Case Study | 運用事例

# CROWDSTRIKE 社「CrowdStrike Falcon」

## Sansan株式会社 様

# CSIRT業務にCrowdStrike Falconを活用しスピーディで効率的なインシデント対応を実現 テレワークでも安全に働ける環境を確立

### Point

- アラート件数が激減し、より付加価値の高い業務への注力が可能になった
- テレワーク／リモートワークの状況下でも安全な業務環境を提供できる
- 強力な検索機能を駆使することで、運用管理業務の効率化にも貢献

### セキュリティと利便性の両立をテーマに社内の安全対策を推進

「出会いからイノベーションを生み出す」という企業ミッションの下、法人向けクラウド名刺管理サービス「Sansan」、並びに個人向け名刺アプリ「Eight」を提供するSansan。デジタル時代の新たな働き方を加速するツールとして、数多くのユーザーに活用されている。

その同社のセキュリティ対策を一手に担っているのが、CISO直轄のセキュリティ専任組織「Sansan-CSIRT」である。同部門の松田健氏は「当社のサービスではお客様の個人情報を取り扱うため、システムやサービスの安全性確保が非常に重要です。CSIRTとしても、最新の脅威に対抗するべく常に継続的な環境改善に努めています」と語る。

特に注目されるのが、現場部門のスタッフもCSIRT活動に参加している点だ。

「いくら安全性が高まっても、それによって生産性や業務効率が下がってしまっては問題です。そこで、現場の要望や意見も積極的に取り入れることで、より実効性の高いセキュリティを目指しているのです」

同社では「セキュリティと利便性を両立する」を企業理念の「Premise」として掲げている。その姿勢は、社内のセキュリティ対策にもしっかりと貫かれているのである。

### CSIRTの活動に貢献するCrowdStrike Falcon

Sansan-CSIRTでは、ビジネスの安心・安全を支えるツールとしてCROWDSTRIKE社の「CrowdStrike Falcon」を活用している。ここでは次世代アンチウイルス「Falcon Prevent」、EDR「Falcon Insight」、脅威ハンティング「Falcon OverWatch」、資産管理「Falcon Discover」、「USB Device Control」など、CrowdStrike Falconの多くの機能が用いられている。

導入に伴うポリシー設計やアラート運用設計なども、特に苦労するような場面はなかったと松田氏。「まずデファクト・スタンダードな設定を押さえた上で、当社に合わせてグルーピングの方法を変化させた形ですね。設定自体がシンプルですし、マクニカのアドバイスも受けられましたので、それほど時間はかかりませんでした」と語る。

業務の自動化に役立つ機能も多かったとのこと。「たとえば、人員増加やサービスの追加により、新たにFalconの管理下に置きたい対象端末が増加した場合でも、CrowdStrike Falconはこれを適切なグループに、ダイナミックに振り分けることができます。『このサーバーはブロック、このサーバーは検知のみ』といった設定を、一台ずつで行わなくて済むので大変便利ですね。同様に、端末用センサーのアップデート作業などもポリシーで自動化できますので、運用にほ

User's Profile

### Sansan株式会社

名　　称：Sansan株式会社
所 在 地：東京都渋谷区神宮前5-52-2
導入時期：2020年2月
U R L：https://jp.sansan.com/

社内にあるすべての名刺情報を集約し、ビジネスプラットフォームとして活用できる法人向けクラウド名刺管理サービス「Sansan」、並びに、取り込んだ名刺から自分だけのビジネスネットワークを構築する個人向け名刺アプリ「Eight」を提供する先進テクノロジー企業。2020年3月に新事業戦略「Sansan Plus」を打ち出すなど、さらなる飛躍に向けた取り組みを意欲的に推進している。

CSIRT
松田 健 氏

とんど手間が掛かりません」

管理対象となる機器はクライアントが約1000台、サーバーが約700～800台にも上るが、既存の端末管理ソフトウェアなどを利用することで、社内への展開もスムーズに進められた。「移行時には、旧アンチウイルス製品との並行稼働も行いましたが、これに伴うトラブルも皆無でした。この手のプロジェクトでは何かしらの問題が起こるのが一般的なだけに、製品の安定性の高さには非常に驚きました」と松田氏は語る。

## インシデント対応プロセスの大幅なシンプル化に成功

CrowdStrike Falconの導入メリットも大きい。旧アンチウイルス製品は検知精度が高かったが、通知されたアラートの約99%は結果的に誤検知だったという。アラートの詳細を見ても原因が特定しづらいものが多く、その対応に多くの時間と工数を費やす必要があった。

