Cisco Fabric Manager セキュリティ コンフィギュレーション ガイド

Cisco Fabric Manager Security Configuration Guide

Cisco MDS NX-OS リリース 4.2(1)
2009 年 8 月

Text Part Number: OL-19536-01-J、Cisco MDS NX-OS リリース 4.2(1)

【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 Fabric Manager セキュリティ コンフィギュレーション ガイド

CONTENTS

新機能および変更された機能

Cisco MDS NX-OS Release 4.2(1) より、新機能に固有のコンフィギュレーション ガイドでソフトウェア設定に関する次の情報を入手できます。

- システム管理
- インターフェイス
- ファブリック
- Quality of service（QoS）
- セキュリティ
- IP サービス
- ハイ アベイラビリティおよび冗長性

これらの新しいマニュアルの情報は、以前は『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』に記載されていました。これらのコンフィギュレーション ガイドは引き続き Cisco.com で入手できます。MDS NX-OS Release 4.2(1) よりも前のすべてのソフトウェア リリースには、これらのマニュアルを使用してください。各マニュアルでは、特定のリリースで導入された機能や使用可能な機能を扱っています。ご使用のスイッチにインストールしたソフトウェアに対応するコンフィギュレーション ガイドを選択し、表示してください。

『*Cisco MDS 9000 Family CLI Configuration Guide*』および『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』の一部の情報は現在、Nexus オペレーティング システムを実行する製品間に共通の次のマニュアルに記載されています。

- 『*Cisco NX-OS Licensing Guide*』: ライセンス モデルと機能ライセンスについて説明します。
- 『*Cisco NX-OS Fundamentals Guide*』: スイッチ セットアップ ユーティリティについて説明し、一般的な Command Line Interface（CLI; コマンドライン インターフェイス）、ファイル システム、および設定情報を示します。

ドキュメント タイトルの全リストについては、「はじめに」にある「関連資料」のリストを参照してください。

Cisco MDS NX-OS Release 4.2(x) の追加情報については、次に示すシスコ システムズの Web サイトで入手可能な『*Cisco MDS 9000 Family Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps5989/prod_release_notes_list.htm

このマニュアルについて

新規の『*Cisco Fabric Manager Security Configuration Guide*』の情報は、以前は『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』のパート 5「Security」に記載されていました。

表 1 に、MDS NX-OS Release 4.2(1) 以降のこのマニュアルに関する新機能および変更された機能を示します。

表 1　Cisco MDS NX-OS Release 4.2(x) の新機能および変更された機能

機能	新規または変更されたトピック	変更が加えられたリリース	説明されている箇所
TrustSec FC LE	MDS スイッチ間のリンクレベルの暗号化に関する情報を追加しました。	4.2(1)	第 11 章「Cisco TrustSec ファイバ チャネル リンク暗号化の設定」 第 8 章「FC-SP および DHCHAP の設定」
ロール サポートのない Terminal Access Controller Access Control System Plus（TACACS+）を使用したコマンドごとの許可	TACACS+ サーバでのユーザの許可に関する情報を追加しました。	4.2(1)	第 4 章「RADIUS および TACACS+ の設定」
MSCHAPv2	Remote Authentication Dial-In User Service（RADIUS）サーバでの認証に関する MSCHAP バージョン 2 の情報を追加しました。	4.2(1)	第 4 章「RADIUS および TACACS+ の設定」

はじめに

ここでは、『*Cisco Fabric Manager 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。さらに、関連資料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、Cisco MDS 9000 ファミリのマルチレイヤ 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としています。

マニュアルの構成

このマニュアルは、次のように構成されています。

章	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	Federal Information Processing Standards（FIPS; 連邦情報処理標準）に関する設定上の注意事項と、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施する方法を説明します。
第 3 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 4 章	RADIUS および TACACS+ 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 Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）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。

章	タイトル	説明
第 5 章	IPv4 および IPv6 のアクセス制御リストの設定	Internet Protocol version 4（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 Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）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	CA およびデジタル証明書の設定	Certificate Authority（CA; 認証局）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い方について説明します。
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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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	Diffie-Hellman（DH）Challenge Handshake Authentication Protocol（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の認証を可能にする Fibre Channel Security Protocol（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	ファブリック バインディングの設定	特定のスイッチ間だけで Inter-Switch Link（ISL; スイッチ間リンク）をイネーブルにする、VSAN のファブリック バインディング セキュリティ機能について説明します。
第 11 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 Small Computer Systems Interface over IP（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*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

関連資料

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 マニュアルを検索するには、次の URL にアクセスし、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*』

準拠規格および安全性情報

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

互換性情報

- 『*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 インストレーション

- 『*Cisco MDS 9500 Series Hardware Installation Guide*』
- 『*Cisco MDS 9200 Series Hardware Installation Guide*』
- 『*Cisco MDS 9100 Series Hardware Installation 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とアップグレード

- 『*Cisco MDS 9000 NX-OS Release 4.1(x) and 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 Family NX-OS Inter-VSAN Routing Configuration Guide*』

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*』

Intelligent Storage Networking Services Configuration Guides

- 『*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リファレンス

- 『*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、Storage Area Network（SAN; ストレージ エリア ネットワーク）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。

この章の内容は、次のとおりです。

FIPS

Federal Information Processing Standards（FIPS; 連邦情報処理標準規格）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「ユーザ ロールおよび共通ロールの設定」を参照してください。

RADIUS および TACACS+

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）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 ではセキュリティ プロトコルを使用して、そのセキュリティ機能を管理します。ルータまたはアクセス サーバをネットワーク 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：Command-Line Interface（CLI; コマンドライン インターフェイス）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 Simple Network Management Protocol（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 ルータで稼動し、認証要求を、すべてのユーザ認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに送信します。
- 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動する TACACS+ デーモン上のデータベースに保持されます。TACACS+ は、独立したモジュラ型の認証、許可、およびアカウンティング機能を実現します。

RADIUS および TACACS+ については、第 4 章「RADIUS および TACACS+ の設定」を参照してください。

IP ACL

IP Access Control List（ACL; アクセス コントロール リスト）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 の設定については、第 5 章「IPv4 および IPv6 のアクセス制御リストの設定」を参照してください。

PKI

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）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 Security Protocol（IPSec; IP セキュリティ プロトコル）、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）、および Secure Shell（SSH; セキュア シェル）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「CA 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 DH 交換を組み合わせたものです。

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。

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 Inter-Switch Link（ISL; スイッチ間リンク）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 10 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 11 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。

CHAPTER 2

FIPS の設定

Federal Information Processing Standards（FIPS; 連邦情報処理標準規格）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。

この章の内容は、次のとおりです。

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 8 文字以上の長さで作成します。
- Telnet をディセーブルにします。ユーザのログインには Secure Shell（SSH; セキュア シェル）だけを使用します。
- RADIUS/TACACS+ によるリモート認証をディセーブルにします。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ます。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、認証用に Secure Hash Algorithm（SHA; セキュア ハッシュ アルゴリズム）およびプライバシー用に Advanced Encryption Standard（AES; 高度暗号化規格）/Triple Data Encryption Standard（3DES; トリプル データ暗号化規格）を設定する必要があります。
- Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）をディセーブルにします。

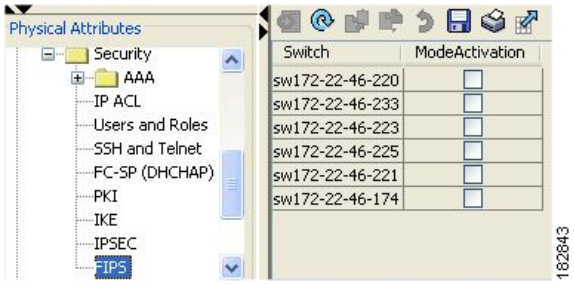
- 認証用 Message Digest 5（MD5; メッセージ ダイジェスト 5）または暗号用 DES のいずれかを含む、すべての Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを削除します。認証用に SHA、暗号用に 3DES/AES を使用するようにポリシーを修正します。
- SSH サーバ の RSA1 キーペアすべてを削除します。

FIPS モードのイネーブル化

Fabric Manager を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] を展開します。[Security] を展開し、[FIPS] を選択します。[Information] ペインに FIPS 有効設定の詳細が表示されます（図 2-1 を参照）。

図 2-1　Fabric Manager での FIPS 有効設定



ステップ 2　FIPS モードをイネーブルにするスイッチの [ModeActivation] チェックボックスをオンにします。

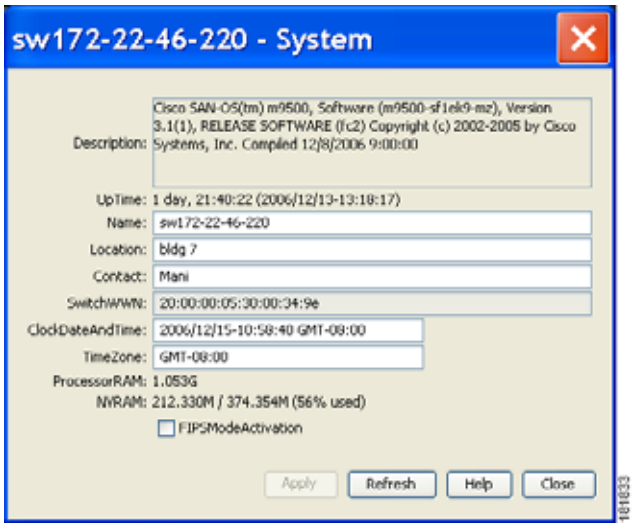
ステップ 3　[Apply Changes] アイコンをクリックして、変更内容をコミットして割り当てます。

ステップ 4　保存していない変更を廃棄するには、[Undo Changes] アイコンをクリックします。

Device Manager を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical] > [System] を選択するか、右クリックして [Configure] を選択します。[System] ダイアログボックスが表示されます（図 2-2 を参照）。

図 2-2　[System] ダイアログボックス



ステップ 2　[FIPSModeActivation] チェックボックスをオンにして、選択したスイッチの FIPS モードをイネーブルにします。

ステップ 3　[Apply] ボタンをクリックして、変更内容を保存します。

ステップ 4　[Close] ボタンをクリックして、ダイアログボックスを閉じます。

FIPS のセルフテスト

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 モードがイネーブルであ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 モードをイネーブルにすると、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。

Known-Answer Test（KAT; 既知解テスト）を使用すると、暗号アルゴリズムは正しい出力があらかじめわかってい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：このテストでは公開キーと秘密キーの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。

これらのテストはいずれも、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。

CHAPTER 3

ユーザ ロールおよび共通ロールの設定

Cisco MDS 9000 ファミリのすべてのスイッチで、Command Line Interface（CLI; コマンドライン インターフェイス）および Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）に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。

ユーザ、パスワード、ロールは CLI ユーザおよび SNMP ユーザ全員が同じものを使用します。CLI を利用して設定したユーザは SNMP を利用して（たとえば Fabric Manager や Device Manager）、スイッチにアクセスできますし、その逆も可能です。

この章の内容は、次のとおりです。

ロール ベースの許可

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。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。

コマンドを実行したり、コマンドを完了させたり、コンテキスト ヘルプを取得したりする場合に、コマンドへのアクセス権限があれば、操作を継続できます。

ここで説明する内容は、次のとおりです。

ロールについて

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用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用コマンドと 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、その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いて、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、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。

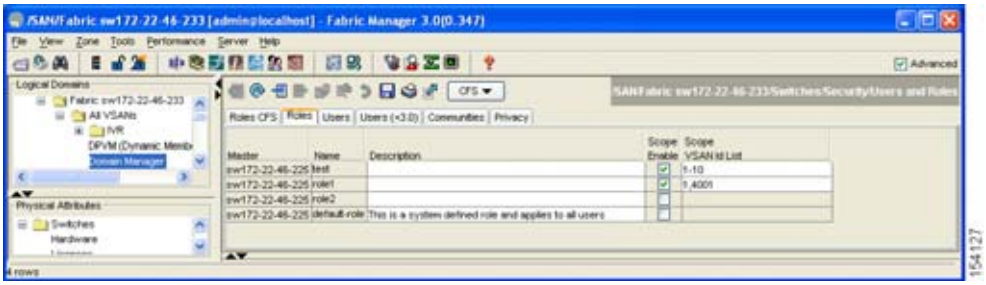
ロールとプロファイルの設定

Fabric Manager を使用して追加のロールを作成する、または既存ロールのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

図 3-1 のとおりの情報が表示されます。

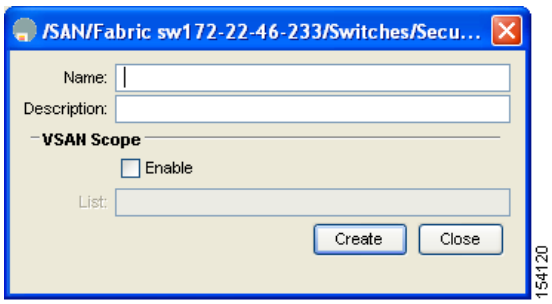
図 3-1　[Users and Roles] 画面の [Roles] タブ



ステップ 2　Fabric Manager でロールを作成するために [Create Row] アイコンをクリックします。

図 3-2 の [Create Roles] ダイアログボックスが表示されます。

図 3-2　[Create Roles] ダイアログボックス



ステップ 3　ロールの設定先のスイッチを選択します。

ステップ 4　[Name] フィールドに、ロールの名前を入力します。

ステップ 5　[Description] フィールドにロールの説明を入力します。

ステップ 6　（任意）[Enable] チェックボックスをオンにして Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）範囲をイネーブルにし、このロールを適用できる VSAN のリストを [Scope] フィールドに入力します。

ステップ 7　ロールを作成するには、[Create] ボタンをクリックします。共通ロールを作成せずに [Roles - Create] ダイアログボックスを閉じるには、[Close] ボタンをクリックします。

（注）　Device Manager では、スイッチのビューを表示するために、Device Manager に必要な 6 つのロールが自動的に作成されます。作成されるロールは、**system**、**snmp**、**module**、**interface**、**hardware**、および **environment** です。

共通ロールの削除

Fabric Manager を使用して共通ロールを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　削除するロールをクリックします。

ステップ 3　[Delete Row] アイコンをクリックして共通ロールを削除します。

ステップ 4　[Yes] をクリックして削除を確認するか、[No] でキャンセルします。

VSAN ポリシーの概要

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 ポリシーも許可されるため、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、そのあとでその設定を許可に設定、または適切な VSAN に設定します。

（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、これらのユーザが、ファブリックのコア テクノロジー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

Fabric Manager で既存のロールの VSAN ポリシーを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles] タブをクリックします。

ステップ 2　[Scope Enable] チェックボックスをオンにして、VSAN 範囲をイネーブルにし、ロールの VSAN 範囲を制限します。

ステップ 3　[Scope VSAN Id List] フィールドに、ロールを制限する VSAN のリストを入力します。

ステップ 4　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

各ロールに対する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。これらのルールは、許可される CLI コマンドを反映します。ユーザ側で指定するルール番号によって、ルールが適用される順序が決まります。たとえば、rule 1 のあとに rule 2 が適用され、rule 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 がすべての **show** CLI コマンドの実行を許可されている場合、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** CLI コマンドの出力を表示できません。

ルールは、特定のロールにより実行できる操作を指定します。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）、CLI コマンド タイプ（たとえば **config**、**clear**、**show**、**exec**、**debug**）、および任意の機能名（たとえば FSPF、zone、VSAN、fcping、interface など）です。

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

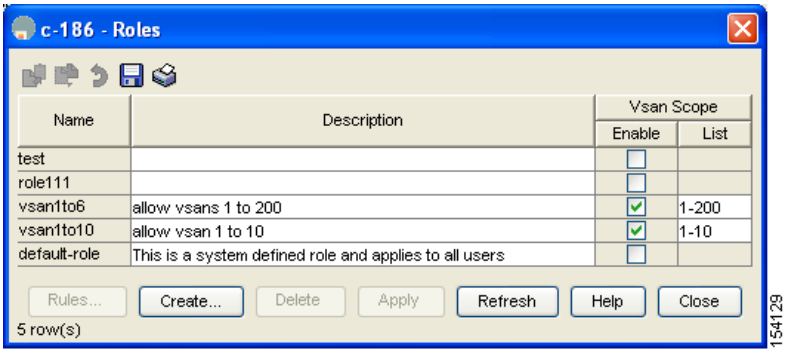
ルールの修正

Device Manager で既存のロールのルールを修正する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] をクリックします。

ステップ 2　[Common Roles] ダイアログボックスが表示されます（図 3-3 を参照）。

図 3-3　Device Manager の [Common Roles] ダイアログボックス

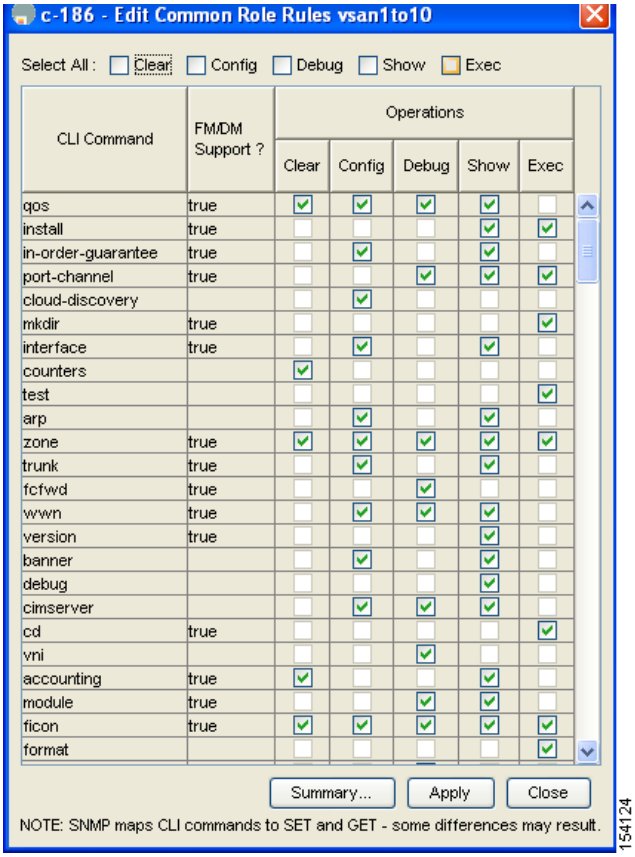


ステップ 3　ルールを編集するロールをクリックします。

ステップ 4　[Rules] ボタンをクリックして、そのロールのルールを表示します。

[Rules] ダイアログボックスが表示されます（図 3-4 を参照）。表示されるまでに数分かかる場合があります。

図 3-4　[Edit Common Role Rules] ダイアログボックス



ステップ 5　共通ロールについて、イネーブルまたはディセーブルにするルールを編集します。

ステップ 6　新しいルールを適用するには、[Apply] ボタンをクリックして [Rules] ダイアログボックスを閉じます。ルールを適用せずに [Rules] ダイアログボックスを閉じるには、[Close] ボタンをクリックします。

---

rule 1 が最初に適用され、たとえば sangroup ユーザがすべての **config** CLI コマンドにアクセスすることが許可されます。次に rule 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** CLI 設定コマンドを除く、他のすべての **config** CLI 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設定コマンドの実行を許可することになります。

ロールベース情報の表示

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い場合は、すべてのロールが表示されます。

Device Manager を使用して特定のロールのルールを表示する手順は、次のとおりです。

ステップ 1　[Security] > [Roles] をクリックします。

[Roles] ダイアログボックスが表示されます。

ステップ 2　ロール名を選択して [Rules] ボタンをクリックします。

[Rules] ダイアログボックスが表示されます。

ステップ 3　このロールに設定されたルールをまとめて表示するには [Summary] ボタンをクリックします。

ロールの配布

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（第 7 章「CFS インフラストラクチャの使用」を参照）。

次の設定内容が配布されます。

- 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

ここで説明する内容は、次のとおりです。

- 「ロール データベースについて」（P.3-7）
- 「ファブリックのロック」（P.3-8）
- 「変更のコミット」（P.3-8）
- 「変更の廃棄」（P.3-9）
- 「配信のイネーブル化」（P.3-9）
- 「セッションの消去」（P.3-9）
- 「データベース マージに関する注意事項」（P.3-10）
- 「配布がイネーブルのときのロールの表示」（P.3-10）

ロール データベースについて

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ランニング データベースです。

- ペンディング データベース：直後の設定変更はペンディング データベースに保存されます。設定を修正した場合は、ペンディング データベースの変更内容をコミットまたは廃棄する必要があります。この処理の実行中は、ファブリックはロックされた状態になります。ペンディング 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。

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がペンディング データベースを作成し、ファブリック全体の機能をロックします。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。

- 他のユーザは、この機能の設定を変更できなくなります。
- 最初の変更にともなって、コンフィギュレーション データベースの複製がペンディング データベースになります。

変更のコミット

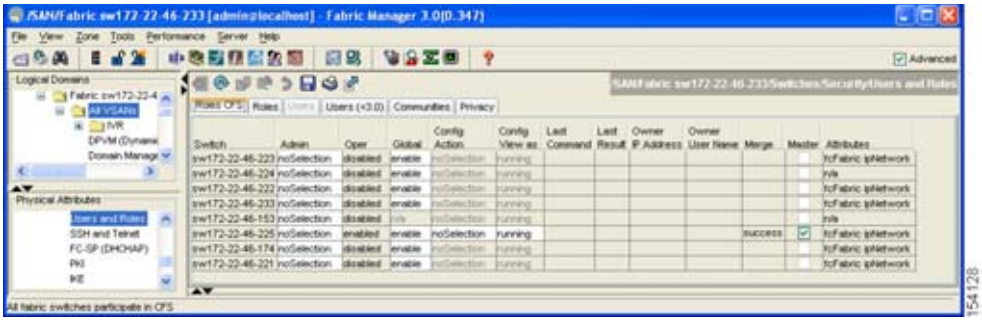
ペンディング データベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、ペンディング データベースは消去されます。

Fabric Manager を使用してロールベース設定変更をコミットする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

図 3-5 のような画面が表示されます。

図 3-5　[Roles CFS] タブ



ステップ 2　[Global] ドロップダウン メニューを [enable] に設定して CFS をイネーブルにします。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ステップ 4　[Config Action] ドロップダウン メニューを [commit] に設定して、CFS を使用してこのロールをコミットします。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

変更の廃棄

ペンディング データベースに行った変更を廃棄（abort）すると、コンフィギュレーション データベースは影響を受けず、ロックが解除されます。

Fabric Manager を使用してロールベース設定変更を廃棄する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Config Action] ドロップダウン メニューを [abort] に設定して、コミットされていないすべての変更を廃棄します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

配信のイネーブル化

Fabric Manager を使用してロールベース設定の配布をイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Global] ドロップダウン メニューを [enable] に設定して CFS 配布をイネーブルにします。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

セッションの消去

Fabric Manager を使用して強制的にファブリック内の既存のロール セッションを消去する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします。

ステップ 2　[Config Action] ドロップダウン メニューを [clear] に設定して、ペンディング データベースを消去します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（注）　セッションを消去すると、ペンディング データベース内のすべての変更が失われます。

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ます。
- いずれのスイッチのロール データベースも、必ず必要なデータベースに編集してからコミットします。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。

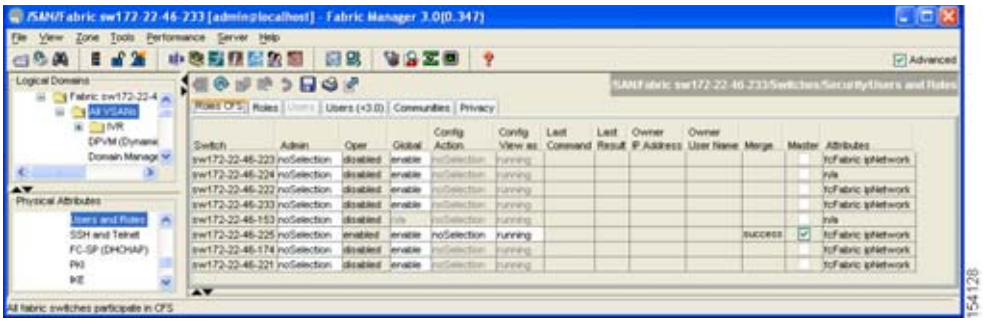
配布がイネーブルのときのロールの表示

ロールに対して配布がイネーブルのときは、ペンディング ロール データベース（配布される前のデータベース）かランニング データベースのいずれかを表示できます。

Fabric Manager を使用してロールを表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Roles CFS] タブをクリックします（図 3-6 を参照）。

図 3-6　[Roles CFS] タブ



ステップ 2　[Config View AS] ドロップダウン メニューを [pending] に設定してペンディング データベースを表示するか、[Config View] ドロップダウン メニューを [running] に設定してランニング データベースを表示します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ユーザ アカウント

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。

この章で説明するタスクを利用すると、ユーザの作成と既存ユーザのプロファイルの修正が行えます。これらのタスクはアドミニストレータにより定義された特権ユーザに制限されます。

次の条件を備えた強力なパスワードを設定する必要があります。

- 最低 8 文字の長さ
- 論理の一貫した文字が多数続かない（「abcd」など）
- 同じ文字が多数連続しない（「aaabbb」など）
- 辞書にある単語を含まない
- 大文字と小文字の両方が含まれている
- 数字が含まれている

強いパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注）　クリア テキストのパスワードに含めることができるのは、アルファベットと数字だけです。ドル記号（$）やパーセント記号（%）などの特殊文字は使用できません。

ここで説明する内容は、次のとおりです。

- 「ユーザの作成に関する注意事項」（P.3-11）
- 「ユーザの設定」（P.3-12）
- 「ユーザの削除」（P.3-14）
- 「ユーザ アカウント情報の表示」（P.3-14）

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になります。オプション **expire** 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。

- 次のワードは予約済みのため、ユーザ設定には使用できません。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
- 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。パスワードは大文字と小文字を区別します。Cisco MDS 9000 ファミリ スイッチでは、デフォルトのパスワードとして「admin」が使われることはなくなりました。強いパスワードを明確に設定する必要があります。

注意　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（Terminal Access Controller Access Control device Plus [TACACS+] または Remote Access Dial-In User Service [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。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 Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）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。

ユーザの設定

Fabric Manager を使用して新しいユーザを設定する、または既存ユーザのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します（図 3-7 を参照）。

図 3-7　[Users] タブの下に表示されるユーザのリスト

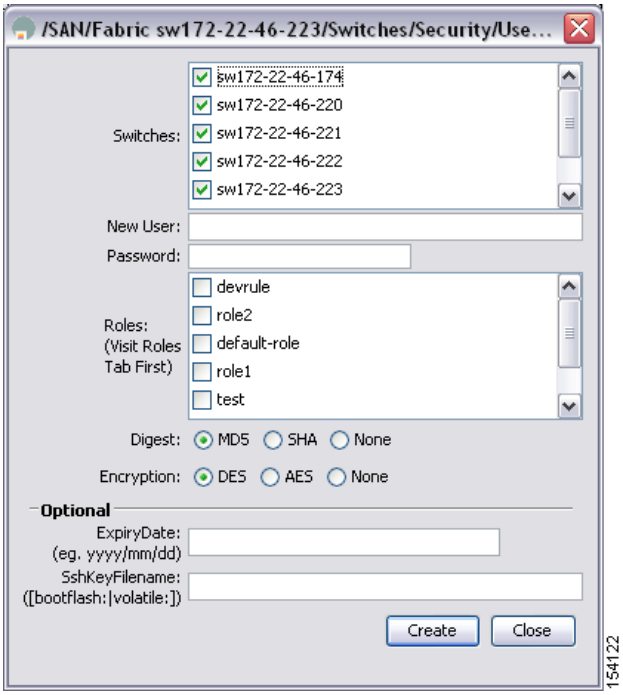
Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

ステップ 2　[Create Row] アイコンをクリックします。

[Create Users] ダイアログボックスが表示されます（図 3-8 を参照）。

図 3-8　[Create Users] ダイアログボックス



ステップ 3　（任意）[Switches] チェックボックスを変更して 1 つ以上のスイッチを指定することもできます。

ステップ 4　[New User] フィールドにユーザ名を入力します。

ステップ 5　[Role] ドロップダウン メニューからロールを選択します。ドロップダウン メニューから選択しない場合、新しいロール名をフィールドに入力することもできます。この場合には、前の手順に戻り、ロールを適切に設定します（「ユーザ アカウント」（P.3-10）を参照）。

ステップ 6　[New Password] フィールドにユーザのパスワードを入力します。[Confirm Password] フィールドに同一の新しいパスワードを入力します。

ステップ 7　[Privacy] チェックボックスをオンにしてパスワード フィールドに入力し、管理トラフィックを暗号化します。

ステップ 8　エントリを作成するには、[Create] ボタンをクリックします。変更内容を保存せずにダイアログボックスを閉じるには、[Close] ボタンをクリックします。

Fabric Manager を使用した管理者パスワードの変更

Fabric Manager で管理者パスワードを変更する手順は、次のとおりです。

ステップ 1　コントロール パネルの [Open] タブをクリックします。

ステップ 2　パスワード フィールドを選択して、ファブリックの既存ユーザのパスワードを変更します。

ステップ 3　[Open] ボタンをクリックして、ファブリックに接続します。

（注）　ファブリックに接続した後に、新しいパスワードが保存されます。ユーザ名とパスワードのフィールドは、ファブリックの接続を解除した後に限り、[Fabric] タブで編集できます。

ユーザの削除

Fabric Manager を使用してユーザを削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザのリストを表示します。

ステップ 2　削除するユーザの名前をクリックします。

ステップ 3　[Delete Row] アイコンをクリックして選択したユーザを削除します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ユーザ アカウント情報の表示

Fabric Manager を使用して、設定したユーザ アカウントの情報を表示する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Security] を展開し、[Users and Roles] を選択します。

ステップ 2　[Users] タブをクリックします。に示す SNMP ユーザのリストが [Information] ペインに表示されます（図 3-9 を参照）。

図 3-9　[Users] タブの下に表示されるユーザのリスト

Switch	User	Primary Role	Other Role	Digest	Encryption
sw172-22-46-182	admin	network-admin		MD5	NoPriv
sw172-22-46-224	abcd	network-operator	network-admin	MD5	DES
sw172-22-46-153	admin	network-admin		MD5	NoPriv
sw172-22-46-182	md5usr	network-operator		MD5	DES
sw172-22-46-224	admin	network-admin		MD5	DES
sw172-22-46-224	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	md5usr	network-admin		MD5	DES
sw172-22-46-153	mchinn	network-operator	network-admin	MD5	DES
sw172-22-46-224	mchinn1	network-operator	network-admin	MD5	NoPriv
sw172-22-46-224	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	md5usr	network-admin		MD5	DES
sw172-22-46-153	junknew	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn1	network-operator	network-admin	MD5	DES
sw172-22-46-153	mchinn5	network-operator	network-admin	MD5	NoPriv
sw172-22-46-153	shadmin	network-operator	network-admin	SHA	DES
sw172-22-46-153	testUser	network-operator	test	MD5	DES

154126

SSH サービス

Cisco MDS 9000 ファミリのすべてのスイッチでは、Telnet サービスはデフォルトでイネーブルになります。Secure Shell（SSH; セキュア シェル）サービスを有効にする場合は、事前にサーバ キー ペアを生成してください（「SSH サーバ キー ペアの生成」（P.3-16）を参照）。

ここで説明する内容は、次のとおりです。

SSH について

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。次の SSH オプションに対する SSH キーを使用できます。

- SSH1
- Rivest, Shamir, Adelman（RSA）を使用する SSH2
- Digital System Algrorithm（DSA）を使用する SSH2

SSH サーバ キー ペアの概要

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の範囲は、768 ～ 2048 です。

SSH サービスでは､SSH バージョン 1 および 2 で使用するキー ペア タイプを 3 つの中から選択できます。

- **rsa1** オプションを使用すると、SSH バージョン 1 プロトコルに対応する RSA1 キー ペアが生成されます。
- **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。

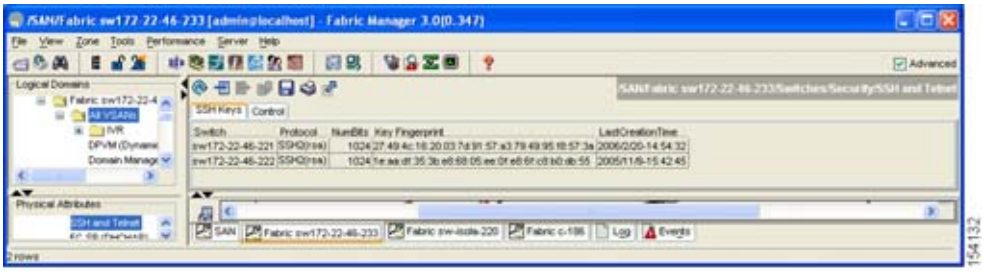
SSH サーバ キー ペアの生成

SSH サーバ キー ペア を生成する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

図 3-10 に示す設定が [Information] ペインに表示されます。

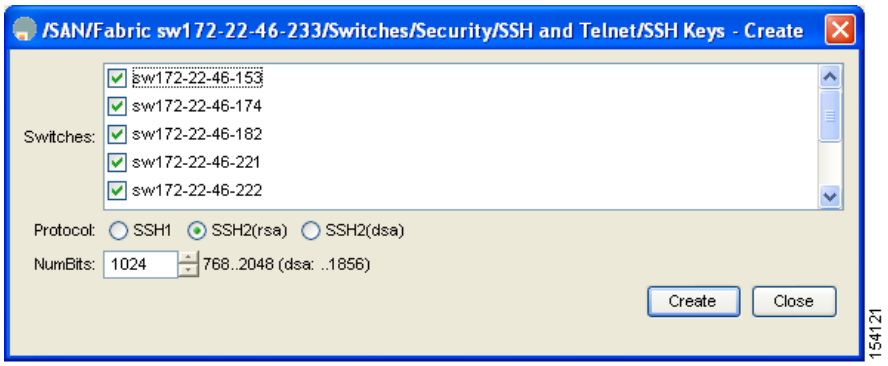
図 3-10　SSH および Telnet の設定



ステップ 2　[Create Row] アイコンをクリックします。

図 3-11 で示す [SSH and Telnet Key - Create] ダイアログボックスが表示されます。

図 3-11　[Create SSH and Telnet] ダイアログ ボックス



ステップ 3　この SSH キー ペアに割り当てるスイッチにチェックを入れます。

ステップ 4　表示された [Protocols] リストからキー ペアのオプション タイプを選択します。表示されるプロトコルは SSH1、SSH2（rsa）、SSH2（dsa）です。

ステップ 5　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 6　これらのキーを生成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

（注）　1856 DSA NumberKeys は、Cisco MDS NX-OS ソフトウェア バージョン 4.1(1) 以降を実行しているスイッチではサポートされません。

生成したキー ペアの上書き

必要なバージョンに対して SSH キー ペア オプションが生成済みの場合は、スイッチでそれまでのキー ペアを上書きすることができます。

Fabric Manager を使用して 前回生成した キー ペア を上書きする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

[Information] ペインに設定が表示されます。

ステップ 2　上書きするキーを選択して [Delete Row] アイコンをクリックします。

ステップ 3　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

ステップ 4　[Create Row] アイコンをクリックします。

[SSH and Telnet Key - Create] ダイアログボックスが表示されます。

ステップ 5　この SSH キー ペアを割り当てるスイッチにチェックを入れます。

ステップ 6　[Protocols] オプション ボタンで、キー ペアのオプション タイプを選択します。

ステップ 7　[NumBits] ドロップダウン メニューで、キー ペアの生成に使用するビット数を設定します。

ステップ 8　これらのキーを生成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

SSH または Telnet サービスのイネーブル化

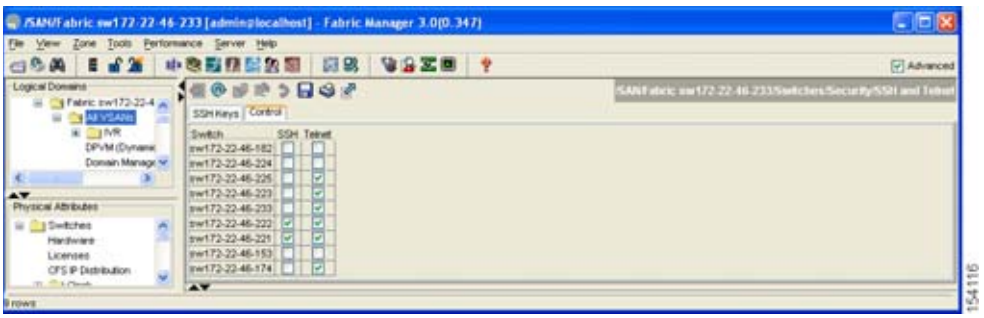
デフォルトでは、SSH サービスはディセーブルです。SSH を設定すると、Fabric Manager は SSH を自動的にイネーブルにします。

Fabric Manager を使用して SSH をイネーブルまたはディセーブルにする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[SSH and Telnet] を選択します。

ステップ 2　[Control] タブを選択し、図 3-12 のように各スイッチの [SSH] チェックボックス、または [Telnet] チェックボックスをオンにします。

図 3-12　[SSH and Telnet] の [Control] タブ



ステップ 3　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

（注）　SSH を介して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は、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。キーストロークを 1 つも入力せずに **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。安全を保証された通信を行うための暗号キーを含み、提出者の身元を確認するために信頼できる Certification Authority（CA; 認証局）により「署名」されています。X.509 デジタル証明書のサポートは、認証のために DSA または RSA のアルゴリズムも提供します。

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 のいずれかにより発行されている場合に、証明書の確認が成功します。

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 認証のいずれかにスイッチを設定できますが、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、その認証が失敗するとパスワードが求められます。

CA およびデジタル証明書の詳細については、第 6 章「CA およびデジタル証明書の設定」を参照してください。

ユーザの作成または更新

他のユーザの権限を変更できるのは、network-admin ユーザだけです。

Fabric Manager を使用して新しいユーザを設定する、または既存ユーザのプロファイルを修正する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[Users and Roles] を選択します。[Information] ペインで [Users] タブをクリックしてユーザ情報を表示します。

ステップ 2　ユーザを作成するには、[Create Row] アイコンをクリックします。

[Create Users] ダイアログボックスが表示されます。

ステップ 3　このユーザにアクセスを許可するスイッチを選択します。

ステップ 4　新しいユーザ名とパスワードを割り当てます。

（注）　ユーザ アカウント名には、数字以外の文字を含める必要があります。

ステップ 5　この新しいユーザに割り当てるロールを選択します。

ステップ 6　作成または更新するユーザのダイジェストおよび暗号化を選択します。

ステップ 7　（任意）ユーザの有効期限と SSH ファイル名を入力します。

ステップ 8　ユーザを作成するには、[Create] ボタンをクリックします。変更を廃棄するには、[Close] ボタンをクリックします。

管理者パスワードの回復

次の 2 つ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で CLI を使用する
- スイッチの電源を再投入する

（注）　管理者パスワードの回復については、『*Cisco MDS 9000 Family NX-OS Security Configuration Guide*』を参照してください。

Cisco ACS サーバの設定

Cisco Access Control Server（ACS）は、TACACS+ および RADIUS 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 3-13、図 3-14、図 3-15、および図 3-16 に、TACACS+ または RADIUS を利用した ACS サーバの network-admin ロールおよび複数のロールのユーザ セットアップ設定の様子を示します。

注意　TACACS+ か RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS NX-OS は、すべて数字のユーザ名をサポートしません。名前がすべて数字のローカル ユーザは作成できません。すべて数字のユーザ名が AAA サーバに存在し、ログインの際に入力しても、そのユーザはログインできません。

（注）　cisco-av-pair に指定されている各ロールは MDS に存在する必要があります。存在しない場合、ユーザには network-operator ロールが設定されます。

図 3-13　RADIUS を使用する場合の network-admin ロールの設定

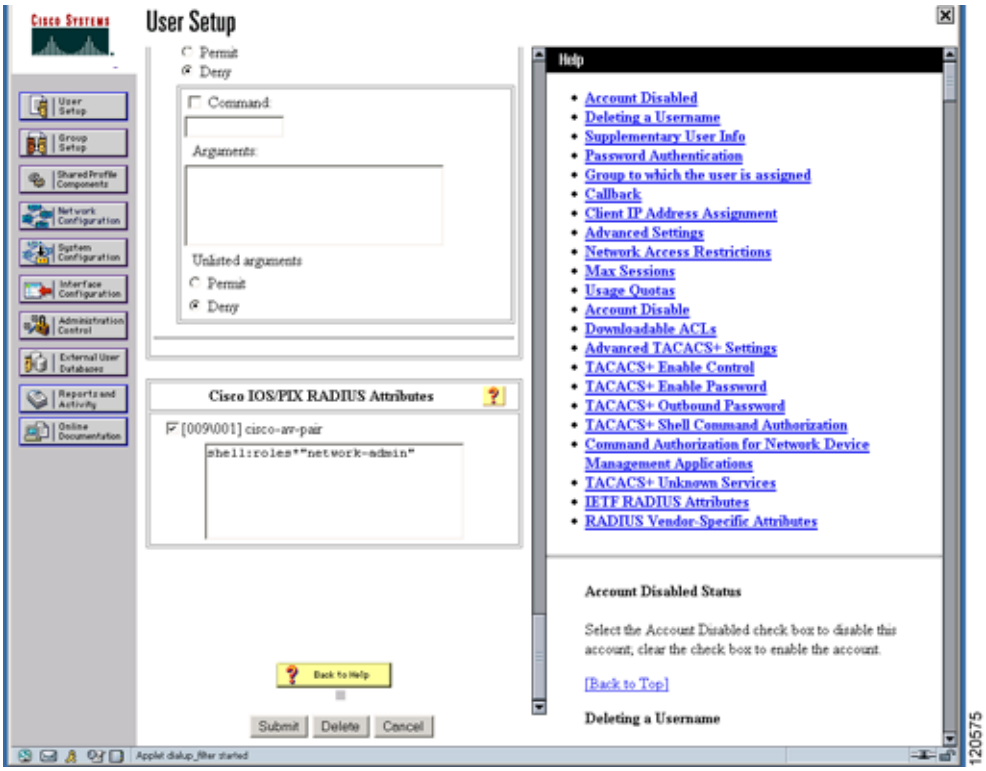


図 3-14　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

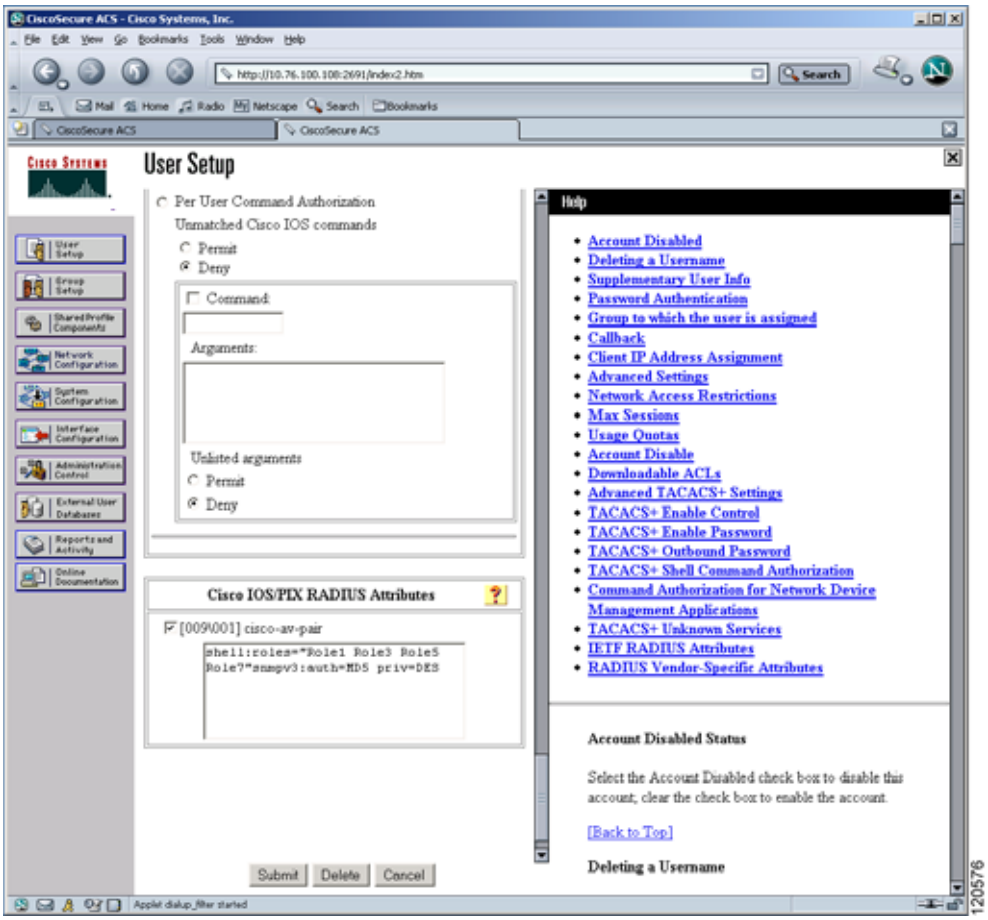


図 3-15　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

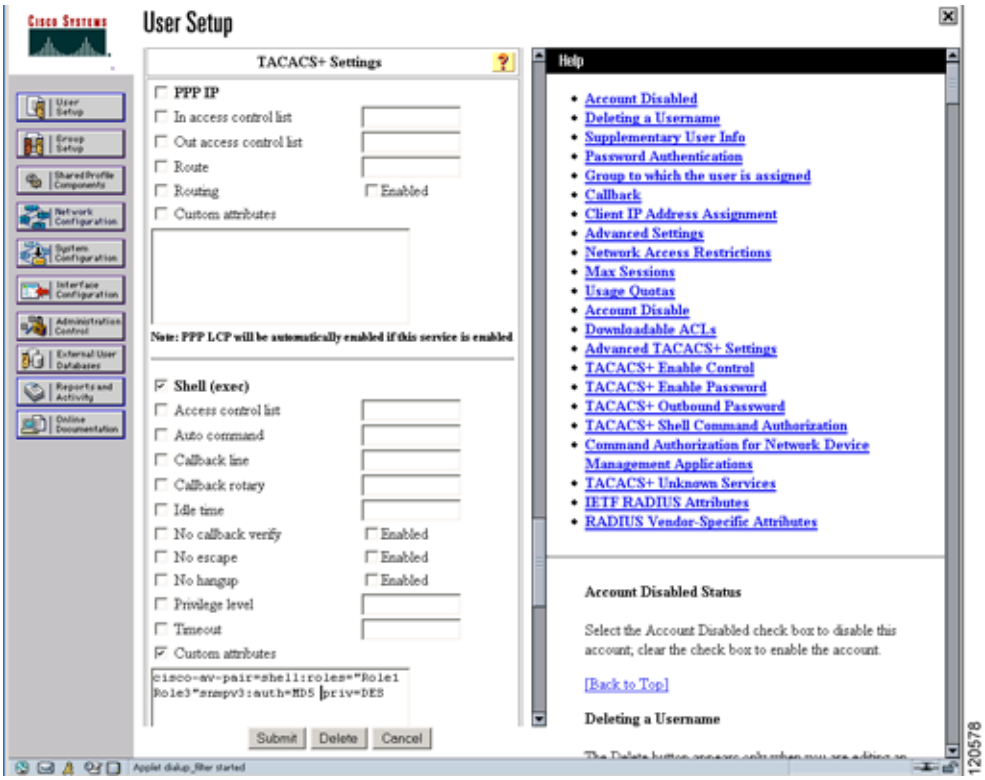
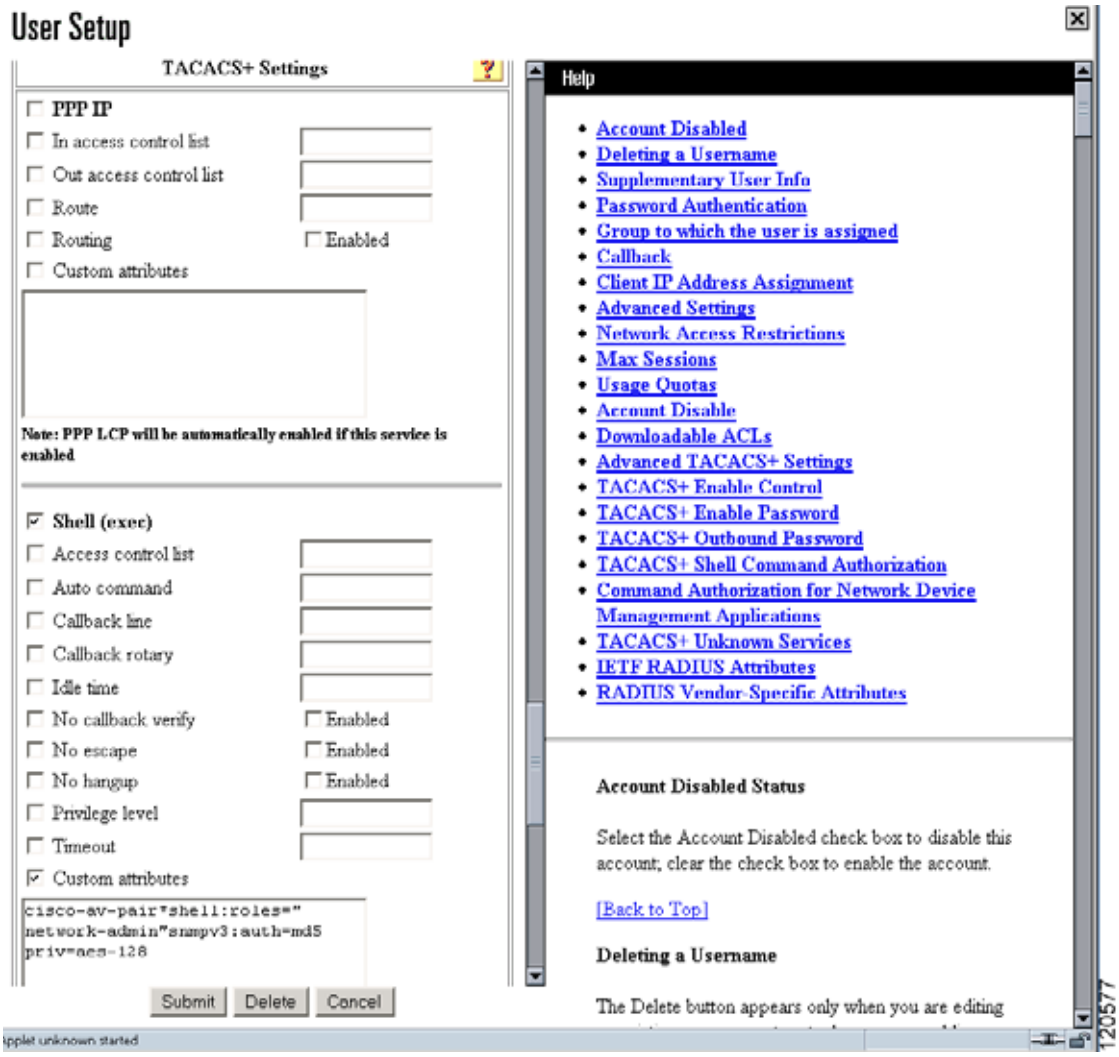


