

Cisco Unified Network Service



シスコ ユニファイド ネットワーク サービス

サービスとネットワークおよびコンピューティングのオーケストレーションを実現



ユニファイド ネットワーク サービス

ビジョン

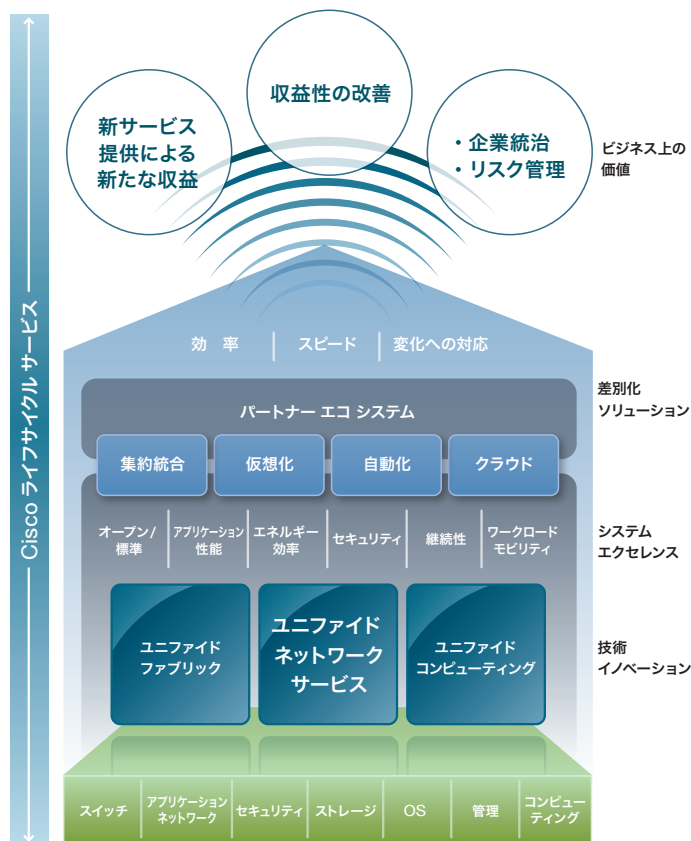
約3年前にシスコが発表した、シスコデータセンター3.0 (DC3.0) 戦略によって、データセンターの環境は統合化、仮想化さらには自動化といった面で大きな進化を遂げました。また同時に DC3.0 ではユニファイドファブリックやユニファイド コンピューティングといった、DC3.0 戦略を支える革新的なテクノロジーを市場に導入しました。

シスコが2010年9月に発表したデータセンタービジネスアドバンテージは、このDC3.0戦略をさらに発展させた、いわばアーキテクチャフレームワークであり、顧客のIT投資とそれによるビジネス上の効果との間に強い結びつきを実現します。

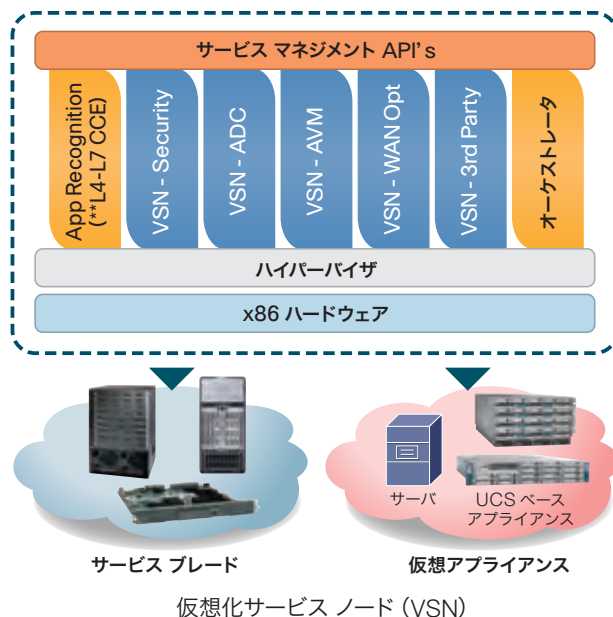
ユニファイド ネットワーク サービス (UNS) は、既存のユニファイド ファブリックやユニファイド コンピューティングと連携して、データセンター ビジネス アドバンテージアーキテクチャを支える革新的なテクノロジーの1つの柱になります。UNS アーキテクチャはサーバ ロードバランサーや WAN 最適化サービス、セキュリティといったネットワーク サービスを従来のアプライアンスに加えて仮想コンピューティング環境にも導入可能にします。さらに、ネットワークおよびコンピューティングとのオーケストレーションを実現します。

