クラウド移行で深刻化した帯域逼迫を FortiGate VMを用いた「プライベートSASE」で解決 スケーラビリティと自由度、コストパフォーマンスを 兼ね備えた新たな選択肢に

アイビーシーでは、サポート期限の到来を機にアプライアンス版FortiGateを仮想版に切り替え、AWSへ移行する方針を決めた顧客の支援を行った。Gateway Load Balancer（ゲートウェイロードバランサー）によってマルチAZで冗長性を確保したいという顧客の要望を満たし、クラウド活用の広がりにともなって逼迫していたネットワークリソースの課題も解決する、クラウドネイティブな新たな選択肢として手応えを感じている。

アイビーシー株式会社

本社所在地　東京都中央区新川一丁目8番8号
設　　立　2002年10月16日
事業内容　ITシステム性能監視ツールの開発 / 販売 / サポート
ITシステムの性能評価サービス
ITシステムの設計・構築、コンサルティング
IoTセキュリティ基盤の開発 / 提供
各種機器、ソフトウェア販売

アイビーシー株式会社
ビジネスソリューション事業本部
コンサル・インテグレーション事業部
コンサルティング部
シニアコンサルタント
井上 周洋氏

導入・構築のポイント

(1) クラウド活用の広がりで生じたネットワークの逼迫を、クラウド環境に最適化された仮想ファイアウォールFortiGate VMで解決

(2) アプライアンス版FortiGateとほぼ同一の操作性を生かし、アクセスポリシーをそのままスムーズに移行

(3) 複数のセキュリティ機能をクラウド上のFortiGate VMで実現し、プライベートSASEという新たな選択肢を提供

クラウドシフトで高まるネットワーク負荷を解消する、クラウドネイティブな新たな選択肢

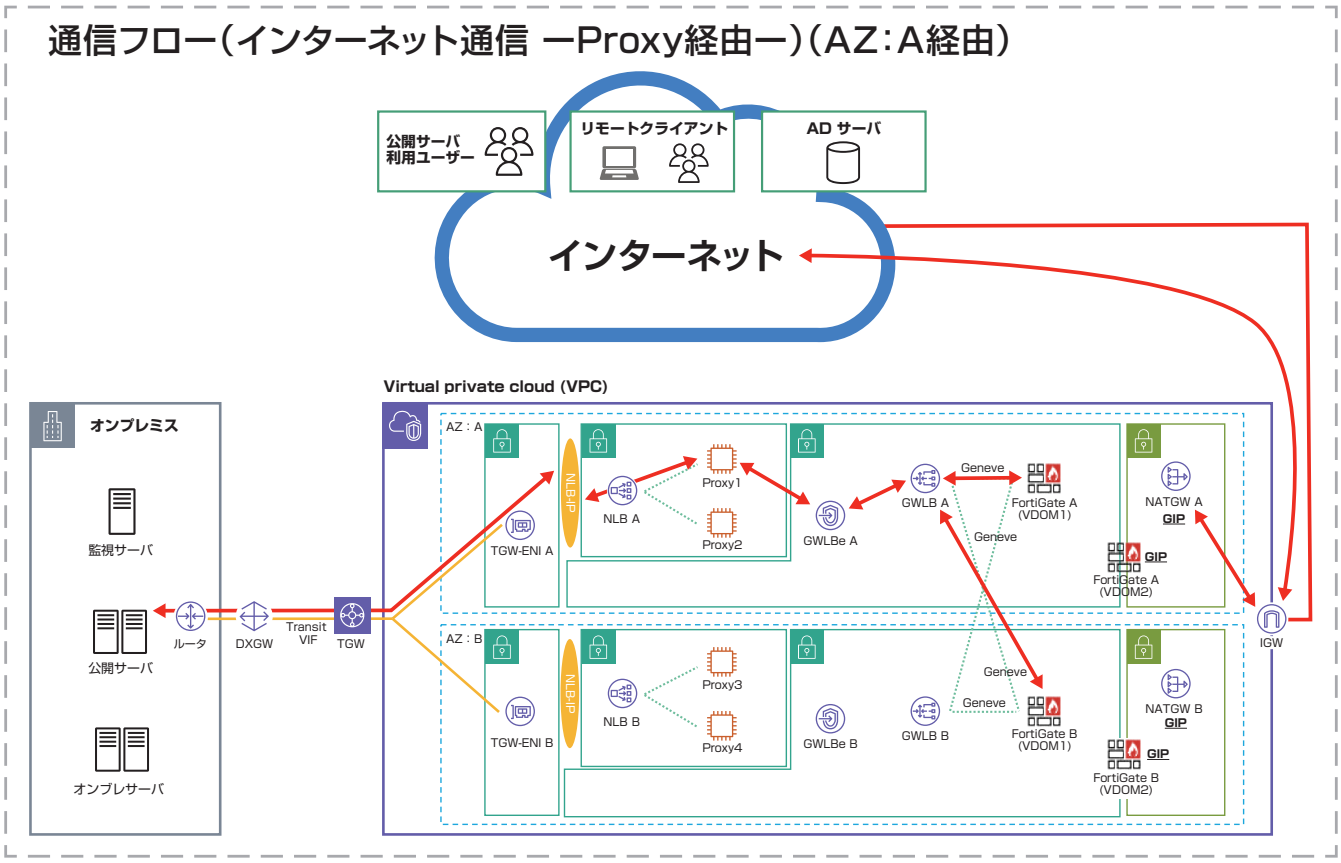
アイビーシー（IBC）は自社開発のシステム情報・性能監視ツールである「System Answer G3」の開発・販売やサポート業務を中心に、そこから得られる情報をベースにしたITインフラ構築のコンサルティングを通して、顧客を支援してきた。

