnet または SSH ログイン名を、SNMPv3 の **auth** および **priv** パスフレーズとして、一時的に使用できます。この一時的な SNMP ログインが許可されるのは、1 つ以上のアクティブな MDS シェル セッションが存在する場合だけです。指定時刻にアクティブなセッションが存在しない場合は、ログインが削除され、SNMPv3 の操作を実行できません。

**cisco-av-pair** 属性でロール オプションが設定されていない場合、デフォルトのユーザ ロールは network-operator になります。

また、VSA フォーマットには、オプションで SNMPv3 認証と機密保全プロトコルの属性を次のように指定できます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。これらのオプションが ACS サーバの **cisco-av-pair** 属性で指定されていない場合は、MD5 および DES がデフォルトで使用されます。

# RADIUS サーバの詳細の表示

設定された RADIUS パラメータを例 4-4 に示されているように表示するには、**show radius-server** コマンドを使用します。

*例 4-4　設定された RADIUS 情報の表示*

```
switch# show radius-server
Global RADIUS shared secret:*******
retransmission count:5
timeout value:10
following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
```

*例 4-5　設定済みの RADIUS サーバ グループ順序の表示*

```
switch# show radius-server groups
total number of groups:4
following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group Group1:
                server: Server3 on auth-port 1812, acct-port 1813
                server: Server5 on auth-port 1812, acct-port 1813
        group Group5:
```

# RADIUS サーバの統計情報の表示

**show radius-server statistics** コマンドを使用して、RADIUS サーバの統計情報を表示できます。

*例 4-6　RADIUS サーバ統計情報の表示*

```
switch# show radius-server statistics 10.1.3.2
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessful 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
        successful transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors:
```

**clear radius-server statistics 10.1.3.2** コマンドを使用して、RADIUS サーバの統計情報をクリアできます。

# ワンタイム パスワード サポート

ワンタイム パスワード サポート（OTP）は、1 回のログイン セッションまたはトランザクションに有効なパスワードです。OTP は、通常の（スタティック）パスワードに関連する多数の欠点を回避します。OTP によって対処される最も重大な欠点は、リプレイ攻撃のリスクにさらされないことです。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

ワンタイム パスワードは RADIUS や TACACS プロトコル デーモンに対してのみ適用できます。RADIUS プロトコル デーモンの場合、スイッチ側からの設定はありません。TACACS プロトコルの場合、次のコマンドで使用できる ascii 認証モードを有効にする必要があります。

```
aaa authentication login ascii-authentication
```

# TACACS+ サーバ モニタリング パラメータの設定

Cisco MDS スイッチは Terminal Access Controller Access Control System Plus（TACACS+）プロトコルを使用して、リモート AAA サーバと通信します。複数の TACACS+ サーバを設定し、タイムアウト値を指定できます。

この項では、次のトピックについて取り上げます。

# TACACS+ の概要

TACACS+ は、TCP（TCP ポート 49）を使用してトランスポート要件を満たすクライアント/サーバ プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチは、TACACS+ プロトコルを使用して中央から認証できます。TACACS+ には、RADIUS 認証と比較して次のような利点があります。

- 独立したモジュラ式 AAA ファシリティを提供します。認証を行わずに、認可を実行できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

# TACACS+ サーバのデフォルト設定

Fabric Manager を利用すると、スイッチとの通信を設定するどの TACACS+ サーバにも利用できるデフォルト設定をセットアップできます。デフォルト設定には次の内容が含まれます。

- 暗号の種類
- 事前共有キー
- タイムアウトの値
- 送信試行回数
- ユーザによるログイン時の TACACS+ サーバ指定の許可

# TACACS+ サーバにおける暗号の種類と事前共有キーのデフォルト値の概要

スイッチを TACACS+ サーバに対して認証するには、TACACS+ 事前共有キーを設定する必要があります。キーの長さは 64 文字に制限され、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）。グローバル鍵を設定して、スイッチにあるすべての TACACS+ サーバ コンフィギュレーションで使用するようにできます。

グローバル キーの割り当てを上書きするには、個々の TACACS+ サーバの設定時に **key** オプションを使用する必要があります。

# TACACS+ のイネーブル化

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで TACACS+ 機能がディセーブルに設定されています。ファブリック認証に関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。この機能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。

Cisco MDS スイッチの TACACS+ をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature tacacs+` | このスイッチの TACACS+ をイネーブルにします。 |
| | `switch(config)# no feature tacacs+` | このスイッチの TACACS+ をディセーブル（デフォルト）にします。 |

# TACACS+ サーバのアドレスの設定

設定されたサーバに秘密キーが設定されていない場合、グローバル キーが設定されていないと、警告メッセージが発行されます。サーバ キーが設定されていない場合は、グローバル キー（設定されている場合）が該当サーバで使用されます（「TACACS+ サーバのタイムアウト間隔および再送信のデフォルト値の設定」セクション（4-104 ページ）を参照）。

（注）　グローバル秘密キーにはドル記号（$）、パーセント記号（%）を使用できます。

TACACS+ サーバの IPv4 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server host 171.71.58.91` | 指定の IPv4 アドレスによって識別される TACACS+ サーバを設定します。 |
| | `switch(config)# no tacacs-server host 171.71.58.91` | IPv4 アドレスによって識別される特定の TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。 |
| ステップ 3 | `switch(config)# tacacs-server host 171.71.58.91 port 2` | すべての TACACS+ 要求に対し TCP ポートを設定します。 |
| | `switch(config)# no tacacs-server host 171.71.58.91 port 2` | サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。 |
| ステップ 4 | `switch(config)# tacacs-server host 171.71.58.91 key MyKey` | 指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。 |
| ステップ 5 | `switch(config)# tacacs-server host 171.71.58.91 timeout 25` | スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。 |

TACACS+ サーバの IPv6 アドレスおよびその他のオプションを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server host 2001:0DB8:800:200C::417A`<br>`warning: no key is configured for the host` | 指定の IPv6 アドレスによって識別される TACACS+ サーバを設定します。 |
| | `switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A` | IPv6 アドレスによって識別される特定の TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。 |
| ステップ 3 | `switch(config)# tacacs-server host 2001:0DB8:800:200C::417A port 2` | すべての TACACS+ 要求に対し TCP ポートを設定します。 |
| | `switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A port 2` | サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。 |
| ステップ 4 | `switch(config)# tacacs-server host 2001:0DB8:800:200C::417A key MyKey` | 指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。 |
| ステップ 5 | `switch(config)# tacacs-server host 2001:0DB8:800:200C::417A timeout 25` | スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。 |

TACACS+ サーバの DNS 名およびその他のオプションを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server host host1.cisco.com`<br>`warning: no key is configured for the host` | 指定の DNS 名によって識別される TACACS+ サーバを設定します。 |
| | `switch(config)# no tacacs-server host host1.cisco.com` | 指定の DNS 名によって識別される TACACS+ サーバを削除します。デフォルトでは、サーバは設定されません。 |
| ステップ 3 | `switch(config)# tacacs-server host host1.cisco.com port 2` | すべての TACACS+ 要求に対し TCP ポートを設定します。 |
| | `switch(config)# no tacacs-server host host1.cisco.com port 2` | サーバ アクセス用にポート 49 を使用する、工場出荷時のデフォルトに戻ります。 |
| ステップ 4 | `switch(config)# tacacs-server host host1.cisco.com key MyKey` | 指定されたドメイン名で指定された TACACS+ サーバを設定し、秘密キーを割り当てます。 |
| ステップ 5 | `switch(config)# tacacs-server host host1.cisco.com timeout 25` | スイッチがタイムアウト障害を宣言する前に、指定したサーバからの応答を待機する、スイッチのタイムアウト期間を設定します。 |

# グローバル秘密キーの設定

すべての TACACS+ サーバで秘密キーに対するグローバル値を設定できます。

(注)　秘密キーが個々のサーバに設定されている場合は、グローバル設定されたキーよりもそれらのキーが優先されます。

(注)　グローバル秘密キーにはドル記号($)、パーセント記号(%)を使用できます。

TACACS+ サーバの秘密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 | `switch# config t` | 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 | `switch(config)# tacacs-server key 7 3sdaA3daKUngd` | TACACS+ サーバにアクセスするには、グローバル秘密キー(暗号化形式)を割り当てます。この例では、使用されている暗号化された形式を表示するのに **7** を指定します。このグローバル キーと各サーバ キーが設定されていない場合、クリア テキスト メッセージが TACACS+ サーバに送信されます。 |
| | `switch(config)# no tacacs-server key oldPword` | 設定されたグローバル秘密キーを TACACS+ サーバにアクセスするために削除し、すべての設定済みのサーバへのアクセスを許可する工場出荷時のデフォルトに戻します。 |

# TACACS+ サーバのタイムアウト間隔および再送信のデフォルト値の設定

デフォルトでは、スイッチは TACACS+ サーバを 1 回だけ試行します。この回数は設定可能です。最大試行回数は、各サーバで 5 回です。TACACS+ サーバに対してタイムアウトの値を設定することもできます。

# タイムアウト値の設定

すべての TACACS+ サーバに対して送信間のグローバル タイムアウト値を設定できます。

(注)　タイムアウト値が個々のサーバに設定されている場合は、グローバル設定された値よりもそれらの値が優先されます。

TACACS+ サーバのグローバル タイムアウト値を設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server timeout 30` | スイッチがタイムアウト障害を宣言する前に、すべての TACACS+ サーバからの応答を待機する、スイッチのグローバル タイムアウト期間（秒）を設定します。指定できる範囲は 1 ～ 1440 秒です。 |
| | `switch(config)# no tacacs-server timeout 30` | 設定済みのタイムアウト期間を削除し、工場出荷時のデフォルトである 5 秒に戻します。 |

# TACACS+ サーバの概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで TACACS+ 機能がディセーブルに設定されています。TACACS+ サーバの設定を行うと、Fabric Manager または Device Manager によって自動的に TACACS+ の機能がイネーブルになります。

設定されたサーバに秘密キーが設定されていない場合、グローバル キーが設定されていないと、警告メッセージが発行されます。サーバ キーが設定されていない場合は、グローバル キー（設定されている場合）が該当サーバで使用されます。

（注）　Cisco MDS SAN-OS リリース 2.1(2) よりも前のバージョンでは、キーでドル記号（$）を使用できますが、二重引用符で囲む必要があります（例、"k$"）。パーセント記号（%）は使用できません。Cisco MDS SAN-OS リリース 2.1(2) 以降では、二重引用符なしでドル記号（$）を使用でき、パーセント記号（%）はグローバル秘密キーで使用できます。

すべての TACACS+ サーバで秘密キーに対するグローバル値を設定できます。

（注）　秘密キーが個々のサーバに設定されている場合は、グローバル設定されたキーよりもそれらのキーが優先されます。

# TACACS+ サーバ モニタリング パラメータの設定

TACACS+ サーバをモニタするためのパラメータを設定できます。

この項では、次のトピックについて取り上げます。

- TACACS+ テスト アイドル タイマーの設定（4-105 ページ）
- テスト ユーザ名の設定（4-106 ページ）
- デッド タイマーの設定（4-106 ページ）

## TACACS+ テスト アイドル タイマーの設定

テスト アイドル タイマーには、MDS スイッチがテスト パケットを送るまで TACACS+ サーバが要求を受信しないでいる時間間隔を指定します。

(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 タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

アイドル タイマーを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server host 10.1.1.1 test idle-time 20` | テスト用のアイドル間隔の値を分で設定します。有効な範囲は 1 ～ 1440 分です。 |
| ステップ 3 | `switch(config)# no tacacs-server host 10.1.1.1 test idle-time 20` | デフォルト値(0 分)に戻します。 |

## テスト ユーザ名の設定

定期的な TACACS+ サーバのステータス テストに使用するユーザ名とパスワードを設定できます。TACACS+ サーバを監視するためのユーザ名とパスワードを設定する必要はありません。デフォルトのテスト ユーザ名(test)とデフォルトのパスワード(test)を利用できます。

定期的な TACACS+ サーバのステータス テストに使用するオプションのユーザ名とパスワードを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server host 10.1.1.1 test username testuser` | テスト ユーザ(testuser)にデフォルトのパスワード(test)を設定します。デフォルトのユーザ名は test です。 |
| | `switch(config)# no tacacs-server host 10.1.1.1 test username testuser` | テスト ユーザ(testuser)を削除します。 |
| | `switch(config)# tacacs-server host 10.1.1.1 test username testuser password Ur2Gd2BH` | テスト ユーザ(testuser)を設定し、強力なパスワードを割り当てます。 |

## デッド タイマーの設定

デッド タイマーには、MDS スイッチが、TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻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の間隔を指定します。

(注)　デフォルトのデッド タイマー値は 0 分です。TACACS+ サーバ モニタリングは、TACACS+ サーバがデッド タイム インターバルが 0 分よりも長い、より大きなグループの一部でない限り、デッド タイマーの間隔が 0 分であれば実行されません。(「RADIUS サーバ モニタリング パラメータの設定」セクション(4-89 ページ)を参照)。

(注)　デッド TACACS+ サーバに TACACS+ テスト メッセージが送信される前に、同サーバのデッド タイマーの期限が切れた場合、同サーバがまだ応答していないとしても再度アライブ状態としてマークされます。このシナリオを回避するには、デッド タイマーの時間よりも短いアイドル時間でテスト ユーザを設定します。

デッド タイマーを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server deadtime 30` | デッド タイム インターバル値を分で設定します。有効な範囲は 1 ～ 1440 分です。 |
| | `switch(config)# no tacacs-server deadtime 30` | デフォルト値(0 分)に戻します。<br>(注)　デッド タイム インターバルが 0 分の場合、TACACS+ サーバがサーバ グループの一部でグループのデッド タイム インターバルが 0 分を超えていないかぎり、TACACS+ サーバ モニタリングは実行されません。(「RADIUS サーバ モニタリング パラメータの設定」セクション(4-89 ページ)を参照してください)。 |

# モニタリング用 TACACS+ テスト メッセージの送信

TACACS+ サーバをモニタするテスト メッセージを手動で送信できます。

TACACS+ サーバにテスト メッセージを送信するには、次の手順を実行します。

| コマンド | 目的 |
|---|---|
| `switch# test aaa server tacacs+ 10.10.1.1 test` | デフォルトのユーザ名(test)とパスワード(test)を使用して TACACS+ サーバにテスト メッセージを送信します。 |
| `switch# test aaa server tacacs+ 10.10.1.1 testuser Ur2Gd2BH` | 設定されたテスト ユーザ名とパスワードを使用して TACACS+ サーバにテスト メッセージを送信します。<br>設定済みのユーザ名およびパスワードはオプションです(「テスト ユーザ名の設定」セクション(4-106 ページ)を参照)。 |

# TACACS+ サーバからのパスワード エージング通知

パスワード エージング通知は、ユーザが TACACS+ アカウント経由で Cisco MDS 9000 スイッチに認証すると開始されます。パスワードの期限切れが近い、または期限が切れたときは、ユーザに通知されます。パスワードの期限が切れると、ユーザはパスワードを変更するように求められます。

（注）　Cisco MDS SAN-OS Release 3.2(1) では、TACACS+ だけがパスワード エージング通知をサポートしています。この機能をイネーブルにして RADIUS サーバを使用しようとすると、RADIUS は SYSLOG メッセージを生成し、認証はローカル データベースにフォールバックします。

パスワード エージング通知により、次の操作が容易になります。

- パスワードの変更：空のパスワードを入力することによってパスワードを変更できます。
- パスワード エージング通知：パスワード エージングを通知します。通知は、AAA サーバが構成され、MSCHAP および MSCHAPv2 がディセーブルになっている場合にだけ発生します。
- 期限切れ後のパスワードの変更：古いパスワードの期限が切れたら、パスワードの変更を開始します。AAA サーバから開始します。

（注）　MSCHAP および MSCHAPv2 認証をディセーブルにしていない場合、パスワード エージング通知は失敗します。

AAA サーバのパスワード エージング オプションをイネーブルにするには、次のコマンドを入力します。

```
aaa authentication login ascii-authentication
```

パスワード エージング通知を AAA サーバで有効または無効になっているかどうかを確認するには、次のコマンドを入力します。

```
show aaa authentication login ascii-authentication
```

# TACACS+ サーバの検証の概要

Cisco SAN-OS リリース 3.0(1) では、TACACS+ サーバを定期的に検証できます。スイッチは、設定されたテスト用ユーザ名とテスト用パスワードを使用してテスト用認証をサーバに送信します。このテスト認証にサーバが応答しない場合、サーバは応答能力がないものと見なされます。

（注）　セキュリティ上の理由から、TACACS+ サーバにはテスト用ユーザを設定しないことを推奨します。

サーバを定期的にテストするためにこのオプションを設定できるほか、1 回だけのテストを行うこともできます。

## TACACS+ サーバの定期的な検証

Fabric Manager を利用して TACACS+ サーバを定期的にテストするようにスイッチを設定する手順は「TACACS+ サーバ モニタリング パラメータの設定」セクション（4-100 ページ）を参照してください。

# ユーザによるログイン時の TACACS+ サーバ指定の概要

デフォルトでは、MDS スイッチは認証要求を TACACS+ サーバ グループの最初のサーバに転送します。どの TACACS+ サーバに認証要求を送信するかをユーザが指定できるようにスイッチを設定できます。この機能をイネーブルにすると、ユーザは *username@hostname* としてログインできます。*hostname* は設定した TACACS+ 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

# ユーザによるログイン時の TACACS+ サーバ指定の許可

MDS スイッチにログインしているユーザが認証用の TACACS+ サーバを選択できるようにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs-server directed-request` | ログイン時に、ユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。 |
| | `switch(config)# no tacacs-server directed-request` | サーバ グループの最初のサーバに認証要求を送信するように戻します(デフォルト)。 |

TACACS+ への誘導要求設定を表示するには、**show tacacs-server directed-request** コマンドを使用できます。

```
switch# show tacacs-server directed-request
disabled
```

# Cisco Secure ACS 5.x GUI でのロールの定義

**ポリシー要素**の GUI で次を入力します。

*表 4-3　ロールの定義*

| 属性 | 要件 | 値 |
|---|---|---|
| shell:roles | 任意 | network-admin |

# ロールのカスタム属性の定義

Cisco MDS 9000 ファミリ スイッチでは、ユーザが所属するロールの設定には、サービス シェルの TACACS+ カスタム属性を使用します。TACACS+ 属性は **name=value** 形式で指定します。このカスタム属性の属性名は、**cisco-av-pair** です。この属性を使用してロールを指定する例を次に示します。

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

オプションのカスタム属性を設定して、同じ AAA サーバを使用する MDS 以外のシスコ製スイッチとの競合を回避することもできます。

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

追加カスタム属性 shell:roles もサポートされています。

```
shell:roles="network-admin vsan-admin"
```

または

```
shell:roles*"network-admin vsan-admin"
```

(注)　TACACS+ カスタム属性は、Access Control Server（ACS）でさまざまなサービス（シェルなど）用に定義できます。Cisco MDS 9000 ファミリ スイッチでは、サービス シェルの TACACS+ カスタム属性を使用して、ロールを定義する必要があります。

## サポートされている TACACS+ サーバ パラメータ

Cisco NX-OS ソフトウェアでは現在、下記の TACACS+ サーバに対して次のパラメータをサポートしています。

- TACACS+

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

- Cisco ACS TACACS+

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

- Open TACACS+

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

# TACACS+ サーバの詳細の表示

例 4-7 から 4-12 に示すように、Cisco MDS 9000 ファミリ内のすべてのスイッチの TACACS+ サーバの設定に関する情報を表示するには、**show aaa** および **show tacacs-server** コマンドを使用します。

***例 4-7　TACACS+ サーバ情報の表示***

```
switch# show tacacs-server
Global TACACS+ shared secret:***********
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
```

```
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:*****
```

*例 4-8　AAA 認証情報の表示*

```
switch# show aaa authentication
         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

*例 4-9　AAA 認証ログイン情報の表示*

```
switch# show aaa authentication login error-enable
enabled
```

*例 4-10　設定した TACACS+ サーバ グループの表示*

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
        group TacacsServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

*例 4-11　すべての AAA サーバ グループの表示*

```
switch# show aaa groups
radius
TacServer
```

*例 4-12　TACACS+ サーバの統計情報の表示*

```
switch# show tacacs-server statistics 10.1.2.3
Server is not monitored

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

Authorization 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
```

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

## TACACS+ サーバ統計情報のクリア

**clear tacacs-server statistics 10.1.2.3** コマンドを使用してすべての TACACS+ サーバの統計情報をクリアできます。

# サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて同じプロトコル（RADIUS または TACACS+）に属している必要があります。設定した順序に従ってサーバが試行されます。

AAA サーバ モニタリング機能は AAA サーバを停止中としてマーク付けできます。スイッチが停止中の AAA サーバに要求を送信するまでの経過時間を分で設定できます（「AAA サーバのモニタリング」セクション（4-72 ページ）を参照してください）。

この項では、次のトピックについて取り上げます。



## サーバ グループの設定の概要

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。AAA ポリシーは CLI ユーザ、または Fabric Manager ユーザや Device Manager ユーザに設定できます。

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。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa group server radius RadServer`<br>`switch(config-radius)#` | RadServer という名前のサーバ 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 サブモードを開始します。 |
| | `switch(config)# no aaa group server radius RadServer` | 認証リストから RadServer という名前のサーバ グループを削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | `switch(config-radius)# server 10.71.58.91` | IPv4 アドレス 10.71.58.91 の RADIUS サーバをサーバ グループ RadServer 内で最初に実行されるように設定します。<br>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 | `switch(config-radius)# server 2001:0DB8:800:200C::417A` | IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバをサーバ グループ RadServer 内で最初に実行されるように設定します。 |
| | `switch(config-radius)# no server 2001:0DB8:800:200C::417A` | IPv6 アドレス 2001:0DB8:800:200C::417A の RADIUS サーバをサーバ グループ RadServer から削除します。 |
| ステップ 5 | `switch(config-radius)# exit` | コンフィギュレーション モードに戻ります。 |
| ステップ 6 | `switch(config)# aaa group server radius RadiusServer`<br>`switch(config-radius)#` | RadiusServer という名前のサーバ 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 サブモードを開始します。 |
| ステップ 7 | `switch(config-radius)# server ServerA` | ServerA を RadiusServer1 と呼ばれるサーバ グループ内で最初に試行されるように設定します。<br>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 8 | `switch(config-radius)# server ServerB` | ServerB をサーバ グループ RadiusServer1 内で 2 番目に試行されるように設定します。 |
| ステップ 9 | `switch(config-radius)# deadtime 30` | モニタリングのデッド タイムを 30 分に設定します。指定できる範囲は 0 ～ 1440 です。<br>（注）　個別の RADIUS サーバのデッド タイム インターバルが 0 よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。 |
| | `switch(config-radius)# no deadtime 30` | デフォルト値（0 分）に戻します。<br>（注）　RADIUS サーバ グループおよび RADIUS サーバの個別の TACACS+ サーバの両方のデッドタイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に RADIUS サーバをデッドとしてマークしません。さらにスイッチは、その RADIUS サーバに対するデッド サーバ モニタリングを実行しません。（「RADIUS サーバ モニタリング パラメータの設定」セクション（4-93 ページ）を参照してください）。 |

設定されたサーバ グループ順序を確認するには、**show radius-server groups** コマンドを使用します。

```
switch# show radius-server groups
total number of groups:2

following RAIDUS server groups are configured:
        group RadServer:
                server 10.71.58.91 on port 2
        group RadiusServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

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。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa group server tacacs+ TacacsServer1`<br>`switch(config-tacacs+)#` | TacacsServer1 という名前のサーバ グループを作成し、そのグループのサブモードを開始します。 |
| | `switch(config)# no aaa group server tacacs+ TacacsServer1` | 認証リストから TacacsServer1 という名前のサーバ グループを削除します。 |
| ステップ 3 | `switch(config-tacacs+)# server ServerA` | ServerA を TacacsServer1 と呼ばれるサーバ グループ内で最初に試行されるように設定します。<br>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 | `switch(config-tacacs+)# server ServerB` | ServerB をサーバ グループ TacacsServer1 内で 2 番目に試行されるように設定します。 |
| | `switch(config-tacacs+)# no server ServerB` | サーバの TacacsServer1 リスト内の ServerB を削除します。 |
| ステップ 5 | `switch(config-tacacs+)# deadtime 30` | モニタリングのデッド タイムを 30 分に設定します。指定できる範囲は 0 ～ 1440 です。<br>(注)　個別の TACACS+ サーバのデッド時間間隔が 0 よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。 |
| | `switch(config-tacacs+)# no deadtime 30` | デフォルト値(0 分)に戻します。<br>(注)　TACACS+ サーバ グループおよび TACACS+ サーバの個別の TACACS+ サーバの両方のデッド タイム間隔が 0 に設定されている場合、スイッチは定期モニタリングによって応答がないと判明した場合に TACACS+ サーバをデッドとしてマークしません。さらにスイッチは、その TACACS+ サーバに対するデッド サーバ モニタリングを実行しません。(TACACS+ サーバ モニタリング パラメータの設定 (4-100 ページ) を参照してください)。 |

(注)　MSCHPv2 認証がイネーブルの場合は、TACACS+ グループを設定できません。

## 無応答サーバのバイパス（回避）の概要

Cisco SAN-OS リリース 3.0(1) では、サーバ グループ内の無応答 AAA サーバをバイパスできます。スイッチが無応答のサーバを検出すると、ユーザを認証する際にそのサーバをバイパスします。この機能を利用すると、障害を起こしたサーバが引き起こすログインの遅延を最小限にとどめることができます。無応答サーバに要求を送信し、認証要求がタイムアウトするまで待つのではなく、スイッチはサーバ グループ内の次のサーバに認証要求を送信します。サーバ グループに応答できる他のサーバが存在しない場合は、スイッチは無応答サーバに対して認証を試み続けます。

# AAA サーバへの配信

MDS スイッチの RADIUS および TACACS+ の AAA 設定は、Cisco Fabric Services（CFS）を使用して配信できます。配信はデフォルトで無効になっています（『*Cisco MDS 9000 Family NX-OS System Management Configuration Guide*』および『*Cisco Fabric Manager System Management Configuration Guide*』を参照）。

配信をイネーブルにすると、最初のサーバまたはグローバル設定により、暗黙のセッションが開始されます。それ以降に入力されたすべてのサーバ コンフィギュレーション コマンドは、一時的なデータベースに保管され、データベースをコミットしたときに、ファブリック内のすべてのスイッチ（送信元スイッチを含む）に適用されます。サーバ キーおよびグローバル キーを除く、さまざまなサーバおよびグローバル パラメータが配信されます。サーバ キーおよびグローバル キーはスイッチに対する固有の秘密キーです。他のスイッチと共有しないでください。

(注)　サーバ グループ設定は配信されません。

この項では、次のトピックについて取り上げます。


- AAA サーバへの配信のイネーブル化（4-116 ページ）
- スイッチでの配信セッションの開始（4-116 ページ）
- セッション ステータスの表示（4-116 ページ）


(注)　AAA サーバ設定配布を行う MDS スイッチは、Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS Release 4.1(1) を実行している必要があります。

# AAA サーバへの配信のイネーブル化

アクティビティに参加できるのは、配信がイネーブルであるスイッチだけです。

RADIUS サーバでの配信をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius distribute` | このスイッチの RADIUS 設定の配信をイネーブルにします。 |
| | `switch(config)# no radius distribute` | このスイッチの RADIUS 設定の配信をディセーブルにします(デフォルト)。 |

TACACS+ サーバでの配信をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs+ distribute` | このスイッチの TACACS+ 設定の配信をイネーブルにします。 |
| | `switch(config)# no tacacs+ distribute` | このスイッチの TACACS+ 設定の配信をディセーブルにします(デフォルト)。 |

# スイッチでの配信セッションの開始

配信セッションは RADIUS/TACACS+ サーバの設定またはグローバル設定を開始した瞬間に始まります。たとえば、次の作業を実行すると、暗黙のセッションが開始されます。

- RADIUS サーバのグローバル タイムアウトの指定
- TACACS+ サーバのグローバル タイムアウトの指定

(注)　AAA サーバに関連する最初のコンフィギュレーション コマンドを発行すると、作成されたすべてのサーバおよびグローバル設定(配信セッションを開始する設定を含む)が一時バッファに格納されます。実行コンフィギュレーションには格納されません。

# セッション ステータスの表示

暗黙の配信セッションが開始すると、Fabric Manager から [Switches] > [Security] > [AAA] を開いて [RADIUS] または [TACACS+] を選択することで、セッションの状況を確認できます。

[CFS] タブに配信状況を表示するには、**show radius** コマンドを使用します。

```
switch# show radius distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

暗黙的な配信 セッションが開始されると、**show tacacs+ distribution status** コマンドを使用してセッション ステータスを確認できます。

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

# 配信する保留中の設定の表示

一時バッファに保存された RADIUS または TACACS+ のグローバル設定またはサーバ設定を、**show radius pending** コマンドを使用して表示する手順は次のとおりです。

```
switch(config)# show radius pending-diff
   +radius-server host testhost1 authentication accounting
   +radius-server host testhost2 authentication accounting
```

一時バッファに保存された TACACS+ のグローバル設定またはサーバ設定を表示するには、**show tacacs+ pending** コマンドを使用します。

```
switch(config)# show tacacs+ pending-diff
   +tacacs-server host testhost3
   +tacacs-server host testhost4
```

# 配信のコミット

一時バッファに格納された RADIUS または TACACS+ グローバル設定またはサーバ設定を、ファブリック内のすべてのスイッチ(送信元スイッチを含む)の実行コンフィギュレーションに適用できます。

RADIUS の設定変更をコミットするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius commit` | 実行コンフィギュレーションへの RADIUS の設定変更をコミットします。 |

TACACS+ の設定変更をコミットするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs+ commit` | 実行コンフィギュレーションへの TACACS+ の設定変更をコミットします。 |

# 配信セッションの廃棄

進行中のセッションの配信を廃棄すると、一時バッファ内の設定が廃棄されます。廃棄された配信は適用されません。

RADIUS セッションの進行中の配信を廃棄する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# radius abort` | 実行コンフィギュレーションへの RADIUS の設定変更を破棄します。 |

TACACS+ セッションの進行中の配信を廃棄する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# tacacs+ abort` | 実行コンフィギュレーションへの TACACS+ の設定変更を破棄します。 |

# セッションのクリア

継続的な CFS 配信セッション（ある場合）をクリアし、RADIUS 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear radius session** コマンドを入力します。

```
switch# clear radius session
```

継続的な CFS 配信セッション（ある場合）をクリアし、TACACS+ 機能のファブリックを最大限に引き出すには、ファブリック内のすべてのスイッチから **clear tacacs+ session** コマンドを入力します。

```
switch# clear tacacs+ session
```

# RADIUS および TACACS+ 設定のマージに関する注意事項

RADIUS および TACACS+ のサーバ設定およびグローバル設定は 2 つのファブリックがマージするときにマージされます。マージされた設定は CFS 配信がイネーブルであるスイッチに適用されます。

ファブリックのマージの際は次の条件に注意してください。

- サーバ グループはマージされません。
- サーバ キーおよびグローバル キーはマージ中に変更されません。
- マージされた設定には、CFS がイネーブルであるすべてのスイッチで見つかったすべてのサーバが含まれます。
- マージされた設定におけるタイムアウトと再送信のパラメータは、個々のサーバ設定とグローバル設定に指定されている値の最大値になります。

(注)　テスト パラメータは、CFS を通じて、TACACS+ デーモンのためだけに配信されます。ファブリックに NX-OS リリース 5.0 スイッチだけが含まれる場合、テスト パラメータは配信されます。5.0 バージョンを実行しているスイッチと NX-OS 4.x リリースを実行しているスイッチがファブリックに含まれる場合、テスト パラメータは配信されません。

注意　設定されたサーバ ポートの 2 つのスイッチの間で矛盾が存在する場合は、マージに失敗します。

**show radius distribution status** コマンドを使用して、RADIUS ファブリックのマージのステータスを参照できます（例 4-13 を参照）。

*例 4-13 RADIUS ファブリックのマージのステータスの表示*

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge response received
merge error: conflict: server dmtest2 has auth-port 1812 on this switch and 1999
on remote

last operation: enable
last operation status: success
```

**show tacacs+ distribution status** コマンドを使用して、TACACS+ ファブリックのマージのステータスを参照できます（例 4-14 を参照）。

*例 4-14 TACACS+ ファブリックのマージのステータスの表示*

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: enable
last operation status: success
```

# CHAP 認証

CHAP（チャレンジ ハンドシェイク認証プロトコル）は、業界標準の Message Digest 5（MD5）ハッシング スキームを使用して応答を暗号化するチャレンジレスポンス認証プロトコルです。CHAP は、さまざまなネットワーク アクセス サーバおよびクライアントのベンダーによって使用されています。ルーティングおよびリモート アクセスを実行しているサーバは、CHAP を必要とするリモート アクセス クライアントが認証されるように、CHAP をサポートしています。このリリースでは、認証方式として CHAP がサポートされています。

## CHAP 認証のイネーブル化

CHAP 認証を有効にするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authentication login chap enable` | CHAP ログイン認証をイネーブルにします。 |
| | `switch# no aaa authentication login chap enable` | CHAP ログイン認証をディセーブルにします。 |

CHAP 認証の設定を表示するには、**show aaa authentication login chap** コマンドを使用できます。

```
switch# show aaa authentication login chap
chap is disabled
```

# MSCHAP による認証

Microsoft チャレンジ ハンドシェイク認証プロトコル（MSCHAP）は Microsoft 版の CHAP です。

Cisco MDS 9000 ファミリ スイッチのユーザ ログインでは、異なるバージョンの MSCHAP を使用してリモート認証を実行できます。MSCHAP は RADIUS サーバまたは TACACS+ サーバでの認証に使用され、MSCHAPv2 は RADIUS サーバでの認証に使用されます。

## MSCHAP のイネーブル化の概要

デフォルトでは、スイッチはスイッチとリモート サーバの間でパスワード認証プロトコル（PAP）認証を使用します。MSCHAP をイネーブルにする場合は、MSCHAP のベンダー固有属性を認識するように RADIUS サーバを設定する必要があります。「ベンダー固有属性の概要」セクション（4-97 ページ）を参照してください。表 4-4 に MSCHAP に必要な RADIUS ベンダー固有属性を示します。

*表 4-4　MSCHAP 用の RADIUS ベンダー固有属性*

| ベンダー ID 番号 | ベンダー タイプ 番号 | ベンダー固有属性 | 説明 |
|---|---|---|---|
| 311 | 11 | MSCHAP-Challenge | AAA サーバから MSCHAP ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。 |
| 211 | 11 | MSCHAP-Response | MS-CHAP ユーザがチャレンジへの応答として提供したレスポンス値が格納されます。Access-Request パケットでしか使用されません。 |

# MSCHAP 認証のイネーブル化

MSCHAP 認証をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authentication login mschap enable` | MSCHAP ログイン認証をイネーブルにします。 |
| ステップ 3 | `switch# no aaa authentication login mschap enable` | MSCHAP ログイン認証をディセーブルにします。 |

MSCHAPv2 認証をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authentication login mschapv2 enable` | MSCHAPv2 ログイン認証をイネーブルにします。 |
| ステップ 3 | `switch# no aaa authentication login mschapv2 enable` | MSCHAPv2 ログイン認証をディセーブルにします。 |

(注)　パスワード エージング、MSCHAPv2、および MSCHAP 認証は、これらの認証のいずれかがディセーブルでないと失敗する可能性があります。

(注)　TACACS+ サーバで MSCHAPv2 認証をイネーブルにするコマンドを実行すると、警告メッセージが表示され、設定が失敗します。

MSCHAP 認証設定を表示するには、**show aaa authentication login mschap** コマンドを使用できます。

```
switch# show aaa authentication login mschap
mschap is disabled
```

MSCHAPv2 認証設定を表示するには、show aaa authentication login mschapv2 コマンドを使用できます。

```
switch# show aaa authentication login mschapv2
mschapv2 is enabled
```

# ローカル AAA サービス

システムによりユーザ名およびパスワードはローカルで保持され、パスワード情報は暗号化形式で格納されます。ユーザの認証は、ローカルに保存されているユーザ情報に基づいて実行されます。

ローカル ユーザとそのロールを設定するには、**username** コマンドを使用します。

ローカル アカウンティング ログを表示するには、**show accounting log** コマンドを使用します（例 4-15 を参照）。

*例 4-15　アカウンティング ログ情報の表示*

```
switch# show accounting log

Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=enabled telnet
Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=configure terminal ;
feature telnet (SUCCESS)
Thu Dec 10 06:19:35 2009:type=start:id=171.69.16.56@pts/1:user=admin:cmd=
Thu Dec 10 06:20:16 2009:type=stop:id=171.69.16.56@pts/1:user=admin:cmd=shell te
rminated gracefully
Thu Dec 10 06:20:20 2009:type=stop:id=console0:user=root:cmd=shell terminated gr
acefully
Thu Dec 10 06:29:37 2009:type=start:id=72.163.177.168@pts/1:user=admin:cmd=
Thu Dec 10 06:29:42 2009:type=update:id=72.163.177.168@pts/1:user=admin:cmd=pwd
(SUCCESS)
Thu Dec 10 06:32:49 2009:type=start:id=72.163.190.8@pts/2:user=admin:cmd=
```

# AAA 認証のディセーブル化

**none** オプションを利用するとパスワード確認をオフにできます。このオプションを設定すると、ユーザは有効なパスワードを提示しなくてもログインできます。ただし、ユーザは少なくとも Cisco MDS 9000 Family スイッチ上のローカル ユーザである必要があります。

**注意**　このオプションは注意して使用してください。このオプションを設定すると、あらゆるユーザがいつでもスイッチにアクセスできるようになります。

パスワード確認をディセーブルにするには、**aaa authentication login** コマンドで **none** オプションを使用します。

**username** コマンドを入力して作成したユーザは、Cisco MDS 9000 ファミリ スイッチのローカルに存在します。

# AAA 認証の表示

**show aaa authentication** コマンドでは、設定された認証方式が例 4-16 のように表示されます。

*例 4-16　認証情報の表示*

```
switch# show aaa authentication

    No AAA Authentication
    default: group TacServer local none
    console: local none
    iscsi: local
    dhchap: local
```

# アカウンティング サービスの設定

アカウンティングは、スイッチの管理セッションごとに保管されるログ情報を意味しています。この情報はトラブルシューティングと監査を目的としたレポートの生成に利用できます。アカウンティングは、(RADIUS を使用して) ローカルまたはリモートで実装できます。アカウンティング ログのデフォルトの最大サイズは 250,000 バイトです。これは変更できません。

ヒント　Cisco MDS 9000 ファミリ スイッチは、interim-update RADIUS アカウンティング要求パケットを使用して、アカウンティング ログ情報を RADIUS サーバに送信します。RADIUS サーバは、これらのパケットで送信された情報を記録するように、適切に設定されている必要があります。一部のサーバは、通常、AAA クライアントの設定内に log update/watchdog packets フラグを持ちます。適切な RADIUS アカウンティングを確実に実行するには、このフラグをオンにします。

(注)　コンフィギュレーション モードで実行された設定操作は、自動的にアカウンティング ログに記録されます。重要なシステム イベント (設定保存やシステム スイッチオーバーなど) もアカウンティング ログに記録されます。

# アカウンティング設定の表示

設定したアカウント情報を表示するには **show accounting** コマンドを使用します。例 4-17 ～ 4-19 を参照してください。表示されるローカル アカウンティング ログのサイズを指定するには、**show accounting log** コマンドを使用します。デフォルトでは、アカウンティング ログの約 250 KB が表示されます。

***例 4-17　設定されたアカウンティング パラメータの 2 つの例の表示***

```
switch# show accounting config
show aaa accounting
               default: local

switch# show aaa accounting
               default: group rad1
```

***例 4-18　60,000 バイトのアカウンティング ログの表示***

```
switch# show accounting log 60000
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
...
```

*例 4-19　ログ ファイル全体の表示*

```
switch# show accounting log
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:17 1981:stop:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:start:snmp_348530298_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:stop:snmp_348530298_171.71.150.105:admin:
...
Fri Jan 16 23:37:02 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 23:37:26 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Fri Jan 16 23:53:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server3
Fri Jan 16 23:54:00 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server5
Fri Jan 16 23:54:22 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerA
Fri Jan 16 23:54:25 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerB
Fri Jan 16 23:55:03 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Sat Jan 17 00:01:41 1981:start:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:41 1981:stop:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:start:snmp_348537702_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:stop:snmp_348537702_171.71.58.100:admin:
...
```

# アカウンティング ログのクリア

現在のログの内容を消去するには、**clear accounting log** コマンドを使用します。

