Case Study

株式会社ケイ・オプティコム

WE MAKE APPS GO FASTER. SMARTER. SAFER.

大規模なDDoS攻撃の経験からフィルタリング機能を実装、サービスへの影響を回避し顧客からの信頼を回復

「光をもっと、あなたのそばに。」をコーポレートスローガンに掲げ、光サービス「eo光」をはじめとする幅広い通信事業を展開する株式会社ケイ・オプティコム（以下、ケイ・オプティコム）。ここではDNSサーバへの大規模なDDoSを受け一時的にDNSの応答が低下した経験から、2014年以降から数年をかけてネットワーク構成の大幅な見直しが行われた。その際に導入されたのがBIG-IP AFM。DDoS攻撃に対応したフィルタリングを、性能劣化なく実行できる点が高く評価された。現在でも小規模なDDoS攻撃を継続的に受けているが、サービスへの影響を完全に回避し、顧客からの信頼も回復されつつある。

「決め手になったのは、AFMを利用した時の圧倒的なパフォーマンスです。iRulesのスクリプト追加でゼロデイ攻撃に対応しやすいことも評価しました」。

株式会社ケイ・オプティコム
技術本部 計画開発グループ ネットワーク技術開発チーム 櫻井 俊和 氏

背景

1988年に関西通信設備サービス株式会社として光ファイバ賃貸事業を開始し、その後複数の企業合併を経て事業を拡大してきたケイ·オプティコム。現在では関西圏で展開する個人向け光サービス「eo光」や、全国展開する格安スマホサービス「mineo」、法人向けの各種通信サービス等、通信を主体とする幅広い事業を手がけている。

特に「eo光」は近畿2府4県を中心に高いシェアを持ち、160万以上の光回線を収容。光ファイバを使ったインターネット接続や、光電話サービス、ケーブルテレビサービス等を提供しており、最近では「eo光」とあわせて利用することで電気料金が安くなる「eo電気」といった事業も展開している。

そのネットワーク構成は、各地域のローカルPOPからのアクセスを2拠点のコアPOPに集約、そこからインターネットへと接続するというもの。各コアPOPにはメールサーバやWebサーバ、DNSサーバ等が設置されている。

ビジネス上の課題

この「eo光」のネットワークにBIG-IPを導入するきっかけになったのは、2014年5月から7月にかけて大規模なDDoS攻撃を受けたことだった。

「まず2014年5月に、インターネットからDNSに大量クエリが送られるDDoS攻撃と、加入者CPEのオープン リゾルバを踏み台にしたリフレクション攻撃が、同時に発生しました」と振り返るのは、技術本部 計画開発グループ ネットワーク技術開発チームの櫻井 俊和氏。この時、DNSサーバの前段に配置したロードバランサ（他社製品）のリソースが枯渇し大量のパケットがドロップされたため、DNSサーバのログ分析では何が起きているのかわからなかったという。

さらに2014年6月にも、網内Bot端末からDNSへの水責め攻撃と、加入者CPEのオープンリゾルバを踏み台にしたリフレクション攻撃が発生。短期間のうちに、2度にわたる大規模攻撃を受けることになったのだ。

いずれのケースでも数時間以内にDNSサーバを復旧させているが、このままの状態では迅速な原因切り分けが困難だと判断。ネットワーク構成を大幅に見直すことになったのである。

Overview

業種

サービスプロバイダ（通信事業）

課題

- DDoS攻撃を防御するためのフィルタリング機能の実装
- フィルタリング実行時のパフォーマンス維持
- ゼロデイ攻撃にも対応できる柔軟性の確保

ソリューション

- BIG-IP Advanced Firewall Manager（AFM）
- BIG-IP Local Traffic Manager（LTM）

メリット

- AFMのフィルタリングでパフォーマンスを低下させずにDDoS攻撃の影響を回避
- iRulesのスクリプト追加によってゼロデイ攻撃にも迅速に対処可能
- BIG-IPのREST APIを活用することでDNSサーバのメンテナンス作業自動化も実現可能に

Customer Profile

株式会社ケイ・オプティコム

1988年4月に関西通信設備サービス株式会社として設立。2000年6月に現在の社名となった。その後、複数の企業合併を経て事業を拡大。現在では「光をもっと、あなたのそばに。」をコーポレートスローガンに掲げ、関西圏で展開する個人向けFTTHサービス「eo光」や全国展開する格安スマホサービス「mineo」、法人向けの各種通信サービス等、通信を主体とする幅広い事業を手がけている。

ソリューション

そこでまずDDoS攻撃防御に向けたネットワーク要件の明確化に着手。コアPOPを大容量化するためのリソース見直し、クエリタイプ別のフィルタリング機能の実装、フィルタリング実行時のパフォーマンス維持、ゼロデイ攻撃にも対応しうる柔軟性等を掲げ、ロードバランサの製品選定を進めていった。その後、2製品に絞ったパフォーマンス テストを実施した上で、BIG-IPの採用を決定する。