最近では「メリハリの効いた」クラウド活用を提案する機会が増えている。「クラウドシフトは進んでいますが、CADなどお客様が利用するアプリケーションや扱う情報によっては、クラウドに持っていくのが非現実的なこともあります」（アイビーシー株式会社 ビジネスソリューション事業本部 コンサル・インテグレーション事業部 コンサルティング部　シニアコンサルタント、井上周洋氏）。そうした要件を踏まえながら、最適なインフラのインテグレーションを行っている。

そんな同社がしばしば顧客から打ち明けられる悩みが、クラウドシフトに伴って高まるネットワークの負荷だ。

かつては、全国各地の拠点をWAN回線で結び、本社・データセンター内のアプリケーションを利用する構成で事足りていた。だがコロナ禍も相まって、Web会議をはじめとするSaaSやクラウドサービスを活用する場面が増えてきた。それにともない、本社とインターネットやクラウドを結ぶゲートウェイやプロキシ、外部接続回線の負荷が高まり、利用に支障を来す場面が目立つようになっている。

SaaSや特定のインターネット接続については本社を介さず直接インターネットに抜ける「ローカルブレイクアウト」という選択肢も有効だ。ただ今回は、クラウド活用を前提としたスケーラブルなネットワークインフラを用意し、従業員に快適な業務環境を提供したいというニーズを踏まえ、IBCは、アマゾン ウェブ サービス（AWS）でFortiGateの仮想アプライアンス「FortiGate



VM」を動かして、「プライベートSASE」と表現できる新しいアプローチを提案した。プライベートSASEならば、もともとのクラウドの利点であるスケーラビリティをフルに享受しつつ、FortiGateの機能を生かし、ニーズに合わせた自由度の高い構成をコストパフォーマンスよく実現できるからだ。

