5つの実ユースケースが示すSDNの計り知れない可能性

--ビジネス加速へ、根本から変わる今後の企業システム

インタビュー

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業本部
サービスデリバリー 技術理事 / ディスティングイッシュド・エンジニア

山下克司氏

日本アイ・ビー・エム株式会社
グローバル・テクノロジー・サービス事業本部
インフラストラクチャー・デリバリー
サービスライン・デリバリー エグゼクティブアーキテクト

陳建和氏

「SDN（Software Defined Networking）」は、場所やデバイスなどの物理的環境に縛られていた旧来のネットワークを開放し、次世代のネットワーク管理を提供する技術・仕組みとして、大いに期待が寄せられている。これまでさまざまな研究や検証が行われてきたが、いよいよ本格的な普及が始まろうとしている。

IDC は 2015 年 3 月、データセンター、企業ネットワーク、通信事業者における SDN ／ NFV が実用期を迎えたと発表した。特に企業ネットワークの分野においては、SDN 技術の適用個所を具体的に検討し、実践から得られた効果を元に、より現実的なアプローチへとシフトしているとのことだ。SDN が企業ネットワークの構築・運用の選択肢として受容されることで、2014 年～ 2019 年の CAGR（年間平均成長率）が 55%という高い数値を示すと予想している。

IBM においても、すでにいくつかのユーザーネットワークを“SDN 化”することで、旧来のネットワークが抱える問題を解決し、ビジネスの目標を実現してきた。同社が手がけてきた実例から得られた実装のパターンを紹介することで、実践レベルへと昇華した最新の SDN の姿を見ていただこう。最大のポイントは、これらはすでに企業が計画、実現しているユースケースであるところにある。

ケース（1）
サーバー仮想化がもたらしたネットワークの複雑性を排除

A 社では、サーバー仮想化技術を積極的に活用し、業務システムの集約を図ってきた。高性能なサーバー上に多数の仮想マシンを搭載することで、非常に高い集約率を実現していた。インスタンスの追加や削除、移動などの煩雑な作業は管理ソフトウェアによって自動化されているため、サーバーの管理負荷は大きく削減できていた。

問題はネットワークだ。仮想マシンが自在に増減・移動できるのに対して、従来のネットワーク技術は柔軟性に乏しく、煩雑な運用を課せられてしまうことになる。

仮想マシン同士をレイヤー 2 で接続しようとすると、MAC アドレスや VLAN の管理が必要となる。しかし、すぐに MAC アドレステーブルや VLAN 数の限界に達してしまい、仮想マシンを増設することができなくなってしまうことは明らかだった。だからと言って、レイヤー 3 接続に変更してしまうと、仮想サーバーのセグメントを超えた移動に伴いネットワークアドレスの変更が必要になり、管理負荷が増大してしまう恐れがあった。

これまでの仮想サーバー環境のネットワーク構成は、およそ下図のとおりだ。複数の物理サーバーにハイパーバイザーを搭載し、多数の仮想マシンを稼働させる。各サーバーは、物理インターフェース上で管理 VLAN とサービス VLAN に接続されている。仮想マシン同士は、仮想スイッチを介して VLAN を構成している。

