CrowdStrike 導入事例

Sansan株式会社様

ゼロトラストで力点をエンドポイントへ
働く場所を選ばないセキュリティを高品質に実現

セキュリティは前提条件 全社を守るCSIRT

名刺管理サービスというアイデアを携えて、5人の仲間が起業した。その名をSansan株式会社という。2007年、同社はその後着実に顧客数を伸ばし、今やクラウド名刺管理サービス「Sansan」の利用企業は7,000社、名刺アプリ「Eight」のユーザーは280万人に上る。

名刺に記載される個人情報を扱う事業特性上、同社にとってセキュリティは最優先課題だ。同社はPremise（前提）として「セキュリティと利便性を両立させる」という一文を掲げている。セキュリティ対策をスピーディーかつ確実に進めていくためには専任組織が存在した方がいいと、2015年、CISO（Chief Information Security Officer）直轄のSansan-CSIRT（Computer Security Incident Response Team）を立ち上げた。保護対象のITリソースは、従業員が利用する端末として約1,500台（OSはWindowsとMacが半々）、クラウド上で運用されているサーバが約1,000台存在する。

拠点増でのセキュリティと 誤検知対応に悩む

近年、同社ではセキュリティの観点から2つの課題に直面していた。

1つは活動拠点が全国に拡大しているという組織の成長によるものだ。支店やサテライトオフィスを含めると国内は11拠点にまで増えていた。従来のような境界防御の考え方でセキュリティを構築するとなると、どこまでも本社を中心として複雑なネットワーク網を構築しなければならない。この先も拠点増が予想される中、果たしてそれは正しい方向性なのかという疑問が生じていた。

もう1つは、Sansan-CSIRTとしての悩みだ。アンチウイルスソフトの誤検知率が高く、その対応に多くの時間が奪われていた。そのためアンチウイルスソフトの運用も工数がかかり、一日の1/3がその対応で"張りついている"状況だった。Sansan株式会社 CSIRT SOCチーム 松田 健氏は次のように語る。

「一番困っていたのは、原因不明の検知です。上がった以上、対応しなければなりません。ヒヤリングのために従業員の元へ行ったり、逆にこちらへ足を運んでもらったり。それでも結局よくわからず、フルスキャンしてしばらく静観という釈然としない対応でした。我々CSIRTは業務であるため、まだ許されますが、従業員は本来業務の時間が中断されてしまいます。一度、参考値として対応にかかる人件費を試算した結果、年間700～800万円にもなって驚きました。このような徒労を解消したいと考えていました」

加えて、Sansan-CSIRTではアンチウイルスソフトとは別にIT資産管理ツールも導入しており、デバイス制御などはこちらで行っていた。少数精鋭チームのため全員が毎日忙しい。ツールが分かれているために、チェックの頻度に優劣がついてしまうこともあった。

軽量さ、安定性、検知性能で CrowdStrike Falconを選択

課題解決をめざして動き出したのは、2019年6月。おりしもCISOからゼロトラストというセキュリティアプローチの話が出てきた。これは境界防御の発想から脱し、社内外や拠点の主従を区別せず、基本的に何も信用しないという考え方に立つ。そして、この世界では重要な"盾"はネットワークではなくエンドポイントに置く。

エンドポイント保護という観点で、Sansan-CSIRTが注目していたのはEDRだった。境界防御発想のアンチウイルスソフトではなく、これからは侵入を前提として検知と対応にフォーカスするEDR。優秀なEDRを導入することは、ゼロトラストを取り入れ、エンドポイントにセキュリティの力点を置こうとしていた中で理にかなった判断だった。

それではどう製品を選定するか。ガートナーやフォレスターなどのアナリスト機関、情報セキュリティコミュニティ、外部のセキュリティコンサルタントなどから幅広く情報収集した結果、5製品が候補に上がってきた。その中でもEDR機能がすぐれたものを2つ選び、

導入製品

- CrowdStrike Falcon Insight EDR
- CrowdStrike Falcon Device Control デバイス制御
- CrowdStrike Falcon Discover IT衛生管理
- CrowdStrike Falcon OverWatch 脅威のハンティング
- CrowdStrike Falcon Spotlight 脆弱性管理
- Falcon Prevent 次世代アンチウイルス

Sansan株式会社

所在地：東京都渋谷区神宮前5丁目52-2

導入時期：2020年2月

URL：https://jp.sansan.com/

出会いからイノベーションを生み出す」をミッションに掲げ、ビジネスの出会いをよりよきものへと変え、世界中の働き方を変えることをめざしている。法人向け名刺管理サービス「Sansan」、個人向け名刺アプリ「Eight」を提供するとともに、最近では、請求書のオンライン受領を可能にする「BillOne」もリリース。日本企業のデジタルトランスフォーメーション推進をさまざまな角度から支援する。

PoC(Proof of Concept)を行った。このプロセスでは、製品のセキュリティスコープや、ソフトウェアそのもののリソース消費や稼働の安定性、ベンダーの活動状況など幅広い観点から比較検討された。また、Sansan-CSIRT内のメンバーがすり抜けテストを行ったりもした。

