NTTアドバンステクノロジ株式会社

AI技術を適用しSOCポータルのWAFチューニングを省力化、フォーティネット製品を活用し中核事業のSOCサービスを展開

NTT研究所で培った通信・ネットワーク技術やセキュリティ技術を生かしつつ、きめ細かなSOCサービスを提供しているNTT-ATでは、顧客とのコミュニケーションに用いている専用ポータルサイトにFortiWebを導入。AI技術を生かし、運用にまつわる煩雑な手間を省きつつ、セキュリティレベルを一段と向上させた。

導入・構築のポイント

(1) FortiWebのAI機能により、これまで手間がかかっていたWAFのバリデーションのチューニング作業を効率化した

(2) AI技術を活用したアンチボット機能により、通常とは異なる機械的なアクセスを検知し、アラートで把握できるようになった

(3) FortiWebだけでなくFortiGate、FortiMail、FortiSandboxといった一連のプロダクトを自社の仮想基盤上に構築し、包括的な対策基盤を構築した

NTTアドバンステクノロジ株式会社

本　　社 神奈川県川崎市幸区大宮町1310 ミューザ川崎 セントラルタワー
設　　立 1976年12月17日（昭和51年）
従業員数 1,865名
（2019年3月31日現在）

NTTアドバンステクノロジ株式会社 NWセキュリティマネジメントセンタ ICTサービスオペレーションセンタ センタ長
松本 公秀氏

NTTアドバンステクノロジ株式会社 NWセキュリティマネジメントセンタ ICTサービスオペレーションセンタ 主任技師
吉野 浩史氏

NTTアドバンステクノロジ株式会社 NWセキュリティマネジメントセンタ ICTサービスオペレーションセンタ 主査
鎌田 理氏

1976年に設立され、NTT研究所で培った通信・ネットワーク技術やセキュリティ技術を世の中に広めていくことをミッションに事業を拡大してきたNTTアドバンステクノロジ（NTT-AT）。最近はクラウドやAI、ロボティクス技術に力を入れており、RPAツール「WinActor®」は国内シェアナンバーワン*を誇っている。

さらに、力を入れているのがセキュリティ事業だ。「NTTグループの技術的中核企業として、もともとネットワーク運用技術に強かったところにセキュリティ人材が加わり、NTTグループ内のセキュリティ対策業務を担ってきた実績をもち、セキュリティ診断、コンサルティング、構築のほか、セキュリティオペレーション（SOC）運用支援サービスを展開しています」（NTT-AT NWセキュリティマネジメントセンタ ICTサービスオペレーションセンタ センタ長 松本 公秀氏）。セキュリティ機器を導入したものの大量のログを見て分析するところまで手が回らない、という企業の悩みに応えてきた。

SOCサービスの顧客向けポータルサイトを一段高いレベルで保護

NTT-ATのSOCサービスではフォーティネットの次世代ファイアウォール／UTM製品「FortiGate」をはじめ、さまざまなセキュリティ機器の監視・分析を24時間365日体制で実施している。「テンプレート通りの機械的な対応ではなく、お客様に寄り添いながら柔軟に対応し、信頼関係を築いています」（NTT-AT セキュリティ事業本部 辻 聡史氏）

顧客とのコンタクトポイントとなっているのがSOCサービス専用のポータルサイトで、ここを通してさまざまな問い合わせやリクエストにきめ細かく応えてきた。

基本的に、このポータルサイトにはNTT-ATのSOC担当者と顧客しかアクセスできない。加えて、「お客様のセンシティブな情報を保有するポータルサイトに万一のことがあってはいけない」という考えから、OSやポータルアプリケーションのミドルウェアへのパッチ適用といった基本的な対策に加え、FortiGateによる防御も導入し、セキュリティ向上に努めてきた。

しかし「最近のサイバー攻撃の動向を見ると、無差別にWebサイトの脆弱性を探索するような動きも増えています。全社的にもう一段セキュリティレベルを上げていく中で、新たな脆弱性が発覚した際、サーバ側で修正対応するまでの間、攻撃を止められる手段が必要だと考え、Web Application Firewall（WAF）を導入することにしました」（NTT-AT NWセキュリティマネジメントセンタ吉野 浩史氏）

NTT-ATは以前からフォーティネットのパートナーとして、FortiGateのほか、FortiMail、FortiSandbox、FortiAnalyzerやセキュリティファブリックの検証を実施してきた。「ちょうどFortiWebの検証も検討していたタイミングで、ポータルサイトでのWAF導入の話が持ち上がったことから、実環境で

