Cisco Nexus 1000V シリーズ スイッチ

データ シート

Cisco Nexus 1000V シリーズ スイッチ

製品概要

Cisco Nexus® 1000V シリーズ スイッチは、仮想マシン（VM）とクラウド ネットワーキングに総合的かつ拡張可能なアーキテクチャのプラットフォームを提供します。このスイッチは、セキュアで透過的な運用によって、サーバの仮想化とマルチテナント クラウドの導入を促進します。VMware vSphere ハイパーバイザと一体化し、VMware vCloud Director と完全に互換性がある Cisco® Nexus 1000V シリーズには、次のような機能があります。

- Cisco NX-OS オペレーティング システムと IEEE 802.1Q スイッチング テクノロジーに基づいた高度な仮想マシン ネットワーキング
- 仮想ネットワーク サービスと効率的、最適に統合された Cisco vPath テクノロジー
- Virtual Extensible Local Area Network（VXLAN）によりクラウド ネットワーキングに対応

このような機能によって、仮想マシンはフル スイッチング機能、および専用環境とマルチテナント クラウド環境の両方における レイヤ 4 ～ 7のさまざまなサービスを備えた、データセンターの基本的な構成要素となります。Nexus 1000V シリーズに VXLAN を 導入すると、従来の VLAN よりも仮想マシンのネットワーク分離を拡張することができ、クラウド規模のネットワーキングに対応できます。

Cisco Nexus 1000V シリーズによる高度な仮想マシン ネットワーキング

Cisco Nexus 1000V シリーズ スイッチは、Cisco NX-OS オペレーティング システムが動作する VMware vSphere 環境に適した仮想マシン アクセス スイッチです。VMware ESX または ESXi ハイパーバイザ内で処理を行う Cisco Nexus 1000V シリーズには、次のような機能があります。

- ポリシーベースの仮想マシン接続
- モビリティのある仮想マシンのセキュリティとネットワーク ポリシー
- サーバ仮想化およびネットワーキング チームのための中断のない運用モデル

データセンターにサーバ仮想化を導入した場合、通常、仮想サーバは物理サーバとは異なる方法で管理されます。サーバ仮想化は特殊な導入として扱われるため、導入にかかる時間が長く、サーバ、ネットワーク、ストレージ、セキュリティそれぞれの管理者間の高度な連携が必要です。Cisco Nexus 1000V シリーズでは、仮想マシン アクセス レイヤからデータセンター ネットワーク インフラストラクチャのコアまですべてに一貫したネットワーキング フィーチャ セットとプロビジョニング プロセスを使用できます。さらに、仮想サーバは、専用の物理ネットワーク ポートに接続された物理サーバのものと同じネットワーク設定、セキュリティ ポリシー、診断ツール、および運用モデルを使用できます。また、移行される仮想マシンと共に定義済みネットワーク ポリシーも移動することで適切な接続を保てるため、仮想化の管理者は貴重な時間を本業である仮想マシンの管理に費やせるようになります。この包括的な一連の機能により、サーバ仮想化の導入にかかる時間を短縮し、サーバ仮想化の利点を短期間で実現することが可能です。

Cisco Nexus 1000V シリーズは VMware との緊密なコラボレーションを通して開発されており、VMware vSphere、vCenter、vCloud Director、ESX、ESXi、およびその他多数の VMware vSphere 機能について VMware から互換性認定を受けています。Cisco Nexus 1000V シリーズを使用すると、サーバ仮想化およびクラウド インフラストラクチャの整合性が保証された状態で仮想マシンの接続管理を行うことができます。

製品アーキテクチャ

Cisco Nexus 1000V シリーズ スイッチには 2 つの主要コンポーネントがあります。1 つは Virtual Ethernet Module（VEM）で、ハイパーバイザの内部で動作します。もう 1 つは外部の Virtual Supervisor Module（VSM）で、VEM を管理します（図 1）。

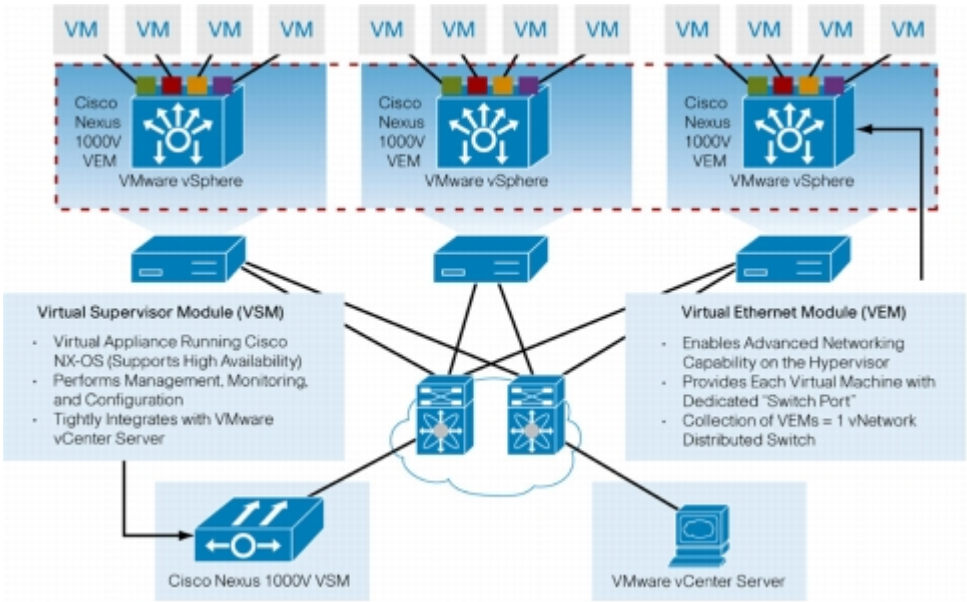

図 1 Cisco Nexus 1000V シリーズのアーキテクチャ

Virtual Ethernet Module

Cisco Nexus 1000V シリーズ VEM は VMware ESX または ESXi カーネルの一部として動作し、VMware Virtual Switch の機能を代わりに実行します。VEM は、シスコと VMware が共同開発した VMware vNetwork Distributed Switch（vDS）API を使用して、仮想マシンに高度なネットワーク機能を提供します。このような高レベルの統合により、Cisco Nexus 1000V シリーズはサーバの仮想化イベント（VMware VMotion、Distributed Resource Scheduler（DRS）など）のすべてを確実に認識できます。VEM は VSM から構成情報を取得し、次のようなレイヤ 2 スイッチングや高度なネットワーク機能を実行します。

- PortChannel
- Quality of service（QoS）
- セキュリティ：プライベート VLAN、アクセス コントロール リスト（ACL）、ポート セキュリティ
- 監視：NetFlow、Switch Port Analyzer（SPAN）、Encapsulated Remote SPAN（ERSPAN）