その結果、最終的に選ばれたのがCrowdStrike Falconだ。しかもEDRであるCrowdStrike Falcon Insightのみならず、CrowdStrike Falcon Device Control(デバイス制御)、CrowdStrike Falcon Discover(IT衛生管理)、CrowdStrike Falcon OverWatch(脅威のハンティング)、CrowdStrike Falcon Spotlight(脆弱性管理)、Falcon Prevent(次世代アンチウイルス)と計6つのモジュールが採用された。松田氏はその理由を次のように語る。

「選定の決め手は4つあります。1つめは、端末やサーバでのリソース消費が少なく軽量で、ユーザーの業務やサーバの動作を妨げないこと。2つめは、製品がWindows環境でも、Mac環境でも安定的に動き、不具合が少ないこと。また、アップデートが迅速に提供されること。3つめは、CrowdStrikeがセキュリティ業界のリーダー的存在で、エンドポイントセキュリティの最先端を突き詰めていること。そして、これはPoCプロセスでわかったことですが、フォーラムを開設して活発かつオープンに発言していたり、セキュリティの考え方をブログで発信していたことも高く評価しました。最後の4つめは、CrowdStrike Falcon OverWatchの存在です。人の目で脅威を検知することに本気で取り組んでいる姿勢に共感しました。

さらに、セキュリティ基盤を統合してそこで多くの機能を享受できるなら、業務効率向上を考えると結果的に安上がりであると判断しました」

誤検知率の大幅減や基盤統合効果で約800万円相当の運用コスト削減

導入を開始したのは2020年1月末。2月中旬には約1,500台の端末へ、3月上旬にはサーバ約1,000台へ製品インストールが完了した。端末のアンチウイルスソフトはアンインストールされ、CrowdStrike Falcon Insight と Preventによる検知は、従業員が本来業務に集中できるよう管理コンソールでのみ把握するようにしている。はからずしもコロナ禍により全社テレワークとなったが、全く不自由なくセキュリティ対応が行えているという。たとえば、検知が上がった場合、管理画面上で状況を事前調査した上で従業員にヒヤリングを行う。ピンポイントで質問できるため、解決までのプロセスも非常にスムーズだという。

同社では特定端末でしかリムーバブルメディアの利用を許可していない。CrowdStrike Falcon Device Controlはその制御を担っている。管理画面が同じであるため、今では特定端末でどんなファイルが書き出されているかチェックする余裕も生まれた。

そしてCrowdStrike Falcon Discoverでは、未管理端末を探し出し対応を行う。

Sansan-CSIRTではまた、定期的にペネトレーションテストを行っている。導入過渡期には、あえて既存のアンチウイルスソフトをインストールしたままテストに臨んだ。その結果、唯一CrowdStrike Falcon OverWatchだけがテスターの存在を知らせたそうだ。

「インシデント対応では、1分1秒を争う場面があるものです。こうした場面では、このサービスがあるとないとでは初動の早さが変わってきます。導入するならこのモジュールも加えておくのがお勧めです」(松田氏)

CrowdStrike Falconの導入によって、Sansanでは、働く場所に依存しない、高レベルかつ均質なセキュリティが実現した。想定していなかったことだが、これはコロナ禍のテレワーク環境にもぴったり合致するものだった。

また、導入前と比較して誤検知率は1/10になり、検知事象の対応時間は1件あたり最大2時間から15分へと短縮した。また、事象の因果関係がはっきり把握できるようになり、対応品質が向上している。Sansan-CSIRTの徒労がなくなり、従業員の本業を妨げなくなったことは、人件費にして年間700〜800万円相当の運用コストが削減されたと考えられている。

取締役、CISO兼DSOCセンター長である常樂 諭氏は、次の様にコメントしている。「新型コロナウイルス流行による非常事態の中、CrowdStrikeの導入は事業を継続させるために良い判断でした。リモートによるCSIRTと従業員の対応を見ていても、何不自由なく対応出来ていることから安心して任せることが出来ました。」

ゼロトラスト発想による対策のエンドポイントシフトは、Sansanに「セキュリティと利便性を両立させる」というPremiseの実現をもたらした。また今回の基盤統合では、Sansan-CSIRTだけでなく、従業員も業務効率向上という大きな果実を手に入れたといえるだろう。

POINT

- セキュリティ対策のエンドポイントシフトが場所を選ばない働き方を実現
- 運用コスト削減につながる誤検知率大幅減や対応時間短縮
- セキュリティ基盤の統合も業務効率向上と対応品質向上に貢献
- 1分1秒を争う際の初動対応を左右する“プロの目”サービス

Sansan株式会社
取締役
CISO兼DSOCセンター長
常樂 諭氏

Sansan株式会社
CSIRT
松田 健氏

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

2021年1月現在　※本カタログに掲載されております社名および製品名は、各社の商標及び登録商標です。