voices

CrowdStrike 導入事例

株式会社NTTデータ

グローバル14万人のエンドポイントを守る 単一ソリューションにCrowdStrike Falconを採用

NTT DATA

株式会社NTTデータ

業種

情報・通信業

所在地

東京都江東区豊洲3-3-3
豊洲センタービル

株式会社NTTデータ

日本電信電話（NTT）のデータ通信事業本部から誕生したシステムインテグレータ。NTTグループ主要5社の一つで、情報サービス専業企業として日本最大手企業である。国内外に300社を超えるグループ企業を持ち、ITを用いて新たな「しくみ」を創造し、社会や組織の発展を支援。現在は「Trusted Global Innovator」をグループビジョンとして掲げ、デジタルを活用した新たな市場の創出、グループの力を結集したより質の高いサービスの提供のため、たゆみなく技術革新を続けている。

URL：https://www.nttdata.com/jp/ja/

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 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：2020年1月

グローバル規模のセキュリティ底上げで ゼロトラストアーキテクチャ構築を決断

日本で最もグローバルなシステムインテグレーションビジネス企業 株式会社NTTデータ。創立から33年を迎えた現在、グループ全体で14万人を超える社員が、世界55の国と地域、200を超える都市でサービスを展開している。このうち日本で働いているのは約4万人。社員の数はグローバルの方がはるかに大きな比率となっている。

同社には、NTTデータグループの事業を技術で支援する技術革新統括本部という本社組織がある。日本のみならず世界のグループ企業を対象としており、一般的な情報システム部門とは異なり、顧客企業に対しても積極的に提案活動を行う。

株式会社NTTデータ 技術革新統括本部 システム技術本部 セキュリティ技術部長 本城啓史氏は、この統括本部のセキュリティ領域責任者である。同社のセキュリティガバナンス方針について、本城氏は次のように語る。

「一言でいえば『グローバル全体でセキュリティレベルの底上げをすること』。1か所でも弱い拠点があれば、そこが狙われてしまうからです」つまり、組織を守るためにはどこにもスキを作らないということが重要なのだ。

ただ、世界中に14万人もの社員がいれば、環境も異なれば、ワークスタイルも異なる。セキュリティの底上げといっても簡単ではない。2018年当時、北米の現地法人ではすでにリモートワークが普及していた。日本においてもクラウド利用が広がり、これなしには仕事にならないという社員も出始めていた。もはやオフィスの中のIT環境さえ守ればいいという境界型防御では立ち行かなくなると判断、同社はいち早くゼロトラストアーキテクチャに着目し、構築を決めた。そして、ID管理や認証管理などを含め、14万人を守るセキュリティ基盤はどうあるべきか検討が進められた。

多機能でグローバル調達が可能な CrowdStrike Falconを採用

エンドポイント保護ももちろん、ゼロトラストアーキテクチャの重要な構成要素だった。世界のグループ企業の一部ではすでに、次世代アンチウイルスソフトやこれにEDRを加える形で強化を進めていたところもあった。一方、日本ではVDIを全面的に導入しており、シンクライアント端末を利用することでセキュアな環境を実現していた。しかし、今回はグローバル導入を重視し、全拠点で一様に利用できるテクノロジーを新しい目で選択しなおすことにした。例外を作ると、セキュリティ運用も、監視や分析の“ものさし”も、揃わなくなってしまうからだ。また、システム選定を進めている、まさにそのときにコロナ禍が勃発。リモートワークシフトでVDIが使い続けられるかどうかは、まだ定かではなかった。

こうしてエンドポイント保護製品を新たに選び直すことになった同社は、大きく2つの要件を挙げた。1つは当然のことながら、グローバル調達が可能であることだ。14万人の社員の環境を守るのに、どこかの国では使えない、販売していない、というのでは採用できなかった。もう1つは性能・機能がすぐれていることだ。同社はシステムインテグレータであり、“ベスト・オブ・ブリード”を組み合わせて顧客に提案するのが仕事。自社で利用するものであっても、自信を持って顧客にも勧められるかどうかは重要な視点だった。

それだけに、選定プロセスにも時間をかけた。まず、先行して市場調査に当たっていた北米の現地法人が候補を挙げた。また、世界各国のCISOたちも別の角度から意見を述べた。結果的に5つの製品・サービスがリストに残り、その中から議論の末に選ばれたのがCrowdStrike Falconだった。本城氏は選定の理由を次のように語る。

「NGAVから脆弱性管理まで、1つのプラットフォームで非常に多くの機能が実現されていることを評価しました。ことエンドポイント保護に関してはCrowdStrike Falconに任せられる、と思えたのが大きかったですね。またサーバ管理の必要がないクラウド型サービスであったこと、対応OSが多かったことも選定を後押ししました。95%ぐらいはWindowsなのですが、Macを利用する部門もあり、社内にはLinuxサーバも

多く、これも欠かせないポイントでした。価格競争力という点で他のものを推す声も、実はありました。しかし、ここで変な妥協をすべきではない、と。将来的にお客様にもお勧めするかもしれない製品を、安価だからという理由で選ぶわけにはいきませんでした」

