

ネットワークインフラに柔軟性

「SD-WAN」が注目されるホントのところ

大野智史 (NTTPC コミュニケーションズ SD-WAN スペシャリスト)

- ITトレンドなんて見通せない -- ネットワークインフラに求められるのは柔軟性
- 目先だけでは判断できない -- ネットワークコストは運用まで含めて考えよう
- ケーススタディで見る SD-WAN の効用 -- 開店も撤退もスピードアップ
- uCPE や vCPE など運用後に生きてくる SD-WAN の管理機能を知ろう
- SD-WAN への移行：
一括導入と段階導入のメリットとデメリットを比較
- SDx 化の先には幸せが待っている!?
-- 全てがソフト化された未来を大胆予想



「SD-WAN」が注目されるホントのところ

ITトレンドなんて見通せない – ネットワークインフラに求められるのは柔軟性

Amazon Web Service (AWS) に Microsoft Azure、そして Google Cloud Platform。IT に携わる読者なら、これらクラウド関連の話題を目にしない日はないだろう。Office 365 に G Suite (旧 Google Apps) など、デスクトップで使うアプリケーションのクラウド化や、VDI でデスクトップ環境自体をクラウド化する企業も増えている。

このような時代に求められる企業ネットワークのあるべき姿について、考えてみたい。

「うちもクラウドにするか」って簡単に言われても…という現状

先述の通り、IT 系各メディアで、クラウドの文字を見ない日はない。

この記事を読んでいるいまこの時も、同じブラウザでサイボウズや Salesforce.com など、クラウドサービスのタブを開いている読者がいることだろう。あるいは Outlook で Office 365 のメールやカレンダーをチェックしているかもしれない。

それくらいクラウドは日常業務に浸透している。いまはオンプレミスでコラボレーション基盤を運用しているとしても、明日にも「Exchange サーバを廃止して全社の業務環境を Office 365 に移行しよう」と言われる可能性があるのが、現在の状況だ。

しかし、クラウドツールへの依存度が高まれば高まるほど問題となるのが、ネットワーク環境だ。本社と

拠点、データセンターを結ぶ WAN 環境は、そうそう簡単に構成を変えられるものではない。あなたがネットワークインフラの担当者であれば、その窮状を経営陣に訴えるだろう。

しかしクラウド化の流れを止めるのは容易ではない。なんとかして対応せざるを得なくなることは明らかだ。

帯域増強？ VLAN 構成の変更？ 各地に分散している拠点との閉域網 (VPN) も見直すべきか……。色々なことが頭に思い浮かぶに違いない。「前回のネットワーク更改時に、これを見越して構成しておけば」と悔やんでも、間に合わない。そもそも数年先の IT トレンドなんて、誰にもわからない。

未来の変化は誰にもわからないから、ネットワークにも柔軟性を

現在の IT トレンドを事前にどれくらい見通すことができただろうか。一例として、業界予測のプロである IDC が 2011 年に公開したレポートを見ると、パブリッククラウド市場は順調に成長し、2016 年の市場規模は 3027 億円にのぼるとある。

しかし同社が最近発表したレポートによれば、2016 年のパブリッククラウド市場は前年比 30.5% 増の 3762 億円。どこまでを「クラウド市場」に含むかの違いにより各社の数字は違うものの、他のリサーチ会社も 2011 年には似たような予測を発表している。

「SD-WAN」が注目されるホントのところ

ここからわかることは、情報収集と予測を本業とするプロフェッショナルでさえ、2割以上読み誤る勢いでパブリッククラウド市場が成長しているということ。社内システムの運用に追われる身で将来を見通すなどほとんど不可能に近い。

IT部門にいれば、モバイルが浸透することくらいは見通せたかもしれない。とはいえ、オフィスのデスクトップとモバイルとの垣根がこれほどまでに低くなることまで見通せた読者は、はたしてどれくらいいるだろうか。

かつてはPCが必須だった業務の多くが、今ではスマートフォンやタブレットだけでこなせるようになっている。端末の性能が高まったことも要因のひとつではあるが、アプリケーションの多くがクラウド化したことが大きな影響を及ぼしている。

モバイルの浸透とアプリケーションのクラウド化。利便性が高まる歓迎すべき変化ではあるが、ネットワーク管理者にとっては、新たな悩みの種でもある。

モバイルデバイスからクラウドアプリケーションを使われると、コンプライアンスを守ることは難しくなる。クラウドアプリケーションへのアクセスをコントロールできる仕組みが必要で、それを整備するのは容易ではない。

しかも、クラウドアプリケーションを利用するメリットのひとつは、始めやすくてやめやすい、乗り換えやすいこと。政府によるテレワークの推進など、働き方の変化も大きく、それにあったツールを選べるのがクラウドの魅力だ。

一方で、コンプライアンス確保のためにはそのたびに認証や接続設定を変えなければならない。ネットワ

ークの柔軟性の低さが、せっかくのクラウド活用の足を引っ張ることになりかねないのが現状なのだ。

先に述べたように、数年後のITトレンドを見通すのは、プロのアナリストでさえ難しい。常に最新技術の恩恵を受けられるようにするためには、将来の変化は読み通せないという前提に立ち、ネットワーク自体に柔軟性を持たせるべきだ。その手法のひとつとして注目され始めたのが、SD-WANだ。

SD-WANがあればドラスティックな変化も怖くなくなる

オンプレミスでコラボレーション基盤を運用しているような企業であれば、各拠点のネットワークはサーバが設置されているデータセンターとのみ通信できれば十分と考えてネットワークが設計されているだろう。

