Case Study
McAfee MVISION ePO

McAfee
Together is power.

セキュリティ管理をオンプレミス運用からSaaS利用にシフト 最新のエンドポイントセキュリティと次世代ウイルス対策で「管理・運用の効率化」と「ウイルス対策の最新化」を両立

Point

- オンプレミスからSaaSへ管理コンソールを更改し、運用負担の軽減とコスト削減を両立
- 次世代ウイルス対策をエンドポイントセキュリティに採用し、新たな脅威に対抗
- 全ての端末をエージェントで管理し、状態の可視化と脆弱性解消を実現

新たに次世代ウイルス対策を導入し 非マルウェア攻撃やゼロデイに対応

ラテン語で「成長する」という意味の名を持つ株式会社クレスコ（以下、クレスコ）は、創業30年以上の歴史を持つ独立系システムインテグレーター（SIer）だ。基盤構築と組込みソフトウェア開発を強みとし、ビジネスアプリケーション事業、基盤事業、組込み事業、サービスビジネス事業を4つの柱とする。

年間約900件のプロジェクトの約9割がリピートオーダーを主体とした受注だという同社は、さまざまな機密情報の慎重な取り扱いと厳格な情報管理を徹底し、大手企業から高い信頼を寄せられている。特に情報セキュリティに関しては、社内に内部統制委員会および情報セキュリティ委員会を設置し、各種ポリシーや規程を整備して情報インフラの更改やマネジメント体制の強化などを不断に行っている。

その一環で、同社は2000年からMcAfee製品を活用し、いくつかの変遷を経て、最近までオンプレミスの管理サーバーである「McAfee ePolicy Orchestrator on-premises（以下、McAfee ePO）」と、「McAfee VirusScan Enterprise（以下、VSE）」を活用。2019年9月からはSaaS型セキュリティ管理コンソールの「McAfee MVISION ePO（以下、MVISION ePO）」と、VSEの後継となる「McAfee Endpoint Security（以下、ENS）」に更改し、さらにシグネチャ方式では検出できない未知の脅威を検出する次世代ウイルス対策モジュール「McAfee Endpoint Security Adaptive Threat Protect（以下、ENS ATP）」も導入した。

McAfee製品をモダナイズした背景には、主に2つの目的があった。1つは、オンプレミス運用からSaaS利用によるクラウド運用への転換。McAfee ePOではサーバーを設置して管理・運用することが大きな負担となっていた。また、クレスコはSIerとしてお客様環境にPCを持ち込むケースも多いが、McAfee ePOではPCのエージェントと通信が発生するため、お客様環境への影響を懸念して一部の端末にはエージェントをインストールすることができなかった。そのため、マルウェアを検知してアラートが上がってもそれをすぐに確認できず、管理面で大きな課題があったという。

クレスコ デジタル変革推進室 室長 原 喜孝氏は、「MVISION ePOは、サブスクリプションのライセンス形式となり、クラウド化を進める当社の方針に合致していたほか、インターネットにつながっていればPCの管理ができるため、常時状況を把握できることが大きなメリットになると考えました」と語る。

もう1つは、次世代ウイルス対策の導入。サイバー攻撃の手法が日々進化する中、非マルウェア攻撃やゼロデイ攻撃などの新たな脅威に備えることが喫緊の課題となっていた。クレスコ デジタル変革推進室 アドバンストジェネラルスペシャリスト 小島 真一氏は、「他社のEDR（エンドポイントでの脅威検知と対応支援）やエンドポイントセキュリティ製品などさまざまな手法を調べましたが、端末の数に応じた追加コストが大きな障害でした。今回MVISIONを検討した際、旧来のVSEで対応していたウイルス対策がENSで強化されることに加え、非マルウェア攻撃やゼロデイ攻撃に対応した次

User Profile

CRESCO

株式会社クレスコ

所　在　地：〒108-6026
東京都港区港南2-15-1
品川インターシティA棟 25階～27階
U　R　L：https://www.cresco.co.jp/
導入時期：2019年9月

1988年にIT基盤システム構築会社とマイクロコンピューターシステム開発会社が合併して誕生。現在は、アプリケーション開発技術、プラットフォーム構築技術、組込み技術3つを中核に先端技術（AI、IoT、ロボティクスなど）を加えた多様な技術領域を有し、幅広いITサービスを提供する独立系システムインテグレーターとして発展。主要顧客は、銀行、保険、流通、旅行、運輸、人材紹介、自動車、家電、医療機器など幅広い。

【導入製品名】
McAfee MVISION ePolicy Orchestrator
McAfee Endpoint Security
McAfee Endpoint Security Adaptive Threat Protect

株式会社クレスコ
デジタル変革推進室
室長
原 喜孝 氏

株式会社クレスコ
デジタル変革推進室
アドバンストジェネラル
スペシャリスト
小島 真一 氏

MACNICA
https://www.macnica.co.jp/

世代ウイルス対策を利用できることに大変注目しました」と話す。

MVISION ePOへの更改は短時間で完了 残る課題はENS ATPのチューニング

2019年4月に更新のタイミングで新旧の切り替えを開始。VSEの環境にあるユーザーを新しいENSに移行する際にはMVISON ePO用のエージェントソフトウェアを既存PCに上書きインストールすることで、トラブルもなく短時間で移行作業が完了したという。

