



セキュリティの概要

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

この章は、次の項で構成されています。

- [FIPS \(1 ページ\)](#)
- [ユーザ ロールおよび共通ロール \(2 ページ\)](#)
- [RADIUS および TACACS+ \(2 ページ\)](#)
- [IP ACL \(3 ページ\)](#)
- [PKI \(3 ページ\)](#)
- [SSH サービス \(3 ページ\)](#)
- [IPsec \(3 ページ\)](#)
- [FC-SP および DHCHAP \(4 ページ\)](#)
- [ポートセキュリティ \(4 ページ\)](#)
- [Fibre Channel Common Transport 管理サーバクエリー \(4 ページ\)](#)
- [ファブリック バインディング \(5 ページ\)](#)
- [TrustSec ファイバチャネルリンク暗号化 \(5 ページ\)](#)

FIPS

連邦情報処理標準 (FIPS) 発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。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、「[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、「[共通ロール](#)」を参照してください。

RADIUS および TACACS+

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

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

このマニュアルの各章では、次の機能について説明します。

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

RADIUS および TACACS+ の設定については、「[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 ファミリー 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、「[IPv4 および IPv6 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、「[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。

SSH サービス

セキュア シェル (SSH) は、Cisco NX-OS CLI に対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。SSH キーは、次の SSH オプションに使用できます。

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

Cisco MDS NX-OS リリース 8.2(1) 以降、SHA2 フィンガー プリント ハッシュはすべての Cisco MDS デバイスでデフォルトでサポートされています。

SSH サービスの設定の詳細については、次を参照してください。[SSH サービスの設定](#)

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、「[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 ファミリー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 交換を組み合わせで構成されています。

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。

FC-SP および DHCHAP の詳細については、「[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、[ポートセキュリティの概要](#)を参照してください。

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

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

ファブリック バインディングの設定については、[Fibre Channel Common Transport の概要](#)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、[ファブリック バインディングの概要](#)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、[Fibre Channel Common Transport の概要](#)を参照してください。

