

Making Everything Easier!™

VMware Special Edition

Network Virtualization FOR DUMMIES®

ネットワーク仮想化を
わかりやすく解説：

- ネットワーク仮想化の必要性
- ネットワーク仮想化の仕組み
- ベストプラクティスと導入方法

Brought to you by

vmware®

Mora Gozani



VMware, Inc.の概要

ヴァイエルムウェア（本社：カリフォルニア州パロアルト）は、クラウド インフラとビジネス モビリティの分野で業界をリードしています。VMwareの業界をリードする仮想化技術をベースとしたソリューション群を通じて柔軟性、俊敏性、安全性に優れたITの新しいモデルを実現します。顧客はあらゆるアプリケーションの開発の高速化、提供の自動化、安全な利用を実現することでこれまで以上にイノベーションを加速できます。VMwareは、50万社を超える顧客、および7万 5,000社を超えるパートナーを有し、米国カリフォルニア州シリコンバレーの本社のほか全世界にオフィスを展開しています。当社の2015年度の売上高は、66億米ドル以上です。

詳細については、www.vmware.com/jp をご覧ください。

***Network
Virtualization***
FOR
DUMMIES®

VMware Special Edition

Mora Gozani 著

WILEY

Network Virtualization For Dummies® VMware Special Edition

出版：

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030 - 5774

www.wiley.com

著作権 © 2016 by John Wiley & Sons, Inc., Hoboken, New Jersey

1976年著作権法の第107章、108章の下、出版社の書面による事前の許可がある場合を除き、本書のいかなる部分も複製してはならず、情報検索システムへの保管や電子、機械、コピー、録音、スキャンなどの形式を含む、いかなる手段での配信も一切認められないものとします。出版社に許可を依頼したい場合は、Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030宛てに郵送、(201) 748-6011まで電話、(201) 748-6008までファックス、または<http://www.wiley.com/go/permissions>からオンラインでお問い合わせください。

商標：Wiley、For Dummies、Dummies Manのロゴ、The Dummies Way、Dummies.com、Making Everything Easier、および関連するトレードドレスは米国またはその他の国に所在するJohn Wiley & Sons, Inc.および/または関連会社の商標または登録商標であり、許可がない限り、使用することは認められません。VMware、vSphere、およびvRealizeはVMware, Inc.の登録商標であり、VMware NSX、VMware vRealize Operations、およびvRealize AutomationはVMware, Inc.の商標です。その他の商標は全て、各商標所有者の財産であり、John Wiley & Sons, Inc.と本書で言及した製品やベンダーとの間には何ら関係がありません。

責任の制限/保証の免責：出版社および著者は、本書の内容に関して、その正確性、完全性、および特定の目的に対する適合性を含み、また、これに限らず、一切の責任を放棄し、保証も一切致しません。また、本書の販売や販促物により保証が適用されたり、その範囲が拡大されるようなことはございません。本書に記載のアドバイスを戦略は、状況により適切でない場合がございます。出版社が法律、会計、その他の専門サービスについてアドバイスを提供する業務に従事していないことを購入者の皆様にご理解頂いていることを想定して本書は販売されております。専門家のアドバイスが必要な場合は、定評のある専門家に相談ください。出版社および著者は、本書により生じた損害に対し、一切責任を負いません。引用および/または詳細な情報源として本書に記載されている企業やウェブサイトに関しましては、その企業やウェブサイトが提供または推奨する情報の正否を著者や出版者が保証するものではないです。また、本書に記載のインターネットウェブサイトが、本書が書かれた時分から読まれるまでの間に、変更される、または無くなる場合がございますことをご理解ください。

弊社の他の製品やサービスの基本情報、また、御社の事業や部門に合わせた「For Dummies」シリーズの制作については、米国の事業開発部までお電話（877-409-4177）またはメール（info@dummies.biz）にてお問い合わせいただくか、www.wiley.com/go/custompubをご覧ください。「For Dummies」ブランドの商品またはサービスを提供するためのライセンス供与に関する情報は、BrandedRights&Licenses@Wiley.comまでお問い合わせください。

ISBN 978-1-119-28414-7 (pbk); ISBN 978-1-119-28416-1 (ebk)

製作：アメリカ合衆国

10 9 8 7 6 5 4 3 2 1

謝辞

本書の出版にあたりご協力いただきました皆様に心より御礼申し上げます。

ディベロップメント エディター：

Becky Whitney

プロジェクト エディター：

Elizabeth Kuball

アキュイジション エディター：

Katie Mohr

エディトリアル マネージャー：

Rev Mengle

事業開発担当：Karen Hattan

Dummiesマーケティング：

Jennifer Webb

プロダクション エディター：

Siddique Shaik

目次

はじめに 1

本書の概要.....	1
対象読者	1
本書で使用するアイコン	2
本書について	2

第1章：ネットワークの新たな進化： Software-Defined Data Centerの登場 3

ビジネスにはスピードが不可欠	4
高まるセキュリティ要件	5
アプリの可搬性	6
ハードウェアベースのネットワークアーキテクチャでは、 SDDCに対応できない	7
ネットワークのプロビジョニングが遅い	7
ワークロードの配置や可搬性が制限される	8
ハードウェアの制限およびロックインによる 複雑さと柔軟性の低さ	9
マニュアル作業による設定プロセスで 時間がかかり、間違いが発生しやすい	9
運用コストおよび設備投資コストが高すぎる	10
ハイブリッドクラウドのリソースを活用できない	11
ネットワークの保護が不十分	12

第2章：ネットワークを仮想化するなら今 13

ネットワーク仮想化の仕組み	13
仮想ネットワーク VS Software-Defined Networking	18
仮想アプライアンス VS ハイパーバイザー内統合	19
なぜネットワーク仮想化のタイミングが今なのか	19
日々変化するビジネスニーズに応える	20
ハードウェアの抽象化で柔軟性を高める	20
ネットワークのマイクロセグメンテーションで セキュリティを強化	21
SDDCプラットフォームの構築	22
ネットワークの再考	22

第3章：ネットワークの変革25

仮想ネットワークの主な機能.....	25
オーバーレイ	25
VXLANの手引き	27
効果は絶大.....	29
VMware NSX：SDDC向けネットワークのご紹介.....	30
仕組み	30
NSXのアーキテクチャ.....	30
既存のネットワークインフラとの統合	31
ネットワークが簡単に	31
最高の柔軟性と拡張性.....	32
実現できること：NSXの主な機能.....	32
全てをソフトウェア上で	33
必要不可欠な分離、セグメンテーションに加え、 高度なセキュリティサービスを提供	33
パフォーマンスとスケーラビリティ	34
圧倒的なネットワーク可視性.....	35
VMware NSXの主なメリット	36
機能的なメリット	36
経済的なメリット	37

第4章：仮想ネットワークの用途39

データセンターのセキュリティ強化.....	39
データセンター内での水平移動を制限	40
データセンター内における East-Westトラフィックの増加.....	41
可視性とコンテキスト	41
分離.....	42
セグメンテーション	44
自動化	44
ユーザー環境の保護： VDIのマイクロセグメンテーション	45
ITプロセスの自動化	46
ITの自動化.....	46
開発者向けクラウド.....	47
マルチテナント型インフラ	47
アプリケーションの持続性を拡大	48
ディザスタリカバリ	48
メトロプーリング.....	48
ハイブリッド クラウド ネットワーキング	49

第5章：仮想ネットワークの運用 51

運用における投資分野	52
組織と人材	52
プロセスとツール	53
アーキテクチャとインフラ	55
大局的に見る	57

**第6章：ネットワーク仮想化を開始する
10（くらい）の方法 59**

基本的なリソースこそ大切に	59
基礎を叩き込む	60
細かく調べる	60
ブロガーとの交流	61
ハンズ オン ラボでNSXのテストドライブを試す	61
御社の環境にNSXをデプロイする方法を学ぶ	62
NSX製品ウォークスルーからプラットフォームの 全容を学ぶ	62
技術情報を詳細に見る	63
Cisco UCSおよびNexus 9000インフラを使ったNSXの 展開	64
既存のネットワークインフラへのNSXの統合	65
ネットワークサービスを提供する エコシステムパートナーとの統合	66



はじめに

.....

Network Virtualization For Dummies へようこそ。データセンターのネットワークを大幅に改善する斬新な方法をご紹介します。

ネットワーク仮想化の核心に迫る前に、まず、本書でカバーするトピックを簡単に説明しましょう。従来のハードウェアに組み込まれたネットワークから、仮想ネットワークが織りなす柔軟な世界へ移行するには、以下の要件を満たし、その土台を築く必要があります（第1章で詳述）。

- ✓ ビジネスと同様、ネットワークも迅速に動かす。
- ✓ ネットワークセキュリティでは、サイバー犯罪者が追いつけないほど先を行く。
- ✓ アプリケーションに、データセンター内を縦横無尽に動く柔軟性を備える。

さて、どのように実現させるのでしょうか。まずは、本書を使って、データセンターのネットワークを実現する新手法のコンセプトを探ってみることで。

本書の概要

薄い本だからと侮ることなかれ。本書には、ネットワークの仮想化を理解する上で役立つ情報が詰まっており、ネットワーク仮想化とは何か、なぜネットワークの仮想化が話題となっているか、運用を開始するにはどうしたらいいか、IT業務で最大の効果を上げるにはどうしたらいいかを分かりやすく簡単な言葉で説明します。

対象読者

本書を書くに当たり、どんな読者が本書を手取るか予想してみました。読者の皆様は、

- ✓ IT部門で働いており、
- ✓ ネットワーク用語をよくご存じで、
- ✓ 仮想化のコンセプトを理解しておられるのではないでしょう

本書で使用するアイコン

便利な情報を分かりやすくお伝えするため、本書では、以下のアイコンを使って重要なポイントをまとめています。



主な「学習」ポイントです。よくお読みください。



技術的な説明が必要な際にお読みください。



時間と手間を省くためのヒントを記載しています。

本書について

本書は参考書として書かれたものであり、最初から最後まで通して読む、関心のあるトピックから読むなど、どんな方法で読んで頂いても構いません。どんな方法で読んで頂いても、ネットワーク仮想化に関する理解を深め、ビジネスの俊敏性、データセンターのセキュリティ、アプリケーションの可搬性を高める上で確実に役立ちます。

第1章

ネットワークの新たな進化：Software-Defined Data Centerの登場

本章の内容

- ▶ Software-Defined Data Centerの概要
- ▶ ネットワーク仮想化のケースを構築する
- ▶ 現代のネットワークの課題を探る

なぜ、ネットワーク仮想化が大事なのでしょう。この質問の答えは、一つではありません。この章では、ある一つの包括的なニーズ、つまり、物理的に組み込まれていたネットワークの時代から、仮想ネットワークの時代への移行にまつわるいくつかのテーマを解説します。そのニーズの高まりの理由は次の通りです。

- ✓ 競争力の強化のために、企業にはSoftware-Defined Data Center (SDDC)の俊敏性が求められています。
- ✓ 時代遅れのネットワークアーキテクチャが、SDDCへの道を妨げています。
- ✓ 旧式のネットワークアーキテクチャは、企業の俊敏性を制限するほか、セキュリティの脅威をチェックできず、コストを増大させるばかりです。

SDDCは、ITサービスを提供する方法を根底から変化させます。SDDCによるアプローチによって、静的で柔軟性がなく非効率なデータセンターから、動的で俊敏性の高い最適化されたデータセンターへと変革させるのです。

この新しい世界では、データセンターインフラのインテリジェンスが仮想化によってハードウェアではなくソフトウェアで活用できるようになります。コンピューティング、ネットワーキング、ストレージを含めて、全ての IT インフラの要素が仮想化される上に、リソースのプールにグループ化され、ほとんど、あるいは全く人間の関与なしで、自動的にデプロイすることができます。全てが柔軟で、自動化されており、ソフトウェアによってコントロールされます。

SDDCでは、新しいアプリケーションをサポートするためのインフラの準備に数日あるいは数週間もの時間を費やすことはありません。アプリの起動、稼動を数分で行い、迅速に導入することができます。

ソフトウェアベースのアプローチは、ITの俊敏性を高め、より的確にITサービスを提供し、全てを低コストで実現できる素晴らしいフレームワークです。まさに、次世代データセンターの要と言えるでしょう。

Taneja Groupによる最近（2014年6月）の調査である「Transforming the Datacenter with VMware's Software-Defined Data Center vCloud Suite（VMwareのSoftware-Defined Data Center vCloudスイートによるデータセンターの変革）」では、SDDCがプロビジョニングや管理にかかる年間経費を56パーセント節約できることを明らかにしています。さらに、ソフトウェアベースのアプローチは、新しいアプリケーションの本番環境で使うネットワークの準備期間を3〜4週間程度から数分単位まで短縮することさえできるのです。

ビジネスにはスピードが不可欠

本章では、まず、ソフトウェアベースのデータセンターのメリットについて解説します。ポイントは、ハードウェアに基づくネットワークアーキテクチャでは、SDDCのスピードや俊敏性に對抗することはできないという点です。

大企業では、ビジネスが驚くべき速さで進み、変化の頻度は増すばかりです。全てにおいて大至急の対応が求められ、ITがどれだけビジネスをサポートできるかにかかっています。この新しい現実が、ネットワークに大きく影響を及ぼしていると言えるでしょう。

企業が新しいアプリで顧客をあっ！と言わせたい時、厳しい競合他社との競争に勝ち抜きたい時、あるいは新たな販売のルー

トを開拓したい時には、週や月の単位では間に合わず、ITサービスによる迅速なサポートが求められます。現在は、すぐにかるか、さもなければ失敗するかの選択しかなく、好機を逃してしまいがちなのです。

企業が重要なサービスをIT部門に依頼する時、聞きたいのは「分かりました。すぐに稼働可能にします。」という返事であって、決して「さて、まずネットワークにこれと、あれと、あれをする必要がありますので、今すぐにはできません。少なくとも2、3週間はかかります。」という弁解ではありません。それではビジネスニーズに対応できないのです。企業のリーダーがこうした話を聞くと、社内のIT部門ではなく、パブリッククラウドのプロバイダーからサービスを受けることを検討するでしょう。

ビジネスの速さは、決して衰えることはありません。チームが団結して、わずか7秒で車の全てのタイヤを交換し、燃料を補給するF1並みのスピードが必要なのです。つまり、より速く対応できるITが必要です。デジタル化が進んだ今、ネットワークには、ターボチャージャー搭載自動車並みのスピードで展開するビジネスに対応できるような変化が求められています。そのために、現在の物理的に組み込まれたネットワークへのアプローチを大きく変える必要があるのです。

高まるセキュリティ要件

若き日のボブ・ディランは「風向きを知るのに天気予報官はいらない。」と歌いました。現在、ネットワークセキュリティについて、ほぼ同じことが言えるでしょう。今日の企業では、ネットワークセキュリティの向上に対する強い要望の風が吹いています。

サイバー犯罪者の手に機密情報が渡るといった、非常にコストの高いセキュリティ違反を避けるには、より詳細な対応が必要なのは周知の事実です。そして、どんな企業もその脅威から逃れられません。ここ数年、巨大企業が攻撃され、メディアの見出しに取り上げられてきたセキュリティ違反を思い出してみてください。医療業界や投資銀行から小売、エンターテインメント業界まで、あらゆる企業がネットワークを保護するために非常にコストがかかる戦いに巻き込まれています。

