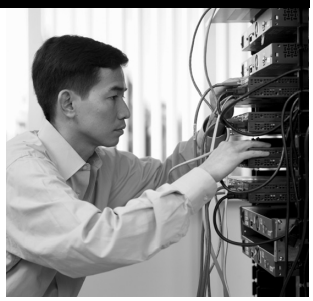
Cisco® MDS Advantage: Cisco MDS 9000 SAN-OS ソフトウェア機能用語集



CISCO SYSTEMS

目次

ストレージ エリア ネットワークのビジネス目標

まえがき

IT 業界のトレンドが静的なリソース管理から「オンデマンド」による動的なリソース管理に移行するにつれて、ネットワークの役割は、応答性に優れたストレージ環境の実現だけでなく、データ ストレージのビジネス目標を達成する上でも重要度を増しています。動的なリソース割り当てとアプリケーションおよびサービスの仮想化という目標を実現するために、ストレージ エリア ネットワーク（SAN）には会社のインフラストラクチャであるアプリケーションおよびコンピューティング環境との緊密な統合だけでなく、インテリジェント性の向上も求められます。

Cisco® MDS Advantage: Cisco MDS 9000 SAN-OS ソフトウェア機能用語集は、シスコシステムズ ® が Cisco MDS 9000 ファミリを通じて現在顧客に提供しているインテリジェント ストレージ ネットワーキング機能を構造的、包括的に観察する視点を提供します。ユーザは Cisco MDS 9000 ファミリを使用することにより、複雑さを軽減し、最適なセキュリティを実現しながら、ビジネスの成長に合わせてネットワークの進展に適合したアプリケーションの最適化を実現できます。

この情報は、エンド ユーザの変化し続けるビジネス目標と検討課題に対応した最新機能を反映するために、随時更新されます。シスコ ストレージ ネットワーキングの製品とソリューションの詳細、およびピアツーピアのユーザ ディスカッション グループと専門家のアドバイスについては、次の URL（英語）を参照してください。

www.cisco.com/go/storagenetworking

はじめに

エンドユーザが何をストレージ エリア ネットワークのビジネス目標としているかをご紹介しましょう。

SAN のビジネス目標

1. SAN 統合
2. ビジネス継続性と災害復旧
3. 高度な SAN セキュリティ
4. 簡素化された SAN 管理
5. インテリジェント ファブリック アプリケーション

SAN のビジネス目標の定義

SAN 統合

SAN 統合とは、SAN インフラストラクチャにアクセスできるデバイス（サーバ、ストレージ アレイ、テープ ドライブなど）を増やす一方で、既存の SAN トポロジ レイアウトを簡素化する取り組みを指します。SAN に接続されるデバイスの数が増えると、ストレージ リソースのコストとプロビジョニングに関する柔軟性が向上し、主にストレージの使用が増加することによって発生するコストの削減と、管理効率の向上が得られます。SAN トポロジ レイアウトの簡素化は、小さな SAN アイランドを接続して大きなファブリックを形成するか、新しいインテリジェント ファブリック仮想化テクノロジーを使用して共通物理ファブリックの上に仮想ファブリックを構築し、物理的な SAN の追加構築を削減してコストを低減することで実現します。

ビジネス継続性と災害復旧

ビジネス継続性と災害復旧とは、どのような障害が発生した場合でも重要ビジネスの中断やデータ損失が発生することがないように、組織が導入するプロセスや手続きのことを指します。今日では、地理的に分散した場所に正しいフェールオーバー メカニズムを配備することはビジネスにとって不可欠です。こうすることで、1 つの場所で障害が発生した場合でも、中断することなくデータ アクセスを継続できます。

高度な SAN セキュリティ

SAN セキュリティとは、ストレージ ネットワークに保存されたデータの整合性と可用性を保護するプロセスと製品機能のことを指します。包括的な SAN セキュリティ ソリューションは、次の 4 つの部分から構成されます。

1. ロールベースのセキュア管理。集中管理によって認証、許可、およびすべての変更のロギングを行います。
2. ネットワークに接続されたデバイスに対する集中管理による認証。これにより、許可されたデバイスだけがネットワークに接続されます。
3. トラフィックの分離とアクセス コントロール。これにより、ネットワークに接続されたデバイスはデータを安全に送受信でき、ネットワーク内の他のデバイスの活動から保護されます。
4. ビジネス継続性、リモート保管、およびバックアップのためにストレージ ネットワークの外部に送られるすべてのデータに対する暗号化。

簡素化された SAN 管理

SAN 管理とは、ストレージ インフラストラクチャを維持し、同時に可用性、信頼性、回復性、および最適なパフォーマンスを保証するために IT マネージャや管理者が従事する活動を指します。

インテリジェント ファブリック アプリケーション

SAN のフレームワークにおける最新の概念に、情報ライフサイクル管理（ILM）を補完するインテリジェント ファブリック アプリケーションがあります。これは、一定期間のデータが持つ価値、エンド ユーザの要求に対して特定のデータを提供する際に要求される応答性とコスト、データを保持する必要がある期間を考慮する集中管理ストレージ機能を指す包括的な用語です。

インテリジェント ファブリック アプリケーションは、ストレージの階層型アプローチに対応しています。この場合、データは保持要件、アクセス ルール、およびビジネス ポリシーに基づいてストレージに割り当てられます。ストレージ ネットワーキングに対するこのようなアプローチを可能にしているインテリジェント機能は、ストレージ プロビジョニング、データの移行と複製、バックアップと回復、ストレージの使用方法、およびストレージ コストの増大に関して顧客が重視している問題に対して、具体的に対応します。

エンド ユーザの検討課題

企業がこれらの目標を達成するために、SAN 管理者は現在の環境に対する変更を決定する前に、さまざまな検討課題に対処する必要があります。また、目標の達成に役立つベンダーを選択する際に、これらの検討課題に対処するための重要な質問に対して現実的な回答を得る必要があります。

SAN 統合に関するエンド ユーザの検討課題は次のとおりです。

- **パフォーマンスとスケーラビリティ**
  - ビジネス ニーズに合わせてソリューションを拡張できるか。このソリューションを選択すると、投資はどのように保護されるか。
  - 新しいインフラストラクチャには、複数のアプリケーションをサポートする能力があるか。
- **移行**
  - ネットワークで実行中のアプリケーションは、移行によって影響を受けるか。
  - 移行の複雑さにどのように対応するか。
- **可用性**
  - 1 つのアプリケーションがダウンした場合に、残りのアプリケーションは影響を受けるか。
- **セキュリティ**
  - 複数のアプリケーションが同一の物理ファブリックに存在する。各アプリケーションを他のアプリケーションからどのように保護するか。
  - 複数の管理者が同一の物理ファブリックで管理を担当している。管理者の分担範囲を安全に分けるにはどのようにしたらよいか。
  - この統合されたソリューションは、準拠と規制の点でどのように役立つか。

- **管理性**
  - 複数のアプリケーションの管理とトラブルシューティングをどのように行うか。
- **総所有コスト（TCO）**
  - SAN 統合によってコスト（運用費用 [OpEx] と設備投資 [CapEx]）を削減できるか。

ビジネス継続性と災害復旧に関するエンド ユーザの検討課題は次のとおりです。

- **パフォーマンス**
  - WAN を使ってデータセンターにアクセスする場合のアプリケーションのパフォーマンスはどの程度か。
- **長距離**
  - どの程度の距離までアクセスできるか。
  - 既存のアプリケーションに対して、距離はどのような影響を与えるか。
- **2 か所に分散しているデータセンターの管理**
  - リモート データセンターをどのように管理するか。
  - WAN またはメトロポリタンエリア ネットワーク（MAN）を使ってデータを移動する場合に、どのような方法でサービス レベル契約（SLA）を満たすか。
- **設計と展開の複雑さ**
  - ビジネス継続性と災害復旧にはどのようなアプリケーションがあるか。
  - どのように着手するか。
- **ソリューションのコスト**
  - WAN パイプの月間使用料（MRC）を最少限に抑えるにはどうすればよいか。
  - SAN アイランドごとにビジネス継続性と災害復旧のネットワークを展開するか。
- **可用性**
  - 1 つのアプリケーションのダウンが他のアプリケーションに影響する場合がある。この影響をどのように回避するか。
  - WAN リンクがダウンした場合に何が起きるか。
  - 障害のポイントは何か。
  - ソリューションは将来の要件に対応できるか。
- **セキュリティ**
  - ビジネス継続性と災害復旧のアプリケーションが抱えるセキュリティ上の潜在的な弱点は何か。
  - データの整合性とプライバシーをどのように保持するか。

SAN セキュリティに関するエンド ユーザの検討課題は次のとおりです。

- コンプライアンス
  - 製品は、各種の規制や基準を満たしているか。
- 管理アクセス
  - アクセス許可のないユーザがネットワークの特定領域にアクセスできるか。
  - アクセス許可を持つユーザがネットワーク内で 1 つの機能を実行したときに、間違いによってネットワークの別の部分をダウンさせることがあり得るか。
  - ネットワーク内で実行されたすべての処理の追跡と表示を 1 か所で集中して行えるか。
  - SAN に保存されたデータを悪意のある攻撃からどのように保護するか。
- デバイスの許可と認証（トラフィックの切り離し）
  - ホストが別のホストのデータにアクセスすることを回避するにはどうすればよいか。
  - ホストまたはターゲットの誤動作が SAN 全体に影響することを回避するにはどうすればよいか。
  - 認定されたデバイスだけをネットワークに接続させるにはどうすればよいか。
- データの整合性の維持と暗号化
  - 不正ユーザによる機密データの表示と変更を防止するにはどうすればよいか。
  - ファイバ チャネル ネットワークを IP ネットワークに接続した場合に、データの整合性に影響するか。

SAN 管理に関するエンド ユーザの検討課題は次のとおりです。

- SAN の正常性と最適なパフォーマンスの確保
  - 問題の根本原因をどのようにして特定するか。
  - SAN の変更をどのように管理するか。
  - SAN パフォーマンスをどのように監視するか。
  - 問題の発生を未然に防ぐにはどうすればよいか。
  - ダウンタイムを避けながら問題をどのように解決するか。
- プロビジョニング
  - SAN プロビジョニングをどのように簡素化するか。
  - サードパーティのスイッチからの移行時に、SAN 管理ツールをどのように使用するか。
- 管理ツールの正しい組み合わせの選択
  - SAN のどの部分を管理できるか。
  - Cisco MDS スイッチは、既存のツールとどのように統合されるか。
  - SAN の管理コスト（OpEx と CapEx）は何か。

- **集中管理された SAN 管理**
  - 異なるプロトコルを含む複数の SAN をどのようにリモート管理するか。
  - 複数の SAN を 1 か所から集中管理できるか。
  - リソースを最大限に活用するために、SAN をどのように管理するか。
  - 拡張された SAN 環境に対して、SAN をどのように提供するか。

インテリジェント ファブリック アプリケーションに関するエンド ユーザの検討課題は次のとおりです。

- **データ移行**
  - データを別のストレージ アレイに移行するとき、アプリケーションのダウンタイムをゼロにするにはどうすればよいか。
- **データ複製**
  - 異種ディスク間（ゴールドからシルバーへ）でどのように複製するか。
  - 複製する場合、データセンターの距離の限界はどの程度か。
- **SLA に基づく階層型ストレージ**
  - 階層型ストレージ環境を実現するために、さまざまなタイプのアレイをどのようにサポートするか。
  - さまざまなアプリケーションに最適なクラスのストレージをどのように提供するか。
- **適切なバックアップと回復**
  - バックアップと回復を迅速に実行するにはどうすればよいか。
  - バックアップと回復を優れた費用効率で実行するにはどうすればよいか。
  - 最高の信頼性を持つバックアップと回復の方法はどのようなものか。
- **コンプライアンスとデータ保持要件**
  - 規制や基準を満たすために必要なことを確実に実行するにはどうすればよいか。
  - 規制に従ってデータを長期間保持する必要があるが、このデータをストレージの別の階層にどのように移動するか。
- **ストレージにかかるコストを低減する必要性**
  - 現在使用中のストレージを表示できるか。
  - リソースをどのように最適化するか。
  - 管理の簡素化や迅速なプロビジョニングの実現によって OpEx をどのようにして削減できるか。
  - クライアントが使用していないファイルの占有記憶域をどのようにして回収できるか。

シスコのインテリジェント ストレージ ネットワーキング ソリューションは、Business Ready Data Center ソリューションを実現するための必須要素であり、ファイバ チャネル、FCIP、iSCSI、ギガビット イーサネット、光ファイバ ネットワークなどが統合されたインフラストラクチャ上での増大する情報リソースに対するアクセス、管理、および保護の適切な方法を提供します。シスコの MDS（Multilayer Datacenter Switch）SAN スイッチ ファミリは、ストレージ ネットワーキングのコストを低減し、多層構造のインテリジェンスをストレージ ネットワークとして組み立てることで、孤立した SAN アイランドから相互接続された SAN への移行を促進します。これらの多層構造のインテリジェンスによって、エンド ユーザは、ここで取り上げている 5 つの SAN ビジネス目標に対する最適なソリューションを実現することができます。