VSM との通信が失われた場合に備えて、VEM にはノンストップ フォワーディング（NSF）機能があり、直前の既知の構成に基づいてトラフィックのスイッチングを続行できるようになっています。したがって、VEM は高度なスイッチングによってデータセンターの信頼性を高めたサーバ仮想化環境を実現します。

Virtual Supervisor Module

Cisco Nexus 1000V シリーズ VSM は、複数の VEM を 1 つの論理モジュラ スイッチとして制御します。VSM は、物理的なライン カード モジュールの代わりに、物理サーバ内部のソフトウェアで実行される複数の VEM をサポートします。構成は VSM を通して実行され、自動的に VEM に伝達されます。管理者は、ハイパーバイザ内でソフト スイッチをホスト単位で設定する必要はありません。単一のインターフェイスで構成を定義して VSM で管理するすべての VEM に適用し、すぐに使用できます。

Cisco Nexus 1000V シリーズには、Cisco NX-OS の機能を利用した次のような利点があります。

- 柔軟性とスケーラビリティ：カテゴリ別にポートを構成する Cisco NX-OS の新機能、ポート プロファイルを利用すると、多数のポートを使用するようにソリューションを拡張できます。共通のソフトウェアを使用して、LAN や SAN など、データセンター ネットワークのあらゆる領域を実行できます。
- ハイ アベイラビリティ：同期機能と冗長性を備えた VSM により、迅速なステートフル フェールオーバーが行われるため、仮想マシン ネットワークのアベイラビリティが確実に維持されます。
- 管理性：Cisco Nexus 1000V シリーズには、Cisco CLI（コマンドライン インターフェイス）、Simple Network Management Protocol（SNMP）、XML API、CiscoWorks LAN Management Solution（LMS）経由でアクセスできます。

また、Virtual Supervisor Module は VMware vCenter Server とも統合されているため、仮想化の管理者は Cisco Nexus 1000V スイッチ内のネットワーク設定を利用することができます。

機能と利点

Cisco Nexus 1000V シリーズは、ポリシーベースの仮想マシン接続、仮想マシンのセキュリティおよびネットワーク プロパティのモビリティ、および中断のない運用モデルを備えたネットワーク インフラストラクチャ（物理か仮想かを問わず）に、単一の共通管理モデルを提供します。

ポリシーベースの仮想マシン接続

仮想マシンの作成およびプロビジョニングを簡素化するために、Cisco Nexus 1000V シリーズにはポート プロファイル機能があり、サーバ仮想化が持つ動的であるという特性に対して、ネットワークの観点から対処することができます（図 2）。ポート プロファイルを使用すると、VSM のさまざまな種類およびクラスの仮想マシン用に仮想マシン ネットワーク ポリシーを定義し、定義したプロファイルを VMware の vCenter GUI 経由で各仮想マシンの仮想 NIC（vNIC）に適用して、ネットワーク リソースの透過的なプロビジョニングを実行できます。ポート プロファイルは、多数の仮想マシンを含むネットワークを構成するためのスケーラブルなメカニズムです。

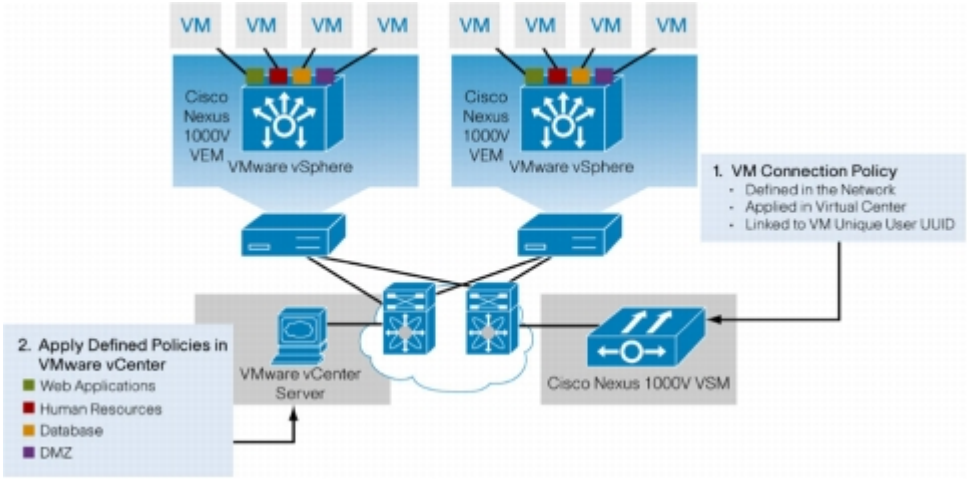

図 2 ポリシーベースの仮想マシン接続

モビリティのある仮想マシンのセキュリティとネットワーク ポリシー

ポート プロファイルで定義したネットワークおよびセキュリティのポリシーは、仮想マシンが別のサーバに移行されたり（図 3）、中断、休止、または再起動されても、仮想マシンをそのライフサイクル全体にわたって追跡管理します。ポリシーの移行に加えて、VSM は、ポート カウンタやフロー統計情報など、仮想マシンのネットワーク状態も移行します。トラフィック監視アクティビティに関与する仮想マシン（Cisco NetFlow や ERSPAN など）は、vMotion の動作によって中断されることなく、トラフィック監視アクティビティを続行できます。特定のポート プロファイルが更新されると、Cisco Nexus 1000V シリーズはそのポート プロファイルを使用しているすべての仮想ポートに対して自動的にライブ アップデートを実行します。ネットワークおよびセキュリティのポリシーを VMware vMotion 経由で移行する機能によって、物理サーバと同じ方法でセキュリティ ポリシーを定義し、Cisco Nexus 1000V シリーズで常に適用できるため、法規制