インターネットにアクセスする必要がある、データセンターを経由してアクセスする。全国に小規模な拠点を多数展開する飲食業や小売店ではよくある構成だ。セキュリティを確保しやすく、ネットワーク利用の統制も容易だ。

そこにいきなり、Office 365やG Suiteのトラフィックが流れ込んで来たら、果たして耐えられるだろうか。データセンターとインターネットを結ぶ回線はあっという間に帯域オーバーとなり、業務のボトルネックになる。慌ててデータセンターからインターネットへのアクセス帯域を増強しても、今度は各拠点とデータセンターを結ぶ回線へとボトルネックが移るだけだ。

こんなとき、拠点間がSD-WANで結ばれていたら…。これらの変化にあっという間に対応し、従業員は

「SD-WAN」が注目されるホントのところ

クラウドサービスを使って快適に業務に当たることができるようになるだろう。

もちろん SD-WAN は万能薬ではないが、変化に対する柔軟性は高く、全体を見渡した管理もしやすいと

いうメリットを持つ。そんな SD-WAN の効果や具体的な使いこなし方、ポイントごとにチェックすべき機能などを解説していきたい。ネットワーク担当者ならずとも、クラウド導入を検討中の読者にも、SD-WAN の魅力を伝えることができれば幸いだ。



「SD-WAN」が注目されるホントのところ

目先だけでは判断できない -- ネットワークコストは運用まで含めて考えよう

前回の記事では、テクノロジーの進化は早く、常に最新技術を業務に取り入れていくためには、将来見込まれる変化に応えられるネットワークが必要であると述べた。これから生まれる技術を取り入れられるソフトウェアベースの拡張性と柔軟性、それらを素早く反映できる即時性が求められる。

そうした期待に応える技術のひとつとして紹介したのが「SD-WAN」という仕組みだ。今回は SD-WAN についてもう少し深掘りして、既存の WAN との違いについて解説していこう。SD-WAN の導入を考える上で悩みがちな課題も取り上げ、それぞれに対する解を示したい。

物理的な機器や回線からネットワークの構成、運用を分離

まずは、SD-WAN と既存 WAN との違いについて紹介しよう。基礎的なことはご存知かと思うが、SD-WAN について詳しくない読者もいると思われるので、基本的な技術をおさらいしておきたい。

SD-WAN を一言で言うなら、データセンターの中で利用が広がる SDN を WAN の世界にまで広げたものだ。各拠点に設置したエッジ機器と、拠点間を結ぶ物理的なネットワークの上に仮想的なオーバーレイネットワークを構築する。

各拠点を結ぶネットワーク回線が光回線であろうが専用線を使った閉域網であろうが関係ない。管理者はオーバーレイネットワークだけを見ればいい。SDN と

同じようにオーケストレータを通じて、物理的な機器やネットワークの変更なしに自由にネットワークを構成、運用できる。

SD-WAN は高い？ 数年先まで見据えて既存ネットワークと比較しよう

SD-WAN について少し調べたことがある読者が、まず考えるのがコストの違いだろう。SD-WAN は、物理ネットワークの上に論理的なオーバーレイネットワークを構築する。それに対して既存の WAN なら、その基礎になっている物理的なネットワークだけで構成できる。単純に考えて、旧来の手法の方が低コストに構築できることは明白だ。しかしネットワークは構築したら運用しなければならない。

5 年間でリプレースすることを前提に、WAN の構築や運用にかかるコストを想定してみよう。いま必要な帯域と構成を考え、その機能を満たすルータ機器を各拠点に配置し、ネットワークを構築する。初期コストは、確かに SD-WAN よりも低く抑えられるだろう。

だが 1 年後、業務システムが変わり、扱うデータ量が急に数倍に膨らんだら、どうなるだろうか。

すべての拠点のネットワーク帯域を強化し、もしかしたらセキュリティ強化のために各拠点のルータ機器をリプレースしなければならないかもしれない。さらに数年後、経営判断のスピードアップを求めて各拠点からリアルタイムに情報収集するよう求め

「SD-WAN」が注目されるホントのところ

られたら？ 逆に各拠点から多拠点の情報も参照しながら現場で経営判断できるよう求められたら？ コンプライアンス強化やコスト適正化のためにネットワーク利用の可視化を求められたら？

こうした要求が発生するたびに新たな機器が導入され、それに対応すべくネットワークの帯域増強やセキュリティ強化、可視化の推進などに取り組まなければならない。

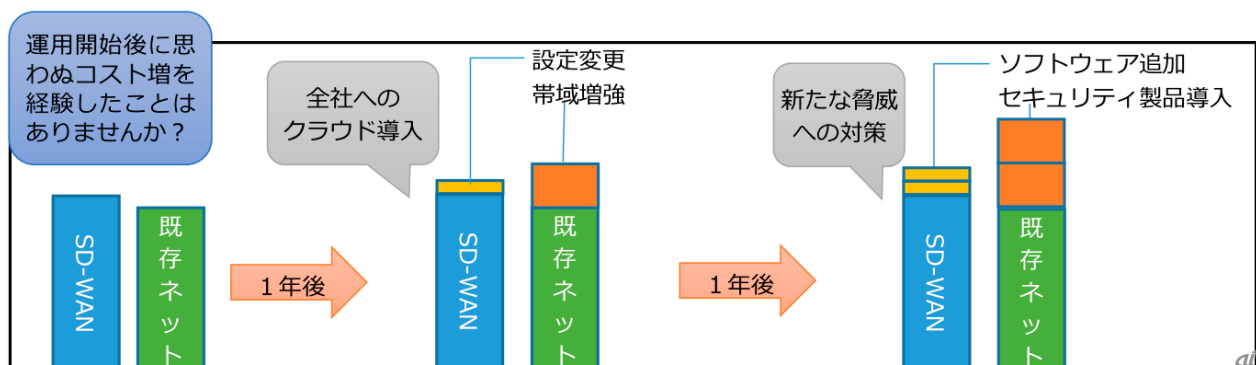
業務を効率化し、あるいは売り上げを伸ばすためのテクノロジーの未来は、誰にも見通せない。数年前に、ここまで急速にクラウド化が進むと予測できた読者はどれくらいいたでしょうか。社内情報を外部に置くことに抵抗を覚えて業務システムをオンプレミスで構築し、償却まで仕方なく使っている企業などもあるのではないだろうか。

