

顧客向けサイトの保護をクラウドWAFからBIG-IP へと移行、TCOの削減とより柔軟で安心できる運用 が可能に

三重県、滋賀県、和歌山県を対象に、ケーブルテレビやインターネット接続サービス、ケーブルプラス電話、ケーブルスマホ、MVNO等のサービスを展開する株式会社ZTV（以下、ZTV）。ここでは顧客向けサービスを提供するサイトの保護を、クラウドWAFからBIG-IP ASMへと移行している。その最大の目的はTCOの削減だ。サービスの拡大に伴い、クラウドWAFの料金負担が大きくなっていったのである。またこの移行によって、よりきめ細かい運用やサーバ証明書の集約も可能になった。今後はiRulesを活用した動的な接続制御や、DDoS対策をBIG-IPで行うことも検討されている。



「顧客向けサービスを保護するためクラウドWAFを利用していましたが、サービス拡大に伴い利用料金の増大が懸念事項となっていました。そこでオンプレミス型のWAF導入を検討、WAF機能が充実しており性能面での安定性も高いBIG-IPを導入しました」

株式会社ZTV 通信技術部 通信課
課長代理 木本 大輔 氏

背景

ZTVは、三重県、滋賀県、和歌山県をサービス提供エリアとするケーブルテレビ局である。

1990年に津ケーブルネットワーク株式会社として設立、1992年に津ケーブルテレビ株式会社として商号を変更し、1994年にケーブルテレビ局を開局。2000年に株式会社ゼットティヴィ、2002年に株式会社ZTVへと商号変更を行った。その後、滋賀ケーブルネットワーク、近江八幡ケーブルネットワーク、アイティービーを吸収合併しサービスエリアを拡大。これと並行してインターネット接続サービス等、サービスの拡充も推進してきた。

2008年にはインターネットデータセンターを完成させ、ケーブルプラス電話サービス、VODサービス、ケーブルスマホサービス等もスタート。また携帯キャリア基地局向けの接続サービス等、法人向け事業も積極的に展開している。最近ではFTTH化も急ピッチで進めており、トラフィック量はこの1年で約2倍になっている。

これらの顧客向けサービスを保護するため、2013年にはクラウドWAFの利用を開始。サービスの拡大に伴い、保護対象となるサーバの数も増えていったのである。

ビジネス上の課題

ここで問題となったのが、クラウドWAFのコストである。保護対象となるサーバ数が増えれば、当然ながらクラウドWAFの利用料金も増大する。また当時使用していたサービスは、保護対象となるサーバ毎にクラウドWAF側にもサーバ証明書を用意する必要があり、その取得コストや運用コストもかさむようになっていた。

「運用面でも問題を抱えていました」と振り返るのは、ZTV 通信技術部 通信課 課長代理の木本 大輔氏。レポート機能もなく、ログも大まかな内容しか記録されていなかったため、具体的にどのような攻撃を受け、それをどのようにブロックしたのかが、よくわからなかったという。「ログを見ると受けた攻撃のリストは出てくるのですが、細かい記述がないため、本当にクラウドWAFで保護されているのか実感もできませんでした」。

そこでZTVは2017年1月に、オンプレミス型WAFの導入検討に着手。ちょうどこの頃、ファイアウォールの更新時期も近づいていたため、ファイアウォールとWAFを統合することも視野に入れた検討が進められた。複数のWAF製品を比較した結果、2017年8月にBIG-IPの採用を決定。2017年11月に導入するのである。

Overview

業種

サービスプロバイダ

課題

- ・顧客向けサービスを提供するサイトを守るためクラウドWAFを利用していたが、サービス拡大に伴い利用料金が大きな負担になっていった。
- ・利用しているクラウドWAFにはレポート機能がなく、ログの内容も十分ではなかった。また柔軟な設定も難しかった。

ソリューション

- ・BIG-IP Application Security Manager (ASM)
- ・BIG-IP Advanced Firewall Manager (AFM)
- ・BIG-IP Local Traffic Manager (LTM)

メリット

- ・豊富なシグネチャときめ細かいログの内容によって、柔軟な運用が可能になった。
- ・WAF機能をオンプレミス化することで、TCOの削減が可能になった。
- ・これまでサーバ数×2が必要だったサーバ証明書を1つに統合でき、これもTCO削減に大きな貢献を果たしている。

Customer Profile

株式会社ZTV

1990年に津ケーブルネットワーク株式会社として設立、1994年に開局したケーブルテレビ局。現在は三重県、滋賀県、和歌山県をサービス提供エリアとし、ケーブルテレビやインターネット接続サービス、ケーブルプラス電話、ケーブルスマホ等のサービスを展開している。またキャリア基地局向けの接続サービス等、法人向け事業も手がけており、最近ではFTTH化も急ピッチで進めている。

ソリューション

BIG-IPを採用した理由について木本氏は「他社ファイアウォール製品のWAF機能はシンプルなものでしたが、BIG-IPは機能が充実しており、性能面でも安定性が高いからです」と説明する。F5製品を導入するのは今回が初めてだったが、これなら十分な保護が可能になると感じたという。

BIG-IP上で利用している機能は、ASM、AFM、LTMの3種類。まずASMのWAF機能でアプリケーション攻撃をブロックした上で、外部からのトラフィックをAFMのファイアウォール機能に通し、LTMで各サーバに振り分けている。