仮想化対応サービスの要件

UNS は単なる仮想化アプライアンスではありません。ネットワーク サービスが単にハードウェア プラットフォームに非依存に展開可能というだけでなく、クラウド サービスオペレータや大規模エンタープライズでの運用を想定した、オンデマンドのサービスのプロビジョニングや、VM モビリティに透過的なネットワーク ポリシーおよび、サービスポリシーの適用といったネットワークとサービスのオーケストレーション、さらにはスケールアウト、マルチテナント対応といった要件を満たしています。



データセンター ビジネス アドバンテージ アーキテクチャ

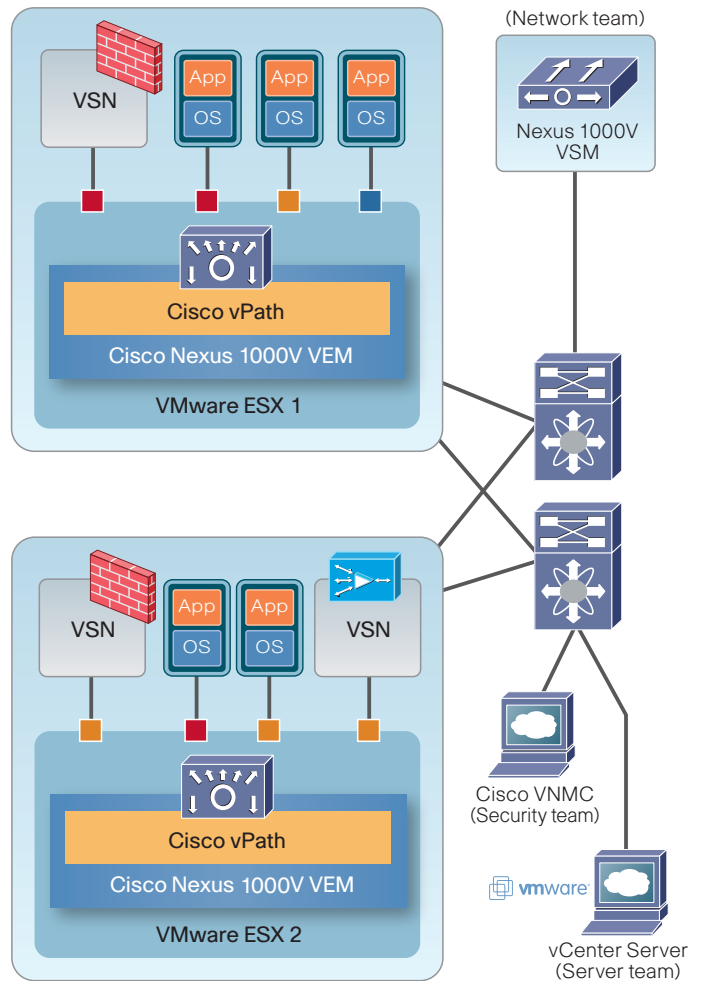


アーキ テクチャ

シスコ ユニファイド ネットワーク サービスは仮想化サービス インスタンス (VSN) ならびに、VM と VM 間および、VM と VSN 間のインテリジェントなトラフィックステアリングや VM モビリティに対するサービス透過性を実現する Cisco Nexus 1000V スイッチから構成されています。

また、マネジメントに関しては、従来からある VMware vCenter と Nexus 1000V VSM (管理モジュール) 間の連携に加えて、XML API を利用した、Cisco Virtual Network Management Center (VNMC) やサードパーティ製のオーケストレータとの連携による透過的な運用管理が可能です。

VSN には、ポリシーベースの VM セキュリティを実現する Virtual Security Gateway (VSG) と WAN とアプリケーション配信の最適化を行う virtual WAAS (vWAAS) をご用意しています。将来的にはこの他のサービスやサードパーティ製の VSN もサポートする予定です。



