Volterra
Part of F5

一元的なセキュリティ設定や管理を実現

エッジからマルチクラウドまで、分散アプリケーションの丸ごとセキュアな運用方法

「クラウドファースト」や「分散アプリケーション」が当たり前となり、複数のクラウドやオンプレミス環境を使い分け、便利で価値の高いアプリケーションを実現できるようになった。ただし、セキュリティ対策の一元化や煩雑な管理が課題だ。

企業のアプリケーション利用の姿が大きく変わろうとしている。従来はオンプレミスやデータセンターを用いた中央集約型の構成で動作するアプリケーションを利用するパターンが主流だった。しかし、IoTデバイスや5Gの普及に伴って、データ駆動型のビジネスが拡大したこと、「Docker」「Containerd」のようなコンテナ技術、「Kubernetes」のようなコンテナオーケストレーションツールが登場したことにより、アプリケーションの分散化が進んでいる。

ユーザーデバイスと、アプリケーションとの間をつなぐ「エッジ」にアプリケーションが散らばる時代が到来する。これを複数のクラウドや既存環境と組み合わせて活用することで、より柔軟に拡張性のあるサービスを実現できる可能性が見えてきた。

このようにして自由度が上がるものの、その反面、分散したアプリケーションをどのように運用していくのかが、新たな課題として浮かび上がってきた。例えばどのサービスのどのAPIが通信しているのかを把握しにくい。クラウドごとに異なるWebアプリケーションファイアウォール（WAF）やアプリケーションゲートウェイを使っているため、ログのひも付けができず、アプリケーション同士の連携やつながりを把握することが難しくなる。

こうしたエッジからクラウド、あるいはクラウド同士などに分散するアプリケーションの通信を可視化し、ひも付けること、そして一貫したセキュリティを実現するためのソリューションをVolterraが提供している。

重要度が増すマルチクラウド環境と運用の課題

「クラウドファースト」を企業が進める動きには理由がある。クラウドはオンプレミス環境に比べコスト面で有利なことに加え、パフォーマンス（性能）や導入のスピード、耐障害性の向上などさまざまなメリットがあるからだ。加えて、必要なときに必要なだけ利用できる柔軟性や拡張性が、デジタル時代の企業の強みや競争力につながるとして注目されている。

クラウドの導入後、複数のクラウドを用途に従って使い分けるマルチクラウドへと進んでいく理由は幾つかある。企業活動の前提となるような重要なアプリケーションを単一のクラウドだけに配置するのは危険だという判断、そしてバックアップとしてクラウドを利用しBCP（事業継続計画）を実現したい判断などがある。

その他にも、1つのクランドベンダーにロックインすることを避け、拡張性や柔軟性を高めたいといった理由があるだろう。

オンプレミス環境ではコストや運用負荷といった課題はあったものの、全てが自社のコントロール下に置かれており、どのアプリケーションがどのようなネットワークやサービスに接続されて処理をしているのかを把握できていた。さらに、扱う情報の重要度に応じて適切なセキュリティレベルを一元的に適用することも難しくなかった。

だが、異なる事業者が提供するマルチクラウド環境、そしてオンプレミスと組み合わせたハイブリッドクラウド環境では、その前提が成り立たなくなる恐れがある。

典型的なマルチクラウド環境を考えてみよう。まず、本社オフィスと支社、データセンターを閉域網でつなぐ。これまで運用してきた本番環境のアプリケーションはオンプレミス環境で稼働させる。同時に新規アプリケーションの開発は、最新の技術を取り入れつつ、パブリッククラウドを利用して進めたいといったケースだ。

