Case Study

QUALICA クオリカ株式会社

WE MAKE APPS GO FASTER. SMARTER. SAFER.

WAFによる脆弱性対策の集中化とアプリケーション機能のマイクロサービス化で、SaaSデリバリスピードの向上を目指す

製造業や流通・サービス業に向け、多岐にわたるSaaSビジネスを展開するクオリカ株式会社。ここではそのデリバリスピードを高めるため、アプリケーションのマイクロサービス※1化が進められている。これと並行して、セキュリティ確保に開発リソースが割かれてしまうことを避けるため、WAFによる脆弱性対応の集中化も実施。ここにBIG-IP ASMを採用すると共に、F5コンサルティングサービスも活用することで、アプリケーションの安全性強化に向けた取り組みを進めている。

※1 マイクロサービス：アプリケーションを複数のサービスの集合体として構成し、これらのサービスをRESTful Web APIのようなシンプルかつ軽量な手段で連携する手法。小規模なサービス群を疎結合で組み合わせることで、従来の「モノリシック（一枚岩）型」のアプリケーションに比べ、変化に対応しやすくなる。

「安全性の担保はサービス提供者の責務ですが、デリバリスピードを向上させるには、開発者の負担を軽減できる仕組みが必要です」

クオリカ株式会社 プラットフォームサービスセンター 副センター長 坪口 智泰 氏

背景

コマツのソフトウェア開発子会社として、1982年にスタートしたクオリカ株式会社。当初は製造業向けソフトウェアの開発を主業務にしていたが、1987年には流通業向けのシステム提供も開始、2000年にTIS傘下に入ってからはさらにそのビジネスを拡大してきた。現在は、外食産業向け営業支援システム「TastyQube」や小売業向け店舗・本部営業支援システム「SpecialtyQube」、クラウド対応生産管理システム「ATOMS QUBE」、ドキュメントソリューション「CSS-Net」等、多岐にわたるSaaSを展開。その一方で、IaaSサービス「Qcloud」やDaaSサービス「Thin Office VDI」といった、IT基盤サービスも提供している。

ビジネス上の課題

これらのSaaS提供で近年大きな課題になっているのが、デリバリスピードの向上だ。市場の変化や顧客の新たなニーズに対したビジネスロジックを、迅速に提供することが求められているのである。「そのため現在アプリケーションの開発・展開方法を刷新している最中です」と語るのは、クオリカ プラットフォームサービスセンター副センター長の坪口 智泰氏。アプリケーションの各種機能をマイクロサービス化し、これらをAPIで疎結合する形態へとシフトすると同時に、アジャイル開発も取り入れつつあると説明する。

その一方で最近では、アプリケーションの脆弱性を狙った攻撃も急増していると指摘。アプリケーションの脆弱性解消が大きな負担になっており、これが開発スピードを阻害する要因になっていると言う。「安全性の担保はサービス提供者の責務ですが、これをアプリケーション開発者任せにしてしまうと、ビジネスロジックに注力しにくくなります。デリバリスピードを向上させるには、開発者の負担を軽減できるセキュリティ確保の仕組みも必要です」。

Overview

業種

エンタープライズ

課題

- SaaSのデリバリスピードの向上
- アプリケーションの脆弱性を狙った攻撃への対応
- 開発者の負担を軽減できるセキュリティ確保の仕組みが必要に

ソリューション

- BIG-IP Application Security Manager (ASM)

メリット

- 脆弱性に特化したトレースで適切な対策が容易に
- 1台のASMで複数サービスへの対応が可能
- コンサルティングサービスを活用したノウハウ蓄積が、新規ビジネスの開拓にも貢献

Customer Profile

クオリカ株式会社

コマツの情報システム子会社として1982年に創業。2000年にTISの傘下に入り、2008年に業界トップクラスのITホールディングスグループ（現TISインテックグループ）の一員となる。製造業や流通・サービス業に向け、業務用システム開発やパッケージソフト開発、システム運用、情報端末製造等の幅広い事業を展開している。

ソリューション

そこでクオリカは2014年に、アプリケーション保護を目的にしたWAF（Web Application Firewall）の導入検討に着手。複数ベンダー製品を比較検討した結果、2016年4月にBIG-IP ASM（Application Security Manager）の導入を決定する。ここで評価されたポイントは「マルチテナントに対応できることと、他社製品に比べて信頼性や機能性が高いこと」だと坪口氏は言う。

ASMの導入に合わせ、アプリケーションのマイクロサービス化を視野に入れた、大きく4つの要素（ステージ）で構成されたシステムの構築にも着手している。まずインターネットに最も近いステージには、ファイアウォールとロードバランサを配置。これらは、リプレースに時間や労力をかけたくないという理由から、既存製品をそのまま利用している。2番目のステージには、冗長化されたAPIゲートウェイを配置。ここでクライアントからのリクエストを受け、その処理に必要なマイクロサービスのAPIへと変換する。3番目のステージにはASMを配置。ここでマイクロサービスに対する通信内容を分析し、セキュリティ上問題のあるトラフィックの検知・防御を行う。そして4番目のステージに配置されたアプリケーションサーバ上のマイクロサービスへと、リクエストを渡すのである。