```
switch# clear accounting log
```

# Cisco Access Control Servers の設定

Cisco Access Control Server（ACS）は TACACS+ と RADIUS のプロトコルを利用して、セキュアな環境を作り出す AAA サービスを提供します。AAA サーバを使用する際のユーザ管理は、通常 Cisco ACS を使用して行われます。図 4-3、図 4-4、図 4-5、および図 4-6 に、RADIUS または TACACS+ を利用した ACS サーバの network-admin ロールおよび複数ロールのユーザ セットアップ設定を示します。

*図 4-3　RADIUS を使用する場合の network-admin ロールの設定*

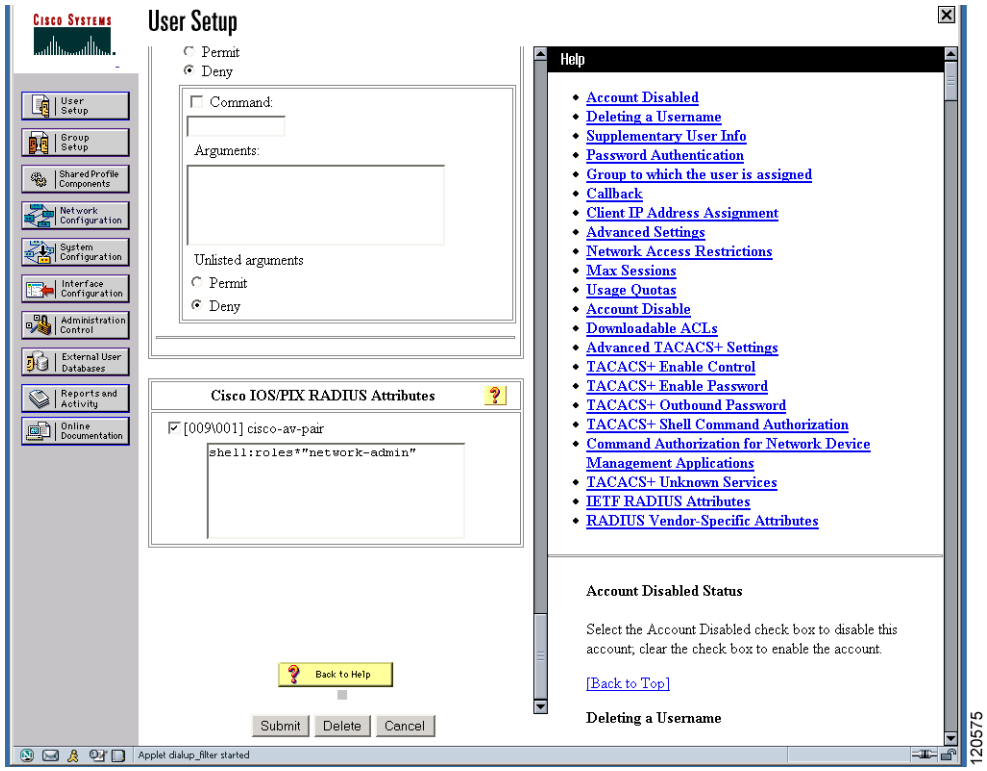


*図 4-4　　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定*

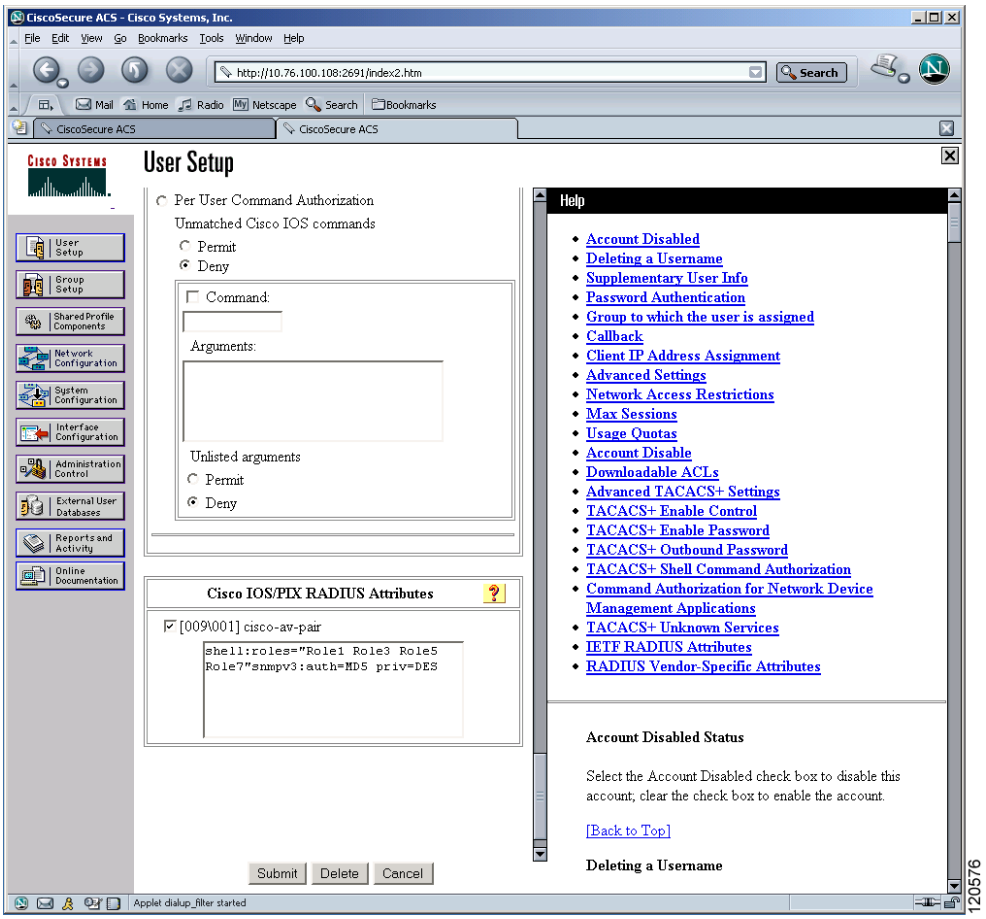


*図 4-5　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定*

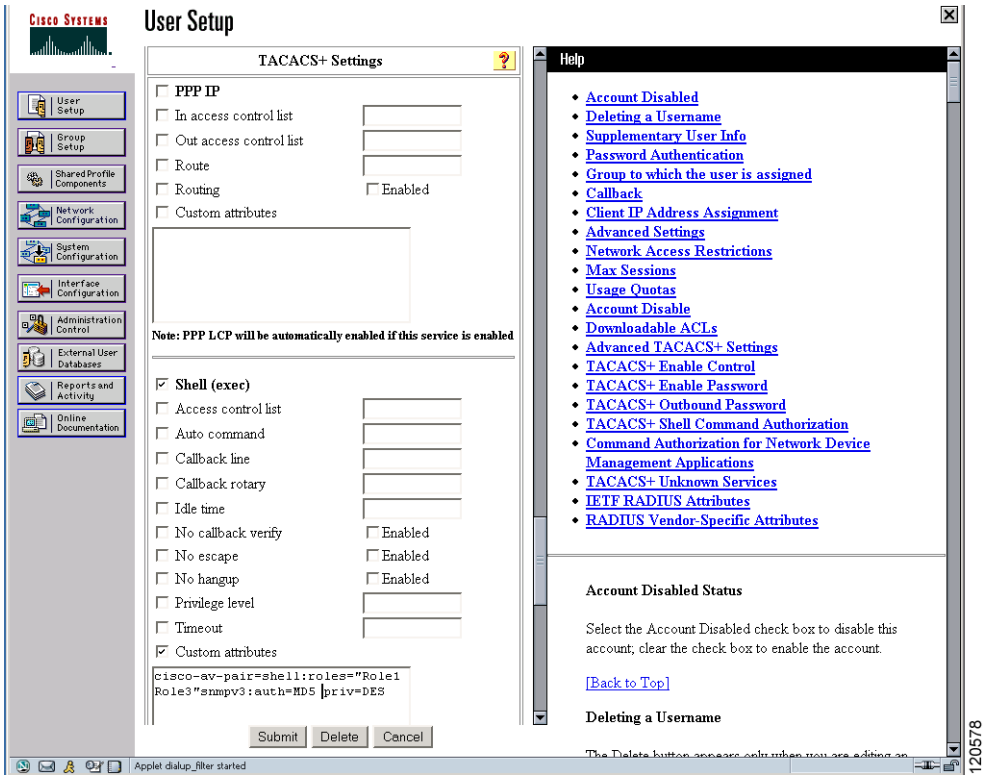
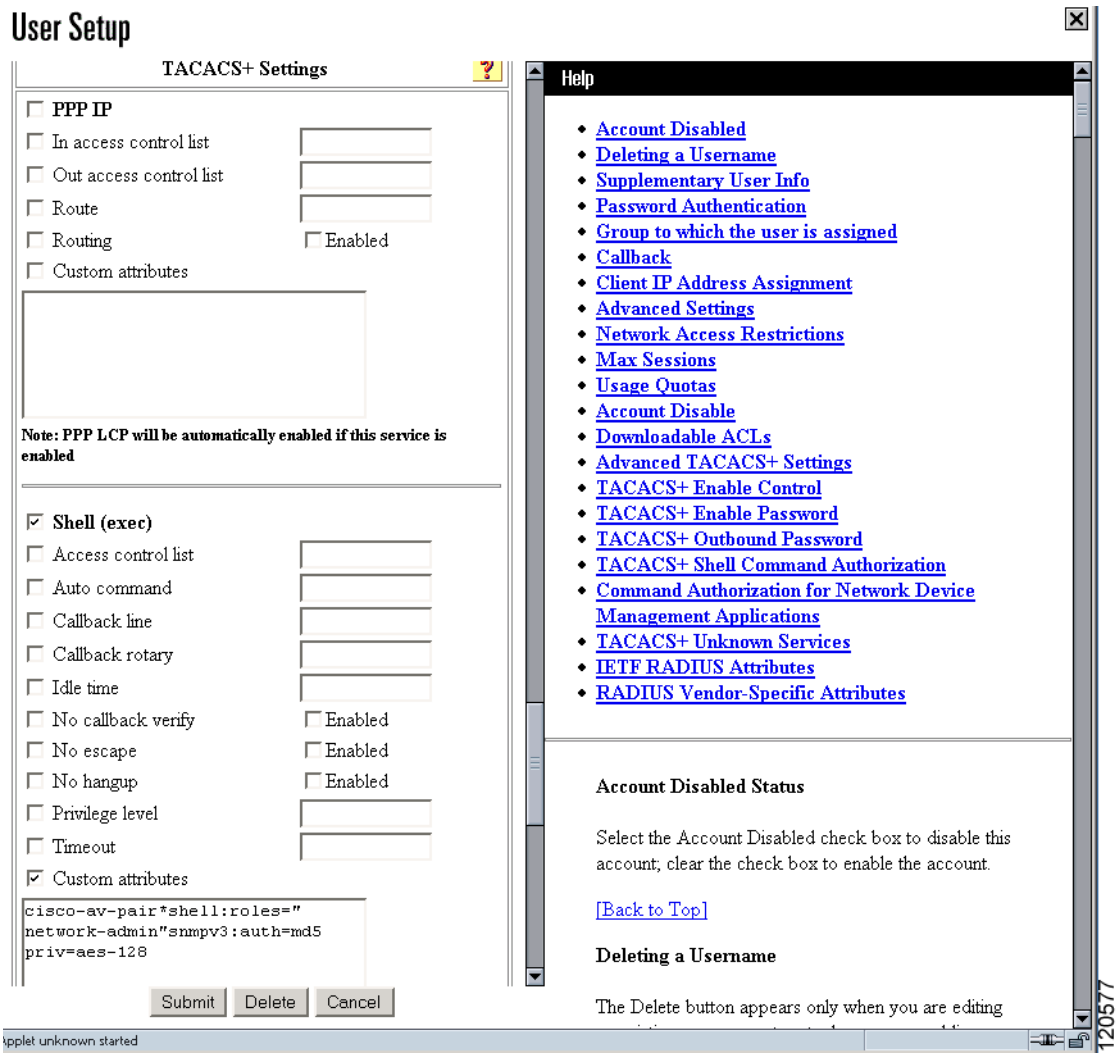


*図 4-6　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定*




# デフォルト設定

表 4-5 に、スイッチのすべてのスイッチ セキュリティ機能のデフォルト設定を示します。

*表 4-5　スイッチ セキュリティのデフォルト設定*

| パラメータ | デフォルト |
|---|---|
| Cisco MDS スイッチでのロール | ネットワーク オペレータ（network-operator） |
| AAA 設定サービス | ローカル |
| 認証ポート | 1812 |
| アカウンティング ポート | 1813 |
| 事前共有キーの送受信 | クリア テキスト |

*表 4-5　スイッチ セキュリティのデフォルト設定（続き）*

| パラメータ | デフォルト |
|---|---|
| RADIUS サーバのタイムアウト | 1 秒 |
| RADIUS サーバ再試行 | 1 回 |
| 許可 | ディセーブル |
| デフォルトの AAA ユーザ ロール | enabled |
| RADIUS サーバへの誘導要求 | ディセーブル |
| TACACS+ | ディセーブル |
| TACACS+ サーバ | 未設定 |
| TACACS+ サーバのタイムアウト | 5 秒 |
| TACACS+ サーバへの誘導要求 | ディセーブル |
| AAA サーバへの配信 | ディセーブル |
| アカウンティング ログ サイズ | 250 KB |


# IPv4 および IPv6 のアクセス コントロール リストの設定

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバ チャネル インターフェイスの間で IP バージョン 4（IPv4）トラフィックをルーティングできます。IP スタティック ルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム（NMS）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス（mgmt0）での IP 転送
- IP over Fibre Channel（IPFC）機能を使用したインバンド ファイバ チャネル インターフェイス上の IP 転送：IPFC は、IP フレームをカプセル化手法を利用してファイバ チャネル上で転送するための方法を定義しています。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

スイッチは仮想ルータ冗長プロトコル（VRRP）機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイ スイッチに提供する、再起動可能なアプリケーションです。

IPv4 アクセス コントロール リスト（IPv4-ACL および IPv6-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

この章は、次の項で構成されています。

# IPv4 および IPv6 のアクセス コントロール リストの概要

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバ チャネル インターフェイスの間で IP バージョン 4（IPv4）トラフィックをルーティングできます。IP スタティック ルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム（NMS）に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス（mgmt0）での IP 転送
- IP over Fibre Channel（IPFC）機能を使用したインバンド ファイバ チャネル インターフェイス上の IP 転送：IPFC は、IP フレームをカプセル化手法を利用してファイバ チャネル上で転送するための方法を定義しています。IP フレームはファイバ チャネル フレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバ チャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング（デフォルト ルーティングおよびスタティック ルーティング）：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

IPv4 アクセス コントロール リスト（IPv4-ACL および IPv6-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

# IPv4-ACL および IPv6-ACL 設定に関する考慮事項

Cisco MDS 9000 ファミリのスイッチまたはディレクタに IPv4-ACL または IPv6-ACL を設定する場合は、次の注意事項に従ってください。

- IPv4-ACL または IPv6-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

**注意**　ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL がすでに設定されている場合は、このインターフェイスをイーサネット ポートチャネル グループに追加できません。IPv4-ACL または IPv6-ACL は、ポートチャネル グループ内の 1 つのメンバーだけに適用しないでください。IPv4-ACL または IPv6-ACL はチャネル グループ全体に適用します。

- 条件の順序は正確に設定してください。IPv4-ACL または IPv6-ACL フィルタは IP フローに順番に適用されるので、最初の一致によって動作が決定されます。以降の一致は考慮されません。最も重要な条件を最初に設定してください。いずれの条件とも一致しなかった場合、パケットは廃棄されます。
- IP ACL を適用する IP ストレージのギガビット イーサネット ポートでは、暗黙的な deny は有効にならないため、明示的な deny を設定してください。

# フィルタの内容について

IP フィルタには、プロトコル、アドレス、ポート、ICMP タイプ、およびサービス タイプ（TS）に基づく IP パケットの一致規則が含まれます。

この項では、次のトピックについて取り上げます。



## プロトコル情報

各フィルタには、プロトコル情報が必要です。この情報により、IP プロトコルの名前または番号を識別します。IP プロトコルは、次のいずれかの方法で指定できます。

- 0 ～ 255 の整数を指定します。この番号は IP プロトコルを表します。
- プロトコルの名前を指定しますが、インターネット プロトコル（IP）、伝送制御プロトコル（TCP）、ユーザ データグラム プロトコル（UDP）、および Internet Control Message Protocol（ICMP）には限定されません。

（注）　ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL を設定する場合は、TCP または ICMP オプションだけを使用してください。

## アドレス情報

各フィルタには、アドレス情報が必要です。アドレス情報により、次の詳細を識別します。

- 送信元：パケット送信元のネットワークまたはホストのアドレス
- 送信元ワイルドカード：送信元に適用されるワイルドカード ビット
- 宛先：パケットの送信先となるネットワークまたはホストの番号
- 宛先ワイルドカード：宛先に適用されるワイルドカード ビット

送信元/送信元ワイルドカードおよび宛先/宛先ワイルドカードは、次のいずれかの方法で指定します。

- 4 つに区切られたドット付き 10 進表記の 32 ビット数を使用します（10.1.1.2/0.0.0.0 はホスト 10.1.1.2 と同じ）。
  - 各ワイルドカード ビットをゼロに設定する場合には、パケットの IPv4 アドレス内の対応するビット位置と送信元の対応するビット位置で、ビット値が正確に一致している必要があります。

  - 各ワイルドカード ビットを 1 に設定する場合は、パケットの IPv4 または IPv6 アドレス内の対応する位置のビット値が 0 および 1 のいずれであっても、現在のアクセス リスト エントリと一致すると見なされます。無視するビット位置に 1 を入れます。たとえば、0.0.255.255 の場合、送信元の最初の 16 ビットだけが完全に一致する必要があります。複数のワイルドカード ビットを 1 に設定する場合、これらのビットが送信元ワイルドカード内で連続している必要はありません。たとえば、送信元ワイルドカード 0.255.0.64 は有効です。

- 送信元/送信元ワイルドカードまたは宛先/宛先ワイルドカード（0.0.0.0/255.255.255.255）の短縮形として、**any** オプションを使用します。

# ポート情報

ポート情報はオプションです。送信元ポートと宛先ポートを比較するためには、**eq**（等号）オプション、**gt**（より大きい）オプション、**lt**（より小さい）オプション、または **range**（ポート範囲）オプションを使用します。ポート情報は次のいずれかの方法で指定できます。

- ポート番号を指定します。ポート番号の範囲は 0 ～ 65535 です。表 5-1 に、関連 TCP ポートおよび UDP ポートについて、Cisco NX-OS ソフトウェアが認識するポート番号を示します。
- TCP または UDP ポートの名前を次のように指定します。
  - TCP ポート名は、TCP をフィルタリングする場合にかぎって使用できます。
  - UDP ポート名は、UDP をフィルタリングする場合にかぎって使用できます。

*表 5-1　TCP および UDP のポート番号*

| プロトコル | ポート | 番号 |
|---|---|---|
| UDP | dns | 53 |
| | tftp | 69 |
| | ntp | 123 |
| | radius アカウンティング | 1646 または 1813 |
| | radius 認証 | 1645 または 1812 |
| | snmp | 161 |
| | snmp-trap | 162 |
| | syslog | 514 |

*表 5-1　TCP および UDP のポート番号(続き)*

| プロトコル | ポート | 番号 |
|---|---|---|
| TCP[1] | ftp | 20 |
| | ftp-data | 21 |
| | ssh | 22 |
| | Telnet | 23 |
| | smtp | 25 |
| | tasacs-ds | 65 |
| | www | 80 |
| | sftp | 115 |
| | http | 143 |
| | wbem-http | 5988 |
| | wbem-https | 5989 |

1. TCP コネクションが確立済みの場合は、**established** オプションを使用して適合するものを探してください。TCP データグラムが ACK、FIN、PSH、RST または URG のコントロール ビット セットを持つ場合は、適合と見なされます。

# ICMP 情報

オプションとして IP パケットは次の ICMP 条件に基づいて選別できます。

- icmp-type：ICMP メッセージ タイプは 0 から 255 の番号から 1 つ選びます。
- icmp-code：ICMP メッセージ コードは 0 から 255 の番号から 1 つ選びます。

表 5-2 に各 ICMP タイプの値を示します。

*表 5-2　ICMP タイプの値*

| ICMP タイプ[1] | コード |
|---|---|
| echo | 8 |
| echo-reply | 0 |
| destination unreachable | 3 |
| traceroute | 30 |
| time exceeded | 11 |

1. ICMP リダイレクト パケットは必ず拒否されます。

# ToS 情報

オプションとして IP パケットは次の ToS 条件に基づいて選別できます。

- ToS レベル：レベルは 0 から 15 の番号で指定します。
- ToS 名：max-reliability、max-throughput、min-delay、min-monetary-cost、および normal から選択できます。

# IPv4-ACL または IPv6-ACL の作成

スイッチに入ったトラフィックは、スイッチ内でフィルタが現れる順番に従って IPv4-ACL または IPv6-ACL のフィルタと比較されます。新しいフィルタは IPv4-ACL または IPv6-ACL の末尾に追加されます。スイッチは合致するまで照合を続けます。フィルタの最後に達して合致するものがなかった場合、そのトラフィックは拒否されます。そのため、フィルタの最上部にはヒットする確率の高いフィルタを置く必要があります。許可されないトラフィックに対して、*implied deny* が用意されています。1 つの拒否エントリしか持たないシングルエントリの IPv4-ACL または IPv6-ACL には、すべてのトラフィックを拒否する効果があります。

IPv4-ACL または IPv6-ACL を設定する手順は次のとおりです。

**ステップ 1**　IPv4-ACL または IPv6-ACL の作成には、フィルタ名と 1 つ以上のアクセス条件を指定します。フィルタには、条件に合致する発信元と宛先のアドレスが必要です。適切な粒度を設定するために、オプションのキーワードを使用できます。

**（注）**　フィルタのエントリは順番に実行されます。エントリは、リストの最後にだけ追加できます。正しい順番でエントリを追加するように注意してください。

**ステップ 2**　指定したインターフェイスにアクセス フィルタを適用します。

# IPv4-ACL または IPv6-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| **ステップ 1** | `switch# config t` | 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** | `switch(config)# ip access-list List1 permit ip any any` | List1 と呼ばれる IPv4-ACL を設定し、任意の送信元アドレスから任意の宛先アドレスへの IP トラフィックを許可します。 |
| | `switch(config)# no ip access-list List1 permit ip any any` | List1 と呼ばれる IPv4-ACL を削除します。 |
| **ステップ 3** | `switch(config)# ip access-list List1 deny tcp any any` | 送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するように List1 を更新します。 |

IPv6-ACL を作成するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# ipv6 access-list List1`<br>`switch(config-ipv6-acl)#` | List1 という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。 |
| | `switch(config)# no ipv6 access-list List1` | List1 と呼ばれる IPv6-ACL とそのエントリをすべて削除します。 |
| ステップ 3 | `switch(config-ipv6-acl)# permit ipv6 any any` | 送信元アドレスから宛先アドレスへの IPv6 トラフィックを許可するエントリを追加します。 |
| | `switch(config-ipv6-acl)# no permit ipv6 any any` | IPv6-ACL からエントリを削除します。 |
| | `switch(config-ipv6-acl)# deny tcp any any` | 送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するエントリを追加します。 |

管理アクセスを規制する IPv4-ACL を定義する手順は次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ip access-list restrict_mgmt permit ip 10.67.16.0 0.0.0.255 any` | 10.67.16.0/24 サブネットのすべてのアドレスを許可する、restrict_mgmt という名前のエントリを IPv4-ACL に定義します。 |
| ステップ 3 | `switch(config)# ip access-list restrict_mgmt permit icmp any any eq 8` | デバイスが MDS（icmp type 8）に ping を実行できるようにする、restrict_mgmt という名前のエントリを IPv4-ACL に追加します。 |
| ステップ 4 | `switch(config)# ip access-list restrict_mgmt deny ip any any` | 明示的に restrict_mgmt という名前のアクセス リストへの他のすべてのアクセスをブロックします。 |

管理アクセスを規制する IPv6-ACL を定義する手順は次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ip access-list RestrictMgmt`<br>`switch(config-ipv6-acl)#` | RestrictMgmt という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config)# permit ipv6 2001:0DB8:800:200C::/64 any` | 2001:0DB8:800:200C::/64 プレフィクスのすべてのアドレスを許可するエントリを定義します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | `switch(config)# permit icmp any any eq 8` | デバイスが MDS（ICMP type 8）に ping を実行できるようにするエントリを追加します。 |
| ステップ 5 | `switch(config)# deny ipv6 any any` | 明示的に他のすべての IPv6 アクセスをブロックします。 |

IPv4-ACL 用のオペランドとポート オプションを使用するには、次の手順を実行してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any` | 1.2.3.0 から送信元ポート 5 を経由する宛先への TCP トラフィックを拒否します。 |

IPv6-ACL 用のオペランドとポート オプションを使用するには、次の手順を実行してください。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ip access-list List2 deny tcp 2001:0DB8:800:200C::/64 eq port 5 any` | 2001:0DB8:800:200C::/64 からソース ポート 5 を経由し、任意の宛先までの TCP トラフィックを拒否します。 |

# 既存の IPv4-ACL または IPv6-ACL への IP フィルタの追加

IPv4-ACL または IPv6-ACL の作成後に、続く IP フィルタを IPv4-ACL または IPv6-ACL の最後に追加できます。IPv4-ACL または IPv6-ACL の中間にはフィルタを挿入できません。設定された各エントリは、自動的に IPv4-ACL または IPv6-ACL の最後に追加されます。

既存の IPv4-ACL にエントリを追加するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port telnet` | Telnet トラフィック用の TCP を許可します。 |
| ステップ 3 | `switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port http` | HTTP トラフィック用の TCP を許可します。 |
| ステップ 4 | `switch(config)# ip access-list List1 permit udp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0` | すべてのトラフィック用の UDP を許可します。 |

既存の IPv6-ACL にエントリを追加するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **ipv6 access-list List2**<br>switch(config-ipv6-acl)# | IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | switch(config-ipv6-acl)# **permit ip 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 23** | Telnet トラフィック用の TCP を許可します。 |
| ステップ 4 | switch(config-ipv6-acl)# **permit tcp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 143** | HTTP トラフィック用の TCP を許可します。 |
| ステップ 5 | switch(config-ipv6-acl)# **permit udp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64** | すべてのトラフィック用の UDP を許可します。 |

# 既存の IPv4-ACL または IPv6-ACL からの IP フィルタの削除

設定されたエントリを IPv4-ACL から削除するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t** | 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 | switch(config)# **no ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any** | IPv4-ACL（List2）からこのエントリを削除します。 |
| | switch(config)# **no ip access-list x3 deny ip any any** | IPv4-ACL（x3）からこのエントリを削除します。 |
| | switch(config)# **no ip access-list x3 permit ip any any** | IPv4-ACL（x3）からこのエントリを削除します。 |

設定したエントリを IPv6-ACL から削除するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **ipv6 access-list List3**<br>switch(config-ipv6-acl)# | IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | switch(config-ipv6-acl)# **no deny tcp 2001:0DB8:800:2010::/64 eq port 5 any** | IPv6-ACL から TCP エントリが削除されます。 |
| ステップ 4 | switch(config-ipv6-acl)# **no deny ip any any** | IPv6-ACL から IP エントリが削除されます。 |

# IPv4-ACL または IPv6-ACL の設定の確認

設定された IPv4-ACL の内容を表示するには、**show ip access-list** コマンドを使用します。IPv4-ACL は 1 つ以上のフィルタを設定できます。（例 5-1 を参照）。

*例 5-1　IPv4 ACL 用に設定されたフィルタの表示*

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

設定されたアクセス フィルタの内容を表示するには、**show ipv6 access-list** コマンドを使用します。各アクセス フィルタには、複数の条件を設定できます。（例 5-2 および例 5-3 を参照）。

*例 5-2　設定した IPv6-ACL の表示*

```
switch# show ipv6 access-list
switch# show ipv6 access-list

IPv6 access list copp-system-acl-bgp6
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
IPv6 access list copp-system-acl-icmp6
        10 permit icmp any any echo-request
        20 permit icmp any any echo-reply
IPv6 access list copp-system-acl-icmp6-msgs
        10 permit icmp any any router-advertisement
        20 permit icmp any any router-solicitation
        30 permit icmp any any nd-na
        40 permit icmp any any nd-ns
        50 permit icmp any any mld-query
        60 permit icmp any any mld-report
        70 permit icmp any any mld-reduction
IPv6 access list copp-system-acl-ntp6
        10 permit udp any any eq ntp
        20 permit udp any eq ntp any
IPv6 access list copp-system-acl-ospf6
        10 permit 89 any any
IPv6 access list copp-system-acl-pim6
        10 permit 103 any ff02::d/128
        20 permit udp any any eq pim-auto-rp
IPv6 access list copp-system-acl-radius6
```

*例 5-3　指定した IPv6-ACL の概要の表示*

```
switch# show ipv6 access-list abc
```

# IP-ACL ログ ダンプの読み取り

廃棄されたエントリに合致するパケットに関する情報をログに記録するには、フィルタ条件の最後に **log-deny** オプションを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。

(注)　ロギング先でこれらのメッセージをキャプチャするには、カーネルおよび ipacl ファシリティに重大度 7 を設定し、ロギング先のログファイル、モニタに重大度 7 を設定する必要があります。次に例を示します。

```
switch# config t
switch(config)# logging level kernel 7
switch(config)# logging level ipacl 7
switch(config)# logging logfile message 7
```

入力 ACL に対しては、ログは無加工の MAC 情報を表示します。キーワード「MAC=」は、MAC アドレス情報を持つイーサネットの MAC フレームの表示を意味しません。ログにダンプされるレイヤ 2 の MAC レイヤ情報を意味します。出力 ACL に対しては、無加工のレイヤ 2 情報はログに記録されません。

入力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:00:08:00:45:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

出力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.12 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

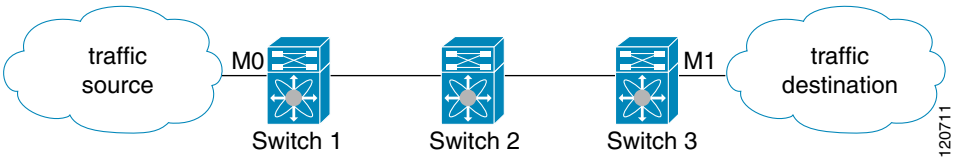
# インターフェイスへの IP-ACL の適用

IP-ACL は適用しなくても定義できます。しかし、IP-ACL はスイッチのインターフェイスに適用されるまで効果は出ません。IP-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。

ヒント　トラフィックの送信元に一番近いインターフェイスに IP-ACL を適用してください。

送信元から宛先へ流れるトラフィックを遮断しようとする場合は、スイッチ 3 の M1 に対するアウトバンド フィルタの代わりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます（図 5-1 を参照）。

*図 5-1　インバウンド インターフェイス上のトラフィックの拒否*




**access-group** オプションによりインターフェイスへのアクセスを規制できます。各インターフェイスは、1 つの方向につき 1 つの IP-ACL にしか関連付けできません。入力方向には、出力方向とは異なる IP-ACL を持たせることができます。IP-ACL はインターフェイスに適用されたときにアクティブになります。

**ヒント**　IP-ACL の中の条件は、インターフェイスに適用する前にすべて作成しておいてください。

**注意**　IP-ACL を作成前にインターフェイスに適用すると、IP-ACL が空白であるため、そのインターフェイスのすべてのパケットが排除されます。

スイッチにおいては、用語としての*イン*、*アウト*、*送信元*、*宛先*は次の意味になります。

- イン：インターフェイスに到達してスイッチ内を通過するトラフィック。送信元はそのトラフィックが発信された場所で、宛先は送信される先（ルータの反対側で）を意味します。

**ヒント**　入力トラフィック用インターフェイスに適用された IP-ACL はローカルおよびリモート両方のトラフィックに作用します。

- アウト：スイッチを通過済みで、インターフェイスから離れたトラフィック。送信元はこれが送信された場所であり、宛先は送信先を意味します。

**ヒント**　出力トラフィック用インターフェイスに適用された IP-ACL はローカル トラフィックにだけ作用します。

インターフェイスに IPv4-ACL を適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# interface mgmt0`<br>`switch(config-if)#` | 管理インターフェイスを設定します（mgmt0）。 |
| ステップ 3 | `switch(config-if)# ip access-group restrict_mgmt` | 入力および出力の両方のトラフィック（デフォルト）の restrict_mgmt と呼ばれる IPv4-ACL を適用します。 |
| | `switch(config-if)# no ip access-group NotRequired` | NotRequired と呼ばれる IPv4-ACL を削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | `switch(config-if)# ip access-group restrict_mgmt in` | 入力トラフィックの restrict_mgmt という IPv4-ACL を適用します(まだ存在しない場合)。 |
| | `switch(config-if)# no ip access-group restrict_mgmt in` | 入力トラフィックの restrict_mgmt と呼ばれる IPv4-ACL を削除します。 |
| | `switch(config-if)# ip access-group SampleName2 out` | 出力トラフィックの SampleName2 という IPv4-ACL を適用します(まだ存在しない場合)。 |
| | `switch(config-if)# no ip access-group SampleName2 out` | 出力トラフィックの SampleName2 と呼ばれる IPv4-ACL を削除します。 |

インターフェイスに IPv6-ACL を適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# interface mgmt0`<br>`switch(config-if)#` | 管理インターフェイスを設定します(mgmt0)。 |
| ステップ 3 | `switch(config-if)# ipv6 traffic-filter RestrictMgmt in` | 入力トラフィックに RestrictMgmt という IPv6-ACL を適用します(まだ存在しない場合)。 |
| | `switch(config-if)# no ipv6 traffic-filter RestrictMgmt in` | 入力トラフィックの RestrictMgmt と呼ばれる IPv6-ACL を削除します。 |
| | `switch(config-if)# ipv6 traffic-filter SampleName2 out` | 出力トラフィックの SampleName2 という IPv6-ACL を適用します(まだ存在しない場合)。 |
| | `switch(config-if)# no ipv6 traffic-filter SampleName2 out` | 出力トラフィックの SampleName2 と呼ばれる IPv6-ACL を削除します。 |

# mgmt0 への IP-ACL の適用

mgmt0 と呼ばれるシステムのデフォルト ACL は、mgmt0 インターフェイス上に存在します。この ACL はユーザに表示されないため、mgmt0 は、ユーザが使用できない予約された ACL 名です。mgmt0 ACL はほとんどのポートをブロックし、許可されたセキュリティ ポリシーに準拠した必須のポートへのアクセスだけを可能にします。

# インターフェイスの IP-ACL 設定の確認

**show interface** コマンドを使用して、インターフェイスの IPv4-ACL 設定を表示します。

```
switch# show interface mgmt 0
mgmt0 is up
    Internet address(es):
        10.126.95.180/24
        2001:420:54ff:a4::222:5dd/119
        fe80::eaed:f3ff:fee5:d28f/64
    Hardware is GigabitEthernet
    Address is e8ed.f3e5.d28f
    MTU 1500 bytes, BW 1000 Mbps full Duplex
    5144246 packets input, 1008534481 bytes
      2471254 multicast frames, 0 compressed
```

```
    0 input errors, 0 frame
    0 overrun, 0 fifo
  1765722 packets output, 1571361034 bytes
    0 underruns, 0 output errors
    0 collisions, 0 fifo
    0 carrier errors
```

**show interface** コマンドを使用して、インターフェイスの IPv6-ACL 設定を表示します。

```
switch# show interface gigabitethernet 2/1
GigabitEthernet2/1 is up
    Hardware is GigabitEthernet, address is 000e.38c6.28b0
    Internet address is 10.1.1.10/24
    MTU 1500  bytes
    Port mode is IPS
    Speed is 1 Gbps
    Beacon is turned off
    Auto-Negotiation is turned on
    ip access-group RestrictMgmt
    5 minutes input rate 1208 bits/sec, 151 bytes/sec, 2 frames/sec
    5 minutes output rate 80 bits/sec, 10 bytes/sec, 0 frames/sec
    6232 packets input, 400990 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    503 packets output, 27054 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

# IP-ACL カウンタのクリーンアップ

指定した IPv4 ACL フィルタ エントリのカウンタをクリアするには、**clear** コマンドを使用します。

(注)　このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)

switch# clear ip access-list counters abc

switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (0 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (0 matches)
```

すべての IPv6-ACL のカウンタをクリアするには、**clear ipv6 access-list** コマンドを使用します。

```
switch# clear ipv6 access-list
```

指定した IPv6 ACL のカウンタをクリアするには、**clear ipv6 access-list** *name* コマンドを使用します。

```
switch# clear ipv6 access-list List1
```

(注)　このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。

CHAPTER 6

# 認証局およびデジタル証明書の設定

この章は、次の項で構成されています。



## CA およびデジタル証明書の概要

公開キー インフラストラクチャ（PKI）サポートは、ネットワーク上での安全な通信を確保するために、Cisco MDS 9000 ファミリ スイッチに、デジタル証明書を取得および使用する手段を提供します。PKI サポートにより、IPsec/IKE および SSH の管理機能およびスケーラビリティが提供されます。

CA は、証明書の要求を管理して、ホスト、ネットワーク デバイス、またはユーザなどの加入エンティティに対して証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスまたはユーザに、秘密キーと公開キーの両方を含むキー ペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

ここでは、認証局（CA）およびデジタル証明書の概要について説明します。内容は次のとおりです。

# CA およびデジタル証明書の目的

CA は、証明書の要求を管理して、ホスト、ネットワーク デバイス、またはユーザなどの加入エンティティに対して証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスまたはユーザに、秘密キーと公開キーの両方を含むキー ペアが設定されます。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。両方のキーは、相互に補完的に動作します。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書自体は、受信者が身元を証明し、デジタル証明書を作成するうえで確実に信頼できるサード パーティである、CA により署名されます。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識している必要があります。このプロセスは通常、アウトオブバンド、またはインストール時に実行される操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。IPSec の基本コンポーネントであるインターネット キー交換（IKE）は、デジタル シグニチャを使用して、セキュリティ アソシエーションを設定する前にピア デバイスをスケーラブルに認証できます。

# 信頼モデル、トラストポイント、アイデンティティ CA

PKI サポートで使用されるトラスト モデルは、設定可能な複数の信頼できる CA による階層構造です。各加入エンティティには、セキュリティ プロトコル エクスチェンジによって取得したピアの証明書を確認できるように、信頼できる CA のリストが設定されます。ただし、その証明書がローカルの信頼できる CA の 1 つから発行されていることが条件になります。これを実行するために、CA が自己署名したルート証明書（または下位 CA の証明書チェーン）がローカルに保管されます。信頼できる CA のルート証明書（または下位 CA の場合には完全な証明書チェーン）を安全に取得し、ローカルで保管するプロセスは、*CA 認証*と呼ばれ、CA を信頼するための必須ステップです。

ローカルに設定された信頼できる CA の情報を *トラストポイント*、CA そのものを *トラストポイント CA* と呼びます。この情報は、CA 証明書（または下位 CA の証明書チェーン）と、証明書失効チェック情報によって構成されます。

MDS スイッチも、（IPsec/IKE などの）アイデンティティ証明書を取得するために、トラスト ポイントに登録できます。このトラストポイントを *アイデンティティ CA* と呼びます。

# RSA キー ペアおよびアイデンティティ証明書

1 つ以上の RSA キー ペアを生成し、各 RSA キー ペアに、アイデンティティ証明書を取得するために MDS スイッチを登録するトラスト ポイント CA を関連付けることができます。MDS スイッチは、各 CA について 1 つのアイデンティティ、つまり 1 つのキー ペアと 1 つのアイデンティティ証明書だけを必要とします。

Cisco MDS NX-OS では、RSA キー ペアの生成時に、キーのサイズ（または絶対値）を設定できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキー ラベルは、スイッチの完全修飾ドメイン名（FQDN）です。

次に、トラスト ポイント、RSA キー ペア、およびアイデンティティ証明書の関連についての要約を示します。

- トラスト ポイントは、MDS スイッチが任意のアプリケーション（IKE または SSH など）に関して、ピアの証明書を確認するために信頼する特定の CA になります。
- MDS スイッチには多数のトラスト ポイントを設定でき、スイッチ上のすべてのアプリケーションは、いずれかのトラスト ポイント CA から発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- MDS スイッチは、アイデンティティ証明書を取得するためのトラスト ポイントに相当する CA に登録されます。スイッチを複数のトラスト ポイントに登録して、各トラスト ポイントから個別のアイデンティティ証明書を取得できます。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張情報として証明書に保管されます。
- トラスト ポイントへの登録時に、認証される RSA キー ペアを指定する必要があります。このキー ペアは、登録要求を作成する前に生成して、トラスト ポイントに関連付ける必要があります。トラスト ポイント、キー ペア、およびアイデンティティ証明書間のアソシエーションは、証明書、キー ペア、またはトラスト ポイントを削除して明示的に廃棄されるまで有効です。
- アイデンティティ証明書のサブジェクト名は、MDS スイッチの FQDN です。
- スイッチに 1 つ以上の RSA キー ペアを生成して、各キー ペアを 1 つ以上のトラスト ポイントに関連付けることができます。ただし、トラスト ポイントに関連付けることができるキー ペアは 1 つだけです。つまり、各 CA から取得できるアイデンティティ証明書は 1 つだけです。
- 複数のアイデンティティ証明書を（それぞれ異なる CA から）取得した場合、アプリケーションがピアとのセキュリティ プロトコル エクスチェンジに使用する証明書は、アプリケーションによって異なります。
- 1 つのアプリケーションに 1 つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- 1 つのトラスト ポイントから複数のアイデンティティ証明書を取得したり、1 つのトラストポイントに複数のキー ペアを関連付ける必要はありません。CA 証明書は、付与されたアイデンティティ（の名前）を一度だけ使用し、同じサブジェクト名で複数の証明書は発行しません。1 つの CA から複数のアイデンティティ証明書を取得する必要がある場合には、同じ CA に対して別のトラスト ポイントを定義し、別のキー ペアを関連付けて、認証を受けます。ただし、その CA が同じサブジェクト名で複数の証明書を発行できることが条件になります。

# 複数の信頼できる CA のサポート

MDS スイッチには、複数のトラスト ポイントを設定して、それぞれ異なる CA に関連付けることにより、複数の信頼できる CA を設定できます。複数の信頼できる CA を設定する場合、ピアに証明書を発行した特定の CA に対して、スイッチを登録する必要はありません。代わりに、ピアが信頼する複数の信頼できる CA をスイッチに設定します。スイッチは、ピアの証明書がスイッチのアイデンティティを定義した CA 以外の CA から発行されていても、設定された信頼できる CA を使用して、ピアの証明書を確認できます。

複数の信頼できる CA を設定することにより、IKE を使用して IPsec トンネルを確立する場合に、異なるドメイン（異なる CA）に登録した 2 台以上のスイッチ間で相互のアイデンティティを確認できます。

# PKI の登録のサポート

登録は、IPsec/IKE または SSH などのアプリケーションに使用する、スイッチのアイデンティティ証明書を取得するプロセスです。このプロセスは、証明書を要求するスイッチと CA 間で実行されます。

スイッチの PKI 登録プロセスでは、次の手順を実行します。

1. スイッチ上に RSA 秘密キーと公開キーのキー ペアを生成します。
2. 証明書要求を標準形式で生成し、CA に転送します。
3. CA が受信した登録要求を承認する場合、CA サーバ上で CA 管理者による手動操作が必要になることがあります。
4. 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
5. 証明書を、スイッチ上の不揮発性ストレージ領域（ブートフラッシュ）に書き込みます。

# カットアンドペーストによる手動登録

Cisco MDS NX-OS は、手動でのカットアンドペースト方式による証明書の検索および登録をサポートしています。カットアンドペーストによる登録では、文字通り、スイッチと CA 間で、証明書要求と生成された証明書をカットアンドペーストする必要があります。手順は、次のとおりです。

1. 登録証明書要求を作成します。この要求は、base64 符号化テキスト形式で表示されます。
2. 符号化された証明書要求テキストを、E メールまたは Web 形式にカットアンドペーストして、CA に送信します。
3. E メール メッセージまたは Web ブラウザでのダウンロードにより、CA から発行された証明書（base64 符号化テキスト形式）を受信します。
4. 証明書インポート機能を使用して、発行された証明書をスイッチにカットアンドペーストします。

# 複数の RSA キー ペアおよびアイデンティティ CA のサポート

複数のアイデンティティ CA をサポートすることにより、スイッチを複数のトラスト ポイントに登録できます。その結果、異なる CA から 1 つずつ、複数のアイデンティティ証明書を取得できます。これにより、各ピアで許容される適切な CA から発行された証明書を使用して、多数のピアとの IPSec および他のアプリケーションにスイッチを加入させることができます。

複数の RSA キー ペアのサポート機能により、スイッチ上で、登録した各 CA ごとに異なるキー ペアを保持できます。したがって、キーの長さなど、他の CA から指定された要件と対立することなく、各 CA のポリシー要件と一致させることができます。スイッチ上で複数の RSA キー ペアを生成し、各キー ペアを異なるトラスト ポイントに関連付けることができます。これにより、トラスト ポイントへの登録時に、関連付けたキー ペアを使用して証明書要求を作成できます。

# ピア証明書の確認

MDS スイッチの PKI サポートを使用して、ピアの証明書を確認できます。スイッチは、IPsec/IKE および SSH など、アプリケーション固有のセキュリティ エクスチェンジの実行時に、ピアから提示された証明書を確認します。アプリケーションは、提示されたピア証明書の有効性を確認します。ピア証明書の確認プロセスでは、次の手順が実行されます。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

証明書失効リスト（CRL）を使用した失効チェックでは、トラスト ポイントがこのメソッドを使用して、ピア証明書が失効していないことを確認します。

# CRL のダウンロード、キャッシュ、およびチェックのサポート

証明書失効リスト（CRL）は、期限前に失効された証明書の情報を提供するために CA によって保持され、レポジトリで公開されます。ダウンロード用の URL が公開され、すべての発行済み証明書にも指定されています。ピア証明書を検証するクライアントは、発行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認する必要があります。クライアントは、自身の信頼できる CA のすべてまたは一部の CRL をローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco MDS NX-OS では、トラスト ポイント用の CRL を事前にダウンロードして、スイッチのブートフラッシュにキャッシュされるように手動で設定できます。IPsec または SSH によるピア証明書の確認では、CRL がローカルでキャッシュされ、失効チェックに CRL が使用されるように設定されている場合にかぎり、発行元 CA の CRL が参照されます。それ以外の場合、他の失効チェック方式が設定されていなければ、失効チェックは実行されず、証明書は失効していないと見なされます。このモードの CRL チェックは、CRL オプションと呼ばれています。

# 証明書および関連キー ペアのインポート/エクスポートのサポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書（または証明書チェーン）とアイデンティティ証明書を標準の PEM（base64）形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。この情報を、以降で同じスイッチ（システム クラッシュ後など）または交換したスイッチにインポートできます。PKCS#12 ファイルには、RSA キー ペア、アイデンティティ証明書、および CA 証明書（またはチェーン）の情報が含まれます。

# CA およびデジタル証明書の設定

ここでは、Cisco MDS スイッチ装置で CA およびデジタル証明書を相互運用するために必要な作業について説明します。ここでは、次の内容について説明します。



## ホスト名および IP ドメイン名の設定

スイッチのホスト名および IP ドメイン名が未設定の場合には、これらを設定する必要があります。アイデンティティ証明書のサブジェクトとして、スイッチの FQDN が使用されるからです。また、キー ペアの生成時にキー ラベルを指定しない場合、デフォルトのキー ラベルとしてスイッチの FQDN が使用されます。たとえば、SwitchA.example.com という名前の証明書は、SwitchA というスイッチのホスト名と、example.com というスイッチの IP ドメイン名で構成されています。

**注意**　証明書の生成後にホスト名または IP ドメイン名を変更すると、証明書が無効になることがあります。

スイッチのホスト名および IP ドメイン名を設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# hostname SwitchA` | スイッチのホスト名（SwitchA）を設定します。 |
| ステップ 3 | `SwitchA(config)# ip domain-name example.com` | スイッチの IP ドメイン名（example.com）を設定します。 |

## RSA キーペアの生成

RSA キー ペアは、IKE/IPsec および SSH などのアプリケーションによるセキュリティ プロトコル エクスチェンジの実行中に、署名およびセキュリティ ペイロードの暗号化/復号化に使用されます。RSA キー ペアは、スイッチの証明書を取得する前に必要になります。

RSA サーバ キー ペアを生成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# crypto key generate rsa` | デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キー ペアを生成します。デフォルトでは、キー ペアはエクスポートできません。<br>(注)　キーの絶対値を指定するときは、ローカル サイト（MDS スイッチ）および CA（登録先）のセキュリティ ポリシー（または要件）を考慮してください。<br>(注)　スイッチに設定できるキー ペアの最大数は、16 です。 |
| | `switch(config)# crypto key generate rsa label SwitchA modulus 768` | ラベル SwitchA、モジュラス 768 の RSA キー ペアを生成します。有効なモジュラスの値は 512、768、1024、1536、および 2048 です。デフォルトでは、キー ペアはエクスポートできません。 |
| | `switch(config)# crypto key generate rsa exportable` | デフォルトのラベルとしてスイッチの FQDN を使用し、デフォルトのモジュラスとして 512 を使用する RSA キー ペアを生成します。キーはエクスポート可能です。<br>⚠<br>注意　キー ペアのエクスポート設定は、キー ペアの生成後は変更できません。<br>(注)　RKCS#12 形式でエクスポートできるのは、エクスポート可能なキー ペアだけです。 |

# トラスト ポイント CA アソシエーションの作成

トラスト ポイント CA アソシエーションを作成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch(config)# crypto ca trustpoint admin-ca`<br>`switch(config-trustpoint)#` | スイッチが信頼するトラストポイント CA を宣言し、トラストポイント コンフィギュレーション サブモードを開始します。<br>(注)　スイッチに設定できるトラストポイントの最大数は 16 です。 |
| | `switch(config)# no crypto ca trustpoint admin-ca` | トラストポイント CA を削除します。 |
| ステップ 2 | `switch(config-trustpoint)# enroll terminal` | カットアンドペーストによる手動での証明書登録を指定します(デフォルト)。<br>(注)　手動でのカット&ペーストの証明書の登録は登録でサポートされている唯一の方法です。 |
| ステップ 3 | `switch(config-trustpoint)# rsakeypair SwitchA` | 登録の目的でこのトラスト ポイントに関連付ける RSA キー ペアのラベルを指定します。「RSA キーペアの生成」セクション (6-152 ページ)で作成した名前です。各 CA に 1 つの RSA キー ペアだけを指定できます。 |
| | `switch(config-trustpoint)# no rsakeypair SwitchA` | トラスト ポイントから RSA キー ペアの関連付けを解除します(デフォルト)。 |
| ステップ 4 | `switch(config-trustpoint)# end`<br>`switch#` | トラストポイント コンフィギュレーション サブモードを終了します。 |
| ステップ 5 | `switch# copy running-config startup-config` | 実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。 |

# CA の認証

信頼できる CA の設定プロセスは、MDS スイッチに対して CA が認証された場合にかぎり、完了します。スイッチは、CA を認証する必要があります。CA を認証するには、CA の公開キーが含まれている CA の自己署名付きの証明書を PEM 形式で取得します。この CA の証明書は自己署名(CA が自身の証明書に署名したもの)であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。

(注)　認証される CA が自己署名した CA ではない場合(つまり、別の CA の下位 CA で、その別の CA もまた、最終的に自己署名した別の CA の下位 CA であるような場合)には、CA 認証の手順で、認証チェーンに含まれるすべての CA の CA 証明書の完全なリストを入力する必要があります。これは、認証される CA の *CA 認証チェーン*と呼ばれます。CA 証明書チェーン内の証明書の最大数は 10 です。

電子メールまたは Web サイトからの証明書のカット アンド ペーストにより CA の証明書を認証するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **crypto ca authenticate admin-ca**<br>input (cut & paste) CA certificate (chain) in PEM format;<br>end the input with a line containing only END OF INPUT :<br>**-----BEGIN CERTIFICATE-----**<br>**MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB**<br>**kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO**<br>**MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE**<br>**ChMFQ2lzY28xEzARBgNVBAsTCm51dHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD**<br>**QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN**<br>**AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth**<br>**cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG**<br>**A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN**<br>**AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI**<br>**OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E**<br>**BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ**<br>**GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs**<br>**L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv**<br>**bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB**<br>**BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea**<br>**NBG7E0oN66zex0EOEfG1Vs6mXp1//w==**<br>**-----END CERTIFICATE-----**<br>**END OF INPUT**<br>Fingerprint(s): MD5<br>Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12<br><br>Do you accept this certificate? [yes/no]: **y** | CA の証明書をカットアンド ペーストするようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名前を使用します。<br>(注)　ある CA に対して認証できるトラストポイントの最大数は 10 です。 |

(注)　証明書の確認および PKCS#12 形式のエクスポートでは CA チェーンが必要になるので、下位 CA の認証の場合には、最終的に自己署名された CA までの CA 証明書の完全なチェーンが必要になります。

# 証明書取消確認方法の設定

クライアント（IKE ピアまたは SSH ユーザなど）とのセキュリティ エクスチェンジの実行中に、MDS スイッチはクライアントから送信されたピア証明書の確認を実行します。この確認プロセスには、証明書失効ステータスのチェックを含めることができます。

送信された証明書が失効しているかどうかを調べるには、CRL 方式を使用できます。CA からダウンロードした CRL を確認するようにスイッチを設定できます（「CRL の設定」セクション（6-159 ページ）を参照）。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。ただし、CRL のダウンロード後に証明書が失効された場合、失効ステータスを認識できません。失効証明書をチェックする最も確実な方法は、ローカル CRL チェックを使用することです。

(注)　証明書の失効チェックを設定する前に、CA を認証する必要があります。

証明書失効確認方式を設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch(config)# crypto ca trustpoint admin-ca`<br>`switch(config-trustpoint)#` | スイッチが信頼するトラストポイント CA を宣言し、トラストポイント コンフィギュレーション サブモードを開始します。 |
| ステップ 2 | `switch(config-trustpoint)# revocation-check crl` | このトラスト ポイントと同じ CA によって発行されたピア証明書の検証の際に適用される失効チェック方式として CRL を指定します(デフォルト)。 |
| | `switch(config-trustpoint)# revocation-check none` | 失効証明書をチェックしません。 |
| | `switch(config-trustpoint)# no revocation-check` | デフォルトの方式に戻ります。 |

# 証明書要求の生成

スイッチの各 RSA キーペアについて、関連付けたトラスト ポイント CA からアイデンティティ証明書を取得するには、要求を生成する必要があります。さらに、表示された要求を、CA 宛ての E メール メッセージまたは Web サイト フォームにカットアンドペーストします。

CA から署名入り証明書要求を生成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# crypto ca enroll admin-ca`<br>`Create the certificate request ..`<br>`Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.`<br>`For security reasons your password will not be saved in the configuration.`<br>`Please make a note of it.`<br>`Password:nbv123`<br>`The subject name in the certificate will be: Vegas-1.cisco.com`<br>`Include the switch serial number in the subject name? [yes/no]: no`<br>`Include an IP address in the subject name [yes/no]: yes`<br>`ip address:172.22.31.162`<br>`The certificate request will be displayed...`<br>`-----BEGIN CERTIFICATE REQUEST-----`<br>`MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ`<br>`KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY`<br>`0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y`<br>`P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S`<br>`VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ`<br>`DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ`<br>`KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt`<br>`PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjg1XMjja8`<br>`8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=`<br>`-----END CERTIFICATE REQUEST-----` | 認証した CA に対する証明書要求を作成します。<br>(注)　チャレンジ パスワードは、設定には保存されません。このパスワードは、証明書を失効する必要がある場合に要求されるので、パスワードを覚えておく必要があります。 |

# アイデンティティ証明書のインストール

CA からのアイデンティティ証明書は、base64 符号化テキスト形式で、E メールまたは Web ブラウザで受信します。CLI インポート機能を使用して符号化テキストをカットアンドペーストすることにより、CA のアイデンティティ証明書をインストールする必要があります。

電子メールまたは Web ブラウザで CA から受信したアイデンティティ証明書をインストールするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# crypto ca import admin-ca certificate`<br>`input (cut & paste) certificate in PEM format:`<br>`-----BEGIN CERTIFICATE-----`<br>`MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G`<br>`CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD`<br>`VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz`<br>`Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w`<br>`NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu`<br>`Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C`<br>`dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47`<br>`glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb`<br>`x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw`<br>`GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR`<br>`bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW`<br>`pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE`<br>`BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w`<br>`DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh`<br>`cm5hIENBghAFYNKJrLQZlE9JEiWMrR16MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6`<br>`Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6`<br>`Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH`<br>`AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl`<br>`LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4`<br>`XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF`<br>`AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw`<br>`E36cIZu4WsExREqxbTk8ycx7V5o=`<br>`-----END CERTIFICATE-----` | admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。<br>(注)　スイッチに設定できるアイデンティティ証明書の最大数は 16 です。 |

# コンフィギュレーションの保存

変更したコンフィギュレーションは、終了時に情報が失われないように、保存しておく必要があります。

# トラスト ポイントの設定がリブート後も維持されていることの確認

トラスト ポイント設定は、標準の Cisco NX-OS コンフィギュレーションであるため、スタートアップ コンフィギュレーションに明示的にコピーした場合にかぎり、システム リブート後も存続します。トラスト ポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラスト ポイントに関連する証明書、キーペア、および CRL が自動的に保持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キーペア、および関連 CRL は保持されません。リブート後に、対応するトラスト ポイント設定が必要になるからです。設定した証明書、キーペア、および CRL を確実に保持するために、必ず、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てください。また、証明書またはキーペアを削除した場合も、削除を反映させるために、実行コンフィギュレーションを保存してください。

特定のトラスト ポイントがスタートアップ コンフィギュレーションに保存されていれば、トラスト ポイントに関連する証明書および CRL は、インポートした時点で（スタートアップ コンフィギュレーションに明示的にコピーしなくても）自動的に存続します。

また、パスワードで保護したアイデンティティ証明書のバックアップを作成して、外部サーバに保存しておくことを推奨します（「PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート」セクション（6-158 ページ）を参照）。

（注）　コンフィギュレーションを外部サーバにコピーすると、証明書およびキーペアも保存されます。

# CA および証明書の設定のモニタリングとメンテナンス

このセクションの作業は、オプションです。この項では、次のトピックについて取り上げます。



## PKCS#12 形式でのアイデンティティ情報のエクスポートとインポート

アイデンティティ証明書を、トラストポイントの RSA キー ペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。後で、スイッチをシステム クラッシュから回復する場合、またはスーパーバイザ モジュールを交換する場合に、証明書および RSA キーペアをインポートできます。

（注）　エクスポートおよびインポートの URL の指定では、**bootflash:***filename* 形式のローカル構文だけがサポートされます。

証明書およびキー ペアを PKCS#12 形式ファイルにエクスポートする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123` | トラストポイント admin-ca のアイデンティティ証明書および関連付けられたキー ペアと CA 証明書をファイル bootflash:adminid.p12 に、パスワード nbv123 によって保護された PKCS#12 形式でエクスポートします。 |
| ステップ 3 | `switch(config)# exit`<br>`switch#` | EXEC モードに戻ります。 |
| ステップ 4 | `switch# copy bootflash:adminid.p12 tftp:adminid.p12` | PKCS#12 形式のファイルを TFTP サーバにコピーします。 |

証明書およびキー ペアを PKCS#12 形式ファイルからインポートする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# copy tftp:adminid.p12 bootflash:adminid.p12` | PKCS#12 形式のファイルを TFTP サーバからコピーします。 |
| ステップ 2 | `switch# config terminal`<br>`switch(config)#` | コンフィギュレーション モードに入ります。 |
| ステップ 3 | `switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123` | トラストポイント admin-ca のアイデンティティ証明書および関連付けられたキー ペアと CA 証明書をファイル bootflash:adminid.p12 から、パスワード nbv123 によって保護された PKCS#12 形式でインポートします。 |

(注)　PKCS#12 ファイルを正常にインポートするには、トラスト ポイントが空白である（RSA キーペアが関連付けられていない、および CA 認証により CA が関連付けられていない）必要があります。

## CRL の設定

ファイルからトラスト ポイントに CRL をインポートする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# copy tftp:adminca.crl bootflash:adminca.crl` | CRL をダウンロードします。 |
| ステップ 2 | `switch# config terminal`<br>`switch(config)#` | コンフィギュレーション モードに入ります。 |
| ステップ 3 | `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl` | ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。 |

## CA 設定からの証明書の削除

トラスト ポイントに設定されているアイデンティティ証明書や CA 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除したあと、トラスト ポイントから RSA キー ペアの関連付けを解除できます。期限切れまたは失効した証明書、キー ペアが信用できない（または信用できない可能性がある）証明書、または信頼できなくなった CA を除去するには、証明書を削除する必要があります。

トラスト ポイントから CA 証明書（または下位 CA のチェーン全体）を削除する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# crypto ca trustpoint myCA` | トラストポイント コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config-trustpoint)# delete ca-certificate` | CA 証明書または証明書チェーンを削除します。 |
| ステップ 4 | `switch(config-trustpoint)# delete certificate` | アイデンティティ証明書を削除します。 |
| | `switch(config-trustpoint)# delete certificate force` | アイデンティティ証明書を削除します。<br>（注）　削除するアイデンティティ証明書が、デバイスの最後または唯一のアイデンティティ証明書である場合には、**force** オプションを使用して削除する必要があります。これは、管理者が最後または唯一のアイデンティティ証明書を誤って削除し、アプリケーション（IKE および SSH など）で使用する証明書が存在しない状態になるのを防止するためです。 |
| ステップ 5 | `switch(config-trustpoint)# end`<br>`switch#` | EXEC モードに戻ります。 |
| ステップ 6 | `switch# copy running-config startup-config` | 実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。 |

## スイッチからの RSA キーペアの削除

特定の状況では、スイッチの RSA キーペアの削除が必要になることがあります。たとえば、何らかの原因で RSA キーペアの信用性が失われ、もはや使用しない場合には、そのキーペアを削除すべきです。

スイッチから RSA キーペアを削除する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal`<br>`switch(config)#` | 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 | `switch(config)# crypto key zeroize rsa MyKey` | ラベルが MyKey である RSA キー ペアを削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | `switch(config)# end`<br>`switch#` | EXEC モードに戻ります。 |
| ステップ 4 | `switch# copy running-config startup-config` | 実行中の設定を起動設定にコピーして、設定がリブート後も保持されるようにします。 |

(注)　スイッチから RSA キーペアを削除した後、CA でそのスイッチの証明書を失効するように、CA 管理者に依頼してください。その証明書を要求した場合には、作成したチャレンジ パスワードを提供する必要があります。「証明書要求の生成」セクション（6-156 ページ）を参照してください。

## キーペアと CA 情報の表示

キーペアと CA 情報を表示するには、EXEC モードで次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `switch# show crypto key mypubkey rsa` | スイッチの RSA 公開キーに関する情報が表示されます。 |
| `switch# show crypto ca certificates` | CA とアイデンティティ証明書についての情報を表示します。 |
| `switch# show crypto ca crl` | CA の CRL についての情報を表示します。 |
| `switch# show crypto ca trustpoints` | CA トラストポイントについての情報を表示します。 |

# 設定例

ここでは、Microsoft Windows Certificate サーバを使用して、Cisco MDS 9000 ファミリ スイッチ上に証明書および CRL を設定するための作業例を示します。

この項では、次のトピックについて取り上げます。

# MDS スイッチでの証明書の設定

MDS スイッチで証明書を設定する手順は、次のとおりです。

**ステップ 1**　スイッチの FQDN を設定します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# switchname Vegas-1
Vegas-1(config)#
```

