SDN利用ガイダンス

ソフトウェア・ディファインド・ネットワーク

(SDN：Software Defined Network)

CSA ジャパン　SDN ワーキンググループ

バージョン 1.0

本書の提供について

本書「**SDN利用ガイダンス**」は、CSAジャパン SDNワーキンググループの以下のメンバーが作成し公開したものです（順不同、敬称略）。

大澤能丈　SDN-WG リーダー
栗田晴彦　SDN-WG サブリーダー
菊池弘治
奥西誠子
林千佳
石井啓介
榎本真弓
片岡武義
山下亮一
諸角昌宏

また、本書は予告なく変更される場合があります。以下の変更履歴（日付、バージョン、変更内容）をご確認ください。

変更履歴

日付	バージョン	変更内容
2020 年 5 月 25 日	1.0	新規リリース

日本クラウドセキュリティアライアンスに関する情報は、以下の URL より参照可能です。

https://cloudsecurityalliance.jp

2020 年 5 月 25 日

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

１．　責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

２．　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

３．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。
(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。
(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

４．　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

コンテンツ

はじめに

ソフトウェア・ディファインド・ネットワーク(Software Defined Network ：SDN) は、 文字通りソフトウェアによって、ネットワークの構成や設定を一元的に簡便に管理する技術のことです。 概念自身は 10 年以上前から存在していたものですが、近年の「クラウドバイデフォルト（Cloud By Default）」の流れの中で、再びより注目すべき技術となってきました。 クラウド上のセキュリティを評価、検討、実装するにあたって、その理解が極めて重要なものとなっており、そのために、2020 年 1 月にこの SDN ワーキンググループが立ち上がりました。

初期段階では、SDN は、オンプレミス（On Premise）の視点で語られることが多かったのですが、システムの仮想化が当たり前になり、クラウド利用、クラウド移行が進むにあたって、仮想化やクラウドを含めて統合的に議論することが必要となっております。 例えば、IaaS（Infrastructure As a Service）上のシステムを構築するにあたり、マネジメント用のコンソールから、仮想マシンや DB の設定を行うと同時に、ネットワーク的な配置やそのセキュリティ制御も定義していきます。 これは裏を返すと、SDN がほぼ完ぺきな形で実現できていると考えられます。 ハイブリッドクラウドで、オンプレミスのシステム、ネットワークと、クラウドのシステム、ネットワークとを統合を考えれば考えるほど、SDN が欠かせないものとなります。 さらに、具体的に導入が進んできている ソフトウェア・デファインド・広域通信網（Software Defined Wide Area Network：SD-WAN）やネットワーク機能仮想化（Network Functions Virtualization：NFV）、次世代のネットワーキング概念である インテントベースネットワーキング（Intent Based Networking：IBN）どれも、SDN の考え方を発展させたり、SDN 実装に大きな関連を有したりしています。

本資料は、日本クラウドセキュリティアライアンス（CSA ジャパン）が発行している「クラウドコンピューティングのためのセキュリティガイダンス v4.0 日本語版 v1.1（2018 年 7 月 24 日）：以下 セキュリティガイダンス」での記載内容をベースに、関連するテクノロジーや利用ユースケースを盛り込みまとめてあります。（各章にベースとしたセキュリティガイダンスの章番号を記載しています。）セキュリティガイダンスの解説書としてご覧いただきたいと思います。

読者が、SDN の概要を把握すると同時に、現存するツール/テクノロジーとその利用ケースをイメージしやすいように、具体的に説明することに心がけました。 また、SDN をより広範に捉えるため、セキュリティガイダンスには触れられていない、前出の 3 テクノロジー（SD-WAN、NFV、IBN）の説明にも紙面を割きました。 利用ケースについては、メンバーの経験に基づき、実際のお客様の状況を反映させることに注力しています。

セキュリティの視点からすると、「ネットワーク」というのは依然として対策のベースであり最初の重要な防御ラインであり続けます。 最近注目を浴びている「ゼロトラストセキュリティ」は、決してネットワークベースのセキュリティに意味がないということではなく、今までの「社外との境界」のみのネットワーク対策が、よりインスタンスやプロセスレベルでのネッ

トワークセキュリティ対策に移行するということで、それを実現しようとすると SDN が前提となります。 本書が、読者皆様方の安全なクラウド利用の一条になれば幸いです。

なお、末筆とはなりますが、本資料作成にあたって有志の方のご協力いただきました。この場をお借りして御礼申し上げます。

SDN WG サブリーダー　栗田 晴彦

1. クラウドコンピューティング概要

※本章はセキュリティガイダンス 「*7-1*」章の解説となります。

クラウドコンピューティング(以降クラウド)は、主に下記の２つの層から構成されます。

① 物理的な層（プロセッサ、メモリなどのクラウドリソースの元）

② 仮想的な層（クラウド利用者により定義・管理される仮想マシン、仮想ネットワークなど）

２つの層の内、クラウド利用者は、仮想的な層のみを定義・管理します。そのため、この層へのセキュリティ対策はクラウド利用者側で行う必要があります。

物理的な層は、クラウド事業者(AWS/Azure/GCP など)が管理しており、この層に対するセキュリティ対策は、クラウド事業者にて行われています。

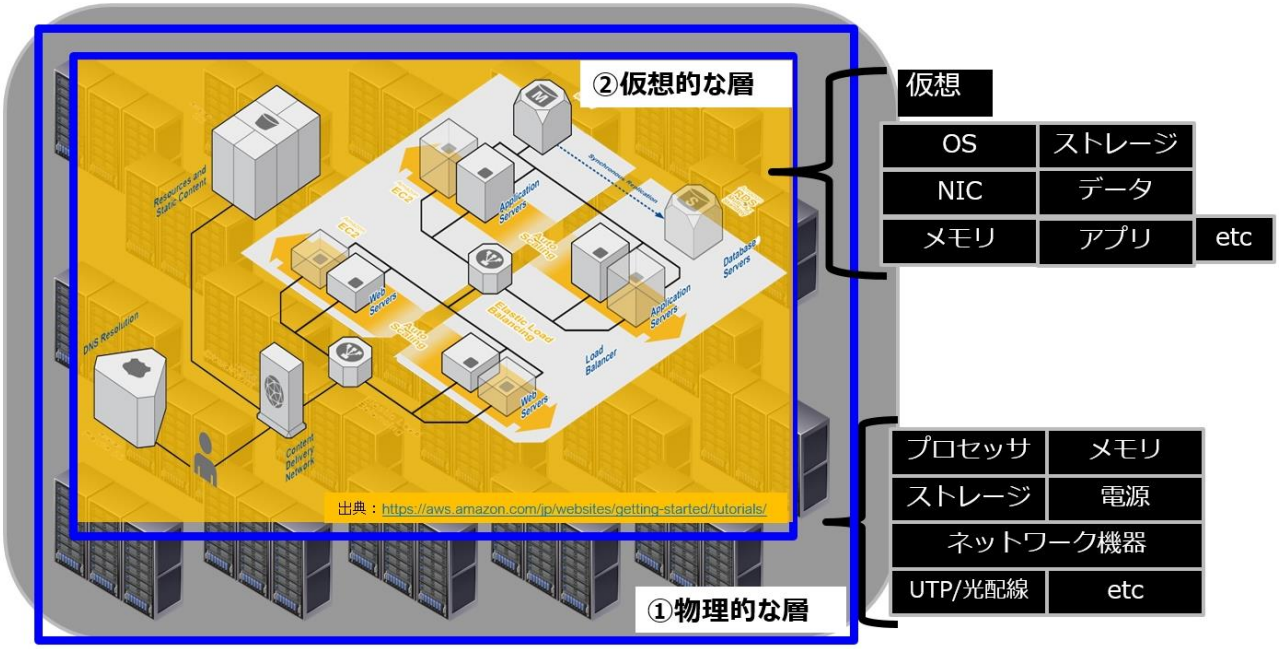


図１：クラウドの２つの層

※上記「② 仮想的な層」へのセキュリティ対策は利用者側で考慮が必要です。

2. クラウドのネットワーク仮想化と SDN

※本章はセキュリティガイダンス 「7-2」章の解説となります。

ネットワーク仮想化のカテゴリ

クラウド利用者から見て仮想ネットワークは以下のように利用されます。

① ネットワークのリソースプールから望ましいネットワーキングを引き当てる

② ネットワーキングリソースを使用する仮想化環境の上限範囲内で設定

例 1 ） 特定のサブネットの中での IP アドレスを割り当てる

例 2 ） 完全なクラス B の仮想ネットワークを引き当てし、サブネットアーキテクチャを完全に定義する

クラウド事業者にとって、そのクラウドを構成するネットワークを物理的に分割することは、運用上やセキュリティ上の理由からも重要です。

最も一般的には、機能的あるいはトラフィックの重複がないようにするために別々のハードウェアに分離した下記の 3 つの異なるネットワークで構成します。

① 管理用ネットワーク

② ストレージ用ネットワーク

③ サービス用ネットワーク

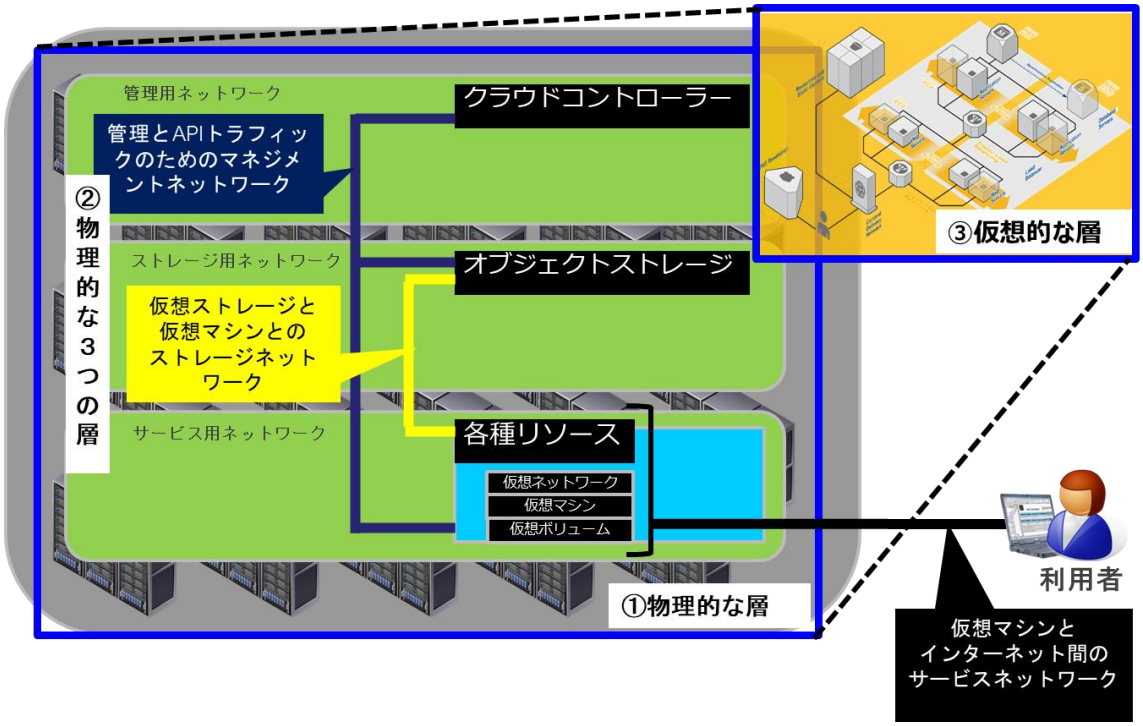


図２：クラウドネットワークの可用性・セキュリティを考慮した物理的な３つの層

このようなネットワーク構成は、プライベートクラウドのネットワークアーキテクチャを構築するための唯一の方法ではないが、共通的なベースラインです。

特にプライベートクラウドの場合は、パブリッククラウド事業者ほどの大きな規模を扱わないが、それでもなお、パフォーマンスとセキュリティとのバランスをとる必要があります。

ネットワーク仮想化のカテゴリ

クラウドでよく見られるネットワーク仮想化には、下記 2 つの主要なカテゴリがあります。

・VLAN

・SDN

また、ネットワーク要素を仮想化する NFV もネットワーク仮想化に主要なテクノロジーとなるため、本章の最後に概念を記載します。

	VLAN	SDN
メリット	・多くのネットワーク機器が標準対応 ・小規模組織への導入が容易	・運用/管理が容易 (ランニングコストの削減などが可能) ・クラウド環境でセキュリティを考慮した構成が可能
デメリット	・運用/管理が煩雑になりやすい ・クラウド環境のセキュリティ向け機能には向かない ・VLANの数に制限がある	・対応機器のコストが高い ・初期投資コストが高い

図３：VLAN と SND のメリットとデメリット

VLAN とは

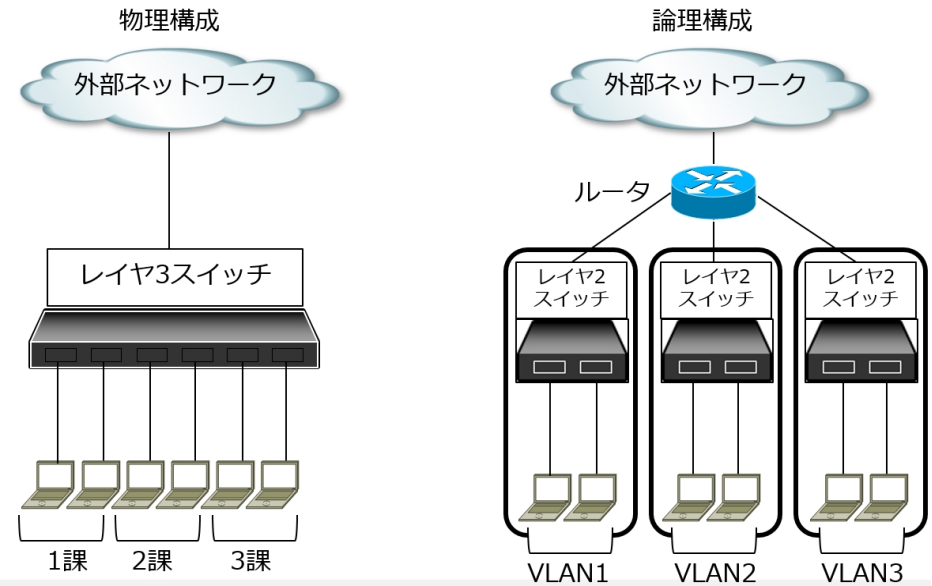


図４：VLAN(Virtual Local Area Network)とは

VLAN 機能を使うことでネットワーク配線を変更せずに論理的にネットワークを分割することが可能です。

VLAN のデメリットとして以下のようなハードウェア依存があります。

・ベンダー固有の OS

→ 機能とライセンス

→ ユーザインターフェイス

・ベンダー固有のハードウェアアーキテクチャ

→ チップ(ASIC)

→ ファブリック

図 5 ：VLAN のハードウェア依存

VLAN は、ほとんどのネットワークハードウェアで実装される既存のネットワーク技術を利用します。クラウドコンピューティングを使わない場合でも、企業ネットワークで極めて一般的に使われ、単一組織のネットワーク（企業内データセンター）において、異なるビジネスユニットや機能など（ゲスト用ネットワークなど）を分離するために使うように設計されています。

また、クラウド規模の仮想化あるいはセキュリティ向けには設計されていませんし、それだけでネットワークを分離するための効果的なセキュリティコントロールになると考えるべきではありません。

VLAN は、決して物理的なネットワーク分離を置き換えるものではありません。

VLAN のデメリットとしては、上記図 5 の通り、ベンダー固有の OS を搭載していることから、ベンダー毎に機能・ライセンス・ユーザーインターフェースがことなり、汎用性が欠けます。また、機器毎に設定を実施する必要があり、運用が煩雑になります。

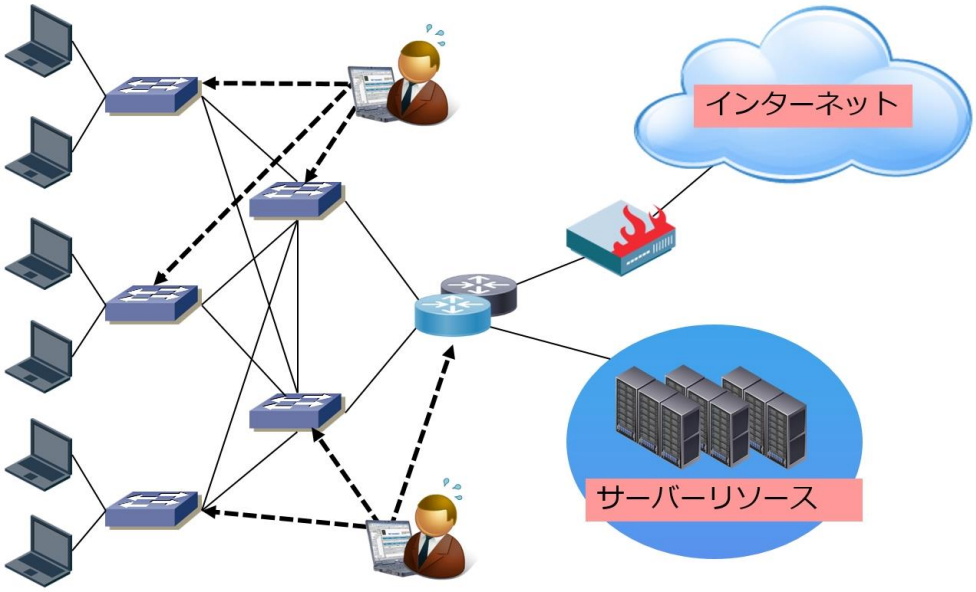


図 6 ：VLAN 運用上のデメリット

ネットワークの構成変更や追加毎に対象となる機器各々で個別に設定を行う必要があり、機器によっては、現物とのコンソール接続が必要となる等、人的リソース枯渇につながります。

このデメリットを解決する手法として SDN が登場し、SDN コントローラにより各ネットワーク機器の一元的な設定・管理が可能なため運用コスト削減などさまざまなメリットがあります。