この後の用語集では、すでに説明したエンド ユーザの検討課題と質問について効果的に対応できる Cisco MDS 9000 ファミリの主要なインテリジェント機能を示します。

Cisco MDS Advantage: Cisco MDS 9000 SAN-OS ソフトウェア機能用語集

用語集におけるキーワードの省略形

定義されている機能と密接に関連するビジネス目標を次の省略形で表しています。

BC/DR Business Continuance/Disaster Recovery（ビジネス継続性と災害復旧）

SC Storage Area Network (SAN) Consolidation（ストレージ エリア ネットワーク統合）

SEC SAN Security（SAN セキュリティ）

MGMT SAN Management（SAN 管理）

IFA Intelligent Fabric Applications（インテリジェント ファブリック アプリケーション

AAA（Authentication, Authorization and Accounting：認証、許可、アカウンティング）

AAA サービスは、ネットワーク アクセスやデバイス アクセスを保護するために使用される標準ベースのプロトコル群であり、セキュリティ アカウンティングを提供します。

認証は、ネットワーク サービスにアクセスするユーザやデバイスの ID を確認する手段を提供します。許可機能は、有効なユーザがアクセスできるリソースやサービス、およびその条件（時間帯など）を決定するポリシーを実装することで、認証サービスに追加されます。アカウンティング機能は、すべてのセッションとネットワーク デバイスのアクセスに使用されるすべての処理のログを追跡、維持管理する機能を提供します。この情報を使用して、トラブルシューティングと監査のためのレポートを生成することができます。アカウンティング ログは、ローカルに保存することも、標準ベースの TACACS+ サービスや RADIUS サービスを実装するリモート AAA サーバに送信することもできます。アカウンティングでは時刻と日付のパラメータが追跡されます。これらは、課金と分析に使用できます。

「RADIUS」、「TACACS+」参照

SEC、MGMT

Advanced Encryption Standard（AES：次世代暗号化標準）

AES は暗号化アルゴリズムです。信頼できない可能性がある WAN 上のデータ セキュリティを確保するために、Cisco® MDS 9000 ファミリ内の AES は、暗号ブロック連鎖（CBC）やカウンタ モードを使って 128 ビットを実装しています。AES は、iSCSI（inflight data packets on Small Computer System Interface over IP）や FCIP（Fibre Channel over IP）にセキュリティを提供するために Cisco MDS 9000 14/2-Port Multiprotocol Services Module（MPSM 14/2）で利用できる 3 つの暗号化アルゴリズム（AES 以外に DES [Digital Encryption Standard] と 3DES [Triple DES]）の 1 つです。

「DES」、「3DES」、「Encryption」、「Hardware Encryption」、「IPSec」参照

BC/DR、SEC

Auto Baseline（自動ベースライン）

自動ベースライン機能は、Cisco Fabric Manager Server におけるパフォーマンス マネージャの機能の 1 つです。スイッチ インターフェイス、デバイス、およびスイッチ パフォーマンスを分析し、1 時間ごとに使用方法のパターンを更新して、過去のパフォーマンス傾向と比較して有意の偏差を特定します。これは、管理者がネットワーク内のトラフィックを正常に保つ上で役立ちます。

「Performance Threshold」参照

MGMT

Auto Learn（自動認識）

すべての Cisco MDS 9000 ファミリ スイッチは、この機能によって接続されたデバイスやスイッチについて自動的に認識することができます。この機能によって、管理者は最初にポート セキュリティを有効にする必要がなく、各ポートを手動設定する手間を省くことができます。

SEC、MGMT

Bridging-Port（B-Port）Interoperability Mode（ブリッジポート [B-Port] 相互運用性モード）

Cisco IP Storage Services（IPS）モジュールの B-Port 機能により、リモート B-Port SAN 拡張アプライアンスは Cisco MDS 9000 ファミリ スイッチと直接通信することができます。これにより、ローカル ブリッジ デバイスが不要になります。このモードは、他の B-Port デバイスのみとネゴシエートできる従来の FCIP（Fibre Channel over IP）SAN 拡張デバイスに対して、下位互換性があります。この機能は、Cisco 7200 シリーズと Cisco 7400 シリーズの FCIP ポートアダプタモジュール（PAM）のユーザにとって価値があります。

BC/DR

Buffer-to-Buffer Credit（バッファ間クレジット）

バッファ間クレジット（BB_credit）機能により、Fibre Channel over SONET/SDH、Dense Wavelength-Division Multiplexing（DWDM）、または Coarse Wavelength-Division Multiplexing（CWDM）を使用するロングホール リンクに対して 1 ポートあたり 255 個の受信バッファを提供することで、ファイバ チャネル リンクを最大限に活用できます。他の SAN ベンダーは、このレベルのバッファ間クレジット機能を提供していません。クレジットの一般的な要件としては、2 Gbps のファイバ チャネル リンクをフル ワイヤレートで 1 km まで延長するために 1 つのクレジットを必要とします。この方法で 255 クレジットを使用した場合、2 Gbps のファイバ チャネル リンクをフル ワイヤレートで 255 km まで延長することができます。

「Extended Buffer-to-Buffer Credit」、「Performance Buffer」参照

BC/DR

Call Home（コール ホーム）

集中管理、最適な可用性、および潜在的な問題への予防的な対処のために、コール ホーム機能は重要なシステム イベントについて電子メールで通知します。さまざまなメッセージ形式が用意されているため、ポケットベル サービス、標準的な電子メール、または XML（Extensible Markup Language）ベースの自動構文解析アプリケーションとの最適な互換性を実現できます。この機能の一般的な用途として、ネットワーク サポート エンジニアの直接呼び出し、ネットワーク オペレーション センターへの電子メール通知、Cisco AutoNotify サービスの利用による Cisco Technical Assistance Center（TAC）向けケースの直接生成などがあります。Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 では、Cisco MDS 9000 ファミリのコール ホーム機能にはメッセージスロットリング（抑止）機能があります。どのようなタイミングでコール ホーム メッセージを受信する必要があるかに応じて、インベントリ メッセージ、ポートの syslog メッセージ、リモート モニタリング（RMON）警告メッセージを送信することができます。

必要であれば、エンド ユーザはシスコ ファブリック サービス機能を使用することにより、ファブリック内の他のすべてのスイッチに対して一貫したコール ホーム設定を保持することもできます。

「Cisco Fabric Services」参照

BC/DR、SC、MGMT

Cisco Fabric Services（シスコ ファブリック サービス）

Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 では、シスコ ファブリック サービスを導入して、埋め込み型管理フレームワークを提供しています。ファブリック内のすべてのスイッチに対して、自動機能によって設定が同期されます。これにより、SAN 管理者の時間が大幅に節約され、SAN の正常性と最適なパフォーマンスが保証されるため、企業の総所有コスト（TCO）を削減することができます。

BC/DR、SC、MGMT

Cisco MDS 9000 SAN-OS Command-Line Interface（CLI：コマンドライン インターフェイス

Cisco MDS 9000 SAN-OS CLI は、広く知られている Cisco IOS® ソフトウェア CLI の構文に準拠したインターフェイスです。Cisco IOS ソフトウェア CLI に習熟したネットワーク管理者とストレージ管理者の場合は、コマンドに類似性があるため、多くの管理機能を持つ Cisco MDS 9000 ファミリの CLI の習得には最少のトレーニングで十分です。Cisco MDS 9000 ファミリの CLI は、企業環境内の管理者にとって最適な機能と使いやすさを備えた効率のよい直接的なインターフェイスです。

MGMT

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

シスコは、Cisco MDS 9000 32 ポート ファイバ チャネル ASM（Advanced Services Module）と Cisco MDS 9000 IP SSM（Storage Services Module）によって、ファブリックでの仮想化を提供しています。Cisco MDS 9000 ファミリに組み込まれている標準ベースの API である FAIS（Fabric Application Interface Standard）API で、仮想化アプリケーションを実行できます。この仮想化されたシスコ スイッチング モジュールは、1 秒あたり 300,000 件以上の I/O を処理し、専用の特定用途向け集積回路（ASIC）により、20 Gbps の帯域幅で配信できます。ASM スイッチング モジュールと SSM スイッチング モジュールは、すべての Cisco MDS 9000 モジュラ シャーシに統合でき、仮想化ソリューションの管理を簡素化します。シスコ スイッチング モジュールは、仮想化アプリケーションに幅広く対応し、エンド ユーザは必要に応じて柔軟にアプリケーション ベンダーを変更できます。

シスコとそのパートナーは、簡潔で集中管理された環境でエンド ユーザがより多くのストレージを使用するための仮想化ソリューションを提供します。このソリューションにより、エンド ユーザはアプリケーション要件に基づいてストレージの適切なクラスを用意することによってストレージを階層化できます。また、移行時に必要な一般的なダウンタイムを排除することにより、リース終了時の条件、ベンダーの変更、メンテナンスなどによるアレイ間のデータ移行の手間が軽減されます。

IFA

CiscoWorks DFM

CiscoWorks DFM（Device Fault Manager）は、300 以上のシスコ製デバイスにリアルタイムの障害分析を提供し、Cisco MDS 9000 ファミリもサポートしています。CiscoWorks DFM は、シスコ ネットワーキング デバイスに対してリアルタイムの障害分析を行います。CiscoWorks DFM は、さまざまなデータ収集と分析の手法を使用して「インテリジェント Cisco トラップ」を生成します。このトラップは、他のマルチデバイスやネットワークにインストールされているマルチベンダー イベント管理システムに転送したり、電子メールやポケットベルに送信したり、DFM アラーム ウィンドウに表示することができます。

MGMT

CiscoWorks Resource Manager Essential（RME）

CiscoWorks RME は、Cisco MDS 9000 マルチレイヤ ディレクタとスイッチをサポートし、ネットワーク管理ソリューション（一般的に IP 環境で使用）を提供する強力な Web ベース アプリケーションのスイートです。CiscoWorks RME ブラウザ インターフェイスでは、ネットワークの動作中に重要な意味を持つ情報に簡単にアクセスでき、時間がかかる管理作業を簡素化できます。CiscoWorks RME の Management Connection 機能は、シスコ製の管理ツール（Cisco Fabric Manager など）やパートナー企業製の管理ツールを Web レベルで統合し、ツールとアプリケーションを簡単な手順で使用して、ネットワークを透過的に集中管理できます。CiscoWorks RME には、次のアプリケーションが含まれます。

- Inventory Manager
  - すべてのハードウェアとソフトウェアのインベントリを追跡します。
- Change Audit
- Device Configuration Manager
- Software Image Manager
- Availability Manager
- Syslog Analyzer
- Cisco Management Connection

MGMT

Compression（圧縮）

圧縮は、特定の符号化方式で情報をより少ないビットや情報単位に符号化する処理です。Cisco MDS 9000 ファミリでは、オプションで圧縮を有効にして FCIP（Fibre Channel over IP）プロトコルの有効なスループットの量を増やすことができます。さまざまな圧縮アルゴリズムを選択して、総合的なスループットや圧縮率を最適化できます。他の環境よりも帯域幅が狭い WAN（T1 の 1.55 Mbps やイーサネットの 10 Mbps）では、圧縮率の最適化の方が重要です。帯域幅が広い WAN（1 ギガビット イーサネット接続など）では、総合的なスループットの最適化の方が重要です。

「Hardware Compression and Decompression」参照

BC/DR、IFA

Continuous Data Protection（CDP）

CDP は、継続バックアップとも呼ばれ、企業のデータに何らかの変更があるたびに、すべてのデータをバックアップするストレージ システムです。つまり、CDP はストレージの完全なスナップショットの電子的なジャーナルを作成します。ストレージのスナップショットがデータが変更されるたびに作成されます。この主な長所は、どの時点にも正確に復元できることです。CDP は、Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.1 で使用できる SSE（Storage Services Enabler）ライセンスの一部です。

BC/DR、IFA

Data Encryption Standard（DES：データ暗号標準）

DES はパケット データの暗号化に使用され、規定の 56 ビット DES CBC（Cipher Block Chaining）を実装します。CBC では、暗号化を開始するための初期ベクトルが必要です。初期ベクトルは、IP セキュリティ（IPSec）パケットで明示的に指定されます。DES は、iSCSI（inflight data packets on Small Computer System Interface over IP）や FCIP（Fibre Channel over IP）にセキュリティを提供するために Cisco MDS 9000 14/2-Port Multiprotocol Services Module で利用できる 3 つの暗号化アルゴリズム（DES 以外に AES [Advanced Encryption Standard] と 3DES [Triple DES]）の 1 つです。