AWSアーキテクトの支援を得ながらマルチAZ環境にFortiGate VMを構築

ことの起こりは、ある顧客がファイアウォールとしてデータセンターで運用していたFortiGateのサポート期限が迫ったことだった。以前から少しずつクラウドシフトを進めていたこの顧客では、「管理の手間も削減するため、せっかくならば物理アプライアンスの後継機種に入れ替えるのではなく、仮想化してクラウド上に持っていきたい」と決断した。帯域をはじめとするリソースを柔軟に拡張できるクラウド全般のメリットに加え、さまざまなツールがそろっており、複雑なシステムでも移行可能であることからAWSを選択した。

ただ、この顧客にはどうしても譲れない条件があった。AWS上でもオンプレミス環境と同様にFortiGate VMを冗長化したいというものだ。それも単一のデータセンターやAZ（アベイラビリティゾーン）内での冗長化ではなく、複数のAZをまたぐ「マルチAZ」で一段高い冗長性を確保する必要があった。この顧客は、親会社も含めたグループ全体の情報子会社として約80社のITリソースを運用監視する立場にあるため、出入り口が万一にも止まってしまうことは許されなかったためだ。

当初、「複数のAmazon VPCでFortiGate VMを稼働させて冗長化させれば済むだろう」と考えていた井上氏だったが、マルチAZまたぎが必須と聞いて思わず「えっ」となったそうだ。「異なるAZに分けて配置するのはいいとして、どのようにトラフィックを振り分けるかで頭を悩ませました」（井上氏）。

そこで助け船になったのがAWSの支援体制だった。「お客様とともに、『どの構成ならば要件を満たせるか』と相談しながらフィージビリティの確認を行いました。その中で、マルチAZ環境で自動的にトラ

フィックの振り分けを行う方法としてGateway Load Balancerの存在を知りました」（井上氏）
これが突破口になったものの、単純にGateway Load Balancerを 使うだけでは意図する切り替えができないことも判明した。さらにあれこれ尋ねながらAWSについての知見を増やしていったという。
「オンプレミスのネットワークはネットワーク機器主体で構成されてきました。これがAWSになるとサーバ主体となり、まるで逆の考え方になります。最初は驚きましたが、多数のインターフェイスを備えたサーバがデータを受け取り、処理して吐き出す……という処理がスタティックルートでつながっていくと考えると、すんなり入っていくことができました」（井上氏）
他のクラウドサービスとは異なり、AWSではアーキテクトが個々の案件に対してアドバイスを行う体制になっている点が特に心強かった。「クラウドは進化が非常に速く、どんどん追加される新機能を網羅できる人材はそう多くはありません。サービスの哲学を踏まえつつ最先端の情報を知っているアーキテクトを紹介していただけたため、現場では非常に助かりました」（井上氏）