SDN については、次項で詳しく説明します。

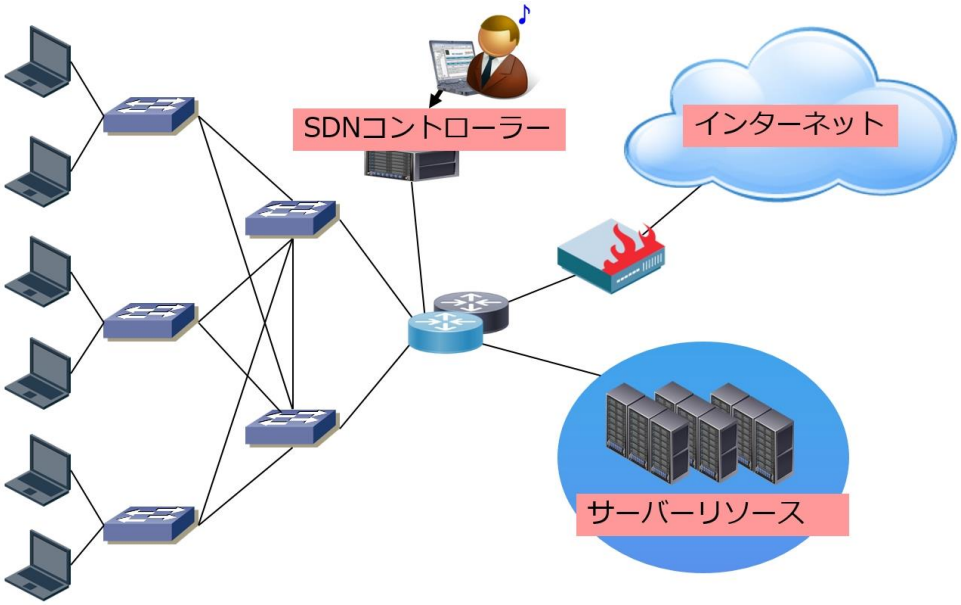


図 7 ：SDN 運用上のメリット

SDN の基本概念

SDN は、ネットワークを個別に設定するのでなく、ネットワーク全体をコントローラで一括して設定、管理し、ネットワークの仮想化/抽象化を行う技術です。

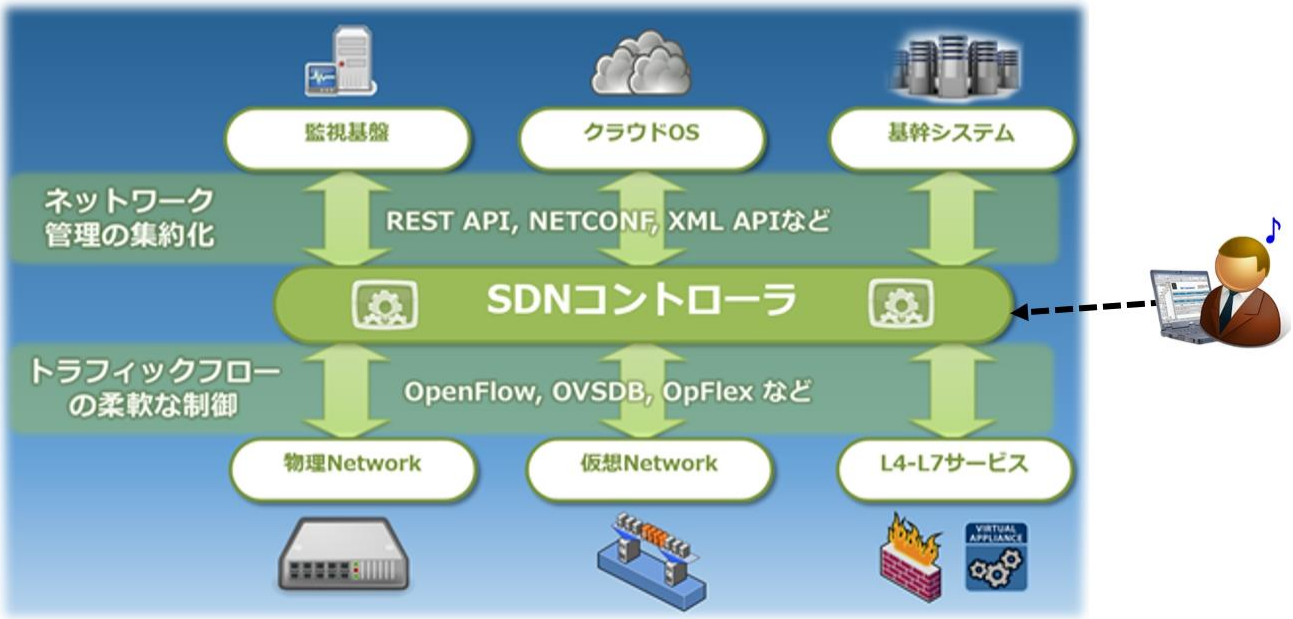


図 8 ：SDN の基本概念

SDN は、ネットワーキングハードウェアの上に形成される、より完全な抽象的化された層で、ネットワークコントロールプレーンとデータプレーンとを切り離します。また API を利用し、統合管理と柔軟性をサポートします。

SDN には複数の実装があり、標準に基づくものや、独自の実装もあります。また、従来 LAN の限界を超えてネットワーキングを抽象化することができるため、例えば、ネットワークを分割する上での VLAN 上限(4094)が、SDN 環境では、VLAN と異なり識別子で論理ネットワークを区別するため、VLAN に捕らわれない構成が可能です。

さらに、従来 LAN では、複数の経路が存在する場合、トラフィックのループを回避するために STP による通信制御が必要となり、その影響で片方の経路は、利用不可となってしまいましたが、SDN 環境では、このような制限も発生しないためより高い柔軟性と隔離を提供できます。

振り返ってみると、今日の多くのクラウドコンピューティングでは、SDN を使用してネットワークを仮想化しているため、下層にある物理インフラからネットワーク管理プレーンを抽象化し、多くの典型的なネットワーク上の制約を取り除きます。（VLAN は、マルチテナントのために重要な隔離機能がないため、クラウドでの配備には適さないです。）

例えば、すべてのトラフィックが適切に分離され隔離されることで、同じ物理ハードウェア上で、複数の仮想ネットワークを、そのアドレス範囲と完全に重複するものでもオーバーレイすることができます。

仮想ネットワークは物理ネットワークとはまったく異なります。物理ネットワーク上で動作するが、抽象化によって、ネットワークの挙動を大きく変えることが可能になり、その結果、多くのセキュリティのプロセスや技術に影響を及ぼします。

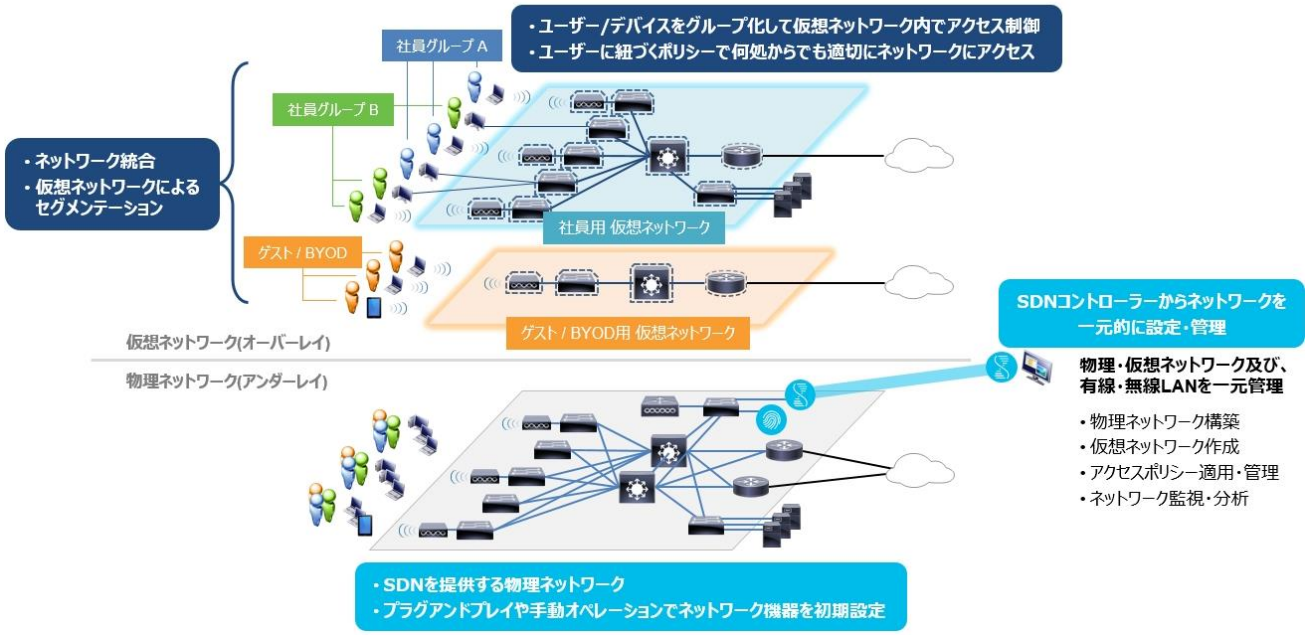


図９：SDN ネットワークイメージ（オーバーレイ・アンダーレイ）

例えば、複数の分離された重複 IP アドレスは、同じ物理ネットワークの上に仮想ネットワークとして配置できます。

適切に実装すれば、また標準的な VLAN とは違って、SDN は効果的なセキュリティ隔離の境界区分を提供します。

SDN は一般的に、ソフトウェア定義による任意の IP 範囲を提供し、クラウド利用者は既存のネットワークをクラウドに上手に拡張することができます。

もしクラウド利用者が 10.0.0.0/16 の CIDR(Classless Inter-Domain Routing)ブロックを必要とするならば、下にあるネットワークアドレス体系が何であれ SDN は提供できます。

SDN は通常、複数のクラウド利用者が同じ内部ネットワーク IP アドレスブロックを使うことさえサポートできます。

表面的に SDN は、クラウド利用者にとって通常のネットワークのように見えるかもしれないが、もっと完全な抽象化によって、水面下では非常に様々な機能を発揮します。

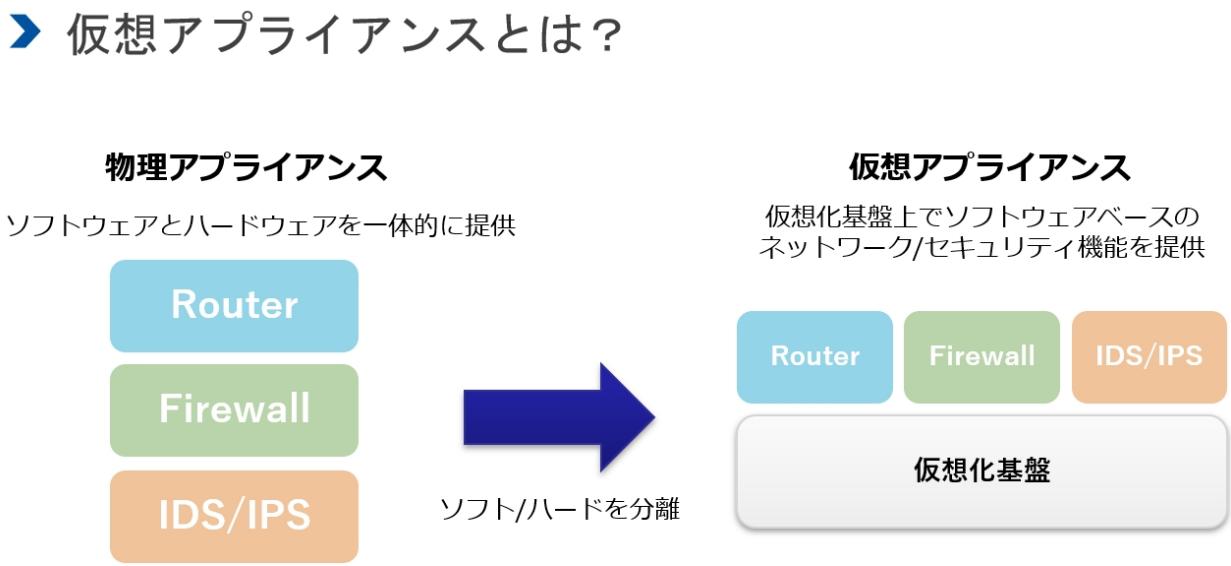
SDN を構成する技術と管理は、クラウド利用者がアクセスするものでないように見えるが、実のところもう少し複雑です。

例えば SDN は、パケットのカプセル化を使って、仮想マシンと他の「標準的な」資産が、それらの下にあるネットワークスタックにいかなる変更も行わなくてよいような機能を提供することが可能です。

仮想化スタックは、仮想ネットワークインタフェースに接続した標準的な OS からパケットを受け取ると、パケットをカプセル化してそれらを実際のネットワークに流します。

仮想マシンは、ハイパーバイザーが提供する、互換性のある仮想ネットワークインタフェース以外に SDN のことを知る必要がありません。

NFV とは



参考：ネットワンシステムズ
ネットワン NFV の全貌と市場への挑戦①
https://www.netone.co.jp/knowledge-center/blog-column/knowledge_takumi_038/index.html

図 10：NFV とは

ネットワーク機器は、従来専用の物理アプライアンスという形でソフトウェアとハードウェアが一体的に提供されてきました。

対して仮想アプライアンスは NFV（Network Function Virtualization）とも呼ばれ、専用アプライアンスで提供されていたネットワークおよびセキュリティ機能を仮想化基盤上のソフトウェア（仮想マシン）で実現するものです。

ネットワーク機器をソフトウェアとハードウェアに分離し、汎用サーバーで構成された仮想化基盤上でネットワークおよびセキュリティ機能を提供します。

今までサーバーで培われてきた仮想化や自動化といった技術を、ネットワーク/セキュリティ機器に活用することで、設備/運用コストの削減やリソースの最適化、迅速なサービス展開等の実現を目標としています。

NFV は、ヨーロッパの標準化団体である ETSI（European Telecommunications Standards Institute）配下に設立された NFV ISG（NFV Industry Specification Group） を中心に議論が進められています。

ETSI NFV ISG の NFV アーキテクチャーでは、仮想アプライアンスのようなネットワーク機能を仮想化するだけには留まらず、仮想化されたネットワーク機能やそれを提供するためのインフラの管理、運用の自動化等についても検討が進められています。

ETSI NFV のハイレベルフレームワークは以下のように定義されています。

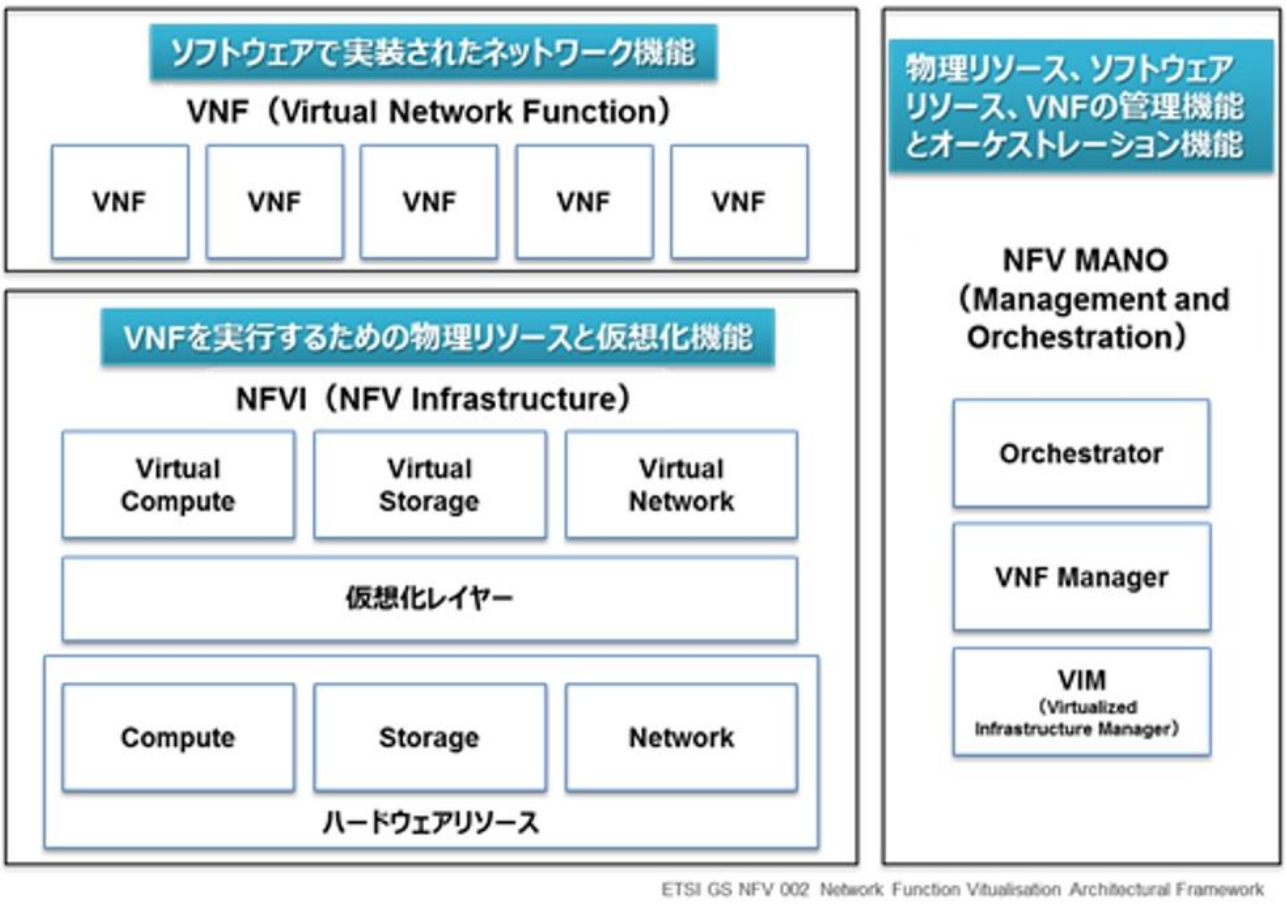


図 11：ETSI NFV のハイレベルフレームワーク

ETSI NFV のアーキテクチャーは、VNF、NFVI、NFV MANO という 3 つの領域に分かれています。
VNF（Virtual Network Function）は、「ソフトウェアで実装されたネットワーク機能」であり、仮想マシンとして動作するネットワーク機器を表します。

NFVI（NFV Infrastructure）は、VNF を実行するための物理リソースと仮想化機能です。NFVI には、IA サーバーやストレージ等のハードウェアリソースと、仮想化のためのハイパーバイザーが含まれます。