しかも、同社はCrowdStrike Falconのほとんどすべての機能を選択した。その内訳は、次世代アンチウイルスFalcon Prevent、EDR製品であるFalcon Insight、プロアクティブな脅威ハンティング である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、脅威インテリジェンスの充実のためのFalcon Xとなる。

「多くの機能を選択したのは、エンドポイントに関して全方位の視野が欲しかったからです。次世代アンチウイルスやEDRだけでは、監視して、なにか検知したら対応するというだけに終わってしまいます。たとえば、IT資産管理でどこにどんなエンドポイントがあるのかを抜け漏れなく把握したり、デバイス制御で怪しいものとは接続できないようにしたりと、侵入前提で対策は行うのですが、それと並行して十分な水際対策体制も整える必要があると考えました」本城氏はこのように語る。

高い技術力を活かし
独自のセキュリティ運用体制を構築

2020年1月、同社は正式に導入を決定し、北米から順に実装をスタートさせた。現在、国外に関しては、対象10万人のうち9万人のエンドポイント端末にエージェントがインストールされた。また、日本でもVDI環境からセキュアFATへの移行を急速に進めている。2022年3月には全世界9割に当たる社員への導入をすませ、次の1年で全面導入を果たす予定となっている。

その運用にあたっては、まずは小規模なPoCを繰り返してナレッジを蓄積、今では完全に一つの体制が確立された。大きく米国、欧州、日本の3拠点でセキュリティ運用チームを組織、チームごとに構築したセキュリティ管理基盤には、Falcon PreventやFalcon Insightなどから上がってくるログ情報を集め、監視・分析を行う。そのレベルは、Tier1～3まで3階層あり、重要と思われるインシデントは1から3へとどんどんエスカレーションさせていく。当初はすべての階層を人が見ていたそうだが、CrowdStrike Falconを含めたセキュリティ製品のログ分析の自動化を積極的に進め、現在ではTier1を自動化。これにより、T2/T3チームあたり20数人いたメンバーを10人にまで削減することができた。米国、欧州、日本以外にも、たとえばアジア・中国を管轄する小規模チームが存在し、そこではTier2に専念、重要インシデントに関してはTier3にエスカレーションするという形を取っているという。

CrowdStrike Falconを専任で運用する担当者はいないという同社だが、それでも個々の機能はよく活用されている。たとえば、自動分析とヒューミントを組み合わせた脅威インテリジェンスサービスのFalcon X について本城氏は「脅威のトレンドを知るのに有益」と語る。

「私たちも技術者集団ですから、感度高く監視・分析を行っているという自負はあります。しかし、攻撃の度合いというのは一定ではなく、常に変動があります。『今はこういう攻撃が増えている』『こういう組織に注意』という情報はいくらあっても多すぎることはないので、いつも参考にしています。もう1つ、私たちが絶対的にカギだと思っている機能に、デバイス制御があります。コントロールできるということが重要です。水際対策の観点からは外部デバイスはすべて禁止したい。しかし、『指紋認証デバイスを使いたい』『業務上どうしてもUSBのやりとりが必要』といった声も挙がってくるので、それらに応えることのできる環境をFalcon Device Controlは与えてくれます」

自由度と生産性を確保しながら
安全に働ける環境が整備

導入開始から約2年が経過した。NTTデータのエンドポイント保護は、CrowdStrike Falconでどのように変わったのだろうか。

「セキュリティ製品の効果測定は難しいものですが、まずは現時点で侵入インシデントは発生していないという事実があります。もう1つ、安全に、自由度高く、生産性も高く、働ける環境が整ったということもいえると思います。この先コロナ禍がどう展開するかはまだ予測できませんが、もし終息したとしても、もう全員出社という世界に戻ることはないでしょう。リモートワークの可能な社員が、当たり前のようにそれを行使できるようになったというのは大きな前進です」

エンドユーザーには、まだ利点がある。アンチウイルスソフトを使っていた時代には、スキャニングが業務生産性を下げていた。特に同社は、健全な労働環境を遵守するために、夜間のPC起動が許可されていなかったため、どうしても就業時間中にスキャンが始まってしまう。それがCrowdStrike Falconでは起こらず、エンドユーザーに存在も気づかせないから業務を妨げないのだ。さらにVDIからセキュアFATに切り替えたエンドユーザからは、「こちらの方がはるかに使い勝手がよい」と歓迎の声が挙がっているそうだ。

今後、同社は全面導入に向けてギアを上げるとともに、グローバルのNTTグループや顧客企業にもCrowdStrike Falconを勧めていく。実際、すでに引き合いは数多く寄せられているといい、CrowdStrike FalconはNTTデータにとって「お客様にこそ届けたいエンドポイント保護ソリューション」となっている。

株式会社NTTデータ
技術革新統括本部 システム技術本部
セキュリティ技術部長
本城 啓史 氏

POINT

- グローバル規模のセキュリティ底上げでゼロトラストアーキテクチャ構築を決断
- エンドポイント保護施策としてCrowdStrike Falconをほぼフルスペックで導入
- 独自に確立したセキュリティ運用体制の中でCrowdStrike Falconを活用
- 今後はグローバルのNTTグループ企業や顧客企業へも推奨予定
- VDIからセキュアFATに切り替えた社員より、業務を妨げず、はるかに使い勝手がよいと評価

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/**