図 3-16　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定値

表 3-1 はすべてのスイッチにおけるスイッチ セキュリティ機能のデフォルト設定です。

表 3-1　デフォルト スイッチ セキュリティ設定

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
認証用ポート	1812
アカウンティング用ポート	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

表 3-1　デフォルト スイッチ セキュリティ設定 （続き）

パラメータ	デフォルト
TACACS+	ディセーブル
TACACS+ サーバ	設定なし
TACACS+ サーバ タイムアウト	5 秒
AAA サーバへの配布	ディセーブル
ロールに対する VSAN ポリシー	許可
ユーザ アカウント	有効期限なし（設定しない場合）
パスワード	なし
アカウンティング ログ サイズ	250 KB
SSH サービス	ディセーブル
Telnet サービス	イネーブル

CHAPTER 4

RADIUS および TACACS+ の設定

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）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。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 データベースを使用したローカル認証または許可、あるいは AAA サーバを使用したリモート認証または許可を実行します。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。

この章の内容は、次のとおりです。

スイッチ管理のセキュリティ

Cisco MDS 9000 ファミリのスイッチ製品における管理セキュリティでは、Command Line Interface（CLI; コマンドライン インターフェイス）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します。

ここで説明する内容は、次のとおりです。

Fabric Manager のセキュリティ オプション

Fabric Manager にアクセスするには、Transmission Control Protocol（TCP; 伝送制御プロトコル）/User Datagram Protocol（UDP; ユーザ データグラム プロトコル）SNMP または Hypertext Transfer Protocol（HTTP）トラフィックを使用します。管理パス（コンソール、Telnet、および Secure Shell（SSH; セキュア シェル））ごとに、ローカル、リモート（RADIUS または TACACS+）、または none のいずれか、あるいは複数のセキュリティ制御オプションを設定できます。

- 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」（P.4-8）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」（P.4-14）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」（P.4-27）を参照してください。

これらのセキュリティ機能は、次の場合にも設定できます。

- Small Computer Systems Interface over IP（iSCSI）認証

  『*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。

スイッチの AAA

CLI または Fabric Manager 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。

ここで説明する内容は、次のとおりです。

認証

認証は、スイッチを管理する人物またはそのスイッチにアクセスするデバイスの ID を確認するプロセスです。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）　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 Protocol Data Unit（PDU; プロトコル データ ユニット）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 の運用を実行できません。

（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」）。

許可

すべての Cisco MDS スイッチ製品に次の許可ロールが存在します。

- 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の変更はできません。
- 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（Fabric Manager および Device Manager）を使用する権限があります。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 ベースの許可を設定します。
- 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 1 つだけに属している場合、このロールが削除されると、ユーザにはデフォルトで network-operator ロールがただちに設定されます。

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 および TACACS+ により提供されるリモート AAA サービスは、ローカルの AAA サービスに比べて次の利点があります。

- 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 サーバは通常、企業全体に配備済みであり、簡単に採用できます。
- 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 で到達可能でなければなりません。
- 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ます。
- オーバーレイ イーサネット 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になります（『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください）。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、アカウンティングを行うためのリモート AAA サーバを、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、1 台のリモート AAA サーバが応答に失敗した場合に、フェールオーバー サーバを提供することにあります。グループ内の最初のリモート サーバが応答に失敗すると、グループ内の次のリモート サーバが応答を試行します。いずれかのサーバが応答を送信するまで、この処理は続きます。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、このサーバ グループ オプションは失敗と見なされます。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 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*』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。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。

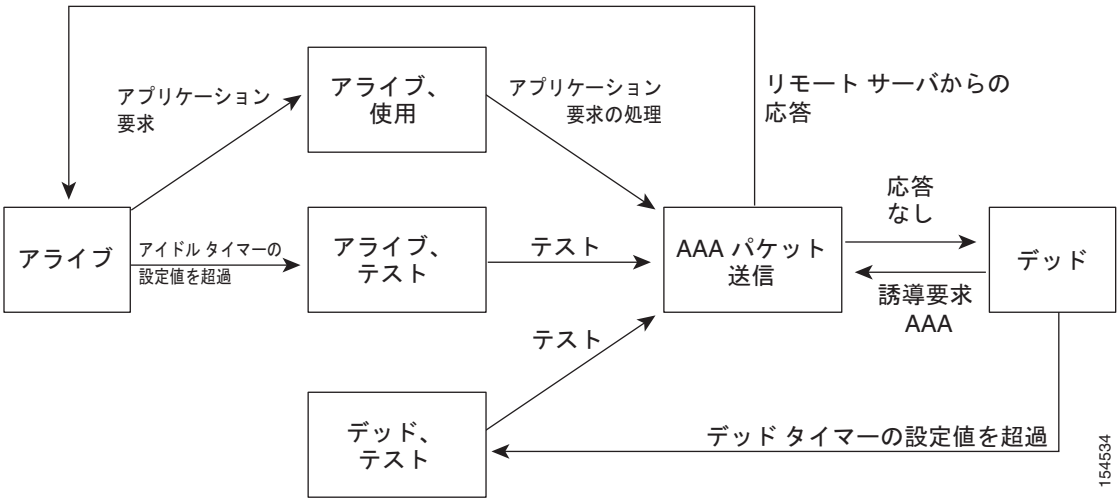
（注）　オプションの 1 つとしてローカルが指定されていない場合でも、その他のすべての設定オプションに失敗したときは、ローカル方式が試行されます。

RADIUS がタイムアウトする際は、常にローカル ログインが試行されます。このローカル ログインを成功させるには、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。

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 サーバが応答する（または機能している）かどうかを確認することができます。MDS スイッチは、応答のない AAA サーバを機能停止と記録します。また、機能停止のいずれの 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機能停止の AAA サーバをモニタし、応答するようになったら機能中と認識します。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 サーバが稼動中であることを確認します。AAA サーバが機能停止または機能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 サーバの状態遷移は図 4-1 を参照してください。

図 4-1　AAA サーバの状態遷移



（注）　稼動中のサーバと停止中のサーバのモニタリング間隔は別々で、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」（P.4-8）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。

認証と許可の手順は、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 グループ認証手順を使用するサーバ 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手順が失敗に終わった場合は、ローカル データベースを利用して認証が行われます。

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、場合に応じて次のアクションが実行されます。

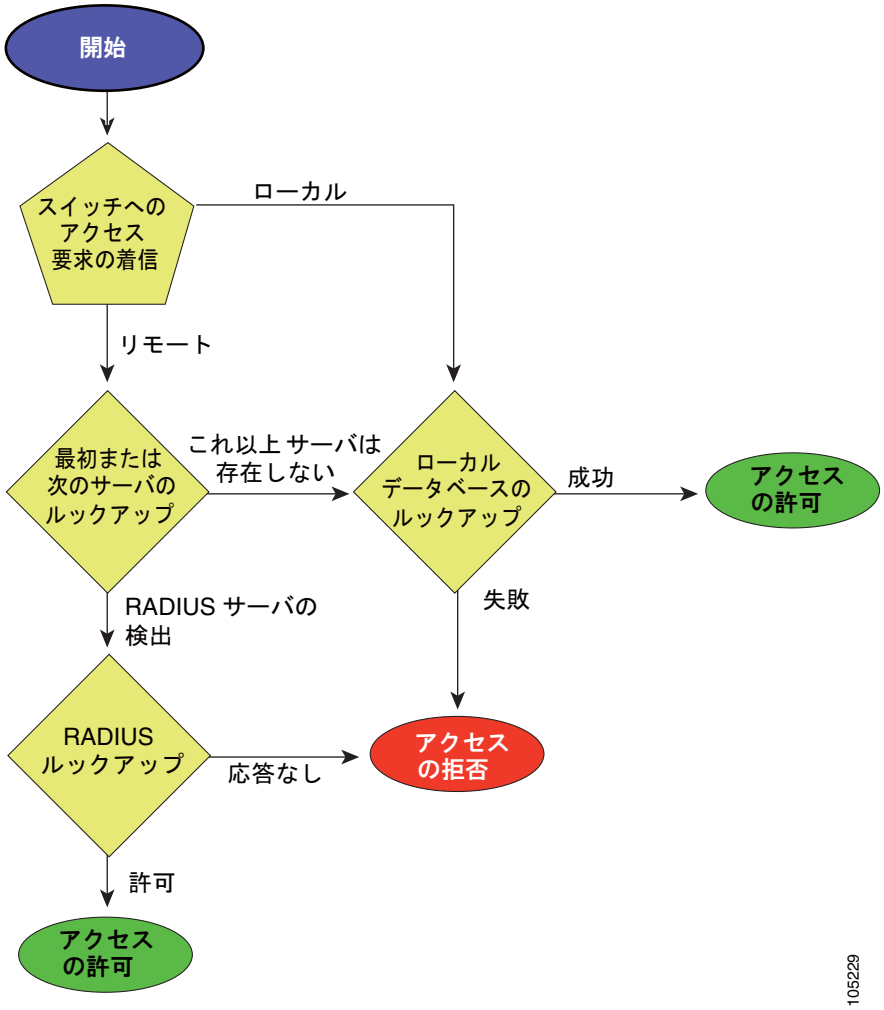
- AAA サーバのプロトコルが RADIUS の場合は、認証応答に伴って **cisco-av-pair** 属性で指定されたユーザ ロールがダウンロードされます。

- AAA サーバのプロトコルが TACACS+ の場合は、同じサーバに別の要求を送信して、シェルのカスタム属性として指定されているユーザ ロールを入手します。
- 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 に許可と認証プロセスのフローチャートを示します。

図 4-2　スイッチの許可と認証のフロー



（注）　残りのサーバ グループがない = どのサーバ グループからも応答がない。
残りのサーバがない = このサーバ グループのどのサーバからも応答がない。

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、不正アクセスからネットワークを保護する分散型クライアント/サーバ プロトコルです。シスコの実装では、RADIUS クライアントは Cisco MDS 9000 ファミリ スイッチで稼動し、認証要求を、すべての認証情報およびネットワーク サービス アクセス情報が格納された中央の RADIUS サーバに送信します。

ここでは、RADIUS の動作を定義し、ネットワーク環境を識別し、設定できる内容について説明します。

ここで説明する内容は、次のとおりです。

RADIUS サーバのデフォルト設定の概要

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
- ログインの際に RADIUS サーバの指定を可能にする

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 文字を使用できます（スペースは使用できません）。スイッチのすべての RADIUS サーバ設定で使用されるグローバル キーを設定できます。

グローバル キーの割り当てを上書きするには、個々の RADIUS 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。

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

Fabric Manager を使用して RADIUS サーバの暗号の種類と事前共有キーのデフォルト値を設定する手順は、次のとおりです。

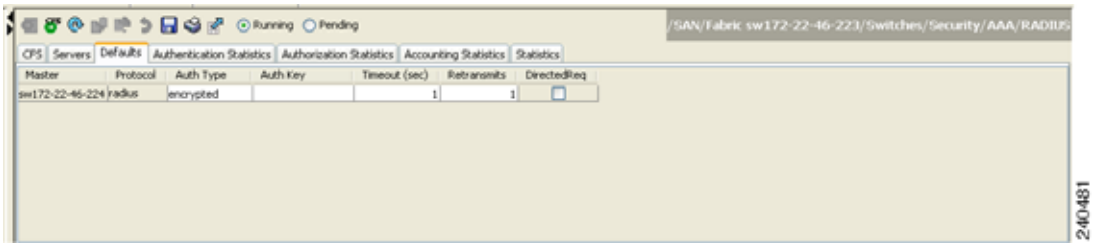
ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

RADIUS のデフォルト設定が表示されます（図 4-3 を参照）。

図 4-3　　RADIUS のデフォルト設定



ステップ 3　[AuthType] ドロップダウン メニューで [plain] または [encrypted] を選択します。

ステップ 4　[Auth Key] フィールドにキーを設定します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

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る前に、RADIUS サーバへの送信の再試行を 1 回だけ行います。再試行の回数はサーバごとに最大 5 回まで増やせます。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。

Fabric Manager を使用して再試行回数と RADIUS サーバへの再送信の間隔を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブを選択します。

RADIUS のデフォルト設定が表示されます。

ステップ 3　認証再試行の [Timeout] および [Retransmits] の各フィールドを入力します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

RADIUS サーバの概要

最大 64 台の RADIUS サーバを追加できます。RADIUS キーは永続的なストレージに暗号化形式で常に格納されています。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。

RADIUS サーバの設定

Fabric Manager を使用して RADIUS サーバとオプションのすべてを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

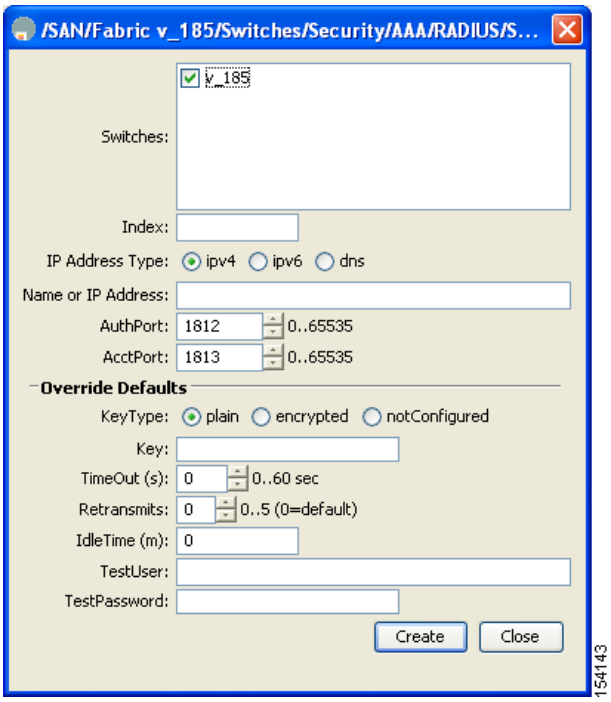
ステップ 2　[Servers] タブをクリックします。

既存の RADIUS サーバが表示されます。

ステップ 3　新しい RADIUS サーバを追加するには、[Create Row] アイコンをクリックします。

[Create RADIUS Server] ダイアログボックスが表示されます（図 4-4 を参照）。

図 4-4　[Create RADIUS Server]



ステップ 4　RADIUS サーバとして割り当てるスイッチを選択します。

ステップ 5　RADIUS サーバを識別するためのインデックス番号を割り当てます。

ステップ 6　RADIUS サーバに与える IP アドレスの種類を選択します。

ステップ 7　RADIUS サーバの IP アドレスまたは名前を入力します。

ステップ 8　（任意）RADIUS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 9　RADIUS サーバに与える適切なキーの種類を選択します。

ステップ 10　タイムアウトの値を秒で選択します。有効な範囲は 0 ～ 60 秒です。

ステップ 11　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を選択します。

ステップ 12　テスト用のアイドル間隔の値を分で入力します。有効な範囲は 1 ～ 1440 分です。

ステップ 13　テスト ユーザをデフォルト パスワードとともに入力します。デフォルトのユーザ名は test です。

ステップ 14　[Create] ボタンをクリックして変更内容を保存します。

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 サーバが要求を待つ時間間隔を指定します。

（注）　アイドル タイマーのデフォルト値は 0 分です。アイドル タイマーの時間間隔が 0 分の場合は、RADIUS サーバによる定期的なモニタリングが行われません。

テスト アイドル タイマーを設定するには、「RADIUS サーバの設定」（P.4-10）を参照してください。

テスト ユーザ名の設定

RADIUS サーバによる定期的なサーバ ステータスのテスト実施に使用するユーザ名とパスワードを設定できます。RADIUS サーバをモニタするためのテスト 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。

RADIUS サーバによる定期的なサーバ ステータスのテスト実施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 サーバの設定」（P.4-10）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 サーバでテスト ユーザ名として設定されたユーザ名を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。

RADIUS サーバの定期的な検証

Fabric Manager を使用して RADIUS 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、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Servers] タブをクリックします。

既存の RADIUS サーバが表示されます。

ステップ 3　新しい RADIUS サーバを追加するには、[Create Row] アイコンをクリックします。

[Create RADIUS Server] ダイアログボックスが表示されます（図 4-4 を参照）。

ステップ 4　IP アドレスを入力します。

ステップ 5　RADIUS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 6　[TestUser] フィールドに入力し、必要に応じて [TestPassword] フィールドを入力します。テスト用のデフォルト パスワードは **Cisco** です。

ステップ 7　テスト認証を送信するまでサービスをアイドル状態に置く [IdleTime] フィールドを設定します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

RADIUS サーバ統計情報の表示

Fabric Manager を使用して RADIUS サーバ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。

RADIUS の統計情報が表示されます。

ログイン時に RADIUS サーバを指定するユーザの概要

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。スイッチに対して要求送信の誘導オプションをイネーブルにする設定を行うと、どの RADIUS サーバに認証要求を送信させるかをユーザが指定できるようになります。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。

ユーザがログイン時に RADIUS サーバを指定可能にする

Fabric Manager を使用して、ユーザが認証用の RADIUS サーバを選択するために MDS スイッチにログインできるようにする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

RADIUS のデフォルト設定が表示されます。

ステップ 3　RADIUS サーバの [DirectedReq] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

VSA（ベンダー固有属性）について

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 Vendor-Specific Attribute（VSA; ベンダー固有属性）の通信方法が規定されています。IETF では属性 26 が使用されます。ベンダーは VSA を使用することにより、一般的な用途に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、仕様で推奨されたフォーマットを使用するベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 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、特定の許可タイプを表すシスコの属性です。**separator** は、必須の属性の場合は = （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、認証情報などのユーザ属性およびユーザ結果を戻すように RADIUS サーバに指示します。この許可情報は、VSA を使用して指定されます。

VSA のフォーマット

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：アカウンティング要求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。

Cisco NX-OS ソフトウェアでは、次の属性が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ストリングです。たとえば、ユーザが **vsan-admin** および **storage-admin** の各ロールに属している場合、値フィールドは「**vsan-adminstorage-admin**」になります。このサブ属性は Access-Accept フレームの VSA 部分に保管され、RADIUS サーバから送信されます。この属性と併用できるのは、シェル プロトコル値だけです。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。その他のシスコ製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 Protocol Data Unit（PDU; プロトコル データ ユニット）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 …"
```

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。

VSA フォーマットはオプションとして、SNMPv3 認証と機密保持プロトコルの属性を次のようにも指定できます。

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

SNMPv3 認証プロトコル オプションは SHA および MD5 です。プライバシー プロトコル オプションは AES-128 および 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。

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 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。

ここで説明する内容は、次のとおりです。

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、許可を実行できます。
- 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、コネクション型プロトコルによる確実な転送を行います。
- 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、さらに優れたデータ保護を実現できます。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の概要

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
- ログインの際に TACACS+ サーバの指定を可能にする

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 文字を使用できます（スペースは使用できません）。スイッチのすべての TACACS+ サーバ設定で使用されるグローバル キーを設定できます。

グローバル キーの割り当てを上書きするには、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+ 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

Fabric Manager を使用して TACACS+ サーバの暗号種類と事前共有キーのデフォルト値を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブが無効になっている場合は、[CFS] タブをクリックします。

ステップ 3　[Defaults] タブをクリックします。

TACACS+ のデフォルト設定が表示されます。

ステップ 4　[AuthType] ドロップダウン メニューで [plain] または [encrypted] を選択し、[Auth Key] フィールドにキーを設定します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

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。

Fabric Manager を使用して再試行回数と TACACS+ サーバへの再送信の間隔を設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします （[Defaults] タブがディセーブルの場合は、[CFS] タブを最初にクリックします）。

TACACS+ のデフォルト設定が表示されます。

ステップ 3　認証再試行の [Timeout] および [Retransmits] の各フィールドに値を入力します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

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。Fabric Manager または Device Manager は TACACS+ サーバの設定を行うと、自動的に TACACS+ の機能をイネーブルにします。

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 Release 2.1(2) よりも前のバージョンでは、キーの中にドル記号（$）を使用できますが、「"」で囲む必要があります（例、"k$"）。パーセント記号（%）は使えません。Cisco MDS SAN-OS リリース 2.1(2) 以降では、引用符号なしにドル記号（$）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。

ACACS+ サーバの設定

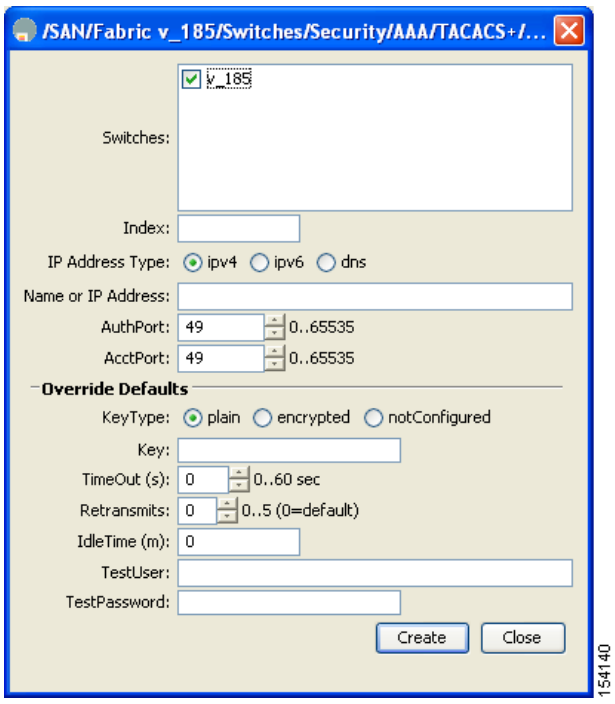
Fabric Manager を使用して TACACS+ サーバとオプションのすべてを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。
[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Servers] タブをクリックします。
既存の TACACS+ サーバが表示されます。

ステップ 3　新しい TACACS+ サーバを追加するには、[Create Row] アイコンをクリックします。
[Create TACACS+ Server] ダイアログボックスが表示されます（図 4-5 を参照）。

図 4-5　[Create TACACS+ Server] ダイアログボックス



ステップ 4　TACACS サーバとして割り当てるスイッチを選択します。

ステップ 5　TACACS サーバを識別するためのインデックス番号を割り当てます。

ステップ 6　TACACS サーバに与える IP アドレスの種類を選択します。

ステップ 7　TACACS サーバの IP アドレスまたは名前を入力します。

ステップ 8　TACACS サーバが使用する認証用ポートおよびアカウンティング用ポートを修正します。

ステップ 9　TACACS サーバに与える適切なキーの種類を選択します。

ステップ 10　タイムアウトの値を秒で選択します。有効な範囲は 0 ～ 60 秒です。

ステップ 11　ローカル認証に戻る前に、スイッチが TACACS サーバへの接続を試行する回数を選択します。

ステップ 12　テスト用のアイドル間隔の値を分で入力します。有効な範囲は 1 ～ 1440 分です。

ステップ 13　テスト ユーザをデフォルト パスワードとともに入力します。デフォルトのユーザ名は test です。

ステップ 14　[Create] ボタンをクリックして変更内容を保存します。

TACACS+ サーバ検証の概要

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 を使用して 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については、「TACACS+ サーバ モニタリング パラメータの設定」（P.4-14）を参照してください。

TACACS+ サーバ統計情報の表示

Fabric Manager を使用して TACACS+ サーバ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Statistics] タブを選択します。

TACACS+ サーバの統計情報が表示されます。

ログイン時に TACACS+ サーバを指定するユーザの概要

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。スイッチを設定すると、どの TACACS+ サーバに認証要求を送信させるかをユーザが指定できるようになります。この機能を有効化すると、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。

ログイン時における TACACS+ サーバの指定許可

Fabric Manager を使用して、ユーザがログイン時に TACACS+ サーバを指定できるようにスイッチを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[Defaults] タブをクリックします。

TACACS+ のデフォルト設定が表示されます。

ステップ 3　[DirectedReq] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ロールのカスタム属性について

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** の形式で指定します。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）　Access Control Server（ACS）には、さまざまなサービス（シェルなど）用に TACACS+ カスタム属性を定義できます。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。

サポート対象の TACACS+ サーバ

Cisco NX-OS ソフトウェアは現在、指定した 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"
```

サーバ グループ

サーバ グループを使用すると、ユーザを認証するための 1 つまたは複数のリモート AAA サーバを指定できます。RADIUS と TACACS+ のいずれにおいても、グループのメンバーはすべて同じプロトコルに属す必要があります。設定した順序に従って一連のサーバが試行されます。

AAA サーバ モニタリング機能は AAA サーバを機能停止として記録できます。スイッチが機能停止の 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」（P.4-5）を参照してください）。

ここで説明する内容は、次のとおりです。

- 「サーバ グループ設定の概要」（P.4-20）
- 「サーバ グループの設定」（P.4-20）

サーバ グループ設定の概要

これらのサーバ グループはいつでも設定できますが、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 または Device Manager のユーザに設定できます。

サーバ グループの設定

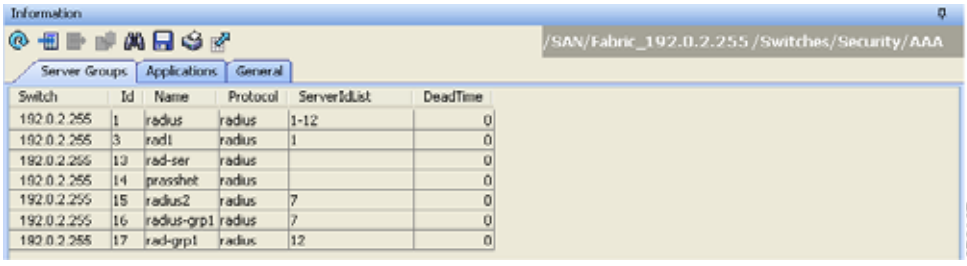
Fabric Manager を使用して RADIUS または TACACS+ サーバ グループを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[AAA] を選択します。

AAA 設定が [Information] ペインに表示されます（図 4-6 を参照）。図 4-6 のような画面が表示されない場合は、[Server Groups] タブをクリックします。

設定した RADIUS または TACACS+ サーバ グループが表示されます。

図 4-6　AAA サーバ グループ



ステップ 2　サーバ グループを作成するには [Create Row] アイコンをクリックします。

[Create Server] ダイアログボックスが表示されます。

ステップ 3　RADIUS サーバ グループを追加するには、[radius] オプション ボタンをクリックします。TACACS+ サーバ グループを追加するには、[tacacs+] オプション ボタンをクリックします。

ステップ 4　ServerIdList フィールドにサーバ名を入力します。

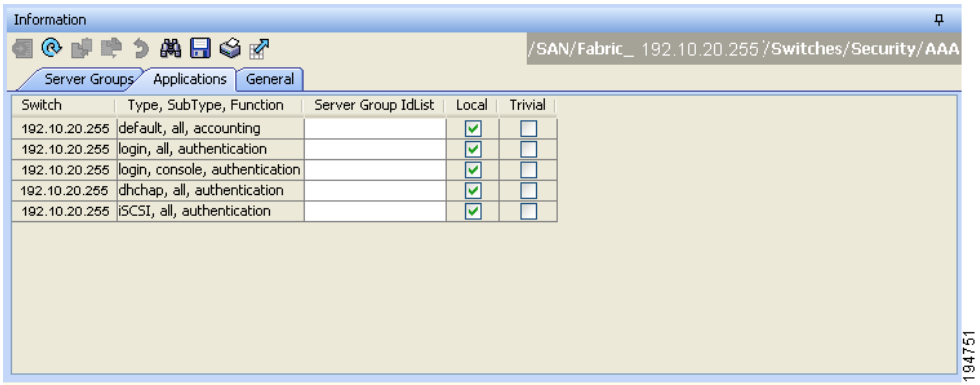
ステップ 5　バイパス（回避）と記録されるまでのサーバ無応答の分数を [DeadTime] フィールドに設定します。「無応答サーバのバイパス（回避）の概要」（P.4-22）を参照してください。

ステップ 6　このサーバ グループを作成するには [Create] ボタンをクリックします。

ステップ 7　[Applications] タブをクリックして、このサーバ グループをアプリケーションに割り当てます（図 4-7 を参照）。

サーバ グループをすべてのアプリケーションに関連付けることも、特定のアプリケーションを指定することもできます。

図 4-7　[Applications] タブ



ステップ 8　[General] タブをクリックして、このサーバ グループに認証の種類を割り当てます（図 3-8 を参照）。

サーバ グループの種類に基づいて、[MSCHAP] または [MSCHAPv2] のいずれかのチェックボックスをオンにします。

図 4-8　[General] タブ

ステップ 9　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（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かわりに、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 サーバにおける配布

MDS スイッチの RADIUS および TACACS+ の AAA 設定は、Cisco Fabric Services（CFS）を使用して配布できます。デフォルトでは、配布はディセーブルです（『*Cisco Fabric Manager System Management Configuration Guide*』を参照）。

配布を有効にすると、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します。それ以降に入力されたすべてのサーバ設定コマンドは、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 パラメータが配布されます。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 グループ設定は配布されません。

ここで説明する内容は、次のとおりです。

- 「AAA サーバにおける配布のイネーブル化」（P.4-22）
- 「スイッチにおける配布セッションの開始」（P.4-23）
- 「セッション ステータスの表示」（P.4-23）
- 「配布する設定の表示」（P.4-24）
- 「配布のコミット」（P.4-24）
- 「配布セッションの廃棄」（P.4-24）
- 「セッションの消去」（P.4-25）
- 「RADIUS および TACACS+ 設定マージの注意事項」（P.4-25）

（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 サーバにおける配布のイネーブル化

配布アクティビティに参加できるのは、配布がイネーブルであるスイッチだけです。

Fabric Manager を使用して RADIUS サーバでの配布を有効にする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] を選択します。

[Information] ペインに RADIUS の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS CFS の設定が表示されます。

ステップ 3　RADIUS の CFS を有効にする全スイッチについて、[Admin] ドロップダウン リストで [enable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

Fabric Manager を使用して TACACS+ サーバでの配布を有効にする手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[TACACS+] を選択します。

[Information] ペインに TACACS+ の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。

TACACS+ CFS の設定が表示されます。

ステップ 3　TACACS+ の CFS を有効にする全スイッチについて、[Admin] ドロップダウン リストで [enable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

スイッチにおける配布セッションの開始

配布セッションは RADIUS/TACACS+ 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設定コマンドを発行すると、すべてのサーバおよびグローバル設定（配布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

暗黙の配布セッションが開始すると、Fabric Manager でセッションの状況を次の手順で確認できます。[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

配布する設定の表示

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、Fabric Manager を使用して表示する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

ステップ 2　[CFS] タブをクリックします。

[CFS] タブに配布状況が表示されます。

ステップ 3　[pending] または [running] オプション ボタンをクリックします。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ステップ 5　[Servers] タブをクリックして保留中または実行中の設定を表示します。

配布のコミット

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は、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。

Fabric Manager を使用して RADIUS または TACACS+ の設定を配布する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。[Information] ペインに RADIUS または TACACS+ の設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS または TACACS+ の CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ の CFS をイネーブルにする全スイッチについて、[Config Action] ドロップダウン リストで [commitChanges] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更をファブリック全体に配布します。

配布セッションの廃棄

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

Fabric Manager を使用して RADIUS または TACACS+ の配布を廃棄する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。[Information] ペインに RADIUS または TACACS+ いずれかの設定が表示されます。

ステップ 2　[CFS] タブをクリックします。RADIUS または TACACS+ いずれかの CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ のペンディング配布を廃棄する各スイッチの [Config Action] ドロップダウン リストで [abort] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックします。

セッションの消去

Fabric Manager を使用して RADIUS または TACACS+ の配布を消去する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] > [AAA] を展開し、[RADIUS] または [TACACS+] を選択します。

[Information] ペインに RADIUS または TACACS+ いずれかの設定が表示されます。

ステップ 2　[CFS] タブを選択します。RADIUS または TACACS+ いずれかの CFS 設定が表示されます。

ステップ 3　RADIUS または TACACS+ のペンディング配布を消去する各スイッチの [Config Action] ドロップダウン リストで [clear] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックします。

RADIUS および TACACS+ 設定マージの注意事項

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 配布がイネーブルの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 キーとグローバル キーは、マージ中は変更されません。
- マージされた設定には、CFS がイネーブルのすべてのスイッチで扱われる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存在する最大値になります。

注意　設定されたサーバ ポートの 2 台のスイッチ間に矛盾がある場合は、マージに失敗します。

MSCHAP による認証

Microsoft Challenge Handshake Authentication Protocol（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 Password Authentication Protocol（PAP）認証を使用します。MSCHAP をイネーブルにする場合は、MSCHAP の VSA（vendor-specific attribute; ベンダー固有属性）を RADIUS サーバが認識するように設定する必要があります。「VSA（ベンダー固有属性）について」（P.4-13）を参照してください。表 4-1 に、MSCHAP に必要な RADIUS ベンダー固有属性を示します。

表 4-1　MSCHAP 用の RADIUS ベンダー固有属性

ベンダー ID 番号	ベンダー種別番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP ユーザへ送るチャレンジを格納。アクセス要求パケットとアクセス チャレンジ パケットの両方で使用可能
211	11	MSCHAP-Response	チャレンジへの応答として MS-CHAP ユーザにより提供される応答値を格納。アクセス要求パケットだけで使用

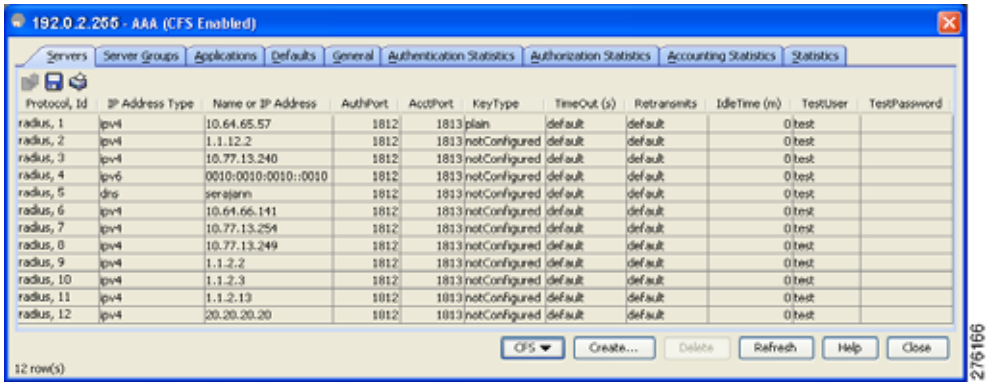
MSCHAP による認証のイネーブル化

Device Manager を使用して MSCHAP 認証をイネーブルにする手順は、次のとおりです。

ステップ 1　[Security] > [AAA] をクリックします。

AAA 設定が [Information] ペインに表示されます（図 4-9 を参照）。

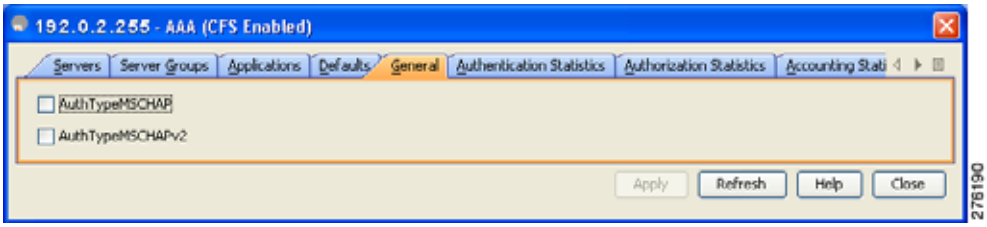
図 4-9　Device Manager での AAA 設定



ステップ 2　[General] タブをクリックします。

MSCHAP 設定が表示されます（図 4-10 を参照）。

図 4-10　MSCHAP の設定



ステップ 3　[AuthTypeMSCHAP] または [AuthTypeMSCHAPv2] チェックボックスをオンにして、スイッチでのユーザ認証に MSCHAP または MSCHAPv2 を利用します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ローカル AAA サービス

システムはユーザ名およびパスワードをローカルで維持し、パスワード情報は暗号化して保存します。ユーザの認証は、ローカルで保存されたユーザ情報に基づいて実行されます。

none オプションを使用して、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 ファミリ スイッチ上のローカル ユーザでなければなりません。

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。

このオプションの設定手順については、『*Cisco MDS 9000 Family NX-OS Configuration Guide*』を参照してください。

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 4-11、図 4-12、図 4-13 および図 4-14 に、RADIUS または TACACS+ を使用した ACS サーバの network-admin ロールおよび複数のロールのユーザ セットアップ設定のようすを示します。

注意　RADIUS または TACACS+ またはローカルのいずれで作成されたものであっても、Cisco MDS NX-OS は、すべて数字で構成されるユーザ名をサポートしません。名前がすべて数字のローカル ユーザは作成できません。すべて数字のユーザ名が AAA サーバに存在し、ログインの際に入力されても、そのユーザはログインできません。

