慶應義塾

「ユーザIDとパスワードで認証を行うSSL VPNに加え、
IPアドレスとMACアドレスに基づくアクセス制限も行うことで、
高い安全性を確保しています。またSSLアクセラレーションを
活用することで、教育研究系システムのSSL化も容易になりました」

慶應義塾 ITC本部（インフォメーションテクノロジーセンター）　大塚 瑞希 氏

三田キャンパスの教育研究系/事務系システムで ネットワーク機器をBIG-IPへと集約 セキュリティ向上と運用負担軽減を実現

慶應義塾のバックボーンと三田キャンパスのネットワークを運用管理する、慶應義塾 ITC本部（インフォメーションテクノロジーセンター）。ここでは三田キャンパスの事務系システムにアクセスするためのVPN装置として、BIG-IP Access Policy Manager（APM）が導入されている。以前はロードバランサとしてBIG-IP Local Traffic Manager（LTM）、VPN製品として他社製品が使用されていたが、BIG-IPを最新モデルへと移行し、新たに導入されたBIG-IP APMをBIG-IP LTMと統合したのである。これによって事務系システムへのVPN接続の安全性をさらに向上すると共に、教育研究系システムのSSL化も容易になった。機器集約によって運用負担も軽減。今後はWAF機能も活用し、サイバー攻撃への防御も強化していく計画だと言う。

従来の課題

セキュリティをどのように確保するかは、大学のシステムでも重要な課題だといえる。しかし大学のネットワークには職員が使う事務システムだけではなく、学生向けの各種Webサイトや研究用サーバ群など、多様なシステムが混在しているため、その実現は決して簡単ではない。この問題の一部をBIG-IPで解決しているのが、慶應義塾のITC本部（インフォメーションテクノロジーセンター）だ。

慶應義塾のネットワークは、キャンパス毎にコアスイッチを用意し、これらをバックボーン ネットワークで接続した構成になっている。各キャンパスにはそれぞれ、キャンパス内のネットワークを運用管理するITCが設置されており、ITC本部がバックボーンと三田キャンパスの一部の運用管理を担当。この三田キャンパスのネットワークの中で、学生向けの「教育研究系システム」と、職員や学外の協力業者が使用する「事務系システム」という、性格の異なるシステムに対するネットワーク機能が、BIG-IPに集約されているのである。

慶應義塾
ITC本部（インフォメーション
テクノロジーセンター
大塚 瑞希 氏

「以前もロードバランサとしてBIG-IPを利用していましたが、事務系システムにアクセスするためのVPN装置は他社製品を使用、L2TPとIPsecによってVPN接続を行っていました」と語るのは、慶應義塾 ITC本部で主に事務系システムの運用管理を担当する大塚 瑞希氏。しかしVPN装置の設定は、いったんユーザが認証されてしまえば、その配下のネットワーク全てにアクセスできる状態になっていたと振り返る。「事務系システムには学内の職員の他、外部の協力業者もアクセスするため、このままでは十分なセキュリティを確保できません。ここを強化すべきだという要望は、以前から出ていました。使用していたハッシュ関数もSHA-1だったため、SHA-2への移行も重要な課題になっていました」

また教育研究系システムのSSL化が進みつつあることで、Webサーバの処理負荷や、証明書管理の負担が増大していたことも問題だったと言う。「さらに、使用機器の台数が多いため無停電運用可能なサーバ室に全てを収容できず、BIG-IPを計画停電が必要なサーバ室に設置していたことも、運用負担の増大につながっていました。せっかくBIG-IPを使っているだからその機能をもっと活用し、機器集約を実現したいと考えていました」

Overview

業種

学校法人

課題

- ロードバランサとVPN装置が分かれており、運用負担が大きかった。
- 事務系システムのVPNで使用していたハッシュ関数がSHA-1であり、設定内容も十分な安全性を確保できていなかった。
- 教育研究系システムのSSL化によって、Webサーバの負荷が増大し、証明書管理の負担も増大していた。

ソリューション

- BIG-IP Local Traffic Manager（LTM）
- BIG-IP Access Policy Manager（APM）

メリット

- ロードバランサとVPN装置の集約により、設置機器の数が少なくなり、運用負担が軽減した。
- SHA-2を使用したSSL VPNに加え、IPアドレスとMACアドレスに基づくアクセス制限等を行うことで、事務系システムの安全性が向上した。
- SSLアクセラレーションを活用することで、Webサーバの負荷が軽減し、証明書管理の負担も軽減した。

Customer Profile

慶應義塾

1858年（安政5年）、福澤諭吉が蘭学塾として開塾。1868年（慶應4年/明治元年）に慶應義塾と命名される。明治初期に『学問のすゝめ』を著し、人間の自由・平等・権利の尊さを説くことで新時代の先導者となった福澤諭吉の教育理念は、現在に至るまでも脈々と受け継がれている。総合学塾として、教育、研究、医療、社会貢献、国際連携等の分野で、さまざまな取り組みを推進。「独立自尊」の精神に基づき、21世紀の日本と世界を先導する人材を育成している。

