Case Study

株式会社ネットプライス

WE MAKE APPS GO FASTER. SMARTER. SAFER.

長年の悲願だったWAFを導入し外部からの攻撃を可視化、攻撃由来のアクセスを遮断することでWebサーバの負荷も軽減

「忙しい女性を笑顔にする。」ことを目指し、2000年からギャザリング（共同購入）によるインターネット通販を手がけている株式会社ネットプライス（以下、ネットプライス）。ここではECサイト運営に必要なWebアプリケーションをサイバー攻撃から保護する手段として、Web Application Firewall（WAF）が導入されている。まず2016年5月にはロギングモードで攻撃に関する情報収集を開始。その1年後の2017年6月からは、攻撃を防御するブロッキングモードでの運用も行っている。これによって攻撃を可視化すると共に、運用上の安心感も向上。攻撃がWebサーバに届く前に遮断することで、Webサーバの負荷軽減にも貢献している。

「これまでアプリケーション攻撃による実被害は発生していません。しかしWebサーバの前段で攻撃をブロックしたいというのは、長年の悲願でした」

株式会社ネットプライス テクノロジー本部 マネージャー 高橋 啓輔 氏

背景

インターネット通販がまだ黎明期だった1999年に創業し、2000年からギャザリングによるインターネット通販を手がけているネットプライス。購買者が多くなるほど価格が下る共同購買の仕組みや、毎日商品が入れ替わるタイムセール、サイズや使用感が合わなかった場合の30日間返品保証など、一般的なECサイトでは見られない特長によって、多くの利用者を惹きつけている。現在の会員数は累計250万人。その多くが30 ～ 40歳代の働く女性だという。

そのビジネスは当然ながら数多くのWebサーバに支えられており、機能毎に分けられたサーバ群へのアクセスは、ロードバランサによって振り分けられている。ロードバランサとしては、2006年から一貫してBIG-IP LTMを採用。URIにもとづく、きめ細かいアクセス振り分けを、iRulesの積極的な活用で実現している。

ビジネス上の課題

ここで課題となっていたのがWAFの導入だった。「Webアプリケーションはセキュアコーディングを意識しており、これまでアプリケーション攻撃による実被害は発生していません」と語るのは、テクノロジー本部 マネージャーの高橋 啓輔氏。しかし、Webサーバの前段でブロックすることで安全性をさらに高めたいというのは、長年の悲願だったと振り返る。「WAFを導入したいという話はすでに2009年から出ていましたが、当時はまだ一般的な機能ではなく、導入コストも高かったため、導入には至りませんでした」

このような状況に終止符が打たれるきっかけになったのが、それまで使ってきたBIG-IPのリプレース時期が近づいてきたことだった。BIG-IP上で稼働していたTMOSのバージョンも古くなり、最新モデルへの移行が必要となったのである。

そこで2015年12月、BIG-IP LTMのマイグレーションに合わせたWAF導入の検討に着手。長年にわたるパートナーである東京エレクトロンデバイス（TED）とも相談した結果、BIG-IP ASMの採用が決まるのである。

Overview

業種

エンタープライズ
（インターネット通信販売業）

課題

- より安全なWebアプリケーション運用の実現
- リーズナブルなコストでのWAF導入
- 新たな機能導入に伴う運用負担増大の回避

ソリューション

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

メリット

- ASMの導入で外部からのアプリケーション攻撃を可視化
- 攻撃由来のアクセスをASMで遮断することで、Webサーバの負荷が軽減し、ログ量も安定化
- それまで利用してきたLTMと同一画面でASMを管理できるため、運用負担の増大も抑制可能に

Customer Profile

株式会社ネットプライス

1999年に創業し、2000年からギャザリングによるインターネット通販を開始。「忙しい女性を笑顔にする。」ことを目指し、購買者が多くなるほど価格が下る共同購買の仕組みの提供や、毎日商品が入れ替わるタイムセール、サイズや使用感が合わなかった場合の30日間返品保証等を行っている。熱い想いを持つ個性派揃いのバイヤー陣の存在も大きな特長であり、彼らが選ぶ選りすぐりの商品が、働く女性を中心とした累計250万人の会員を惹きつけ続けている。

ソリューション

WAFとしてASMが選ばれた理由は大きく2点ある。第1は、LTMと同じプラットフォーム上でASM機能を有効化するだけで利用できるため、機器の数を増やす必要がないことだ。これによって導入コストの抑制が可能になる。また「LTMのマイグレーションを行った後、ネットワーク構成を全く変えることなくWAFを導入できるのも、大きな魅力でした」と高橋氏は語る。

第2の理由はLTMと同じ管理画面で一緒に管理できることだ。これによって運用負担の増加を抑えながら、WAFの活用が可能になると期待されたのである。

リプレースに伴うLTMの設定変更やiRulesのマイグレーションはTEDが担当。旧システムと同様の動作を問題なく再現することに成功し、2016年4月から運用を開始している。その後ASMの機能を有効化し、ロギングモードでの運用を2016年5月から開始。TEDの支援のもと、シグネチャのチューニングを数回実施し、2017年6月にブロッキングモードへと切り替えている。