「AES」、「Encryption」、「Hardware Encryption」、「IP Sec」参照

SEC

Diffie-Hellman

この暗号化方式では、送信側と受信側が公開鍵を交換し、この公開鍵から両者が共有の秘密鍵を生成します。両者は異なる乱数を使用して、共通の数字をそれぞれ累乗します。結果が互いに送信されます。受信した数字を最初の累乗計算に使用した同じ乱数で累乗すると、結果が両側で同じになります。（出典：TechWeb）

SEC

Encryption（暗号化）

暗号化は、可逆的なデータ変換で、元の形式（平文）から解読が難しい形式（暗号文）に変換し、機密性、整合性、および場合によっては信用性も保護するメカニズムです。暗号化は、暗号化アルゴリズムと 1 つ以上の暗号化キーを使用します。Cisco MDS 9000 の IP セキュリティ（IPSec）プロトコルでは、暗号化アルゴリズムとして、次世代暗号化標準（AES）、データ暗号標準（DES）、トリプルデータデータ暗号標準（3DES）を使用します。

「AES」、「DES」、「3DES」、「IPSec」、「Hardware Encryption」、「RFC」参照

SEC

End-to-End Connectivity Analysis（エンドツーエンド接続分析）－ Cisco Fabric Manager

Cisco Fabric Manager のエンドツーエンド接続分析は、特定の VSAN（バーチャル SAN）内の Cisco MDS スイッチと末端のデバイス（ホスト バス アダプタ [HBA] とストレージ デバイス）間の相互接続を確認する Cisco FC Ping（Fibre Channel Ping）機能を使用して、SAN 管理とトラブルシューティングを簡素化します。Cisco Fabric Manager は、基本的な接続性のほかに、オプションで次のことを確認できます。

- 指定した値よりもレイテンシが小さい。
- パスが冗長である。
- ゾーンに複数のメンバが含まれる。
- 末端のデバイスが管理可能なスイッチに接続されている(アクティブなインバンド管理パスまたはアウトバンド管理パスがある)。

MGMT

Ethernet PortChannel（イーサネット ポート チャネル）（「Cisco EtherChannel® technology」）

イーサネット ポート チャネルは、高可用性を実現するために、Cisco MDS ギガビット イーサネット ポートとそれに接続しているイーサネット スイッチ間にリンク冗長性を提供します。SAN 可用性では、ギガビット イーサネット ポートで障害が発生したりイーサネット接続が切断されると、代替のポートがアクティブになり、アクティブでなくなったギガビット イーサネット ポートを引き継ぎます。

BC/DR

Extended Buffer-to-Buffer Credit（拡張 BB_credit）

災害復旧ソリューションの範囲を拡張するこの距離拡張機能は、Cisco MDS 9216i マルチレイヤ ファブリック スイッチと Cisco MDS 9000 14/2 ポート マルチプロトコル サービス モジュールのすべてのファイバ チャネル ポートに適用されます。シスコの標準の BB_credit（Buffer-to-Buffer Credit）機能により、Fibre Channel over SONET などを使用した長距離リンクに最大 255 個の受信バッファを設定できますが、2 Gbps の速度で距離が 255 km を超える場合には 255 個の BB_credit でも不十分です。長距離リンクで BB_credit を利用するために、拡張 BB_credit フロー制御メカニズムを Cisco MDS 9216i と Cisco MDS 9000 14/2 ポート マルチプロトコル サービス モジュール（Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 以降が必要）に導入しました。これにより、エンド ユーザは 1 つのファイバ チャネル ポートに最大 3500 の受信 BB_credit を設定できます。他の SAN ベンダーは、このレベルのバッファ間クレジット機能を提供していません。

「Buffer-to-Buffer Credit」参照

BC/DR

Fabric Binding（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は、IBM の FICON ベースの SAN に適しています。ファブリック バインディング設定で認証されたスイッチ間だけで ISL（Inter-Switch Link）を有効にして、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の動作を中断することを防止します。

BC/DR、SC、SEC、MGMT

Fabric Configuration Analysis（ファブリック設定分析）ー Cisco Fabric Manager

Cisco Fabric Manager には、ファブリック設定分析ツールが組み込まれています。ファブリック内のすべての Cisco MDS 9000 スイッチの設定をリファレンス スイッチまたはポリシー ファイルと比較します。管理者は、チェック対象の機能と実行するチェックの種類を事前に定義できます。分析ツールは、チェックしているスイッチでのミスマッチのある値や、欠落している値、または余計な値を管理者に通知します。200 以上の設定のチェックを実行できます。分析後、結果がミスマッチのある設定の詳細と共に表示されます。[resolve] ボタンをクリックすると、ツールを使用して設定の違いを自動的に解消できます。Cisco Fabric Manager は、スイッチがリファレンス スイッチまたはポリシー ファイルと一致するように、自動的に設定します。Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 で提供されるシスコ ファブリック サービスとは異なり、ファブリック設定分析はオンデマンド ベースでさまざまなスイッチの設定間の相違を検出しますが、設定の自動的な同期は実行しません。

「Cisco Fabric Services」参照

MGMT

Fabric Manager

Cisco Fabric Manager は、簡単に使用できる包括的な Java ベースの管理アプリケーションで、すべての Cisco MDS 9000 マルチレイヤ スイッチに埋め込まれて提供されます。統合されたアプローチによってマルチプロトコル ファブリック管理を行い、ストレージ管理者に幅広い管理機能を提供します。具体的には、マルチプロトコル ディスカバリ、ホスト バス アダプタ（HBA）とストレージ ディスカバリ、複数のスイッチ設定、ネットワーク トラフィックのホットスポット分析のためのリアルタイム ネットワーク モニタリング、VSAN（バーチャル SAN）ベースの管理とトラブルシューティングなどです。Cisco Fabric Manager は、スイッチの設定にかかる時間を大幅に短縮し、全体的なファブリックの信頼性を向上させ、設定の不統一を解決するための包括的な診断を提供します。

この用語集で取り上げたツールの大部分は、Cisco Fabric Manager で簡単に管理できます。

「Cisco Fabric Manager Server」参照

BC/DR、SC、SEC、MGMT

Fabric Manager Server

Cisco Fabric Manager Server は、企業内のすべての Cisco Fabric Manager アクティビティのデータベースを集中化し、スケーラブルな SAN 管理を実現します。集中管理する管理者は、高度なパフォーマンス履歴モニタリング、キャパシティ計画、集中管理によるファブリック ディスカバリ、Cisco MDS の継続的な正常性およびイベント モニタリング、トラブルシューティング、複数のファブリックの設定ができ、企業の TCO が大幅に削減されます。

「Cisco Fabric Manager」参照

BC/DR、SC、MGMT

FCID Persistence（FCID パーシスタンス）

FCID パーシスタンスは、ファブリックに接続されたデバイスが SAN ファブリックから切り離された後で再度接続された場合も、一貫した FCID（Fibre Channel Identifier）を維持できる Cisco MDS 9000 独自の機能です。HP-UX や AIX などの一部のオペレーティング システムでは、ストレージ デバイスを FCID に基づいて指定するので、その FCID が変更されるとホストのストレージ設定が無効になり、管理者の作業が必要になってダウンタイムが発生する可能性があるため、この機能は重要です。

SC、SEC

FCIP（Fibre Channel over IP）

この IP ストレージ プロトコル標準は、リモート ファイバ チャネル SAN アイランドをローカル SAN からリモート SAN へ IP インフラストラクチャで転送して、透過的に接続するように設計されています。Cisco MDS 9000 の FCIP の実装は、暗号化と復号化、圧縮化と圧縮解除、長距離でのディスクやテープの操作のパフォーマンスの最適化といった組み込み機能を備えています。FCIP は、外部のゲートウェイ アプライアンスを使用せず、通常は既存の IP WAN を利用して Cisco MDS 9000 プラットフォームに組み込まれるので、TCO の削減に役立ちます。すべての Cisco MDS 9000 の FCIP リンクは、1 Gbps のスループットを完全に維持したまま、最大 20,000 km まで延長できます。

BC/DR、SC、IFA

FCIP Auto-Compression（FCIP 自動圧縮）

FCIP（Fibre Channel over IP）機能のパフォーマンスの最適化とインテリジェントな自動調整のために、Cisco MDS 9000 IP のストレージ設定は、さまざまなネットワーク パフォーマンス変数の動的な変更による自動的な圧縮調整機能を備えています。

「Compression」参照

BC/DR

FCIP Tape Acceleration（FCIP テープ アクセラレーション）

FCIP テープ アクセラレーション機能は、管理者による長距離サービスでのテープの書き込みパフォーマンスを高めることにより、SAN パフォーマンスを向上させます。テープは、ユーザ データをシーケンシャルに保存して読み出すためのストレージ デバイスです。テープ ドライブにアクセスするアプリケーションは、通常は待機中の SCSI（Small Computer System Interface）書き込み操作を 1 つだけ処理します。このコマンドでは、リモートのテープ バックアップ ソリューションのスループットが制限されます。このコマンドがバックアップとアーカイブ パフォーマンスに影響を与えるのは、直前の書き込み I/O が正常に終了したことを示すステータス応答をホストがテープ ドライブから受け取るまで、SCSI の各書き込み操作が完了しないためです。Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 で導入された FCIP テープ アクセラレーション機能は、この問題を解決します。長距離 WAN リンクでのホストからテープへのデータ ストリーミングをより速く実行でき、テープのバックアップおよびアーカイブ操作が向上します。

BC/DR、IFA

FCIP Write Acceleration（FCIP ライト アクセラレーション）

FCIP ライト アクセラレーション機能では、ストレージ トラフィックが WAN 上で FCIP（Fibre Channel over IP）を使用してルーティングされる場合に、管理者によるアプリケーションの書き込みパフォーマンスを大幅に向上できます。FCIP ライト アクセラレーションが有効になると、SCSI（Small Computer System Interface）プロトコル ネゴシエーション中に着信ディスク書き込みコマンドをローカルにバッファリングし、書き込みデータが WAN を経由してリモート SAN まで伝達されるため、WAN のスループットが最大化されます。FCIP ライト アクセラレーションの実質的な効果は、長距離 FCIP データ複製ソリューションにおいて、一定の距離で達成可能なパフォーマンスが倍増すること、逆の見方をすれば、一定の I/O パフォーマンスでの距離が倍増することです。

BC/DR、IFA

Fibre Channel Ping

SAN 管理者がエンドツーエンドのラウンドトリップ接続性をチェックしてノードのファブリック到達可能性を検証できる FC Ping（Fibre Channel Ping）トラブルシューティング機能は、Cisco MDS 9000 だけで提供されます。この高度な機能は、Cisco MDS 9000 ファミリ SAN-OS ソフトウェアに組み込まれており、統合 SAN やビジネス継続性ソリューションにおいて、費用効率が高く簡単な管理と迅速なトラブルシューティングのために欠かせません。Cisco Fabric Manager またはコマンドライン インターフェイス（CLI）で有効になり、アプリケーションの可用性と最適な正常性および SAN パフォーマンスを確保します。

Fibre Channel Ping は、FCID（Fibre Channel Identifier）、宛先ポート ワールドワイド名（WWN）、またはデバイス エイリアス情報を指定して実行します。

BC/DR、SC、MGMT

Fibre Channel Trace（ファイバ チャネル トレースルート）

Cisco MDS 9000 ファミリ独自のファイバ チャネル トレース機能により、2 つのデバイス間のデータ トラフィックが通るファブリックの接続ルートを追跡し、スイッチ間（ホップバイホップ）レイテンシを計算できます。この高度な機能は、Cisco MDS 9000 ファミリ SAN-OS ソフトウェアに組み込まれており、統合 SAN やビジネス継続性ソリューションにおいて、費用効率が高く簡単な管理と迅速なトラブルシューティングのために欠かせません。Cisco Fabric Manager またはコマンドライン インターフェイス（CLI）で動作し、アプリケーションの可用性と最適な正常性および SAN パフォーマンスを確保します。

ファイバ チャネル トレースは、FC_ID、N_port または宛先の NL_port WWN を指定して実行します。FC トレース機能を使用し、TE_port（Trunking E_Port）で転送されている限り、探索フレームは通常どおりにルーティングされます。フレームがファブリック（指定されたポート WWN または FC_ID でエンドノードに接続された F_port または FL_port）の末端に到達すると、フレームは発信人とルートにループバックされ（ソース ID と宛先 ID の入れ替え）、ホップバイホップ レイテンシが報告されます。

BC/DR、SC、MGMT

Fibre Channel Protocol Analysis（ファイバ チャネル プロトコル分析）ー Cisco Fabric Analyzer

Cisco MDS 9000 ファミリのパフォーマンス分析ソリューションは、リアルタイムのフレームデコード レベルで、または Cisco Fabric Manager アプリケーションのキャプチャ ファイルから、ファイバ チャネルのトラフィックを分析する機能も提供します。データキャプチャ フィルタリングでは、不要なフレームを除外してファイル サイズを削減できます。ディスプレイ フィルタにより、付加情報を削除し、対象のファイバ チャネル フレームだけを表示できます。ファイバ チャネル要求と応答に対応する独自の機能により、関連する情報の検索を大幅に簡素化し、問題解決にかかる時間が削減されます。

