Case Study

大学共同利用機関法人
情報・システム研究機構 国立情報学研究所

WE MAKE APPS GO FASTER. SMARTER. SAFER.

サービスをマルチクラウドで安全に提供するため クラウドのセキュリティ機能に依存しない アプリケーション・セキュリティゲートウェイを構築

「研究」と「事業」を活動の両輪とし、事業面では日本全国の大学や研究機関等の学術情報基盤であるSINET5に加え、学術情報ナビゲータ『CiNii』や目録所在情報サービス『NACSIS-CAT/ILL』、共用リポジトリ『JAIRO Cloud』等の各種サービスを提供している国立情報学研究所（NII）。ここではこれらのサービスをマルチクラウド化するための布石として、特定のクラウド事業者に依存することなく高度なセキュリティを一元的に実現する、アプリケーション・セキュリティゲートウェイを、IP Anycast構成で実現している。ここで重要な役割を果たしているのが、異なるデータセンタに導入された4台のBIG-IPだ。統合的な運用を視野にBIG-IQも導入されており、これらのBIG-IPの集中管理も実施。今後の多様なコンテンツサービスの実現に向けた活用も検討している。

「内製で得た知見をもとに、同等以上の機能を持ちかつ実績のある製品を採用したことで、マルチクラウドに展開したサービスを保護可能な、十分に信頼できるアプリケーション・セキュリティゲートウェイを実現できました」

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 学術基盤推進部 学術基盤課
特任技術専門員　三浦 竜哉 氏

サービス提供上の課題

日本全国の学術情報基盤として、重要な役割を担っているSINET。全国で800以上の大学・研究機関等で、300万人以上の研究者や学生等がこれを活用している。2016年4月にはSINET5の運用がスタート。全都道府県を100Gbpsの超高速ネットワークでつなぎ、欧州との直通回線や米国西海岸との100Gbps接続も実現した。このSINETの構築・運用を行っているのが、大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（NII）だ。NIIではSINET5への接続サービスに加え、学術情報ナビゲータ『CiNii』や目録所在情報サービス『NACSIS-CAT/ILL』、共用リポジトリ『JAIRO Cloud』等、様々なサービスをSINET上で提供。これらも研究や教育を支える基盤として、重要な役割を果たしている。

しかし「これまでのサービス提供システムにはいくつかの課題がありました」と語るのは、NII特任技術専門員の三浦 竜哉氏。これらのサービスはNII所管施設内のプライベートクラウドで運用されているが、年1回行われる法定点検時の全館停電によって1 ～ 2日サービスが停止する、災害対策（DR）が十分ではない、システム運用にコストがかかる、といった問題を抱えていたのである。NIIはこれらの問題を解決するため、2014年よりクラウド化の検討に着手、一部のシステムを先行で2014年11月にクラウドへ移行した。しかしここでも複数の課題が浮上したと言う。

「クラウドを採用した場合には、その時々の調達の結果クラウド事業者が変更されることがあり、提供されるセキュリティの機能や質も変わってしまう可能性があります。またクラウド活用でDRを実現したとしても、DNSで接続先を切り替えるのであればDNSの浸透期間によって、切り替え前後でシステム間に不整合が発生することも危惧されます。さらにJavaのDNS永続キャッシュ問題もあり、適切な対応を行っていないクライアントソフトを使用しているユーザのサポートにも工数がかかってしまいます」（三浦氏）。

これらに加え、近年増加傾向にあるDDoS対策も難しいと指摘する。このクラウド化構想は、複数のクラウドサービスとデータセンタの利用を前提としていたが、それぞれの環境でDDoS対策を行うだけのリソースを確保しようとすると、膨大なコストがかかることが予測されたのだ。

Overview

業種

研究機関

課題

- NII所管施設内で各種サービスを提供しているが、大震災時の計画停電等によるサービス停止の回避や運用コスト削減のため、これらをクラウド化することになった。
- クラウドを採用した場合、その時々の調達の結果でクラウド事業者が変更され、セキュリティ機能や質も変わる可能性がある。クラウド事業者に依存しないセキュリティを確保する必要がある。
- マルチクラウドでDRを実現した場合、DNS浸透期間（プロパゲーション期間）によって不整合が生じる危険性がある。
- これらの課題を解決するために、クラウド等システム基盤からネットワークトラフィック制御とセキュリティ機能を切り離し独立させた、全サービスで共通に使えるアプリケーション・セキュリティゲートウェイを構築することになった。

ソリューション

- BIG-IP Local Traffic Manager（LTM）
- BIG-IP DNS
- BIG-IP Application Security Manager（ASM）
- Advanced Routing Module
- BIG-IQ

メリット

- BIG-IP DNS と Advanced Routing Module の機能によってIP Anycast構成が可能になり、複数拠点で冗長化された堅牢なアプリケーション・セキュリティゲートウェイを実現できた。
- BIG-IPの高い処理能力によるDDoS対策や、BIG-IP ASMを活用したアプリケーション攻撃への防御も実現可能になった。
- BIG-IQも導入することで、異なるデータセンタに設置されたBIG-IPの集中管理も実現できた。

ソリューション

このような問題を解決するための手段としてNIIが採用したのが、ユーザからのリクエストを一手に引き受け、リクエスト内容を解析した上で各種サービスに引き渡す「アプリケーション・セキュリティゲートウェイ（以下、ゲートウェイ）」の実装である。NIIではこれまでにも一部のサービスで、内製のゲートウェイを利用した経験があり、適切なアプローチであることは検証済み。そこでこれを全サービスに展開するため、マルチクラウドに対応できるゲートウェイを立ち上げ、ハイブリッド構成でセキュリティを確保することが目指されたのである。