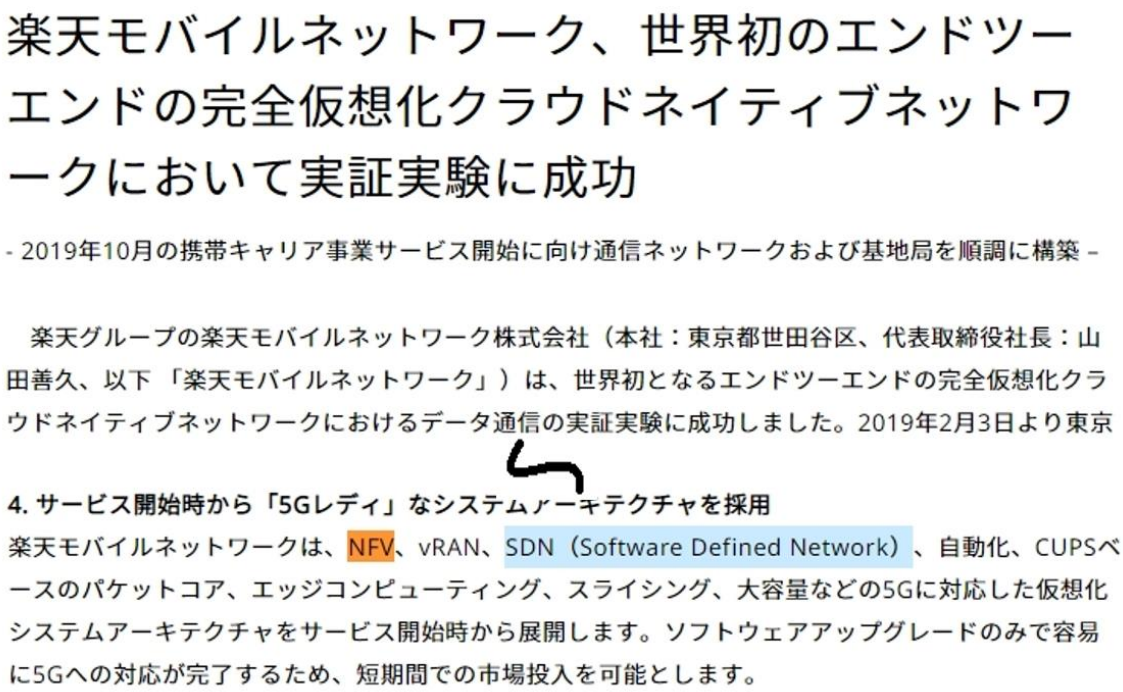
NFV MANO（Management and Orchestration）は、物理リソース、ソフトウェアリソース、VNF の管理機能とオーケストレーション機能を提供します。MANO は、自動化の中心的な役割を担う「Orchestrator」、VNF の管理を行う「VNF Manager」、NFVI の制御を行う「VIM（Virtualized Infrastructure Manager）」で構成されます。

NFV ではオープンソースソフトウェアの利用も注目されています。
2014 年に発足したオープンソースプロジェクトである OPNFV（Open Platform for NFV）では、オープンソースソフトウェアを組み合わせたキャリアグレードの NFV プラットフォームの実現に向けて活動が行われています。

2015 年 6 月に最初のリリースである「Arno」が公開されました。「Arno」では、OpenStack、KVM、OpenDaylight 等のソフトウェアを組み合わせて、ETSI NFV アーキテクチャーの NFVI と VIM 機能を提供しています。

NFV 事例

近年、SDN・NFV の技術を全面的に使いサービス展開を行った楽天モバイルネットワークの事例です。



楽天モバイルネットワーク、世界初のエンドツーエンドの完全仮想化クラウドネイティブネットワークにおいて実証実験に成功

- 2019年10月の携帯キャリア事業サービス開始に向け通信ネットワークおよび基地局を順調に構築 -

楽天グループの楽天モバイルネットワーク株式会社（本社：東京都世田谷区、代表取締役社長：山田善久、以下 「楽天モバイルネットワーク」）は、世界初となるエンドツーエンドの完全仮想化クラウドネイティブネットワークにおけるデータ通信の実証実験に成功しました。2019年2月3日より東京

4. サービス開始時から「5Gレディ」なシステムアーキテクチャを採用

楽天モバイルネットワークは、NFV、vRAN、SDN（Software Defined Network）、自動化、CUPSベースのパケットコア、エッジコンピューティング、スライシング、大容量などの5Gに対応した仮想化システムアーキテクチャをサービス開始時から展開します。ソフトウェアアップグレードのみで容易に5Gへの対応が完了するため、短期間での市場投入を可能とします。

出典：
https://corp.rakuten.co.jp/news/press/2019/0212_06.html

図 12：SDN・NFV 事例

3. クラウドインフラストラクチャの管理

※本章はセキュリティガイダンス 「*8-1-2-2*」章の解説となります。

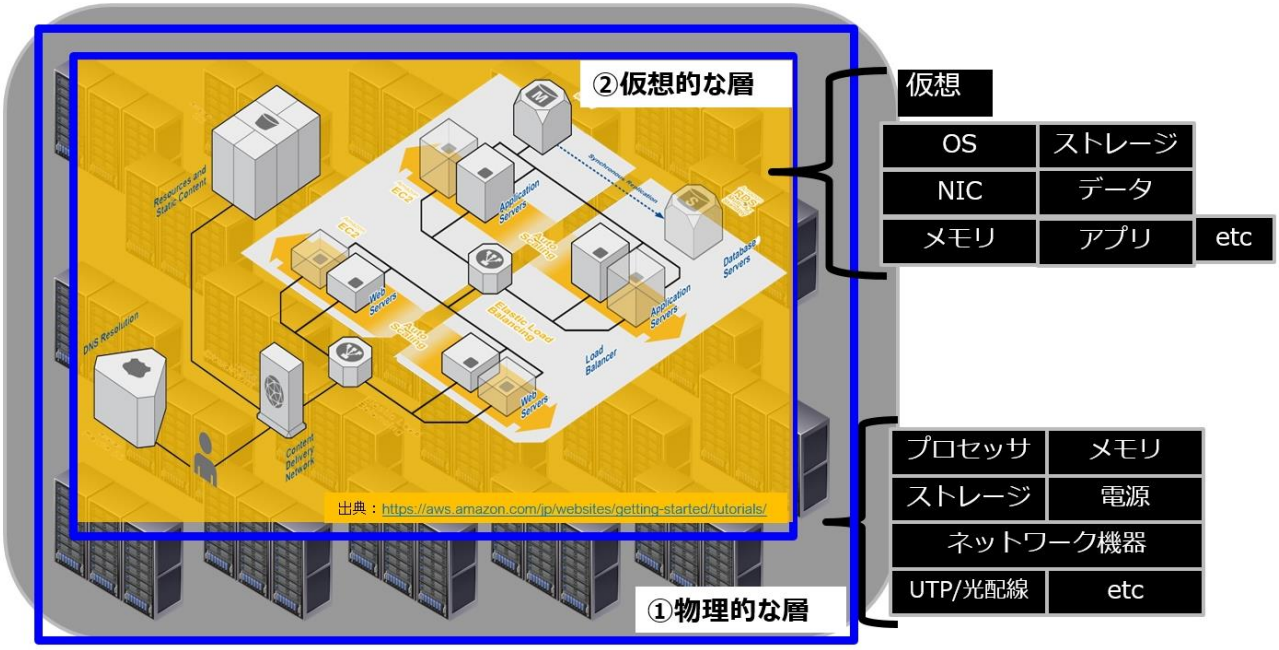


図 13：クラウドインフラストラクチャの管理

管理インフラストラクチャ

クラウドコンピューティングの仮想ネットワークは常にリモート管理をサポートしているため、管理用ダッシュボードやメタストラクチャのセキュリティは重要です。

場合によっては、複雑なネットワーク全体を、少数の API 呼び出しや Web コンソール上の数回のクリックにより、構築したり、また破壊したりすることも可能です。

クラウド事業者の責任

クラウド事業者は本来、セキュアなネットワークインフラを構築し、適切に設定する責任があります。

セキュリティの絶対的な最優先事項は、テナントが他のテナントのトラフィックを参照できないようにするための、ネットワークトラフィックの分離と隔離です。

これは、全てのマルチテナントネットワークで最も基本的なセキュリティ制御です。

クラウド事業者は、テナント間でデータや設定を見えるようにしてしまう可能性のあるパケットスニッフィングやその他のメタデータの「漏洩」を無効にする必要があります。

またテナント独自の仮想ネットワーク内であっても、パケットスニッフィングを無効にする必要があります。

それにより、非仮想ネットワーク上では一般的である、攻撃者があるノードに侵入してネットワークをモニタ（スニッフィング）する可能性を減らすべきです。

タギングやその他の SDN レベルのメタデータもまた、管理用ダッシュボードの外部に曝されないようにすべきである。さもないと、侵入されたホストが SDN 自体の中に入り込むために使われる可能性があります。

すべての仮想ネットワークでは、ホストファイアウォールや外部製品を必要としないで済むように、クラウド利用者用に組込みのファイアウォール機能を利用可能とすべきです。

クラウド事業者はまた、基盤となる物理ネットワークと仮想化プラットフォームに対する攻撃を検出して防御する責任があります。その責任には、クラウド自体の境界セキュリティも含まれます。

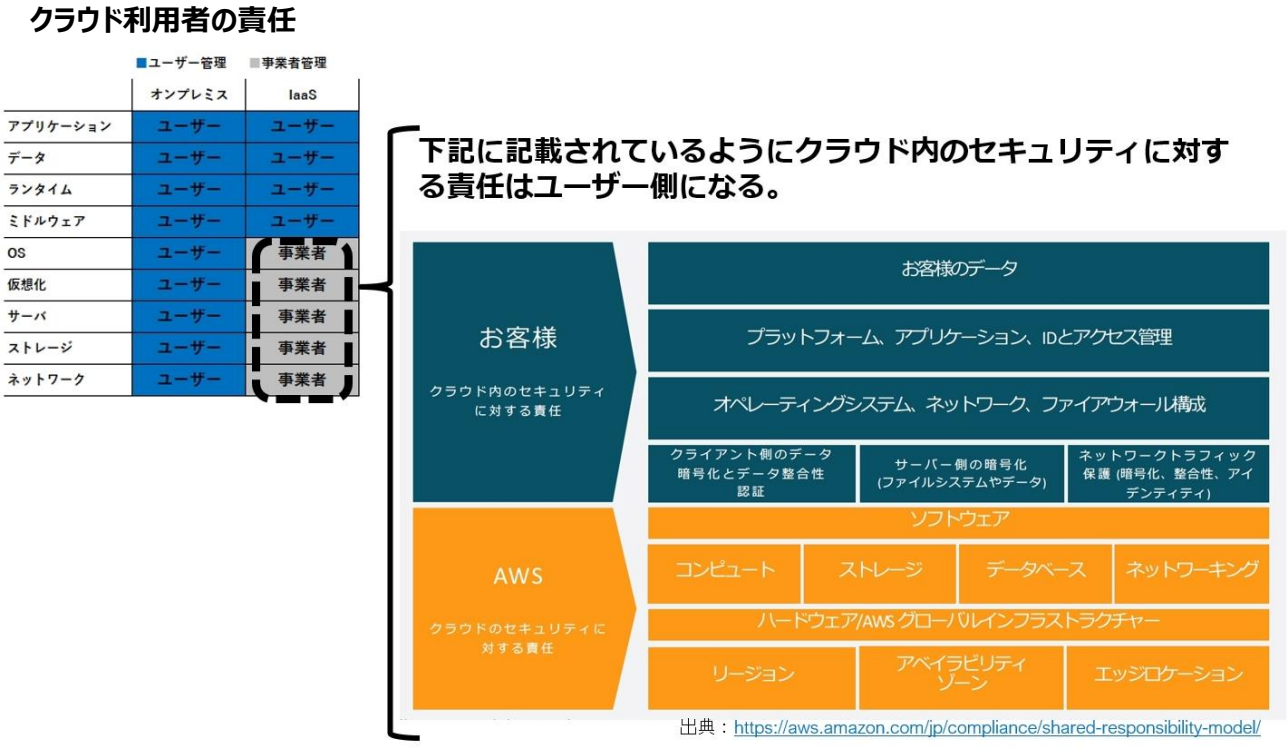


図 14：クラウド事業者とクラウド利用者の責任分界点

クラウドの利用者は第一に、仮想ネットワーク、特に全ての仮想ファイアウォールの配備を適切に設定する責任があります。

物理的な接続やルーティングに制約されないため、ネットワークアーキテクチャは仮想ネットワークのセキュリティにおいてより大きな役割を担っています。

仮想ネットワークはソフトウェア構造であるため、複数の別々の仮想ネットワークを使用すると、従来の物理ネットワークでは不可能な、マイクロセグメンテーションの利点がもたらされる可能性があります。

すべてのアプリケーションスタックを各々の仮想ネットワークで実行でき、これにより、悪意を持った者が攻撃の足場を得た場合の攻撃にさらされる口が劇的に減少します。

物理ネットワーク上で同等のアーキテクチャーを築くことはコスト面で不可能です。

変更無用なネットワークは、ソフトウェアテンプレートを使用して、一部のクラウドプラットフォームで設定することができ、有効性が確認されている設定を適用するのに役立ちます。

有効性が確認されているネットワーク設定は、全ての設定を手動で設定するのではなく、テンプレートの中で全て定義できます。

このことにより、セキュアなベースラインを備えたネットワークを数多く構築する能力がなくても、有効性が確認されている設定からの逸脱を検出し、場合によってはそれを元に戻すこともできます。

クラウド利用者は、さらに、管理用ダッシュボード内に表示されるコントロールの適切な権限管理と構成設定に責任があります。

仮想ファイアウォールまたは監視機能がセキュリティニーズを満たしていない場合、クラウド利用者は仮想セキュリティアプライアンスまたはホストセキュリティエージェントにより補う必要があります。

4. クラウドネットワーキングでセキュリティがどのように変わるか

※本章はセキュリティガイダンス 「*7-3*」章の解説となります。

クラウド環境におけるネットワークの侵入検知

クラウド利用以前の企業 ICT ネットワークにおいて、セキュリティを高める上で重要となるネットワークの侵入検知対策とは、どのようなものであったでしょうか。クラウド以前の環境においては、物理のサーバー間で実際に流れる通信を、物理的に侵入検知システム（IDS）/侵入防止システム（IPS）を設置して、通信を複製又は直接監視していました。IDS は、ネットワークに発生するイベントを監視し、不正侵入等セキュリティ侵害の兆候を検知し、管理者に通知します。また IPS は、検知した不正を自動的に遮断します。

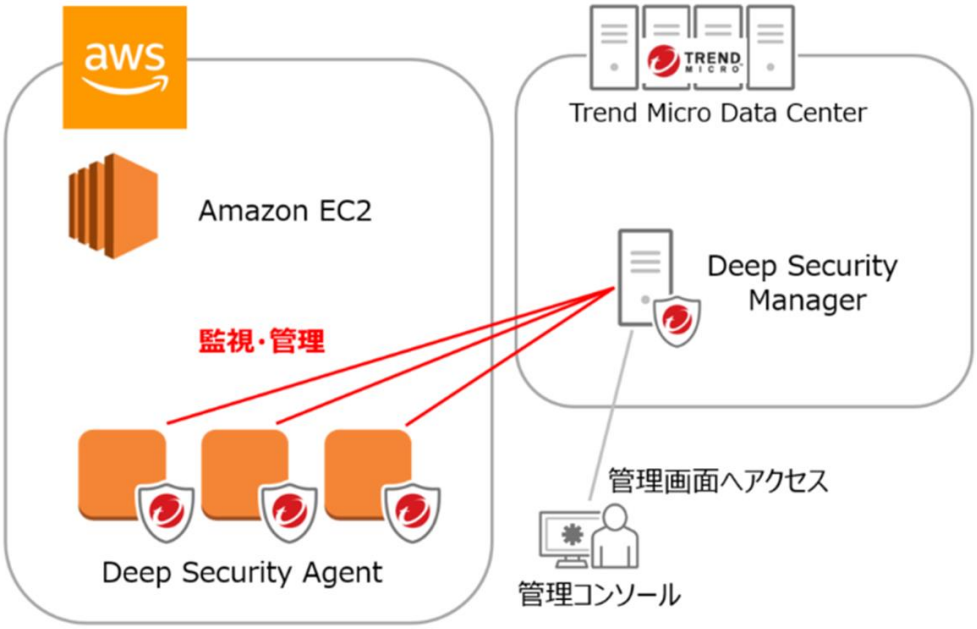
物理環境の通信を監視対象としてきた、従来の物理 IDS/IPS におけるネットワーク侵入検知機能は、監視対象のトラフィックがあくまで物理環境を流れる通信であり、一方クラウド環境においては、監視対象となる通信がクラウドのインスタンス及び仮想マシン間の通信であることから、機能しません。したがってクラウド環境においては、環境に適した侵入検知機能を採用する必要があります。そこで、クラウド環境における IDS/IPS の実装に関する考え方は、次の 2 種類が考えられます。

- 仮想アプライアンスによる検知
- 各インスタンスにインストールするソフトウェアベースの検知

ただし前者は、システムの性能面においてボトルネック箇所を生む事になり、後者は多くの仮想マシンが稼働するクラウド環境において、物理サーバーの CPU 負荷を高めやすい、というデメリットが存在します。したがってクラウド環境に適した、侵入検知手法を選択する必要があります。

クラウド環境に適した、侵入検知方法とは

クラウド環境においても、物理サーバーやオンプレミスの環境と同等のセキュリティを実現するにはどうすればいいのでしょうか？　具体的な実装例として、Amazon AWS 上のインスタンスのセキュリティ保護、侵入検知を行う製品である、Trend Micro Deep Security（以下、Deep Security）を取り上げます。



出典：https://esp-online.com/solutions/trend-micro-deep-security-service

図 15：クラウド環境に適した、侵入検知方法とは

こちらの製品は、ウィルス対策、IPS/IDS（侵入検知）、ファイアウォール、セキュリティログ監視等を総合的に提供します。Deep Security Manager と呼ばれる仮想アプライアンス型の管理サーバーから、各 AWS のインスタンス上に上記の保護モジュールが Deep Security Agent としてインストールされます。

