Canon

Solution REPORT
ソリューションレポート

導入事例 株式会社フューチャーイン 様

FortiGateとキヤノンが提供するインシデント分析サービスDIASS※1が高度なセキュリティ環境を実現

ハードウェアの販売からシステム構築、そして保守メンテナンスまで、IT関連サービスをワンストップで提供するフューチャーイン。自社のネットワーク機器切り替えをきっかけに、FortiGateと組み合わせたセキュリティ・インシデント分析通知サービス「DIASS」などを導入することで、より高度なセキュリティ環境を構築。より安心・安全な環境で顧客のDXを推進・支援することができるようになった。

課題

- 多様化する脅威に対抗できるようなより堅固なセキュリティ対策を講じたい
- 自社がどの程度のセキュリティ脅威にさらされているのか客観的に把握したい
- ネットワーク機器保守切れに伴う入れ替えをできるだけ少ない工数で実施したい

効果

- UTM機能の導入とインシデント管理ソリューションDIASSにより、常に安心できる環境を構築
- CTAPによる事前アセスメントで、従来どの程度自社が危険な状態にあったのかが把握できた
- 自社での実績があり信頼性も高いFortiGateを選択することで、必要最低限の工数で切り替えできた

＜お客さまプロファイル＞

株式会社 フューチャーイン

一般企業向けをはじめ文教や公共の各領域向けITソリューション事業、およびBPO関連の受託事業を柱として事業展開している。さまざまな領域のDXを推進・支援する立場としてDX認定を取得。DX検定にも取り組み、約8割の社員が合格するなど人材育成にも力を入れている。また、クラウド関連事業も他の事業者に先駆けて取り組みを始めた実績がある。

お話を伺った方

写真左から、北川様、野田様、落合様

株式会社フューチャーイン
取締役
管理本部長　野田 智明 様

管理本部　経営企画部
エキスパート　北川 謙司 様

システム技術本部　プラットフォーム技術部
システム構築課
課長　落合 由貴 様

導入前の課題と背景

多様な脅威に対応するためセキュリティ対策強化

以前からFortiGateをお使いだとお聞きしましたが。

「元々拠点間も含めた社内のネットワーク接続や、社内から外部のインターネットへの出口の境界線上のファイアウォールとしてFortiGateを使用していました。これまで、セキュリティ対策としてファイアウォール上での接続ポートの管理や出口のログ管理などを実施してきました。しかし、近年さまざまな脆弱性を狙った多様なサイバー攻撃が発生しており、そのような新たな脅威に対して柔軟に対応する必要性を感じていました。今回保守契約更新のタイミングで、機器の刷新に合わせてセキュリティ対策の見直しも検討することとしました」（北川様）

昨年「DX認定事業者」に認定されましたね。

「昨今の産業界の流れを踏まえて、当社でも企業のDXを支援する取り組みを推進しています。昨年2022年6月、『DX認定制度』において『DX認定事業者』として認定を取得。DX認定制度は、経済産業省が定める『デジタルガバナンス・コード』に沿ったビジョンの策定、戦略や体制の整備を行い、優良な取り組みを実施している事業者を認定する制度です。また、CISO（最高情報セキュリティ責任者）を私自らが務めるとともに情報セキュリティ基本方針を策定。さらに情報セキュリティ認証として『ISO/IEC 27001』を取得するなど、DX支援やシステム開発を通じて重要情報を取り扱う企業として、当然必要となるガバナンスやセキュリティ対策強化にも務めています」（野田様）

導入の必然性

運用実績のあるFortiGateとキヤノン独自のセキュリティソリューションを採用

今回セキュリティ機器として、従来と同様FortiGateを選択されたようですが。

「機器の入れ替えに際しては、先ほど申し上げたセキュリティ強化に加えて、通信速度の向上も図るため最新機種への切り替えが前提となりました。検討の結果、当社での導入実績があり、扱える技術部門スタッフが多いことや、一部のネットワークを二重化するなど当社の独自のネットワーク環境に合わせた設定を引き継げることから、FortiGateの後継機を選択しました。また、これまで同様の機器を何種類か使用してきた中でも、最も故障頻度が少なく信頼性が高かったのもFortiGateを選択した

要因です」（北川様）

「技術部門としては、やはり移行時の作業負荷をできるだけ抑えたかったということから、同じFortiGateへの切り替えが選択肢となりました」（落合様）

今回のキヤノンのご提案内容はいかがでしたか。

「通常の業者に手配してもらう場合、大抵はハードウェアとしてのFortiGateと必要なライセンスを納入してくるだけです。しかし、キヤノン様の場合は、日本に特化した脅威データベース『JLIST』※2によってセキュリティ機能を強化させた『SecuritySuite JL』※3や、FortiGateやJLIST、Syslogなどから得られるデータを基に状況を分析し、『DIASS』で収集したインシデントをアラート通知しレポート管理するなど、独自のセキュリティ強化ソリューションを併せて提案いただきました。また、今回最終的にキヤノン様にお願いしたいと感じた理由は、やはりその技術力の高さにもありました。FortiGateの技術研修を実施していただいたり、FortiManagerやFortiCloudなどの付帯サービスに関しての説明や問い合わせに対する回答も非常に的確なものでした。また、技術者の数のみならず、技術的な体制の厚さに特に魅力を感じました」（落合様）

