

アピリッツがクラウド型WAFを選んだ唯一の理由

株式会社アピリッツ(以下、アピリッツ)は、ウェブサイトのSEOなどのコンサルティングからサイト開発、運用サポート、効果測定まで、顧客のウェブビジネスの運営をワンストップで提供しています。アピリッツがウェブ構築の上流工程から下流工程の各分野を安心してサポートする上で、外部からのウェブアプリケーションへの攻撃に対してきめ細かく検知・防御するWAF(Web Application Firewall)を顧客へ提案し、WAFの運用サービスを提供することは必然でした。そこで、海外製WAFを自社環境に設置し、運用してきたアピリッツでしたが、数年間の運用後に自社でのWAFサポートを断念し、デジサートのクラウド型WAFの再販に切り替えました。なぜ、アピリッツはクラウド型WAFを選んだのでしょうか。その理由は、たった1つ「WAFを手放し運転できること」でした。



<http://www.appirits.co.jp/>

業種：システムインテグレータ
課題：海外製WAFの運用負荷軽減
導入サービス：
シマンテック クラウド型WAF

株式会社アピリッツ

Webシステム開発・ECサイト構築・マーケティング支援などの「ビジネス事業」と、スマホアプリ・オンラインゲームなどの「エンターテインメント事業」を展開。創造・実証を掲げ、お客様に喜ばれるインターネットサービスをつくり続ける企業です。

非常に負荷の高い海外製ハードウェアWAFの運用

アピリッツはインターネットの黎明期より、ウェブサイトのシステム開発や運用を行っており、特に個人情報を多く扱う「求人サイト」の構築運用において多くのノウハウがあります。求人サイトの場合、安全なサイト運用を求められるため、WAFによる防御を前提としたシステム構築を提案する案件が多くありました。

このような背景から、アピリッツは2010年にWAFの月額サービス提供を開始しました。このサービスは、海外製のハードウェアWAFを冗長構成にし、アピリッツによる24時間365日運用監視を提供するサービスでした。また、アピリッツでは顧客サイトの定期的な診断も行っていました。診断で発見された脆弱性は、

ウェブサイトにパッチを当てたり、作り直したりすることで脆弱性の対策が求められますが、WAFをサービスとして提供し、その対策になるシグネチャをアピリッツが作成することで、ほとんどのウェブサイトの脆弱性は外部からの攻撃から守られることになりました。

ある大手保険会社グループの求人サイトに対しても、アピリッツは海外製 WAF を導入し、運用を行ってきました。しかし、この海外製 WAF では運用面に課題がありました。具体的な例をあげると、一般的な Firewall やサーバと異なり、海外製 WAF では再起動時に Master/Slave の切り替えが正常に行われないことが多々あったのです。年に 3-4 回発生するファームウェアアップデートについては、事前に手順書を作成し、リハーサルを行っているにもかかわらず、一度で正しくアップデートが行われずに、毎回サービス停止を伴うトラブルが発生していました。このような状況のため、メンテナンス作業は必ず深夜から早朝にかけて行っていました。

また、日本の環境では、海外製 WAF で初期設定されている防御ポリシーをそのまま運用すると、誤検知が発生することがありました。例えば、日本でのみ流通している日本製のスマートフォンやフィーチャーフォンから海外製 WAF 導入サイトへアクセスした場合、ブラウザの UserAgent が特殊なため、正常通信がブロックされることがありました。さらに、ファームウェアアップデートにより、文字長制限 (Length Check) のポリシーが強化されたために、以前は問題がなかった通信が急に遮断されることがありました。ファームウェアアップデートを行う際は、変更内容の確認、及び全設定パラメータのチェックが必要となり、多大なリソースが必要でした。

