



関東電気保安協会

フォーティネット製品をフル活用して情報漏洩防止を図る関東電気保安協会 セキュリティ ファブリックを構成し、約50拠点のセキュリティ強化、 有線/無線LANの統合および可視化、一元管理を実現

生活に欠かせない電気の安心・安全を担う関東電気保安協会では、電気設備の保守点検業務で取り扱う個人情報を保護するため、ソフト、ハードの両面でセキュリティ対策を推進。本部とデータセンターに続き、約50カ所の拠点すべてにFortiGateを導入。短期間で一元的に管理可能なセキュリティ対策を実現した。

導入・構築のポイント

- (1)本部やデータセンターに続き
拠点にもFortiGateを導入して
セキュリティを強化し、
情報漏洩を未然に防止
- (2)FortiSwitchとFortiAPも
採用して有線/無線LANの管理も
統合し、拠点ネットワーク全体を
可視化
- (3)FortiManagerとテンプレートを
活用し、約50拠点への導入作業を
1カ月程度の短期間で実現

一般財団法人 関東電気保安協会

本部所在地 東京都港区芝浦4-13-23
MS芝浦ビル7階
従業員数 約4,000名
事業拠点数 64箇所



関東電気保安協会
保安本部
総合監視指令センター 副長
初鹿 孝夫氏



関東電気保安協会
企画本部
情報システム部長
三浦 修氏



関東電気保安協会
企画本部 情報システム部
課長補佐
池田 真哉氏

電気設備の保守点検業務や啓蒙活動を通じて、私たちの生活や産業活動に欠かせない「電気」を安全に、安心して使えるようにする環境を作っているのが関東電気保安協会だ。関東一円と山梨、静岡に設けた約50カ所の拠点をベースに、約3000人の社員が一般家庭や商店の低圧電気設備、さらには工場などの高圧・特高電気設備の点検作業を担い、必要に応じて改修などのワンストップサービスも展開している。

点検に当たってはさまざまな機材とともにiPadやPDAといった端末を活用し、可能な限り即座に点検結果を反映する仕組みを構築している。同協会の企画本部 情報システム部では、パートナー企業の協力を得ながらこのプラットフォームの開発・保守運用に当たってきた。業務の性質上、ECサイトのようにダイレクトに顧客情報を扱うサービスを展開しているわけではない。だが総合監視指令センターの初鹿孝夫氏は、「点検に必要なため、個人宅のデータも含め多数のお客様情報を保有しています。間違ってもこうしたデータが流出することがあってはならず、セキュリティ対策を重視しています」と述べる。

このため同協会では、外部からダイレクトにデータベースにアクセスできない形にプラットフォームを統一するとともに、エンドポイントなどいくつかのセキュリティ対策を導入してきた。さらに、これまで部署ごとに個別に定められてきた個人情報の取り扱い規定類を見直し、あらためて全社的なセキュリティポリシーを策定。それに沿って社員教育や訓練も実施し、ハードとソフトの両面に対策を進めてきた。

「情報を外部に流出させない」、 本社、データセンター、 そして拠点で次世代 ファイアウォールを導入

関東電気保安協会では2015年に本部を現在の場所に移転したが、その際、無線LAN

と同時にフォーティネットの次世代ファイアウォール製品、FortiGate 300Dを導入し、セキュリティ強化を図った。

このときには、「まずは試験的に導入してみよう」という位置付けだったが、特に大きな問題なく運用できることが分かり、その後データセンターにもFortiGate 3200Dを冗長構成で導入。基幹システムや人事システムなどシステムの性質や扱う情報に合わせてセグメントを分け、万が一ウイルスが侵入してもまん延する事態を防ぐ仕組みを作り上げていった。