まるで巨大なウォーゲームのようです。企業が強力な新しいファイアウォールでデータセンターを強化しても、サイバー犯罪

者は、あるクライアントシステムのシンプルな脆弱性を攻撃するなど、今まで知られていなかったバックドアからそっと忍び込み、データセンター内を自由に動き回ります。データセンターの内側も保護できるように、従来の境界を守る戦略を大幅にアップデートする必要があります。

戦略を練る間も、ブランド評価の低下や賠償額など、コストは上がり続けます。権威あるPonemon Instituteが2015年5月に発表したレポート、「2015 Cost of Data Breach Study: Global Analysis (2015年度データ漏洩調査：国際分析)」によると、データ漏洩の平均総コストは2014年で379万ドルに達しており、機密および秘密情報の紛失や盗難で支払われる平均費用は、6パーセント増の154ドルとなっています。

明らかに、何らかの対応が必要です。企業は、サイバー攻撃から身を守るために、より良いアーキテクチャを必要としており、それが仮想化によるネットワークの変革を後押ししています。

アプリの可搬性

仮想サーバーの登場により、多くのことが可能になりました。大きな進化として、アプリケーションは特定の場所にある単一の物理的サーバーに存在する必要がなくなり、今では、ディザスタリカバリ用のデータセンターへのアプリの複製や、社内データセンターから別のデータセンターへのアプリの移動、ハイブリッドクラウド環境へのスライドが可能になりました。

ただし、ネットワークへの配慮も重要です。昔のカウボーイの言葉を借りるなら、「進め！」といったところでしょうか。ネットワーク構成がハードウェアと結びついていると、たとえアプリが比較的容易に動くことができるとしても、物理的に組み込まれたネットワーク接続が足かせになりかねません。

ネットワークサービスは、例えば社内データセンターとクラウドのように、データセンターによって非常に異なる傾向があります。そのため、アプリが異なるネットワーク環境でも機能できるよう、多くのカスタマイズが求められ、アプリの可搬性を妨げる主な弊害となり、ネットワークの変革に仮想化を活用するもう一つの要因ともなります。

ハードウェアベースのネットワークアーキテクチャでは、SDDCに対応できない

SDDCは、最新のデータセンターにも対応する最も俊敏で、即応性が高いアーキテクチャです。これは、全てのインフラ要素のインテリジェンスがソフトウェアで稼動することで実現されています。それでは、最新の状況を確認してみましょう：

- ✓ 現在、大部分のデータセンターが、サーバー仮想化によって非常に効率の高いコンピューティング環境を実現しています。
- ✓ 現在、多くのデータセンターが、仮想化によってストレージ環境を最適化しています。
- ✓ ネットワーク環境を仮想化しているデータセンターはほとんどありません。

多くの企業はサーバーやストレージの仮想化を活用する中で、初代データセンターの頃から存在するハードウェア中心の、マニュアル作業によるプロビジョニングに頼ったレガシー型ネットワークインフラから生じる課題に悩まされています。

ここからは、こうしたレガシー型アーキテクチャの課題をいくつか取り上げます。

ネットワークのプロビジョニングが遅い

確かに、ハードウェアベースのシステムでも、一部のネットワーク プロビジョニング プロセスはスクリプト化できます（Software-Defined Networkはもちろんこれを実現します）が、仮想化されたコンピューティングやストレージとの連携は自動化されていません。結果として、関連するコンピューティングやストレージの作成、移動、スナップショット、削除、およびクローンの作成を行うネットワークを自動的にプロビジョニングする方法がなく、自動化ツールを活用しても、ネットワークのプロビジョニングは遅いままです。

結果として、ビジネスにとって最も重要である、新しいアプリの迅速な稼動は、ネットワークサービスのプロビジョニングにかかる時間とマニュアル作業による間違いの多いプロセスのためにはしばしば遅れていました。

全体の構図から考えると、これは非常に皮肉なことです。レガシー型ネットワークの制約が、現在の動的な仮想環境を、柔軟性がなく融通が利かないハードウェアへ縛り付けており、迅速に再利用されるべきサーバーやストレージのインフラが、ネットワークが追いつくのを待たなければならないのです。こうしてプロビジョニングは、まるで大きな「急いで片付けてあとは待つ」ゲームのようになってしまいます。つまり、不測の事態を想定し、余裕をもったプロビジョニングを行う必要があります。

ワークロードの配置や可搬性が制限される

今日の動きの速いビジネス環境ではアプリの俊敏性が不可欠であり、ある場所から別の場所へ速やかに移動できなければなりません。これには、オフサイトのバックアップとリカバリ用のデータセンターへの複製、社内データセンター内での移動、あるいはクラウド環境への出入りなどが含まれます。

サーバーおよびストレージの仮想化は、このような可搬性を実現しますが、ネットワークについても対応が必要です。現在の物理的に組み込まれたネットワークのサイロは、アプリの可搬性の妨げになっており、仮想マシン内のワークロードでさえ、物理ネットワークのハードウェアやトポロジーに繋ぎ止められています。問題を難しくしているのは、異なるデータセンターが、異なるネットワークサービスを採用していることです。そのため、データセンターAで最適なパフォーマンスで動作しているアプリをデータセンターBで適切に設定するには非常に困難な作業が必要になります。

これら全てが、ワークロードの配置やアプリの可搬性を制限し、変更を困難で危険なものにします。結局、単に今まで通りにしておくことが、最も簡単で、最も安全な方法ということになるのです。



現在のハードウェア中心のネットワークへのアプローチは、ワークロードの可搬性を個々の物理サブネットやアベイラビリティゾーンに制限します。データセンターで利用可能なコンピューティングリソースにアクセスするには、ネットワークオペレーターはスイッチング、ルーティング、ファイアウォールルールをボックス毎に設定しなければなりません。このプロセスは、遅く複雑であるだけでなく、たとえば、LAN 1個あたり VLAN 4,096個という技術的な制限の壁に結果として突き当たってしまいます。

ハードウェアの制限およびロックインによる複雑さと柔軟性の低さ

現在の閉鎖的でブラックボックス化しているネットワークへのアプローチ（カスタム オペレーティング システム、ASIC、CLI、管理を含む）は、オペレーションを複雑化させ、俊敏性を制約します。こうした古いアプローチは、現在のハードウェアへのロックインを増長させるだけでなく、ネットワークのアーキテクチャをますます複雑なものにし、IT部門の対応力や、革新を阻むものです。そして、ビジネスはITのスピードに合わせざるを得ないため、ビジネス自体にも同じ制約が課されるのです。

Dynamic Marketsによる「Network Agility Research 2014（2014年度ネットワークの俊敏性調査）」によると、企業の90%がネットワークの複雑さによる不利益を被っており、それはいつ、どこで、どのようなアプリケーションやサービスをデプロイするかに影響を与えています。同調査からは、次のような点も明らかになっています：

- ✓ IT 部門は、平均して、12カ月で10の変更を社内ネットワークに行っており、それぞれにメンテナンス期間を設ける必要があります。メンテナンスが完了するまでの期間は、それぞれ平均27日です。
- ✓ IT部門によるサービスの刷新や改善に、年間合計で270日から最長9.6カ月もの期間を要しています。
- ✓ 大規模企業では、より多くの変更が必要となり、さらに長いメンテナンス期間も必要となります。

マニュアル作業による設定プロセスで時間がかかり、間違いが発生しやすい

物理ネットワークでは、ネットワークチームが日常的に単調なマニュアル作業を強いられます。業務部門から新しいアプリケーションやサービスの要請を受けると、VLAN の作成からスイッチやアップリンクにわたる VLAN のマッピング、ポートのグループ化、サービスプロファイルの更新まで、膨大な作業が必要になるのです。しかも、多くの場合、設定作業は扱いにくいCLIによって行われます。

第2章で説明するSoftware-Defined Network (SDN) の発展により、プログラムによってハードウェアを制御することが可能になりますが、それでもまだ多くの困難な仕事が残ります。例えば開発、

テスト、本番環境の各チームをサポートするために同一のネットワークを複数構築する必要は依然として残り、仮想化されたコンピューティングやストレージによって、（ハードウェアベースの）ネットワークをデプロイできるわけでもありません。

さらに、他の問題もあります。このようなマニュアル作業による設定作業は間違いやすく、実際、ダウンタイムの主な原因はマニュアル作業によるエラーです。度重なる調査により、ネットワーク事故の最大の原因は、人的ミスによる設定エラーであると発表されており、その割合は32～33.3%に及びます（33.3%はDimension Dataのレポート「2015 Network Barometer Report（2015年度ネットワークバロメーター調査）」の推定であり、32%は、Ponemon Instituteのレポート「2013 Cost of Data Center Outages（2013年度データセンターのダウンタイムによる損害）」の推定に因る）。

運用コストおよび設備投資コストが高すぎる

レガシー型ネットワークアーキテクチャにおける制限は、データセンターの運用コスト（OpEx）および設備投資コスト（CapEx）を上昇させます。

運用コスト

マニュアル作業によるプロセスを頻繁に使用すると、ネットワークの運用コストが上昇するにも拘わらず、物理ネットワークの構成、プロビジョニング、管理には膨大なマニュアル作業が必要です。サポートする必要がある全ての環境全体をカバーするには、このような作業工数は何倍にもなり、その対象は開発、テスト、ステージングおよび本番環境から、異なる部門ネットワーク、アプリケーション環境、プライマリサイトとリカバリサイトなど多岐にわたります。自動プロセスなら数分で、もしくはネットワークの自動デプロイなら瞬時に完了するようなタスクでさえ、マニュアル作業では数時間、数日、時には数週間かかるのです。

さらに、マニュアル作業が原因で発生する設定エラーに伴う隠れたコストもあります。一つの間違いが、ビジネス全体に影響を与える、重大な接続の問題やシステムの停止を引き起こすことさえあるのです。計画外のデータセンター停止による財務的影響は、時に莫大です。Dynamic Marketsによる「Network Agility Research 2014（2014年度ネットワーク俊敏性調査）」で報告されている事故による平均停止時間は86分で、1分当たり7,900ドルものコストが費やされており、一件の事故当たりの平均総コストは690,200ドルにもなります。

設備投資コスト

設備投資面ではどうでしょう。レガシー型ネットワークアーキテクチャでは、データセンター運用の基礎となる多くのネットワーク機能やセキュリティの機能において、スタンドアロン型のソリューションに対する投資が必要となります。これにはルーティング、ファイアウォール、ロードバランサーなどが含まれ、必要な全ての場所で、これらの機能を提供するには、多大な費用がかかります。

また、ピーク需要に対応するためのハードウェアのオーバープロビジョニングや、アクティブ/パッシブ設定のデプロイという問題もあり、実質的には、可用性を確保するために2倍のハードウェアを購入する必要があるのです。

そして、フォークリフトアップグレードのコストもあります。最新のネットワークテクノロジーを活用するには、多くの企業のネットワークオペレーターが3～5年の更新サイクルでレガシー型の機器を交換しなければなりません。また、ハードウェアに基づくレガシー型ネットワークアーキテクチャでは、突発的な需要に対処するため、オーバープロビジョニングも必要となります。ハードウェアベースのネットワークでは、要求に基づいて自動的に拡張できないため、非効率적となり、ネットワークのコストが上昇するのです。

また、レガシー型ネットワークアーキテクチャが、違う形で非効率性を引き起こすこともあります。多くの場合、ネットワーク設計者は、個別のセキュリティやコンプライアンスの要件に対応するために、ネットワークの一部を確保しなければなりません。オーバープロビジョニングのニーズと併せ、必要かどうかも定かでないままに、「念のため」、「ダークサーバー」を配置せざるを得ず、非効率性はさらに加速してしまいます。その結果、ひどく断片化されたハードディスクのようになるのです。

ハイブリッドクラウドのリソースを活用できない

クラウドサービスのプロバイダーにより、アプリケーションやサービスを要求に応じてプロビジョニングできるようになり、企業は、場所を問わず、同じレベルのスピードと俊敏性を享受したいと望むようになりました。このような状況下で、先見性のある経営陣は、データストレージやディザスタリカバリからソフトウェアの開発やテストまで、あらゆるケースでハイブリッドクラウドを使うことを検討しています。

ただし、ここでもネットワークに関連して考慮すべきポイントがあります。クラウドへの移行を探る中で、企業はベンダー指定のネッ

トワークハードウェアと物理トポロジーによって縛られるのです。レガシー型データセンターアーキテクチャに付き纏うこうした制約が、ハイブリッドクラウドの導入を難しくするのです。ハイブリッドクラウドは、オンプレミスのデータセンターをパブリッククラウドのリソースにシームレスに拡張できることが特長ですが、ハードウェアのネットワークシステムをミラーリングしてパブリッククラウドのネットワークを制御することができない場合、パブリッククラウドのメリットを実現する手立てはありません。

ネットワークの保護が不十分

近年公表されたサイバー攻撃の多くには、ある共通点があります。データセンターの境界内で、悪意のあるコードがサーバーからサーバーへ移り、機密データを集めて、サイバー犯罪者に送っていたのです。これは、ネットワークセキュリティの統制に限度があり、攻撃がデータセンター内で広がることを食い止められないという今日のデータセンターの脆弱性を浮かび上がらせました。

境界ベースのファイアウォールは、多くの攻撃を食い止めますが、全てを止めることはできません。最近の攻撃から分かるように、依然として脅威は合法的なアクセスポイントからデータセンターに入り込み、中に入った途端、致命的なウイルス性疾患のように拡散するのです。この問題は、物理ネットワークアーキテクチャの実態から判断して、解決しようのないものでした。簡単に言えば、レガシー型ネットワークシステムで、データセンター内の全てのワークロード間でのトラフィックにファイアウォールを設置するには、コストがあまりに高額で、East-West トラフィックを使って攻撃がサーバーからサーバーへと水平方向に広がるのを止めるのは困難なのです。

それでは、まとめましょう。ここまですべて重要なポイントは次の通りです。

- ✓ 企業の競争力を維持するには、Software-Defined Data Centerの俊敏性が必要です。
- ✓ 時代遅れのネットワークアーキテクチャが、SDDCへの道を妨げています。
- ✓ 旧式のネットワークアーキテクチャは、企業の俊敏性を制限し、セキュリティの脅威をチェックしきれず、コストを増大させるばかりです。

以上のことから、物理的に組み込まれたネットワークの時代から、仮想ネットワークの時代への移行が求められていることが分かります。

第2章

ネットワークを 仮想化するなら今

本章の内容

- ▶ ネットワーク仮想化の基本
- ▶ 仮想化という新しいアプローチで得られる利益
- ▶ 仮想ネットワークの主な特長

本章では、ネットワーク仮想化のコンセプトを掘り下げます。仮想ネットワークとは何か、ネットワークに対する他のアプローチと何が違うのか、なぜ今がチャンスなのか説明しましょう。

まず、大局的な視点から、現代のネットワークの最先端を行くネットワーク仮想化の背景から今に至るまでを見てみましょう。

ネットワーク仮想化の仕組み

仮想ネットワークは、プログラムにより構築、プロビジョニング、および管理が可能で、基盤となる物理ネットワークをシンプルなパケット転送バックプレーンとして活用します。ソフトウェアのネットワークおよびセキュリティサービスはハイパーバイザーを介して提供され、接続されたアプリケーションを規定するネットワークポリシーおよびセキュリティポリシーに従って個々の仮想マシン（VM）に「アタッチ」されます。仮想マシンが他のホストに移動すると、そのネットワークおよびセキュリティサービスも共に移動します。また、アプリケーションの規模を広げるために新規仮想マシンを作成すると、新規仮想マシンにも必要なポリシーが動的に適用されます。

