CrowdStrike 導入事例

# 国立研究開発法人農業・食品産業技術総合研究機構

## 10,000台のエンドポイントを守り抜くため CrowdStrike Falcon の8機能をフル活用

### 3つの異なるツールによるセキュリティ実現に課題を認識

ぶどうの"シャインマスカット"、りんごの"ふじ"。これらを生み出した研究機関が、今回ご紹介する国立研究開発法人　農業・食品産業技術総合研究機構（コミュニケーションネーム（通称）：農研機構）である。農研機構はこの分野における日本最大の国立研究機関だ。北は北海道から、南は沖縄まで幅広く研究センターや部門があり、その最大の拠点がつくば学園都市にある。AI、ロボティクス、遺伝資源、食品産業、畜産、動物衛生、農作物の育種、農業環境、農業工学、植物防疫、種苗管理、基礎研究への支援など食と農に関する幅広い研究を行っており、まさに食と農の未来を創造する場だ。

一般的に、国の研究機関は公的な存在であり、最先端の技術・研究情報を保有していることから、外部脅威から狙いをつけられやすい。そのため、農研機構でもサイバーセキュリティ業務を重視。 情報統括部　情報セキュリティ課内に職員メンバーから成るCSIRTを設置し、全国の研究者や職員が利用する約10,000台のエンドポイントを日々監視するとともに、何かインシデントが発生すれば情報統括部長や理事をトップに緊急対応チームを結成する。また、攻撃者につけいる隙を与えないためには、エンドポイント環境の“クリーンさ”も重要であると考え、IT資産管理にも力を入れている。

同機構では、2021年3月31日、導入していた3つのセキュリティ製品が保守満了を迎えることになっていた。その3つとは、全エンドポイントを対象に導入していたアンチウイルスソフトウェア、IT資産管理ツール、管理職向けエンドポイント保護のためのEDR製品だ。情報セキュリティ課は、既存の運用体制で抱えていた課題を次期導入製品・サービスで解決したいと考えていた。国立研究開発法人農業・食品産業技術総合研究機構　情報統括部　情報セキュリティ課　サイバーセキュリティマネージャー　山田雅邦氏は、従来の課題を次のように語る。

「NIST（米国国立標準研究所）のサイバーセキュリティフレームワークでは、特定、防御、検知、対応、復旧という5つの機能が中核となるとされていますが、当機構ではそれを3つの異なるツールで実現している状態でした。それぞれに管理コンソールが存在することから相応の運用工数が必要で、なかなか本来の業務に時間が割けませんでした。また、エンドポイントにも3つのエージェントのインストールが必要となるため、エンドユーザーへの負荷、影響も大きかったと思います」

アンチウイルスソフトとIT資産管理ツールはオンプレミス製品であったため、それに起因する運用負荷も高かったようだ。

「とにかく調整業務がたくさんありました。毎月のサーバメンテナンスでは、ハードウェア運用部隊にバックアップを依頼したり、保守会社と日程調整したり、ユーザーにメンテナンス実施を周知したり。」国立研究開発法人農業・食品産業技術総合研究機構 情報統括部 情報セキュリティ課 土田隆裕氏は、こう語る。

そこで、次期製品・サービスの入札に当たって、情報セキュリティ課は3つの基本方針を立てた。

1つめは、対応OSの拡大だ。研究機関であるため、エンドポイントにWindowsを使うユーザーもいれば、Macを使うユーザーもいる。加えて、AI研究者の養成にも力を入れていることから、今後はUbuntu端末も増加することが確実だった。3つのOSへの対応は必須だったのである。

2つめは、クラウド型であることだ。コロナ禍によって働き方が一転した。もはやLANにつながった拠点だけが仕事場ではなく、機構支給の端末を自宅に持ち帰り使用する、ユーザーがどこにいても保護可能な環境の構築が求められた。また現在、日本は国を挙げてDXの推進を後押ししており、その一環で政府機関の情報システムにおいては、『クラウド・バイ・デフォルトの原則』の方針が打ち出されていた。国の研究機関としては、その方針に沿うのが順当だった。

農研機構 NARO 国立研究開発法人 農業・食品産業技術総合研究機構

**業種**

国立研究開発法人

**所在地**

茨城県つくば市観音台3-1-1

**国立研究開発法人農業・食品産業技術総合研究機構**

国立研究開発法人農業・食品産業技術総合研究機構は、日本の農業と食品産業におけるわが国の最大の研究機関だ。基礎から応用まで対象分野は広く、全国各地に拠点を配置して研究活動を行っている。起源は明治26年に設立された農商務省農事試験場にあり、農林水産省の試験研究機関の時代を経て、数回の統合後、現在の姿となった。研究成果を社会に実装するため、産官学と連携した共同研究や技術移転活動、生産者や消費者への情報提供も積極的に進めている。

URL：https://www.naro.go.jp/index.html

**導入製品**

- CrowdStrike Falcon Prevent™ NGAV（次世代アンチウイルス）
- CrowdStrike Falcon Insight™ EDR
- CrowdStrike Falcon OverWatch™ プロアクティブな脅威ハンティング
- CrowdStrike Falcon Device Control™ USBデバイス制御
- CrowdStrike Falcon Discover™ IT資産管理
- CrowdStrike Falcon Spotlight™ 脆弱性管理
- CrowdStrike Falcon Firewall Management™ ホストファイアウォール管理
- CrowdStrike Falcon X™ インテリジェンスを活用した脅威分析の自動化