図 4-11　RADIUS を使用する場合の network-admin ロールの設定

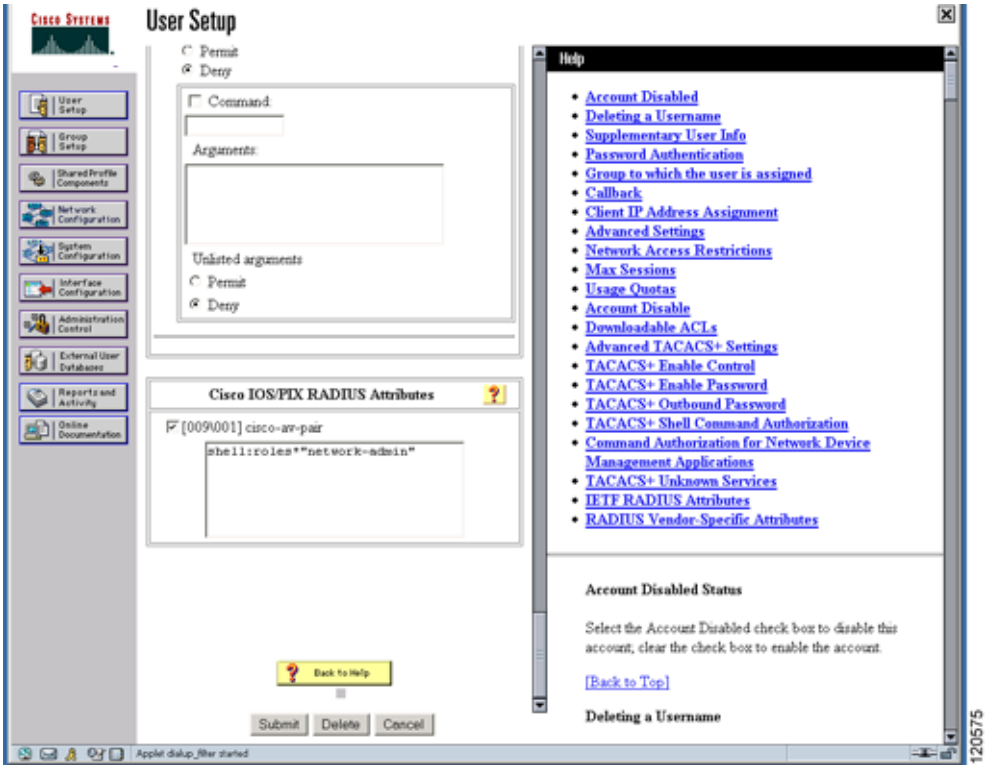


図 4-12　RADIUS を使用する場合の SNMPv3 属性を持つ複数ロールの設定

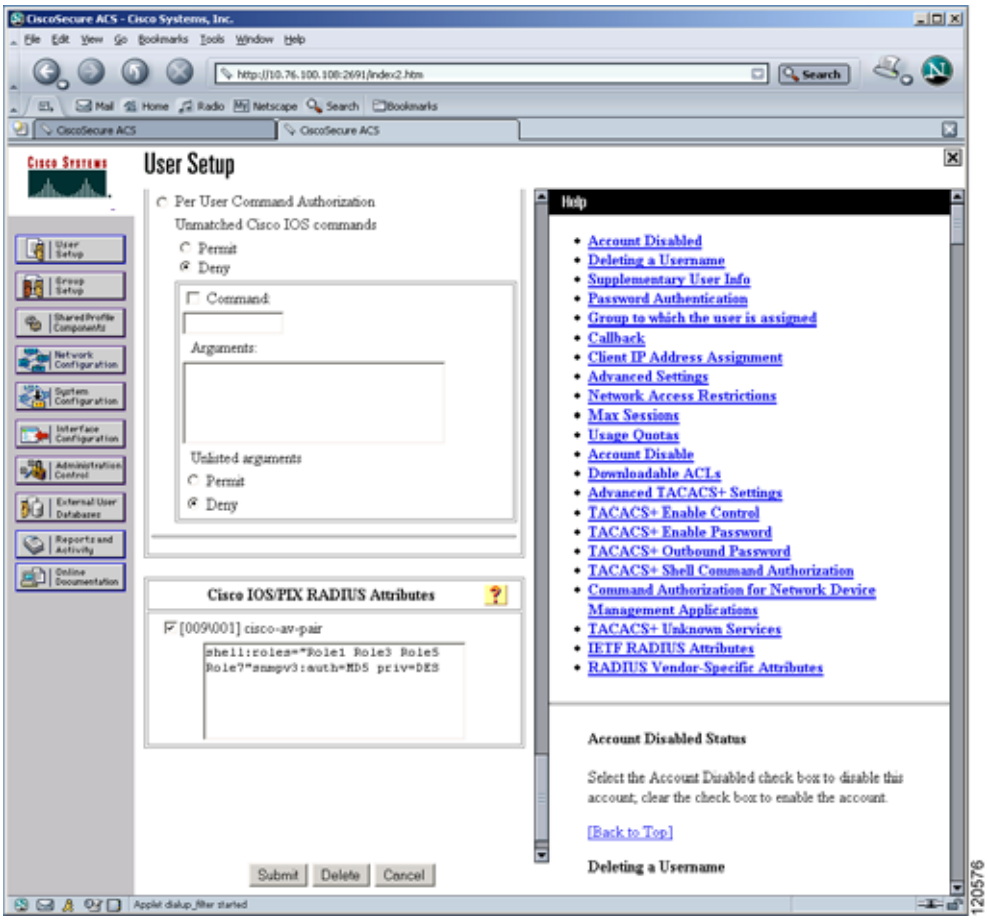


図 4-13　TACACS+ を使用する場合の SNMPv3 属性を持つ network-admin ロールの設定

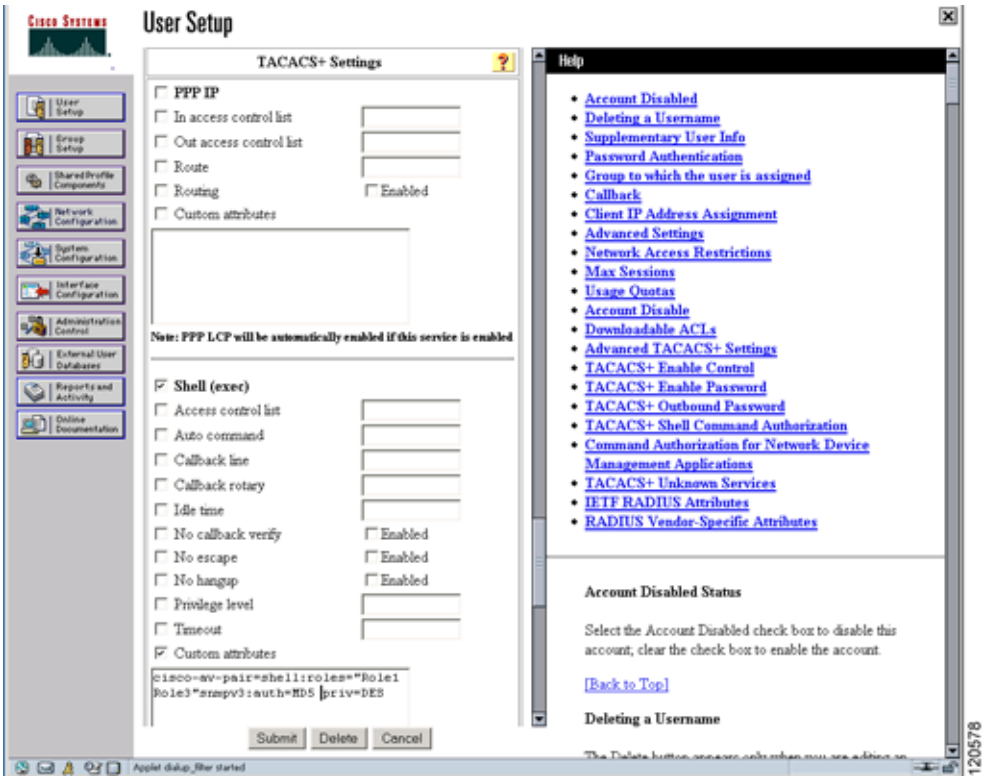
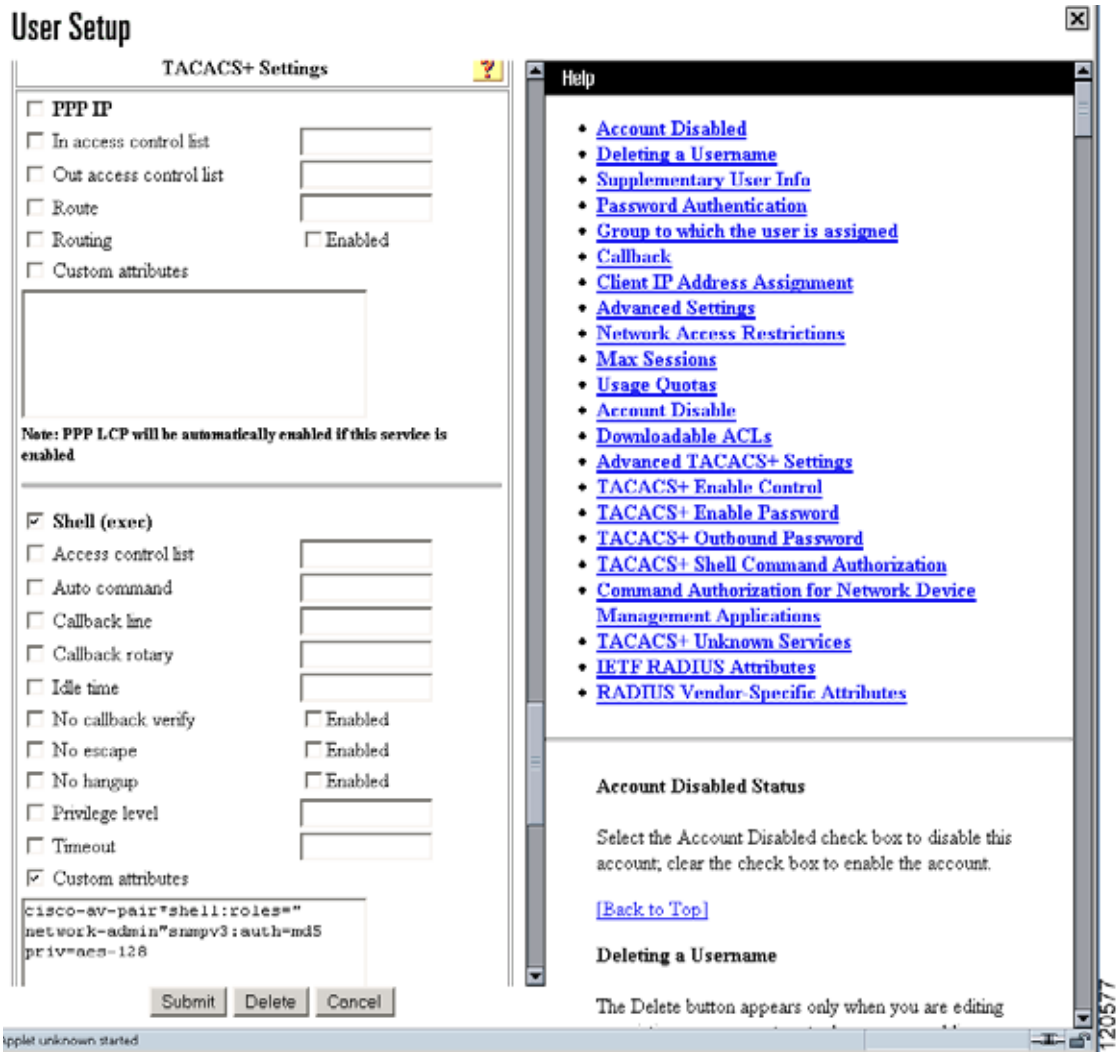


図 4-14　TACACS+ を使用する場合の SNMPv3 属性を持つ複数ロールの設定



デフォルト設定値

表 4-2 はすべてのスイッチにおけるスイッチ セキュリティ機能のデフォルト設定です。

表 4-2　デフォルト スイッチ セキュリティ設定

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
認証用ポート	1812
アカウンティング用ポート	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

表 4-2　デフォルト スイッチ セキュリティ設定 （続き）

パラメータ	デフォルト
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	イネーブル
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	設定なし
TACACS+ サーバ 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 サーバへの配布	ディセーブル
アカウンティング ログ サイズ	250 KB

CHAPTER 5

IPv4 および IPv6 のアクセス制御リストの設定

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 Internet Protocol（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 Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）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 Network Management System（NMS; ネットワーク管理システム）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設けられたアウトオブバンド 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、カプセル化手法を利用して IP フレームをファイバ 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。

スイッチの Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）機能は RFC 2338 標準規格に準拠しています。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。

この章の内容は、次のとおりです。

IPv4-ACL および IPv6-ACL の設定時の注意事項

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 を設定する場合には、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、管理用インターフェイス、Intrusion Prevention System（IPS; 侵入防御システム）モジュールおよび 14/2 Multiprotocol Services（MPS-14/2; 14/2 マルチプロトコル サービス）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　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 グループに追加することができません。IPv4-ACL の設定に関する注意事項については、『Cisco Fabric Manager IP Services Configuration Guide』を参照してください。

注意　IPv4-ACL または IPv6-ACL の適用は、ポートチャネル グループ内の 1 つのメンバーだけに限定しないでください。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ます。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。ど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 ストレージ ギガビット イーサネット ポートには暗黙の拒否は影響しないので、IP ACL を適用するにはこれらのポートに明示的な拒否を設定します。

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、Internet Control Message Protocol（ICMP）タイプ、および Type of Service（ToS; サービス タイプ）に基づく IP パケットの一致規則が含まれます。

ここで説明する内容は、次のとおりです。

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 の範囲の整数を指定します。この数字は、IP プロトコルを示します。
- プロトコルの名前を指定します。指定できるプロトコルには、Internet Protorol（IP）、Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）などがあります。

（注）　ただし、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ます。

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。ポート番号の有効範囲は 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限って使用できます。
  - UDP ポート名は、UDP をフィルタリングする場合に限って使用できます。

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 accounting	1646 または 1813
	radius authentication	1645 または 1812
	snmp	161
	snmp-trap	162
	Syslog	514
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 接続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 ～ 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 ～ 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]	コード番号
エコー	8
エコー応答	0
宛先不達	3
traceroute	30
時間超過	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 条件に基づいてフィルタにより選別できます。

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

IP-ACL ウィザードを使用した 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は、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立の高いフィルタを置きます。許可されないトラフィックに対しては *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。

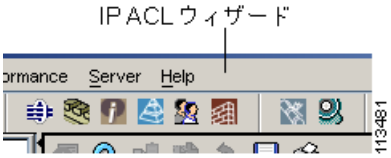
（注）　フィルタのエントリは順番に実行されます。エントリはリストの最後にだけ追加できます。正しい順番でエントリを追加するように注意してください。

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 の名前付きプロファイルの中に順番に並べた IP フィルタのリストを、Fabric Manager の IPv4-ACL ウィザードを使用して作成する手順は、次のとおりです。

ステップ 1　Fabric Manager ツールバーで [IP ACL Wizard] アイコンをクリックします（図 5-1 を参照）。

図 5-1　[IP ACL Wizard]



IP ACL ウィザードが表示されます。

ステップ 2　IP-ACL プロファイルの名前を入力します。

（注）　IPv6-ACL を作成する場合は、IPv6 チェックボックスをオンにします。

ステップ 3　[Add] ボタンをクリックし、この IP-ACL に新しいルールを追加します。テーブルに新しい規則とデフォルト値が表示されます。

ステップ 4　必要に応じて、フィルタの送信元 IP および送信元マスクを修正します。

（注）　IP-ACL ウィザードで作成できるのは、着信 IP フィルタだけです。

ステップ 5　[Application] ドロップダウン リストで、適切なフィルタ タイプを選択します。

ステップ 6　[Action] ドロップダウン リストで [permit] または [deny] を選択します。

ステップ 7　追加する IP フィルタに対して、ステップ 3 ～ステップ 6 を繰り返します。

ステップ 8　[Up] ボタンまたは [Down] ボタンをクリックして、IP-ACL フィルタの順序を決定します。

ヒント　IP フィルタの順序は慎重に決定してください。トラフィックは、指定された順序で IP フィルタと比較されます。最初の一致が適用され、以降のフィルタは無視されます。

ステップ 9　[Next] ボタンをクリックします。

この IP-ACL を適用できるスイッチのリストが表示されます。

ステップ 10　この IP-ACL を適用したくないスイッチは、選択を取り消します。

ステップ 11　この IP-ACL を適用する**インターフェイス**を選択します。

ステップ 12　[Finish] ボタンをクリックして、この IP-ACL を作成し、選択したスイッチに適用します。

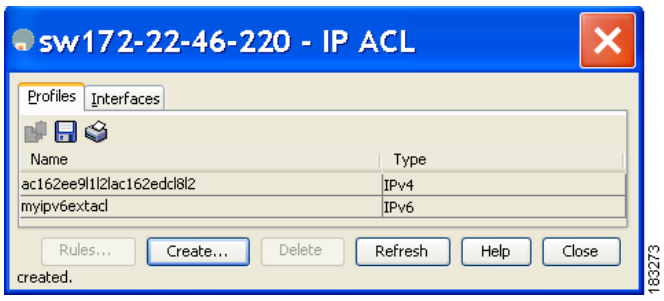
Device Manager での IPv4-ACL または IPv6-ACL の作成

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL にエントリを追加する手順は、次のとおりです。

ステップ 1　[Security] > [IP ACL] を選択します。

[IP ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

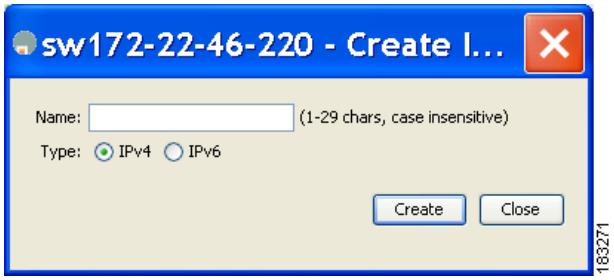
図 5-2　[IP ACL] ダイアログボックス



ステップ 2　[Create] ボタンをクリックして、IP-ACL プロファイルを作成します。

[Create IP ACL Profiles] ダイアログボックスが表示されます（図 5-3 を参照）。

図 5-3　[Create IP ACL Profiles] ダイアログボックス



ステップ 3　IP-ACL プロファイルの名前を入力します。

ステップ 4　[Create] ボタンをクリックしてから [Close] ボタンをクリックします。

新しい IP-ACL プロファイルを作成します。

ステップ 5　作成した IP-ACL をクリックし、[Rules] ボタンをクリックします。

Device Manager を使用している場合は、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。Fabric Manager を利用すると、1 つのプロファイルに対する既存のルールを並び替えることができます。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。

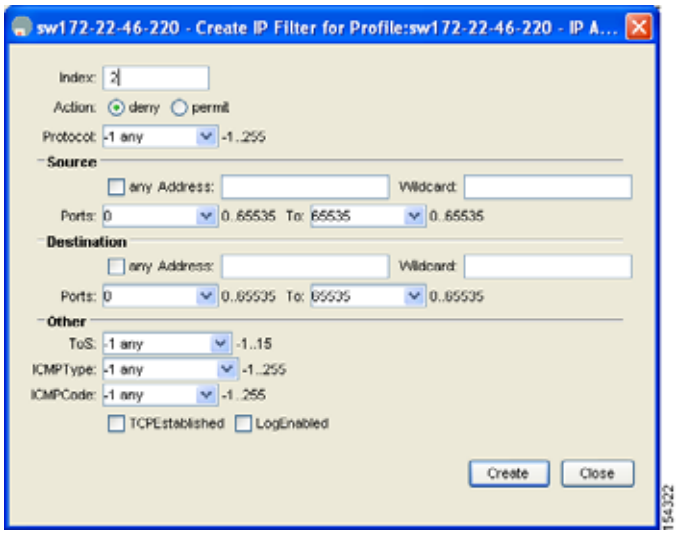
[IP ACL] ダイアログボックスが表示されます（図 5-4 を参照）。

図 5-4　[IP ACL Profile] ダイアログボックス

ステップ 6　[Create] ボタンをクリックして、IP フィルタを作成します。

[Create IP Filter] ダイアログボックスが表示されます（図 5-5 を参照）。

図 5-5　[Create IP Filter] ダイアログボックス



ステップ 7　[Action] から [permit] または [deny] のいずれかのオプション ボタンを選択し、[Protocol] フィールドに IP 番号を設定します。ドロップダウン メニューには、一般的なフィルタリングされたプロトコルが提供されています。

ステップ 8　フィルタを適用する送信元 IP アドレスおよびワイルドカード マスクを設定します。すべての IP アドレスに対して適用する場合には、[any] チェックボックスをオンにします。

これにより、フレームの送信元 IP アドレスをチェックする IP フィルタが作成されます。

（注）　ワイルドカード マスクには、一致させる IP アドレスのサブネットを指定します。フィルタは、指定したアドレス範囲に対して適用されます。

ステップ 9　TCP または UDP のプロトコルを選択した場合には、トランスポート レイヤの送信元ポート範囲を設定します。

ステップ 10　宛先 IP アドレスおよびポート範囲について、ステップ 8 とステップ 9 を繰り返します。

これにより、フレームの宛先 IP アドレスをチェックする IP フィルタが作成されます。

ステップ 11　必要に応じて、[ToS]、[ICMPType]、および [ICMPCode] フィールドを設定します。

ステップ 12　ACK、FIN、PSH、RST、SYN、または URG 制御ビット セットを含む TCP 接続を一致させたい場合には、[TCPEstablished] チェックボックスをオンにします。

ステップ 13　この IP フィルタと一致する全フレームのログを作成する場合には、[LogEnabled] チェックボックスをオンにします。

ステップ 14　[Create] ボタンをクリックして、この IP フィルタを作成し、IP-ACL に追加します。

既存の IPv4-ACL または IPv6-ACL からの IP フィルタの削除

Device Manager を使用して既存の IPv4-ACL または IPv6-ACL から、設定したエントリを削除する手順は、次のとおりです。

ステップ 1　[Security] > [IP ACLs] を選択します。
[IP ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

ステップ 2　修正する IP-ACL をクリックしてから [Rules] ボタンをクリックします。
このプロファイルに関連する IP フィルタのリストが表示されます（図 5-4 を参照）。

ステップ 3　削除するフィルタを選択してから [Delete] ボタンをクリックし、その IP フィルタを削除します。

IP-ACL の削除

IP-ACL を削除する前に、IP-ACL とインターフェイスの関連付けを削除する必要があります。
Fabric Manager で IP-ACL を削除する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。
[Information] ペインに、IP-ACL の設定が表示されます。

ステップ 2　[Profiles] タブをクリックします。
スイッチ、ACL、およびプロファイル名のリストが表示されます。

ステップ 3　削除する行を選択します。複数の行を削除する場合は、Shift キーを押しながら行を選択します。

ステップ 4　[Delete Row] をクリックします。IP-ACL が削除されます。

IP-ACL ログ ダンプの読み取り

このフィルタ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、IP フィルタ作成の際に [LogEnabled] チェックボックスを使用します。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。