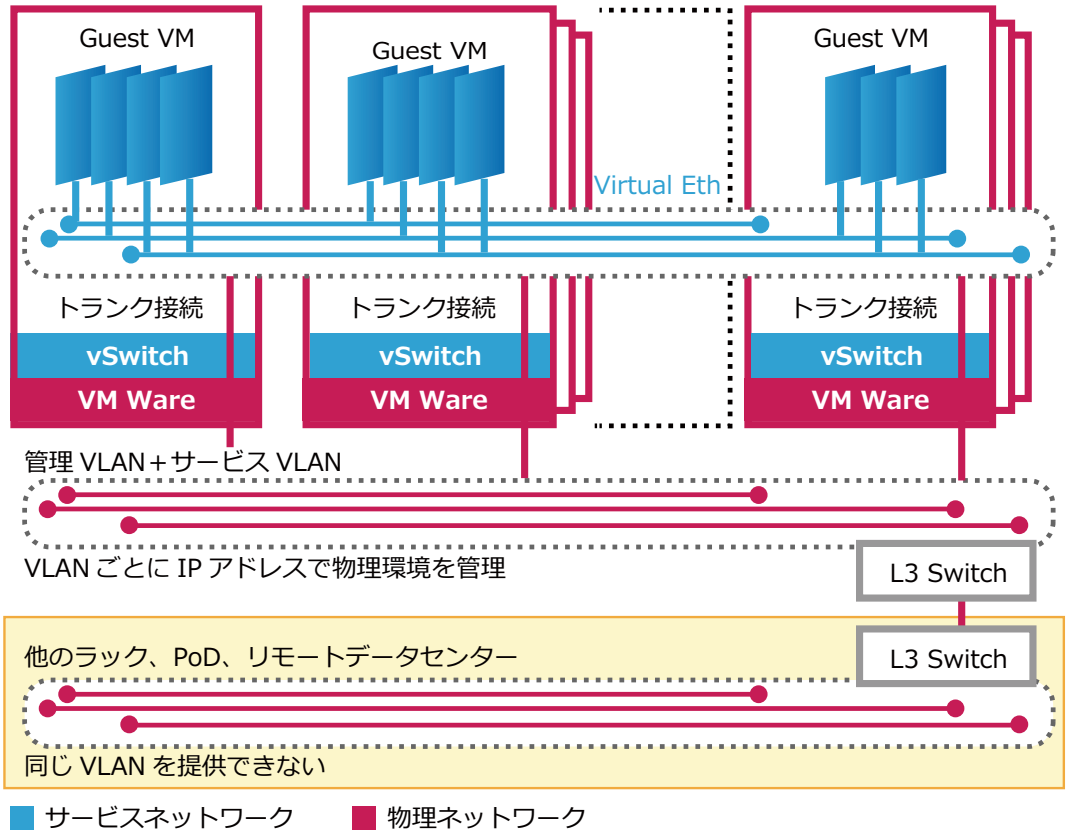


図 1. 仮想化されたサーバーファームのネットワーク

これらの VLAN を運用するためには、多数の IP アドレスの対比を適切に管理する必要がある。仮想マシンと仮想スイッチの構成変更はソフトウェアで自動化できても、都度、物理スイッチ上の VLAN 設定は手作業で設定しなければならない。しかも、リモートサイト間やラック・POD 間は L3 接続で、同一の VLAN を割り当てることはできないため、IP アドレスの管理はいっそう複雑になる。

そこで IBM では、イーサネットオーバーレイを実現する SDN ソフトウェア製品によって「分散仮想イーサネット」を構成し、SDN によるネットワーク構築を図った。

新しい物理環境においては、従来のように管理 VLAN とサービス VLAN を共存させる必要はなく、単にハードウェアのみを相互接続するための IP アドレスが振られ、管理インフラとして機能する。

サービスネットワークは、SDN によって管理インフラと分離され、完全に独立した仮想イーサネットとして形成される。ネットワークの物理構成を鑑みることなく、SDN コントローラーによるソフトウェア制御のみで、自由に構成を変更できるようになった。仮想マシンにどのような変更があっても、それに合わせて自動的にネットワーク構成が変更され、ハードウェアはいっさい手を付ける必要がなくなった。

さらに、仮想イーサネットの接続には物理的にはサーバー間の IP 通信が可能であればよいため、他のラックや PoD、リモートサイトにも、同一のサービス VLAN を提供できるようになった。

物理環境と仮想化環境が完全に分離されるということは、管理業務も分離できるということになる。つまり、物理ネットワークの管理者は物理サーバーのハードウェアの IP 通信を管理するだけでよく、実際に稼動している仮想サーバーや仮想化されたネットワーク環境の管理者はアンダーライニングしている物理環境を省みる必要がない。したがって、例えば物理環境だけの管理を外部委託するというようなアウトソーシングも可能となる。SDN は、管理負荷の最適化にも役立つということだ。