SC、MGMT

Fibre Channel Congestion Control（FCC）

FCC は、ファイバ チャネル ネットワークの輻輳を軽減する Cisco MDS 9000 独自の機能です。ネットワーク内のノードは、出力ポートで輻輳状態を検出すると、特別なフレームを作成して入力ポートに送信します。これらのフレームは、ファイバ チャネルの宛先 ID とソース ID でルーティングされます。Cisco MDS 9000 スイッチは、この特別なフレームを受信すると、輻輳しているポート宛の入力フレーム フローに対してレートの制限を開始することで、アップストリームのパフォーマンスの問題を軽減します。これは、多くのホスト ポートが少ないストレージ デバイスに接続され、帯域幅のコンテンションが発生しやすい統合 SAN 環境で有効な機能です。

SC、MGMT

Fibre Channel Security Protocol（FC-SP：ファイバ チャネル セキュリティ プロトコル）

ネットワーク セキュリティを目的とする Cisco MDS 9000 プラットフォームの FC-SP 機能は、スイッチ間およびホストとスイッチ間の認証を提供し、企業全体のファブリックに対するセキュリティ上の脅威に対応します。DH-CHAP（Diffie-Hellman Challenge Handshake Authentication Protocol）は、Cisco MDS 9000 ファミリ スイッチと他のデバイス間の認証を提供するために実装された FC-SP プロトコルです。CHAP プロトコルと Diffie-Hellman 鍵交換が組み合わされています。

「Diffie-Hellman」参照

BC/DR、SEC

Hardware Compression and Decompression（ハードウェアの圧縮と圧縮解除）

災害復旧環境での FCIP（Fibre Channel over IP）ベースのリモート テープ バックアップとデータ複製のパフォーマンスを向上させるために、FCIP ハードウェア圧縮と圧縮解除は、専用の特定用途向け集積回路（ASIC）を使用してデータ パケットの転送に必要な帯域幅を最小化し、データ転送の実効スループットを最適化します。この機能により、データ転送に使用する WAN の帯域幅を効率化でき、ネットワークの TCO を削減できます。

「Compression」参照

BC/DR

Hardware Encryption and Decryption（ハードウェアによる暗号化と復号化）（FCIP と iSCSI プロトコルの IPSec）

ハードウェアによる暗号化は、データ パケットの内容が不正なソースから見られることを防ぐために、専用の特定用途向け集積回路（ASIC）を使用して暗号化と復号化を行います。そのため、公共の IP インフラストラクチャを災害復旧に使用できます。

「AES」、「Encryption」、「IP Sec」参照

BC/DR、SEC

Hardware-Enforced Zoning（ハードウェア強制ゾーン分割）

ハードウェア強制ゾーン分割サービスは、SAN 接続された末端のデバイス（ホスト サーバ、テープ デバイス、ディスクアレイ）によって構成されるグループ内でのアクセス可能性を制御することを目的としており、ファイバ チャネル ポートから送信される各フレームに対してポートごとのハードウェアによって実行されるため、最もセキュアなタイプのゾーン分割です。フレームがスイッチに入ってくると、ソースの宛先 ID がソースの宛先 ID の組み合わせの許可リストと比較され、フレームはワイヤ スピードで許可されます。

ハードウェア強制ゾーン分割（ハード ゾーン分割）は、Cisco MDS 9000 ファミリのゾーン分割のすべての形式に適用され、不正なアクセスを防止します。これとは別にネームサーバ レベルでのゾーン分割の形式もあり、ソフトウェア強制ゾーン分割（ソフト ゾーン分割）と呼ばれます。ソフト ゾーン分割では、デバイスが他のデバイスのスプーフィングを行って不正なアクセスを実行することが考えられます。この種類のゾーン分割はセキュアではありません。

VSAN（バーチャル SAN）とゾーン分割の違いについては、VSAN も参照してください。

SEC

Historical Performance Monitoring（履歴パフォーマンス モニタリング）ー Cisco Fabric Manager

Cisco Fabric Manager Server（FMS）は、ネットワーク全体のパフォーマンスをモニタリングおよび分析します。すべてのホストとストレージ デバイスの接続のスループット、ISL（Inter-Switch Link）、特定のファイバ チャネルのソースと宛先（フロー）を監視できます。日、週、月、年単位のパフォーマンス統計情報の履歴を維持し、パフォーマンスと正常性のトレンド分析やチャージバックなどによって TCO を削減できます。

BC/DR、SC、MGMT

Host-to-Switch Authentication（ホストとスイッチ間の認証）

ファブリック全体のセキュリティのために、Cisco MDS 9000 ファミリのスイッチおよびダイレクタの FC-SP（Fibre Channel Security Protocol）は、ファブリック全体でスイッチ間またはホストとスイッチ間の認証を有効にすることができます。スイッチとホストの認証は、各ファブリック内でローカルまたはリモートで実行されます。ストレージ アイランドが企業全体のファブリックに統合されて移行すると、新しいセキュリティの問題が発生します。多くの SAN ソリューションでは、企業全体のファブリックにおけるストレージ アイランドの物理的な安全性を常に保証することはできません。Cisco MDS 9000 ファミリで提供されるようなホストとスイッチ間の認証といった形式のプロトコル セキュリティが存在しない場合は、このような種類の問題によって ISL（Inter-Switch Link）の切り離しやリンクの中断が発生する可能性があります。

SC、MGMT、SEC

Hotspot Analysis（ホットスポット分析）ー Cisco Fabric Manager

Cisco MDS SAN の全体的なパフォーマンスは、Cisco Fabric Manager 内に表示され、詳細なモニタリングと検査を必要とするポイントがただちに指摘されます。Top 10 Summary は、ホストとストレージ接続のスループットの平均とピークの値、ISL（Inter-Switch Link）、およびフローを 1 つの簡潔なレポートにまとめたリストです。

SC、MGMT

Internet Key Exchange（IKE：インターネット鍵交換）

IKE は、ユーザを認証し、暗号化手段をネゴシエートし、秘密鍵を交換する、セキュリティ結合を確立する手段です。IKE は、IP セキュリティ（IPSec）プロトコルで使用されます。

BC/DR、SEC

Ingress Port Rate Limiting（入力ポート レート制限）

入力ポート レート制限機能は、各ファイバ チャネル ポートの帯域幅を制御します。ポート レート制限は、ファイバ チャネル ポートへの入力トラフィックを制限するので、入力レート制限とも呼ばれます。この機能を使って管理者は、特定のエントリ ポイントよりも他のエントリ ポイントに高い優先順位を指定することにより、そのポイントからネットワークに送られるフレームの数を制限して、トラフィック フローを制限できます。ポート レート制限は、すべてのファイバ チャネル ポートで 1% ～ 100% の範囲です。デフォルトは 100% です。

SC、MGMT

Integrated Multiprotocol（統合マルチプロトコル）

集中化と SAN 統合のために、Cisco MDS 9000 ファミリでは、アプライアンスや管理ソフトウェアを追加することなく、複数のストレージ プロトコル（ファイバ チャネル、Small Computer System Interface over IP [iSCSI]、Fibre Channel over IP [FCIP]、および IBM Fiber Connection [FICON]）を同一プラットフォーム上で同時に実行できます。この機能では、集中管理プラットフォーム上のすべてのプロトコルを集中管理するため、管理と再トレーニングのコストを削減できます。

BC/DR、SC、MGMT

Internet Storage Name Service（iSNS：インターネット ストレージ ネーム サービス）

iSNS は Cisco MDS 9000 ファミリの機能の 1 つで、iSCSI（Small Computer System Interface over IP）プロトコル向けの単純なネーム サービス、検索サービス、および管理サービスです。iSNS が提供する機能は、Fibre Channel Simple Name Service が従来からファイバ チャネルに提供してきた機能に、認証とセキュリティのための拡張機能を加えています。IP ネットワークと比較した場合、iSNS は、IP ベースのストレージ デバイスを除き、ドメイン ネーム サービス（DNS）と同様の機能を提供します。Cisco MDS 9000 ファミリは、iSNS サーバと iSCSI の実装での iSNS クライアントの機能を提供し、管理の簡素化と集中化を実現します。

MGMT

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

柔軟な展開を行うために、IVR では、複数のバーチャル SAN（VSAN）に関わるファイバ チャネル リソースを、他の VSAN の利便性を保ったまま、まとめてゾーンに割り当てることができます。仮想ファブリックをマージすることなく、テープ ライブラリなどの貴重なリソースを VSAN 間で簡単に共有できます。必要な場合は、複数のスイッチを含む 1 つ以上の VSAN を通過するルートを設定して、必要な相互接続を確立することができます。FCIP と連携した IVR によって、ビジネス継続性や災害復旧の効率的なソリューションが提供され、管理者はストレージ リソースを最適化することができます。

注： SAN の異種環境で柔軟性と相互運用性を強化するために、Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.1 の機能に追加された IVR ネットワーク アドレス変換（NAT）では、それまで VSAN 間で必要だった一意のドメイン ID が不要になりました。

「VSAN」参照

BC/DR、SC

IP ACL（IP アクセス コントロール リスト）

ファブリックのセキュリティと管理を拡張するために、IP アクセス コントロール リスト（IP ACL）は、Cisco MDS 9000 ファミリのスイッチに IP ベースの基本的なネットワーク セキュリティを提供します。IP ACL を使用して、イーサネット インターフェイス上でパケットの転送を制御できます。インターフェイスの目的は、スイッチの管理、FCIP（Fibre Channel over IP）、iSCSI（Small Computer System over IP）通信などが考えられます。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。IP フィルタは、ユーザが設定するシーケンシャルなリストで、許可と拒否の状態で構成され、IP フローに適用されます。各 IP パケットは、フィルタに指定された状態と比較されます。フィルタは、パケットと最初に一致するエントリを特定し、一致したパケットだけに通過する許可を与えます。他のすべてのパケットは拒否されます。

BC/DR、SEC

IPSec

IP セキュリティ（IPSec）プロトコルは、iSCSI（Small Computer System Interface over IP）および FCIP（Fibre Channel over IP）のインフライト データを保護するニーズに応えるためのオープン標準のフレームワークであり、参加ピアにデータ機密性、データ整合性、およびデータ認証を提供します。IPSec は IETF によって開発されています。IPSec は、2 つのホスト間、2 つのセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するなど、IP レイヤでセキュリティ サービスと暗号化（次世代暗号化標準 [AES]、データ暗号化標準 [DES]、およびトリプル DES [3DES]）サービスを提供します。Cisco MDS 9000 IPSec 全体の実装は、RFC 2401 の最新バージョンに基づいています。Cisco MDS 9000 SAN-OS IPSec は RFC 2402 ～ 2410 を実装しています。

セキュア ソケット レイヤ（SSL）はレイヤ 4 でサービスを提供し、2 つのアプリケーションを保護しますが、IPSec はレイヤ 3 で動作し、ネットワーク内のすべての要素を保護します。AES、DES、および 3DES は、IPSec プロトコル向けに Cisco MDS 9000 で使用される 3 つの暗号化アルゴリズムです。

「AES」、「DES」、「3DES」、「Encryption」、「Hardware Encryption and Decryption」、「RFC」参照

BC/DR、SC、SEC

LAN-Free Backup（LAN フリー バックアップ）

SAN インフラストラクチャは LAN インフラストラクチャから完全に切り離されているため、管理者は Cisco MDS 9000 ファミリの LAN フリー バックアップ機能を使用することにより、SAN を使ってデータをディスク ストレージからテープ ライブラリにバックアップできます。これにより、テープのバックアップと復元に伴って LAN で発生していたホスト サーバ、ディスクアレイ、テープ ライブラリ間のデータ トラフィックによる過負荷が解消するため、ホスト サーバ間のアプリケーション通信のパフォーマンスに影響を与えることなく LAN を引き続き使用できます。

BC/DR、MGMT、IFA

LUN Zoning（LUN ゾーン分割）

論理ユニット番号（LUN）ゾーン分割は、Cisco MDS 9000 ファミリ独自のセキュリティ拡張機能であり、ファブリック内のトラフィック切り離しのために、ファイバ チャネル ターゲットだけでなく、ファイバ チャネル ターゲットの個々の LUN に対するアクセスまでも制限することで、詳細なゾーン分割を行います。

「Hardware-Enforced Zoning」、「VSAN」参照

BC/DR、SEC

Network-Accelerated Serverless Backup（ネットワーク高速化サーバレス バックアップ）

Cisco MDS 9000 スイッチのネットワーク高速化サーバレス バックアップ機能では、サーバフリー バックアップのデータ移動で使用される高価なメディア サーバが不要になるため、総所有コスト（TCO）が大幅に削減されます。この機能では、SCSI-3（Small Computer System Interface 3）の拡張コピー コマンド（XCOPY）を利用して、ディスク アレイとテープ デバイス間でデータの読み取りと書き込みを直接行います。この機能は、市場で一般的なバックアップ アプリケーションの既存のモジュールを利用して、バックアップ プロセス全体を調整することもできます。