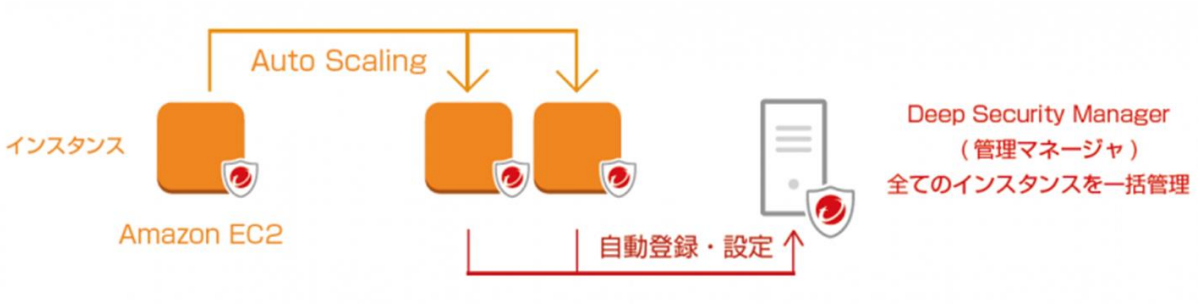
特徴として各 AWS インスタンス上で、脆弱性に対応する IPS/IDS ルール「仮想パッチ」が動作する事で、攻撃から各インスタンスを保護する事が可能な点が挙げられます。Windows、Linux の主要なサーバーOS や、Apache、WordPress、Oracle Database 等多くの OS やアプリケーションに対応し、OS やミドルウェアで対応できないセキュリティ防御の仕組みを提供します。

適用するルールは、「防御モード」（パケットを破棄するモード）と、「検出モード」（イベントのみをログに記録しトラフィックは通過させるモード）を選択することが可能です。

「防御モード」は、疑わしいパケットは通さずに遮断する仕組みで、不正アクセスや攻撃と思われるパケットをすべて遮断することでネットワークの安全性を維持するための仕組みです。一方、「検出モード」では疑わしい通信があった場合に、管理者に通知します。

導入にあたり、最初は「検出モード」で様子を見て、正常動作を確認後に、「防御モード」に移行する事で、誤検知による通信遮断を防いで、安全に導入する事が可能です。

また、AWS のオートスケーリングで増えたインスタンスにも自動で Deep Security エージェントはインストールされ、手動で管理を実施する必要はありません。クラウド環境で利用される事の多い、Docker コンテナ環境にも対応しています。



出典：https://esp-online.com/solutions/trend-micro-deep-security-service

図 16：Auto Scaling への対応

このようにクラウド環境に合った形の製品を選択する事で、セキュリティ保護を適切に行う事が可能です。

5. 仮想アプライアンスの課題

※本章はセキュリティガイダンス 「*7-3-1*」章の解説となります。

仮想アプライアンスには物理アプライアンスとは異なる課題があります。以下に挙げる点をそれぞれ解説していきます。

① フェイルオープンができないため、障害時にボトルネックとなりうる

② パフォーマンスを出すためのリソース、コストが増加する

③ オートスケーリングをサポートしているか？

④ マルチリージョン、マルチ AZ による可用性への対応

⑤ 変化の頻度による運用ポリシーの設計

① フェイルオープンができないため、障害時にボトルネックとなりうる

仮想アプライアンス版の IDS/IPS も各セキュリティベンダーや、パブリッククラウドにて提供されていますが、フェイルオープンに対応していないケースがあります。

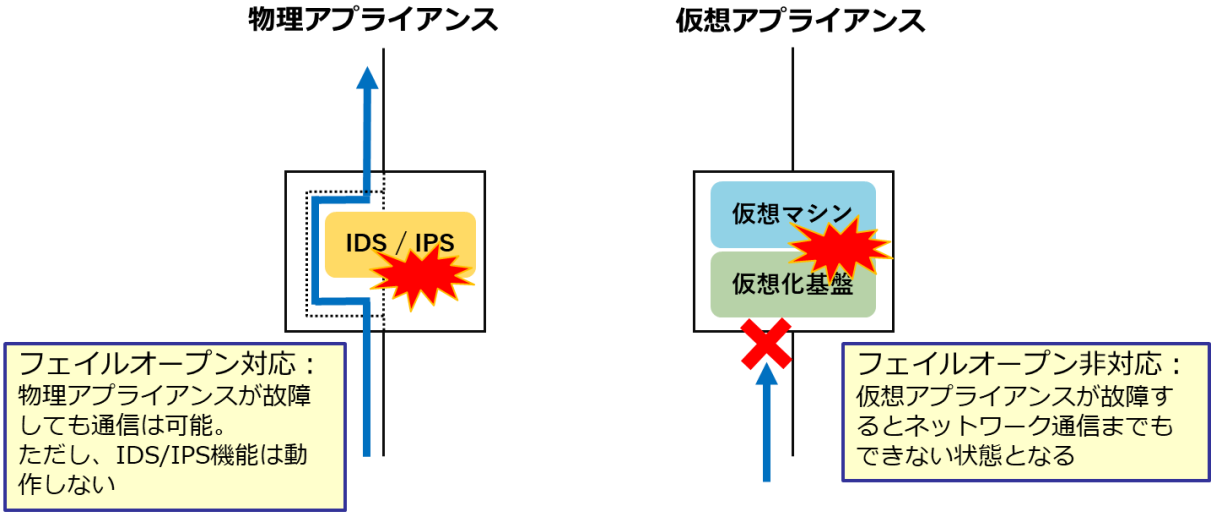


図 17：フェイルオープンができないため、障害時にボトルネックとなりうる

フェイルオープンはハードウェアが故障したときには物理的な経路に切り替えて全ての通信を通すモードです。このモードになった場合には、IDS/IPS の機能は使用できず、悪意のある攻撃を遮断することができなくなりますが、ネットワークの通信は止まることがありません。セキュリティより通信サービスを優先する形になります。

各社が提供している物理アプライアンスの IPS/IDS ではフェイルオープンに対応していますが、仮想アプライアンス版はソフトウェアでの構成になるためフェイルオープンを実装できず、仮想アプライアンスのフェイルオーバー（冗長）構成にするといった設計が必要となります。

② パフォーマンスを出すためのリソース、コストが増加する

一般的な仮想化環境において、パケット転送処理のボトルネックポイントが存在します。Linux に代表される汎用 OS はネットワーク処理専用に開発された物では無く、様々な要因で割り込み処理が発生するため、カーネルが提供するネットワーク機能はパケット転送処理におけるボトルネックと成り得ます。

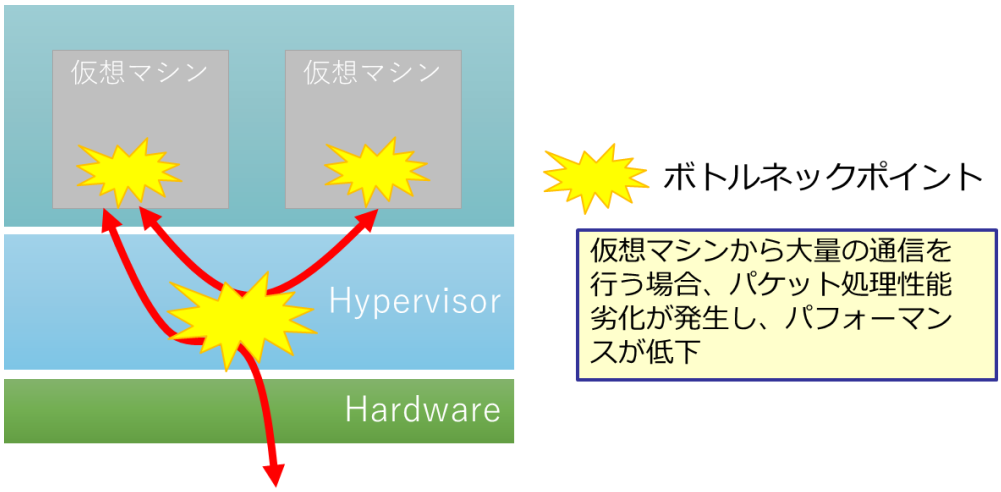


図 18：パフォーマンスを出すためのリソース、コストが増加する

ホスト OS であるハイパーバイザーおよび、ゲスト OS である仮想マシン自身でそれぞれボトルネックポイントがあるため、仮想マシンから大量の通信を行う場合、パケット処理性能劣化が発生します。

このようなボトルネック問題に対し、複数の方策が提供されています。代表的なものに DPDK（Data Plane Development Kit）、PCI Pass Through with SR-IOV（Single Root I/O Virtualization）等の方

式でパケット処理向上技術が提供されますが、これらの機能をサポートしていない場合もあり、期待するパフォーマンスを出すためには仮想アプライアンスの台数が多く必要となり、リソース増、コスト増となりえます

③ オートスケーリングをサポートしているか？

ファイアウォール、WAF、IDS/IPS といったセキュリティデバイスにおいても仮想アプライアンスへの対応が増えています。また、仮想アプライアンス製品について、AWS 等のパブリッククラウド上で稼働させ、オートスケーリング機能を有効化することで、トラフィックの状況に応じて動的にインスタンスを追加してキャパシティ拡張できる機能を提供します。これは物理アプライアンスにはないメリットになります。

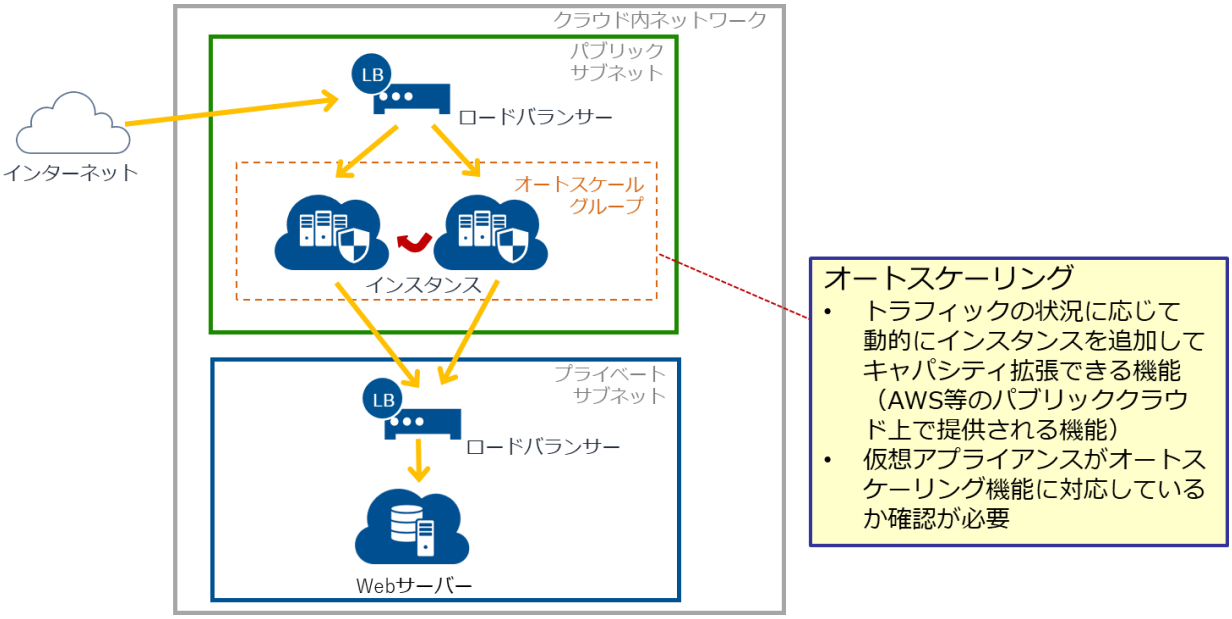


図 19：オートスケーリングをサポートしているか

注意点として仮想アプライアンスのライセンスがオートスケーリング機能に対応していることを確認する必要があります。例えば、台数ライセンスの場合、オートスケーリングによりインスタンスが追加されてしまうと、ライセンス台数を超えてしまい、機能しないケースも考えられます。スループットやデータ使用量をベースにしたオートスケーリング対応のライセンス体系である必要があります。

④　マルチリージョン、マルチ AZ による可用性への対応

AWS や Azure のようなパブリッククラウドではインフラがリージョンおよびアベイラビリティゾーン(AZ)という構成単位で提供されています。リージョンは国、地域単位での構成を表しており、全世界に約 20 か所のリージョンで構成されています。AZ はデータセンター単位を表しており、1 つのリージョンは 2 つ以上の AZ から成り立っており、同一リージョン内の各 AZ は地理的に離れた場所のデータセンターに置かれています。これをマルチリージョン、マルチ AZ と言います。マルチリージョン、マルチ AZ を利用することによって自然災害、停電等による地理的要因に対しての耐障害性向上につながります。

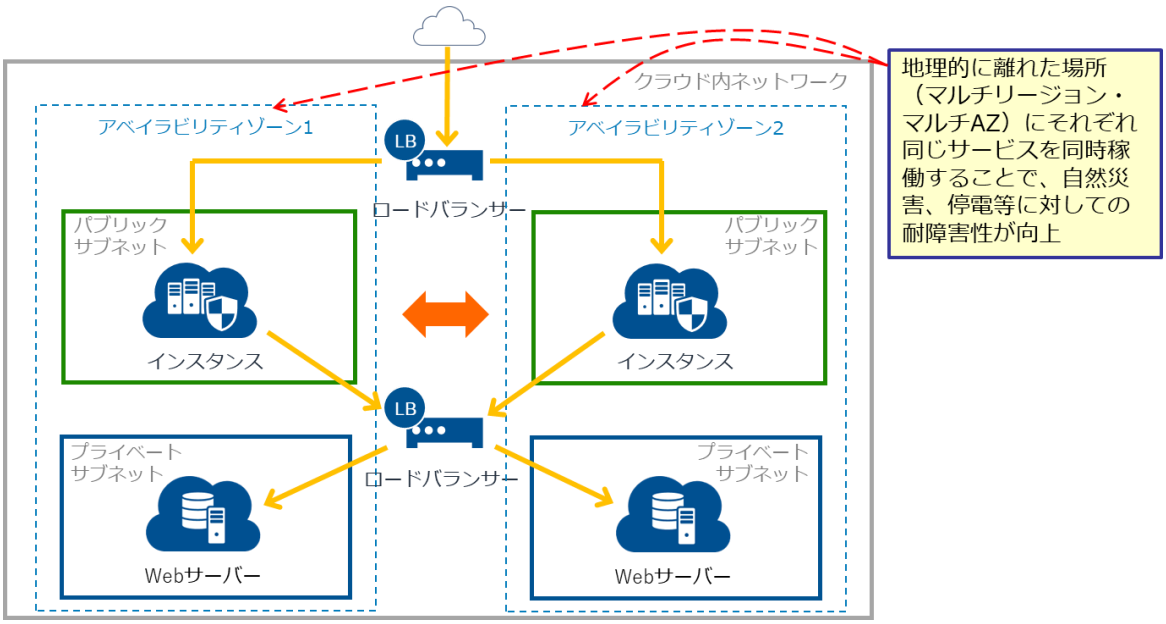


図 20：マルチリージョン、マルチ AZ による可用性への対応

注意点として一般的にパブリッククラウドにおいて AZ を跨いだ通信は利用料が発生するためコスト増加と、AZ 間の距離によっては、速度低下を招く場合があるため、これらを念頭に置いて設計する必要があります。

⑤　変化の頻度による運用ポリシーの設計

従来の物理アプライアンスの監視・管理では IP アドレスをベースとしており、物理アプライアンスの増減、変更の度にポリシー設定の追加変更が必要とされていました。仮想アプライアンスはオートスケーリングによって使用状況に応じてインスタンスの増減が頻繁に発生する場合もあり、そのためセキュリティ、管理、監視といった運用ポリシーが変わってきます。

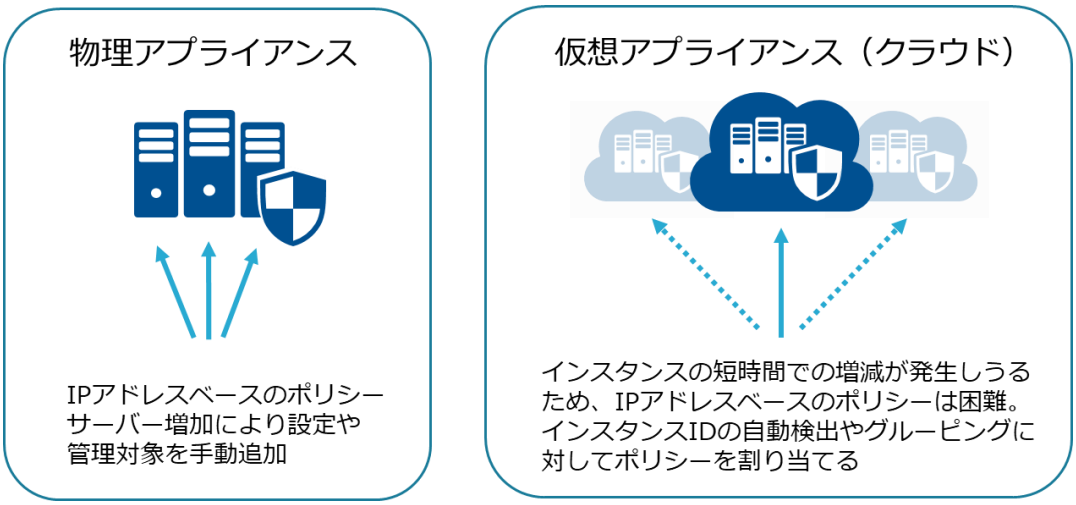


図 21：変化の頻度による運用ポリシーの設計

例えば、オートスケーリングによりインスタンスが追加起動し、短期間の稼働後に追加分が自動で終了するケースにおいて、

- インスタンスの追加による起動時においてファイアウォールルールの追加や監視対象機器の設定追加を自動で行う
- インスタンスの自動停止時には、停止アラートが飛ばないようにする

等の運用が必要となる場合もあります。

この場合、インスタンスが短時間の利用となり、IP アドレスが頻繁に変更される場合があり、また、同じ IP アドレスの使い回しも起こりうるため、IP アドレスベースでの運用は負荷が高くなってしまいます。そのため、IP アドレスによる識別ではなく、インスタンス ID やグループポリシーなどを使った識別で運用する点を考慮する必要があります。