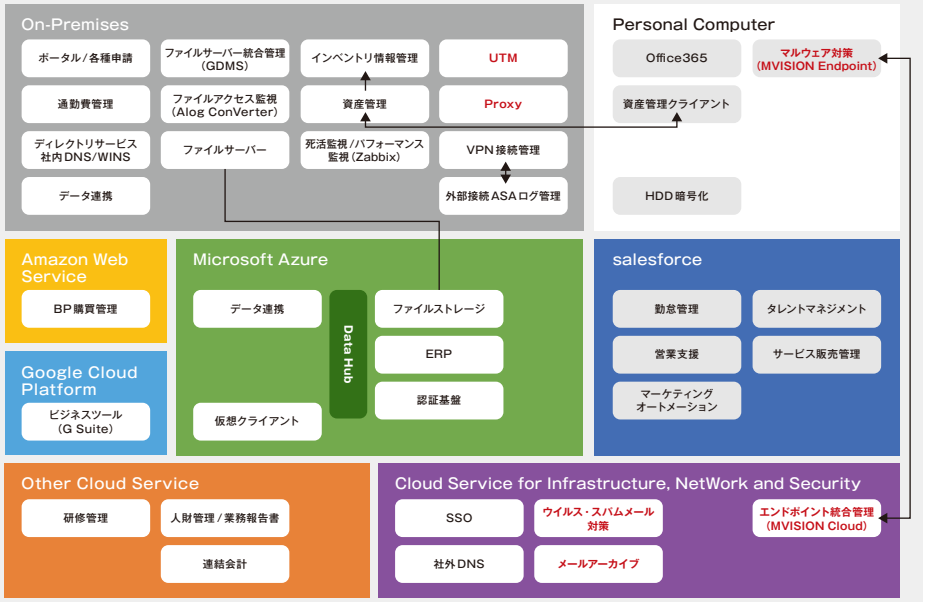
小島氏は、「当社は元々McAfee Endpoint Threat Protection（ETP）ライセンスを保有していました。MVISIONライセンスに乗り換えた後も移行期間としてETPの保守料金が1年間無料となったこともメリットでした。社内のユーザー数が多く、社外勤務を含めたカバー範囲も広いため、ENSへの移行をポータルで通知しても周知徹底するまでにタイムラグが生じてしまうのです。今回時間を十分に取ることができたことは大きな安心感につながりました」と述べる。

しかし、次世代ウイルス対策のしきい値設定が課題として残った。クレスコの社内には開発系や管理系のさまざまな独自アプリケーションが存在し、それらが軒並み“疑わしいもの”として誤検知され、アラートが大量に上がってしまったのだ。「本来は、新しいアプリケーションを作るたびにホワイトリスト化すべきなのですが、数が多く、全てを網羅することが困難でした。そのため、マクニカネットワークスからアドバイスを得ながらチューニングを進め、機能別にグループ化して既知のものはホワイトリスト化するなど、今後も最適な値を慎重に探っていく予定です」（小島氏）

オンプレミス運用からSaaS利用に変更し 目標とするクラウドファーストを促進

2019年9月、MVISION ePO、ENS、ENS ATPは本格的に運用を開始。それにより、次の3つが変化として実感できたという。第1に運用・管理の効率化。原氏は、「オンプレミス運用からSaaS利用に

社内システム全体イメージ図（セキュリティ観点）



変更することによって、サーバー運用・管理の負担が大幅に削減され、全てのインフラをクラウドに移行するという“クラウドファースト”を促進させることができました。それによりコスト削減にも少なからず貢献しています。端末管理がクラウドから可能になったので、非常に運用がしやすくなったことも大きなポイントです」と高く評価する。

第2にウイルス対策の最新化。近年はクレスコのような大手企業と取引のあるサプライチェーンへの攻撃が増える中、ENSとENS ATPの活用で未知のウイルスに対する備えやゼロデイ攻撃にも対応し、安心感は増しているという。小島氏は、「インターネットの出入り口やメールは多段・多層防御を講じて比較的分厚くセキュリティ対策は行っているものの、最後の砦はやはりエンドポイントです。今回ENSとENS ATPに乗り換えたことで安全性はさらに強化されましたが、100回誤検出しても1度として本物をスルーさせないことが社内のセキュリティとしては望ましいという立場で、これからも厳しく運用していくつもりです」と話す。

そして第3が全ての端末の可視化。VSEの運用時は、エージェントを入れる端末、入れることのできない端末が混在し、手動で管理していたが、MVISION ePO管理になったことで全ての端末を対象にエージェントを介した管理が可能になった。これまで見えづらかった端末も、見えるようになったことは脆弱性の解消に向けた大きな前進だと捉えているという。

クレスコでは今後、社員やビジネスパートナーも増え続けていく傾向にあることを前提に、ライセンスの追加契約を検討している。また、テレワークや在宅勤務の機会が増えることも想定し、MVISION ePOのライセンスを活用した自宅PCの業務利用の可能性を探っていく考えだ。さらに、現在スマートフォンを業務で活用しているが、より安全な利用環境を実現する「MVISION Mobile Advanced」の活用も検討の俎上に上げていくという。

今回のプロジェクトを振り返り、原氏は、「MVISION ePOとENS、ENS ATPの導入により、クラウドシフトによる運用管理の効率化や、未知マルウェア対策、トータルコストの削減などが同時に実現でき高く評価しています。マクニカネットワークスからのサポートも密に受けられたことでマイグレーションも無事成功しました。まだ次世代ウイルス対策のチューニングが課題として残っていますが、今後もMcAfee製品に関する知見の蓄積とサポートの充実を期待しています」と語る。

https://www.macnica.co.jp/
MACNICA
株式会社マクニカ　ネットワークス カンパニー
〒222-8563 横浜市港北区新横浜1-5-5
TEL.045-476-2010　FAX.045-476-2060
西日本オフィス
〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL.06-6227-6916　FAX.06-6227-6917