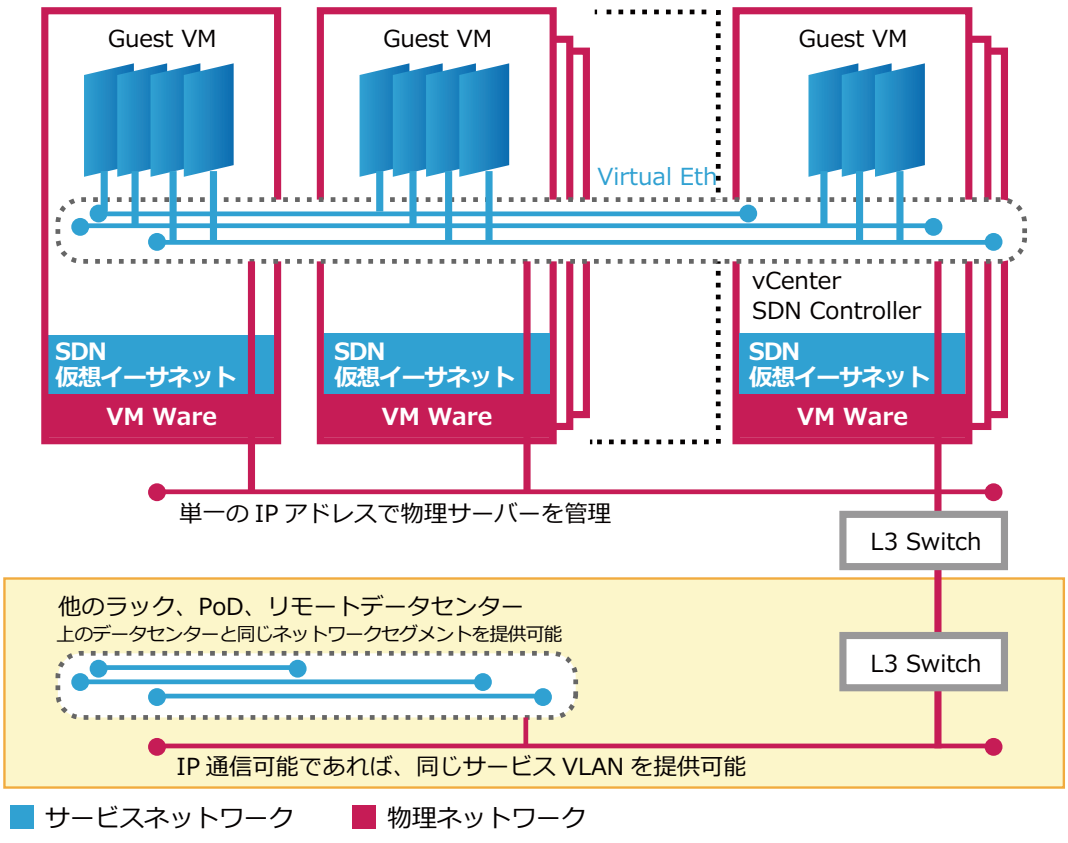


図 2. 仮想化されたサーバーファームのネットワーク【効果】

ケース（2）
最適なセキュリティを、仮想ネットワークの柔軟なゾーニングで提供へ

B 社では、将来的なビジネスのグローバル展開を柔軟かつ容易に実現できるシステム作りに取り組んでいた。日本のデータセンターで構築したシステムを、海外にも迅速に展開していくという想定だ。

しかし B 社のネットワークは、ゾーニングルールが非常に煩雑化しているという問題があった。というのも、全社的にポリシーが統一されておらず、アプリケーションサーバーへのアクセスルールが LoB ごとに乱立しているためだ。

さらに、2007 年ごろに IDS/IPS を導入しており、ホワイトリスト型の運用を行ってきたことが複雑さに拍車をかけていた。アプリケーション単位、グループ会社単位のフィルタリングと特殊なルーティングがデータセンター内や WAN 接続に偏在しており、複雑さに拍車をかけていた。異なる部門の事業所に出張するとノート PC の接続ができないなど、ユーザーの不便さも極まっていた。

検討や設定も煩雑で、1 つのアクセスコントロールリスト（ACL）を適用する計画を立てるのに一週間もかかるような環境だ。そのため、新しいアプリケーションを導入したり、グループ会社のサーバーを集約したりしようと思っても、スピーディに IT サービスを提供できない状況が続いていた。

さらに物理環境も複雑で、ネットワークだけでも多数のラックとデバイスを用いており、運用コストの肥大化を招いていた。

こうした問題に対して、IBM はデータセンター内外の従来型の物理ネットワークを、構成を一元化したファブリックネットワークによってまとめる。このアンダーレイネットワークの上に、SDN によってオーバレイネットワークを構築するという手法を採った。