への準拠の徹底がはるかに簡単になります。

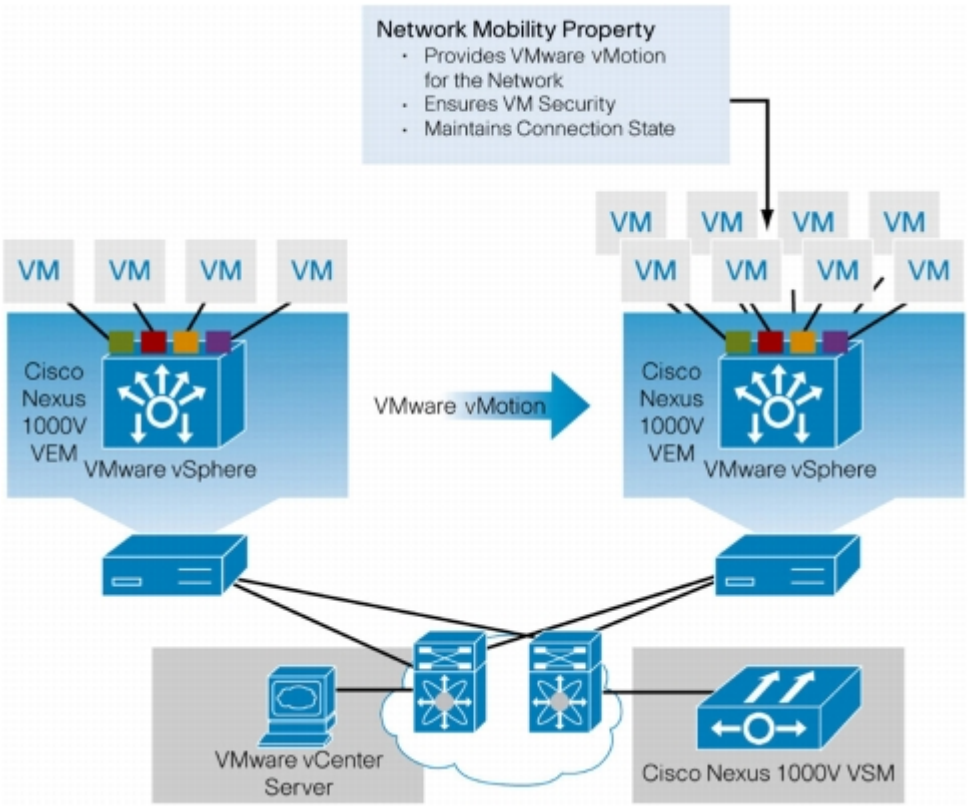

図 3 ネットワークおよびセキュリティのプロパティのモビリティ

中断のない運用モデル

Cisco Nexus 1000V シリーズは VMware vCenter Server と緊密に統合されているため、仮想化の管理者は仮想マシンのプロビジョニングに VMware ツールを引き続き使用できます。同時に、ネットワーク管理者は、Cisco CLI および SNMP を ERSPAN や NetFlow のようなツールと共に使用して、物理ネットワークと同じ方法で仮想マシン ネットワークのプロビジョニングと運用を実行できます（図 4）。両方のチームが使い慣れたツールを使用して別々に作業しながら、Cisco Nexus 1000V シリーズで一貫した構成とポリシーをサーバ仮想化環境に適用できます。このレベルで統合を行うことで、サーバ、ネットワーク、セキュリティ、およびストレージの各担当チーム間でさまざまな組織の境界を維持したまま、所有コストを削減できます。

VMware vCenter Server の内部では、仮想マシンは従来と同じように構成されます。vCenter Server でネットワーク構成を定義しなくても、VSM で定義されたポート プロファイルが vCenter によってポート グループとして表示されます。仮想化の管理者は、あらかじめポート グループを構成しておくことで、仮想マシン管理に注力できるようになり、ネットワーク管理者はポート プロファイルを使用して多数のポートにポリシーを一括適用できるようになります。2 つのチームが協力して、運用コストを抑えたサーバ仮想化をより効率的に導入できます。

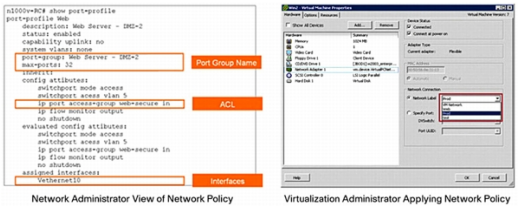

図 4 中断のない運用モデル
※画像をクリックすると、大きな画面で表示されます

Cisco vPath を使用した仮想化ネットワーク サービス

仮想マシン スイッチングに加えて、Cisco Nexus 1000V シリーズは、単一のアーキテクチャでレイヤ 4 ～ 7 の複数のネットワーク サービスをサポートする Cisco vPath に対応します。Cisco vPath アーキテクチャでは、仮想サービス ノードが仮想ファイアウォール、ロード バランシング、WAN アクセラレーションなど、さまざまなネットワーク サービスを提供できます。具体的には、Cisco vPath アーキテクチャによって、次が提供されます。

- インテリジェントなトラフィックの誘導
  - ネットワーク サービスを要求しているサーバから仮想サービス ノード（VSN）にトラフィックをリダイレクト
  - ネットワーク サービス プロファイルを含めるようにポート プロファイルを拡張
- 柔軟な導入
  - それぞれの VSN が複数の物理サーバにサービスを提供可能
  - 別のサーバ上や専用のサーバ上で VSN のホスティングが可能
- ネットワーク サービスの高速化
  - ネットワーク サービス ポリシーに基づくアクションのキャッシング：Cisco Nexus 1000V シリーズでは過去のトラフィックに適用したポリシーに基づくアクション（forward、drop など）が vPath にキャッシュされるため、すべてのパケットが仮想サービス ノードを経由する必要がなく、高速なサービスが実現可能
  - ハイパーバイザ カーネルの機能拡張によって仮想ネットワーク サービスのパフォーマンスの高速化が可能

図 5 では、仮想化ネットワーク サービスを必要としている VM 2 に VM 1 からパケットを送信すると、VEM が要求を VSN（異なるホスト上に存在していてもかまいません）に転送します。VSN は、適切なアクション（たとえば、このフローではパケットの送信または廃棄）を転送元の VEM に指示します。転送元の VEM は、VSN が要求したアクションのキャッシュと実行を行います。以降の VM 1 から VM 2 へのパケットでは、VEM は、VSN への要求を行わずに仮想化ネットワーク サービスを実装できます。このように、VEM は次のことを行います。

- 仮想化ネットワーク サービスのアクションの実行およびキャッシング
- ネットワーク サービスの高速化（ハイパーバイザ カーネル上で実行されているため）

- ネットワーク サービスの拡大（VEM はすべてのハイパーバイザのホスト上に存在するため）

さらに、VSN はどのホスト上にも配置できるので、柔軟性が増し、実稼働のワークロードとネットワーク サービスを分離することができます。つまり、vPath アーキテクチャは、さまざまなネットワーク サービスのサポートを目的として設計されています。

