セキュリティと一体化したSD-WAN

クラウド時代に適した「ネットワーク×セキュリティ」の在り方

日本企業にも「Office 365」などのクラウド利用が広がり始めた。それに伴い、対処が難しいネットワークの課題が浮上してきた。その課題とは何か。対処方はあるのか。

フォーティネットジャパン
山田 麻紀子氏
（マーケティング本部
プロダクトマーケティング
マネージャー）

クラウド利用の広がりに伴って生まれた新たな課題

「これまでは、メールサーバをはじめとする業務用のサーバは社内のインフラにあったため、ほぼ社内で完結していたトラフィックが、クラウド利用によってその多くがインターネットにアクセスするパターンに変わっていく」。フォーティネットジャパン（以下、フォーティネット）の山田 麻紀子氏（マーケティング本部プロダクトマーケティング）は、こう指摘する。

このようにトラフィックパターンが変わった結果、既存のネットワーク構成に2つのゆがみが生じているという。

1つ目は、クラウドとの、つまりインターネットとのトラフィックが増加し、データセンターからインターネットへの接続回線やゲートウェイの負荷が増大していることだ。特にOffice 365のようなSaaSを利用している場合には、トラフィックもさることながらセッションも多く消費するため、プロキシサーバには大きな負荷がかかる。表示が遅くて待たされるなど、従業員の利用に支障が生じるケースもある。また拠点ネットワークから閉域網を経由したトラフィックが増加するため、閉域網のサービス費用が増大するケースもある。

2つ目はセキュリティ面の課題だ。従来はシステムがオンプレミスにあったため「セキュリティも自身で構築しなければいけない」という一種の責任感がユーザー企業側にもあった。だがクラウドでは「事業者側がセキュリティサービスを合わせて提供するケースもあり、『お任せ』のスタンスになりがちだ」（山田氏）。実際には事業者とユーザー企業のそれぞれが責任を果たす「責任共有モデル」がクラウドセキュリティのベースとなっており、企業側でも適切な対策が必要だ。

既存のネットワーク構成に起因する課題を解決し、クラウドのもたらす利便性を享受するには、どうしたらいいだろうか。こうした課題を解消するためのコンセプトとしてフォーティネットが提唱するのが「セキュアSD-WAN」だ。

ネットワークを拡張するだけでなくセキュリティもともに提供する「セキュアSD-WAN」

拠点間を結ぶWANをソフトウェアで制御し、柔軟なルーティングを実現する「Software-Defined WAN」（SD-WAN）。サーバやストレージだけでなくWANもまたソフトウェア化し、柔軟に制御することで、より高い品質の回線サービスをより安価に利用可能にしたり、管理者が不在の拠点側ネットワークをセンター側（本社側）で一括制御できるようにしたりしよう、というものだ。

フォーティネットが提供するセキュアSD-WANも、ネットワークの基本の部分はSD-WANと同じだ。ただし「単にネットワークを拡張するだけでは不十分。そこにきちんとセキュリティが載っていなければならない」と山田氏は述べる。長年にわたり、統合脅威管理（UTM）をはじめとするセキュリティ製品を提供してきたフォーティネットが、SD-WANに取り組む意義はそこにある。

「FortiGate」が実現するセキュアSD-WAN

セキュアSD-WANの中核となるのは、フォーティネットのセキュリティアプライアンス「FortiGate」だ。FortiGate専用の独自OS「FortiOS」は標準機能としてプロキシ機能やSD-WAN機能を含む。追加ライセンスを購入する必要はない。これらの機能を活用すれば、重要なアプリケーションには高品質な回線を割り当てたり、帯域を消費するアプリケーションには安価な回線を複数割り当てたりと、アプリケーションに合わせて利用する回線を設定するポリシーベースのルーティングが容易に実現できる。

SaaSとのトラフィックにポリシールーティングを適用する際、考慮すべき課題がある。SaaS側では不定期にIPアドレスやポート番号などが変更されることがあり、ある日突然設定当初のポリシーが有効に機能していない状態になる可能性がゼロではないことだ。かといって企業の担当者がSaaS側の設定を小まめにウォッチし、追随するのも骨が折れる。

