Overview

The Cisco NX-OS software supports security features that can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

This chapter includes the following sections:

ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1 つの NXOS ソフトウェア イメージで構成されます（たとえば n9000-dk9.6.1.2.I1.1.bin）。 このイメージは、すべての Cisco Nexus 9000 シリーズ スイッチで実行されます。

ソフトウェアの互換性

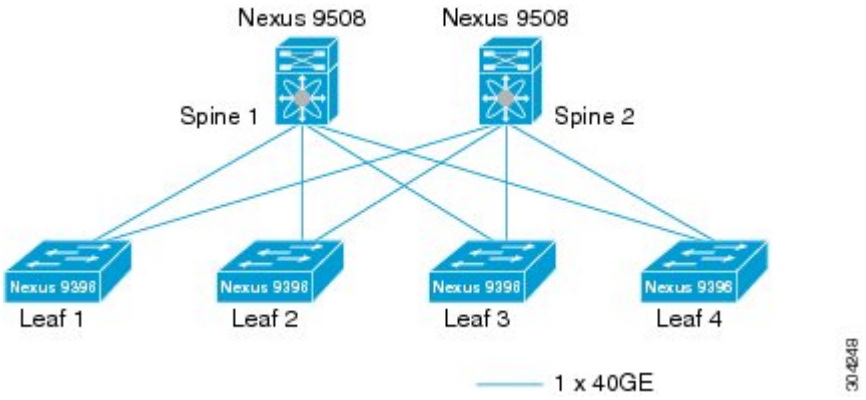
Cisco NX-OS ソフトウェアは、Cisco IOS ソフトウェアのどのバリエーションを実行するシスコ製品とも相互運用できます。 また、Cisco NX-OS ソフトウェアは、IEEE および RFC 準拠標準に準拠するどのネットワーキング オペレーティング システムとも相互運用できます。

スパイン/リーフ型トポロジ

Cisco Nexus 9000 シリーズ スイッチは、2 階層のスパイン/リーフ型トポロジをサポートします。

この図は、2 つの Spine スイッチ（Cisco Nexus 9508）に接続している 4 つの Leaf スイッチ（Cisco Nexus 9396 または 93128）、および各 Leaf から各 Spine までの 2 つの 40G イーサネット アップリンクが存在するスパイン/リーフ型トポロジの例を示しています。

図 *1*： スパイン/リーフ型トポロジ



モジュラ式のソフトウェア設計

Cisco NX-OS ソフトウェアは、対称型マルチプロセッサ（SMP）、マルチコア CPU、分散データ モジュール プロセッサ上の分散マルチスレッド処理をサポートします。 Cisco NX-OS ソフトウェアは、ハードウェア テーブル プログラミングのような大量の演算処理を要するタスクを、データ モジュールに分散された専用のプロセッサにオフロードします。 モジュール化されたプロセスは、それぞれ別の保護メモリ領域内でオンデマンドに生成されます。 機能がイネーブルになったときにだけ、プロセスが開始されてシステム リソースが割り当てられます。 これらのモジュール化されたプロセスはリアルタイム プリエンプティブ スケジューラによって制御されるため、重要な機能が適切なタイミングで実行されます。

サービスアビリティ

Cisco NX-OS ソフトウェアには、デバイスがネットワークのトレンドやイベントに対応できるサービスアビリティ機能が組み込まれています。 これらの機能は、ネットワーク プランニングおよび応答時間の短縮に役立ちます。

スイッチド ポート アナライザ

SPAN 機能を使用すると、外部アナライザが接続された SPAN の終点ポートに、セッションに負担をかけずに SPAN セッション トラフィックが送信されるようになり、ポート（SPAN ソース ポートと呼びます）間のすべてのトラフィックを分析できるようになります。 SPAN の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

Ethanalyzer

Ethanalyzer は、Wireshark（旧称 Ethereal）オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。 Ethanalyzer は、パケットのキャプチャとデコード用の Wireshark のコマンド ライン バージョンです。 Ethanalyzer を使用してネットワークをトラブルシューティングし、コントロール プレーン トラフィックを分析できます。 Ethanalyzer の詳細については、『*Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*』を参照してください。

