



## 複数製品で構成されていたネットワーク機器をBIG-IPに集約、 トータルコストの削減とセキュリティ強化を同時に実現

### Products

- ・ BIG-IP Local Traffic Manager
- ・ BIG-IP Application Security Manager
- ・ BIG-IP Advanced Firewall Manager
- ・ BIG-IP DNS

### Challenges

- ・ 複数製品で構成されたネットワーク機器の運用負担
- ・ BINDのセキュリティパッチ適用の作業負担
- ・ 不徹底なSSL復号やWAFの機能制約による不十分なセキュリティ

### Benefits

- ・ ネットワーク機器集約による調達コストの削減と運用負荷軽減
- ・ DNSをBIG-IPへと移行したことで不要になったBINDのパッチ適用
- ・ 全てのSSL通信を復号しWAFで防御することによるセキュリティ強化
- ・ 国別認証ポリシーの実現により、ユーザー認証の安全性と利便性のバランスも向上

キリスト教精神に基づく「良心」を建学精神とし、京都府内の複数のキャンパスで約3万人の学生が学ぶ同志社大学。以前は複数の製品で構成されていたネットワーク機器が、BIG-IPへと集約されています。これによって調達コストを低減させる共に、占有ラックスペースや運用負担も大幅に削減。また全てのSSLトラフィックを確実に復号しWAFで解析することで、脅威に対する防御も強化しています。さらに、アクセス元の国別認証ポリシーを定義することで、ユーザー認証の安全性と利便性のバランスも向上。将来はクラウド上にBIG-IP Cloud Editionを展開し、学内のBIG-IPと共にBIG-IQで統合管理することも検討されています。

### 課題 (Business Challenges)

2018年に4年毎の学内システムを更改を迎えた同志社大学。ネットワーク機器もこれに合わせて、コストパフォーマンスの最適化とセキュリティ強化を目標に掲げた再構築が行われました。

「以前のネットワークは、個別メーカーのロードバランサやファイアウォール、大手WAF専門メーカーの製品などで構成されていました」と語るのは、同志社大学で情報ネットワーク係長を務める山北 英司 氏。そのため多くのラックスペースが必要となり、運用も個別にログインして行わなければならないといった。またDNSはオープンソースのBINDを使用しており、合計8台分のセキュリティパッチを年に数回適用する作業も、大きな負担になっていました。さらに、SSLで暗号化されたWebサイトへの攻撃について、十分検知できていなかった可能性もあると振り返ります。DMZに向かうトラフィックは復号してWAFによるチェックを行っていましたが、L2構成のため通信を終端しておらず、暗号化方式がサーバー側のみ最新化されWAF側で追従できない場合には、セキュリティチェックが確実とは言い切れなかったのです。また当時使用していたWAF専用機では、WEBコンテンツ内に複数の文字コードが使われている場合トラフィックを解析できず、防御できない脅威も存在していたといいます。

「重大なインシデントは発生していませんが、脅威の多様化や高度化に対応するには、防御をさらに強化していく必要があると考えました。」

### 解決策 (Solution)

これらの課題解決のために選択されたのがF5 BIG-IPです。それまで複数の製品で構成されていたネットワーク機器を、BIG-IPで集約する提案を採用したのです。

「最も重視したのは安定性です」と山北氏。その上で、最も大きくコスト削減できる案を選択したと説明します。

「BIG-IPでネットワーク機器を集約することで、調達コストは期待以上に削減できました。  
脅威を自動的にブロックすることで、セキュリティも強化しています」

同志社大学  
総務部 情報企画課 情報ネットワーク係長 ITサポートオフィス

山北 英司 氏

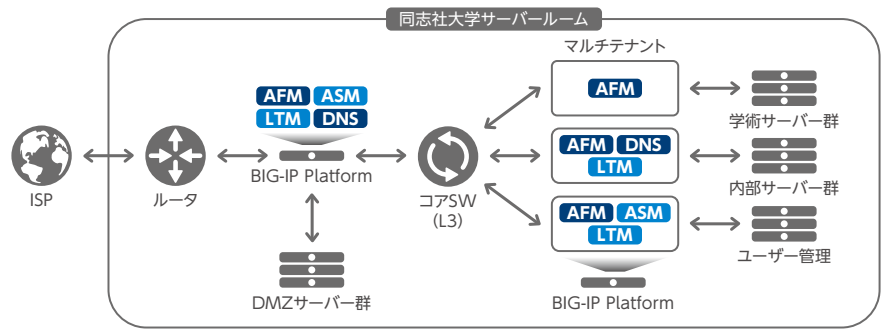


「また複数のネットワーク機能を集約しやすいことや、機器集約やSSL処理によって処理速度が低下しないことも評価しました」。

2018年3月には契約を締結し、同年8月には機器の切り替えを実施。外部ネットワークと学内のコアルータの間に1セット、コアルータと各学内システムとの間には1セットのBIG-IPをマルチテナント機能によって、運用者単位に3つに分割して、運用権限も分割して導入できました。

