

URL一本化を機に、 運用ごと任せられる安心を選ぶ

Q：WAF導入のきっかけと、Ray-SOC WAFを選ばれた理由を教えてください。

施設ごとに個別のサーバーを立てていた方式から、AWS上のマルチテナント方式に移行したことが大きなきっかけです。URLが一本化され、多くのお客様が一つのFQDNに集約される中で、水際対策の強化が急務となりました。

仕組みを導入するだけではAWSのWAFでも対応できませんが、監視・運用まで自社で手が回らないのが実情でした。営業やサービス開発にリソースを集中させたい中で、セキュリティ運用まですべて自前で行うのは現実的ではありませんでした。

その点、Ray-SOC WAFはSOCによる監視・運用までセットの「オールインワン」サービスであり、価格もリーズナブルでした。トライアル期間に実際のアクセス状況を測定した上で本番導入に進められる流れにも、安心感がありました。

(こちらは抜粋版のため、詳細はWebサイトでご覧ください)

インタビュー対応者:株式会社マトリクス 代表取締役 小林孝弘様



AIだけでなく、人の目がある。 それが一番の安心感

Q：導入後に感じている効果を教えてください。

プッシュ型でレポートが送られてくるのが非常に重宝しています。何もしなくても「何か変なアクセスがありますが大丈夫ですか」と知らせてもらえるため、座って待っているだけで状況を把握できます。

アクセスの内訳まで可視化されたことも大きな付加価値でした。

当社のような小規模な企業でも相当数の攻撃が確認されており、ここ2~3年で日本への攻撃はさらに増加している印象です。

一番大事なのは、有資格者の方が人の目で確認してくださっている点です。AIだけでは誤検知の可能性もありますので、専門家がフィルタリングしてくれているという安心感は非常に大きいです。

Q：WAFの導入によって、社内や対外的な変化はありましたか？

医療機関のお客様から「セキュリティはどう対応されていますか？」と聞かれる機会が増えていますが、「専門の業者に24時間監視を委託しています」と回答できるのは大きな強みです。最近はずいぶん聞かれます。オンプレが主流の医療機関ではクラウド稼働時のセキュリティを懸念されるケースが多く、WAF導入を強力な対策としてご提示できるようになりました。WAFの導入はISMS認証取得の足がかりにもなったと感じています。



導入した当社のサービス



ホワイトハッカーの知見を学習させた独自AIエンジン (CloudCoffer AI Engine) 搭載のクラウド型WAFに、24時間365日の有人監視 (SOC) をセットにしたマネージドWAFサービスです。

ゼロデイ攻撃やAIを利用した高度な攻撃にも対応し、シグネチャベースのWAFでは防げない未知の攻撃パターンも高精度にブロックします。

導入はDNS設定の変更だけで完了。WAF運用、誤検知チューニング、DDoS対策、月次レポートもすべて標準で提供。ユーザー側の運用作業は不要です。

最大2ヶ月の無償トライアルでは、有償利用と同一品質のサポートを提供し、通信量の測定と最適プランのご提案まで行います。

月額 35,000円から (税抜)

※FQDN単位の価格設定。

通信量に応じた従量プランもご用意しています。

Webアプリケーションへの攻撃、 他人事ではありません。

IPAの調査によると、Webアプリケーションの脆弱性を狙った攻撃は年々増加し、医療・福祉分野も標的となっています。SQLインジェクションやクロスサイトスクリプティングなど、WAFで防御可能な攻撃が被害の大半を占めています。

「うちは小規模だから大丈夫」は、もはや通用しません。

株式会社レイ・イージス・ジャパン

© 2019 - 2026 Ray Aegis Information Security, Ray Aegis Japan, Inc. All rights reserved.