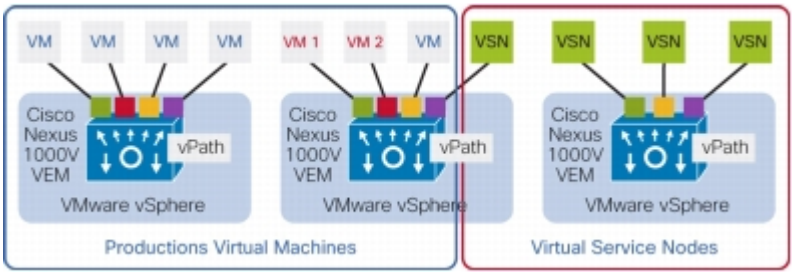

図 5 Cisco vPath アーキテクチャ

vPath を使用する最初の VSN は、Cisco Virtual Security Gateway（VSG）です。Cisco VSG によって、シングルテナント環境およびマルチテナント環境に、属性ベースのセキュリティ ポリシーが適用可能になります。Cisco VSG は仮想アプライアンスとして提供されるので、vPath アーキテクチャを使用し、導入する Cisco VSG アプライアンスの数を要求に応じて増やすことによって、導入規模を拡大できます。

vPath をサポートしないレイヤ 4 ～ 7 のサービスの仮想マシンを所有している場合にも、Cisco Nexus 1000V シリーズでは仮想サービス ドメイン（VSD）によって、ポリシーベースのプロビジョニングが可能になります。VSD によって、複数のサーバ上に存在する可能性がある仮想マシンを各ゾーンにグループ化し、レイヤ 4 ～ 7 のサービスの仮想マシン（ファイアウォールなど。VMware vShield Zones を含みます）を通じてゾーン間でトラフィックの送受信が行われるようにします（図 6）。Cisco Nexus 1000V シリーズでは、この拡張可能な機能によって、レイヤ 4 ～ 7 のさまざまなサービスが非常に使用しやすくなっています。

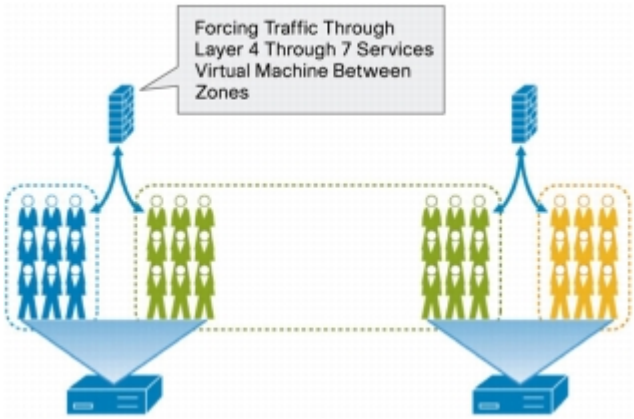

図 6 仮想サービス ドメイン

Cisco Nexus 1010 および 1010-X Virtual Services Appliance

VSM を仮想アプライアンスとして導入すると、特に電力とスペースが不足しているデータセンターにおいて高い柔軟性が得られます。ただし、VSM のホスティングに専用のコンピューティング アプライアンスを希望しているネットワーク管理者に対し、シスコは Nexus 1010 および 1010-X Virtual Services Appliance をご用意しています（図 7）。

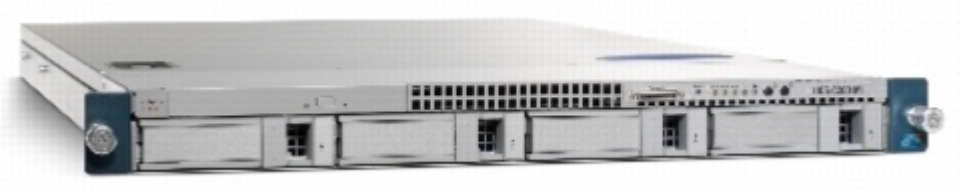

図 7 Cisco Nexus 1010 Virtual Services Appliance

Cisco Nexus 1010は、最大 6 台の VSM、および Network Analysis Module（NAM）などの追加の仮想サービス ブレードをホストするように設計されています。Cisco Nexus 1010-X は、最大 10 台の仮想サービス ブレードをサポートします。Cisco Nexus 1010 および 1010-X を使用すると、ネットワーク管理者は VSM を稼働させるためにサーバ管理者に依存する必要がなくなります。したがって、サーバ管理者とネットワーク管理者は、仮想化データセンターの導入において複雑性と相互依存性を緩和することができます。Cisco Nexus 1010 と 1010-X は追加の仮想サービス ブレードをホストできるため、追加の仮想サービス用のプラットフォームとなります（図 8）。

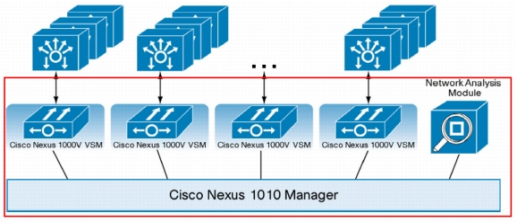

図 8 Cisco Nexus 1010 と 1010-X の内部アーキテクチャ
※画像をクリックすると、大きな画面で表示されます

サーバ仮想化とクラウド導入の最適化

差別化された QoS

今日において、ネットワーク インターフェイスが VMware Console や vMotion といった特定のトラフィック専用になっていることは珍しいことではありません。Cisco Nexus 1000V シリーズでは、サーバ上のすべてのネットワーク インターフェイス カード（NIC）を単一の論理チャネルと

して扱い、それぞれのトラフィック向けに QoS 機能を提供できます。VMware vSphere Version 4.1 を使用すると、Cisco Nexus 1000V シリーズで、実稼働の仮想マシンにさまざまなサービス レベル契約（SLA）を提供することもできます。これを活用することで、大量のトラフィックが生じるアプリケーションを仮想化して、サーバへのトラフィックに対する帯域利用率を効率化できます。

デスクトップのセキュアな仮想化

CPU パフォーマンスがムーアの法則に従っているのと同様、サーバ上で稼働している仮想マシンの数は、特に仮想デスクトップ環境では急速に増加しています。サーバ上に仮想マシンが多数存在すると、ウィルスやマルウェアに感染した仮想マシンから、同じサーバ上の他の仮想マシンに感染が急速に拡大する可能性があります。感染した仮想マシンが VMware vMotion によって別のサーバに移行され、ウィルスがさらに拡大する可能性もあります。したがって、仮想マシンにも物理サーバと同じセキュリティ ポリシーが必要です。

Cisco Nexus 1000V シリーズには、Cisco Integrated Security Features が含まれています。この機能はシスコの物理スイッチに搭載されており、さまざまな攻撃のシナリオを阻止します（表 1）。たとえば、不正な仮想マシンが MAC アドレスと IP アドレスのスプーフィングを行って既存の実稼働仮想マシンになりすまし、VMware vMotion による移行された仮想マシンの場所の通知方法を模倣した不正なアドレス解決プロトコル（ARP）トランザクションを送信し、実稼働の仮想マシンから不正な仮想マシンにトラフィックを転送する場合があります。Cisco Integrated Security Features によって、このタイプの攻撃はシンプルなネットワーキング ポリシーで簡単に阻止できます。デスクトップおよびサーバのワークロードにサーバ仮想化が使用されているので、仮想化環境を適切に運用するには、このタイプのセキュリティ機能の導入が非常に重要になります。