入力 ACL に対しては、ログは無加工の Media Access Control（MAC; メディア アクセス制御）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 フレームの表示ではなく、ログにダンプされるレイヤ 2 の MAC レイヤ情報を指しています。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
```

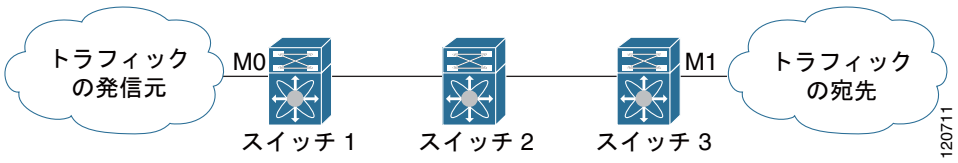
インターフェイスへの IP-ACL の適用

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、管理用インターフェイス、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　トラフィックフ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ブロックする場合は、スイッチ 3 の M1 に対するアウトバンド フィルタのかわりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます（図 5-6 を参照）。

図 5-6　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 トラフィックだけに作用します。

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 インターフェイスに存在します。mgmt0 は予約済みの ACL 名であり、使用することができないので、ユーザには表示されません。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。

Fabric Manager を使用してインターフェイスに IP-ACL を適用する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IP ACL] を選択します。

[Information] ペインに、IP-ACL の設定が表示されます。

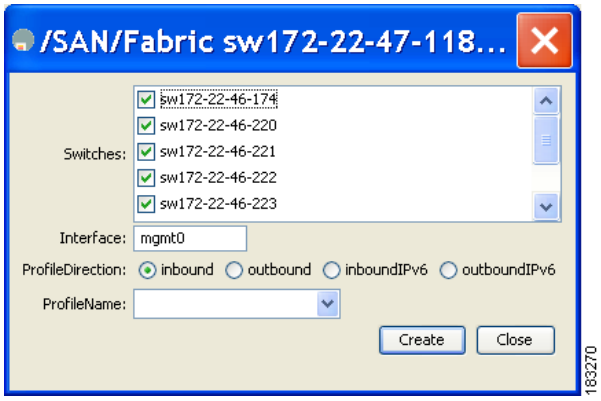
ステップ 2　[Interfaces] タブをクリックします。

インターフェイスおよび関連 IP-ACL のリストが表示されます。

ステップ 3　[Create Row] アイコンをクリックします。

[Create Interfaces] ダイアログボックスが表示されます（図 5-7 を参照）。

図 5-7　[Create Interfaces] ダイアログボックス



ステップ 4　（任意）IP-ACL に含めないスイッチを削除する場合は、スイッチ アドレス横のチェックボックスをオフにします。

IPv4-ACL または IPv6-ACL に関連付けるインターフェイスを [Interface] フィールドで設定します。

ステップ 5　[ProfileDirection]（[inbound] または [outbound] のいずれか）を選択します。

ステップ 6　[Profile Name] フィールドに IP-ACL の名前を入力します。

（注）　この IP-ACL 名は、すでに [Create Profiles] ダイアログボックスを使用して作成済みでなければなりません。作成されていない場合、[Create Profiles] ダイアログボックスを開いてプロファイルを作成するまで、どのフィルタもイネーブルになりません。

ステップ 7　[Creat] ボタンをクリックして IP-ACL に関連付けます。

新しく関連づけたアクセス リストが IP-ACL のリストの中に表示されます。

IP-ACL 設定の例

管理アクセスを規制する IP-ACL を、Device Manager を使用して定義する手順は、次のとおりです。

ステップ 1　[Security] > [IP ACL] を選択します。

[IP-ACL] ダイアログボックスが表示されます（図 5-2 を参照）。

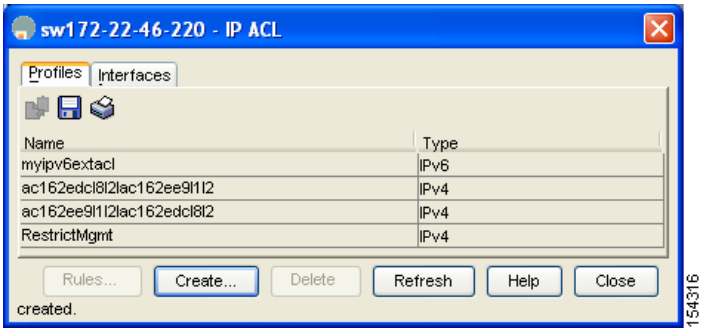
ステップ 2　[Create] ボタンをクリックして IP-ACL を作成します。

[Create IP ACL Profiles] ダイアログボックスが表示されます（図 5-3 を参照）。

ステップ 3　プロファイル名として **RestrictMgmt** を入力してから [Create] ボタンをクリックします。

RestrictMgmt という名前の空の IP-ACL が作成されます（図 5-8 を参照）。

図 5-8　リストに追加された RestrictMgmt プロファイル



ステップ 4　[RestrictMgmt] を選択してから [Rules] ボタンをクリックします。

このプロファイルに関連する IP フィルタの空のリストが表示されます。

ステップ 5　[Create] ボタンをクリックして最初の IP フィルタを作成します。

[Create IP Filter] ダイアログボックスが表示されます（図 5-5 を参照）。

ステップ 6　信頼できるサブネットからの管理コミュニケーションを許可するための IP フィルタを作成します。

a.　[Action] から [permit] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

b.　送信元 IP アドレスを 10.67.16.0 に、ワイルドカード マスクを 0.0.0.255 に設定します。

（注）　ワイルドカード マスクには、一致させる IP アドレスのサブネットを指定します。フィルタは、指定したアドレス範囲に対して適用されます。

c.　宛先アドレスとして [any] チェックボックスをオンにします。

d.　[Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a ～ステップ d を繰り返して、10.67.16.0/24 サブネットのすべてのアドレスに通信を許可する IP フィルタを作成します。

ステップ 7　ICMP ping コマンドを許可するフィルタを次の手順で作成します。

a.　[Action] から [permit] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [1-ICMP] を選択します。

b. 送信元アドレスとして [any] チェックボックスをオンにします。

c. 宛先アドレスとして [any] チェックボックスをオンにします。

d. [ICMPType] ドロップダウン メニューで [8 echo] を選択します。

e. [Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

ステップ a ～ステップ e を繰り返して、ICMP ping を許可する IP フィルタを作成します。

ステップ 8　他のすべてのトラフィックをブロックする最後の IP フィルタを次の手順で作成します。

a. [Action] から [deny] オプション ボタンを選択し、[Protocol] ドロップダウン メニューで [0 IP] を選択します。

b. 送信元アドレスとして [any] チェックボックスをオンにします。

c. 宛先アドレスとして [any] チェックボックスをオンにします。

d. [Create] ボタンをクリックしてこの IP フィルタを作成し、RestrictMgmt IP-ACL に追加します。

e. [Close] ボタンをクリックして、[Create IP Filter] ダイアログボックスを閉じます。

ステップ a ～ステップ d を繰り返して、他のすべてのトラフィックをブロックする IP フィルタを作成します。

ステップ 9　次の手順で mgmt0 インターフェイスに RestrictMgmt IP ACL を適用します。

a. [Security] をクリックし、[IP ACL] を選択してから [IP ACL] ダイアログボックスで [Interfaces] タブをクリックします。

b. [Create] ボタンをクリックします。

[Create IP-ACL Interfaces] ダイアログボックスが表示されます。

c. [Interfaces] ドロップダウン メニューで [mgmt0] を選択します。

d. [Profile Director] の [inbound] オプション ボタンを選択します。

e. [ProfileName] ドロップダウン メニューで [RestrictMgmt] を選択します。

f. [Create] ボタンをクリックして RestrictMgmt IP-ACL を mgmt0 インターフェイスに適用します。

ステップ a ～ステップ f を繰り返して、IP-ACL を mgmt0 インターフェイスに適用します。

CHAPTER 6

CA およびデジタル証明書の設定

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）サポートにより、Cisco MDS 9000 ファミリ スイッチでは、デジタル証明書を取得および使用して、ネットワーク上での安全な通信を実現できます。PKI サポートにより、IP Security Protocol（IPSec; IP セキュリティ プロトコル）/Internet Key Exchange（IKE; インターネット キー エクスチェンジ）および Secure Shell（SSH; セキュア シェル）の管理機能およびスケーラビリティが提供されます。

この章の内容は、次のとおりです。

CA およびデジタル証明書の概要

ここでは、Certificate Authorities（CA; 認証局）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、加入エンティティに中央集中型のキー管理を実現します。

公開キー暗号法に基づくデジタル シグニチャにより、デバイスおよび個々のユーザがデジタル認証されます。Rivest, Shamir, Adelman（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、秘密が保守され、キーを所有しているデバイスまたはユーザだけに知らされます。一方、公開キーはすべてのエンティティに知らされます。両方のキーは、相互に補完的に動作します。一方のキーで暗号化された情報は、他方のキーで復号化できます。送信者の秘密キーによってデータが暗号化されると、シグニチャが形成されます。受信者は、送信者の公開キーを使用してメッセージを復号化し、シグニチャを確認します。このプロセスでは、受信者が送信者の公開キーのコピーを取得していて、そのキーが確実に送信者のものであり、送信者を装っている他者のものではないことを確信している必要があります。

デジタル証明書は、デジタル シグニチャと送信者をリンクします。デジタル証明書には、名前、シリアル番号、会社名、部門名、または IP アドレスなど、ユーザを識別する情報が含まれています。また、エンティティの公開キーのコピーも含まれています。証明書そのものは、アイデンティティの確認およびデジタル証明書の作成について、受信者によって明示的に信頼されている第三者である CA により署名されています。

CA のシグニチャを確認するには、受信者が CA の公開キーを知っ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、ほとんどの Web ブラウザには、デフォルトでいくつかの 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 エクスチェンジ（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。

トラスト モデル、トラスト ポイント、およびアイデンティティ 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で信頼できる 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 ポイントは、*アイデンティティ CA* と呼ばれます。

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 サイズは 512 です。RSA キーペア ラベルを設定することもできます。デフォルトのキー ラベルは、スイッチの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）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に限定されることはありません。
- 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。アプリケーションは、発行元 CA によって証明書に指定された目的に基づいて、アイデンティティ証明書を使用します。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 スイッチの完全修飾ドメイン名です。
- 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。
- アプリケーションに 1 つ以上のトラスト ポイントを指定する必要はありません。アプリケーションは、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、どのトラスト ポイントから発行された証明書でも使用できます。
- 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たりする必要はありません。CA は、指定されたアイデンティティ（名前）を 1 度だけ認証し、同じサブジェクト名で複数の証明書を発行することはありません。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。

信頼できる CA を複数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 登録サポート

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. CA から発行され、CA の秘密キーが署名された証明書を受信します。
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。

（注） Fabric Manager は、カットアンドペーストをサポートしていません。代わりに、登録要求（証明書署名要求）をファイルに保存して、CA に手動で送信できます。

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 1 つから発行されているかどうかの確認。
- ピア証明書が、現時点で有効（期限切れではない）かどうかの確認。
- ピア証明書が発行元 CA により失効されていないかどうかの確認。

失効チェックでは、2 つの方式がサポートされています。Certificate Revocation List（CRL; 証明書失効リスト）および Online Certificate Status Protocol（OCSP）です。トラスト ポイントは、いずれかまたは両方の方式を使用して、ピア証明書が失効され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。ピア証明書を確認するクライアントは、発行元 CA から最新の CRL を取得し、この情報を使用して、証明書が失効しているかどうかを判別する必要があります。クライアントは、すべてのまたは一部の信頼できる CA の CRL をローカルでキャッシュし、CRL が期限切れになるまで、必要に応じて使用できます。

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限り、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。

OCSP サポート

Online Certificate Status Protocol（OCSP）は、オンラインでの証明書失効チェックを容易にします。各トラスト ポイントに OCSP URL を指定できます。アプリケーションは、失効チェック方式を、指定された順序で選択します。CRL、OCSP、none、またはこれらの方式の組み合わせを指定できます。

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 認証および登録プロセスの一環として、下位 CA の証明書（または証明書チェーン）およびアイデンティティ証明書を、標準 Privacy Enhanced Mail（PEM）（base64）形式でインポートできます。

また、トラスト ポイントの完全なアイデンティティ情報を、パスワードで保護された Public Key Certificate Syntax（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。

ホスト名および IP ドメイン名の設定方法については、『*Cisco MDS 9000 NX-OS Fundamental Configuration Guide*』を参照してください。

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。

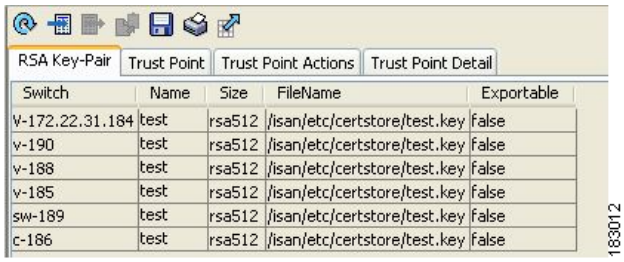
Fabric Manager を使用して RSA キーペアを生成する手順は、次のとおりです。

ステップ 1　[Information] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[RSA Key-Pair] タブをクリックします。

図 6-1 の情報が表示されます。

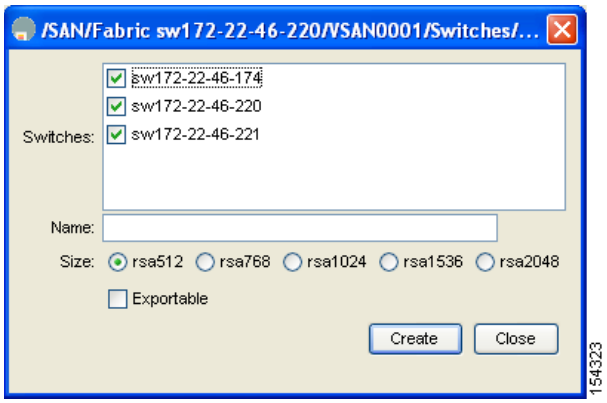
図 6-1　RKI RSA キーペア情報



ステップ 3　[Create Row] アイコンをクリックします。

[Create RSA Key-Pair] ダイアログボックスが表示されます（図 6-2 を参照）。

図 6-2　[Create RSA Key-Pair] ダイアログボックス



ステップ 4　RSA キーペアを作成したいスイッチを選択します。

ステップ 5　RSA キーペアに名前を指定します。

ステップ 6　サイズまたは絶対値を選択します。有効な絶対値は、512、768、1024、1536、および 2048 です。

（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。

（注）　スイッチに設定できるキーペアの最大数は、16 です。

ステップ 7　キーをエクスポート可能にする場合には、[Exportable] チェックボックスをオンにします。

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。

（注）　PKCS#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。

ステップ 8　[Create] ボタンをクリックして、RSA キーペアを作成します。

トラスト ポイント CA アソシエーションの作成

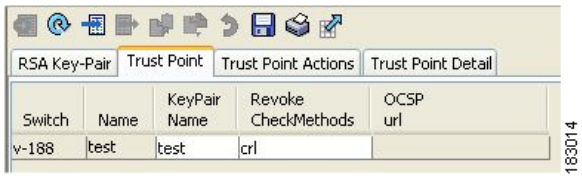
Fabric Manager を使用してトラスト ポイント CA アソシエーションを作成する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point] タブをクリックします。

図 6-3 の情報が表示されます。

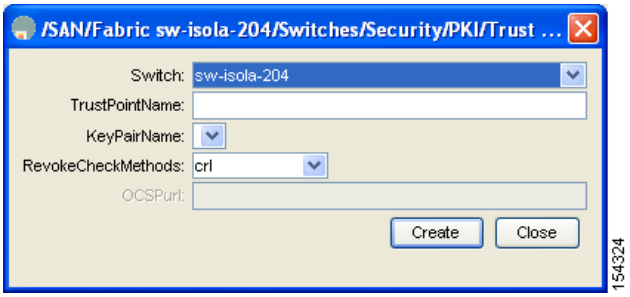
図 6-3　[Trust Point] タブ



ステップ 3　[Create Row] アイコンをクリックします。

[Create Trust Point] ダイアログボックスが表示されます（図 6-4 を参照）。

図 6-4　[Create Trust Point] ダイアログボックス



ステップ 4　[Switch] ドロップダウン メニューから、トラスト ポイント CA を作成するスイッチを選択します。

ステップ 5　トラスト ポイント CA に名前を指定します。

ステップ 6　登録時に、このトラスト ポイントに関連付けるキーペアの名前を選択します。「RSA キーペアの生成」（P.6-6）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。

ステップ 7　[RevokeCheckMethod] ドロップダウン メニューから、使用したい証明書失効チェック方式を選択します（図 6-4 を参照）。CRL、OCSP、CRL OCSP、または OCSP CRL を使用して、証明書の失効をチェックできます。CRL OCSP オプションでは、最初にローカルに保管されている CRL を使用して証明書の失効がチェックされます。見つからない場合、OCSP を使用して、ステップ 7 で指定した URL 上で証明書の失効がチェックされます。

ステップ 8　OCSP 証明書失効チェック方式を選択した場合には、OCSP の URL を入力します。

（注）　OCSP の URL は、失効チェック方式を設定する前に、設定しておく必要があります。

ステップ 9　[Create] ボタンをクリックして、トラスト ポイント CA を作成します。

ブートフラッシュへのファイルのコピー

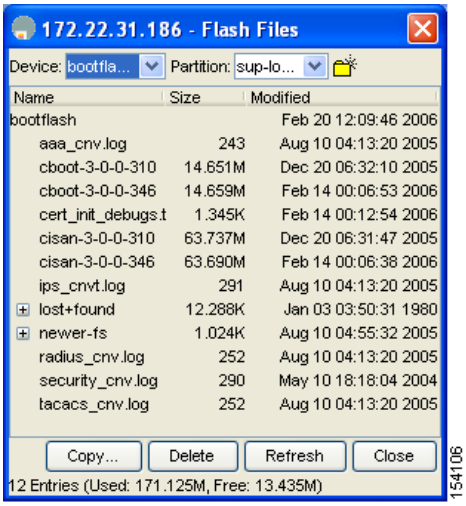
Device Manager を使用してブートフラッシュにファイルをコピーする手順は、次のとおりです。

ステップ 1　[Admin] > [Flash Files] を選択します。

ステップ 2　[Device] フィールドでブートフラッシュを選択します。

図 6-5 に示すダイアログボックスに、フラッシュ ファイルのリストが表示されます。

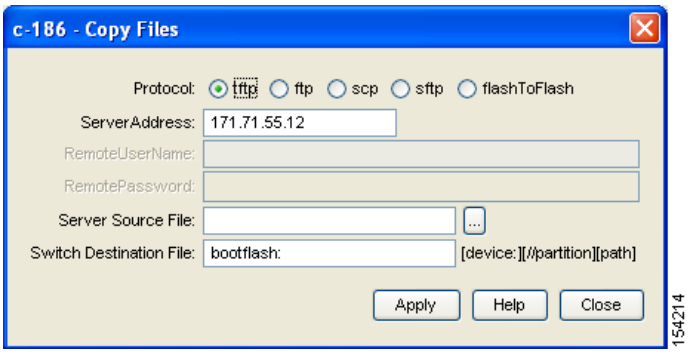
図 6-5　　フラッシュ ファイル



ステップ 3　[Copy] をクリックします。

[Copy Files] ダイアログボックスが表示されます（図 6-6 を参照）。

図 6-6　　[Copy Files] ダイアログボックス



ステップ 4　[Protocol] フィールドで、[tftp] を選択します。

ステップ 5　[Browse] ボタンをクリックして、ブートフラッシュにコピーする適切なファイルを検索します。

ステップ 6　[Apply] ボタンをクリックして、変更内容を適用します。

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限り、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。CA の証明書は自己署名されている（CA が自身の証明書に署名する）ので、CA 証明書のフィンガープリントを比較するために、CA の管理者に連絡して CA の公開キーを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、証明書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 証明書チェーン*と呼ばれます。CA 証明書チェーンに含めることができる証明書の数は、最大 10 個です。

Fabric Manager を使用して CA を認証する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

図 6-7 の情報が表示されます。

図 6-7　[Trust Point Actions] タブ

ステップ 3　[Command] フィールドのドロップダウン メニューをクリックして、適切なオプションを選択します。選択可能なオプションは、[caauth]、[cadelete]、[certreq]、[certimport]、[certdelete]、[pkcs12import]、および [pkcs12export] です。CA を認証して、その CA の証明書または証明書チェーンをトラスト ポイントに設定するには、[caauth] オプションを選択します。

ステップ 4　[URL] フィールドの [Browse] ボタンをクリックして、[Bootflash Files] ダイアログボックスから適切なインポート証明書ファイルを選択します。bootflash:filename 形式で、CA 証明書またはチェーンが含まれているファイル名です。

（注） 特定の CA に対して最大 10 のトラスト ポイントを認証できます。

（注） [Import Certificate] ダイアログボックスで必要なファイルが見つからない場合には、ファイルがブートフラッシュにコピーされているかどうかを確認します。「ブートフラッシュへのファイルのコピー」（P.9）を参照してください。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

認証が確認されるかどうかは、フィンガープリントの手動検証によって証明書が受け入れられるかどうかによります。

（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。

CA 認証の確認

「CA の認証」（P.6-10）のステップ 5 で説明したように、フィンガープリントの確認に基づいて CA 証明書を受け入れるには、CA 認証のあとに CA の確認が必要です。

Fabric Manager を使用して CA 認証を確認する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　トラスト ポイント行の [IssuerCert FingerPrint] カラムの表示から、確認する CA 証明書のフィンガープリントを書き留めます。CA 証明書のフィンガープリントと、CA から通知された（CA の Web サイトから取得した）フィンガープリントを比較します。

フィンガープリントが正確に一致していれば、[Command] ドロップダウン メニューの [certconfirm] コマンドを使用して、CA を受け入れます。一致していない場合は、[certnoconfirm] コマンドを使用して CA を拒否します。

ステップ 4　ステップ 3 で [certconfirm] を選択した場合は、[Command] ドロップダウン メニューから [certconfirm] アクションを選択します。[Apply Changes] アイコンをクリックします。

ステップ 3 で [certnoconfirm] を選択した場合は、[Command] ドロップダウン メニューから [certnoconfirm] アクションを選択します。[Apply Changes] アイコンをクリックします。

証明書の失効チェック方式の設定

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、複数の方式があります。スイッチが CA からダウンロードした CRL をチェックするように設定するか（「CRL の設定」（P.6-15）を参照）、ネットワークでサポートされている場合には OSCP を使用するか、またはその両方を使用できます。CRL をダウンロードしてローカルでチェックを実行する場合には、ネットワーク 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。OSCP では、CA の最新の CRL をチェックできます。ただし、OSCP を使用するとネットワーク トラフィックが生成されるので、ネットワークの効率に影響することがあります。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 チェックと OSCP の両方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。

Fabric Manager では、トラスト ポイント CA の作成時に証明書失効チェック方式を設定できます。「トラスト ポイント CA アソシエーションの作成」（P.6-8）を参照してください。

証明書要求の生成

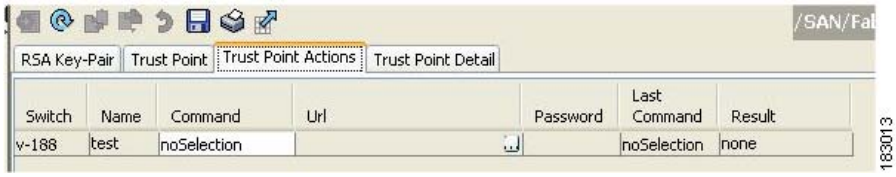
スイッチの各 RSA キーペアについて、関連付けたトラスト ポイント CA からアイデンティティ証明書を取得するには、要求を生成する必要があります。さらに、表示された要求を、CA 宛ての E メール メッセージまたは Web サイト フォームにカットアンドペーストします。

Fabric Manager を使用して、CA への署名入り証明書要求を生成する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします（図 6-8 を参照）。

図 6-8　[Trust Point Actions] タブ



ステップ 3　[Command] ドロップダウン メニューから、[certreq] オプションを選択します。このトラスト ポイント エントリに対応する CA のアイデンティティ証明書を取得するために必要な pkcs#10 Certificate Signing Request（CSR; 証明書署名要求）が生成されます。エントリには、関連付けたキーペアが必要です。CA 証明書または証明書チェーンが、**caauth** 処理によって設定されている必要があります。「CA の認証」（P.6-10）を参照してください。

ステップ 4　生成した証明書要求を保管する出力ファイル名を入力します。PEM 形式で生成された CSR が保管されます。bootflash:filename 形式を使用します。この CSR を、アイデンティティ証明書を取得する CA に送信する必要があります。アイデンティティ証明書を取得したあと、証明書をこのトラスト ポイントにインストールします。「アイデンティティ証明書のインストール」（P.6-12）を参照してください。

ステップ 5　CSR に含める *チャレンジ* パスワードを入力します。

（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。

ステップ 6　[Apply Changes] アイコンをクリックして、変更内容を保存します。

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。符号化テキストをカットアンドペーストして、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。

Fabric Manager を使用して、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手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [certimport] オプションを選択して、このトラスト ポイントにアイデンティティ証明書をインポートします。アイデンティティ証明書は、事前に生成した CSR により、対応する CA から取得します（「証明書要求の生成」（P.6-12）を参照）。

（注）　アイデンティティ証明書は、ブートフラッシュ内に PEM 形式のファイルで保存されている必要があります。

ステップ 4　URL フィールドに、ブートフラッシュにコピーされている証明書ファイルの名前を、bootflash:filename 形式で入力します。

ステップ 5　[Apply Changes] アイコンをクリックして変更内容を保存します。

正常に実行されると、アイデンティティ証明書の値、および証明書のファイル名などの関連オブジェクトが、アイデンティティ証明書内の対応する属性に応じて、適切な値に自動的に更新されます。

コンフィギュレーションの保存

変更した設定は、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。

Fabric Manager を使用してコンフィギュレーションを保存する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] を展開し、[Copy Configuration] を選択します。

ステップ 2　RSA キーペアおよび証明書を含む、スイッチのコンフィギュレーションを選択します。

ステップ 3　[Apply Changes] アイコンをクリックして、変更内容を保存します。

リブート後のトラスト ポイント設定の存続

トラスト ポイント設定は、標準の Cisco NX-OS 設定なので、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た場合に限り、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」（P.6-14）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。ここで説明する内容は、次のとおりです。

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は、トラストポイントの RSA キーおよび CA 証明書と一緒に PKCS#12 形式のファイルにエクスポートしてバックアップできます。以降で、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* 形式だけがサポートされます。

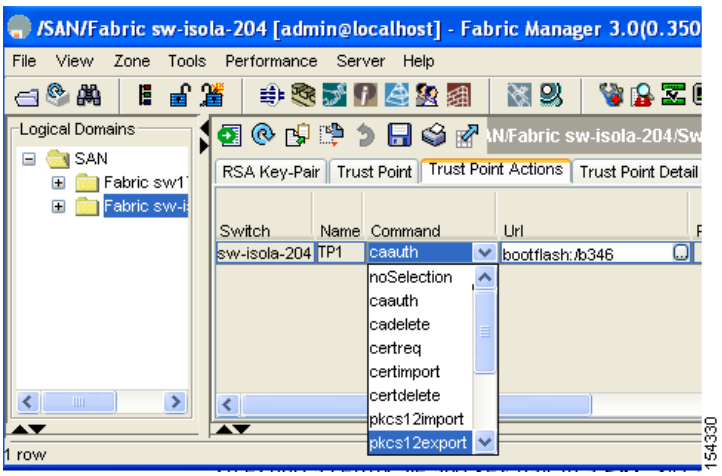
Fabric Manager を使用して、証明書およびキーペアを PKCS#12 形式ファイルにエクスポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします（図 6-9 を参照）。

ステップ 3　[Command] ドロップダウン メニューで [pkcs12export] オプションを選択し、選択したトラスト ポイントからキーペア、アイデンティティ証明書、および CA 証明書または証明書チェーンを PKCS#12 形式でエクスポートします。

図 6-9　キーペアをエクスポートする [pkcs12export] オプション



ステップ 4　エクスポートした PKCS#12 アイデンティティを保存する出力ファイル名を、bootflash:filename 形式で入力します。

ステップ 5　必要なパスワードを入力します。このパスワードは、PKCS#12 データの符号化用に設定されます。正常に完了すると、エクスポートしたデータがブートフラッシュ内の指定ファイルに格納されます。

ステップ 6　[Apply Changes] アイコンをクリックして、変更内容を保存します。

PKCS#12 形式ファイルとして保存された証明書およびキーペアをインポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします（図 6-9 を参照）。

ステップ 3　[Command] ドロップダウン メニューで [pkcs12import] オプションを選択し、PKCS#12 形式のキーペア、アイデンティティ証明書、および CA 証明書または証明書チェーンを、選択したトラスト ポイントにインポートします。

ステップ 4　PKCS#12 アイデンティティを含む入力ファイル名を、bootflash:filename 形式で入力します。

ステップ 5　必要なパスワードを入力します。このパスワードは、PKCS#12 データの復号化用に設定されます。完了すると、インポートしたデータがブートフラッシュ内の指定ファイルに格納されます。

ステップ 6　[Apply Changes] アイコンをクリックして、変更内容を保存します。

完了すると、RSA キーペア テーブルに、インポートしたキーペアに対応するトラスト ポイントが作成されます。トラスト ポイントの証明書情報が更新されます。

（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

Fabric Manager を使用して、ファイルからトラスト ポイントに CRL を設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [crlimport] オプションを選択して、選択したトラスト ポイントに CRL をインポートします。

ステップ 4　[URL] フィールドに、CRL の入力ファイル名を bootflash:filename の形式で入力します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

