CrowdStrike 導入事例

ディップ株式会社

根本原因が分からなければ対症療法しかできない ディップが「EDR」を選んだ理由

境界防御からエンドポイント防御へ

「バイトル」「バイトルNEXT」「はたらこねっと」など、ディップは国内有数の求人メディアを展開する企業だ。

社名の「dip」には、創業者の冨田英揮氏が草創期に抱いた「dream」（夢）、「idea」（アイデア）、「passion」（情熱）という意味が込められている。ディップは、AI（人工知能）やRPA（Robotic Process Automation）といったDX関連事業にも果敢に挑戦している。これは、少子高齢化に伴い労働力不足が深刻化する中、「労働力に関する諸問題の解決にさまざまな角度から貢献したい」という同社の思いの表れだ。

挑戦を続ける中、ディップが直面したのはセキュリティの課題だ。クラウドサービスの業務利用拡大に伴い、「境界防御」から「エンドポイント防御」へとセキュリティの考え方を大きく切り替える必要があった。セキュリティ製品の導入でこの課題を解決することにしたが、市場にはさまざまな製品があるため検討には時間がかかった。製品選定から導入まで1年を要したという。

同社が選んだ製品とは何だったのか。製品選定に関わったディップの運用担当者に話を聞いた。

SaaS利用増加を機会に、境界防御からエンドポイント防御にかじを切る

ディップは、ビジネスの発展に合わせてセキュリティ対策にも注力してきた。2004年のプライバシーマーク取得に始まり、2005年に情報セキュリティ規格「BS7799」と「ISMS認証基準」の認証を取得、2006年には情報セキュリティマネジメントシステム「ISO 27001（JIS Q 27001）」認証を取得している。

こうした背景もあり、SaaS（Software as a Service）の業務利用が増えたタイミングで即座にセキュリティの検討が始まった。もちろん、その時点でウイルス対策ソフトは導入しており、脅威もある程度検知できていた。だが、ディップの田端義典氏（商品開発本部 情報システム部 部長）は「ウイルス対策ソフトには一抹の不安があった」と語る。

「最も不安だったのは『何も起こらないこと』だ。安全だったのか、それとも検知していないだけなのか、そこが懸念だった。一方で『脅威を検知すればよい』というわけでもない。検知できても、根本原因が分からなければPCの隔離や入れ替えといった対症療法しかできない。根本原因が分からないので社内にも『危なそうだから気を付けて』と曖昧な指示しか出せない。それが歯がゆかった」

SaaSといっても従業員のほとんどが利用するものもあれば、特定の部門だけが利用する業務特化型のSaaSもある。これらのサービスの利便性を下げずにセキュリティを確保するためには、境界防御からエンドポイント防御に考え方を変える必要がある。そこで、情報システム部は「EDR」（Endpoint Detection and Response）導入に向けて動きだすことにした。2019年2月のことだった。

CrowdStrike Falcon®を選んだ理由

取引のある事業者へのヒアリングや情報セキュリティ専門展示会、セミナー参加、ベンダーへの問い合わせなどを基にセキュリティ製品の情報を集め、3つの製品が候補に残った。重視したのは「事業継続性」と「サポート体制」だ。

「ユーザーが快適に業務を遂行できなければ事業継続に支障が出る。セキュリティ製品の中には、既存アプリケーションとの相性が良くなかったり動作が重かったりして、ユーザーの業務を中断させてしまうものもある。それは何としても避けたいと考えた」（田端氏）

一方で、脅威の攻撃手口が年々凶悪化する中、社内エンジニアだけで全ての脅威に対応するのは難しいとも田端氏は考えていた。とはいえ、丸ごと外部にサポートを委託するのではコストが高くなり、社内にセキュリティナレッジを蓄積できない。「いかに柔軟なサポートを提供してくれるか」は製品を選ぶ上で外せない要件だった。

そこでディップの鎌田昌樹氏（商品開発本部 情報システム部 インフラ運用課 課長）は、候補に挙がった3つの製品に対して導入の価値がある

業種

人材サービスおよびDXサービス

所在地

東京都港区六本木3-2-1

六本木グランドタワー31F

ディップ株式会社

「私たちdipは夢とアイデアと情熱で社会を改善する存在となる」の企業理念のもと、”Labor force solution company”をビジョンに掲げ、『労働力の総合商社』として、求人情報サイト「バイトル」「バイトルNEXT」「はたらこねっと」などの運営、看護師転職支援サービス、DXサービス「コボット」の開発・提供を行っており、人材サービス（Human labor force）と、AI・RPAサービス（Digital lebor force）を展開している。