機能	概要	製品名
Virtual Services Node (VSN)	VM で動作するサービス インスタンスの総称。	Cisco Virtual Security Gateway (VSG: 仮想アプライアンス) Cisco Virtual WAAS (仮想アプライアンス)
Virtual Network Mgmt Center (VNMC)	VSG に関するセキュリティ ポリシー マネージャ。 VMware vCenter および、Nexus 1000V VSM と連携して VM モビリティに透過なポリシー管理を実現。	Cisco VNMC (仮想アプライアンス)
Nexus 1000V VEM	ESX ハイパーバイザ上で動作する仮想スイッチ。 リリース 1.4 からは VSN に関するトラフィックの効率的なルーティングを行う vPATH 機能を追加。	Cisco Nexus 1000V (ソフトウェア リリース 1.4 以降)
Nexus 1000V VSM	Nexus 1000V VEM の管理モジュール。 VM 上またはアプライアンスで動作可能。	Cisco Nexus 1000V (仮想アプライアンス) Cisco Nexus 1010 (VSM アプライアンス)

仮想化ネットワーク サービスの基盤

Cisco Nexus 1000V シリーズ スイッチ は、VMware ESX 環境用に開発されたインテリジェント ソフトウェア スイッチです。VMware ESX ハイパーバイザの内部で実行される Cisco Nexus 1000V は、Cisco VN-Link サーバ仮想化テクノロジーをサポートし、以下の特徴を備えています。

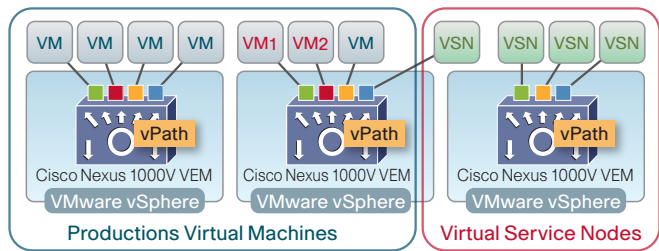


図 4-1 Cisco vPath アーキテクチャ

ポリシーベースの VM 接続

VM 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 にはポート プロファイルを用意しています。さまざまな種類およびクラスの VM 用に VM ネットワーク ポリシーを定義し、定義したポリシーを VMware vCenter 経由で各 VM の仮想 NIC 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。

VM のセキュリティおよびネットワークのプロパティのモビリティ

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、Cisco Nexus 1000V VSM によって VM が別のサーバに移動したり、中断、休止、または再起動されても、VM を追跡管理します。特定のポート プロファイルが更新されると、VSM 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。このため、vMotion による VM の移動に対してネットワークおよびセキュリティのポリシーを常に透過的に適用できます。

混乱を生じない運用モデル

Cisco Nexus 1000V は VMware vCenter Server と統合されているため、サーバ管理者は VM 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 のようなツールとともに使用して、物理ネットワークと同じ方法で VM 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。

Cisco vPath を使用した仮想化ネットワーク サービス

Nexus 1000V リリース 1.4 で追加された vPath アーキテクチャは仮想アプライアンスをより効果的に導入可能にするもので、インテリジェントなトラフィックのステアリング、ポート プロファイルを拡張したサービスの VM 移動に対する透過性などをサポートしています。vPath はマルチテナントに対応しているため、VM とそれをサービスする VSN は同一ホストにある必要はありません。例えば 図 4-1 では、仮想化ネットワーク サービスを必要としている VM2 へ VM1 からトラフィックを送信すると、vPath によって 1 番目のホスト上にある VSN へリダイレクトされます。