**ステップ 2**　スイッチの DNS ドメイン名を設定します。

```
Vegas-1(config)# ip domain-name cisco.com
Vegas-1(config)#
```

**ステップ 3**　トラストポイントを作成します。

```
Vegas-1(config)# crypto ca trustpoint myCA
Vegas-1(config-trustpoint)# exit
Vegas-1(config)# do show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
Vegas-1(config)#
```

**ステップ 4**　スイッチの RSA キーペアを作成します。

```
Vegas-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Vegas-1(config)# do show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes

Vegas-1(config)#
```

**ステップ 5**　RSA キー ペアとトラスト ポイントを関連付けます。

```
Vegas-1(config)# crypto ca trustpoint myCA
Vegas-1(config-trustpoint)# rsakeypair myKey
Vegas-1(config-trustpoint)# exit
Vegas-1(config)# do show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
Vegas-1(config)#
```

**ステップ 6**　Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします（「CA 証明書のダウンロード」セクション（6-165 ページ）を参照）。

**ステップ 7**　トラストポイントに登録する CA を認証します。

```
Vegas-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
```

```
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12


Do you accept this certificate? [yes/no]:y
Vegas-1(config)#

Vegas-1(config)# do show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

**ステップ 8**　トラスト ポイントに登録するために使用する証明書要求を作成します。

```
Vegas-1(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
ip address:10.10.1.1
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

Vegas-1(config)#
```

**ステップ 9**　Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します（「アイデンティティ証明書の要求」セクション（6-169 ページ）を参照）。

**ステップ 10**　アイデンティティ証明書をインポートします。

```
Vegas-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Vegas-1(config)# exit
Vegas-1#
```

**ステップ 11**　証明書の設定を確認します。

```
Vegas-1# show crypto ca certificates
Trustpoint: myCA
certificate:
subject= /CN=Vegas-1.cisco.com
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0A338EA1000000000074
notBefore=Nov 12 03:02:40 2005 GMT
notAfter=Nov 12 03:12:40 2006 GMT
MD5 Fingerprint=3D:33:62:3D:B4:D0:87:A0:70:DE:A3:87:B3:4E:24:BF
purposes: sslserver sslclient ike

CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/L=Bangalore/O=Yourcompany/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

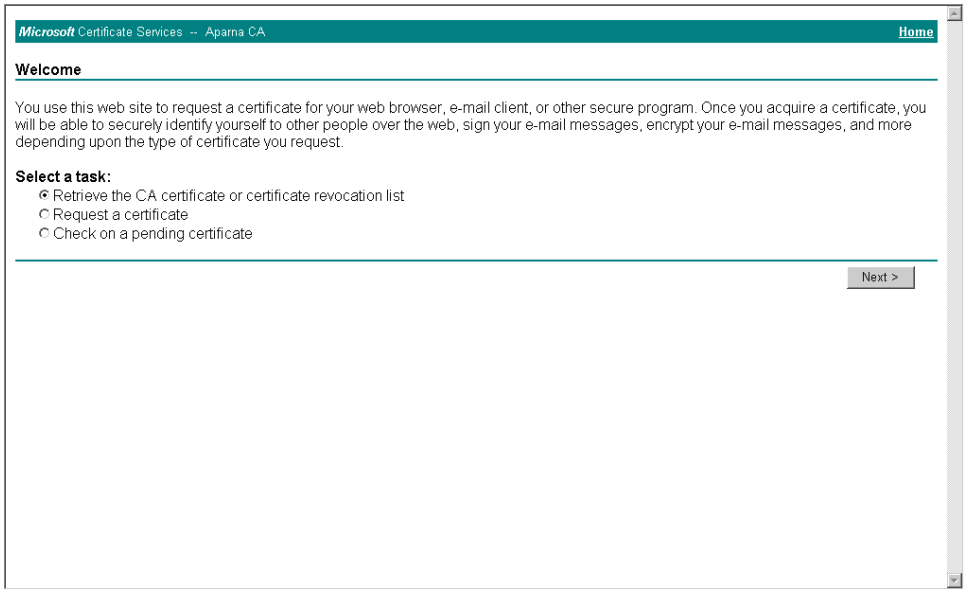
**ステップ 12**　証明書の設定をスタートアップ コンフィギュレーションに保存します。

```
Vegas-1# copy running-config startup-config
```

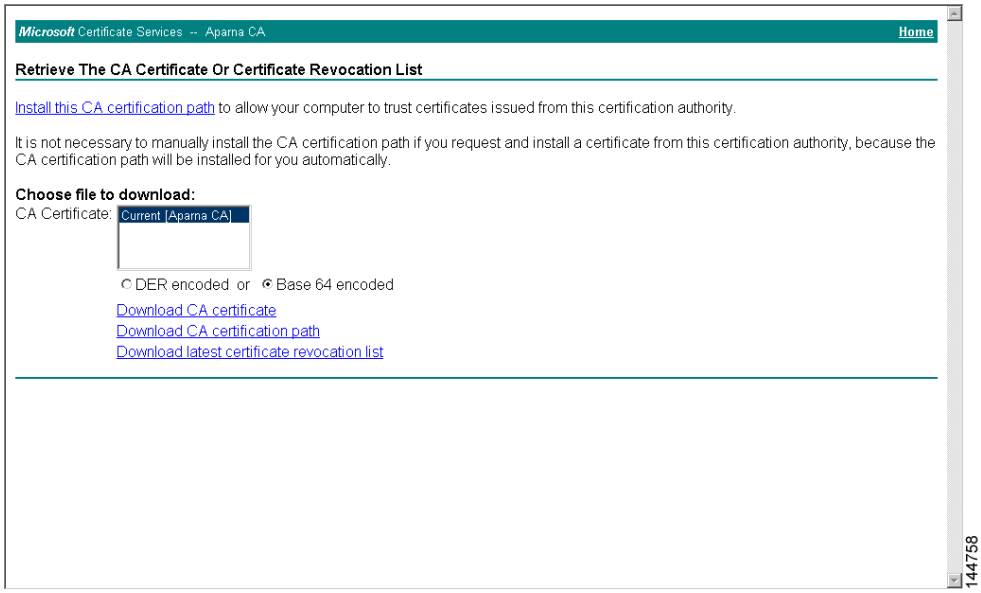
# CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

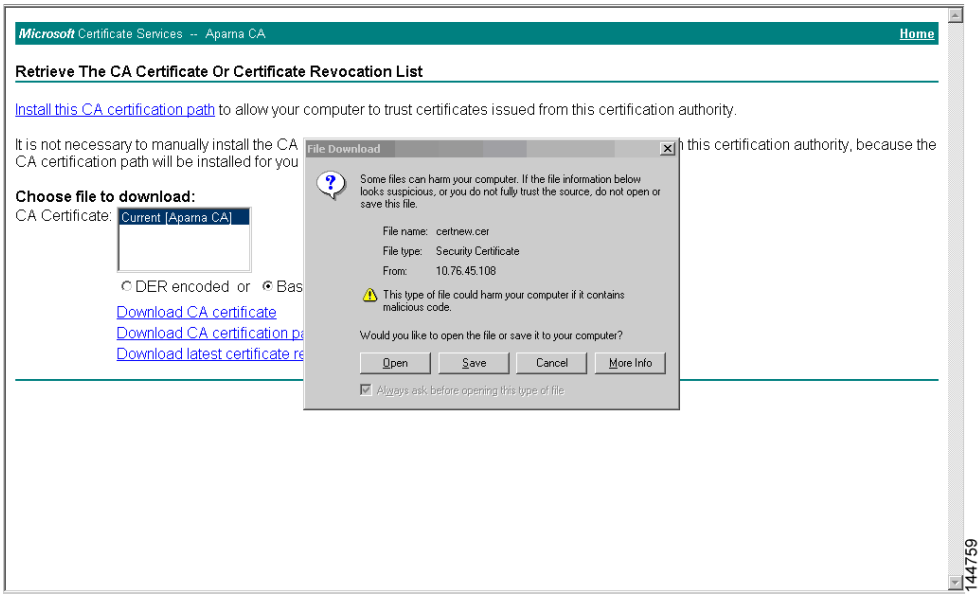
**ステップ 1**　Microsoft Certificate Services Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。



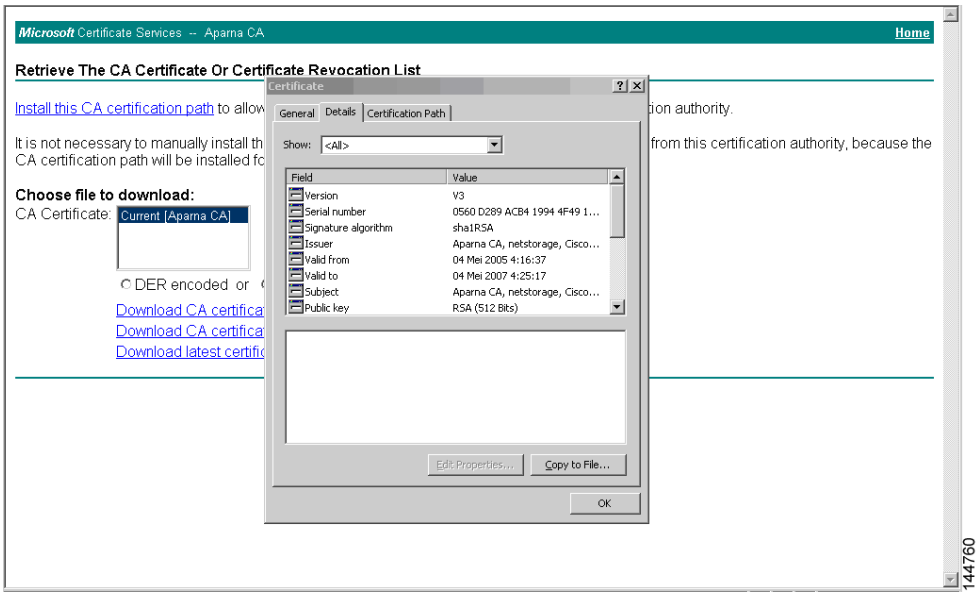

**ステップ 2**　表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。



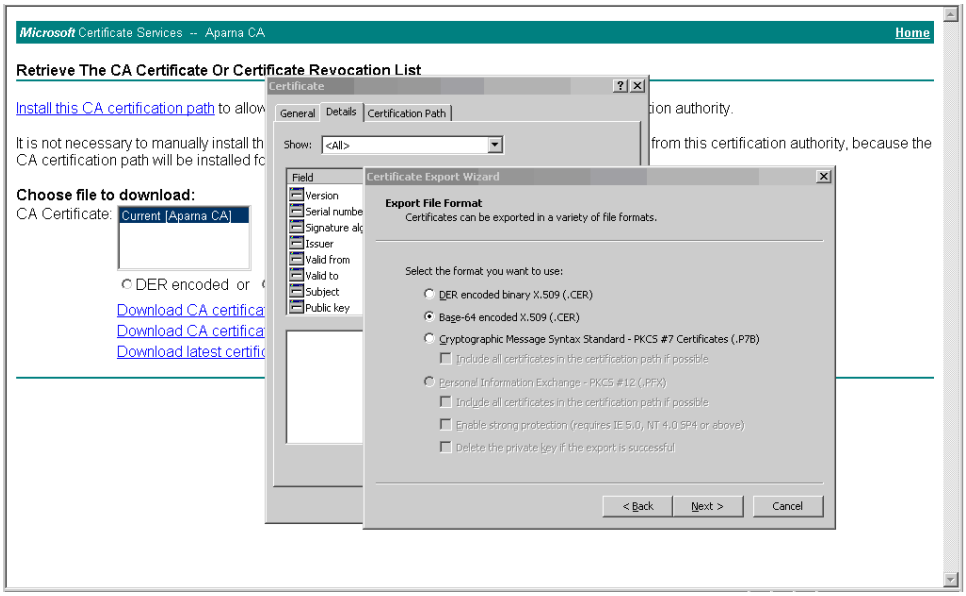
**ステップ 3**　[File Download] ダイアログボックスで、[Open] ボタンをクリックします。



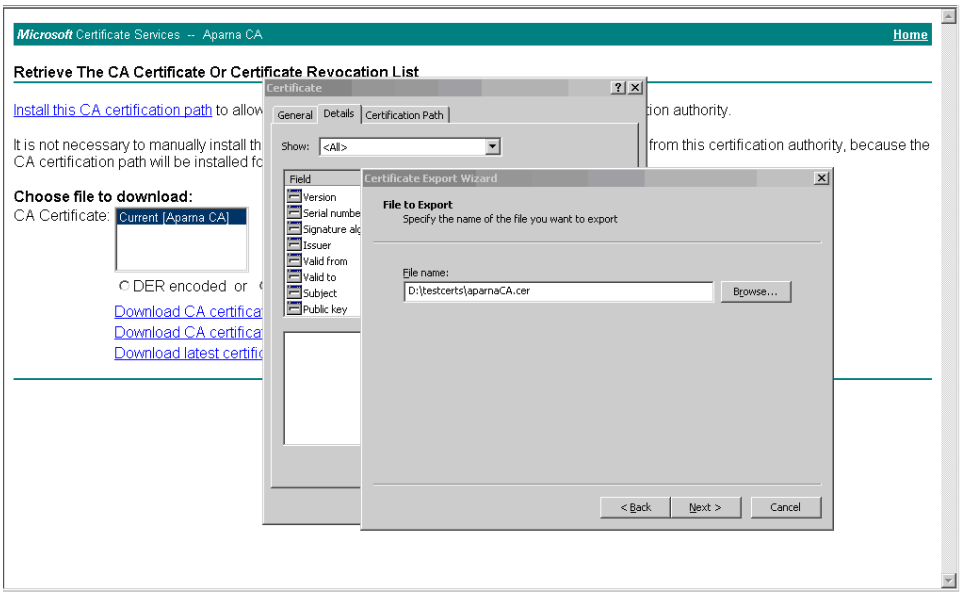

**ステップ 4**　[Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] をクリックします。



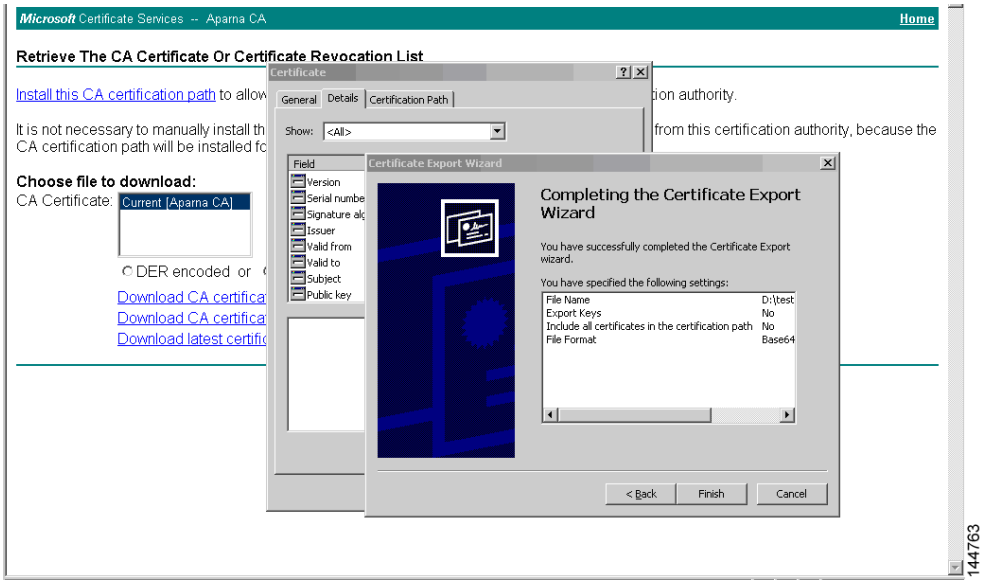
**ステップ 5**　[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



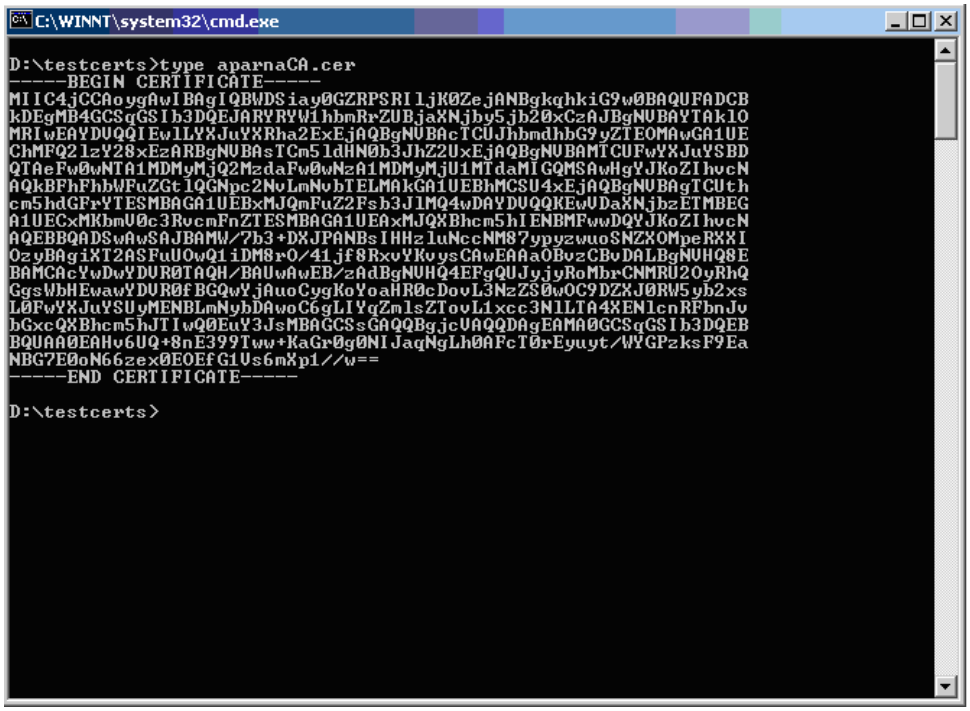

**ステップ 6**　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。



**ステップ 7**　[Certificate Export Wizard] ダイアログボックスの [Finish] ボタンをクリックします。



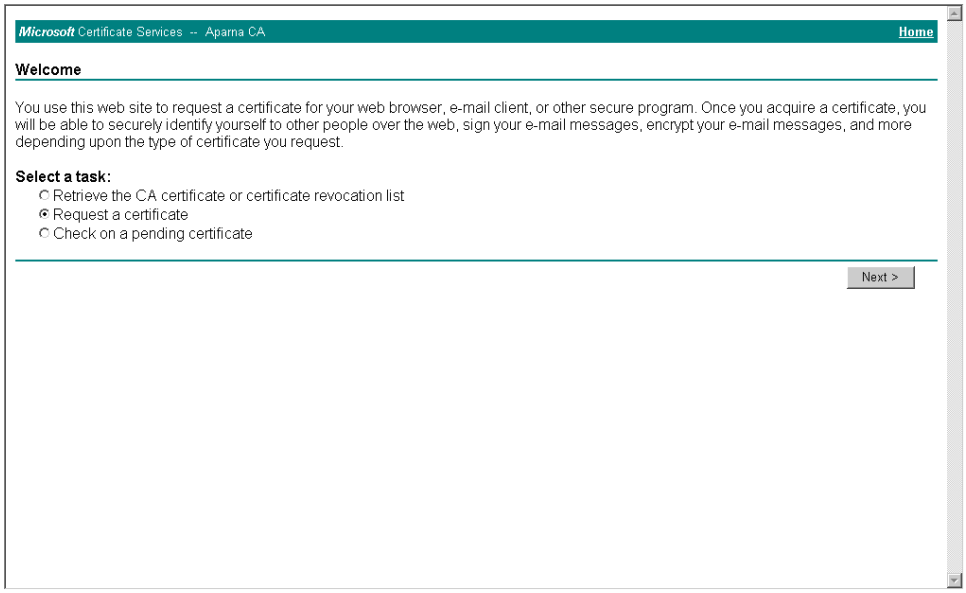

**ステップ 8**　Microsoft Windows の **type** コマンドを使用して、Base-64（PEM）形式で保存されている CA 証明書を表示します。



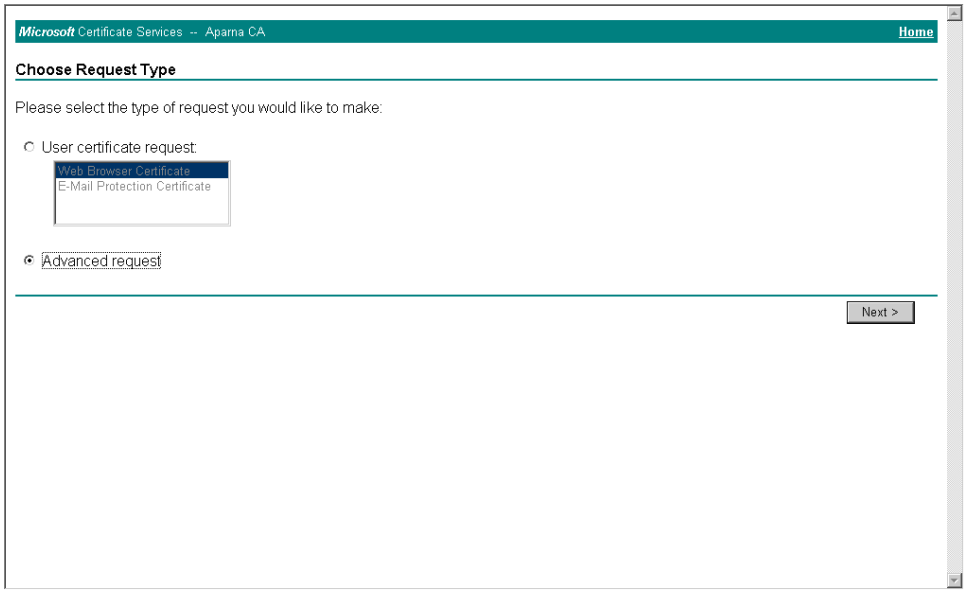
# アイデンティティ証明書の要求

PKCS#10 CRS を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求する手順は、次のとおりです。

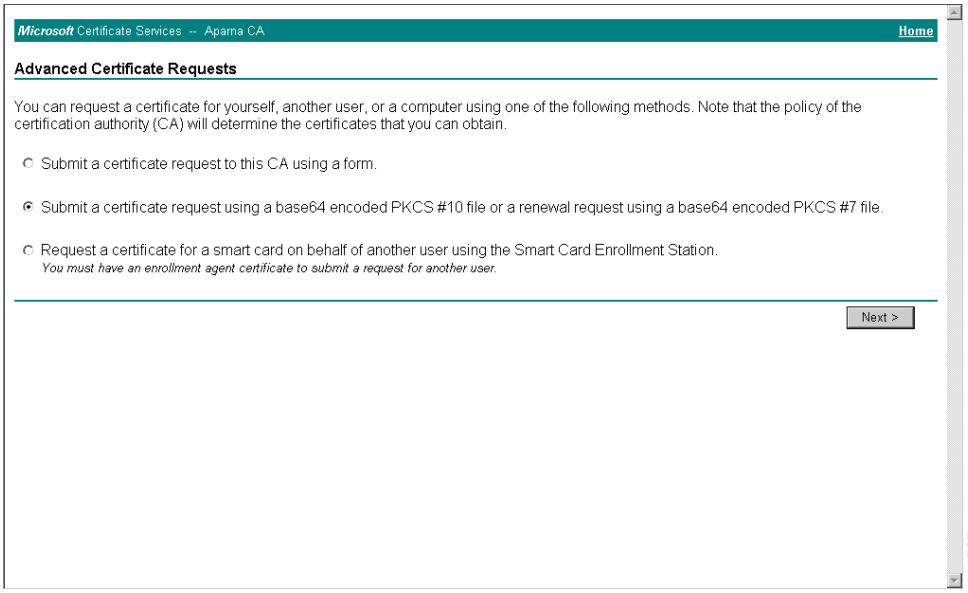
**ステップ 1**　Microsoft Certificate Services Web インターフェイス上の [Request a certificate] ラジオ ボタンを選択し、[Next] をクリックします。




**ステップ 2**　[Advanced Request] ラジオ ボタンを選択し、[Next] をクリックします。

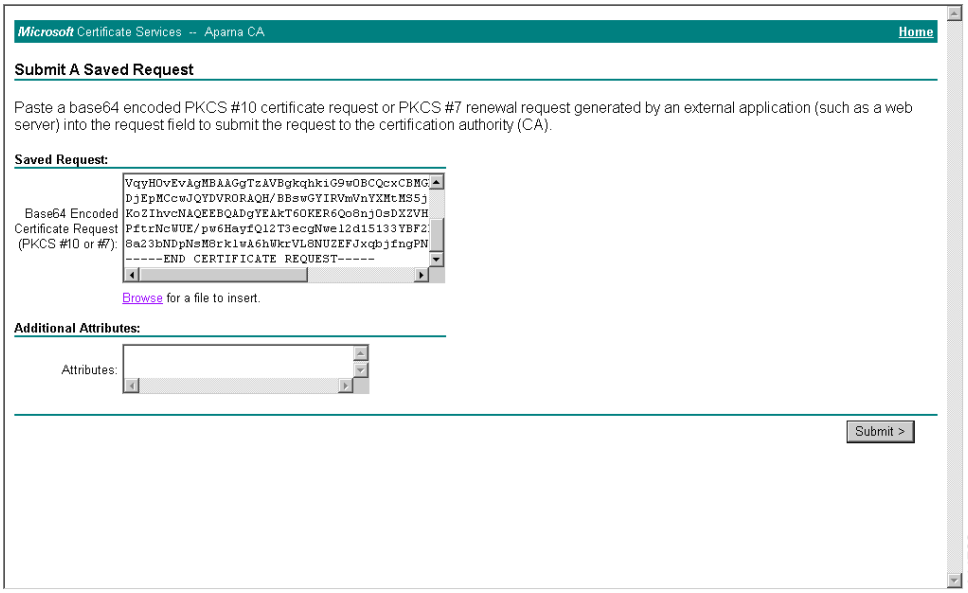


ステップ 3　[Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。

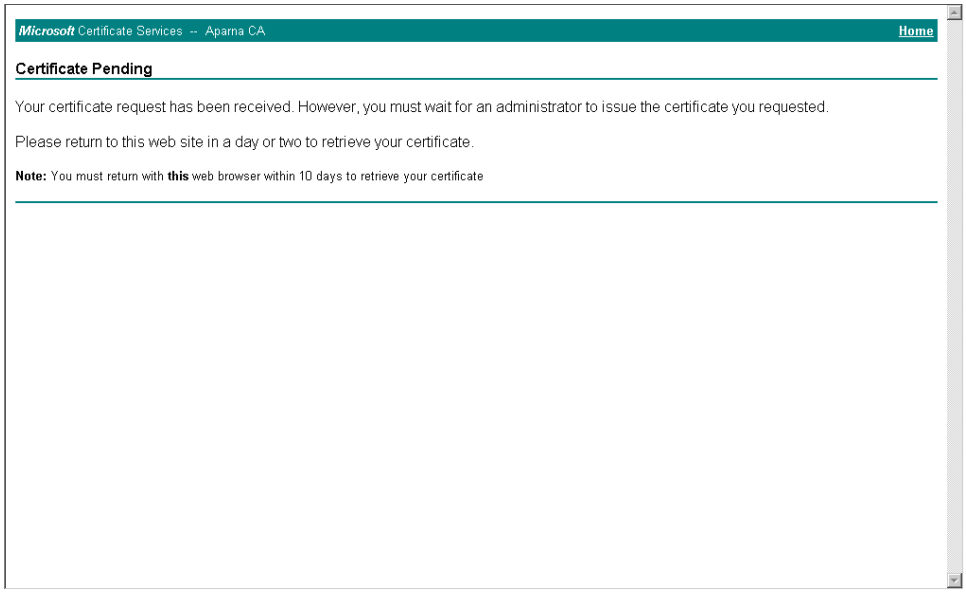



ステップ 4　[Saved Request] テキスト ボックスに base64 PKCS#10 証明書要求をペーストし、[Next] をクリックします。

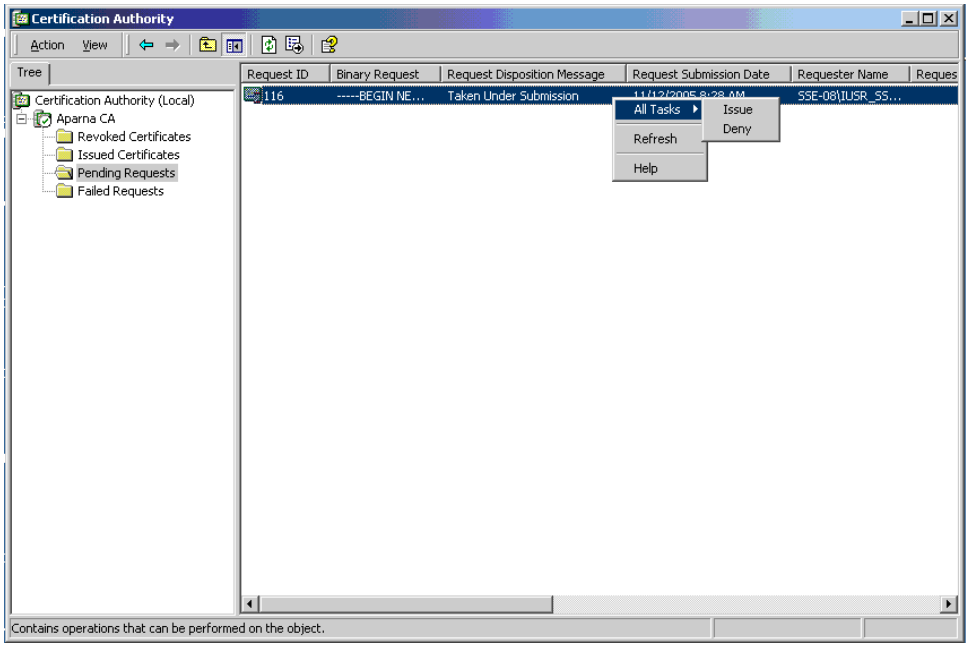
MDS スイッチのコンソールから、証明書要求がコピーされます（「証明書要求の生成」セクション（6-156 ページ）および「MDS スイッチでの証明書の設定」セクション（6-162 ページ）を参照）。



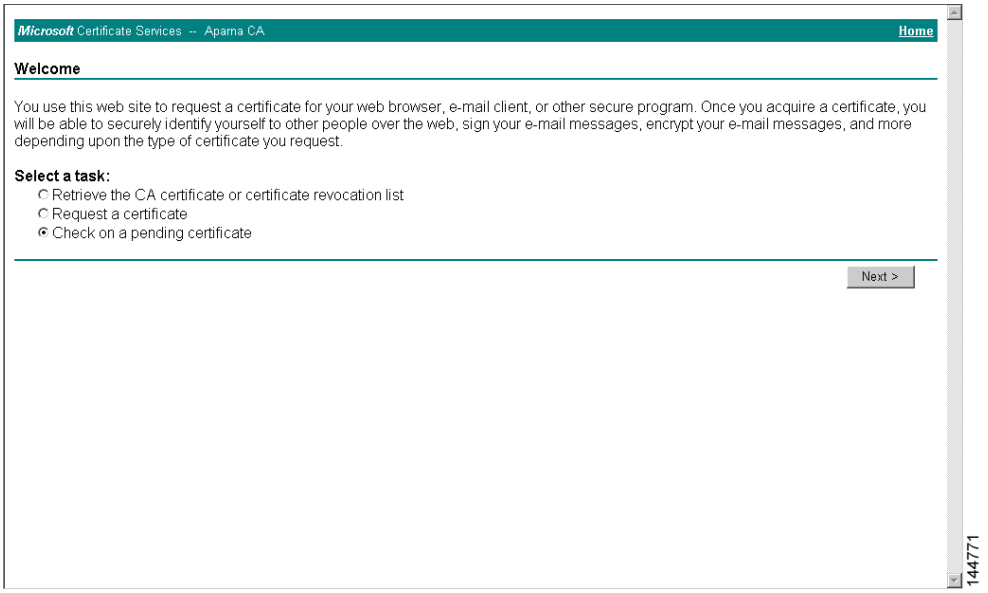
**ステップ 5**　CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。



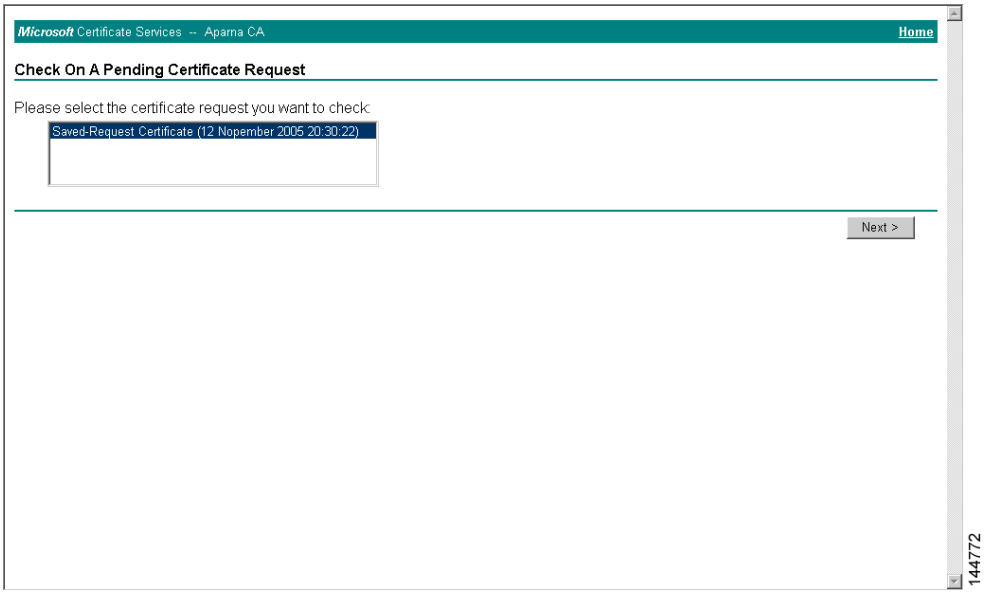

**ステップ 6**　CA 管理者により証明書要求が承認されます。



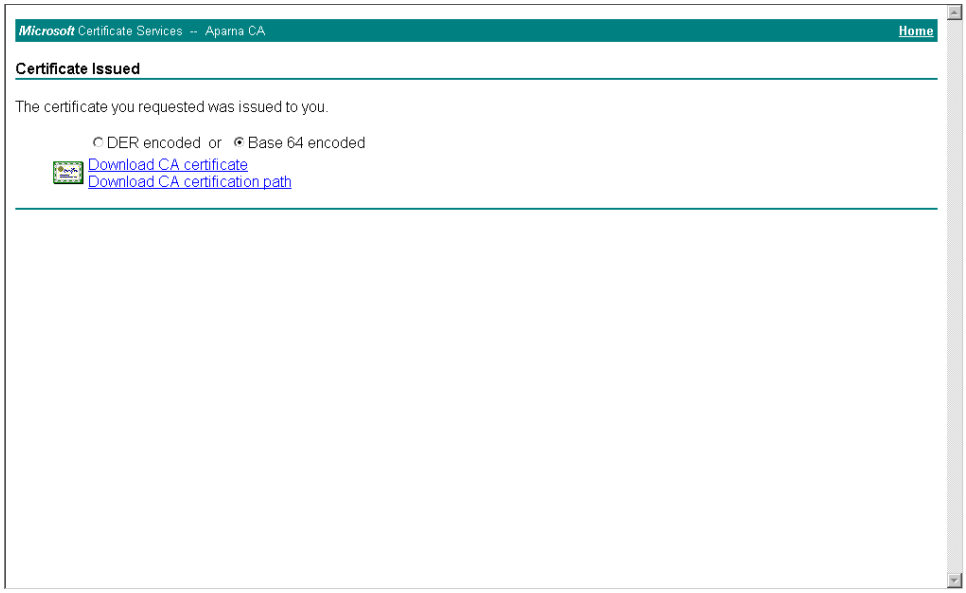
**ステップ 7**　Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。