6. SDN のセキュリティ上の利点

※本章はセキュリティガイダンス「*7-3-2*」章の解説となります。

SDN の導入によるセキュリティ上のメリット

SDN の利用により、従来の物理ネットワーク環境では存在しなかった様々なセキュリティ保護が可能となります。以下にセキュリティ上のメリットを説明します。

- ネットワークの隔離の容易性
- クラウド環境に適した柔軟なファイアウォール運用
- ファイアウォールの拡張性
- パケットの暗号化

これらの SDN におけるセキュリティ上の利点について、主要なオンプレミス・プライベートクラウド型の SDN 製品である、VMware NSX®Data Center（以下、NSX Data Center）を例に紹介します。

VMware NSX Data Center とは

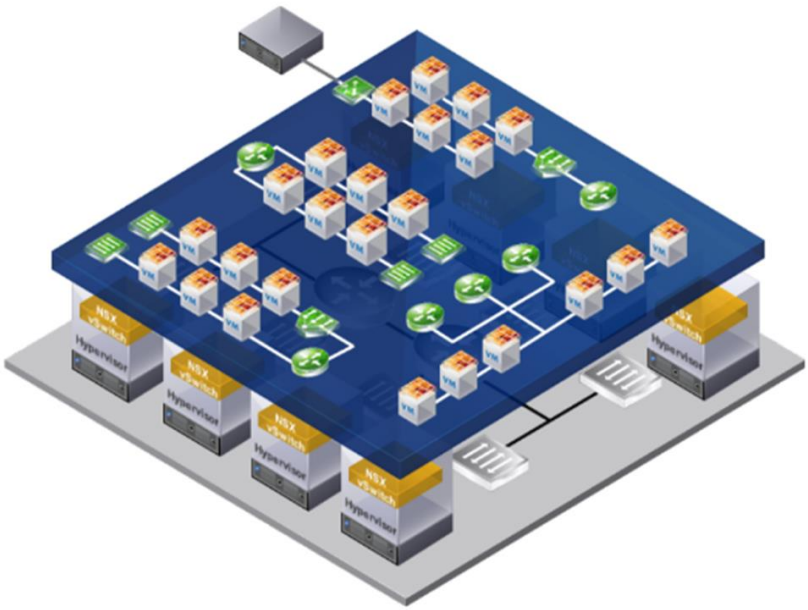


図 22：VMware NSX Data Center とは

NSX Data Center は、オンプレミスのクラウド環境においてネットワーク仮想化を実現するソフトウェアです。企業システム上で NSX Data Center を構成することにより、迅速性、柔軟性、管理性そしてセキュリティの向上を実現し、ソフトウェア型のネットワーク仮想化を実現します。サーバー仮想化がコンピュートリソースを抽象化して仮想マシンを提供するように、ネットワークを抽象化し、ネットワークの隔離、ルーティング、NAT、ファイアウォール、ロードバランサーなど、様々なネットワーク機能を、ソフトウェアとして提供し、必要な物理機器の台数を削減出来ます。従来ネットワーク機器で提供していた様々な機能を集約し、NSX Manager と呼ばれる管理コンポーネントから集中管理する事が可能です。

ネットワークの隔離の容易性

クラウドを活用した企業 ICT 環境において、多くの仮想マシンが稼働する環境の適切なセキュリティ保護は重要な問題です。外部ネットワークからのセキュリティ保護も重要ですが、もし、企業内部の仮想マシンが攻撃対象となった場合に、即座に該当仮想マシンをネットワーク環境から隔離する事が必要となります。SDN は、こうした隔離作業を簡単・迅速に行うことによって、企業システム環境全体への大きなインパクトを防ぐことが可能となります。

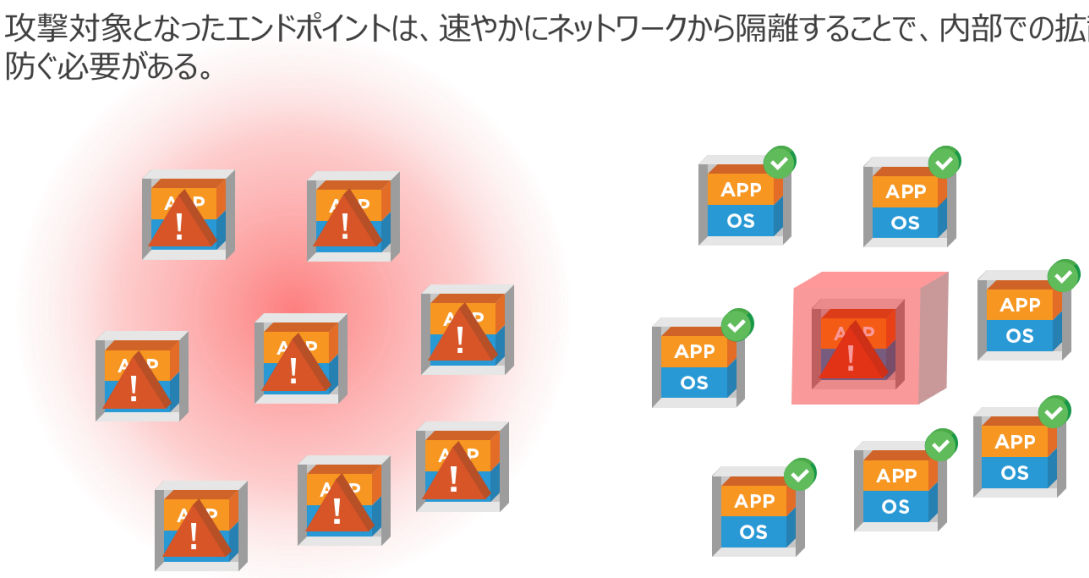


図 23：ネットワークの隔離の容易性

NSX Data Center と、Trend Micro Deep Security（以下、Deep Security）の連携利用により、マルウェア感染検知（攻撃検出）と拡散防止（攻撃対象の隔離）が可能になります。具体的には Deep

Security が仮想マシンのウィルス感染を検知したのち、即座に NSX Data Center が、該当の仮想マシンを通常のネットワークから隔離セグメントに移動させます。この仕組みの導入により、同じネットワーク内の他の仮想マシンへの感染拡大を防ぐことが可能です。

クラウド環境に適した柔軟なファイアウォール運用

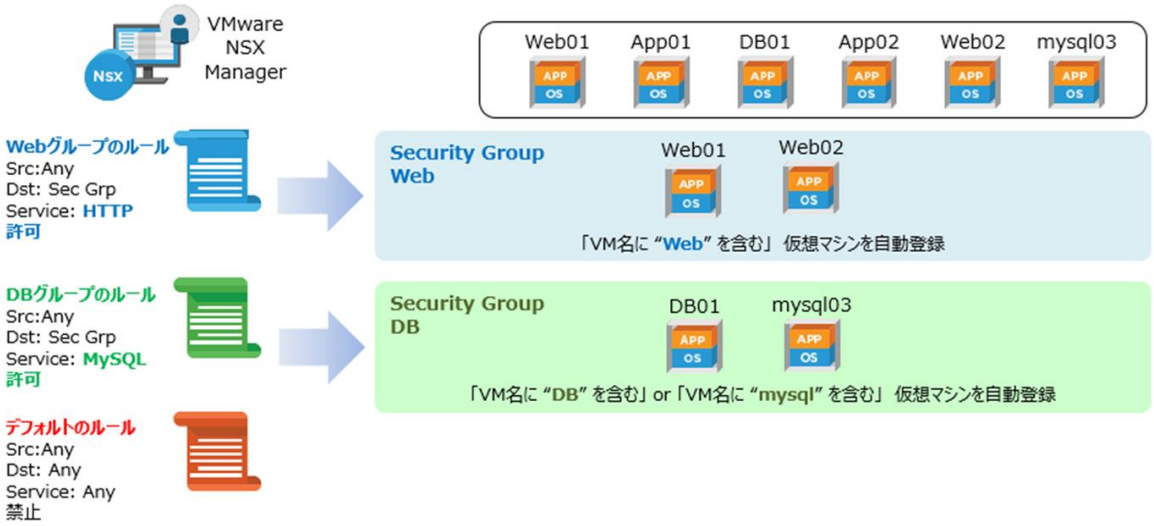
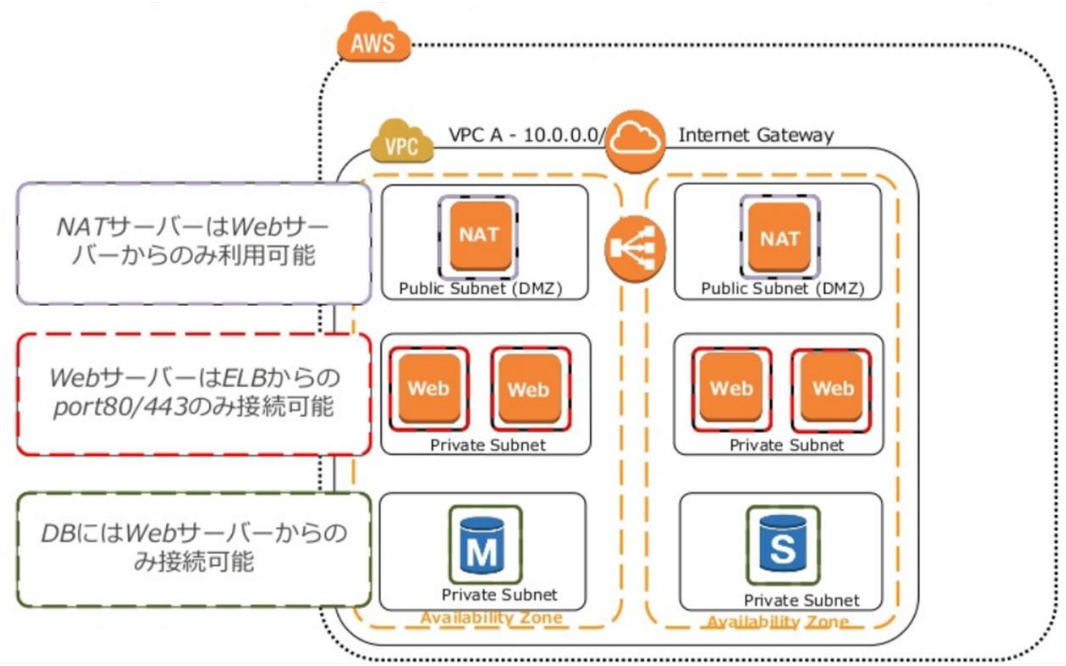


図 24：クラウド環境に適した柔軟なファイアウォール運用

SDN のファイアウォールは、従来の物理のファイアウォールによる運用と異なり、物理ネットワークの境界内部のみの保護でなく、クラウド環境全体において、より柔軟なルールで運用できます。例えば NSX Data Center において、仮想マシンを名前単位でグループ化し（例：仮想マシン名に「Web」を含む Web サーバー群）グループ毎に個別のファイアウォールルール（例：「Web」グループには HTTP 通信を許可）を定義出来ます。これによって、新たに名前に「Web」を含む仮想マシンが増設された場合、該当の仮想マシンには「Web」グループのファイアウォールが自動で定義されます。このように動的な仮想マシングループを利用したファイアウォールの定義により、仮想マシンの増設の際にも、手動による追加のファイアウォールの設定は不要で、運用負荷の削減と作業ミスを防ぎ、セキュリティの向上を図る事が可能です。AWS における Auto Scaling のような、仮想マシンのスケールアウトする環境に柔軟に対応可能です。

また、パブリッククラウドにおけるファイアウォールの運用について、AWS (Amazon Web Services) の例を見ていきます。AWS にはセキュリティグループと呼ばれる、EC2 インスタンスに適用可能な標準のファイアウォール機能が存在します。セキュリティグループは、EC2 インスタンスへのアクセスを許可し、トラフィックを制御するファイアウォールとして動作します。また、1 つのセキュリティグループを複数の EC2 インスタンスに割り当てることもできます。



出典：https://www.slideshare.net/AmazonWebServicesJapan/aws-webinar-47323216

図 25：AWS ファイアウォール運用　Security Group

例えばセキュリティグループを利用する事で、Web サーバー群は、負荷分散の ELB(Load Balancer)からのみアクセスを許可し、DB サーバー群は、Web サーバーからのアクセスのみを許可するといった、仮想サーバー毎の共通の設定を行う事が出来ます。各セキュリティグループは、EC2 インスタンスへのアクセスを許可するトラフィックのデフォルトのルールを設定し、ここで許可しないアクセストラフィックは全て拒否されます。

SDN のファイアウォールは、パブリッククラウド、プライベートクラウドの区別を問わず、デフォルトで通信を禁止し、許可する通信を定義するホワイトリスト型の形式を取る事が多く、一般的な物理でのファイアウォールの運用と異なりますが、ポートの閉め忘れのようなトラブルを防げる効果もあり、よりセキュアなモデルを採用しています。

ファイアウォールの拡張性

クラウド環境における SDN のセキュリティ上のメリットとして、ファイアウォールの拡張にあたって、簡易性の向上が挙げられます。

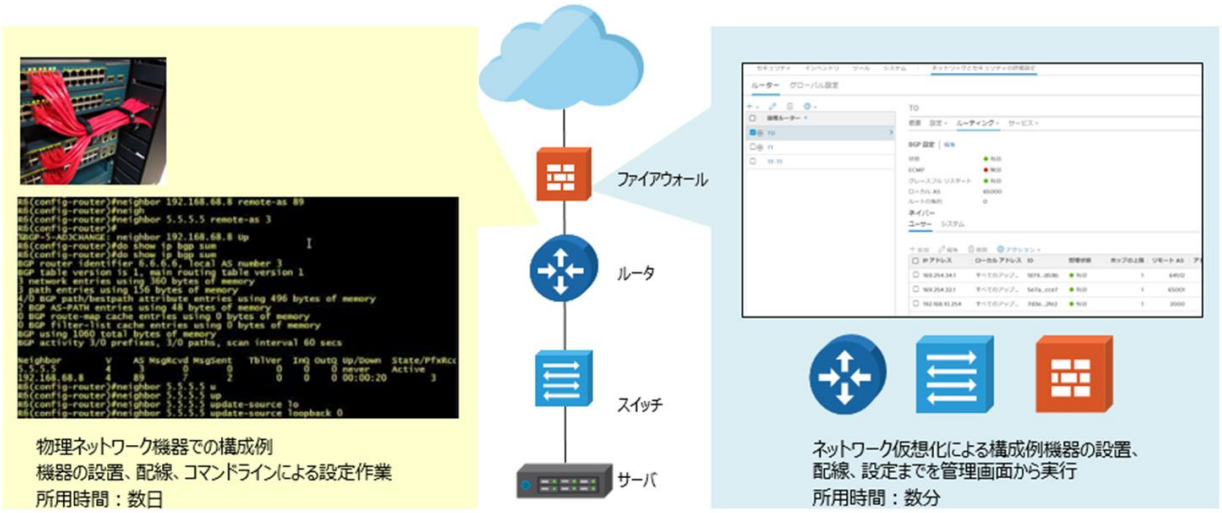


図 26：ファイアウォールの拡張性

従来の物理ネットワーク機器によるセキュリティ保護と異なり、SDN を利用した場合は、機能の拡張性・迅速性が大幅に向上します。例えば物理の機器を利用して新規にファイアウォールを構成した場合、各ネットワーク機器とのケーブリング、また各機器に対して必要なコマンドの入力が必要となり、作業時間としては少なくとも数日を要します。一方 SDN を利用した場合、ファイアウォールの増設を行う際においても、管理画面から数クリック設定を実施するのみで、ケーブリングや必要な設定の投入が行われます。作業時間は分単位と大幅に削減され、セキュリティの運用管理性を向上します。

パケットの暗号化

また、NSX Data Center 等の SDN 製品においては、L2 VPN や IPsec VPN 等をサポートしており、データセンター拠点間の通信を暗号化してセキュアに行う事が可能です。

SDN を利用する事で、従来の物理のネットワーク環境で提供されていたものと同様のセキュリティ機能を利用可能なだけでなく、追加でクラウド環境に適した機能を提供可能です。

7. マイクロセグメンテーション（微細分割機能）と SDP（Software Defined Perimeter）

※本章はセキュリティガイダンス 「*7-3-3*」章の解説となります。

マイクロセグメンテーションとは

SDN 独自のセキュリティ提供機能として、マイクロセグメンテーションがあげられます。マイクロセグメンテーションとは、ネットワークのより細かな、粒度の高い分割とセキュリティ保護機能を意味します。マイクロセグメンテーションは、CSA の SDP（Software Defined Perimeter）ワーキンググループの定義によりますと、次のものから構成されます。