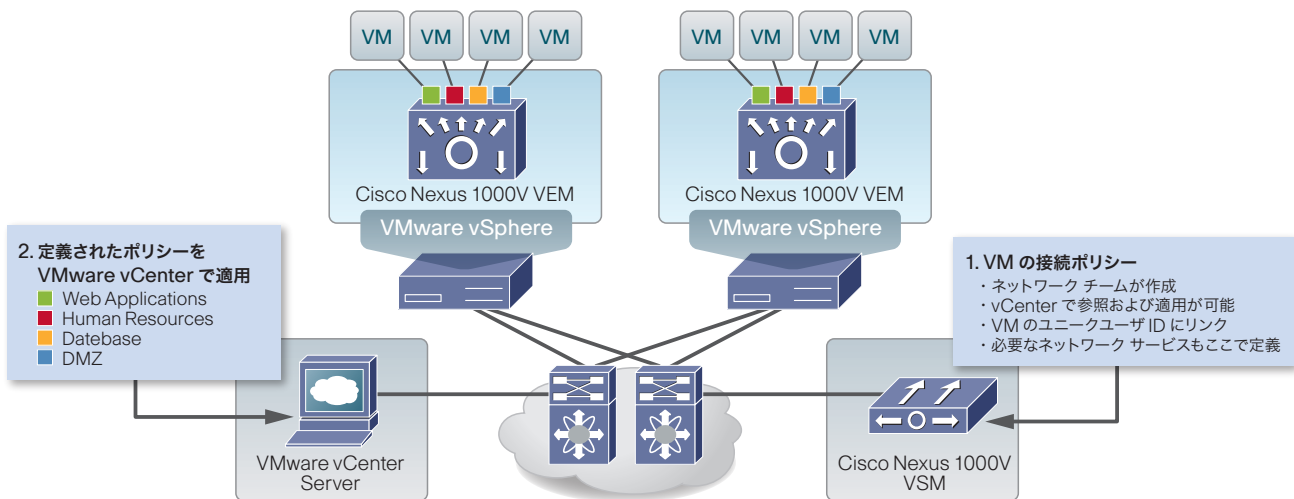


図 4-2 ポリシーベースの VM 接続性

ポリシーベースの VM セキュリティ

Cisco Virtual Security Gateway (VSG) は、企業およびクラウド プロバイダーの仮想化されたデータセンターにおいて、ポリシーベースのセキュリティを VM レベルで実現する仮想アプライアンスです。

Cisco VSG は、仮想化環境の保護と、優れた効率とアベイラビリティ、高パフォーマンスを実現する制御パスとデータパスの分割など、高度なネットワークのコンセプトの上に設計されています。Cisco VSG は、図 5-2 に示すように、Cisco Nexus 1000V シリーズ VEM に組み込まれた仮想ネットワーク サービス データパス (vPath) テクノロジーを利用します。

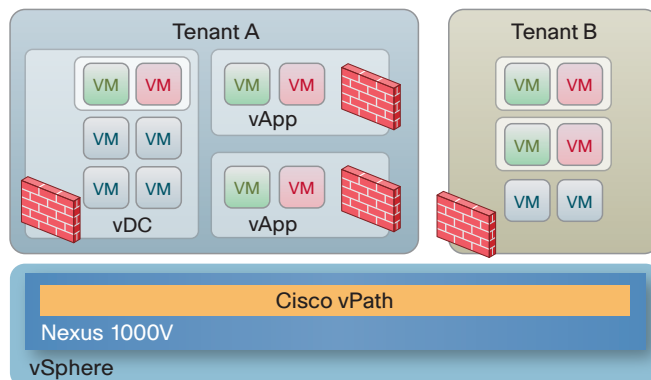


図 5-1 VSG による階層的なゾーニング

Cisco VSG と Nexus 1000V の組み合わせによる効果

効率的な展開

Nexus 1000V vPath がマルチテナントに対応しているため、VSG がどの ESX ホストに存在するかを意識する必要はありません。サーバごとに仮想アプライアンスを導入する必要がなくなります。図 5-2

高性能

Cisco VSG はフローの最初のパケットだけポリシーを評価し、そのアクションを vPath にキャッシュします。それ以降のパケットの処理は VSG を経由せず、vPath にオフロードされます。vPath は VEM の一部としてハイパーバイザに統合されているため、VM に比べて高いスループットが得られます。

簡素化された運用

Cisco VSG は、複数のスイッチを作成したり、仮想マシンを一時的に異なるスイッチやサーバに移行させることなく、ワンアームモードで透過的に挿入できます。ゾーンのスケールリングは、仮想アプライアンスに限定される仮想ネットワーク インターフェイス カード (vNIC) ではなく、セキュリティ プロファイルに基づきます。