同じように WAN も簡単には再構築できず、IT の進化に場当たり的に対応するしかなく、いつの間にか高

コストなネットワークを抱え込んでしまうことになる。そのうえ、前回の記事で指摘したように、それらのシステムとしてクラウドが採用される可能性も高い。

インターネットへの接続を効率しつつセキュリティを確保するためには、データセンターを中心にしたネットワーク構成自体を変更しなければならない事態も考えられ、コストを理由にプロジェクトを断念せざるを得ない事態さえあり得る。

一方 SD-WAN は、初期コストにおいて既存の WAN に比べて高く感じられるかもしれないが、追加コストをほとんどかけることなく上述の変化に対応できる。安定したコストで将来の変化にも対応していけるため、数年先までの投資対効果 (ROI) で比較すれば決して高価ではないことがわかるだろう。ネットワークコストだけではなく、それらの構成変更にかかる IT 部門の人的リソース、時間的リソースもあわせて考えれば、SD-WAN のコスト優位性はさらに高まる。



運用開始後の思わぬコスト増 (筆者作成)

「SD-WAN」が注目されるホントのところ

論理ネットワークならではの 高いセキュリティを低い運用負荷で

閉域網など、閉鎖的な物理ネットワークや専用線を使うことで、セキュリティを担保しているという企業もあるだろう。SD-WAN は物理ネットワークに異存しないオーバーレイネットワークを構成するので、同じような発想でのセキュリティ確保は難しいように見えるかもしれない。では SD-WAN のセキュリティは低いのか？ 答えはノーだ。

オーバーレイネットワークを構成するために、各エッジ機器同士は暗号化通信で結ばれる。セッション盗聴の不安とは無縁だ。すべての通信が高度に暗号化されるため、アプリケーションの種類や使用回線によりセキュリティレベルが異なる事態も避けられる。

なおかつオーケストレータはすべてのトラフィックを把握し、多くの SD-WAN サービスで用意されるコントロールパネルではトラフィックを可視化する機能を備えている。不適切な通信を把握して、強制的に帯域を抑制したり特定のトラフィックだけを停止したりすることさえ可能だ。

さらに高いセキュリティを望むなら、uCPE (Universal Customer Premises Equipment = 汎用構内通信機器) としてエッジ機器にセキュリティ機能を追加することもできるし、オーバーレイネットワーク上に仮想の統合脅威管理 (UTM) を設置して、

WAN 内やインターネットからの脅威を退けることもできる。

暗号化やトラフィックの可視化は、セキュリティ機器を導入すれば既存の WAN でも実現できる。一方で、拠点の増減やセキュリティ機器のポリシー変化へのたびに数多くの機器の設定変更が生じ、ヒューマンエラーを招く恐れもある。

その点 SD-WAN の場合は、新たな拠点のエッジ機器を設置するだけで、機器が持つ固有情報を使って認証し、正しいネットワークに自動的に接続され、最新の設定を読み込んでネットワークに参加する。正しい通信先として認められたエッジ機器同士でしか通信できない仕組みにより、なりすましを防ぐほか、拠点の増減はゼロタッチプロビジョニング、セキュリティ設定は一元管理と、ヒューマンエラーや悪意ある操作が入り込む余地を最小限に抑えている。

今回は理屈が多く固い内容となってしまったが、実際の使い方を知れば、既存の WAN よりもコストメリットを得やすく、運用負荷も低いことをわかってもらえるだろう。もちろん、新しい技術の習得や運用体制の変更など、解決しなければならない課題もない訳ではない。

ということで、次回以降は実際の使い方や導入の際の留意点など、SD-WAN をより具体的に見ていきたいと思う。

「SD-WAN」が注目されるホントのところ

ケーススタディで見る SD-WAN の効用 -- 開店も撤退もスピードアップ

これまでの連載において、初期コストと運用コスト、導入後の柔軟性が高いことによるメリットなどについて概略的に紹介してきた。今回はさらに踏み込み、SD-WAN と既存の WAN を使った場合の具体的な違いをケーススタディで見ていきたい。

今回取り上げるのは、飲食店や小売店など、広い地域に多店舗を展開しているケースだ。ネットワークの構築、運用に頭を悩ませる担当者が多い業態でもあり、きっと参考になるだろう。

シーン 1： 新店舗開設時も数営業日で社内ネットワークに接続完了

チェーン展開されているコンビニエンスストアや飲食店に顕著だが、生活に密着した小売業、飲食業では住民の動向変化にあわせて店舗を展開する。ビジネスに有利な立地を探し、物件を手配した後は、できる限り早く開店することが求められる。

什器の設置や現地での従業員確保などさまざまな準備が必要だ。それだけではない。

販売時点情報管理 (POS) システムで全国の店舗の情報を把握することが、ビジネスの現状を知り次の一手を考えるための必須要件になっている今、ネットワークの整備も営業開始に欠かせない要件のひとつだ。ビジネス部門からの要望に短時間で応えることが IT 部門に求められ、それはパートナーであるシステムインテグレーター (Sler) も同様だ。