- コントローラ： クライアントの認証及びゲートウェイへの接続
- ゲートウェイ： クライアントの通信を規定
- クライアント： 保護対象のクライアント

本項では、マイクロセグメンテーションのもたらすメリットを、従来の物理のネットワークセキュリティ環境と比較して説明します。

マイクロセグメンテーションのもたらすメリット

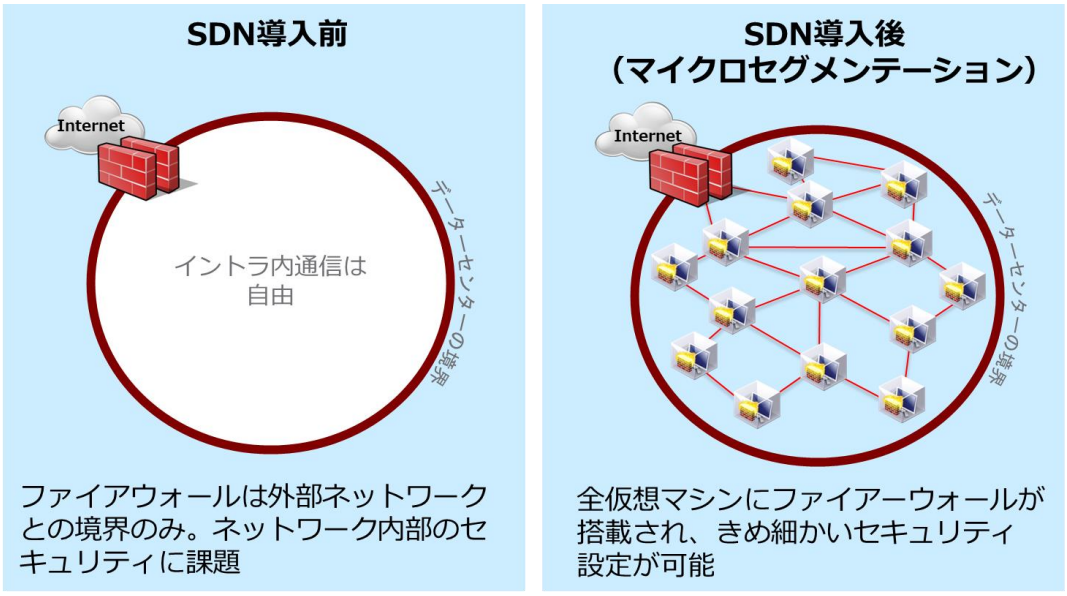


図 27：マイクロセグメンテーションのもたらすメリット

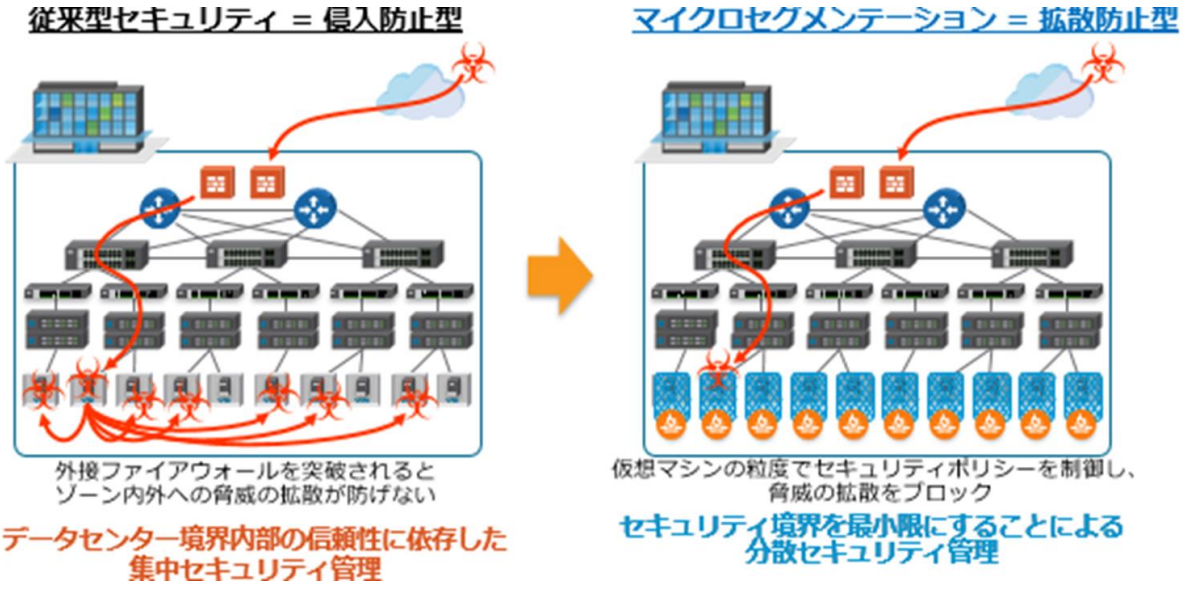


図 28：侵入防止型から拡散防止型へ

企業ネットワークを狙ったセキュリティ侵害として代表的に「標的型攻撃」があります。「標的型攻撃」は、攻撃者がマルウェアをメール等で攻撃先企業の PC に送り込みます。侵入したマルウェアは企業ネットワーク内で拡散し、企業の機密情報を窃取し、情報漏洩を引き起こします。この「標的型攻撃」においては、従来の物理ファイアウォールによる境界型のファイアウォールでは、企業内での拡散・窃取活動が、正常な通信として通過してしまい、検知が出来ません。これまでの物理による侵入防止型のファイアウォールに加えて、拡散防止型のセキュリティ保護機能が求められます。

SDN のマイクロセグメンテーションを活用したセキュリティ保護は、この拡散防止型のファイアウォールとして機能します。個別の仮想マシン（もしくは個別の仮想ネットワークインタフェース）単位でファイアウォールを設定する事が可能になります。従来の侵入防止型のセキュリティ管理は引き続き必要ですが、一度境界型のファイアウォールが侵害された場合、内部ネットワークにおける拡散を抑止する仕組みが必要となります。この拡散を防止する仕組みがマイクロセグメンテーションであり、仮想マシンの細かい粒度でのセキュリティ管理が可能になります。

この、拡散防止型のセキュリティは、クラウド環境において今後ますます重要性が高まる考え方となります。

8. クラウド事業者とプライベートクラウドのための留意事項

※本章はセキュリティガイダンス 「*7-3-4*」章の解説となります。

クラウド全体のセキュリティの確保

2 章で見た通り、クラウドの利用者側のみでなく、クラウド事業者側のセキュリティ対策も考慮した上で、サービスを選択する事も重要です。

クラウド事業者におけるセキュリティ保護においては、以下の 2 つの観点での対策が重要となります。

- 物理基盤における、従来型の境界セキュリティの保護
- クラウド上の各テナントのセキュリティの独立性

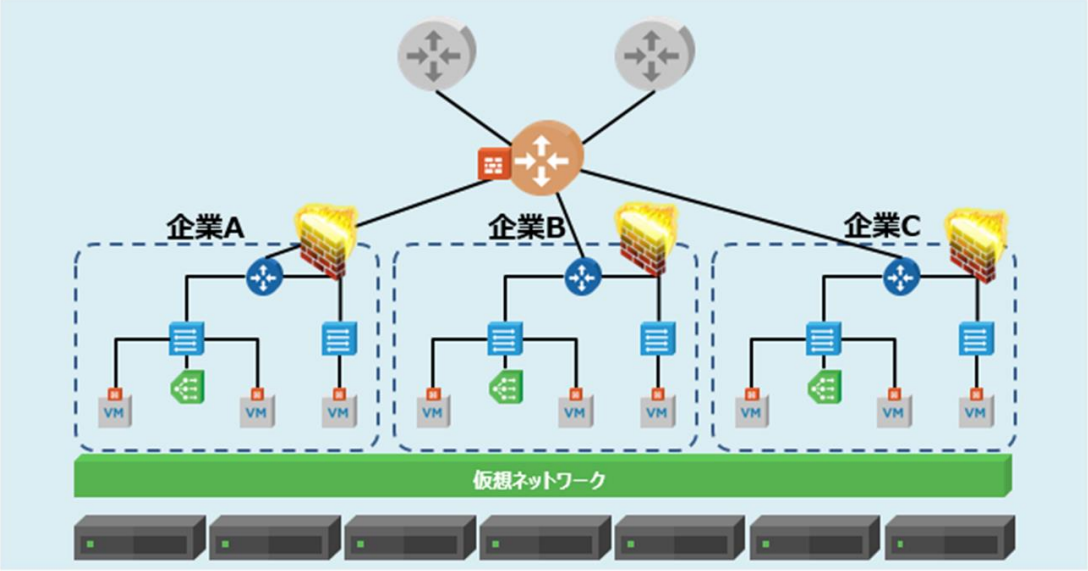


図 29：マルチテナントのセキュリティ

プラットフォームの基礎となる物理基盤における、従来型の境界型の IPS/IDS、及びファイアウォール等を利用したセキュリティ保護は、クラウド環境全体のセキュリティのすべての出発点になります。また、サーバーの仮想基盤となるハイパーバイザーにおいても、最新のパッチを適用する事で、セキュリティホールの対策を取る事が求められます。物理ネットワーク環境におけるセキュリティ事故は、全てのクラウド利用者のセキュリティを侵害する事になり、甚大な被害を引き起こします。

続いてクラウド事業者環境で求められるのは、物理基盤上で稼働する個別のマルチテナントのセキュリティの分離・独立性です。特定のテナントにおけるセキュリティ侵害や、もしくは悪意のある動作を行った場合に、全テナント環境への影響を防御する必要があります。こうした各テナント単位のセキュリティ保護は、テナント利用者のワークロードに影響を及ぼさない形で実装する事が求められます。

SDN 環境において各テナントのサービス開通にあたり、境界及び内部セキュリティも踏まえて、サービス構築がなされます。テナント内部のワークロードに応じたキャパシティを確保した IPS/IDS、及びファイアウォールを配置する事で、テナント単位の独立性を担保する事が可能となります。

9. ハイブリッドクラウドにおける留意事項

※本章はセキュリティガイダンス 「*7-3-5*」章の解説となります。

ハイブリッドクラウド間接続のセキュリティの確保

企業の ICT 環境において、Amazon AWS をはじめとするパブリッククラウドの利用と、企業内のプライベートクラウド環境の双方を利用する、ハイブリッド・混在型のクラウドの利活用が浸透しています。こうしたハイブリッドクラウド環境においては、パブリック・プライベートクラウド全体にまたがった、セキュリティ管理ツールが求められますが、実際にはクラウド毎に管理ツールが異なっています。いくつかハイブリッドクラウド用途のネットワーク管理ツールは存在するものの、デファクトとなるような統合管理ツールは存在せず、用途ごとに選択する必要があるのが現状です。

ハイブリッドクラウド間接続におけるセキュリティの管理は、クラウド全体に影響を及ぼすため、プライベートクラウドとパブリッククラウド事業者間の接続には、専用 WAN 回線または VPN 接続による、接続点におけるセキュリティの確保が求められます。

ハイブリッドクラウド間接続におけるセキュリティに関しては、次 2 点の観点の考慮が必要となります。

- ハイブリッドクラウド間接続の最小化（接続拠点の数を、物理的に削減）によるセキュリティ侵害リスクの低減
- 乗り継ぎネットワーク（セキュアな接続点）を利用した、ハイブリッドクラウド間接続の最適化

ハイブリッドクラウド間接続における乗り継ぎネットワークとは

出典：https://www.netone.co.jp/service/technology/cloudservice-cloudhub/

図 30：ハイブリッドクラウド環境における、乗り継ぎネットワークの必要性

Amazon AWS、Microsoft Azure といったパブリッククラウドと、企業のプライベートクラウドは、セキュアな専用 WAN 回線や VPN 等で接続する必要があります。また相互の接続においては、ファイアウォールやマルウェア対策、ログ監視等のセキュリティ対策が求められます。一例として、ネットワンシステムズの提供する「クラウド HUB サービス」では、こうしたパブリック、プライベートクラウド間のセキュアな接続環境をサービスとして月額課金で利用する事が可能です。こうしたサービスを利用する事で、セキュリティリスクの低減を図りながら、適切なハイブリッドクラウド環境の構築を図る事が出来ます。

10. 監視とフィルタリング

※本章はセキュリティガイダンス 「*8-1-2-2*」章の解説となります。

仮想ネットワークの監視とフィルタリング

仮想化技術を基盤とした、今日のクラウド環境において、SDN が多くのネットワーク環境を仮想化し、セキュリティの管理機能も実装している事をこれまでの章で見てきました。SDN は、従来の VLAN のみでは難しかった、マルチテナントにおけるテナント単位の隔離機能を提供可能です。この章では、仮想ネットワーク環境における監視とフィルタリング機能について見て行きます。

セキュリティ管理の観点で、監視とフィルタリング機能の実装を考える上で、トラフィックがどう流れるかは考慮の必要があります。従来の物理環境におけるトラフィックの監視は、2 台の物理サーバー間を監視していれば実施出来ました。ただし仮想環境では、同じ物理サーバー上にある 2 台の仮想マシン間で直接通信が流れる為、従来の方法でトラフィック監視を行う事が出来ません。

この問題の解決策として、物理サーバー上に、専用の仮想アプライアンス等を設置し、全ての仮想マシンのトラフィックが経由するように設定することが出来ますが、通信のボトルネックにもつながります。また、パブリッククラウド環境においても、こうしたネットワーク監視の為の機能は、コスト等の面から一般的にサービス提供されておらず、利用者が用意する必要が生じます。

また、パブリッククラウドにおいて、様々なサービスを利用する上で、各 SaaS、PaaS 製品のトラフィックはクラウド事業者のネットワークを流れ、クラウド利用者管理下の仮想ネットワークとは異なる領域を通る事となります。こうした、クラウド事業者の利用するセキュリティ管理は、SDN 上で動作するファイアウォールで実装され、これまで見てきたようにクラウドに特化したセキュリティ保護の仕組みが実装されます。

このようなクラウド環境におけるネットワークの監視とフィルタリングにおいて、求められる要件について見て行きます。

仮想ネットワークの監視とフィルタリングに求められるもの

パブリック、プライベートを問わず、クラウド環境のネットワークの監視とフィルタリングに必要とされる要件は次の 2 点です。

- 仮想化基盤に対応したネットワークの監視、可視化ツールの利用
- パブリッククラウド、プライベートクラウド双方の管理

この章では一例として、VMware 社の提供するネットワーク監視・可視化ツールである VMware vRealize® Network Insight™（以下、vRealize Network Insight）を例に見て行きます。vRealize Network Insight は、VMware NSX によるネットワーク仮想化を導入している環境において、トラフィック監視と運用管理の機能を提供します。vRealize Network Insight の特徴は、次の通りです。

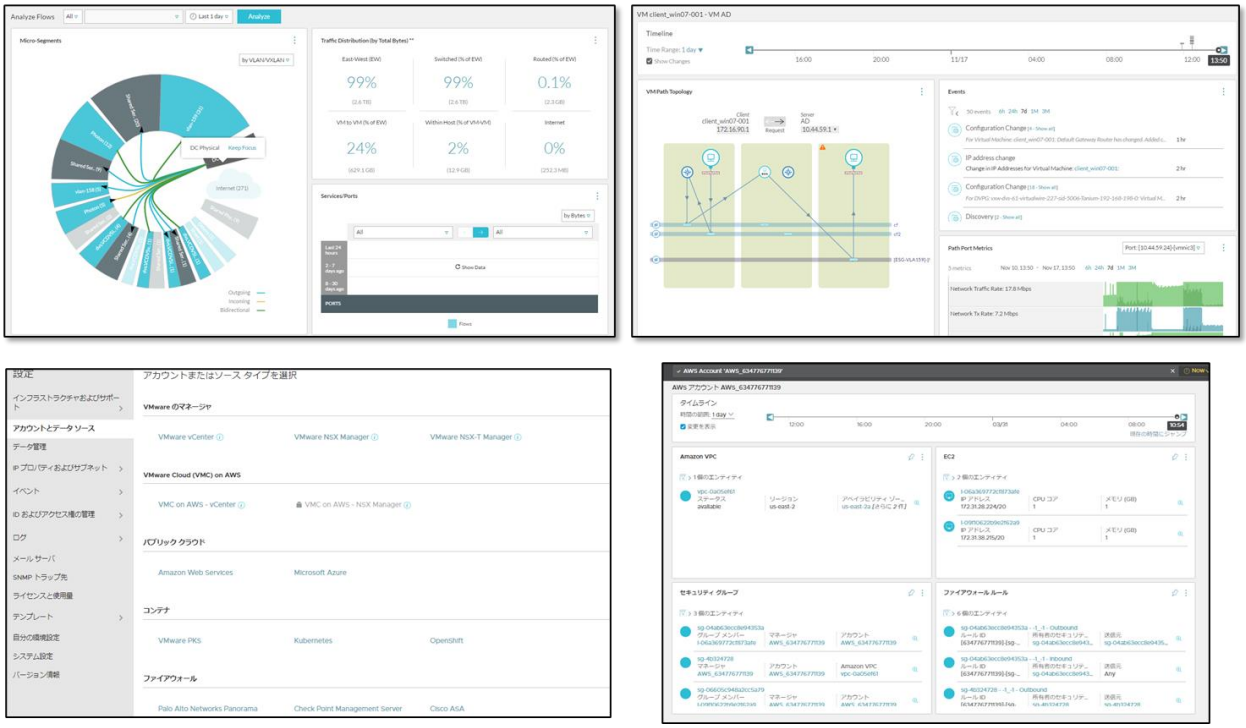


図 31：VMware vRealize Network Insight

vRealize Network Insight は、物理、仮想（パブリック、プライベートクラウド）両方のネットワーク基盤の経路及びトラフィック情報をトータルに可視化するツールです。特定の期間内に仮想マシン間や仮想ネットワーク間で、どのようなアプリケーション種別の通信（例：HTTP、ログ、認証トラフィック）が、どの程度発生しているかを可視化出来ます。可視化だけでなく、不正通信の早期発見や内部不正の防止にも効果を発揮します。

また、通信障害が発生した際にも、どの経路を確認する必要があるのか、視覚的に確認する事が可能です。

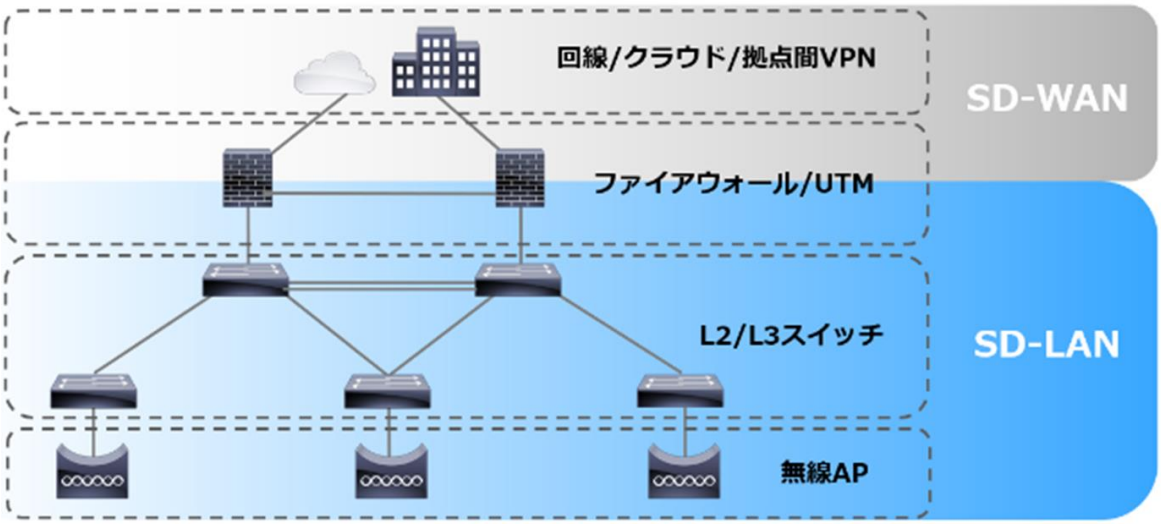
監視対象として、プライベートクラウド環境のみでなく、パブリッククラウド（AWS、Azure）や、物理ネットワーク機器も対象としており、クラウドにおける統合的な監視ツールとして利用できます。現在のトラフィック状況から、推奨のファイアウォールルールを自動で策定することもできます。