表 1 Cisco Integrated Security Features

機能	内容	阻止できること
ポート セキュリティ	ポートでの MAC アドレスの制限	不正な仮想マシンによる MAC アドレスのスプーフィング
IP ソース ガード	IP アドレスと MAC アドレスのマッピング	IP アドレスと MAC アドレスのスプーフィング
ダイナミック ARP インスペクション	仮想マシンの ARP トランザクションの監視（VMware vMotion にも使用される）	他の仮想マシン、ホスト、およびネットワーク デバイスで感染を拡大している ARP キャッシュ
Dynamic Host Configuration Protocol（DHCP）スヌーピング	• DHCP クライアントの要求が信頼されていないエンティティに到達することを阻止 • 信頼されていないエンティティが DHCP サーバとして機能することを阻止 • DHCP 要求のレート制限に	• 不正な DHCP サーバ • DHCP サービスに対するサービス拒絶

よりサービス拒絶
（DoS）攻撃を阻止

セキュアなマルチテナント機能

サーバ仮想化の機能では、異なるワークロードを単一のコンピューティング インフラストラクチャに統合することができます。ただし、このようなワークロードは、法規制の遵守またはコンプライアンスを目的として、論理的に分離されている必要があります。Cisco VSG などの仮想ファイアウォールを導入すると、このような論理的な分離を簡単かつ効率的に行うことができます。実際、このタイプの導入では、ビジネスのニーズに応じてワークロードを動的に作成できます。図 9 のように、Cisco Nexus 1000V シリーズと Cisco vPath を使用すると、このタイプの導入が Cisco VSG によってサポートされ、企業内に独自のプライベート クラウドを構築できます。

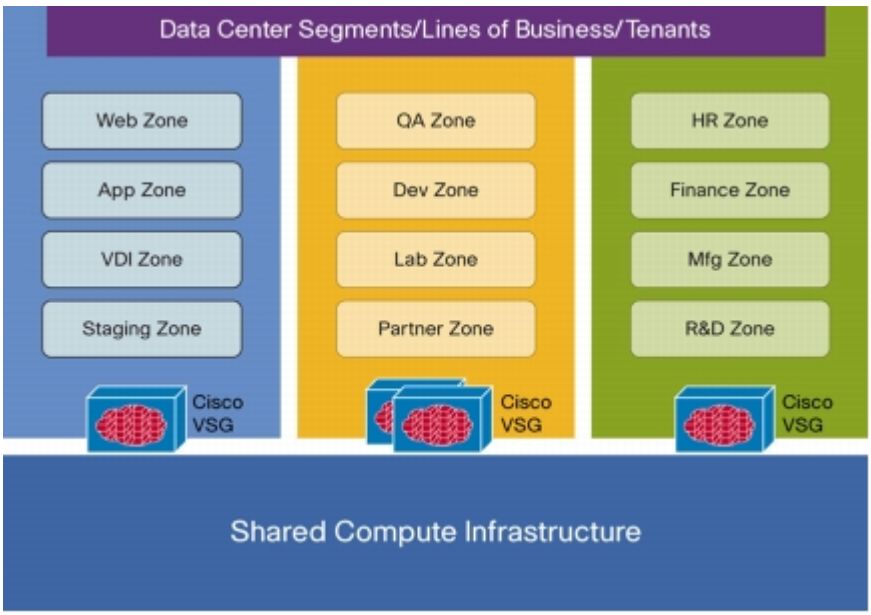

図 9 Cisco VSG をサポートする Cisco Nexus 1000V シリーズによるセキュアなマルチテナント機能

VXLAN によるクラウド ネットワーキング

クラウドベースのコンピューティングは多数の顧客とアプライアンスをサポートする必要があり、よりスケーラブルなネットワークが求められます。特に、テナントおよびそのアプリケーションごとに、他のネットワークから論理的に分離された独自のネットワークが必要です。一般的に、従来のサーバは適切に通信するために一意のネットワーク アドレスを持っていましたが、VMware vCloud Director はアプリケーションのインスタンスごとに仮想マシンのアドレスを複写します。したがって、VMware vCloud Director はアプリケーションのインスタンスごとに専用の論理ネットワークを必要とします。

このように論理ネットワークの必要性が増したため、シスコは Cisco Nexus 1000V シリーズに

Virtual Extensible Local Area Network（VXLAN）を導入しました。VXLAN では、仮想マシンがフレームを送信するときに、フレームは 24 ビットのセグメント ID とともにユーザ データグラム プロトコル（UDP）パケットにカプセル化されます。セグメント ID によってブリッジ ドメインが一意に識別され、専用の論理ネットワークが提供されます（図 10）。VXLAN では、アーキテクチャ上 1,600万までの論理ネットワークが可能になり、大規模なクラウド導入に対応できます。

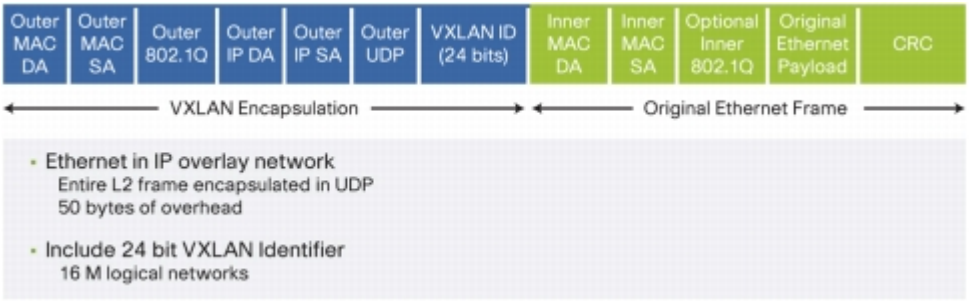

図 10 Virtual Extensible Local Area Network（VXLAN）

Cisco Nexus 1000V シリーズおよび VXLAN は、VMware vCloud Director と完全に統合され、新しいセグメントを迅速にプロビジョニングできます。さらに、VXLAN を使用した場合には次の利点があります（図 11）。

- UDP のレイヤ 3 の性質により、VXLAN トラフィックはレイヤ 3 の境界を越えることができます。
- クラウド コンピューティングのニーズに柔軟に対応できるように、新しいサーバを異なるレイヤ 2 ドメインに追加できます。したがって、VXLAN のアーキテクチャでは繰り返し使用可能なポッドによってクラウドの規模を拡張できます。
- Cisco Nexus 1000V と VXLAN は、物理ネットワークからクラウドまで一貫した運用モデルを実現します。
- クラウド プロバイダーはテナント単位でネットワーク ポリシーをカスタマイズし、提供するクラウド サービスを差別化することができます。
- VXLAN では、UDP カプセル化により PortChannel のリンクを効率的に使用します。