Smart Call Home

Call Home は、ハードウェア コンポーネントとソフトウェア コンポーネントを継続的にモニタリングし、重要なシステム イベントを E メールで通知する機能です。 さまざまなメッセージ フォーマットが用意されており、ポケットベル サービス、標準の E メール、および XML ベースの自動解析アプリケーションに対応します。 アラートをグループ化する機能や、宛先プロファイルのカスタマイズも可能です。 この機能の利用方法には、ネットワーク サポート技術者を直接ポケットベルで呼び出す、ネットワーク オペレーション センター（NOC）に電子メール メッセージを送信する、および Cisco AutoNotify サービスを使用して Cisco Technical Assistance Center（TAC）へ問題を直接送信する、などの方法があります。 Smart Call Home の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

オンライン診断

Cisco Generic Online Diagnostics（GOLD）では、ハードウェアおよび内部データ パスが設計どおりに動作していることを確認します。 Cisco GOLD フィーチャ セットには、起動時診断、継続監視、オンデマンド テスト、スケジュール テストが含まれます。 GOLD では障害を迅速に特定し、システムを継続的に監視できます。 GOLD の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

Embedded Event Manager

Cisco Embedded Event Manager（EEM）は、ネットワーク イベントが発生した場合の動作をカスタマイズできる、デバイスおよびシステムの管理機能です。 EEM の設定の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

管理性

この項では、Cisco Nexus 9000 シリーズ スイッチの管理の簡易性に関する機能について説明します。

簡易ネットワーク管理プロトコル

Cisco NX-OS ソフトウェアは、簡易ネットワーク管理プロトコル（SNMP）バージョン 1、2、および 3 に準拠しています。 多くの管理情報ベース（Management Information Base）がサポートされます。 SNMP の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

設定の確認およびロールバック

Cisco NX-OS ソフトウェアでは、設定をコミットする前に、設定の一貫性や必要なハードウェア リソースの可用性を確認することができます。 デバイスを事前に設定し、確認した設定を後から適用することができます。 設定には、必要に応じて、既知の良好な設定にロール バックできるチェック ポイントを含めることができます。 ロールバックの詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。

ロールベース アクセス コントロール

ロールベース アクセス コントロール（RBAC）では、ユーザにロールを割り当てることで、デバイス操作のアクセスを制限できます。 アクセスが必要なユーザだけにアクセスを許可するように、カスタマイズすることが可能です。 RBAC の詳細については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』を参照してください。

Cisco NX-OS デバイス コンフィギュレーション方式

Cisco NX-OS デバイスを設定するには、次の方法を使用できます。

- セキュア シェル（SSH）セッション、Telnet セッション、またはコンソール ポートからの CLI。 SSH ではデバイスへの安全な接続が提供されます。 CLI コンフィギュレーション ガイドは機能別に編成されています。 詳細については、Cisco NX-OS のコンフィギュレーション

ガイドを参照してください。 SSH と Telnet の詳細については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』を参照してください。

- CLI を補完する NETCONF プロトコルに基づくプログラマチック方式である、XML 管理インターフェイス。 詳細については、『*Cisco NX-OS XML Interface User Guide*』を参照してください。
- ローカル PC で稼動し、Cisco DCNM サーバで Web サービスを使用する、Cisco Data Center Network Management（DCNM）クライアント。 Cisco DCNM サーバでは XML 管理インターフェイスを使用してデバイスを設定します。 Cisco DCNM クライアントの詳細については、『*Cisco DCNM Fundamentals Guide*』を参照してください。

プログラマビリティ

この項では、Cisco Nexus 9000 シリーズ スイッチのプログラマビリティに関する機能について説明します。

Python API

Python は簡単に習得できる強力なプログラミング言語です。 効率的で高水準なデータ構造を持ち、オブジェクト指向プログラミングに対してシンプルで効果的なアプローチを取っています。 Python は、簡潔な構文、動的な型付け、およびインタープリタ型という性質によって、ほとんどのプラットフォームのさまざまな分野でスクリプティングと高速なアプリケーション開発を実現する理想的な言語です。 Python のインタープリタと広範な標準ライブラリは、Python Web サイト（http://www.python.org/）から、主要なプラットフォームに対応したソース形式またはバイナリ形式で自由に利用できます。 Python スクリプト機能は、さまざまなタスクを実行するために CLI と Power On Auto Provisioning（POAP）または Embedded Event Manager（EEM）アクションへのプログラムによるアクセスを提供します。 Python API と Python スクリプト機能の詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

