CrowdStrike 導入事例

国立研究開発法人 国立環境研究所

政府の情報セキュリティ基準への準拠をめざし 研究所端末2,200台にCrowdStrike Falconを導入

国立研究開発法人
国立環境研究所
National Institute for Environmental Studies

政府統一基準に準拠した
エンドポイント保護への刷新を決断

国立環境研究所（以下、NIES）は、日本の国立研究開発法人の一つで、環境問題に関する公的研究機関である。主なミッションは、環境研究業務と、環境情報の収集・整理・提供業務である。2021年度より開始された第５期中長期計画では、これまでの実績を踏まえつつ、国内外からの新たな要請にも答えるべく研究分野の再編成がなされた。具体的には、「地球システム分野」「環境リスク・健康分野」など8つの戦略的研究プログラムが設定され、個別分野を超えた連携によって統合的な研究が進められている。

NIESは、新たな知を生み出す国の研究機関であるため、情報セキュリティは重要な課題である。内閣サイバーセキュリティセンター（以下、NISC）は、政府機関向けに「政府統一基準」を定期的に改定しており、NIESにおいても統一基準への準拠が求められており、着実に防護のレベルを向上させてきた。

2021年に改定された最新の政府統一基準では、ゼロトラストアーキテクチャというサイバーセキュリティの新しい考え方が明記され、境界防御を超える守りに関する記述が加わった。パターンマッチングで怪しい攻撃を防ぐというだけではなく、ファイヤーウォールを通過しないネットワーク経由やエンドポイントに侵入してくる脅威を検知し対応する仕組みも備えた方がいい、との内容だった。つまり、EDRである。

それまで、NIESで利用されているWindows端末約2,000台、Mac端末約200台に関しては、それぞれ異なるウイルス対策ソフトウェアを環境情報部情報管理室が一括調達して使用しており、契約を更新していた。そのため、管理者は二重管理を余儀なくされていた。また、Mac端末用ソフトウェアについては管理サーバを構築しておらず、管理者が端末での検知状況を思うように把握できないという課題も存在した。加えて、ソフトウェアベンダーの1社が2021年度4月からのライセンス価格値上げを通告。これを機に、NIESはエンドポイント保護体制をEDRの観点を加えて抜本的に見直すことにした。

エンドポイントに検知で
負荷をかけないことが大前提
将来の拡張性も条件に

情報収集に当たったのは、NIES 環境情報部情報管理室 土谷 純一氏である。インターネットなどを使った市場調査を始め、つくばに集う研究所で構成している情報交換網、国立研究開発法人協議会の情報交換網も利用し、候補となり得る製品を絞りこんでいった。そして、その中のいくつかは実際に操作して評価も行い、結果として入札仕様書に掲げた条件は、次のようになった。

・Windows、Mac、Linux環境に対応していること

・エンドポイントからなるべく多くの情報を取得できること

・エンドポイントに負荷をかけないこと

・ウイルス対策やEDRにとどまらず、将来的な拡張への道が開かれていること

・24時間365日対応が可能であること

・フルクラウドで稼働すること

土谷氏は次のように語る。

「Windows、Macに加えて、Linuxも対応対象としたのは、研究所にはLinuxサーバも数多く存在するからです。基本的にはサーバを所有している部署でセキュリティを担保しているのですが、随時相談には乗っており、このOSもカバーできた方がいいと考えました。

また、情報を取得するのであれば、少ないよりも多い方がそれだけ多くの知見が得られます」

NIES 環境情報部情報管理室 村上 功氏は、土谷氏を補足して次のように語る。

「何より重要なのが、エンドポイント端末に負荷をかけないことでした。近年、性能が大幅に

業種
国立研究開発法人

所在地
茨城県つくば市小野川16-2

国立研究開発法人 国立環境研究所

国立環境研究所は、社会とその変化や、国民の生活に関係の深い課題を研究している。1974年に国立公害研究所としてスタート、1990年にはより広範化した環境問題を扱うため国立環境研究所と名称を変更した。ここ数年、頻発する気象災害と気候変動の関係が国内外で大きな話題となり、政府も気候変動への適応やカーボンニュートラルの実現を宣言している。そうした中、同研究所では、これら環境に関係した多くの課題について研究を進め、政府や国民の意思決定の根拠となる科学的知見を提供することを使命としている。

URL：https://www.nies.go.jp/

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

導入時期：2021年1月

向上し、エンドポイント端末はサーバやワークステーション級のパワーを持てるようになっています。そのため、研究者はこれを計算機資源と捉え、そのCPUやメモリを最大限に活用したいと考えています。情報セキュリティ保護のためとはいえ、仕事を阻害するものは入れることは、研究に支障を来すことから、できるかぎり軽量に動くものでなければなりませんでした。