POS や業務用 PC を社内ネットワークに接続するための WAN 整備は、従来であれば通信会社か、広域をカバーできる Sler が担当していた。ネットワーク担当者は新店舗を担当する部署と連携しつつ、通信会社や Sler に連絡を取り、新店舗に新たな回線を引くことになるだろう。一般的には 2 週間程度かかる、この作業が、営業開始のアシを引っ張らないようにスケジュールを考えなければならない。

これが SD-WAN になるとどう変わるのか。まず、最大の違いはネットワーク接続までにかかる時間だ。従来の WAN では 2 週間程度を見積もっていたのに対して、SD-WAN なら数営業日で社内ネットワークに新店舗を組み入れることができる。

物理ネットワーク選択の柔軟性と、設定に必要な作業時間に大きな違いがあるため、このような差が生じるのだ。IT 管理を内製化している場合の理想値ではなく、Sler にネットワーク設定や管理を依頼する際にも同様の効果は得られる。Sler が現地に出向いて機器を設定する必要がなくなり、ネットワーク設定のスピードとコストに好影響をもたらす。

SD-WAN なら、物理ネットワークは何でもいい。既存店舗で地元ケーブルテレビが提供する通信回線を契約している場合には、その回線を使って SD-WAN に組み入れることも可能だし、暫定的に営業に間に合わせるだけなら LTE ネットワークでも構わない。

さらに、SD-WAN ではネットワーク設定がオーケストレーターで集中管理されるので、新店舗をネット

「SD-WAN」が注目されるホントのところ

ワークに加える設定変更にも短時間で対応できる。現地で必要なことは、工期とコストから最適な回線を選んで敷設し、SD-WANのエッジ機器を設置することだけだ。

シーン 2： 店舗移転時や臨時店舗での営業でも 魅力が生きる

住民の生活動線の変化に応じて、より良い立地へと店舗を移転することもあるだろう。そうした場合にもSD-WANならスピーディに対応できる。

移転先店舗にネットワークを敷設したら、旧店舗からエッジ機器を移すだけ。IPアドレス書き換えなども不要だ。あえて言うなら、管理者がわかりやすいように、オーケストレーター上に表示される店舗名を変更する必要があるくらいだろうか。

移転に伴うネットワーク変更がここまで容易になれば、これまでは諦めていたことも可能になる。たとえば店舗の改装時に、一時的に違う場所で営業を継続する場合などがそれに当てはまる。臨時店舗をWANに組み入れるのはコスト面でのデメリットが大きい。

従来なら、諦めて運用でカバーするか、デメリットを承知で高いコストを負担して短期間しか使わないWANを敷設し、設定を変更するしかなかった。Slerにネットワーク管理を依頼している場合には、何度もネットワーク設定変更を依頼しなければならず、そのコストも無視できるものではなかったはずだ。

しかし、SD-WANなら臨時店舗であってもすぐに社内ネットワークに組み入れることができる。オーケストレーターと通信可能なネットワークさえ確保でき

ればよく、帯域の問題がなければ、前述の通りLTEネットワークでも構わないのだ。Slerの負担も軽減されるので、運用コストの低減が期待できる。

こうした使い方を応用すれば、海水浴場やスキー場などに期間限定で出店する場合でも、WANに接続されたPOSを提供できるようになる。SD-WANによって社内ネットワークへの接続は、ここまで柔軟になれるのだ。

これはビジネスを推進する企業にとってネットワークがより有用になるだけではなく、これまでWANに組み入れるのを諦めていたシーンがSlerにとっての新たなビジネスチャンスになることも意味する。

シーン 3： 撤退時でも機器もコストも 無駄を出さない

拡大だけではなく縮退にも素早い決断が求められる昨今、撤退時のコストを最小限に抑えることも重視しなければならない。小売店や飲食店の場合、出店先地域の変化やフランチャイズ契約の終了によって閉店することも多いだろう。そうした場合のコストや手間も、SD-WANなら従来のWANに比べて低く抑えることができる。

閉店時に店舗側で必要となるのは、店舗に敷設したネットワーク回線を解約し、エッジ機器を本社に送り返すだけ。あとはオーケストレーター上の設定を書き換え、当該店舗の情報を削除すればネットワーク設定の変更はおしまいだ。回収したエッジ機器は次に開店する店舗で使えるので、機器調達費を削減可能。機器もコストも無駄がない。

「SD-WAN」が注目されるホントのところ

uCPE や vCPE など運用後に生きてくる SD-WAN の管理機能を知ろう

SD-WAN のメリットがわかりやすい例として、前回
は小規模多店舗展開する業態における SD-WAN の拡
大、変更、縮小について紹介した。今回は SD-WAN 入
門の続編として、導入後の運用にフォーカスしてみたい。

WAN に限らずネットワークはあって当然のものとして日々使われる。そのため構築だけではなく、導入後の運用負担の大小は、選定の大きなポイントになる。業務現場に影響を与えずに、なおかつ少ない手間で、刻々と変わるセキュリティ事情に対応できるのも SD-WAN の魅力なのだ。

SD-WAN の強みは設定、 運用の集中管理

本連載の前半で、SD-WAN ならプロビジョニング
の手間を大幅に省けることを紹介した。簡単におさ
いすると、新しい拠点の追加は、当該の現地拠点にエ
ッジ機器を設置するだけのゼロタッチプロビジョニ
ング、エッジ機器同士の通信を暗号化することで仮想ネ
ットワークレイヤの機密性を保持、そしてコントロー
ルパネルによるネットワーク設定の一元管理などが
SD-WAN の一般的な特長と言える。

