筑波大学
University of Tsukuba

「最近ではDoS攻撃やDDoS攻撃が増加しています。
今後これらを防御するには、
F5が提供するアプリケーションレベルでの
対策が必要になるはずです」

国立大学法人 筑波大学 情報環境機構学術情報メディアセンター ネットワーク研究開発部門 准教授 博士（工学） 佐藤 聡 氏

キャンパス情報ネットワークの更新に伴いBIG-IPを導入 外部からのアクセス経路の境界ファイアウォールを1台に集約 DDoS攻撃やDNSへの攻撃に対する防御にも期待

インターネット黎明期からすでに30年にわたり、学内ネットワークを運営している国立大学法人 筑波大学。ここでは2015年8月に実施されたキャンパス情報ネットワークの更新に伴い、外部からのアクセス経路にBIG-IP 7200vが導入されている。これによって、以前は複数の機器で負荷分散を行っていた境界ファイアウォールを1台に集約、管理性と処理能力を高めているのだ。また近年急増しているDDoS攻撃へのより高度な対策や、DNSを狙った攻撃への対応も可能になると期待されている。

従来の課題

筑波大学は、他に例を見ない幅広い学問分野を有する総合大学である。学内の情報ネットワークはインターネット黎明期から運用が開始されており、2004年の国立大学法人へと移行したタイミングで機器のリース化を実施、その後は6年をめどに機器入れ替えが行われている。直近のリプレースは2015年8月に実施され、同年9月から新ネットワークによるサービスが開始された。

「今回のリプレースで大きな課題になったのは、運用管理の集中化とセキュリティの向上です」と説明するのは、筑波大学 情報環境機構学術情報メディアセンターネットワーク研究開発部門 准教授の佐藤 聡氏。筑波大学では情報ネットワーク運用開始当初から、各研究科等の部局ごとに管理者を立ててもらい、部局内のネットワークは個別に管理する体制だった。しかし運用開始から約30年が経過、管理担当者の退官によって、多くの部局で引き継ぎが必要な状況になっていると言う。「引き継ぎを受けた人にネットワークに関する十分な知識がない場合には、思わぬ障害が発生する危険性があります。またセキュリティ面から見ても、危ないネットワークになりかねません」。

国立大学法人 筑波大学
情報環境機構
学術情報メディアセンター
ネットワーク研究開発部門 准教授
博士（工学）
佐藤 聡 氏

その一方で、最近ではDoS攻撃やDDoS攻撃が増加していることも、大きな問題になっていると佐藤氏は指摘する。

「私は2013年から、学内の未使用IPアドレスに対するHTTPリクエストを、ハニーポットを使って収集、分析しているのですが、非常に多くのリクエストが来ていることがわかっています。未使用IPへのアクセスが大量に発生しているということは、筑波大学がDoS攻撃のターゲットになっていることを示唆しています」。

また学内が複数のドメインに別れており、DNSサーバが散在していることが、今後セキュリティ上の問題を引き起こす可能性があるとも指摘する。最近ではDNSを狙った攻撃も増えており、適切な更新が行われていないDNSサーバが存在すれば、攻撃のターゲットになる危険性が高くなるからだ。

Overview

業種
国立大学法人

課題
- ファイアウォールの管理性向上
- 近年急増しているDDoS攻撃へのより高度な対策
- 学内に散在するDNSサーバ攻撃への対応

ソリューション
- BIG-IP Application Security Manager（ASM）
- BIG-IP Advanced Firewall Manager（AFM）
- BIG-IP Domain Name System（DNS）

メリット
- 以前はファイアウォール×2台と負荷分散装置の組み合わせだった機器構成を、1台のBIG-IPに集約することで管理性が向上
- BIG-IP ASMによってDDoS攻撃に対するアプリケーション レベルでの対策が可能
- DNSプロキシ機能で学外用のリゾルバを分離することで、DNSのセキュリティ確保も容易に

Customer Profile

国立大学法人 筑波大学

1872年（明治5年）、日本初の師範学校（教員養成校）として発足、その後、東京師範学校、高等師範学校、東京高等師範学校と発展、1949年（昭和24年）に東京文理大学等4校が統合して東京教育大学となり、1973年（昭和48年）の筑波研究学園都市への移転を機に、現在の筑波大学となる。よき伝統と特色を活かしながらも、大学に対する内外からのさまざまな要請に応えるため、国内の大学としては初となる抜本的な大学改革を実施し、「開かれた大学」「教育と研究の新しい仕組み」「新しい大学自治」を特色とした総合大学として、活力に富んだ国際競争力のある大学づくりを推進。またつくばの人材育成拠点、産官学協働の拠点としても、大きな貢献を果たしている。

茨城県つくば市天王台1-1-1
URL：https://www.tsukuba.ac.jp

ソリューション

これらの課題を解決するため、2015年8月の機器更新ではまず、ネットワーク セグメントの整理に着手。また、研究科や部局ごとに分かれていたセグメントを、サーバセグメントやクライアントセグメントといった、機能別セグメントへと移行しつつある。これによって学術情報メディアセンターの限られた人員でも、ネットワークの末端まで管理可能な環境を作っているのだ。

その一方で、インターネット（SINET5）からのアクセス経路上には、高度なDDoS対策が可能なBIG-IPを設置することで、外部からの攻撃に備えている。

※SINET5への移行は、2016年4月に実施予定

メリット

複数の機器をBIG-IPに集約することで管理性が向上

以前のインターネットからのアクセス経路には、ファイアウォールを2台設置し、その前後に負荷分散装置を置くことで、4Gbpsの処理能力を確保していた。このような構成になっていたのは、SINET4へのアクセス帯域が10Gbpsであるにも関わらず、当時はこれに対応できる十分な処理能力を持ったファイアウォールが存在しなかったからだと佐藤氏は振り返る。しかしDDoS攻撃を受けた際には、負荷分散装置の処理能力を越える負荷がかかることもあり、対策としては十分とは言えなかったと語る。

