CrowdStrike 導入事例

株式会社アスカネット

従来と変わらぬコストで高度なセキュリティ対策を実現
従来型アンチウイルスから次世代型アンチウイルスへ

写真館にルーツを持ち、創業から一貫して写真加工の技術を追求してきたアスカネット。同社は現在、葬儀葬祭市場に特化した「フューネラル事業」、フォトブック関連の「フォトブック事業」、空中ディスプレイ関連の「空中ディスプレイ事業」の3事業をメインに展開している。中でも、空中ディスプレイ事業における新製品「ASKA3Dプレート」は、特殊なパネルを使って実像の反対側の空中に結像させることができるもので、新しい空中結像技術として特許を取得済。センサーや触覚を加えて空中タッチパネルとしても利用できるため、次世代の非接触インターフェイスとして世界中から高い注目を集めている。

既存利用アンチウイルス製品の更新タイミングで新たなセキュリティ製品を検討

同社では、長年に渡って利用を続けてきたアンチウイルス製品にライセンス更新を機に価格変更が生じることを受けて、新たな製品選定へと舵を切った。戦略企画部IT推進グループ マネージャーの有馬和彦氏は「当社では500名の社員が700台の端末を使用しています。端末にはWindowsとMacがありますが、双方に対応できることでこの製品を使い続けてきました。」と状況を語る。

しかしながら、使い勝手やサポート面がより良い製品へと切り替えたいという考えも持っていた。

「たとえばバージョンアップに伴い、強制的に端末が再起動することがありました。当社の業務では受注した翌日に納品というケースが少なくありません。そうした業務の最中に予期せず再起動がかかると、それだけ業務が滞ってしまうのです」（有馬氏）

さらには、不具合が起きたときに問い合わせを行っても、対応や回答が満足のいくものではなかったこともしばしばあり、こうした背景から、同社はセキュリティ製品の乗り換えを検討することにしたのである。

フルクラウドで提供される製品 全体コストが既存アンチウイルス製品とほぼ同等

アスカネットは2020年7月より本格的にセキュリティ製品の情報収集を開始した。既存製品と同じシグネチャ方式のアンチウイルス製品を含め、6つの製品をピックアップして比較した。この際、既存製品で運用に多くの手間がかかっていたこと、オンプレミス製品ではサイバー攻撃への追従にタイムラグがあり、攻撃をうける可能性が高まることなどを考慮し、クラウド製品であることを要件に入れた。

また同社は、エンドポイント全体をしっかり把握できる製品であることも求めた。というのも、既存製品の管理コンソールでは、端末の管理台帳との整合性が取れていないケースがあり、いわゆる"野良PC"と呼ばれる未管理端末の存在が問題となっていたためだ。

検討を重ねた結果、最終的に同社は次世代アンチウイルス製品「CrowdStrike Falcon Prevent™」を選定した。その理由について「クラウド対応をうたっている製品は他にもありましたが、実態は管理サーバーを必要とする製品が大半でした。一方、クラウドストライク製品は、フルクラウドで提供されることを高く評価しました。私自身、カンファレンスなどでクラウドストライク製品の説明を受けたことがあったのも大きかったですね」と語る。

さらに、懸案材料だったコストも既存製品とほぼ同等、入替作業や展開が容易、ユーザーインターフェースがわかりやすいなどの点も評価されたという。

同社は2020年9月に販売店に問い合わせを

業種
印刷

所在地
広島県広島市安佐南区祇園3-28-14

株式会社アスカネット

1995年設立。「思いをかたちに」という経営理念のもと、独自の写真加工技術を強みに、新しい製品やサービスを生み出してきた。現在はフューネラル事業、フォトブック事業、空中ディスプレイ事業と、それぞれに位置づけや特色が異なる3つの事業を柱にしている。

URL：https://www.asukanet.co.jp/

導入製品

- CrowdStrike Falcon Prevent™
  次世代アンチウイルス
- CrowdStrike Falcon Firewall Management™
  ホストファイアウォール管理