また、トラフィックの総容量も可視化する事が出来、ICT のネットワーク環境の構築の上で、将来的な容量増強計画にも活用出来るといった特徴があります。

このような、物理環境を含めた総合的なクラウドの監視ツールを利用する事で、効果的な ICT 環境全体におけるネットワーク監視計画を立てる事が可能です。

A-1. SD-WAN とセキュリティ

クラウドから SD-WAN へ



出典：https://licensecounter.jp/engineer-voice/blog/articles/20190806_post_15.html

図 32：クラウドから SD-WAN へ

これまで本資料内では、クラウドのセキュリティについて、主に企業内、LAN 側のセキュリティを扱って来ました。ただ昨今の企業ネットワークは、LAN 内にとどまらず、拠点間の WAN 接続に関しても管理及びセキュリティの確保が求められています。本項では WAN 管理における一つの潮流となっている SD-WAN のご紹介と、SD-WAN におけるセキュリティの課題を説明します。

SD-WAN の導入メリット

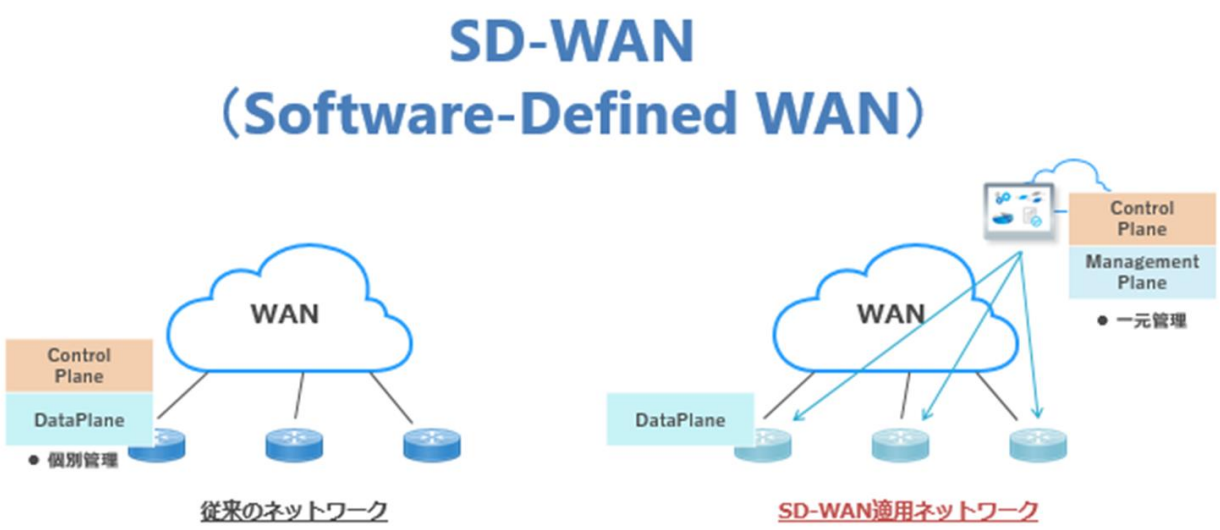


図 33：SD-WAN とは

SD-WAN とは「Software Defined Wide Area Network」の略で、ソフトウェアにより WAN・広域通信網における仮想的なネットワークを作る技術を意味します。従来の物理機器で構成されていた WAN 環境をソフトウェアにて管理する事が出来、企業の経営判断や IT 運用のトレンドに合わせて柔軟なネットワークインフラを構築する事が可能です。

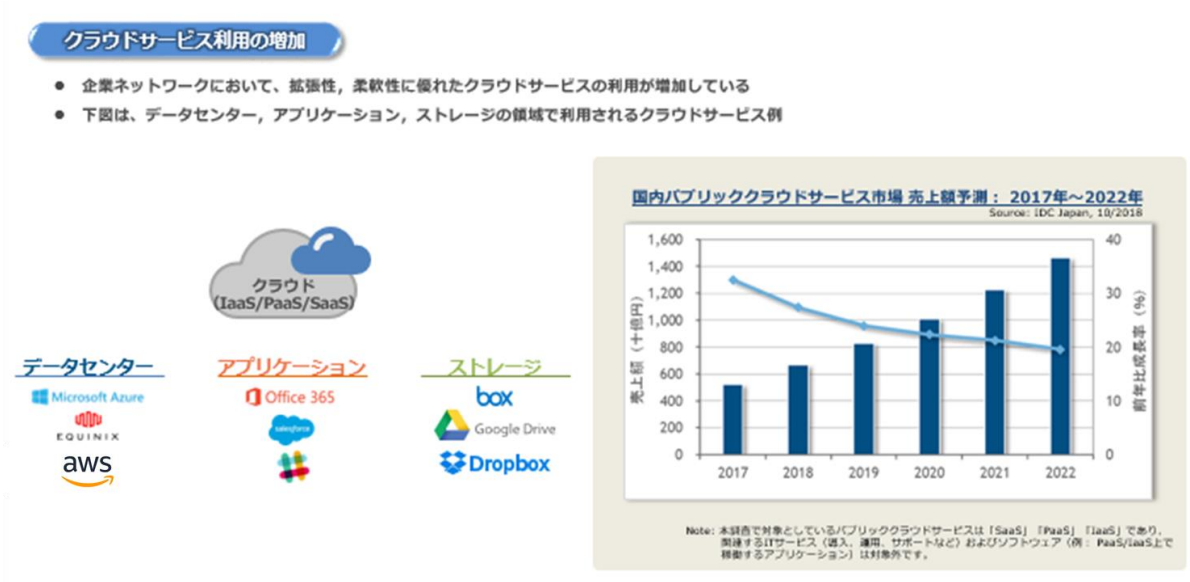


図 34：SD-WAN の導入メリットについて

企業の ICT 環境において、一般的に専用線やブロードバンド回線、LTE 等のモバイル回線を利用して WAN 環境を構築しています。SD-WAN では、こうした物理回線を基盤に利用しながら、ソフトウェアにて自社の環境に必要な環境を柔軟に構築する事が可能です。

また、ネットワークを取り巻く ICT 環境も変化しています。Office365 に代表される SaaS やパブリッククラウドの利用拡大により通信量は激増し、また働き方改革によりビジネスにおけるテレワークの利用も激増しています。こうした中、従来のデータセンター集約型の WAN では、トラフィックがひっ迫し、品質・コスト・セキュリティ面の課題が浮上しています。こうした中、ビジネス要求に対して、迅速、柔軟 WAN 環境を提供するのが、SD-WAN です。

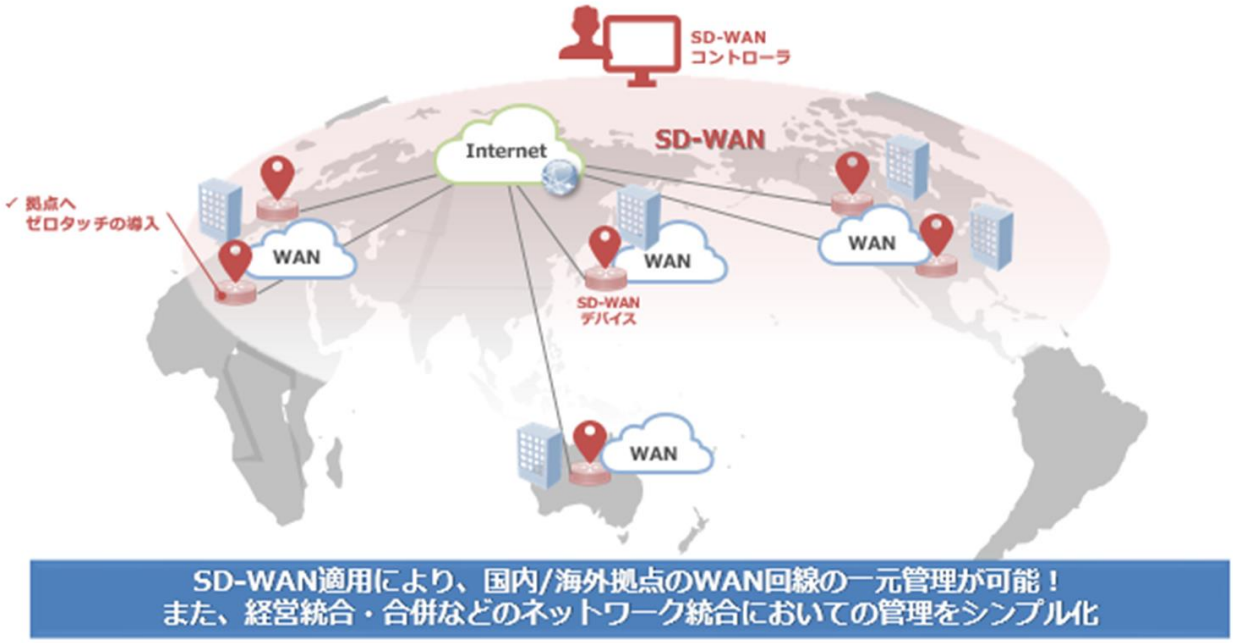


図 35：SD-WAN による一元管理

SD-WAN 導入によるメリットの一つに、企業の各拠点に配置された WAN 機器を、中央から一元管理が可能となる点です。これにより、従来企業のシステム部門が抱えていた、多くの拠点の WAN 接続における運用管理負荷を低減する事が可能です。

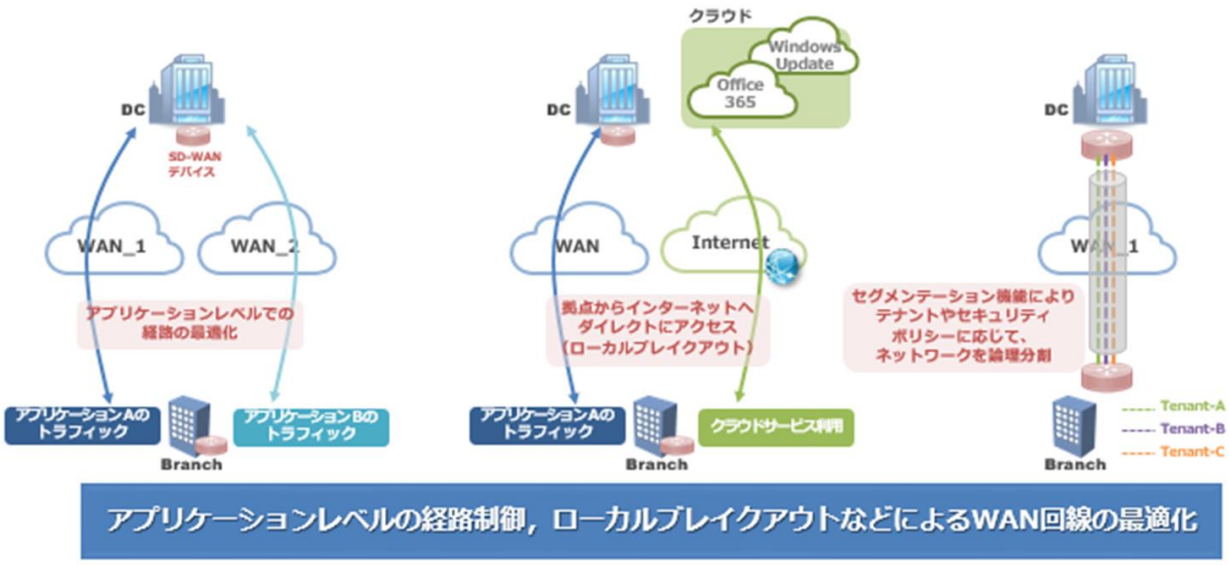


図 36：SD-WAN による WAN 回線の最適化

また、SD-WAN の大きなメリットとして、従来の WAN 回線の利用を最適化可能な点が挙げられます。例えば各企業拠点から、データセンターへのアクセス環境において、各業務アプリケーション単位で WAN の回線品質を最適化する事が可能です。例えば工場間のアプリケーションや社内業務用のアプリケーション等、求められる回線品質が異なるアプリケーション毎に最適化を図る事が出来ます。

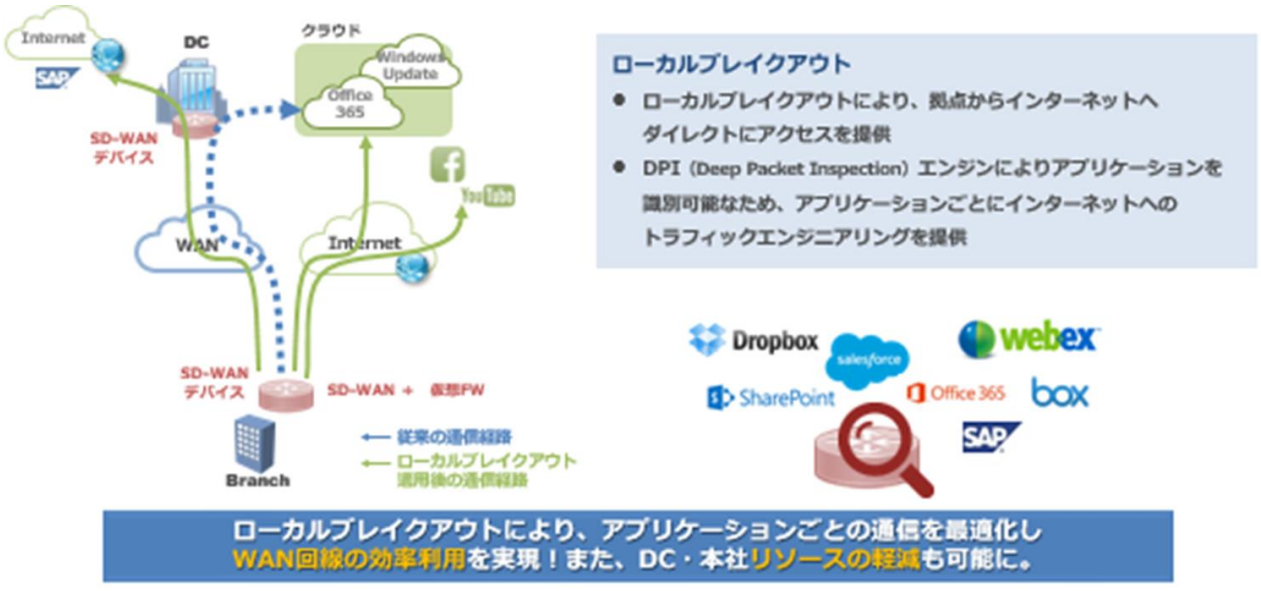


図 37：ローカルブレイクアウト

続いて SD-WAN が注目を集める理由の一つに、「ローカルブレイクアウト」が挙げられます。ローカルブレイクアウトとは、各拠点におけるインターネット上のサービスの利用において、通信を企業データセンターに集約するのでなく、直接インターネットへのアクセスを許可するものです。具体的には、Office365 に代表されるクラウド上の SaaS の利用において適用されます。これにより、急激に増大するクラウドサービス利用時の通信が、データセンターに向かう企業データ通信全体のトラフィックをひっ迫させる事態を防ぎます。

SD-WAN のセキュリティの考慮点

SD-WAN 環境におけるセキュリティについては、上記のローカルブレイクアウトを利用する際に検討する必要があります。というのも、各拠点から直接インターネット上のサービスを利用する為、外部環境からの攻撃対象となる事を防ぐ必要があるからです。ローカルブレイクアウト利用時のセキュリティの実装方法として、現時点でいくつか考えられますが、まだ定まったものがないのが現状です。

ローカルブレイクアウト利用時のセキュリティの確保について

- 拠点に配置するルーターにてファイアウォールを実装：ただし、ある程度の価格のものでないと、機能、ログ保管量が不十分
- ローカルブレイクアウト利用目的のデータセンターを個別に準備：コスト面の課題
- クラウド型のインターネットゲートウェイサービス（Cisco Umbrella、Zscaler 等）

A-2. Intent-Based Networking について

昨今、ネットワークは数多くのデバイスで大規模に構成され、数多くのルールにより複雑化され、また様々なベンダーで多様に構成されており、運用が困難になってきています。従来の手動でのデバイス単位でのオペレーションを実施することによって設定変更ミスを引き起こし、ネットワークやセキュリティのトラブルへとつながってしまう点が問題となっています。

これらの解決策として SDN (Software-Defined Network) が登場し普及してきていますが、さらに次のキーコンセプトとして Intent-Based Networking (IBN)が登場しました。IBN は、SDN の概念を拡張して、ネットワークの自動化を強化し、複雑な手動でのネットワーク運用を抽象化して負荷を削減します。

IBN は Gartner が 2017 年 2 月に提唱しており、利用者の意図に沿って設計・構築・運用・最適化サイクルをソフトウェアを用いて自動で行うネットワークを提供するものです。以下 4 つの機能を提供します。

① 利用者のビジネスポリシーをもとに設計と構成を作成し、その内容についての検証を実施する機能
② ネットワークインフラに対して自動でコンフィグを投入する機能
③ ネットワークの状態を取り込む機能
④ システムが利用者の intent（意図）に沿ったものか継続的に検証し、必要に応じて修正して、最適化を行う機能