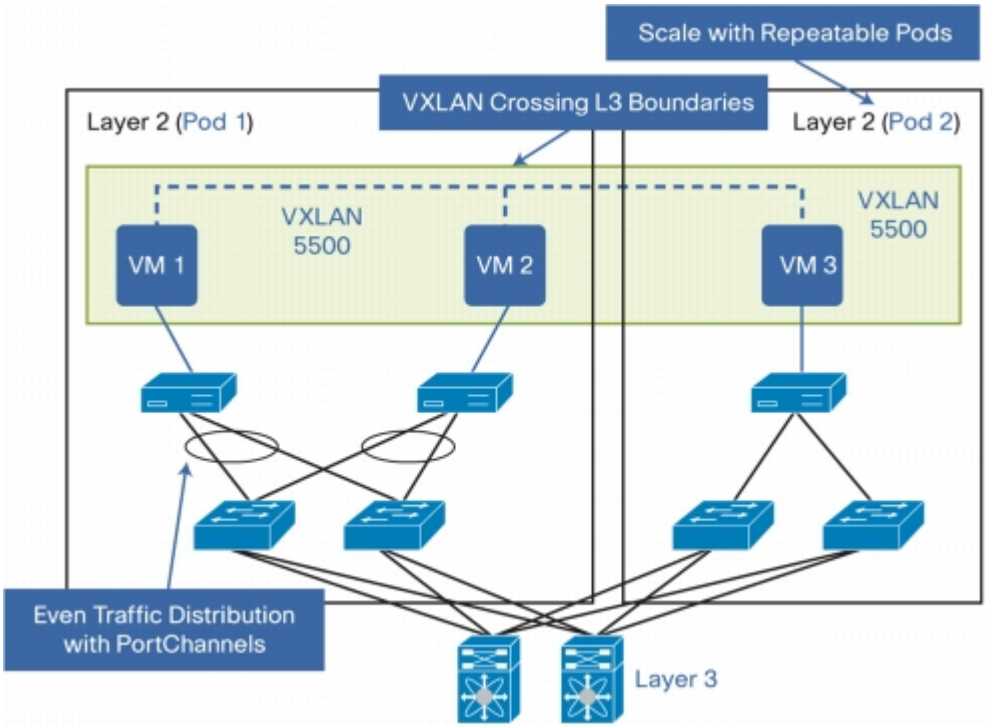

図 11 Cisco Nexus 1000V と VXLAN の利点

Cisco NX-OS ソフトウェアの概要

Cisco NX-OS ソフトウェアは、モジュール性、復元性、サービスアビリティを基盤として構築された、データセンター クラスの OS です。実績のある Cisco MDS 9000 SAN-OS ソフトウェアを基に開発された Cisco NX-OS ソフトウェアは、継続的なアベイラビリティの保証に役立ち、ミッションクリティカルなデータセンター環境の標準を確立します。自己修復機能を備え、高度にモジュール化された Cisco NX-OS は、ゼロインパクトの運用を現実化し、きわめて柔軟な運用を可能にします。データセンターの要件に特化した Cisco NX-OS は、現在および将来のデータセンターのイーサネットとストレージのネットワーキング要件を満たす、包括的な機能を備えています。Cisco IOS® ソフトウェアと同じ CLI を持つ Cisco NX-OS は、主要なネットワーキング標準およびシスコが持つ真のデータセンター クラスのさまざまな革新的技術を実装した、最先端の OS です。

Cisco NX-OS ソフトウェアの機能と利点

- ソフトウェアの互換性：Cisco NX-OS ソフトウェア リリース 4.0 は、Cisco IOS ソフトウェア OS を実行するシスコ製品との相互運用が可能です。また、サポート対象としてこのデータ シートに掲載されているネットワーキング標準に準拠したネットワーキング OS とも相互運用できます。
- データセンターに共通のソフトウェア：Cisco NX-OS は、データセンターの運用環境を簡素化します。統合 OS として、LAN、SAN、レイヤ 4 ～ 7 ネットワーク サービスなど、デ

ータセンター ネットワークのあらゆる領域を実行できるように設計されています。
- モジュラ式のソフトウェア設計：Cisco NX-OS のモジュラ式プロセスは、それぞれ別の保護メモリ領域内にオンデマンドでインスタンス化されます。したがって、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るのは、機能が新たに有効化されたときだけです。これらのモジュラ式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。
- インサービス ソフトウェア アップグレード（ISSU）：Cisco Nexus 1000V シリーズでは、サーバとネットワークの管理者が VEM と VSM のソフトウェアを透過的にアップグレードできるため、ダウンタイムが短縮され、ネットワーク運用にほとんどまたはまったく悪影響を与えることなく最新機能を統合できます。ネットワークとサーバの管理者は、別のメンテナンス ウィンドウでの作業中に VSM と VEM をアップグレードして、Cisco Nexus 1000V シリーズの運用を継続することができます。
- 拡張機能および問題修復プログラムの迅速な開発：モジュラ型という特徴を持つ Cisco NX-OS では、新機能、拡張機能、および問題修復プログラムを迅速にソフトウェアに組み込むことができます。したがって、モジュール化した修復プログラムの開発、テスト、実装を短時間で行うことができます。
- SNMP および XML API：Cisco NX-OS は、SNMPv1、v2、および v3 に準拠しています。さまざまな MIB がサポートされます。Cisco NX-OS には、文書化されたフル機能の XML API もあり、サードパーティの管理ツールとの統合が可能です。
- ロールベース アクセス コントロール（RBAC）：管理者がユーザにロールを割り当てることで、スイッチ操作へのアクセスを制限することができます。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。

製品仕様

互換性：VMware 製品

Cisco Nexus 1000V シリーズは VMware Ready Certified 認定を受けており、VMware ESX と ESXi ハイパーバイザ、および VMware vCenter Server との統合をサポートする vNetwork 分散スイッチとして VMware vSphere との互換性があります。

互換性：VMware vSphere 機能

Cisco Nexus 1000V シリーズは次の VMware vSphere 機能をサポートします。

- VMware vMotion
- VMware Distributed Resource Scheduler（DRS）
- VMware High Availability（HA）
- VMware Storage vMotion
- VMware Fault Tolerance（FT）
- VMware Update Manager
- VMware vShield Zones
- VMware Auto Deploy

サポートされる最大構成

- VSM あたりの VMware ESX または ESXi ホスト数：64
- VMware vDS あたりの仮想イーサネット ポート数：2048（物理ホストあたりの仮想イーサネット ポート数：216）
- アクティブな VLAN 数：2048
- ポート プロファイル数：2048
- 物理ホストあたりの物理 NIC 数：32
- VMware vDS あたりのポートチャネル数：256（物理ホストあたりのポートチャネル数：8）