この方法によるバックアップでは、追加のメディア サーバが不要になるので運用コスト全体が削減され、トラフィック調整のためのメディア サーバとのトラフィックのやり取りが不要になるのでバックアップのパフォーマンス全体が向上します。

BC/DR、MGMT、IFA

Performance Buffer（パフォーマンス バッファ）

パフォーマンス バッファは、SAN 拡張のパフォーマンス向上に対する要求に応えるために、Cisco MDS 9000 ファミリ内に事前に設定される追加のバッファ間クレジットです。145 個のパフォーマンス バッファが Cisco MDS 9000 16-Port Fibre Channel Switching Module の各ポートに追加されます。管理者は、必要に応じて（たとえば、数千キロを超える超長距離を Fibre Channel over IP [FCIP] インターフェイスを使ってフレーム転送する場合など）、このパフォーマンス バッファを内部バッファ割り当てよりも優先的に手動で使用できます。他の SAN ベンダーは、この機能を提供していません。

「Buffer-to-Buffer Credit」、「Extended Buffer-to-Buffer Credit」参照

BC/DR

Performance Threshold（パフォーマンスしきい値）－ Cisco Fabric Manager

Cisco MDS 9000 Fabric Manager Server（FMS）内で、Cisco FMS が監視する各スループットの統計に対して、イベントのしきい値を 2 つまで設定できます。しきい値には、ユーザが指定するレベルまたはパフォーマンス履歴から自動的に計算されたベースライン値を設定できます。しきい値の設定により、トラフィックが通常の負荷を超えた場合に管理者に警告することができます。

「Auto Baseline」参照

MGMT

Port Analyzer Adapter（PAA：ポート アナライザ アダプタ）

Cisco MDS 9000 ポート アナライザ アダプタ（PAA）は小型のハードウェア製品で、ネットワーク内の任意の場所のファイバ チャネル トラフィックをいつでも低コストで効果的に分析することができます。このデバイスは、ファイバ チャネルとイーサネット間のスタンドアロンのコンバータであり、単純で透過的なプロトコル デコードとファブリック内のファイバ チャネル トラフィックの分析を行います。具体的には、ネットワークを切断することなくファイバ チャネル レイヤの FC-2、FC-3、FC-4 をプロトコル レベルで検査できます。Cisco MDS 9000 PAA は、ファイバ チャネルのすべてのフレーム サイズをサポートします。また、Extended Inter-Switch Link（EISL）ヘッダーをカプセル化して分析の対象に含めることができます。

Cisco MDS 9000 PAA は、外部ソフトウェアなしで動作する独立したハードウェア デバイスで、ファイバ チャネルと IBM Fiber Connection（FICON）の両方をサポートします。

PAA は Cisco Fabric Manager と組み合わせることにより、ネットワークのパフォーマンスを正確に監視するための強力なツールになります。拡張された PAA は、ファイバ チャネルのフレームがイーサネットにカプセル化されるときに切り捨てられるフレームの元のサイズを記録できます。これにより、Cisco Fabric Manager は、すべてのフレームを転送せずにパフォーマンス データを計算することができます。

BC/DR、SC、MGMT

PortChannel

Cisco MDS 9000 ファミリに組み込まれている PortChannel 機能では、最大 16 個までの FCIP（Fibre Channel over IP）または Fibre Channel ISL（Inter-Switch Link）を 1 つの論理 PortChannel に集約して、高可用性と最適な SAN パフォーマンスを引き出すことができます。1 つの PortChannel に集約されると、SAN ファブリックはそのリンクを 1 つの論理 ISL として処理します。これまでは、個々の ISL に障害が発生した場合でも、ルーティング プロトコルの FSPF（Fabric Shortest Path First）が新しいパスを再計算するため、障害がファブリック全体に及んでいましたが、PortChannel 機能によってこれが防止されます。そのため、1 つの ISL が停止した場合の影響は、集約された総帯域幅の減少だけです。失敗した ISL が再設定されると、自動的に PortChannel に再結合されるため、PortChannel は元の完全な帯域幅に復元されます。個々のリンクに問題があっても、PortChannel によってアプリケーションのダウンタイムを防止できるため、総所有コスト（TCO）が削減されます。

注： 各ベンダーが用語を独自に作成しているため、一部で混乱があります。たとえば、シスコで「PortChannel」と呼んでいるものは、一般的には「ISL トランキング」と呼ばれます。次の表で、独自に作成された各ベンダーの呼び名を理解し、互いの呼び名を比較できます。

「VSAN Trunking」参照

BC/DR、SC

ファイバ チャネル スイッチ ベンダー間の用語の相違

シスコ社の用語	Brocade 社の用語	McData 社の用語
PortChannel 複数の物理インターフェイスを 1 つの論理インターフェイスに集約して、帯域幅、負荷分散、リンク冗長性を高いレベルで集約します。 シャーシ内部の任意のモジュールの任意のファイバ チャネル ポートから、最大 16 個の ISL と 32 Gbps のスループットを 1 つの PortChannel に集約できます。	**Inter-Switch Link（ISL）Trunking（スイッチ間リンク [ISL] トランキング）** 複数の物理インターフェイスを 1 つの論理インターフェイスに集約して、帯域幅、負荷分散、リンク冗長性を高いレベルで集約します。 集約は、1 つのクワッド（最大 4 つの連続したインターフェイスで構成されるグループ）内で行う必要があります。	**Open Trunking（オープン トランキング）** ファブリック環境内の ISL 間に、自動的で動的な統計情報に基づいたトラフィックの負荷分散を提供します。 不正なフレームが配信される可能性があります。 リンクを 1 つの論理リンクに集約する機能はありません。
VSAN Trunking（VSAN トランキング） VSAN トランキングでは、相互接続（Trunking Expansion）ポートが同一の物理リンクを使用して、複数のバーチャル SAN（VSAN）でフレームを送受信することができます。	同等の機能はありません。	同等の機能はありません。
Hardware Zoning（ハードウェア ゾーン分割）（別名「Hardware-Enforced Zoning」） 特定用途向け集積回路（ASIC）ベースのハードウェアを使用して、ファイバ チャネル フレーム内の FCID（Fibre Channel Identifier）と照合するゾーン分割です。 最も安全な形式のゾーン分割です。ASIC レベルでゾーン分割が行われます。	**Port Based Zoning（ポートベースのゾーン分割）（別名「Hard Port Zoning」）** 物理スイッチ ドメインとポート ペアを経由したアクセスを禁止または許可するためのゾーン分割。 ポート レベルのゾーン分割です。	**SANtegrity Zoning（SANtegrity ゾーン分割）（別名「Hardware Enforced Zoning」）** 指定され、設定されたゾーン以外のデバイスに着信ポートがアクセスするのを防ぐためのゾーン分割。 ポート レベルのゾーン分割です。

Port Security（ポート セキュリティ）

一般的な SAN ソリューションでは、任意のファイバ チャネル デバイスが任意の SAN スイッチポートに接続し、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、セキュリティを細かく調整するために、Cisco MDS 9000 ファミリでスイッチポートへの不正アクセスを禁止します。ポート セキュリティ機能の場合、ファイバ チャネル デバイスのポート ワールドワイド名（pWWN）またはノード ワールドワイド名（nWWN）を使用して、ファブリックへの接続が許可されたノード ポート（Nx ポート）を指定します。複数のスイッチを接続する ISL（Inter-Switch Link）の場合は、スイッチ固有の名前（swwn）を使用して、接続が許可されたポートを指定します。各 N_Port と E_Port を設定して、1 つのポートまたはポートの範囲を制限できます。これにより、ポート レベルで不正なアクセスを防ぐことができます。

SEC

Port Tracking（ポート トラッキング）

Cisco MDS 9000 ファミリ独自のこの機能は、ビジネス継続性と災害復旧のソリューションでのアプリケーションの可用性を向上させ、（ホスト サーバとストレージ アレイなど）2 つの終端装置間を接続するファイバ チャネル リンクで間接的な障害が発生した場合に、アプリケーションのダウンタイムを低減します。ポート トラッキング機能を有効にすると、実際に失敗したリンクに対して指定された従属リンクを停止して、ただちに別の冗長リンクにトラフィックを強制的に移動します。

BC/DR

Quality of Service（サービス品質）

サービス品質（QoS）機能により、SAN 管理者は、アプリケーションごとに優先順位を付けてファイバ チャネルのトラフィックに事前に対処して、ファブリック内のアプリケーションに生じる遅延を制御できるだけでなく、アプリケーション トラフィックの相対的な帯域幅も保証することができます。これは特に、アプリケーション トラフィックがデータセンターから WAN に向かう場合に、最適なパフォーマンスを保証するために役立ちます。サービス品質は、（特定の始点から特定の終点への）フローによって強制的に使用されるか、ゾーン分割パラメータに設定された優先順位に基づいて使用できます（「Zone-Based QoS」とも呼ぶ）。また、バーチャル SAN（VSAN）ベースでも使用できます。

BC/DR、MGMT、IFA

RADIUS

Cisco MDS 9000 ファミリ スイッチは、RADIUS プロトコルを使って認証、許可、アカウンティング（AAA）のリモート サーバと通信することができます。RADIUS は、認証サーバ（AAA サーバ）の業界標準プロトコルです。RADIUS では、認証にチャレンジ&レスポンス方式を使用します。RADIUS は、ルータ、モデム サーバ、スイッチなどの埋め込みネットワーク デバイスに広く使用されています。RADIUS が使用される理由は次のとおりです。

- 通常、スイッチなどのネットワーキング デバイスは、一意の認証情報によって大量のユーザを処理することはできません。多くのネットワーク デバイスは、この処理に必要な大きさのメモリやストレージを持っていないためです。
- RADIUS は、ユーザの集中管理を容易にします。ユーザの集中管理は、多くのネットワーク アプリケーションのユーザ認証にとって重要です。多くのインターネット サービス プロバイダー（ISP）は、数万、数十万、場合によっては数百万のユーザを抱えます。ユーザの追加や削除は 1 日中発生し、ユーザ認証情報は絶えず変化します。このような環境では、ユーザの集中管理は運用上の必須条件です。
- RADIUS は、スニファなどの攻撃者に対抗するために、一定レベルの保護を継続的に提供します。他のリモート認証プロトコルは、断続的な保護、不十分な保護、または存在しないに等しい保護しか提供していません。リモート認証で RADIUS の代わりに使用される主なプロトコルは、TACACS+（シスコが開発し、Cisco MDS 9000 ファミリ内でも使用するセキュリティ プロトコル）と Lightweight Directory Access Protocol（LDAP）です。Cisco MDS 9000 ファミリのユーザは、認証プロトコルに RADIUS か TACACS+ のいずれかを選択できます。LDAP はもともと、スニファなどの攻撃者に対抗するための保護を提供していません。

「TACACS+」参照

SEC

RBAC（Role-Based Access Control：ロールベース アクセス コントロール）

RBAC は、ロールをユーザに割り当て、この割り当てたロールに従ってスイッチ管理機能へのアクセスを制限します（ローカルではスイッチ上で設定し、リモートでは認証、許可、アカウンティング [AAA] サーバを使用します）。

これにより、RBAC は不正な管理アクセスを防ぎます。アクセスは、各ユーザ ID に関連付けられた権限レベルに基づいて割り当てられます。管理者は、各ユーザに完全なアクセスを提供したり、スイッチに関連する特定のコマンドや機能へのアクセスを制限することができます。Cisco MDS 9000 SAN-OS ソフトウェア リリース 1.2(0) では、コマンドライン インターフェイス（CLI）か Cisco Fabric Manager（SNMPv3 を使用）のいずれかを使った一貫性のあるアクセスを提供するために、Cisco MDS 9000 ファミリ内のすべてのスイッチの CLI と SNMP（Simple Network Management Protocol）のロールを同期しています。必要に応じて、各ロールを 1 つ以上のバーチャル SAN（VSAN）に制限することもできます。

「VSAN-Based Role」参照

MGMT、SEC

Read-Only Zone（読み取り専用ゾーン）

Cisco MDS 9000 ファミリ独自の読み取り専用ゾーンは、指定されたグループのホスト サーバにディスク ターゲットやディスク論理ユニット番号（LUN）への読み取り専用アクセス権を付与することで、高度なレベルの SAN セキュリティを提供します。

BC/DR、SC、SEC

Real-Time Performance Monitoring（リアルタイム パフォーマンス モニタリング）ー Cisco Fabric Manager

管理者が常に SAN のパフォーマンスを監視できるように、Cisco MDS 9000 ファミリのパフォーマンス管理ソリューションには、ファイバ チャネル、ギガビット イーサネット、IBM Fiber Connection（FICON）の各ポートとインターフェイスに対するリアルタイムのモニタリングが含まれています。管理者は、クラス別のバイト数とフレーム数、特定のエラーの発生件数、プロトコルに関する各種の統計情報など、Cisco MDS 9000 ファミリの 60 を超える統計情報を表示およびグラフ表示できます。

