「ゼロトラストセキュリティ」の実現に向け 信頼の脅威情報で標的型攻撃への防御を固める

ビジネス成長を阻むセキュリティリスクを最小化するために

世界中で愛されるポケモン。そのプロデュースをする企業が、株式会社ポケモン（以下、ポケモン社）だ。ポケモンのゲームソフトやカードゲームのプロデュースをはじめ、映画・映像の制作、キャラクターグッズの監修・企画・制作、各種イベントの開催、オフィシャルサイトの運営などを手がけている。また、傘下の The Pokémon Company International と Pokémon Korea, Inc. などとともに、全世界におけるポケモンブランドの管理も担う。

こうしたポケモン社にとって、その成長のスピードを鈍化させかねないリスクと言えるのがサイバー攻撃の脅威だ。その点に関して、同社のテクニカルディレクターとして社内情報システムを見ている関 剛氏は次のように指摘する。

「標的型攻撃に代表される今日のサイバー攻撃は実に巧妙で高度です。社内ネットワークとインターネットとの境界線の防御をいくら高く積み上げても、攻撃による脅威の侵入を 100%阻止するのは至難でしょう。とはいえ、その攻撃から機密情報を守るすべを確立しなければ、ビジネスを安全にスケールしていくことはできず、情報漏えいによってポケモンのブランドを毀損してしまうリスクは低減できません。攻撃への備えを整えることは、極めて重要なビジネス課題と言えました」

究極のゴールは“ゼロトラストセキュリティ”

関氏によれば、ポケモン社における働き方の特性は、情報セキュリティが確保しやすいものでは決してないという。

例えば、同社の社員は、出張・イベント・店舗など、拠点外で働くことが多くあり、リモートから社内ネットワークへのアクセスを頻繁に発生させる。また、ビジネスパートナーの数も非常に多いうえに、それぞれの IT に関するセキュリティ基準も異なる。加えて、ポケモン社の事業では、数多くの情報を扱う。そのため、情報ごとに細かくアクセス権限を分けて、厳格に管理していく必要もある。

こうした中で、2017 年に社内情報システムを担当することになった関氏は、認証基盤の整備と SSO（シングルサインオン）の導入によって不正アクセスに対する防御を固めた。また、第三者機関によるセキュリティリスクアセスメントも実施し、社内情報システムに潜在するリスクも洗い出したという。

「結果として、リスクは何も発見されず、喫緊（きっきん）のリスク対策として、ランサムウェア対策（端末のデータのクラウドバックアップ）などを講じました。ただし、リスクが発見されなかったからと言って、それで標的型攻撃への備えが万全という証明にはなりません。今後は、標的型攻撃や機密情報の抜き取りを、早期に検知して未然に防ぐことが重要になっていくと感じました」（関氏）。

こうして、サイバー攻撃への備えについて考えを巡らした結果、関氏がたどりついた答えの一つが、「ゼロトラストセキュリティ」の実現だった。

「サイバー攻撃の高度化によって境界型の防御に限界が見えている以上、ネットワークを信用するエリアと信用しないエリアに分けて、セキュリティを担保するという従来型の手法は通用しなくなっているはずです。となれば、必要なのは、あらゆるエリアからのアクセスも信用せず、全てについて検査・認可・認証の制御をかけていくことです。つまり、ゼロトラストの考え方が今後は必要だということです」と、関氏は説く。

もっともゼロトラストセキュリティにも課題はあると、同氏は語り、こう続ける。

「このセキュリティモデルの最大の懸念は運用負荷の増大です。社内情報システム部門の人的リソースには限りがあり、新たなセキュリティ対策によって運用負荷が高まるような状況は避けなければなりませんでした」

The Pokémon Company

COMPANY
株式会社ポケモン
本社　：〒 106-6108
東京都港区六本木 6-10-1
六本木ヒルズ森タワー 8F
資本金　：3 億 6,540 万円
設立　：1998 年 4 月
https://www.pokemon.co.jp/corporate/

INDUSTRY
メディア & エンターテインメント

SOLUTIONS
- Enterprise Threat Protector（ETP）

KEY IMPACTS
- 標的型攻撃に“気づけない”不安を潜在脅威の見える化で解消
- セキュリティ運用の負荷を減らしながら、標的型攻撃対策を実現
- 「Enterprise Application Access（EAA）」の追加導入も計画。ゼロトラストセキュリティの実現へ

<株式会社ポケモンについて>
1998 年 4 月に、任天堂とクリーチャーズ、ゲームフリークの 3 社の共同出資によって設立された。設立当初の社名はポケモンセンター株式会社。のちの 2000 年 10 月に現社名に変更し、手がける領域をポケモンのブランドマネジメント全般に拡大させた。現在は、ポケモンのゲームソフト、アニメ、カードゲーム、映画、ならびに関連キャラクターグッズのプロデュースと販売、ライセンス管理を手がけ、ポケモンオフィシャルサイトなどの運用も担う。子会社に、ポケモンセンター等のオフィシャルショップの運営を担う株式会社ポケモンセンターや、北米や欧米などアジア地域以外のポケモン事業を担う The Pokémon Company International、韓国での事業を担う Pokémon Korea, Inc. などがある。