「これに対して、CrowdStrike Falconは、無用なアラートをほとんど出しません。以前は毎日数十件上がっていたアラートが、今では1件あるかないかです。導入当初は検知モードのみで動かしていましたが、この結果を見て自信を持ってブロックモードに移行できました」

インシデント対応のプロセスも、これまでより大幅にシンプル化された。疑わしい端末が発見された場合、以前は再スキャンを行ったり、当該端末をCSIRTに送ってもらったりする必要があった。

「その点、Falcon Insightの『Real Time Response』機能を利用すれば、ユーザーの端末に直接リモートで入って調査できます。おかげで、こうした面倒な手続きが一切不要になりました」

これにより、全国各地の支店やサテライトオフィスで働くユーザーへの対応も格段にスピードアップ。松田氏は「現物を送ってもらって調査するとなると、どうしても一週間程度は掛かります。それが現在では2～3時間で対処できますから、劇的な違いがあります」と続ける。

インシデントに関わるログを網羅的に分析できるため、分析・調査の精度も飛躍的に向上。中には、テレワークで働くユーザーのネットワーク機器に不具合があることを突き止めたケースもあるという。

「以前の環境では、こうしたトラブルの原因を短時間で発見するのは不可能に近かったでしょう」

さらに、大きな安心感につながっているのが、「Falcon OverWatch」の脅威ハンティングだ。

「Falcon導入後、国内でトップクラスの人材を有する企業に委託してペネトレーションテストを実施した際、Falcon OverWatchだけが脅威を検知したケースがありました。普段は『お守り』のような感じですが、こうした環境があることはやはり心強い」

## テレワーク時代に即した安心・安全な業務環境を実現

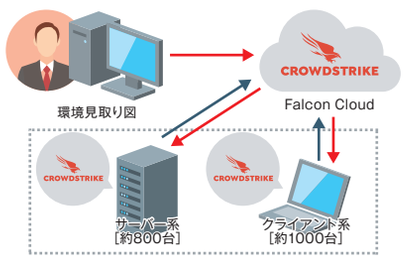
もう一つ見逃せないのが、日常的な運用管理にも役立っている点だ。

「たとえば情シス部門から、社内で稼働している端末のシリアル番号を簡単に洗い出せないかと相談されたことがあります。別に管理する仕組みもありますが、棚卸しの際に1つ1つ最新の状態か確認し修正するのが意外と大変です。そこで必要な検索文を作って、渡しました」

「Falcon Discover」の機能も便利に活用されている。端末に導入されたソフトやバージョンの管理はもちろんのこと、何らかのソフトをインストールした際に別のアンチウイルス製品が一緒に入れられたり、キッティング時に必要なソフトウェアが抜けたりするようなことを効果的に防げるとのことだ。ちなみに、USBメモリなどのデバイスについては、使用を禁止してしまう企業も多いが、同社では「USB Device Control」を利用することで、安全に活用できる環境を提供している。

今回の取り組みを振り返って「大成功だった」と語る松田氏。「新型コロナウイルスの問題が起きる以前に、リモートでも安心して働ける環境を整備できたことは大きな成果。導入や活用を支援してくれたマクニカのサポートにも大いに感謝しています。今後も『セキュリティと利便性を両立する』を前提とした、より安全で快適な環境を整備していきたいですね」と語った。

今後の展望としては、CrowdStrike FalconのEDRで可能になった社内外のエンドポイントの検知と対処に加えて、リスクのある環境への対策強化（脆弱性運用）に重点を置いていくことを検討している。CrowdStrike FalconのSpotlightモジュールを利用して、エンドポイントのオペレーションを強化する見通しが立っている。




**ご利用中の機能一覧**

- NGAV（Falcon Prevent）
- EDR（Falcon Insight）
- 脅威ハンティング（Falcon Overwatch）
- 脆弱性可視化（Falcon Spotlight）
- 資産可視化（Falcon Discover）
- USB制御（Falcon DeviceControl）

**導入メリット**

- ■ポリシーやユーザーグループをあらかじめ設定することで、管理・設定作業を自動化。
- ■インシデント対応も、リモートから直接端末を操作することで、対応時間を短縮。
- ■インシデントログの分析機能により、トラブルの原因の特定が可能に。
- ■端末のシリアル番号、インストールしているソフトの制御、USBの使用の可否など、端末管理を効率化。

http://www.macnica.net/crowdstrike/

macnica networks

**マクニカネットワークス株式会社**

本社　〒222-8562 横浜市港北区新横浜 1-5-5
TEL.045-476-2010　FAX.045-476-2060
西日本営業所　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916　FAX.06-6227-6917
cs_sales@cs.macnica.net