BC/DR、SC、MGMT

Redundant Crossbar（冗長クロスバー）

Cisco MDS 9000 スイッチ アーキテクチャは、冗長なノン・ブロッキング クロスバーのペアで構成されます。高可用性アーキテクチャに必須のコンポーネントであるクロスバー ファブリックは、システムのスイッチング エンジンです。クロスバーは、システム内のすべてのポート間のスイッチングパスの高速マトリクスを提供します。クロスバー ファブリックは、各スーパーバイザ エンジン モジュールに埋め込まれます。このため、2 つのスーパーバイザ モジュールを持つ冗長システムには、2 つのクロスバー ファブリックが存在します。2 つのクロスバー ファブリックは、負荷共有アクティブ - アクティブ モードで動作します。各クロスバーは、720 Gbps のスイッチング キャパシティを持つので、組み合わせた冗長ペアのスイッチング キャパシティは 1.44 Tbps です。完全実装の Cisco MDS 9500 シリーズ ディレクタを使用すると、スーパーバイザ モジュール（クロスバー ファブリック）の 1 つが取り除かれたり障害が発生しても、システムは停止したりパフォーマンスが低下することがありません。

BC/DR、SC

Remote Switched Port Analyzer（RSPAN：リモート スイッチド ポート アナライザ）

Cisco MDS 9000 のスイッチド ポート アナライザ（SPAN）のトラブルシューティング機能は、リモート SPAN（RSPAN）機能によって拡張され、ファイバ チャネル、FCIP（Fibre Channel over IP）、iSCSI（Small Computer System Interface over IP）ファブリックの 1 つ以上のソース スイッチに分散する SPAN ソースのトラフィックをリモートから監視できます。RSPAN 機能は非干渉的で、SPAN ソース ポートの実稼動トラフィックに影響を与えません。

「SPAN」、「Fibre Channel Trace」参照

BC/DR、SC、MGMT

RFC（Request for Comment：コメント要求）

RFC は、推奨される技術の仕様を記載したドキュメントです。

RFC は、IETF などの標準化組織が使用します。1970 年代に、最初に ARPAnet プロトコルの作成で使用されました。IETF は、2500 以上の RFC を公開しており、すべて www.ietf.org/rfc.html で確認できます。

「IPSec」参照

SEC

Roaming Management Profile（ローミング管理プロファイル）－ Cisco Fabric Manager

標準バージョンの Cisco Fabric Manager は、インストールされているコンピュータのローカルにユーザ プリファレンスとトポロジ マップの更新を保存します。複数のコンピュータをストレージ ネットワークの管理に使用する場合は、管理者は各コンピュータのプリファレンス設定とトポロジ マップをカスタマイズする必要があります。

Cisco Fabric Manager Server ローミング ユーザ プロファイル機能は、プリファレンスとトポロジ マップ レイアウトをサーバに保存するので、管理者が SAN の管理にどのコンピュータを使用してもユーザ インターフェイスは一定です。

MGMT

SAN Extension Tuner（SET：SAN 拡張チューナ）

Cisco MDS 9000 ファミリ独自の機能で、SCSI（Small Computer System Interface）I/O コマンドの読み書きを生成し、SAN ファブリック内の他のスイッチ内に埋め込まれた仮想ターゲットにそのトラフィックを誘導します。これにより、エンド ユーザは FCIP（Fibre Channel over IP）のパフォーマンスを最適化することができます。この方法で、SAN 管理者は事前に SAN 拡張実装のベンチマークをテストしておき、結果を実際のアプリケーションと比較することで、サービスの非効率性や問題を発見できます。

BC/DR、SC、MGMT

SANTap

SANTap は、Cisco MDS 9000 IP SSM（Storage Services Module）で動作するプロトコルで、長距離での複製と継続的なバックアップなどの仮想化サービスに使用されます。

SANTap により、Fibre Channel スイッチは、ホスト サーバとストレージ間の I/O データのコピーをストレージ アプリケーション アプライアンス（Kashya、Alacritus、Topio などのシスコ パートナー製品）にリアルタイムで途切れることなく転送（タッピング）できます。ストレージ アプリケーション アプライアンスは、プライマリ トラフィック パスの外部に存在するので、ストレージ アプライアンスを利用する他の手段とは異なり、ホストやディスクアレイに干渉することはありません。

SANTap には、次のメリットがあります。

- アプライアンス ベースのストレージ アプリケーションの透過的な挿入とプロビジョニング。
- サーバからストレージ アレイへの主要な I/O の中断がない。
- オンデマンドのストレージ サービスを使用できる。
- 一般的なアプライアンス ベースのストレージ アプリケーションを拡張できる。

BC/DR、MGMT、IFA

SCSI Flow Statistics（SCSI フロー統計情報）

この拡張機能は、Cisco MDS 9000 SAN-OS ソフトウェア リリース 2.0 に導入され、すべての発信側とターゲットの組み合わせについて、論理ユニット番号（LUN）レベルの統計情報をリアルタイムで提供します。

MGMT

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

Cisco MDS 9000 ファミリのマルチレイヤ パフォーマンス分析ソリューションは、フレーム レベルでリアルタイムに、または Cisco Fabric Manager GUI で取得されたファイルから、SCSI（Small Computer System Interface）トラフィックを分析します。データ キャプチャ フィルタリングでは、不要なフレームを除外してファイル サイズを削減できます。管理者は、ディスプレイ フィルタで付加情報を削除して、重要なフレームだけを表示できます。SCSI 要求と応答に対応する独自の機能により、関連する情報の検索を大幅に簡素化し、応答時間が削減されます。

SC、MGMT

Secure FTP（SFTP）

SFTP は、通常の FTP セッションを SSH（Secure Shell）プロトコル接続でトンネリングする処理です。Cisco MDS 9000 では、Cisco MDS スイッチとの間でイメージやファイルをアップロードまたはダウンロードするときに推奨される手段です。

「SSH」参照

BC/DR、SC、SEC

Secure Sockets Layer（SSL）

SSL は、暗号プロトコルの 1 つで、インターネット経由での安全な通信を提供します。SSL は、一般的に HTTP（Web）トラフィックの安全な転送に使用されます。

SEC

SNMPv3

簡易ネットワーク管理プロトコル（SNMP）は、TCP/IP ベースのネットワークで広く使用されているネットワーク管理プロトコルです。SNMPv3 は RFC 3411 ～ 3418（STD0062）で定義され、2004 年時点で最新の SNMP の標準バージョンです。以前の 2 つのバージョンにおけるセキュリティ上の問題の多くに対応しています。

基本的に、ネットワーク設定には、2 種類のシステムがあります。エージェントとマネージャです。PC、ワークステーション、サーバ、ブリッジ、ルータなどの管理されるネットワークのすべてのノードには、エージェントモジュールが含まれます。エージェントの役割は次のとおりです。

- ローカル環境の情報の収集と管理
- 要求に対する応答として、または注目する必要がある状況が発生した場合は要求なしで、ローカル環境の情報をマネージャに提供
- ローカルの設定やオペレーティング パラメータを変更するマネージャ コマンドへの応答

設定には、1 つ以上のマネージャ（「管理ステーション」とも呼ばれる）が含まれます。このマネージャは通常ユーザ インターフェイスを提供し、これによってネットワーク管理者はネットワーク管理処理を制御したり観察できます。このインターフェイスにより、ユーザはコマンドの発行（リンクを無効にしたり、パフォーマンス統計情報を収集するなど）、システムが収集した情報の集約やフォーマットなどを実行できます。

SNMPv3 プロトコルは、エージェントから管理情報を取得してコマンドをエージェントに発行するための基本的な機能を提供します。

ネットワーク管理システムの中核は、ネットワーク管理の要件を満たす一連のアプリケーションです。システムには、最少限でもパフォーマンス モニタリング、設定管理、アカウンティングの基本的なアプリケーションが含まれます。すべてのネットワーク管理アプリケーションは、共通のネットワーク管理プロトコルを共有します。このプロトコルは、エージェントから管理情報を取得してコマンドをエージェントに発行するための基本的な機能を提供します。したがって、共通のネットワーク管理プロトコルは TCP/IP サービスを使用できます。

基本的には、SNMPv3 プロトコルは次の 4 つの機能を提供します。

1. GET： エージェントの MIB のアイテムを取得するためにマネージャが使用します。
2. SET： エージェントの MIB の値を設定するためにマネージャが使用します。
3. TRAP： マネージャにアラートを送信するためにエージェントが使用します。
4. INFORM： 他のマネージャにアラートを送信するためにマネージャが使用します。

「SNMP MIB」参照

MGMT、SEC

SNMP MIB

MIB は、監視される特定のデバイス、プロトコル、または一連の情報を記述する簡易ネットワーク管理プロトコル SNMP（Simple Network Management Protocol）構造です。MIB は、デバイスから取得できる情報や取得できるデータ形式を示すテンプレートです。

「SNMPv3」参照

MGMT

SPAN（Switch Port Analyzer）

SPAN は Cisco MDS 9000 ファミリの機能で、SAN のトラブルシューティングの際に FC Trace（Fibre Channel Traceroute）プロトコル レベルのデータを実稼動トラフィックのへの割り込みなしで取得できるため、管理者はダウンタイムを削減できます。

取得可能な SPAN トラフィック ソースには、IP サービスのファイバ チャネル ポート、iSCSI（Small Computer System Interface over IP）、FCIP（Fibre Channel Interface Protocol）仮想インターフェイスがあります。市販のプロトコル アナライザと Cisco MDS 9000 PAA（Port Analyzer Adapter）のどちらも SPAN を使用できます。

「RSPAN」、「FC Trace」参照

SC、MGMT

SSH（Secure Shell Protocol）

SSH は、コンピュータ プログラムでもあり、それに対応するネットワーク セキュリティ プロトコルでもあります。リモート コンピュータにログインしてコマンドを実行するために設計されました。初期の rlogin、Telnet、rsh プロトコルの後を継ぎ、信頼できない 2 つのデバイス間のセキュリティ保護されていないネットワークで、安全で暗号化された通信を提供します。

SEC、MGMT

Switch Health Analysis（スイッチ ヘルス分析）－ Cisco Fabric Manager

Cisco Fabric Manager は、すべての重要なシステム、モジュール、ポート、ファイバ チャネル サービスのステータスを検証できる詳細なスイッチ ヘルス分析機能を提供します。スイッチポートごとに 40 以上の項目がチェックされます。このツールを使用して、Cisco MDS スイッチの正常性をごく短時間で、簡単に、詳細に評価できます。

MGMT

Switch Interoperability Mode（スイッチ相互運用モード）

スイッチ相互運用モードにより、Cisco MDS 9000 ファミリのスイッチはそのままサードパーティのファイバ チャネル スイッチと相互運用できます。第一世代の SAN からの既存のファブリック インフラストラクチャとスムーズに共存したり、最少限の中断で従来のプラットフォームから Cisco MDS 9000 プラットフォームに移行するための重要な機能です。

相互運用には、3 つのモードがあります。1 つのモードは、すべてのベンダーのスイッチに汎用です。2 つのモードは、Brocade Communications の製品ラインの各モデル専用です。

SC、MGMT

Syslog（メッセージ ロギング サーバ）

Syslog は、Cisco MDS 9000 がハードウェアとソフトウェアで発生したすべてのファブリック イベントを追跡するためのロギング機能です。イベントには、接続および切断アクティビティ、動力やファンの停止、設定の変更、環境の変更、予防的あるいは対処的なファブリックの変更があります。Syslog サービスは、イベントの種類、発生した時間、ファブリック内の問題が発生した場所、重要度のレベルなどを通知します。ログは、情報の保存を選択している場合は保存されます。

MGMT

TACACS+

TACACS+ プロトコルは、ユーザにネットワーク アクセスを提供するデバイス（TACACS+ クライアント）とユーザの認証情報を置くデバイス（TACACS+ サーバ）の間の情報交換をセキュアにするために、シスコシステムズが開発したセキュリティ プロトコルです。TACACS+ は、認証、許可、アカウンティング（AAA）モデルに基づきます。

TACACS+ ベースのリモート アクセス環境には、主に 3 つのコンポーネントがあります。

アクセス クライアント、ネットワーク アクセス サーバ、TACACS+ サーバです。

アクセス クライアントは、サービス プロバイダーにダイヤルしてさまざまなインターネット サイトに接続するユーザの場合もあります（従来型のユーザ）。また、アクセス クライアントはデバイスの場合もあります。スモールオフィスやホーム オフィスで複数のユーザにネットワークへのアクセスを提供する ISDN ルータや、ダイヤルオンデマンド ルータが考えられます。