URL：https://www.dip-net.co.jp

導入製品

- CrowdStrike Falcon Insight™ EDR
- CrowdStrike Falcon Prevent™ 次世代アンチウイルス

導入時期：2020年2月

かどうかを検証する「PoV」(Proof of Value：価値実証)を実施した。

製品につき2〜3週間かけ、端末へのインストールは簡単か、どういった環境で動作するのか、どのログを取得できるかといったさまざまな項目をチェックし、減点方式で採点した。その結果、最も減点が少なく、要件を満たしていたのが「CrowdStrike Falcon®」だった。CrowdStrike Falcon®は、さまざまなセキュリティサービスを利用できるセキュリティプラットフォームだ。

「セキュリティに携わる立場としては『もしものときにさかのぼって追跡できること』は非常に重要な要素だ。そのためにはさまざまな情報を収集しておく必要がある。ユーザーモードで動く製品は収集できる範囲に制約があり、十分なログを取得できないことがある。その点、CrowdStrikeのEDR『Falcon Insight™』はOSの中核である『カーネル』と同じレベル(カーネルモード)で動くため、より多くの情報を集められる。プロセスをグラフィカルに確認できるので分かりやすく、直感的に操作できることも評価している」(鎌田氏)

田端氏はクラウドストライクのパートナーが提供するMDRサービスも選定した理由の一つだ」と補足する。

『運用の主体はディップのままで、いざというときに問い合わせ対応や技術サポートをする』という理想的な提案をしてくれた」

当初はEDRの導入だけを考えていたが、次世代ウイルス対策製品である「Falcon Prevent™」が従来のウイルス対策ソフトの機能を包括し、なおかつ未知の脅威に強いと同パートナー企業に薦められ、EDRと同時に導入を決めた。

約2700台の端末へ導入、
日々の運用はどう変わった？

2019年12月にCrowdStrike Falcon®の導入を決定した。会計年度が終わる2020年2月中にPCへの導入を終えることを目標にし、まずは情報システム部と商品開発本部に導入した。問題がないことを確認し、日本全国にある約40カ所の拠点に一斉展開した。導入したPCの数は約2700台になった。その後、物理・仮想合わせて約100台のサーバにも導入した。

かなりの導入台数だが、現在どのように運用されているのか。

「私を含め、インフラ運用課のメンバーが4人でアラートや問い合わせの一次受けをしている。脅威が検知された場合は脅威のレベルに応じてMDRパートナー企業と情報共有し、適宜対処する。サーバやネットワーク運用業務の一部として対応しているので、管理画面を見る時間は全就業時間の5%ぐらいで済んでいる。セキュリティ対策に手を取られるという感覚はほとんどない」(鎌田氏)

絶妙のタイミングでテレワークシフトを実現

田端氏によると、「CrowdStrike Falcon®導入で得られた最初の効果は全社テレワークシフトに間に合ったこと」だと語る。同社の従業員はCrowdStrike Falcon®が導入された会社支給のノートPCを持ち帰るだけで、コロナ禍がまさに日本に広がり始めたタイミングでスムーズにテレワーク体制に移行できた。田端氏は「少しでも提供タイミングが遅れていたら大変なことになっていた」と当時を振り返る。

セキュリティ対策強化という観点では、可視化と予防措置の実現が大きな導入効果だと田端氏は言う。

「『何が起こっているか、何をしなくてはいけないか』、そういった情報が的確に分かるようになった。原因は分からないがとにかく対処するという対症療法を脱し、社内に対して因果関係を説明しながら注意喚起できるようになった。2020年に流行したマルウェア『Emotet』の被害も防げた。明確にインシデント防止の効果が得られている」

ディップはCrowdStrike Falcon®によってエンドポイント保護を実現した。その後もセキュリティ強化を進めており、現在は統一の認証基盤やセキュアゲートウェイ導入などゼロトラストモデルに基づいた対策を推進している。田端氏はビジネスの成長を支えるため、今後も高いレベルのセキュリティを目指すという。

「専任部署を設置するなどして今以上にセキュリティに力を入れていく。コロナ禍もあり、システムを取り巻く環境は大きく変化している。CrowdStrike、そしてMDRパートナーには、今後もこうした環境変化に合わせた提案活動を続けてほしい」

ディップ株式会社
商品開発本部 情報システム部 部長
田端 義典 氏

ディップ株式会社
商品開発本部 情報システム部
インフラ運用課 課長
鎌田 昌樹 氏

POINT

- 「境界防御」から「エンドポイント防御」へ考え方を大きく転換
- 「事業継続性」と「サポート体制」を重視し製品選定
- 万が一の際にさかのぼり追跡できる情報を収集するカーネルモード
- 可視化と予防措置の実現

CROWDSTRIKE

we stop breaches

クラウドストライク 株式会社
お問い合わせ: **crowdstrike.jp/request-information/**