PROTECTORS
STORIES

CrowdStrikeお客様事例

# 株式会社 博報堂プロダクツ

## 『そばにスペシャリストがいる感じです』深い調査から修復まで完璧に対応するMDRでエンドポイントを脅威から保護

### CrowdStrike Falconプラットフォームを導入するもSOCのスコープと社内運用負荷に課題

株式会社 博報堂プロダクツは、総合制作事業会社だ。同社の各コア事業が追求している専門技術（＝こしらえるスキル）と、売り場における生活者心理や流通動向などの知見（＝売りのノウハウ）を掛け合わせ、デジタルテクノロジーで「こしらえる」を進化させ、主軸事業であるプロモーション領域を拡張し続けている。

同社では、クリエイターを始めとする多様な業務を行う社員が存在し、Windows PCとMacを利用し業務を進めている。その割合は3:2であるといい、社内全体ではその数 約4,500台に上る。エンドポイントの保護については、アンチウイルスソフト（AV）を利用していた。しかし、そこにいくつかの課題が浮上するようになった。アンチウイルスがマルウェアを見つけて隔離するが、隔離されたから大丈夫で終わって良いのか、AVだけでは前後関係もわからず何も手を打てない、そして新しいサイバー脅威に対応できるのかという点である。頼みの綱がシグネチャのみというのも懸念だった。

そうした中、クラウドストライク製品の話を聞き、導入を決断する。株式会社 博報堂プロダクツ 情報システム室 室長代理 木本 邦史氏は、その理由を次のように語る。

「クラウドストライクはEDRの概念をわかりやすく説明いただきました。アンチウイルスソフトとどう違うのか、メリットだけではなくデメリットがどこにあるのかもクリアにイメージできました。自分たちはエンドポイント保護の考え方を根本から改めなければいけないと思いました。クラウドストライク製品を導入することで、既存のAVの様にパターンファイルができるのを待つ必要がなく、今まで抱えていた課題が解決できることも理解できました」

クラウドネイティブで構築されたクラウド環境から提供されるSaaSであることも魅力でしかなかったという。

製品は、CrowdStrike Falcon® Prevent（次世代アンチウイルス）、CrowdStrike Falcon® Insight XDR（EDR）、CrowdStrike Falcon® Adversary OverWatch（プロアクティブな脅威ハンティング）3モジュールを導入することを決定した。日々の運用については心配が残った。セキュリティ分野は専門性を問われるため、外部SOCの協力を得ることにした。導入運用を開始したのは2019年10月のことだ。

しかし、まもなく外部SOCサービスの運用上の懸念が複数明らかになる。一つは、月次で報告される定期レポートに情報の不足を感じたことである。見たい角度での情報が盛りこまれていなかった。もう一つは、作業スコープだ。一般的なSOCでは「検知しました。ブロックします」といった一次作業は担うが、それ以上は顧客の責任になりがちだ。その後の分析調査、対応などは情報システム室で実施しなければならないため結局人手が必要となる。こうした作業の負担が非常に重く、何のために外部SOCを導入しているのかといった疑念が沸いた。さらにもう一つは、それらが“機械的な対応”であることだった。あるソフトのファイルパスを保護対象からはずしたいと申し出ると、それはそのまま受け入れられた。インシデントの原因がうまく特定できないと、提案されるのは決まってOSの再インストールだった。

### クラウドストライクがMDRを提供 CrowdStrike Falcon® Completeへ切り替えを決断

情報システム室では、博報堂グループ全体でOffice 365導入が決まったこともあり、ゼロトラストネットワーク構築に向けて動き出していた。コロナ禍を契機に在宅勤務が一気に進んでおり、ユーザーがSaaSを含めさまざまなリソースを安心・安全に利用できるよう支援する必要があった。エンドポイントにはクラウドストライク製品が入っている、そして新たにSASE（Secure Access Service Edge）ソリューション Netskopeの導入を2023年3月に決定した。

