CrowdStrike 導入事例

CROWDSTRIKE

鴻池運輸株式会社様

情報システム改革でデジタルワークを推進する
鴻池運輸のセキュリティ戦略

鴻池運輸の情報システムはかつて、日本企業の多くがそうであったように「従業員がオフィスで働くこと」を前提としたものだった。

社内の閉域ネットワークを信頼し、インターネットゲートウェイはセキュリティアプライアンスにより境界のセキュリティを確保、エンドポイント端末はデスクトップPCやノートPCが中心で、社外に持ち出すモバイルPCは必要な時に貸し出されていた。

業務システムは適材適所でその都度導入、オンプレミスシステムを置くデータセンターが4カ所存在し、それぞれのシステムに複数のベンダー、複数の通信事業者が関わりサイロ化していた。エンドポイント端末は統一されておらず、アンチウイルスソフトも複数利用、海外拠点のIT管理は現地に一任されているなど、ITガバナンスと総合的なセキュリティを効かせにくい状態に陥っていた。

このような状況に経営トップは危機感を覚え、抜本的な改革に取り組む。改革の一つとしてエンドポイント端末のモバイル化を進めていたことで、新型コロナウイルス感染症（COVID-19）対策としていち早く全面テレワークに舵を切り、本社部門出社率ゼロを達成した。鴻池運輸は、クラウド化やモバイル化といったIT施策においてどのようなセキュリティ戦略を取っているのだろうか。

抜本的な情報システム改革、ワークスタイル変革に向けた取り組みも

“これから日本はますます少子高齢化が進み、人口が減少する中、請負・物流サービスといった業態は、より積極的なIT投資で労働生産性を上げなければ立ち行かなくなる。国内経済が縮む分、海外事業に大きな軸足を置く必要があるのにITが現地任せというのでは困る”。そう考えた鴻池運輸の経営トップは、IT部門のてこ入れを始めた。そこで招かれたのがCIO（最高情報責任者）経験を有する小河原 茂氏（執行役員 ICT推進本部本部長、コウノイケITソリューションズ代表取締役）だった。2018年4月、ICT推進本部本部長に就任した小河原氏は、抜本的な改革に着手した。

小河原氏は、全体戦略の基本を「デジタルイノベーション」と「クラウドシフト」に定めた。データセンターやネットワーク、エンドポイント端末、共通ソフトウェアなどをできる限り集約し、集中購買によりコストダウンと運用管理工数の減少を図った。また、グローバル管理を可能にし、情報システム部門を運用管理から解放して“攻めのIT”に専念させた。コアビジネスに属さないものはなるべくSaaS（Software as a Service）といったクラウドのサービスを活用し、コアビジネスに関わる基幹システムも内製を強化しながら将来的にクラウドを目指すことになった。

エンドポイント端末には、場所を選ばず働けるようにWebカメラとLTE対応の軽量小型ノートPCを標準機種として採用した。業務をサポートするクラウドサービスとして、Webミーティング「Zoom」に加え、ビジネスチャットやクラウドストレージなどのクラウドツールの展開も進めている。ただし、場所を選ばず働ける環境では、セキュリティは万全を期す必要がある。社外での業務で利用するネットワークは、安全ではない可能性があるからだ。

そのため、鴻池運輸の佐藤 雅哉氏（ICT推進本部デジタルトランスフォーメーション推進部長代理）は、ネットワークセキュリティとエンドポイントセキュリティの両面から対策することを決めた

エンドポイントデバイス利用がセキュアであってこそのワークスタイル変革

ネットワークセキュリティを担うものとして選ばれたのは、クラウド型セキュアWebゲートウェイサービスを提供するZscalerだった。

それでは、エンドポイントデバイスのセキュリティはどうするか。「水際対策のみのアンチウイルスソフトでは

導入製品

- **CrowdStrike Falcon Insight** EDR
- **CrowdStrike Falcon Prevent** 次世代アンチウイルス
- **CrowdStrike** Falcon OverWatch 驚異のハンティング
- **CrowdStrike Falcon Discover** IT衛生管理
- **CrowdStrike Falcon Spotlight** 脆弱性管理

鴻池運輸株式会社

所在地：大阪本社　大阪府大阪市中央区伏見町4-3-9
東京本社　東京都中央区銀座6-10-1

導入時期：2019年6月

URL：https://www.konoike.net/

鴻池運輸は、製造業やサービス業をサポートする請負サービスと、国内外のあらゆるニーズに対応する物流サービスを展開する企業だ。多角化を図りながら事業規模を拡大し続け、2020年には創業140周年を迎えた。近年は、製造業向けの物流に加えてアパレル、食品、メディカル、空港事業にも力を入れている。港湾物流にも精通しているため早くから海外進出し、北米・中米、アジア地域を中心に35拠点、国内外約2万5000人の従業員を擁するグローバルカンパニーとなった。