Tcl

Tool Command Language（Tcl）は、スクリプト言語です。 Tcl を使用すると、デバイスの CLI Commands をより柔軟に使用できます。 Tcl を使用して **show** コマンドの出力の特定の値を抽出したり、スイッチを設定したり、Cisco NX-OS コマンドをループで実行したり、スクリプトで EEM ポリシーを定義したりすることができます。

Cisco NX-API

Cisco NX-API は Cisco Nexus 9000 シリーズ スイッチへの Web ベースのプログラムによるアクセスを提供します。 このサポートは NX-API のオープンソースの Web サーバによって提供されています。 Cisco NX-API は Web ベースの API を介して、コマンドライン インターフェイス（CLI）の完全な設定および管理機能を公開します。 XML または JSON 形式で API コールの出力を公開す

るようにスイッチを設定できます。 Cisco NX-API の詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

（注） NX-API は、スイッチ上の Programmable Authentication Module（PAM）を使用して認証を行います。 Cookie を使用して PAM の認証数を減らし、PAM の負荷を減らします。

Bash シェル

Cisco Nexus 9000 シリーズ スイッチは、Linux シェルの直接アクセスをサポートしています。 Linux シェルのサポートにより、スイッチの Linux システムにアクセスして、Linux コマンドを使用してベース システムを管理できます。 Bash シェルのサポートの詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

Broadcom シェル

Cisco Nexus 9000 シリーズ スイッチの前面パネルおよびファブリック モジュール ラインカードには複数の Broadcom ASIC が含まれます。 CLI を使用し、これらの ASIC のコマンドライン シェル（bcm シェル）にアクセスできます。 この方法を使用して bcm シェルにアクセスするメリットは、**pipe include** や **redirect output to file** などの Cisco NX-OS 拡張コマンドを使用できることです。また、アクティビティは bcm シェルから直接入力するアカウンティング ログに記録されないコマンドとは異なり、監査のためにシステム アカウンティング ログに記録されます。 Broadcom シェルのサポートの詳細については、『*Cisco Nexus 9000 Series NX-OS Programmability Guide*』を参照してください。

注意 Broadcom シェル コマンドは、シスコのサポート担当者の直接監督下または要求された場合のみ注意して使用してください。

トラフィックのルーティング、転送、および管理

ここでは、Cisco NX-OS ソフトウェアでサポートされるトラフィックのルーティング、転送、および管理機能について説明します。

イーサネット スイッチング

Cisco NX-OS ソフトウェアは、高密度、高性能のイーサネット システムをサポートし、次のイーサネット スイッチング機能を提供します。

- IEEE 802.1D-2004 高速スパニングツリー プロトコル（RSTP）およびマルチ スパニングツリー プロトコル（802.1w および 802.1s）

- IEEE 802.1Q VLAN およびトランク
- IEEE 802.3ad リンク アグリゲーション
- アグレッシブ モードと標準モードの Unidirectional Link Detection（UDLD； 単一方向リンク検出）

詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』および『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

IP ルーティング

Cisco NX-OS NX-OS ソフトウェアは、IP Version 4（IPv4）および IP Version 6（IPv6）、および次のルーティング プロトコルをサポートしています。

- Open Shortest Path First（OSPF）プロトコル バージョン 2（IPv4）および 3（IPv6）
- Intermediate System-to-Intermediate System（IS-IS）プロトコル
- ボーダー ゲートウェイ プロトコル（BGP）（IPv4 および IPv6）
- Enhanced Interior Gateway Routing Protocol（EIGRP）（IPv4 のみ）
- Routing Information Protocol Version 2（RIPv2）

