

株式会社ベガルタ仙台



所在地：宮城県仙台市青葉区本町3-6-16
URL：https://www.vegalta.co.jp/

CrowdStrike Falcon プラットフォーム で エンドポイントセキュリティを強化 運用効率化とコスト削減に成功

[BEFORE]

- ◆現状のエンドポイント対策が適切かどうか不安が残る
- ◆オンプレミスの管理サーバーの運用管理負荷が重い

[AFTER]

- ◆未知の脅威やファイルレス攻撃などにも対処できるセキュアな環境を実現
- ◆クラウド型ソリューションへの移行により運用管理負荷の軽減に成功

東北を代表するJリーグクラブとして 地域貢献に向けた活動も 意欲的に展開

東北エリアを代表するJリーグクラブとして知られるベガルタ仙台。2024年に設立30周年を迎えた同クラブでは、地域のファン・サポーターの期待に応えるべく、日々熱い戦いを繰り広げている。

ベガルタ仙台 経営企画部長 兼 スタジアムパーク構想推進室長 磯田 敦氏は「発足にあたり約33万人もの署名が集まるなど、当クラブはまさに市民の思いから生まれたプロサッカークラブです。それだけに、勝利を目指すのはもちろんのこと、地域貢献に向けた活動も重要な使命だと考えています」と力強く語る。



株式会社ベガルタ仙台
経営企画部長
兼 スタジアムパーク構想推進室長
磯田 敦氏

そうした取り組みの一つが、現在推進中の「スタジアムパーク構想」だ。ここでは、ホームスタジアムであるユアテックスタジアム仙台を中心とした泉中央地区を舞台に、街のにぎわいを創出できる方法を模索中。磯田氏は「せっかくスタジアムという場があるわけですから、ゲームが無い日も人々が集まるような環境を目指したい。様々な取り組みを通して、地域と一緒に盛り上がってほしい」と意気込みを語る。こうした同クラブの

姿勢は、地域と共に歩むJリーグの理念を体現するものと言えるだろう。

ランサムウェアなどの脅威に備えるべく エンドポイントセキュリティの 見直しに着手

このような多面的な活動を展開する同クラブだが、日常的な業務については一般企業とさほど大きな違いはないという。磯田氏は「プロサッカークラブと言えども、企業活動に必要な機能は他の会社と変わりありません。当部門が中心となり、総務や人事、財務などのバックオフィス業務全般を担当しています」と説明する。特に近年では、情報セキュリティの強化に力を入れているとのこと。磯田氏は「当クラブに限らず、プロスポーツチームには高い公共性／公益性が求められます。万一、重大なインシデントが発生するようなことがあると、ステークホルダーの方々にもご迷惑をお掛けすることになりますので、細心の注意を払ってセキュリティ対策に取り組んでいます」と続ける。

その一環として今回取り組んだのが、エンドポイントセキュリティの強化である。磯田氏はその背景を「サイバー攻撃の脅威は年々増しており、ランサムウェアによる被害なども数多く報道されています。そこで、現状のエンドポイント対策に問題はないか、今一度見直す必要があると考えました」と語る。

見直しにあたってのポイントとしては、まず社外で使われる端末の確実な保護が挙げられる。ベガルタ仙台 経営企画部 総務課 主任 金森 隼平氏は「Jリーグの試合は全国で行われますし、海外へ遠征するケースもあります。必然的にスタッフが外出先で端末を使う機会も増えますので、これをきちんと守れることが求められました」と語る。



株式会社ベガルタ仙台
経営企画部 総務課
主任
金森 隼平氏

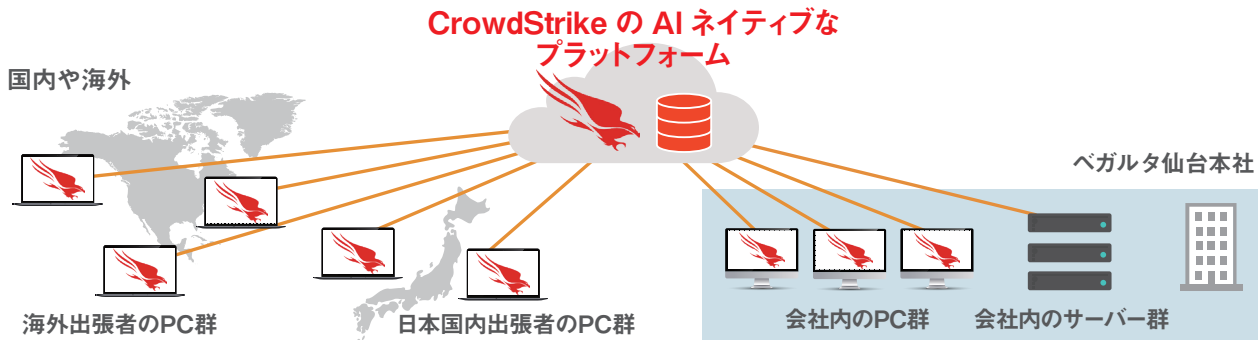
もう一つのポイントが、運用管理負荷の軽減だ。金森氏は「当クラブには専任の情シス部門がありませんので、我々総務部門でIT関連の業務も行っています。しかし、既存のセキュリティ製品は、PC入れ替え時の設定作業などが煩雑な上に、管理サーバーを自前で運用する必要もありました」と続ける。