ハイ アベイラビリティ

Cisco VSG は、アクティブ スタンバイ モードで展開できます。この方式では、アクティブな Cisco VSG が利用不可能になった場合に vPath がパケットをスタンバイ状態の Cisco VSG にリダイレクトするため、可用性の高い運用環境を実現できます。

独立したキャパシティ計画

Cisco VSG は、セキュリティ チームが管理する専用サーバへの配置も可能です。これにより、アプリケーションの作業負荷に見合ったコンピューティング能力の割り当て、サーバおよびセキュリティ チームから独立したキャパシティ計画の実施、セキュリティ、ネットワーク、およびサーバ チーム間の運用上の分離を維持することができます。

また、各 VM は複数のゾーンに所属することが可能となっており、テナント レベル、vDC レベル、vApp レベルといった階層的なゾーニングが可能です。図 5-1

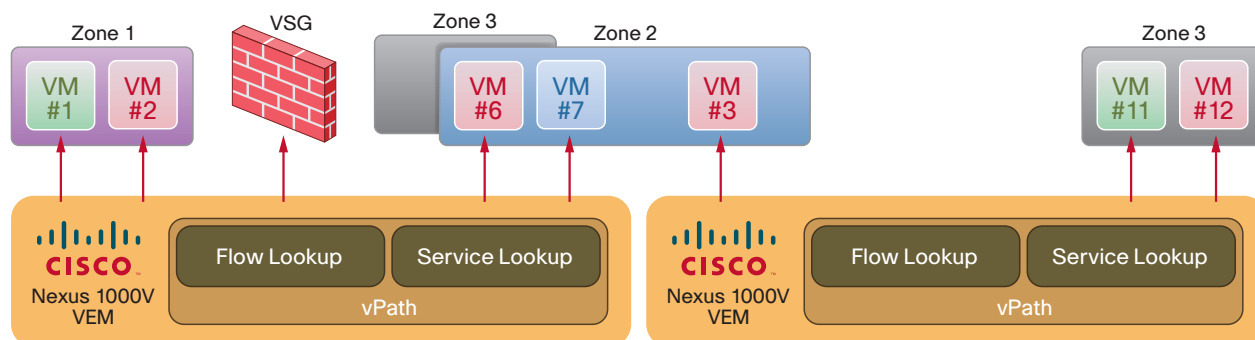


図 5-2 分散 VSG アーキテクチャ

Cisco VSG のセキュリティ ポリシーを一元管理

シスコ バーチャル ネットワーク マネジメント センター (VNMC) は Cisco Virtual Security Gateway (VSG) の管理用仮想 アプライアンスです。

Cisco VNMC は 企業やクラウド サービス オペレータのマルチ テナント環境に適用可能な拡張性、一貫したポリシーベースのオペレーション、XML API 経由の VMware vCenter、Nexus 1000V VSM およびサードパーティ製マネージャとの連携による自動化を実現しています。



多階層のセキュリティ ポリシー管理

セキュリティ プロファイルによる容易な管理

Cisco VNMC はセキュリティ ポリシーの設定にテンプレートベースのセキュリティ プロファイルを使用します。このセキュリティ プロファイルを事前に作成しておき、VM が生成された際オンデマンドで適用することができます。セキュリティ ポリシーの管理が非常にシンプルで一貫性を保つことができるため、大規模で多階層のマルチテナント環境のマネジメントを容易にします。

XML API による管理の自動化

Cisco VNMC は VMware vCenter と連携して VM コンテキスト アウェアなセキュリティ ポリシーを実現します。さらに Cisco VNMC は Cisco Nexus 1000V VSM とも連携してセキュリティ プロファイルをポート プロファイルにバインドするため、VM の生成や移動に対してポリシーを透過的に適用できます。

混乱を生じない管理モデル

Cisco VNMC はロールベースのアクセス コントロールを採用しており、既存の管理部門の境界の維持とマネジメントの自動化を両立しています。

- セキュリティ管理者はセキュリティ プロファイルの作成と管理を行います。前述のとおり、セキュリティ プロファイルは Nexus 1000V のポート プロファイルから参照可能です。
- ネットワーク管理者はポート プロファイルを作成、管理します。さらにポート プロファイルは VMware vCenter から利用可能です。
- サーバ管理者は VM 生成の際に必要なポート プロファイルを VMware vCenter から選択するだけです。