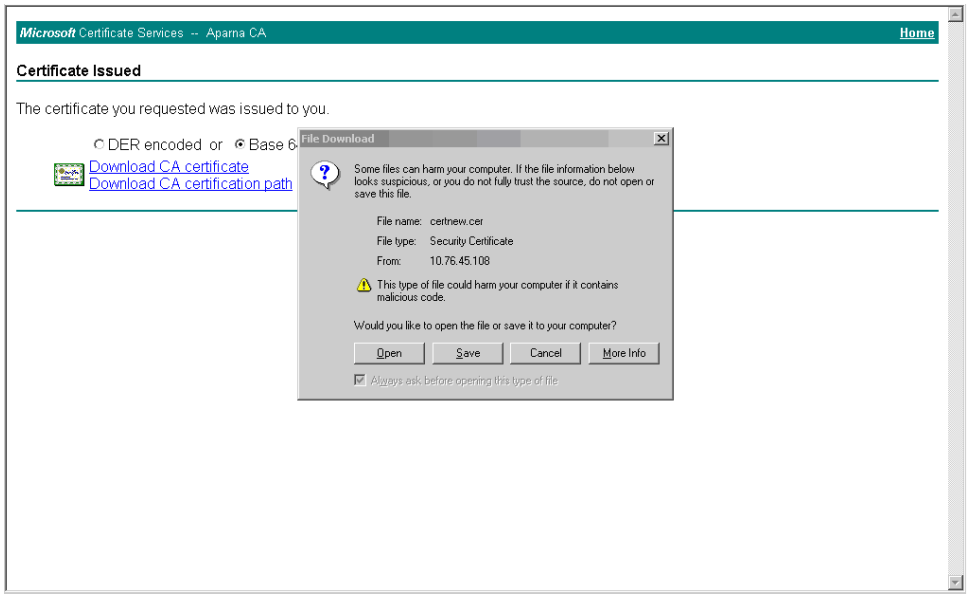

**ステップ 8**　確認する証明書要求を選択し、[Next] をクリックします。



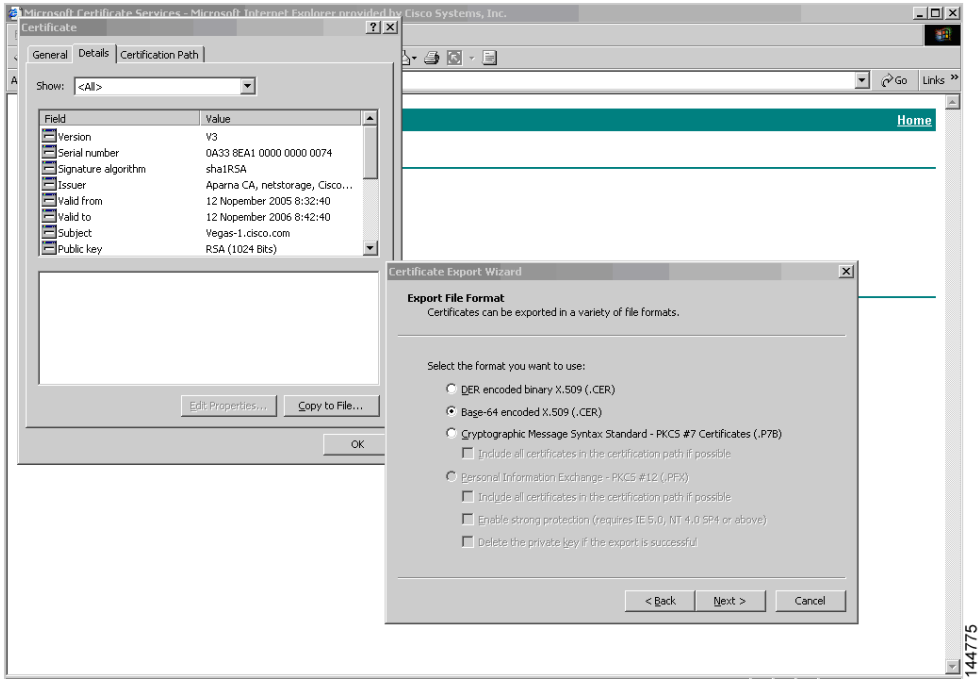
**ステップ 9**　[Base 64 encoded] を選択し、[Download CA certificate] リンクをクリックします。



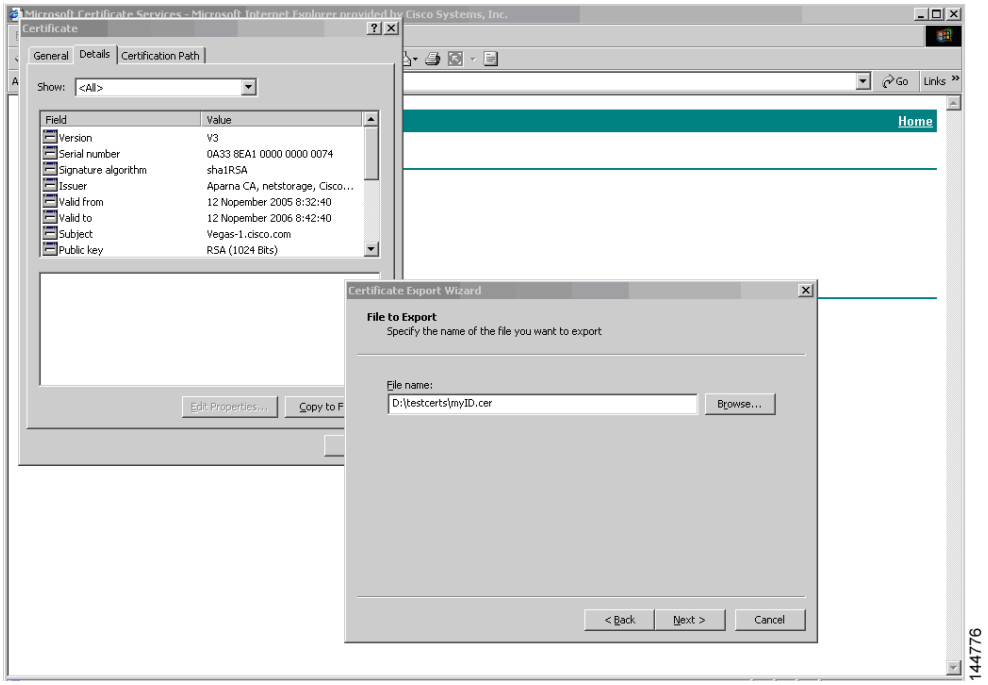

**ステップ 10**　[File Download] ダイアログボックスで、[Open] をクリックします。



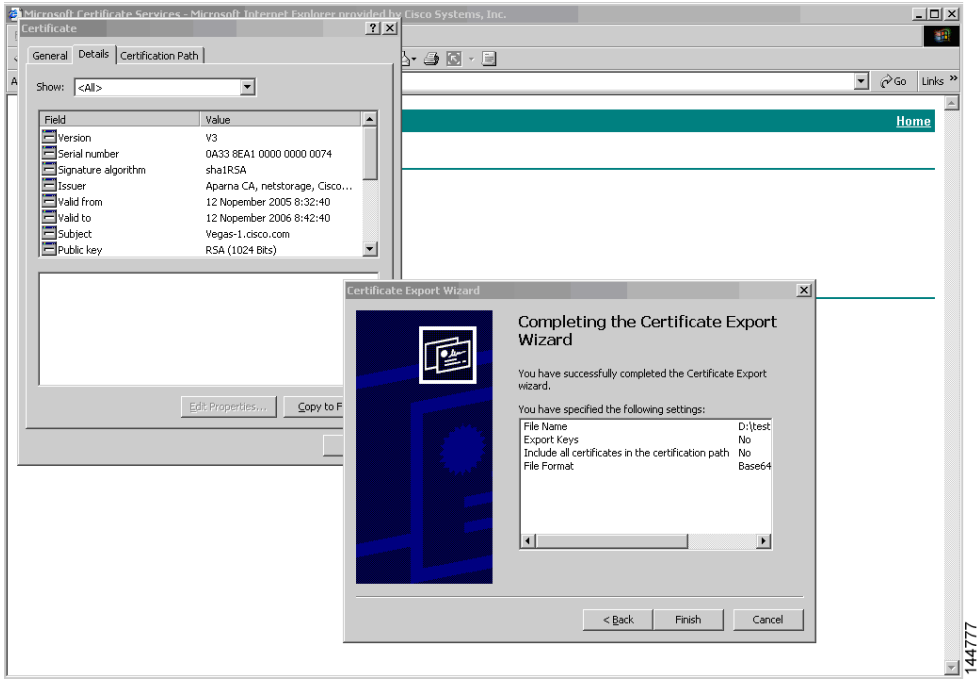

**ステップ 11**　[Certificate] ダイアログボックスで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション ボタンを選択し、[Next] ボタンをクリックします。



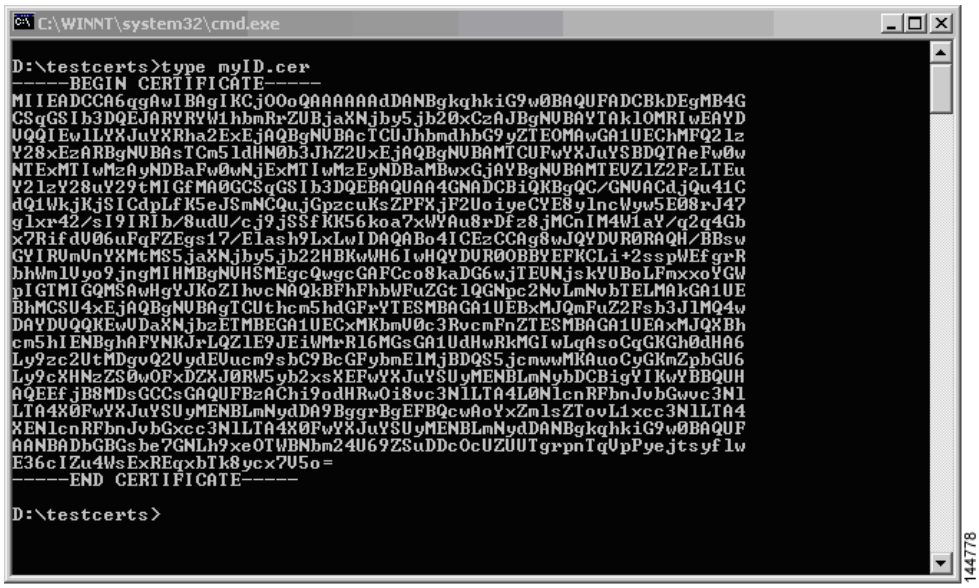

**ステップ 12**　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] をクリックします。




**ステップ 13**　[Finish] をクリックします。




**ステップ 14**　Microsoft Windows の **type** コマンドを使用して、base-64 符号化形式のアイデンティティ証明書を表示します。

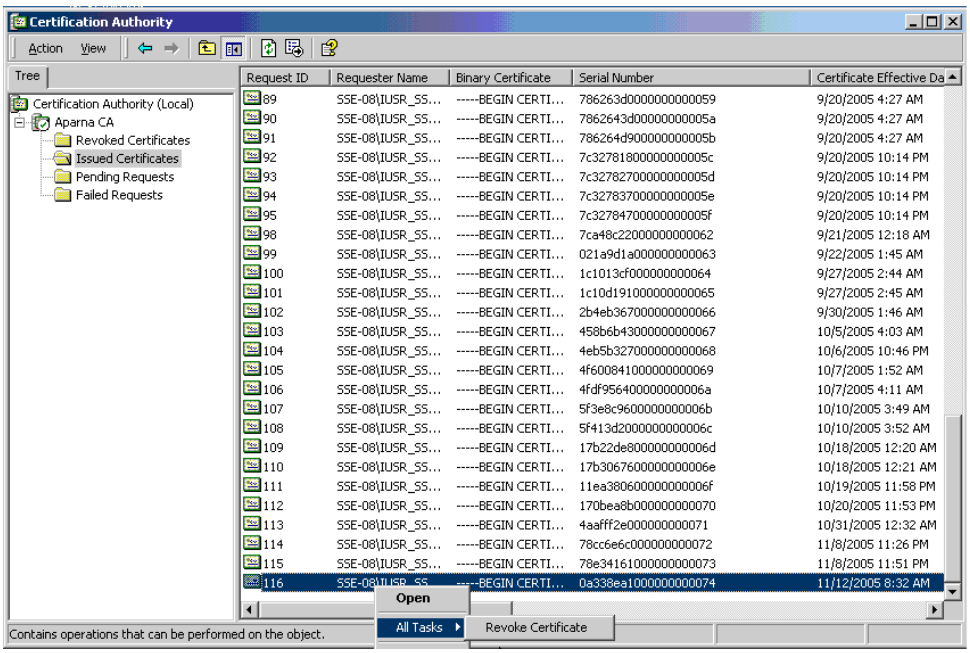


# 証明書の失効

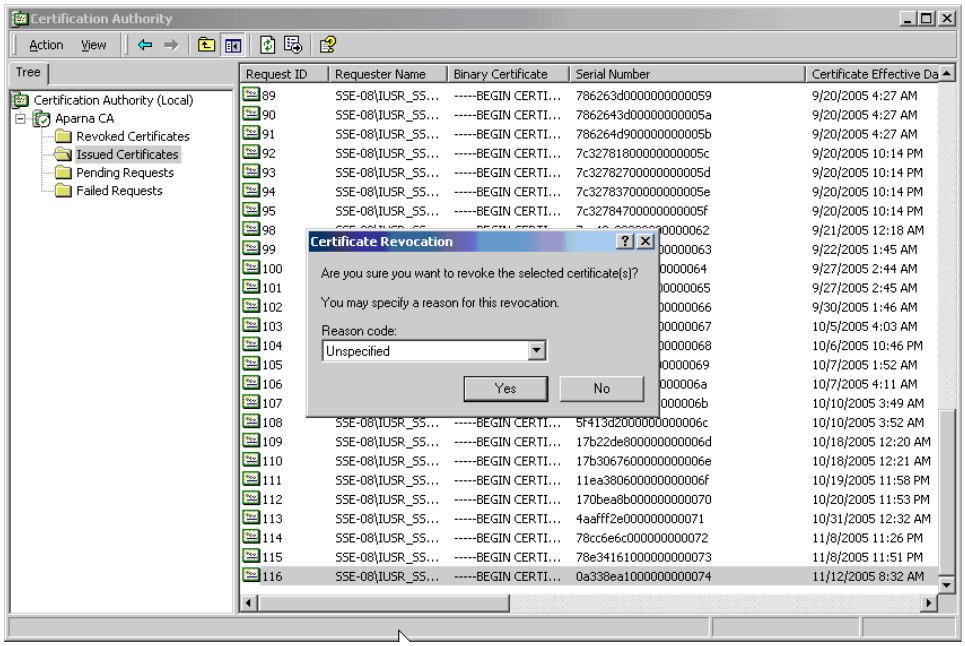
Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

**ステップ 1**　Certification Authority ツリーで、**Issued Certificates** フォルダをクリックします。リストから、失効させる証明書を右クリックします。

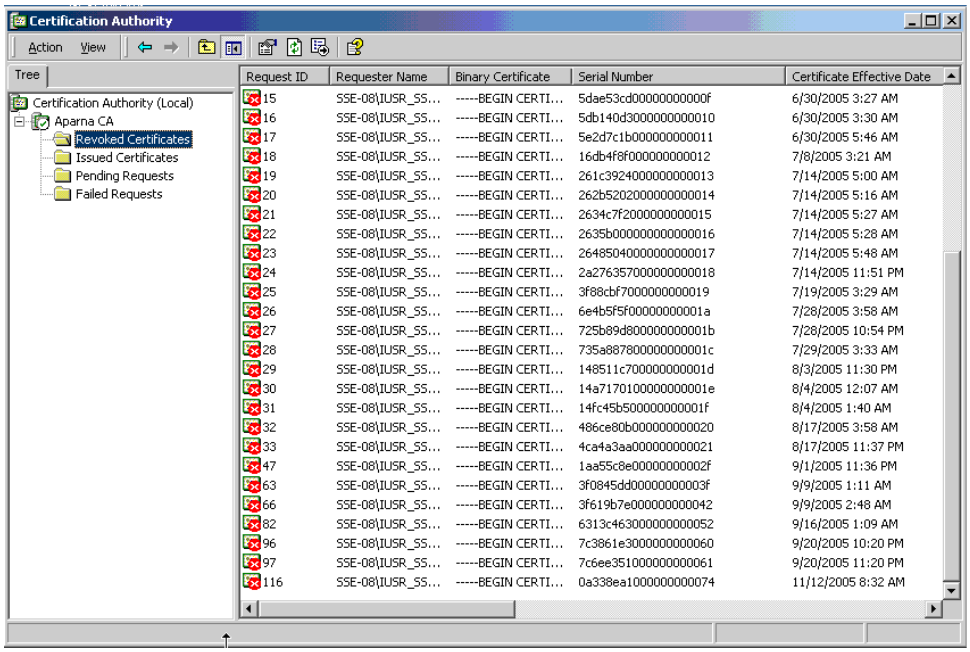
**ステップ 2**　[All Tasks] > [Revoke Certificate] を選択します。




**ステップ 3**　[Reason code] ドロップダウン リストから失効の理由を選択し、[Yes] をクリックします。



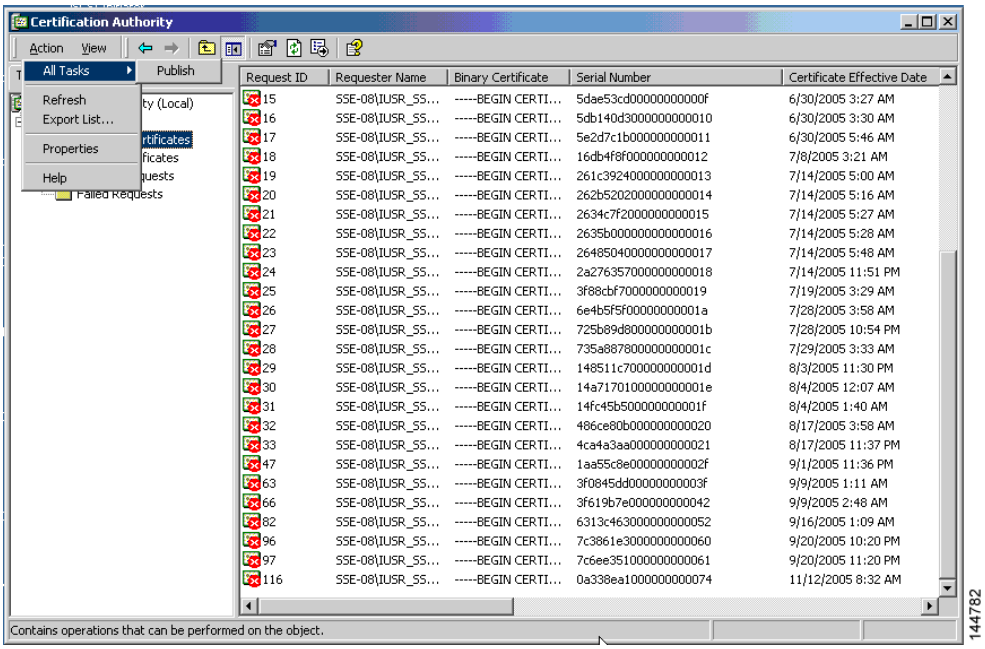

ステップ 4　[Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。



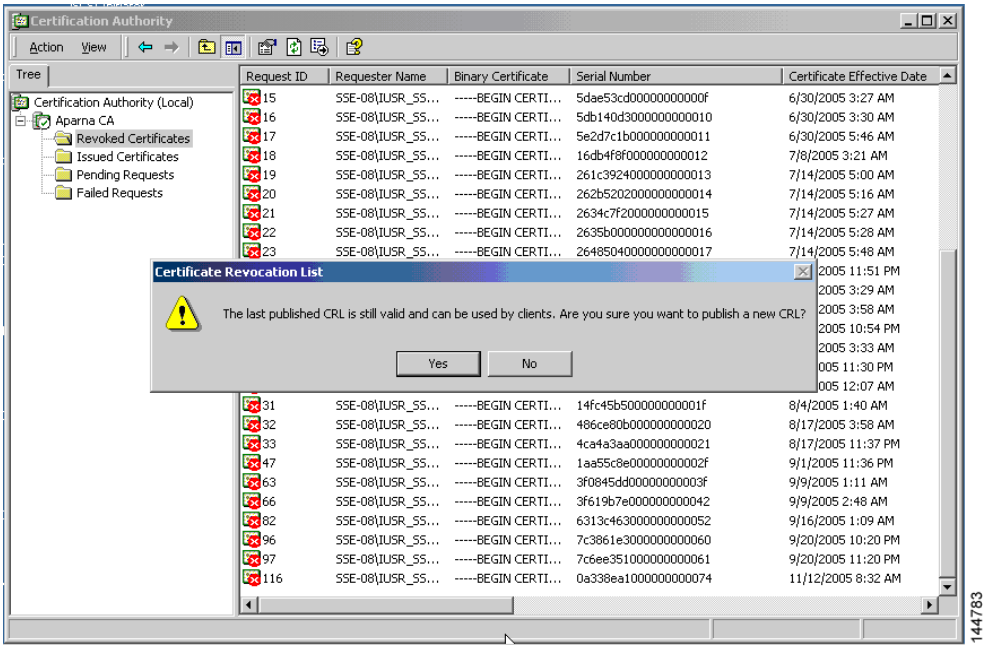
# CRL の生成および公開

Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

**ステップ 1**　[Certification Authority] 画面で、[Action] > [All Tasks] > [Publish] を選択します。



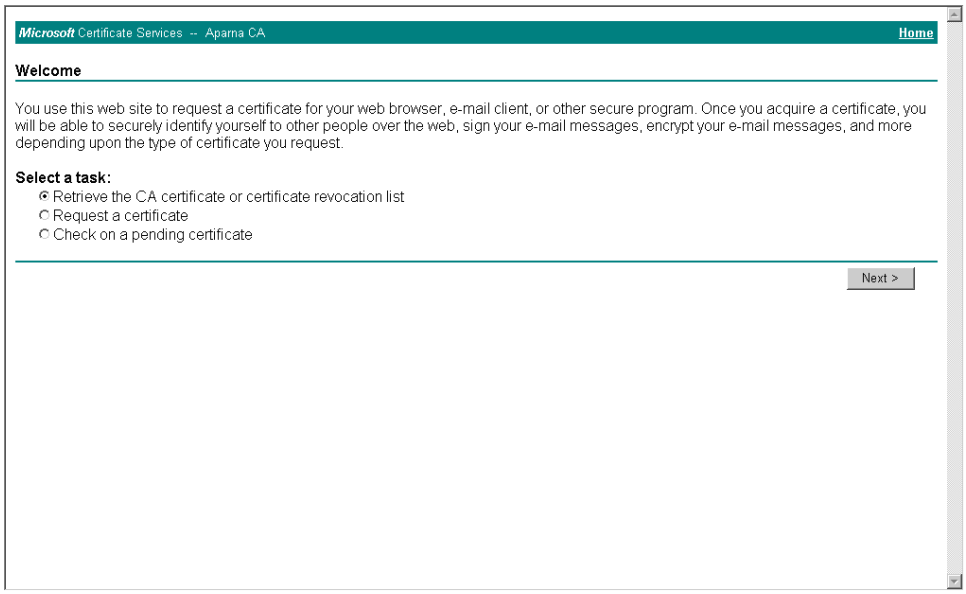

**ステップ 2**　[Certificate Revocation List] ダイアログボックスで [Yes] をクリックし、最新の CRL を公開します。



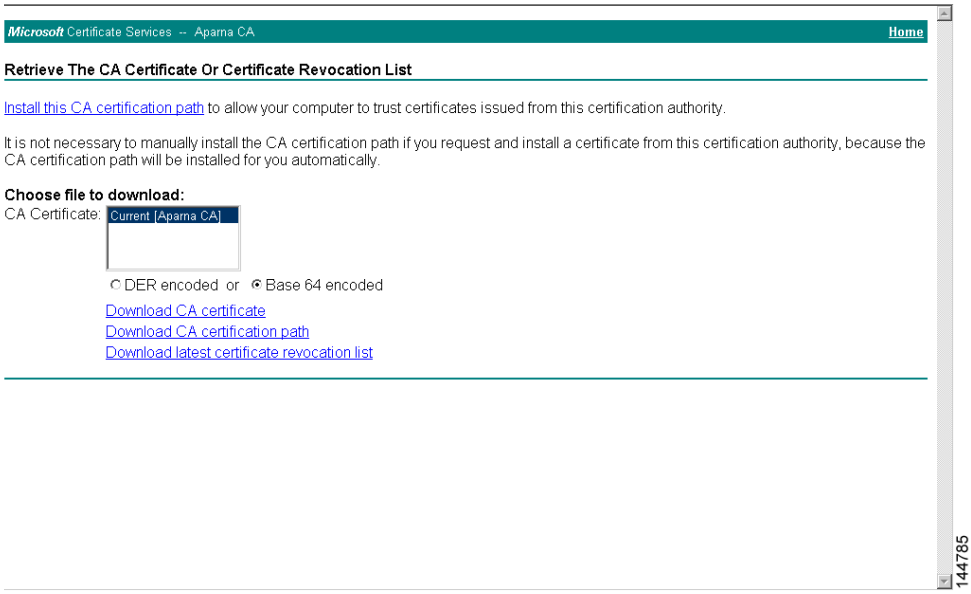
# CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

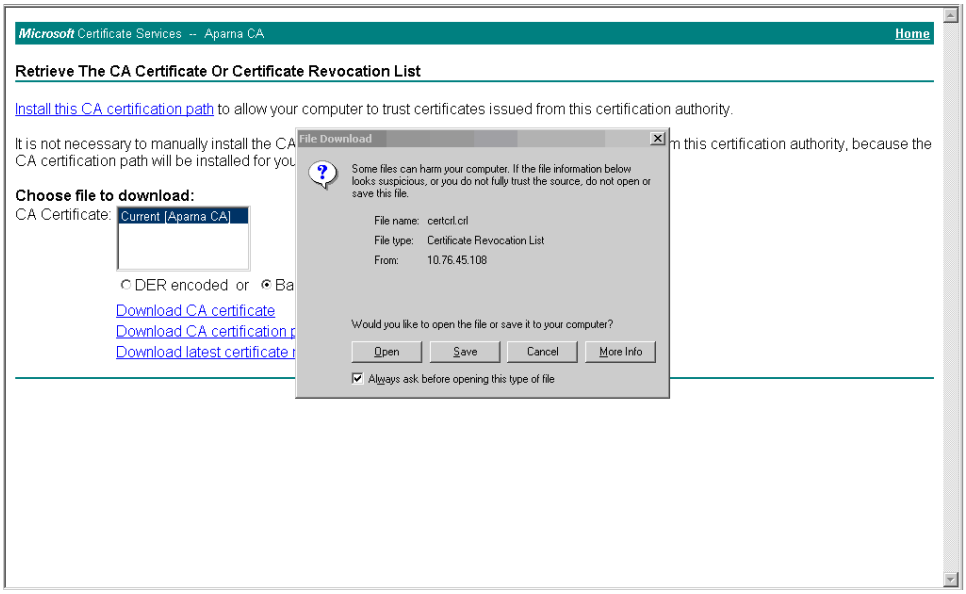
**ステップ 1**　Microsoft Certificate Services Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。



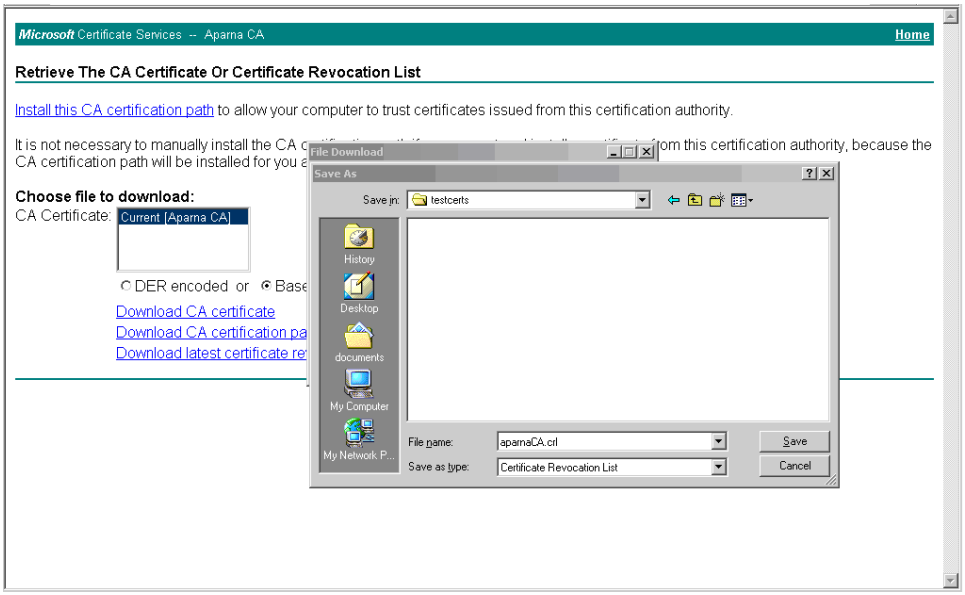

**ステップ 2**　[Download latest certificate revocation list] リンクをクリックします。



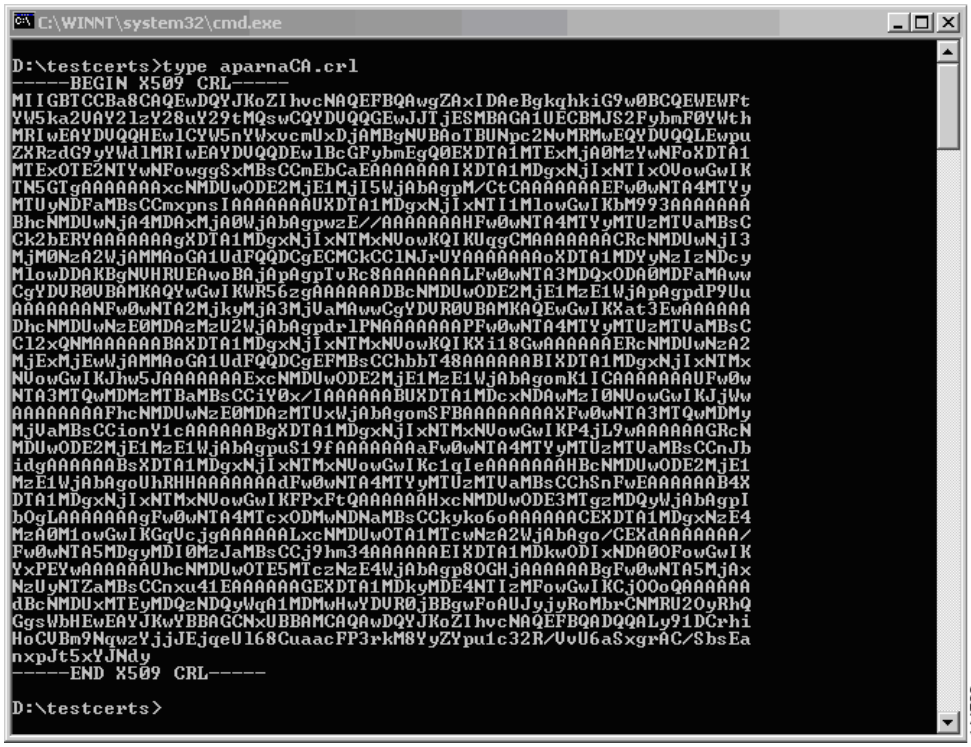

**ステップ 3**　[File Download] ダイアログボックスで、[Save] をクリックします。




ステップ 4　[Save As] ダイアログボックスに宛先ファイル名を入力し、[Save] をクリックします。




ステップ 5　Microsoft Windows の **type** コマンドを使用して、CRL を表示します。




# CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

**ステップ 1**　CRL ファイルを MDS スイッチのブートフラッシュにコピーします。

```
Vegas-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
```

**ステップ 2**　CRL を設定します。

```
Vegas-1# config terminal
Vegas-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Vegas-1(config)#
```

**ステップ 3**　CRL の内容を表示します。

```
Vegas-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
        Last Update: Nov 12 04:36:04 2005 GMT
        Next Update: Nov 19 16:56:04 2005 GMT
        CRL extensions:
```

```
            X509v3 Authority Key Identifier:
            keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1

            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 611B09A1000000000002
        Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
        Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
        Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
        Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 5349AD4600000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 53BD173C00000000000B
        Revocation Date: Jul  4 18:04:01 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Certificate Hold
Serial Number: 591E7ACE00000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Key Compromise
Serial Number: 5DAB771300000000000E
        Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD00000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Cessation Of Operation
Serial Number: 16DB4F8F000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F2000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
```

```
        Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 3F88CBF7000000000019
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 6E4B5F5F000000000001A
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 725B89D8000000000001B
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 735A887800000000001C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 148511C700000000001D
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A71701000000000001E
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14FC45B500000000001F
        Revocation Date: Aug 17 18:30:42 2005 GMT
    Serial Number: 486CE80B000000000020
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 4CA4A3AA000000000021
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 1AA55C8E00000000002F
        Revocation Date: Sep  5 17:07:06 2005 GMT
    Serial Number: 3F0845DD00000000003F
        Revocation Date: Sep  8 20:24:32 2005 GMT
    Serial Number: 3F619B7E000000000042
        Revocation Date: Sep  8 21:40:48 2005 GMT
    Serial Number: 6313C463000000000052
        Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
        Revocation Date: Sep 20 17:52:56 2005 GMT
    Serial Number: 7C6EE351000000000061
        Revocation Date: Sep 20 18:52:30 2005 GMT
    Serial Number: 0A338EA1000000000074       <-- Revoked identity certificate
        Revocation Date: Nov 12 04:34:42 2005 GMT
    Signature Algorithm: sha1WithRSAEncryption
        0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
        44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
        29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
        1a:9f:1a:49:b7:9c:58:24:d7:72
```

(注)　失効しているスイッチのアイデンティティ証明書（シリアル番号 0A338EA1000000000074）は、最後にリストされます。

# 最大限度

表 6-1 に、CA およびデジタル証明書のパラメータの最大限度を示します。

*表 6-1　CA およびデジタル証明書の最大限度*

| 機能 | 最大制限 |
|---|---|
| スイッチ上で宣言するトラスト ポイント | 16 |
| スイッチ上で生成する RSA キー ペア | 16 |
| スイッチ上に設定するアイデンティティ証明書 | 16 |

*表 6-1　CA およびデジタル証明書の最大限度(続き)*

| 機能 | 最大制限 |
|---|---|
| CA 証明書チェーンに含まれる証明書 | 10 |
| 特定の CA に対して認証されるトラスト ポイント | 10 |

# デフォルト設定

表 6-2 に、CA およびデジタル証明書のパラメータのデフォルト設定を示します。

*表 6-2　CA およびデジタル証明書のパラメータのデフォルト値*

| パラメータ | デフォルト |
|---|---|
| トラスト ポイント | なし |
| RSA キー ペア | なし |
| RSA キー ペアのラベル | Switch FQDN |
| RSA キー ペアのモジュール | 512 |
| RSA キー ペアのエクスポートの可否 | Yes |
| トラスト ポイントの失効チェック方式 | CRL |


# IPSec ネットワーク セキュリティの設定

IP Security（IPSec）プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供するオープン規格のフレームワークです。IPSec は、Internet Engineering Task Force（IETF）により開発されました。IPSec は、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つまたは複数のデータ フローの保護など、IP レイヤにセキュリティ サービスを提供します。IPSec 実装全体は、RFC 2401 の最新バージョンに準じています。Cisco NX-OS の IPSec は、RFC 2402 ～ RFC 2410 を実装しています。

IPSec はインターネット キー交換（IKE）プロトコルを使用して、プロトコルおよびアルゴリズムのネゴシエーションを処理し、IPSec で使用される暗号キーおよび認証キーを生成します。IKE は他のプロトコルとともに使用できますが、その初期実装時は IPSec プロトコルで使用します。IKE は、IPSec ピアを認証し、IPSec セキュリティ アソシエーションをネゴシエーションし、IPSec キーを確立します。IKE は RFC 2408、2409、2410、2412 を使用し、さらに draft-ietf-ipsec-ikev2-16.txt ドラフトを実装しています。

(注) IPSec という用語は、IPSec データ サービスのプロトコル全体および IKE セキュリティ プロトコルを示す場合や、データ サービスだけを示す場合に使用されることがあります。

この章は、次の項で構成されています。

# 機能情報

このセクションには、リリースの新機能と更新機能が一時的にについて説明します。

*表 7-1　新機能および変更された機能*

| 機能 | リリース | 説明 |
|---|---|---|
| Cisco MDS 9700 シリーズ スイッチでの SHA2 の IPSec および IKEv2 のサポート | 7.3(1)DY(1) | この機能は、Cisco MDS 9700 シリーズ スイッチでの SHA2 の IPSec およびで IKEv2 のサポートを有効にします。 |
| SHA2 の IPSec および IKEv2 のサポート | 7.3(0)D1(1) | この機能は、Cisco MDS 9250i スイッチでの SHA2 の IPSec および IKEv2 のサポートを有効にします。 |

# IPSec の概要

IP Security（IPSec）プロトコルは、加入ピア間にデータ機密保持、データの整合性、およびデータ認証を提供するオープン規格のフレームワークです。IPSec は、Internet Engineering Task Force（IETF）により開発されました。IPSec は、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つまたは複数のデータ フローの保護など、IP レイヤにセキュリティ サービスを提供します。IPSec 実装全体は、RFC 2401 の最新バージョンに準じています。Cisco NX-OS の IPSec は、RFC 2402 ～ RFC 2410 を実装しています。

IPSec はインターネット キー交換（IKE）プロトコルを使用して、プロトコルおよびアルゴリズムのネゴシエーションを処理し、IPSec で使用される暗号キーおよび認証キーを生成します。IKE は他のプロトコルとともに使用できますが、その初期実装時は IPSec プロトコルで使用します。IKE は、IPSec ピアを認証し、IPSec セキュリティ アソシエーションをネゴシエーションし、IPSec キーを確立します。IKE は RFC 2408、2409、2410、2412 を使用し、さらに draft-ietf-ipsec-ikev2-16.txt ドラフトを実装しています。

IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPSec はネットワーク層で機能し、参加する IPSec デバイス（ピア）間の IP パケットを保護し、認証します。

（注）　HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeCenter 対応 Cisco Fabric Switch は、IPSec をサポートしていません。

IPSec は、インターネットなどの保護されていないネットワークを使用して機密情報を送信する場合に、セキュリティを提供します。IPSec はネットワーク層で機能し、参加する IPSec デバイス（ピア）間の IP パケットを保護し、認証します。

IPSec は、次のネットワーク セキュリティ サービスを提供します。一般に、関与する 2 つの IPSec デバイス間でどのサービスが使用されるかは、ローカル セキュリティ ポリシーによって決まります。

- データ機密性:ネットワークにパケットを伝送する前に IPSec 送信側がパケットを暗号化できます。
- データ整合性:IPSec 受信者は、IPSec 送信者から送信されたパケットを認証し、伝送中にデータが変更されていないかを確認できます。
- データ送信元認証:IPSec 受信者は、送信された IPSec パケットの送信元を認証できます。このサービスは、データ整合性サービスに依存します。
- リプレイ防止:IPSec 受信側でリプレイ パケットを検出し、拒否できます。

(注)　*データ認証*は、通常、データ整合性およびデータ発信元認証を意味します。この章では、特に明記されていないかぎり、データ認証にはリプレイ防止サービスも含まれます。

IPSec を使用すれば、データを、観察、変更、またはスプーフィングされることを心配することなく、パブリック ネットワークを介して転送できます。これにより、インターネット、エクストラネット、およびリモート ユーザ アクセスを含む、バーチャル プライベート ネットワーク（VPN）などのアプリケーションが可能となります。

Cisco NX-OS ソフトウェアに実装された IPSec は、カプセル化セキュリティ ペイロード（ESP）プロトコルをサポートしています。このプロトコルはデータをカプセル化して保護し、データ プライバシー サービス、オプションのデータ認証、およびオプションのリプレイ防止サービスを提供します。

(注)　カプセル化セキュリティ ペイロード（ESP）プロトコルは、既存の TCP/IP パケットに挿入されたヘッダーで、サイズは実際の暗号化およびネゴシエートされた認証アルゴリズムによって異なります。フラグメンテーションを防止するために、暗号化パケットは、インターフェイスの最大伝送単位（MTU）と一致します。TCP のパス MTU の暗号化計算には、ESP ヘッダーの追加分、およびトンネル モードの外部 IP ヘッダーが考慮されます。MDS スイッチは、IPSec 暗号化によるパケット増加を 100 バイトまで許容します。

(注)　IPSec および IKE を使用するとき、IPS モジュール（18+4、および 24/10 ポート SAN 拡張モジュール）上の各ギガビット イーサネット インターフェイスは、独自の IP サブネット内で設定する必要があります。同じ IP サブネットの IP アドレスまたはネットワークマスクで複数のギガビット イーサネット インターフェイスが設定される場合、IKE パケットは正しいピアに送信されず、IPSec トンネルは起動しません。

# IKE の概要

IKE は、IPSec セキュリティ アソシエーション（SA）を自動的にネゴシエートし、IPSec 機能を使用してすべてのスイッチのキーを生成します。IKE の具体的な利点は次のとおりです。

- IPSec SA をリフレッシュできます。
- IPSec でアンチ リプレイ サービスが使用可能です。
- 管理可能でスケーラブルな IPSec 設定をサポートします。
- ピアのダイナミック認証が可能です。

(注)　HP c-Class BladeSystem 対応 Cisco Fabric Switch および IBM BladeSystem 対応 Cisco Fabric Switch は、IKE をサポートしていません。

# IPSec の前提条件

IPSec 機能を使用するには、次の作業を実行する必要があります。

- ENTERPRISE_PKG ライセンスを取得します（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。
- IKE を設定します。「IKE 初期設定の概要」セクション（7-195 ページ）を参照してください。

# IPSec の使用方法

IPSec 機能を使用する手順は、次のとおりです。

ステップ 1　ENTERPRISE_PKG ライセンスを取得して、IPSec for Small Computer Systems Interface over IP（iSCSI）および IPSec for Fibre Channel over IP（FCIP）をイネーブルにします。詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。

ステップ 2　IKE を設定します。「IPsec および IKE の手動設定」セクション（7-194 ページ）を参照してください。

（注）　IPSec 機能は、既存のパケットに新しいヘッダーを挿入します（詳細については、『Cisco MDS 9000 Family NX-OS IP Services Configuration Guide』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。



## IPSec の互換性

IPSec 機能は、次の Cisco MDS 9000 ファミリ ハードウェアと互換性があります。

- Cisco 18/4 ポート マルチサービス モジュール（MSM-18/4）。
- Cisco MDS 9250i マルチサービス ファブリック スイッチ。
- Cisco MDS 9700 シリーズ スイッチの Cisco MDS 24/10 ポート SAN 拡張モジュール。
- IPSec 機能は、管理インターフェイス上ではサポートされません。

IPSec 機能は、次のファブリック設定と互換性があります。

- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装している、2 台の接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco MDS SAN-OS Release 2.0(1b) 以降または Cisco NX-OS 4.1(1) を実装し、任意の IPSec 互換デバイスに接続された Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタ。
- Cisco NX-OS 上に実装された IPSec 機能では、次の機能はサポートされません。

- 認証ヘッダー（AH）
- トランスポート モード
- SA のバンドル
- SA の手動設定
- クリプト マップにおけるホスト単位の SA オプション
- SA アイドル タイムアウト
- ダイナミック クリプト マップ

(注)　このマニュアルでは、クリプト マップという用語は、スタティック クリプト マップだけを意味します。

# IPSec および IKE に関する用語

ここでは、この章で使用する用語について説明します。

- セキュリティ アソシエーション（SA）：IP パケットの暗号化および暗号解除に必要なエントリに関する、2 つの参加ピア間の合意。ピア間に双方向通信を確立するには、ピアごとに各方向（着信および発信）に対応する 2 つの SA が必要です。双方向の SA レコードのセットは、SA データベース（SAD）に保管されます。IPSec は IKE を使用して SA をネゴシエートし、起動します。各 SA レコードには、次の情報が含まれます。
  - セキュリティ パラメータ インデックス（SPI）：宛先 IP アドレスおよびセキュリティ プロトコルと組み合わせて、特定の SA を一意に識別する番号。IKE を使用して SA を確立する場合、各 SA の SPI は疑似乱数によって生成された番号です。
  - ピア：IPSec に参加するスイッチなどのデバイス。IPSec をサポートする Cisco MDS スイッチまたはその他のシスコ製ルータなどがあります。
  - トランスフォーム：データ認証およびデータ機密保持を提供するために実行される処理のリスト。Hash Message Authentication Code（HMAC）-MD5 認証アルゴリズムを使用する ESP プロトコルなどがあります。
  - セッション キー：セキュリティ サービスを提供するためにトランスフォームによって使用されるキー。
  - ライフタイム：SA を作成した時点から、ライフタイム カウンタ（秒およびバイト単位）がカウントされます。制限時間が経過すると、SA は動作不能になり、必要に応じて、自動的に再ネゴシエート（キーが再設定）されます。
  - 動作モード：IPSec では通常、2 つの動作モード（トンネル モードおよびトランスペアレント モード）を使用できます。Cisco NX-OS に実装された IPSec は、トンネル モードだけをサポートします。IPSec トンネル モードは、ヘッダーを含めた IP パケットを暗号化して、認証します。ゲートウェイは、ホストおよびサブネットの代わりにトラフィックを暗号化します。Cisco NX-OS に実装された IPSec では、トランスペアレント モードはサポートされません。