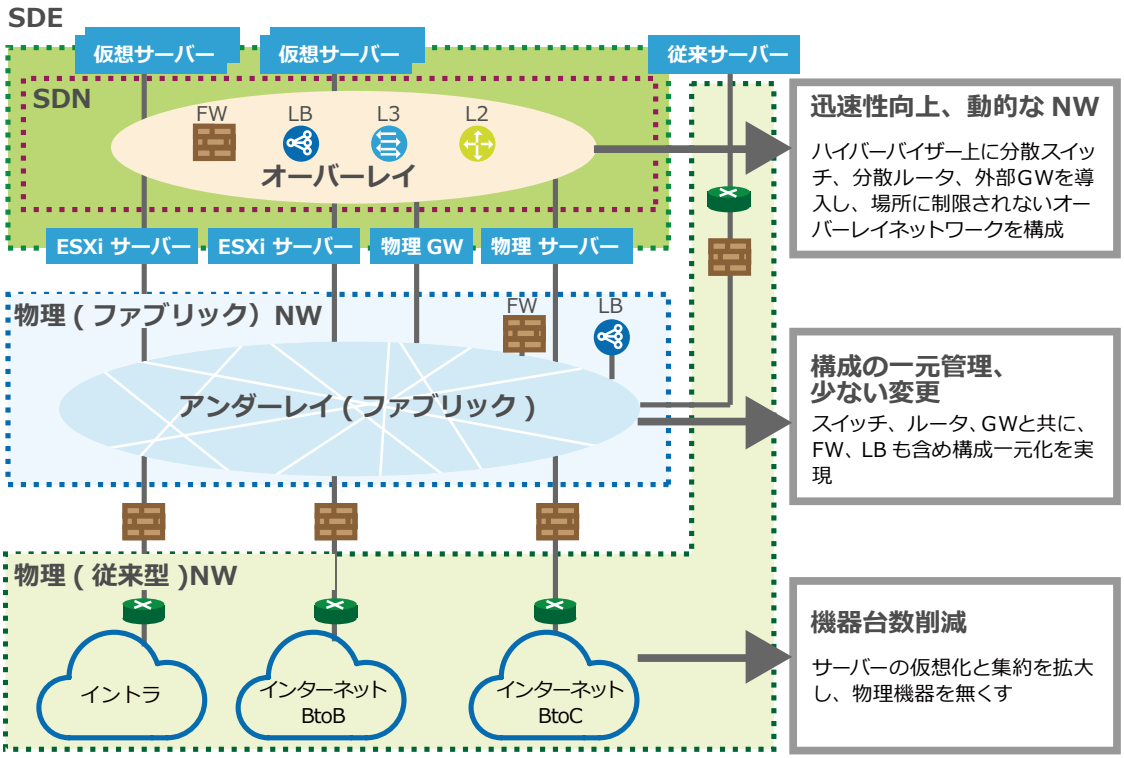


図 3. 仮想サーバー・物理サーバー間のオーバーレイネットワーク

まず物理環境においては、サーバーの仮想化と集約を推進し、物理的な機器を大幅に削減した。

次に、各ネットワークを収容するアンダーレイネットワークを、標準技術を活用して構築し、できる限りシンプルな構成に仕立てあげた。スイッチやルータ、ファイアウォール、ロードバランサなどのデバイスを一元管理できるような仕組みを設けた。

仮想化環境上では、SDN 技術を用いて分散スイッチと分散ルータ、ファイアウォールやロードバランサを実行するソフトウェア（NFV）を導入し、オーバーレイ･ネットワークを構築した。仮想マシンどうしは､オーバーレイ・ネットワークを用いて接続されるため、場所の制約を受けることもなく、要件に合わせたネットワークを迅速に構築できる。

従来の企業ネットワークでは、ゲートウェイ、DMZ、内部ネットワークという一連の構成要素をゾーニングによって分離してセキュリティを確保する。SDN では、そうしたゾーン管理をソフトウェア的に行うことができる点がメリットだ。セキュリティを含めたひとかたまりのネットワーク･インフラを、サーバーやアプリケーションの要件に合わせて提供。業務毎に異なるレベルのセキュリティを、ネットワークの物理要件に左右されることなく、より柔軟に最適に提供できる。

これは、上記の例のような LOB 毎に乱立するゾーニングに対処するだけではなく、一時的なキャンペーンサイトなどテンプレート化された使い捨てネットワークを簡単に作成するなど、高度な柔軟性を実現できる。

ケース（3）
アプリケーション指向型ネットワークの実現

上述の B 社では、仮想化環境の IA サーバーだけでなく、UNIX のハイエンドサーバーも基幹システムとして用いていた。これらを仮想ネットワーク上で柔軟に組み合わせることのできる環境を実現したかった。

ヘテロ環境では、ホスト－ IA サーバー、ホスト－ UNIX サーバーという物理要件に加えて、アプリケーションごとに異なる通信要件が発生し、さまざまなトラフィックパターンが混在することになる。そうした要件に合わせて、物理ネットワークを動的にコントロールする仕組みが必要だ。いわゆる「アプリケーション指向型ネットワーク」の実現である。

そこで IBM は、ケース（2）でオーバーレイ・ネットワークの構成に用いられていた SDN の適用範囲を、アンダーレイネットワークまで広げるという構成を提案した。サーバーの OS や仮想 OS の種類に左右されることなく、ネットワーク仮想化や管理が可能となるテクノロジーの採用である。アプリケーションの通信要件（帯域やセキュリティ、経路など）をプロファイル化し、API やソフトウェアインタフェースを介して、ネットワーク機器を動的にコントロールする仕組みも実現できた。種類の異なるネットワークデバイスも集約され、運用コストの削減にも寄与したと考えられる。