Cisco NX-OS ソフトウェアでのこれらのプロトコルの実装は、最新の規格に完全に準拠しています。また、4 バイト自律システム番号（ASN）とインクリメンタル Shortest Path First（SPF）が含まれています。 すべてのユニキャスト プロトコルでは、ノンストップ フォワーディング グレースフル リスタート（NSF-GR）をサポートしています。 すべてのプロトコルは、イーサネット インターフェイス、VLAN インターフェイス、サブインターフェイス、ポート チャネル、およびループバック インターフェイスなど、すべてのインターフェイスタイプをサポートしています。

詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IP サービス

Cisco NX-OS ソフトウェアでは、次の IP Services を使用できます。

- VPN ルーティングおよび転送（VRF）
- Dynamic Host Configuration Protocol（DHCP）ヘルパー
- ホットスタンバイ ルータ プロトコル（HSRP）
- 拡張オブジェクト トラッキング
- ポリシーベース ルーティング（PBR）
- IPv4 の全プロトコルに対するユニキャスト グレースフル リスタート、および IPv6 の OSPFv3 に対するユニキャスト グレースフル リスタート

詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IP マルチキャスト

Cisco NX-OS ソフトウェアには、次のマルチキャスト プロトコルと機能が用意されています。

- Protocol Independent Multicast（PIM）Version 2（PIMv2）
- PIM スパース モード（IPv4 の Any-Source マルチキャスト（ASM））
- Anycast ランデブー ポイント（Anycast-RP）
- IPv4 のマルチキャスト NSF
- ブートストラップ ルータ（BSR）を使用する RP-Discovery（Auto-RP およびスタティック）
- インターネット グループ管理プロトコル（IGMP）バージョン 1、2、3 ルータ ロール
- IGMPv2 ホスト モード
- IGMP スヌーピング
- Multicast Source Discovery Protocol（MSDP）（IPv4）

（注） Cisco NX-OS ソフトウェアでは、PIM デンス モードをサポートしていません。

詳細については、『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*』を参照してください。

Quality of Service

Cisco NX-OS ソフトウェアでは、分類、マーキング、キューイング、ポリシング、およびスケジューリングに対する Quality of Service（QoS）機能をサポートしています。 Modular QoS（MQC）の CLI では、すべての QoS 機能をサポートしています。 MQC を使用すると、シスコのさまざまなプラットフォームで同一の設定を行うことができます。 詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

ネットワーク セキュリティ機能

Cisco NX-OS ソフトウェアには、次のセキュリティ機能があります。

- コントロール プレーン ポリシング（CoPP）
- メッセージ ダイジェスト アルゴリズム 5（MD5）のルーティング プロトコル認証
- 認証、許可、アカウンティング（AAA）

- RADIUS および TACACS+
- SSH プロトコル バージョン 2
- SNMPv3
- 名前付き ACL でサポートされている MAC アドレスおよび IPv4 アドレスに基づくポリシー（ポート ベース ACL（PACL）、VLAN ベース ACL（VACL）、およびルータ ベース ACL（RACL））
- トラフィック ストーム制御（ユニキャスト、マルチキャスト、およびブロードキャスト）

詳細については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』を参照してください。

ライセンス

Cisco NX-OS ソフトウェアでは、デバイスの高度な機能を使用する場合は、その機能に対応するライセンスをインストールする必要があります。 ライセンス パッケージに含まれていない機能は、Cisco NX-OS ソフトウェアにバンドルされており、追加費用は一切発生しません。

各デバイス用のライセンスを購入してインストールする必要があります。

（注） ライセンスをインストールしないでも機能をイネーブルにできます。Cisco NX-OS ソフトウェアには、ライセンスを購入する前に機能を試すことができる猶予期間があります。

Cisco NX-OS ソフトウェアのライセンスの詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ライセンスに関する問題のトラブルシューティングの詳細については『*Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*』を参照してください。

サポートされる規格

次の表に、IEEE 準拠標準を示します。

表 *1*：*IEEE* 準拠標準

規格	説明
802.1D	MAC ブリッジ
802.1s	マルチ スパニングツリー プロトコル
802.1w	高速スパニングツリー プロトコル

規格	説明
802.3ad	LACP によるリンク集約
802.3ab	1000Base-T（銅線 10/100/1000 イーサネット）
802.3ae	10 ギガビット イーサネット
802.1Q	VLAN タギング
802.1p	イーサネット フレームのサービス クラス（CoS）タギング