  (注)　*トンネル モード*という用語は、FCIP リンクで接続された 2 台のスイッチなど、2 つのピア間のセキュアな通信パスを示すための *トンネル*とは異なります。

- リプレイ防止：受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービス。IPSec は、データ認証とシーケンス番号を組み合わせて使用することにより、このオプション サービスを提供します。

- データ認証:データ認証は整合性だけ、または整合性と認証の両方を意味することがあります(データ発信元認証はデータ整合性に依存します)。
  - データ整合性:データが変更されていないことを確認します。
  - データ発信元認証:要求を受けた送信側からデータが実際に送信されたことを確認します。
- データ機密保護:保護されたデータを傍受できないようにするセキュリティ サービス。
- データ フロー:送信元アドレス/マスクまたはプレフィックス、宛先アドレス/マスクまたはプレフィックス長、IP ネクスト プロトコル フィールド、および送信元/宛先ポートの組み合わせで識別されるトラフィック グループ(プロトコルおよびポート フィールドにいずれかの値を設定できます)。これらの値の特定の組み合わせと一致するトラフィックは、1 つのデータ フローに論理的にグループ化されます。データ フローは、2 台のホスト間の単一の TCP 接続、あるいは 2 つのサブネット間のトラフィックを示します。IPSec 保護はデータ フローに適用されます。
- Perfect Forward Secrecy(PFS):取得された共有シークレット値に対応する暗号特性。PFS を使用すると、1 つのキーが損なわれても、これ以降のキーは前のキーの取得元から取得されないため、前および以降のキーには影響しません。
- Security Policy Database(SPD):トラフィックに適用される順序付きポリシー リスト。ポリシーにより、パケットに IPSec 処理が必要かどうか、クリア テキストでの送信を許可するかどうか、または廃棄するかどうかが判別されます。
  - IPSec SPD は、クリプト マップのユーザ設定から取得されます。
  - IKE SPD はユーザが設定します。

# サポート対象の IPSec トランスフォームおよびアルゴリズム

IPSec に実装されたコンポーネント テクノロジーには、次のトランスフォームが含まれます。

- Advanced Encrypted Standard(AES):暗号化アルゴリズム。AES は Cipher Block Chaining(CBC)またはカウンタ モードを使用して、128 ビットまたは 256 ビットを実装します。
- データ暗号規格(DES):パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル(IV)が必要です。IV は IPSec パケットに明示的に指定されます。
- Triple DES(3DES):信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。

(注)　強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- Message Digest 5(MD5):HMAC バリアントを使用するハッシュ アルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュ バリアントです。
- Secure Hash Algorithm(SHA-1、SHA-2)はハッシュ メッセージ認証コード(HMAC)バリアントを使用するハッシュ アルゴリズムです。Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降の Cisco MDS 9250i マルチサービス ファブリック スイッチで、IPsec は SHA-2 をサポートします。

- AES-XCBC-MAC：AES アルゴリズムを使用する Message Authentication Code（MAC）。
- IPsec は、Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降の Cisco MDS 24/10 ポート SAN 拡張モジュール（Cisco MDS 9700 シリーズ スイッチ）で SHA-2 をサポートしています。

## サポート対象の IKE トランスフォームおよびアルゴリズム

IKE に実装されたコンポーネント テクノロジーには、次のトランスフォームが含まれます。

- Diffie-Hellman（DH）：保護されていない通信チャネルを介して 2 つのパーティが共有シークレットを確立できるようにする、公開キー暗号化プロトコル。Diffie-Hellman は、IKE 内でセッション キーを確立するために使用されます。グループ 1（768 ビット）、グループ 2（1024 ビット）、およびグループ 5（1536 ビット）がサポートされます。
- Advanced Encrypted Standard（AES）：暗号化アルゴリズム。AES は、CBC を使用する 128 ビット、またはカウンタ モードを実装します。
- データ暗号規格（DES）：パケットデータを暗号化するために使用され、必須の 56 ビット DES-CBC を実装します。CBC には、暗号化を開始するための初期ベクトル（IV）が必要です。IV は IPSec パケットに明示的に指定されます。
- Triple DES（3DES）：信頼できないネットワーク上で重要な情報を送信できるようにする、168 ビット暗号キーを使用した強力な DES 形式です。

（注）　強力な暗号化を使用する Cisco NX-OS イメージは、米国政府の輸出規制の対象で、配信が制限されています。米国以外の国でインストールされるイメージには、輸出許可が必要です。米国政府の規制により、お客様の注文が拒否されたり、納入が遅れたりすることがあります。詳細については、営業担当者または販売業者、あるいは export@cisco.com までお問い合わせください。

- Message Digest 5（MD5）：HMAC バリアントを使用するハッシュ アルゴリズム。HMAC はデータの認証に使用されるキー付きハッシュ バリアントです。
- Secure Hash Algorithm（SHA-1、SHA-2）はハッシュ メッセージ認証コード（HMAC）バリアントを使用するハッシュ アルゴリズムです。IKEv2 は Cisco MDS NX-OS リリース 7.3(0)D1(1) 以降、Cisco MDS 9250i マルチサービス ファブリック スイッチで SHA-2 をサポートします。

（注）　IKEv1 は SHA-2 をサポートしません。

- スイッチの認証アルゴリズム：IP アドレスに基づく事前共有キーを使用します。
- IKEv2 は、Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降の Cisco MDS 24/10 ポート SAN 拡張モジュール（Cisco MDS 9700 シリーズ スイッチ）で SHA-2 をサポートしています。

# IPSec デジタル証明書のサポート

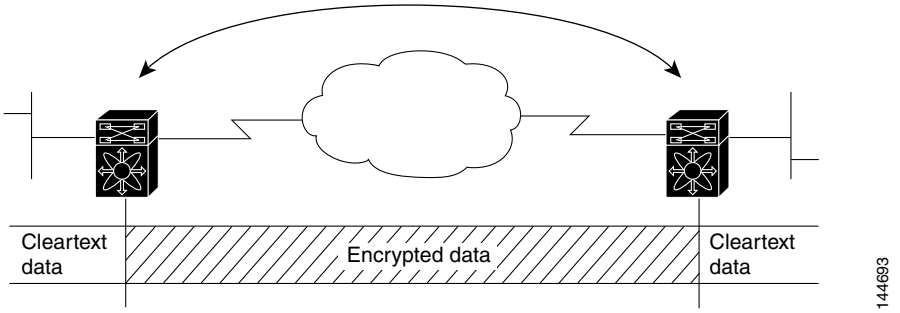
ここでは、認証局（CA）およびデジタル証明書を使用した認証の利点について説明します。

# CA およびデジタル証明書を使用しない IPSec の実装

CA およびデジタル証明書を使用しない場合、2 台の Cisco MDS スイッチ間で IPSec サービス（暗号化など）をイネーブルにするには、各スイッチに他方のスイッチのキー（RSA 公開キーまたは共有キーなど）が必要になります。IPSec サービスを使用するファブリック内の各スイッチに、RSA 公開キーまたは事前共有キーのどちらかを手動で指定する必要があります。また、ファブリックに新しいデバイスを追加する場合、安全な通信をサポートするには、ファブリック内の他方のスイッチを手動で設定する必要があります。各（図 7-1 を参照）スイッチは他方のスイッチのキーを使用して、他方のスイッチのアイデンティティを認証します。この認証は、2 台のスイッチ間で IPsec トラフィックが交換される場合に、必ず実行されます。

複数の Cisco MDS スイッチをメッシュ トポロジで配置し、すべてのスイッチ間で IPSec トラフィックを交換させる場合には、最初に、すべてのスイッチ間に共有キーまたは RSA 公開キーを設定する必要があります。

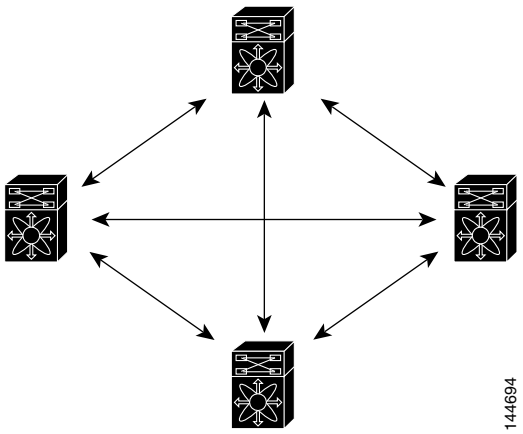
*図 7-1　CA およびデジタル証明書を使用しない 2 台の IPSec スイッチ*




IPSec ネットワークに新しいスイッチを追加するごとに、新しいスイッチと既存の各スイッチ間にキーを設定する必要があります（図 7-2 の場合、このネットワークに 1 台の暗号化スイッチを追加するには、新たに 4 つのスイッチ間キーの設定が必要になります）。

したがって、IPSec サービスを必要とするデバイスが増えるほど、キー管理は複雑になります。このアプローチでは、より大型で複雑な暗号化ネットワークには拡張できません。

*図 7-2　CA およびデジタル証明書を使用しない 4 台の IPSec スイッチ*

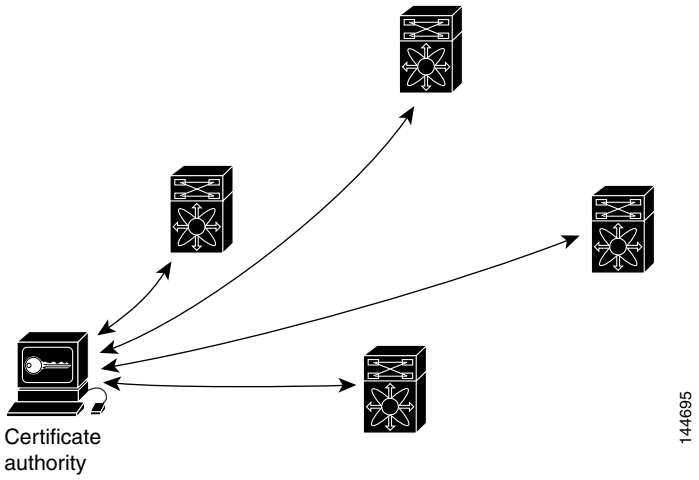


# CA およびデジタル証明書を使用した IPSec の実装

CA およびデジタル証明書を使用する場合には、すべての暗号化スイッチ間にキーを設定する必要はありません。代わりに、加入させる各スイッチを CA に個別に登録し、各スイッチの証明書を要求します。この設定が完了していれば、各加入スイッチは、他のすべての加入スイッチをダイナミックに認証できます。2 台のデバイスが通信する場合、証明書を交換し、データをデジタル署名して、お互いを認証します。ネットワークに新しいデバイスを追加する場合には、そのデバイスを CA に登録するだけでよく、他のデバイスの設定を変更する必要はありません。新しいデバイスが IPSec 接続を試みると、証明書が自動的に交換され、そのデバイスが認証されます。

図 7-3 に、デバイスをダイナミックに認証するプロセスを示します。

*図 7-3　CA によるデバイスのダイナミックな認証*




ネットワークに新しい IPSec スイッチを追加する場合、新しいスイッチが CA に証明書を要求するように設定するだけでよく、既存の他のすべての IPSec スイッチとの間に複数のキー設定を行う必要はありません。

# IPSec デバイスによる CA 証明書の使用方法

2 台の IPSec スイッチが IPSec で保護されたトラフィックを交換するには、最初に相互に認証しあう必要があります。認証されていない場合、IPSec 保護が適用されません。この認証を行うには、IKE を使用します。

IKE では、2 つの方法を使用してスイッチを認証できます。CA を使用しない場合には事前共有キーを使用し、CA を使用する場合には RSA キー ペアを使用します。どちらの方法も、2 台のスイッチ間にキーが事前設定されている必要があります。

CA を使用しない場合、スイッチは RSA 暗号化事前共有キーを使用して、リモート スイッチに対して自身を認証します。

CA を使用する場合、スイッチはリモート スイッチに証明書を送信し、何らかの公開キー暗号法を実行することによって、リモート スイッチに対して自身を認証します。各スイッチは、CA により発行されて検証された、スイッチ固有の証明書を送信する必要があります。このプロセスが有効なのは、各スイッチの証明書にスイッチの公開キーがカプセル化され、各証明書が CA によって認証されることにより、すべての加入スイッチが CA を認証局として認識するからです。この機構は、RSA シグニチャを使用する IKE と呼ばれます。

スイッチは、証明書が期限切れになるまで、複数の IPSec ピアに対して、複数の IPSec セッション用に自身の証明書を継続的に送信できます。証明書が期限切れになった場合、スイッチ管理者は CA から新しい証明書を取得する必要があります。

また、CA は、IPSec に参加しなくなったデバイスの証明書を失効できます。失効された証明書は、他の IPSec デバイスから有効とは見なされません。失効された証明書は、証明書失効リスト（CRL）にリストされ、各ピアは相手側ピアの証明書を受け入れる前に、このリストを確認できます。

IKE の証明書サポートでは、次の考慮事項に留意してください。

- IKE 用の証明書をインストールする前に、スイッチの FQDN（ホスト名およびドメイン名）が設定されている必要があります。
- IKE が使用するのは、IKE 用または汎用として設定された証明書だけです。
- スイッチに設定された最初の IKE 用または汎用証明書が、IKE のデフォルトの証明書として使用されます。
- ピアが別の証明書を指定しないかぎり、すべての IKE ピアに対してデフォルトの証明書が使用されます。
- ピアが、そのピアが信頼する CA によって署名された証明書を要求した場合、IKE は、要求された証明書がスイッチに存在すれば、デフォルトの証明書でなくても、その証明書を使用します。
- デフォルトの証明書が削除された場合、次の IKE 用または汎用証明書が存在すれば、IKE はそれをデフォルトの証明書として使用します。
- IKE では、証明書チェーンはサポートされません。
- IKE は、CA チェーン全体ではなく、アイデンティティ証明書だけを送信します。ピア上で証明書が確認されるには、ピア上に同じ CA チェーンが存在する必要があります。

# IPsec および IKE の手動設定

ここでは、IPSec および IKE を手動で設定する方法について説明します。

IPSec は、加入ピア間に安全なデータ フローを提供します。2 つのピア間では、異なる SA セットを使用する各トンネルで異なるデータ フローを保護することにより、複数の IPSec データ フローをサポートできます。

IKE 設定の完了後、IPSec を設定します。

各加入 IPSec ピアに IPSec を設定する手順は、次のとおりです。

**ステップ 1**　トラフィック用の安全なトンネルを確立する必要があるピアを識別します。

**ステップ 2**　必要なプロトコルとアルゴリズムにより、トランスフォーム セットを設定します。

**ステップ 3**　クリプト マップを作成し、適切なアクセス コントロール リスト（IPv4-ACL）、トランスフォーム セット、ピア、およびライフタイム値を適用します。

**ステップ 4**　クリプト マップを、必要なインターフェイスに適用します。

ここでは、次の内容について説明します。



# IKE 初期設定の概要

IPSec 機能により必要なピアでデータ フローを確立するには、IKE 機能をイネーブルにして、設定しておく必要があります。Fabric Manager では、IKE の最初の設定時に、IKE が初期設定されます。

IPSec がイネーブルの場合には、IKE をディセーブルにできません。IKE 機能をディセーブルにすると、IKE 設定が実行コンフィギュレーションから消去されます。

# IKE のイネーブル化

IKE をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# feature crypto ike` | IKE 機能をイネーブルにします。 |
| | `switch(config)# no feature crypto ike` | IKE 機能をディセーブル（デフォルト）にします。<br>（注）　IKE 機能をディセーブルにする前に、IPsec をディセーブルにする必要があります。 |

# IKE ドメインの概要

ローカル スイッチのスーパーバイザ モジュールにトラフィックを到達させるには、IPSec ドメインに IKE 設定を適用する必要があります。Fabric Manager では、IKE の設定時に IPSec ドメインが自動的に設定されます。

# IKE ドメインの設定

ローカル スイッチのスーパーバイザ モジュールにトラフィックを到達させるには、IPSec ドメインに IKE 設定を適用する必要があります。

IPsec ドメインを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto ike domain ipsec` | IPsec ドメインに対する IKE の設定を許可します。 |

# IKE トンネルの概要

IKE トンネルは、2 つのエンドポイント間の安全な IKE セッションです。IKE は、IPSec SA ネゴシエーションで使用される IKE メッセージを保護するために、このトンネルを作成します。

Cisco NX-OS の実装では、2 つのバージョンの IKE が使用されています。

- IKE バージョン 1（IKEv1）は、RFC 2407、2408、2409、および 2412 を使用して実装されます。
- IKE バージョン 2（IKEv2）は、より効率的な簡易バージョンで、IKEv1 とは相互運用できません。IKEv2 は、draft-ietf-ipsec-ikev2-16.txt ドラフトを使用して実装されます。

# IKE ポリシー ネゴシエーションの概要

IKE ネゴシエーションを保護するには、各 IKE ネゴシエーションを共通（共有）IKE ポリシーで開始します。IKE ポリシーを使い、IKE ネゴシエーション中に使用するセキュリティ パラメータの組み合わせを定義します。デフォルトでは、IKE ポリシーは設定されません。各ピアに IKE ポリシーを作成する必要があります。このポリシーにより、以降の IKE ネゴシエーションを保護するために使用するセキュリティ パラメータを指定し、ピアの認証方法を指示します。最低 1 つのポリシーがリモート ピアのポリシーと一致するように、各ピアに優先順位を付けた複数のポリシーを設定できます。

ポリシーは、暗号化アルゴリズム（DES、3DES、AES）、ハッシュ アルゴリズム（SHA、MD5）、および DH グループ（1、2、5）に基づいて設定できます。各ポリシーに、パラメータ値の異なる組み合わせを設定できます。設定したポリシーには、固有のプライオリティ番号を指定します。この番号の範囲は、1（最上位のプライオリティ）～ 255（最下位のプライオリティ）です。スイッチに、複数のポリシーを設定できます。リモート ピアに接続する必要がある場合、ローカル スイッチの少なくとも 1 つのポリシーが、リモート ピアに設定されているパラメータ値と一致する必要があります。同じパラメータ設定のポリシーが複数ある場合には、最も小さい番号のポリシーが選択されます。

表 7-2 に、許可されるトランスフォームの組み合わせのリストを示します。

*表 7-2　IKE トランスフォーム設定パラメータ*

| パラメータ | 許容値 | キーワード | デフォルト値 |
|---|---|---|---|
| 暗号化アルゴリズム | 56 ビット DES-CBC | **des** | **3des** |
| | 168 ビット DES | **3des** | |
| | 128 ビット AES | **aes** | |
| ハッシュ アルゴリズム | SHA-1（HMAC バリアント）、SHA-2（HMAC バリアント） | **sha**<br>**sha256** | **sha** |
| | MD5（HMAC バリアント） | **sha512**<br>**md5** | |
| 認証方式 | 事前共有キー | 設定なし | 事前共有キー |
| DH グループ識別名 | 768 ビット DH | **1** | **1** |
| | 1024 ビット DH | **2** | |
| | 1536 ビット DH | **5** | |

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPSec および IKE 暗号化認証アルゴリズムの設定を示します。

| プラットフォーム | IKE | IPSec |
|---|---|---|
| Microsoft iSCSI 発信側（Microsoft Windows 2000 プラットフォームの Microsoft IPSec 実装） | 3DES、SHA-1、SHA-2、または MD5、DH グループ 2 | 3DES、SHA-1、SHA-2 |
| Cisco iSCSI イニシエータ、Linux プラットフォームへの Free Swan IPsec の実装 | 3DES、MD5、DH グループ 1 | 3DES、MD5 |

(注)　ハッシュ アルゴリズムを設定すると、対応する HMAC バージョンが認証アルゴリズムとして使用されます。

IKE ネゴシエーションが開始されると、IKE は、両ピア上で同一の IKE ポリシーを検索します。ネゴシエーションを開始したピアがすべてのポリシーをリモート ピアに送信し、リモート ピアの方では一致するポリシーを探そうとします。リモート ピアは、相手側ピアから受信したすべてのポリシーと自身の最優先ポリシーを比較することにより、一致しているポリシーを検索します。一致するポリシーが見つかるまで、リモート ピアは優先順位が高い順に各ポリシーをチェックします。

2 つのピアの暗号化、ハッシュ アルゴリズム、認証アルゴリズム、および DH グループ値が同じであれば、一致していると判断されます。一致しているポリシーが見つかると、IKE はセキュリティ ネゴシエーションを完了し、IPSec SA が作成されます。

一致しているポリシーが見つからない場合、IKE はネゴシエーションを拒否し、IPSec データ フローは確立されません。

# IKE ポリシーの設定

IKE ポリシー ネゴシエーション パラメータを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto ike domain ipsec` | IPsec ドメインをこのスイッチで設定できます。 |
| ステップ 3 | `switch(config-ike-ipsec)# identity address` | IKE プロトコルが IP アドレスを使用するようにアイデンティティ モードを設定します(デフォルト)。 |
| | `switch(config-ike-ipsec)# identity hostname` | IKE プロトコルが完全修飾ドメイン名(FQDN)を使用するようにアイデンティティ モードを設定します。<br>(注)　FQDN は認証に RSA シグニチャを使用する必要があります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | `switch(config-ike-ipsec)# key switch1 address 10.10.1.1` | ピアの IP アドレスに事前共有キーを関連付けます。 |
| | `switch(config-ike-ipsec)# key switch1 hostname switch1.cisco.com` | ピアの FQDN と事前共有キーを関連付けます。<br>(注)　FQDN を使用するには、ピアのスイッチ名とドメイン名を設定する必要があります。 |
| ステップ 5 | `switch(config-ike-ipsec)# policy 1` | 設定するポリシーを指定します。 |
| ステップ 6 | `switch(config-ike-ipsec-policy)# encryption des` | 暗号化ポリシーを設定します。 |
| ステップ 7 | `switch(config-ike-ipsec-policy)# group 5` | DH グループを設定します。 |
| ステップ 8 | `switch(config-ike-ipsec-policy)# hash md5` | ハッシュ アルゴリズムを設定します。 |
| ステップ 9 | `switch(config-ike-ipsec-policy)# authentication pre-share` | 認証方式を事前共有キーを使用するように設定します(デフォルト)。 |
| | `switch(config-ike-ipsec-policy)# authentication rsa-sig` | 認証方式を RSA シグニチャを使用するように設定します。<br>(注)　認証のために RSA シグニチャを使用するには、FQDN を使用してアイデンティティ認証モードを設定する必要があります(ステップ 3 を参照)。 |

(注)　IKE 証明書は FQDN タイプのサブジェクト名を使用するので、認証方式が rsa-sig の場合には、IKE 用のアイデンティティ ホスト名が設定されていることを確認してください。

(注)　Cisco MDS NX-OS リリース 5.2(x) にダウングレードする前に、事前共有キーを解除します。ダウングレードを完了したら、**key** *key-name* **hostname** *host* または **key** *key-name* **address** *ip-address* コマンドを使用して、事前共有キーを再設定します。

# オプションの IKE パラメータの設定

IKE 機能には、オプションで次のパラメータを設定できます。

- 各ポリシーのライフタイム アソシエーション:ライフタイムの範囲は 600 ～ 86,400 秒です。デフォルトは、86,400 秒(1 日)です。各ポリシーのライフタイム アソシエーションは、IKE ポリシーの設定時に設定します。「IKE ポリシーの設定」セクション(7-197 ページ)を参照してください。
- 各ピアのキープアライブ タイム(IKEv2 を使用する場合):キープアライブの範囲は 120 ～ 86,400 秒です。デフォルトは、3,600 秒(1 時間)です。
- 各ピアの発信側バージョン:IKEv1 または IKEv2(デフォルト)。発信側バージョンの選択は、リモート デバイスがネゴシエーションを開始する場合、相互運用性に影響しません。このオプションは、ピア デバイスが IKEv1 をサポートしていて、指定したデバイスを IKE の発信側として動作させる場合に設定します。FCIP トンネルの発信側バージョンを設定する場合には、次の事項に注意してください。

- FCIP トンネルの両側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1) を実行している場合、IKEv1 だけを使用するには、FCIP トンネルの両側に発信側バージョン IKEv1 を設定する必要があります。FCIP トンネルの一方の側が IKEv1 を使用し、他方の側が IKEv2 を使用している場合には、FCIP トンネルは IKEv2 を使用します。
- FCIP トンネルの片側のスイッチが MDS SAN-OS Release 3.0(1) 以降または Cisco NX-OS 4.1(1b) を実行し、FCIP トンネルの他方の側のスイッチが MDS SAN-OS Release 2.x を実行している場合、どちらか（または両方）の側に IKEv1 を設定すると、FCIP トンネルは IKEv1 を使用します。

**（注）** 2.x MDS スイッチと 3.x MDS スイッチ間の IPSec 構築では、IKEv1 だけがサポートされます。

**注意** 通常の環境ではスイッチが IKE 発信側として動作しない場合でも、発信側バージョンの設定が必要になることがあります。このオプションを常に使用することにより、障害時にトラフィック フローをより速く回復できます。

**ヒント** キープアライブ タイムが適用されるのは、IKEv2 ピアだけで、すべてのピアではありません。

**（注）** ホストの IPSec 実装により IPSec キー再設定を開始する場合には、Cisco MDS スイッチの IPSec のライフタイム値を、必ず、ホストのライフタイム値よりも大きい値に設定してください。

この項では、次のトピックについて取り上げます。



# ポリシーのライフタイム アソシエーションの設定

各ポリシーのライフタイム アソシエーションを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto ike domain ipsec` | IPsec ドメインをこのスイッチで設定できます。 |
| ステップ 3 | `switch(config-ike-ipsec)# policy 1` | 設定するポリシーを指定します。 |
| ステップ 4 | `switch(config-ike-ipsec-policy) lifetime seconds 6000` | 6,000 秒のライフタイムを設定します。 |

# ピアのキープアライブ タイムの設定

各ピアのキープアライブ タイムを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto ike domain ipsec` | IPsec ドメインをこのスイッチで設定できます。 |
| ステップ 3 | `switch(config-ike-ipsec)# keepalive 60000` | すべてのピアのキープアライブタイムを 60,000 秒に設定します。 |

# 発信側バージョンの設定

IPv4 を使用して発信側バージョンを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto ike domain ipsec` | IPsec ドメインをこのスイッチで設定できます。 |
| ステップ 3 | `switch(config-ike-ipsec)# initiator version 1 address 10.10.10.1` | デバイス 10.10.10.0 で IKE を開始するときに、IKEv1 を使用するようにスイッチを設定します<br>（注）　IKE は、IPv4 アドレスをサポートし、IPv6 アドレスはサポートしません。 |

# IKE トンネルまたはドメインのクリア

IKE 設定に IKE トンネル ID を指定していない場合は、EXEC モードで **clear crypto ike domain ipsec sa** コマンドを発行することにより、既存のすべての IKE ドメイン接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa
```

**注意**　IKEv2 トンネル内のすべての SA を削除すると、その IKE トンネルは自動的に削除されます。

IKE 設定に SA を指定している場合、EXEC モードで **clear crypto ike domain ipsec sa** *IKE_tunnel-ID* コマンドを発行して、指定した IKE トンネル ID 接続をクリアできます。

```
switch# clear crypto ike domain ipsec sa 51
```

**注意**　IKEv2 トンネルを削除すると、その IKE トンネルの下の関連付けられた IPsec トンネルが自動的に削除されます。

# SA のリフレッシュ

IKEv2 設定変更が行われた後に SA をリフレッシュするには、**crypto ike domain ipsec rekey IPv4-ACL**-*index* コマンドを使用します。

# クリプト IPv4-ACL

IP アクセス コントロール リスト（IPv4-ACL）は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4 IP-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを制限します。IPv4-ACL の作成および定義の詳細については、第 5 章「IPv4 および IPv6 のアクセス コントロール リストの設定」を参照してください。

クリプト マップのコンテキストでは、IPv4-ACL は標準の IPv4-ACL と異なります。標準の IPv4-ACL は、インターフェイス上で転送またはブロックするトラフィックを判別します。たとえば、IPv4-ACL を作成して、サブネット A とサブネット Y 間のすべての IP トラフィックを保護したり、ホスト A とホスト B 間の Telnet トラフィックを保護できます。

ここでは、次の内容について説明します。



## クリプト IPv4-ACL の概要

クリプト IPv4-ACL は、暗号による保護が必要な IP トラフィックと、必要ではないトラフィックとを定義するために使用します。

IPSec のクリプト マップ エントリに関連付けるクリプト IPv4-ACL には、4 つの主要な機能があります。

- IPSec で保護する発信トラフィックを選択する（permit に一致したものが保護の対象）。
- IPSec SA のネゴシエーションの開始時に、新しい SA で保護するデータ フロー（1 つの permit エントリで指定）を示す。
- 着信トラフィックを処理して、IPSec で保護すべきであったトラフィックをフィルタリングして廃棄する。
- IPSec ピアからの IKE ネゴシエーションの処理時に、要求されたデータ フローのために、IPSec SA の要求を受け入れるかどうかを判別する。

ヒント　一部のトラフィックに 1 つのタイプの IPSec 保護（暗号化だけ、など）を適用し、他のトラフィックに異なるタイプの IPSec 保護（認証と暗号化の両方など）を適用する場合には、2 つの IPv4-ACL を作成してください。異なる IPSec ポリシーを指定するには、異なるクリプト マップで両方の IPv4-ACL を使用します。

（注）　IPSec は、IPv6-ACL をサポートしていません。

## クリプト IPv4-ACL の注意事項

IPSec 機能に関する IPv4-ACL を設定する場合には、次の注意事項に従ってください。

- Cisco NX-OS ソフトウェアで使用できるのは、名前ベースの IPv4-ACL だけです。
- IPv4-ACL をクリプト マップに適用するときは、次のオプションを適用します。
  - 許可（permit）：トラフィックに IPSec 機能を適用します。
  - 拒否（deny）：クリア テキストを許可します（デフォルト）。

  （注）　IKE トラフィック（UDP ポート 500）は、必ずクリア テキストで送信されます。

- IPSec 機能が考慮するのは、送信元/宛先 IPv4 アドレスとサブネット マスク、プロトコル、および 1 つのポート番号だけです。IPSec では、IPv6 はサポートされません。

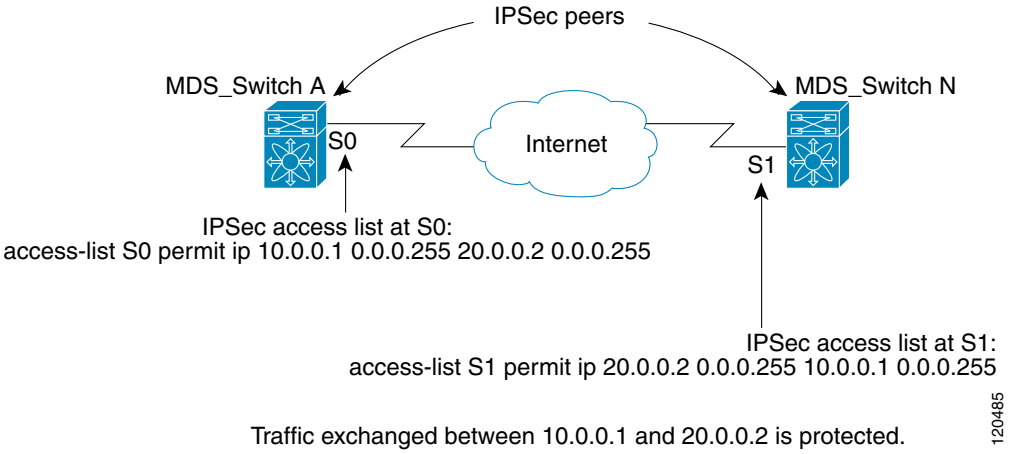
  （注）　IPSec 機能はポート番号範囲をサポートしていないので、指定されている場合には上位ポート番号フィールドは無視されます。

- permit オプションを指定すると、対応するクリプト マップ エントリで指定されたポリシーを使用して、指定条件に一致するすべての IP トラフィックが暗号によって保護されます。
- deny オプションを指定すると、トラフィックは暗号によって保護されません。最初の deny ステートメントにより、トラフィックはクリア テキストで送信されます。
- 定義するクリプト IPv4-ACL がインターフェイスに適用されるのは、対応するクリプト マップ エントリを定義して、インターフェイスにクリプト マップ セットを適用したあとです。
- 同じクリプト マップ セットのエントリごとに、異なる IPv4-ACL を使用する必要があります。
- インバウンドおよびアウトバウンド トラフィックは、同じアウトバウンド IPv4-ACL に対して評価されます。したがって、IPv4-ACL の条件は、スイッチからの発信トラフィックに対して順方向に、スイッチへの着信トラフィックに対して逆方向に適用されます。
- クリプト マップ エントリに割り当てられた各 IPv4-ACL フィルタは、1 つのセキュリティ ポリシー エントリと同等です。
- スイッチ A の S0 インターフェイスから発信されたデータがスイッチ インターフェイス S1 にルーティングされるときに、スイッチ インターフェイス S0（IPv4 アドレス 10.0.0.1）とスイッチ インターフェイス S1（IPv4 アドレス 20.0.0.2）間のトラフィックに IPsec 保護（図 7-4 を参照）が適用されます。10.0.0.1 から 20.0.0.2 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。
  - 送信元 = IPv4 アドレス 10.0.0.1
  - 宛先 = IPv4 アドレス 20.0.0.2

20.0.0.2 から 10.0.0.1 へのトラフィックの場合、スイッチ A の IPv4-ACL エントリは次のように評価されます。

- 送信元 = IPv4 アドレス 20.0.0.2
- 宛先 = IPv4 アドレス 10.0.0.1

*図 7-4　クリプト IPv4-ACL の IPSec 処理*




- IPSec に使用する指定のクリプト IPv4-ACL に複数のステートメントを設定した場合には、一致した最初の permit ステートメントにより、IPSec SA の有効範囲が判別されます。その後、トラフィックがクリプト IPv4-ACL の別の permit ステートメントと一致した場合には、新しい、別の IPSec SA がネゴシエートされ、新たに一致した IPv4-ACL ステートメントと一致するトラフィックが保護されます。
- クリプト マップ エントリに IPSec がフラグ設定されている場合、クリプト IPv4-ACL 内の permit エントリと一致する保護されていないインバウンド トラフィックは、IPSec によって保護されていると見なされ、廃棄されます。
- すべての IP-ACL を表示するには、**show ip access-list** コマンドを使用できます。トラフィックをフィルタリングするために使用される IP-ACL は、暗号化にも使用されます。
- IPSec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号（デフォルトは 3260）を指定します。この設定により、ギガビット イーサネット インターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。
- IPv4-ACL エントリの次の例では、MDS スイッチの IPv4 アドレスが 10.10.10.50 で、暗号化 iSCSI セッションが実行中のリモート Microsoft ホストが 10.10.10.16 であることを示しています。