ソリューション

そこで慶應義塾ITC本部では、これらのネットワーク機器のリースアップのタイミングに合わせ、BIG-IPの最新モデルへのリプレースを行い、VPN装置もBIG-IPへと集約することに決定。まず2015年8月にBIG-IP Local Traffic Manager（LTM）を新たに導入し、既存のBIG-IPから移行。同年9月にはBIG-IP Access Policy Manager（APM）も導入し、VPN装置も集約した。このタイミングで他社VPN装置が不要になったため、新規導入されたBIG-IPは無停電運用可能なサーバ室への設置が可能になった。

バックボーンからBIG-IPへの経路は、教育研究系システム向けか事務系システム向けかによって異なるグローバルIPアドレス（GIP）が設定されており、アクセスはまずここで振り分けられる。教育研究系システムへのアクセスは、LTMで負荷分散された上で各Webサーバに配分。事務系システムへのアクセスは、APMによるVPNの認証が行われ、業務サーバへと送られるようになっている。なお複数のGIPへの戻り経路は、BIG-IPのSecure NAT機能によって自動制御されている。

メリット

■VPNアクセスのセキュリティを強化

「BIG-IPによるVPN接続では、ユーザIDとパスワードで認証を行うSSL VPNを採用し、アクセス元のIPアドレスとMACアドレスに基づくアクセス制限も行っています」と大塚氏。また各ユーザがどのエリアにアクセスできるのかもきめ細かく設定しており、以前に比べて高い安全性を確保しているという。さらにVPNで使用するハッシュ関数もSHA-2へと移行、これもセキュリティ強化に貢献している。

教育研究系システムのSSL化も容易になった。BIG-IPのSSLアクセラレータ機能を活用することでWebサーバの負荷を軽減すると共に、SSL証明書もBIG-IPに集約できるようになったからだ。

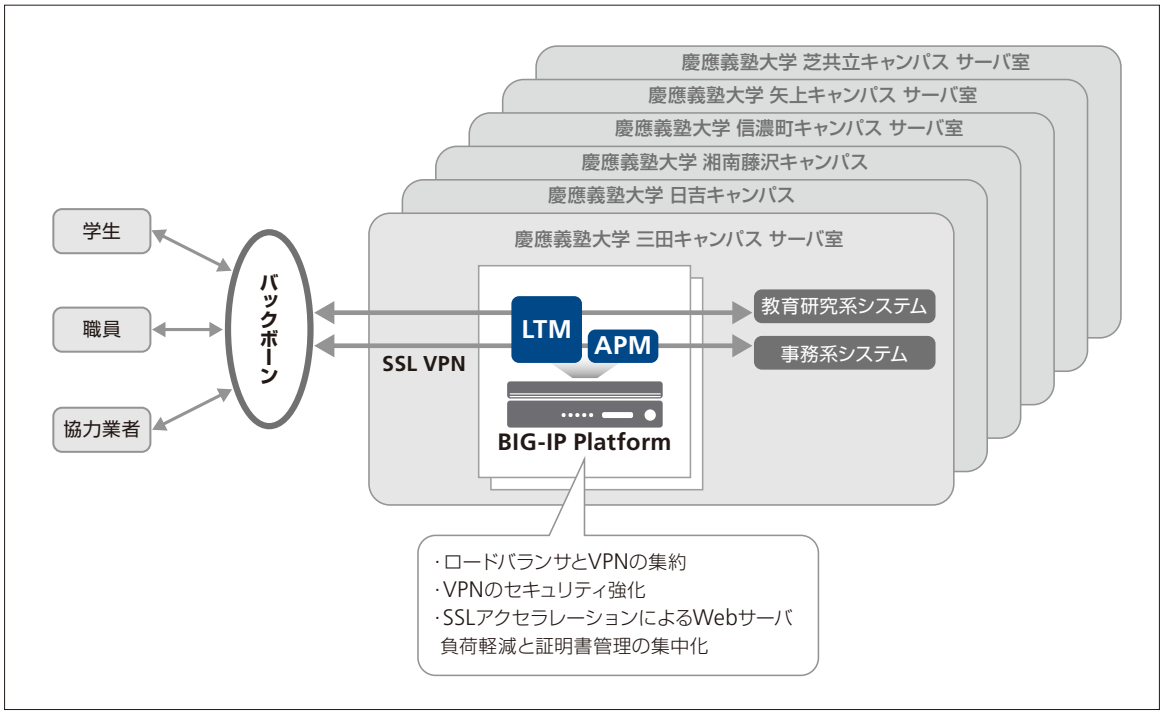
■機器集約によって運用負担も軽減

ネットワーク機器を集約したことで、管理対象となる機器の数が少なくなり、運用負担も軽減した。また以前は、BIG-IPが設置されていたサーバ室の計画停電のたびに、ロードバランサ配下のサーバを全てシャットダウンしなければならなかったが、現在ではその必要もなくなっている。さらに、機器の保守費用が削減されたことも、メリットの1つだと言う。

■今後はWAFも活用しサイバー攻撃を防御

三田キャンパスには職員用のメールサーバが3台設置されているが、2016年夏にはこれらもBIG-IPの配下に置く予定だと大塚氏は語る。これによってメールもSSL化しやすくなり、通信の安全性をさらに高められると言う。

またBIG-IP Application Security Manager（ASM）を導入し、アプリケーション ファイアウォール（WAF）機能を活用することも検討されている。「最近では海外から教育研究系システムへの不正アクセスが発見されています。大学は狙われやすい組織なので、このようなサイバー攻撃も、BIG-IPで防御し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5月