一方、拡張性という観点は、管理をなるべく簡素化したいというところから来ています。機能が基準を満たしているという前提で、いろいろなツールを使い分けるより、1つのツールで完結できた方が、少人数で管理している運用側としては助かります。

さらに、攻撃者がわれわれの勤務時間に合わせて動くわけではないため、何らかの形で24時間365日カバーされることも求めたいと考えました」

フルクラウドであることも欠かせない条件だった、と、NIES 環境情報部情報管理室 椎名 愛里氏は語る。

「コロナ禍を契機に、研究所では自宅就業が定着しています。まん延防止等重点措置が発令されている際は我々のチームも週に3日程度の出勤にとどめています。ゼロトラストアーキテクチャの実装という意味でも、withコロナの中でも滞りなくセキュアに仕事をするという意味でも、“フルクラウド”は重要なキーワードでした」

決まったのは
CrowdStrike Falconでの体制確立
3カ月かけずに2,200台へ一斉展開

2020年10月に入札公告を公示し、同年12月の開札の結果、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をセキュリティ専門家が提供するFalcon OverWatchという3つのモジュールを導入。これらにより、ウイルス対策に加えてEDRも実装可能になっただけでなく、24時間365日の外部監視も実現することになった。

情報管理室は早くも2021年1月より導入作業を開始。4月から始まる新年度、同じタイミングでやってくる既存ウイルス対策ソフトウェアの契約更新時期に合わせて、迅速に所内展開が進められた。現在は、NIESで利用されている2,200台の端末でCrowdStrike Falconがフルに稼働している。

政府統一基準への準拠、
自宅就業者にも迅速に検知・対応できる体制が確立

CrowdStrike Falconの導入によって、研究所の情報セキュリティが最新の政府統一基準へ準拠した。村上氏はこの点について次のように語る。

「国の研究機関にとって、NISCの政府統一基準はわれわれの情報セキュリティのすべてといえるほど重い方針です。NIESは情報通信を研究テーマとしているわけではないため、情報システム分野最先端を走るという使命までは帯びていないものの、それでも必要な対策を行う必要があります。限られた予算の中でNISCの基準をどう満たせるかが問われた事案でしたが、CrowdStrike Falconで実現することができました」

現場では、土谷氏が検知の状況を迅速に把握して対応できる体制が確立された。

「自宅就業者も含めて、アラート検知後の状況が理解できるようになりました。以前の環境だと、検知したという情報だけで、『これは一体何なんだ？』と戸惑うことも多かったのです。CrowdStrike Falconを導入してからは、検知してからウイルスやマルウェアがどういうプロセスを踏んで動くのか、その流れがよく見えるようになりました。話には聞いていましたが、実際使い始めて『なるほど、こういう風に可視化されるのだな』と肌でわかった感じですね。Falcon Insightで攻撃がつかめるようになったことにより、検知後、調査に時間をかけずに原因をつかみ、確信を持って判断し、すばやく対応に当たれるようになったことを実感しています」

CrowdStrike Falconが確かにフルクラウドで稼働し、エージェントの動きは軽量で、エンドポイントには負荷をかけないという点も、試用のときから村上氏、土谷氏の間で見解が一致していた。実際、ユーザーがエンドポイント端末を計算機資源として活用する中でもCrowdStrike Falconが稼働していることを意識していないという。

NIESでは、今後もNISCが策定する最新の政府統一基準に追従し、準拠すべく、情報セキュリティ対策を進めていく。さらにCrowdStrike Falconから提供される他の機能についても、現在利用している製品や方法を、代替可能なだけの機能を有しているかどうか確認、検討を行う計画もある。

リソースが限られる中、政府の示す情報セキュリティ基準にキャッチアップし続けるべく、NIESに導入されたのはCrowdStrike Falconだった。

国立研究開発法人 国立環境研究所
環境情報部 情報管理室
村上 功 氏

国立研究開発法人 国立環境研究所
環境情報部 情報管理室
土谷 純一 氏

国立研究開発法人 国立環境研究所
環境情報部 情報管理室
椎名 愛里 氏

POINT

- 最新の政府統一基準に準拠するためEDR観点を加えたエンドポイント保護へ移行
- 攻撃者が我々の勤務時間に合わせて動く訳ではないと、24時間365日の脅威ハンティングも採用
- ゼロトラストアーキテクチャの実装という意味でもフルクラウドでの稼働を重視
- 管理の簡素化に向け、ワンプラットフォームで多様な機能を実現する拡張性を評価

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/**