```
switch(config)# ip access-list aclmsiscsi2 permit tcp 10.10.10.50 0.0.0.0 range port
3260 3260 10.10.10.16 0.0.0.0
```

## ミラーイメージ クリプト IPv4-ACL

ローカル ピアで定義されたクリプト マップ エントリがある場合は、このエントリで指定されたすべてのクリプト IPv4-ACL に対して、リモート ピアでミラー イメージ クリプト IPv4-ACL を定義します。この設定により、ローカルで適用された IPSec トラフィックをリモート ピアで正しく処理できるようになります。

ヒント　また、クリプト マップ エントリ自体が共通のトランスフォームをサポートし、ピアとして他のシステムを参照する必要があります。

図 7-5 に、ミラー イメージ IPv4-ACL を使用した場合と、使用しない場合のサンプル シナリオを示します。

*図 7-5　ミラー イメージ設定の IPSec 処理*

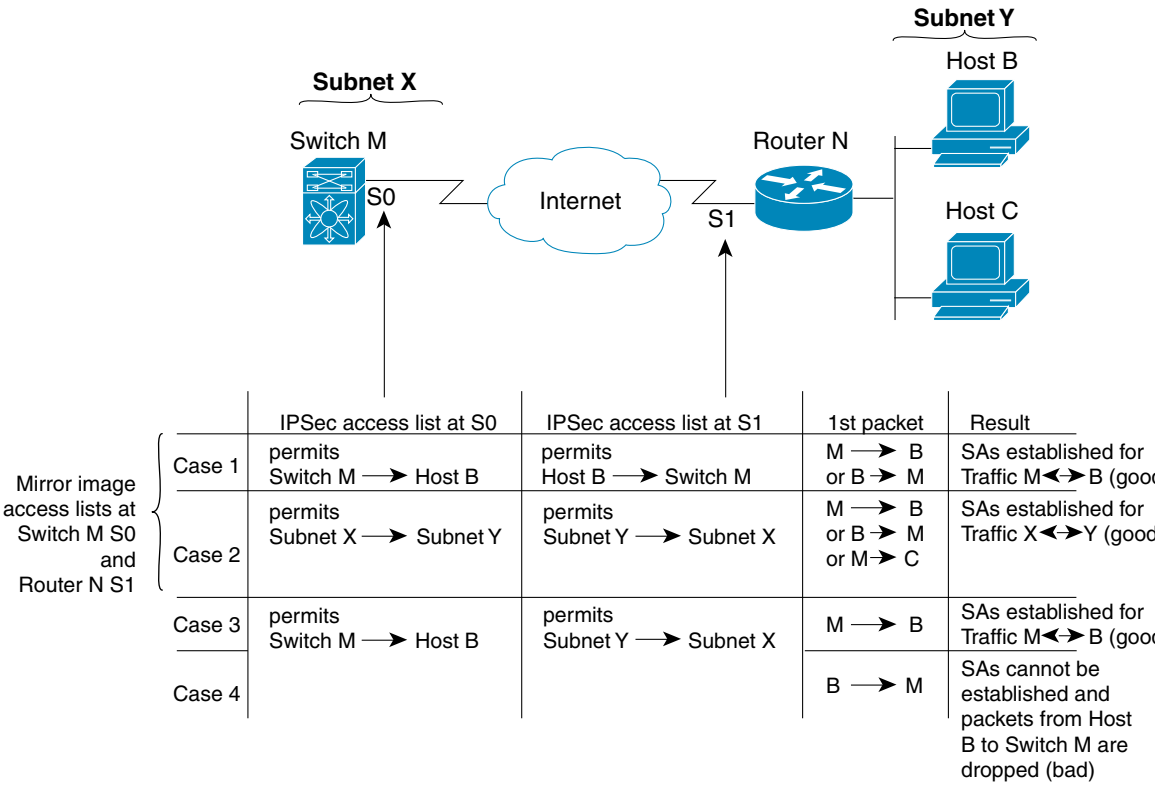



図 7-5 に示すように、2 つのピアのクリプト IPv4-ACL が相互のミラー イメージである場合、想定どおりに IPSec SA を確立できます。ただし、IPv4-ACL が相互のミラー イメージでない場合にも、IPSec SA を確立できることがあります。たとえば、図 7-5 のケース 3 および 4 のように、一方のピアの IPv4-ACL エントリが他方のピアの IPv4-ACL エントリのサブセットになっている場合です。IPSec SA の確立は、IPSec にとって非常に重要です。SA が存在しないと IPSec は機能せず、クリプト IPv4-ACL の条件と一致するパケットは、IPSec セキュリティで保護されて転送される代わりに、すべて廃棄されます。

ケース 4 では、SA を確立できません。開始元パケットが終了すると、クリプト IPv4-ACL に従って必ず SA が要求されるためです。ケース 4 では、ルータ N はサブネット X とサブネット Y 間のすべてのトラフィックを保護するように要求します。ただし、このトラフィックはスイッチ M のクリプト IPv4-ACL で許可される特定のフローのスーパーセットであるため、要求は許可されません。スイッチ M の要求はルータ N のクリプト IPv4-ACL で許可される特定のフローのサブセットであるため、ケース 3 は機能します。

ピア IPSec デバイスにクリプト IPv4-ACL をミラー イメージとして設定しないと、設定が複雑化するので、ミラー イメージ クリプト IPv4-ACL を使用することを強く推奨します。

## クリプト IPv4-ACL の any キーワード

ヒント　IPSec で使用するミラー イメージ クリプト IPv4-ACL は、**any** オプションを使用しないで設定することを推奨します。

IPSec インターフェイスを経由してマルチキャスト トラフィックを転送すると、permit ステートメントの **any** キーワードは廃棄されます。これは、マルチキャスト トラフィックの転送が失敗する原因になります。

**permit any** ステートメントを使用すると、すべてのアウトバウンド トラフィックが保護され（保護されたすべてのトラフィックが、対応するクリプト マップ エントリで指定されたピアに送信され）、すべてのインバウンド トラフィックの保護が必要になります。ルーティング プロトコル、NTP、エコー、エコー応答用のパケットを含む、IPSec で保護されないすべてのインバウンド パケットは、自動的に廃棄されます。

保護するパケットを確実に定義する必要があります。permit ステートメント内で **any** オプションを使用する必要がある場合は、保護しないすべてのトラフィックを除外する一連の deny ステートメントを、permit ステートメントの前に付加する必要があります（付加しない場合、これらのトラフィックが permit ステートメントの対象になります）。

# クリプト IPv4-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# ip access-list List1 permit ip 10.1.1.100 0.0.0.255 11.1.1.100 0.0.0.255` | 指定のネットワークから、または指定のネットワークへの、すべての IP トラフィックを許可します。 |

（注）　**show ip access-list** コマンドでは暗号マップ エントリは表示されません。関連エントリを表示するには、**show crypto map** コマンドを使用します。

必要に応じて、permit および deny ステートメントを追加します（第 5 章「IPv4 および IPv6 のアクセス コントロール リストの設定」を参照）。各 permit および deny は、保護する必要がある IP パケットを指示するための条件を指定します。

# IPSec のトランスフォーム セットの概要

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPSec SA のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

複数のトランスフォーム セットを指定し、これらのトランスフォーム セットの 1 つまたは複数をクリプト マップ エントリに指定できます。クリプト マップ エントリで定義されたトランスフォーム セットは、このクリプト マップ エントリのアクセス リストで指定されたデータ フローを保護するために、IPSec SA ネゴシエーションで使用されます。

IKE との IPSec セキュリティ アソシエーションのネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。同一のトランスフォーム セットが検出された場合には、そのトランスフォーム セットが選択され、両方のピアの IPSec SA の一部として、保護するトラフィックに適用されます。

**ヒント**　トランスフォーム セット定義を変更した場合には、トランスフォーム セットを参照するクリプト マップ エントリだけに変更が適用されます。変更は既存の SA には適用されませんが、新規 SA を確立するために以降のネゴシエーションで使用されます。新規設定を即座に有効にする場合には、SA データベースのすべてまたは一部を消去します。

**（注）**　IPSec をイネーブルにすると、Cisco NX-OS ソフトウェアにより、AES-128 暗号化および SHA-1 認証アルゴリズムを使用したデフォルトのトランスフォーム セット（ipsec_default_transform_set）が自動的に作成されます。

表 7-3 に、IPSec で使用できるトランスフォームの組み合わせを示します。

***表 7-3　IPSec トランスフォーム設定パラメータ***

| パラメータ | 許容値 | キーワード |
|---|---|---|
| 暗号化アルゴリズム | 56 ビット DES-CBC | **esp-des** |
| | 168 ビット DES | **esp-3des** |
| | 128 ビット AES-CBC | **esp-aes 128** |
| | 128 ビット AES-CTR[1] | **esp-aes 128 ctr** |
| | 256 ビット AES-CBC | **esp-aes 256** |
| | 256 ビット AES-CTR[1] | **esp-aes 256 ctr** |
| ハッシュ/認証アルゴリズム[1]（任意） | SHA-1（HMAC バリアント） | **esp-sha1-hmac** |
| | SHA-2（HMAC バリアント） | **esp-sha256-hmac** |
| | MD5（HMAC バリアント） | **esp-sha512-hmac** |
| | AES-XCBC-MAC | **esp-md5-hmac** |
| | | **esp-aes-xcbc-mac**[2] |

1. AES カウンタ（CTR）モードを設定する場合には、認証アルゴリズムも設定する必要があります。
2. Cisco MDS NX-OS リリース 5.2(2) 以降、**esp-aes-xcbc-mac** 認証アルゴリズム はサポートされていません。

次の表に、Microsoft Windows および Linux プラットフォームでサポートおよび検証されている、IPSec および IKE 暗号化認証アルゴリズムの設定を示します。

| プラットフォーム | IKE | IPSec |
|---|---|---|
| Microsoft iSCSI 発信側（Microsoft Windows 2000 プラットフォームの Microsoft IPSec 実装） | 3DES、SHA-1、SHA-2、または MD5、DH グループ 2 | 3DES、SHA-1、SHA-2 |
| Cisco iSCSI イニシエータ、Linux プラットフォームへの Free Swan IPsec の実装 | 3DES、MD5、DH グループ 1 | 3DES、MD5 |

# トランスフォーム セットの設定

トランスフォーム セットを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto transform-set domain ipsec test esp-3des esp-md5-hmac` | 3DES 暗号化アルゴリズムと MD5 認証アルゴリズムを指定する、test というトランスフォーム セットを設定します。表 7-3 を参照して、トランスフォームの組み合わせが使用可能かどうかを確認してください。 |
| | `switch(config)# crypto transform-set domain ipsec test esp-3des` | 3DES 暗号化アルゴリズムを指定する、test というトランスフォーム セットを設定します。この例では、デフォルトの認証は実行されません。 |

# クリプト マップ エントリの概要

クリプト IPv4-ACL とトランスフォーム セットの作成が完了すると、次のように、IPSec SA のさまざまな部分を組み合わせたクリプト マップ エントリを作成できます。

- IPSec で保護するトラフィック（クリプト IPv4-ACL 単位）。クリプト マップ セットには、それぞれ異なる IPv4-ACL を使用する複数のエントリを設定できます。
- SA セットで保護するフローの詳細度。
- IPSec で保護されるトラフィックの宛先（リモート IPSec ピアの名前）。
- IPSec トラフィックが使用するローカル アドレス（インターフェイスに適用）。
- 現在のトラフィックに適用する IPSec セキュリティ（1 つまたは複数のトランスフォーム セットから選択）。
- IPSec SA を定義するその他のパラメータ。

同じクリプト マップ名（マップ シーケンス番号が異なる）を持つクリプト マップ エントリは、クリプト マップ セットにグループ化されます。

クリプト マップ セットをインターフェイスに適用すると、次のイベントが発生します。

- そのインターフェイス用の Security Policy Database（SPD）が作成されます。
- インターフェイスを経由するすべての IP トラフィックが、SPD に対して評価されます。

クリプト マップ エントリにより保護を必要とするアウトバウンド IP トラフィックが確認されると、クリプト マップ エントリ内のパラメータに従って、SA とリモート ピアのネゴシエーションが行われます。

SA のネゴシエーションでは、クリプト マップ エントリから取得したポリシーが使用されます。ローカル スイッチがネゴシエーションを開始した場合、ローカル スイッチはクリプト マップ エントリに指定されたポリシーを使用して、指定された IPSec ピアに送信するオファーを作成します。IPSec ピアがネゴシエーションを開始した場合、ローカル スイッチはクリプト マップ エントリのポリシーを調べて、ピアの要求（オファー）を受け入れるか、または拒否するかを判断します。

2 つの IPSec ピア間で IPSec を成立させるには、両方のピアのクリプト マップ エントリに互換性のあるコンフィギュレーション ステートメントが含まれている必要があります。

## ピア間の SA の確立

2 つのピアが SA を確立する場合、各ピアのクリプト マップ エントリの 1 つまたは複数と、相手ピアのクリプト マップ エントリの 1 つに互換性がなければなりません。

2 つのクリプト マップ エントリで互換性が成立するには、少なくとも次の基準を満たす必要があります。

- クリプト マップ エントリに、互換性のあるクリプト IPv4-ACL（ミラー イメージ IPv4-ACL など）が含まれていること。応答側のピア エントリがローカルで暗号化されている場合、IPv4-ACL がこのピアのクリプト IPv4-ACL で許可されている必要があります。
- クリプト マップ エントリが互いに相手ピアを識別しているか、または自動ピアが設定されていること。
- 特定のインターフェイスに複数のクリプト マップ エントリを作成するときは、各マップ エントリの seq-num を使用して、マップ エントリにランクを設定します。seq-num の値が小さいほど、プライオリティは高くなります。クリプト マップ セットがあるインターフェイスでは、トラフィックは、最初にプライオリティの高いマップ エントリに対して評価されます。
- IKE ネゴシエーションを実行して SA を確立するには、クリプト マップ エントリに最低 1 つの共通トランスフォーム セットが含まれている必要があります。IPSec SA のネゴシエーション中に、両ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することに合意します。

パケットが特定の IPv4-ACL 内の permit エントリと一致すると、対応するクリプト マップ エントリにタグが付けられ、接続が確立されます。

## クリプト マップ設定の注意事項

クリプト マップ エントリを設定する場合には、次の注意事項に従ってください。

- ポリシーが適用される順序は、各クリプト マップのシーケンス番号によって決まります。シーケンス番号が小さいほど、プライオリティは高くなります。
- 各クリプト マップ エントリに使用できる IPv4-ACL は 1 つだけです（IPv4-ACL 自体には複数の permit エントリまたは deny エントリを設定できます）。
- トンネル エンドポイントが宛先アドレスと同じである場合は、auto-peer オプションを使用して、ピアをダイナミックに設定できます。
- IPSec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル iSCSI TCP ポート番号（デフォルトは 3260）を指定します。この設定により、ギガビット イーサネット インターフェイスのシャットダウン、VRRP スイッチオーバー、ポート障害などにより処理が中断されても、暗号化 iSCSI セッションを迅速に回復できます。

# クリプト マップ エントリの作成

（注）　暗号マップ エントリで指定されたピアの IP アドレスがリモートの Cisco MDS スイッチの VRRP IP アドレスである場合、IP アドレスが **secondary** オプションを使用して作成されることを確認します（詳細については、『*Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*』を参照してください）。

必須の暗号マップ エントリを作成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto map  domain ipsec SampleMap 31` | シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。 |
| ステップ 3 | `switch(config-crypto-map-ip)# match address SampleAcl` | このクリプト マップ エントリのコンテキストで、IPsec によって保護するトラフィックと保護しないトラフィックを決定する ACL を指定します。 |
| ステップ 4 | `switch(config-crypto-map-ip)# set peer 10.1.1.1` | 特定のピアの IPv4 アドレスを設定します。<br>(注)　IKE は、IPv4 アドレスのみをサポートし、IPv6 アドレスはサポートしません。 |
| ステップ 5 | `switch(config-crypto-map-ip)# set transform-set SampleTransform1 SampleTransmfor2` | 指定した暗号マップ エントリに対し許可するトランスフォーム セットを指定します。複数のトランスフォーム セットをプライオリティ順（最高のプライオリティのものが最初）に列挙します。 |

# SA ライフタイム ネゴシエーションの概要

SA 固有のライフタイム値を設定することにより、グローバル ライフタイム値（サイズおよびタイム）を書き換えることができます。

SA ライフタイム ネゴシエーション値を指定する場合、指定したクリプト マップにライフタイム値を設定することもできます。この場合、設定されたライフタイム値によってグローバルな設定値が上書きされます。クリプト マップ固有のライフタイムを指定しない場合には、グローバル値（またはグローバルなデフォルト値）が使用されます。

グローバル ライフタイム値の詳細については、「グローバル ライフタイム値」セクション（7-212 ページ）を参照してください。

# SA ライフタイムの設定

指定したクリプト マップ エントリの SA ライフタイムを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto map domain ipsec SampleMap 31` | シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定サブモードを開始します。 |
| ステップ 3 | `switch(config-crypto-map-ip)# set security-association lifetime seconds 8640` | 暗号マップのエントリに対するグローバルなライフタイムとは異なる IPsec SA ライフタイムを使用して、この暗号マップのエントリに対する SA ライフタイムを指定します。 |
| ステップ 4 | `switch(config-crypto-map-ip)# set security-association lifetime gigabytes 4000` | 指定したトラフィック量（GB 単位）が SA を使用して FCIP リンクを通過した後、この SA のトラフィック量ライフタイムがタイムアウトするように設定します。ライフタイムの範囲は 1 ～ 4095 GB です。 |

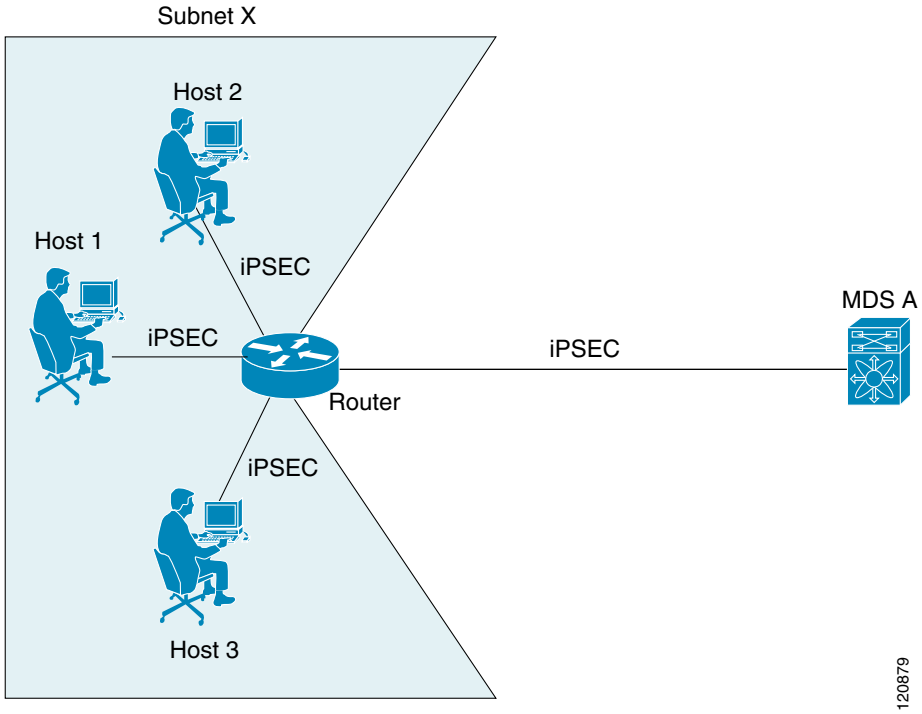
# AutoPeer オプションの概要

クリプト マップ内でピア アドレスを **auto-peer** として設定した場合は、トラフィックの宛先エンドポイントが SA のピア アドレスとして使用されます。同じクリプト マップを使用して、クリプト マップの IPv4-ACL エントリで指定されたサブネット内の各エンドポイントに、固有の SA を設定できます。auto-peer を使用すると、トラフィック エンドポイントが IPSec に対応している場合に、設定が簡素化されます。auto-peer は、同じサブネット内の複数の iSCSI ホストで個別の設定が必要ない場合、特に役立ちます。

図 7-6 に、auto-peer オプションによって設定が簡素化される例を示します。auto-peer オプションを使用すると、サブネット X からの全ホストについて、1 つのクリプト マップ エントリだけを使用してスイッチとの SA を確立できます。各ホストは独自の SA を確立しますが、クリプト マップ エントリは共有されます。auto-peer オプションを使用しない場合、各ホストに 1 つのクリプト マップ エントリが必要になります。

詳細については、「iSCSI の設定例」セクション（7-223 ページ）を参照してください。

*図 7-6　auto-peer オプションを使用した iSCSI のエンドツーエンド IPSec*



# AutoPeer オプションの設定

auto-peer オプションを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto map domain ipsec SampleMap 31` | シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。 |
| ステップ 3 | `switch(config-crypto-map-ip)# set peer auto-peer` | ソフトウェアに（SA セットアップの間に）宛先ピアの IP アドレスを動的に選択するように指示します。 |

# PFS の概要

SA ライフタイム ネゴシエーション値を指定する場合、オプションでクリプト マップの完全転送秘密（PFS）値を設定できます。

PFS 機能は、デフォルトではディセーブルです。PFS グループを設定する場合は、DH グループ 1、2、5、または 14 のうちの 1 つを設定できます。DH グループを指定しない場合、グループ 1 がデフォルトで使用されます。

# PFS の設定

PFS 値を設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto map domain ipsec SampleMap 31` | シーケンス番号が 31 の SampleMap というエントリに対し、暗号マップ設定モードを開始します。 |
| ステップ 3 | `switch(config-crypto-map-ip)# set pfs group 2` | IPsec がこの暗号マップ エントリの新しい SA を要求した場合、PFS を要求するように、または IPsec ピアから受信する要求に PFS が含まれることを要求するように指定します。 |

# クリプト マップ セット インターフェイスの適用の概要

IPSec トラフィック フローが通過する各インターフェイスにクリプト マップ セットを適用する必要があります。インターフェイスにクリプト マップ セットを適用すると、スイッチはそのインターフェイスのすべてのトラフィックを指定されたクリプト マップ セットに対して評価し、指定されたポリシーを接続中または SA ネゴシエーション中に使用して、トラフィックが暗号によって保護されるようにします。

1 つのインターフェイスに適用できるクリプト マップ セットは 1 つだけです。複数のインターフェイスに同じクリプト マップを適用できます。ただし、各インターフェイスに複数のクリプト マップ セットを適用できません。

## クリプト マップ セットの適用

クリプト マップ セットをインターフェイスに適用する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# interface gigabitethernet 4/1` | IPsec 暗号マップが適用される、必要なギガビット イーサネット インターフェイス（および必要な場合はサブインターフェイス）を選択します。 |
| ステップ 3 | `switch(config-if)# crypto map domain ipsec cm10` | 暗号マップ セットを選択したインターフェイスに適用します。 |

# IPsec のメンテナンス

設定の変更は、後続の SA のネゴシエーション時まで適用されません。新しい設定をすぐに適用するには、変更した設定を使用して SA が再確立されるように、既存の SA をクリアする必要があります。スイッチが IPSec トラフィックをアクティブに処理している場合には、SA データベースのうち、設定変更が影響する部分だけを消去してください（つまり、指定のクリプト マップ セットによって確立された SA だけを消去します）。SA データベース全体を消去するのは、大規模な変更を行った場合、またはルータが他の IPSec トラフィックをほとんど処理していない場合だけにしてください。

ヒント　**show crypto sa domain interface gigabitethernet** *slot/port* コマンドの出力から SA インデックスを得ることができます。

SA データベースの一部を消去するには、次のコマンドを使用します。

```
switch# clear crypto sa domain ipsec interface gigabitethernet 2/1 inbound sa-index 1
```

# グローバル ライフタイム値

クリプト マップ エントリにライフタイムが設定されていない場合、新しい IPSec SA のネゴシエーション時にグローバル ライフタイム値が使用されます。

タイムまたはトラフィック ボリュームの 2 つのライフタイムを設定できます。どちらか一方のライフタイムに到達すると、SA は期限切れになります。デフォルトのライフタイムは 3,600 秒（1 時間）および 450 GB です。

グローバル ライフタイムを変更した場合、新しいライフタイム値は既存の SA には適用されず、以降に確立される SA のネゴシエーションに使用されます。新しいライフタイム値をすぐに使用する場合は、SA データベースのすべてまたは一部を消去します。

特定のクリプト マップ エントリにライフタイム値が設定されていない場合、スイッチは新規 SA を要求するときに、ピアへの要求内でグローバル ライフタイム値を指定します。この値は、新規 SA のライフタイム値として使用されます。ピアからのネゴシエーション要求を受信すると、スイッチは使用中の IKE バージョンによって決まる値を使用します。

- IKEv1 を使用して IPSec SA を設定する場合、SA ライフタイム値は、2 つの候補のうち小さい方の値になります。トンネルの両端で、同じ値がプログラムされます。
- IKEv2 を使用して IPSec SA を設定する場合、各端の SA に独自のライフタイム値が設定されるので、両端の SA は個別に期限切れになります。

SA（および対応するキー）は、指定時間（秒単位）または指定トラフィック量（バイト単位）のどちらか一方が先に経過した時点で、期限切れになります。

既存の SA のライフタイムしきい値に到達する前に、新しい SA がネゴシエートされます。これは、既存の SA が期限切れになる前にネゴシエーションを完了するためです。

新しい SA は、次のいずれかのしきい値に先に到達した時点でネゴシエートされます。

- ライフタイムが期限切れになる 30 秒前
- ライフタイムの残りのバイト数が約 10 % になったとき

ライフタイムが期限切れになった時点でトラフィックが送受信されていない場合、新しい SA はネゴシエートされません。新しい SA がネゴシエートされるのは、IPSec が別の保護対象パケットを確認した場合だけです。

グローバル SA ライフタイムを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# crypto global domain ipsec security-association lifetime seconds 86400` | 指定した秒数が経過した後、IPsec SA のグローバル ライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 120 ～ 86400 秒です。 |
| ステップ 3 | `switch(config)# crypto global domain ipsec security-association lifetime gigabytes 4000` | 指定したトラフィック量（GB 単位）が SA を使用して FCIP リンクを通過した後、IPsec SA のグローバル トラフィック量ライフタイムがタイムアウトするように設定します。グローバル ライフタイムの範囲は 1～4095 GB です。 |
| | `switch(config)# crypto global domain ipsec security-association lifetime kilobytes 2560` | グローバル トラフィック量のライフタイムを設定します（KB 単位）。グローバル ライフタイムの範囲は 2560 ～ 2147483647 KB です。 |
| | `switch(config)# crypto global domain ipsec security-association lifetime megabytes 5000` | グローバル トラフィック量のライフタイムを設定します（MB 単位）。グローバル ライフタイムの範囲は 3 ～ 4193280 MB です。 |

# IKE 設定の表示

**show** コマンドのセットを使用して、IKE 情報を確認できます。例 7-1 ～ 7-5 を参照してください。

*例 7-1　各 IKE ポリシー用に設定されたパラメータの表示*

```
switch# show crypto ike domain ipsec
keepalive 60000
```

*例 7-2　イニシエータ設定の表示*

```
switch# show crypto ike domain ipsec initiator
initiator version 1 address 1.1.1.1
initiator version 1 address 1.1.1.2
```

*例 7-3　キーの設定の表示*

```
switch# show crypto ike domain ipsec key
key abcdefgh address 1.1.1.1
key bcdefghi address 1.1.2.1
```

*例 7-4　IKE 用の現在確立されたポリシーの表示*

```
switch# show crypto ike domain ipsec policy 1
Priority 1, auth pre-shared, lifetime 6000 secs, encryption 3des, hash md5, DH group 5
Priority 3, auth pre-shared, lifetime 86300 secs, encryption aes, hash sha1, DH group 1
Priority 5, auth pre-shared-key, lifetime 86400 secs, encryption 3des, hash sha256, DH
group 1
```

*例 7-5　IKE 用の現在確立された SA の表示*

```
switch# show crypto ike domain ipsec sa
Tunn    Local Addr          Remote Addr         Encr     Hash    Auth Method     Lifetime
------------------------------------------------------------------------------------------
1*      172.22.31.165[500]  172.22.31.166[500] 3des     sha1    preshared key   86400
2       172.22.91.174[500]  172.22.91.173[500] 3des     sha1    preshared key   86400
------------------------------------------------------------------------------------------
NOTE: tunnel id ended with * indicates an IKEv1 tunnel
```

# IPsec 設定の表示

**show** コマンドのセットを使用して、IPsec 情報を確認できます。例 7-6 ～ 7-19 を参照してください。

*例 7-6　指定された ACL の情報の表示*

```
switch# show ip access-list acl10
ip access-list acl10 permit ip 10.10.10.0 0.0.0.255 10.10.10.0 0.0.0.255 (0 matches)
```

例 7-6 では、表示出力一致に、この条件を満たすインターフェイス（暗号マップではない）だけが表示されます。

*例 7-7　トランスフォーム セットの設定の表示*

```
switch# show crypto transform-set domain ipsec
Transform set: 1/1 {esp-3des esp-sha256-hmac}
    will negotiate {tunnel}
Transform set: ipsec_default_transform_set {esp-aes 128 esp-sha1-hmac}
    will negotiate {tunnel}
```

*例 7-8　設定されたすべての暗号マップの表示*

```
switch# show crypto map domain ipsec
Crypto Map "cm10" 1 ipsec
        Peer = Auto Peer
        IP ACL = acl10
            permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
        Transform-sets: 3des-md5, des-md5,
        Security Association Lifetime: 4500 megabytes/3600 seconds
        PFS (Y/N): N
        Interface using crypto map set cm10:
            GigabitEthernet4/1
Crypto Map "cm100" 1 ipsec
        Peer = Auto Peer
        IP ACL = acl100
            permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
        Transform-sets: 3des-md5, des-md5,
        Security Association Lifetime: 4500 megabytes/3600 seconds
        PFS (Y/N): N
        Interface using crypto map set cm100:
            GigabitEthernet4/2
```

*例 7-9　特定のインターフェイス用の暗号マップ情報の表示*

```
switch# show crypto map domain ipsec interface gigabitethernet 4/1
Crypto Map "cm10" 1 ipsec
        Peer = Auto Peer
        IP ACL = acl10
            permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
        Transform-sets: 3des-md5, des-md5,
        Security Association Lifetime: 4500 megabytes/3600 seconds
        PFS (Y/N): N
        Interface using crypto map set cm10:
            GigabitEthernet4/1
```

*例 7-10　指定した暗号マップ情報の表示*

```
switch# show crypto map domain ipsec tag cm100
Crypto Map "cm100" 1 ipsec
        Peer = Auto Peer
        IP ACL = acl100
            permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
        Transform-sets: 3des-md5, des-md5,
        Security Association Lifetime: 4500 megabytes/3600 seconds
        PFS (Y/N): N
        Interface using crypto map set cm100:
            GigabitEthernet4/2
```

*例 7-11　指定したインターフェイス用の SA アソシエーションの表示*

```
switch# show crypto sad domain ipsec interface gigabitethernet 4/1
interface: GigabitEthernet4/1
    Crypto map tag: cm10, local addr. 10.10.10.1
    protected network:
    local ident (addr/mask): (10.10.10.0/255.255.255.0)
    remote  ident (addr/mask): (10.10.10.4/255.255.255.255)
    current_peer: 10.10.10.4
      local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
```

```
     current outbound spi: 0x30e000f (51249167), index: 0
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 423624704
     current inbound spi: 0x30e0000 (51249152), index: 0
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 423624704
```

*例 7-12　すべての SA アソシエーションの表示*

```
switch# show crypto sad domain ipsec
interface: GigabitEthernet4/1
    Crypto map tag: cm10, local addr. 10.10.10.1
    protected network:
    local  ident (addr/mask): (10.10.10.0/255.255.255.0)
    remote  ident (addr/mask): (10.10.10.4/255.255.255.255)
    current_peer: 10.10.10.4
      local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
     current outbound spi: 0x30e000f (51249167), index: 0
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 423624704
     current inbound spi: 0x30e0000 (51249152), index: 0
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 423624704
```

*例 7-13　ポリシー データベースに関する情報の表示*

```
switch# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet4/1, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
#  63:      deny  ip any any
Policy Database for interface: GigabitEthernet4/2, direction: Both
#   0:      deny  udp any port eq 500 any <----------------------UDP default entry
#   1:      deny  udp any any port eq 500 <---------------------- UDP default entry
#   3:      permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
#  63:      deny  ip any any <---------------------------------------- Clear text default entry
```

*例 7-14　特定のインターフェイス用の SPD 情報の表示*

```
switch# show crypto spd domain ipsec interface gigabitethernet 4/2
Policy Database for interface: GigabitEthernet3/1, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
# 127:      deny  ip any any
```

*例 7-15　特定のインターフェイスの詳細な iSCSI セッション情報の表示*

```
switch# show iscsi session detail
Initiator iqn.1987-05.com.cisco:01.9f39f09c7468 (ips-host16.cisco.com)
    Initiator ip addr (s): 10.10.10.5
  Session #1 (index 24)
    Discovery session, ISID 00023d000001, Status active
```

```
  Session #2 (index 25)
    Target ibm1
    VSAN 1, ISID 00023d000001, TSIH 0, Status active, no reservation
    Type Normal, ExpCmdSN 42, MaxCmdSN 57, Barrier 0
    MaxBurstSize 0, MaxConn 1, DataPDUInOrder Yes
    DataSeqInOrder Yes, InitialR2T Yes, ImmediateData No
    Registered LUN 0, Mapped LUN 0
    Stats:
      PDU: Command: 41, Response: 41
      Bytes: TX: 21388, RX: 0
    Number of connection: 1
    Connection #1
      iSCSI session is protected by IPSec <----------The iSCSI session protection status
      Local IP address: 10.10.10.4, Peer IP address: 10.10.10.5
      CID 0, State: Full-Feature
      StatSN 43, ExpStatSN 0
      MaxRecvDSLength 131072, our_MaxRecvDSLength 262144
      CSG 3, NSG 3, min_pdu_size 48 (w/ data 48)
      AuthMethod none, HeaderDigest None (len 0), DataDigest None (len 0)
      Version Min: 0, Max: 0
      FC target: Up, Reorder PDU: No, Marker send: No (int 0)
      Received MaxRecvDSLen key: Yes
```

*例 7-16　特定のインターフェイス用の FCIP 情報の表示*

```
switch# show interface fcip 1
fcip1 is trunking
    Hardware is GigabitEthernet
    Port WWN is 20:50:00:0d:ec:08:6c:c0
    Peer port WWN is 20:10:00:05:30:00:a7:9e
    Admin port mode is auto, trunk mode is on
    Port mode is TE
    Port vsan is 1
    Speed is 1 Gbps
    Trunk vsans (admin allowed and active) (1)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    Using Profile id 1  (interface GigabitEthernet2/1)
    Peer Information
      Peer Internet address is 10.10.11.1 and port is 3225
    FCIP tunnel is protected by IPSec <----------The FCIP tunnel protection status
    Write acceleration mode is off
    Tape acceleration mode is off
    Tape Accelerator flow control buffer size is 256 KBytes
    IP Compression is disabled
    Special Frame is disabled
    Maximum number of TCP connections is 2
    Time Stamp is disabled
    QOS control code point is 0
    QOS data code point is 0
    B-port mode disabled
    TCP Connection Information
      2 Active TCP connections
        Control connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65520
        Data connection: Local 10.10.11.2:3225, Remote 10.10.11.1:65522
      2 Attempts for active connections, 0 close of connections
    TCP Parameters
      Path MTU 1400 bytes
      Current retransmission timeout is 200 ms
      Round trip time: Smoothed 2 ms, Variance: 1
      Advertized window: Current: 124 KB, Maximum: 124 KB, Scale: 6
```

```
    Peer receive window: Current: 123 KB, Maximum: 123 KB, Scale: 6
    Congestion window: Current: 53 KB, Slow start threshold: 48 KB
    Current Send Buffer Size: 124 KB, Requested Send Buffer Size: 0 KB
    CWM Burst Size: 50 KB
  5 minutes input rate 128138888 bits/sec, 16017361 bytes/sec, 7937 frames/sec
  5 minutes output rate 179275536 bits/sec, 22409442 bytes/sec, 46481 frames/sec
    10457037 frames input, 21095415496 bytes
       308 Class F frames input, 32920 bytes
       10456729 Class 2/3 frames input, 21095382576 bytes
       9907495 Reass frames
       0 Error frames timestamp error 0
    63792101 frames output, 30250403864 bytes
       472 Class F frames output, 46816 bytes
       63791629 Class 2/3 frames output, 30250357048 bytes
       0 Error frames
```

*例 7-17　スイッチのグローバル IPsec 統計情報の表示*

```
switch# show crypto global domain ipsec
IPSec global statistics:
        Number of crypto map sets: 3
        IKE transaction stats: 0 num, 256 max
        Inbound SA stats: 0 num
        Outbound SA stats: 0 num
```

*例 7-18　指定したインタフェースの IPsec 統計情報の表示*

```
switch# show crypto global domain ipsec interface gigabitethernet 3/1
IPSec interface statistics:
        IKE transaction stats: 0 num
        Inbound SA stats: 0 num, 512 max
        Outbound SA stats: 0 num, 512 max
```

*例 7-19　グローバル SA ライフタイム値の表示*

```
switch# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 450 gigabytes/3600 seconds
```

# FCIP の設定例

図 7-7 では 1 つの FCIP リンク（トンネル 2）の IPSec の実装に注目しています。トンネル 2 は MDS A と MDS C 間で暗号化データを伝送します。

*図 7-7　FCIP のシナリオの IP セキュリティの使用*

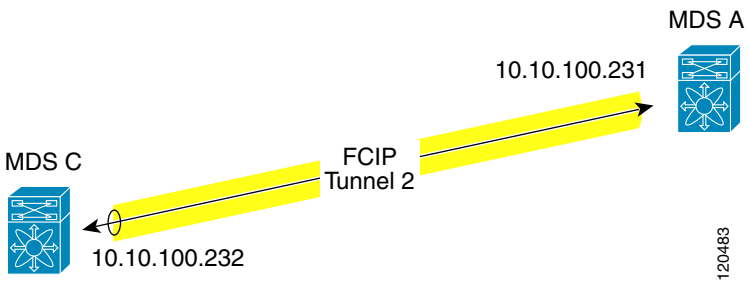


図 7-7 に示す FCIP シナリオで IPsec を設定するには、次の手順を実行します。

**ステップ 1**　スイッチ MDS A で IKE および IPsec をイネーブルにします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# feature crypto ike
sw10.1.1.100(config)# feature crypto ipsec
```

**ステップ 2**　スイッチ MDS A に IKE を設定します。

```
sw10.1.1.100(config)# crypto ike domain ipsec
sw10.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.232
sw10.1.1.100(config-ike-ipsec)# policy 1
sw10.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw10.1.1.100(config-ike-ipsec-policy)# hash md5
sw10.1.1.100(config-ike-ipsec-policy)# end
sw10.1.1.100#
```

**ステップ 3**　スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.100.231 0.0.0.0 10.10.100.232
0.0.0.0
```

**ステップ 4**　スイッチ MDS A にトランスフォーム セットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128 esp-sha1-hmac
```

**ステップ 5**　スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer 10.10.100.232
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw10.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw10.1.1.100(config-crypto-map-ip)# set pfs group5
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

**ステップ 6**　スイッチ MDS A の暗号マップ セットにインターフェイスをバインドします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# int gigabitethernet 7/1
sw10.1.1.100(config-if)# ip addr 10.10.100.231 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# exit
sw10.1.1.100(config)#
```

**ステップ 7**　スイッチ MDS A に FCIP を設定します。

```
sw10.1.1.100(config)# feature fcip
sw10.1.1.100(config)# fcip profile 2
sw10.1.1.100(config-profile)# ip address 10.10.100.231
sw10.1.1.100(config-profile)# int fcip 2
sw10.1.1.100(config-if)# peer-info ipaddr 10.10.100.232
sw10.1.1.100(config-if)# use-profile 2
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

**ステップ 8**　スイッチ MDS A の設定を確認します。

```
sw10.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw10.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
        Peer = 10.10.100.232
        IP ACL = acl1
            permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
        Transform-sets: tfs-02,
        Security Association Lifetime: 3000 gigabytes/3600 seconds
        PFS (Y/N): Y
         PFS Group: group5
Interface using crypto map set cmap-01:
    GigabitEthernet7/1

sw10.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-sha1-hmac}
    will negotiate {tunnel}

sw10.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet7/1, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip 10.10.100.231 255.255.255.255 10.10.100.232 255.255.255.255
#  63:      deny  ip any any

sw10.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw10.1.1.100# show crypto ike domain ipsec key
key ctct address 10.10.100.232

sw10.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH group 1
```

**ステップ 9**　スイッチ MDS C で IKE および IPsec をイネーブルにします。

```
sw11.1.1.100# conf t
sw11.1.1.100(config)# feature crypto ike
sw11.1.1.100(config)# feature crypto ipsec
```

**ステップ 10**　スイッチ MDS C に IKE を設定します。

```
sw11.1.1.100(config)# crypto ike domain ipsec
sw11.1.1.100(config-ike-ipsec)# key ctct address 10.10.100.231
sw11.1.1.100(config-ike-ipsec)# policy 1
sw11.1.1.100(config-ike-ipsec-policy)# encryption 3des
sw11.1.1.100(config-ike-ipsec-policy)# hash md5
sw11.1.1.100(config-ike-ipsec-policy)# exit
sw11.1.1.100(config-ike-ipsec)# end
sw11.1.1.100#
```

**ステップ 11**　スイッチ MDS C に ACL を設定します。

```
sw11.1.1.100# conf t
sw11.1.1.100(config)# ip access-list acl1 permit ip 10.10.100.232 0.0.0.0 10.10.100.231
0.0.0.0
```

**ステップ 12**　スイッチ MDS C にトランスフォーム セットを設定します。

```
sw11.1.1.100(config)# crypto transform-set domain ipsec tfs-02 esp-aes 128 esp-sha1-hmac
```

**ステップ 13**　スイッチ MDS C に暗号マップを設定します。

```
sw11.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw11.1.1.100(config-crypto-map-ip)# match address acl1
sw11.1.1.100(config-crypto-map-ip)# set peer 10.10.100.231
sw11.1.1.100(config-crypto-map-ip)# set transform-set tfs-02
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime seconds 3600
sw11.1.1.100(config-crypto-map-ip)# set security-association lifetime gigabytes 3000
sw11.1.1.100(config-crypto-map-ip)# set pfs group5
sw11.1.1.100(config-crypto-map-ip)# exit
sw11.1.1.100(config)#
```

**ステップ 14**　スイッチ MDS C のクリプト マップ セットにインターフェイスをバインドします。

```
sw11.1.1.100(config)# int gigabitethernet 1/2
sw11.1.1.100(config-if)# ip addr 10.10.100.232 255.255.255.0
sw11.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)#
```

**ステップ 15**　スイッチ MDS C の FCIP を設定します。

```
sw11.1.1.100(config)# feature fcip
sw11.1.1.100(config)# fcip profile 2
sw11.1.1.100(config-profile)# ip address 10.10.100.232
sw11.1.1.100(config-profile)# int fcip 2
sw11.1.1.100(config-if)# peer-info ipaddr 10.10.100.231
sw11.1.1.100(config-if)# use-profile 2
sw11.1.1.100(config-if)# no shut
sw11.1.1.100(config-if)# exit
sw11.1.1.100(config)# exit
```

**ステップ 16**　スイッチ MDS C の設定を確認します。

```
sw11.1.1.100# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds

sw11.1.1.100# show crypto map domain ipsec
Crypto Map "cmap-01" 1 ipsec
        Peer = 10.10.100.231
        IP ACL = acl1
            permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
        Transform-sets: tfs-02,
        Security Association Lifetime: 3000 gigabytes/3600 seconds
        PFS (Y/N): Y
         PFS Group: group5
Interface using crypto map set cmap-01:
    GigabitEthernet1/2

sw11.1.1.100# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet1/2, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip 10.10.100.232 255.255.255.255 10.10.100.231 255.255.255.255
#  63:      deny  ip any any

sw11.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet1/2
    Crypto map tag: cmap-01, local addr. 10.10.100.232
    protected network:
    local  ident (addr/mask): (10.10.100.232/255.255.255.255)
    remote  ident (addr/mask): (10.10.100.231/255.255.255.255)
    current_peer: 10.10.100.231
      local crypto endpt.: 10.10.100.232, remote crypto endpt.: 10.10.100.231
```

```
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
     current outbound spi: 0x38f96001 (955867137), index: 29
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 3221225472000
     current inbound spi: 0x900b011 (151040017), index: 16
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 3221225472000

sw11.1.1.100# show crypto transform-set domain ipsec
Transform set: tfs-02 {esp-aes 128 esp-sha1-hmac}
    will negotiate {tunnel}

sw11.1.1.100# show crypto ike domain ipsec
keepalive 3600

sw11.1.1.100# show crypto ike domain ipsec key

key ctct address 10.10.100.231

sw11.1.1.100# show crypto ike domain ipsec policy
Priority 1, auth pre-shared, lifetime 86300 secs, encryption 3des, hash md5, DH
group 1

sw11.1.1.100# show crypto ike domain ipsec sa
Tunn    Local Addr          Remote Addr         Encr    Hash    Auth Method     Lifetime
------------------------------------------------------------------------------------------
1*      10.10.100.232[500]  10.10.100.231[500]  3des    md5     preshared key   86300
------------------------------------------------------------------------------------------
NOTE: tunnel id ended with * indicates an IKEv1 tunnel
```

**ステップ 17**　スイッチ MDS A の設定を確認します。

```
sw10.1.1.100# show crypto sad domain ipsec
interface: GigabitEthernet7/1
    Crypto map tag: cmap-01, local addr. 10.10.100.231
    protected network:
    local  ident (addr/mask): (10.10.100.231/255.255.255.255)
    remote  ident (addr/mask): (10.10.100.232/255.255.255.255)
    current_peer: 10.10.100.232
      local crypto endpt.: 10.10.100.231, remote crypto endpt.: 10.10.100.232
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
     current outbound spi: 0x900b01e (151040030), index: 10
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 3221225472000
     current inbound spi: 0x38fe700e (956198926), index: 13
      lifetimes in seconds:: 3600
      lifetimes in bytes:: 3221225472000

sw10.1.1.100# show crypto ike domain ipsec sa
Tunn Local Addr          Remote Addr         Encr  Hash  Auth Method   Lifetime
-------------------------------------------------------------------------------
   1 10.10.100.231[500]  10.10.100.232[500]  3des  md5   preshared key    86300
```

これで、スイッチ MDS A および MDS C の両方に IPsec を設定しました。

# iSCSI の設定例

図 7-8 では、サブネット 12.12.1/24 のホストと MDS A の間の iSCSI セッションに注目しています。**auto-peer** オプションを使用して、サブネット 12.12.1.0/24 からのホストが、MDS スイッチのギガビット イーサネット ポート 7/1 へ接続しようとしたときに、ホストと MDS の間に SA が作成されます。auto-peer を使用して、1 つの暗号マップだけが、同じサブネット内のすべてのホストの SA を作成するために必要です。auto-peer がないと、ホストごとに 1 つの暗号マップが必要です。

*図 7-8　iSCSI のエンドツーエンド IPSec*

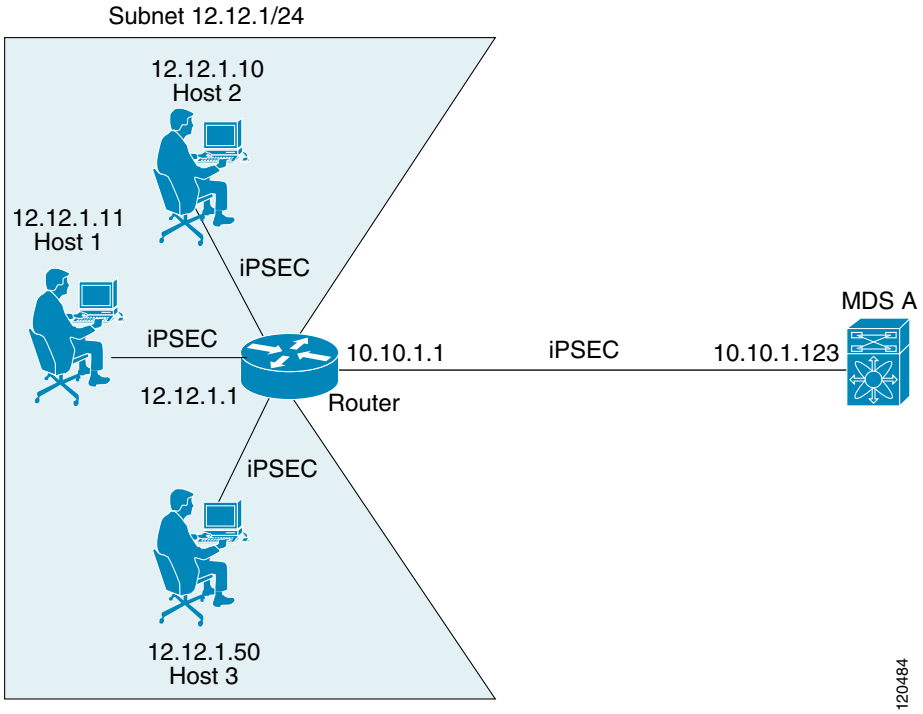



図 7-8 に示す iSCSI シナリオで IPsec を設定するには、次の手順を実行します。

**ステップ 1**　スイッチ MDS A に ACL を設定します。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# ip access-list acl1 permit tcp 10.10.1.0 0.0.0.255 range port 3260
3260 12.12.1.0 0.0.0.255
```

**ステップ 2**　スイッチ MDS A にトランスフォーム セットを設定します。

```
sw10.1.1.100(config)# crypto transform-set domain ipsec tfs-01 esp-3des esp-md5-hmac
```

**ステップ 3**　スイッチ MDS A に暗号マップを設定します。

```
sw10.1.1.100(config)# crypto map domain ipsec cmap-01 1
sw10.1.1.100(config-crypto-map-ip)# match address acl1
sw10.1.1.100(config-crypto-map-ip)# set peer auto-peer
sw10.1.1.100(config-crypto-map-ip)# set transform-set tfs-01
sw10.1.1.100(config-crypto-map-ip)# end
sw10.1.1.100#
```

**ステップ 4**　スイッチ MDS A の暗号マップ セットにインターフェイスをバインドします。