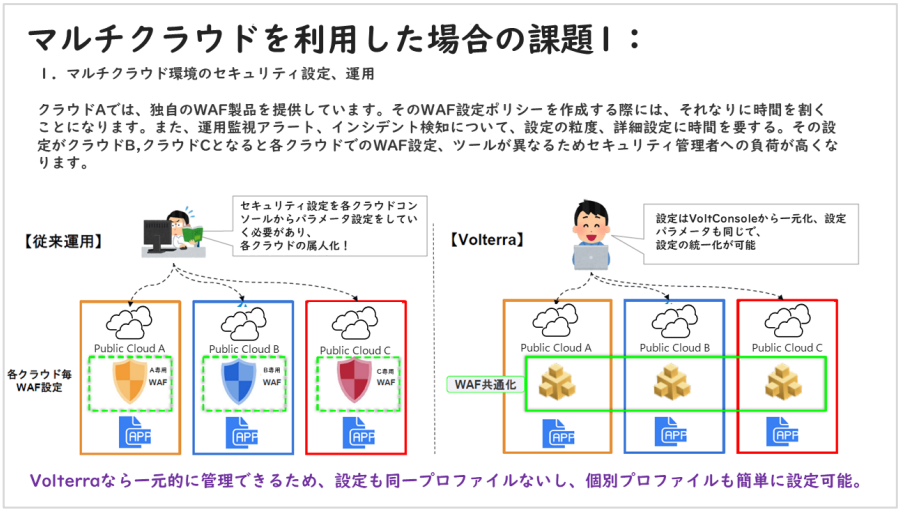
もう一つ身近な例は、ショッピングやスマート配車など、スマートフォンで日々利用するさまざまなアプリケーションだ。こうしたアプリケーションでは、全ての機能をモノリシックな1つのソフトウェアで提供することはほとんどない。位置情報を取得するGPSサービスや在庫管理システム、画面に表示される動画や画像を提供するCDN（Content Delivery Network）のキャッシュやストリーミングサービス、決済処理を担うオンプレミスの自社データセンターなど、複数のクラウドサービスやシステムが連携してはじめて実現に至る。

マルチクラウド環境やハイブリッドクラウド環境になってくると、複数のアプリケーション提供基盤にまたがって活用することになる。その中でいかに適切なセキュリティを実現し、最適な負荷分散を実現するのかが課題になってきている。

特に厄介なのは、どのようにして複数のクラウドやオンプレミスにまたがって統一されたセキュリティポリシーを適用し、セキュリティ水準を保つかだ。

もちろんクラウドサービス事業者はそれぞれ、シンプルなファイアウォール機能に始まり、より高度なWAFに至るまで、さまざまなセキュリティ機能を提供している。一つのクラウド内に閉じるのならば、十分運用できるようになっている。問題はそれが複数の環境や基盤にまたがる場合だ。

1つのアプリケーションの裏で多数の分散されたサービスが動いている例とその課題



クラウドごとに異なるWAF設定とVoltConsoleによるセキュリティ設定の一元化の例

企業としてのセキュリティポリシーはあっても、それを複数のクラウドの設定に落とし込むところが課題となる。大まかな機能は同じでも、クラウドごとに設定項目やパラメーターが異なるケースもあり、「A 社のクラウドではこれを設定すればよいが、同じことをするための設定は B 社のクラウドや C 社のクラウドだとどれに当たるのか分からない」といった事態が生じてしまう。

今のところ最も多いのは、担当者の能力や努力に頼り、各クラウドサービスの設定を理解してもらって設定することだ。だが、これでは負荷の増大や属人化は避けられない。

こうして設定を統一したとしても、マルチクラウド環境の全体像を把握するのが困難であることに変わりはない。アプリケーションやサービスが分散するにつれ、どれとどれが、どのようにつながっているか、把握や管理が難しくなっている。マルチクラウド環境になればなるほど、一元的に管理する方法が求められている。

一元的なセキュリティ設定や可視化を実現する「VoltMesh」

こうした背景から F5 Networks が買収した「Volterra」は、次のような手法でマルチクラウドにまつわるエンジニアの負荷削減を実現しようとしている。

ルーティングやロードバランサーといったネットワーク機能と、ファイアウォールや WAF などのセキュリティ機能を SaaS 形式で提供する「VoltMesh」と、それらの一元管理を行う「VoltConsole」の展開だ。

VoltMesh は企業向け IT 市場で活用が進む「Amazon Web Services」（AWS）、「Microsoft Azure」（Azure）、「Google Cloud Platform」（GCP）という 3 つのパブリッククラウドサービスに対応している。VoltConsole で WAF に関する設定を変更すれば、それが各パブリッククラウドの WAF 設定に反映される仕組みだ。パラメーターも含めて各パブリッククラウドの WAF 設定を共通化し、見える化を実現して一元管理できるため、運用の負荷を低減できるという。

VoltMesh と VoltConsole の組み合わせには、企業側の環境の変化や拡張に容易に対応できるという利点もある。

これまで、新規拠点を追加した場合、利用したいクラウドサービスごとに接続設定を施し、必要に応じて VPN トンネルを張ったり、ネットワーク機器やセキュリティ機器を個別に設定したりする必要があった。