導入時期：2021年1月

実施。社内でのテストを実施した上で、同年末までに採用を正式決定。順次、利用をスタートさせた。

「当社の業務は事業ごとに大きく異なるため、各業務からそれぞれ20台程度を対象として、誤作動の有無などを重点的にチェックしました。この際、誤検知がないことには驚きました」（有馬氏）

高度なセキュリティ対策を実現
作業負荷が削減され、端末の利用実態も把握可能に

アスカネットでは現在、社内のWindows系端末300台のうち9割にあたる270台にCrowdStrike Falconエージェントを導入している。

「導入の最大の効果は、より高度なセキュリティ対策を今までとほとんど変わらないコストで導入できたことですね」（有馬氏）

CrowdStrike Falconは完全にクラウドから提供されるサービスのため、管理サーバーの運用が不要だ。管理サーバーを立てる費用が削減され、管理サーバー自身の運用・保守作業も削減された。端末のOSバージョンアップが行われた際、OSへの追従もクラウドストライクは迅速である。これらにより、管理者の作業負荷が大幅に減少したという。同部門の尾崎健一氏も「既存製品は不具合が多く、サポートも満足のいくものではなかったため、対応にとても苦労させられましたが、CrowdStrike Falconの導入で状況は大きく改善しました。実際、ユーザーからの問い合わせは全くと言っていいほどなくなっており、工数はかなり削減されたと思います」と評価する。

管理コンソールもわかりやすく使いやすいと付け加えた。「本当に必要な情報に絞ってわかりやすく表示されているので、知りたい情報が確実に得られます。既存製品には豊富な機能がありましたが、細かな情報が多すぎて、何を見れば良いのか判断に困ることもありました」（有馬氏）

さらに振る舞い検知でアラートが上がったことから、実際に社内で使われている怪しいソフトウェアなどの利用実態も把握できることがあるという。

なお同社では、CrowdStrike Falconセンサーが導入されている各端末のシリアル番号やMacアドレスが取得できるため、PCの台帳作成にも活用しているとのことだ。

「アラートが上がった際、そのプロセスを辿ることができるので、何が原因だったのかを知ることができます。以前はアラートの理由を特定することも大変でしたから、大きな違いですね。ユーザに状況を確認する際にも情報が役立っています」

今回の導入では、ユーザーにとっても多くのメリットが生まれている。既存製品ではバージョンアップに伴う再起動が発生していたため、ユーザーはそのたびに作業の手を止めなければならなかった。しかしクラウドストライクの製品は端末に影響を及ぼしたことはない。さらに、一般のアンチウイルス製品のようなフルスキャン処理を行わないため、動作が軽くなったと現場も感じている。

社内の端末に順次導入を予定
本格的なEDRの導入も検討

アスカネットでは次世代アンチウイルス製品CrowdStrike Falcon Preventに加えてホストFW管理製品CrowdStrike Falcon Firewall Managementも導入した。すべてのWindows系端末についてCrowdStrike Falcon エージェントの展開を完了したところで、サーバーについても適用を予定している。

「Macでは既存AV製品を使っていますが、こちらも順次切り替えを考えています。また次世代アンチウイルスだけでなく、CrowdStrike Falconが強みとする本格的なEDR（CrowdStrike Falcon Insight™）の導入も検討したいと思います」（有馬氏）

最後に、同様の状況にある他社に言葉を投げかけるとすれば、何を伝えたいかという問いに対し、「エンドポイント製品を変えるのは難しいことです。 しかし今まで使っていたからではなく、考えて選択し、何をしたいのかを実現するのが良いのではないかと思います。地味ではあるが、本質的なところを見ることで情報システム部をしあわせにすることができるのではないかと思います。」と、有馬氏はコメントした。

株式会社アスカネット
戦略企画部IT推進グループ
マネージャー
有馬 和彦 氏

株式会社アスカネット
戦略企画部IT推進グループ
尾崎 健一 氏

POINT

- 既存アンチウイルス製品運用にかかるコストとほとんど変わらないコストで次世代型アンチウイルスを導入
- フルクラウドで提供される製品であり、管理者の作業負荷が大幅に削減
- 現場の従業員もフルスキャンから開放され、端末の動作が軽くなったことを実感

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/**