



概要

- [プログラマビリティの概要](#) (1 ページ)
- [サポートされるプラットフォーム](#) (2 ページ)
- [標準的なネットワーク管理機能](#) (2 ページ)
- [高度な自動化機能](#) (2 ページ)
- [プログラマビリティのサポート](#) (2 ページ)

プログラマビリティの概要

Cisco Nexus 9000 シリーズ スイッチ上で動作する Cisco NX-OS ソフトウェアには、次のような特徴があります。

- **耐障害性**
クリティカルなビジネスクラスの可用性を確保します。
- **モジュラ型**
ビジネス ニーズに対応する拡張機能があります。
- **高度なプログラム性**
アプリケーションプログラミングインターフェイス (API) を介した迅速な自動化とオーケストレーションを可能にします。
- **セキュア**
データと運用を保護し維持します。
- **柔軟性**
新しいテクノロジーを統合して有効にします。
- **優れた拡張性**
ビジネスと要件に対応して拡大できます。
- **使いやすさ**

必要な学習量が少なく、展開がシンプルで、管理が容易です。

Cisco NX-OS オペレーティング システムでは、デバイスはユニファイド ファブリック モードで機能し、プログラムによる自動化機能を備えたネットワーク接続を提供します。

Cisco NX-OS には、オープン ソース ソフトウェア (OSS) と商用テクノロジーが含まれており、これらは自動化、オーケストレーション、プログラマビリティ、モニタリング、コンプライアンスをサポートします。

オープンな NX-OS の詳細については、<https://developer.cisco.com/site/nx-os/>を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降、「[Nexus スイッチ プラットフォーム サポート マトリクス](#)」を使用して、選択した機能をサポートするさまざまな Cisco Nexus 9000 および 3000 スイッチのリリース元である Cisco NX-OS を知ることができます。

標準的なネットワーク管理機能

- SNMP (V1、V2、V3)
- Syslog
- RMON
- NETCONF
- CLI および CLI スクリプト

高度な自動化機能

デバイスでの機能が強化された Cisco NX-OS は、自動化をサポートします。プラットフォームには、電源投入時自動プロビジョニング (POAP) のサポートが含まれています。

デバイスでの機能が強化された Cisco NX-OS は、自動化をサポートします。プラットフォームには、自動化をサポートする機能が含まれています。

プログラマビリティのサポート

スイッチ上の Cisco NX-OS ソフトウェアは、プログラマビリティを支援する複数の機能をサポートしています。

NX-API のサポート

Cisco NX-API を使用すると、HTTP ベースのプログラムによってスイッチにアクセスすることが可能になります。このサポートは、オープンソースの Web サーバーである NX-API によって提供されています。NX-API では、Web ベース API を通じて Cisco NX-OS CLI のすべての構成機能および管理機能を提供しています。デバイスは、XML または JSON フォーマットで API 呼び出しの出力を公開するように設定できます。この API により、スイッチでの迅速な開発が可能になります。

Python スクリプティング

Cisco NX-OS は、Python v2.7.5 を、インタラクティブ モードと非インタラクティブ（スクリプト）モードの両方でサポートしています。

Cisco NX-OS リリース 9.3(5) 以降、Python 3 もサポートされています。

デバイスの Python スクリプト機能は、さまざまなタスクを実行するためのスイッチの 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。Cisco NX-OS CLI を呼び出す Python コールへの応答は、テキストまたは JSON 出力を返します。

Python インタープリタは Cisco NX-OS ソフトウェアに含まれています。

Tcl スクリプティング

Cisco Nexus 9000 シリーズスイッチは、Tcl（ツール コマンド言語）をサポートします。Tcl は、スイッチで CLI コマンドを柔軟に使用できるようにするスクリプト言語です。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。

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 モジュールのラインカードには Broadcom のネットワーク転送エンジン (NFE) が搭載されています。これらの NFE から Broadcom コマンドラインシェル (bcm-shell) にアクセスすることができます。

bash

Cisco Nexus スイッチは、Bourne-Again Shell (Bash) への直接アクセスをサポートします。Bash では、デバイス上の基盤となる Linux システムにアクセスし、システムを管理できます。

bash シェルへのアクセスと Linux コンテナのサポート

Cisco Nexus スイッチは、Linux シェルへの直接アクセスと Linux コンテナをサポートしています。Linux シェルへのアクセスでは、スイッチ上の基盤となっている Linux システムにアクセ