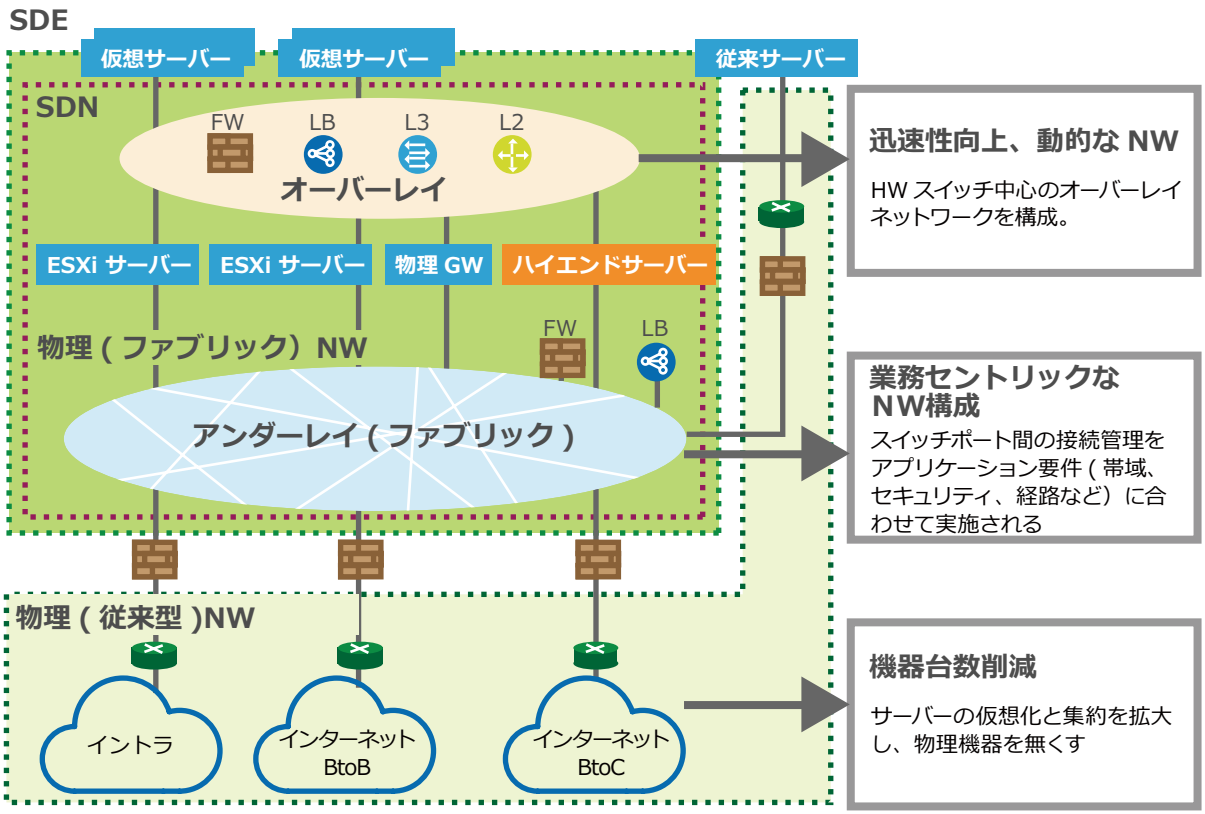


図 4. ヘトロ環境のオーバーレイネットワーク

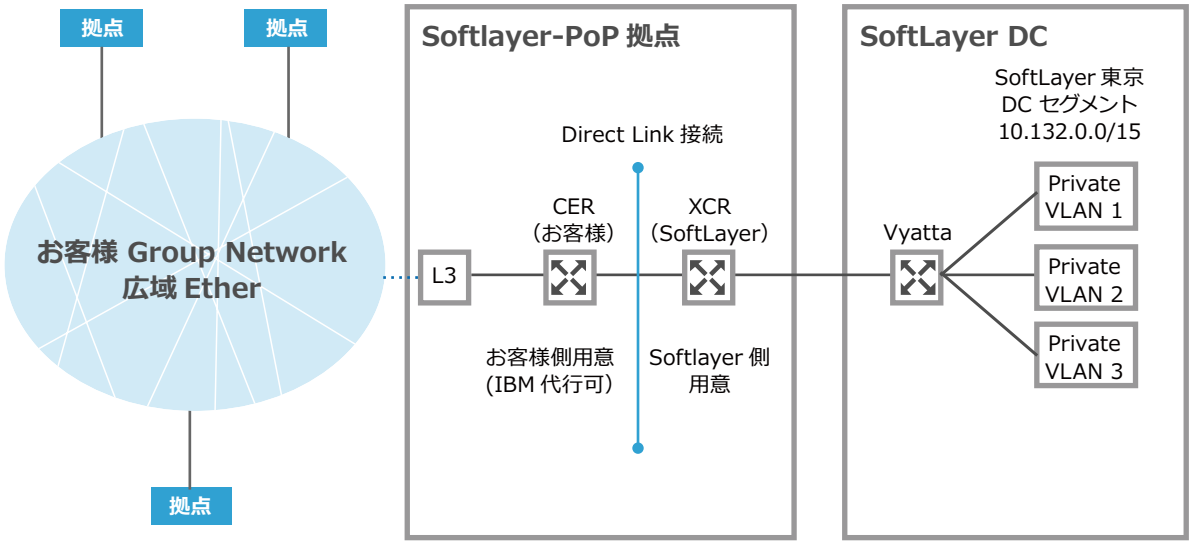
ケース（4）
パブリッククラウドのネットワーク・インフラを活用

グローバル展開を図るC社では、パブリッククラウドの柔軟性や迅速性をビジネスに活用し、クラウドと自社システム間でリソースを自由に配置転換できるような仕組みが求められていた。

しかし、一般的なパブリッククラウドサービスでは、サーバーやストーレッジ資源の迅速な調達は柔軟だが、ネットワーク環境は制限が厳しく、自由度は非常に制限される。自社システムで採用している戦略的なネットワーク構造を統合することは困難だった。

そこでIBM が提供したソリューションは、IBM SoftLayer で提供されているベアメタルサーバーを用い、SDN 技術（VMware NSX）と NFV 技術（Vyatta）を用いてオーバーレイ・ネットワークを構築するというものだった。

C社では、広域Ethernetを利用して拠点間を接続したグループネットワークを構築していた。これをSoftLayer上の仮想イーサネットまで延伸し、SoftLayer上に構成されたグローバルネットワーク上に組み込むという方式だ。



CER:Customer Edge Router
XCR:Cross-Connect Router
Vyatta: 米国 Vyatta 社によりオープンソースで開発されていたソフトウェアルータ

図 5. クラウドサービスのネットワーク上の制約を SDN で解決 (回線接続)

物理的にも、ケース（2）と同様にシンプルな構成となっている。

SoftLayer では、強力で高性能なネットワーク機能を提供しているため、ユーザーがネットワークを構築する必要はない。さらに、SoftLayer の特長の 1 つであるベアメタルサーバーを利用すれば、通常の IaaS のクラウドでは困難な、ネットワークも含めたインフラ・デザインが可能で、SoftLayer の高速な回線をグローバルに疎通できるアンダーレイネットワークが提供され、その上に仮想ネットワークを形成するという方法が実現できるのだ。