少数精鋭主義が前提である情報システム室において担わなくてはならない製品が増えた中、外部SOCサービスによるクラウドストライク製品の運用について全面的に見直しをかけることにした。

クラウドストライクでも24時間365日体制の専門家によるMDR（Managed Detection and Response）を提供している、しかもこのCrowdStrike Falcon® Complete であれば、今まで運用してきた3モジュールにITハイジーンを提供するCrowdStrike Falcon® Discoverも加わり、MDRに一次作業のみならず、二次作業、三次作業といった調査の深掘り部分から対応までも任せられることがわかった。情報システム室は、こちらへ切り替えることを即断した。木本氏は次のように語る。

「製品のことを一番よく知っているベンダーが、直接すべてのスコープをカバーしてくれることに大きな安心感がありました。また、Falcon Completeは、想定よりも安価に契約できました。選ばない理由がありませんでした。」

## ・PRODUCT'S・

### 業種
総合制作事業会社

### 所在地
東京都江東区豊洲5-6-15
NBF豊洲ガーデンフロント

**株式会社 博報堂プロダクツ**

「こしらえる」という創業以来の武器を手に、専門性と実施力で勝負する総合制作事業会社、博報堂プロダクツ。8つの事業領域をベースに18の事業本部と3つの支社、11のグループ会社から構成されている。デジタル時代の現在、同社はデジタルテクノロジーで「こしらえる」を進化させ、5年、10年、その先も成長し続けるために、主軸事業であるプロモーション領域を拡張し、専門性のさらなる強化に取り組んでいる。

https://www.h-products.co.jp/

### 導入サービス
- CrowdStrike Falcon® Complete MDR 含まれるコンポーネント
  - CrowdStrike Falcon® Prevent 次世代アンチウイルス
  - CrowdStrike Falcon® Insight XDR EDR
  - CrowdStrike Falcon® Discover ITハイジーン
  - CrowdStrike Falcon® Adversary OverWatch プロアクティブな脅威ハンティング

導入時期：2019年10月


**クラウドストライクのMDRはそばに**
**スペシャリストがいるような運用体制を実現、**
**情シス内の工数は1/6に**

Falcon Completeでの運用は、2023年9月から始まった。このときから情報システム室側での作業は、管理画面でクラウドストライクによる対応を把握・確認するのみになった。株式会社 博報堂プロダクツ 情報システム室 情報システム部 ITサービスデザインチーム チーフITプロデューサー 石森 圭氏は、導入効果を次のように語る。

「運用にかかる時間が目に見えて減少しました。今まで8時間の勤務時間のうち毎日2〜3時間はかかっていたのが、画面で対応を確認するだけになり30分以下になりました。工数でいえば1/6になっています。しかし、これは日々の情報システム室だけの工数の話です。今まで対応修復作業でOSの再インストールとなると、ユーザーにデバイスを送ってもらい、こちらからは代替のデバイスを送る、別の部隊にキッティングを頼むといった具合に、いろいろな関係者を巻きこんでいました。これは会社全体で工数がかかっていました。それらが解消されたのは非常に大きな効果です」

株式会社 博報堂プロダクツ 情報システム室 情報システム部 ITサービスデザインチーム ITプロデューサー 杉山 祐貴氏は、「Falcon Completeの担当者は常に最善を考え提言をくれます。あるソフトのファイルパスを保護対象から外したいとお伝えした際に、『すべてを除外するのは危険であるためお勧めできません。もう少し範囲を絞りましょう』との返答がありました。」とFalcon Completeチームの取り組み姿勢を評価する。

定性的効果については、株式会社 博報堂プロダクツ 情報システム室 情報システム部 ITサービスデザインチーム ITプロデューサー 堀田 果梨氏がこのように語っている。

「クラウドストライクのMDRエンジニアによるサポートは、社内にスペシャリストがいるような心強さを感じます。また、対応が四角四面ではなく、メールの文面一つとっても、こちらの状況を把握し的確に内容が記されています。長くIT業界にいて、サポートとは機械的なものと思ってきましたが、そうではないサポートがあると知り、とても衝撃を受けました」