導入時期：2021年4月

3つめは、1つの製品・サービスで、より多くのセキュリティ業務を担えることである。ワンエージェント、ワンコンソールで済めば、運用工数の削減と迅速な対応が期待できる。少数精鋭で構内CSIRTをも運営している同機構にとって不可欠の要件といえた。

**CrowdStrike Falconは求める高レベルの仕様を満たした**

農研機構における次期セキュリティ製品・サービス選定の意見招請が行われたのは、2020年7月。その一方で、情報セキュリティ課では、入札で提出する最終仕様書をブラッシュアップするため、複数製品・サービスをピックアップしてリサーチを行った。そこで重視した観点は「柔軟なUSB制御が可能か」「IT資産管理機能が既存製品以上か」「サンドボックス機能は存在するか」というものだった。土田氏は語る。

「USB制御は本格的に運用したいと考えている機能でした。当機構では、USBデバイスはユーザーが購入したものを情報セキュリティ課に登録してもらうことにしています。登録されたUSBデバイスであればエンドポイントでの書き込みを許可するといった、きめこまかい制御を望んでいた。また、IT資産管理も、脅威からの保護と同じぐらい私たちにははずせない機能でした。怪しい検体の分析も行っていましたが、セキュリティベンダーの有償サービスやフリーサービスでは、素性の判明していない検体は分析できなかったり、当機構で分析した事実が知られてしまうデメリットがありました。新しい検体をシークレットに分析できるサンドボックス機能がほしいと思いました」

これらの要望を盛りこんで最終仕様書を作成、2021年1月27日入札を実施したところ、CrowdStrike Falconが落札し、採用となった。農研機構はこれで決定とし、NGAV(次世代アンチウイルス):Falcon Prevent、EDR:Falcon Insight、プロアクティブな脅威ハンティング:Falcon OverWatch、USBデバイス制御:Falcon Device Control、IT資産管理:Falcon Discover、脆弱性管理:Falcon Spotlight、ホストファイアウォール管理:Falcon Firewall Management、サンドボックス機能を含むインテリジェンスを活用した脅威分析の自動化:Falcon Xと、8機能を採用した。既存の3つのツールをリプレースするのみならず、専門家による脅威ハンティングサービスであるFalcon OverWatchを含めたのはどういう理由だったのか。

山田氏は次のように語る。「当初は、外部のマネージドセキュリティサービス(MSS)の活用も考えましたが、私たち自身がCrowdStrike Falconに慣れていない状態では委託内容をうまく定義できません。そこでまず自分たちで運用して知見を貯めようと考えました。しかし専門家のチェックも欲しかったためFalcon OverWatchを採用しました。

ほぼフル機能を導入しましたのでそれなりに費用はかかりました。そこは経営層のセキュリティ投資への深い理解があったためと感謝しています。一方、セキュリティツールをクラウド型の単一製品に統合したことで運用工数が減らせて、できることが増えましたので、全体的にはリーズナブルだと思っています」

**インフラレイヤーの運用工数が9割減にエンドポイント保護の品質も向上**

2021年4月1日、CrowdStrike Falconは本格稼働し、これによって、3つのOSへの対応、クラウド型サービスへの移行、セキュリティ業務の統合という基本方針が達成された。そして、その結果として、セキュリティ業務のあり方自体も大きく改善された。土田氏は語る。

「物理筐体がなくなったため、インフラのメンテナンスに関わる運用工数は、9割削減しました。また、CrowdStrike Falconのレポートをエクスポートするといった定型業務は協力会社に任せ、私自身は主要なアプリケーションがきちんとアップデートされているか、怪しいファイルが入りこんでいないかなどをチェック、問題があれば直接エンドユーザーに連絡を取って対応を依頼できるようになりました。

気に入っているのは、これでCrowdStrike Falconが入っていない機器が把握できるようになったことです。従来のIT資産管理ツールではわからないことでした。これによって、その機器を持っている拠点に連絡を取り、エンドポイントであるならちゃんとFalconのエージェントを導入してほしいと申し入れることができます」

つまり、同機構の重視するエンドポイント環境の“クリーンさ”が、CrowdStrike Falconによって向上可能になったのだ。

今後、情報セキュリティ課では、このサービスを徹底利用しながら、構想していたUSB制御やより深いレベルのエンドポイント保護を進めていく予定だ。セキュリティ業務を真正面から受け止め、自らイニシアチブを取って組織を守り抜こうとする姿勢が印象的だった。

国立研究開発法人農業・食品産業技術総合研究機構
情報統括部 情報セキュリティ課 課長
小野寺 達也 氏

国立研究開発法人農業・食品産業技術総合研究機構
情報統括部 情報セキュリティ課
サイバーセキュリティマネージャー
山田 雅邦 氏

国立研究開発法人農業・食品産業技術総合研究機構
情報統括部 情報セキュリティ課
土田 隆裕 氏

## POINT

- 旧来の3つのセキュリティ機能が統合されただけでなく、8つのセキュリティ機能を1つのエージェントで実現
- クラウド型サービス採用で、管理サーバが不要となり、インフラレイヤーの運用工数が9割減
- クラウド型サービスへの全面移行で働き方が広がる中でもエンドポイントを厳重保護
- マルウェア検体の解析を、自組織内でFalconコンソールの中で即実施可能に



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/**