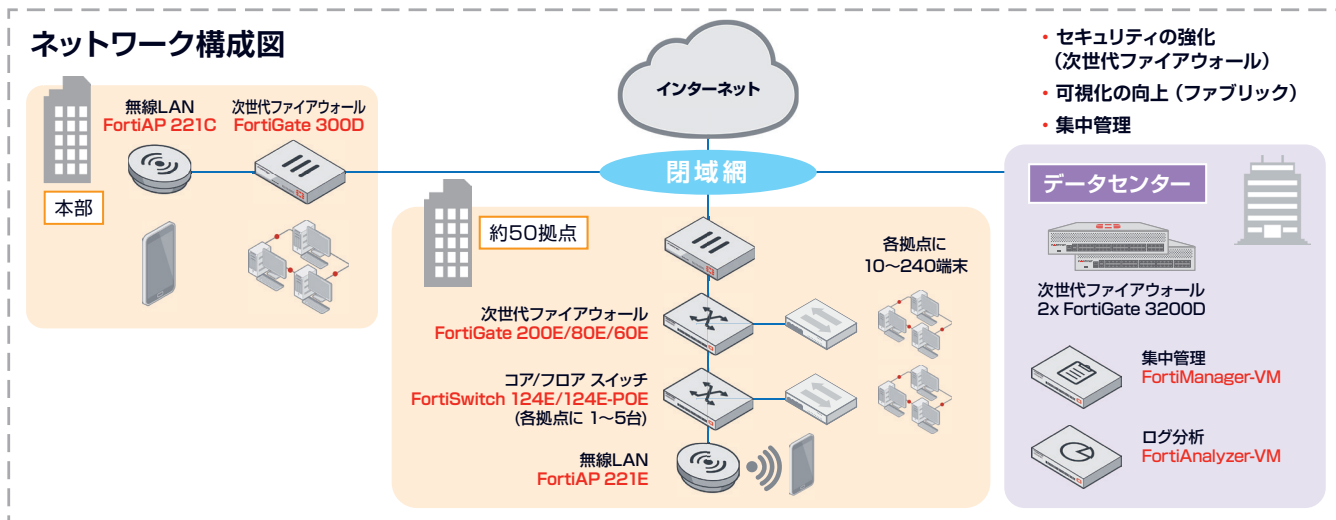
次に着手したのが、閉域網を介してつながっている約50カ所に上る拠点のセキュリティ対策だ。セキュリティはしばしば「鎖」に例えられるとおり、もっとも弱い部分が狙われがちだ。本部とデータセンターという本丸を固めたのだから、拠点という外堀もきっちり管理していくことが狙いだった。

「PCについてはウイルス対策ソフトを導入して一元管理を行っていますが、それでも脅威の侵入を100%防ぐのは不可能です。仮にUSBメモリなどさまざまな経路から侵入があったとしても、情報を外部に流出させないことをポイントに考え、拠点にも次世代ファイアウォールを導入することにしました」(初鹿氏)

いくつかの製品を比較検討した結果、ここでも、ポット対策も含めた統合的なセキュリティ機能を備えていたFortiGate 200E/80E/60Eを選定することにした。本部やデータセンターでの実績に加え、



FortiGate 200Eが設置された多摩事業本部



約50カ所という多数の拠点に導入することから、一元管理が可能でコストパフォーマンスに優れていることも不可欠な要素だったが、その点でも合格だったという。

有線／無線LANの管理も統合し、可視化も

合わせて拠点LANにFortiAPとFortiSwitchを採用し、FortiGateによる有線／無線LANの統合管理を整え、拠点ネットワーク全体の可視化を実現。これにより現場の点検作業用端末のOS更新は各拠点の無線LAN経由とするなど運用も変化した。また、FortiManagerとFortiAnalyzerを用いて全拠点をリモートから一元的に運用管理できる環境も実現した。

今後は末端までFortiSwitchを導入し、FortiAnalyzerからのアラート通知に基づいて、端末単位で即座に自動隔離できる仕組み作りも検討しているという。

テンプレートを活用し、わずか1カ月ほどで約50拠点での導入を完了

機器搬入と設定・導入作業は約1カ月で、

しかも回線の増速工事と同時並行で進める突貫工事だったが、「FortiManager」を活用し、設定テンプレートを一括配布することで作業時間を大きく短縮できた。

作業時間は昼休みなどに限定されたが、実際に各拠点を回った情報システム部 課長補佐の池田真哉氏は「テンプレートを配布しておけば済むため展開自体は非常に楽で、1拠点当たりの作業時間は1時間弱、多少トラブルがあったとしても2時間程度で済ませることができ、予定された停止時間をオーバーすることなく終わられました。逆に、FortiManagerがなければこの短期間で導入することはできなかったと思います」と振り返る。

こうして土日も含め、1日当たり2拠点ずつというペースで作業を進めていった。情報システム部長の三浦修氏は、GUIの使いやすさも相まって「どんどんFortiGateの設定作業の習熟度が上がり、最後の方は効率的に作業できました」と述べている。

こうして関東電気保安協会では2019年3月までに全拠点でFortiGate/FortiSwitch/FortiAPの導入を完了し、次世代ファイアウォールの運用を開始した。FortiManagerやFortiAnalyzerを介してリモートから拠点

の状況を一元的に管理できるようになり、限られた人員での運用体制において運用管理の省力化で効果を実感しているという。「今後はFortiAnalyzerのレポート機能も活用し、経営層や情報セキュリティ委員会での定期的な報告に活用していきたいと考えています」(初鹿氏)

働き方改革が叫ばれる中、同協会では直行直帰などの多様なワークスタイルの実現を視野に入れ、Office 365の導入をはじめとする新たな基盤作りを進めている。その際には、これまでのネットワーク構成を変更して各拠点から直接インターネットに接続する構成を予定。今回導入したFortiGateのSD-WAN機能を使用した「インターネットブレイクアウト」によってWAN回線の効率的な活用を進めたり、アプリケーションコントロールによる統制の実現も検討していく方針だ。AIやIoTを活用し、安定した電力供給のための新しい基盤作りを進めていく関東電気保安協会を、フォーティネットの製品はこれからもセキュリティ面から支えていく。

FORTINET

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