杉山氏と堀田氏にはさらに忘れられないエピソードがある。

「簡単に原因の特定できないインシデントが発生したとき、『今すぐZoomで会話できますか』というメールが送られてきたときは、心からびっくりしました。そんなことまでもクラウドストライクのMDRで可能だとは思いもしませんでした」（堀田氏）

「その時点でもう夜の8時ぐらいでした。『明日に持ち越すのではなく、もう少し調査させてください』というご連絡であり、調査を続け解決に至りました。彼らの熱心さを感じる出来事でした。またFalcon Completeは脅威レベルLowを含めてすべてを確認するMDRサービスでもあり、だからこそ全幅の信頼を置いています」（杉山氏）

**知らぬ間に強固なセキュリティを実現している**
**Netskope連携**

FalconプラットフォームはNetskope製品とさまざまな連携が可能だ。博報堂プロダクツでは、API経由でIOC（Indicator of Compromise）の共有自動化と双方向更新を行うNetskope Cloud Threat Exchangeを通じたほぼリアルタイムの脅威情報の取り込みをおこなっている。Falconプラットフォームで検知した脅威情報はNetskopeにも適用され、逆にNetskope側で検知した脅威はFalconプラットフォームにも適用される。これにより、ファイルハッシュや悪意あるURLを無効化するなどのセキュリティ対策を改善する効果がある。Netskope上の設定を有効化するだけで実現できる連携の容易さも評価された。

両製品による多層防御に加えこの連携によっても、安心感を得ているという。

**現状の足固めをしつつ**
**今後のさらなるセキュリティ強化に向かう**

今後、情報システム室では、Falcon Complete導入で新しく加わったITハイジーン製品であるFalcon Discoverを、もう一歩踏みこんだ形で活用していきたいそうだ。NetskopeとFalconプラットフォームの更なるゼロトラスト連携機能の活用なども検討し、導入しているソリューションのより効果的な運用を目指す。

それ以外に企業全体のセキュリティ対策を考えた際には、クラウドセキュリティポスチャ管理CSPM（Cloud Security Posture Management）の必要性も見えてきたという。石森氏は次のように語る。

「クラウドでのアプリケーション構築の際、最低限のガイドラインは用意していますが、ドキュメントのガイドラインというのはなかなか読んでもらえません。そのため、担当者によって設定が異なってしまう、担当者の力量に依存している状態のためそれを平均化したいと考えています。CSPMを入れることによって、セキュリティの点数が何点以上ならリリース可能といった具合に、しくみとして安全を組みこめるようになることも今後検討しています」

博報堂プロダクツでは、企業と社員を守るため今後も自社の状況に合わせセキュリティ対策の改善、推進を検討されている。

株式会社 博報堂プロダクツ
情報システム室 室長代理
木本 邦史 氏

株式会社 博報堂プロダクツ
ITサービスデザインチーム
チーフITプロデューサー
石森 圭 氏

株式会社 博報堂プロダクツ
ITサービスデザインチーム
ITプロデューサー
杉山 祐貴 氏

株式会社 博報堂プロダクツ
ITサービスデザインチーム
ITプロデューサー
堀田 果梨 氏

## POINT

- クラウドストライク製品を導入し外部SOCを利用するも、さまざまな課題から、全てを任せられるクラウドストライクのMDRに移行
- Falcon Completeの採用で、情シスのエンドポイント保護運用にかかる工数が1/6に
- スピード感があり、人間味があり、本当に全てを見て調査、対応を行うFalcon Completeチームに、「まるでそばにスペシャリストがいるよう」と全幅の信頼を寄せる
- FalconプラットフォームとNetskopeのほぼリアルタイムの脅威情報の双方向取り込みで、安心感のあるより強固なセキュリティを実現



CROWDSTRIKE

we stop breaches

クラウドストライク合同会社
お問い合わせ: **http://crowdstrike.jp/contact-us/**