グローバルでの実績を評価し CrowdStrike Falconを採用

こうした課題を解消できる製品として、新たに採用されたのが、ネットワークが提供するクラウドストライク社のセキュリティプラットフォーム「CrowdStrike Falcon」である。

「ITパートナーのイベントに参加した折に、

CrowdStrike Falcon で場所や環境問わずあらゆるエンドポイントを強力に保護



海外や国内の出張やリモートワークが多い社員のPC環境も、会社内のPCとサーバー環境も、トータルに保護

導入メリット

- ・世界中29,000社以上の導入企業から信頼された検知・防御力と最高峰の脅威情報による保護
- ・クラウドサービスで、サーバー管理やパターンファイル更新不要で、管理者と社員双方の負担軽減に
- ・攻撃を防御した際の侵入経路や原因特定もグラフィカルに表示されるため、把握が容易

CrowdStrike Falconの紹介を受けました。詳しく内容を聞いてみると、グローバルでトップシェアを誇るセキュリティ製品とのこと。世界中の企業で導入されているということは、製品の安全性を証明するものと言えます。また、クラウド型のソリューションであるため、既存製品のように社内に管理サーバーを立てる必要もありません。これは非常に優れたソリューションだと感じましたね」と金森氏は振り返る。

CrowdStrike Falconには数多くの機能が用意されているが、今回同クラブではNGAV(次世代アンチウイルス)の「Falcon Prevent」を導入。この機能はパターンファイルを利用する従来型のアンチウイルス製品と異なり、機械学習や振る舞い検知などの技術を用いて脅威への対処を行う。このため、未知のマルウェアやファイルレス攻撃などの確に検知・防御することが可能。パターンファイルの定期的な更新やフルスキャンなどの作業も一切不要である。「端末側にもエージェントを一つインストールするだけですから、社内展開も特に苦労することなく進められました」と金森氏。この結果、2024年4月より無事本番稼働を開始している。

セキュリティ運用には大きな改善効果が現れている。「まず一つ目は、社員が快適に端末を利用できるようになった点です。以前の環境では、不要なポップアップ通知がしばしば表示されており、業務の妨げになっていました。基本的には問題のないものばかりなのですが、やはりポップアップが通知されれば不安ですし、我々管理者側にも対応負荷が生じます。その点、CrowdStrike Falconは過検知・誤検知が少なく、ほとんど不要なポップアップを出しません」と金森氏は語る。また、磯田氏も「動作が非常に軽快な点も良かったですね。以前はPCの動作がもたつようなケースもありましたが、現在ではこうしたことを全く感じません。おかげで普段はセキュリティのことを意識せずに済むようになりました」と続ける。

加えて見逃せないのが、運用管理負荷を軽減できた点だ。管理サーバーの面倒を見る必要がなくなった上に、各種の設定作業などもコンソールから簡単に行うことができる。「旧環境で手間の掛かっていたPC入れ替え時の作業なども、格段に楽に行えるようになりました」と金森氏。しかも、これだけのメリットを得られた一方で、導入・運用に掛かるコストは以前より下がったとのこと。磯田氏は「セキュリティの見直しに踏み切った甲斐がありました」と満足感を示す。

今回の取り組みを支援したネットワークに

も、高い評価が寄せられている。「我々もITやセキュリティの専門家ではないので、どのような設定が適切なのかなかなか判断が付きません。幸い、今回はネットワークが丁寧にアドバイスしてくれましたので、スムーズに実運用にこぎ着けられました。この点には大変感謝しています」と金森氏は語る。今後は製品の使いこなしに務めると共に、EDRなど他の機能の活用も検討していく考えだ。「日本一のJリーグクラブを目指す上では、しっかりとした企業基盤が欠かせません。我々も『縁の下力持ち』として、チームの勝利に貢献していきたい」と抱負を語る磯田氏。その同クラブの安心・安全を、ネットワークとCrowdStrike Falconが下支えしていくのである。

お問い合わせ

株式会社ネットワーク

<https://www.networkworld.co.jp/>

✉ crowdstrike-info@networkworld.co.jp

本社 〒101-0051 東京都千代田区神田神保町 2-11-15
住友商事神保町ビル
TEL : 03-5210-5020,5031,5095

関西支店 〒530-0001 大阪市北区梅田 3-3-20
明治安田生命大阪梅田ビル 24F
TEL : 06-7777-4174

中部支店 〒450-0003 名古屋市中村区名駅南 1-17-23
ニッパビル 10F
TEL : 052-588-7611

九州支店 〒812-0013 福岡市博多区博多駅東 2-6-1
九勤筑紫通ビル 3F
TEL : 092-461-7815

安全で快適な業務環境を実現 運用管理負荷軽減にも成功

CrowdStrike Falconの導入後、同クラブの