仮想マシンが論理的なコンピューティングサービスをアプリケーションに提供するソフトウェアコンテナであるのと同様、仮想ネットワークは接続されているワークロードに論理スイッチ、ルーター、ファイアウォール、ロードバランサー、VPNなどの論理ネットワークサービスを提供するソフトウェアコンテナです。これらのネットワークおよびセキュリティサービスは、ソフトウェア上で実行され、必要なのは下位の物理ネットワークによるIPパケット転送のみです。ワークロードはソフトウェア版の物理ネットワーク「ワイヤ」を通して接続されます。これにより、ネットワーク全体をソフトウェア上で構成することが可能になります。（図2-1参照）。

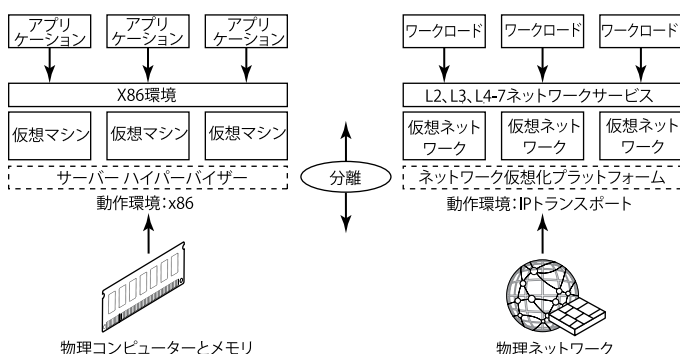


図 2-1： コンピューティングとネットワークの仮想化

ネットワークの仮想化により、サーバーハイパーバイザー内の仮想スイッチと接続された仮想マシン向けのネットワークサービスが連動し、効率よくプラットフォーム（またはネットワークハイパーバイザー）を稼働させ、仮想ネットワークを構築できます（図2-2参照）。

仮想ネットワークをプロビジョニングする方法の1つに、クラウド管理プラットフォーム（CMP）を使用して、対応するワークロード用の仮想ネットワークおよびセキュリティサービスを要求することが考えられます。これを行うと、コントローラーが対応する仮想スイッチに必要なサービスを配置し、対応するワークロードに論理的にアタッチします（図2-3参照）。

このアプローチでは、様々な仮想ネットワークを同じハイパーバイザー上の様々なワークロードに関連付けられるだけでなく、わずか2つのノードから成る基礎的な仮想ネットワークから、複数のセグメントを持つ複雑なネットワークポロジに合わせた上級構造まで、何でも構築できます。

接続されたワークロードにとって、仮想ネットワークは従来の物理ネットワークと見た目も動作も変わりません（図2-4参照）。ワークロードから「見える」のは、従来の物理構造と同じL2、L3、L4～L7ネットワークサービスです。ただし、これらのネットワークサービスは、ローカルホスト上のハイパーバイザーで稼働して

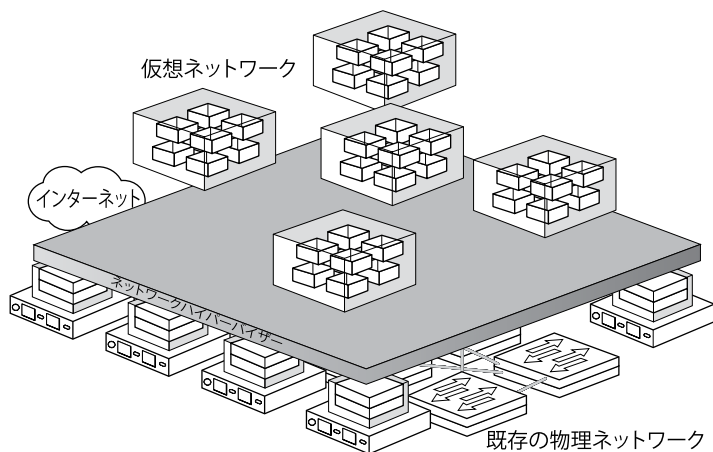


図 2-2：「ネットワークハイパーバイザー」

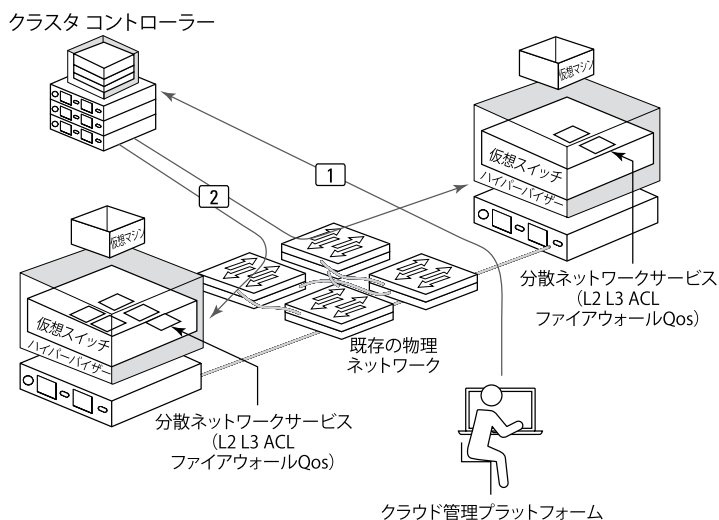


図 2-3：仮想ネットワークのプロビジョニング

いる分散ソフトウェアモジュールの論理インスタンスであり、仮想スイッチの仮想インターフェースに割り当てられています。

物理ネットワークにとって、仮想ネットワークは従来の物理ネットワークと見た目も動作も変わりません(図2-5参照)。物理ネットワークから「見える」のは、従来の物理ネットワークと同じL2ネットワークフレームです。仮想マシンは、ソースハイパーバ

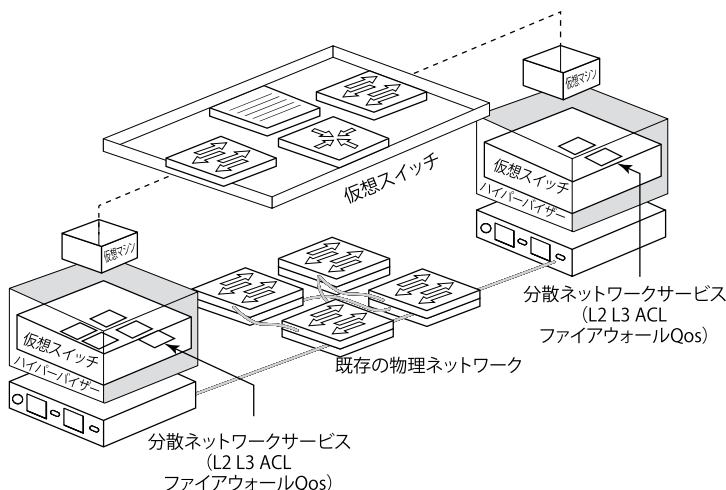


図 2-4：（論理）ワークロードの視点から見た仮想ネットワーク

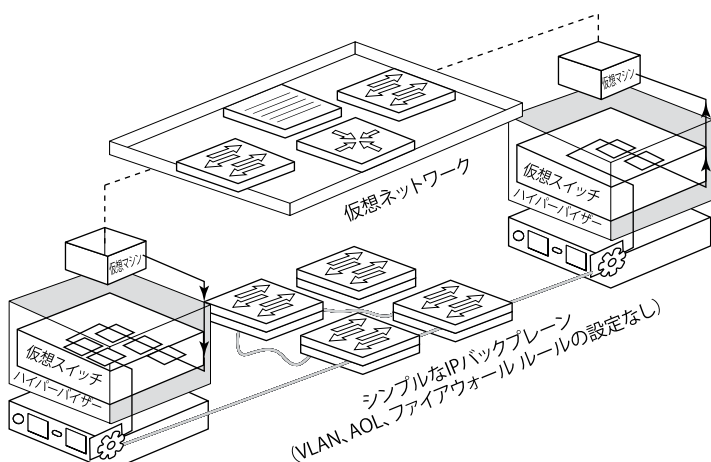


図 2-5：（物理）ネットワークの視点から見た仮想ネットワーク

イザーで追加のIP、ユーザーデータグラムプロトコル（UDP）、および仮想拡張LAN（VXLAN）ヘッダーとともにカプセル化された標準的なL2ネットワークフレームを送信します。物理ネットワークは標準的なL2ネットワークフレームとして、このフレームを転送し、宛先のハイパーバイザーがヘッダーをカプセルから出して、元のL2フレームを宛先の仮想マシンへ送ります。

仮想スイッチの仮想インターフェースでセキュリティサービスを適用し、実行する機能により、同じハイパーバイザー上にある2つの仮想マシン間の横のトラフィックにおけるヘアピンング（第3章参照）はなくなります。異なるサブネットでは、ルーターやファイアウォールなどの基礎的なサービスにアクセスするため、ネットワークを横断する必要があります。

仮想ネットワークとVLANの違い

ネットワーク関係の仕事に携わっている方ならば、VLANまたは仮想ローカルエリアネットワークについてはご存じかと思います。VLANは、長年取り扱われていますが、では何故、VLANでは不十分なのでしょう？VLANと仮想ネットワークの違いを見ながら考えてみましょう。

VLANは物理的なローカルエリアネットワークを複数の仮想ネットワークに分散させる手法をとっています。ポートグループがそれぞれ独立しており、異なる物理ネットワークで動作しているかのようです。VLANは、大きなネットワークというパイを、食べやすい大きさのネットワークにスライスしているようなものです。長期的に見ると、ネットワークが拡大するにつれ、いずれ限界に達します（LAN当たり4,096個のVLAN制限）。

VLANの問題はこれだけではありません。ネットワークの保存や

スナップショット、削除、複製、移動ができないのも大きな制限となっています。また、VLANには固有のセキュリティ問題があります。同じVLAN上にある2つのシステム間のトラフィックを制御できないのです。これにより、1つのシステムが攻撃されると別のシステムに飛び火する恐れがあります。

ネットワークの仮想化はVLANより何歩も先を行っており、ソフトウェア上でスイッチやルーター、ファイアウォール、ロードバランサーなど、ネットワーク全体を構成できます。これにより、従来よりも格段に柔軟性が高まりました。ネットワークおよびセキュリティサービスをソフトウェアで管理し、仮想マシンに展開できることで、手間がかかる管理や設定のプロセスを効率化および自動化でき、ワークロードのニーズに合ったネットワークを自動で作成できます。

仮想ネットワーク VS Software-Defined Networking

ネットワークの仮想化とSoftware-defined networking (SDN) は似ていると思われがちですが、実は、この2つには大きな違いがあります。では、両者のコンセプトを見てみましょう。

Software-defined networking という用語については人それぞれ解釈が違いますが、これだけは明らかなです。SDNでは、ソフトウェアがネットワークと物理デバイスを制御します。SDNはソフトウェア対ハードウェアのアプローチであり、次世代のネットワーク管理ソリューションと言えるでしょう。SDNは中央管理型で、ネットワークスイッチやルーターをソフトウェア経由で制御できますが、すべてのネットワーク機能やコンポーネントを仮想化するわけではありません。簡単に言えば、SDNではネットワーク全体をソフトウェア上に構成することはできないのです。ネットワークの動力は、ハードウェアに託されます。

SDNと違い、仮想ネットワークは、ネットワークリソースと下位のハードウェアを完全に切り離します。ネットワークに必要なコンポーネントと機能はソフトウェア上で忠実に複製されます。必要に応じて割り当て、使用、再利用が行える柔軟なトランスポートキャパシティのプールを作るため、物理ネットワークのインフラにも仮想化の原則が適用されます。

物理インフラから隔離されたネットワークリソースにより、下位のハードウェアに対する作業は一切なくなります。仮想マシンはネットワークの再設定やドメイン同士の接続を行う手間なく論理ドメイン間を移動できます。ネットワークの仮想化はネットワークスイッチ上ではなく、x86サーバー上のハイパーバイザーレイヤーで実行します。上述の通り、物理ネットワークは、上位から制御されるパケット転送バックプレーンとして作動します。



Software-defined networkingでは、ソフトウェア経由でネットワークスイッチやルーターの制御が可能です。ただし、全てのネットワーク機能やコンポーネントを仮想化できるわけではありません。



ネットワークの仮想化では、ネットワークに必要なコンポーネントと機能の全てをソフトウェア上に複製できます。これにより、ネットワーク全体をソフトウェア上に構成することが可能です。

仮想アプライアンス VS ハイパーバイザー内での統合

仮想アプライアンスはどうでしょう？ネットワーク機能は仮想アプライアンス（ハイパーバイザー上で動作するセットアップ済み仮想マシン）でも、もちろん実行できます。仮想アプライアンスは通常、ルーター、WANアクセラレーター、またはネットワークファイアウォールといった単一のネットワーク機能を実行するために設計されています。

仮想アプライアンスは目的こそ果たすことはできますが、いくつか不利な点があります。まず、仮想アプライアンスはハイパーバイザーの最上位でゲストとして稼働するため、パフォーマンスが制限されます。また、仮想アプライアンスの急増も懸念されます。デバイスのパフォーマンスが制限されるため、完全なデータセンターの規模に追いつくには何十、何百、何千もの仮想アプライアンスをデプロイする羽目になるかもしれません。設備投資コスト面でも大きな障壁となりますし、作業量も膨れ上がります。

ネットワーク仮想化の真の意義は、全てのネットワーク機能をハイパーバイザー内に統合することで姿を現します。この洗練されたアプローチでは、仮想マシンがサーバー間を移動する際に、ネットワークとその機能の全てが仮想マシンに追従します。全てがソフトウェア上で構成されるので、ネットワーク接続を再設定する必要はありません。つまり、ネットワークは仮想化されたデータセンター内を自由に行き来できます。

ハイパーバイザーをベースにしたネットワークの仮想化には、他にも多数の利点がありますが、これについては、第3章で説明します。とりあえず今は、データセンターの俊敏性が格段に向上するだけで申し上げておきましょう。ホームネットワークがハードウェア間の接続から無線接続になるような感じです。物を自由に動かせて、しかもネットワークに必要な要素が全て付いてまわるのです。

なぜネットワーク仮想化の タイミングが今なのか

ネットワーク仮想化は、これまで何年も話し合われてきました。現代のデータセンターの差し迫るニーズを満たすならば、今です。

それでは、ネットワーク仮想化のタイミングが今である理由を説明しましょう。

日々変化するビジネスニーズに 대응

簡単に言うと、ソフトウェアはハードウェアよりも速く動けます。ソフトウェア上で全て構成されているなら、サービスのデプロイや何らかの変更、前バージョンへのロールバックも、もっと簡単にできます。現代のビジネスにおいては、日々要求が変わります。そのため、IT部門は変化に対応する必要性に迫られているのです。ネットワーク環境がソフトウェア上で稼働するならば、より柔軟に変化へ対応できるようになり、IT部門のビジネスニーズを満たすことが可能になります。

ハードウェアの抽象化で柔軟性を高める

ネットワークの仮想化により、専用ハードウェアのインテリジェンスを柔軟なソフトウェアに移して、IT部門やビジネスの俊敏性を高めることができます。このコンセプトを抽象化と呼びます。このコンセプトを説明するに当たっては、お馴染みのサーバーの仮想化から始めましょう。

サーバーの仮想化では、抽象化レイヤーまたはハイパーバイザーが物理サーバーの属性（CPU、RAM、ディスクなど）をソフトウェア上で複製します。抽象化により、これらの属性が瞬時に組み合わせられ、固有の仮想マシンを作り出します。