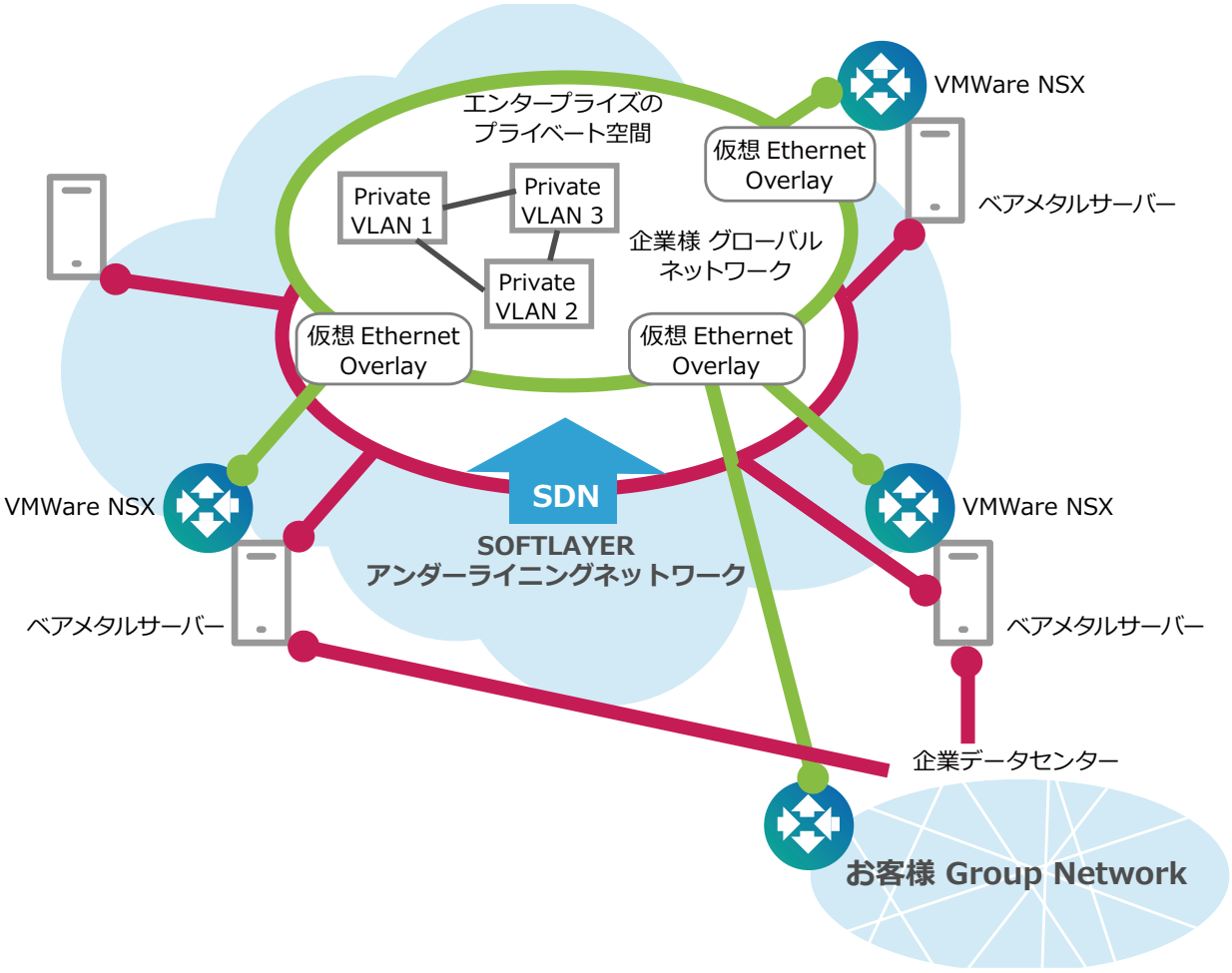


図 6. クラウドサービスのネットワーク上の制約を SDN で解決 (Overlay NW)

ケース（5）
顧客の要求に合わせて最適なネットワークを迅速に提供

サービスプロバイダーである D 社では、マルチテナント型のネットワーク環境で自社サービスを顧客に提供しているが、SDN を採用することでより信頼性の高いネットワーク環境の構築に成功した。

同社では、顧客のセキュリティに対する要求が非常に高まっており、どのようなネットワークでサービスを提供すべきかという課題を持っていた。設計上は最大で 10,000 の論理的に分離された VLAN が必要となった。そのため D 社では、テナントのアプリケーションごとにトラフィックを確実に分離できる柔軟性の高いネットワークを求めていた。

そこで IBM が提供したのが、下図のようなネットワークである。

仮想イーサネットをオーバーレイする SDN を構築し、NFV 技術でネットワークサービスを提供する。その際の仮想ネットワーク製品としては、イーサネットオーバーレイを実現する SDN、サーバー仮想化を実現する VMWare、ルータおよびファイアウォール機能を実現する NFV 機能などマルチベンダー製品を組み合わせる。これにより、パブリッククラウドが提供する実際のネットワークの制限などを意識せず、自由に VLAN を設計、利用することができ、プライベート、パブリックの両面で自分のアドレス空間を保持できる。

ポイントは、SDN コントローラー をドメインごとに提供しており、完全に分離された VLAN のグループをテナント毎に構成できるところにある。つまり、仮想イーサネットの管理ドメインそのものをテナントのセキュリティゾーンにマッピングしてしまうイメージだ。

