「BIG-IP ASMでセキュリティ対応を集中化することで、管理負担増大を最小限に抑えながらセキュリティを強化できます。またログ管理を集中化することで、情報セキュリティガバナンスも効率的に確立できると期待しています」

大学共同利用機関法人 高エネルギー加速器研究機構 計算科学センター研究機関講師 村上 晃一 氏

BIG-IP：高エネルギー加速器研究機構 管理負担の増大を最小限に抑えながら サイバー攻撃からの守りを強化 情報セキュリティガバナンスの効率化にも期待

最先端の大型粒子加速器を用いた各種研究活動を支える、高エネルギー加速器究機構（KEK）の中央計算機システム。そのリニューアルが行われる2016年9月のタイミングで、WAF機能を提供するBIG-IP ASMが導入されることとなった。目的は煩雑な管理業務の増大を最小限に抑えながら、サイバー攻撃への対応を強化すること。セキュリティインシデントに関するログ管理をASMに集中化することで、情報セキュリティガバナンスも効率化できると期待されている。

ビジネス上の課題

1930年台に誕生して以来、科学の発展に大きな貢献を果たしてきた加速器科学。原子核や素粒子の研究はもちろんのこと、生命現象の解明するための新たな研究手法の確立や、工業利用・医療などの応用分野でも重要な役割を担っている。その基盤となる粒子加速器の研究開発と、これを用いた基礎科学研究のための世界的な拠点になっているのが、大学共同利用機関法人 高エネルギー加速器研究機構（KEK）だ。国内では大学共同利用機関として、大学の研究者や大学院生に最先端の研究の場を提供。国外からも毎年のべ8万人を超える研究者が来訪し、共同研究を進めている。これによって小林・益川理論の証明、多くの複合粒子の発見、ニュートリノ振動の解明など、様々な成果が生み出されているのである。

大学共同利用機関法人
高エネルギー加速器研究機構
計算科学センター研究機関講師
村上 晃一 氏

このような研究では、実験で生み出される膨大なデータの解析はもちろんのこと、他の研究者との情報共有や協業も重要になる。このような活動を支える上で不可欠な存在になっているのが、KEK 計算科学センターが運営する中央計算機システムだ。

「このシステムには日本国内はもちろんのこと、世界各国の研究者からのアクセスがあり、多様な活用方法に対応しなければなりません」と語るのは、KEK 計算科学センター 研究機関講師の村上 晃一氏。その一方で、システムが停止すれば研究業務も止まってしまうため、可用性の確保も重要課題になっていると説明する。「可用性を維持するには、サイバー攻撃からの防御も欠かせません。KEKのような研究機関は攻撃対象になりやすく、実際にSQLインジェクション攻撃を受けることもあります。また最近ではDDoS攻撃の脅威も高まっています」

しかし、これらに対してアプリケーション毎に対応するのでは、膨大な工数が必要になる。KEKの中央計算機システムには、データ解析システムはもちろんのこと、電子メールシステムや各種Webシステム、会議支援システム、電子証明書の認証局等、多岐にわたるアプリケーションが稼働しており、Webアプリケーションを動かす言語も、PHPやJava、Python等、様々なものが利用されているからだ。

Overview

業種

研究機関

課題

- 最近ではサイバー攻撃が増えており、これによるシステム停止を回避する必要があった。
- その一方で管理負担の増大は、最小限に抑制することが求められた。
- 情報セキュリティガバナンスを効率的に確立することも必要だった。

ソリューション

- BIG-IP Local Traffic Manager(LTM)
- BIG-IP Application Security Manager (ASM)

メリット

- 幅広いセキュリティ機能をホスト毎にきめ細かく設定できるため、多様なシステムが混在する環境でもセキュリティ対応の集中化が容易になり、管理負荷増大を抑制しながらセキュリティを強化できるようになった。
- ログ管理をASMに集中化することで、セキュリティインシデントをはじめとするログデータの収集と可視化が容易になり、情報セキュリティガバナンスの効率的な確立も可能になると期待されている。

Customer Profile

大学共同利用機関法人
高エネルギー加速器研究機構

1955年の東京大学原子核研究所が前身。1971年の高エネルギー物理学研究所設立などを経て、2004年より大学共同利用機関法人となった。最先端の大型粒子加速器を用いた基礎科学を推進する研究所として、宇宙の起源、物質や生命の根源を探求。研究者の自由な発想による「真理の追究」を目指し、研究開発を推進している。

「KEKは大学共同利用機関法人なので、情報セキュリティガバナンスの確立も不可欠です。この責務を効率的に果たすためにも、セキュリティ対応を集中化できる仕組みが必要だと考えていました」

ソリューション

そのために導入されたのが、Web Application Firewall (WAF) 機能を提供するBIG-IP Application Security Manager (ASM) である。中央計算機システムは2016年9月にリニューアルされる予定だが、このタイミングでASMの利用を開始する計画になっている。