KONOIKE GROUP　KONOIKE

脅威が高度化している今日の実情に合っていない」と佐藤氏は考え、侵入を前提として対策を図るEDR（Endpoint Detection and Response）に主眼を移した。

複数のサービスの中から調査機関のGartnerが高評価を付けた2つに候補を絞り、それぞれを評価した結果、「CrowdStrike Falcon」を採用した。佐藤氏は選定の理由を次のように語る。

「当社において、特に現場では多くのITシステムが稼働しており、ITリテラシーも部門によって異なるため、導入が容易で、既存システムとのコンフリクトが起きないことを重視しました。一方、セキュリティとして、レジストリの変更やディスク、メモリへのアクセスなど深いところまで見てほしかったので、カーネルレベルで動作するCrowdStrike Falconは当社に合っていました。選定の段階では、ファイルやフォルダの検知対象除外を設定することなく、そのまま利用できることも高く評価しました。スクラッチの自社開発システムのモジュールなどは過検知の対象になるケースもありますが、除外すればそこがセキュリティリスクになるため、最小限に抑えられる点も重要なポイントでした。」

CrowdStrike Falconは、1つのエージェントで多くのエンドポイントに必要なセキュリティ機能を提供するのが特徴だ。鴻池運輸は、EDRである「Falcon Insight」のみならず、次世代アンチウイルスの「Falcon Prevent」、リアルタイムで不審な振る舞いを検出しサイバー攻撃を検知するプロフェッショナル脅威ハンティングチームが提供する「Falcon OverWatch」、IT衛生管理の「Falcon Discover」、脆弱（ぜいじゃく）性管理の「Falcon Spotlight」など5機能を導入した。

こうして従業員が分からないところでセキュリティが確保されている環境を構築していった。東京での夏季の大規模イベント開催に照準を合わせて体制を整備していたところ、新型コロナウイルス禍が勃発した。

コロナ禍でいち早い全面テレワーク実現、本社部門出社ゼロを達成

鴻池運輸は、政府による緊急事態宣言を待たず、2020年3月末から本社部門をテレワークに移行した。もともとITによるワークスタイル変革を推進していたことと、夏季に予定されていた大規模イベントに向けてテレワークの準備を進めていたことが功を奏し、一気に舵を切ることができた。

しかし、いざ蓋を開けてみると想定外の事が起きた。一部の従業員は、テレワークを予定していなかったため、デスクトップPCや大きな画面を確保できる重量級ノートPCを使用しており、テレワークに即座に移れなかった。

担当するIT部門は、本来持ち出す想定でなかったノートPCのセキュリティ対応、通信環境の手配と、一部で利用していたクラウド型仮想デスクトップサービスの「Amazon WorkSpaces」を急きょ拡大展開するなど、通常業務を脇に置いて奔走したという。そのかいもあって、大阪本社と東京本社では出社率ゼロを達成した。

IT部門側も、PCのセキュリティに関して、CrowdStrike Falconを導入したことで、既存のアンチウイルスソフトは必要なくなった。複数の対策を取らなければならないPCセキュリティが、1つのエージェント、1つのコンソールにまとまったことで利便性が上がり、よりシンプルな管理とユーザビリティを下げない良いバランスを確立できた。

情報システム改革により、デジタルワークを推進する鴻池運輸。小河原氏はセキュリティについて次のように語る。

「グローバル拠点の管理を実現するためにもクラウドシフトは必然です。セキュリティに関しては、攻めのITに専念するためにも専門家に任せた方がいいと考えています。CrowdStrike Falconは、サービスを選んだというよりCrowdStrikeに長く付き合えるパートナーの役割を務めてもらいたいと思って選びました。セキュリティ分野は進歩も速いので、イノベーションに努め、常にアナリスト機関から高評価を獲得し続ける存在であることを期待しています」

鴻池運輸は今後、海外拠点のエンドポイント端末に対しても、2021年3月をめどにセキュリティ対策を進めていく予定だ。「コロナ禍がどこまで長引くか不明な中ではありますが、従業員の生産性や利便性に直結するIT施策をこれからも積極的に仕掛けていきます」と小河原氏は明言した。

POINT

- コアビジネスに属さないものはなるべくSaaS(Software as a Service)といったクラウドのサービスを活用
- AVでは脅威が高度化している今日の実情に合っていないと、侵入を前提として対策を図るEDRを検討
- PCセキュリティが、1つのエージェント、1つのコンソールにまとまり、利便性が上がり、よりシンプルな管理とユーザビリティを下げない良いバランスを確立
- コロナ禍でいち早い全面テレワーク実現、本社部門出社ゼロを達成

鴻池運輸株式会社

執行役員　ICT推進本部本部長
コウノイケITソリューションズ代表取締役

小河原 茂氏

鴻池運輸株式会社

ICT推進本部
デジタルトランスフォーメーション推進部長代理

佐藤 雅哉氏

クラウドストライク 株式会社
〒104-0031 東京都中央区京橋2丁目2-1 | crowdstrike.jp

2020年6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。