運用の工夫

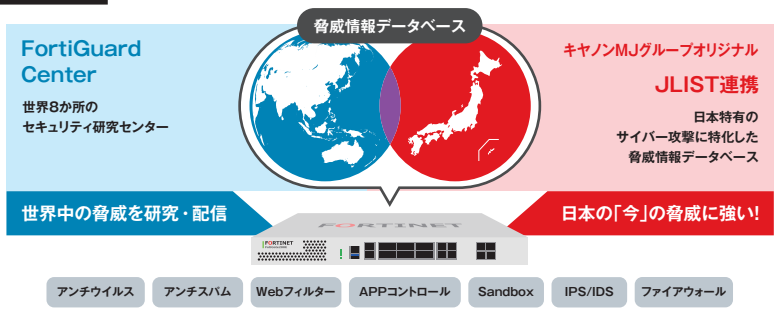
「CTAP」による事前のセキュリティアセスメントで実態を把握

新機種への切り替えはどのように進められたのでしょうか。

「2022年4月頃からFortiGate切り替えの検討を開始し、社内調整を経て同年10月に仕様を最終決定。11月からテストなどの切り替え準備を始め、翌2023年2月に主要拠点の新機器への切り替えが完了しました」（北川様）

「社内での検討期間中に、インターネットへの出入り口の部分の通信状況を、『CTAP』※4という仕組みを活用してアセスメントを実施しました。幸い当社の場合は脅威となるような通信は見つかりませんでした。しかし、企業のセキュリティ対策如何によっては、脆弱な箇所などが発見できる場合もあり、必要なセキュリティ対策を検討する段階では有効な手段だと感じました」（落合様）

サービスイメージ



取り組みの成果

UTMにより安心感のあるセキュリティ環境を実現、インシデント管理ソリューション「DIASS」活用に向けた検証を実施中

新機種への入れ替え後の状況はいかがでしょうか。

「従来はファイアウォールとしてしか機能させていなかったFortiGateですが、今回の更改後はアンチウイルスやWebフィルターなどを含むUTMとして機能させることで、さまざまな脅威に対応できるようになりました。セキュリティ事象に関しては、何も起こらないことが良い状態ですので、導入後の効果を評価するのが難しいところがあります。しかし、従来は何らかの脅威が発生していても気付かずに見過ごしているだけかもしれないという不安がありましたが、Webフィルターなどの UTM機能によって、今後は何らかの脅威が発生したとしても、そこで食い止めてくれるだろうという安心感があります」（北川様）

「分析ソリューションのDIASSに関しては、現在試用期間として内容や活用方法の検証を行っている段階です。具体的に今後どのように活用していくかを、実際のレポートを見ながら検討しています」（落合様）

IT環境整備などに関する今後の方向性について教えてください。

「VPNによるインターネット回線を持つ主要の約10拠点に関してはすでに切り替えが完了しましたが、その他の拠点に関しては2023年4月までに順次切り替えを完了する予定です。今後はBCP対策強化のため、現在社内にあるサーバーをデータセンターへ移管させることを検討していく予定です」（北川様）

「近年、サイバー攻撃の被害内容はより深刻なものへ変化しています。セキュリティ機器導入後の運用・管理が新たな業務負担になっているのが実情です。現在試用中のDIASSについては、自社内だけでなく当社ソリューションを提供しているお客さま企業に対しても、より堅固なセキュリティ環境をご提供できるようさらに検証を進めていきたいと考えております」（落合様）

「サイバー攻撃によるリスクは企業存亡に関わるほど大きなものになっています。サイバー攻撃対策は、もはやIT担当者の責任範囲ではなく、経営レベルのリスクであると言えます。我々も最重要事項として経営メンバーの理解と参画に重視して、BCPと連動した事故対応体制も継続して整備していきます」（野田様）

※1 株式会社データコントロールが提供するセキュリティ・インシデント分析通知サービス Datacontrol Incident Analysis Security Serviceの略称。

※2 株式会社ラックが提供するサイバー攻撃を防御・検知するための国産ブロックリストを提供するサービス。

※3 キヤノンMJグループが提供するサービスパック。FortiGate本体に、UTMとして利用する際の主要なライセンスと「JLIST」を独自パッケージ化したサービス、その他、本事例に掲載されている商品またはサービスなどの名称は、各社の商標または登録商標です。

※4 Fortinet社が提供する無料評価プログラム「Cyber Threat Assessment Program」の略称。

お問い合わせ先

Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南 2-16-6 CANON S TOWER

canon.jp/business/case