株式会社MCCマネジメント
IT・ロジスティクス推進本部 IT部 データ・基盤課 課長 野田 裕氏

“運用の優劣で価値が決まる”EDRプロジェクトに伴走。全社のPCを可視化し、サーバー群への展開も進行中。

株式会社MCCマネジメント（以下、MCCマネジメント）は、EDRプロジェクトに着手。日本情報通信（以下、NI+C）を導入と運用のパートナーに選定した。NI+Cは、チャットツールを駆使することで迅速に対応し、将来参照できる記録として蓄積。定期的な報告会では、EDR製品のアップデート情報の中からプロジェクトで採用すべきものを重点的に取り上げるなど、セキュリティ支援にとどまらない密なサポートを提供している。

業種：流通・小売

MatsukiyoCocokara & Co.

MCCマネジメントは、株式会社マツモトキヨシホールディングス、株式会社ココカラファインの統合により、両社の英知を結集させ、グループシナジーを最大化させるために設立された会社となります。
これまでのそれぞれの会社にあった商品仕入機能やプライベートブランド商品の企画・開発機能に加え、販売促進機能などを集約し、グループのマーチャンダイジング戦略の策定と実行を行います。
また、店舗開発や店舗運営支援機能など、グループ内のノウハウや成功事例を活用し、各グループへの水平展開を図る役割も担います。

本　社	〒101-0062 東京都千代田区神田駿河台4丁目3番地 新お茶の水ビルディング2階
設　立	2021年2月18日
資本金	1億円
URL	https://www.matsukiyococokara.com/

EDRで必要十分なレベルのセキュリティを適切に運用することを目指す

MCCマネジメントは、ドラッグストアチェーン大手のマツモトキヨシホールディングス（以下、マツキヨGP）とココカラファイン（以下、ココカラGP）の経営統合により設置された統合シナジー創出のための戦略会社だ。旧マツキヨGPと旧ココカラGPで共通化する方がより有効になると判断できるビジネス領域は、すべて同社が担当。人事や採用、財務経理や総務はもちろん、情報システムもその業務範囲になる。システムの共通化を進めることは、コスト削減と業務の効率化につながり、さらに同じシステムを利用することで人材交流が加速するなどの効果も期待できる。

同社のIT部門には、「データ・基盤課」が設置されている。データ基盤ではなく、データと基盤を分けている点に特色があり、データウェアハウスなどのデータそのものを扱う業務と、インフラやネットワーク、セキュリティ基盤を扱う業務をどちらも担当する。統合前の2社は、当然ながら別々のITインフラを運用しており、セキュリティポリシーも個別に規定していた。統合後は、全社共通のセキュリティ方針を策定して施策を推進する方向にあり、データ・基盤課としては多面的に情報収集を行うことになった。

IT・ロジスティクス推進本部 IT部 データ・基盤課 課長 野田 裕氏は、「世の中の動向を踏まえつつ、上場企業として社会的な責任に応えるためにクリアすべき基準を慎重に検討しました。そのうえで、社内のシステムとデータを守り、万が一侵入された場合でも被害を最小限に食い止められること、そしてコストと効果のバランスが最も優れた対策は何かという検討をしていました」と話す。

その結果、MCCマネジメントは全社共通のセキュリティ基盤として、EDR（Endpoint Detection and Response）がニーズに合うと判断した。EDRは、PCやサーバーなどのエンドポイントデバイス上で行われる不正な活動を検知し、迅速に対応するためのセキュリティソリューション。IT・ロジスティクス推進本部 IT部 システムサービス課 兼 データ・基盤課 課長代理 大嵩 真人氏と同課 主事 平 誠氏の2人はEDRについてより深く知るため、さまざまなセミナーに参加するなどの情報収集を行った。

大嵩氏は、「EDRを採用する方向性は定まりましたが、私たちにとって全く初めての経験です。人的なリソースも限られており、当時の体制ではソリューションの導入や運用を社内だけで実行することは現実的ではありません。そこで、EDR製品を比較するのではなく、運用を含めて一緒にやってくれるパートナーを探すことにしました」と話す。

PoCで2社のサポートを体感した上で、NI+Cを採用

パートナー選定にあたっては、運用能力に期待できるシステムインテグレーターを中心に幅広く提案を打診した。複数社からの提案内容を書類ベースの選考で5社に絞り込み、2023年夏ごろにはプレゼンテーション形式で3社から最終提案をしてもらった。そこで2社に絞り、2023年11月からPoCを実施。その結果で最終判断することになった。