フォーティネットは「Internet Service Database」（ISDB）というデータベースを構築し、どのアプリケーションがどのIPアドレスとポートを利用しているかといった情報を格納している。Office 365に加えて「Box」「Dropbox」など、グローバルで利用されている約300種類のアプリケーションを網羅している。これを参照するだけで、最新の情報に基づいたポリシールーティングを実現できる。

本社側にも拠点側にも適用可能、クラウド時代に適したネットワークを実現

セキュアSD-WANには2通りの実現方法がある。1つ目はデータセンター側にFortiGateを導入し、Office 365専用のプロキシとして活用する方法だ（図1上）。これまで1台のプロキシが担ってきた負荷を分散させつつ、クラウドへのアクセスを可視化する。これまで運用してきたプロキシも、Office 365以外の通信にそのまま生かせば、既存の投資が無駄になることもない。

2つ目は拠点側にFortiGateを導入し、いわゆる「インターネット・ブレイクアウト」を実現する方法だ（図1下）。全てのトラフィックをデータセンター側に回すのではなく、Office 365をはじめとするクラウドへのトラフィックについては、FortiGateを介して拠点から直接インターネットに抜けるようにする。データセンター側の負荷が大幅に減るだけでなく、Office 365へのアクセスログも残り、きちんと利用状況を可視化できる。

FortiGateは、次世代ファイアウォール（NGFW）やプロキシ機能も備えている。これらを活用すれば、どの従業員がどのアプリケーションを利用しているかを把握し、可視化できる。従業員の認証情報を把握し、正しい従業

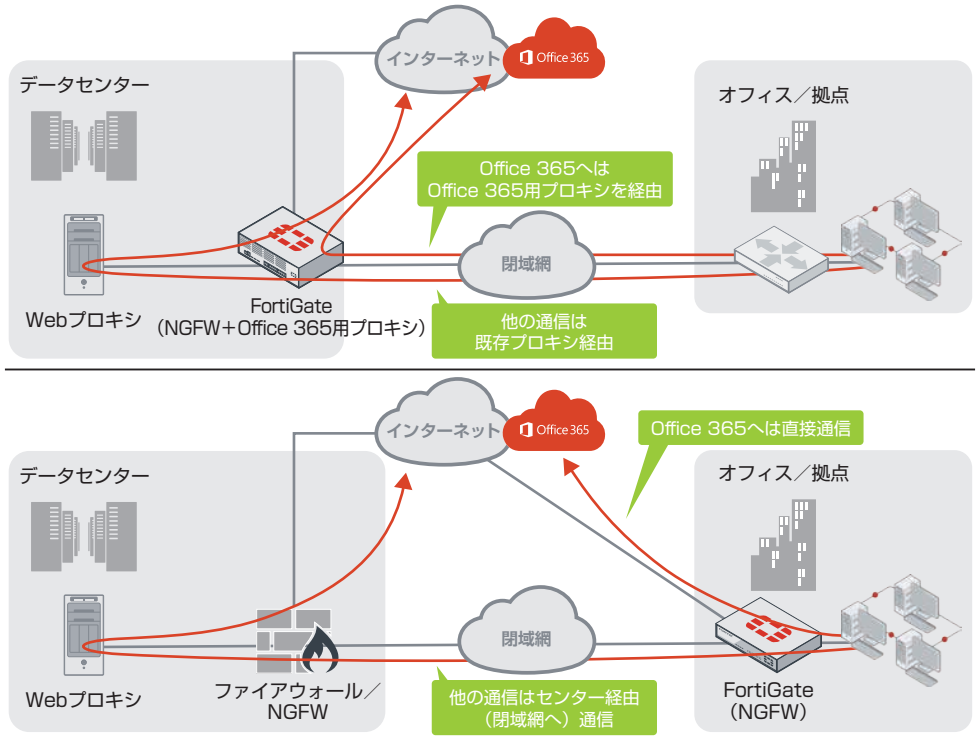

図1 データセンター側（上）、拠点側（下）のセキュアSD-WAN導入

員のアカウントか否かに応じてOffice 365へのアクセスを制御するテナント制限機能も実装し「悪意ある持ち出しはもちろん、操作ミスによる機密情報のアップロードも起きないよう保護できる」と山田氏は述べる（図1）。SSL暗号化通信をしていても、標準機能で復号して制御可能だ。