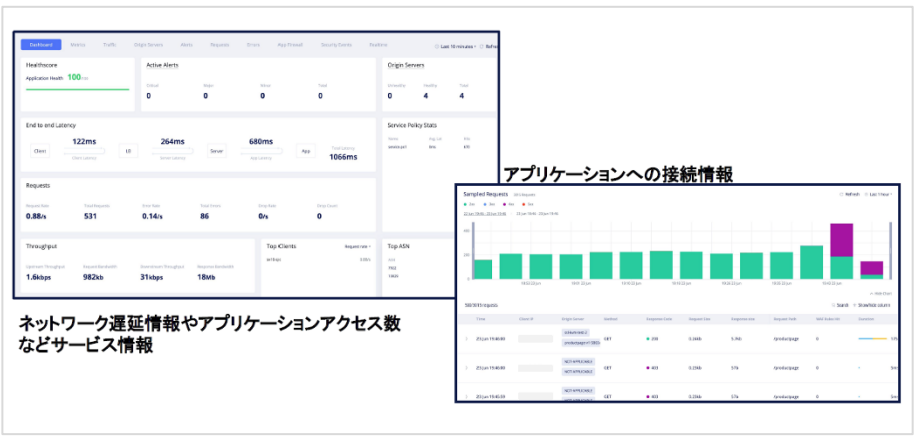
こうした機器の多くにはコマンドラインインタフェース（CLI）が採用されており、ログインや設定、反映を担当者が手作業で対応する必要があった。加えて、物理的なケーブル配線作業の際にミスが生じる恐れもある。さらに、アプリケーションの負荷分散や WAF 設定も別々に進めなければならず、煩雑だった。設定以前に、専用アプライアンスの調達や配送、設置といった作業にもかなりの時間がかかることが常だ。

これに対し VoltMesh は SaaS ベースで提供されるため、何らかの仮想基盤があればすぐに運用できる形だ。しかもゼロタッチプロビジョニングで導入でき、必要な設定は VoltConsole から「降ってくる」というイメージだ。

VPN トンネルの設定から負荷分散、ファイアウォールや WAF に至るまで自動的に設定が反映されるため、わざわざエンジニアを現地に派遣しなくても迅速に、しかも一元的な設定を適用できる。この結果、支社や拠点を開いたらすぐに、社員の PC から必要なパブリッククラウドのリソースを安全に、安定的に利用できるようになり、業務をすぐにスタートできるというわけだ。

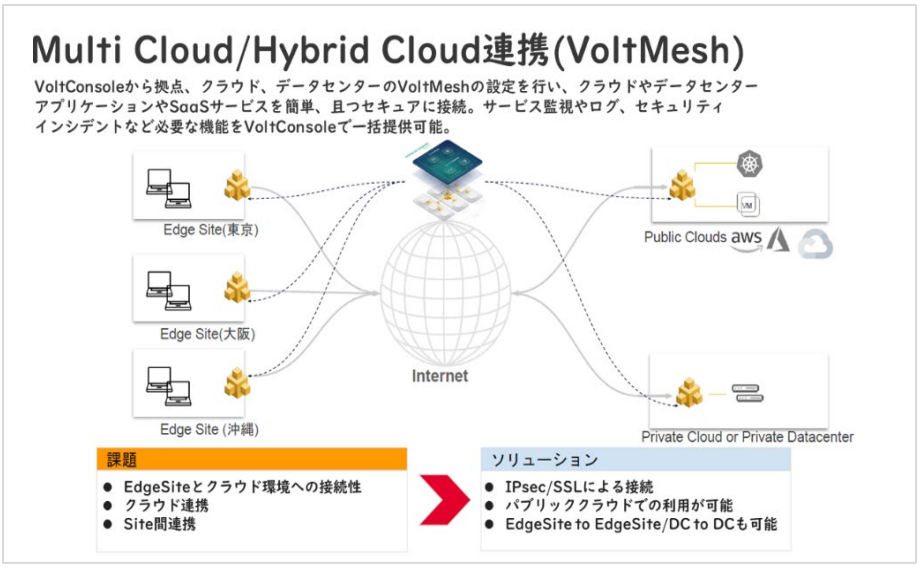
VoltConsole はもう一つの課題だった「可視化」も実現できる。現状では AWS、Azure、GCP それぞれで管理コンソールに入ってログを管理するか、別途解析用サーバを構築してログを転送し、集約、解析する手間がかかっていたが、VoltConsole ではそれらを一元的に見ることができる。どの IP アドレスからどういったところにアクセスしているかといったレイヤー3～7 の情報に加え、アプリケーションに対する API リクエストまで可視化し、把握できるという。