ネットワークの仮想化も同じです。ネットワークの仮想化により、「ネットワークハイパーバイザー」と同等の機能がネットワークサービス（スイッチ、ルーター、アクセス制御、ファイアウォール、QoS、ロードバランサーなど）をソフトウェア上で複製します。全てがソフトウェア上で構成されるため、仮想サービスがどんな組み合わせでも固有の仮想ネットワークを数秒で作り出せます。

この俊敏性が、Software-defined data centerの大きな利点であり、ネットワーク仮想化における争点でもあります。

ネットワークのマイクロセグメンテーションでセキュリティを強化

ネットワークの仮想化におけるもう一つの争点は、より強固なセキュリティの必要性です。ネットワークの仮想化はマイクロセグメンテーション（きめ細かなポリシーとネットワーク制御によりデータセンター内のセキュリティを確保）の構成要素として、セキュリティを強化します。マイクロセグメンテーションでは各ワークロードに関連するセキュリティをパッケージングでき、サーバー間で脅威が広がることを防げます。これについては第4章で詳しく説明しましょう。

ネットワークの仮想化では、ネットワークがデフォルトで個別に分離され、無関係のネットワーク間でワークロードがお互いに影響し合うようなことは絶対にありません。コンプライアンスへの対応や脅威の封じ込め、もしくは開発、テスト、本番環境が互いに影響し合うことを防ぐためにも、分離することがネットワークセキュリティの基礎となります。仮想ネットワークを構築しても、誰かがそれらを接続しない限り、すべて個別に分離された状態のままです。分離を行う上で、物理サブネット、VLAN、アクセス制御リスト（ACLs）、ファイアウォール設定は一切必要ありません。

また、仮想ネットワークは下位の物理ネットワークからも分離されます。この分離により、任意の仮想ネットワークでの変更が他の仮想ネットワークに影響を与えることを防ぐだけでなく、仮想ネットワーク内のワークロードのいずれかで発生した脅威から下位の物理インフラを守ることができます。何度も言いますが、この分離を実現するためにVLAN、ACL、ファイアウォール設定は一切必要ありません。ネットワークを仮想化すれば自然に実現します。

マイクロセグメンテーションの詳細

マイクロセグメンテーションのコンセプトを深く知りたい方は、http://info.vmware.com/content/33851_Micro-Segmentation_Reg?CID=70134000000NzKR&src=test&touch=1から、『Micro-segmentation For

Dummies（出版：Wiley）』をダウンロードしてください。この本ではVMwareの提供により、VMware NSXを使用したマイクロセグメンテーションのコンセプトやテクノロジー、利点について詳細に解説しています。

SDDCプラットフォームの構築

第1章でも述べた通り、低コストでIT部門の俊敏性を高め、対応力の高いITサービスを提供するため、Software-Defined Data Centerというフレームワークが求められています。コンピューティングの仮想化とストレージの仮想化の上に立つ、SDDCで最も重要な第3の柱として、ネットワークの仮想化はSDDCの鍵を握っています。

ネットワークの仮想化は、既存のネットワークハードウェアの上位にネットワーク全体を構成し、平行して稼働できる、変化に対応可能なアーキテクチャです。これにより、ワークロードのデプロイ速度が上がり、益々動的になっていくデータセンターに合わせて俊敏性とセキュリティを強化できます。

ネットワークの再考

既存のネットワークハードウェアを活用できるとは言え、ネットワークの仮想化は、全く新しいアプローチです。従って、ネットワークに対する新しい見解が必要になります。これまで、ネットワーク機能はハードウェアを中心としていました。でも今は、ソフトウェアの柔軟性を備えています。

仮想ネットワークは、ネットワーク全体にわたり構築および機能を搭載し、ソフトウェア上で複製することを可能にします。



既存のネットワークハードウェアの上位に仮想ネットワークを構成し、平行して稼働することができます。仮想ネットワークは仮想マシンと同様に構築、保存、削除、復元が可能です。対象がネットワーク全体になります。

具体的に言うと、仮想ネットワークでは、

- ✓ 下位のハードウェアからネットワークを切り離し、ネットワークインフラに仮想化の原則を適用できます。
- ✓ 必要に応じて割り当て、使用、再利用が行える柔軟なトランスポートキャパシティのプールを作成できます。
- ✓ ソフトウェア上で他の仮想ネットワークやデータセンターでの変更から完全に切り離されたネットワークをデプロイできます。

- ✓ 仮想コンピューティングや仮想ストレージで行うのと同様にネットワークを転送、移動、複製できます。
- ✓ 社内のどこでも安定したネットワーク機能を利用できます。

さて、どうやって実現させるのでしょうか？それについては、ネットワークの変遷を支えるテクノロジーも含めて、第3章でお話ししましょう。

第3章

ネットワークの変革

本章の内容

- ▶ 仮想ネットワークの主な機能
- ▶ ネットワーク仮想化テクノロジー
- ▶ 仮想ネットワークの主な特長
- ▶ 機能的および経済的メリット

本

章では、お使いのネットワーク環境の仮想化からメリットを得るために必要なテクノロジーを考察します。まず、ネットワーク仮想化の背景にあるコンセプトから入り、マルチハイパーバイザーおよびマルチクラウド管理対応のネットワーク仮想化プラットフォーム、VMware NSXの詳細を説明していきます。

仮想ネットワークの主な機能

それでは、オーバーレイやパケットフローといった仮想ネットワークの主な機能を詳しく見てみましょう。

オーバーレイ

ネットワークの仮想化では、物理ネットワークハードウェアの上層にあり、サーバーのハイパーバイザー層で稼働するオーバーレイ技術を使用します。図3-1で示す通り、論理スイッチはオーバーレイの使用により実現します。

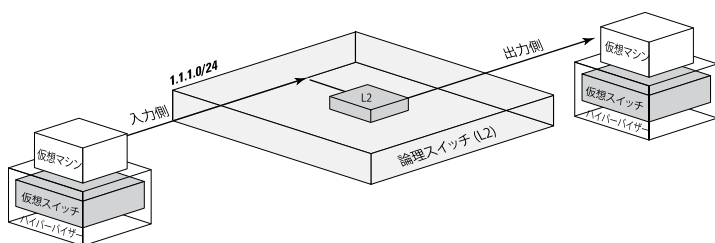


図 3-1：オーバーレイを使用した論理スイッチ

オーバーレイネットワークにより、基盤となる物理ネットワークインフラから抽出されたネットワーク全体をソフトウェアで稼働させることができます。これは、データセンターネットワーク内にトンネルを作るようなものです。

送受信者間のパケットフロー

既にお伝えした通り、仮想ネットワークは、基盤となる物理ネットワークをシンプルなパケット転送バックプレーンとして活用します。仮想マシン間での通信時、パケットは宛先のハイパーバイザーのIPアドレス情報と共にカプセル化されます。まず、物理ネットワークが宛先のハイパーバイザーにアウターヘッダーを除去できるフレームを送り、その後ローカルvSwitchインスタンスが仮想マシンにフレームを送ります。

この場合、基盤となる物理ネットワークをSTPもVLANもACLもファイアウォール ルールもない、シンプルなIPバックプレーンとして使用して通信が行われます。このアプローチにより、設定管理を大幅に簡略化でき、物理ネットワークの変更をネットワークのプロビジョニングプロセスから除去できます。

オーバーレイ技術

オーバーレイ技術は様々ですが、業界標準技術の一つとして、Virtual Extensible Local Area Network (VXLAN) が挙げられます。VXLANは、仮想L2ネットワークをL3ネットワークにオーバーレイするフレームワークを提供します。

また、NVGREという種類のオーバーレイも耳にしたことがあるかと思います。NVGREは、Network Virtualization Using Generic Routing Encapsulationの略で、用途はVXLANと似ていますが、オ

オーバーレイを作る手法が異なります。NVGREは勢いに乗るVXLANと比べると、用途が制限されます。

VMware環境では、VXLANを基にネットワークを仮想化します。この標準はVMwareと大手通信企業とが共同で開発し、広く利用されています。

VXLANの基礎

幅広い業界からの支持により、VXLANは業界標準のオーバーレイ（またはカプセル化）プロトコルとなりました。VXLANは、従来のL2テクノロジーを悩ませてきたエラーやスケーラビリティの問題なく、ワークロード間でL2アジャセンシーを提供する論理ネットワークを構築する上で重要な役割を担っています。

VXLANは、同じ論理L2セグメントに接続されたワークロード（仮想または物理）が生成した元のイーサネットフレームをカプセル化するオーバーレイ技術で、通常、論理スイッチ（LS）と呼ばれます。

VXLANはL2をL3にオーバーレイする方式（L2oL3方式）のカプセル化技術です。ワークロードが生成した元のイーサネットフレームは、外部VXLAN、UDP、IP、およびイーサネットヘッダーと共にカプセル化されるため、VXLANのエンドポイント（仮想マシン）と相互接続されているネットワークインフラ間で移動できます。

従来のスイッチで見られたLANあたり4,096個のVLAN制限も、論理スペースに作られたL2セグメントと関連付けられたVXLAN Network Identifier（VNI）という24ビットの識別子を活用することで解消されました。この値はVXLANヘッダー内に運ばれ、従来VLANで行われていたように通常IPサブネットに関連付けられます。同じ仮想ネットワークに接続されたデバイス間でイントラIPサブネット通信が行われるのです（論理スイッチ）。

その後、元のイーサネットフレームに存在するL2、L3、L4ヘッダーのハッシュ化が行われ、外部UDPヘッダーの送信元ポート値が抽出されます。このプロセスは、VXLANトラフィックの負荷を伝送ネットワークインフラ内で利用可能なコストパス全体に分散する上で重要です。

外部IPヘッダーで使用する送信元、送信先IPアドレスは、VXLANによるフレームのカプセル化を開始および終了するホストを個別に特定します。このハイパーバイザーベースの論理機能は通常、VXLAN Tunnel EndPoint (VTEP) と呼ばれます。

元のイーサネットフレームをUDPパケットにカプセル化することで、IPパケットのサイズが増えます。ここでは、物理インフラにあり、フレームを伝送する全てのインターフェースの最大伝送量 (MTU) を1,600バイト以上に増やすことをお勧めします。VXLANのカプセル化を行うVTEPが持つ仮想スイッチアブリックのMTUは、VXLANのVTEP設定時に自動で増えます。

図3-2では、VXLANオーバーレイ機能を活用している仮想マシン間のL2通信の構築に必要な手順を詳しく説明しています。

- 仮想マシン1 (VM1) が同じL2論理セグメント (IPサブネット) の仮想マシン2 (VM2) に宛てたフレームを発信します。
- 送信元VTEPがVM2に接続された送信先VTEPを識別し、伝送ネットワークに送信する前にフレームをカプセル化します。
- 伝送ネットワークは送信元VTEPと送信先VTEPのIP通信を可能にする目的でのみ必要です。
- 送信先VTEPがVXLANフレームを受信し、カプセルを開け、属するL2セグメントを識別します。
- フレームがVM2に送られます。

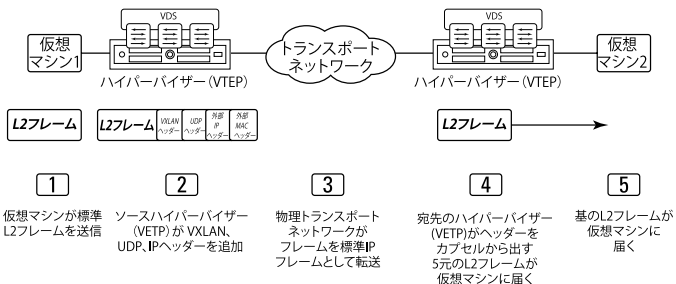


図 3-2： VXLANを使用した仮想マシン間のL2通信の構築

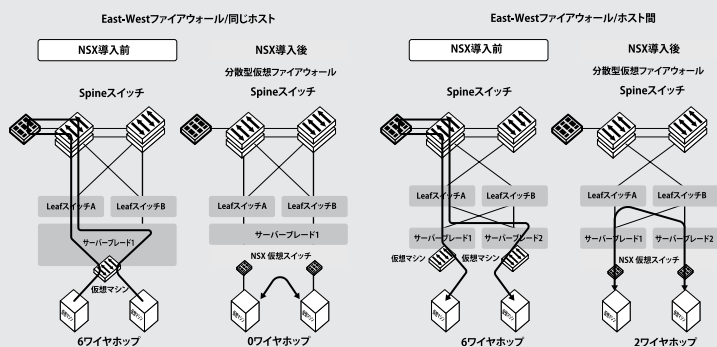
ネットワークの仮想化：実例

ここで、ネットワークの仮想化によりセキュリティとネットワーク管理が改善され得る例を一つ紹介します。

従来のネットワーク上での通信は、ファイアウォールなどのサービスを利用している場合に効率が悪くなることがあります。仮想環境外にトラフィックをルーティングし、物理セキュリティのインフラ（中央管理型ファイアウォール）をくぐらせて、

仮想環境に戻さなければなりません。このヘアピンと呼ばれるプロセスにより、複雑さが増す上に、不安定になり、ワークロードを移動させる能力も落ちるのです。

ところが、ネットワークサービスをハイパーバイザーに統合すると、ヘアピンのプロセスが不要になります。このコンセプトについては、下の図で説明します。



効果は絶大

ネットワークを仮想化すれば、データセンター ネットワークで稼働する多くのプロセスを自動化および簡略化でき、スピードや俊敏性、セキュリティの改善において大いに役立ちます。

この新しいアプローチにより得られる主なメリットをチェックリストにまとめてみました。ネットワークの仮想化により、

- ✓ ネットワークのプロビジョニングにかかる時間を数週間から数分単位に短縮できます。
- ✓ マニュアル作業によるプロセスを自動化することで作業効率が大幅に向上します。

- ✓ 物理トポロジーのワークロードを個別に配置および移動できます。
- ✓ データセンター内のネットワークセキュリティを改善できます。

VMware NSX：SDDC向け ネットワークのご紹介

まず、簡単にご説明しましょう。VMware NSXは、Software-Defined Data Center向けのネットワーク仮想化プラットフォーム兼セキュリティプラットフォームです。NSXはソフトウェア上にネットワークモデル全体を複製します。このエンド ツー エンドモデルにより、シンプルなものから複雑な多層ネットワークまで、どんなネットワークトポロジーも数秒で作成およびプロビジョニングできます。これにより、第2章で説明したネットワーク仮想化のメリットをすべて実現できます。

NSXは、俊敏性を向上させ、ネットワークに対するアプローチを円滑化しながら、データセンター内のセキュリティを強化します。このセキュリティの強化は、個別の仮想マシンやグループ化された仮想リソース周りのセキュリティコントロールを包括する自動化された細かいポリシーにより実現されます。このアプローチは、ワークロード間を飛び回り、データセンター内を水平方向に移動する、伝播を阻むことが非常に難しいか不可能な攻撃をブロックする上で大いに役立ちます。NSXを利用すれば、ワークロード一つ一つが独自のネットワークを持っているかのように、それぞれを隔離することが可能です。

仕組み

それでは、具体的にVMware NSXの秘密を探ってみましょう。

NSXのアーキテクチャ

NSXを利用したネットワークの仮想化では、物理ネットワークを、必要に応じて使用および再利用可能なトランスポートキャパシティのプールとして扱えます。仮想ネットワークの作成、プロビジョニング、および管理は、既存の物理ネットワークをシンプルなパケット転送バックプレーンとして使用してソフトウェア上で行われます。