なお今回のASM導入では、F5コンサルティングサービスも活用している。その理由について「WAFを導入しているにもかかわらず適切な設定ができていないため、その効果を引き出せていない先行事例が少なくありません。自社で安全にWAF導入/運用を進めるには、F5コンサルタントのリードが必要だと判断しました」と坪口氏は語る。

「ASMはアプリケーションの脆弱性に特化したトレースを行うため、適切な対策の立案・実施が行いやすくなります」

クオリカ株式会社 プラットフォームサービスセンター
副センター長 坪口 智泰 氏

メリット

■脆弱性に特化したトレースで適切な対策が容易に

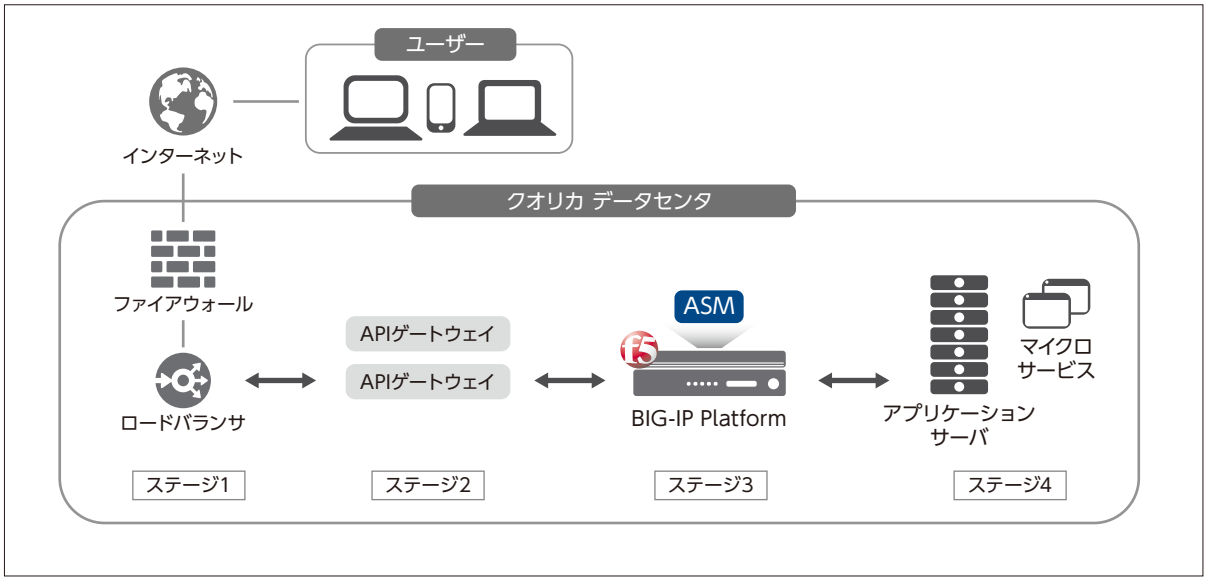
2017年1月には「TastyQube」に対するASMのステージング（ポリシーテスト）機能の運用を開始。これによって、アプリケーション脆弱性への攻撃がどのように行われているのか、これまで以上にはっきりと分かるようになった。「トラフィックをトレースする製品は他にもありますが、見るべきポイントが絞り込まれていないため、そこから有益な情報を抽出するのは簡単ではありません。これに対してASMは、アプリケーションの脆弱性に特化したトレースを行うため、適切な対策の立案・実施が行いやすくなります。2017年3月からはこれらの情報を活用し、攻撃防御の運用も開始する予定です」（坪口氏）。

■1台のASMで複数サービスへの対応が可能

F5製品はマルチテナントに対応しているため、1台のBIG-IPで複数のサービスを保護できることも大きなメリットだ。「現在の適用対象は『TastyQube』のみですが、すでに『ATOMS QUBE』や『CSS-Net』、『SpecialtyQube』への適用が決まっており、最終的にはクオリカが提供する全てのSaaSに適用していく計画です」と坪口氏。クオリカのSaaSは全てWAFで守られているという状況にすることで、攻撃者を牽制すると共に、顧客にも安全性を訴求していきたいと言う。

■新規ビジネスの開拓にも貢献

F5コンサルティングサービスの活用で、WAFを適切に運用するためのノウハウも蓄積されつつある。このノウハウをベースに、IaaSやホスティングでWAFサービスを提供するといった取り組みも進められている。「今後も継続的にコンサルティングを利用し、運用ポリシーの見直し等をお手伝いしていただきたいと考えています」（坪口氏）。



F5ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210　FAX 03-5114-3201

西日本支社
〒530-0012 大阪市北区芝田1-1-4 阪急ターミナルビル16階
TEL 06-7222-3731　FAX 06-7222-3838

http://f5.com/jp

2017年3月