ネットワーク アクセス サーバは、ネットワーク エッジ（主要なシスコ ネットワーク環境）の外部からの接続要求を認識して処理するデバイスです。ネットワーク アクセス サーバは、ユーザの接続要求を受信すると、ポイントツーポイント プロトコル（PPP）かシリアル ライン インターネット プロトコル（SLIP）プロトコルで、ユーザとの最初のアクセス ネゴシエーションを実行します。このネゴシエーションは、特定のデータ（ユーザ名、パスワード、ネットワーク アクセス サーバ ポート番号など）を確定します。次に、ネットワーク アクセス サーバは、このデータを TACACS+ サーバに渡し、認証を要求します。

TACACS+ サーバは、要求を認証し、この接続上でサービスが使用されることを承認します。TACACS+ サーバは、この処理を実行するために、ネットワーク アクセス サーバ要求からのデータが既知の信頼できるデータベースの内容と一致するかどうかを確認します。

SEC、MGMT

Tape Acceleration（テープ アクセラレーション）

FCIP テープ アクセラレーションは、Cisco MDS 9000 ファミリ独自の機能で、長距離でのテープの書き込みパフォーマンスを改善します。データは、テープ デバイスにシリアル形式で長距離から書き込まれ、書き込みの確認も実行されるため、バックアップ パフォーマンスは大きな影響を受けることがあります。FCIP テープ アクセラレーション機能は、FCIP（Fibre Channel over IP）トンネルのソースとターゲットの終端にバッファリングを提供し、データがシリアルでテープ デバイスに書き込まれている間もトラフィックを継続的に宛先に送信できます。

「Write Acceleration」参照

BC/DR、IFA

TCP Buffer（TCP バッファ）

TCP は、IP ネットワーク上で FCIP（Fibre Channel over IP）と iSCSI（Small Computer System Interface over IP）ストレージ トラフィックに信頼性が高い配信とフロー制御を実現します。Cisco MDS 9000 独自の機能として、各 FCIP セッションおよび iSCSI セッションは 2 組の TCP バッファを持ちます。1 組は、長距離で利用可能なネットワーク帯域幅を最適に使用するためのものです（FCIP では最大 32 MB、または 1 Gbps で最大 20,000 km）。もう 1 組は、データを途切れることなく FCIP または iSCSI に送信し、アプリケーション パフォーマンスを最適化します。

「TCP Tuning」参照

BC/DR

TCP Tuning（TCP 調整）

手動で FCIP（Fibre Channel over IP）と iSCSI（Small Computer System Interface over IP）のパフォーマンスを最適化して設定を拡張するために、TCP パラメータを手動で調整して上書きできます。パラメータには、TCP 最大帯域幅、最小帯域幅、推定ラウンドトリップ時間、TCP 輻輳ウィンドウ モニタ バッファ サイズなどがあります。TCP 調整の例として、IP パケットのサイズの調整があります。IP パケットのサイズまたは最大伝送ユニット（MTU）は通常 1500 バイト長ですが、これを 2300 バイトに増やしてファイバ チャネル フレーム（2112 バイト長）の内容全体が 1 つの IP パケットに入るようにし、ファイバ チャネル フレームのセグメント化を不要にすることができます。

「TCP Buffers」参照

BC/DR

Traffic Analyzer（トラフィック アナライザ）

Cisco MDS 9000 ファミリは、ファイバ チャネル トラフィックをリアルタイムで、または取得したファイルから処理できます。Web ブラウザのインターフェイスで、特定のファイバ チャネルの発信元と宛先間のスループット、特定の VSAN（バーチャル SAN）内のすべてのトラフィック、すべての SPAN（Switched Port Analyzer）を簡単に判断できます。ラウンドトリップの応答時間、1 秒あたりの SCSI（Small Computer System Interface）I/O 数、SCSI 読み込みトラフィック対書き込みトラフィックのスループットとフレーム数、SCSI セッション ステータスと管理業務情報を提供します。ファイバ チャネル フレーム サイズと制御トラフィックに関するその他の統計情報も用意されています。このデータのモニタリング能力は、管理者が SAN のパフォーマンスを診断、管理する際に役立ちます。

「SCSI Traffic Analyzer」参照

SC、MGMT

Triple DES（3DES：トリプル DES）

3DES は DES 暗号化を強化した形式で、信頼できないネットワークで機密情報を送信できる 168 ビット暗号化キーを提供します。3DES は、iSCSI（inflight data packets on Small Computer System Interface over IP）や FCIP（Fibre Channel over IP）にセキュリティを提供するために Cisco MDS 9000 14/2-Port Multiprotocol Services Module で利用できる 3 つの暗号化アルゴリズム（3DES 以外に AES [Advanced Encryption Standard] と DES [Data Encryption Standard]）の 1 つです。

「AES」、「Encryption」、「Hardware Encryption」、「IP Sec」参照

SEC

Trunking（トランキング）

「VSAN Trunking」参照

BC/DR、SC、MGMT

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

シスコは、Cisco MDS 9000 32 ポート ファイバ チャネル ASM（Advanced Services Module）と Cisco MDS 9000 IP SSM（Storage Services Module）によって、ファブリックでの仮想化を提供しています。Cisco MDS 9000 ファミリに組み込まれている標準ベースの API である FAIS（Fabric Application Interface Standard）API で、仮想化アプリケーションを実行できます。この仮想化された、シスコ スイッチング モジュールは、1 秒あたり 300,000 件以上の I/O を処理し、専用の特定用途向け集積回路（ASIC）により、20 Gbps の帯域幅で配信できます。ASM スイッチング モジュールと SSM スイッチング モジュールは、すべての Cisco MDS 9000 モジュラ シャーシに統合でき、仮想化ソリューションの管理を簡素化します。シスコ スイッチング モジュールは、仮想化アプリケーションに幅広く対応し、エンド ユーザは必要に応じて柔軟にアプリケーション ベンダーを変更できます。

シスコとそのパートナーは、簡潔で集中管理された環境でエンド ユーザがより多くのストレージを使用するための仮想化ソリューションを提供します。このソリューションにより、エンド ユーザはアプリケーション要件に基づいてストレージの適切なクラスを用意することによってストレージを階層化できます。また、移行時に必要な一般的なダウンタイムを排除することにより、リース終了時の条件、ベンダーの変更、メンテナンスなどによるアレイ間のデータ移行の手間が軽減されます。

IFA

Virtual Router Redundancy Protocol（VRRP：仮想ルータ冗長プロトコル）

VRRP は、高可用性を目的としたゲートキーパーで、外部ルータと IP スイッチから Cisco MDS 9000 IP ストレージ インターフェイスへのトラフィックを管理します。VRRP は、仮想 IP アドレスを外部ルータに提供し、トラフィックをプライマリの Cisco MDS 9000 IP ストレージ インターフェイスに誘導します。プライマリ インターフェイスにアクセスできない場合、VRRP は、管理者が事前に割り当てた定義済みの代替パス ルートを経由して、トラフィックをセカンダリ IP インターフェイスに誘導します。

BC/DR、SC

Virtual SAN（VSAN：バーチャル SAN）

この機能は、複数の SAN を統合物理インフラストラクチャに仮想ファブリック（VSAN）として配備（展開）します。各 VSAN は、それぞれ専用のファブリック サービス、サービス品質（QoS）、セキュリティ、管理機能のセットを持ちます。VSAN は、Cisco MDS 9000 ファミリの一部としてシスコシステムズが独自に提供し、エンドユーザが、費用効率が高く、高い可用性を持ち、セキュアでスケーラブルな SAN 統合およびビジネス継続性ソリューションを構築することを可能にします（例：VSAN により、1 つの物理デバイス内に複数の隔離した SAN アイランドを展開できます。一方、他のソリューションでは、多くの物理デバイス、ISL [Inter-Switch Link]、ファームウェア、複雑な管理が必要です）。シスコの VSAN は、ANSI INCITS T11 技術委員会により、VSAN 構築のための業界標準として認定され、推奨されています。

注： VSAN とゾーン分割では次の点が異なります。

- VSAN は、共通の物理インフラストラクチャの上に、完全に隔離された仮想ファブリックを構築するために必要なテクノロジーです。それに対してゾーン分割は、独立した各仮想ファブリック内で、アクセスを制限するために使用するセキュリティ メカニズムを指します。つまり、VSAN ごとに別々のゾーン分割設定が存在します。
- VSAN ごとにアカウンティングやチャージバックに役立つ統計情報が収集されますが、ゾーンにはこのような機能はありません。
- VSAN の隔離は、デバイスをスイッチに接続する前に適用されますが、ゾーン分割では後に適用されます。

「Inter-VSAN Routing」参照。

BC/DR、SC、SEC、MGMT、IFA

VSAN-Based Role（VSAN ベースのロール）

Cisco MDS 9000 ファミリ独自のロールベース アクセス コントロール（RBAC）には、VSAN（バーチャル SAN）ごとの管理を可能にする細分性があります。これにより、SAN のそれぞれ異なる部分に対して所有権と責任を持つ複数の SAN 管理者に、管理されたシステム的な方法で管理者特権を委任できます。その結果、物理デバイスと論理設定の数が増加するのに合わせて、セキュアでスケーラブルで管理が簡単な SAN を作成できます。

「RBAC（Role-Based Access Control）」参照。

SEC、MGMT

VSAN Trunking（VSAN トランキング）

VSAN トランキングは、トランキングとも呼ばれ、Cisco MDS 9000 ファミリのスイッチ独自の機能です。トランキングにより、複数の VSAN（バーチャル SAN）からのデータ トラフィックが ISL（Inter-Switch Link）を経由できます。トランキングでは、相互接続しているポートのデータ トラフィックは、EISL（Extended ISL）フレーム形式を使用して同じ物理リンクで 1 つ以上の VSAN でフレームを送受信できます。

BC/DR、SC、MGMT

Wizard（ウィザード）

ウィザードは、面倒で間違えやすい管理業務と設定を簡単にする直感的でグラフィカルなポップアップ アプリケーションです。Cisco MDS 9000 ファミリでは、FCIP（Fibre Channel over IP）トンネル、iSCSI（Small Computer System Interface over IP）接続、ポート チャネル、IVR（Inter-VSAN Routing）ゾーン分割、ソフトウェア インストール、ライセンス インストール、サービス品質（QoS）、VSAN（バーチャル SAN）作成、IP アクセス コントロール リスト（ACL）、Ping、トレースルートの設定でウィザードを使用できます。

BC/DR、SC、MGMT

Write-Acceleration（ファイバ チャネル ライト アクセラレーションおよび FCIP ライト アクセラレーション）

FCIP（Fibre Channel over IP）およびファイバ チャネル ライト アクセラレーションは、Cisco MDS 9000 ファミリ独自の技術で、長距離でのディスク書き込みパフォーマンスを改善します。長距離のディスク書き込みコマンドでは、ラウンドトリップ時間（レイテンシ）がソースとターゲットの距離に比例して増加し、距離が長くなると時間も長くかかります。このため、ソースは、次のデータを送信できるようになるまで、書き込みコマンドがターゲットへのコピーを終了するのを待機する時間が発生します。ライト アクセラレーション機能では、書き込みコマンドはローカルで確認応答（スプーフ）され、ディスクへの書き込みが途切れずに長距離の SAN 接続を流れることができます。Cisco MDS 9000 プラットフォームでは、FCIP ライト アクセラレーションは IP ストレージ モジュール（Cisco MDS 9000 4 ポートおよび 8 ポート IP SSM [storage services module]）と Cisco MDS 9000 14/2 ポート マルチプロトコル サービス モジュールで実装されます。ファイバ チャネル ライト アクセラレーションは、SSM で実装されます。

「Tape Acceleration」参照。

BC/DR、IFA

Zone Merge Analysis（ゾーン マージ分析）－ Cisco Fabric Manager

Cisco MDS 9000 のゾーン マージ分析ツールは、Cisco Fabric Manager の [Zone] メニューから使用でき、2 つのスイッチが相互接続された場合にゾーンのマージが成功するかどうかを判断できます。

2 つのゾーンのマージが成功するかどうかを判断するために、ゾーン マージ分析ツールは正確なゾーン メンバ、ゾーン名、VSAN（バーチャル SAN）名、2 つのスイッチ間の拡張ポートの設定が一致するかどうかを調べます。この機能により、統合 SAN と SAN 拡張ソリューションの移行と展開が簡素化されます。

BC/DR、SC、MGMT

Cisco MDS 9000 SAN-OS ソフトウェア機能一覧

快適なパフォーマンスを保証する Cisco® MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーク機能