NTTアドバンステクノロジ株式会社 NWセキュリティマネジメントセンタ ICTテクニカルセンタ 主任
相場 崇氏

NTTアドバンステクノロジ株式会社 セキュリティ事業本部 マネージドサービスビジネスユニット 副主任技師
辻 聡史氏

の検証も兼ねて導入することにしました」（NTT-AT NWセキュリティマネジメントセンタ 相場 崇氏）

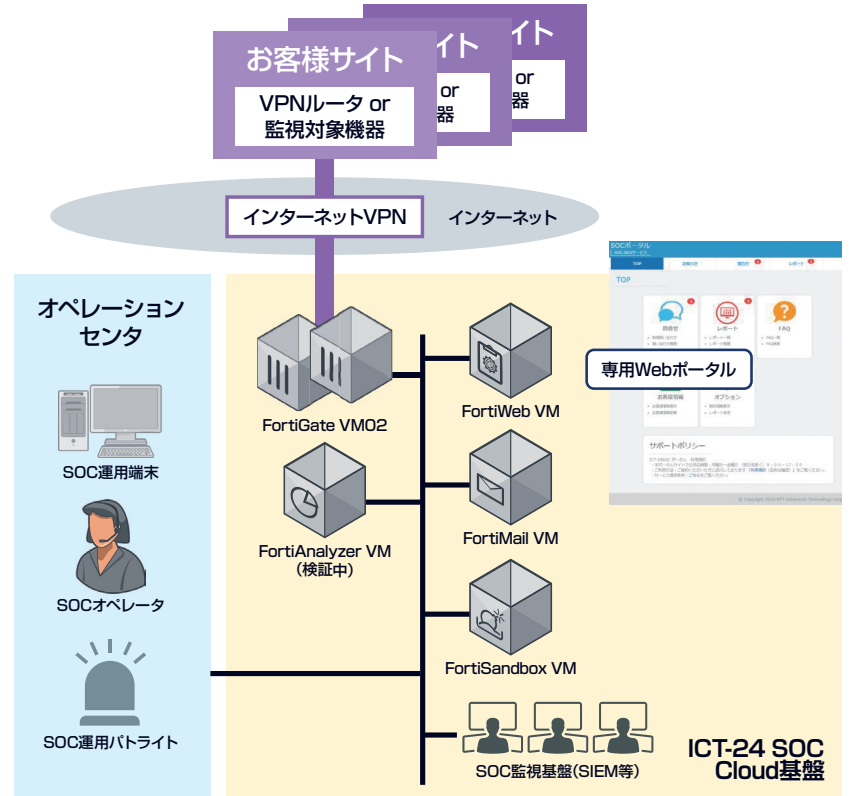
優れたコストパフォーマンスに加え、NTT-ATが着目したのがFortiWebのAIによるチューニング機能だ。「一般にWAFは、ログを見ながらどんな通信をブロックすべきかチューニングしていかないと、どうしても過検知や誤検知が発生してしまうため、運用に非常に手間がかかります。日々新たな脆弱性が発覚するため、昨日まではよくても、明日はよくない、という判断に変わることもあります。その部分を自動化できないかと常々考えていました」（吉野氏）

AIの活用で手間のかかっていたWAFチューニングを効率化

NTT-ATでは2018年11月から顧客向けポータルサイトでFortiWebの検証を開始した。NTT-AT NWセキュリティマネジメントセンタの鎌田 理氏は、「すでにFortiGateを使っていたこともあってユーザーインターフェイスに慣れていたので、導入、運用もすんなりいきました」と述べる。

検証のポイントだったAIによるバリデーションのチューニングは、期待通りの効果を見せている。「以前はスキルを持ったエンジニアが1つ1つパラメータを確認し、実装し、テストして……と非常に手間がかかっていました。AI機能を活用すればボタン一つで簡便にセキュリティレベルを上げることができ、有益な機能だと評価しています」（相場氏）。そこに費やしていたエンジニアのリソースを、より手厚いサービスに振り分けられるのではないかと期待している。

また、明確にNGと判断できる不正アクセスとは異なり、ボットによる機械的なアクセスを検知するのは一般には困難だ。だが「AIを用いたFortiWebのアンチボット機能も評価しましたが、トラフィックのアノマリーを検知し、通常のユーザーとは異なる振る舞いとしてアラートを出してくれています」（相場氏）。2019年12月の本格稼働以降も、学習したトラフィックパターンに対する最適な閾値を模索しつつ、セキュリティレベルの向上に努めている。



専門家のナレッジとAIの相乗効果で付加価値の高いセキュリティサービスを

セキュリティビジネスを重点分野の1つと位置付けているNTT-ATでは、今後もさらにSOCサービスを拡充していく。ポータルサイトでのノウハウを踏まえ、顧客向けにFortiWebのマネージドサービスを提供していくことも検討しており、その意味で、フォーティネットの各製品のさらなる連携に期待しているという。

「長時間ログを監視したり、大量のデータを解析したりといった部分にはAIや機械学習、深層学習といった技術をどんどん活用して効率化しつつ、最終的に必要になる人手による判断や遮断対応といった部分では、われわれのスキルや経験を生かし、より付加価値の高いサービスを提供していきます」（吉野氏）

*出典：ミック経済研究所2019年10月発刊「驚異的な拡大続くRPAソリューションの市場動向2019年度版」

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