レイヤ 2 機能

- レイヤ 2 スイッチ ポートおよび VLAN トランク
- IEEE 802.1Q VLAN カプセル化
- Link Aggregation Control Protocol（LACP）：IEEE 802.3ad
- レイヤ 2、3、および 4 の情報に基づいた高度なポートチャネル ハッシュ
  - 送信元 MAC アドレス（既定）
  - 仮想ポート ID
  - 宛先 IP アドレス、レイヤ 4 ポート
  - 宛先 IP アドレス、レイヤ 4 ポート、VLAN
  - 宛先 IP アドレス、VLAN
  - 宛先 MAC アドレス
  - 宛先レイヤ 4 ポート
  - 送信元/宛先 IP アドレス、レイヤ 4 ポート
  - 送信元/宛先 IP アドレス、レイヤ 4 ポート、VLAN
  - 送信元/宛先 IP アドレス、VLAN
  - 送信元/宛先 MAC アドレス
  - 送信元/宛先レイヤ 4 ポート
  - 送信元 IP アドレス、レイヤ 4 ポート
  - 送信元 IP アドレス、レイヤ 4 ポート、VLAN
  - 送信元 IP アドレス、VLAN
  - 送信元 MAC アドレス
  - 送信元 レイヤ 4 ポート
  - VLAN のみ
- 仮想 PortChannel ホスト モード
- 混合、独立、コミュニティ ポートを備えたプライベート VLAN
- トランク上でのプライベート VLAN
- Internet Group Management Protocol（IGMP）スヌーピング バージョン 1、2、3
- ジャンボ フレームのサポート、最大 9216 バイト
- スパニング ツリー プロトコルを使用しないブリッジ プロトコル データ ユニット（BDPU）フィルタを使用した、内蔵型ループ防止機能

QoS（仮想マシンのグラニュラリティを含む）

- 分類

    - アクセス グループ（ACL）
    - IEEE 802.1p CoS
    - IP Type of Service（ToS; タイプ オブ サービス）：IP precedence または DSCP（RFC 2474）
    - User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート
    - パケット長
- マーキング
    - Two Rate Three Color Marker（trtcm）（RFC 2698）
    - IEEE 802.1p CoS マーキング
    - IP Type of Service（ToS; タイプ オブ サービス）：IP precedence または DSCP（RFC 2474）
- トラフィック ポリシング（発信および着信レートの制限）
- クラスベース重み付け均等化キューイング（VMware vSphere 4.1 以降のバージョンのみ）
- Modular QoS CLI（MQC）準拠

セキュリティ

- イーサネットおよび仮想イーサネット ポートに対する入力/出力 ACL
- 標準および拡張レイヤ 2 ACL：
    - MAC アドレス、IPv4
    - 送信元 MAC アドレス
    - 宛先 MAC アドレス
    - EtherType
    - VLAN
    - Class of Service（CoS; サービス クラス）
- 標準および拡張レイヤ 3 ～ 4 ACL：
    - 送信元 IP
    - 宛先 IP
    - DSCP
    - Precedence
    - プロトコル（TCP、UDP、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）、IGMP）
    - 送信元ポート
    - 宛先ポート
    - TCP フラグ
    - ICMP、IGMP タイプ
    - ICMP コード
- ポートベース ACL（PACL）
- 名前付き ACL
- ACL 統計情報
- Cisco Integrated Security Features
    - ポート セキュリティ
    - IP ソース ガード
    - ダイナミック ARP インスペクション
    - DHCP スヌーピング
- 仮想サービス ドメイン（レイヤ 4 ～ 7 のサービスの仮想マシンが対象）

仮想化ネットワーク サービスのサポート

- Cisco vPath とレイヤ 2 およびレイヤ 3 は、Virtual Ethernet Module と仮想サービス ノード間の接続をサポートします。
- 仮想サービス ドメイン

VXLAN

- スケーラブルなネットワーク分離
- VMware vCloud Director と完全に統合
- ポート統計情報
- ポート セキュリティ
- ACL
- QoS
- Cisco vPath

ハイ アベイラビリティ

- ステートフル スーパーバイザ フェールオーバー：同期された冗長スーパーバイザが常にフェールオーバー可能な状態と一貫した信頼性の高い状態を維持します。
- ノンストップ フォワーディング：VSM と VEM の通信が失われても転送は継続されます。
- プロセスの存続可能性：重要なプロセスは独立して実行されるため、切り分け、障害の封じ込め、およびアップグレードが容易です。プロセスを個別にミリ秒単位で再起動でき、ステート情報の消失、データ転送への影響、または隣接デバイスやサービスへの影響が発生しません。

管理

- 仮想化およびネットワークの管理者用の VSM インストレーション ウィザード
  - VSM を VEM にインストール
  - 物理 NIC のポート プロファイルを作成
  - VSM のハイ アベイラビリティを設定
  - VSM から VEM への通信オプションを設定
- VSM と VEM 間のレイヤ 2 接続およびレイヤ 3 接続
- Cisco NX-OS CLI コンソール
- ISSU
- SPAN：物理インターフェイスのローカル ポートのミラーリング、ポートチャネル、VLAN、ポート プロファイル
- Enhanced Remote SPAN（ERSPAN）Type III：リモート ポートのミラーリング
- NetFlow Version 9（NetFlow データ エクスポート（NDE）付属）
- Cisco Discovery Protocol バージョン 1 および 2
- ACL のロギング
- SNMP（read）v1、v2、v3
- SNMP ACL
- XML（API）サポート
- 拡張 SNMP MIB のサポート

- SSH v2
- Telnet
- Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）
- TACACS+
- RADIUS
- Syslog
    - VMware vMotion イベントを含む
- RBAC
- インターフェイスごとの入出力パケット カウンタ
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）RFC 1305
- 管理インターフェイス用 Domain Name Services（DNS; ドメイン ネーム サービス）
- CiscoWorks LMS v3.1、v3.0.1、v2.6（サービス パック 1、SP1 を含む）

SNMP MIB

- 一般的な MIB
    - CISCO-TC
    - SNMPv2-MIB
    - SNMP-COMMUNITY-MIB
    - SNMP-FRAMEWORK-MIB
    - SNMP-NOTIFICATION-MIB
    - SNMP-TARGET-MIB
- 設定 MIB
    - ENTITY-MIB
    - IF-MIB
    - CISCO-ENTITY-EXT-MIB
    - CISCO-ENTITY-FRU-CONTROL-MIB
    - CISCO-FLASH-MIB
    - CISCO-IMAGE-MIB
    - CISCO-CONFIG-COPY-MIB
    - CISCO-ENTITY-VENDORTYPE-OID-MIB
    - ETHERLIKE-MIB
    - CISCO-LAG-MIB
    - MIB-II
- モニタリング MIB
    - NOTIFICATION-LOG-MIB
    - CISCO-PROCESS-MIB
    - CISCO-VIRTUAL-NIC-MIB
- セキュリティ MIB
    - CISCO-AAA-SERVER-MIB
    - CISCO-COMMON-MGMT-MIB
    - CISCO-PRIVATE-VLAN-MIB
- その他の MIB
    - CISCO-CDP-MIB
    - CISCO-LICENSE-MGR-MIB
    - CISCO-ENTITY-ASSET-MIB