株式会社ポケモン　プロダクト本部 システム部／
テクニカルディレクター インフラエンジニア　関 剛氏（左）
株式会社ポケモン　プロダクト本部 システム部　マネジャー
井上 絵美子氏（右）

株式会社ポケモン

最小限の運用負荷で潜在脅威の見える化と抑止

運用の負荷増を最小限に抑えながら、ゼロトラストセキュリティの実現に向けた環境を整えていく――。この課題を一挙に解決しうるセキュリティソリューションとして、関氏が注目したのが、アカマイの「Enterprise Threat Protector（ETP）」と「Enterprise Application Access（EAA）」だった。すでに、ETP については導入をすませ、EAA についても、導入の準備を進めている。

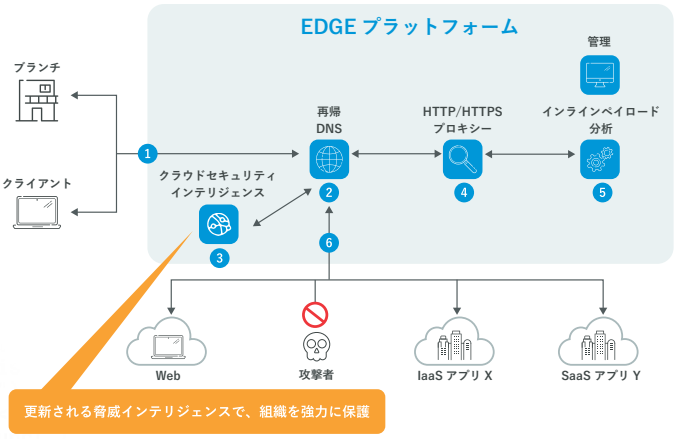
ETP は、アカマイが保持する膨大な脅威インテリジェンス（脅威情報）によって、不正な DNS クエリをブロックするクラウドセキュリティソリューションだ。社内の端末から不正サイトや C&C サーバへの接続を未然に防ぎ、フィッシング、マルウェア侵入、情報の窃取といった標的型攻撃による実害の発生を阻止することができる。

「ETP で優れているのは、DNS サーバへのクエリの向け先を ETP のアドレスに変更するだけで利用が開始できる簡単さです。しかも、クラウドサービスなので、運用に手間がかからず、社外の端末でも同じセキュリティレベルが確保できます」と、関氏は評価し、こう付け加える。

「おそらく、アカマイのサーバは、インターネット上で最も普及しているデバイスでしょう。ゆえに、アカマイのもとに集められる脅威情報は世界で最も多いはずで、その脅威インテリジェンスは全幅の信頼に値するものと見ています」（関氏）。

また、ETP を日々の運用で活用しているポケモン社の井上 絵美子氏は、関氏の言葉を裏づけるように次のように話す。

「ETP 導入でセキュリティ運用はかなり楽になりました。例えば、何らかのインシデントが起きた場合、通常では、異なる機器からのログを照らし合わせて、分析するといった作業が必要ですが、ETP ではそのような作業をする必要は全くなく、その管理画面を通じて、社内ネットワークでいま、何が起きているかが直感的に把握できます。ETP のおかげで、セキュリティ運用のことを意識する必要すらなくなったように感じています」



Akamai ETP サービス提供イメージ

「アカマイのソリューションの信頼性は CDN でよく知っていたので、ETP の採用にも迷いはありませんでした。その判断は正解だったと今でも感じています」（関氏）

「ETP で減らせた分のリソースを、他のセキュリティ対策の強化に投入できるようになったことが、ETP 導入の最大の効果だと考えています」（井上氏）

さらに、井上氏は ETP をこうも評価する。

「とにかく、ETP は管理画面がシンプルなので、他のメンバーに、画面のどこを、どう見れば、何がとらえられるかが簡単に説明できます。ドリルダウンなどの操作によって、目的の情報にたどりつくのも容易ですし、どのユーザーが不正なサイトにアクセスしようとしたかといった情報も可視化できています。ですので、インシデントに対するプロアクティブな対処も可能になっています」

EAA の採用でゼロトラストへ向けさらに前進

一方、ポケモン社が、導入を予定している Akamai EAA は、クラウド上に提供される「ID 認識型プロキシ」だ。ID 管理、認証、認可、暗号化通信を一元的に提供する。これにより管理者は、SaaS、IaaS、オンプレミスへのアクセス制御をクラウドから集中管理し、安全な環境を実現することができる。SSO 機能を提供するほか、二要素認証・アクセス元の IP アドレスや国など詳細な制御も可能としている。

「この EAA によって、運用管理に手間のかかる VPN が廃止できますし、社内リソースへのリモートアクセスの高速化も期待できます。ETP で標的型攻撃対策を固めて、EAA でリモートアクセス制御の環境を整える。これによって、ゼロトラストセキュリティの実現に大きく近づけると考えています」（関氏）。

ポケモンのビジネスをセキュアに、よりスピーディに成長させる。そのための整備は着実に前に進んでいる。

アカマイ・テクノロジーズ合同会社 ［英文名：Akamai Technologies GK］ email：info_jp@akamai.com HP：https://www.akamai.com/jp/ja

東京本店 〒104-0031 東京都中央区京橋2-1-3 京橋トラストタワー Tel：03-4589-6500 Fax：03-4589-6501