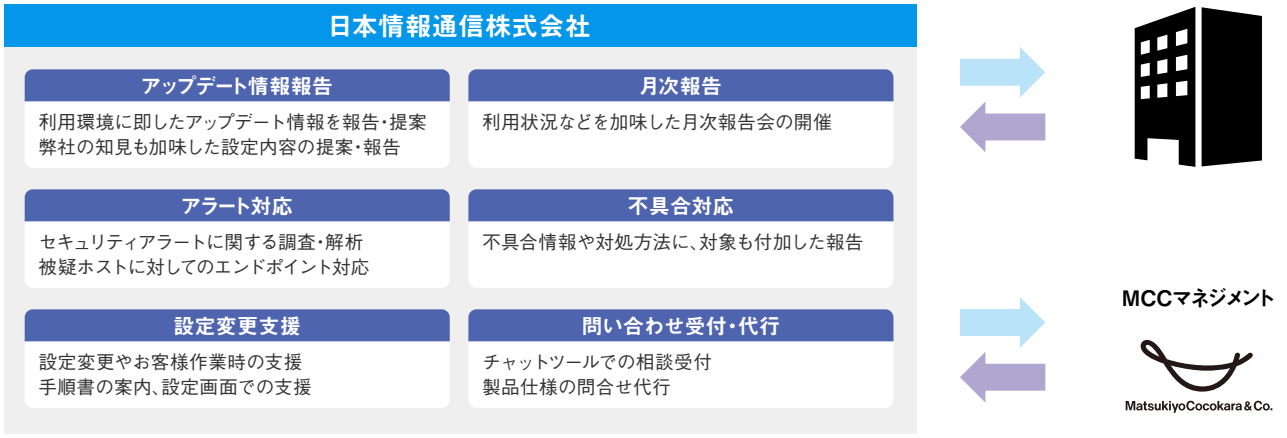
大嵩氏は、「私たちは、セキュリティの専門家ではありません。職場はデータ・基盤課ですが、EDRについての知識は一般人に近いのです。そういう人たちがEDRで検知する情報に基づいてさまざまな判断を下せるようなサポートが欲しかった。つまり、うまく情報を伝えてくれたり、対応方針を提案してくれたりできるのかどうかを実体験したいと考えました」と話す。

PoCをやることで、使用するEDR製品についても、カタログスペックで機能を並べるだけではわからないところが見えてくる。管理画面だけを見ても、実際に動いているところを触って初めてわかることがある。今回、NI+Cが運用サービスとセットで提案したEDR製品は、NI+C社内で使っているもので、NI+C自身がユーザーとしての豊富な知見を持っていた。PoC期間中に疑問を感じることがあれば、「弊社ではこのように対応しています」というリアルな話を聞くことができた。EDR製品のすばらしさも欠点も知った上で、欠点を包み隠すことなく誠実に話をしてくれた。

