CHAPTER 1

# セキュリティの概要

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

この章の内容は、次のとおりです。



## FIPS

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

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

# ユーザ ロールおよび共通ロール

ロールベースの許可は、ユーザをロール（役割）に割り当てることによってスイッチ操作へのアクセスを制限します。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+

認証、許可、アカウンティング（AAA）機能は、スイッチを管理するユーザの ID 確認、ユーザへのアクセス権付与、およびユーザ アクションの追跡を実行します。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 RADIUS および TACACS+ の各プロトコルを利用します。このセキュリティ機能は、AAA サーバでの中央集中型のユーザ アカウント管理機能を実現します。

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

このマニュアルの各章では、次の機能について説明します。

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

# LDAP

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 台のアクセス コントロール サーバ（LDAP デーモン）で各サービス認証と認可を個別に提供できます。各サービスを固有のデータベースに接続し、デーモンの機能に応じてそのサーバまたはネットワークで利用できる他のサービスを使用できます。

LDAP クライアント/サーバ プロトコルでは、トランスポート要件を満たすために、TCP（TCP ポート 389）を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

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

# IP ACL

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

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

# PKI

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

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

# IPSec

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

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

# FC-SP および DHCHAP

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

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

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

# ポート セキュリティ

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

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

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

# ファブリック バインディング

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

ファブリック バインディングの設定については、第 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。