仮想ネットワークサービスは、基盤となるネットワークハードウェアまたはトポロジーの仮想マシンそれぞれに個別に分散されます。これは、ワークロードを瞬時に追加または移動でき、仮想マシンにアタッチされたネットワークとセキュリティサービスの全てがデータセンター内を一緒に移動するということです。既存のアプリケーションは変更なく使用できます。アプリケーションから見て、仮想ネットワークとの接続と物理ネットワークとの接続に違いはありません。

既存のネットワークインフラとの統合

NSXは、既存のコンピューティングインフラ、ネットワークングインフラ、アプリケーション、およびセキュリティ製品に対応するため、現在使用しているインフラを中断することなくデプロイできます。

さらに、NSXのアプローチは「0か100か」ではないため、ネットワーク全体を仮想化する必要がありません。NSXプラットフォームにハイパーバイザーノードを追加するだけで、ネットワークの一部を柔軟に仮想化できます。

VMwareのソフトウェアまたはVMwareのパートナーが提供するトップオブブラック スイッチハードウェアとして入手できるゲートウェイを使用すれば、仮想ネットワークと物理ネットワークをシームレスに相互接続することができます。この方法は、例えば、仮想ネットワークに接続されたワークロードをネットワークへアクセスさせたり、レガシー型のVLANとベアメタルワークロードを仮想ネットワークと直接接続するのに使用できます。

ネットワークが簡単に

NSXをデプロイした後の物理ネットワークとのやり取りは、ほぼ必要ありません。VLANやACL、スパンニングツリーの物理ネットワーク設定や複雑なファイアウォール ルールの設定、複雑なトラフィックパターンのヘアピンもネットワークを仮想化すれば必要ありません。



NSX仮想ネットワークをデプロイすれば、物理ネットワークの設定や設計をより簡単に行えるようになります。物理ネットワークは安定した高速パケット転送のみできればいいので、ベンダーロックインが通用しなくなります。これにより、様々な製

品ラインやベンダーによるハードウェアを組み合わせ使用できます。

最高の柔軟性と拡張性

NSXは柔軟性と拡張性がとても高く、幅広く対応できます。また、強力なトラフィックステアリング機能により、どんなネットワークやセキュリティサービスでも好きな順番で組み合わせることができ、全てが各ワークロードに設定したアプリケーションポリシーによって定義されます。

この柔軟性の高さは、NSXのネイティブサービスだけでなく、次世代ファイアウォールの仮想/物理インスタンス、アプリケーションデリバリーコントローラー、侵入防止システムなど、サードパーティ製ソリューションにも幅広く対応します。

では一步引いて大局的に見てみましょう。VMwareのパートナー企業が販売するNSX対応製品の多さが、NSXプラットフォームによってもたらされる新しい運用モデルへの業界の支持を証明しています。仮想ネットワークの世界に足を踏み入れる皆様にとって心強いことでしょう。巨大なエコシステムが味方についているのですから。

実現できること：NSXの主な機能

では、VMware NSXの主な機能を技術的観点から見てみましょう。まず、ここで説明するポイントを頭に入れておいてください。NSXは全てのネットワーク機能を仮想化します。これは、ハードウェア上で行っていたことをソフトウェア上で行えるようになるということです。言ってみれば、NSXは、これから説明するネットワークギアの上を漂う魔法のじゅうたんのようなもののなのです。



全てをソフトウェア上で

VMware NSXの主な機能は以下の通りです。

- ✓ **論理スイッチ**：NSXを使用すれば、基盤となるハードウェアから切り離れたL2とL3のスイッチング機能を仮想環境で複製できます。
- ✓ **NSXゲートウェイ**：L2ゲートウェイにより、物理ワークロードやレガシー型のVLANとスムーズに接続できます。
- ✓ **論理ルーティング**：論理スイッチ間のルーティングにより、異なる仮想ネットワーク間における動的なルーティングが可能です。
- ✓ **論理/分散ファイアウォール**：NSXを使用すれば、ハイパーバイザーに統合され、ワークロードそれぞれに個別のセキュリティを配した分散ファイアウォールを作成できます。
- ✓ **論理ロードバランサー**：NSXはSSL Terminationを使用して完全なロードバランス機能を提供します。
- ✓ **論理VPN**：NSXは、ソフトウェア上でのサイト間VPNおよびリモートアクセスVPNに対応します。
- ✓ **NSX API**：RESTful APIにより、どんなクラウド管理プラットフォームにも統合できます。

必要不可欠な分離、セグメンテーションに加え、高度なセキュリティサービスを提供

データセンターの境界保護には毎年何十億もの資金が投じられています。その効果はというと、データへの侵入は一向に減りません。境界保護はセキュリティ戦略の要であるものの、全てを満たしてくれるわけではないのです。データセンターセキュリティには新しいモデルが必要であり、第2章でご紹介したマイクロセグメンテーションというコンセプトが、このモデルを提供します。

NSXは自動化されたきめ細かなポリシーを仮想マシンに結び付けることで、データセンター内のセキュリティを確保します。ネットワークのセキュリティポリシーは、データセンター内に分散しているハイパーバイザーに統合されたファイアウォールの管理により適用され、仮想マシンの移動に付随して、データセンターでの変更にも動的に適応します。

仮想ネットワークは独自のアドレス空間で稼働するか、重複するアドレス空間を持ち、お互いに干渉することはありません。仮想ネットワークは最初から、他の仮想ネットワークや基盤となる物理ネットワークから個別に分離されます。どの仮想ネットワークもデータセンターという海に浮かぶ孤島のようなものです。このアプローチにより、ネットワークそれぞれを確実に切り離すことが可能になります。つまり、データセンター向けのセキュリティモデルそのものを改善できるというわけです。ファイアウォールをすり抜ける悪質なソフトウェアもサーバー間を移動できなくなります。

もちろん、お気に入りのネットワーク セキュリティ ソリューションが無駄になるというわけではありません。NSXは業界をリードするネットワークソリューションやセキュリティソリューションをSoftware-Defined Data Centerで共用するためのプラットフォームです。NSXプラットフォームとの緊密な統合により、サードパーティ製品やソリューションを必要に応じてデプロイでき、データセンター内の環境の変化にも動的に適応します。



NSXでネットワークを仮想化すれば、以下に挙げるマイクロセグメンテーションの主な機能3つを活用できます。

- ✓ **分離**：関連性のないネットワーク間の通信は一切なし
- ✓ **セグメンテーション**：ネットワーク内の通信をコントロール
- ✓ **高度なセキュリティサービス**：サードパーティ製セキュリティソリューションとの緊密な統合により実現

パフォーマンスとスケーラビリティ

NSXのパフォーマンスとスケーラビリティは実証されています。ネットワーク機能がハイパーバイザーに実装されているため、NSXは、追加機能をシームレスに拡張でき、可用性と信頼性も確保したスケールアウトアーキテクチャを備えています。

ここで、NSXの素晴らしいスケーラビリティについて例を交えて説明しましょう。あるNSXの導入事例では、たった一つのクラスタコントローラーが1万の仮想ネットワークを稼働するのに使用され、1万のネットワークが10万の仮想マシンを支えています。



NSX環境では、

- ✓ 分散型ネットワークサービスの実行に必要なプロセスは、仮想スイッチが接続済みのワークロードに対して既に行っているプロセスの増分のみです。
- ✓ 仮想スイッチは、全てのNSXのネットワークやセキュリティサービスと共にハイパーバイザーカーネルに統合されたモジュールです。
- ✓ 仮想ネットワークのトランスポートキャパシティは新しいハイパーバイザーやホストの追加とともに（仮想マシンのキャパシティに基づいて）リニアに拡張し、スイッチングおよびルーティングキャパシティが20Gbps、ファイアウォールキャパシティが19.6Gbps追加されます。

圧倒的なネットワークの視認性

NSXにより、ネットワークの視認性は一つ上の段階へ進みます。従来のネットワークでは、全く異なる多数のネットワークデバイスに設定や転送条件が散らばっていました。この細分化がネットワークを見づらくし、トラブルシューティングを複雑にしていたのです。

それに比べてNSXは、全てのネットワーク接続およびサービス向けの設定と条件全てを一か所で提供します。NSXのコンポーネントや仮想ネットワークの要素（論理スイッチ、ルーターなど）の接続性に関するステータスやログに簡単にアクセスでき、まるで仮想ネットワークトポロジーと基盤となる物理ネットワーク間のマッピングのようです。これにより、通信し合っている仮想マシンが同じホスト上にあり、トラフィックが物理ネットワークに到達しない場合でも、仮想マシン間のトラフィックを完全に可視化できます。



しかも、NSXならTraceFlowのような高度なトラブルシューティングツールを利用できます。この機能により、統合型パケットを仮想スイッチポートに投入でき、物理ネットワークシステムおよび論理ネットワークシステムを横断する際のネットワークパスを確認できます。従って、管理者はパケットが通るパスの全容を特定することができ、道半ばでパケットがドロップしたポイント（ファイアウォールのポリシーが原因など）に対してトラブルシューティングを行えます。

従来の物理ネットワークハードウェアでこのレベルの視認性を得ることは不可能であり、同じホスト上で2つの仮想マシンが通信している状況での物理ネットワークでは絶対に実現できません。

VMware NSXの主なメリット

ここからが本題です。VMware NSXを利用したネットワークの可視化により実現した機能を活用するにはどうしたらいいのでしょうか。機能的なメリットと経済的なメリットの2つに分けて考えてみましょう。

機能的なメリット

NSXの機能的なメリットは、Software-Defined Data Centerの4本柱、スピード、俊敏性、セキュリティ、信頼性に集約されます。では、このようなメリットが生まれる仕組みを見てみましょう。

ネットワーク全体をソフトウェア上で素早く構築

NSXは論理スイッチやルーター、ファイアウォール、ロードバランサー、VPN、ワークロードのセキュリティといった論理ネットワークの要素およびサービスのライブラリを備えています。これらのコンポーネントを組み合わせれば、分離された仮想ネットワークポロジを数秒で作成できます。

データ漏洩によるリスクとダメージを最小限に

NSXを使用すれば、ワークロードを分離させ、それぞれ独立したセキュリティを確保することができます。これにより、データセンター内で脅威を封じ込め、悪質なソフトウェアの移動をブロックできます。内部セキュリティの強化により、データ漏洩により発生するコストを回避または削減できます。

ITサービスの提供や開発にかかる時間を短縮

ネットワークの仮想化により、多層ネットワークおよびセキュリティサービスのプロビジョニングにかかる時間を数週間から数分に短縮できます。中にはNSXにより、アプリケーションチームに全てのセルフサービスのプロビジョニング機能を与えている企業もあります。さらに、NSXの自動化およびオーケストレーション機能により、マニュアル作業による設定エラーのリスクを防げます。

ネットワークトラフィックのフローを簡略化

NSXはキャパシティを超えたコア上にあるサーバー間のトラフィック（East-Westトラフィック）により発生する負荷の抑制にも使用できます。仮想ネットワークでは、仮想スイッチまたはアグリゲーションファブリックを介して仮想マシン同士が互いに通信します。これにより、East-Westトラフィックのホップ数を削減

でき、入り組んだトラフィックパターンに潜在する危険を回避できます。既存の資産をうまく利用しつつ、コアのキャパシティを増やすためにハードウェアを追加するコストも回避することが可能になるのです。

サービスの可用性が向上

クラウド規模のデータセンターは、ネットワーク上のポイント間には等価コストマルチパス（Equal-cost multipath：ECMP）ルーティング機能を持ったフラットなファブリックを備えているため、停止することがあります。シンプルなleaf-spine型ファブリックなら、個別のリンクまたはデバイスが意味を成さなくなるため、ネットワークは複数のデバイスエラーが同時に起こっても停止することなく対応できます。NSXのネットワーク仮想化機能により、データセンター内でも高い可用性を保てます。

経済的なメリット

NSXを使用したネットワーク仮想化の経済的なメリットは、設備投資コストも運用コストも抑えられることにあります。

損失の大きい漏洩リスクを削減

増え続けるデータセンター内のEast-Westトラフィックに対するコントロールを強めることを目的としたファイアウォールのデプロイはこれまで、多くの企業にとって大変費用がかかることでした。しかも、必要なデバイスの多さやファイアウォールルールの複雑なマトリックスを設定し、管理する手間を考えると、このアプローチは実行不可能でした。仮想ネットワークに備わっているマイクロセグメンテーション機能を利用すれば、この作業が低コストで実行できます。結果として、余計なハードウェアやソフトウェアを買い足さずに済むため、莫大な設備投資を行わずにデータセンターセキュリティの侵害リスクを削減できます。

時間と労力を節約

ネットワークの仮想化は、ネットワークに関するタスクを実行するのにかかる時間と労力を大幅に削減します。通常、NSXは労力を時間単位から分単位に、サイクル時間を日単位から分単位に抑えます。開発からテスト、ステージング、本番環境まで、物理ネットワークのプロビジョニングと管理に必要なマニュアル作業を考えてみてください。NSXがこれらを自動化すれば、運用コストを抑えられるのは明白でしょう。

サーバーの使用効率を改善

従来のトポロジでは、ネットワーク クラスタがそれぞれ独自のコンピューティングキャパシティを備えていました。他のクラスタで利用可能なキャパシティにアクセスするためには長時間かかり、エラーも多いネットワークの再構築を行う必要がありますが、IT管理者はそれを避けるため、コンピューティングをオーバープロビジョニングすることよくあります。NSXなら、この作業も、もっと簡単に行えます。NSXを使用して2つ以上のネットワーク クラスタに橋をわたり、未使用のスペースにワークロードをデプロイするのです。既存のサーバーキャパシティをより効率よく使うことで、新しい物理サーバーを購入する必要がなくなります。

コストパフォーマンスを改善

NSXの機能とネットワーク仮想化を使用することで、多くの企業が高価な専用ハードウェアの使用を止め、様々なベンダーが販売している低価格のものから選んだ、安くパフォーマンスの高いインフラに乗り換えています。

ハードウェアのライフサイクルを延ばす

NSXは既存のネットワークインフラを最大限活かす上でも役立ちます。仕組みを説明しましょう。NSXは増え続けるネットワーク コアからのEast-Westトラフィックをオフロードします。これにより、高額なキャパシティを追加することなく、ハードウェアのライフサイクルを延ばすことができます。NSXなら、基盤となるネットワークハードウェアをシンプルなIP転送バックプレーンとして使用でき、耐用年数を延ばすことで、減価償却年度末にネットワークギアを一新する必要がなくなります。キャパシティを追加する時、または故障したハードウェアを交換する時以外にハードウェアをいじる必要は一切ありません。

第4章

仮想ネットワークの 用途

本章の内容

- ▶ データセンターのセキュリティ強化
- ▶ ITプロセスの自動化
- ▶ アプリケーションの継続性の改善

本章では、仮想ネットワークが実際どのように使用されているか、例を挙げて説明します。第3章で述べた通り、NSXを使用した仮想化は、「0か100か」というアプローチではありません。ネットワーク全体を仮想化する必要はないのです。ネットワークを用途に合わせて部分的に仮想化し、時間をかけて仮想ネットワークの利用を拡大していけばいいのです。

ここでお伝えしたいのは、用途がたった一つでも、NSXにかかるコストの妥当性を証明できる企業が多いということです。しかも、ITを自動化する戦略的プラットフォームを構築しつつ、他の用途やプロジェクトをじっくり増やしていけるのです。

次の項では、ネットワークの仮想化における最も一般的な用途をいくつか詳述し、プロセスの高速化やセキュリティ強化、アプリケーションの継続性の向上方法を説明します。

データセンターのセキュリティ強化

先述の通り、セキュリティに対する懸念は、非常に重要で大きくなるばかりです。ここで、ネットワークの仮想化がデータ漏洩リスクを抑える上で役立つ仕組みを見てみましょう。