現在ではこれらを1台のBIG-IPに集約している（スタンバイ用のBIG-IPを含めると2台構成になるが、外部からのパケットは常に1台のBIG-IPを通過するようになっている）。導入モデルはBIG-IP 7200v、最大スループットは40Gbpsなので、以前のように外部から来るパケット量が処理能力を超えることはない。また機器を1台に集約したことで、管理性も向上している。

DDoS攻撃に対するより高度な対策も可能

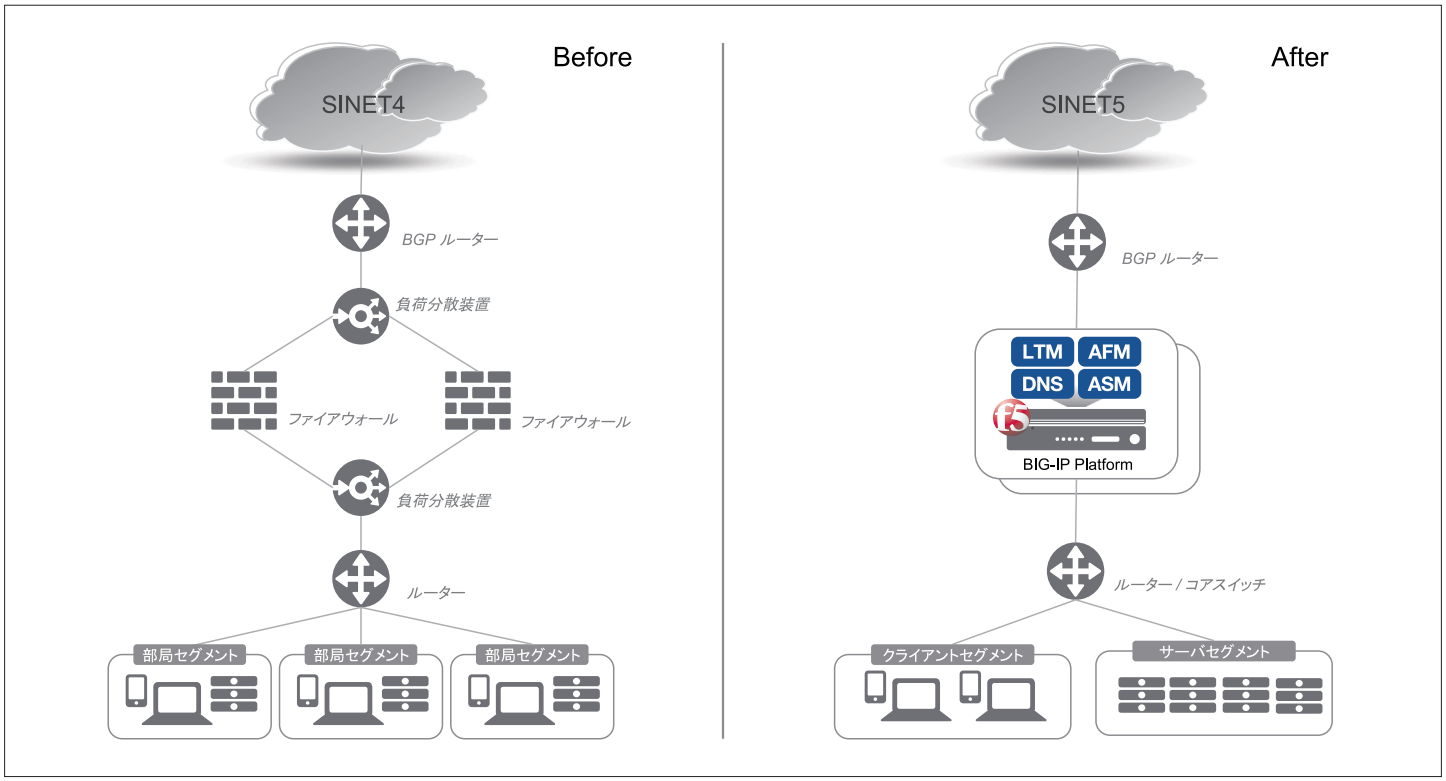
DDoS攻撃への対応を、より柔軟に行えることも、高く評価されている。現在はBIG-IP AFMの機能を使用し、IPアドレス レベルでの静的な設定で対処しているが、今後はBIG-IP ASMのアプリケーション ファイアウォール（WAF）機能によって、アプリケーション レベルでのDDoS検出や防御が可能になると期待されている。

「これまでは、特定の外部IPアドレスから複数の内部IPアドレスへのスキャンを行う『1対N』の攻撃や、多数の外部IPアドレスから特定の内部IPアドレスを狙う『N対1』の攻撃だけでしたが、今後は多数の外部アドレスから複数の内部アドレスを狙う『N対N』の攻撃も登場するはずです。このような攻撃は、IPアドレスのフィルタリングだけでは防げません。F5が提供するアプリケーション レベルでの対策が必要になるはずです」（佐藤氏）。

DNSプロキシ機能でDNS攻撃への防御も容易に

BIG-IPにはDNSプロキシ機能も装備されているが、これに対する期待も高い。学内用と学外用とでリゾルバを分けることで、DNSに対する外部からの攻撃も防御しやすくなるからだ。

「BIG-IPにはセキュリティに関するさまざまな機能があります」と佐藤氏。「これらをうまく活用することで、少ない管理者数でも安全性をさらに向上できると期待しています」。



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

2015年00月A