中でも運用開始時に大きく響いてくるのが、コント
ロールパネルによる集中管理だ。各機器の設定を変更
するために現場に出向く必要がないだけではない。セ
キュリティポリシーを各拠点に確実に適用できるこ
と、そして、その状況を可視化して確認できることが
大きなメリットだ。各拠点で勝手に設定変更をするこ

とはできないので、セキュリティポリシーで禁止され
ているアプリケーションを勝手に使われるような心
配からは解放される。

クラウドを考えるなら トラフィックの分散を視野に

一元管理できるのが SD-WAN のいいところでは
あるが、セキュリティにこだわるあまり、全ての通信
を管理下に置こうとすれば、やはり運用の負担は大き
くなる。もちろん、回線の帯域も厳しくなるだろう。

そこで覚えておいてもらいたいのが、SD-WAN で
はトラフィックを可視化した上で適切な経路を使わ
せるようにすること。最もわかりやすい例が、業務
用アプリケーションにアクセスする場合と、Office
365 や G Suite のようなパブリッククラウドにアク
セスする場合の使い分けだろう。

オフィスからしか利用させたくない業務用アプリ
ケーションには、必ず SD-WAN を経由してアクセス
するようにする。一方で、サービス事業者側である程
度のセキュリティが確保されているパブリッククラ
ウドにアクセスする場合には、各拠点からそのままイ
ンターネットに接続させるのだ。

こうすることで WAN 回線の帯域を有効に使うこと
ができ、各拠点の従業員は快適な速度で、パブリック
クラウドを利用できるようになる。インターネットブ
レイクアウトなどと呼ばれる機能だ。

「SD-WAN」が注目されるホントのところ

なお、直接インターネットに出て行くトラフィックも各拠点に設置したエッジ機器を通すことで、どのようなサービスにアクセスしているのかをコントロールパネルから監視したり、業務に不要なサービスにアクセスできなくするセキュリティポリシーの適用は可能だ。

エッジとクラウドの両方のセキュリティ機能をチェックすべし

インターネットブレイクアウトなどの機能を使えば、WAN回線の帯域を無駄にせず、なおかつセキュリティを確保できる。しかし、各拠点のエッジ機器がインターネットからの脅威にさらされることになるため、全てをSD-WAN経由にする場合とまったく同等のセキュリティを確保できるとは言いきれない。ではどのような対策を取ればいいのか。

こうした心配を取り除くには、各拠点のエッジ機器にセキュリティ機能をプラスすればいい。各拠点に追加機器が不要という前半の話と相反するように聞こえるかもしれないが、そんなことはない。

SD-WANサービスの多くが、セキュリティ機能をソフトウェアとしてエッジ機器に追加できるオプションを用意している。「uCPE」などと呼ばれる機能だ。そして、それらの有効化/無効化や細かい機能設定はコントロールパネルから一元管理できるようになっている。

エッジ側だけではなく、仮想ネットワークレイヤ側でもセキュリティを強化したい場合には「vCPE」と呼ばれる仮想の統合脅威管理(UTM)を活用するといえる。こちら物理的な機器として設置するのではなく仮想化されており、クラウド上で動作する。

uCPE、vCPEと似た名前の機能が出てきたところで、その違いを整理しておこう。

そもそも「CPE (Customer Premises Equipment : 顧客側に設置された機器)」はネットワークの世界では、ネットワークの終端に設置されるモデムやルータ、ファイアウォールなどの機器を指す。データセンターに設置されるファイアウォールやセキュリティアプライアンスなどがそれに当たるのだが、SD-WANにおいてはネットワーク全体が仮想化され、データセンターに当たる終端は存在しない。

そこで登場するのが「vCPE (Virtual CPE)」という訳だ。仮想ネットワークレイヤ上に設置される、仮想化されたセキュリティ機器と考えればしっくり来るだろう。一方で、拠点側には物理的な終端が残っている。こちらを守るのが、分散型セキュリティ機能である「uCPE (Universal CPE)」だ。

名前は似ているが、動作する場所にセキュリティ保護の方針に大きな違いがある。vCPEはクラウド上に仮想的に設置され、全体のセキュリティを一元管理する。uCPEは分散してセキュリティを管理するために、各拠点に設置される。もっともuCPEもエッジ機器の追加機能として提供されるのが一般的であり、物理機器として設置される訳ではない。

ネットワーク全体のセキュリティを守るvCPEとエッジに分散してセキュリティを守るuCPEを併用することで、拠点側と仮想ネットワークレイヤの双方でセキュリティコントロールできるようになり、より強固なWANを構築できるだろう。

SD-WANの柔軟性を生かすためにもセキュリティ機能は欠かせないので、エッジ側、仮想ネットワークレイヤ側のそれぞれにセキュリティ機能を持つサービスを選ぶのがひとつの選定ポイントになるだろう。

「SD-WAN」が注目されるホントのところ

SD-WAN への移行：一括導入と段階導入のメリットとデメリットを比較

既存ネットワークと比較した SD-WAN の特長や生かすところについては、これまでの連載でおおまかにわかっていただけたのではないだろうか。しかし、メリットがわかって、日々の業務に使われるネットワークをそう簡単に移行できるものでもない。

一気に入れ替えるとしたら、どのようなタイミングがいいのか、日常業務をこなしながら順次入れ替えていくにはどのような工夫をするべきなのか。今回はそうした移行について考えてみよう。