スして、基盤システムを管理できます。また、Linux コンテナを使用して、独自のソフトウェアを安全にインストールし、Cisco Nexus スイッチの機能を強化することもできます。たとえば、Cobbler などのベアメタルプロビジョニングツールを Cisco Nexus スイッチにインストールして、トップオブブラック スイッチからベアメタル サーバーを自動的にプロビジョニングすることができます。

ゲストシェル

<p>プロセスホスト型展開では、仮想サービス実行環境 (VSEE) が、NOS が提供するコアルーティングおよびスイッチングアプリケーションから onePK アプリケーションを分離します。この環境はまた、そのコンテンツを同じホスト上の他の仮想サービスから分離します。アプリケーション開発者は、指定された量の CPU 時間、メモリ、ディスク容量、およびその他のリソースを特定の VSEE に割り当てることができます。</p>
<p>シスコは、Cisco Secure Development Lifecycle (SDLC) を利用して、クローズドな Cisco システム上の VSEE で実行される onePK アプリケーションを開発します。SDLC は、シスコが提供するアプリケーション、VSEE、およびプラットフォームの脆弱性フットプリントを削減する、業界で認められている一連のベスト プラクティスとツール (シスコ独自のツールを含む) で構成されています。これらのプラクティスには、ロードする前にシスコが署名したバイナリの整合性を確保するランタイム チェックの使用と、シスコが提供する onePK アプリケーションが信頼できるプロセスとして実行できる信頼ドメインの確立が含まれます。</p>
<p>VSEE の onePK アプリケーションは、onePK SDK が提供する onePK API を使用してネットワーク要素と通信します。セキュア通信チャネルが、VSEE と onePK サーバーの間でメッセージを伝送します。信頼ドメインを使用することで、シスコが提供する VSEE 内のプロセス間通信の整合性が保証され、追加のセキュリティ対策により VSEE とシスコホスト間の通信が保護されます。</p>
<p>ネットワーク管理者は、ネットワーク要素と対話する VSEE およびアプリケーションの展開を直接制御します。ネットワーク管理者の職務には、アプリケーションパッケージの完全性と有効性を検証する責任が含まれます。シスコは、ネットワーク管理者が標準のソフトウェア開発ツールを使用して、アプリケーションパッケージを展開する前にその完全性を検証できるようにする情報 (デジタル署名や MD5 チェックサムなど) を提供します。さらに、onePK VSEE セキュリティ インフラストラクチャのデフォルト設定では、シスコが署名したアプリケーションパッケージのみがプロセス ホスト モードで実行できます。署名されていないコンテナまたはサードパーティによって署名されたコンテナの展開を許可するには、ネットワーク管理者が明示的なアクションを実行する必要があります。</p>
<p>onePK ではネットワーク要素への低レベルのアクセスが許可されるため、ネットワーク管理者は、onePK へのアクセスを許可するユーザー プロファイルとアプリケーションについて慎重に選択する必要があります。</p>

Cisco Nexus 9000 シリーズ スイッチは、セキュア Linux コンテナ (LXC) 内で実行される仮想サービス環境をサポートします。仮想サービス環境のゲストシェルで実行されているアプリケーションを、ホスト Cisco NX-OS が提供する他のルーティングおよびスイッチングアプリケーションから分離します。また、この環境は、そのコンテンツを同じホスト上の他の仮想サービスから分離します。指定した量の CPU 時間、メモリ、ディスク容量、およびその他のリソースを特定の仮想サービス環境に割り当てることができます。

シスコは、Cisco Secure Development Lifecycle (SDLC) を利用して、Cisco Nexus 9000 シリーズ デバイスの仮想サービス環境で実行されるアプリケーションを開発します。SDLC は、シスコが提供するアプリケーション、仮想サービス環境、およびプラットフォームの脆弱性フットプリントを削減する、業界で認められている一連のベストプラクティスとツール (シスコ独自のツールを含む) で構成されています。これらのプラクティスには、ロードする前にシスコが署名したバイナリの整合性を確保するランタイムチェックの使用と、シスコが提供するアプリケーションが信頼できるプロセスとして実行できる信頼ドメインの確立が含まれます。

ゲストシェルのアプリケーションは、API を使用してネットワークと通信します。セキュア通信チャンネルが、ゲストシェルとデバイス間でメッセージを送ります。信頼ドメインを使用することで、シスコが提供するゲストシェル内のプロセス間通信の整合性が保証され、追加のセキュリティ対策によりゲストシェルとデバイス間の通信が保護されます。