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および 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てから、CA 証明書を削除する必要があります。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。

Fabric Manager を使用して、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。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [cadelete] オプションを選択して、トラスト ポイントからアイデンティティ証明書を削除します。

（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の場合には、**forcecertdelete** 処理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 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

アイデンティティ証明書を削除するには、[Trust Point Actions] タブをクリックし、[Command] ドロップダウン メニューから [certdelete] または [forcecertdelete] を選択します。

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。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[PKI] を選択します。

ステップ 2　[Information] ペインで、[RSA Key-Pair] タブをクリックします。

ステップ 3　[Delete Row] アイコンをクリックします。

ステップ 4　[Confirmation] ダイアログボックスで、[Yes] ボタンまたは [No] ボタンをクリックします。

（注）　スイッチから RSA キーペアを削除したあと、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」（P.6-12）を参照してください。

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。

ここで説明する内容は、次のとおりです。

- 「アイデンティティ証明書の要求」（P.6-23）
- 「証明書の失効」（P.6-30）
- 「CRL の生成および公開」（P.6-32）
- 「CRL のダウンロード」（P.6-33）
- 「CRL のインポート」（P.6-35）

MDS スイッチでの証明書の設定

Fabric Manager を使用して MDS スイッチに証明書を設定する手順は、次のとおりです。

ステップ 1　[Switches] を選択し、[LogicalName] フィールドでスイッチのホスト名を設定します。

ステップ 2　[Switches] > [Interfaces] > [Management] > [DNS] を選択し、[DefaultDomainName] フィールドを設定します。

ステップ 3　次の手順で、スイッチの RSA キーペアを作成します。

a. [Switches] > [Security] > [PKI] を選択し、[RSA Key-Pair] タブを選択します。

b. [Create Row] アイコンをクリックし、名前とサイズのフィールドを設定します。

c. [Exportable] チェックボックスをオンにして、[Create] ボタンをクリックします。

ステップ 4　次の手順で、トラスト ポイントを作成し、RSA キーペアを関連付けます。

a. [Switches] > [Security] > [PKI] を選択し、[Trustpoints] タブを選択します。

b. [Create Row] アイコンをクリックし、[TrustPointName] フィールドを設定します。

c. [KeyPairName] ドロップダウン メニューから RSA キーペアを選択します。

d. [CARevoke] ドロップダウン メニューから、証明書失効方式を選択します。

e. [Create] ボタンをクリックします。

ステップ 5　[Switches] > [Copy Configuration] を選択し、[Apply Changes] アイコンをクリックして、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、トラスト ポイントとキーペアを保存します。

ステップ 6　トラスト ポイント CA として追加したい CA から、CA 証明書をダウンロードします。

ステップ 7　次の手順で、トラスト ポイントに登録したい CA を認証します。

a. Device Manager を使用して、[Admin] > [Flash Files] を選択し、[Copy] ボタンを選択して、CA 証明書をブートフラッシュに Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）でコピーします。

b. Fabric Manager を使用して、[Switches] > [Security] > [PKI] を選択し、[TrustPoint Actions] タブを選択します。

c. [Command] ドロップダウン メニューから、[cauth] を選択します。

d. [URL] フィールドで [...] をクリックし、ブートフラッシュから CA 証明書を選択します。

e. [Apply Changes] アイコンをクリックして、トラスト ポイントに登録したい CA を認証します。

f. [Information] ペインで [Trust Point Actions] タブをクリックします。

g. トラスト ポイント行の [IssuerCert FingerPrint] カラムの表示から、確認する CA 証明書のフィンガープリントを書き留めます。CA 証明書のフィンガープリントと、CA から通知された（CA の Web サイトから取得した）フィンガープリントを比較します。フィンガープリントが正確に一致していれば、トラスト ポイントの **certconfirm** 処理を実行して、CA を受け入れます。一致していない場合は、トラスト ポイントの **certnoconfirm** 処理を実行して、CA を拒否します。

h. ステップ g で **certconfirm** を選択した場合には、[Trust Point Actions] タブを選択し、[Command] ドロップダウン メニューから [certconfirm] を選択して、[Apply Changes] アイコンをクリックします。

i. ステップ g で **certnoconfirm** を選択した場合には、[Trust Point Actions] タブを選択し、[Command] ドロップダウン メニューから [certnoconfirm] を選択して、[Apply Changes] アイコンをクリックします。

ステップ 8　次の手順で、トラスト ポイントに登録させるための証明書要求を生成します。

a. [Information] ペインで [Trust Point Actions] タブをクリックします。

b. [Command] ドロップダウン メニューから、[certreq] を選択します。このトラスト ポイント エントリに対応する CA のアイデンティティ証明書を取得するために必要な pkcs#10 証明書署名要求（CSR）が生成されます。

c. 生成した証明書要求を保管する出力ファイル名を入力します。bootflash:filename 形式で指定する必要があります。このファイルに、生成した CSR が PEM 形式で保管されます。

d. CSR に含めるチャレンジパスワードを入力します。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。

e. [Apply Changes] アイコンをクリックして、変更内容を保存します。

ステップ 9　CA にアイデンティティ証明書を要求します。

（注）　アイデンティティ証明書が発行される前に、CA から手動での確認が要求されることがあります。

ステップ 10　次の手順で、アイデンティティ証明書をインポートします。

a. Device Manager を使用して、[Admin] > [Flash Files] を選択し、[Copy] ボタンを選択して、CA 証明書をブートフラッシュに TFTP でコピーします。

b. Fabric Manager を使用して、[Switches] > [Security] > [PKI] を選択し、[TrustPoint Actions] タブを選択します。

c. [Command] ドロップダウン メニューから [certimport] オプションを選択して、このトラスト ポイントにアイデンティティ証明書をインポートします。

（注）　アイデンティティ証明書は、ブートフラッシュ内に PEM 形式のファイルで保存されている必要があります。

d. [URL] フィールドに、ブートフラッシュにコピーした証明書ファイルの名前を、bootflash:filename の形式で入力します。

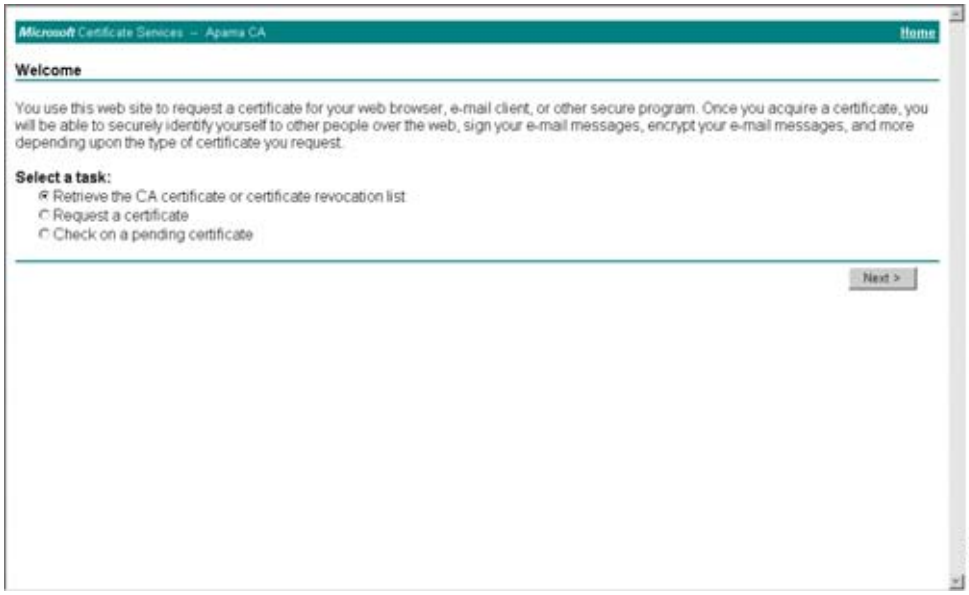
e. [Apply Changes] アイコンをクリックして変更内容を保存します。

正常に実行されると、アイデンティティ証明書の値、および証明書のファイル名などの関連オブジェクトが、アイデンティティ証明書内の対応する属性に応じて、適切な値に自動的に更新されます。

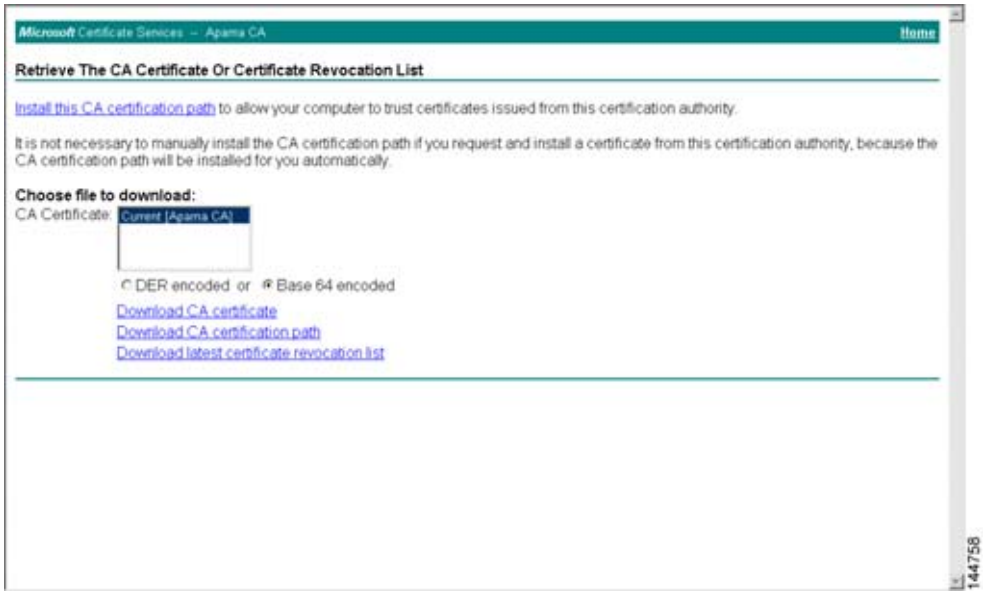
CA 証明書のダウンロード

Microsoft Certificate Services 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。

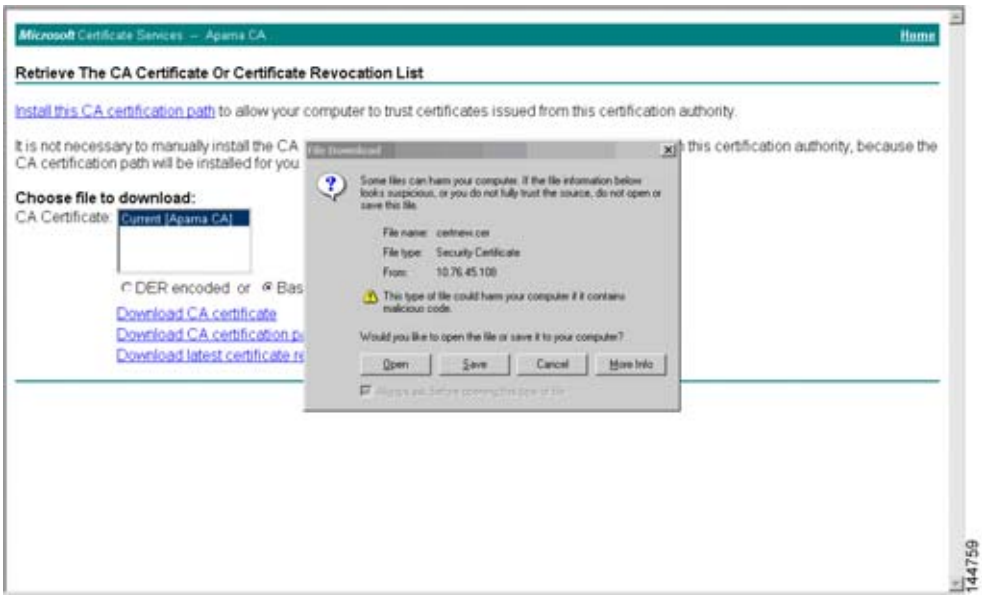
ステップ 1　Microsoft Certificate Services Web インターフェイスの [Retrieve the CA certificate or certificate revocation task] オプション ボタンを選択し、[Next] ボタンをクリックします。



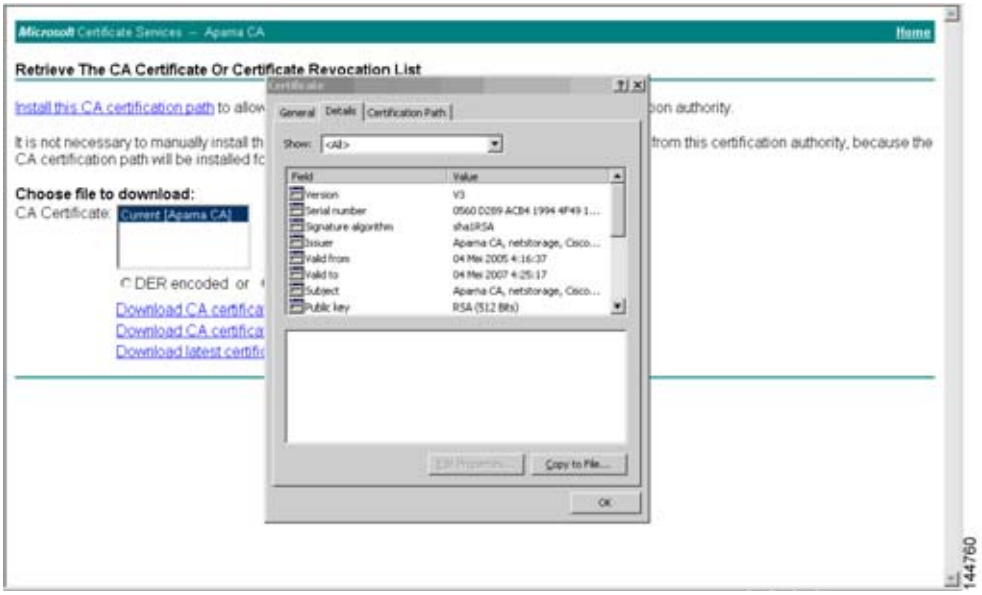
ステップ 2　表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] オプション ボタンをクリックし、[Download CA certificate] リンクをクリックします。



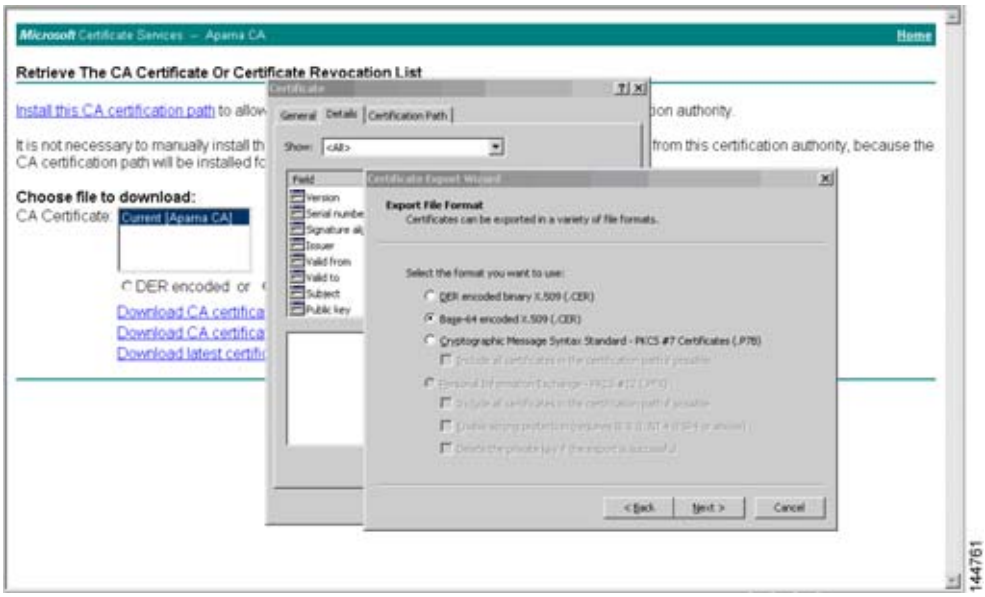
ステップ 3　[File Download] ダイアログボックスで、[Open] ボタンをクリックします。



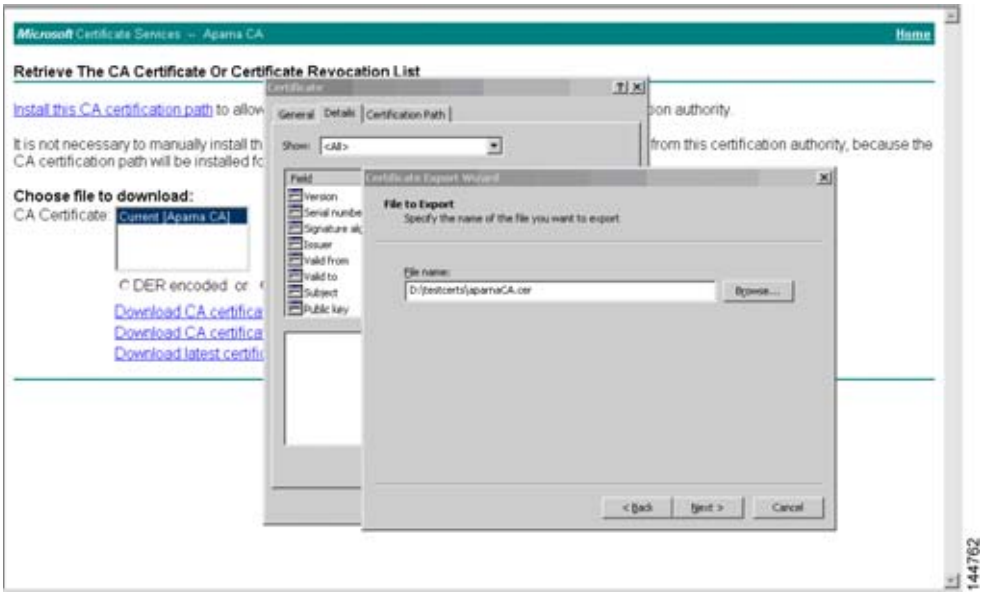
ステップ 4　[Certificate] ダイアログボックスで [Copy to File] ボタンをクリックし、[OK] ボタンをクリックします。



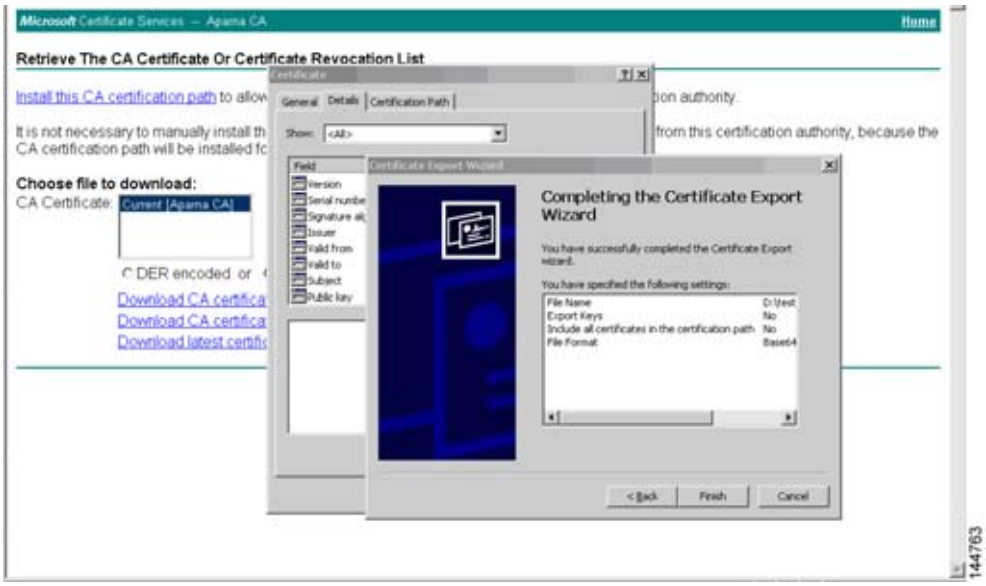
ステップ 5　[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (CER)] オプション ボタンを選択し、[Next] ボタンをクリックします。



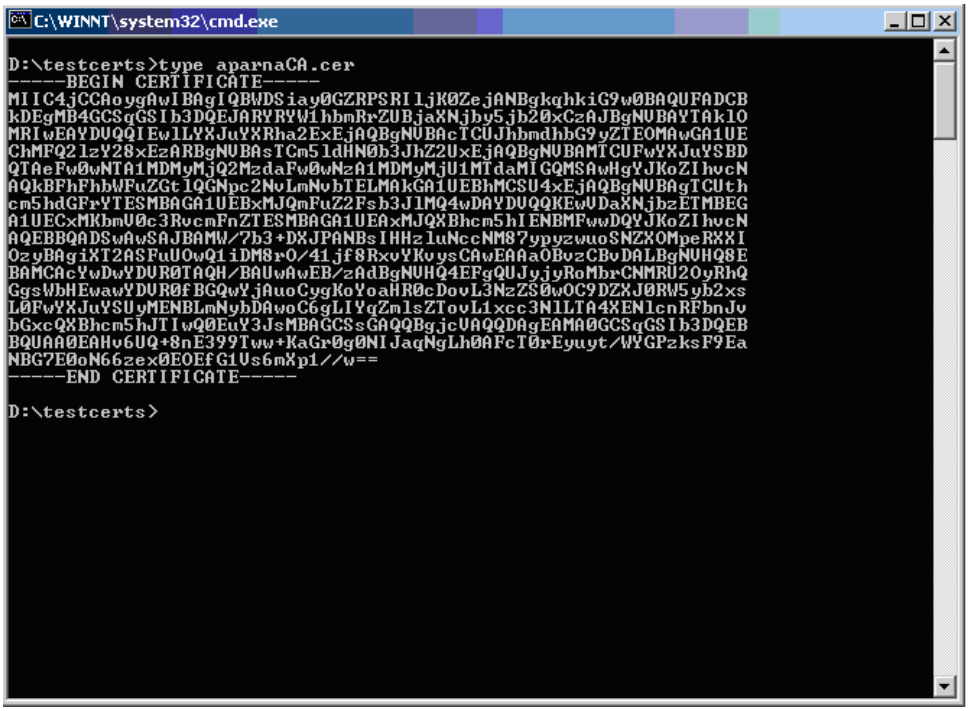
ステップ 6　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] ボタンをクリックします。



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。



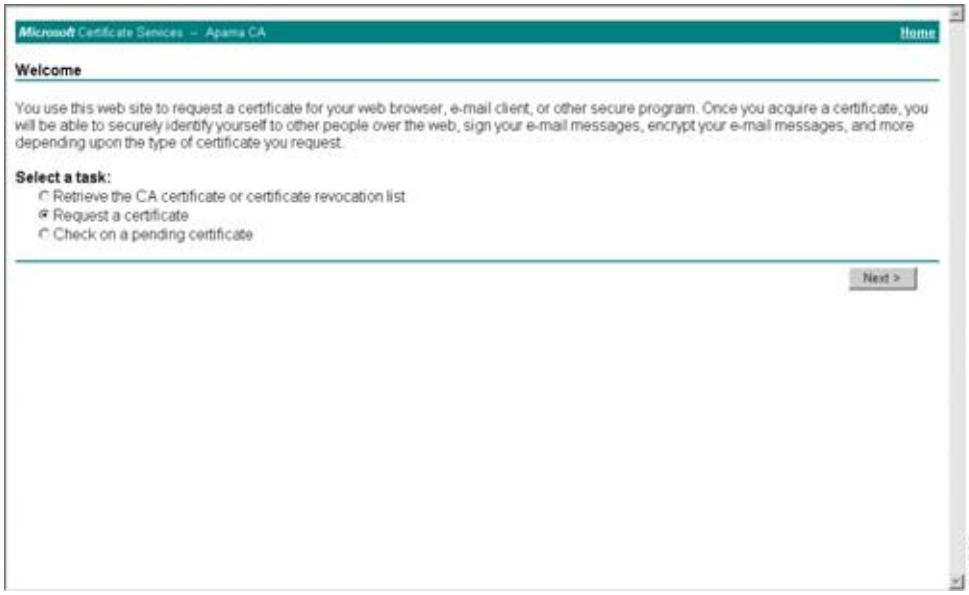
ステップ 8　Microsoft Windows の **type** コマンドを使用して、Base-64（PEM）形式で保存されている CA 証明書を表示します。



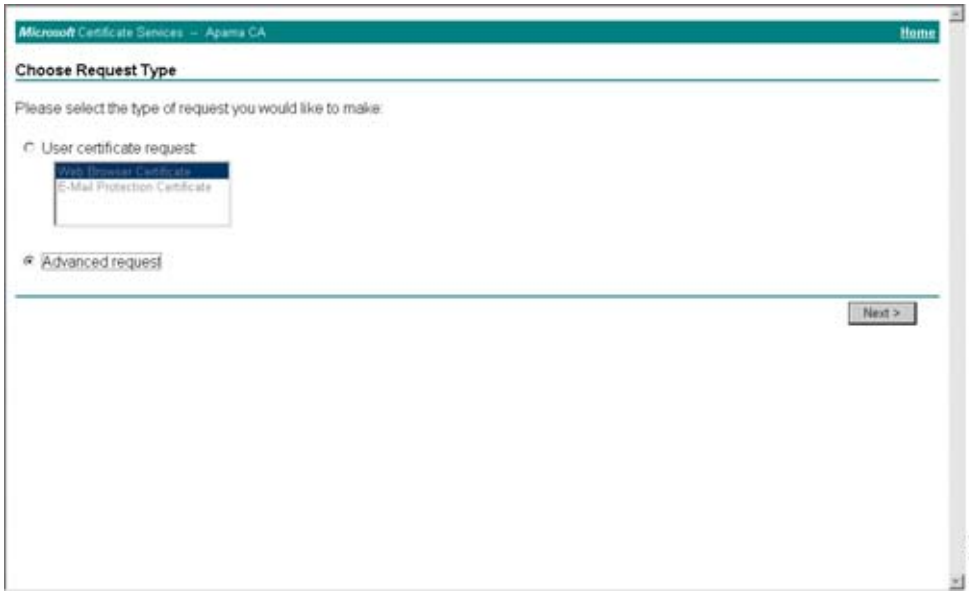
アイデンティティ証明書の要求

PKCS#10 証明書署名要求（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。

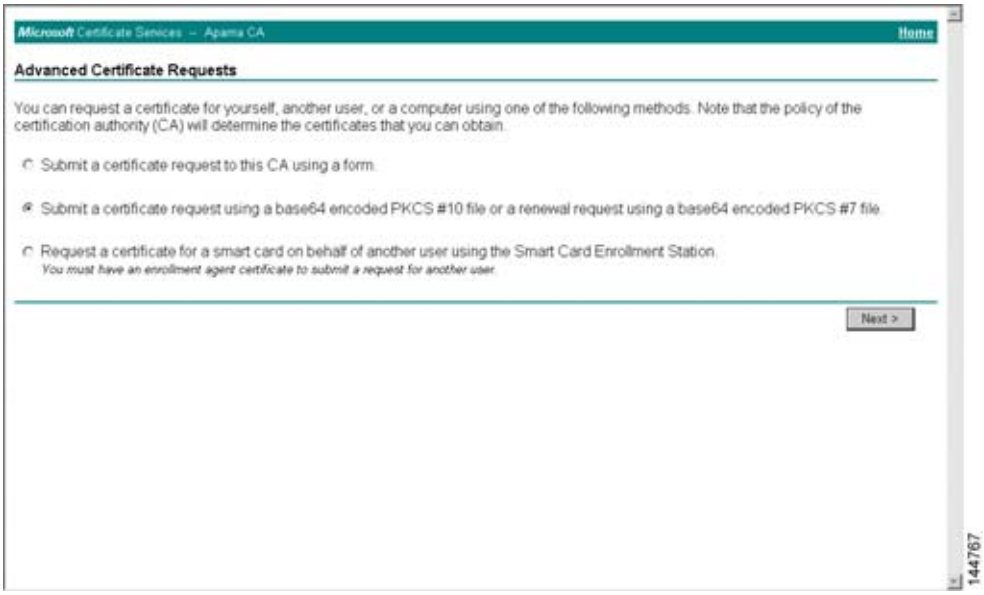
ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request a certificate] オプション ボタンを選択し、[Next] ボタンをクリックします。



ステップ 2　[Advanced Request] オプション ボタンを選択し、[Next] ボタンをクリックします。

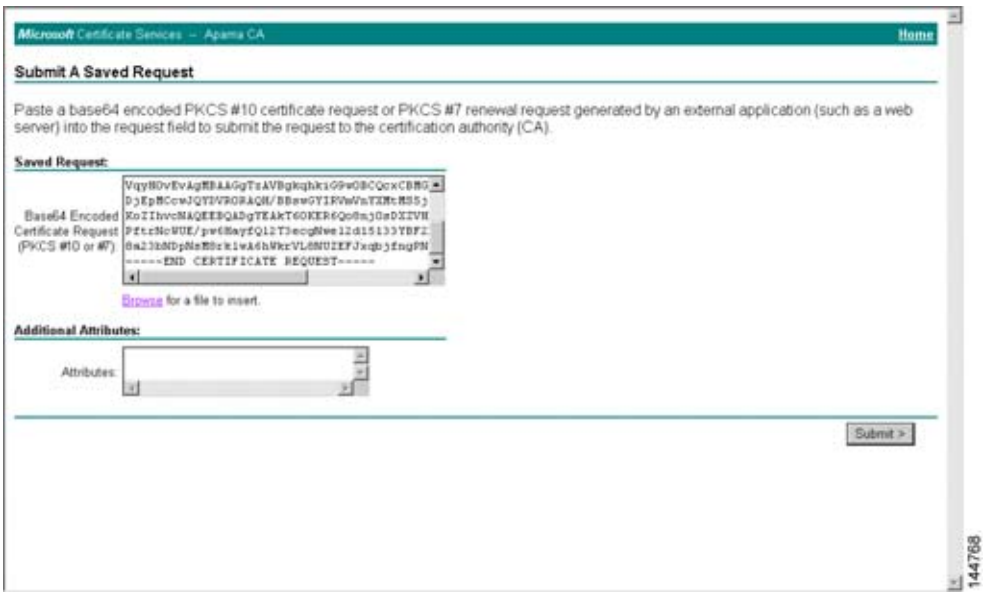


ステップ 3　[Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] オプション ボタンを選択し、[Next] ボタンをクリックします。

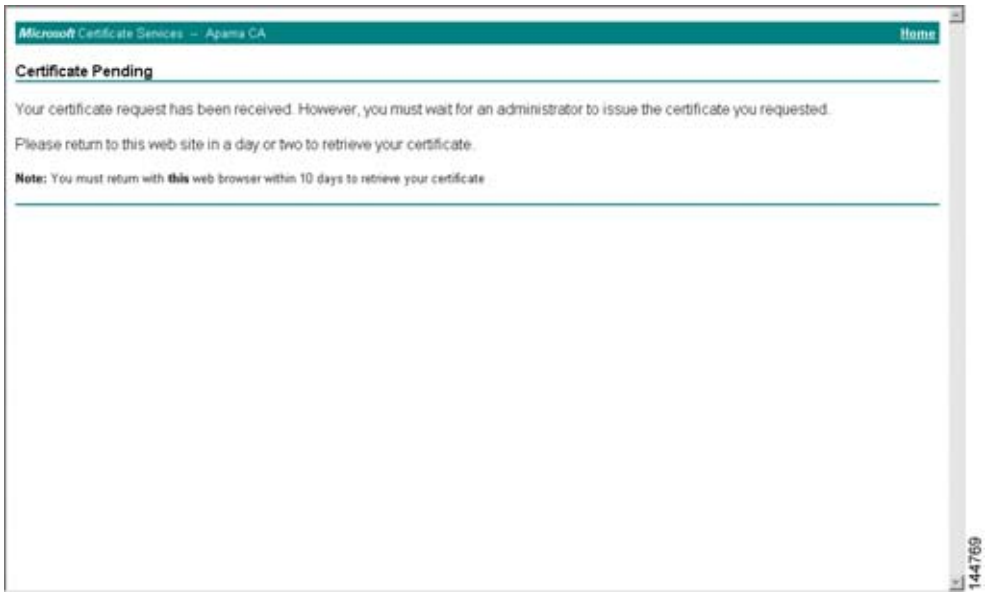


ステップ 4　[Saved Request] テキスト ボックスに base64 PKCS#10 証明書要求をペーストし、[Next] ボタンをクリックします。

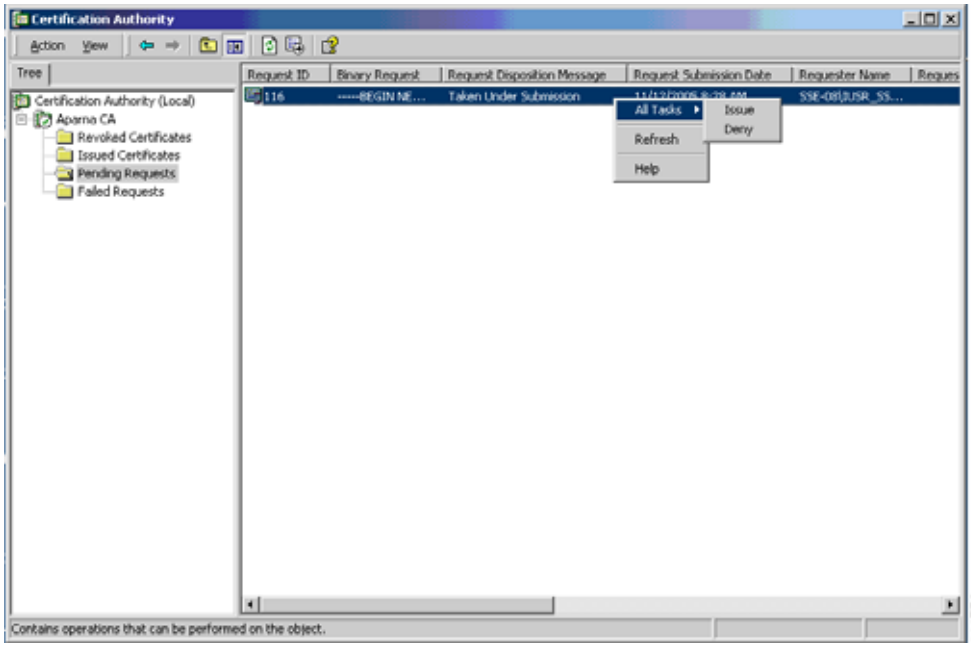
MDS スイッチのコンソールから、証明書要求がコピーされます（「証明書要求の生成」（P.6-12）および「MDS スイッチでの証明書の設定」（P.6-17）を参照）。



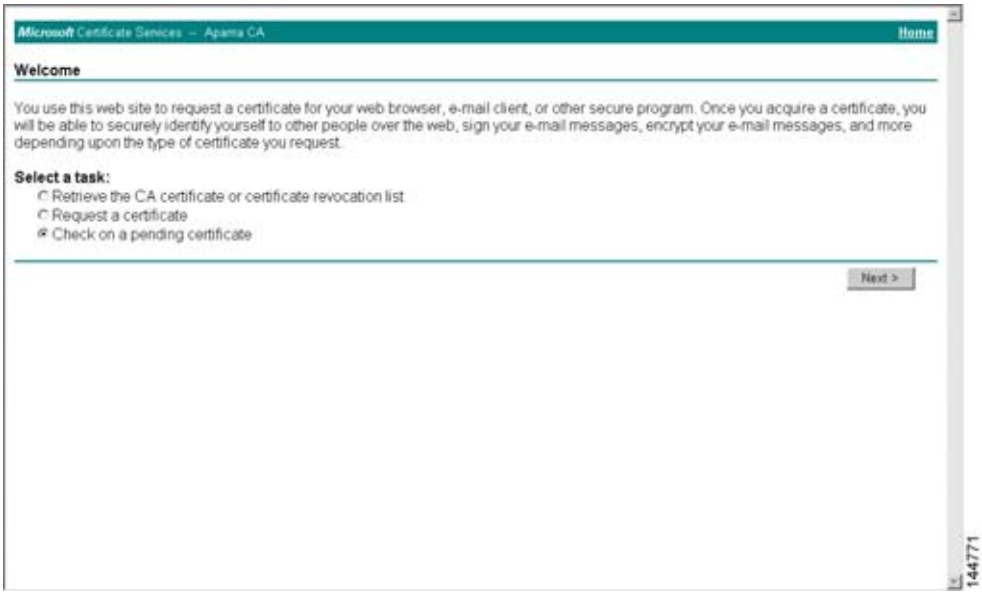
ステップ 5　CA 管理者によって証明書が発行されるまで、1 ～ 2 日、待機します。



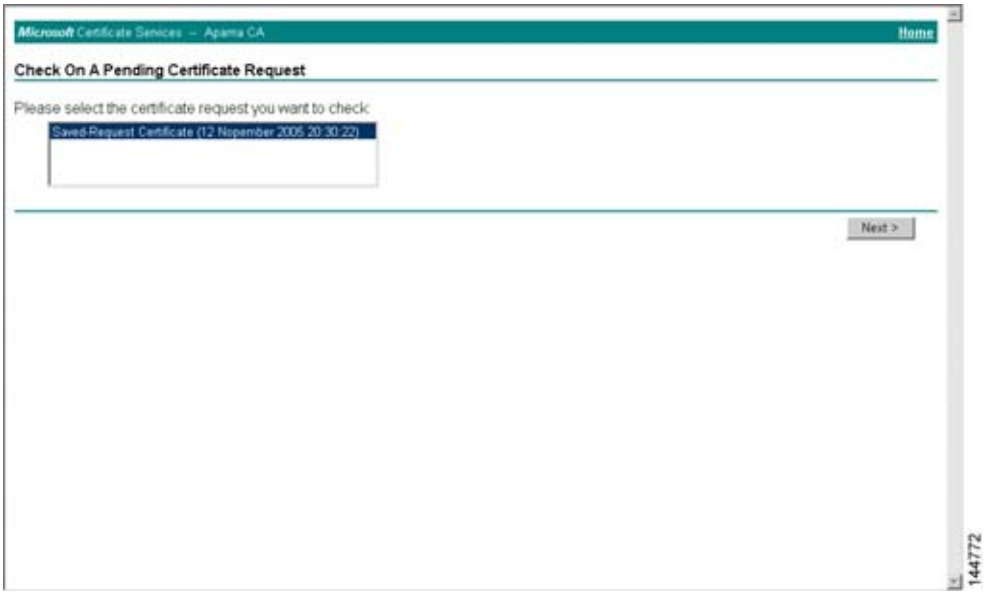
ステップ 6　CA 管理者により証明書要求が承認されます。



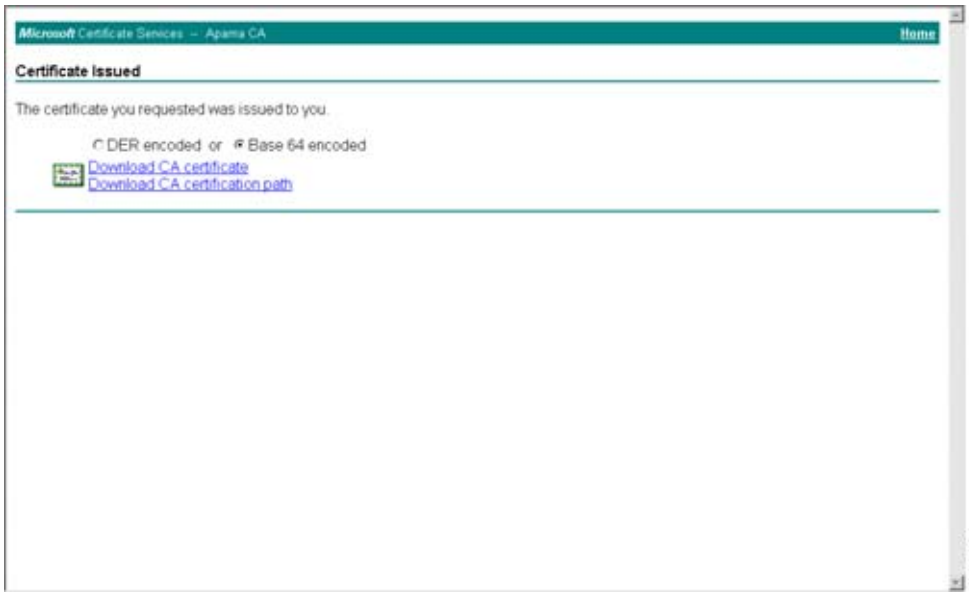
ステップ 7　Microsoft Certificate Services Web インターフェイス上の [Check on a pending certificate] オプションボタンを選択し、[Next] ボタンをクリックします。



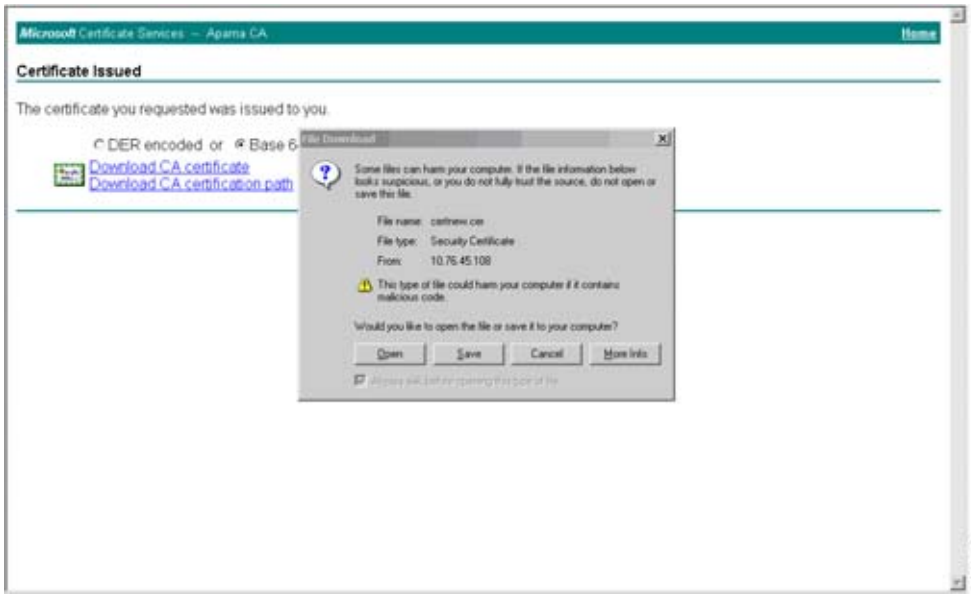
ステップ 8　確認したい証明書要求を選択し、[Next] ボタンをクリックします。



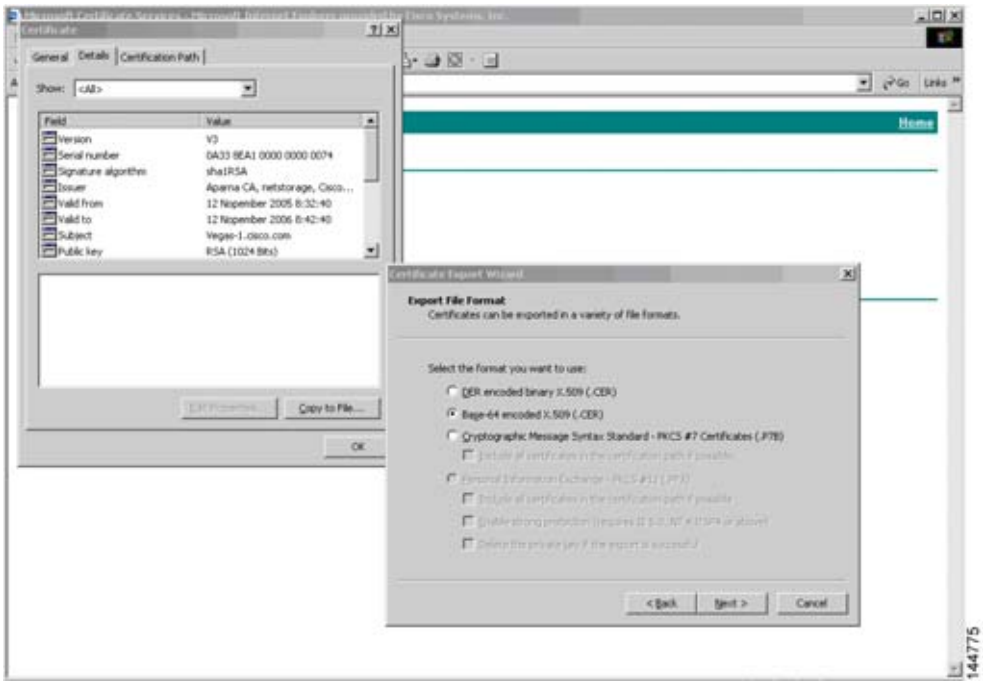
ステップ 9　[Base 64 encoded] オプション ボタンを選択し、[Download CA certificate] リンクをクリックします。



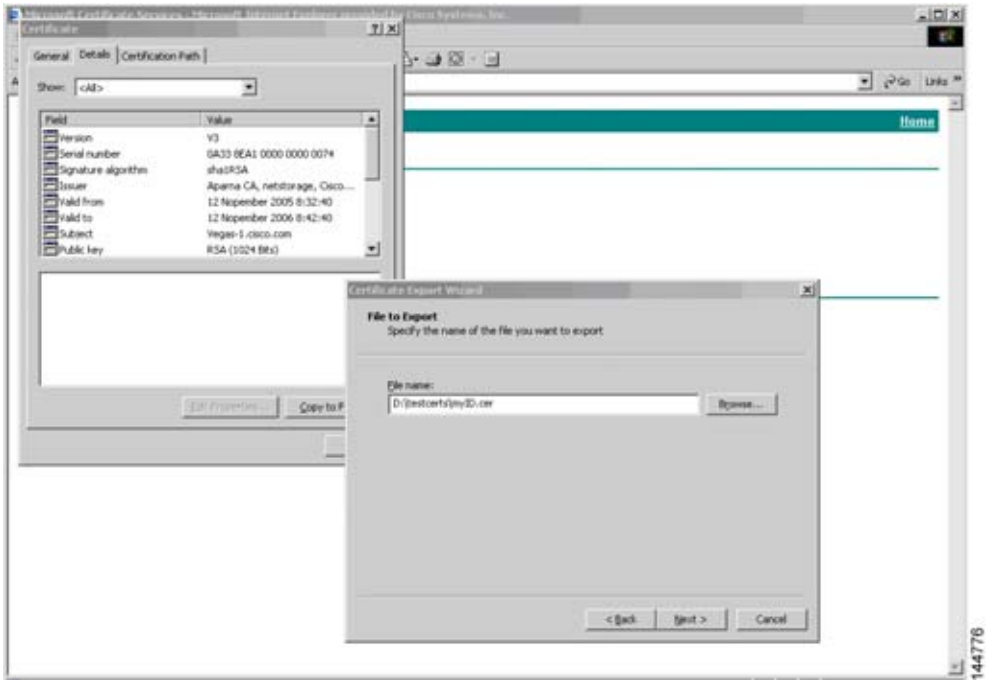
ステップ 10　[File Download] ダイアログボックスで、[Open] ボタンをクリックします。



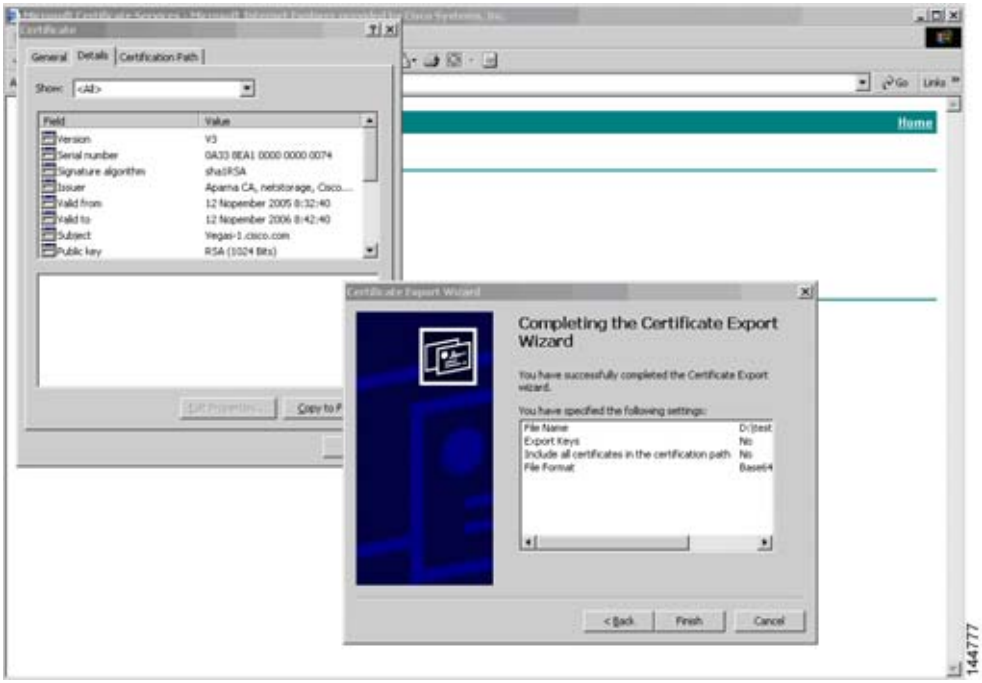
ステップ 11　[Certificate] ダイアログで [Details] タブをクリックし、[Copy to File] ボタンをクリックします。[Certificate Export Wizard] ダイアログボックスで [Base-64 encoded X.509 (.CER)] オプション ボタンを選択し、[Next] ボタンをクリックします。



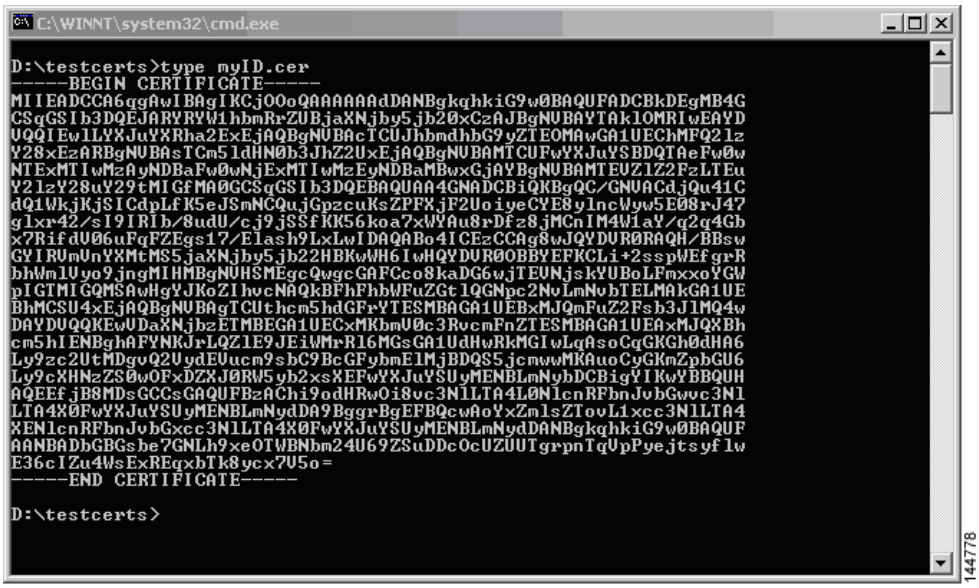
ステップ 12　[Certificate Export Wizard] ダイアログボックスの [File name:] テキスト ボックスに宛先ファイル名を入力し、[Next] ボタンをクリックします。



ステップ 13　[Finish] ボタンをクリックします。



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。

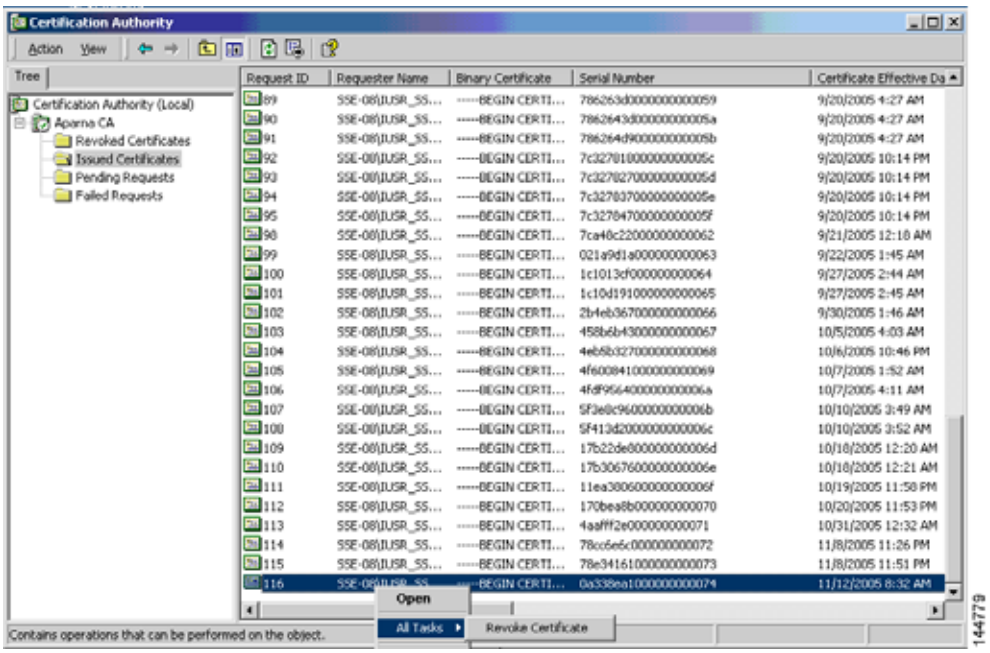


証明書の失効

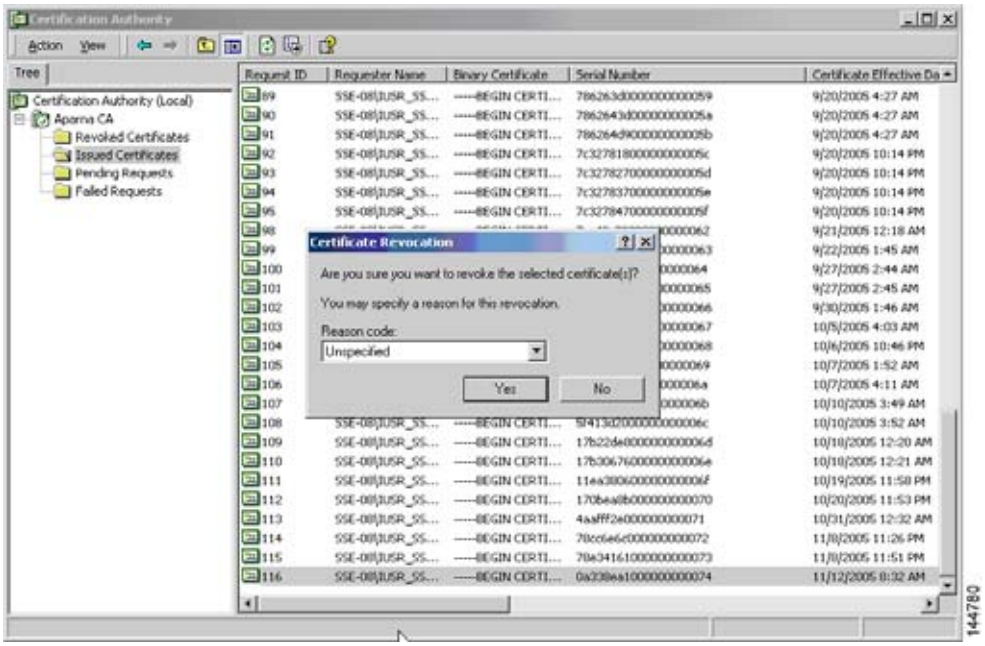
Microsoft CA 管理者プログラムを使用して証明書を失効する手順は、次のとおりです。

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、失効したい証明書を右クリックします。

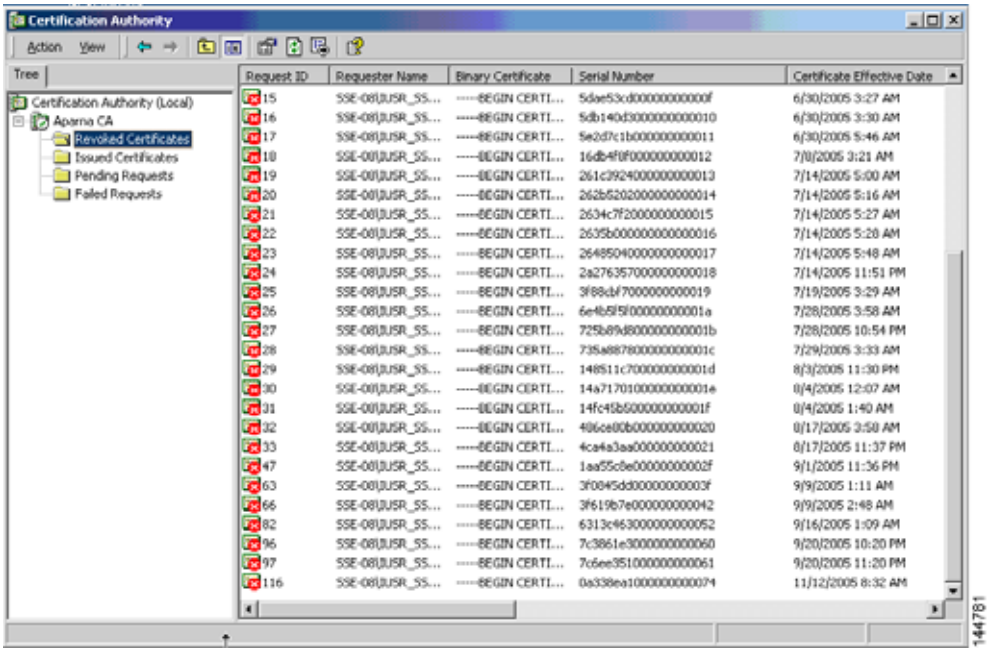
ステップ 2　[All Tasks] > [Revoke Certificate] を選択します。



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] ボタンをクリックします。



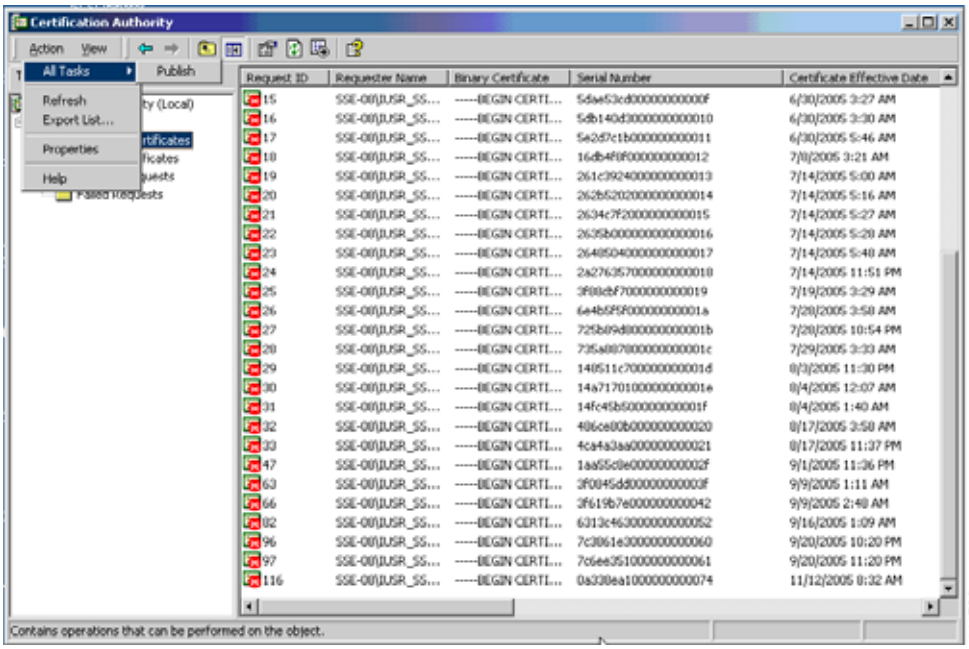
ステップ 4　[Revoked Certificates] フォルダをクリックして、失効証明書を表示し、証明書が失効されたことを確認します。



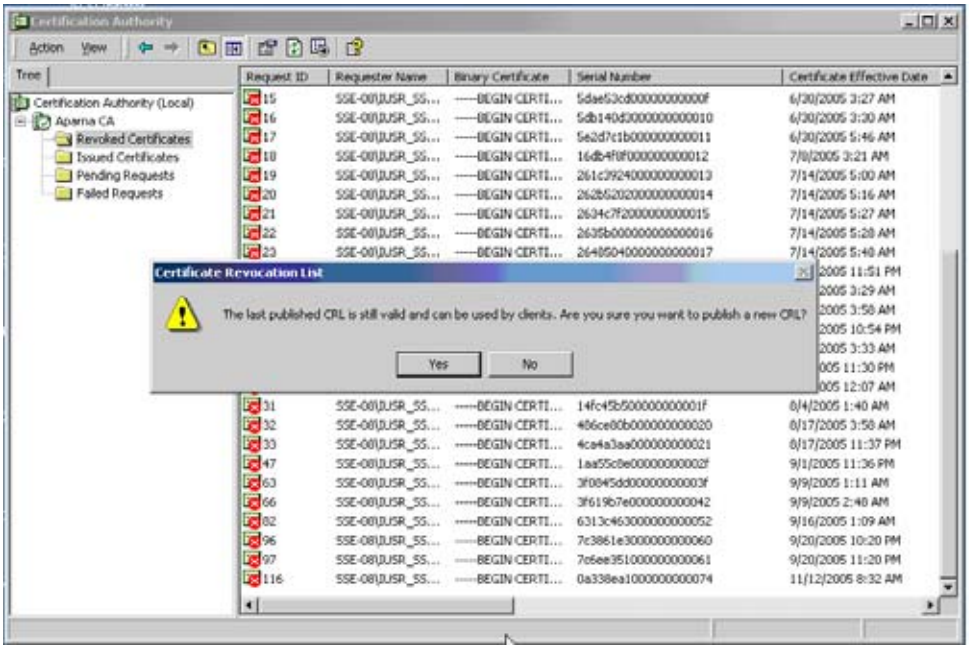
CRL の生成および公開

Microsoft CA 管理者プログラムを使用して CRL を生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。



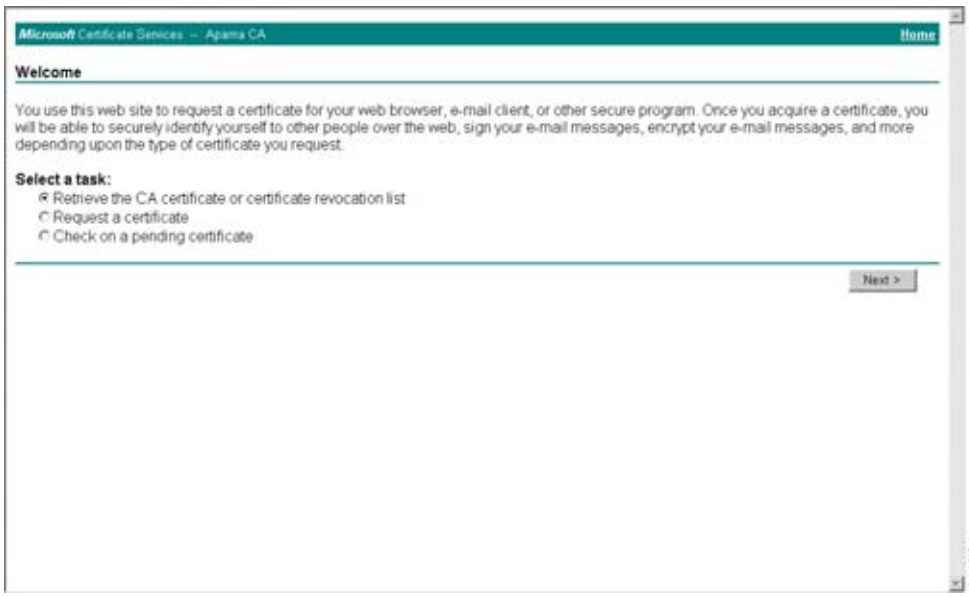
ステップ 2　[Certificate Revocation List] ダイアログボックスで [Yes] ボタンをクリックし、最新の CRL を公開します。



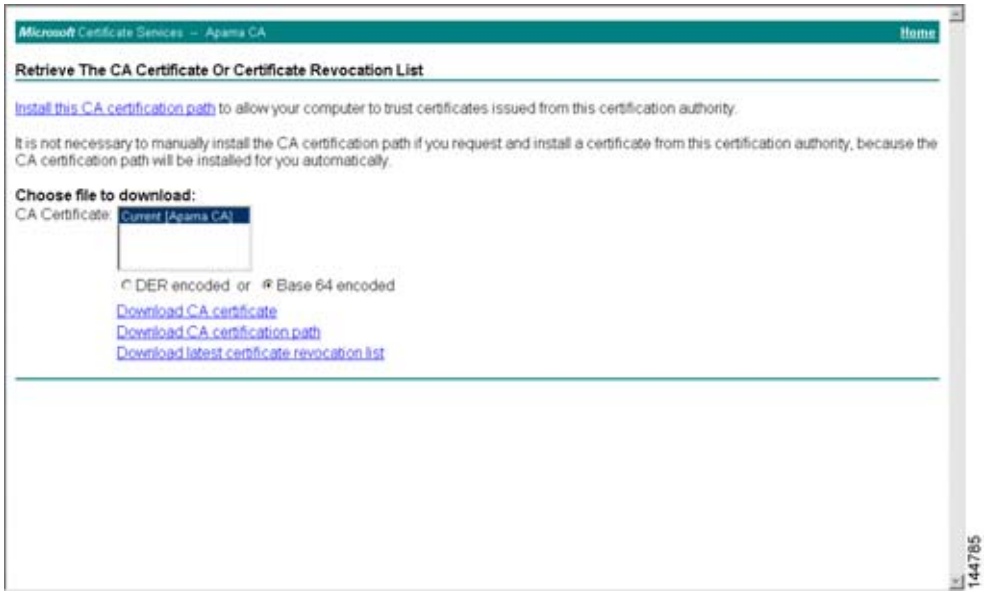
CRL のダウンロード

Microsoft CA 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。

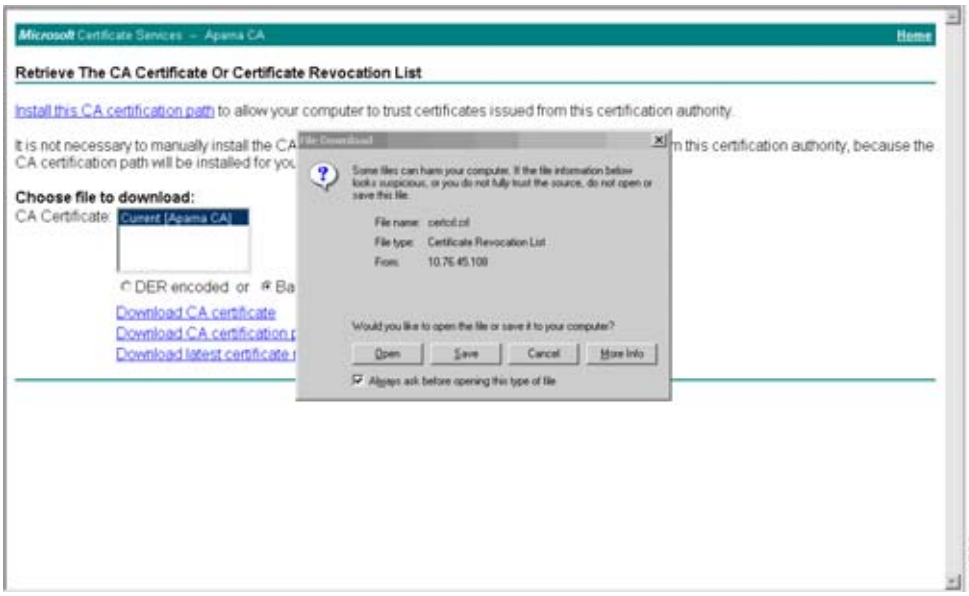
ステップ 1　Microsoft Certificate Services Web インターフェイス上の [Request the CA certificate or certificate revocation list] オプション ボタンを選択し、[Next] ボタンをクリックします。



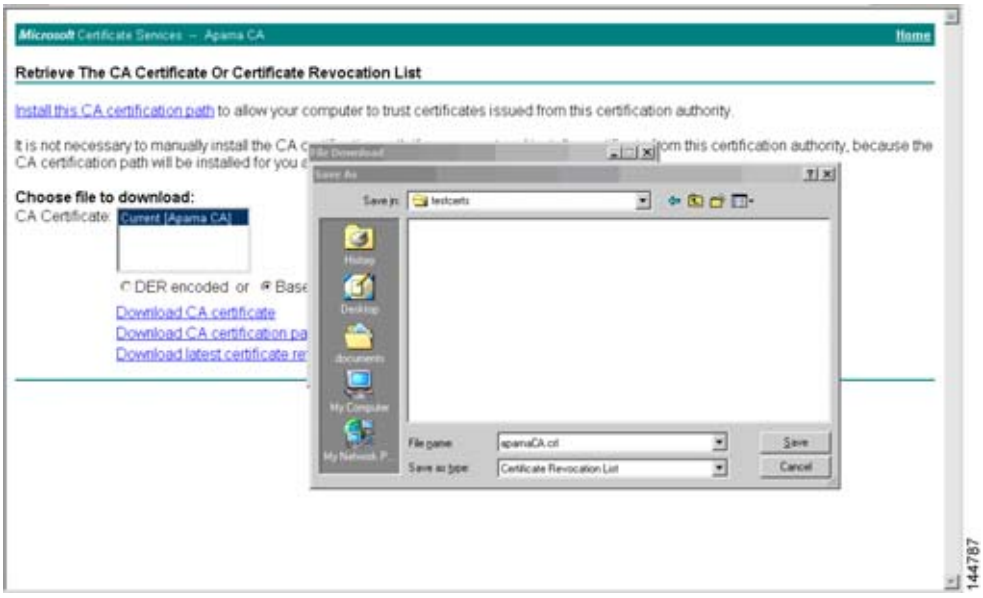
ステップ 2　[Download latest certificate revocation list] リンクをクリックします。



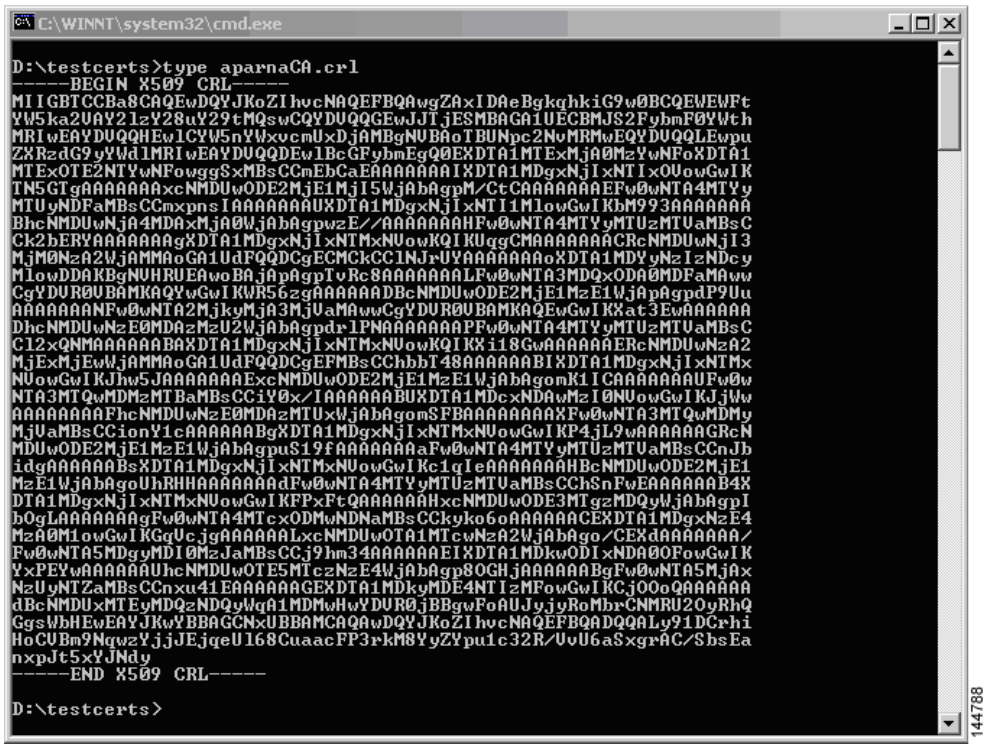
ステップ 3　[File Download] ダイアログボックスで、[Save] ボタンをクリックします。



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] ボタンをクリックします。



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

CA に対応するトラスト ポイントに CRL をインポートする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで、[Switches] > [Security] > [PKI] をクリックします。

ステップ 2　[Information] ペインで [Trust Point Actions] タブをクリックします。

ステップ 3　[Command] ドロップダウン メニューから [crlimport] オプションを選択して、選択したトラスト ポイントに CRL をインポートします。

ステップ 4　[URL] フィールドに、CRL の入力ファイル名を bootflash:filename の形式で入力します。

ステップ 5　[Apply Changes] アイコンをクリックして、変更内容を保存します。

（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	最大制限値
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
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

デフォルト設定値

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 レベル	Switch FQDN
RSA キーペア絶対値	512
RSA キーペアのエクスポート	可能
トラスト ポイントの失効チェック方式	CRL

CHAPTER 7

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実現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 Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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併用できますが、最初の実装には IPSec プロトコルが使用されます。IKE は、IPSec ピア認証を提供し、IPSec Security Association（SA; セキュリティ アソシエーション）をネゴシエートし、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。

この章の内容は、次のとおりです。

IPSec の概要

（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。

インターネットなどの保護されていないネットワーク上で重要な情報を伝達する場合は、IPSec によってセキュリティを確保します。IPSec はネットワーク レイヤで機能し、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。

- データ機密保護：IPSec 送信側で、ネットワーク上で送信するパケットを事前に暗号化できます。
- データ整合性：IPSec 受信側で、IPSec 送信側から送信されたパケットを認証し、送信中にデータが改ざんされていないかを確認できます。
- データ発信元認証：IPSec 受信側で、送信された IPSec パケットの発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 を使用すると、データの参照、改ざん、またはスプーフィングの危険を伴わずに、パブリック ネットワーク上でデータを送信できます。これにより、イントラネット、エクストラネット、リモート ユーザ アクセスを含む、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）などのアプリケーションの使用が可能になります。

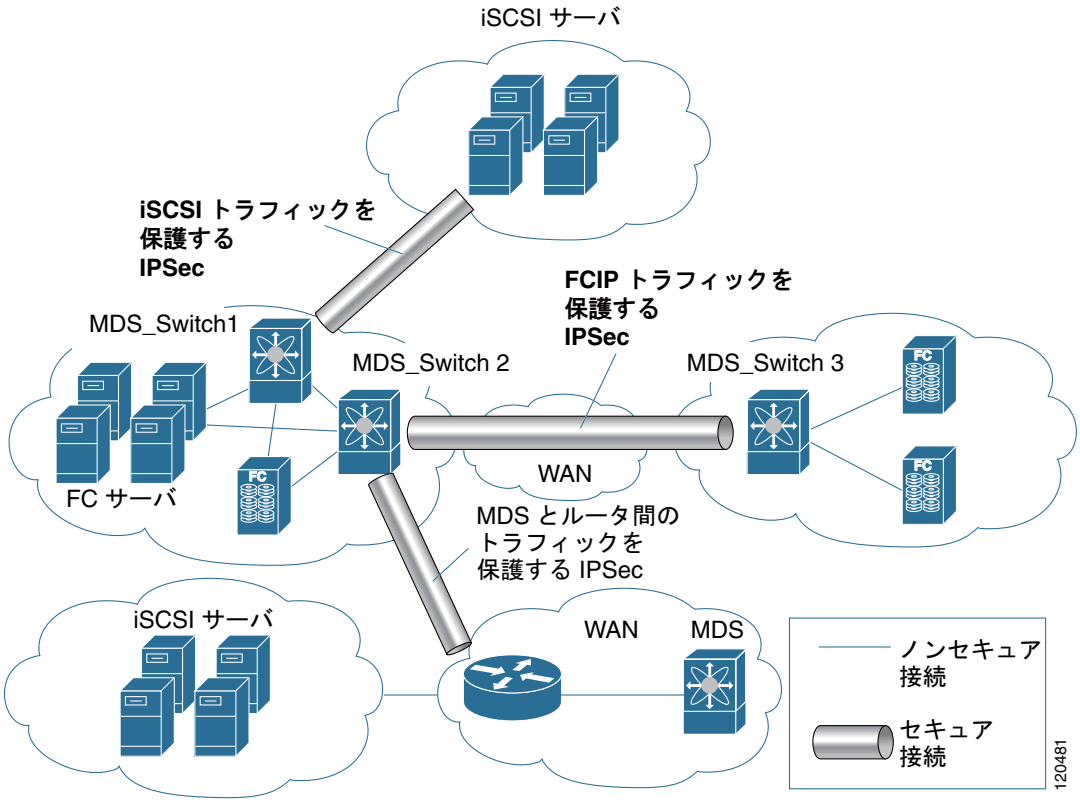
Cisco NX-OS ソフトウェアに実装された IPSec は、Encapsulating Security Payload（ESP）プロトコルをサポートしています。このプロトコルはデータをカプセル化して保護し、データ プライバシー サービス、オプションのデータ認証、およびオプションのリプレイ防止サービスを提供します。

（注）　ESP プロトコルは、既存の Transmission Control Protocol（TCP; 伝送制御プロトコル）/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ユニット（Maximum Transmission Unit; 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 を使用する際、IPS モジュール（14+2 LC または 18+4 LC のいずれか）上の各ギガビット イーサネット インターフェイスをそれぞれ独自の IP サブネットに設定する必要があります。同じ IP サブネット内の IP アドレスまたはネットワークマスクが設定されたギガビット イーサネット インターフェイスが複数存在する場合、IKE パケットを適切なピアに送信できず、IPSec トンネルが起動しません。

図 7-1 に、いくつかの IPSec のシナリオを示します。

図 7-1　MPS-14/2 モジュールを使用する FCIP および iSCSI のシナリオ



IKE の概要

IKE は、IPSec セキュリティ アソシエーション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 でリプレイ防止サービスを提供できます。
- 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を実現します。

（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」（P.7-13）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」（P.7-13）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 Fabric Manager 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 Multi-Service Module（MSM-18/4）モジュールおよび MDS 9222i Module-1 モジュール
- Cisco MDS 9200 スイッチまたは Cisco MDS 9500 ディレクタの Cisco 14/2 ポート Multiprotocol Services（MPS-14/2）モジュール
- 統合スーパーバイザ モジュールに 14/2 ポート マルチプロトコル機能を備えた Cisco MDS 9216i スイッチ。Cisco MDS 9216i スイッチの詳細については、『*Cisco MDS 9200 Series Hardware Installation Guide*』を参照してください。
- 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。
  - Authentication Header（AH; 認証ヘッダー）
  - トランスポート モード
  - セキュリティ アソシエーションのバンドル
  - セキュリティ アソシエーションの手動設定
  - クリプトマップにおけるホスト単位のセキュリティ アソシエーション オプション

- セキュリティ アソシエーション 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復号化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 Database（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。
  - Security Parameter Index（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）：Message Digest 5（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ポート 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、トランスポート 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クス、宛先アドレス/マスクまたはプレフィクス長、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; 完全転送秘密）：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、前のキーおよび以降のキーに影響はありません。これは、以降のキーの取得元が前のキーではないからです。
- 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; 高度暗号化規格）：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。
- Data Encryption Standard（DES; データ暗号化規格）：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 Initialization Vector（IV; 初期ベクトル）が必要です。IV は IPSec パケット内で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、配布が制限されています。米国以外の地域でイメージをインストールする場合には、輸出許可が必要です。米国政府の規制によって、発注が拒否されたり、遅れたりすることがあります。詳細については、製品を購入された代理店に問い合わせるか、export@cisco.com に電子メールで問い合わせてください。

- 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 は認証データに使用されるキー付きのハッシュ バリアントです。
- Secure Hash Algorithm（SHA-1）：HMAC バリアントを使用するハッシュ アルゴリズム。
- AES-XCBC-MAC : AES アルゴリズムを使用する Message Authentication Code（MAC; メッセージ認証コード）。

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。DH は、セッション キーを確立するために IKE 内で使用されます。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。
- 高度暗号化規格（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。
- データ暗号化規格（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、暗号化を開始する初期ベクトル（IV）が必要です。IV は IPSec パケット内で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、配布が制限されています。米国以外の地域でイメージをインストールする場合には、輸出許可が必要です。米国政府の規制によって、発注が拒否されたり、遅れたりすることがあります。詳細については、製品を購入された代理店に問い合わせるか、export@cisco.com に電子メールで問い合わせてください。

- 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 は認証データに使用されるキー付きのハッシュ バリアントです。
- Secure Hash Algorithm（SHA-1）：HMAC バリアントを使用するハッシュ アルゴリズム。
- 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。

IPSec デジタル証明書のサポート

ここでは、Certificate Authority（CA; 認証局）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。

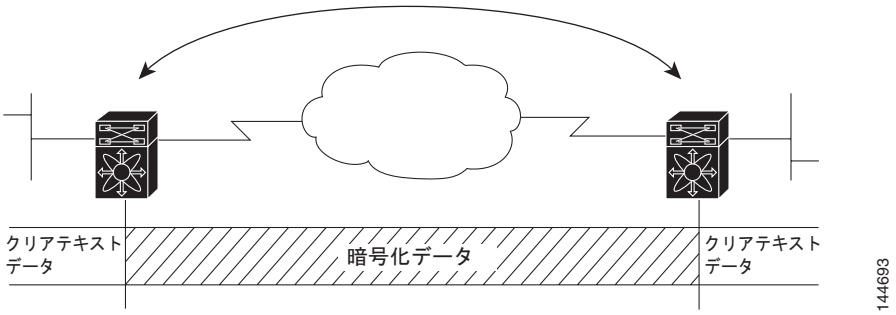
CA およびデジタル証明書を使用しない IPSec の実装

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（Rivest, Shamir, Adelman [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。

図 7-2 では、各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 IP 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。

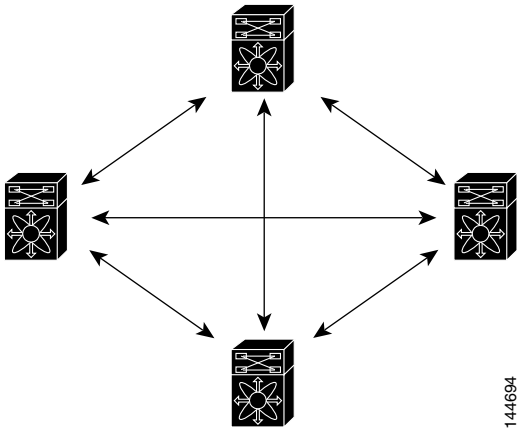
図 7-2　CA およびデジタル証明書を使用しない 2 台の IPSec スイッチ



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 7-3 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 7-3　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

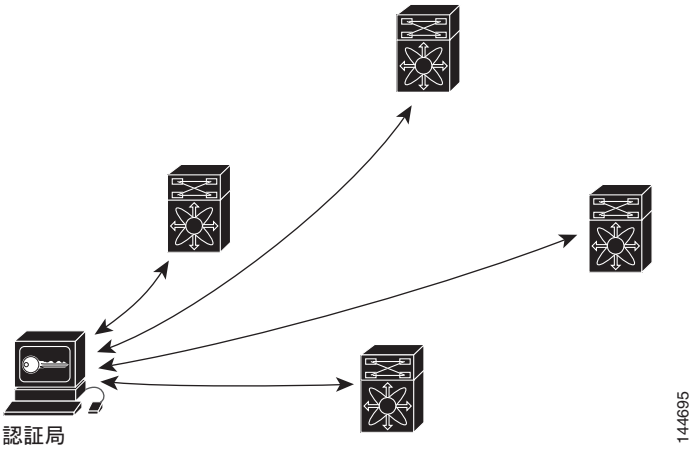


CA およびデジタル証明書を使用した IPSec の実装

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、両デバイスは相互に認証するために、証明書およびデジタル署名データを交換します。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 7-4 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 7-4　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、Certificate Revocation List（CRL; 証明書失効リスト）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には、スイッチの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）（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限り、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。

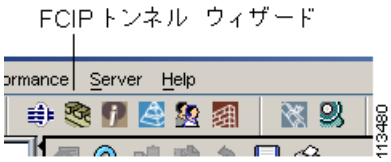
FCIP ウィザードを使用した IPSec の設定

Fabric Manager では、FCIP ウィザードを使用する FCIP 設定の一環として IPSec および IKE をイネーブルにし、設定することによって、これらの機能を簡単に設定できます。

Fabric Manager の FCIP ウィザードを使用して IPSec をイネーブルにする手順は、次のとおりです。

ステップ 1　ツールバーの [FCIP Wizard] アイコンをクリックします。

図 7-5　　FCIP ウィザード



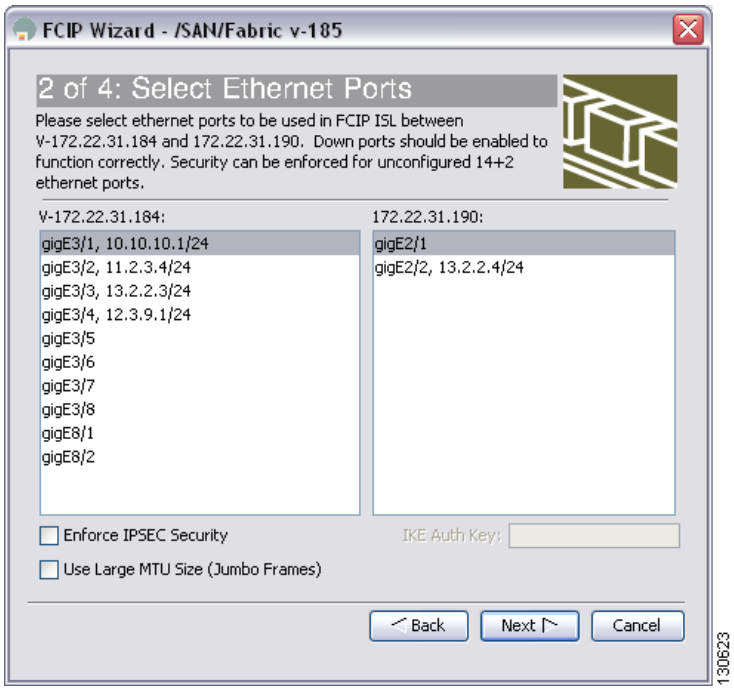
ステップ 2　FCIP リンクのエンドポイントとして動作するスイッチを選択し、[Next] ボタンをクリックします。

（注）　FCIP リンク上に IPSec を設定するには、これらのスイッチに MPS-14/2 モジュールが搭載されている必要があります。

ステップ 3　FCIP リンクを形成する各 MPS-14/2 モジュール上のギガビット イーサネット ポートを選択します。

ステップ 4　[Enforce IPSEC Security] チェックボックスをオンにして、IKE Auth Key を設定します（図 7-6 を参照）。

図 7-6　FCIP リンク上での IPSec のイネーブル化



ステップ 5　[Next] ボタンをクリックします。[Specify Tunnel Properties] ダイアログボックスに、TCP 接続特性が表示されます。

ステップ 6　FCIP リンク上の TCP 接続の最小および最大帯域幅、および往復時間を設定します。[Measure] ボタンをクリックし、ギガビット イーサネット エンドポイント間の往復時間を測定します。

ステップ 7　[Enable Write Acceleration] チェックボックスをオンにして、FCIP リンク上の FCIP 書き込みアクセラレーションをイネーブルにします。

ステップ 8　[Enable Optimum Compression] チェックボックスをオンにして、FCIP リンク上の IP 圧縮をイネーブルにします。

ステップ 9　FCIP トンネル パラメータを設定するには、[Next] ボタンをクリックします。