ネットワーク担当者や SRE（Site Reliability Engineering）担当者に有用な管理機能も備えている。リソースの死活監視や ping によるネットワークレイヤーの疎通確



VoltConsoleによる可視化画面

認だけではなく、アプリケーションのレスポンスや遅延までを確認できるようになっており、何か問題があったとき、足回りのインターネット回線が遅いのか、それともアプリケーション側に問題があるのかといった事柄を一元的に確認でき、問題を迅速に切り分けることができる。



*Volterra*のプラットフォームでエッジからクラウド、マルチクラウド間もセキュアに接続

マルチクラウドのみならずエッジ環境も含めた1つの基盤を実現

マルチクラウドからさらにエッジ環境へと企業 IT が拡大していったとき、エッジ環境も含めた基盤が必要になる。

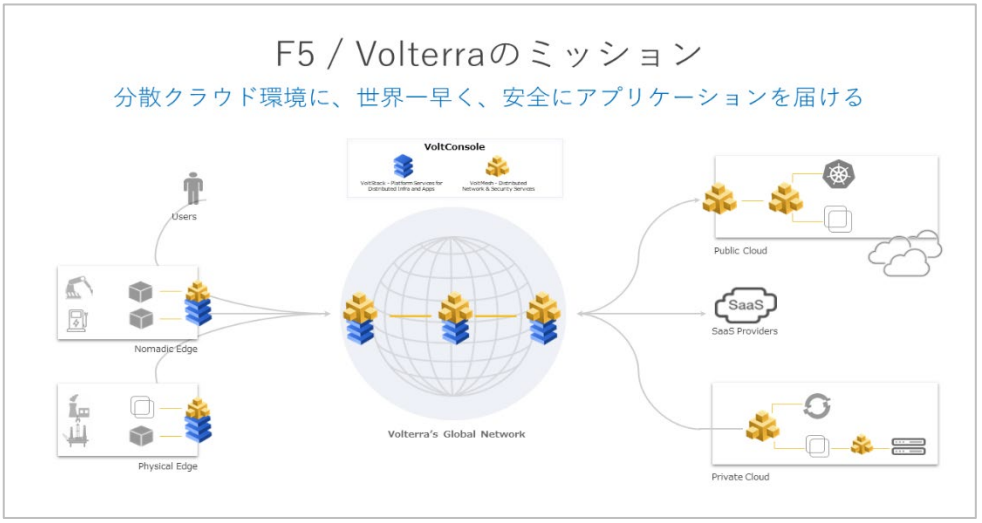
Volterra はカスタマーエッジへのアプリケーション分散を見据えたソリューションであることをうたっている。具体的にはグローバルに展開するネットワーク基盤「Volterra Global Network」を持っており、前述の 3 つのコンポーネントとグローバルネットワークで、エッジからクラウド、あるいはクラウド同士、オンプレミスからエッジなど、どのような接続形態も可能にすることを目標にしている。

ヨーロッパのある大手金融機関では、マルチクラウド環境の効率的な運用のために Volterra を採用した。VoltMesh による各種設定の一元化と可視化を実現するだけでなく、エッジ側に Kubernetes 環境を実現する「VoltStack」もあり、これはアプリケーションの分散化も図るという先進的な取り組みだ。

例えば IP カメラを導入したならば、収集したデータの一次解析までをローカル側に導入した VoltStack 上のアプリケーションで進め、詳細な解析は連携先のパブリッククラウドにあるアプリケーションに任せる仕組みなどが実現できるという。

さらに VoltMesh を組み合わせることで、従来のオンプレミスであろうと、VoltStack を導入したエッジであろうと、あるいはパブリッククラウドや Kubernetes を利用したコンテナ環境であろうと、簡単に、同一水準のセキュリティレベルで接続し、1 つの基盤として活用できるようになるだろう。

F5 ネットワークスジャパンによれば、今後 10 年間を見据えても、マルチクラウドやハイブリッドクラウドは当たり前になるという。クラウド時代に、「管理が煩雑だから」「セキュリティ設定が面倒だ」といった理由でその歩みがスローダウンしては本末転倒だ。VoltMesh はそうした課題を解消し、マルチクラウド、ハイブリッドクラウド環境の活用を加速させる助けとなる。



Volterraはエッジからクラウド、マルチクラウドからハイブリッド環境など分散クラウド環境をセキュアに接続

● 製品や F5 に関するお問い合わせは、以下の URL のお問い合わせフォームよりご連絡ください。
https://www.f5.com/ja_jp/ContactFormJP