ネットワーク管理者は、ネットワークと対話する仮想サービス環境およびアプリケーションの展開を制御します。ネットワーク管理者の職務には、アプリケーションパッケージの完全性と有効性を検証する責任が含まれます。シスコは、ネットワーク管理者が標準のソフトウェア開発ツールを使用して、アプリケーションパッケージを展開する前にその完全性を検証できるようにする情報 (デジタル署名や MD5 チェックサムなど) を提供します。さらに、ゲストシェルセキュリティインフラストラクチャのデフォルト設定では、シスコが署名したアプリケーションパッケージのみがホスト上で実行できます。署名されていないコンテナまたはサードパーティによって署名されたコンテナの展開を許可するには、ネットワーク管理者が明示的なアクションを実行する必要があります。

Cisco Nexus 9000 シリーズ スイッチは、ホスト Cisco Nexus 9000 NX-OS ソフトウェアから分離されたホストシステム上の Linux 実行スペースへの Bash アクセスを提供するゲストシェルをサポートします。ゲストシェルを使用すると、ホストシステムソフトウェアに影響を与えることなく、必要に応じてソフトウェアパッケージを追加し、ライブラリを更新できます。

ゲストシェルで実行されているアプリケーションは、ソケット API を介してホストシステムと外部ネットワークに IP 接続します。

ゲストシェルはセキュア Linux コンテナ (LXC) として実装され、ホストシステムの起動時に自動的に開始されます。これにより、システムの起動時にゲストシェル内のアプリケーションを自動的に起動できます。ゲストシェルに使用される CPU、メモリ、およびブートフラッシュ領域の量は、ゲストシェルとホストシステム間のリソース使用率のバランスが取れるように調整できます。ゲストシェルはシステムのブートフラッシュをマウントし、Linux コマンドを使用してブートフラッシュ上のファイルにアクセスできるようにします。

コンテナトラッカーのサポート

Cisco NX-OS は、特定のスイッチポートの背後にあるコンテナの機能を理解するため、Kubernetes API サーバーと通信するように構成されます。

次のコマンドにより、Kubernetes API サーバーと通信します。

- **show containers kubernetes** コマンドは、HTTP 経由の API コールを使用して *kube-apiserver* からデータを取得します。
- **kubernetes watch resource** コマンドは、デーモンを使用して要求されたリソースにサブスクライブし、*kube-apiserver* からのストリーミングデータを処理します。
- **watch** コマンドで割り当てられた **action** は、事前定義されたトリガーにより実行されます。（たとえば、ポッドの追加または削除）。

Perl モジュール



(注) Cisco NX-OS リリース9.2(2)以降では、-R ラインカードを備えた Cisco Nexus 9504 および 9508 スイッチでの Perl モジュールのサポートが追加されています。

より多くのアプリケーションをサポートするために、次の Perl モジュールが追加されました。

- bytes.pm
- feature.pm
- hostname.pl
- lib.pm
- overload.pm
- Carp.pm
- Class/Struct.pm
- Data/Dumper.pm
- DynaLoader.pm
- Exporter/Heavy.pm
- FileHandle.pm
- File/Basename.pm
- File/Glob.pm
- File/Spec.pm
- File/Spec/Unix.pm

- File/stat.pm
- Getopt/Std.pm
- IO.pm
- IO/File.pm
- IO/Handle.pm
- IO/Seekable.pm
- IO/Select.pm
- List/Util.pm
- MIME/Base64.pm
- SelectSaver.pm
- Socket.pm
- Symbol.pm
- Sys/Hostname.pm
- Time/HiRes.pm
- auto/Data/Dumper/Dumper.so
- auto/File/Glob/Glob.so
- auto/IO/IO.so
- auto/List/Util/Util.so
- auto/MIME/Base64/Base64.so
- auto/Socket/Socket.so
- auto/Sys/Hostname/Hostname.so
- auto/Time/HiRes/HiRes.so

FPM 並列ルックアップ

Nexus 9332D-H2R プラットフォーム スイッチは、ダイ上の 2 つの連続する FPM インスタンス間の並列ルックアップをサポートし、40 すべての FPM インスタンスをルックアップするためにかかる全体のサイクルを削減します。2 つの FPM インスタンス間の並列ルックアップを有効にするには、2 つのブロック間に、ルックアップキーまたはインデックスの派生への依存関係が存在しないようにする必要があります。たとえば、隣接関係インデックスは IP ルートルックアップから取得されるため、一方に IP ルートがあり、もう一方に隣接エントリがある 2 つの FPM インスタンス間では、並列ルックアップを有効にすることはできません。スイッチでの並列ルックアップ機能はデフォルトで有効になっています。この機能を無効にすることはできません。

翻訳について

このドキュメントは、米国シスコ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。