ステップ 10　[Port VSAN] を [nontrunk/auto] に設定し、トランク トンネルに許可される Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）のリストを設定します。この FCIP リンクに [Trunk Mode] を選択します。『*Cisco Fabric Manager IP Services Configuration Guide*』を参照してください。

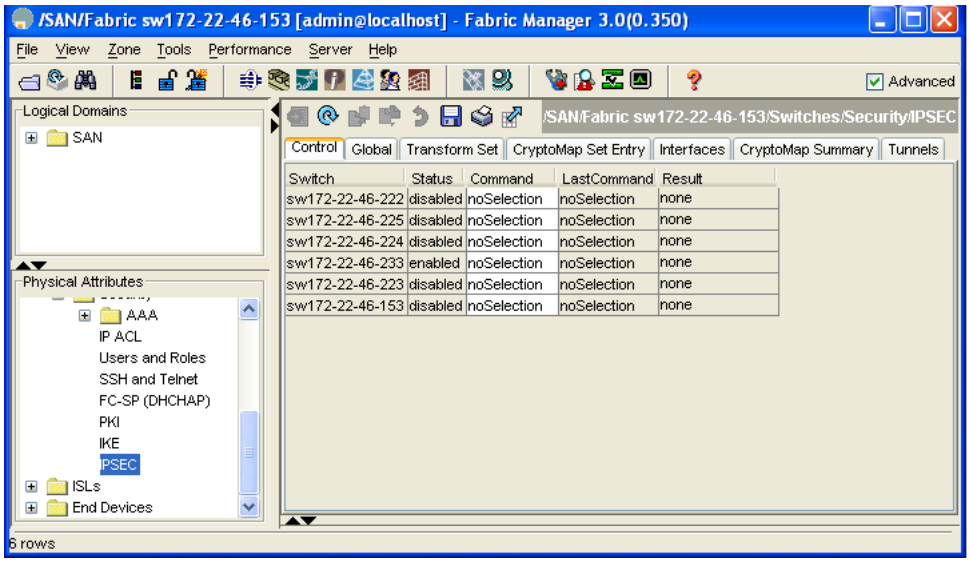
ステップ 11　FCIP リンクを作成するには、[Finish] ボタンをクリックします。FCIP リンクを作成しないで FCIP ウィザードを終了するには、[Cancel] ボタンをクリックします。

Fabric Manager を使用して、IPSec および IKE がイネーブルかどうかを確認する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。

[Information] ペインに IPSec の設定が表示されます（図 7-7 を参照）。

図 7-7　IPSec の設定

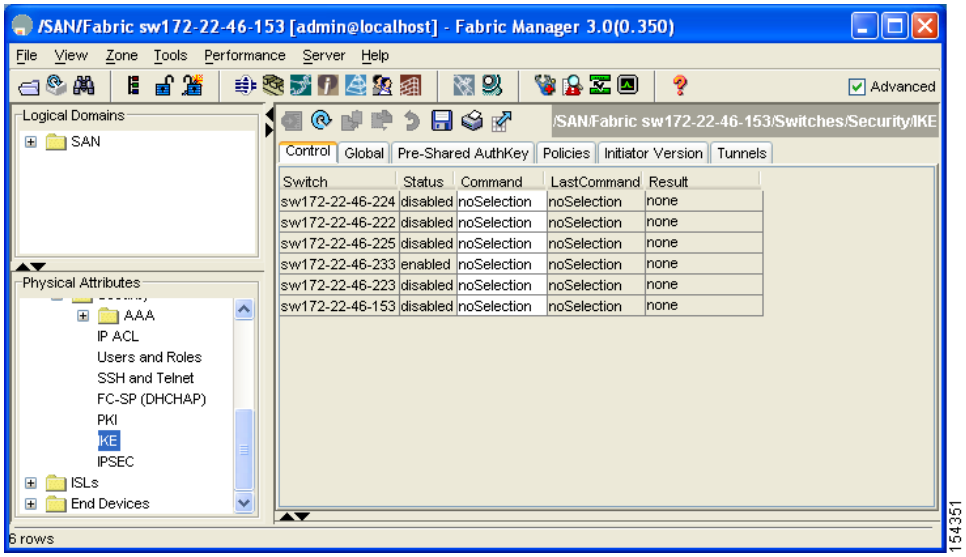


ステップ 2　[Control] タブがデフォルトです。[Status] カラムで、IPSec を適用するスイッチがイネーブルに設定されているかどうかを確認します。

ステップ 3　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-8 を参照）。

図 7-8　IKE の設定



ステップ 4　[Control] タブがデフォルトです。[Status] カラムで、IKE を変更するスイッチがイネーブルに設定されているかどうかを確認します。

IPSec および IKE の手動設定

ここでは、FCIP ウィザードを使用しない場合、IPSec および IKE を手動で設定する手順について説明します。「FCIP ウィザードを使用した IPSec の設定」（P.7-10）を参照してください。

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 Access Control List（ACL; 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 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 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 ポリシーは、IKE ネゴシエーション実行中に使用されるセキュリティ 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 7-1 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 7-1　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**	**sha**
	MD5（HMAC バリアント）	**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 または MD5、DH グループ 2	3DES、SHA-1
Cisco iSCSI 発信側（Linux プラットフォームの Free Swan IPSec 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するピアからリモート ピアに対してすべてのポリシーが送信されると、リモート ピアが一致するポリシーを検索します。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。リモート ピアは、一致しているポリシーが見つかるまで、プライオリティの順に（最優先が最初）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。

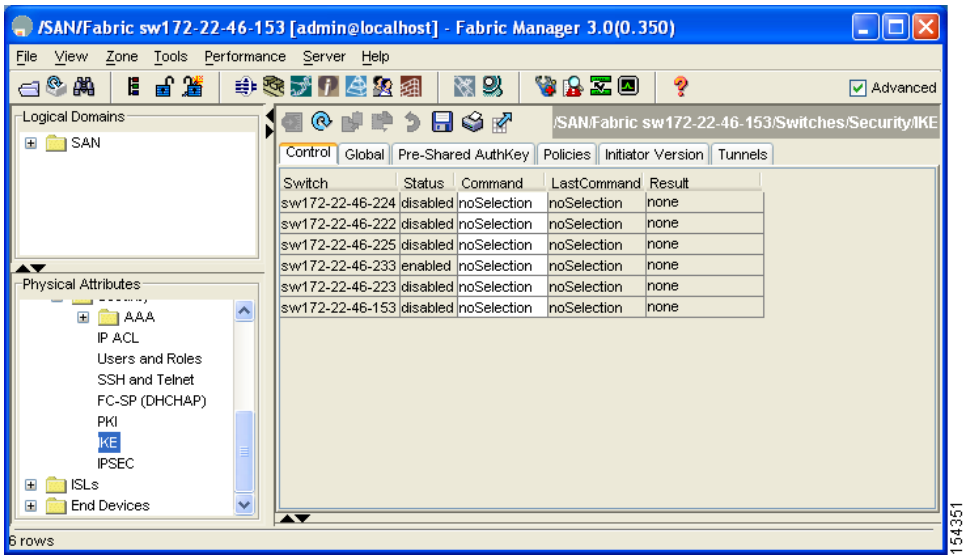
IKE ポリシーの設定

Fabric Manager を使用して IKE ポリシー ネゴシエーション パラメータを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-9 を参照）。

図 7-9　　IKE の設定



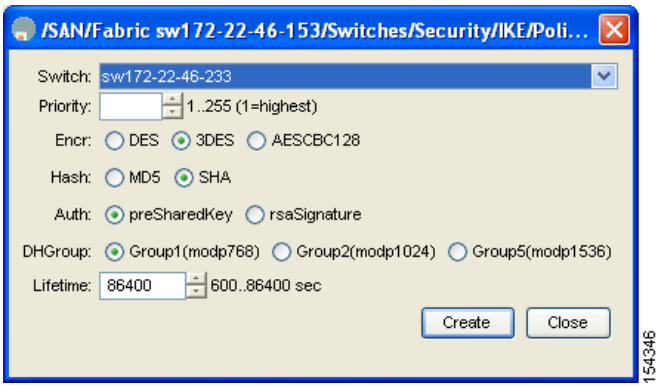
ステップ 2　[Policies] タブをクリックします。

[Information] ペインに既存の IKE ポリシーが表示されます。

ステップ 3　[Create Row] アイコンをクリックして、IKE ポリシーを作成します。

[Create Policy] ダイアログボックスが表示されます（図 7-10 を参照）。

図 7-10　IKE の作成



ステップ 4　このスイッチの [Priority] を入力します。1 ～ 255 の値を入力できます。1 が最優先です。

ステップ 5　暗号化、ハッシュ、認証、および DH グループのフィールドで、適切な値を選択します。

ステップ 6　ポリシーのライフタイムを入力します。600 ～ 86400 秒のライフタイムを入力できます。

ステップ 7　このポリシーを作成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

（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。

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」（P.7-15）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。

ここで説明する内容は、次のとおりです。

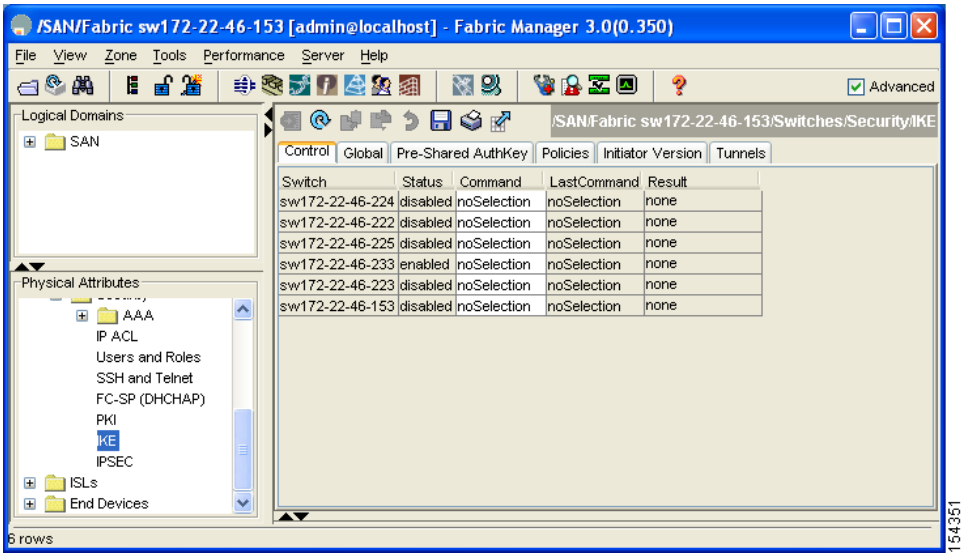
ピアのキープアライブ タイムの設定

Fabric Manager を使用して、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。

ステップ 1　[Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-11 を参照）。

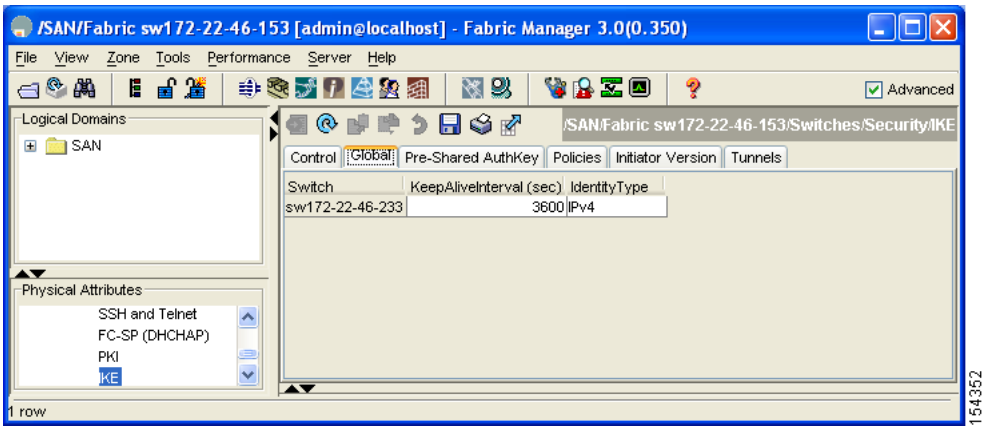
図 7-11　IKE の設定



ステップ 2　[Global] タブを選択します。

[Information] ペインに特定の IKE プロトコルのグローバル統計情報が表示されます（図 7-12 を参照）。

図 7-12　[IKE Global] タブの情報



ステップ 3　[KeepAliveInterval (sec)] に値（秒数）を入力します。秒単位のキープアライブ インターバルは、管理対象デバイスの IKE エンティティがすべてのピアとともに、この概念的な行に対応する Domain of Interpretation（DOI; 解釈領域）に使用するものです。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

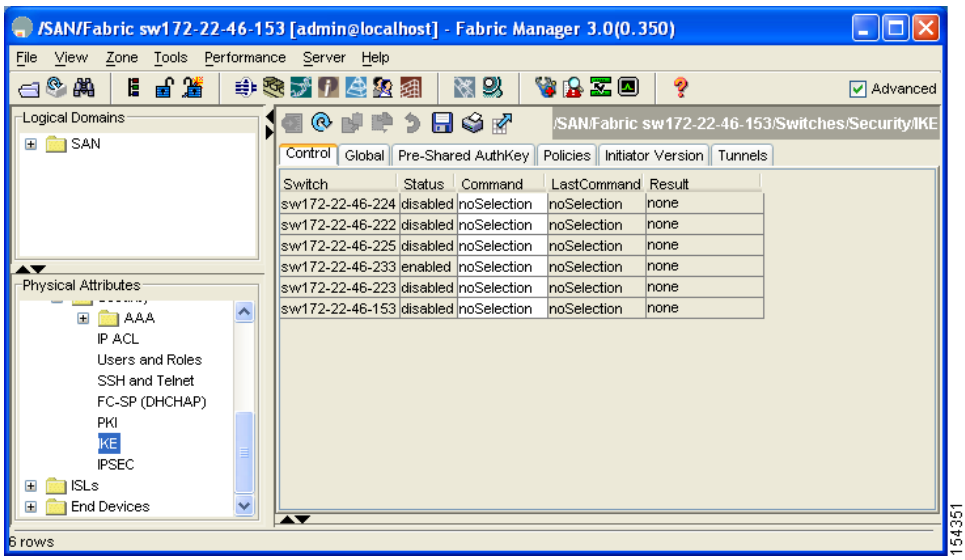
発信側バージョンの設定

Fabric Manager を使用して発信側バージョンを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-13 を参照）。

図 7-13　　IKE の設定



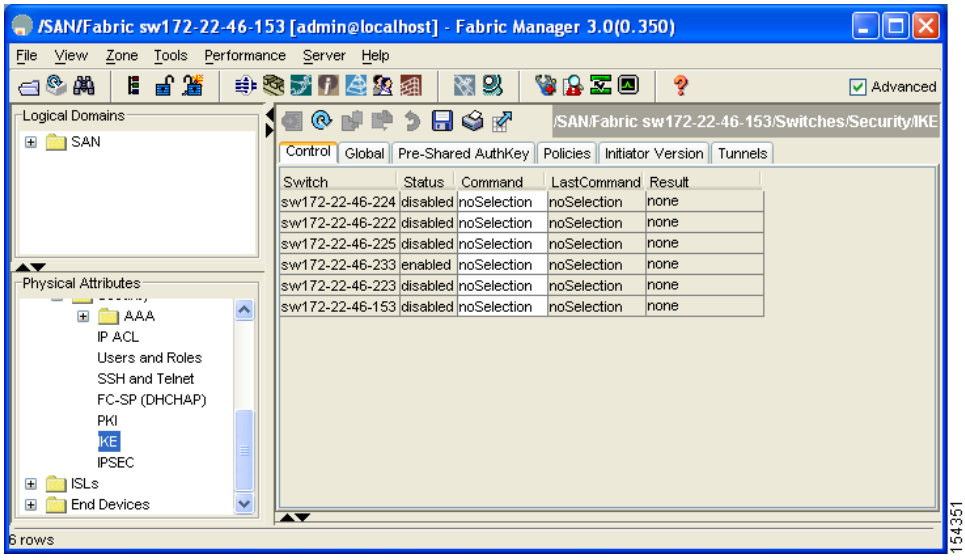
ステップ 2　[Initiator Version] タブを選択します。

[Information] ペインにピアの既存の発信側バージョンが表示されます。

ステップ 3　[Create Row] アイコンをクリックして、発信側バージョンを作成します。

[Create Initiator Version] ダイアログボックスが表示されます（図 7-14 を参照）。

図 7-14　　[Create Initiator Version] ダイアログボックス



ステップ 4　IKE プロトコル 発信側を設定するリモート ピアのスイッチを選択します。

ステップ 5　リモート ピアの IP アドレスを入力します。

IKEv1 は、リモート ピアに接続するときに使用される IKE プロトコル バージョンです。

ステップ 6　この発信側バージョンを作成するには、[Create] ボタンをクリックします。変更内容を保存しないで終了するには、[Close] ボタンをクリックします。

IKE トンネルまたはドメインのクリア

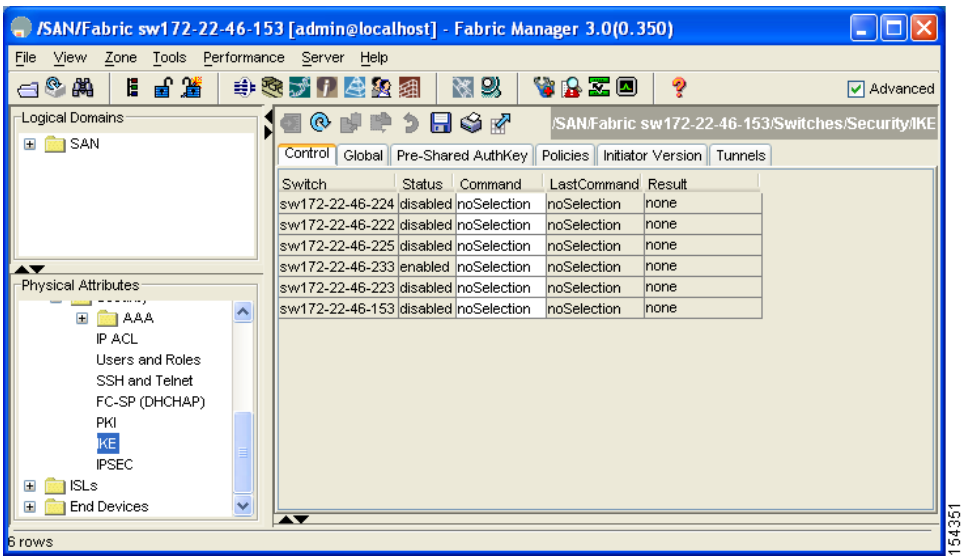
IKE 設定に IKE トンネル ID を指定していない場合、既存のすべての IKE ドメイン接続をクリアできます。

Fabric Manager を使用して、すべての IKE トンネルまたはドメインをクリアする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IKE] を選択します。

[Information] ペインに IKE の設定が表示されます（図 7-15 を参照）。

図 7-15　IKE の設定



ステップ 2　[Information] ペインで [Tunnels] タブをクリックします。

IKE トンネルが表示されます。

ステップ 3　[Action] カラムをクリックし、[Clear] ボタンを選択して、トンネルをクリアします。

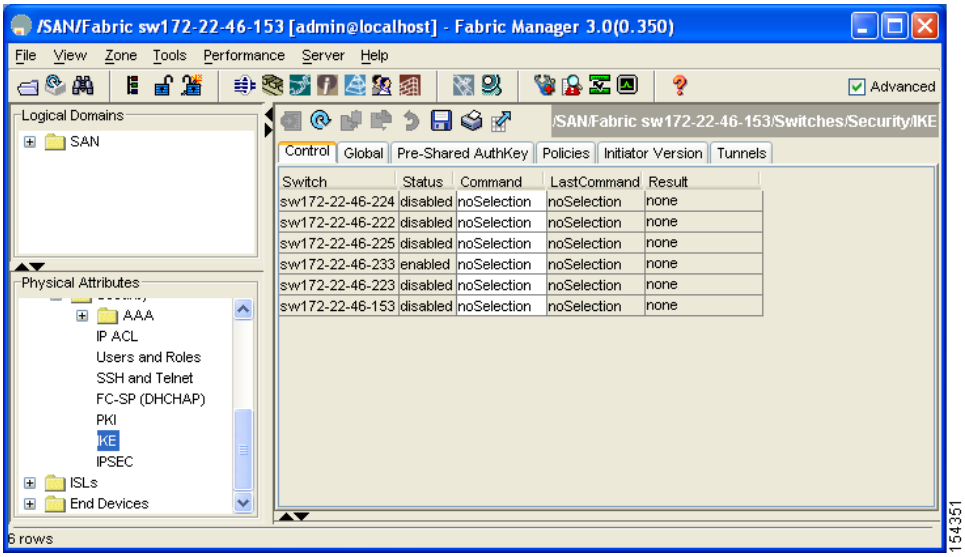
SA のリフレッシュ

Fabric Manager を使用して、IKEv2 設定の変更後に SA をリフレッシュする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IKE] を選択します。

IKE の設定が表示されます（図 7-16 を参照）。

図 7-16　IKE の設定



ステップ 2　[Information] ペインで、[Pre-Shared AuthKey] タブをクリックします。

ステップ 3　[Refresh Values] をクリックします。

クリプト IPv4-ACL

IP ACL（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 のアクセス制御リストの設定」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したりできます。

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 によって保護するアウトバウンド トラフィックを選択する（permit = 保護を適用）。
- 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。
- インバウンド トラフィックを処理して、IPSec で保護されていたはずのトラフィックをフィルタリングして除外し、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。

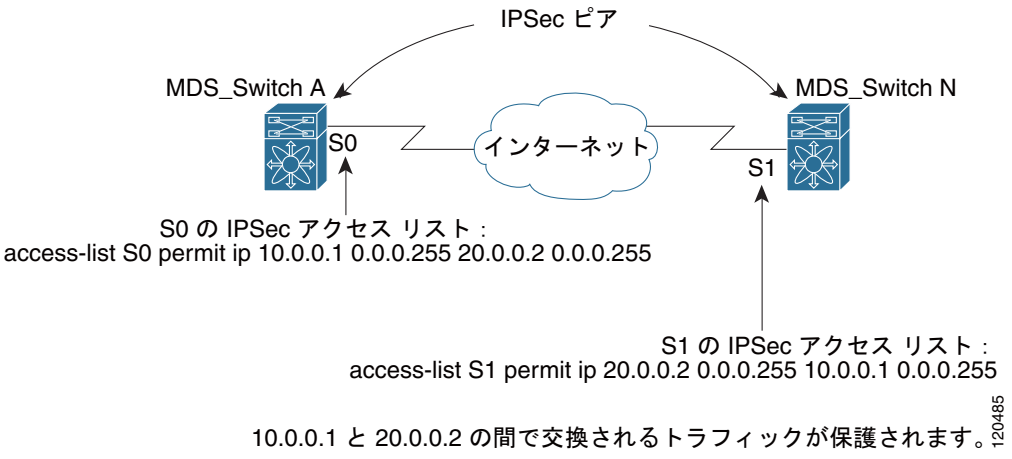
- IPSec 機能が考慮するのは、送信元/宛先 IPv4 アドレスとサブネット マスク、プロトコル、および 1 つのポート番号だけです。IPSec では、IPv6 はサポートされません。

  （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。IPSec 機能は、各 MPS-14/2 モジュールおよび Cisco MDS 9216i スイッチに対して、最大 120 のセキュリティ ポリシー エントリをサポートします。
- 図 7-17 では、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 7-17　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。
- 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、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）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。

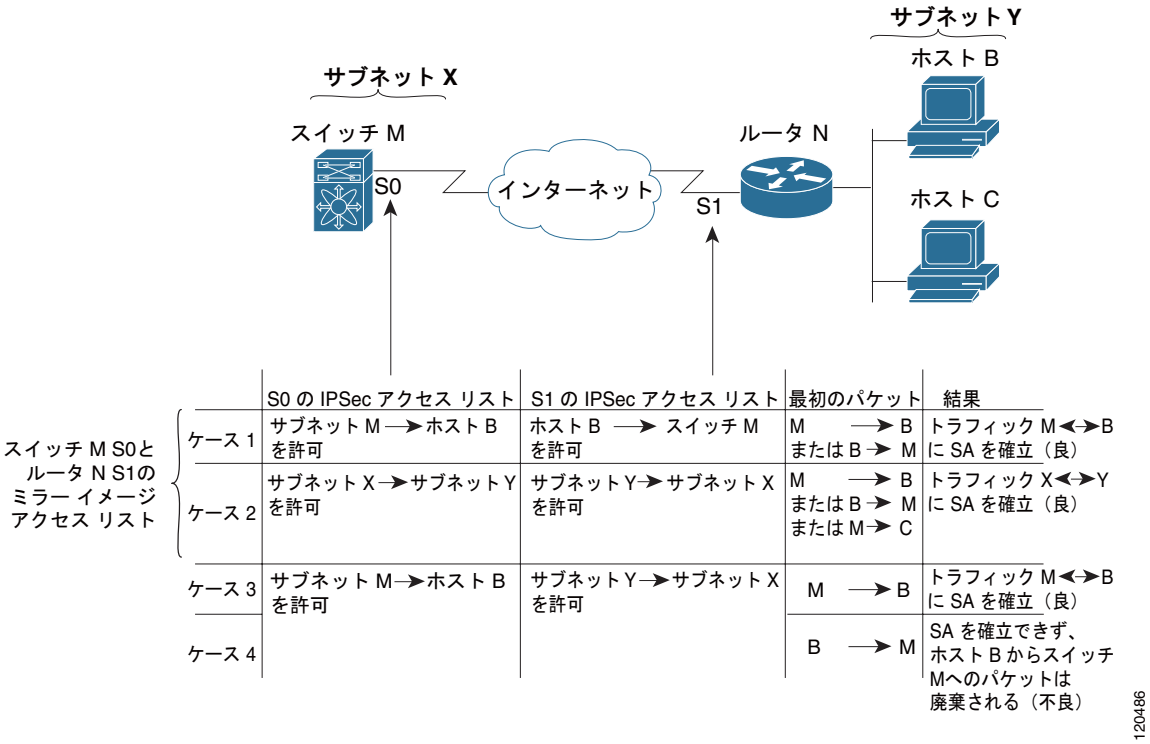
ミラー イメージ クリプト IPv4-ACL

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 7-18 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 7-18　ミラー イメージ設定の IPSec 処理



		S0 の IPSec アクセス リスト	S1 の IPSec アクセス リスト	最初のパケット	結果
スイッチ M S0 とルータ N S1 のミラー イメージ アクセス リスト	ケース 1	サブネット M → ホスト B を許可	ホスト B → スイッチ M を許可	M → B または B → M	トラフィック M ↔ B に SA を確立（良）
	ケース 2	サブネット X → サブネット Y を許可	サブネット Y → サブネット X を許可	M → B または B → M または M → C	トラフィック X ↔ Y に SA を確立（良）
	ケース 3	サブネット M → ホスト B を許可	サブネット Y → サブネット X を許可	M → B	トラフィック M ↔ B に SA を確立（良）
	ケース 4			B → M	SA を確立できず、ホスト B からスイッチ M へのパケットは廃棄される（不良）

図 7-18 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 7-18 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、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、エコー、エコー応答用のパケットなど、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。

保護するパケットは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、保護対象外とする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

クリプト IPv4-ACL の作成については、第 5 章「IPv4 および IPv6 のアクセス制御リストの設定」を参照してください。

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、セキュリティ プロトコルおよびアルゴリズムの特定の組み合わせを表します。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、クリプト マップ エントリに 1 つまたは複数のトランスフォーム セットを指定できます。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 セキュリティ アソシエーションの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一のトランスフォーム 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 セキュリティ アソシエーションの一部として、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 セットの定義を変更すると、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内容が適用されます。変更内容は既存のセキュリティ アソシエーションには適用されませんが、新規のセキュリティ アソシエーション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には、セキュリティ アソシエーション データベースのすべてまたは一部をクリアします。

（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 7-2 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 7-2　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**
	MD5（HMAC バリアント）	**esp-md5-hmac**
	AES-XCBC-MAC	**esp-aes-xcbc-mac**

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。

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 または MD5、DH グループ 2	3DES、SHA-1
Cisco iSCSI 発信側（Linux プラットフォームの Free Swan IPSec 実装）	3DES、MD5、DH グループ 1	3DES、MD5

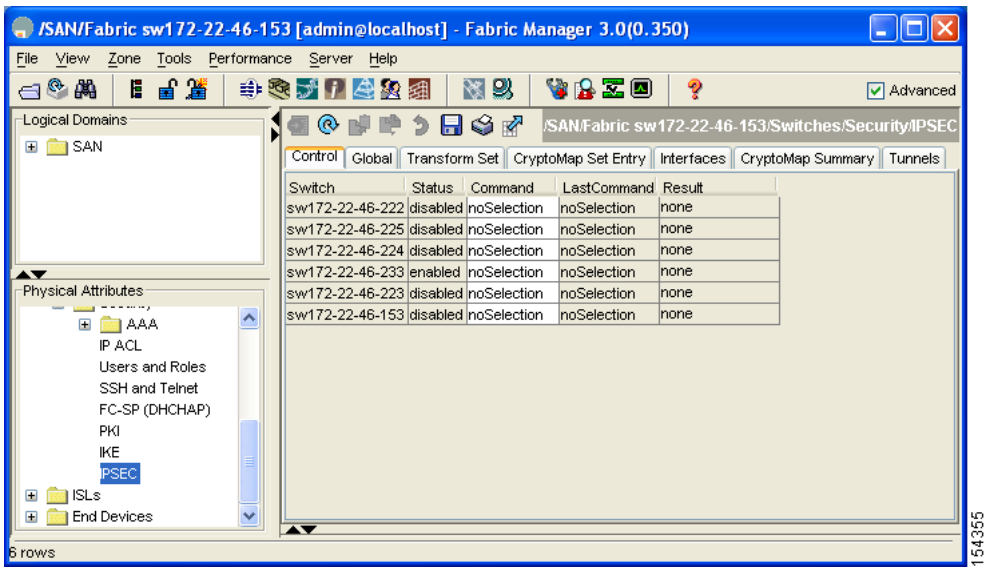
トランスフォーム セットの設定

Fabric Manager を使用してトランスフォーム セットを設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSec] を選択します。

IPSec の設定が表示されます（図 7-19 を参照）。

図 7-19　IPSec の設定

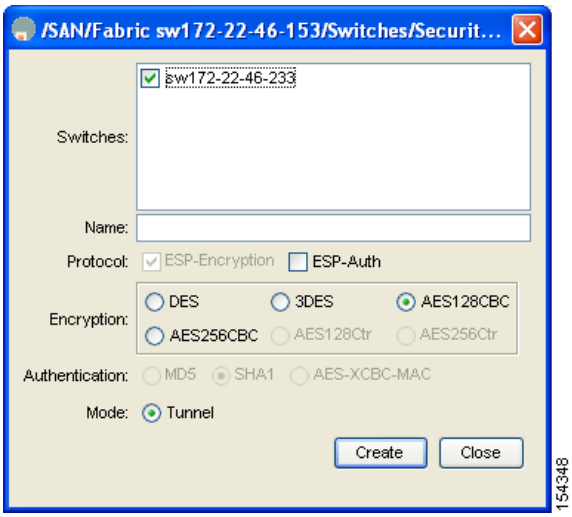


ステップ 2　[Information] ペインで [Transform Set] タブをクリックします。

ステップ 3　[Create Row] アイコンをクリックします。

[Create IPSEC] ダイアログボックスが表示されます（図 7-20 を参照）。

図 7-20　IPSec の作成



ステップ 4　[Create Transform Set] ダイアログボックスで、トランスフォーム セットを作成するスイッチを選択します。

ステップ 5　トランスフォーム セットの名前とプロトコルを指定します。

ステップ 6　暗号化および認証アルゴリズムを選択します。表 7-2 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。

ステップ 7　[Create] ボタンをクリックしてトランスフォーム セットを作成するか、[Close] ボタンをクリックします。

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 マップ名を持つ（ただし、マップ シーケンス番号が異なる）クリプト マップ エントリは、クリプト マップ セットとして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 エントリが互換性を持つためには、次の最低基準を満たしている必要があります。

- 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 マップが設定されたインターフェイス上で、トラフィックは、最初にプライオリティが高いマップ 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。

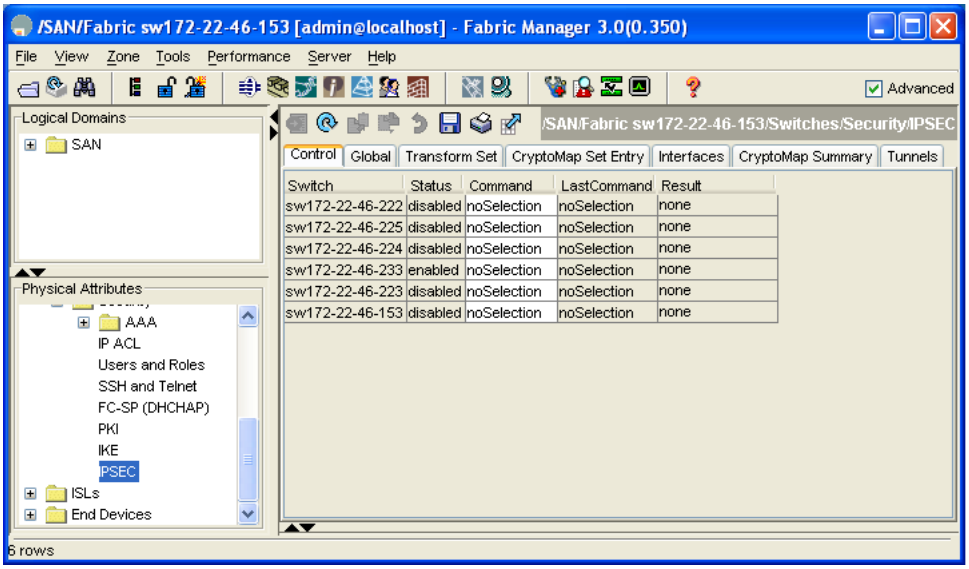
- ポリシーが適用される順序は、各クリプト マップのシーケンス番号によって決まります。シーケンス番号が小さいほど、プライオリティは高くなります。
- 各クリプト マップ エントリに使用できる IPv4-ACL は 1 つだけです（IPv4-ACL 自体には複数の permit エントリまたは deny エントリを設定できます）。
- トンネル エンドポイントが宛先アドレスと同じである場合は、auto-peer オプションを使用して、ピアをダイナミックに設定できます。
- IPSec を Microsoft iSCSI 発信側と効率的に相互運用するには、IPv4-ACL に TCP プロトコルとローカル 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

Fabric Manager を使用して必須のクリプト マップ エントリを作成する手順は、次のとおりです。

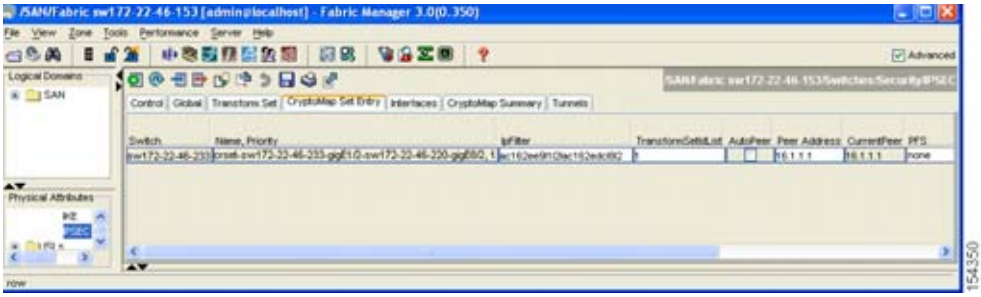
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。
[Information] ペインに IPSec の設定が表示されます（図 7-21 を参照）。

図 7-21　IPSec の設定



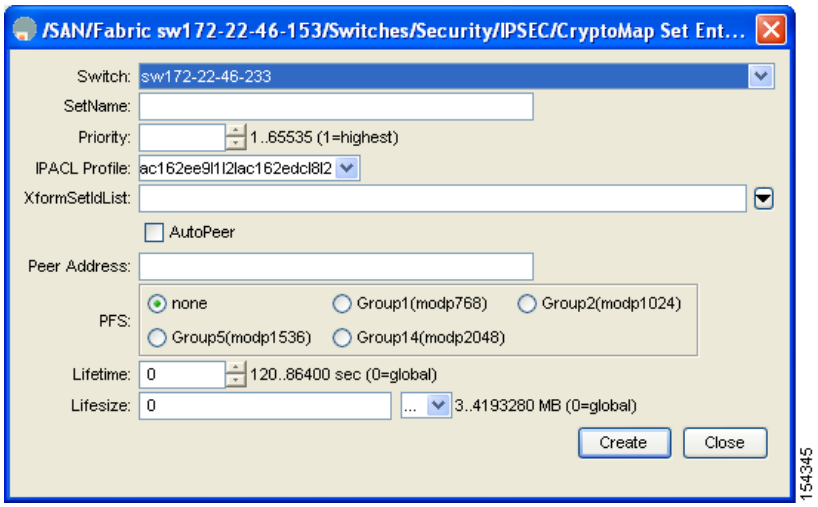
ステップ 2　[CryptoMap Set Entry] タブを選択します。
設定されている既存のクリプト マップが表示されます（図 7-22 を参照）。

図 7-22　既存のクリプト マップ



ステップ 3　（任意）[Create Row] アイコンをクリックして、クリプト マップ エントリを作成します。
[Create Crypto Map] ダイアログボックスが表示されます（図 7-23 を参照）。

図 7-23　[Create Crypto Map] ダイアログボックス



ステップ 4　設定または変更したいスイッチを選択します。クリプト マップを作成する場合には、クリプト マップの setName およびプライオリティを設定します。

ステップ 5　ドロップダウン リストから、このクリプト マップの [IPv4-ACL Profile] および [TransformSetIdList] を選択します。

ステップ 6　（任意）[AutoPeer] チェックボックスをオンにするか、クリプト マップを作成する場合はピア のアドレスを設定します。「[AutoPeer] オプションの概要」（P.7-33）を参照してください。

ステップ 7　適切な [PFS] を選択します。「完全転送秘密の概要」（P.7-35）を参照してください。

ステップ 8　[Lifetime] および [LifeSize] を設定します。「SA ライフタイム ネゴシエーションの概要」（P.7-31）を参照してください。

ステップ 9　クリプト マップを作成する場合は、[Create] ボタンをクリックします。既存のクリプト マップを変更する場合は、[Apply Changes] アイコンをクリックします。

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。

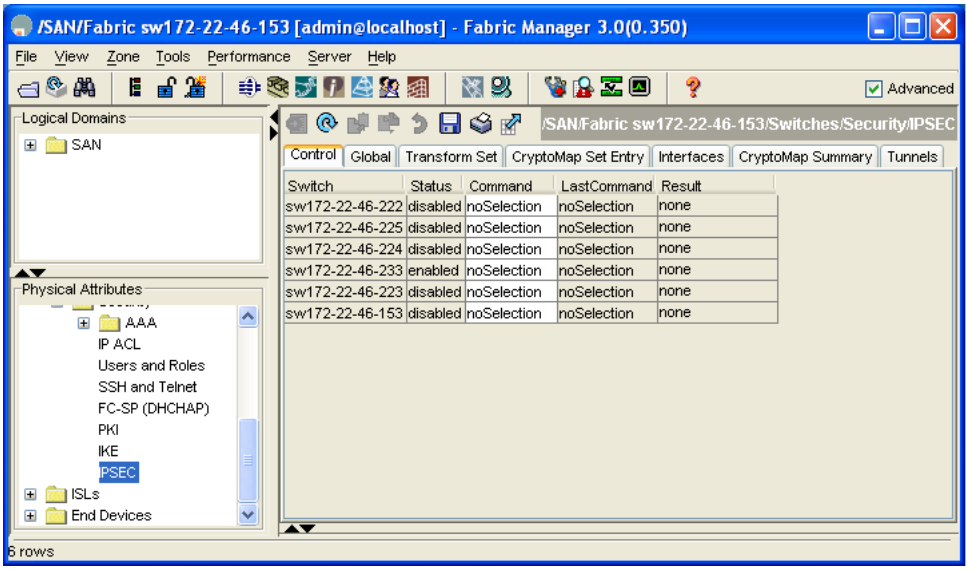
グローバル ライフタイム値の詳細については、「グローバル ライフタイム値」（P.7-38）を参照してください。

SA ライフタイムの設定

Fabric Manager を使用して、指定したクリプト マップの SA ライフタイムを設定する手順は、次のとおりです。

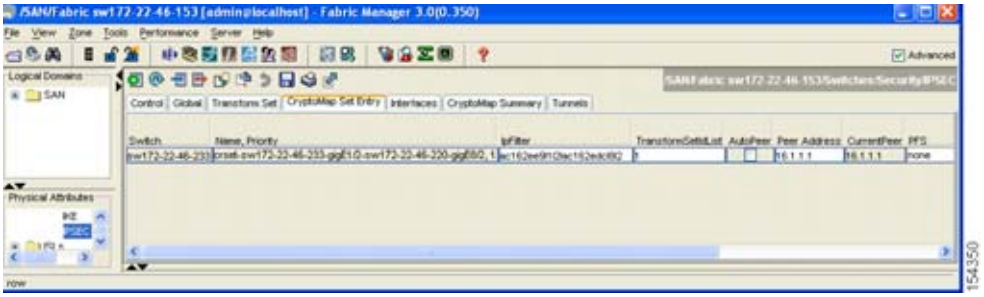
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。
[Information] ペインに IPSec の設定が表示されます（図 7-24 を参照）。

図 7-24　IPSec の設定



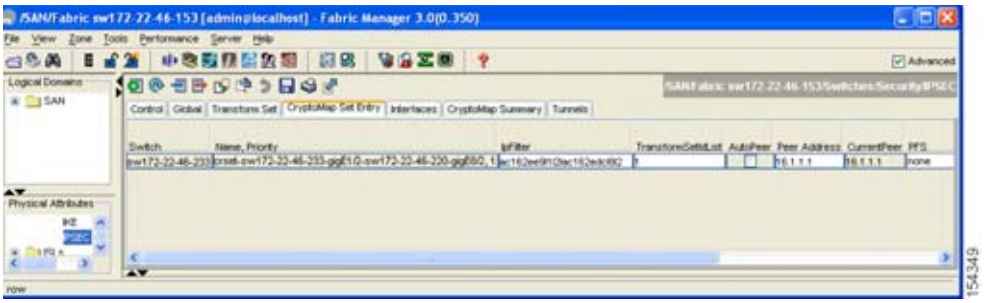
ステップ 2　[CryptoMap Set Entry] タブを選択します。
設定されている既存のクリプト マップが表示されます（図 7-25 を参照）。

図 7-25　既存のクリプト マップ：左端カラム



ステップ 3　スクロールして、ダイアログボックスの右半分を表示します。
別のカラムが表示されます（図 7-26 を参照）。

図 7-26　既存のクリプト マップ：右端カラム



ステップ 4　[Life Time(sec)] カラムをダブルクリックし、値を変更します。

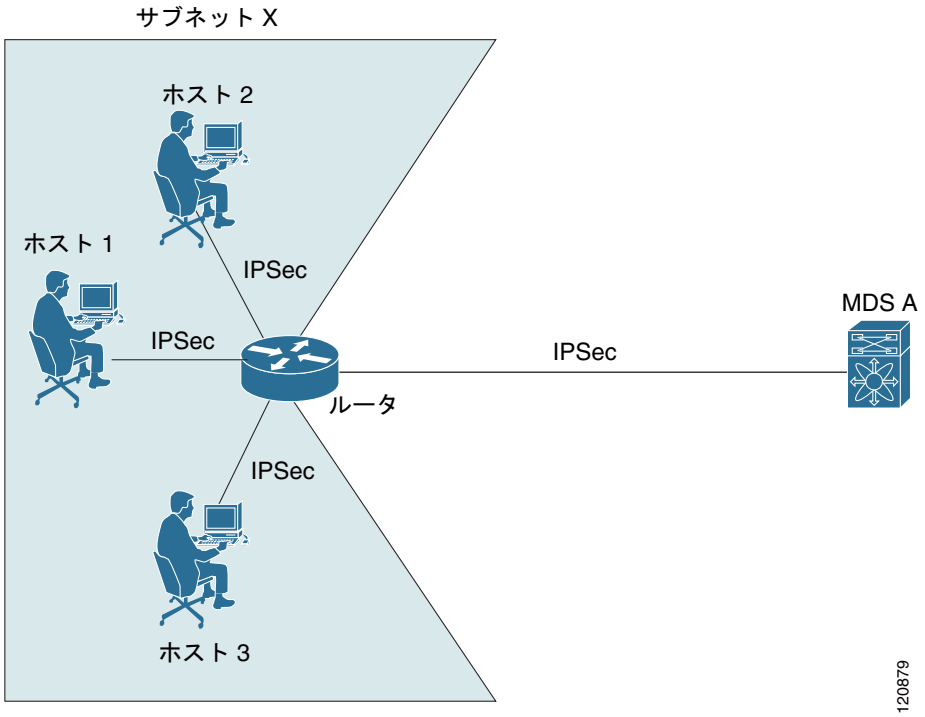
ステップ 5　[Apply Changes] アイコンをクリックして変更内容を保存します。

[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 [**AutoPeer**] 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 7-27 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。

図 7-27　auto-peer オプションを使用した iSCSI のエンドツーエンド IPSec

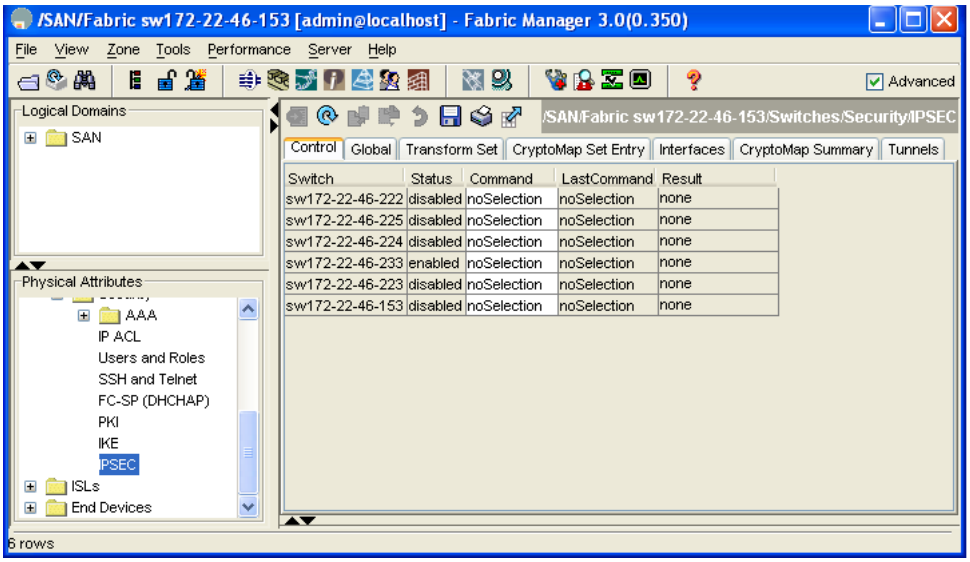


[AutoPeer] オプションの設定

Fabric Manager を使用して [AutoPeer] オプションを設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。[Information] ペインに IPSec の設定が表示されます（図 7-28 を参照）。

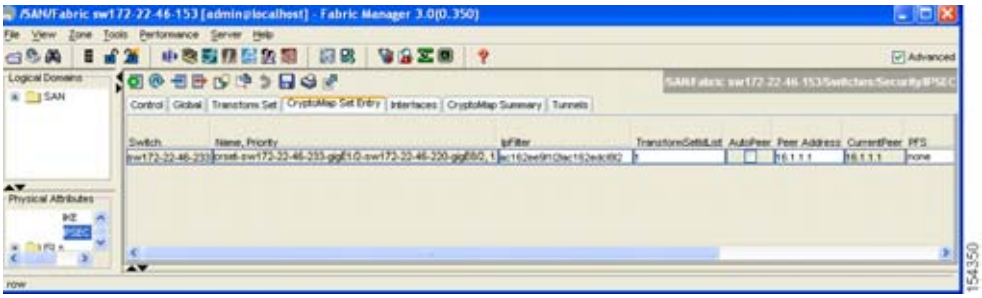
図 7-28　IPSec の設定



ステップ 2　[CryptoMap Set Entry] タブをクリックします。

設定されている既存のクリプト マップが表示されます（図 7-29 を参照）。

図 7-29　既存のクリプト マップ



ステップ 3　選択したクリプト マップ セット エントリの [AutoPeer] オプションを選択または選択解除します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

完全転送秘密の概要

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 Perfect Forward Secrecy（PFS; 完全転送秘密）値を設定できます。

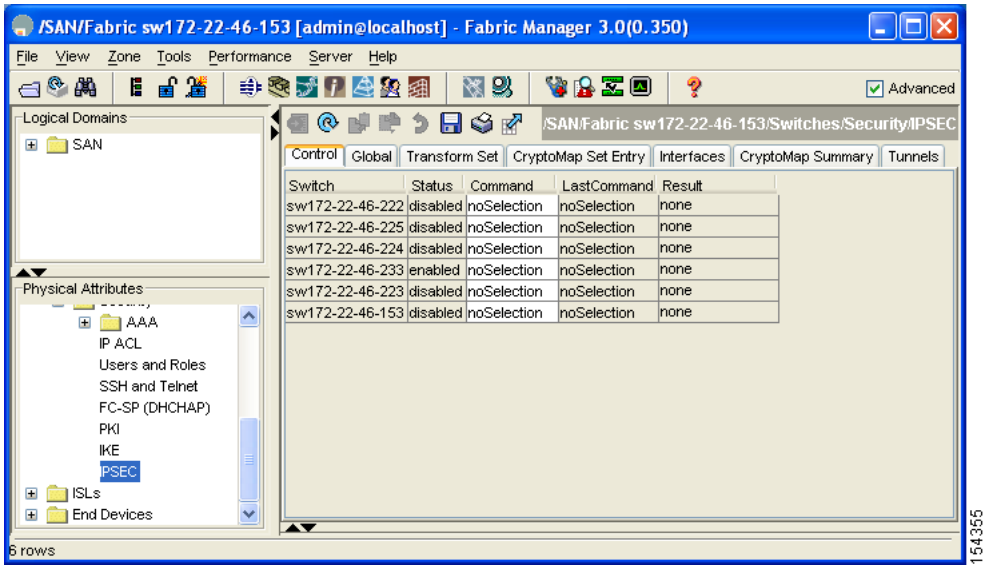
PFS 機能は、デフォルトではディセーブルです。PFS グループを設定する場合は、DH グループ 1、2、5、または 14 のうちの 1 つを設定できます。DH グループを指定しない場合、グループ 1 がデフォルトで使用されます。

完全転送秘密の設定

Fabric Manager を使用して PFS 値を設定する手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。[Information] ペインに IPSec の設定が表示されます（図 7-30 を参照）。

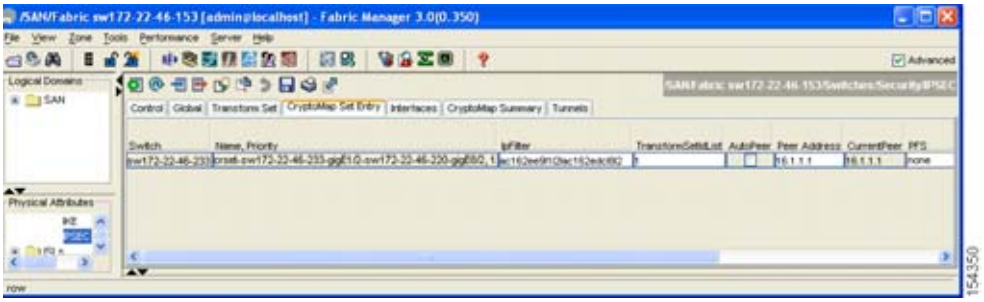
図 7-30　IPSec の設定



ステップ 2　[CryptoMap Set Entry] タブをクリックします。

設定されている既存のクリプト マップが表示されます（図 7-31 を参照）。

図 7-31　既存のクリプト マップ



ステップ 3　[PFS] カラムのドロップダウン リストをクリックして、適切な値を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

クリプト マップ セットの適用の概要

IPSec トラフィックが通過するインターフェイスごとに、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 セットを適用することはできません。

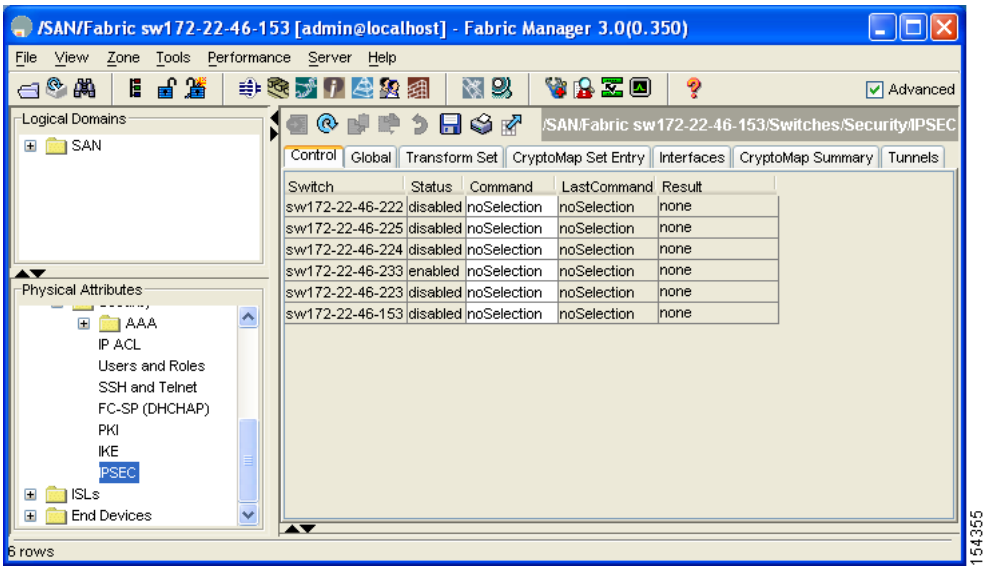
クリプト マップ セットの適用

Fabric Manager を使用してクリプト 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。

ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。

[Information] ペインに IPSec の設定が表示されます（図 7-32 を参照）。

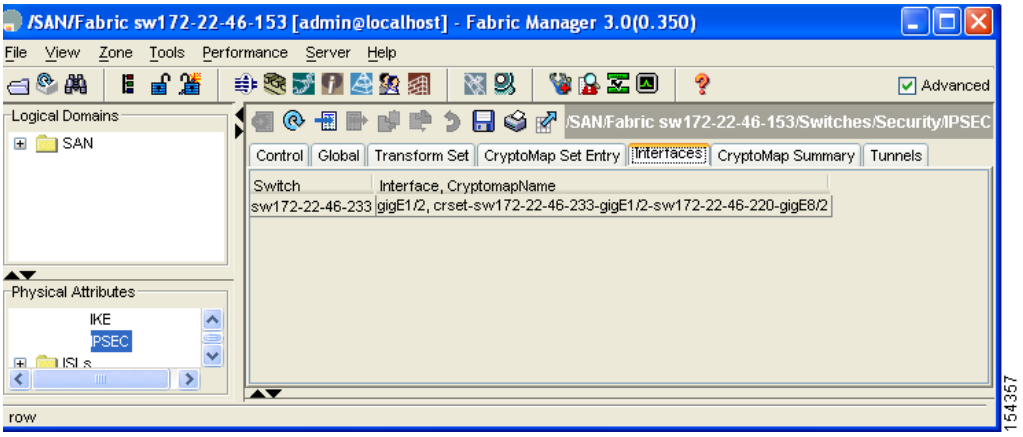
図 7-32　IPSec の設定



ステップ 2　[Interfaces] タブをクリックします。

クリプト マップ設定に既存のインターフェイスが表示されます（図 7-33 を参照）。

図 7-33　クリプト マップ インターフェイス



ステップ 3　設定するスイッチおよびインターフェイスを選択します。

ステップ 4　[CryptomapSetName] フィールドに、このインターフェイスに適用するクリプト マップの名前を入力します。

ステップ 5　選択したインターフェイスにクリプト マップを適用するには、[Create] ボタンをクリックします。クリプト マップを適用しないでダイアログボックスを閉じるには、[Close] ボタンをクリックします。

IPSec のメンテナンス

設定の変更は、後続のセキュリティ アソシエーション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セキュリティ アソシエーションが再確立されるように、既存のセキュリティ アソシエーション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、セキュリティ アソシエーション データベースのうち、設定変更が影響する部分だけをクリアしてください（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セキュリティ アソシエーションだけをクリアします）。セキュリティ アソシエーション データベース全体をクリアするのは、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。

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クリアします。

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。

Fabric Manager を使用してグローバル SA ライフタイムを設定する手順は、次のとおりです。

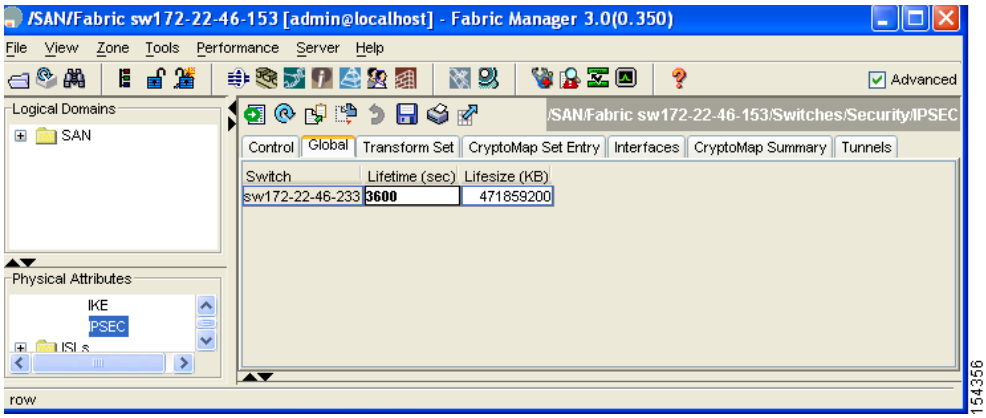
ステップ 1　[Physical Attributes] ペインで [Switches] > [Security] を展開し、[IPSEC] を選択します。

ステップ 2　[Information] ペイン内に IPSec 設定が表示されます。

ステップ 3　[Global] タブをクリックします。

ステップ 4　[Life Time(sec)] カラムをダブルクリックして、値を変更します（図 7-34 を参照）。

図 7-34　IPSec 設定の [Global] タブ



ステップ 5　[Apply Changes] アイコンをクリックして変更内容を保存します。

デフォルト設定値

表 7-3 に、IKE パラメータのデフォルト設定を示します。

表 7-3　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	設定不可（事前共有キーを使用）
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 00 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 7-4 に、IPSec パラメータのデフォルト設定を示します。

表 7-4　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

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 DH 交換を組み合わせたものです。

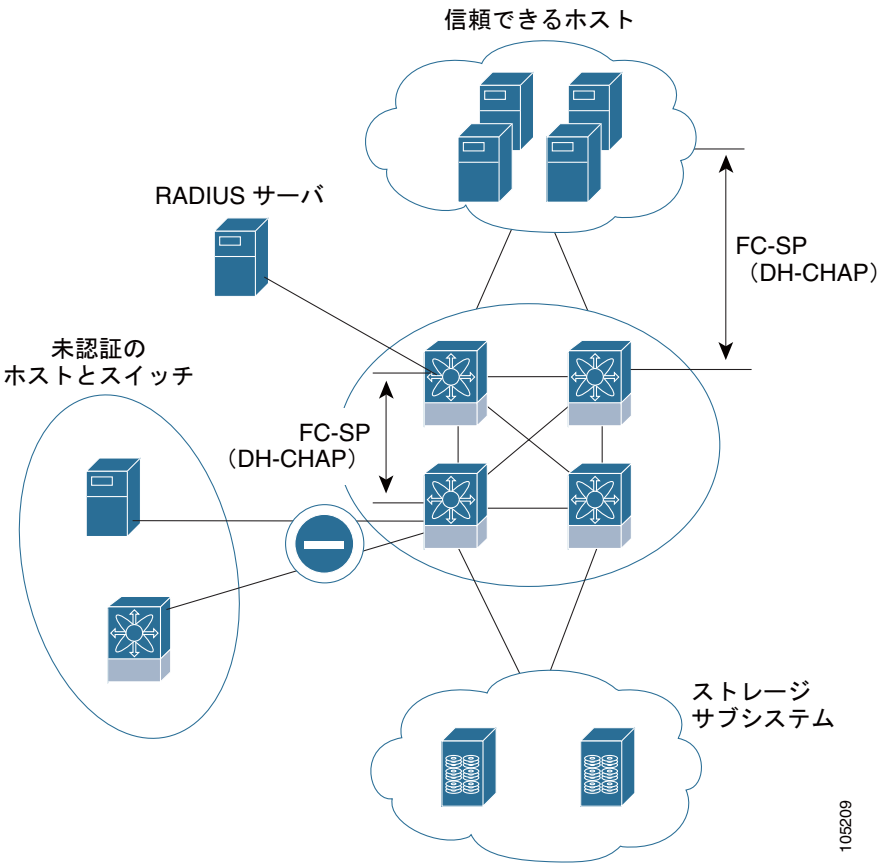
この章の内容は、次のとおりです。

ファブリック認証の概要

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に実行することも、リモートで実行することもできます。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を相互接続することにより、Inter-Switch Link（ISL; スイッチ間リンク）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



DHCHAP

DHCHAP は、スイッチに接続された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、スイッチ間およびホストとスイッチ間の認証をサポートする、必須のパスワードベースのキーエクスチェンジ認証プロトコルです。DHCHAP は、ハッシュ アルゴリズムおよび DH グループとネゴシエートしてから、認証を実行します。また、Message Digest 5（MD5）および Secure Hash Algorithm（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上の他のスイッチの DHCHAP パスワードを設定します。
ステップ 5　再認証用の DHCHAP タイムアウト値を設定します。
ステップ 6　DHCHAP 設定を確認します。

ここで説明する内容は、次のとおりです。

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。

- ポートチャネル インターフェイス：ポートチャネルに属しているポートに対して DHCHAP がイネーブルの場合、DHCHAP 認証はポートチャネル 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。
- Fibre Channel over IP（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。
- Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）：DHCHAP 認証は VSAN 単位では実行されません。

- High Availability（HA; 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設定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。

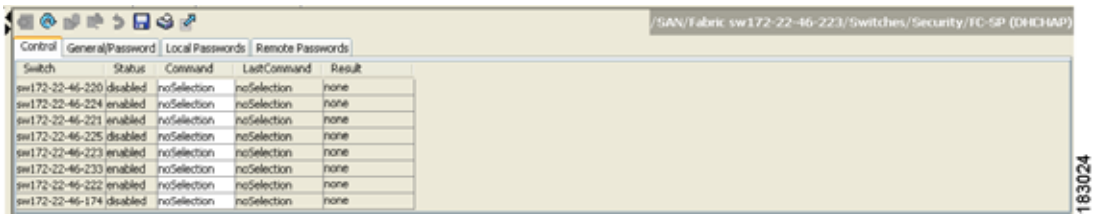
DHCHAP のイネーブル化

Fabric Manager を使用して 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。

ステップ 1　[Switches]、[Security] の順に展開し、[FC-SP] を選択します。

[Information] ペインに FC-SP（DHCHAP）の設定が表示されます（図 8-2 を参照）。

図 8-2　FC-SP の設定



[Control] タブがデフォルトです。ファブリック内の全スイッチの FC-SP イネーブル ステートが表示されます。

ステップ 2　FC-SP をイネーブルにするすべてのスイッチについて、[Command] ドロップダウン メニューを [enable] に設定します。

ステップ 3　[Apply Changes] アイコンをクリックし、選択したスイッチ上で FC-SP および DHCHAP をイネーブルにします。

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、設定された DHCHAP ポート モードによって異なります。

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 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、スイッチの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、スイッチの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、認証シーケンスの残りが継続されます。