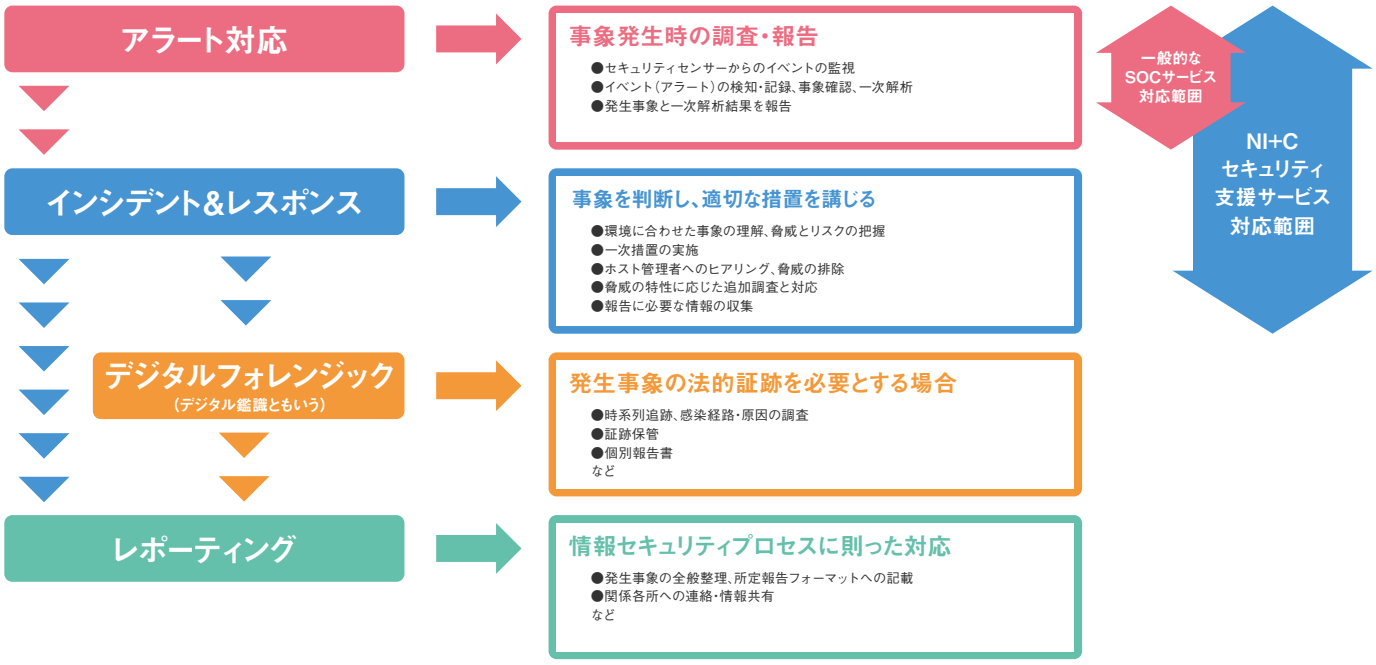
PoC期間中に目立って大きなトラブルはなかったため、万一の際にどのようにサポートしてくれるのかは体験していないが、それでも、NI+Cの運用体制の価値を十分に理解できた。定期的な報告会を開催し、優れた内容のレポートを仕上げてくれた。EDR製品のバージョンアップがあれば、内容をすべて報告するのではなく、要点を整理し、使った方が良い新機能などを的確に提案してくれた。また、NI+C自身がユーザーであるため、EDRベンダーとの連携が密に取れているように感じられ、レスポンスが速かった。

「NI+Cさんをパートナーとして連携できれば、万一の際にもEDRベンダーと二人三脚で対応してくれそうだという安心感を得ることができました」（平氏）

NI+Cセキュリティ支援サービスのサービス構成例



セキュリティインシデント対応におけるNI+Cセキュリティ支援サービスの対応範囲



イレギュラー対応時には詳細の手順書を用意

2024年に入ると正式にNI+Cをパートナーに選定することになり、PoC環境をベースに全社のEDR基盤へと発展させる形でプロジェクトは開始された。準備期間を経て端末へのエージェント配布を本格化し、本部の従業員が使うPC、店舗のPCへと展開。同時に、段階的にサーバー群への配布も進めている。

ライセンスは年間契約し、展開予定を見定めてNI+Cがコストと余裕のバランスを見たライセンス数を提案してくれている。稼働させるソフトウェアが限定的なPOSを対象外とするなど、現場の利用方法を工夫することで、ライセンス費用を抑えながら必要十分なセキュリティを担保することを目指している。

プロジェクトはすべてが順調に進んだわけではない。エージェントをPCに配布するだけでも苦労はあった。基本的に、“一般的な業務で使うWindows PC”への配布は、NI+Cの手を借りずに実行できるようになってはいる。ただ、特殊なマシンやサーバーへのインストールにあたっては、手動で実施する必要が出てくるケースがある。

大嵩氏は、「OSによってインストール手順が異なるため、たとえば“MacBookにも導入してほしい”、といったニーズがある場合はイレギュラー対応になりました。そうした際に、NI+Cの担当者さんは、エラーが発生する原因を突き止めてくれた上で、詳細な手順書を作ってくれてました」と話す。

NI+Cは、リモートでMCCマネジメントのスタッフをサポートする。そのために、EDRプロジェクトにかかわるすべての人がアクセスできるチャットツールが用意されており、何か相談があればだれもがそこに書き込める。書き込みを見たNI+C側は、サポートメンバーのだれかが迅速に対応することになる。「NI+Cさんのレスポンスがかなり速いので助かっています。記録が残ってバックログを見られるため、チャットツールはプロジェクトメンバーにとってなくてはならないツールになりました」（平氏）。