「BIG-IP Local Traffic Manager (LTM) は負荷分散装置として以前から活用していましたが、同一アプライアンスにWAF機能も実装できれば、高いコスト効率が実現できます」と村上氏。BIG-IPはこれまでトラブルがほとんどなく、運用ノウハウが蓄積されていることも、ASM採用のメリットだと指摘する。「もちろんセキュリティ機能を網羅的に装備していることも、ASMの大きな魅力です」

今回のシステム更改では、Webシステムの9つのサービスと検証用システムの入口部分にBIG-IPを設置。それぞれLTMとASMの機能を実装する構成になっている。

メリット

■多様なシステムの保護を集中化可能

「現在（2016年7月）はまだ正式サービス前の段階ですが、実際にASMに触れてみた結果、サイバー攻撃からの防御を強化できるという手応えを感じています」と村上氏。保護対象となるホスト毎に設定を変えられるため、多様なシステムが混在していても、セキュリティ対応の集中化が容易だと言う。

「これによってセキュリティインシデントへの対応を迅速化でき、一貫性のあるサービスレベルを実現できます。もちろん管理コストの削減も可能になるはずです」

■ログ管理集中化で情報セキュリティガバナンスも効率化

ASMにセキュリティインシデントに関するログを集中できることも、大きなメリットだと村上氏は指摘する。これまではアプリケーション毎にログを取得しており、それらを収集しなければならなかったため、ログ分析の負担も大きかった。しかしログ管理をASMに集中化できれば、この負担も軽減できる。

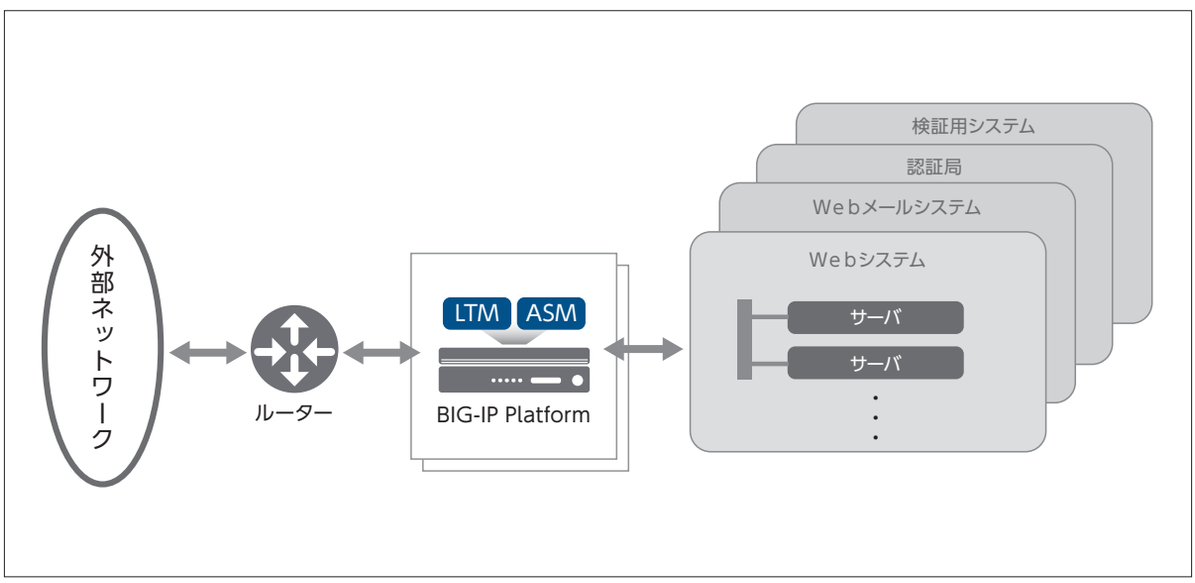
取得できるログの種類が幅広いこともメリットの1つ。上記のアクセスログに加え、WAFによるセキュリティのログや、サーバの応答遅延等の性能データまでもが、1台のBIG-IPで取得できるのだ。レポーティング機能も充実しており、攻撃状況や稼働状況の統合的な可視化や、任意の時間における攻撃内容のグラフィカルな分析表示等が可能。状況を視覚的に監視することで、異常検知を迅速に行えることも高く評価されている。

「最近では情報セキュリティガバナンスに関する文部科学省からの要求レベルも高くなっています。これに対応するためにも、BIG-IPのログ機能は必須だと言えます」

■将来はSSL処理にも活用、Silverlineにも興味あり

今後はWebシステムのSSL化も進んでいくことになるだろうと村上氏は語る。これに伴い、Webサーバの SSL 処理負荷や、証明書管理の負担も増大することになるが、SSL の処理を BIG-IP に集中化することで、これらを軽減することも視野に入っていると言う。またDDoS 対策機能をクラウドで提供する F5 Silverline にも興味があると言及。これよって二重防御が可能になり、より安心な運用が可能になるからだと説明する。

「F5 製品はアプライアンスを入れ替えることなく、新たな機能を追加することが可能です。これからも時代の流れに合わせて、必要なものを取り込んで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7月