- 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 認証を開始した場合には、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。

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 N DHCHAP モード	スイッチ 1 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

Fabric Manager を使用して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。

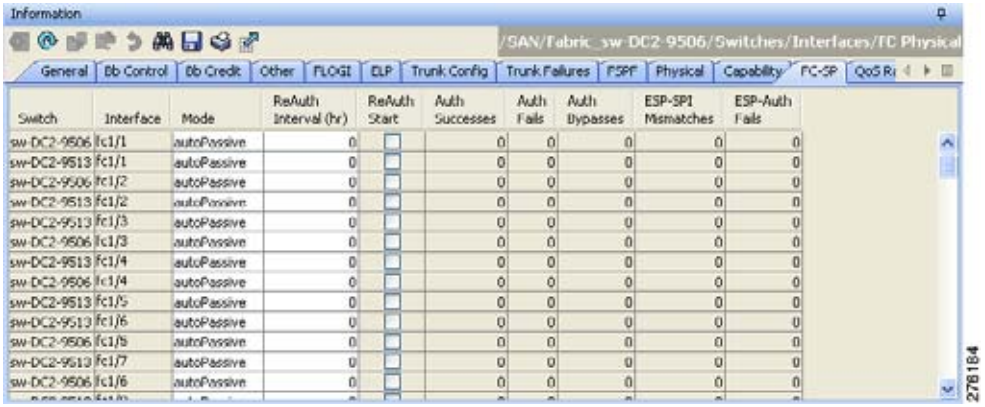
ステップ 1　[Switches]、[Interfaces] の順に展開し、[FC Physical] を選択します。

[Information] ペインにインターフェイス設定が表示されます。

ステップ 2　[FC-SP] タブをクリックします。

[Information] ペインに FC-SP（DHCHAP）の設定が表示されます（図 8-3 を参照）。

図 8-3　FC-SP（DHCHAP）インターフェイス モード



ステップ 3　[Mode] ドロップダウン メニューで、インターフェイスに設定する DHCHAP 認証モードを設定します。

ステップ 4　[Apply Changes] アイコンをクリックして、DHCHAP ポート モードの設定を保存します。

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には、ファブリック内のすべてのスイッチに対してグローバルに変更します。

注意　Remote Access Dial-In User Service（RADIUS）および Terminal Access Controller Access Control System Plus（TACACS+）プロトコルは CHAP 認証に必ず MD5 を使用します。ハッシュ アルゴリズムとして SHA-1 を使用すると、これらの Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）プロトコルが DHCHAP 認証に対してイネーブルに設定されていても、RADIUS および TACACS+ を使用できないことがあります。

DHCHAP ハッシュ アルゴリズムの設定

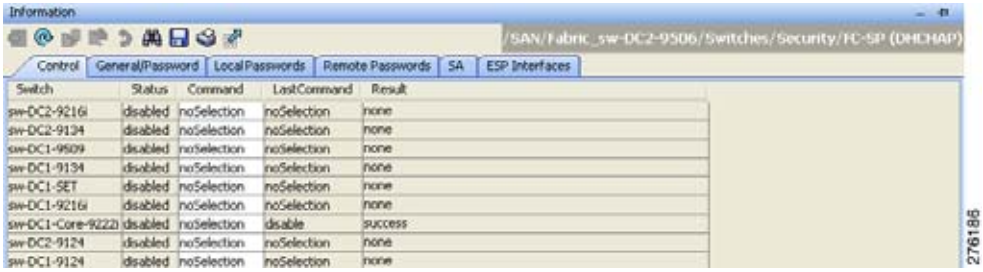
Fabric Manager を使用してハッシュ アルゴリズムを設定する手順は、次のとおりです。

ステップ 1　[Switches] > [Security] を選択し、[FC-SP] を選択します。

ステップ 2　[General/Password] タブをクリックします。

各スイッチの DHCHAP 一般設定モードが表示されます（図 8-4 を参照）。

図 8-4　[General/Password] タブ



ステップ 3　ファブリック内の各スイッチの DHCHAP HashList を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP グループ設定の概要

すべての Cisco MDS ファミリ スイッチは、標準で指定されたすべての DHCHAP グループをサポートします。これらのグループは、0（Diffie-Hellman 交換を実行しないヌル DH グループ）、1、2、3、または 4 です。

ヒント　DH グループの設定を変更する場合には、ファブリック上の全スイッチに対してグローバルに変更してください。

DHCHAP グループの設定

Fabric Manager を使用して DH グループ設定を変更する手順は、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。

ステップ 2　[General/Password] タブをクリックします。

ステップ 3　ファブリック内の各スイッチの DHCHAP GroupList を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新したハッシュ アルゴリズム プライオリティ リストを保存します。

DHCHAP パスワードの概要

DHCHAP 認証を方向ごとに実行するには、接続された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、このファブリック上では同じパスワードを使用してそのスイッチを認証することになります。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には、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。新規スイッチを追加する場合は、ファブリック上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） すべてのパスワードは 64 個の英数字に制限され、変更可能ですが、削除はできません。

ヒント 6 台以上のスイッチを含むファブリックでは、RADIUS または TACACS+ の使用を推奨します。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

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 World Wide Name（WWN）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] ボタンをクリックして、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

ファブリック上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 またはデバイス WWN と呼ばれるデバイス名によって識別されます。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。

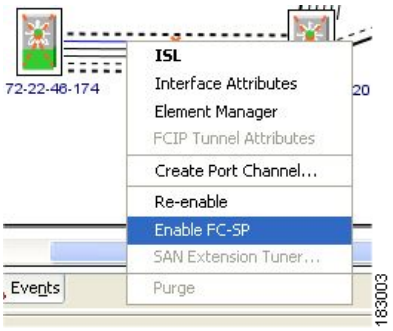
（注）　スイッチ WWN は物理スイッチを識別します。スイッチ WWN はスイッチを認証する場合に使用され、VSAN ノードの WWN とは異なります。

リモート デバイスの DHCHAP パスワードの設定

Fabric Manager を使用して、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。

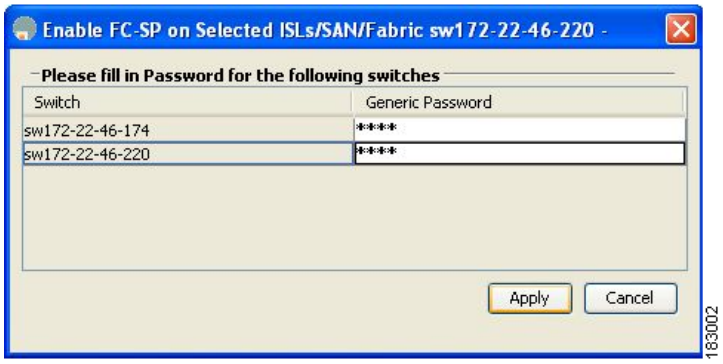
ステップ 1　ISL を右クリックし、ドロップダウン リストから [Enable FC-SP] を選択します（図 8-5 を参照）。

図 8-5　[Enable FC-SP]



[Enable FC-SP] ダイアログボックスが表示されます。

図 8-6　[Enable FC-SP] ダイアログボックス



ステップ 2　[Apply] ボタンをクリックして、更新したパスワードを保存します。

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。このインターバルは 20（認証が実行されない）～ 1000 秒です。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。
- ファブリック上の全スイッチに同じ値を設定する必要があります。

DHCHAP タイムアウト値の設定

Fabric Manager を使用して DHCHAP タイムアウト値を設定する手順は、次のとおりです。

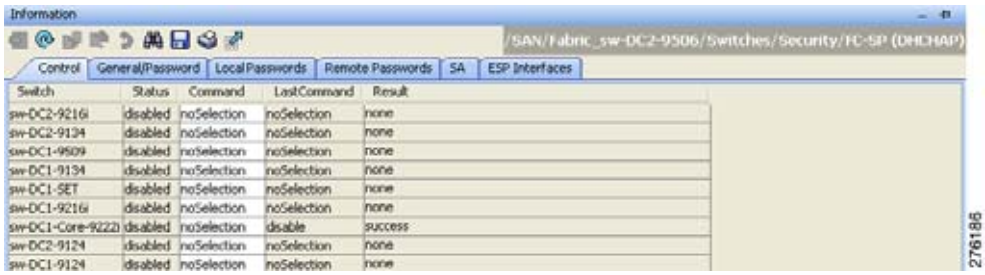
ステップ 1　[Switches] > [Security] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[General/Password] タブをクリックします。

各スイッチの DHCHAP 一般設定モードが表示されます（図 8-7 を参照）。

図 8-7　[General/Password] タブ



ステップ 3　ファブリック内の各スイッチの DHCHAP タイムアウト値を変更します。

ステップ 4　[Apply Changes] アイコンをクリックして、更新情報を保存します。

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 認証の設定については、第 4 章「RADIUS および TACACS+ の設定」を参照してください。

ISL 上での FC-SP のイネーブル化

Fabric Manager には、ISL のどちらかの側のスイッチ上で FC-SP をイネーブルにする、[Enable FC-SP] と呼ばれる ISL のポップアップ メニューがあります。FC-SP 一般パスワードを入力し、関連ポートの FC-SP インターフェイス モードを ON に設定します。この機能を設定するには、ISL を右クリックして、[Enable FC-SP] ポップアップ メニューをクリックします。

デフォルト設定値

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　ファブリック セキュリティのデフォルト設定

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 セキュリティがサポートされるのは、ファイバ チャネル ポートだけです。

この章の内容は、次のとおりです。

ポート セキュリティの概要

通常、Storage Area Network（SAN; ストレージ エリア ネットワーク）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。
- 設定の配布は Cisco Fabric Services（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ます。配布はデフォルトでディセーブルです。
- 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）。

ここで説明する内容は、次のとおりです。

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、デバイスまたはスイッチに、それぞれを接続するポート インターフェイスを設定し、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ごとに、およびポートの起動時に適用されます。

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、設定変更を受け入れて、実装します。

- コンフィギュレーション データベース：設定の変更はすべて、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：ファブリックで現在実行されているデータベースです。ポート セキュリティ機能を実行するには、スイッチに接続しているすべてのデバイスを、ポート セキュリティ アクティブ データベースに登録する必要があります。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

指定した期間にわたって、スイッチがポート セキュリティ設定を自動学習（auto-learn）するように設定できます。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最初にアクティブにするときに、この機能を使用すると、各ポートを手動で設定する面倒な作業が軽減されます。自動学習は、Virtual SAN（VSAN; 仮想 SAN）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、スイッチにログインしていないデバイスまたはインターフェイスに関する学習だけが実行されます。自動学習がイネーブルのときにポートをシャットダウンすると、そのポート上で学習されたエントリは消去されます。

学習によって、設定済みのポート セキュリティ ポリシーが上書きされることはありません。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。自動学習モードであっても、他のすべての pWWN はブロックされます。

シャットダウン状態のポートについては、エントリは学習されません。

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 セキュリティをアクティブにする前に自動学習をイネーブルにした場合、自動学習をディセーブルにしないと、ポート セキュリティをアクティブにできません。

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。

- 自動学習が自動的にイネーブルになります。
  - この時点から、スイッチにログインしていないデバイスまたはインターフェイスに限り、自動学習が実行されます。
  - 自動学習をディセーブルにするまでは、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が学習され、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をアクティブにするには、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て、自動学習をディセーブルにすることもできます。

ヒント　ログインが拒否されてシャットダウンしたポートは、その後ログインが許可されるようにデータベースを設定しても、自動的には起動しません。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には、自動学習の動作が異なります。

ここで説明する内容は、次のとおりです。

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」（P.9-9）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」（P.9-19）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」（P.9-10）を参照してください。

ステップ 4　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）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　すべてのスイッチおよびホストが自動学習されるまで待機します。

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」（P.9-15）を参照してください。

ステップ 7　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）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　アクティブ データベースを、各 VSAN のコンフィギュレーション データベースにコピーします。「ポート セキュリティ データベースのコピー」（P.9-23）を参照してください。

ステップ 9　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）を参照してください。これにより、ファブリック内のすべてのスイッチで、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 配信を使用しないポート 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」（P.9-9）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」（P.9-10）を参照してください。

ステップ 3　すべてのスイッチおよびホストが自動学習されるまで待機します。

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」（P.9-15）を参照してください。

ステップ 5　アクティブ データベースを、各 VSAN のコンフィギュレーション データベースにコピーします。「ポート セキュリティ データベースのコピー」（P.9-23）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によるポート 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」（P.9-9）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」（P.9-17）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」（P.9-10）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」（P.9-15）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。

設定ウィザードを使用したポート セキュリティの設定

ポート セキュリティの設定ウィザードを使用すると、選択した VSAN のポート セキュリティ ポリシーの設定をステップバイステップ方式で実行できます。ポート セキュリティの設定ウィザードでは、設定全体の一元的な管理を可能にする、CFS を使用した中央管理をサポートしています。

ウィザードでは自動的に、いくつかの必須操作が行われます。たとえば、中央管理が必要な場合は、ウィザードが CFS 機能をチェックし、CFS をイネーブルにして、CFS コミットを発行する操作を適切な段階で実行します。

特定のポートでセキュリティを管理する場合は、このウィザードを使って VSAN 全体のポート セキュリティ ポリシーを設定する必要はなく、そのポート自体でアクセスを直接編集できます。この操作は、[Port Binding] ダイアログボックスで実行できます。ポートが付属するスイッチでポート セキュリティをまだイネーブルにしていない場合、ダイアログボックスではまずセキュリティをイネーブルにします。ポート セキュリティがイネーブルになると、ダイアログボックスではユーザの操作に基づいてポリシー データベースが編集されます。

前提条件

ポート セキュリティを設定するための前提条件は、次のとおりです。

- スイッチでポート セキュリティがイネーブルである。
- ポート セキュリティ ポリシーが、バインドされたデバイス、スイッチ、またはポートを編集することによって手動で、または自動学習機能を使用して定義されている。
- ポート セキュリティ ポリシーがアクティブである。

- アクティブ化されたデータベースと設定済みデータベースがコピーによって同期化されている。
- アクティブ化されたデータベースが、スタートアップ コンフィギュレーションにするためにコピーされいる。
- CFS が VSAN 内のすべてのスイッチでイネーブルである。すべての設定の実行に CFS マスタースイッチが選択されている。すべての変更は、CFS **commit** コマンドを使って VSAN に配布されます。

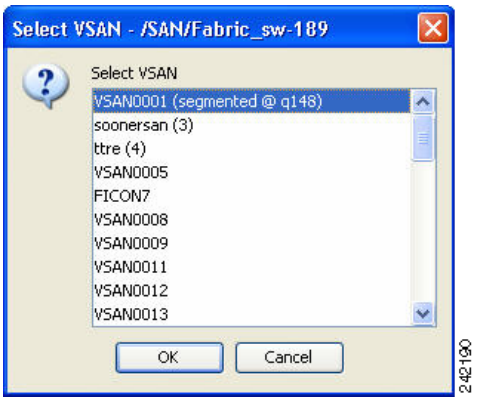
ポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ツールバーの [Port Security]  ボタンをクリックします。

[Port Security Setup Wizard] を起動する前に、Fabric Manager によって VSAN 内のスイッチの CFS 機能がチェックされます。

VSAN コンテキストを使用できない場合、VSAN を選択するプロンプトが表示されます（図 9-1 を参照）。

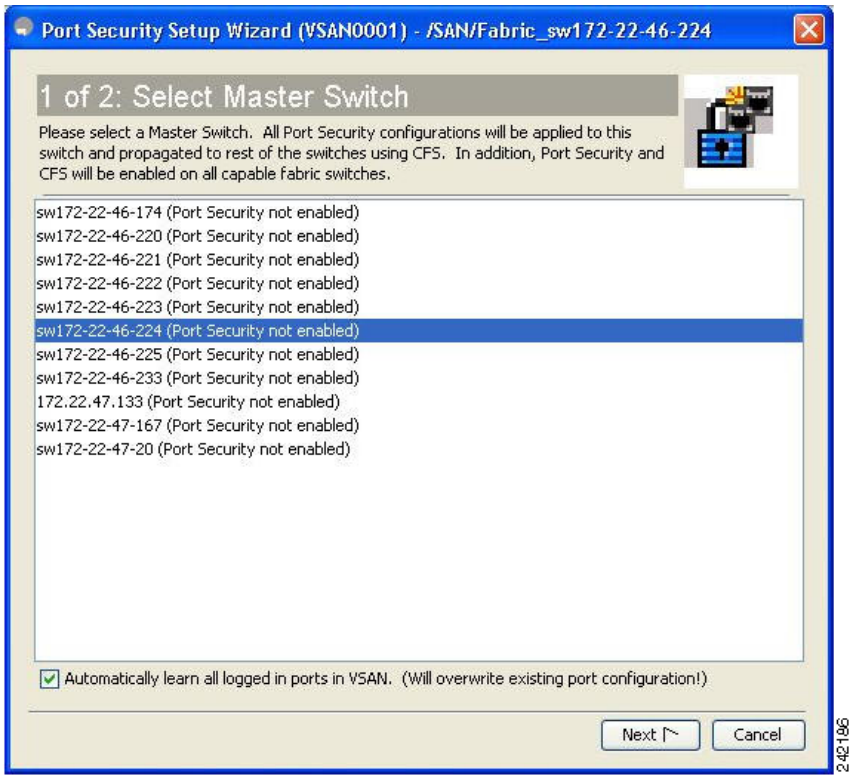
図 9-1　[Select VSAN] ウィンドウ



ステップ 2　リストから VSAN を選択し、[OK] ボタンをクリックします。

[Port Security Setup Wizard] の最初のページが表示されます（図 9-2 を参照）。

図 9-2　[Select Master Switch] ページ



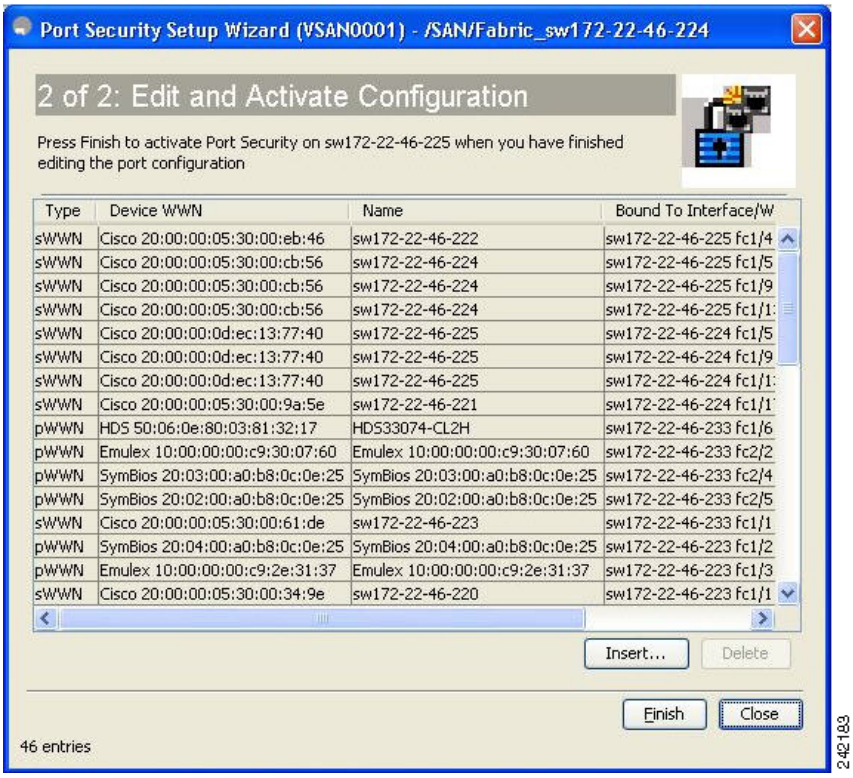
ステップ 3　[Select Master Switch] ページで次の操作を行います。

- 必要なマスター スイッチを選択します。
- ポート設定を自動学習させるには、[Automatically learn all logged in ports in VSAN] チェックボックスをオンにします。

ステップ 4　[Next] ボタンをクリックして先に進みます。

[Edit and Activate Configuration] ページが表示されます（図 9-3 を参照）。

図 9-3　[Edit and Activate Configuration] ページ



ステップ 5　[Insert] ボタンをクリックして、ポート バインディングを作成します。

[Insert Port Security Devices] ダイアログボックスが表示されます（図 9-4 を参照）。

図 9-4　*[Insert Port Security Devices] ダイアログボックス*

ステップ 6　[Insert Port Security Devices] ダイアログボックスでは、次の 2 つのタイプのポート バインディングを作成できます。

- [Port WWN]：インターフェイス WWN にバインドされる pWWN
- [Switch]：インターフェイスにバインドされるスイッチ WWN （主に ISL バインディングに有効）

ステップ 7　オプション ボタンをクリックしてポート バインディングのタイプを選択し、サポートする値を入力します。

ステップ 8　[OK] ボタンをクリックします。

ステップ 9　[Close] ボタンをクリックして [Insert Port Security] ウィンドウを終了します。

（注）　ウィザードの [Edit and Activate Configuration] ページのエントリを削除するには、[Delete] ボタンをクリックします。

ステップ 10　[Finish] をクリックして、選択したスイッチのポート セキュリティの設定を完了します。

ポート セキュリティのイネーブル化

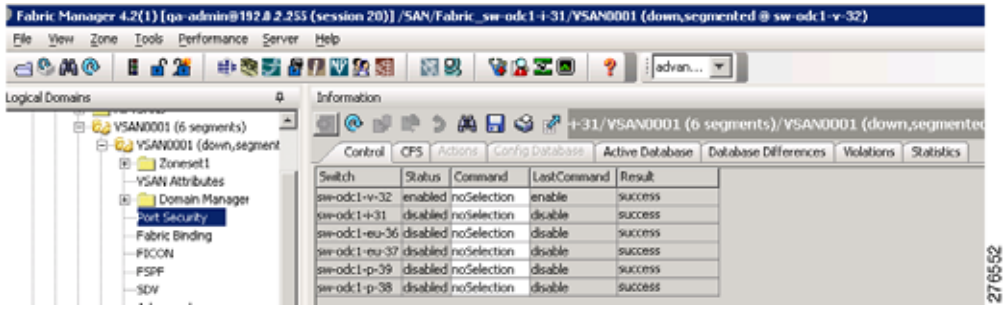
デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポート セキュリティ機能はディセーブルです。

Fabric Manager を使用してポート セキュリティをイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-5 を参照）。

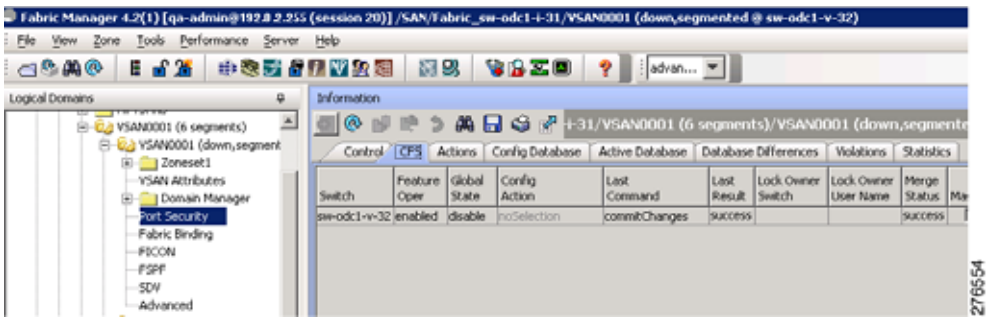
図 9-5　ポート セキュリティ設定



ステップ 2　[CFS] タブをクリックします。

図 9-6 のような情報が表示されます。

図 9-6　ポート セキュリティ CFS



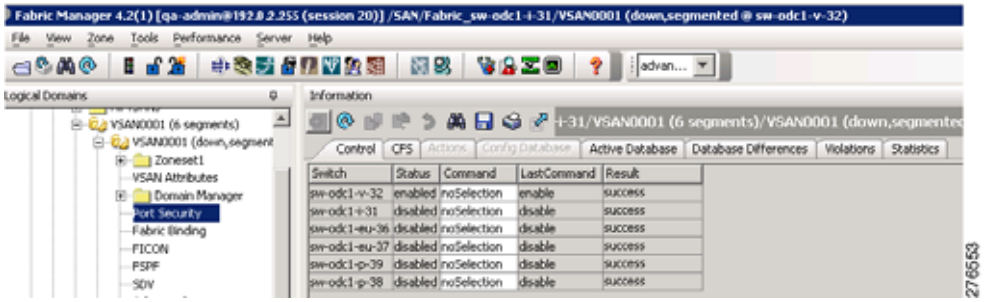
ステップ 3　[Global] カラムの各エントリをクリックし、[enable] を選択して、VSAN 内のすべての参加スイッチ上の CFS をイネーブルにします。

ステップ 4　[Apply Changes] アイコンをクリックし、ポート セキュリティ機能の CFS 配布をイネーブルにします。

ステップ 5　[Control] タブをクリックします。

選択した VSAN 内の全スイッチのポート セキュリティ イネーブル ステートが表示されます（図 9-7 を参照）。

図 9-7　　ポート セキュリティ設定



ステップ 6　VSAN 内の各スイッチについて、[Command] カラムを [enable] に設定します。

ステップ 7　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 8　[Apply Changes] アイコンをクリックして、VSAN 内の全スイッチに、イネーブルにしたポート セキュリティを配信します。

ポート セキュリティのアクティブ化

ここで説明する内容は、次のとおりです。

ポート セキュリティのアクティブ化

Fabric Manager を使用してポート セキュリティをアクティブにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックします。ドロップダウン メニューに、次のオプションが表示されます。

- [activate]：有効なポート セキュリティ設定をアクティブにします。
- [activate (TurnLearningOff)]：有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- [forceActivate]：強制的にアクティブにします。
- [forceActivate (TurnLearningOff)]：強制的にアクティブにし、自動学習をオフにします。
- [deactivate]：現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- [NoSelection]：何も実行しません。

ステップ 4　スイッチに適用する [Action] フィールドを設定します。

ステップ 5　自動学習をディセーブルにするには、VSAN の各スイッチの [AutoLearn] チェックボックスをオフにします。

ステップ 6　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 7　Fabric Manager で [Apply Changes] アイコンをクリックするか、Device Manager で [Apply] ボタンをクリックし、変更内容を保存します。

（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」（P.9-15）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 データベースに存在するが、アクティブ データベースにはない場合。
- アクティブ化する前に、自動学習機能がイネーブルに設定されていた場合。この状態で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、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 つまたは複数発生し、データベースのアクティブ化が拒否された場合でも、ポート セキュリティを強制的にアクティブ化すれば、処理を続行できます。

ポート セキュリティの強制的なアクティブ化

ポート セキュリティのアクティブ化要求が拒否された場合、アクティブ化を強制的に実行できます。

（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。

Fabric Manager を使用してポート セキュリティ データベースを強制的にアクティブ化する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックし、[forceactivate] オプションを選択します。

ステップ 4　スイッチに適用する [Action] フィールドを設定します。

ステップ 5　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 6　Fabric Manager で [Apply Changes] アイコンをクリックするか、Device Manager で [Apply] ボタンをクリックし、変更内容を保存します。

データベースの再アクティブ化

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、処理を継続できません。

Fabric Manager を使用してポート セキュリティ データベースを再アクティブ化する手順は、次のとおりです。

ステップ 1　自動学習をディセーブルにします。

ステップ 2　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。

ヒント　アクティブ データベースが空の場合には、この手順を実行できません。

ステップ 3　必要に応じて、コンフィギュレーション データベースを変更します。

ステップ 4　データベースをアクティブにします

コンフィギュレーション データベースへのアクティブ データベースのコピー

Fabric Manager を使用して、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する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　データベースをコピーするスイッチの横にある、[CopyActive ToConfig] チェックボックスをオンにします。

セキュリティ設定がアクティブになると、アクティブ データベースがコンフィギュレーション データベースにコピーされます。

ステップ 4　セキュリティ設定をアクティブにしたときにデータベースをコピーしない場合は、[CopyActive ToConfig] チェックボックスをオフにします。

ステップ 5　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 6　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

アクティブなポート セキュリティ設定の表示

Fabric Manager を使用してアクティブなポート セキュリティ設定を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Active Database] タブをクリックします。

その VSAN のアクティブなポート セキュリティ設定が表示されます。

ポート セキュリティ統計情報の表示

Fabric Manager を使用してポート セキュリティ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。

その VSAN のポート セキュリティ統計情報が表示されます。

ポート セキュリティ違反の表示

ポート違反とは、不正なログイン試行のことです（たとえば、不正なファイバ チャネル デバイスからログイン要求があった場合）。Fabric Manager を使用すると、これらの試行に関するリストを VSAN 単位で表示できます。

ポート セキュリティ違反を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Violations] タブをクリックします。その VSAN のポート セキュリティ違反が表示されます。

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

自動学習の設定の状態は、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非アクティブである場合、自動学習はデフォルトでディセーブルになります。
- 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になります（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 上の自動学習がイネーブルである場合、**force** オプションを使用しないと、その VSAN のデータベースをアクティブ化できません。

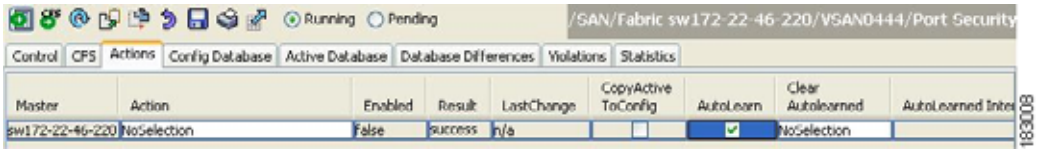
自動学習のイネーブル化

Fabric Manager を使用して自動学習をイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

図 9-8　ポート セキュリティ設定



ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックします。ドロップダウン メニューに、次のオプションが表示されます。

- [activate]：有効なポート セキュリティ設定をアクティブにします。

- [activate (TurnLearningOff)]：有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- [forceActivate]：強制的にアクティブにします。
- [forceActivate (TurnLearningOff)]：強制的にアクティブにし、自動学習をオフにします。
- [deactivate]：現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- [NoSelection]：何も実行しません。

ステップ 4　そのスイッチに適用する、いずれかのポート セキュリティ オプションを選択します。

ステップ 5　自動学習をイネーブルにするには、VSAN の各スイッチの [AutoLearn] チェックボックスをオンにします。

ステップ 6　[Apply Changes] アイコンをクリックして変更内容を保存します。

自動学習のディセーブル化

Fabric Manager を使用して自動学習をディセーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

ステップ 2　[Actions] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　自動学習をディセーブルにするには、スイッチの横にある [AutoLearn] チェックボックスをオフにします。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

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示します。

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（自動学習がイネーブルの場合）
4			拒否（自動学習がディセーブルの場合）

表 9-1　許可される自動学習デバイス要求 （続き）

条件	デバイス（pWWN、nWWN、sWWN）	接続先	許可
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できるスイッチ 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

許可のシナリオ

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ものとします。

- 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示します。ここに示す条件は、表 9-1 の条件に基づいています。

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 だけで許可されます。
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。

表 9-2　各シナリオの許可結果 （続き）

デバイス接続要求	許可	条件	理由
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 および 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（*）一致です。

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。

ここで説明する内容は、次のとおりです。

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と、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が保存されます。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

バインドする必要がある WWN 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。