次の表に、RFC 準拠標準を示します。

表 *2*：*RFC* 準拠標準

規格	説明
BGP	
RFC 1997	『BGP Communities Attribute』
RFC 2385	『Protection of BGP Sessions via the TCP MD5 Signature Option』
RFC 2439	『BGP Route flap damping』
RFC 2519	『A Framework for Inter-Domain Route Aggregation』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3065	『Autonomous System Confederations for BGP』
RFC 3392	『Capabilities Advertisement with BGP-4』
RFC 4271	『BGP version 4』
RFC 4273	『BGP4 MIB - Definitions of Managed Objects for BGP-4』
RFC 4456	『BGP Route reflection』

規格	説明
RFC 4486	『Subcodes for BGP cease notification message』
RFC 4724	『Graceful Restart Mechanism for BGP』
RFC 4893	『BGP Support for Four-octet AS Number Space』
IETF ドラフト	『Bestpath transition avoidanc』（draft-ietf-idr-avoid-transition-05.txt）
IETF ドラフト	『Peer table objects』（draft-ietf-idr-bgp4-mib-15.txt）
IETF ドラフト	『Dynamic Capability』（draft-ietf-idr-dynamic-cap-03.txt）
OSPF	
RFC 2370	『OSPF Opaque LSA Option』
RFC 2328	『OSPF Version 2』
RFC 2740	『OSPF for IPv6 (OSPF version 3)』
RFC 3101	『OSPF Not-So-Stubby-Area (NSSA) Option』
RFC 3137	『OSPF Stub Router Advertisement』
RFC 3509	『Alternative Implementations of OSPF Area Border Routers』
RFC 3623	『Graceful OSPF Restart』
RFC 4750	『OSPF Version 2 MIB』
RIP	
RFC 1724	『RIPv2 MIB extension』
RFC 2082	『RIPv2 MD5 Authentication』

規格	説明
RFC 2453	『RIP Version 2』
IS-IS	
RFC 1142（OSI 10589）	『OSI 10589 Intermediate system to intermediate system intra-domain routing exchange protocol』
RFC 1195	『Use of OSI IS-IS for routing in TCP/IP and dual environment』
RFC 2763	『Dynamic Hostname Exchange Mechanism for IS-IS』
RFC 2966	『Domain-wide Prefix Distribution with Two-Level IS-IS』
RFC 2973	『IS-IS Mesh Groups』
RFC 3277	『IS-IS Transient Blackhole Avoidance』
RFC 3373	『Three-Way Handshake for IS-IS Point-to-Point Adjacencies』
RFC 3567	『IS-IS Cryptographic Authentication』
RFC 3847	『Restart Signaling for IS-IS』
IETF ドラフト	『Internet Draft Point-to-point operation over LAN in link-state routing protocols』（draft-ietf-isis-igp-p2p-over-lan-06.txt）
IP サービス	
RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP

規格	説明
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 959	FTP
RFC 1027	プロキシ ARP
RFC 1305	NTP v3
RFC 1519	CIDR
RFC 1542	BootP リレー
RFC 1591	DNS クライアント
RFC 1812	IPv4 ルータ
RFC 2131	DHCP ヘルパー
RFC 2338	VRRP
IP マルチキャスト	
RFC 2236	『Internet Group Management Protocol, Version 2』
RFC 3376	『Internet Group Management Protocol, Version 3』
RFC 3446	『Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』
RFC 3618	Multicast Source Discovery Protocol（MSDP）
RFC 4601	『ASM - Sparse Mode (PIM-SM): Protocol Specification (Revised)』

規格	説明
RFC 4607	『Source-Specific Multicast for IP』
RFC 4610	『Anycast-RP Using Protocol Independent Multicast (PIM)』
IETF ドラフト	『Mtrace server functionality, to process mtrace-requests』（draft-ietf-idmr-traceroute-ipm-07.txt）