Auto Baseline（自動ベースライン）

Buffer-to-Buffer Credit（バッファ間クレジット）

Cisco Fabric Services（シスコ ファブリック サービス）

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

Extended Buffer-to-Buffer Credit（拡張 BB_credit）

Fabric Manager

Fabric Manager Server

FCIP（Fibre Channel over IP）

FCIP Auto-Compression（FCIP 自動圧縮）

FCIP Tape Acceleration（FCIP テープ アクセラレーション）

FCIP Write Acceleration（FCIP ライト アクセラレーション）

Fibre Channel Protocol Analysis（ファイバ チャネル プロトコル分析）－ Cisco Fabric Analyzer

Hardware Compression and Decompression（ハードウェアの圧縮と圧縮解除）

Historical Performance Monitoring（履歴パフォーマンス モニタリング）

Hotspot Analysis（ホットスポット分析）

Ingress Port Rate Limiting（入力ポート レート制限）

Internet Storage Name Service（iSNS：インターネット ストレージ ネーム サービス）

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

LAN-Free Backup（LAN フリー バックアップ）

Network-Accelerated Serverless Backup（ネットワーク高速化サーバレス バックアップ）

Performance Buffer（パフォーマンス バッファ）

Performance Threshold（パフォーマンスしきい値）

PortChannels

Quality of Service（サービス品質）

Read-Only Zone（読み取り専用ゾーン）

Real-Time Performance Monitoring（リアルタイム パフォーマンス モニタリング）

Redundant Crossbar（冗長クロスバー）

Remote Switched Port Analyzer（RSPAN：リモート スイッチド ポート アナライザ）

SAN Extension Tuner（SET：SAN 拡張チューナ）

SANTap

SCSI Flow Statistics（SCSI フロー統計情報）

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

SPAN（スパン）

Switch Health Analysis（スイッチ ヘルス分析）

TCP Buffer（TCP バッファ）

TCP Tuning（TCP 調整）

Traffic Analyzer（トラフィック アナライザ）

Virtual Router Redundancy Protocol（VRRP：仮想ルータ冗長プロトコル）

高可用性と柔軟性を持つ SAN を管理する Cisco MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーキング機能

AAA

AES

Buffer-to-Buffer Credit（バッファ間クレジット）

Call Home（コール ホーム）

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

Continuous Data Protection（CDP）

Data Encryption Standard（DES：データ暗号標準）

Triple DES（3DES：トリプル DES）

Encryption（暗号化）

End-to-End Connectivity Analysis（エンドツーエンド接続分析）

Extended Buffer-to-Buffer Credit（拡張 BB_credit）

Fabric Binding（ファブリック バインディング）

Fabric Configuration Analysis（ファブリック設定分析）

Fabric Manager

Fabric Manager Server

FCIP（Fibre Channel over IP）

FCIP Auto-Compression（FCIP 自動圧縮）

FCIP Tape Acceleration（FCIP テープ アクセラレーション）

FCIP Write Acceleration（FCIP ライト アクセラレーション）

Fibre Channel Ping

Fiber Channel Trace（ファイバ チャネル トレースルート）

Fibre Channel Protocol Analysis（ファイバ チャネル プロトコル分析）－ Cisco Fabric Analyzer

Fibre Channel Congestion Control（FCC）

Fibre Channel Security Protocol（FC-SP：ファイバ チャネル セキュリティ プロトコル）

Hardware Compression and Decompression（ハードウェアの圧縮と圧縮解除）

Historical Performance Monitoring（履歴パフォーマンス モニタリング）

Host-to-Switch Authentication（ホストとスイッチ間の認証）

Hotspot Analysis（ホットスポット分析）

Internet Key Exchange（IKE：インターネット鍵交換）

Internet Storage Name Service（iSNS：インターネット ストレージ ネーム サービス）

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

IP ACL（IP アクセス コントロール リスト）

IPSec

LAN-Free Backup（IPSec LAN フリー バックアップ）

Network-Accelerated Serverless Backup（ネットワーク高速化サーバレス バックアップ）

Performance Buffer（パフォーマンス バッファ）

Performance Threshold（パフォーマンスしきい値）

PortChannels

Port Security（ポート セキュリティ）

Port Tracking（ポート トラッキング）

Quality of Service（サービス品質）

RADIUS

RBAC（Role-Based Access Control：ロールベース アクセス コントロール）

Read-Only Zone（読み取り専用ゾーン）

Real-Time Performance Monitoring（リアルタイム パフォーマンス モニタリング）

Redundant Crossbar（冗長クロスバー）

Remote Switched Port Analyzer（RSPAN：リモート スイッチド ポート アナライザ）

SANTap

SCSI Flow Statistics（SCSI フロー統計情報）

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

Secure FTP（SFTP）

Secure Sockets Layer（SSL）

SNMPv3

SPAN（スパン）

SSH

Switch Health Analysis（スイッチ ヘルス分析）

Syslog（メッセージ ロギング サーバ）

TACACS+

Traffic Analyzer（トラフィック アナライザ）

Virtual Router Redundancy Protocol（VRRP：仮想ルータ冗長プロトコル）

Virtual SAN（VSAN：バーチャル SAN）

VSAN-based role（VSAN ベースのロール）

VSAN Trunking Zone Merge Analysis（VSAN トランキング ゾーン マージ分析）－ Cisco Fabric Manager

SAN の正常性を維持する Cisco MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーク機能

Auto Baseline（自動ベースライン）

Call Home（コール ホーム）

Cisco Fabric Services（シスコ ファブリック サービス）

CiscoWorks DFM

CiscoWorks RME

End-to-End Connectivity Analysis（エンドツーエンド接続分析）

Fabric Configuration Analysis（ファブリック設定分析）

Fabric Manager

Fabric Manager Server

Fibre Channel Ping

Fibre Channel Trace（ファイバ チャネル トレースルート）

Fibre Channel Protocol Analysis（ファイバ チャネル プロトコル分析）－ Cisco Fabric Analyzer

Fibre Channel Congestion Control（FCC）

Historical Performance Monitoring（履歴パフォーマンス モニタリング）

Hotspot Analysis（ホットスポット分析）

Port Tracking（ポート トラッキング）

Real-Time Performance Monitoring（リアルタイム パフォーマンス モニタリング）

Remote Switched Port Analyzer（RSPAN：リモート スイッチド ポート アナライザ）

SAN Extension Tuner（SET：SAN 拡張チューナ）

SCSI Flow Statistics（SCSI フロー統計情報）

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

SNMPv3

SPAN（スパン）

Switch Health Analysis（スイッチ ヘルス分析）

Syslog（メッセージ ロギング サーバ）

Traffic Analyzer（トラフィック アナライザ）

Virtual SAN（VSAN：バーチャル SAN）

VSAN-based role（VSAN ベースのロール）

VSAN Trunking（VSAN トランキング）

Zone Merge Analysis（ゾーン マージ分析）－ Cisco Fabric Manager

Cisco MDS 9000 Storage Services Module と連動してストレージ プロビジョニング、データの移行と複製、バックアップと回復、ストレージの利用を集中管理する Cisco MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーク機能

AAA

AES

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

Continuous Data Protection（CDP）

Data Encryption Standard（DES：データ暗号標準）

Triple DES（3DES：トリプル DES）

Encryption（暗号化）

Fabric Binding（ファブリック バインディング）

Fabric Manager

Fabric Manager Server

FCIP Auto-Compression（FCIP 自動圧縮）

FCIP Tape Acceleration（FCIP テープ アクセラレーション）

FCIP Write Acceleration（FCIP ライト アクセラレーション）

Fibre Channel Security Protocol（FC-SP：ファイバ チャネル セキュリティ プロトコル）

Hardware Compression and Decompression（ハードウェアの圧縮と圧縮解除）

Historical Performance Monitoring（履歴パフォーマンス モニタリング）

Host-to-Switch Authentication（ホストとスイッチ間の認証）

Internet Key Exchange（IKE：インターネット鍵交換）

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

IP ACL（IP アクセス コントロール リスト）

IPSec

LAN-Free Backup（LAN フリー バックアップ）

LUN Zoning（LUN ゾーン分割）

Network-Accelerated Serverless Backup（ネットワーク高速化サーバレス バックアップ）

Port Security（ポート セキュリティ）

Quality of Service（サービス品質）

RADIUS

RBAC（Role-Based Access Control：ロールベース アクセス コントロール）

Read-Only Zone（読み取り専用ゾーン）

SANTap

SCSI Flow Statistics（SCSI フロー統計情報）

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

Secure FTP（SFTP）

Secure Sockets Layer（SSL）

SNMPv3

SSH

Syslog（メッセージ ロギング サーバ）

TACACS+

Virtual SAN（VSAN：バーチャル SAN）

Zone Merge Analysis（ゾーン マージ分析）－ Cisco Fabric Manager

スケーラブルな SAN への投資保護を最適化する Cisco MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーク機能

AAA

AES

Auto Learn（自動認識）

B-Port 相互運用性

Buffer-to-Buffer Credit（バッファ間クレジット）

Cisco Fabric Services（シスコ ファブリック サービス）

Cisco MDS 9000 Family Virtualization Solution（Cisco MDS 9000 ファミリ仮想化ソリューション）

CiscoWorks DFM

CiscoWorks RME

Data Encryption Standard（DES：データ暗号標準）

Triple DES（3DES：トリプル DES）

Encryption（暗号化）

End-to-End Connectivity Analysis（エンドツーエンド接続分析）

Extended Buffer-to-Buffer Credit（拡張 BB_credit）

Fabric Binding（ファブリック バインディング）

Fabric Configuration Analysis（ファブリック設定分析）

Fabric Manager

Fabric Manager Server

FCIP（Fibre Channel over IP）

FCIP Auto-Compression（FCIP 自動圧縮）

FCIP Tape Acceleration（FCIP テープ アクセラレーション）

FCIP Write Acceleration（FCIP ライト アクセラレーション）

Fibre Channel Ping

Fibre Channel Trace（ファイバ チャネル トレースルート）

Fibre Channel Protocol Analysis（ファイバ チャネル プロトコル分析）－ Cisco Fabric Analyzer

Fibre Channel Congestion Control（FCC）

Fibre Channel Security Protocol（FC-SP：ファイバ チャネル セキュリティ プロトコル）

Hardware Compression and Decompression（ハードウェアの圧縮と圧縮解除）

Hardware-Enforced Zoning（ハードウェア強制ゾーン分割）

Historical Performance Monitoring（履歴パフォーマンス モニタリング）

Host-to-Switch Authentication（ホストとスイッチ間の認証）

Hotspot Analysis（ホットスポット分析）

Internet Key Exchange（IKE：インターネット鍵交換）

Ingress Port Rate Limiting（入力ポート レート制限）

Integrated Multiprotocol（統合マルチプロトコル）

Internet Storage Name Service（iSNS：インターネット ストレージ ネーム サービス）

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

IP ACL（IP アクセス コントロール リスト）

IPSec

LAN-Free Backup（IPSec LAN フリー バックアップ）

LUN Zoning（LUN ゾーン分割）

Network-Accelerated Serverless Backup（ネットワーク高速化サーバレス バックアップ）

Performance Buffer（パフォーマンス バッファ）

Performance Threshold（パフォーマンスしきい値）

Port Channel（ポート チャネル）

Port Security（ポート セキュリティ）

Port Tracking（ポート トラッキング）

Quality of Service（サービス品質）

RADIUS

RBAC（Role-Based Access Control：ロールベース アクセス コントロール）

Read-Only Zone（読み取り専用ゾーン）

Real-Time Performance Monitoring（リアルタイム パフォーマンス モニタリング）

Redundant Crossbar（冗長クロスバー）

Remote Switched Port Analyzer（RSPAN：リモート スイッチド ポート アナライザ）

Roaming Management Profile（ローミング管理プロファイル）

SAN Extension Tuner（SET：SAN 拡張チューナ）

SANTap

SCSI Flow Statistics（SCSI フロー統計情報）

SCSI Traffic Analyzer（SCSI トラフィック アナライザ）

Secure FTP（SFTP）

Secure Sockets Layer（SSL）

SNMPv3

SPAN（スパン）

SSH

Switch Health Analysis（スイッチ ヘルス分析）

Switch Interoperability Mode（スイッチ相互運用モード）

TACACS+

TCP Buffer（TCP バッファ）

TCP Tuning（TCP 調整）

Traffic Analyzer（トラフィック アナライザ）

Virtual Router Redundancy Protocol（VRRP：仮想ルータ冗長プロトコル）

Virtual SAN（VSAN：バーチャル SAN）

VSAN-based role（VSAN ベースのロール）

VSAN Trunking（VSAN トランキング）

Zone Merge Analysis（ゾーン マージ分析）－ Cisco Fabric Manager

スイッチの相互運用性を実現する Cisco MDS 9000 SAN-OS ソフトウェア インテリジェント ネットワーク機能

B-Port Interoperability（B-Port 相互運用性）

Fabric Binding（ファブリック バインディング）

Fabric Manager

Fabric Manager Server

FCID Persistence（FCID パーシスタンス）

FCIP（Fibre Channel over IP）

Integrated Multiprotocol（統合マルチプロトコル）

Internet Storage Name Service（iSNS：インターネット ストレージ ネーム サービス）

Inter-VSAN Routing（IVR：VSAN 間ルーティング）

Switch Interoperability Mode（スイッチ相互運用モード）

Virtual SAN（VSAN：バーチャル SAN）

VSAN Trunking（VSAN トランキング）