Fabric Manager を使用して、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手順は、次のとおりです。

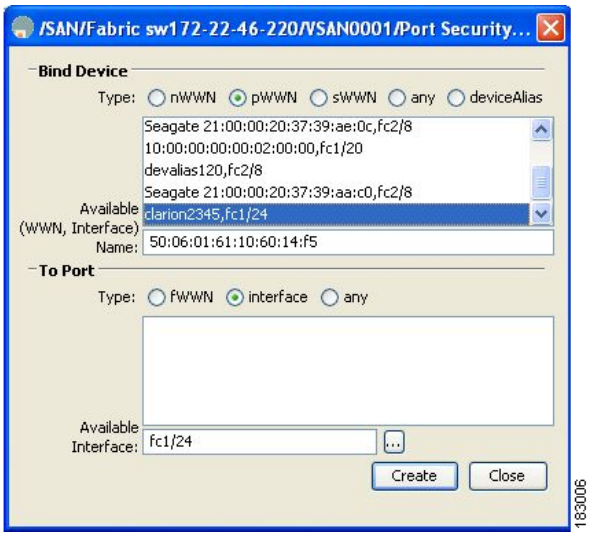
ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

ステップ 2　[Config Database] 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、許可済みのポート ペアを追加します。

[Create Port Security] ダイアログボックスが表示されます（図 9-9 を参照）。

図 9-9　[Create Port Security] ダイアログボックス



ステップ 4　リストから、ポート セキュリティ設定を作成するデバイスをダブルクリックします。

ステップ 5　リストから、デバイスをバインドするポートをダブルクリックします。

ステップ 6　[Create] ボタンをクリックして、ポート セキュリティ設定を作成します。

ステップ 7　[Apply Changes] アイコンをクリックして変更内容を保存します。

ポート セキュリティ設定の削除

スイッチ上の既存のデータベースからポート セキュリティ設定を削除する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

ステップ 2　[Config Database] タブをクリックします。

VSAN の既存のポート セキュリティ設定が表示されます。

ステップ 3　削除する行をクリックします。

ステップ 4　[Delete Row] をクリックします。

確認ダイアログボックスが表示されます。

ステップ 5　行を削除するには、[Yes] ボタンをクリックします。行を削除しないで確認ダイアログボックスを閉じるには、[No] ボタンをクリックします。

ステップ 6　[Apply Changes] アイコンをクリックして変更内容を保存します。

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行し、VSAN 内のファブリック全体に単一の設定を提供して、ファブリック全体でポート セキュリティ ポリシーを施行します（第 7 章「CFS インフラストラクチャの使用」を参照）。

ここで説明する内容は、次のとおりです。

- 「配信のイネーブル化」（P.9-19）
- 「ファブリックのロック」（P.9-20）
- 「変更のコミット」（P.9-20）
- 「アクティブ化および自動学習の設定の配信」（P.9-20）

配信のイネーブル化

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）データベースに保管されます。設定を変更するには、保留中のデータベースの変更を設定にコミットするか、廃棄する必要があります。この処理の実行中は、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の変更は、変更をコミットするまでは、設定に反映されません。

（注）　CFS 配信がイネーブルの場合、CFS コミットが実行されるまでは、ポートのアクティブ化または非アクティブ化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有効になりません。適正な設定を保持するには、必ず、CFS コミットに関するいずれかの処理を行ってください。「アクティブ化および自動学習の設定の配信」（P.9-20）を参照してください。

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。

Fabric Manager を使用して配信をイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

ステップ 2　[Control] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　[Command] カラムをクリックして、ドロップダウン メニューから [enable] または [disable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ファブリックのロック

既存設定の変更を開始すると、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。

- 他のユーザは、この機能の設定を変更できなくなります。
- 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。

変更のコミット

設定に変更をコミットすると、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。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。

アクティブ化および自動学習の設定の配信

配信モードでのアクティブ化および自動学習の設定は、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される動作として認識されます。

学習されたエントリは一時的なもので、ログインが許可されるかどうかには影響しません。したがって、学習されたエントリは配信には含まれません。学習をディセーブルにして保留中のデータベースの変更をコミットすると、学習されたエントリがアクティブ データベース内のスタティックなエントリになり、ファブリック内のすべてのスイッチに配信されます。コミット実行後は、すべてのスイッチのアクティブ データベースが同一になるので、学習をディセーブルにできます。

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	操作	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 と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	1. ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	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*}	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 = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル}
	2. 新規エントリ E をコンフィギュレーション データベースに追加	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、C*、D*}	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 = {ヌル} 保留中のデータベース = {A、B、E + アクティブ化がイネーブル}
	3. コミットを発行	適用外	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
コンフィギュレーション データベースに A と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	1. ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	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*}	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 = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル}
	2. 学習をディセーブルにする	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}	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 = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル + 学習がディセーブル}
	3. コミットを発行	適用外	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}、デバイス C と D がログアウト。自動学習をディセーブルにしたアクティブ化と同等。 保留中のデータベース = 空

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 マージに関する注意事項

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）エントリの統合を意味します。

2 つのファブリック間でデータベースをマージする場合には、次の事項に注意してください。

- 両方のファブリックのアクティブ化および自動学習が同じ状態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ます。

注意　この 2 つの条件が満たされていない場合、マージは失敗します。次の配信によって、ファブリックのデータベースおよびアクティブ化の状態が強制的に同期化されます。

データベースの相互作用

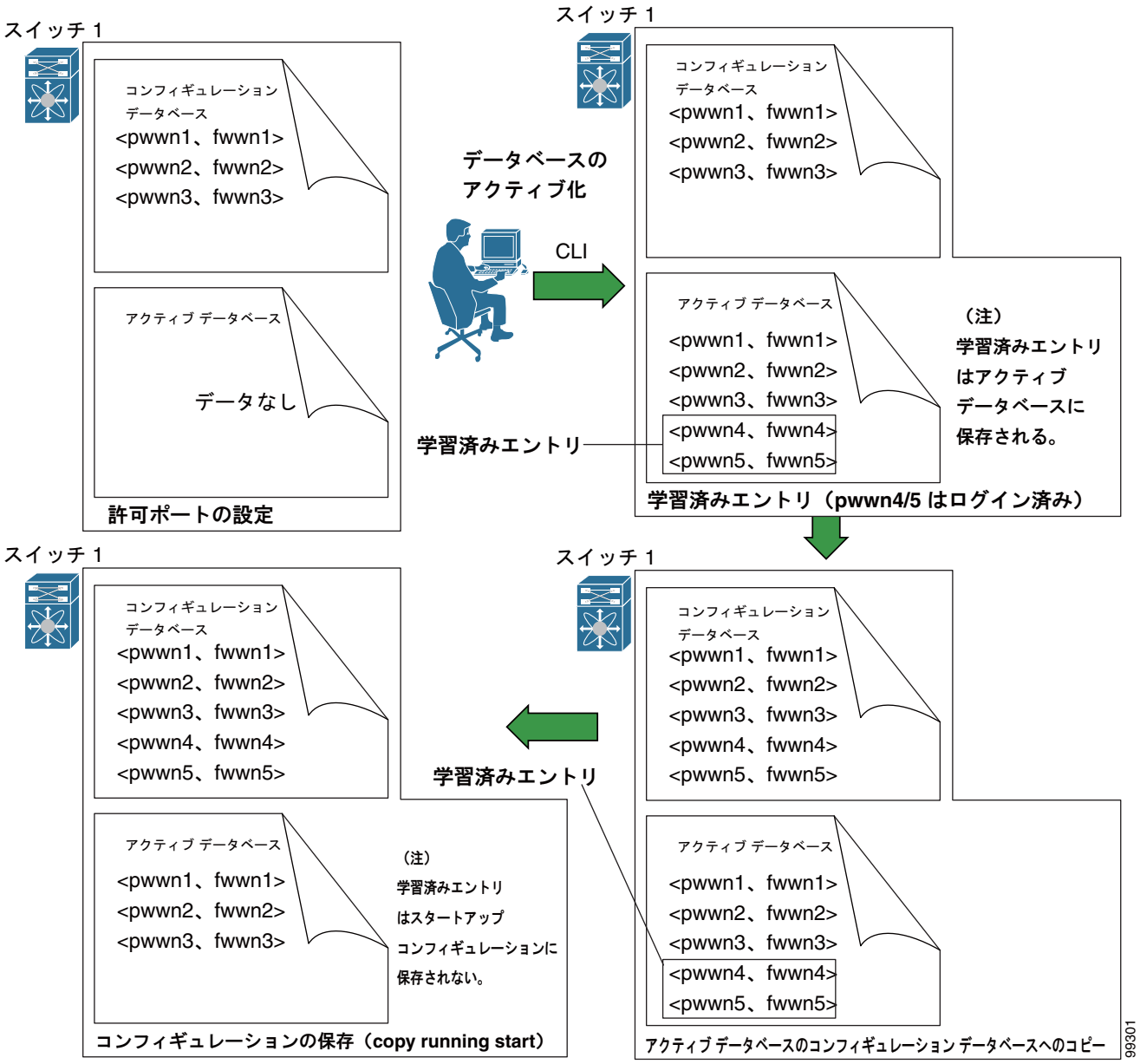
ここで説明する内容は、次のとおりです。

- 「データベースのシナリオ」（P.9-22）
- 「ポート セキュリティ データベースのコピー」（P.9-23）
- 「ポート セキュリティ データベースの削除」（P.9-24）
- 「ポート セキュリティ データベースのクリーニング」（P.9-25）

データベースのシナリオ

図 9-9 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。

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

ヒント　自動学習をディセーブルにしてから、アクティブ データベースをコンフィギュレーション データベースにコピー 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 データベースを完全に同期化できます。配信がイネーブルの場合には、このコマンドにより、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ます（同時にファブリックがロックされます）。ファブリックがロックされた場合、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。

Fabric Manager を使用して、アクティブ データベースをコンフィギュレーション データベースにコピーする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

ステップ 2　[Actions] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Copy Active to Config] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

Fabric Manager を使用して、アクティブ データベースとコンフィギュレーション データベース間の差分を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Database Differences] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択します。[Active] または [Config] オプションを選択して、選択したデータベースとアクティブ/コンフィギュレーション データベース間の差分を比較します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

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、削除を実行すると、データベースのコピーが作成されます。データベースを実際に削除するには、明示的な削除が必要です。

Fabric Manager を使用してポート セキュリティ データベースを削除する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Config Database] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Delete Row] ボタンをクリックします。

ステップ 4　コンフィギュレーション データベースを削除する場合は、[Yes] ボタンをクリックします。

ポート セキュリティ データベースのクリーニング

Fabric Manager を使用して、指定した VSAN に関するすべての既存の統計情報をポート セキュリティ データベースからクリアする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。
[Information] ペインに、ポート セキュリティ情報が表示されます（図 9-8 を参照）。

ステップ 2　[Statistics] タブをクリックします。
すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Clear] オプションを選択します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

Fabric Manager を使用して、VSAN 内の指定したインターフェイスについて、すべての学習済みエントリをアクティブ データベースからクリアする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。
[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Actions] タブを選択します。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[AutoLearn] オプションを選択します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

（注）　[Statistics] タブおよび [AutoLearn] オプションで情報をクリアできるのは、ロックが適用されないローカル スイッチだけです。また、学習済みエントリはスイッチのローカル情報になるだけで、配信には含まれません。

デフォルト設定値

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

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 **（注）**　配信をイネーブルにすると、スイッチのすべての VSAN 上でイネーブルになります。

CHAPTER 10

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。この章の内容は、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 Inter-Switch Link（ISL; スイッチ間リンク）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 Virtual Storage Area Network（VSAN; 仮想ストレージ エリア ネットワーク）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たりすることがなくなります。Exchange Fabric Membership Data（EFMD）プロトコルにより、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ります。

ここで説明する内容は、次のとおりです。

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 ライセンスのどちら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、相互に補完するように設定できる 2 つの独立した機能です。表 10-1 に、2 つの機能の比較を示します。

表 10-1　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 Switch World Wide Name（sWWN; スイッチ WWN）および永続的ドメイン ID を使用します。	Port WWN（pWWN）/Node WWN（nWWN）または Fabric WWN（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（またはリスト）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は学習しません。	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。
Cisco Fabric Services（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。

- スイッチのログインは、特定の VSAN に対して、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 チェックは、ポート VSAN 上で次のように実行されます。
  - ポート VSAN 上での E ポート セキュリティ バインディング チェック
  - 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 チェック

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、スイッチ WWN（sWWN）を設定して、各スイッチに 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に、およびポートを起動しようとした場合に実行されます。Fibre Connection（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、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 Release 3.0(1) および NX-OS Release 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させるファブリック内の各スイッチで、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の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に設定されている場合だけです。この設定をディセーブルにすると、関連するすべてのコンフィギュレーションが自動的に廃棄されます。

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、ファブリック内のスイッチ WWN（sWWN）のリストが含まれています。sWWN がファブリックへの参加を試みたとき、その sWWN がリストに含まれていない場合、またはその sWWN が許可リストで指定されたドメイン ID と異なるドメイン ID を使用していた場合には、その VSAN 内でスイッチとファブリック間の ISL が自動的に隔離され、スイッチのファブリックへの参加は拒否されます。

sWWN とともに永続的ドメイン ID を指定できます。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ので、エンド デバイスにより、ファブリック内のすべてのスイッチでドメイン 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。

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では、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。これらの状態は、強制的に上書きすることができます。

（注） データベースをアクティブにすると、現在のアクティブ 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以前にログインを拒否されたすべてのスイッチが、再初期化されます。

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することはできません。

デフォルト設定値

表 10-2 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 10-2　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 11

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 Fibre Channel（FC; ファイバ チャネル）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。

この章の内容は、次のとおりです。

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。

- Galois Counter Mode（GCM; ガロア カウンタ モード）：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。
- Galois Message Authentication Code（GMAC; ガロア メッセージ認証コード）：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。
- Security Association（SA; セキュリティ アソシエーション）：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。デフォルト値はゼロです。
- 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。デフォルト値はゼロです。
- Security Parameters Index（SPI; セキュリティ パラメータ インデックス）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 ～ 4,294,967,295 です。

AES 暗号化のサポート

Advanced Encryption Standard（AES; 高度暗号化規格）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、Encapsulating Security Protocol（ESP）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。

ここで説明する内容は、次のとおりです。

サポートされているモジュール

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。

- 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）

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設定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 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。

（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

Fabric Manager を使用してキーや 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。

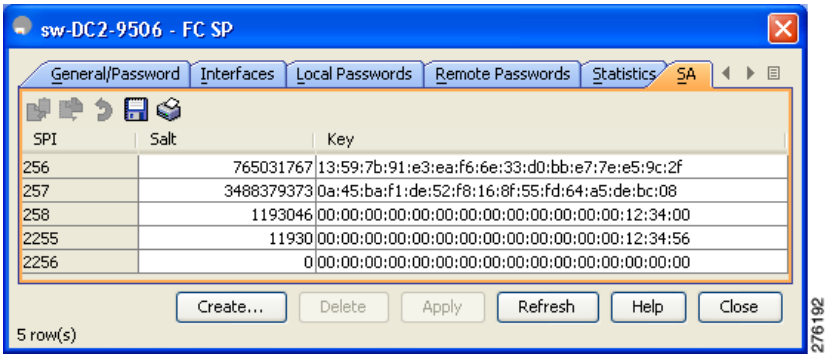
ステップ 1　[Switches] > [Security] を展開し、[FC-SP (DHCHAP)] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[SA] タブをクリックします。

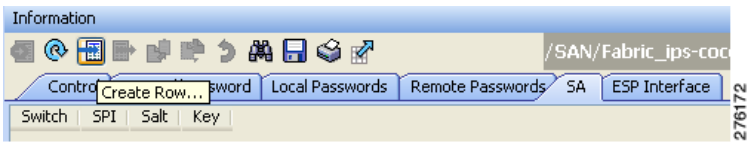
各スイッチの SA パラメータが表示されます（図 11-1 を参照）。

図 11-1　[SA] タブ



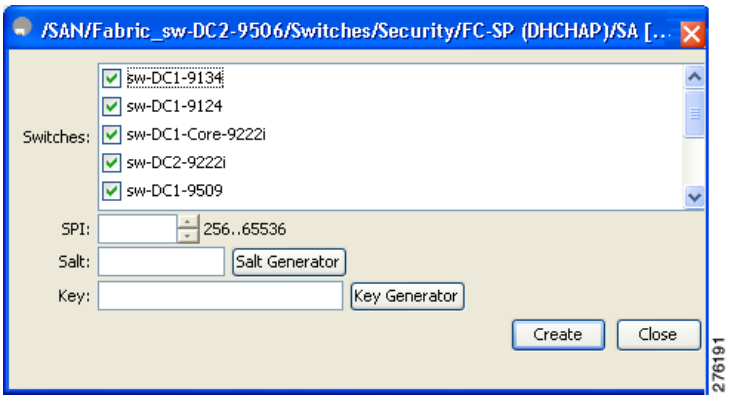
ステップ 3　[Create Row] アイコンをクリックします（図 11-2 を参照）。

図 11-2　[Create Row] アイコン



[Create SA Parameters] ダイアログボックスが表示されます（図 11-3 を参照）。

図 11-3　[Create SA Parameters]



ステップ 4　暗号化を実行するスイッチを選択します。

ステップ 5　SP の値を選択します。有効な範囲は 256 ～ 65536 です。

ステップ 6　salt の値を入力します。または、[Salt Generator] ボタンをクリックして値を選択します。

ステップ 7　キーの値を入力します。または、[Key Generator] ボタンをクリックして値を選択します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

Device Manager を使用してキーや 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。

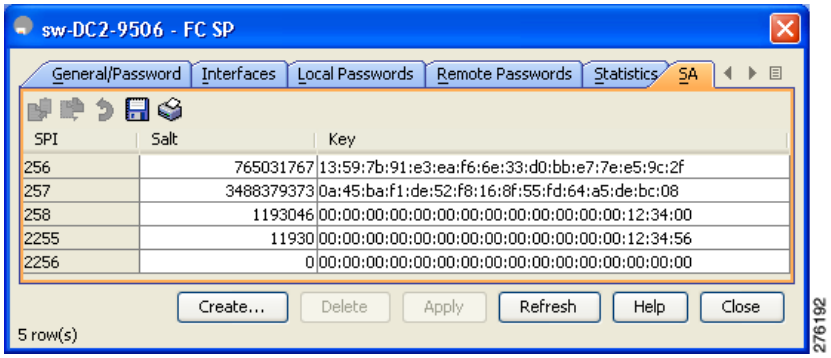
ステップ 1　[Switches] > [Security] を選択し、[FC-SP] を選択します。

[FC-SP] 設定ダイアログボックスが表示されます。

ステップ 2　[SA] タブをクリックします。

各スイッチの SA パラメータが表示されます（図 11-4 を参照）。

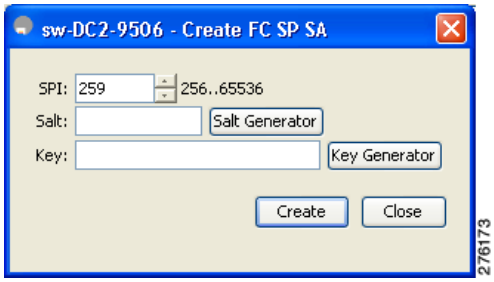
図 11-4　[SA]



ステップ 3　[Create] ボタンをクリックして、新しいパラメータを作成します。

[Create FC-SP SA] ダイアログボックスが表示されます（図 10-2 を参照）。

図 11-5　[Create FC-SP SA]



ステップ 4　SP の値を選択します。有効な範囲は 256 ～ 65536 です。

ステップ 5　salt の値を入力します。または、[Salt Generator] ボタンをクリックして値を選択します。

ステップ 6　キーの値を入力します。または、[Key Generator] ボタンをクリックして値を選択します。

ステップ 7　[Create] ボタンをクリックして変更内容を保存します。

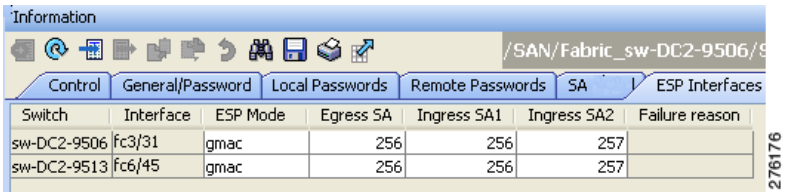
ESP の設定

Fabric Manager を使用して ESP 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 (DHCHAP)] を選択します。
[Information] ペインに、FC-SP の設定が表示されます。

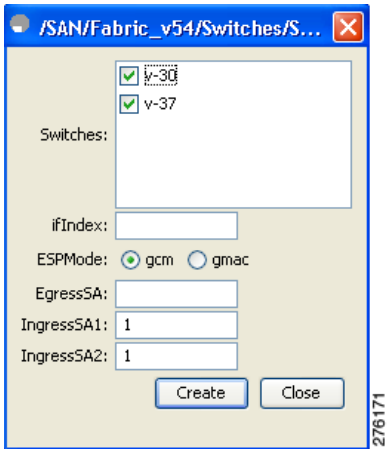
ステップ 2　[ESP Interfaces] タブをクリックします。
各スイッチのインターフェイスの詳細が表示されます（図 10-4 を参照）。

図 11-6　[ESP Interfaces] タブ



ステップ 3　[Create Row] アイコンをクリックします。
[Create ESP Interfaces] ダイアログボックスが表示されます（図 10-2 を参照）。

図 11-7　[Create ESP Interfaces]



ステップ 4　暗号化を実行するスイッチを選択します。

ステップ 5　選択したスイッチのインターフェイスを入力します。

ステップ 6　暗号化用に適切な ESP モードを選択します。

ステップ 7　暗号化用に適切な出力ポートを入力します。

ステップ 8　暗号化用に適切な入力ポートを入力します。

ステップ 9　[Create] ボタンをクリックして変更内容を保存します。

Device Manager を使用して ESP 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。

[FC-SP] 設定ダイアログボックスが表示されます。

ステップ 2　[ESP Interfaces] タブをクリックします。

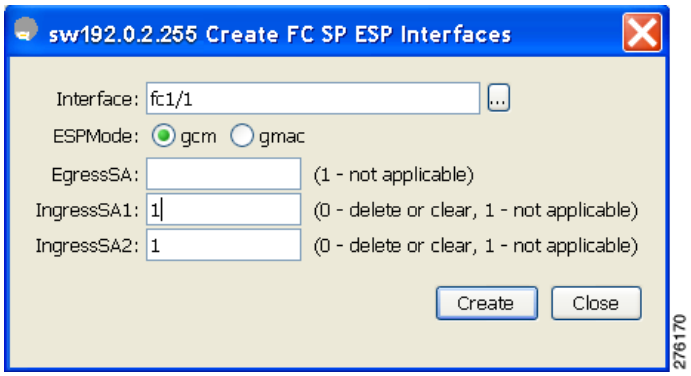
各スイッチのインターフェイスの詳細が表示されます（図 11-8 を参照）。

図 11-8　[ESP Interfaces] タブ

ステップ 3　[Create] ボタンをクリックします。

[Create FC-SP ESP Interfaces] ダイアログボックスが表示されます（図 11-9 を参照）。

図 11-9　[Create ESP Interfaces]



ステップ 4　暗号化用にスイッチのインターフェイスを入力します。または、選択したスイッチに使用できるインターフェイスから値を選択することもできます（図 11-10 を参照）。

図 11-10　使用可能なインターフェイス

ステップ 5　暗号化用に適切な ESP モードを選択します。

ステップ 6　暗号化用に適切な出力ポートを入力します。

ステップ 7　暗号化用に適切な入力ポートを入力します。

ステップ 8　[Create] ボタンをクリックして変更内容を保存します。

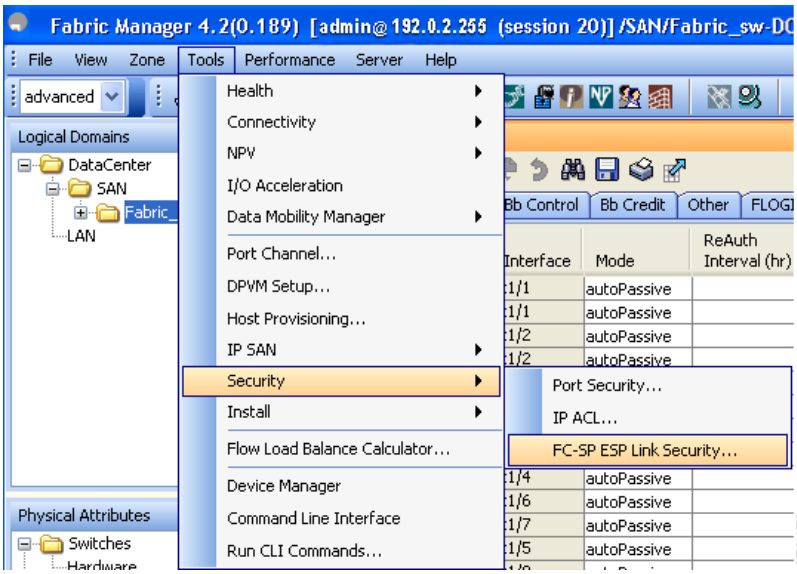
ESP ウィザードを使用した ESP の設定

Fabric Manager を使用して、スイッチ間のリンクレベル暗号化を設定できます。このウィザードを使用して、既存の Inter-Switch Link（ISL; スイッチ間リンク）をセキュアな ISL として設定することも、既存のセキュアな入力 SPI および出力 SPI を編集することもできます。

ESP ウィザードを使用して ESP を設定する手順は、次のとおりです。

ステップ 1　[Tools] > [Security] > [FC-SP ESP Link Security] を右クリックして、Fabric Manager から ESP ウィザードを起動します（図 11-11 を参照）。

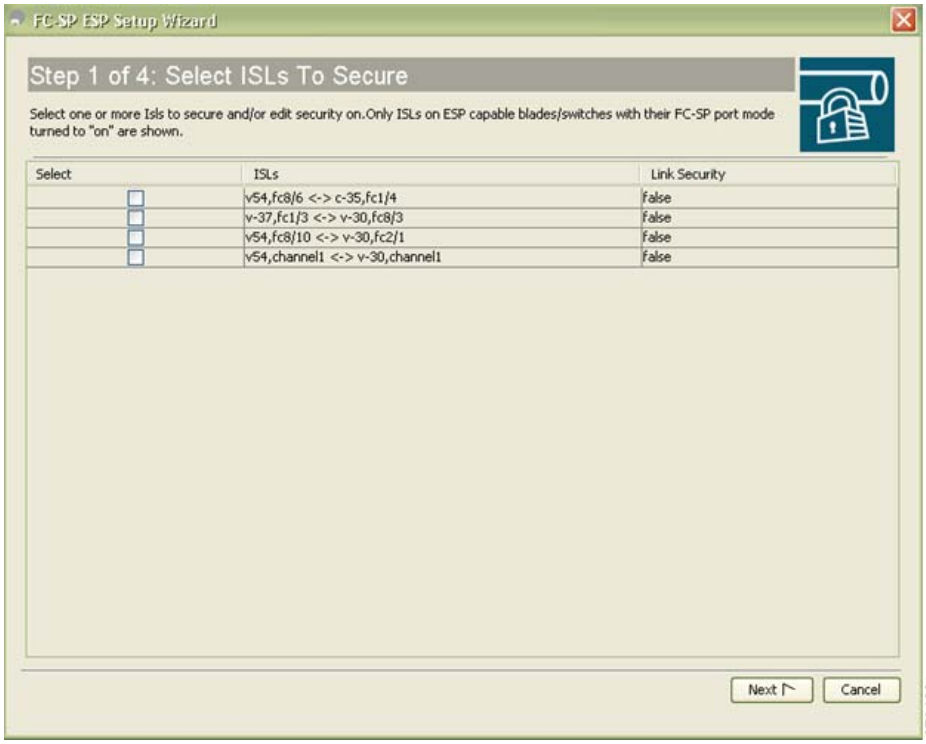
図 11-11　FC-SP ESP ウィザードの起動



ステップ 2　保護する、またはセキュリティを編集する適切な ISL を選択します（図 11-12 を参照）。

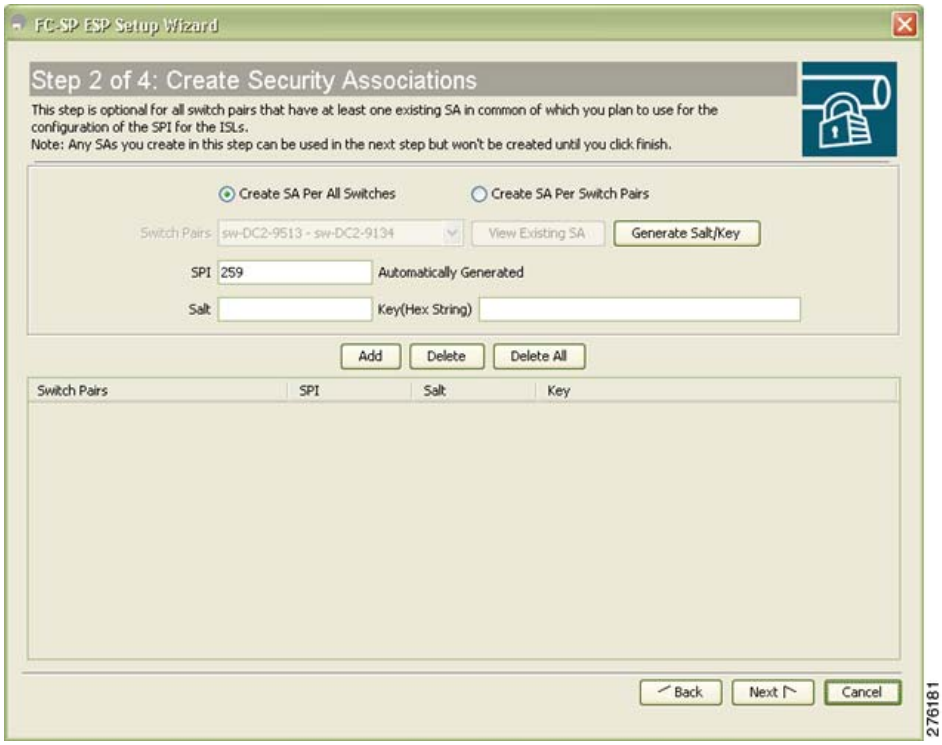
（注）　FC-SP ポート モードが有効で、ESP 対応のスイッチまたはブレードで使用可能な ISL だけが表示されます。

図 11-12　[Select ISL To Secure]



ステップ 3　新しいセキュリティ アソシエーション（SA）を作成します（図 11-13 を参照）。

図 11-13　[Create Security Associations]



スイッチごとに新しい SA を作成することも、既存の SA を使用することもできます。既存の SA を表示するには、[View Existing SA] をクリックします。

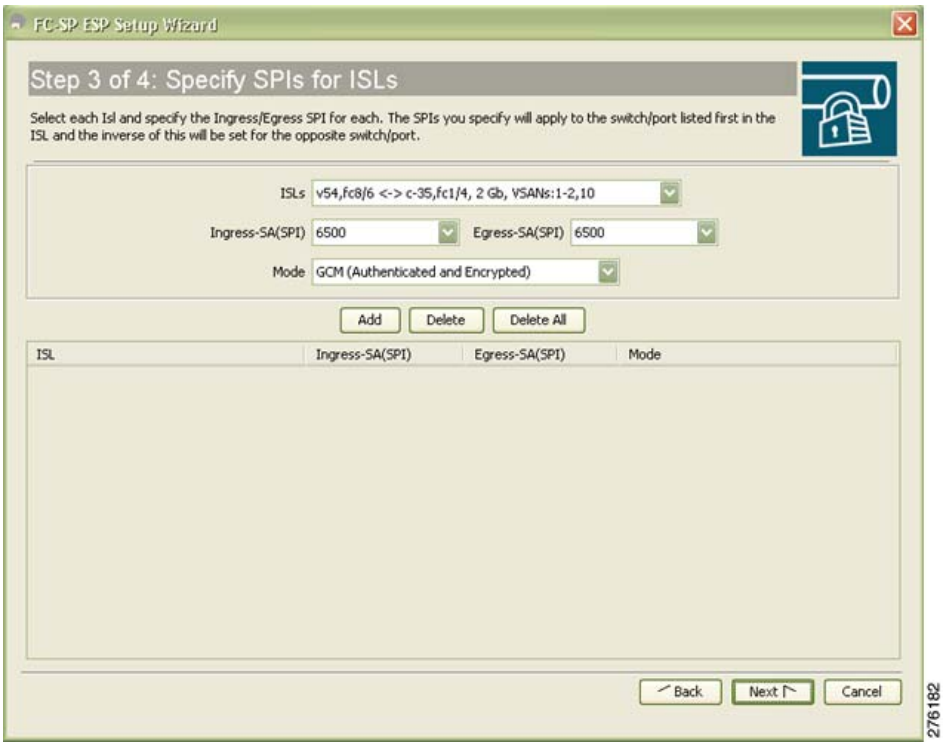
（注）　既存の SA のリストには、1 台のスイッチに対する既存の SA がすべて表示されます。ウィザードは、スイッチのペアに共通の SA が存在する場合だけ稼動します。[Next] ボタンを選択すると、この要件がチェックされ、スイッチのペアに共通の SA が存在しない場合は警告メッセージが表示されます。このウィザードを実行するには、スイッチのペアに共通の SA を作成する必要があります。

ステップ 4　選択した ISL に関する出力ポート、入力ポート、および ESP モードを指定します（図 11-14 を参照）。

セキュリティで保護された ISL の場合、スイッチのペアに共通する SA の SPI が出力ポートと入力ポートに自動入力されます。

この場合、モードはディセーブルになります。セキュリティで保護された ISL のモードは編集できません。

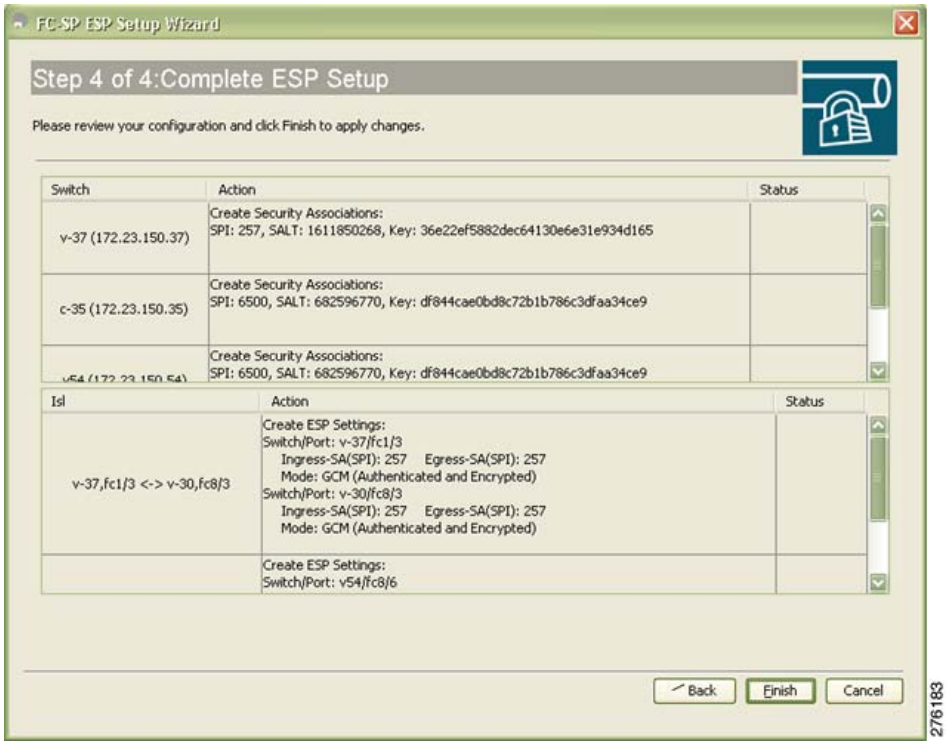
図 11-14　[Specify SPIs for ISLs]



（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。

ステップ 5　設定を確認します（図 11-15 を参照）。

図 11-15　[Complete ESP Setup]



ステップ 6　[Finish] ボタンをクリックして、ESP の設定を開始します。ステータス カラムに設定のステータスが表示されます。

Cisco TrustSec FC リンク暗号化の統計情報の表示

Fabric Manager または Device Manager 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。

ここで説明する内容は、次のとおりです。

- 「Fabric Manager を使用した FC-SP インターフェイス統計情報の表示」（P.11-11）
- 「Device Manager を使用した FC-SP インターフェイス統計情報の表示」（P.11-12）

Fabric Manager を使用した FC-SP インターフェイス統計情報の表示

Fabric Manager を使用して、Encapsulating Security Protocol（ESP）Security Parameter Index（SPI）の不一致や、Interface-Encapsulating Security Protocol 認証エラーの情報を示す統計データを表示できます。

Fabric Manager を使用してインターフェイスの ESP 統計情報を表示する手順は、次のとおりです。

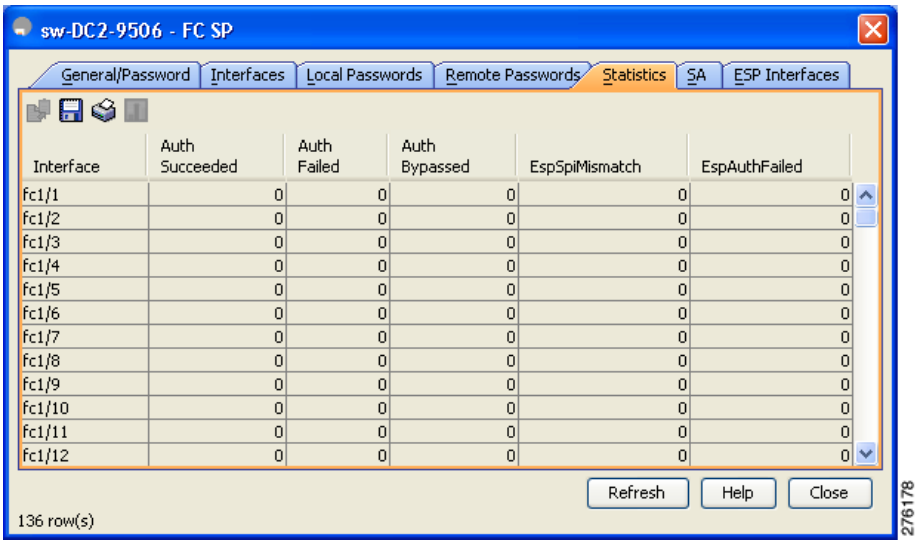
ステップ 1　[Interfaces] > [FC Physical] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[FC-SP] タブをクリックします。

[Information] ペインに FC-SP 統計情報が表示されます（図 11-16 を参照）。

図 11-16　Fabric Manager での FC-SP 統計情報



ステップ 3　[Refresh] ボタンをクリックして、統計データをリフレッシュします。

Device Manager を使用した FC-SP インターフェイス統計情報の表示

Device Manager を使用してインターフェイスの ESP 統計情報を表示する手順は、次のとおりです。

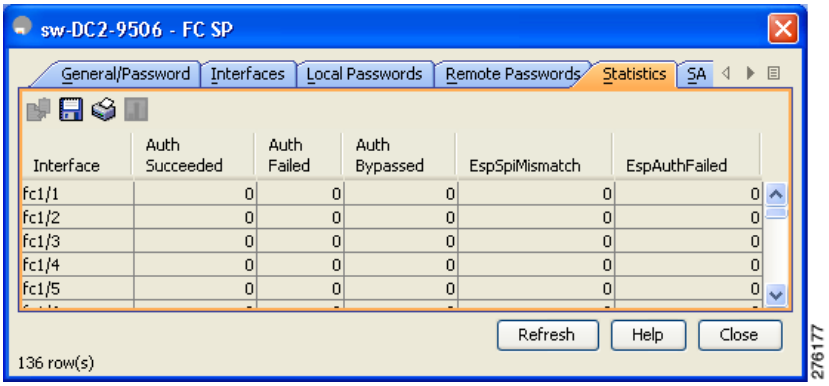
ステップ 1　[Security] > [FC Physical] を展開し、[FC-SP] を選択します。

[Information] ペインに、FC-SP の設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。

[Information] ペインに統計情報が表示されます（図 11-17 を参照）。

図 11-17　Device Manager での FC-SP 統計情報



ステップ 3　[Refresh] ボタンをクリックして、統計データをリフレッシュします。

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。

ここで説明する内容は、次のとおりです。

- 「一般的なベスト プラクティス」（P.11-13）
- 「キーの変更に関するベスト プラクティス」（P.11-13）

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。

INDEX

記号

数字

A

C

D

E

F

I

M

O

P

R

S

T

U

V

W

あ

い

え

か

き

く

こ

さ

し

す

せ

て

と

に

ね

は

ふ

へ

ほ

ま

ゆ

れ

ろ