サポートされる標準

表 2 に IEEE 準拠情報を、表 3 に RFC 準拠情報を示します。

表 2 IEEE 準拠

標準	説明
IEEE 802.1p	イーサネット フレームの CoS タギング
IEEE 802.1Q	VLAN タギング
IEEE 802.3	イーサネット
IEEE 802.3ad	Link Aggregation Control Protocol（LACP）

表 3 RFC 準拠

標準	説明
	IP サービス
RFC 768	UDP（User Data Protocol）
RFC 791	IP
RFC 792	ICMP（インターネット制御メッセージ プロトコル）
RFC 793	TCP
RFC 826	ARP（アドレス解決プロトコル）
RFC 854	Telnet
RFC 894	IP over Ethernet
RFC 1305	ネットワーク タイム プロトコル バージョン 3
RFC 1492	TACACS+
RFC 1591	DNS（ドメイン ネーム システム）クライアント
RFC 2068	HTTP サーバ
RFC 2138	RADIUS 認証
RFC 2139	RADIUS アカウンティング
	IP マルチキャスト
RFC 1112	IGMPv1 スヌーピング
RFC 2236	IGMPv2 スヌーピング
RFC 3376	IGMPv3 スヌーピング
	QoS（Quality of Service）
RFC 2474	DSCP マーキング
RFC 2698	Two Rate Three Color Marker

システム要件

- VMware vSphere Enterprise Plus バージョン 4.1 以降、VMware vSphere 5.0 をサポート
- VMware vCloud Director 1.5 以降との互換性
- Cisco Nexus 1000V シリーズ VSM：
  - VSM は VMware ESX/ESXi 3.5U2 以降、または ESX/ESXi 4.0 に仮想マシンとして導入可能
  - ハードディスク：3 GB
  - RAM：2 GB
  - 動作周波数 1.5 GHz の仮想 CPU x 1
- Cisco Nexus 1000V シリーズ VEM
  - VMware ESX または ESXi 4.0 以降
  - ハードディスク空き容量：6.5 MB
  - RAM：150 MB
- VSM と VEM 間のレイヤ 2 接続の VLAN の数：1
- VMware ハードウェア互換性リスト（ http://www.vmware.com/go/hcl/ [英語] ）に掲載されているサーバ
- アップストリーム物理スイッチとの互換性（すべての Cisco Nexus、Cisco Catalyst® スイッチ、および他のベンダー製のイーサネット スイッチを含む）
- VXLAN にはマルチキャスト（RFC 2236）をサポートする物理スイッチが必要

ライセンス/発注情報

Cisco Nexus 1000V シリーズのライセンスは、VEM を実行するサーバの物理 CPU 数に基づいて計算されます。表 4 に、Cisco Nexus 1000V シリーズの発注情報を示します。

表 4 Cisco Nexus 1000V シリーズ発注情報

製品番号	説明
N1K-VSMK9-404S12=	Nexus 1000V VSM 物理メディア
N1K-VLCPU-01=	Nexus 1000V 書面による CPU ライセンス パック：数量 1
N1K-VLCPU-04=	Nexus 1000V 書面による CPU ライセンス パック：数量 4
N1K-VLCPU-16=	Nexus 1000V 書面による CPU ライセンス パック：数量 16
N1K-VLCPU-32=	Nexus 1000V 書面による CPU ライセンス パック：数量 32
L-N1K-VLCPU-01=	Nexus 1000V eDelivery CPU ライセンス パック：数量 1
L-N1K-VLCPU-04=	Nexus 1000V eDelivery CPU ライセンス パック：数量 4
L-N1K-VLCPU-16=	Nexus 1000V eDelivery CPU ライセンス パック：数量 16
L-N1K-VLCPU-32=	Nexus 1000V eDelivery CPU ライセンス パック：数量 32

保証

Cisco Nexus 1000V シリーズにはソフトウェアに関する 90 日間の限定保証があります。Cisco Nexus 1000V シリーズの保証に関する詳細については、http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html [英語] を参照してください。

サービスおよびサポート

Cisco Software Application Support plus Upgrades（SASU）は、お客様のビジネスに不可欠なアプリケーションのアベイラビリティ、セキュリティ、パフォーマンスを保持および強化する上で有用な、包括的サポート サービスです。Cisco SASU には次のリソースが含まれます。

- ソフトウェアのアップデートとアップグレード：Cisco SASU サービスではソフトウェアのアップデートとアップグレードが適切なタイミングで中断なしに提供されるため、既存システムの安定性を維持し、ネットワークのリリース レベルを最新に保つことができます。アップデート リリースには、ライセンスをお持ちのフィーチャ セットに対する大規模なアーキテクチャの変更や新機能などを含むメジャー アップグレード リリースも含まれます。これらのアップデート リリースは、Cisco.com からのダウンロードか、CD-ROM の発送で提供されます。
- Cisco Technical Assistance Center（TAC）：シスコの TAC エンジニアは、機能停止時間の削減とパフォーマンス低下防止を実現するため、ソフトウェア アプリケーションの問題に関する正確な診断結果と解決策を迅速に提供します。エンジニアは全員ソフトウェア アプリケーションのエキスパートで、Cisco Nexus 1000V シリーズのサポートを提供するためのトレーニングを受けています。サポートは年中無休の 24 時間体制で、電話、ファックス、E メール、インターネットのいずれの方法でもお問い合わせいただけます。
- オンライン サポート：Cisco SASU には、問題の迅速な解決、ビジネスの継続性のサポート、競争力の強化に役立つさまざまなオンライン ツールやコミュニティが用意されています。

関連情報

- Cisco Nexus 1000V シリーズの詳細については、http://www.cisco.com/jp/go/nexus1000/ を参照してください。
- Cisco Nexus 1010 Virtual Services Appliance の詳細については、http://www.cisco.com/web/JP/product/hs/switches/nexus1000/nexus1010/index.html を参照してください。
- Cisco Virtual Security Gateway の詳細については、http://www.cisco.com/jp/go/vsg/ を参照してください。
- Cisco NX-OS ソフトウェアの詳細については、http://www.cisco.com/jp/go/nxos を参照して

ください。

- VMware vSphere の詳細については、http://www.vmware.com/jp/products/vsphere/ を参照してください。
- VMware vCloud Director の詳細については、http://www.vmware.com/jp/products/vcloud-director/ を参照してください。
- シスコと VMware の協力体制については、http://www.vmware.com/cisco/ [英語] を参照してください。

.