NIIがそのために提示した要件は主に4点あった。L7プロトコルの解析とフォワーディングが行えること、ファイアウォールだけではなくDDoS対策やWAF等のセキュリティ機能を実装できること、ゲートウェイ自体を複数データセンタで冗長構成にすることで堅牢性を確保すること、そしてSINET5の100Gbpsフルメッシュアーキテクチャを活かせる性能を持つことだ。

この要件に基づき2015年10月に入札を実施し、2016年4月に4つのデータセンタで冗長化されたゲートウェイを構築。ここで重要な役割を果たしているのが、BIG-IPなのである。

メリット

■IP Anycast構成によって高い可用性を確保

BIG-IPは全国4か所のデータセンタに設置され、BIG-IP DNSとAdvanced Routing Moduleの機能によって、全てがアクティブかつ同一グローバルIPを持つIP Anycast構成となっている。エンドユーザからの接続は、ネットワーク経路的に最も近いBIG-IPが担当。これがダウンした場合には、残りのデータセンタのBIG-IPが自動的に接続を受けるため、全データセンタがダウンしない限り可用性が確保される。また統合的な運用を視野にBIG-IQも導入されており、現在4台のBIG-IPの集中管理を実施。今後の多様なコンテンツサービス環境の実現に向け、さらなる活用を検討している。

■DDoS攻撃やWebアプリケーションへの攻撃を防御

サイバー攻撃の不正トラフィックもまずBIG-IPで受け、ゲートウェイの持つセキュリティ機能で対処される。BIG-IPはDDoS対策機能を装備しており、大規模な攻撃にも耐えられる処理能力を持っていると評価されている。またWAF機能を持つBIG-IP Application Security Manager（ASM）も導入されており、アプリケーションへの攻撃にも対応可能だ。

■実績のある製品ならではの安心感も大きなメリット

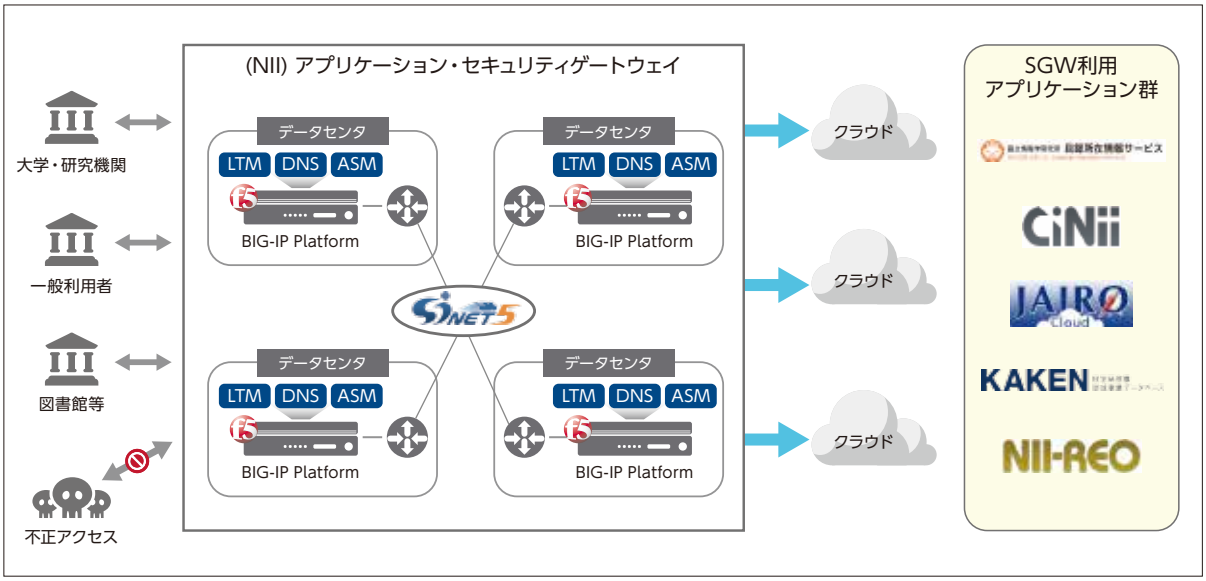
さらに三浦氏は「内製で得た知見をもとに、同等以上の機能を持ちかつ実績のある製品を採用したことで安心感も向上しています」と指摘。マルチクラウドに展開したサービスを保護する上で、十分に信頼できるゲートウェイを実現できたと語る。「現在はWebサービスをゲートウェイの主な対象としていますが、BIG-IPは様々なアプリケーションに対応しているため、HTTP以外のプロトコルへの適用も検討しています。また充実したログ機能でトラフィックを分析し、対策に活用することも考えています」。

2017年度にはNII提供の全サービスが、このゲートウェイに接続される予定になっていると言う。

Customer Profile

大学共同利用機関法人
情報・システム研究機構 国立情報学研究所

情報学という新しい学問分野での「未来価値創成」を使命とする国内唯一の学術総合研究所である。研究分野は幅広く、情報学における基礎論から人工知能やビッグデータ、IoT、情報セキュリティといった最先端のテーマまで、総合的に研究開発を推進。また大学共同利用機関として、学術コミュニティ全体の研究・教育活動に不可欠な最先端の学術情報基盤の構築・運用を推進するとともに、全国の大学や研究機関のみならず民間企業や社会活動との連携・協力を重視した運営を行っている。さらに、独創的・国際的な学術研究の推進や先導的学問分野の開拓を目指す大学院教育にも取り組んでいる。



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

2016年11月