「EDRは、きちんとした知見と運用体制があって成り立つもの」

幸いなことに、EDRが稼働して以来、極めて重大なインシデントは発生していないというが、プロジェクトは十分な成果を得ることができている。最大の成果は、可視化だ。平氏は、「たとえば、無料の動画編集ソフトをインストールしているユーザーを発見して指摘したところ、実際に業務に必要だったケースがありました。現場もコスト意識を持っているので、以前なら強く言えなかったかもしれませんが、“セキュリティソフトが危険だと言っている”と主張できるため、抑止力が高まっています」と話します。

対応力は確実に上がってきたと感じている。大嵩氏は、「私たちも扱い慣れては来ましたが、それでも社内で判断できないケースもあります。そうした際には、NI+Cさんに相談します。中には、“検知しない設定にした方が良い”と提案されることもあり、その理由も明確に答えてくれるため納得して対策を実行できます。対応を要するインシデントがあれば、詳細な情報を伝えてくれます。NI+Cの担当者さんと直接顔を合わせる機会は少ないですが、それでもプロジェクトメンバーの一員のように感じています」と話してくれた。

EDRプロジェクトは、導入することより運用し続けることで成果を得るものだ。野田氏は、「EDRは、きちんとした知見と運用体制があって成り立つもの。どう運用できるかをわからずに走り出した私たちを、NI+Cさんはしっかり支えてくれています。いまは、ようやくEDRでできることが見えてきた段階です。今後は、万一の事態に備えた“避難訓練”を実施しながら、事態が起きれば迅速に行動し、“EDRがあって良かった”と感じられる体制を作り上げていかなければなりません。NI+Cさんには、さらなるサポートを期待しています」と現時点のプロジェクトを総括してくれました。

株式会社MCCマネジメント
IT・ロジスティクス推進本部
IT部 データ・基盤課 課長
野田 裕氏

株式会社MCCマネジメント
IT・ロジスティクス推進本部
IT部 システムサービス課 兼
データ・基盤課 課長代理
大嵩 真人氏

株式会社MCCマネジメント
IT・ロジスティクス推進本部
IT部 データ・基盤課 兼
ストアシステム課 主事
平 誠氏

＜担当より＞

エンタープライズ第二事業本部
第三営業部
小林 昭喜

提案時にネックになったのは、私たちのサポート窓口が平日9～17時のみの対応しかできなかったことでした。それでも、そのほかの部分を総合的にご評価いただき、選んでもらえて光栄です。営業担当者として少しでもお客様にご満足いただけることを願って、定例会に参加するなど、私もプロジェクトメンバーの一員として伴走してきました。現場はリモートですが、優秀な担当者が良いチームを組んでがんばってくれています。今後も有意義な情報を提供できるよう務めていきます。

セキュリティ&ネットワーク事業本部
セキュリティソリューション部
池嶋 悟

一度経験したインシデントや解決した疑問点については、お客様が社内対応できるようになることが理想ですから、それを意識して、丁寧な手順書を作るなどのサポートを続けています。EDRの運用は、日々新たな脅威が生まれ、ソリューションが常にアップデートされていく領域です。今後も、「なにかあればNI+Cに聞いてみよう」と思っていただける関係を続けていきたいと考えています。

セキュリティ&ネットワーク事業本部
セキュリティソリューション部
金城 明憲

運用担当者として多くのプロジェクトにかかわってきましたが、MCCマネジメント様は私たちへの要望が整理されていて、提案の取捨選択がうまくできていると感じます。10月には、支援サービスの一部機能を24時間365日対応できるようになる予定です。私たちもサービスを日々進化させていきますので、より密な関係を築き上げ、よりご満足いただけるサポートを提供できるようがんばっていきたいです。

NI+C
おもひをITでカタチに

関連ソリューション

NI+Cセキュリティ支援サービス
https://www.niandc.co.jp/sol/managedsecurity/

日本情報通信株式会社について

https://www.niandc.co.jp/

日本情報通信株式会社(NI+C)は、1985年にNTTと日本IBMの合弁会社として設立。システム開発から基盤構築、クラウド化への対応、社内外データ統合とAIによる分析、EDIサービスやセキュリティ、ネットワークサービス、運用保守までをトータルに提供しています。

「おもひをITでカタチに」をスローガンに、先進技術と業務に精通したプロフェッショナルの育成により、お客様の経営課題解決に貢献できる真のベストパートナーを目指しております。

NI+C 日本情報通信株式会社

お問い合わせ sec-contact@niandc.co.jp 日本情報通信株式会社 ソリューション担当

ここに掲載されている情報は
2025年7月のものです。