これらの機能に加えてマルチベンダー化も重要な要素となります。

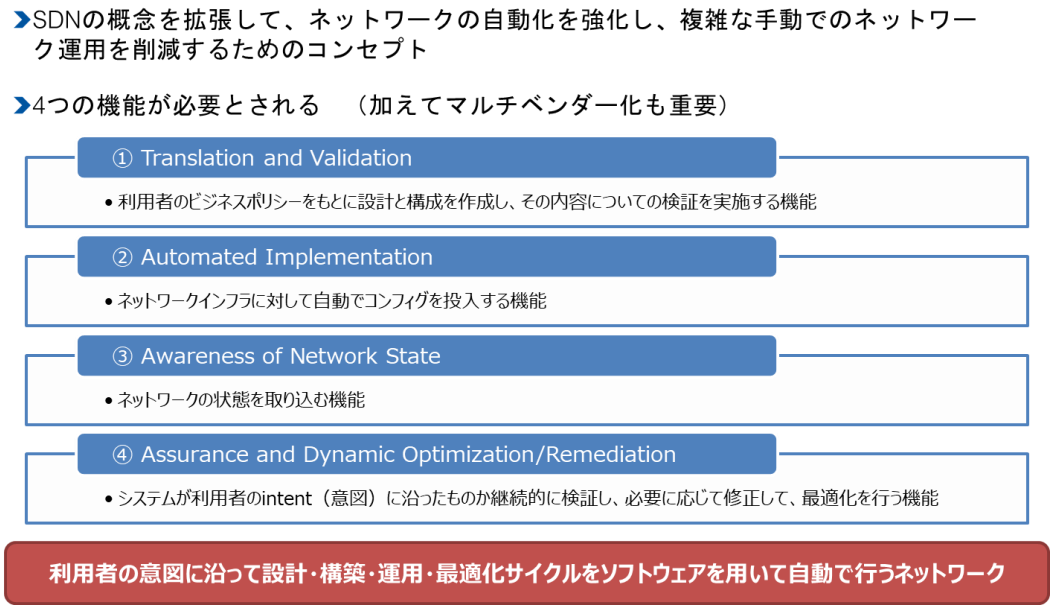


図 38：Intent-Based Networking について

IBN はまだ理想形でもあり、言葉が先行している部分もありますが、IBN ベースの製品も出てきています。例えば、Cisco や Huawei のような大手ネットワークベンダーは IBN の全ての機能実装をめざす取り組みを行っています（ただし主に自社製のネットワーク機器を対象としたベンダーロックインとなります）。あるいは Apstra、ForwardNetworks、Veriflow（現在は VMware に買収）といったスタートアップ系ベンダーのように、部分的な機能をサポートする製品を出しているところもあります。現時点ではまだこれからの状況となりますが、今後の機能実装によって大きく普及が見込まれています。

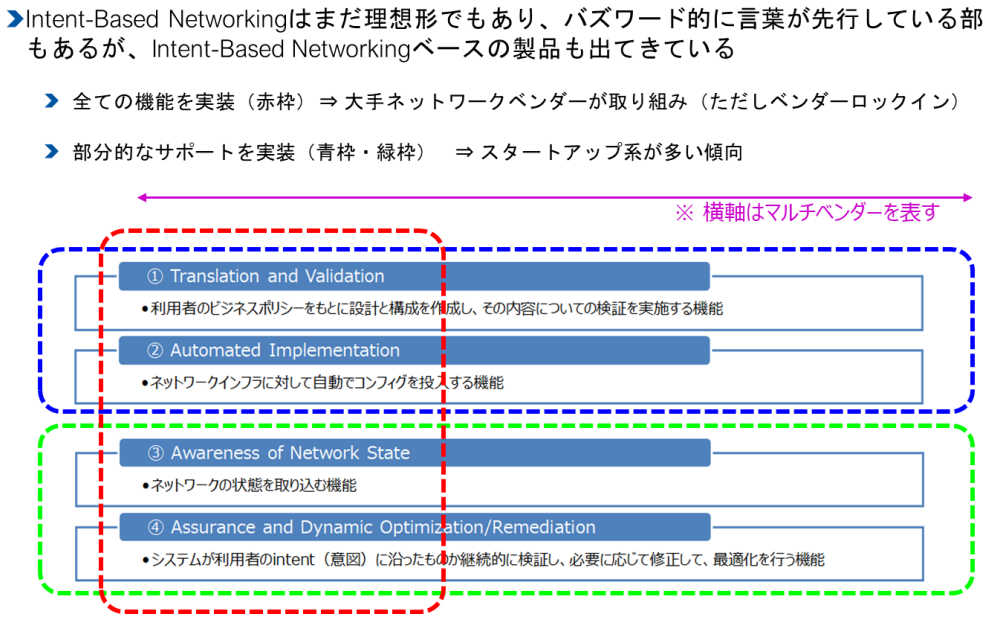


図 39：Intent-Based Networking の現在地

A-3. SDN と SD-WAN のユースケース

ユースケース 1: 支店や店舗の WAN 運用の簡素化

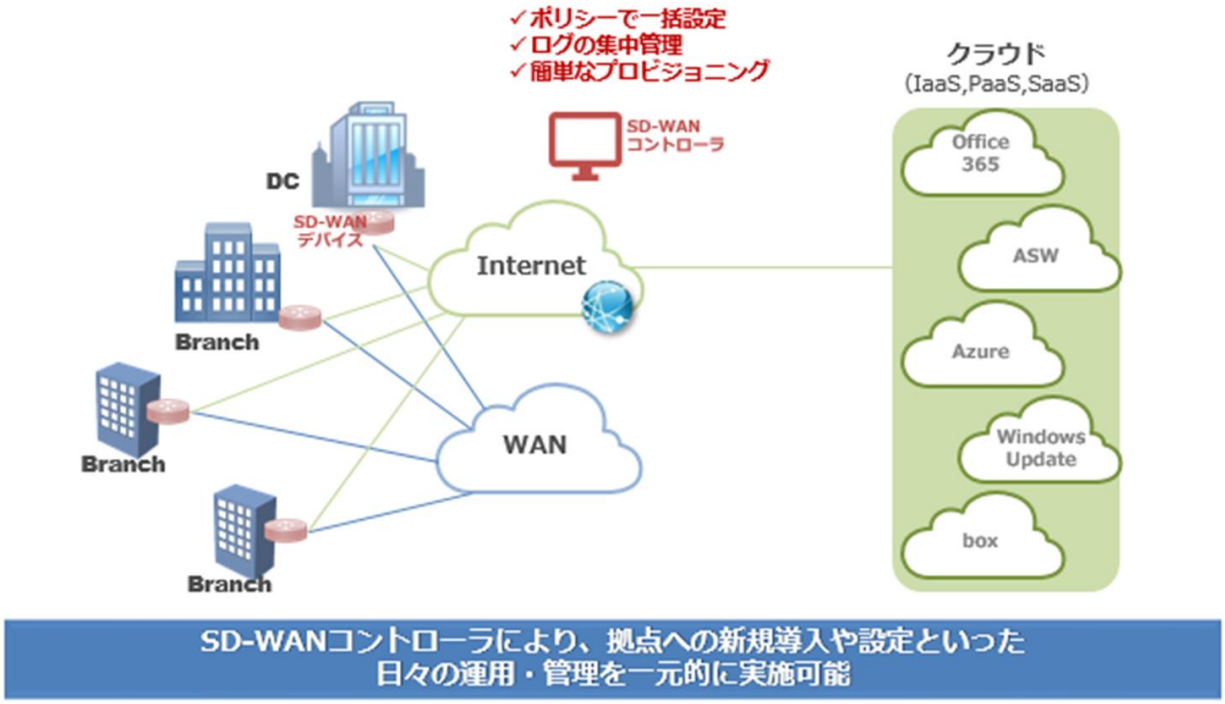


図 40：支店、店舗の WAN 運用の簡素化

SD-WAN の代表的な導入事例としては、企業 ICT 環境における、支店や店舗の WAN 環境の管理の簡素化が挙げられます。支店や店舗の拡張や統廃合等が頻繁に行われるような企業環境において、各拠点の WAN 環境の管理は、システム部門において大きな負荷となります。例えば拠点における WAN 環境の開設やトラブルの対応等においては、拠点側に IT 担当者が存在しない事が多く、その度に本社から技術者を派遣して管理する形となります。拠点数の増減が多い環境においては、運用負荷が増大します。

SD-WAN の導入により、こうした企業拠点（支店、店舗）に簡易な SD-WAN 装置が送付される形になります。拠点の担当者は WAN の開設にあたり、SD-WAN 装置をネットワークに接続するのみで、特段の IT スキルは不要です。設定の投入や管理作業は中央のデータセンターから行われ、支店や店舗の WAN 環境の管理運用が効率的かつ一元的に管理されます。

ユースケース２： ローカルブレイクアウトと集中管理

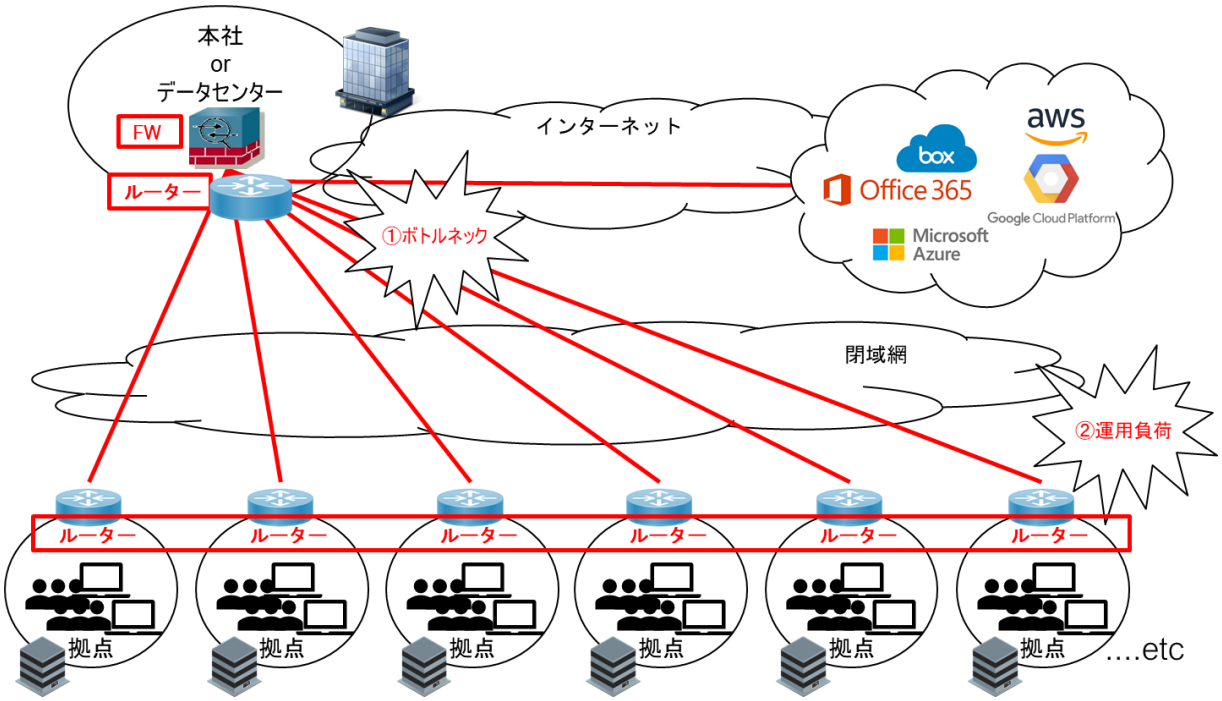


図 41：ボトルネックと運用負荷増大

クラウドサービスを利用する企業の問題点として以下の 2 点があります。

① ボトルネック

各種クラウドサービスの利用増により従来型のネットワーク構成がボトルネックとなる。

ユースケースの背景と問題点：

- 従来構成は、セキュリティ面を考慮し、閉域 VPN による DC または本社への全面引き回しによる一括インターネット接続を実施
- 昨今のクラウドサービス(主に O365)利用増に伴い回線容量及びコネクション数増のひっ迫と、増速コストが課題

② 運用負荷

各拠点が海外含め、遠方にあることでネットワーク構成変更や追加にかかる運用負荷増

ユースケースの背景と問題点：

- 拠点が大量にあり、都度各地へ設定に行かなければならない
- ルーター等へのメンテナンスや設定の集中管理が困難

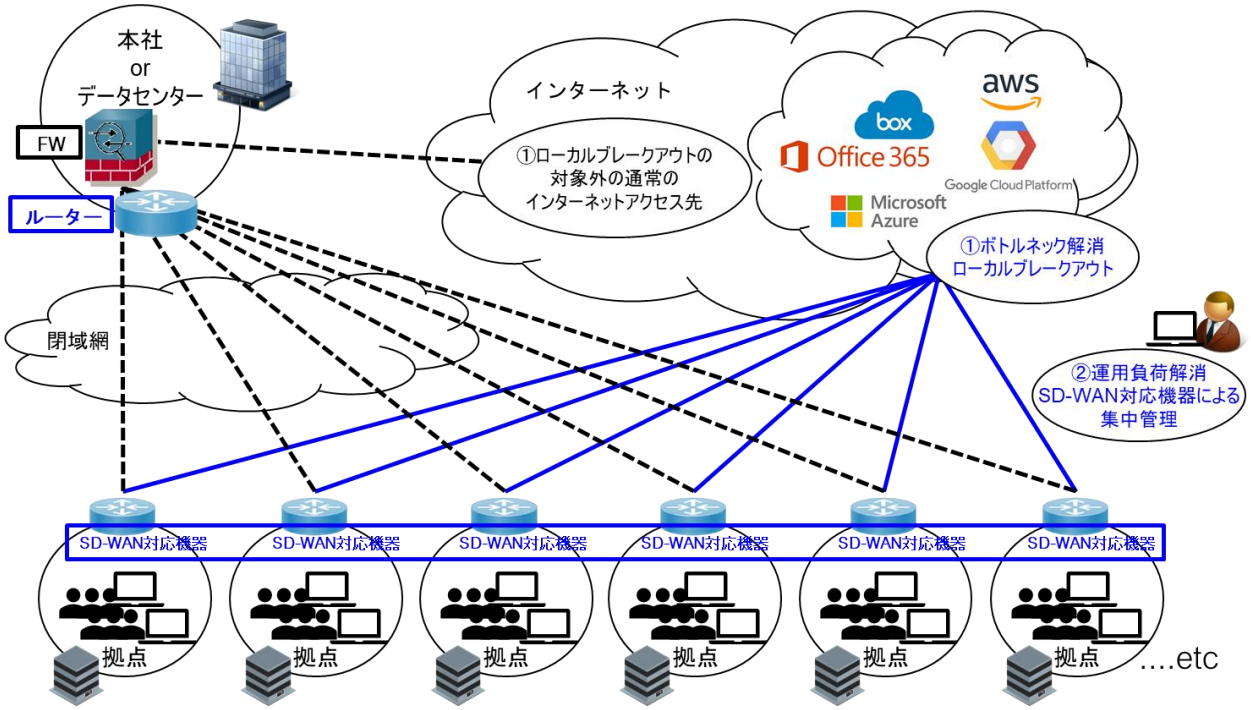


図 42：SD-WAN によるローカルブレイクアウトと集中管理

対応策としては以下になります。

① ローカルブレイクアウトによるボトルネック解消

- 新構成では、SD-WAN によるローカルブレイクアウト(インターネットブレイクアウト)により、各拠点から特定のクラウドサービスへのみ直接アクセス可能とします。
  ローカルブレイクアウト対象外への通信については、セキュリティ面を考慮し、従来通り DC または本社経由での引き回しを実施。
  ただし、従来構成から新構成に移行することで、セキュリティに関する懸念点が発生することがあります。
  その対策として、昨今では下記の検討が求められるケースがあります。
  1)拠点がルーターにセキュリティ機能を実装する。
  2)クラウドセキュリティサービス(クラウド FW やクラウドプロキシなど)を利用する。
  従来型の DC または本社経由での引き回しと全く同じセキュリティレベルを求める場合、各拠点に同一の FW 等セキュリティ製品の導入が必要となりますが、運用・コスト面から現実的ではないため、上記の
- ような対策が主に検討されるケースが見受けられます。

② 集中管理による運用負荷解消

- 新構成では、各拠点の NW をすべて SD-WAN に直し、管理部門による集中管理することで、機器への直接アクセスが不要になる。

・ ルーターがゼロタッチ導入可能な製品にすることで、拠点側での接続は、IT スキルの無い担当でも可能になる。

ユースケース３：ソフトウェア上でのテスト環境の構築

課題	従来、大規模システムをテスト・検証するために、本番とは別のテスト用環境を物理的に構築しなければならず、コスト、時間を要していた
解決	SDN (あるいはIBN)により、テスト用のコピー（デジタルツイン）環境を即時に構築し、物理的なコスト削減や、環境構築のための時間短縮、さらには各機器の設定について定期収集や自動チェックを行うことによる設定ミス削減といった運用負荷軽減のメリットも挙げられる

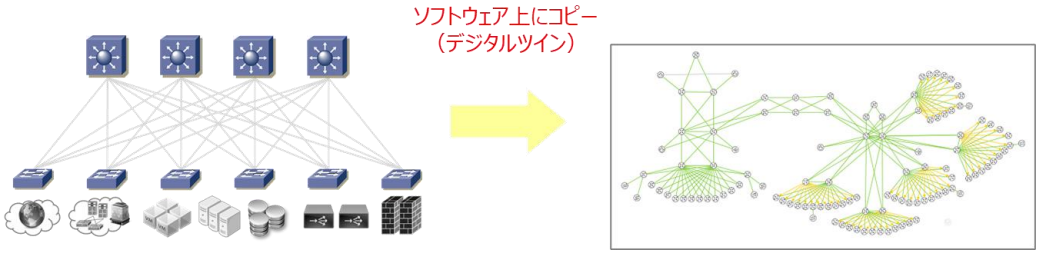


図 43：ソフトウェア上でのテスト環境の構築

従来、大規模システムをテスト・検証するためには、本番とは別の環境を物理的に構築する必要がありますが、そのためのコストおよび構築への時間を要するという課題がありました。これを SDN あるいは IBN を利用することで、デジタルツインとの呼ばれるテスト用のコピー環境を即時に構築することができるようになり、物理的なコスト削減や、環境構築のための時間短縮が可能となります。

さらに加えて各機器の設定について定期収集や自動チェックを行うことができ、

- ネットワーク構成・コンフィグが常に最新のものを管理
- トラフィックが正しい経路を通るかをチェック
- インタフェース間の VLAN やリンクスピード設定のチェックによる設定ミスの早期発見
- ACL/FW ルールのソフトウェア上での事前検証

等による運用負荷や設定ミス削減が可能となります。

おわりに

本資料では、CSA ジャパンが、2018 年 7 月に発行した「クラウドコンピューティングのためのセキュリティガイダンス v4.0 日本語版 v1.1（2018 年 7 月 24 日）」をベースに、新しいテクノロジー、利用のユースケースを加え、SDN 利用ガイダンスとしてまとめました。

SDN というのは、広範なツールやテクノロジーを包含する、重要なネットワーキングやその管理の在り方で、クラウド、オンプレミス、ハイブリッドなど、その利用局面において、様々な形態となって現われてきます。

今後のセキュリティ対策の参考にしていただければ幸いです。