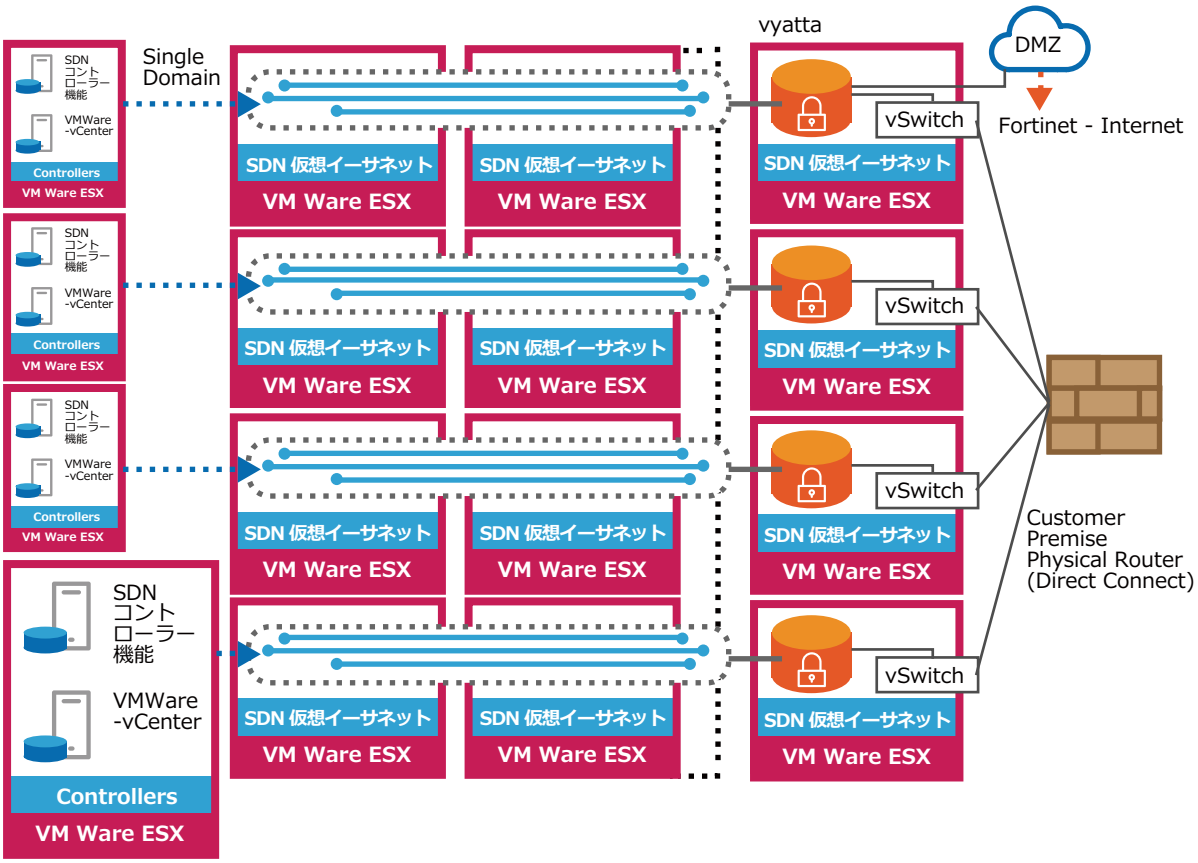


図 7. テナントのサービスリクエストに応じたネットワークの払い出し

最適なネットワーク構築のためのネットワークアーキテクト

SDN は技術的には、2 種類ある。つまり、「ホップバイホップ方式」を採る OpenFlow などの技術と、今回の事例の中心となっていた「イーサネットオーバーレイ方式」を取る仮想イーサネットだ。

Google や Facebook など巨大なデータセンターを世界中で運用しているメガクラウドプロバイダーでは、OpenFlow やホワイトボックススイッチを活用して、ダイナミックにリソースを移行できる巨大なネットワークを形成している。

日本アイ・ビー・エムのグローバル・テクノロジー・サービスの技術理事 山下克司氏は、「メガクラウドの規模だからこそ、ダイナミックな操作が実現できる OpenFlow が意味を持つ」と述べる。

「固定的なネットワークを運用する事の多いエンタープライズレベルでは、(OpenFlow の採用は) いままでと同じネットワークを安価なスイッチで構築できるというような事例に陥りがちです。前述の事例で示したように、データセンターを中心にしたイーサネットオーバーレイ方式では、既存ネットワーク技術の上で SDN のさまざまなメリットが得られます」(山下氏)

しかし SDN ――仮想空間にネットワークを形成する世界では、ユーザー自身が構築を行うのは難しい。非常に高度な技術力とノウハウが必要なためだ。

そこで IBM では、インフラストラクチャー・デリバリー サービスライン・デリバリー エグゼクティブアーキテクトの陳建和氏のような、ネットワーク専門のアーキテクトを配備し、さまざまなビジネス要件に最適なソリューションを提供できるように体制を整えている。

「ネットワーク構築の現場では、接続方式やアプリケーションなどの機能要件と、可用性やセキュリティ対策といった非機能要件という 2 種類の要件を検討・決定していきます。最近では、こうしたアーキテクチャ・デザインの判断を体系的に記録していく『アーキテクチュアル・デシジョン』という考え方が浸透しつつあります。SDN のようにネットワークの構成が変化していく環境では、この考え方は非常に重要です」(陳氏)

つまり、旧来のネットワーク設計のようにネットワーク配線図を提出するだけではなく、どうやって設計したか、この設計はどのような将来的な柔軟性等の意味を持つのかという機能に説明を加えた機能設計図が必要となるのである。こうした設計手法によってネットワーク構成が変化したときにも、そもそもの設計理由に立ち戻ることができる。

「IBM は、古くからさまざまな業種・業態のネットワークの設計・構築に従事しており、膨大な知見を蓄積しています。さらに最新のネットワーク構築を提供するため、優秀なネットワークアーキテクトとスペシャリストを確保しています。ビジネスに最適なネットワークを実現するために、当社へぜひご相談ください」
(山下氏)