ハードルはあるがコストメリットが魅力の一括導入

考え方としては、最もシンプルなのが一括導入だ。従来の WAN を一気に SD-WAN に置き換える。SD-WAN のメリットを最大限に受けることができるし、既存ネットワークとの併用期間を最小限にできるのでコストメリットが大きい。

しかし、ネットワークコストだけを見ていては見失うデメリットもあることを指摘せざるを得ない。それは、ネットワークを一気に刷新する際に起こりがちな、検証不足や確認不足に起因するトラブルだ。

他の導入方法と比べるために、一括導入の際のメリットとデメリットをまとめてみよう。

最大のメリットは言うまでもなく、ネットワークコストの最適化。一括で導入するからこそ、すぐに社内ネットワーク全体の可視化ができ、帯域やルート設定の最適化も行える。

デメリットは、SD-WAN を前提としたネットワークの再設計に時間を要することと、個別システムの動作検証に多くの時間を割けないこと。アプリケーションレイヤ、TCP/IP で動作する昨今のアプリケーションであれば理論上は動作に問題ないはずだが、理論上問題がないのと実際に問題がないのとは別の話。それは、システムインテグレーター（Sier）や IT 担当者の多くが知るところだろう。

社内ネットワークの大規模更改を計画中の企業なら、その機会に SD-WAN を導入すれば恩恵を最大限に受けることができるので、一括導入は魅力ある選択肢となるだろう。しかし、そのような企業ばかりではないはずだ。

では、一気に SD-WAN に移行するほかにどのような移行手法があるのかといえば、やはり段階的導入ということになる。

ここではステップバイステップで移行する手法として 2 つのケースを紹介し、それぞれについてメリット、デメリットを考察してみたいと思う。

「SD-WAN」が注目されるホントのところ

まずは出口を SD-WAN 化、 可視化によるコンプライアンス強化から

ステップバイステップで SD-WAN を導入するひとつの方法として考えられるのが、クラウドやインターネットへの出口のみ SD-WAN 化すること。現状で本社を経由してインターネットに接続しているなら、本社のネットワークに SD-WAN のエッジ機器を設置。データセンターを経由しているなら、データセンターからインターネットへの出口にエッジ機器を設置する。

既存のネットワーク機器に新たなルーティング設定を追加するだけなので、ネットワーク変更に伴う作業は少ない。必要なエッジ機器も 1 台からと最小限に抑えられるので、SIer としても低リスクで SD-WAN への第一歩を提案できる。

しかし、各拠点にエッジ機器を設置するだけのゼロタッチプロビジョニング、ネットワーク全体の可視化とコントロールが SD-WAN 最大のメリットだったのではないか。この連載の読者はそう感じるかもしれない。それは、まったくその通りだ。

しかし前述の通り、社内ネットワーク全体を一気に更改するのは容易ではない。では部分的に導入するなら、どこから手をつけるのが効果的なのかという問いへの答が、境界から SD-WAN に置き換えていこうという訳だ。各拠点を結ぶネットワークが既存の仕組みのままなので、SD-WAN の恩恵を受けられないと思うかもしれないが、そんなことはない。

SD-WAN のメリットとして、ネットワークトラフィックの可視化とコントロールが挙げられる。社内ネットワークのトラフィックが集中する本社やデータセンターにエッジ装置を設置することで、まずは社内ネットワークの可視化から取り組むことができる。

クラウド化により想定よりもインターネットへのトラフィックが増えている、トラフィック全体に占める業務用アプリケーションの割合が高いなどの現状を把握し、次の一手を考えるための材料をまずは手に入れるのだ。

現状を把握した上で、それに対応するための社内ネットワークのあり方を考えれば、その先の SD-WAN 導入拡大を効率化できる。新規拠点から順次導入する、特定のアプリケーションだけから導入するなど自社に合った展開を検討できるだろう。

もしかしたら SD-WAN に向いていないアプリケーションが見つかるかもしれない。その場合には、アプリケーションの改修を含めて全体効率を重視したネットワーク更改の計画を立てることもできる。

既存の物理網を生かしたまま、 アプリケーションを順次移行

ステップバイステップ導入のもうひとつの方法は、物理ネットワークレイヤに依存しないという SD-WAN の特長を生かしたものだ。まず既存の社内ネットワークはそのままに、各拠点にエッジ機器を設置して全体を SD-WAN 化する。

しかしトラフィックのルーティングは変更せず、業務では当面の間、既存ネットワークを使う。アプリケーションから見れば、ネットワークが変わらないので、日々の業務に支障をきたす恐れがない。

こうした下準備をした上で、日常業務への影響が少ないものから順次、SD-WAN 上での動作を検証し、問題がなければ SD-WAN へとルーティングを変えていく。ミッションクリティカルなものは開発環境を用意しての検証が必要かもしれないが、その

「SD-WAN」が注目されるホントのところ

時間も十分に取れる。実際に敷設した SD-WAN を使って検証できるので、結果に問題がなければすぐに移行できる。

この方法であれば、全拠点導入によりネットワークを一気に最適化できるという一括導入のメリットと、可視化されたトラフィックを確認し、アプリケーションごとの動作を検証しつつ部分ごとに移行することでリスクヘッジができるという、ステップバイステップ導入のメリットを同時に得られる。

とはいえ、いいことばかりではない。エッジ機器を一括導入する初期コストの負担、移行期間中は論理的な社内ネットワークが二重に存在するため、管理負荷が一時的に高まることは覚悟しなければならない。