個人アカウント経由の情報漏えいの懸念

残念ながら、クラウド利用時の設定ミスが原因となり、情報が漏えいしてしまう事件は少なくない。個人PCで利用するために、Office 365の個人アカウントを持っている従業員がいるとしよう。適切に設定していないと、個人のアカウントで社内LANからOffice 365へログインできてしまう。社外秘のデータをOffice 365にアップロードすれば、LANの外へ持ち出せることになる。

日本マイクロソフトはこうした課題への対策として、プロキシでヘッダを制御し、アクセス先を自社テナントのみに絞る「テナントの制限」機能の利用を推奨している。だが必要性や方法が分からず、こうした状況を放置している企業は少なくない。

既にこうした利点を評価し、クラウドへの移行を前提に、FortiGateの仮想マシン版をパブリッククラウド「Microsoft Azure」内に構築し、直接接続サービス「ExpressRoute」を介してOffice 365用のプロキシとして活用している大手企業もあるという（図2）。またFortiGateをOffice 365のプロキシとして利用し、ポリシールーティングをしつつ使用状況の透明化を狙う企業もあるという。

クラウドの採用に伴って、閉域網の回線増強やセンター側プロキシの増強、インターネット回線の増速といった、コストのかかる解決策を迫られている企業は少なくない。セキュアSD-WANの採用によって、セキュリティという付加価値を組み合わせながら、こうした課題を解決できる可能性がある。フォーティネットでは今後、ISDBの増強やクラウド利用時の制御・可視化をする「CASB」（Cloud Access Security Broker）との連携などを実現しながら、クラウド時代に適したセキュアなネットワーク環境をさまざまな企業に提供する構えだ。

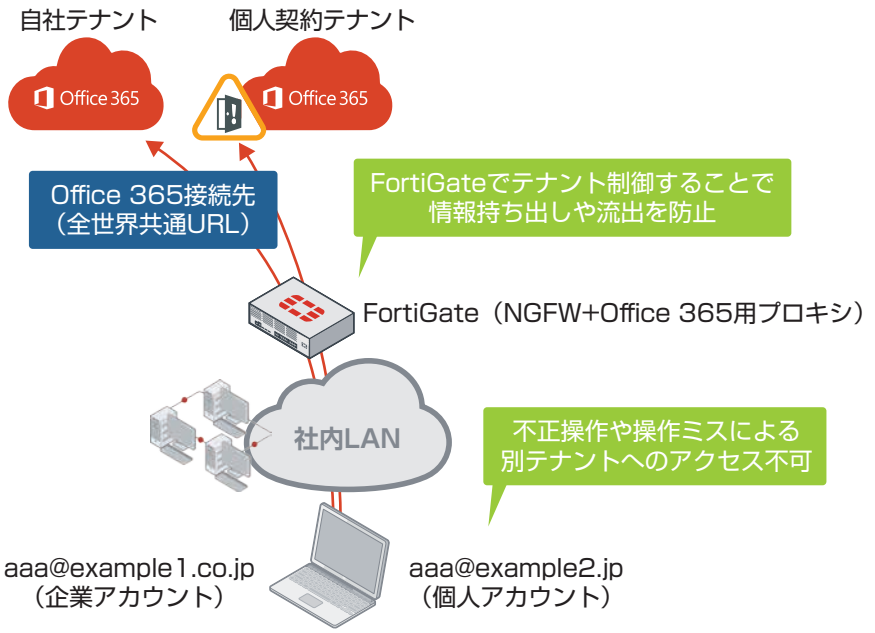

図2 FortiGateのテナント制限機能

※この冊子は、TechTargetジャパン（http://techtarget.itmedia.co.jp/）、キーマンズネット（http://www.keyman.or.jp/）に2018年4月に掲載されたコンテンツを再構成したものです。

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ

WP-ITmedia-SecureSD-WAN-201804-R1