「決め手になったのは、AFMを利用した時の圧倒的なパフォーマンスです」と櫻井氏。ソースIPベースの流量制限、クエリタイプを判別した上でのフィルタリング（秒間クエリ数が一定レベルを超えた時にパケットをドロップするなど）といった動作を、AFMならほとんど性能劣化なく実行できるという。「フィルタリングの有無でパフォーマンスが大きく変化しないため、キャパシティ プランニングも容易になります」。

またiRulesを使用することで、フィルタリングのルールが追加しやすいことも高く評価。これならゼロデイ攻撃も、ロードバランサで食い止めることが可能になると語る。

機器更改のタイミングに合せ、2016年4月にBIG-IPを導入。AFMによるDDoS攻撃防御の運用を開始している。

「現在も小規模な攻撃を毎週のように受けていますが、すべてAFMで防御しています。攻撃対応のためのログ分析も不要になり、運用負担も軽減しました」。

株式会社ケイ・オプティコム
技術本部 計画開発グループ ネットワーク技術開発チーム
櫻井 俊和 氏

メリット

■DDoS攻撃の影響がなくなり顧客からの信頼も回復

BIG-IP導入の最大のメリットは、DDoS攻撃の影響を受けなくなったことである。現在も小規模な攻撃を毎週のように受けているが、これらはすべてAFMで防御できており、サービスへの影響はまったく出ていない。顧客からの信頼も回復されつつあるという。

「すでに1年以上問題なく運用できているため、DDoS攻撃への不安もなくなりました」と櫻井氏。攻撃対応のためのログ分析も不要になり、運用負担も軽減したという。

■ゼロデイ攻撃への迅速な対応も可能

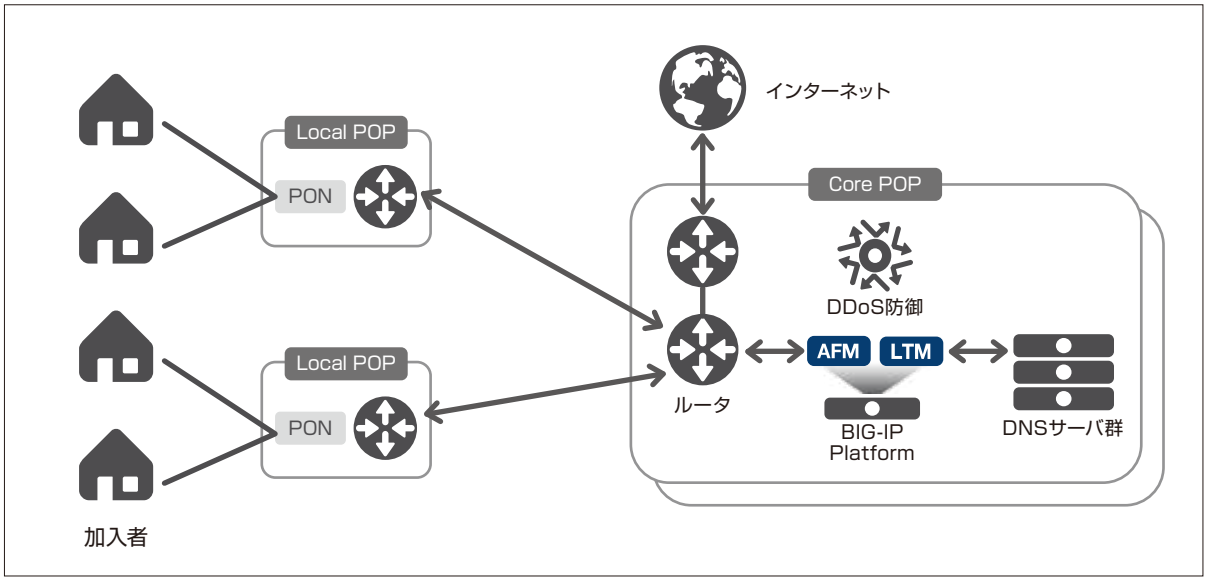
ゼロデイ攻撃に対する不安も解消されている。iRulesでスクリプトを作成・実装することで、対策内容を追加できるからだ。

「F5はゼロデイ攻撃が発見された時、2～3日後には対応するiRulesスクリプトを、F5のコミュニティサイトであるDev Centralにリリースしています。これを自社ネットワークに合せてカスタマイズして実装すればいいため、スクリプトの追加も容易です。まずBIG-IPで対応を行い、その後DNSサーバのパッチを適用すればいいので、ゼロデイ攻撃発生時にも慌てずに対処できます」。

■今後はDNSサーバのメンテナンス自動化も

今後はDNSサーバのメンテナンスに必要な作業を、自動化していくことも視野に入っている。Ansibleのような構成管理ツールからAPI経由でBIG-IPを操作することで、メンテナンスの際に必要なDNSサーバの切り離しと再接続を実行しようというのだ。

「BIG-IPには豊富なREST APIが用意されており、この点でもF5はマーケットリーダーであると感じています。すでにDevCentralの技術情報を参考にしながら動作確認を進めており、2017年度中にはサービス環境に実装していき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

お問合わせ先：https://f5.com/jp/fc/