日常業務に絶対に影響を与えたくない、しかし全体の SD-WAN 化をスムーズかつスピーディに進めたいと考える企業なら、通常通り業務アプリケーション

を提供しつつ移行できるメリットの方が大きいはずだ。

それぞれのロードマップに沿った手法の選択を

SD-WAN 導入の方法論を 3 つ紹介したが、それぞれはモデルケースに過ぎない。ネットワークに依存するアプリケーションを持つ企業もあるかもしれないし、帯域制御装置などの導入によりデータセンターにおけるトラフィックの可視化はすでにできているという企業もあるだろう。それぞれ自社に合う導入方法を検討してもらいたい。

検討の際には、ネットワークだけではなくアプリケーションの知識も求められるので、社内の IT 部門だけでは荷が重いかもしれない。そんなときにはネットワーク構築に関わった Sler や業務アプリケーション開発を依頼した Sler に意見を求めるといいだろう。ぜひ、自社にとって最適なロードマップを描いて進んでもらいたい。

「SD-WAN」が注目されるホントのところ

SDx 化の先には幸せが待っている！？ -- 全てがソフト化された未来を大胆予想

これまでの連載で、既存の社内ネットワークに対する SD-WAN のメリットと、その生かし方、取り入れ方を語ってきた。SDN というキーワードが流行ってから数年、十分実用的なレベルに達したネットワークの “SD 化”、その現状の理解に役立てば幸いだ。

今回は連載最後を締めくくる意味で、今後考えられるさまざまな “SDx” が実用化したらシステム管理はどう変わっていくのか、筆者の夢を交えつつ語ってみたい。

あらゆるものがソフトウェア化するのは IT 進化の不可避な流れ

SD-WAN 以外にどのようなものがソフトウェア化されていくのか。それを考える前に、あらゆるものがソフトウェア化されるという方向性が本当に IT 進化の流れに沿っているのか考えてみたい。

SD-WAN、SDN といったネットワークのソフトウェア化よりも先に普及したのは、サーバインフラのソフトウェア化だ。x86 系サーバの仮想化技術は 1990 年代から広まり始め、2000 年代に商用レベルとなって一気に広まった。

今や物理サーバ 1 台で 1 つの OS インスタンスを動かすのは、よほど高い負荷が想定される場合に限られる。セキュリティ製品やネットワーク機器も、物理アプライアンスではなく仮想アプライアンスとして提供されるものが増えた。

さらに遡ると、PC 自体も OS がソフトウェア化してから飛躍的に進化したものだ。ROM に書き込まれた決められた動作しかできなかったものが、起動時に OS やアプリケーションを読み込むことで汎用性を得た。

ハードウェアと切り離された OS の進化により、PC 自体の性能向上の向上も可能になった。似たようなもので近年の例を考えると、携帯電話が似たような道を歩んでいる。発売時の性能がすべてだったフィーチャーフォンとは違い、スマートフォンは OS やアプリケーションの進化により性能向上を続ける。

初期にはハードウェア処理に頼ることでパフォーマンスを追い、やがて十分な性能を得ると自由度や拡張性を高めるためにソフトウェア化されていく。これは IT 機器とそれを取り巻くシステム群の生態系のようなものなのだ。

“情シスロボット” で日々の運用業務から解放される日が来るかも？

IT を取り巻く全てのものソフトウェア化されるのは、避けられない。いまそこに、人工知能 (AI) が加わりようとしている。

サーバやネットワーク、さらに近いうちにアプリケーションの管理までがソフトウェアにより、かなり高度に自動化されるだろう。そうなったときの IT 部門の働き方はどのようになるのだろうか。

「SD-WAN」が注目されるホントのところ

24時間365日休むことなく、システムを監視するAI。アプリケーションの健全性やネットワークのセキュリティを監視し、セキュリティ上のリスクを発見すれば、当該通信のみ遮断するなど、人間の手を借りることなく処理できる範囲も広がっていくはずだ。

アプリケーションの応答速度や機器の稼働温度などから、故障につながるファクターを見つけることができれば、ハードウェア故障を予知して交換を促すなど、予防まで自動化できるかもしれない。

SD-WANのようにハードウェアとは完全に別のレイヤを構築できるものの場合、ソフトウェアの動作や設定を別のソフトウェアが監視し、軽微な不具合であれば、修復や復旧までも自動化できる可能性がある。ハードウェア、ソフトウェア双方の監視から故障パターンが見えてくれば、事前に対処することで免疫力アップも望める。

AIやボットなどの技術が進化すれば、いまは人手に頼っている社内からの問い合わせもソフトウェア化されそう。パスワード忘れや定型的なアプリケーションの利用申請などは、ボットが対応し、AIが判断し、アプリケーションやネットワークの設定をソフトウェア上で変更するだけで対応できてしまう。いわば、“情シスロボット”の実現だ。

このまま進化が進めば、人間の仕事はなくなってしまうのではないかという論調もある。しかし筆者はそうは考えない。ITを取り巻くあらゆるものと述べたが、当面はソフトウェア化できそうにない部分がある。

それは最も低いレイヤのラストワンマイルと、逆に超高度な判断が必要な部分だ。

人間にしかできないことに最大限のリソースを注ぐため、SDxへの第一歩を

SD-WANがどれだけ進化しても、物理的な回線を各拠点に敷設するところまではソフトウェア化できない。機械による省力化は進むかもしれないが、人間が回線を敷設し、ネットワーク機器と接続する作業全体が自動化されるのは相当に先のことだろう。

逆に、物凄く高度な判断が求められるシーンにも人間の出番が残っている。ITを経営にどのように生かしていくのか、現場からの要望に応えるためにどのようなシステムを次に導入すべきなのか。

そうした俯瞰的でビジネス的な視点は、人間でなければ持てない。現状の可視化やそこから導き出される予測により判断材料を提供してくれるにはなるだろう。しかし、それらを使ってビジネスを進めるのが人間である以上、どのようなシステムが適しているかを判断するのも人間でなければならない。

こうした高度な判断に時間を割くことこそ、これからのIT部門に求められる機能になるだろう。そのためにも、ソフトウェアで自動化できることはできるだけ自動化し、人間の能力は人間にしかできないことに当てるべきだと考える。そのためのSDxであり、そこに向けて今すぐ踏み出せる第一歩がSD-WANの導入なのだ。

Master'sONE CloudWAN[®]

セキュアパッケージ

ネットワークは もっと軽快になる!