外部ネットワークとコアルータをつなぐBIG-IP

では、BIG-IP LTM、BIG-IP ASM (WAF)、BIG-IP AFM、BIG-IP DNSが稼働。ここでDMZ内サーバーのロードバランシングや学内システムに対するトラフィック制御、SSLの復号を行った上でのセキュリティチェック、脅威の防御などを行っています。またBIG-IPのGeolocation機能も活用されており、国内からのアクセスにはID、Passwordでの認証ですが、海外からのアクセスには多要素認証を適用するなど、ユーザー認証も強化されています。コアルータと学内システムとの間のBIG-IPは、主に学内サーバーのロードバランシングを担当。またここでもファイアウォールやWAFを動かすことで、多層防御も実現しています。



**効果 (Benefits)**

「機器集約で調達コストは期待以上に削減できました」と山北氏。その一方で性能も十分に出ており、全WebサーバーのSSL処理をBIG-IPにオフロードしても、ボトルネックは発生していないといいます。「ユーザーからも『遅い』と言われたことは一度もありません」。

機器の設置スペースも合計でラック1本分を削減。「実は並行してサーバールームの耐震補強も実施したのですが、これによって補強対象の面積を縮小できたことも、コスト削減に貢献しています」と、同志社大学 情報ネットワーク系の藤堂 慈 氏は語ります。

「運用負担も軽減しています」というのは、同志社大学 情報ネットワーク系の高木 育史 氏。複数のネットワーク機能の運用を、BIG-IPにログインするだけで行えるようになったからです。また以前のロードバランサはバージョンアップ時にサービスを停止する必要がありましたが、BIG-IPは停止させずにバージョンアップが可能であるため、サービス停止のアナウンスも必要なくなりました。「BINDのセキュリティパッチも、以前のシステムでは4年間で11回も適用していましたが、DNS機能をBIG-IPに集約したことでその作業も不要になっています」。

もちろんセキュリティも強化されています。現在では全てのSSLトラフィックが復号された上で、WAFで解析されるため、脅威となるトラフィックが自動的にブロックされているからです。

「初めてBIG-IPのレポートを見たときには『ここまでチェックしているのか』と、解析範囲の広さに驚きました」と振り返るのは、同志社大学 情報ネットワーク系の藤江 悠五 氏。以前は防御が難しかったL4-L7のDDoS攻撃も防御でき、なりすまし攻撃にも対応できるようになっています。「自動的にきちんと守られているという実感があり、以前にも増して安心して運用できるようになりました」。

さらに藤江氏は、iRulesによるカスタマイズ性の高さも、BIG-IPの大きな魅力だと付け加えます。例えばリダイレクトを行う場合、以前はサーバー側で処理する必要がありましたが、現在ではBIG-IPで実行可能です。そのためトラフィックの集中管理も容易になったのです。

今回のシステム更改では、メールをMicrosoft Office 365へと移行するなど、クラウド化への取り組みも行われ、今後は可用性や新規サービス展開のスピードアップのためにサーバー環境をクラウド化していくことも検討されています。



同志社大学 総務部 情報企画課 情報ネットワーク係

「多数の学外事業者クラウド環境でのシステム構築を委託するなかで、迅速にセキュリティを実装できるようテンプレート化されたWAFの設定までを各事業者に委任し、なおかつ適切な権限管理の元で、大学と事業者双方でサービスの状態やトラフィックを把握・管理できる環境が重要になります」と山北氏。そのために、マルチクラウドに対応するBIG-IP Cloud Editionや管理基盤としてBIG-IPの活用も視野に入っていると語ります。同志社大学はBIG-IPを導入することでコスト削減やセキュリティ強化を実現しただけではなく、アプリケーションデリバリの新たな可能性も切り拓きつつあるのです。



**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/>