```
sw10.1.1.100# conf t
sw10.1.1.100(config)# int gigabitethernet 7/1
sw10.1.1.100(config-if)# ip address 10.10.1.123 255.255.255.0
sw10.1.1.100(config-if)# crypto map domain ipsec cmap-01
sw10.1.1.100(config-if)# no shut
sw10.1.1.100(config-if)# end
sw10.1.1.100#
```

Cisco MDS IPsec および iSCSI 機能を使用して、MDS A に IPsec を設定しました。

# デフォルト設定

表 7-4 に、IKE パラメータのデフォルト設定を示します。

*表 7-4　IKE パラメータのデフォルト値*

| パラメータ | デフォルト |
|---|---|
| IKE | ディセーブル |
| IKE バージョン | IKE version 2 |
| IKE 暗号化アルゴリズム | 3DES |
| IKE ハッシュ アルゴリズム | SHA |
| IKE 認証方式 | 事前共有キー |
| IKE DH グループ識別名 | グループ 1 |
| IKE ライフタイム アソシエーション | 86,400 秒（24 時間） |
| 各ピアの IKE キープアライブ タイム（v2） | 3,600 秒（1 時間） |

表 7-5 に、IPSec パラメータのデフォルト設定を示します。

*表 7-5　IPSec パラメータのデフォルト値*

| パラメータ | デフォルト |
|---|---|
| IPSec | ディセーブル |
| トラフィックへの IPSec の適用 | 拒否（deny）：クリア テキストを許可 |
| IPSec PFS | ディセーブル |
| IPSec グローバル ライフタイム（トラフィック量） | 450 GB |
| IPSec グローバル ライフタイム（タイム） | 3,600 秒（1 時間） |

CHAPTER 8

# FC-SP および DHCHAP の設定

この章は、次の項で構成されています。



## ファブリック認証の概要

Fibre Channel Security Protocol（FC-SP）機能は、スイッチ間およびホストとスイッチ間で認証を実行して、企業全体のファブリックに関するセキュリティ問題を解決します。Diffie-Hellman Challenge Handshake Authentication Protocol（DHCHAP）は、Cisco MDS 9000 ファミリ スイッチとその他のデバイス間で認証を行う FC-SP プロトコルです。DHCHAP は、CHAP プロトコルと Diffie-Hellman 交換を組み合わせて構成されています。

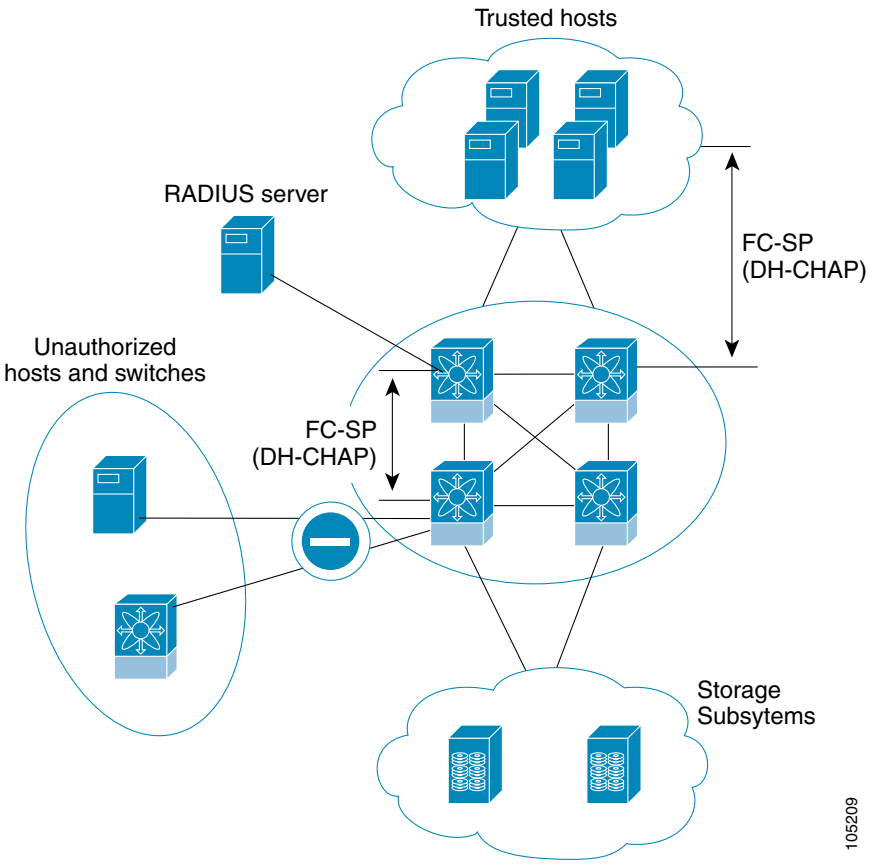
（注） Cisco NX-OS リリース 6.2(1) は Cisco MDS 9710 のみでファイバ チャネル セキュリティ プロトコル（FC-SP）機能をサポートしていません。Cisco MDS 9710 での FC-SP のサポートは、Cisco NX-OS リリース 6.2(9) 以降です。

VFC ポートを介して認証するには、FC-SP が通信にポート VSAN を使用する必要があります。したがって、認証メッセージを送受信するには、両方のピアでポート VSAN が同じで、かつアクティブになっている必要があります。

Cisco MDS 9000 ファミリのスイッチはすべて、スイッチ間またはスイッチとホスト間の認証をファブリック全体で実行できます。これらのスイッチおよびホスト認証は、各ファブリックでローカルまたはリモートで実行できます。ストレージ アイランドを企業全体のファブリックに統合して、移行すると、新しいセキュリティ問題が発生します。ストレージ アイランドを保護する方法が、企業全体のファブリックで必ずしも保証されなくなります。

たとえば、スイッチが地理的に分散しているキャンパス環境では、他のユーザが故意に、またはユーザ自身が偶然に、互換性のないスイッチに故意に相互接続することにより、スイッチ間リンク（ISL）分離やリンク切断が発生することがあります。Cisco MDS 9000 ファミリ スイッチでは、物理セキュリティに対するこのようなニーズに対応しています（図 8-1 を参照）。

*図 8-1　　スイッチおよびホストの認証*




(注)　ホスト スイッチ認証には、適切なファームウェアおよびドライバを備えたファイバ チャネル（FC）Host Bus Adapter（HBA）が必要です。

# DHCHAP

DHCHAP は、スイッチに接続しているデバイスを認証する認証プロトコルです。ファイバ チャネル認証を使用すると、信頼できるデバイスだけをファブリックに追加できるので、不正なデバイスのスイッチへのアクセスを防止できます。

(注)　この章では、FC-SP および DHCHAP という用語を共通の意味で使用しています。

DHCHAP は、必須のパスワードに基づくキー交換による認証プロトコルであり、スイッチ間およびホスト スイッチ間の認証をサポートします。DHCHAP はハッシュ アルゴリズムおよび DH グループをネゴシエートしてから、認証を実行します。また、MD5 および SHA-1 アルゴリズムベース認証をサポートします。

DHCHAP 機能の設定には、ENTERPRISE_PKG ライセンスが必要です（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。

ローカル パスワード データベースを使用して DHCHAP 認証を設定する手順は、次のとおりです。

**ステップ 1**　DHCHAP をイネーブルにします。
**ステップ 2**　DHCHAP 認証モードを識別して設定します。
**ステップ 3**　ハッシュ アルゴリズムおよび DH グループを設定します。
**ステップ 4**　ローカル スイッチおよびファブリックの他のスイッチの DHCHAP パスワードを設定します。
**ステップ 5**　再認証の DHCHAP タイムアウト値を設定します。
**ステップ 6**　DHCHAP の設定を確認します。

この項では、次のトピックについて取り上げます。



# 既存の Cisco MDS 機能との DHCHAP の互換性

ここでは、DHCHAP 機能および既存の Cisco MDS 機能の設定の影響について説明します。

- PortChannel インターフェイス：PortChannel に属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証は PortChannel レベルでなく、物理インターフェイス レベルで実行されます。
- FCIP インターフェイス：DHCHAP プロトコルは、物理インターフェイスの場合と同様に、FCIP インターフェイスと連携します。
- ポート セキュリティまたはファブリック バインディング：ファブリック バインディング ポリシーは、DHCHAP によって認証される ID に基づいて実行されます。

- VSAN：DHCHAP 認証は、VSAN 単位では実行されません。
- ハイ アベイラビリティ：DHCHAP 認証は既存の HA 機能とトランスペアレントに連携します。

# DHCHAP イネーブル化の概要

デフォルトでは、Cisco MDS 9000 ファミリの全スイッチで DHCHAP 機能はディセーブルに設定されています。

ファブリック認証用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、DHCHAP 機能をイネーブルにする必要があります。この機能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。

# DHCHAP のイネーブル化

Cisco MDS スイッチの DHCHAP をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature fcsp` | このスイッチ上で DHCHAP をイネーブルにします。 |
| | `switch(config)# no feature fcsp` | このスイッチ上で DHCHAP をディセーブル（デフォルト）にします。 |

# DHCHAP 認証モードの概要

各インターフェイスの DHCHAP 認証ステータスは、DHCHAP ポート モードの設定によって変化します。

スイッチ内で DHCHAP 機能がイネーブルの場合には、各ファイバ チャネル インターフェイスまたは FCIP インターフェイスを次の 4 つの DHCHAP ポート モードのいずれかに設定できます。

- On：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、リンクが分離状態になります。
- auto-Active：接続元デバイスが DHCHAP 認証をサポートしている場合、スイッチ初期化中に認証シーケンスが実行されます。接続元デバイスが DHCHAP 認証をサポートしていない場合には、ソフトウェアにより、初期化シーケンスの残りが実行されます。
- auto-Passive（デフォルト）：スイッチは DHCHAP 認証を開始しませんが、接続元デバイスが DHCHAP 認証を開始すれば、DHCHAP 認証に参加します。
- Off：スイッチは DHCHAP 認証をサポートしません。このようなポートに認証メッセージが送信された場合、開始元スイッチにエラー メッセージが戻されます。

（注）　DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

（注）　VE リンクの DHCHAP ポート モードの変更には、両端のポート フラップが必要です。

表 8-1 に、さまざまなモードに設定した 2 台の Cisco MDS スイッチ間での認証動作について説明します。

*表 8-1　2 台の MDS スイッチ間の DHCHAP 認証ステータス*

| スイッチ番号 DHCHAP モード | スイッチ 1 の DHCHAP モード | | | |
|---|---|---|---|---|
| | **on** | **auto-active** | **auto-passive** | **off** |
| **on** | FC-SP 認証が実行されます。 | FC-SP 認証が実行されます。 | FC-SP 認証が実行されます。 | リンクがダウンになります。 |
| **auto-Active** | | | | FC-SP 認証は*実行されません。* |
| **auto-Passive** | | | FC-SP 認証は*実行されません。* | |
| **off** | リンクがダウンになります。 | FC-SP 認証は*実行されません。* | | |

# DHCHAP モードの設定

特定のインターフェイスに DHCHAP モードを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# interface fc2/1-3`<br>`switch(config-if)#` | インターフェイスの範囲を選択し、インターフェイス コンフィギュレーション サブモードを開始します。 |
| ステップ 3 | `switch(config-if)# fcsp on` | 選択したインターフェイスの DHCHAP モードを on ステートに設定します。 |
| | `switch(config-if)# no fcsp on` | これら 3 つのインターフェイスを出荷時デフォルトの auto-passive に戻します。 |
| ステップ 4 | `switch(config-if)# fcsp auto-active 0` | 選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。0 は、ポートが再認証を実行しないことを表します。 |
| | `switch(config-if)# fcsp auto-active 120` | DHCHAP 認証モードを選択したインターフェイスの auto-active に変更し、最初の認証後に再認証を 2 時間（120 分）ごとにイネーブルにします。 |
| | `switch(config-if)# fcsp auto-active` | 選択したインターフェイスの DHCHAP 認証モードを auto-active に変更します。再認証はディセーブルになります（デフォルト）。 |

# DHCHAP ハッシュ アルゴリズムの概要

Cisco MDS スイッチは、DHCHAP 認証用のデフォルト ハッシュ アルゴリズム プライオリティ リスト（MD5 のあとに SHA-1）をサポートしています。

ヒント　ハッシュ アルゴリズムの設定を変更する場合は、ファブリック上の全スイッチに対して設定をグローバルに変更してください。

**注意**　fcsp dhchap 用の AAA 認証を有効にすると、AAA 認証に RADIUS または TACACS+ を使用する場合は、MD5 ハッシュ アルゴリズムを設定する必要があります。これは、RADIUS および TACACS+ のアプリケーションが他のハッシュ アルゴリズムをサポートしていないためです。

# DHCHAP ハッシュ アルゴリズムの設定

ハッシュ アルゴリズムを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# fcsp dhchap hash sha1` | SHA-1 ハッシュ アルゴリズムだけを使用するように設定します。 |
| | `switch(config)# fcsp dhchap hash MD5` | MD5 ハッシュ アルゴリズムだけを使用するように設定します。 |
| | `switch(config)# fcsp dhchap hash md5 sha1` | DHCHAP 認証に対して、MD5 ハッシュ アルゴリズムを使用してから SHA-1 を使用するデフォルトのプライオリティ リストを定義します。 |
| | `switch(config)# no fcsp dhchap hash sha1` | 出荷時デフォルトのハッシュ アルゴリズム プライオリティ リスト（最初に MD5、次に SHA-1）に戻します。 |

# DHCHAP グループ設定の概要

FC-SP では、複数の DHCHAP グループがサポートされています。使用できるグループは、デフォルト リストから変更される可能性があります。リストは、優先順位の最も高いものから低いものへの順序で FC-SP ピアとネゴシエートするときに使用されるように設定されています。どちらの側も、受信したグループのリストとローカル グループのリストを比較し、優先度の最も高いグループが使用されます。各グループは設定コマンドで一度しか指定できません。

グループに関する詳細については、『*Cisco MDS 9000 Series NX-OS Command Reference Guide*』の fcsp dhchap コマンドを参照してください。

**ヒント**　DH グループの設定を変更する場合は、ファブリック内のすべてのスイッチの設定をグローバルに変更してください。

# DHCHAP グループの設定

DH グループ設定を変更する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# configure terminal` | 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 | `switch(config)# fcsp dhchap dhgroup 2 3 4` | DH グループ リストを使用するように指定します。リストは降順の優先度の順に指定されます。指定されないグループは DHCHAP により使用から除外されます。 |
| | `switch(config)# no fcsp dhchap dhgroup 2 3 4` | DHCHAP のデフォルトの順番に戻ります。 |

# DHCHAP パスワードの概要

DHCHAP 認証を実行する方向ごとに、接続デバイス間の共有シークレット パスワードが必要です。このパスワードを使用するには、DHCHAP に参加するファブリック上のすべてのスイッチで、次の 3 つの方法のいずれかを使用してパスワードを管理します。

- 方法 1: ファブリック上のすべてのスイッチに同じパスワードを使用します。これは最も簡単な方法です。新しいスイッチを追加する場合、このファブリック内では同じパスワードを使用してそのスイッチを認証します。したがって、ファブリック内のいずれかのスイッチに外部から不正アクセスを試みる場合、これは最も脆弱な方法です。
- 方法 2: ファブリック上のスイッチごとに異なるパスワードを使用して、このパスワード リストを維持します。新しいスイッチを追加する場合は、新規パスワード リストを作成して、この新規リストを使用してすべてのスイッチを更新します。いずれかのスイッチにアクセスすると、このファブリック上のすべてのスイッチに関するパスワード リストが生成されます。
- 方法 3: ファブリック上のスイッチごとに異なるパスワードを使用します。新しいスイッチを追加する場合は、ファブリック内の各スイッチに対応する複数の新規パスワードを生成して、各スイッチに設定する必要があります。いずれかのスイッチが被害にあっても、他のスイッチのパスワードは引き続き保護されます。この方法では、ユーザ側で大量のパスワード メンテナンス作業が必要になります。

(注)　パスワードはすべて 64 文字以内の英数字に制限されます。パスワードは変更できますが、削除はできません。

ヒント　スイッチが 6 台以上のファブリックでは、RADIUS または TACACS+ の使用をお勧めします。ローカル パスワード データベースを使用する必要がある場合には、方法 3 を使用し、Cisco MDS 9000 ファミリ Fabric Manager を使用して、パスワード データベースを管理します。

# ローカル スイッチの DHCHAP パスワードの設定

ローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp dhchap password 0 mypassword` | ローカル スイッチのクリアテキスト パスワードを設定します。 |
| | `switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを設定します。 |
| | `switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを削除します。 |
| | `switch(config)# fcsp dhchap password 7 sfsfdf` | ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。 |
| | `switch(config)# fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを設定します。 |
| | `switch(config)# no fcsp dhchap password 7 sfsfdf 29:11:bb:cc:dd:33:11:22` | 指定 WWN のデバイスで使用する、ローカル スイッチに対して暗号化フォーマットで入力されるパスワードを削除します。 |
| | `switch(config)# fcsp dhchap password mypassword1` | 接続するデバイスで使用する、ローカル スイッチのクリア テキスト パスワードを設定します。 |

Fabric Manager を使用してローカル スイッチに DHCHAP パスワードを設定する手順は、次のとおりです。

**ステップ 1**　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

**ステップ 2**　[Local Passwords] タブをクリックします。

**ステップ 3**　[Create Row] アイコンをクリックして、新しいローカル パスワードを作成します。

[Create Local Passwords] ダイアログボックスが表示されます。

**ステップ 4**　(任意)同じローカル パスワードを設定するスイッチをチェックします。

**ステップ 5**　スイッチの WNN を選択し、[Password] フィールドにパスワードを入力します。

**ステップ 6**　[Create] をクリックして、更新したパスワードを保存します。

# リモート デバイスのパスワード設定の概要

ファブリック内の他のデバイスのパスワードを、ローカル認証データベースに設定できます。他のデバイスは、スイッチ WWN やデバイス WWN といったデバイス名で表されます。パスワードは 64 文字に制限され、クリア テキスト（0）または暗号化テキスト（7）で指定できます。

（注）　スイッチ WWN は、物理スイッチを識別します。この WWN はスイッチの認証に使用されます。また、VSAN ノード WWN とは異なります。

# リモート デバイスの DHCHAP パスワードの設定

ファブリック内の別のスイッチのリモート DHCHAP パスワードをローカルで設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword` | スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。 |
| | `switch(config)# no fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password NewPassword` | ローカル認証データベースから、このスイッチのパスワード エントリを削除します。 |
| | `switch(config)# fcsp dhchap devicename 00:11:55:66:00:aa:bb:cc password 0 NewPassword` | スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのクリア テキスト パスワードを設定します。 |
| | `switch(config)# fcsp dhchap devicename 00:11:22:33:55:aa:bb:cc password 7 asdflkjh` | スイッチ WWN デバイス名で表される、ファブリック内の他のスイッチの暗号化形式で入力されるパスワードを設定します。 |

# DHCHAP タイムアウト値の概要

DHCHAP プロトコルの交換中に、MDS スイッチが待機中の DHCHAP メッセージを指定インターバル内に受信しなかった場合、認証は失敗したと見なされます。この（認証が失敗したと見なされるまでの）時間は、20 ～ 1000 秒の範囲で設定できます。デフォルトは 30 秒です。

タイムアウト値を変更する場合には、次の要因について考慮してください。

- 既存の RADIUS および TACACS+ タイムアウト値。
- ファブリック内のすべてのスイッチに同じ値を設定する必要もあります。

# DHCHAP タイムアウト値の設定

DHCHAP タイムアウト値を構成する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# fcsp timeout 60` | 再認証タイムアウトを 60 秒に設定します。 |
| | `switch(config)# no fcsp timeout 60` | 出荷時デフォルトの 30 秒に戻します。 |

# DHCHAP AAA 認証の設定

認証オプションは個別に設定できます。認証を設定しない場合、デフォルトでローカル認証が使用されます。

AAA 認証を設定するには、第 4 章「外部 AAA サーバでのセキュリティ機能の設定」を参照し、その手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# aaa authentication dhchap default group TacacsServer1` | 認証に TACACS+ サーバ グループ（この例では、TacacsServer1）を使用する DHCHAP をイネーブルにします。 |
| | `switch(config)# aaa authentication dhchap default local` | ローカル認証用の DHCHAP をイネーブルにします。 |
| | `switch(config)# aaa authentication dhchap default group RadiusServer1` | 認証に RADIUS サーバ グループ（この例では、RadiusServer1）を使用する DHCHAP をイネーブルにします。 |

# プロトコル セキュリティ情報の表示

ローカル データベースの設定を表示するには、**show fcsp** コマンドを使用します（例 8-1 から 8-6 を参照）。

***例 8-1　FC インターフェイスの DHCHAP 設定の表示***

```
switch# show fcsp interface fc1/9

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

***例 8-2　FC インターフェイスの DHCHAP 統計情報の表示***

```
switch# show fcsp interface fc1/9 statistics

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Statistics:
        FC-SP Authentication Succeeded:5
```

```
        FC-SP Authentication Failed:0
        FC-SP Authentication Bypassed:0
```

*例 8-3　指定されたインターフェイスを介して接続されたデバイスの FC-SP WWN の表示*

```
switch# show fcsp interface fc 2/1 wwn

fc2/1:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Other device's WWN:20:00:00:e0:8b:0a:5d:e7
```

*例 8-4　ハッシュ アルゴリズムとローカル スイッチ用に設定された DHCHAP グループの表示*

```
switch# show fcsp dhchap
Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1

Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_NULL
DHCHAP_GROUP_1536
DHCHAP_GROUP_1024
DHCHAP_GROUP_1280
DHCHAP_GROUP_2048
```

*例 8-5　DHCHAP ローカル パスワード データベースの表示*

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:**********
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is ******
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is *********

Other Devices' Passwords:
        Password for device with WWN:00:11:22:33:44:aa:bb:cc is ***********
```

*例 8-6　デバイス WWN の ASCII 表記の表示*

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22
Ascii representation of WWN to be used with AAA servers:Ox_3011bbccdd331122
```

ヒント　RADIUS サーバおよび TACACS+ サーバにスイッチ情報を設定する場合、デバイス WWN の ASCII 表記（例 8-6 で太字で表記）を使用してください。

# 設定例

ここでは、図 8-2 に示した例を設定する手順を示します。

*図 8-2　DHCHAP 認証の例*

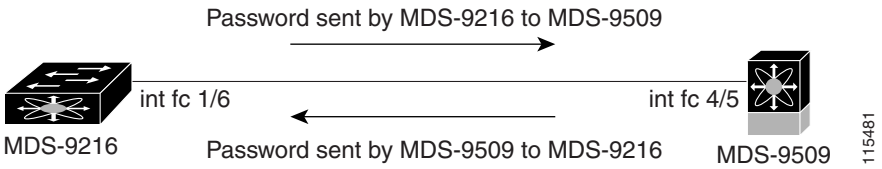



図 8-2 に示す認証設定を設定するには、次の手順を実行します。

**ステップ 1**　ファブリック内の MDS 9216 スイッチのデバイス名を取得します。ファブリック内の MDS 9216 スイッチは、スイッチ WWN によって識別されます。

```
MDS-9216# show wwn switch
Switch WWN is 20:00:00:05:30:00:54:de
```

**ステップ 2**　このスイッチで DHCHAP を明示的にイネーブルにします。

**（注）**　DHCHAP 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。

```
MDS-9216(config)# feature fcsp
```

**ステップ 3**　このスイッチのクリア テキスト パスワードを設定します。このパスワードは、接続先デバイスで使用されます。

```
MDS-9216(config)# fcsp dhchap password rtp9216
```

**ステップ 4**　スイッチ WWN デバイス名で表される、ファブリック上の他のスイッチのパスワードを設定します。

```
MDS-9216(config)# fcsp dhchap devicename 20:00:00:05:30:00:38:5e password rtp9509
```

**ステップ 5**　目的のファイバ チャネル インターフェイスの DHCHAP モードをイネーブルにします。

**（注）**　DHCHAP ポート モードを off モード以外のモードに変更すると、再認証が実行されます。

```
MDS-9216(config)# interface fc 1/16
MDS-9216(config-if)# fcsp on
```

**ステップ 6**　DHCHAP ローカル パスワード データベースを表示して、このスイッチに設定されたプロトコル セキュリティ情報を確認します。

```
MDS-9216# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:38:5e is *******
```

**ステップ 7**　ファイバ チャネル インターフェイスの DHCHAP 設定を表示します。

```
MDS-9216# show fcsp interface fc 1/6
fc1/6
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

**ステップ 8**　接続先の MDS 9509 スイッチでこれらの手順を繰り返します。

```
MDS-9509# show wwn switch
Switch WWN is 20:00:00:05:30:00:38:5e
MDS-9509(config)# feature fcsp
MDS-9509(config)# fcsp dhchap password rtp9509
MDS-9509(config)# fcsp dhchap devicename 20:00:00:05:30:00:54:de password rtp9216
MDS-9509(config)# interface fc 4/5
MDS-9509(config-if)# fcsp on
MDS-9509# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:*******
Other Devices' Passwords:
        Password for device with WWN:20:00:00:05:30:00:54:de is *******
MDS-9509# show fcsp interface fc 4/5
Fc4/5
        fcsp authentication mode:SEC_MODE_ON
        Status:Successfully authenticated
```

これで、図 8-2 に示す設定例の DHCHAP 認証のイネーブル化と設定の作業が終わります。

# デフォルト設定

表 8-2 に、スイッチのすべてのファブリック セキュリティ機能のデフォルト設定を示します。

*表 8-2　デフォルトのファブリック セキュリティ設定値*

| パラメータ | デフォルト |
|---|---|
| DHCHAP 機能 | ディセーブル |
| DHCHAP ハッシュ アルゴリズム | 最初に MD5、次に SHA-1 のプライオリティ リストで DHCHAP 認証を実行 |
| DHCHAP 認証モード | auto-passive |
| DHCHAP グループのデフォルトの交換プライオリティ | 0、4、1、2、3 の順 |
| DHCHAP タイムアウト値 | 30 秒 |

CHAPTER 9

# ポート セキュリティの設定

Cisco MDS 9000 ファミリのスイッチにはすべて、侵入の試みを拒否し、管理者に侵入を報告するポート セキュリティ機能があります。

(注) ポート セキュリティは、fc ポート セキュリティとしてファイバ チャネル ポートと Fibre Channel over Ethernet（FCoE）ポートの両方をサポートします。

この章は、次の項で構成されています。

# ポート セキュリティの概要

Cisco MDS 9000 ファミリのスイッチにはすべて、侵入の試みを拒否し、管理者に侵入を報告するポート セキュリティ機能があります。

通常、SAN 内のすべてのファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続して、ゾーン メンバーシップに基づいて SAN サービスにアクセスできます。ポート セキュリティ機能は、次の方法で、Cisco MDS 9000 ファミリのスイッチ ポートへの不正アクセスを防止します。

- 不正なファイバ チャネル デバイス（Nx ポート）およびスイッチ（xE ポート）からのログイン要求は拒否されます。
- 侵入に関するすべての試みは、システム メッセージを通して SAN 管理者に報告されます。
- 設定配信は CFS インフラストラクチャを使用し、CFS 対応スイッチに制限されています。配信はデフォルトでディセーブルになっています。
- ポート セキュリティ ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。

この項では、次のトピックについて取り上げます。



# ポート セキュリティの実行

ポート セキュリティを実行するには、デバイスおよびスイッチ ポート インターフェイス（これらを通じて各デバイスまたはスイッチが接続される）を設定し、設定をアクティブにします。

- デバイスごとに Nx ポート接続を指定するには、Port World Wide Name（pWWN）または Node World Wide Name（nWWN）を使用します。
- スイッチごとに xE ポート接続を指定するには、Switch World Wide Name（sWWN）を使用します。

Nx および xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定することができます。

ポート セキュリティ ポリシーはポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。

ポート セキュリティ機能は 2 つのデータベースを使用して、設定の変更を受け入れ、実装します。

- コンフィギュレーション データベース：すべての設定の変更がコンフィギュレーション データベースに保存されます。
- アクティブ データベース：ファブリックが現在実行しているデータベース。ポート セキュリティ機能を実行するには、スイッチに接続されているすべてのデバイスがポート セキュリティ アクティブ データベースに格納されている必要があります。ソフトウェアはこのアクティブ データベースを使用して、認証を行います。

# 自動学習の概要

指定期間内にポート セキュリティ設定を自動的に学習するように、スイッチを設定できます。この機能を使用すると、任意の Cisco MDS 9000 ファミリ スイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。ポート セキュリティ機能を初めてアクティブにするときに、この機能を使用してください。ポートごとに手動で設定する面倒な作業が軽減されます。自動学習は、VSAN 単位で設定する必要があります。この機能をイネーブルにすると、ポート アクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習をイネーブルにすると、学習は、すでにスイッチにログインしているデバイスまたはインターフェイス、およびログインする必要がある新しいデバイスまたはインターフェイスで実行されます。ポートでの学習済みエントリは、自動学習がまだイネーブルな場合、そのポートをシャットダウンした後でクリーンアップされます。

学習は、既存の設定済みのポート セキュリティ ポリシーを上書きしません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習によって、そのインターフェイスに他の pWWN を許可する新しいエントリが追加されることはありません。他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。

(注)　ポート セキュリティ機能をアクティブにすると、自動学習機能はデフォルトで有効になります。自動学習がディセーブルであるか、または非アクティブであり、再度アクティブ化されるまで、ポート セキュリティを再度アクティブ化することはできません。

# ポート セキュリティのアクティブ化

デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポート セキュリティ機能は非アクティブです。

ポート セキュリティ機能をアクティブにすると、次の処理が適用されます。

- 自動学習も自動的にイネーブルになります。つまり、
  - ここから、自動学習はすでにスイッチにログインしたデバイスまたはインタフェース、および今後ログインする新しいデバイスに対して発生します。
  - 自動学習をディセーブルにするまで、データベースをアクティブにできません。
- すでにログインしているすべてのデバイスは学習され、アクティブ データベースに追加されます。
- 設定済みデータベースのすべてのエントリがアクティブ データベースにコピーされます。

データベースをアクティブにすると、以降のデバイスのログインは、自動学習されたエントリを除き、アクティブ化されたポートによってバインドされた WWN ペアの対象になります。自動学習されたエントリがアクティブになる前に、自動学習をディセーブルにする必要があります。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。ポート セキュリティ機能をアクティブにし、自動学習をディセーブルにすることもできます。

ヒント　ポートがログインを拒否されて停止している場合、その後でログインを許可するようにデータベースを設定しても、ポートは自動的に起動しません。そのポートをオンラインに戻すには、**no shutdown** CLI コマンドを明示的に発行する必要があります。

# ポート セキュリティ設定

ポート セキュリティを設定する手順は、使用する機能によって異なります。CFS 配信を使用している場合、自動学習の動作が異なります。

この項では、次のトピックについて取り上げます。



## 自動学習と CFS 配信を使用するポート セキュリティの設定

自動学習および CFS 配信を使用してポート セキュリティを設定する手順は、次のとおりです。

**ステップ 1**　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」セクション（9-244 ページ）を参照してください。

**ステップ 2**　CFS 配信をイネーブルにします。「配信のイネーブル化」セクション（9-251 ページ）を参照してください。

**ステップ 3**　各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。「ポート セキュリティのアクティブ化」セクション（9-244 ページ）を参照してください。

**ステップ 4**　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。「変更のコミット」セクション（9-252 ページ）を参照してください。この時点で、すべてのスイッチがアクティブになり、自動学習が有効になります。

**ステップ 5**　すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

**ステップ 6**　各 VSAN で、自動学習をディセーブルにします。「自動学習のディセーブル化」セクション（9-247 ページ）を参照してください。

**ステップ 7**　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。「変更のコミット」セクション（9-252 ページ）を参照してください。この時点で、すべてのスイッチから自動学習されたエントリが、すべてのスイッチに配信されるスタティックなアクティブ データベースに組み込まれます。

**ステップ 8**　各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。「ポート セキュリティ データベースのコピー」セクション（9-256 ページ）を参照してください。

**ステップ 9**　CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。「変更のコミット」セクション（9-252 ページ）を参照してください。これで、ファブリック内のすべてのスイッチのコンフィギュレーション データベースが同一になります。

**ステップ 10**　ファブリック オプションを使用して、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。これにより、ポート セキュリティ コンフィギュレーション データベースが、ファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。

# 自動学習を使用し、CFS を使用しない場合のポート セキュリティの設定

自動学習を使用し、CFS 配信を使用しないポート セキュリティを設定する手順は、次のとおりです。

**ステップ 1**　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」セクション (9-244 ページ) を参照してください。

**ステップ 2**　各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。「ポート セキュリティのアクティブ化」セクション (9-244 ページ) を参照してください。

**ステップ 3**　すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

**ステップ 4**　各 VSAN で、自動学習をディセーブルにします。「自動学習のディセーブル化」セクション (9-247 ページ) を参照してください。

**ステップ 5**　各 VSAN のコンフィギュレーション データベースにアクティブ データベースをコピーします。「ポート セキュリティ データベースのコピー」セクション (9-256 ページ) を参照してください。

**ステップ 6**　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。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

**ステップ 7**　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 6 を繰り返します。

# 手動データベース設定を使用する場合のポート セキュリティの設定

ポート セキュリティを設定し、ポート セキュリティ データベースを手動設定する手順は、次のとおりです。

**ステップ 1**　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」セクション (9-244 ページ) を参照してください。

**ステップ 2**　各 VSAN のコンフィギュレーション データベースにすべてのポート セキュリティ エントリを手動で設定します。「ポート セキュリティの手動設定」セクション (9-249 ページ) を参照してください。

**ステップ 3**　各 VSAN で、ポート セキュリティをアクティブにします。デフォルトで自動学習が有効になります。「ポート セキュリティのアクティブ化」セクション (9-244 ページ) を参照してください。

**ステップ 4**　各 VSAN で、自動学習をディセーブルにします。「自動学習のディセーブル化」セクション (9-247 ページ) を参照してください。

**ステップ 5**　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。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

**ステップ 6**　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 5 を繰り返します。

# ポート セキュリティのイネーブル化

デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポート セキュリティ機能はディセーブルです。

ポート セキュリティをイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature port-security` | スイッチ上でポート セキュリティをイネーブルにします。 |
| | `switch(config)# no feature port-security` | スイッチ上でポート セキュリティをディセーブル（デフォルト）にします。 |

# ポート セキュリティのアクティベーション

この項では、次のトピックについて取り上げます。

- ポート セキュリティのアクティブ化（9-244 ページ）
- データベースのアクティブ化の拒否（9-245 ページ）
- ポート セキュリティのアクティベーションの強制（9-245 ページ）

# ポート セキュリティのアクティブ化

ポート セキュリティ機能をアクティブ化するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# port-security activate vsan 1` | 指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。 |
| | `switch(config)# port-security activate vsan 1 no-auto-learn` | 指定された VSAN のポート セキュリティ データベースをアクティブにし、自動学習をディセーブルにします。 |
| | `switch(config)# no port-security activate vsan 1` | 指定された VSAN のポート セキュリティ データベースを無効にし、自動的に自動学習をディセーブルにします。 |

（注）　必要に応じて、自動学習をディセーブルに設定できます（「自動学習のディセーブル化」セクション（9-247 ページ）を参照）。

# データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

- 存在しないエントリや矛盾するエントリがコンフィギュレーション データベースにあるが、アクティブ データベースにはない場合。
- アクティベーションの前に、自動学習機能がイネーブルに設定されていた場合。この状態のデータベースを再アクティブ化するには、自動学習をディセーブルにします。
- 各ポート チャネル メンバーに正確なセキュリティが設定されていない場合。
- 設定済みデータベースが空であり、アクティブ データベースが空でない場合。

上記のような矛盾が 1 つ以上発生したためにデータベース アクティベーションが拒否された場合は、ポート セキュリティ アクティベーションを強制して継続することができます。

# ポート セキュリティのアクティベーションの強制

ポート セキュリティ アクティベーション要求が拒否された場合は、アクティベーションを強制できます。

**（注）** **force** オプションを使用してアクティブ化すると、アクティブ データベースに違反している既存のデバイスをログアウトさせることができます。

存在しないエントリや矛盾するエントリを表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

ポート セキュリティ データベースを強制的にアクティブにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# port-security activate vsan 1 force` | 競合にもかかわらず、VSAN 1 ポート セキュリティ データベースを強制的にアクティブ化します。 |

# データベースの再アクティブ化

ポート セキュリティ データベースを再アクティブ化するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# no port-security auto-learn vsan 1` | 自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | switch(config)# **exit**<br>switch# **port-security database copy vsan 1** | アクティブ データベースから設定済みデータベースにコピーします。 |
| ステップ 4 | switch# **config t**<br>switch(config)# **port-security activate vsan 1** | 指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。 |

ヒント　自動学習がイネーブルで、データベースをアクティブ化できない場合、自動学習機能をディセーブルにするまで **force** オプションなしで作業を進めることはできません。

# 自動学習

ここでは、次の内容について説明します。



## 自動学習のイネーブル化の概要

自動学習設定の状態は、ポート セキュリティ機能の状態によって異なります。

- ポート セキュリティ機能がアクティブでない場合、自動学習はデフォルトでディセーブルです。
- ポート セキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルです（このオプションを明示的にディセーブルにしていない場合）。

ヒント　VSAN 上で自動学習がイネーブルの場合、**force** オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

## 自動学習のイネーブル化

自動学習をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **port-security auto-learn vsan 1** | 自動学習をイネーブルにして、VSAN 1 へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるようにします。これらのデバイスは、ポート セキュリティ アクティブ データベースに記録されます。 |

# 自動学習のディセーブル化

自動学習をディセーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# no port-security auto-learn vsan 1` | 自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。 |

# 自動学習デバイスの許可

表 9-1 に、デバイス要求に対して接続が許可される条件をまとめます。

*表 9-1　許可される自動学習デバイス要求*

| 条件 | デバイス（pWWN、nWWN、sWWN） | 接続先 | 許可 |
|---|---|---|---|
| 1 | 1 つまたは複数のスイッチ ポートに設定されている場合 | 設定済みスイッチ ポート | 許可 |
| 2 | | 他のすべてのスイッチ ポート | 拒否 |
| 3 | 設定されていない場合 | 設定されていないスイッチ ポート | 許可される条件: 自動学習が有効 |
| 4 | | | 拒否される条件: 自動学習が無効 |
| 5 | 設定されている場合、または設定されていない場合 | 任意のデバイスを接続許可するスイッチ ポート | 許可 |
| 6 | 任意のスイッチ ポートにログインするように設定されている場合 | スイッチ上の任意のポート | 許可 |
| 7 | 設定されていない場合 | その他のデバイスが設定されたポート | 拒否 |

# 許可の例

ポート セキュリティ機能がアクティブで、アクティブ データベースに次の条件が指定されていることが前提です。

- pWWN（P1）には、インターフェイス fc1/1（F1）からアクセスできる。
- pWWN（P2）には、インターフェイス fc1/1（F1）からアクセスできる。
- nWWN（N1）には、インターフェイス fc1/2（F2）からアクセスできる。
- インターフェイス fc1/3（F3）からは、任意の WWN にアクセスできる。

- nWWN（N3）には、任意のインターフェイスからアクセスできる。
- pWWN（P3）には、インターフェイス fc1/4（F4）からアクセスできる。
- sWWN（S1）には、インターフェイス fc1/10 ～ 13（F10 ～ F13）からアクセスできる。
- pWWN（P10）には、インターフェイス fc1/11（F11）からアクセスできる。

表 9-2 に、このアクティブ データベースに対するポート セキュリティ許可の結果をまとめます。ここに示す条件は、表 9-1 の条件を参照しています。

*表 9-2　各シナリオの許可結果*

| デバイス接続要求 | 許可 | 条件 | 理由 |
|---|---|---|---|
| P1、N2、F1 | 許可 | 1 | 競合しません。 |
| P2、N2、F1 | 許可 | 1 | 競合しません。 |
| P3、N2、F1 | 拒否 | 2 | F1 が P1/P2 にバインドされています。 |
| P1、N3、F1 | 許可 | 6 | N3 に関するワイルドカード一致です。 |
| P1、N1、F3 | 許可 | 5 | F3 に関するワイルドカード一致です。 |
| P1、N4、F5 | 拒否 | 2 | P1 が F1 にバインドされています。 |
| P5、N1、F5 | 拒否 | 2 | N1 は F2 でだけ許可されます。 |
| P3、N3、F4 | 許可 | 1 | 競合しません。 |
| S1、F10 | 許可 | 1 | 競合しません。 |
| S2、F11 | 拒否 | 7 | P10 が F11 にバインドされています。 |
| P4、N4、F5（自動学習が有効） | 許可 | 3 | 競合しません。 |
| P4、N4、F5（自動学習が無効） | 拒否 | 4 | 一致しません。 |
| S3、F5（自動学習が有効） | 許可 | 3 | 競合しません。 |
| S3、F5（自動学習が無効） | 拒否 | 4 | 一致しません。 |
| P1、N1、F6（自動学習が有効） | 拒否 | 2 | P1 が F1 にバインドされています。 |
| P5、N5、F1（自動学習が有効） | 拒否 | 7 | P1 と P2 だけが F1 にバインドされています。 |
| S3、F4（自動学習が有効） | 拒否 | 7 | P3 と F4 がペアになります。 |
| S1、F3（自動学習が有効） | 許可 | 5 | 競合しません。 |
| P5、N3、F3 | 許可 | 6 | F3 および N3 に関するワイルドカード（*）一致です。 |
| P7、N3、F9 | 許可 | 6 | N3 に関するワイルドカード（*）が一致しています。 |

# ポート セキュリティの手動設定

Cisco MDS 9000 ファミリの任意のスイッチにポート セキュリティを設定する手順は、次のとおりです。

**ステップ 1**　保護する必要があるポートの WWN を識別します。

**ステップ 2**　許可された nWWN または pWWN に対して fWWN を保護します。

**ステップ 3**　ポート セキュリティ データベースをアクティブにします。

**ステップ 4**　設定を確認します。

この項では、次のトピックについて取り上げます。



## WWN の識別の概要

ポート セキュリティを手動で設定する場合は、次の注意事項に従ってください。

- インターフェイスまたは fWWN でスイッチ ポートを識別します。
- pWWN または nWWN でデバイスを識別します。
- Nx ポートが SAN スイッチ ポート Fx にログインできる場合、その Nx ポートは指定された Fx ポートを通した場合に限りログインできます。
- Nx ポートの nWWN が Fx ポート WWN にバインドされている場合、Nx ポートのすべての pWWN は暗黙的に Fx ポートとペアになります。
- TE ポート チェックは、トランク ポートの許可 VSAN リスト内の VSAN ごとに実行されます。
- 同じポートチャネル内のすべてのポートチャネル xE ポートに、同じ WWN セットを設定する必要があります。
- E ポートのセキュリティは、E ポートのポート VSAN に実装されます。この場合、sWWN を使用して許可チェックを保護します。
- アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
- 実行コンフィギュレーションを保存することにより、コンフィギュレーション データベースおよびアクティブ データベース内のアクティブ化されたエントリを保存します。アクティブ データベース内の学習済みエントリは保存されません。

# 許可済みのポート ペアの追加

許可済みのポート ペアをポート セキュリティに追加するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | switch# **config t**<br>switch(config)# | 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 | switch(config)# **port-security database vsan 1**<br>switch(config-port-security)# | 指定された VSAN に対してポート セキュリティ データベース モードを開始します。 |
| | switch(config)# **no port-security database vsan 1**<br>switch(config)# | 指定された VSAN からポート セキュリティ コンフィギュレーション データベースを削除します。 |
| ステップ 3 | switch(config-port-security)# **swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5** | PortChannel 5 を介した場合だけログインするように、指定された sWWN を設定します。 |
| | switch(config-port-security)# **any-wwn interface fc1/1 - fc1/8** | 指定されたインターフェイスを介してログインするようにすべての WWN を設定します。 |
| | switch(config-port-security)# **pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e** | 指定された fWWN を介した場合だけログインするように、指定された pWWN を設定します。 |
| | switch(config-port-security)# **no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e** | 前の手順で設定した、指定した pWWN を削除します。 |
| | switch(config-port-security)# **nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e** | 指定された fWWN を介した場合だけログインするように、指定された nWWN を設定します。 |
| | switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66** | ファブリック内の任意のポートを介してログインするように、指定された pWWN を設定します。 |
| | switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80** | 指定されたスイッチ内の任意のインタフェースを介してログインするように、指定された pWWN を設定します。 |
| | switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80 interface fc3/1** | 指定されたスイッチの指定されたインターフェイスを介してログインするように、指定された pWWN を設定します |
| | switch(config-port-security)# **any-wwn interface fc3/1** | 任意のスイッチの指定されたインターフェイスを介してログインするようにすべての WWN を設定します。 |
| | switch(config-port-security)# **no any-wwn interface fc2/1** | 前の手順で設定したワイルドカードを削除します。 |

バインドする必要がある WWN ペアを識別したら、これらのペアをポート セキュリティ データベースに追加します。

ヒント　リモート スイッチのバインドは、ローカル スイッチで指定できます。リモート インターフェイスを指定する場合、fWWN または sWWN インターフェイスの組み合わせを使用できます。

# ポート セキュリティ設定の配信

ポート セキュリティ機能は Cisco Fabric Services（CFS）インフラストラクチャを使用して効率的なデータベース管理を実現し、VSAN 内のファブリック全体に 1 つの設定を提供します。また、ファブリック全体でポート セキュリティ ポリシーを実行します。

この項では、次のトピックについて取り上げます。



## 配信のイネーブル化

ポート セキュリティ配信をイネーブルにするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# port-security distribute` | 配信をイネーブルにします。 |
| | `switch(config)# no port-security distribute` | 配信をディセーブルにします。 |

たとえば、ポート セキュリティをアクティブにし、自動学習をディセーブルにし、保留状態のデータベースに変更をコミットすると、**port-security activate vsan** *vsan-id* **no-auto-learn** コマンドを発行した場合と同じ結果になります。

配信モードで実行されたすべての設定は保留中の（一時的な）データベースに保存されます。設定を変更する場合、設定に対して保留中のデータベースの変更をコミットまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、変更をコミットするまで設定に反映されません。

（注）　CFS 配信がイネーブルの場合、ポートのアクティベーションまたは非アクティベーションおよび自動学習のイネーブル化またはディセーブル化は、CFS コミットを発行するまで有効になりません。常に CFS コミットとこれらの処理のいずれかを使用して、正しい設定を確認してください。「アクティブ化および自動学習の設定の配信」セクション（9-253 ページ）を参照してください。

ヒント　この場合、各処理の最後にコミットを実行することを推奨します。つまり、ポート セキュリティのアクティブ化のあと、および自動学習のイネーブル化のあとです。

# ファブリックのロック

既存の設定を変更するときの最初のアクションが実行されると、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースのコピーが保留中のデータベースになります。

CFS のロック情報を表示するには、**show cfs lock** コマンドを使用します。詳細については、『*Cisco MDS 9000 Family Command Reference*』を参照してください。

# 変更のコミット

設定に加えられた変更をコミットする場合、保留中のデータベースの設定が他のスイッチに配信されます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更をコミットするには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# port-security commit vsan 3` | 指定された VSAN のポート セキュリティの変更をコミットします。 |

# 変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、設定は影響されないまま、ロックが解除されます。

CFS のロック情報を表示するには、**show cfs lock** コマンドを使用します。詳細については、『Cisco MDS 9000 Family Command Reference』を参照してください。

指定された VSAN のポート セキュリティ設定の変更を破棄するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# port-security abort vsan 5` | 指定された VSAN のポート セキュリティの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。 |

# アクティブ化および自動学習の設定の配信

配信モードのアクティベーション設定および自動学習設定は、保留中のデータベースの変更をコミットするときに実行する処理として記憶されます。

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブ データベース内のスタティック エントリになり、ファブリック内のすべてのスイッチに配信されます。コミット後は、すべてのスイッチのアクティブ データベースは同一です。

変更をコミットする場合、保留中のデータベースに複数のアクティブ化および自動学習の設定が含まれていると、アクティブ化と自動学習の変更が統合され、処理が変更されることがあります（表 9-3 を参照）。

*表 9-3　配信モードでのアクティブ化および 自動学習の設定シナリオ*

| シナリオ | アクション | 配信がオフの場合 | 配信がオンの場合 |
|---|---|---|---|
| コンフィギュレーション データベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。 | 1. ポート セキュリティ データベースをアクティブにし、自動学習をイネーブルにします。 | コンフィギュレーション データベース = {A、B} | コンフィギュレーション データベース = {A、B} |
| | | アクティブ データベース = {A、B、C[1]、D*} | アクティブ データベース = {ヌル} |
| | | | 保留中のデータベース = {A、B + アクティベーション（イネーブル）} |
| | 2. 新規のエントリ E がコンフィギュレーション データベースに追加されました。 | コンフィギュレーション データベース = {A、B、E} | コンフィギュレーション データベース = {A、B} |
| | | アクティブ データベース = {A、B、C*、D*} | アクティブ データベース = {ヌル} |
| | | | 保留中のデータベース = {A、B、E + アクティベーション（イネーブル）} |
| | 3. コミットを行います。 | N/A | コンフィギュレーション データベース = {A、B、E} |
| | | | アクティブ データベース = {A、B、E、C*、D*} |
| | | | 保留中のデータベース = 空の状態 |

*表 9-3　配信モードでのアクティブ化および(続き)自動学習の設定シナリオ(続き)*

| シナリオ | アクション | 配信がオフの場合 | 配信がオンの場合 |
|---|---|---|---|
| コンフィギュレーション データベースに A および B が存在し、アクティベーションが行われておらず、デバイス C および D がログインされています。 | 1. ポート セキュリティ データベースをアクティブにし、自動学習をイネーブルにします。 | コンフィギュレーション データベース = {A、B}<br>アクティブ データベース = {A、B、C*、D*} | コンフィギュレーション データベース = {A、B}<br>アクティブ データベース = {ヌル}<br>保留中のデータベース = {A、B + アクティベーション(イネーブル)} |
| | 2. 学習をディセーブルにします。 | コンフィギュレーション データベース = {A、B}<br>アクティブ データベース = {A、B、C、D} | コンフィギュレーション データベース = {A、B}<br>アクティブ データベース = {ヌル}<br>保留中のデータベース = {A、B + アクティベーション(イネーブル) + 学習(ディセーブル)} |
| | 3. コミットを行います。 | N/A | コンフィギュレーション データベース = {A、B}<br>アクティブ データベース = {A、B}、デバイス C および D がログアウトされます。これは、自動学習をディセーブルにした場合のアクティベーションと同じです。<br>保留中のデータベース = 空の状態 |

1. *(アスタリスク)は学習されたエントリを意味します。

**ヒント**　各処理の最後にコミットを実行することを推奨します。つまり、ポート セキュリティのアクティブ化の後、および自動学習のイネーブル化の後です。

# データベース マージに関するガイドライン

データベースのマージとは、コンフィギュレーション データベースとアクティブ データベース内のスタティック(学習されていない)エントリの統合を指します。

2 つのファブリック間のデータベースをマージする場合は、次のことに気をつけて行ってください。

- アクティベーション ステータスと自動学習ステータスが両方のファブリックで同じであることを確認します。
- 両方のデータベースの各 VSAN のコンフィギュレーションの合計数が、2 K を超えていないことを確認してください。

**注意**　この 2 つの条件に従わない場合は、マージに失敗します。次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

# データベースの相互作用

表 9-4 に、アクティブ データベースとコンフィギュレーション データベース間の相違、および相互作用を示します。

*表 9-4　アクティブおよびコンフィギュレーション ポート セキュリティ データベース*

| アクティブ データベース | コンフィギュレーション データベース |
|---|---|
| 読み取り専用。 | 読み取りと書き込み。 |
| 設定を保存すると、アクティブなエントリだけが保存されます。学習済みエントリは保存されません。 | 設定を保存すると、コンフィギュレーション データベース内のすべてのエントリが保存されます。 |
| アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブ データベースに追加されます。 | アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。 |
| アクティブ データベースを設定済みデータベースで上書きするには、ポート セキュリティ データベースをアクティブ化します。強制的にアクティブにすると、アクティブ データベースの設定済みエントリに違反が生じることがあります。 | コンフィギュレーション データベースをアクティブ データベースで上書きできます。 |

（注）　**port-security database copy vsan** コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

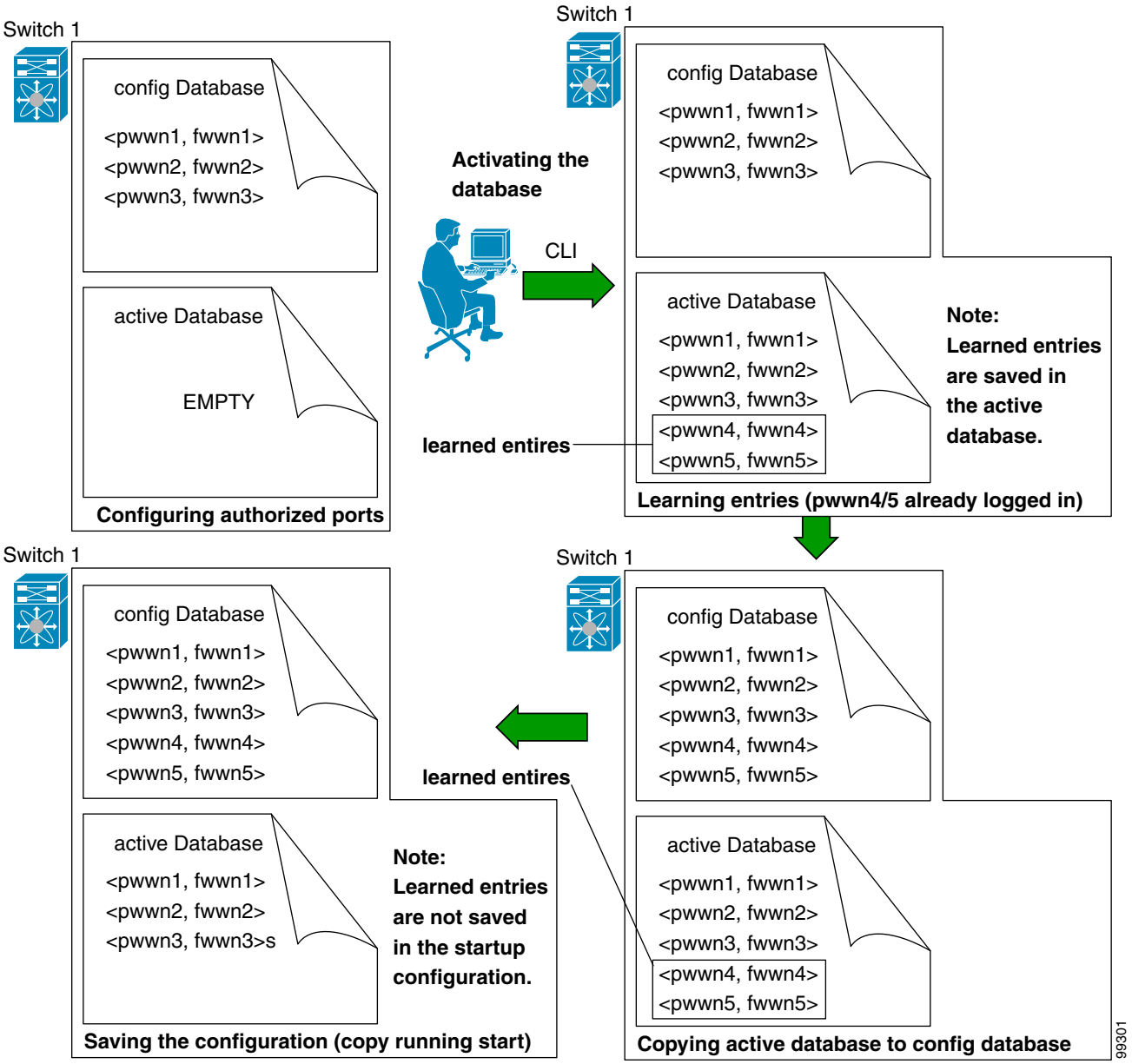
ここで説明する内容は、次のとおりです。

- データベースのシナリオ（9-255 ページ）
- ポート セキュリティ データベースのコピー（9-256 ページ）
- ポート セキュリティ データベースの削除（9-257 ページ）
- ポート セキュリティ データベースのクリア（9-257 ページ）

# データベースのシナリオ

図 9-1 の各シナリオは、ポート セキュリティ設定に基づくアクティブ データベースとコンフィギュレーション データベースのステータスを示しています。

*図 9-1　　ポート セキュリティ データベースのシナリオ*




# ポート セキュリティ データベースのコピー

アクティブ データベースから設定済みデータベースにコピーするには、**port-security database copy vsan** コマンドを使用します。アクティブ データベースが空の場合、このコマンドは受け付けられません。