「BIG-IPのWAF機能はシグネチャが豊富で柔軟な設定を行いやすく、ログにもきめ細かい記録が残るため、安心して運用できます。またBIG-IPを導入したことでサーバ証明書の統合も可能になり、結果的にはこれもコスト削減につながっています」



株式会社ZTV
通信技術部 通信課
課長代理
木本 大輔 氏

メリット

■クラウドWAFに比べてきめ細かい運用が可能

クラウドWAFからBIG-IPへと移行した結果、これまで以上にきめ細かい運用が可能になった。

「BIG-IPのWAF機能は、利用できるシグネチャが豊富で柔軟な設定を行いやすく、ログにも『なぜ攻撃だと認識したのか』『それに対してどのような処理を行ったのか』が細かく記録されています。そのためシグネチャを適用したときの効果もはっきりとわかり、安心して運用できます。また日常的にログを見ることで、実際にどのような攻撃を受けているのかも明確に把握でき、対策立案や社内でのセキュリティ啓蒙活動も行いやすくなりました」(木本氏)。

■サーバ証明書を集約しTCOも大幅に削減

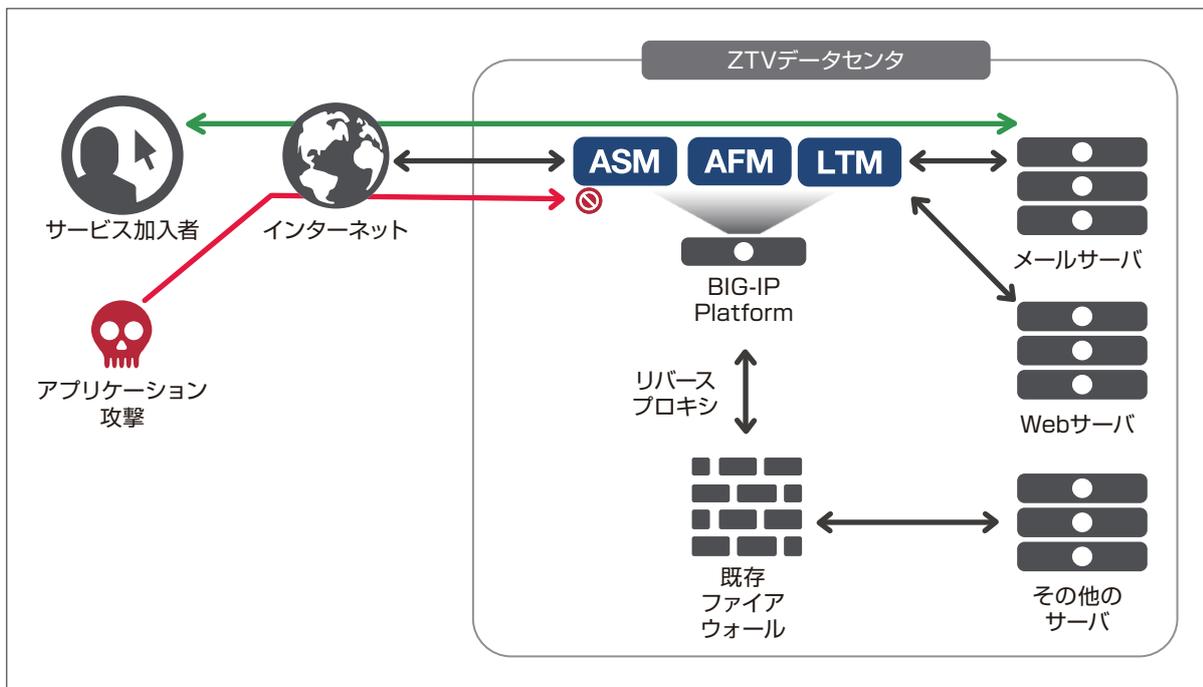
WAFをクラウドサービスからオンプレミスへと移行したことで、利用料金の増大という問題も解消可能になった。これに加えサーバ証明書の統合によって、サーバ証明書の取得・管理コストも大幅に削減されている。以前はクラウド側とサーバ側を合わせ、保護対象のサーバ数×2の証明書が必要だったが、現在では1つのワイルドカード証明書をBIG-IPに格納するだけで、すべてのサーバをカバーできるようになったのだ。導入検討時

には証明書の統合までは考えていなかったが、結果的にはこれもTCO削減に大きな貢献を果たしているという。

■iRulesやIPインテリジェンスの活用も検討

iRulesによって動的な接続制御を行うことや、IPインテリジェンスの活用も検討されている。これらを組み合わせた防御の一例として木本氏が挙げるのが、SMTPサーバを踏み台にしたメール攻撃への対処だ。この種の攻撃で使われるIPアドレスからのアクセスをIPインテリジェンスでブロックすると共に、一定時間内に大量のメールを送信してきたIPアドレスからのアクセスをiRulesで一時的にブロックする、といった使い方を考えているという。

また現在はDDoS対策のアプライアンスがBIG-IPとは別に運用されているが、将来はこれもBIG-IPに集約し、さらなるコストダウンにつなげることも検討可能になっていると語る。「FTTH化が進むことでトラフィックはさらに増大していくはず。これからもBIG-IPには、高いパフォーマンスと安定性を発揮してもらいたいと考えています」。



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 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

お問い合わせ先: <https://f5.com/jp/fc/>