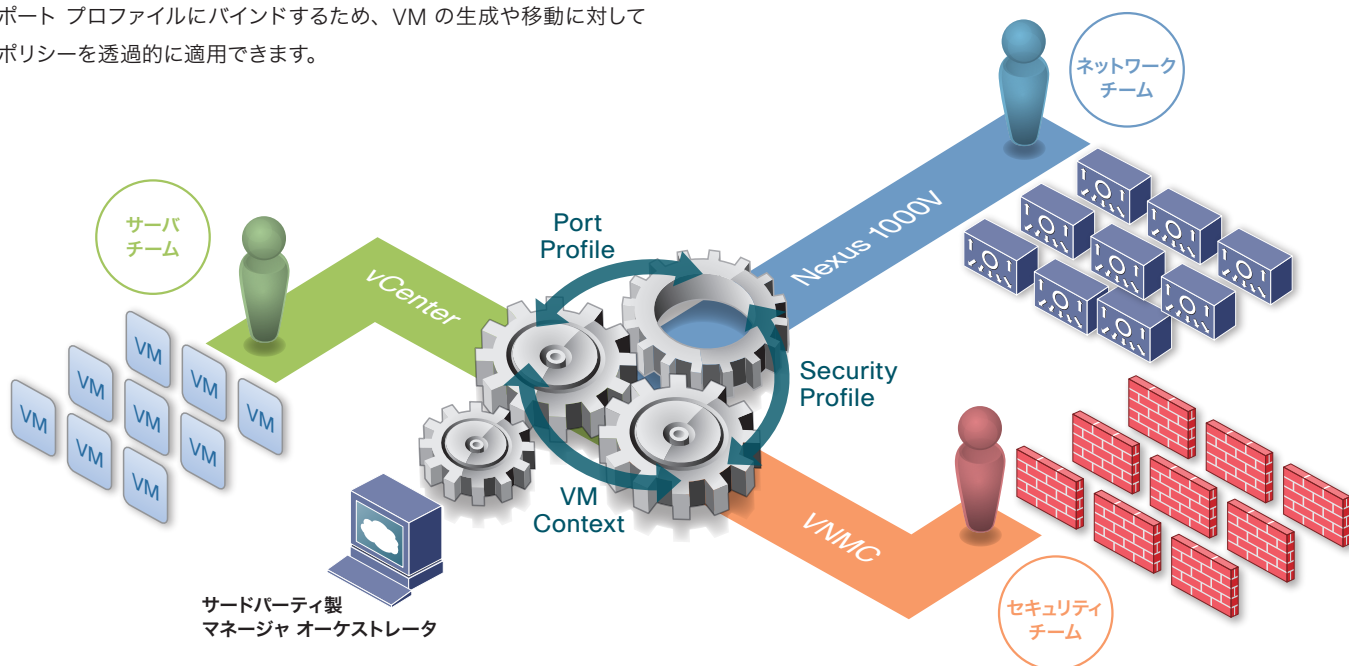


図 6-1 ロールベースの管理モデル

クラウドに最適な WAN 最適化ソリューション

Cisco vWAAS はオンデマンド サービス オーケストレーションを実現した、最初の WAN 最適化ソリューションです。仮想化アプライアンスとして提供され、主にプライベート クラウドやバーチャル プライベート クラウドからのアプリケーション配信を最適化します。

2 つの導入オプション

Cisco vWAAS は下記 2 つの方法で導入が可能です。図 7-1

1. WAN エッジにおいて Web Cache Control Protocol (WCCP) などのプロトコルを用いてトラフィックのインターセプションを行う方法 (従来のアプライアンスと同じ)
2. データセンター内部、アプリケーション サーバと同じ場所で Nexus 1000V スイッチと シスコ ユニファイド ネットワーク サービス フレームワークを利用してクラウドに最適化されたアプリケーション サービスを実現する