AWSへの移行を機にVPNやプロキシ機能もFortiGate VMに統合

過去に類例のない案件だったが、IBCはフォーティネットやAWSの支援を得ながら、2022年7月から3ヶ月ほどかけ、インターネットに公開するWebサーバとVPN経由でのリモートアクセスという2つの部分に分けて設計を煮詰めていった。
続けて順次AWS上に環境を構築し、動作確認やクライアントPCに導入するFortiClientとの連携について検証を進めている。表示できないサイトが見つかり焦ったこともあったが、原因を突き詰めてみるとWebサイト側の作りにあることが判明し、Gateway Load Balancerを用いた「ヘアピンカーブ式」のアーキテクチャは問題なく動いている。
並行してFortiGateの設定も整理した。以前は、別のベンダーのSSL VPN製品とプロキシ製品を組み合わせていたが、AWSとFortiGate VMへの移行をきっかけに複数の機能を統合する方針を固めた。これを機に、約1000行に上っていたアクセスコントロールに関するポリシーやSSL VPNのグループの棚卸しを行い、重複しているルールやグループを整理した。
この際メリットとなったのが、FortiGate VMの設定がアプライアンス版のFortiGateとほぼ同様で、容易に行えたことだ。「見た目や使い勝手はほとんど変わらず、操作している限りでは、アプライアンス版かVM版か区別が付かないほどです」と井上氏は言う。以前のファイアウォールのルールをそのまま載せ替えられるかを懸念していたが、問題なく移行できた。
インテグレーションを担う立場としては、仮想環境の特長を生かして迅速に構築でき、スピード感を持って対応できたこともポイントだ。「物理的なアプライアンスを構築しようとすると、もろもろの手配を行った上で箱から出してセットアップし……とかなり大変ですが、画面操作だけでできてしまいました」（井上氏）。顧客の本番環境との違いに留意する必要はあるが、事前にIBC社内に検証環境を構築することで、スムーズな構築が可能になったという。
何よりクラウド環境に移行することで、本来の特徴であるスケーラビリティを大いに享受できている。特に「インターネットアクセス回線の帯域を気にしなくてすむ点が一番大きかったと思います」と井上氏は言う。現在この顧客では、2つの異なるAZでFortiGate VMを運用し、Gateway Load Balancerを用いた構成で運用している。NAT Gatewayは100Gbpsまで自動的に拡張するため、ボトルネックに悩まされることはなくなった。
「データセンターへ集約してしまうとゲートウェイがボトルネックになり、ユーザーから苦情があればそこを増やすしかありません。拠点ごとに端末を個別に管理する手間を省きつつ高速化できるという意味で、クラウドにFortiGateを持っていくのは非常に楽で素晴らしい選択肢だと強く感じました」（井上氏）
現在IBCは、新環境でセキュリティポリシーの追加を行う際の顧客向け運用手順の整備などを進めている。また将来的にはAmazon CloudWatchで監視を一元化し、アラートを受けて自動的に切り替えを行う仕組みをAWS Lambdaを活用して実現していく計画だ。

クラウドプロキシと同等以上の機能を安価に実現する新たな選択肢へ

IBCは今回の案件を通して、AZをまたいでの負荷分散も含めた、FortiGateのクラウド移行の経験則を多く積むことができたと実感している。これにより、クラウド利用拡

大に伴う帯域逼迫の問題を解決できる新たな選択肢が用意できた。

さらに今後は、クラウド上で運用するFortiGateのさまざまな機能を生かし、ファイアウォールやVPN、IDS/IPS、マルウェア対策といったさまざまなセキュリティ対策をIaaS上で実現するプライベートSASEという形で、いわゆるゼロトラスト環境やクラウドプロキシの代替策となる新たな提案が実現できると予感している。

今、さまざまなゼロトラストソリューションが登場しているが、顧客が期待するコストを一桁、二桁上回ることも少なくない。これに対しFortiGate VMをクラウド上に構築するケースでは、冗長化し、かつスケールアウトによって広帯域を利用してもコストはおおむね半分程度に抑えられる見込みだ。

「非常に安価に提案できるため、お客様にとってもハードルが下がると考えています。現に今、ゼロトラストを検討されていたいくつかのお客様に対して『クラウドにファイアウォールを持って行きませんか』とご提案を進めています」（井上氏）

プライベートSASEには、オンプレミスのファイアウォールと同じように容易に設定でき、かつきめ細かな制御が可能という利点もある。「クラウドプロキシは設定項目が少ないため導入しやすいと言われていますが、裏を返せばこれは細かな設定ができないことでもあります。これをFortiGate VMに置き換えることで、お客様のコントロール配下に置いた形でユーザー管理やアクセス元IPアドレスの制限といった細かな制御を、安価に提案できると考えています」（井上氏）

ゼロトラストのような新しいキーワードは魅力的だが、長年にわたって運用され、さまざまな事情を抱えるシステムからは一気に移行しにくいのも事実だ。「クラウド利用時の帯域の縛りをなくしたいが、運用負荷も気になる」「ゼロトラストセキュリティはコストパフォーマンスが心配だ」と考えるこうした企業にとって、FortiGate VMとマルチAZ化したクラウドの組み合わせは、魅力的な選択肢になり得るという。

FORTINET
フォーティネットジャパン合同会社

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

お問い合わせ

CS-i-IBC-2309-JP-R3