```
switch# port-security database copy vsan 1
```

アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**port-security database diff active vsan** コマンドを使用します。このコマンドは、矛盾を解決する場合に使用できます。

```
switch# port-security database diff active vsan 1
```

コンフィギュレーション データベースとアクティブ データベースとの違いに関する情報を表示するには、**port-security database diff config vsan** コマンドを使用します。

```
switch# port-security database diff config vsan 1
```

ヒント　自動学習をディセーブルにしてから 、**port-security database copy vsan** コマンドを発行することを推奨します。これにより、コンフィギュレーション データベースとアクティブ データベースを確実に同期化できます。配信がイネーブルの場合、このコマンドによってコンフィギュレーション データベースの一時的なコピーが作成され、結果としてファブリックがロックされます。ファブリックをロックする場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

# ポート セキュリティ データベースの削除

ヒント　配信がイネーブルの場合、削除によってデータベースのコピーが作成されます。実際にデータベースを削除するには、明示的に **port-security commit** コマンドを入力する必要があります。

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no port-security database vsan** コマンドを使用します。

```
switch(config)# no port-security database vsan 1
```

# ポート セキュリティ データベースのクリア

指定された VSAN のポート セキュリティ データベースから既存の統計情報をすべてクリアするには、**clear port-security statistics vsan** コマンドを使用します。

```
switch# clear port-security statistics vsan 1
```

VSAN 内の指定されたインターフェイスに関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn interface** コマンドを使用します。

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

VSAN 全体に関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn vsan** コマンドを使用します。

```
switch# clear port-security database auto-learn vsan 1
```

（注）　**clear port-security database auto-learn** および **clear port-security statistics** コマンドはローカル スイッチだけに関連するので、ロックを取得しません。また、学習済みエントリはスイッチにだけローカルで、配信に参加しません。

VSAN 内で、任意のスイッチから VSAN の保留中のセッションをクリアするには、**port-security clear vsan** コマンドを使用します。

```
switch# clear port-security session vsan 5
```

# ポート セキュリティ設定の表示

**show port-security database** コマンドを使用すると、設定されたポート セキュリティ情報が表示されます（例 9-1 ～ 9-11 を参照）。

***例 9-1　ポート セキュリティ コンフィギュレーション データベースの内容の表示***

```
switch# show port-security database
-------------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point       (Interface)
-------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)
1       50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/12)
2       20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128)
3       20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

**show port-security** コマンドで fWWN や VSAN、またはインターフェイスや VSAN を指定すると、アクティブなポート セキュリティの出力を表示することもできます（例 9-2 を参照）。

***例 9-2　VSAN 1 のポート セキュリティ コンフィギュレーション データベースの表示***

```
switch# show port-security database vsan 1
-------------------------------------------------------------------------------
Vsan   Logging-in Entity              Logging-in Point        (Interface)
-------------------------------------------------------------------------------
1                  *                  20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

***例 9-3　アクティブ化されたデータベースの表示***

```
switch# show port-security database active
-------------------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point     (Interface)          Learnt
-------------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)   20:0d:00:05:30:00:95:de(fc1/13)            Yes
1       50:06:04:82:bc:01:c3:84(pwwn)   20:0c:00:05:30:00:95:de(fc1/12)            Yes
2       20:00:00:05:30:00:95:df(swwn)   20:0c:00:05:30:00:95:de(port-channel 128) Yes
3       20:00:00:05:30:00:95:de(swwn)   20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

***例 9-4　一時的なコンフィギュレーション データベースの内容の表示***

```
switch# show port-security pending vsan 1
Session Context for VSAN 1
---------------------------
Activation Status: Active
Auto Learn Status: On
Force activate: No
```

```
Config db modified: Yes
Activation done: Yes
Session owner: admin(2)
Session database:
-------------------------------------------------------------------------------
VSAN Logging-in Entity Logging-in Point (Interface)
-------------------------------------------------------------------------------
1 20:11:00:33:22:00:2a:4a(pwwn) 20:41:00:05:30:00:4a:1e(fc2/1)
[Total 1 entries]
```

*例 9-5　一時的なコンフィギュレーション データベースとコンフィギュレーション データベースの相違の表示*

```
switch# show port-security pending-diff vsan 1
Session Diff for VSAN: 1
------------------------
Database will be activated
Learning will be turned ON
Database Diff:
+pwwn 20:11:00:33:22:00:2a:4a fwwn 20:41:00:05:30:00:4a:1e
```

各ポートのアクセス情報は個別に表示されます。fWWN または interface オプションを指定すると、(その時点で)アクティブ データベース内で指定された fWWN またはインターフェイスとペアになっているすべてのデバイスが表示されます(例 9-6 から 9-8 を参照)。

*例 9-6　VSAN 1 内のワイルドカード fWWN ポート セキュリティの表示*

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

*例 9-7　VSAN 1 内の設定済み fWWN ポート セキュリティの表示*

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

*例 9-8　VSAN 2 内のインターフェイス ポート情報の表示*

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

ポート セキュリティの統計情報は、常時更新され、いつでも入手できます(例 9-9 を参照)。

*例 9-9　ポート セキュリティ統計の表示*

```
switch# show port-security statistics
Statistics For VSAN: 1
-----------------------
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0

Total Logins permitted  : 4
Total Logins denied     : 0
```

```
Statistics For VSAN: 2
-----------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
...
```

アクティブなデータベースおよび自動学習設定のステータスを確認するには、**show port-security status** コマンドを使用します（例 9-10 を参照）。

***例 9-10　ポート セキュリティのステータスの表示***

```
switch# show port-security status
Fabric Distribution Enabled
VSAN 1 :No Active database, learning is disabled, Session Lock Taken
VSAN 2 :No Active database, learning is disabled, Session Lock Taken
...
```

**show port-security** コマンドは、デフォルトでこれまでの 100 の違反を表示します（例 9-11 を参照）。

***例 9-11　ポート セキュリティ データベースでの違反の表示***

```
switch# show port-security violations

-------------------------------------------------------------------------------------------
VSAN    Interface       Logging-in Entity               Last-Time          [Repeat count]
-------------------------------------------------------------------------------------------
1       fc1/13          21:00:00:e0:8b:06:d9:1d(pwwn)   Jul  9 08:32:20 2003    [20]
                        20:00:00:e0:8b:06:d9:1d(nwwn)
1       fc1/12          50:06:04:82:bc:01:c3:84(pwwn)   Jul  9 08:32:20 2003    [1]
                        50:06:04:82:bc:01:c3:84(nwwn)
2       port-channel 1  20:00:00:05:30:00:95:de(swwn)   Jul  9 08:32:40 2003    [1]
[Total 2 entries]
```

**show port-security** コマンドを **last** *number* オプションを指定して発行すると、先頭に表示される指定した数のエントリだけが表示されます。

# デフォルト設定

表 9-5 に、スイッチのすべてのポート セキュリティ機能のデフォルト設定を示します。

***表 9-5　セキュリティのデフォルト設定値***

| パラメータ | デフォルト |
|---|---|
| 自動学習 | ポート セキュリティがイネーブルの場合は、イネーブル。 |
| ポート セキュリティ | ディセーブル |
| 配信 | ディセーブル<br>(注)　配信をイネーブルにすると、スイッチ上のすべての VSAN の配信がイネーブルになります。 |

CHAPTER 10

# Fibre Channel Common Transport 管理セキュリティの設定

この章では、Cisco MDS 9000 シリーズ スイッチの Fibre Channel Common Transport（FC-CT）管理セキュリティ機能について説明します。

## Fibre Channel Common Transport の概要

FC-CT 管理セキュリティ機能により、ストレージ管理者またはネットワーク管理者だけが、スイッチに対してクエリーを送信し、情報にアクセスできるようにネットワークを設定できます。このような情報には、ファブリック内のログイン デバイス、ファブリック内のスイッチなどのデバイス、デバイスの接続方法、各スイッチのポートの数、各ポートの接続先、設定済みゾーンの情報、ゾーンまたはゾーン セットの追加と削除の権限、ファブリックに接続するすべてのホストのホスト バス アダプタ（HBA）の詳細などがあります。

（注） Cisco MDS NX-OS Release 6.2(9) では、FC 管理機能はデフォルトで無効です。FC 管理機能を有効にするには、**fc-management enable** コマンドを使用します。

FC-CT 管理クエリーを送信し、管理サーバへの要求を変更できる pWWN を設定できます。いずれかのモジュール（ゾーン サーバ、ゾーン分割されていないファイバ チャネル ネーム サーバ（FCNS）、またはファブリック コンフィギュレーション サーバ（FCS）など）が FC-CT 管理クエリーを受信すると、FC 管理データベースに対する読み取り操作が実行されます。FC 管理データベースでデバイスが検出されると、付与されている権限に基づいて応答が送信されます。デバイスが FC 管理データベースにない場合は、各モジュールが拒否を送信します。FC 管理が無効な場合、各モジュールが各管理クエリーを処理します。

## 設定時の注意事項

FC 管理セキュリティ機能には、次の設定に関する注意事項があります。

- Cisco MDS スイッチで FC 管理セキュリティ機能が有効な場合、管理クエリーを送信するデバイスのポート ワールドワイド ネーム（pWWN）が FC 管理データベースに追加されていないと、サーバへのすべての管理クエリーが拒否されます。
- FC 管理を有効にすると、N_Port Virtualization（NPV）スイッチから N_Port Identifier Virtualization（NPIV）スイッチへの FC-CT 管理サーバ クエリーが拒否されます。FC 管理セキュリティ機能を有効にした後で、NPV スイッチのスイッチ ワールドワイド ネーム（sWWN）を NPIV スイッチの FC 管理データベースに追加することが推奨されます。

# Fibre Channel Common Transport クエリーの設定

FC-CT 管理セキュリティを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config terminal` | 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 | `switch(config)# fc-management enable`<br>`switch(config)#` | FC-CT 管理セキュリティを有効にします。 |
| ステップ 3 | `switch(config)# fc-management database vsan 1` | FC-CT 管理セキュリティ データベースを設定します。 |
| ステップ 4 | `switch(config-fc-mgmt)# pwwn 1:1:1:1:1:1:1:1 feature all operation both` | pWWN を FC 管理データベースに追加します。また、**pwwn** コマンドを設定するときには次に示すオプションのキーワードも使用できます。<br>• **fcs**：ファブリック コンフィギュレーション サーバに対する FC-CT クエリーを有効または無効にします。<br>• **fdmi**：FDMI に対する FC-CT クエリーを有効または無効にします。<br>• **unzoned-ns**：ゾーン分割されていないネーム サーバに対する FC-CT クエリーを有効または無効にします。<br>• **zone**：ゾーン サーバに対する FC-CT クエリーを有効または無効にします。 |
| ステップ 5 | `switch# show fc-managment database` | 設定された FC-CT 管理情報を表示します。 |

# Fibre Channel Common Transport 管理セキュリティの確認

**show fc-management database** コマンドは、設定されている FC-CT 管理セキュリティ機能の情報を表示します（例 10-1 を参照）。

*例 10-1 Fibre Channel Common Transport クエリーの表示*

```
switch# show fc-management database
-------------------------------------------------------------
VSAN PWWN FC-CT Permissions per FC services
-------------------------------------------------------------
1 01:01:01:01:01:01:01:01 Zone(RW), Unzoned-NS(RW), FCS(RW), FDMI(RW)
1 02:02:02:02:02:02:02:02 Zone(R), Unzoned-NS(R), FCS(R), FDMI(R)
1 03:03:03:03:03:03:03:03 Zone(W), Unzoned-NS(W), FCS(W), FDMI(W)
-------------------------------------------------------------
Total 3 entries
switch#
```

FC 管理セキュリティ機能が有効であるかどうかを確認するには、**show fc-management status** コマンドを使用します。

```
switch# show fc-management status
Mgmt Security Disabled
switch#
```

# デフォルト設定値

表 10-1 に、Cisco MDS 9000 ファミリ スイッチの FC 管理セキュリティ機能のデフォルト設定を示します。

*表 10-1　デフォルトの FC 管理設定*

| パラメータ | デフォルト |
|---|---|
| FC-management | 無効化 |

デフォルト設定値


# ファブリック バインディングの設定

この章では、Cisco MDS 9000 ファミリのディレクタおよびスイッチに組み込まれているファブリック バインディング機能について説明します。内容は次のとおりです。



## ファブリック バインディングの概要

ファブリック バインディング機能を使用すると、ファブリック バインディング設定で指定されたスイッチ間でだけ、ISL をイネーブルにできます。ファブリック バインディングは、VSAN 単位で設定します。

この機能を使用すると、不正なスイッチがファブリックに参加したり、現在のファブリック処理が中断されることがなくなります。この機能では、Exchange Fabric Membership Data（EFMD）プロトコルを使用することによって、ファブリック内の全スイッチで、許可されたスイッチのリストが同一になるようにします。

ここでは、次の内容について説明します。



### ライセンスの要件

ファブリック バインディングを使用するには、スイッチ上に MAINFRAME_PKG ライセンスまたは ENTERPRISE_PKG ライセンスのいずれかをインストールする必要があります。

ライセンス機能のサポートとインストールの詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。

# ポート セキュリティとファブリック バインディングの比較

ポート セキュリティとファブリック バインディングは、相互補完するように設定可能な、2 つの独立した機能です。表 11-1 では、2 つの機能を比較します。

*表 11-1　ファブリック バインディングとポート セキュリティの比較*

| ファブリック バインディング | ポート セキュリティ |
|---|---|
| 一連の sWWN および永続的ドメイン ID を使用します。 | pWWN/nWWN または fWWN/sWWN を使用します。 |
| スイッチ レベルでファブリックをバインドします。 | インターフェイス レベルでデバイスをバインドします。 |
| ファブリック バインディング データベースに格納された設定済み sWWN にだけ、ファブリックへの参加を許可します。 | 設定済みの一連のファイバ チャネル デバイスを SAN ポートに論理的に接続できます。WWN またはインターフェイス番号で識別されるスイッチ ポートは、同様に WWN で識別されるファイバ チャネル デバイス（ホストまたは別のスイッチ）に接続されます。これらの 2 つのデバイスをバインドすると、これらの 2 つのポートがグループ（リスト）にロックされます。 |
| VSAN 単位でアクティブ化する必要があります。 | VSAN 単位でアクティブ化する必要があります。 |
| ピア スイッチが接続されている物理ポートに関係なく、ファブリックに接続可能な特定のユーザ定義のスイッチを許可します。 | 別のデバイスを接続できる特定のユーザ定義の物理ポートを許可します。 |
| ログインしているスイッチについて学習しません。 | 学習モードがイネーブルの場合、ログインしているスイッチまたはデバイスについて学習します。 |
| CFS によって配信できず、ファブリック内の各スイッチで手動で設定する必要があります。 | CFS によって配信できます。 |

xE ポートのポート レベル チェックは、次のように実行されます。

- スイッチ ログインは、指定された VSAN にポート セキュリティ バインディングとファブリック バインディングの両方を使用します。
- バインディング検査は、ポート VSAN で次のように実行されます。
  - ポート VSAN での E ポート セキュリティ バインディング検査
  - 許可された各 VSAN での TE ポート セキュリティ バインディング検査

ポート セキュリティはファブリック バインディングを補完する関係にありますが、これらの機能は互いに独立していて、個別にイネーブルまたはディセーブルにできます。

# ファブリック バインディングの実行

ファブリック バインディングを実行するには、Switch World Wide Name（sWWN）を設定して、スイッチごとに xE ポート接続を指定します。ファブリック バインディング ポリシーは、ポートがアクティブになるたび、およびポートを起動しようとした場合に実行されます。FICON VSAN でファブリック バインディング機能を実行するには、すべての sWWN をスイッチに接続し、永続的ドメイン ID をファブリック バインディング アクティブ データベースに格納する必要があります。ファイバ チャネル VSAN では、sWWN だけが必要であり、ドメイン ID はオプションです。

（注）　ファブリック バインディングを使用するファイバ チャネル VSAN の全スイッチで、Cisco MDS SAN-OS リリース 3.0(1) および NX-OS リリース 4.1(1b) 以降を実行している必要があります。

# ファブリック バインディングの設定

ファブリック内の各スイッチにファブリック バインディングを設定する手順は、次のとおりです。

**ステップ 1**　ファブリック設定機能をイネーブルにします。

**ステップ 2**　ファブリックにアクセス可能なデバイスに sWWN のリスト、および対応するドメイン ID を設定します。

**ステップ 3**　ファブリック バインディング データベースをアクティブにします。

**ステップ 4**　ファブリック バインディング アクティブ データベースを、ファブリック バインディング コンフィギュレーション データベースにコピーします。

**ステップ 5**　ファブリック バインディング設定を保存します。

**ステップ 6**　ファブリック バインディング設定を確認します。

# ファブリック バインディングのイネーブル化

ファブリック バインディングに参加するファブリック内のスイッチごとに、ファブリック バインディング機能をイネーブルにする必要があります。デフォルトでは、この機能は Cisco MDS 9000 ファミリのすべてのスイッチでディセーブルになっています。ファブリック バインディング機能に関する設定および確認コマンドを使用できるのは、スイッチ上でファブリック バインディングがイネーブルな場合だけです。この設定をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。

参加させるスイッチのファブリック バインディングをイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| **ステップ 1** | `switch# config t` | 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** | `switch(config)# feature fabric-binding` | 現在のスイッチ上でファブリック バインディングをイネーブルにします。 |
| | `switch(config)# no feature fabric-binding` | 現在のスイッチ上でファブリック バインディングをディセーブル（デフォルト）にします。 |

ファブリック バインディングがイネーブルになっているスイッチのファブリック バインディング機能のステータスを表示するには、**show fabric-binding status** コマンドを発行します。

```
switch# show fabric-binding status
VSAN 1:Activated database
VSAN 4:No Active database
```

# スイッチ WWN リストの設定

ユーザ指定のファブリック バインディング リストには、ファブリック内の sWWN のリストが含まれています。リストにない sWWN、または許可リストで指定されているドメイン ID と異なるドメイン ID を使用する sWWN がファブリックへの参加を試みると、スイッチとファブリック間の ISL が VSAN 内で自動的に隔離され、スイッチはファブリックへの参加を拒否されます。

永続的ドメイン ID は sWWN とともに指定できます。FICON VSAN では、ドメイン ID 許可が必要です。FICON VSAN では、ドメインがスタティックに設定されているため、エンド デバイスによって、ファブリック内のすべてのスイッチにおけるドメイン ID の変更が拒否されます。ファイバ チャネル VSAN の場合には、ドメイン ID 許可は不要です。

FICON VSAN 用の sWWN およびドメイン ID のリストを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# fabric-binding database vsan 5`<br>`switch(config-fabric-binding)#` | 指定された VSAN のファブリック バインディング サブモードを開始します。 |
| | `switch(config)# no fabric-binding database vsan 5` | 指定された VSAN のファブリック バインディング データベースを削除します。 |
| ステップ 3 | `switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11 domain 102` | 設定したデータベース リストにスイッチの sWWN およびドメイン ID を追加します。 |
| | `switch(config-fabric-binding)# swwn 21:00:05:30:23:1a:11:03 domain 101` | 設定したデータベース リストに別のスイッチの sWWN およびドメイン ID を追加します。 |
| | `switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101` | 設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。 |
| ステップ 4 | `switch(config-fabric-binding)# exit`<br>`switch(config)#` | ファブリック バインディング サブモードを終了します。 |

ファイバ チャネル VSAN 用の sWWN および任意のドメイン ID のリストを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# fabric-binding database vsan 10`<br>`switch(config-fabric-binding)#` | 指定された VSAN のファブリック バインディング サブモードを開始します。 |
| | `switch(config)# no fabric-binding database vsan 10` | 指定された VSAN のファブリック バインディング データベースを削除します。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 3 | `switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11` | 設定したデータベース リストに全ドメインのスイッチの sWWN を追加します。 |
| | `switch(config-fabric-binding)# no swwn 21:00:05:30:23:11:11:11` | 設定したデータベース リストから全ドメインのスイッチの sWWN を削除します。 |
| | `switch(config-fabric-binding)# swwn 21:00:05:30:23:1a:11:03 domain 101` | 設定されたデータベース リストに、特定のドメイン ID 用の別のスイッチの sWWN を追加します。 |
| | `switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101` | 設定されたデータベース リストから、スイッチの sWWN およびドメイン ID を削除します。 |
| ステップ 4 | `switch(config-fabric-binding)# exit`<br>`switch(config)#` | ファブリック バインディング サブモードを終了します。 |

# ファブリック バインディングのアクティブ化

ファブリック バインディング機能によって、コンフィギュレーション データベース（config-database）およびアクティブ データベースが保持されます。コンフィギュレーション データベースは、実行された設定を収集する読み書きデータベースです。これらの設定を実行するには、データベースをアクティブにする必要があります。データベースがアクティブになると、アクティブ データベースにコンフィギュレーション データベースの内容が上書きされます。アクティブ データベースは、ログインを試みる各スイッチをチェックする読み取り専用データベースです。

デフォルトでは、ファブリック バインディング機能は非アクティブです。設定したデータベース内の既存のエントリがファブリックの現在の状態と矛盾していると、スイッチ上のファブリック バインディング データベースをアクティブにできません。たとえば、ログイン済みのスイッチの 1 つが、コンフィギュレーション データベースによってログインを拒否されている場合などです。これらの状態を強制的に上書きできます。

（注）　アクティベーションのあと、現在アクティブなデータベースに違反するログイン済みのスイッチは、ログアウトされ、ファブリック バインディング制限によってログインが拒否されたすべてのスイッチは再初期化されます。

ファブリック バインディング機能をアクティブにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# fabric-binding activate vsan 10` | 指定された VSAN のファブリック バインディング データベースをアクティブにします。 |
| | `switch(config)# no fabric-binding activate vsan 10` | 指定された VSAN のファブリック バインディング データベースを非アクティブにします。 |

## ファブリック バインディングの強制的なアクティベーション

上記のような矛盾が 1 つまたは複数発生したためにデータベースのアクティブ化が拒否された場合は、**force** オプションを使用してアクティブ化を継続できます。

ファブリック バインディング データベースを強制的にアクティブにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t`<br>`switch(config)#` | 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 | `switch(config)# fabric-binding activate vsan 3 force` | 指定した VSAN のファブリック バインディング データベースを強制的に（設定が許可されていない場合でも）アクティブにします。 |
| | `switch(config)# no fabric-binding activate vsan 3 force` | 元の設定状態、または（状態が設定されていない場合は）出荷時の設定に戻します。 |

# ファブリック バインディング設定の保存

ファブリック バインディング設定を保存すると、コンフィギュレーション データベースが実行コンフィギュレーションに保存されます。

**注意**　FICON がイネーブルである VSAN では、ファブリック バインディングをディセーブルにできません。

- アクティブ データベースからコンフィギュレーション データベースにコピーするには、**fabric-binding database copy vsan** コマンドを使用します。設定されたデータベースが空の場合、このコマンドは受け付けられません。

  `switch# fabric-binding database copy vsan 1`

- アクティブ データベースとコンフィギュレーション データベース間の違いを表示するには、**fabric-binding database diff active vsan** コマンドを使用します。このコマンドは、矛盾を解決する場合に使用できます。

  `switch# fabric-binding database diff active vsan 1`

- コンフィギュレーション データベースとアクティブ データベース間の違いに関する情報を表示するには、**fabric-binding database diff config vsan** コマンドを使用します。

  `switch# fabric-binding database diff config vsan 1`

- 再起動後にファブリック バインディング設定データベースを使用できるように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保存するには、**copy running-config startup-config** コマンドを使用します。

  `switch# copy running-config startup-config`

# ファブリック バインディング統計情報のクリア

指定された VSAN のファブリック バインディング データベースから既存の統計情報をすべてクリアするには、**clear fabric-binding statistics** コマンドを使用します。

```
switch# clear fabric-binding statistics vsan 1
```

# ファブリック バインディング データベースの削除

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no fabric-binding** コマンドを使用します。

```
switch(config)# no fabric-binding database vsan 10
```

# ファブリック バインディング設定の確認

**show** コマンドを使用して、このスイッチに設定されているすべてのファブリック バインディング情報を表示します（例 11-1 ～ 11-9 を参照）。

*例 11-1　設定したファブリック バインディング データベース情報の表示*

```
switch# show fabric-binding database
---------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
---------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
4      21:00:05:30:23:11:11:11         Any
4      21:00:05:30:23:1a:11:03         Any
4      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xea(234) [Local]
[Total 7 entries]
```

*例 11-2　アクティブ ファブリック バインディング情報の表示*

```
switch# show fabric-binding database active
---------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
---------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239) [Local]
```

*例 11-3　設定した VSAN 固有のファブリック バインディング情報の表示*

```
switch# show fabric-binding database vsan 4
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
4      21:00:05:30:23:11:11:11          Any
4      21:00:05:30:23:1a:11:03          Any
4      20:00:00:05:30:00:2a:1e   0xea(234) [Local]
[Total 2 entries]
```

*例 11-4　アクティブな VSAN 固有のファブリック バインディング情報の表示*

```
switch# show fabric-binding database active vsan 61
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239) [Local]
[Total 3 entries]
```

*例 11-5　ファブリック バインディング統計情報の表示*

```
switch# show fabric-binding statistics
Statistics For VSAN: 1
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 4
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 61
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 345
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 346
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
```

```
Statistics For VSAN: 347
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 348
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 789
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 790
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
```

*例 11-6　VSAN ごとのファブリック バインディング状態の表示*

```
switch# show fabric-binding status
VSAN 1 :Activated database
VSAN 4 :No Active database
VSAN 61 :Activated database
VSAN 345 :No Active database
VSAN 346 :No Active database
VSAN 347 :No Active database
VSAN 348 :No Active database
VSAN 789 :No Active database
VSAN 790 :No Active database
```

*例 11-7　ファブリック バインディング違反の表示*

```
switch# show fabric-binding violations
--------------------------------------------------------------------------------
VSAN Switch WWN [domain]     Last-Time              [Repeat count] Reason
--------------------------------------------------------------------------------
2    20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003   [2]    Domain mismatch
3    20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003      [2]    sWWN not found
4    20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003      [1]    Database mismatch
```

**(注)**　VSAN 3 では、sWWN 自体がリストにありません。VSAN 2 では、sWWN がリストで見つかりましたが、ドメイン ID が一致しませんでした。

*例 11-8　EFMD 統計情報の表示*

```
switch# show fabric-binding efmd statistics

EFMD Protocol Statistics for VSAN 1
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0

EFMD Protocol Statistics for VSAN 61
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

*例 11-9　指定した VSAN の EFMD 統計情報の表示*

```
switch# show fabric-binding efmd statistics vsan 4

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

# デフォルト設定

表 11-2 に、ファブリック バインディング機能のデフォルト設定を示します。

*表 11-2　ファブリック バインディングのデフォルト設定*

| パラメータ | デフォルト |
|---|---|
| ファブリック バインディング | ディセーブル |

CHAPTER 12

# Cisco TrustSec ファイバ チャネル リンク暗号化の設定

この章では、Cisco TrustSec ファイバ チャネル（FC）リンクの暗号化機能の概要を示し、スイッチ間にリンク レベルの暗号化を設定する方法について説明します。

この章は、次の項目を取り上げます。



## Cisco TrustSec FC リンク暗号化に関する用語

この章では、次に示す Cisco TrustSec FC リンク暗号化関連の用語を使用します。

- ガロア カウンタ モード（GCM）：機密保持とデータ発信元認証を行う操作のブロック暗号モード。
- ガロア メッセージ認証コード（GMAC）：データ発信元認証だけを行う操作のブロック暗号モード。GCM の認証限定バリアントです。
- セキュリティ アソシエーション（SA）：セキュリティ認定証を処理し、それらの認定証をスイッチ間にどのように伝播するかを制御する接続。SA には、salt やキーなどのパラメータが含まれます。
- キー：フレームの暗号化および復号化に使用する 128 ビットの 16 進数字列。デフォルト値は 0 です。
- Salt：暗号化および復号化の際に使用する 32 ビットの 16 進数字列。適切な通信を行うには、接続の両側に同じ salt を設定する必要があります。デフォルト値は 0 です。
- セキュリティ パラメータ インデックス（SPI）番号：ハードウェアに設定される SA を識別する 32 ビットの数字。有効な範囲は 256 ～ 65536 です。

# AES 暗号化のサポート

Advanced Encryption Standard（AES）は、ハイ レベルなセキュリティを実現する対称暗号アルゴリズムであり、さまざまなキー サイズを受け入れることができます。

Cisco TrustSec FC リンク暗号化機能は、セキュリティ暗号用に 128 ビットの AES をサポートし、インターフェイスに AES-GCM または AES-GMAC のいずれかをイネーブルにします。AES-GCM モードではフレームの暗号化と認証が可能であり、AES-GMAC では 2 つのピア間で送受信されるフレームの認証だけが可能です。

# Cisco TrustSec FC リンク暗号化の概要

Cisco TrustSec FC リンク暗号化は、Fibre Channel-Security Protocol（FC-SP）の拡張機能であり、既存の FC-SP アーキテクチャを使用してトランザクションの整合性と機密保持を実現します。セキュリティを保ち、望ましくないトラフィック傍受を防止するため、ピア認証機能に暗号化が追加されました。ピア認証は、Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（DHCHAP）プロトコルを使用した FC-SP 標準に従って実装されます。

（注）　Cisco TrustSec FC リンク暗号化は現在、Cisco MDS スイッチ間に限りサポートされています。この機能は、カプセル化セキュリティ ペイロード（ESP）プロトコルをサポートしていないソフトウェア バージョンにダウングレードするとサポートされなくなります。

この項では、次のトピックについて取り上げます。



## サポートされるモジュール

次のモジュールは、Cisco TrustSec FC リンク暗号化機能に対応しています。

- 2/4/8/10/16 Gbps 48 ポート アドバンスド ファイバ チャネル モジュール（DS-X9448-768K9）
- 8 Gbps 32 ポート拡張ファイバ チャネル スイッチング モジュール（DS-X9232-256K9）
- 8 Gbps 48 ポート拡張ファイバ チャネル スイッチング モジュール（DS-X9248-256K9）
- 1/2/4/8 Gbps 24 ポート ファイバ チャネル スイッチング モジュール（DS-X9224-96K9）
- 1/2/4/8 Gbps 48 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-96K9）
- 1/2/4/8 Gbps 4/44 ポート ファイバ チャネル スイッチング モジュール（DS-X9248-48K9）
- 2/4/8/10/16 Gbps 96 ポート ファイバ チャネル スイッチング モジュール（DS-C9396S-K9）
- 24/10 ポート SAN 拡張モジュール（DS-X9334-K9）

（注）　24/10 ポート SAN 拡張モジュール（DS-X9334-K9）は、Cisco MDS NX-OS リリース 7.3(0)DY(1) 以降の Cisco MDS 9700 シリーズ ディレクタでサポートされています。

# Cisco TrustSec FC リンク暗号化のイネーブル化

Cisco MDS 9000 ファミリのすべてのスイッチの FC-SP 機能と Cisco TrustSec FC リンク暗号化機能は、デフォルトでディセーブルになります。

ファブリック認証および暗号化用のコンフィギュレーション コマンドおよび確認コマンドにアクセスするには、FC-SP 機能をイネーブルにする必要があります。この機能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。

Cisco MDS スイッチの FC-SP をイネーブルにする手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# feature fcsp` | FC-SP 機能をイネーブルにします。 |
| | `switch(config)# no feature fcsp` | このスイッチの FC-SP 機能をディセーブル（デフォルト）にします。 |

Cisco TrustSec FC リンク暗号化機能を設定するには、ENTERPRISE_PKG ライセンスが必要です。詳細については、『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照してください。

# セキュリティ アソシエーションの設定

スイッチ間で暗号化を実行するには、セキュリティ アソシエーション（SA）を設定する必要があります。暗号化を実行するには、管理者があらかじめ手動で SA を設定する必要があります。SA には、キーや salt など、暗号化に必要なパラメータが含まれます。スイッチには、最大 2000 の SA を設定できます。

2 台のスイッチ間の SA 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 | `switch# config t` | 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 | `switch(config)# fcsp esp sa` *spi_number* | SA を設定するための SA サブモードを開始します。*spi_number* の範囲は 256 ～ 65536 です。 |
| ステップ 3 | `switch(config)# no fcsp esp sa` *spi_number* | スイッチ間の SA を削除します。[1] |

1. 指定した SA が現在ポートにプログラムされている場合、このコマンドは SA が使用中であることを伝えるエラーを返します。

どのポートが SA を使用しているかを調べるには、**show running-config fcsp** コマンドを使用します。「実行中のシステム情報の表示」セクション（12-281 ページ）を参照してください。

（注）　Cisco TrustSec FC リンク暗号化は現在、on モードと off モードの DHCHAP だけでサポートされています。

# セキュリティ アソシエーション パラメータの設定

キーや salt などの SA パラメータを設定する手順は、次のとおりです。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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<br>ステップ 3 | `switch(config)# fcsp esp sa spi_number` | SA を設定するための SA サブモードを開始します。<br>*spi_number* の範囲は 256 ～ 65536 です。 |
| ステップ 4 | `switch(config-sa)# key key` | SA のキーを設定します。*key* の最大サイズは 34 です。 |
| ステップ 5 | `switch(config-sa)# no key key` | SA からキーを削除します。 |
| ステップ 6 | `switch(config-sa)# salt salt` | SA の salt を設定します。有効な範囲は 0x0 ～ 0xffffffff です。 |
| ステップ 7 | `switch(config-sa)# no salt salt` | SA の salt が削除されます。 |

# ESP の設定

この項では、次のトピックについて取り上げます。

- 入力および出力ポートでの ESP の設定（12-278 ページ）
- ESP モードの設定（12-279 ページ）

## 入力および出力ポートでの ESP の設定

SA が作成されると、ポートにカプセル化セキュリティ プロトコル（ESP）を設定する必要があります。同等のネットワーク間でパケットを暗号化および復号化する出力および入力ポートを指定する必要があります。出力 SA はどのキーまたはパラメータがスイッチから出るパケットの暗号化に使用されるかを指定します。入力 SA はどのキーまたはパラメータが特定のポートに入るパケットの復号化に使用されるかを指定します。

この項では、次のトピックについて取り上げます。

- 入力ポートでの ESP の設定（12-278 ページ）
- 出力ポートでの ESP の設定（12-279 ページ）

### 入力ポートでの ESP の設定

入力のハードウェアに SA を設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# interface fc x/y` | スロット *x* のポート *y* に FC インターフェイスを設定します。<br>**（注）** ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。 |
| ステップ 3 | `switch(config-if)# fcsp esp manual` | ESP コンフィギュレーション サブモードを開始します。 |
| ステップ 4 | `switch(config-if-esp)# ingress-sa spi_number` | 入力のハードウェアに SA を設定します。 |
| ステップ 5 | `switch (config-if-esp)# no ingress-sa spi_number` | 入力のハードウェアから SA を削除します。[1] |

1. SA が入力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

### 出力ポートでの ESP の設定

出力のハードウェアに SA を設定するには、次の手順を実行します。

| | | |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# interface fc x/y` | スロット *x* のポート *y* に FC インターフェイスを設定します。<br>(注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。 |
| ステップ 3 | `switch(config-if)# fcsp esp manual` | ESP コンフィギュレーション サブモードを開始します。 |
| ステップ 4 | `switch(config-if-esp)# egress-sa spi_number` | 出力のハードウェアに SA を設定します。 |
| ステップ 5 | `switch(config-if)# no fcsp esp manual` | 入力と出力のハードウェアから SA を削除します。[1] |

1. SA が出力ポートで設定されていない場合、このコマンドを実行すると、エラー メッセージが返されます。

(注)　インターフェイスの入力および出力ハードウェアに SA を適用するには、インターフェイスが admin shut モードである必要があります。

## ESP モードの設定

GCM としてポートがメッセージ認証と暗号化を有効にする、または GMAC としてポートがメッセージ認証を有効にするように、ESP を設定します。

デフォルトの ESP モードは AES-GCM です。

この項では、次のトピックについて取り上げます。

- AES-GCM の設定（12-279 ページ）
- AES-GMAC の設定（12-280 ページ）

### AES-GCM の設定

AES-GCM モードを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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<br>ステップ 3<br>ステップ 4 | `switch(config)# interface fc x/y` | スロット *x* のポート *y* に FC インターフェイスを設定します。<br>(注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。 |
| | `switch(config-if)# fcsp esp manual` | 各ポートの ESP を設定するために ESP コンフィギュレーション サブモードを開始します。 |
| ステップ 5 | `switch(config-if-esp)# mode gcm` | インターフェイスの GCM モードを設定します。 |

### AES-GMAC の設定

AES-GMAC モードを設定するには、次の手順を実行します。

| | コマンド | 目的 |
|---|---|---|
| ステップ 1 | `switch# config t` | 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 | `switch(config)# interface fc x/y` | スロット *x* のポート *y* に FC インターフェイスを設定します。<br>(注)　ポート チャネルを選択すると、ポート チャネルのすべてのメンバの設定が適用されます。 |
| ステップ 3 | `switch(config-if)# fcsp esp manual` | 各ポートの ESP を設定するために ESP コンフィギュレーション サブモードを開始します。 |
| ステップ 4 | `switch(config-if-esp)# mode gmac` | インターフェイスの GMAC モードを設定します。 |
| ステップ 5 | `switch(config-if-esp)# no mode gmac` | GMAC モードをインターフェイスから削除し、デフォルトの AES-GCM モードを適用します。 |

(注)　ESP モードが設定されるのは、入力または出力ハードウェアに SA が設定されている場合だけです。SA が設定されていない場合は、ESP がオフになり、カプセル化は行われません。

(注)　ポートを設定した後で ESP モードを変更した場合は、変更がシームレスでないため、常にポートのフラップが必要です。ただし、設定は拒否されません。

(注)　FC-SP ポート モードが有効で、ESP 対応のスイッチまたはブレードで使用可能な ISL だけが表示されます。

(注)　選択した ISL がイネーブルであれば、既存の ESP 設定を変更できます。

# Cisco TrustSec FC リンク暗号化情報の表示

Fabric Manager または Device Manager では、**show** コマンドを使用して Cisco TrustSec FC リンク暗号化機能の情報を表示できます。

この項では、次のトピックについて取り上げます。


- FC-SP のインターフェイス情報の表示（12-281 ページ）
- 実行中のシステム情報の表示（12-281 ページ）
- FC-SP インターフェイス統計情報の表示（12-281 ページ）

# FC-SP のインターフェイス情報の表示

**show fcsp interface** コマンドを使用して、特定のインターフェイスのすべての FC-SP 関連情報を表示します。

```
switch# show fcsp interface fc7/41

fc7/41:
        fcsp authentication mode:SEC_MODE_OFF
        ESP is enabled
        configured mode is: GCM
        programmed ingress SA: 300, 303
        programmed egress SA: 300
        Status:FC-SP protocol in progress
```

# 実行中のシステム情報の表示

FC-SP に関連するすべての実行時の情報を表示するには、**show running-config fcsp** コマンドを使用します。ESP および設定されたインターフェイスに関するすべての詳細が表示されます。どのポートが SA を使用しているか調べるには、次のコマンドを使用します。

```
switch# show running-config fcsp
version 4.1(2)
feature fcsp
fcsp esp sa 300
  key 0x00000000000000000000000000123456
  salt 0x123456
fcsp esp sa 301
  key 0x00000000000000000000000000123456
  salt 0x1234567
fcsp esp sa 302
  key 0x00000000000000000000000000123456
  salt 0x123456

interface fc8/48
  fcsp off
  fcsp esp manual
    ingress-sa 300
    ingress-sa 301
    egress-sa 300
```

# FC-SP インターフェイス統計情報の表示

インターフェイスに対し DHCHAP と ESP に関連するすべての統計情報を表示するには、**show fcsp interface statistics** コマンドを使用します。示されている ESP 統計情報はポート ASIC でサポートされている ESP により異なります。

```
switch# show fcsp interface fc3/31 statistics

fc7/41:
       fcsp authentication mode:SEC_MODE_ON
        ESP is enabled
        configured mode is: GMAC
        programmed ingress SA: 256, 257
        programmed egress SA: 256
        Status:Successfully authenticated
```

```
Authenticated using local password database
 Statistics:
 FC-SP Authentication Succeeded:17
 FC-SP Authentication Failed:3
 FC-SP Authentication Bypassed:0
 FC-SP ESP SPI Mismatched frames:0
 FC-SP ESP Auth failed frames:0
```

# Cisco TrustSec FC リンク暗号化のベスト プラクティス

ベスト プラクティスとは、Cisco TrustSec FC リンク暗号化を適切に動作させるための推奨手順です。

この項では、次のトピックについて取り上げます。


- 一般的なベスト プラクティス（12-282 ページ）
- キーの変更に関するベスト プラクティス（12-282 ページ）


## 一般的なベスト プラクティス

ここでは、Cisco TrustSec FC リンク暗号化に関する一般的なベスト プラクティスを示します。

- Cisco TrustSec FC リンク暗号化が MDS スイッチ間だけでイネーブルであることを確認します。この機能は、E ポートまたは ISL だけでサポートされており、MDS 以外のスイッチを使用している場合はエラーが発生します。
- 接続にかかわるピアの設定が同一であることを確認します。設定に相違があると、「port re-init limit exceeded」というエラー メッセージが表示されます。
- スイッチ インターフェイスの入力および出力ハードウェアに SA を適用する前に、インターフェイスが admin shut モードであることを確認します。

## キーの変更に関するベスト プラクティス

入力および出力ポートに SA を適用した後は、キーの設定を定期的に変更してください。トラフィックの中断を避けるには、キーを順番に変更する必要があります。

例として、2 つのスイッチ、Switch1 と Switch2 の間に作成されたセキュリティ アソシエーションについて考えます。SA は、次の例に示すように、入力および出力ポートに設定されます。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 256
switch(config-if)# egress-sa 256
```

これらのスイッチのキーを変更するには、次の手順を実行します。

**ステップ 1**　Switch1 と Switch2 に新しい SA を追加します。

```
switch# config t
switch(config)# fcsp esp sa 257
switch(config-sa)# key 0xAC9EF8BC8DB2DBD2008D184F794E0C38
switch(config-sa)# salt 0x1234
```

ステップ 2　Switch1 に入力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
```

ステップ 3　Switch2 に入出力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# ingress-sa 257
switch(config-if)# egress-sa 257
```

ステップ 4　Switch1 に出力 SA を設定します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# egress-sa 257
```

ステップ 5　両方のスイッチから以前に設定された入力 SA を削除します。

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)# fcsp esp manual
switch(config-if)# no ingress-sa 256
```