閉域ネットワークで
SD-WAN機能を利用



IPoE接続により
低遅延



トラフィックの
可視化可能



国内VPNサービス初!^{*}
日本のネットワー
ク環境に適した
SD-WANサービス

Windows Update、
Office 365など
インターネットオフロードが可能

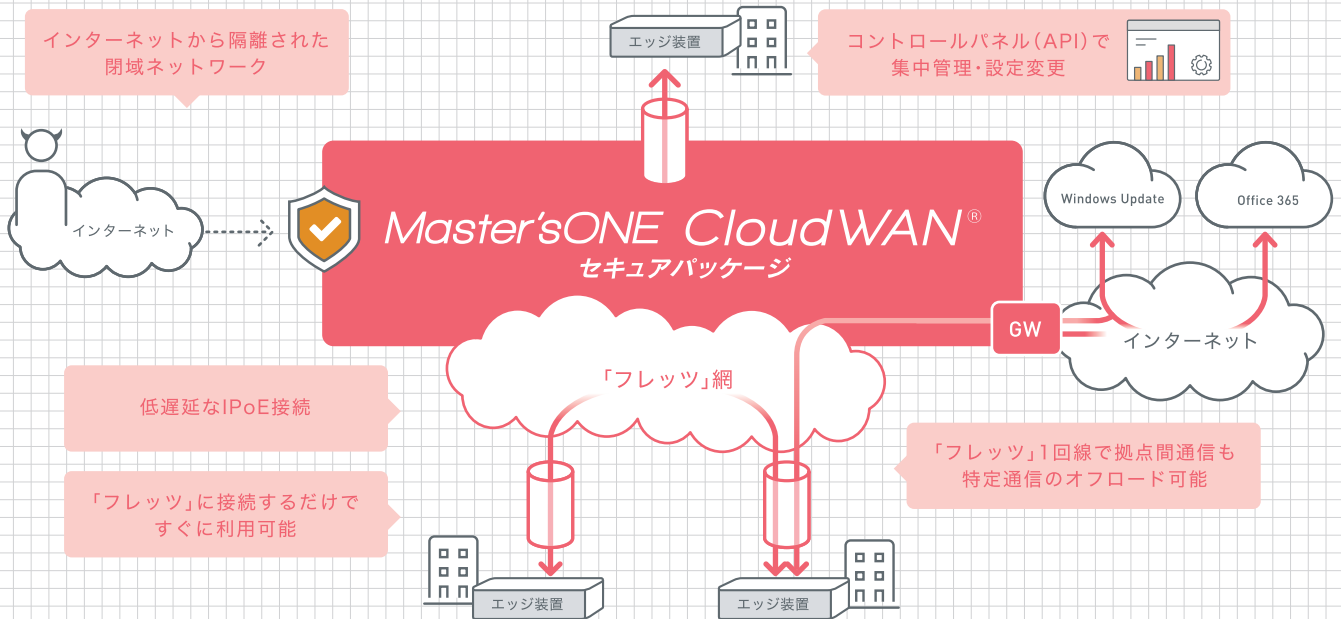


ネットワークはもっと軽快になる!

Master'sONE CloudWAN[®] セキュアパッケージ

提供イメージ

日本企業の多くが利用しているネットワーク環境(閉域性)の良さを残したまま、安心してSD-WAN機能を導入できる、今までにないSD-WANサービスです。低遅延・セキュアかつ低コストで、即時性に優れた企業ネットワークの構築を実現します。



主な特長

セキュアかつ安定した通信を実現



インターネット経由によるセキュリティリスクが無く、安心して利用できます。またIPoE接続を採用しており、輻輳(混雑)しにくい低遅延な通信を実現します。

トラフィック可視化・制御



ネットワークに流れるアプリケーション種別とそのトラフィック量をグラフィカル表示で確認できます。輻輳や遅延の原因をアプリケーション単位で特定でき、回避策・解決策へと役立てられます。

WebやAPIで、運用効率化



各拠点にあるエッジ装置の管理・設定変更を、WebやAPI経由で一元的に遠隔にて実施可能。現地に赴く必要なく、迅速にネットワークの設定・変更を行えます。

価格(税別)

Master'sONE CloudWAN[®] セキュアパッケージ

2018年7月5日
受付開始!

月額料金

初期料金

月額料金		初期料金	
スタンダード	インターネットオフロード	スタンダード	インターネットオフロード
/拠点	/VPN	/拠点	/VPN
19,000円	30,000円	0円	0円

・初期料金は、NTTPCオーケストレーター初期設定料金、NTTPC閉域ネットワーク初期料金、エッジ装置送料が含まれます(オンサイト取付工事は含まれておりません)。エッジ装置の設定はお客様にてご実施ください。
・月額料金は、NTTPCオーケストレーター利用料金、NTTPC閉域ネットワーク月額料金、エッジ装置利用料金(センドバック保守)、コントロールパネル利用料金が含まれます。

お問合せ・サービス詳細

<https://cloudwan.nttpc.co.jp>