「WAFを利用するのはこれが初めてであり、当初は設定内容もよくわかっていませんでしたが、TEDの支援によって問題なく導入できました」と高橋氏。「ASMとは何か」から実践的な設定方法に至るまで、きめ細かいトレーニングをTEDから受けた結果、現在では問題なく自社運用できているという。「WAFは想像以上に高度でハードルも高い機能でしたが、TEDのようなパートナーがいたおかげでそのポテンシャルを引き出すことが可能になりました」。

「外部からの攻撃は予想以上に多く、1日16万回の攻撃を受けたこともあります。これらをASMでブロックすることでWebサーバの負荷が軽減し、ログ量も安定するようになりました」

株式会社ネットプライス テクノロジー本部
マネージャー 高橋 啓輔 氏

メリット

■以前は把握できなかった攻撃の可視化が容易に

ロギングモードでのASM運用を開始してわかったのは、外部からのアプリケーション攻撃が、想定外と言えるほど多いことだった。「1日数万回の攻撃は日常的に起きており、最近では16万回もの攻撃を受けたこともあります。攻撃元の国も中国や米国をはじめとする海外が多く、日本国内からの攻撃は少ないことも意外でした」と高橋氏。攻撃内容としては、WordPress等のOSSの脆弱性を狙うもの、SQLインジェクション、クロスサイトスクリプティング（XSS）が目立っているという。

■前段でのブロッキングでWebサーバの負荷も軽減

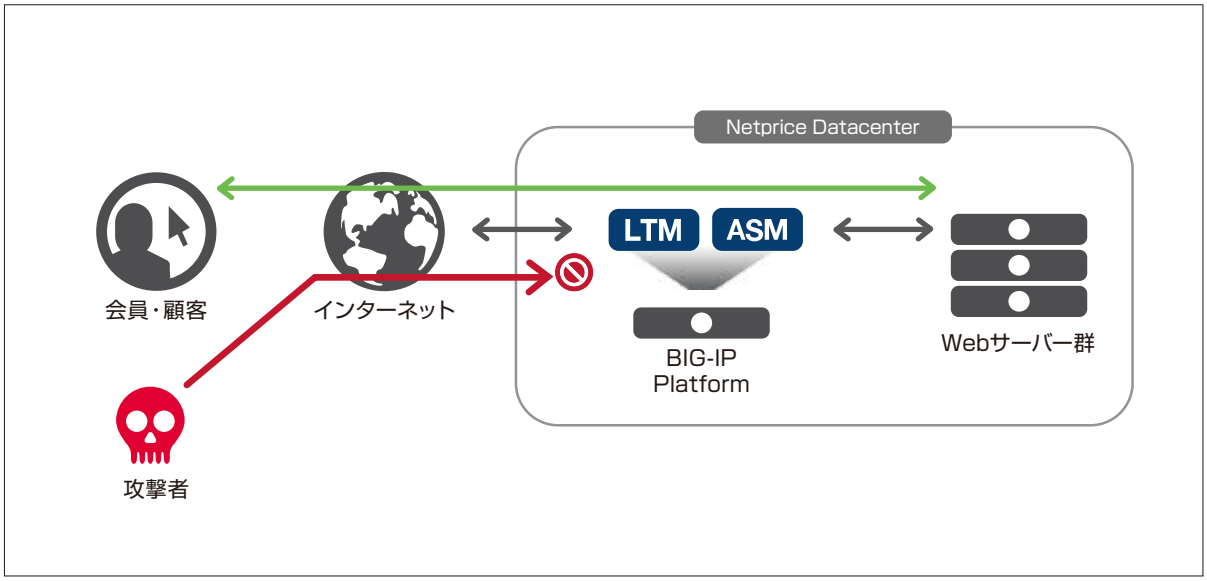
ブロッキングモードに切り替えてからは、Web サーバの負荷が軽減した。1 日数万回という膨大な攻撃由来のアクセスが、ASM で遮断されたからだ。また Web サーバが出力するログの量も安定化している。以前はログの量が急増するケースがあったが、その主な理由も攻撃の増大だったことが判明している。

「以前は Web サーバのログが予想以上に増大した時に、ログの内容から原因を究明する必要がありました。現在では攻撃由来のログは BIG-IP、その他のログは Web サーバに記録されるため、問題発生時の切り分けも以前より容易になりました」（高橋氏）。

■SSL処理の集中化で証明書の管理負担も軽減

ネットプライスでは、SSL 処理も BIG-IP で実行している。これによって Web サーバの処理負荷と共に、SSL 証明書の管理負担も軽減しているのだ。また証明書の数を削減することで、コスト抑制にも貢献している。

WAF に関しては、現在はシグネチャにもとづく攻撃検知を採用しており、そのチューニングも行っている。今後はその手間を軽減するため、ASM が提供するシグニチャ以外の手法の活用も検討していくという。



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

2017年8月