データセンター内での水平移動を制限

現代の攻撃は、従来の境界ベースのネットワークセキュリティ戦略が生まれ持つ弱点を突いて企業のデータセンターに侵入します。攻撃は、データセンターの境界セキュリティをすり抜けると、データセンター内のワークロード間を水平方向に移動するため、伝播を阻むことが非常に困難または不可能になってしまいます。

データセンターネットワークのマイクロセグメンテーションは、許可されていない水平方向の移動を制限しますが、現在のところ、データセンターネットワークでの実行は現実的ではありません。

従来のパケットフィルタリング型ファイアウォールも最新の次世代ファイアウォールも、ネットワーク上の物理または仮想チャックポイントでのコントロールを実行しています。アプリケーションのワークロードトラフィックがコントロールポイントを通ると、そのコントロールポイントに設定されたファイアウォールルールに基づいて、ネットワークパケットはブロックされるかファイアウォールの通過を許可されます。

従来のファイアウォールを使ったマイクロセグメンテーションには、スループットキャパシティとセキュリティ管理という2つの問題があります。

トランスポートキャパシティの制限については、乗り越えられないわけではないですが、コストが高つくきます。マイクロセグメンテーションを行うのに必要なキャパシティを確保できるだけの物理または仮想ファイアウォールを購入することは可能ですが、ほとんど（全て）のIT部門にとって、マイクロセグメンテーションで効果を出せるほどファイアウォールを購入することは現実的ではありません。この説明は、仮想マシン1台につき個別のファイアウォールを備えることが前提です。御社のデータセンターには何台の仮想マシンがあるでしょう。数百台でしょうか。それとも数千台でしょうか。一般的なデータセンターならファイアウォールの数は数千に及ぶでしょう。

セキュリティ管理の問題も、ワークロードの数や現代のデータセンターが日に日に動的になっていくのに比例して増えていきます。もしも新しい仮想マシンを追加、移動、または停止する度にファイアウォールルールをマニュアル作業により追加、削

除、変更しなければならないとすれば、変更の頻度にIT業務が追いつかなくなるでしょう。データセンター内での包括的なマイクロセグメンテーションや、特権管理を最小限に抑えたユニットレベルの保護戦略を実現しようと、セキュリティチームが必死で練った計画が計画倒れになってきたのは、このためです。

Software-Defined Data Center (SDDC) はネットワーク仮想化プラットフォームを活用して、自動プロビジョニング、ワークロードの自動移動/追加/変更、仮想インターフェースの分散稼働、および各ハイパーバイザーに分散され、プラットフォーム内に作りこまれたファイアウォールのカーネル内スケールアウトパフォーマンスといった、従来のネットワークセキュリティを凌駕する大きなメリットを実現します。

データセンター内におけるEast-Westトラフィックの増加

ここ十年の間に、多層サーバーインフラにデプロイされるアプリケーションが増え、データセンタートラフィックにおいてEast-West（サーバー間）通信が占める割合が、North-South（クライアント対サーバー）通信やインターネット通信が占める割合よりも格段に多くなりました。事実、データセンター内のトラフィックは、全ネットワークトラフィックの8割を占めています。こういった多層アプリケーションインフラは通常、システム間の通信を制限するセキュリティコントロールが弱い、全く備えられていません。

攻撃者たちは、このデータセンタートラフィックにおける方向転換と、境界ベースの保護戦略にデータセンター内のネットワーク通信に対するコントロールがほとんど、または全くないことを利用するため、攻撃戦略を変えてきました。社内のセキュリティチームも境界ベースの保護ばかりに気を取られるのではなく、ネットワークトラフィックの大半が保護されずに存在しているデータセンター内の保護戦略を、攻撃者と同様、模索する必要があります。

視認性とコンテキスト

データセンター内でのEast-Westトラフィックの増大とサーバー仮想化の成長は、データセンターに視認性とコンテキストが欠けていることに気づかせてくれました。

多くの場合、データセンター内のEast-Westサーバー通信は、ファイアウォールを通過せず、検査されることもありません。このトラフィックは事実上、ネットワークセキュリティチームからは見えないのです。ファイアウォールのチョークポイントをバックホールさせるヘアピンなどの手法で、East-Westトラフィックに無理やりファイアウォールを通過させる場合、通信パスが複雑で効率の悪いものとなり、データセンター全体のネットワークパフォーマンスに悪影響を及ぼします。

サーバー仮想化におけるイノベーションは、データセンター内にある従来のデータやコンテキストにおいて基盤となるネットワーク構造やセキュリティ構造を大幅に上回ります。複数の仮想ワークロードを複数のネットワーク インターフェース カード (NIC) が設定された単一の物理ホストにデプロイすることは、仮想サーバー環境では一般的なことです。仮想スイッチなしでは、個別の仮想マシンを行ったり来たりするトラフィックを特定することは簡単ではありません。問題を探し出し、修正しようとしているネットワークチームにとって、これは大きな問題であり、攻撃者の温床となるのです。

仮想ネットワークのネットワークハイパーバイザーは、データセンター内のトラフィック全てを、仮想マシンそれぞれのワークロードレベルまで見渡せる独特の位置にあります。この可視性およびコンテキストレベルの高さが、オペレーションシステムやパッチレベル、稼働サービス、その他多数のプロパティといった、各ワークロード特有の属性に基づいたマイクロセグメンテーションを可能にするのです。この機能により、データセンター内のワークロードそれぞれの目的を理解した上で、ネットワークおよびセキュリティポリシーに関する適切な判断を下すことができます。例えば、基盤となるネットワークポロジに縛られることなく、受注アプリケーションのウェブ層や企業の人事管理システムなど、個々のワークロードのニーズに基づいて専用のポリシーを設定することができます。

分離

コンプライアンスへの対応や脅威を封じ込めるため、また、開発、テスト、本番環境を切り離しておくためにも、分離はネットワークセキュリティにおける重要な原則となります。データセンター内のネットワークを確実に分離するため、従来はルーティング、アクセス コントロール リスト (ACL)、物理デバイス上のファイアウォール ルールがマニュアル作業により設定、管理されていました。



Forrester Research社は、情報セキュリティおよび分離に関して、境界ベースのセキュリティコントロールをデータセンター全体に拡張する「ゼロトラスト」モデルを提唱しています。この場合、IT部門は、外部および内部データリソースを保護し、厳格なアクセスコントロールを実行しなければなりません。「ゼロトラスト」は、権限が必要な機能を実行する上で必要なアクセスや権限を最小限に制限する情報セキュリティの基本理念、最小権限の原則を採用しています。（レーガン元大統領には申し訳ないですが）「信ぜよ、されど確認せよ」という概念はもう古いのです。安全でセキュアな世界の合い言葉は「信じるな、常に確認せよ」です。

仮想ネットワークは、他の仮想ネットワークや基盤となる物理ネットワークから個別に分離されるよう設計されています。この概念は、データセンター内に一定の信頼性を想定する従来のアプローチとは明らかに違っています。分離は、ネットワークの仮想化が生まれ持った機能であり、その実行には、物理サブネットやVLAN、ACL、ファイアウォールルールも必要ありません。仮想ネットワークは作成された時から分離され、意図的に且つ明確に接続されるまで分離されたままです。

分離された仮想ネットワークは、データセンター内に分散されたワークロードから作成でき、同じ仮想ネットワーク内にあるワークロードは、同じハイパーバイザーにも別のハイパーバイザーにも移動できます。また、複数の分離された仮想ネットワークにまたがるワークロードを同じハイパーバイザーに移動することもできます。仮想ネットワークの分離により、IPアドレスの重複も可能になります。例えば、分離された開発、テスト、本番仮想ネットワークがあるとして、それぞれのアプリケーションのバージョンが違っていてもIPアドレスが同じである場合、同じ物理インフラを基盤として同時に操作を行うことができます。

最後に、仮想ネットワークは、基盤となる物理インフラからも分離されます。ハイパーバイザー間のトラフィックは封じ込められるため、物理ネットワークデバイスは、仮想ネットワークに接続されたワークロードではなく、全く異なる場所で動作します。例えば、一つの仮想ネットワークでIPv4物理ネットワークに加え、IPv6アプリケーションのワークロードに対応できます。この分離により、仮想ネットワーク内のワークロードから発生した攻撃から基盤となる物理インフラを保護できます。もう一度言いますが、これまで分離に必要なだったVLAN、ACL、ファイアウォールルールがなくてもこれら全てを実現できます。

セグメンテーション

分離に似ていますが、多層から成る仮想ネットワーク内で利用されるのがセグメンテーションです。これまで、ネットワークセグメンテーションは、ウェブ層、アプリケーション層、データベース層のトラフィックなど、ネットワークのセグメントや層の間を行きかうトラフィックを許可または拒否する物理ファイアウォールやルーターを使用して行われてきました。セグメンテーションでは、異なるネットワークセグメントに異なる信頼レベルを定義でき、境界ベースの保護が破られた際の攻撃対象領域を抑えることができるため、セキュリティ設計において重要です。残念ながら、データセンターのネットワークセグメントは規模が大きすぎて効率が悪く、従来のプロセスでは、セグメンテーションの定義や設定に時間がかかり、人的エラーも多く、結局セキュリティ侵害を防げませんでした。

ネットワークセグメンテーションは分離と同様、ネットワーク仮想プラットフォームの要となる機能です。仮想ネットワークは、多層ネットワーク環境に対応しており、ワークロードのセキュリティポリシーに定義される分散型ファイアウォールを使って、単一のL2セグメント上に複数のL2セグメントとL3セグメンテーション（またはマイクロセグメンテーション）を構築できます。例えば、これがウェブ層、アプリケーション層、データベース層として機能します。

仮想ネットワークでは、ワークロードと共にプロビジョニングされるL2、L3、ACL、ファイアウォール、サービス品質（quality of service：QoS）などのネットワークおよびセキュリティサービスをプログラムとして作成し、それをハイパーバイザー仮想スイッチに送り、仮想インターフェースで実行します。仮想ネットワーク内の通信が仮想環境を出ることはなく、ネットワークセグメンテーションを物理ネットワークやファイアウォールで設定、管理する必要がなくなります。

自動化

自動プロビジョニングにより、ワークロードがプログラムとして作成された際に正しいファイアウォールポリシーをプロビジョニングでき、ワークロードがデータセンター内またはデータセンター間を移動するとポリシーも付随するようになります。

また、アプリケーションが削除されると、セキュリティポリシーがシステムから自動で削除されることも重要です。この機能によ

り、パフォーマンスを劣化させ、セキュリティの問題を引き起こしがちな何千もの古い、旧式のファイアウォール ルールを残さずに、大きな欠点であるファイアウォール ルールの膨張を防ぐことができます。

また、企業は、高度なセキュリティサービスを連携させ、それぞれのセキュリティシナリオを基に異なるサービスを実行することで、様々なパートナー機能を組み合わせて利用できます。これにより、IT部門は既存のセキュリティ技術を統合でき、より包括的で相関性のあるセキュリティ機能をデータセンター内に構築できます。実を言うと、データセンター内のワークロードそれぞれにおける仮想トラフィックの視認性やコンテキストの面では、既存のセキュリティ技術の方が他の方法よりもマイクロセグメンテーションとの相性が良く、完全なセキュリティソリューションの一部として仮想マシンのワークロード毎にセキュリティ操作をカスタマイズできます。

例えば、ワークロードを標準ファイアウォールでプロビジョニングでき、異なるタイプのワークロードにアクセスすることを許可または制限できます。また、通常の脆弱性スキャン中にワークロードで脆弱性が検出された場合、より制限性の高いファイアウォールポリシーを適用し、脆弱性を修正するツール以外がワークロードへアクセスすることを制限することも同じポリシーで定義できます。



セキュリティ製品のメーカーは、ネットワーク仮想化プラットフォーム利用して、異なるセキュリティ製品メーカーのソリューションに対応する、高度なセキュリティサービスの提供を開始できます。これもネットワーク仮想化により勢いづいたイノベーションの一つです。

ユーザー環境の保護：VDIのマイクロセグメンテーション

多くの企業が、仮想化技術をデータセンター以外にも利用しようと、仮想デスクトップインフラ（VDI）の導入を行ってきました。マイクロセグメンテーションにより、こういった企業はSDDCのセキュリティにおける以下のようなメリットの多くをデスクトップに拡張することが可能になり、今ではモバイル環境さえも、その視野に入っています。

- ✓ 主なネットワーク機能やセキュリティ機能をVDI管理に統合
- ✓ VDIユーザー毎に異なる複雑なポリシーセットやトポロジを排除
- ✓ ファイアウォールやトラフィックにフィルタを設定し、論理的なグルーピングポリシーを指定
- ✓ セキュリティポリシーをネットワークトポロジから分離し、管理を簡単に

マイクロセグメンテーションを実行する機能も備えてはいるものの、VMware NSXでは、仮想デスクトップ毎に独自のファイアウォールを設定できます。これにより、仮想ネットワークインターフェースの隅々まで、より細かいセキュリティレベルを設定できます。仮想マシンを行き来するトラフィックは全てポリシーに基づいて保護され、仮想マシン間またはワークロード間の許可されていない通信を防ぐことができます。エンドユーザーの仮想デスクトップでセキュリティ侵害が起こっても、被害はそのユーザーのみに抑えられるのです。

ITプロセスの自動化

大きなデータセンターにおいて、IT管理者にとっての災いの元、および経営者にとっての経済的痛手となり得るのがマニュアル作業によるプロセスです。ネットワークの仮想化は、ネットワーク設定やプロビジョニング、管理など、大きな労力を要し、エラーの温床となるタスクを自動化することで、マニュアル作業による問題の解決に役立ちます。

ITの自動化

NSXを使用すれば、その強力なオーケストレーション機能により、仮想マシンと並行してネットワークサービスを提供できます。NSXは、ネットワークトポロジやサービスから成る、事前に定義されたテンプレートを標準化および管理する上で役立ちます。テンプレートにより、一貫した設定やセキュリティを使って、数秒で環境をプロビジョニングできます。



NSXのIT自動化機能というバットを振れば、三冠王は確実です。経費を削減し、開発時間を早め、迅速にITサービスを提供できるのですから。

開発者向けクラウド

NSXは他のInfrastructure-as-a-Service (IaaS) への取り組みと同様、セルフサービスの開発者向けクラウドプラットフォームとして理想的です。ネットワークやサービスのプロビジョニングを自動化することで、開発チームやテストチームが必要なインフラに素早くアクセスできるようになり、ソフトウェア アプリやアップグレードをユーザーの手にいち早く届けることが可能になります。

NSXは開発、テスト、ステージング環境にある何千もの分散されたネットワーク全てを同じ物理インフラ上でプロビジョニングできます。この斬新な手法により、NSXはマニュアル作業やネットワークインフラの調達、インストール、設定にかかるサイクル時間を排除します。ネットワークはワークロードと共に、しっかりと審査されたセルフサービスのトランザクションとして順番にデプロイされ、アプリケーションはIPアドレスに変更を加える必要なく、迅速に開発、テスト、ステージング、本番環境へと進みます。