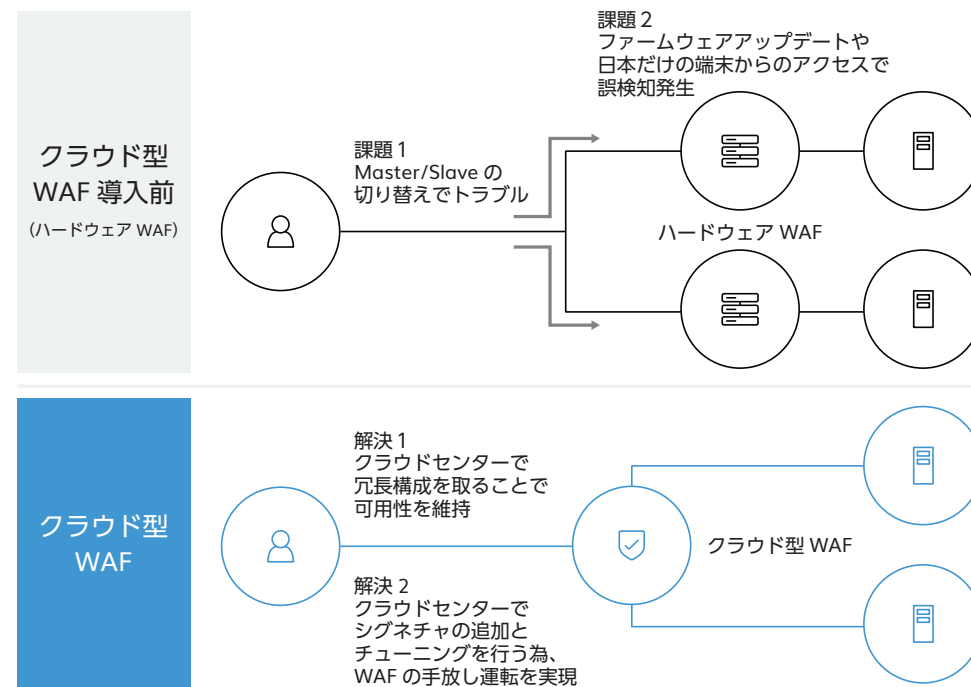


株式会社アピリッツ
執行役員
データインバージョン部長
西脇 学氏

アピリッツ 執行役員データインバージョン部長の西脇氏は、「WAF がエンドユーザの前面に設置されるため、WAF が停止するとサイト自体が停止になります。WAF のファームウェアアップデートだけでも手順書作成からリハーサルを事前に実施し、実際のアップデート作業は深夜早朝帯のメンテナンス時間で実施する必要がありました。そこまでしても、正常なアップデートができないケースが多々あったために、その度に原因調査に時間やリソースを割かれてしまい、非常に WAF 運用の負荷が高かったのです。そこで“手放し運転”ができる WAF サービスへの切り替えを検討せざるを得なかったのです」と話します。

クラウドWAFへのリプレースは 一か月で完了

2014 年より、アピリッツは代替となる WAF サービスの検討を本格的に開始しました。複数の代替サービスを検討したところ、実績が豊富で、運用までをまとめてアウトソースでき、既存顧客の満足度を維持できる「クラウド型 WAF」の紹介を受け、取り扱いに踏み切りました。海外製 WAF を導入していた大手保険会社グループの求人サイトでは、個人情報保護の観点から WAF の運用が必須となっており、ハードウェア WAF と同等以上の防御性能、パフォーマンスが求められていました。アピリッツでは、クラウド型 WAF の検証を実施し、約 1 ヶ月でリプレースを完了させました。



アピリッツ メディアサービス部 部長の鈴木氏は、「クラウド型 WAF の導入は思いのほか簡単でした。Hosts 型のテストなど、インフラの知識がない部門でも手順書に従えばテストや導入が可能なレベルです。また、手順書ではカバーできない当社システム固有の問題についても、メールでスムーズに対応いただけました。全体的に、非常に丁寧な導入支援でした」と感想を話します。また、前出の西脇氏は、「技術者の中でも、アプリケーション開発者とネットワーク運用管理者はノウハウが全く異なり、両立は難しいのです。開発者は総じて運用管理は苦手な傾向にあります。クラウド WAF は、ネットワーク運用管理者がアプリケーションセキュリティ管理をできるという点に大きなメリットがありました」と語ります。

エンジニアの運用負荷大幅削減により、TCO削減を達成

また、クラウド型 WAF 導入後の運用についても、「手放し運転」ができています。実際、アピリッツではクラウド型 WAF の保守に関しては、ほとんど時間をかけていないとのこと。西脇氏は、「エンジニアの運用負荷が大幅に削減できたため、TCO 削減できています」と話します。また、実際の運用業務を行うアピリッツ デジタルビジネス部 サイバーセキュリティラボの千葉氏は、「定期的にクラウド型 WAF の管理画面で、防御ログをダウンロードして内容を確認する程度で、それ以外の時間はかけていません」と、運用負荷が軽減したことについて述べています。

クラウド化を進めるにあたって「安心感」の補完

アピリッツでは、データセンタの仮想化など、所有から利用への移行を進めており、セキュリティもクラウド利用にシフトしたのは必然の流れと考えています。顧客に対して総合的にサービスを提供することを優先的に考えており、アピリッツ社の自社製のものを提供することには特にこだわっておりません。前出の西脇氏は、「クラウド化を進めるにあたって、お客様から求められるのは「安心感」です。これを実現するためにはクラウド型 WAF による安心感は強い味方であり、デジサートとますます連携を深めていきたいです。」と、今後の展望について熱く語っています。



株式会社アピリッツ
メディアサービス部
部長
鈴木 利夫 氏



株式会社アピリッツ
デジタルビジネス部
サイバーセキュリティラボ
千葉 正博 氏

デジサート・ジャパン合同会社

<https://www.digicert.co.jp> | 03-4560-3900 | websales_jp@digicert.com

DigiCert, Inc. All rights reserved. DigiCert, Geo Trust および DigiCert, Geo Trust のロゴは DigiCert, Inc の商標または登録商標です。シマンテック(Symantec)、ノートン(Norton)、およびチェックマークロゴの商標は Symantec Corporation のライセンスにもとづき使用されています。その他の名称もそれぞれの所有者による商標である可能性があります。