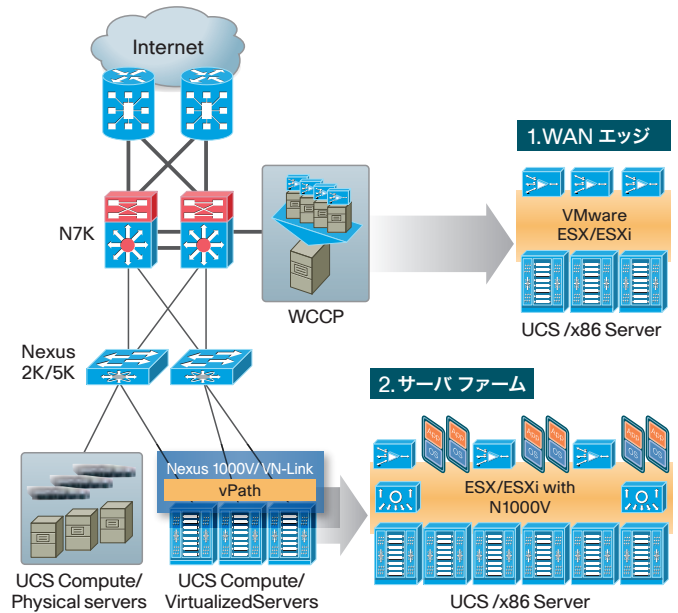


図 7-1 2 つの導入オプション

オンデマンド オーケストレーション

特に 2 番目の方法では、Nexus 1000V の特徴であるポリシーベースのコンフィグレーションにより、Cisco vWAAS サービスは、自動的にアプリケーション VM に関連づけられます。この関連づけは VM が生成されたときだけでなく、移動した場合にも引き継がれます。図 7-2 VM がどのホスト上にあっても、その入出力トラフィックは Nexus 1000V vPath によって関連づけられた vWAAS ヘルパーティングされます。このためクラウド事業者は最低限の設定を行うだけで、サービスに影響の少ない運用を行うことができます。

SAN のサポート

Cisco vWAAS は DRE キャッシュなどで利用するストレージとして新たに SAN をサポートすることで、物理アプライアンスと比較してより高い可用性を実現しています。

WAAS アプライアンスとの互換性を保証

Cisco vWAAS は既存の Cisco WAAS アプライアンスやブランチ ルータ統合型 (WAAS on ISR) との互換性を保証しています。また、仮想・物理アプライアンス共通のマネージャである、Cisco vWAAS センtral マネージャ (vCM) を仮想アプライアンスでご用意しています。

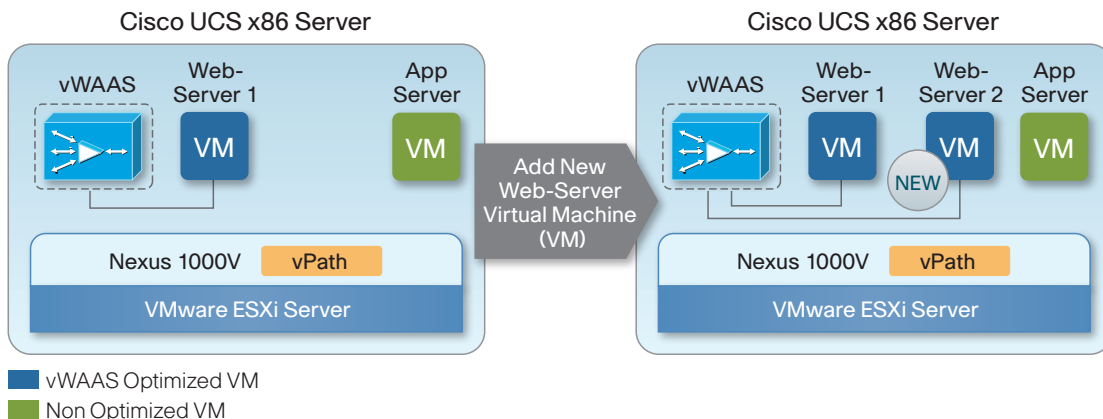


図 7-2 Nexus 1000V 連携によるオンデマンド オーケストレーション

シスコ ユニファイド ネットワーク サービスの詳細は、次のウェブサイトをご覧ください。 <http://www.cisco.com/jp/go/uns>

©2010 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は 2010 年 11 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS 含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

お問い合わせ先