仮想化のおかげで、開発/テストチームがネットワークインフラのプロビジョニングに足を引っ張られることがなくなり、業務の高速化および開発時間の短縮を実現できます。

マルチテナント型インフラ

マルチテナント型クラウド環境では、NSXのマイクロセグメンテーション機能と分離機能を使用して、テナント同士の分離状態を維持できます。NSXを使うことで、仮想ネットワークを構築し、他の仮想ネットワークや基盤となる物理ネットワークから完全に分離させた状態を維持できます。2つの異なるテナントを同じ物理インフラの同じIPアドレスで稼働しても、仮想ネットワークは2つのテナントや物理ネットワークの存在にすら気づかないため、IPアドレスの対立なく稼働させることができます。

仮想ネットワーク、ネットワークセグメント、またはセキュリティグループに基いて高度なサービスを追加し、ソリューションの範囲を広げることもできます。例えば、Palo Alto Networks社製のファイアウォールを介したディープ パケット インスペクションなどを追加できます。このサービスを利用すれば、Palo Alto Networks社製のVM-Series対応ファイアウォールにリダイレクトして検査および実行するトラフィックの流れを細かく定義できま

す。VM-Series対応のファイアウォールにより許可されたトラフィックは、NSXの仮想スイッチに戻され、最終目的地（ゲスト仮想マシンまたは物理デバイス）へ送られます。

アプリケーションの継続性を拡大

アプリケーションの継続的な稼働はIT部門にとって最も重要な要件の一つです。ネットワークの仮想化により実現されるディザスタリカバリやデータセンター間でのプール、およびハイブリッドクラウド機能は、アプリの機能を維持する上で役立ちます。

ディザスタリカバリ

NSXを既存のディザスタリカバリソリューションに加えることで、復旧を速め、ダウンタイムを短縮できます。このケースでは、NSXがネットワーク全体と、そのセキュリティ環境を複製します。その後はリカバリサイトの複製を維持しつつ、ネットワークやアプリケーション、サービスの構造を定期的にスナップショットすることができます。

仮想ネットワークは、基盤となるハードウェアやトポロジから分離されているため、IPアドレスを変更する必要がなく、簡単です。ディザスタリカバリサイトはプライマリサイトと同じですが、機能やパフォーマンスのトレードオフがありません。複製された環境はスタンバイモードでリカバリサイトに留まり、障害時にボタンを押すことで動作します。ソースネットワークに対する変更は全て、リカバリサイトの複製環境にも自動的に反映されます。

データセンター間のプール

ネットワークの仮想化により、異なる物理スペースにありながら極めて近い（ローカルまたは都市間）コンピューティングリソースのプールが可能になります。その後、複数の異なるデータソースは統一された単一のコンピューティングリソースセットとして扱われます。アプリケーションはどこでもデプロイでき、サイト内のリソースにスムーズに接続できます。これは、複数サイトにNSXをデプロイするケースで広く利用されています。

ハイブリッド クラウド ネット ワーキング

NSXは、オンプレミスネットワークをパブリック クラウドに拡大するハイブリッドクラウド環境にもピッタリなネットワークです。NSXはITリソースへのセキュアなオンデマンドアクセスを可能にし、特殊なニーズに応えられるよう、ワークロードをオンサイトにもオフサイトにも移動できる柔軟性を兼ね備えています。

さらに、NSXはあらゆるクラウド管理プラットフォームと連携できるよう設計されています。多くのプラットフォーム向けに、NSXを追加設定なしで使用するためのサポートを提供しており、NSX APIにより他の管理プラットフォームとの統合も可能です。これにより、プライベートクラウドで必要なセキュリティをパブリック クラウドに拡張可能な状態で手に入れることができます。

第5章

仮想ネットワークの運用

本章の内容

- ▶ 運用のコンセプト
- ▶ 運用における投資分野
- ▶ 人材と業務に関する問題の解決

NSXの運用には、ネットワーク仮想化およびそのセキュリティ機能を使用する人材、プロセス、技術を最適化することが必要です。

ネットワーク仮想化の恩恵を得るには、NSXの運用を実現し、スピード、俊敏性、セキュリティといった包括的なメリットを獲得することが必要不可欠です。NSXの運用を開始する方法により、ITおよびビジネスにおけるメリットをどれだけ速く実現できるかが決まります。

仮想ネットワークの運用は、ハードウェア定義のデータセンターからソフトウェア定義のデータセンターへの移行に伴い、企業の成熟度をより高める過程において、段階的な文化や技術革新のステップのひとつと言えます。10年前に起こったコンピューターの仮想化と同じく、この進歩においてもヒーローや専門職が誕生するでしょう。

本章の目的は、NSXの運用に何が必要かを全て解説するわけではなく、ネットワーク仮想化の実現に向けて考慮すべき主な事項をまとめてご紹介することです。全てを書こうとすれば、本一冊など、すぐに埋まってしまいますからね。



NSX運用までの旅路をスタートさせるに当たり、SDDCの最適化を実現するための長期計画を明確にしましょう。その計画を実現するために、人材やプロセス、技術をどう成長させていくかを考えるのです。

運用における投資分野

ネットワークの仮想化を運用するに当たり、考慮すべき主な投資分野は6つあります。これらの分野に投資することで御社の事業価値やITスタッフのキャリア価値を最大限まで引き出せます。

以下のコンセプトを網羅する包括的なアプローチをお勧めします。

- ✓ 組織構造
- ✓ 業務と責任
- ✓ プロセス
- ✓ ツール
- ✓ アーキテクチャ
- ✓ インフラストラクチャ

組織と人材

SDDCの運用はIT部門におけるほとんどの業務に影響を与えます。運用による影響はコンピューティングやネットワーク、ストレージ、セキュリティに渡り、オペレーターや管理者、エンジニア、設計者などの人材にも広がります。NSXの運用を開始する際は、透明性を保ち、関わる人材全てをプロセスに関与させることが大切です。

ここで、IT部門とそのメンバーによるベストプラクティスを紹介しましょう。

- ✓ **既存のネットワークチームとセキュリティチームにNSXを任せましょう。** チームを変更したり、新しく作る必要はありません。役割分担（設計者、エンジニア、オペレーター、管理者など）もそのままです。現在の業務と責任範囲にネットワークの仮想化が加わるということです。

- ✓ **クラウドチームとの連携を向上させる方法を考えましょう。**担当や責任範囲を越えたスキルの活用、共通の目標やオペレーション原則の導入、チーム間のトレーニングや能力開発、事業のサービス提供に関わる調整などを検討します。
- ✓ **クラウドネットワークに必要なネットワーク業務およびセキュリティ業務を考えましょう。**アーキテクチャ、セキュリティ、オーケストレーションと自動化、開発と統合、管理、オペレーション、サポート、およびエスケーシング業務などを考慮します。
- ✓ **チームの支持を得ましょう。**より面白く、戦略的なプロジェクトに取り組む機会を与えられる中で、チームの誰もが、そのバリュープロポジションと個人的、職務的意義を理解できるようにしましょう。
- ✓ **ネットワーク業務に携わる人材の雇用を保証しましょう。**ネットワーク業務に携わる人材の仕事が自動化後も無くないこと、また、仮想化チームに移譲されないことを明確にしましょう。仮想ネットワークを運用するのは、現在ネットワーク業務を行っている人材です。必要なネットワーク知識を持っているのは、彼らだけですから。
- ✓ **クラウド運用スタッフを早い段階から評価プロセスに参加させましょう。**NSXにより、いかに業務がやりやすくなるかを学ぶことで、プロジェクトの支持者になってもらいます。導入直前に驚かれることがないようにしましょう。
- ✓ **セキュリティチームを早い段階から評価に参加させましょう。**セキュリティチームは、分離された仮想ネットワークが物理ネットワークと同様に安全であることを理解する必要があります。また、マイクロセグメンテーションが既存のNorth-Southトラフィック向け境界ベースのファイアウォールに取って代わるものではなく、データセンター内でのEast-Westトラフィックのコントロールを行えるようにするためのものであることを学ぶ必要があります。



VMwareのオペレーションに特化したリソース（技術ガイドやワークショップ、トレーニング、認定書など）を最大限に活かして、ネットワークの仮想化およびSDDCの運用に必要な専門性やスキル、知識を得ましょう。

プロセスとツール

ネットワークの仮想化による主なメリットの一つとして、マニュアル作業の自動化が挙げられます。ただし、これを実現するに

は、事前に適切なツールに投資することが必要になります。NSX Manager内で直接自動化できるタスクもありますが、その他のタスクの自動化は、クラウド管理プラットフォームなどのツールを利用して行います。

NSXは管理の中心を担うNSX Managerにより、仮想ネットワークの作成、管理、監視を行います。NSX環境の運用は自動的にNSX Manager中心となり、他のツール（VMware vRealize Automation、VMware vRealize Operations、OpenStack、その他サードパーティ製ツールなど）はUIまたはAPI経由でNSX Managerにコールします。

また、NSXコンポーネント（コントローラー、エッジノード、ハイパーバイザー）とネットワークインフラ（アンダーレイ）の両方を含む下層インフラの管理も必要になります。NSXはこういった要素を管理する機能を提供し、サードパーティ製ツールもインフラを管理する上で中心的な役割を担うのです。



NSXの運用を開始する際は、プロセスやツールへの影響にも注意が必要です。特に、以下のベストプラクティスを覚えておきましょう。

- ✓ **既存のネットワークやセキュリティプロセスを分析し、詳しく理解しましょう。** オークストレーションと自動化により、どのようにプロセスを簡略化および円滑化するか考えます。
- ✓ **監視やトラブルシューティング、変更管理、リリース管理、キャパシティ管理といった業務に対するネットワーク仮想化の影響を考えましょう。** こういった主要な業務の仕組みや簡略化の方法を理解します。
- ✓ **ネットワークプロセスの自動化と環境の標準化（設定やポリシー）における優先順位を決めて、手間とコストを抑えましょう。** ネットワークとサービスの自動化およびポリシーベースのプロビジョニングにより、よくある設定エラーを排除し、監査やコンプライアンスのために行われた変更を簡単に検索できるようになります。
- ✓ **既存の管理ツールおよびオペレーションツールを使用するか、最新ツールの採用を検討するか決めましょう。** 最新ツールを利用すれば、コンピューティング、ストレージ、およびネットワーク全体におけるアプリケーションの健全性を全て確認でき、仮想コンポーネントと物理コンポーネント間のオブジェクト関係を見ることもできます。

- ✓ **仮想および物理コンポーネントの管理に使用するVMware製またはサードパーティ製ツールを探しましょう。** NSXのネイティブ機能とAPIを活用して、クラウド管理プラットフォームやオーケストレーションツール、自動化ツールなど、既に持っているツールと深いレベルで統合する方法を探ります。
- ✓ **既存のツールを使って仮想ネットワークを運用しましょう。** 仮想ネットワークは、物理ネットワークに期待される運用情報（パケット/バイトカウンター、NetFlowエクスポートなど）を全て提供します。多くの既存ツールはNSXから提供された情報を利用して運用タスクを実行できます。
- ✓ **既存の使い慣れたツールを使って監視とトラブルシューティングを実行しましょう。** ベンダーを一つに絞るアプローチでは、視認性が制限される場合もあります。複数のツール（vRealize Operations、Splunk、Wireshark、NetFlowコレクターなど）を使用すれば、ネットワークインフラの監視とトラブルシューティングを最大限に活用できます。

アーキテクチャとインフラ

NSXによるネットワークの仮想化では、ネットワークサービスを基盤となる物理インフラから切り離します。これにより、基盤となる物理インフラが特定の機能やサービスに対応するのではなく、オペレーション効率を高めることに集中できるように設計できます。物理ネットワークは安定性第一に構築することができ、物理ネットワークの設定への変更は稀になります。

オペレーションの面から言うと、ネットワーク機能（ファイアウォールなど）のデプロイを物理インフラのデプロイから切り離せることになります。これにより、アプリケーション毎に新しい機能を徐々にデプロイしていく基盤を整えることができます。また、ハードウェアのアップグレード（新しいネットワークスイッチのデプロイなど）もNSXのデプロイから切り離せることになります。

NSXでは、統合仮想プラットフォームにより、オペレーション全体に渡ってシンプルさと一貫性を実現できます。また、ネットワーク、セキュリティ機能、および分散型ポリシーの実装も可能です。さらに、自動化により、セキュリティポリシーをより効率よく、正確に適用できるようになるので、マニュアル作業による物理ネットワークへの変更が最小限に抑えられます。

他にも、NSXの運用により、VLANやIPアドレスの処理といった手間からワークロードを開放できるという重要なメリットもあります。これは、プロビジョニングやアプリケーションへのアクセスが速くなることで、リソースの活用効率が上がり、オペレーションコストが抑えられ、アプリケーションチームのストレスが軽減されるといった直接的な影響をオペレーションに与えます。

NSXの運用を開始する上での今後の手順は以下の通りです。

- ✓ **ネットワークの仮想化とセキュリティを徐々に展開していきましょう。** たった一つの用途とアプリケーションから徐々に始められます。最もリスク/リターンプロファイルが優秀なワークロードを探し出し、新しい機能を活用しましょう。
- ✓ **高額なリッピングや物理ネットワークの代替品を最小限に抑えましょう。** NSXは物理ネットワークの再構築を必要としない上に、ネットワークアーキテクチャでの変更を実行しやすくします。NSXにより、仮想ネットワークのトポロジ（仮想マシン視点）が物理トポロジから抽出されるため、ネットワーク設計者はleaf-spine型アーキテクチャを使用できるようになります。
- ✓ **物理インフラや仮想インフラのアプリケーションそれぞれに対する監視やトラブルシューティングを一か所で行うためのビューを作りましょう。** NSXスイッチが仮想マシンに出入りするパケット全てを監視してくれるため、NSXは、ネットワークトラフィックにおいて最高レベルの可視性を提供します。
- ✓ **新しいクラウドネットワーク機能およびセキュリティ機能を開発し、運用するための標準的なリズムを確立しましょう。** これにより、クラウドインフラやアプリケーションチームから積極的な参加とフィードバックを得られます。
- ✓ **仮想ネットワークおよびセキュリティの管理と監視を、中央から制御しましょう。** サービスの分散環境を統合管理することで、運用に細かいポリシーを適用できます。例えば、3層構造のアプリで、同じ層にある仮想マシン同士の通信を禁じ、他の層のマシンとの通信を許可することもできます。
- ✓ **下層のコンポーネント（IPアドレスなど）ではなく、上層のコンポーネント（OS名、ユーザー、グループなど）に基づいてセキュリティポリシーを設定しましょう。** セキュリティポリシーをより効率よく、正確に適用できます。

- ✓ NSXを既存の物理ネットワークインフラに接続されたハイパーバイザー上に展開し、あらゆるベンダーの次世代ファブリックやトポロジに対応しましょう。

大局的に見る

これまでの大きなITの取り組みがそうであったように、ネットワークの仮想化はデータセンターのあり方を大きく変えます。ただ、中には変わらないこともあり、その一つが雇用の安定です。仮想ネットワーク環境を成功に導くには、ネットワークのプロが必要であり、彼らの支えがなければ成功できないのです。

ネットワーク仮想化の一端を担うということは、企業のネットワークおよびセキュリティの変革に参加し、貢献する機会を得られるということです。コンピューティングの仮想化でヒーローとなり、キャリアを構築した人々と同じように、あなた自身にとっても素晴らしい成果となるでしょう。リーダーシップを執れるこの機会を利用しない手はありません。



インフラを仮想化し、プロセスを自動化すれば、もっと面白く、戦略的な取り組みに時間を費やすことができます。例えば、ルーターの設定やファイアウォール ルールの更新といった単調な業務ではなく、spine-leaf型ネットワークの設計やネットワークおよびセキュリティワークフローの自動化、開発者クラウドの構築などに取り組みます。

今はネットワークの黄金時代です。ネットワークの仮想化という取り組みに参加すれば、10年前のサーバー仮想化でサーバー管理者が経験したように、充実したキャリアを重ね、将来の役に立つだけでなく、業界で貴重な存在になります。



ネットワークの仮想化はキャリアを成長させ、ネットワークアーキテクチャ関連の業務や設計、トラフィックの調整にもっと時間を費やせるようになります。

- ✓ ネットワークの仮想化に伴い、業務を自動化しても仕事はなくなることはありません。むしろ、もっと面白く、戦略的なプロジェクトに携われるようになります。
- ✓ あなたの業務が仮想化チームに移譲されることはありません。NSXは物理ネットワークと同じネットワークコンセプトおよび技術に則っており、ネットワークやセキュリティに関する専門知識が必要です。

✓ 仮想化により難しくなる業務はありません。仮想オーバーレイに加え、自動化や簡略化された物理アンダーレイを組み合わせることで、ネットワークのプロビジョニングと管理をスムーズに行えます。

第6章

ネットワーク仮想化を開始する10（くらい）の方法

本章の内容

- ▶ 貴重な分析に基づく厳選された情報
- ▶ 最高クラスのハンズオンラボ（実習ラボ）での試用
- ▶ 御社の環境にNSXを導入する方法

本章では、ネットワークの仮想化を開始する上で、聞きたいけど聞けないことを10（くらい）まとめました。ネットワーク仮想化に関する情報を案内しながら、CiscoインフラにVMwareのNSXプラットフォームを展開する可能性を紹介し、既存のインフラ、およびロードバランサーデバイスや次世代ファイアウォールなどのネットワークサービスを提供するサードパーティ製ソリューションとNSXを統合する方法を説明します。

基本的な情報こそ大切に

まず、ネットワークの仮想化や仮想ネットワークのコンポーネント、運用開始に便利なツールを理解する上で役立つ情報を見ましょう。

基礎を叩き込む

VMwareは、ネットワーク仮想化の基礎を理解する上で役立つ情報を幅広く提供しています。

- ✓ **VMware NSX製品紹介ページ** (<http://www.vmware.com/jp/products/nsx/>) : NSX製品紹介ページでは、NSXプラットフォームの基本的な特長や機能、メリットをまとめています。また、技術情報や法人向けコンテンツなど、幅広い詳細情報へのリンクを提供するポータルとしての役割も担っています。
- ✓ **VMware NSX紹介ビデオ** (https://www.youtube.com/watch?v=8oo_U_SGSU0) : このビデオは、VMware NSXがネットワーク仮想化プラットフォームの基盤として、ネットワークで仮想マシンのオペレーションモデルを実現する方法を4分ほどで簡単に説明します。イノベーションも追いつかないほど忙しい企業で働くラジさんがビデオのナレーターを務めます。
- ✓ **#VirtualizeYourNetwork** (<http://virtualizeyour-network.com/>、英語) : #VirtualizeYourNetworkは、ネットワークの仮想化を採用することでデータセンターのオペレーションやコストを改善に取り組む担当者、チーム、部門のためのオンラインリソースです。このサイトでは、ネットワークとデータセンターの変革の現状から、先駆者や同業他社の取り組み、ITキャリアを発展させる上で役立つ情報などを提供しています。

細かく調べる

ビジネス関連の議論、技術概要、業界分析などを網羅したホワイトペーパーや、マイクロセグメンテーションを利用して、よりセキュアなデータセンターを構築することに特化したガイドも提供されています。以下の情報は、1-2回クリックするだけでご覧頂けます。

- ✓ **「VMware NSXネットワーク仮想化プラットフォームに関するホワイトペーパー」** (www.vmware.com/files/pdf/products/nsx/VMware-NSX-Network-Virtualization-Platform-WP.pdf、英語) : VMware NSXプラットフォームの機能、特性、性能、およびメリットを紹介する全12ページのテクニカルホワイトペーパーです。技術に精通した企業がネットワーク仮想化プラットフ

オームとしてNSXを選ぶ理由をよく理解して頂ける内容になっています。

- 『*Micro-segmentation For Dummies*』 (http://info.vmware.com/content/33851_Micro-Segmentation_Reg?CID=70134000000NzKR&src=test&touch=1) : この本は、マイクロセグメンテーションの仕組みや背景にある技術、幅広いセキュリティ上のメリットなどを詳細に説明しており、オンラインでお読み頂けます。データセンター内で脅威が水平方向に広がることを防ぐ、本質的にセキュアなデータセンターを構築する方法をご覧ください。

ブロガーとの交流

VMware製品を利用したネットワーク仮想化の専門家が、その分析や実体験を様々なブログで語っています。ネットワーク仮想化に現在進行形で携わっている人々の体験談を直接お読み頂けます。

- ネットワーク仮想化ブログ (<http://blogs.vmware.com/networkvirtualization>、英語) : ネットワーク仮想化に関する最新ニュースと技術分析については、こちらのブログをご覧ください。ネットワーク仮想化に関する正確なニュースと事実に基づく情報を提供する業界情報のソースとして利用して頂けます。
- スコット・ロウのウェブログ (<http://blog.scottlowe.org>、英語) : 書籍やビデオ トレーニング シリーズ、プレゼンテーションも手がけるITのプロ、スコット・ロウが仮想化、ネットワーキング、オープンソースのソリューション、およびクラウドコンピューティングに関する分析を自身のウェブログで語っています。ネットワークの仮想化に関連する情報、分析、および技術的知識を得る場としては最適です。

ハンズ オン ラボでNSXを試用する

VMware NSXのようなプラットフォームに対する理解を深めるには、実際に試用してみると良いでしょう。VMwareが誇るハンズ オン ラボ (www.vmware.com/go/try-nsx-en) はそのためにあると言っても過言ではありません。

VMware/ハンズ オン ラボでは、特別な設定を行う必要なく、本番稼動しているデスクトップ上で、VMware製品をお試し頂けます。クリック毎にガイドが表示される上、全製品がプリインストールされていますので、最も気になる機能を存分にお試しください。お使いのシステムにソフトウェアをインストールすることなく、VMware NSXの機能を知ることができる素晴らしい方法です。

御社の環境にNSXを導入する方法を学ぶ

導入に関するオプションを検討する段階になったら、オンデマンドのリソースでネットワークの仮想化とNSXについて学びましょう。VMwareは、オンラインコースからライブウェビナー、オンデマンドの自習コースまで、ネットワークの仮想化とNSXのメリットを体験できる様々な方法を提供しています。

VMware教育コースに参加する

ネットワーク仮想化の基礎とNSXで解決できる業務上の課題を学ぶことから始めましょう。その後、NSXをインストール、設定、および管理する方法を簡単に学べるオンデマンドの自習コースに進めます。http://campaign.vmware.com/imgs/apac/jp_dwn/PDF/EDU_DATASHEET_NSXICM_V6.pdfらご参加ください。

NSX Product Walkthrough からプラットフォームの全容を 学ぶ

ネットワーク仮想化について積極的な方には、技術に特化したNSXの機能紹介ビデオシリーズ、NSX Product Walkthrough (<https://featurewalkthrough.vmware.com>: 英語) で学習を続けることをお勧めします。

NSX Product Walkthroughでは、NSXの基本機能からVMwareやパートナー製品との統合まで、幅広く説明します。ご覧いただけるプレゼンテーションは以下の通りです。

- ✓ **VMware NSXのご紹介**：NSX Manager、ゲートウェイサービス、ファイアウォール、監視とトラブルシューティング、およびCMP統合など、NSXの主な機能と性能を説明します。
- ✓ **VMware NSX for vSphere**：VXLAN、ネットワーク仮想化、VXLAN-to-VLANブリッジサービスといったVMware NSXの機能を学べます。
- ✓ **セキュリティとコンプライアンス**：Software-Defined Data Centerを採用する上でのセキュリティ上の課題や、VMware NSXのネットワーク仮想化機能を使用して分散型ファイアウォールを追加する方法、およびNSX Service Composerを使用するメリットを検討します。
- ✓ **NSXとパートナー製品との統合**：VMware NSXの拡張性とサードパーティ製ゲートウェイ機能およびセキュリティ機能との統合について学べます。
- ✓ **VMwareコンポーネントとの統合**：NSXを他のVMware製品と統合するメリットを学べます。

技術情報を詳細に見る

技術的な視点に立った分析も大切です。まずは、NSXデザインガイドとNSXガイドをご覧ください。本章で説明している通り、技術的な視点で書かれています。

- ✓ **「VMware NSX for vSphere Network Virtualization Design Guide」** (<https://communities.vmware.com/docs/DOC-27683>)：詳細な技術仕様がが必要な場合は、デザインガイドをダウンロードしてください。本書は、VMware NSX ネットワーク仮想化ソリューションのvSphere環境への展開を検討されている仮想化アーキテクトおよびネットワークアーキテクトの皆様を対象としており、以下のトピックに関する詳細な情報が記載されています。
 - NSX-v機能コンポーネント
 - 機能サービス
 - 設計における検討事項

✓ 「Getting Started Guide for NSX vSphere」 (<https://communities.vmware.com/docs/DOC-27705>) : 本書では、vSphere環境でNSXによってネットワークサービスを設定する方法を、以下のようなトピック毎に、順を追って説明します。

- 論理スイッチ
- 論理分散ルーター
- 分散ファイアウォール
- ダイナミックルーティング機能と多対一のネットワークアドレス変換 (NAT) 機能を持った統合論理ルーター (エッジ)
- 論理ロードバランサー (エッジ)

Cisco UCSおよびNexus 9000 インフラを使ったNSXの展開

NSXが普及していく中、VMwareは多くのIT部門から、最新のCiscoインフラ（特にCisco UCSブレードサーバーとCisco Nexus 9000シリーズスイッチ）と並行してNSXを運用したいとの声を受けてきました。この組み合わせなら、基盤となるハードウェアをより速く、フレキシブルにソフトウェアに移行できます。



他のIPファブリックと同様、NSXはアンダーレイとしてNexus 9000と緊密に連携します。NSXとNexus 9000シリーズスイッチをスタンドアロンモードで組み合わせれば、SDDCのメリットを実現できます。

将来的に、この組み合わせをIT部門が導入できるよう、VMwareは、VMware NSX for vSphere Network Virtualization Design Guideと共に追加設定の必要がない参照アーキテクチャを提供しています。この参照アーキテクチャでは、VMware ESXiとNSXの連携を実現するための基盤と、Cisco UCSとの推奨設定、およびUCSとNexus 9000スイッチの接続性をカバーしています。

参照アーキテクチャの詳細については「リファレンスデザイン：Cisco UCSおよびNexus 9000インフラを使ったNSXの展開」 (www.vmware.com/files/pdf/products/nsx/Design-Guide-for-NSX-with-Cisco-Nexus-9000-and-UCS.pdf、英語) をご覧ください。

既存のネットワークインフラへのNSXの統合

NSXは、既存のネットワークインフラと統合し、L2ゲートウェイ機能を使って物理ネットワークと仮想ネットワークのブリッジになるよう設計されています。この統合により、現代のデータセンターのような非常に動的な環境で、アンダーレイの伝送ネットワークとオーバーレイのネットワーク仮想化ソリューションが互いに依存し合い、パフォーマンスや安定性、拡張性を最適化できるようになります。

この統合を実現するため、VMwareは、L2スイッチパートナー企業と緊密に連携し、アンダーレイ インフラの能力を最大限活用する俊敏なオーバーレイとしてNSXを使用するための、参照アーキテクチャとデザインガイドを作成しました。

NSXと既存のネットワークインフラとの統合に役立つ技術資料は以下の通りです。

- ✓ **Arista**：「VMwareとAristaの連携によるVMware vSphere環境向けネットワーク仮想化リファレンスデザインガイド」
(www.vmware.com/files/pdf/products/nsx/White_Paper_Design_VMware_Arista_3-15-2014.pdf)
- ✓ **Brocade**：「VMwareとBrocadeの連携によるネットワーク仮想化リファレンスホワイトペーパー」 (<https://communities.vmware.com/docs/DOC-28347>)
- ✓ **Cisco**：「リファレンスデザイン：Cisco UCSおよびNexus 9000インフラを使ったNSXのデプロイ」 (<https://communities.vmware.com/docs/DOC-29373>)
- ✓ **Dell**：「DellインフラとVMware NSX参照アーキテクチャを使ったネットワークの仮想化」 (<https://communities.vmware.com/docs/DOC-27684>)
- ✓ **Juniper**：「VMware NSXとJuniperプラットフォームを使った物理ネットワークと仮想ネットワークの接続」 (<https://communities.vmware.com/docs/DOC-27610>)

ネットワークサービスを提供するエコシステムパートナーとの統合

既存のネットワークインフラとの統合に加え、NSXはロードバランサー、次世代ファイアウォール、次世代サービスなど、様々なネットワークサービス用のソリューションと統合できるよう設計されています。

ここでは、今後参画予定のNSXパートナーの一部をご紹介します。

- ✓ **Physical-to-virtual (P2V)** : Arista、Brocade、Cumulus、Dell、HP、Juniper
- ✓ **ネットワークセキュリティ** : Check Point、Fortinet、Intel Security、Palo Alto Networks、Rapid 7、Symantec、Trend Micro
- ✓ **可視化および監視** : Arkin Net、EMC Smarts、NetScout、Gigamon、Tufin、Riverbed (SteelCentral)
- ✓ **アプリケーション デリバリー コントローラー** : F5 Networks

御社でも仮想ネットワークを活用しましょう!

現代のデータセンターは、仮想サーバーや仮想ストレージに頼り切ってきており、Software-Defined Data Centerを使用するメリットは十分にあるでしょう。ただし、ネットワークへの配慮も重要です。これまでのネットワークはハードウェアに組み込まれているため、従来のネットワークでサービスを行うには、手作業によるプロビジョニングが必要になり、ベンダー固有のハードウェアやトポロジーに縛られています。このような古いやり方では、アプリケーションのデプロイに時間がかかり、Software-Defined Data Centerの導入も遠のいてしまうのです。

ネットワークの仮想化は、この方程式を覆します。仮想ネットワークの構築、プロビジョニング、管理を全てソフトウェア上で行えるため、1ランク上の俊敏性、効率性、安全性を備えたデータセンターの運用が可能になります。本書では、ネットワーク仮想化の核となるコンセプトや重要なコンポーネントをシンプルで、分かりやすく解説しています。

- **大局的に見る** — 仮想化とは何か、従来のネットワークアーキテクチャとは何が違うのか、何故ネットワークの仮想化により効率性が上がるのかを説明します。
- **アーキテクチャを理解する** — ネットワーク仮想化という斬新なアプローチのメリットとデメリットを探ります。
- **導入方法を学ぶ** — 導入する上でのヒントやコツ、ベストプラクティスや落とし穴など、分析した情報をご提供します。


Mora Gozaniは現在、VMwareのNetwork and Security (NSX) 部門にてシニア プロダクト ライン マーケティング マネージャーを務めています。カリフォルニア大学サンタバーバラ校で学士号を取得した後、サンダーバード国際経営大学院で理学修士を修め、現在はカリフォルニア州のロスアルトスに在住です。



本書から学べること:

- ネットワークに対して新しいアプローチを仕掛けるタイミングが今である理由
- ネットワーク仮想化の主な用途
- ネットワークの仮想化が Software-Defined Data Center の礎となる理由

WILEY

 Also available
as an e-book

ISBN: 978-1-119-28414-7
非売品

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.