長崎県

PC4,000台超のセキュリティとアプリケーションの状況を把握 FortiEDRによってより高いセキュリティを変わらぬコストで実現した長崎県教育庁

「従来型のウイルス対策ソフトでは昨今の脅威は防ぎきれないのでは」そんな危惧を抱いていた長崎県教育庁は、文部科学省のガイドライン改定も踏まえ、より強固なセキュリティを実現すべくEDRの導入を模索。コスト効果に優れたFortiEDRを選択し、県内のすべての県立学校で教職員が利用する校務用端末に導入した。管理画面のわかりやすさも相まって、円滑な運用を実現している。

長崎県教育庁

所在地　長崎県長崎市尾上町3-1

長崎県教育庁
教育政策課
情報化推進班
参事
山田 春仁氏

長崎県教育庁
教育政策課
情報化推進班
主任主事
中尾 純氏

ランサムウェアの脅威を前に、従来型EPPの防御に感じた限界

この数年間で学校のICT環境は様変わりした。文部科学省が打ち出した「GIGAスクール構想」を受け、生徒一人に一台の端末を配布し、高速なネットワーク環境を整備して動画なども含めたリッチコンテンツを生かしながら、新たな学びを実現する動きが進んでいる。

導入・構築のポイント

(1) 既存ウイルス対策ソフトに投じるコストを増やすことなく、EDRを導入しセキュリティを強化

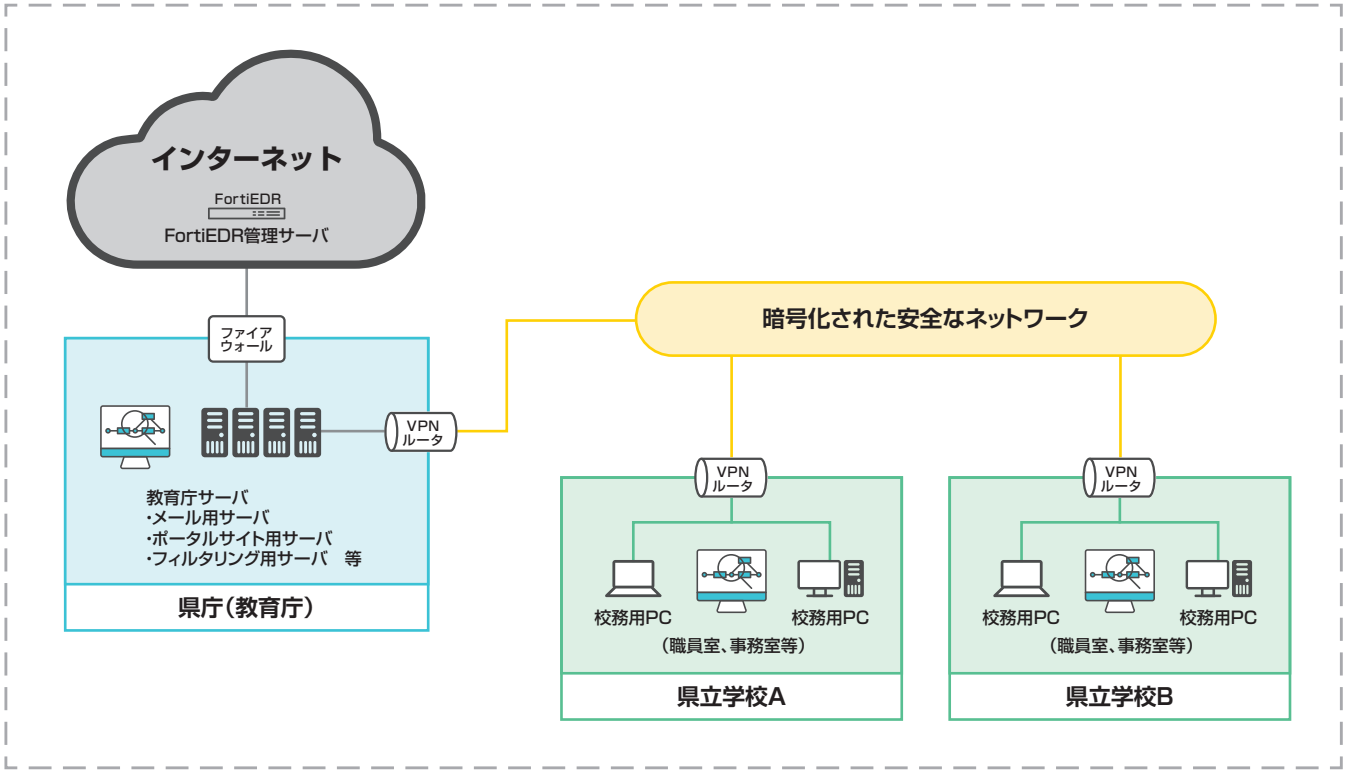
(2) 日本語化されたわかりやすい管理画面で円滑な運用に移行し、セキュリティの状態と利用アプリの可視化も実現

長崎県教育庁も、離島や半島部が少なくない長崎県の地理的特性を踏まえながら、教育用ネットワークの強化を進め、誰一人取り残さない教育の実現に取り組んできた。同時に、校務支援ネットワークの運用を通して、教職員が日常業務をより効率的に行える環境作りも進めている。

生徒の成績や個人情報などを扱う以上、セキュリティ対策は必須だ。かといって何もかも禁止していては効率が損なわれてしまう。「セキュリティを厳格化しすぎず、現場の声を取り入れながら利便性とバランスの取れた運用を目指しています」（長崎県教育庁 教育政策課 情報化推進班 主任主事 中尾純氏）

文部科学省の「教育情報セキュリティポリシーに関するガイドライン」改訂を踏まえ、2022年には長崎県県立学校のセキュリティポリシーも大幅に改訂し、クラウドサービスや生成AIといった新たな技術についても利用指針を定めた。たとえば、複数の教員で確認し合いながら採点が行えるクラウドサービスの利用を許可し、効率化を実現している。

そんな中、近年整備した教育系ネットワークに比べ、校務系ネットワークでのセキュリティ対策が課題として浮上していた。同庁では折に触れて注意喚起を行い、教職員のセキュリティ意識の向上を図るほか、定義ファイルベースのウイルス対策ソフトを導入して端末を保護してきた。しかし「従来型のエンドポイントプロテクション（EPP）をすり抜けるランサムウェアの被害が増えていると聞くたびに、このままでは防御が不十分ではないかと危機感を抱く



ようになりました」（中尾氏）

このウイルス対策ソフトの更新期限が迫っていたことに加え、文科省のセキュリティガイドラインが改訂され、不審な動きを検知し、早期の対応を支援するEndpoint Detection and Response（EDR）の導入が推奨項目として含まれたことを踏まえ、新たな一手を本格的に検討することにした。

ほぼ変わらない予算で、より高いセキュリティを実現するFortiEDRを導入

EDRを導入し、より備えを強固にしたいと考えた長崎県教育庁にとって大きなハードルとなったのは予算だった。「当初は財政状況を考え、従来のエンドポイントプロテクションをそのまま更新することも考えました」（中尾氏）

そんなときにFortiEDRの紹介を受ける機会があった。他社のEDR製品も検討していたが、かなりの投資が必要になると見込まれた。これに対しFortiEDRは、既存のEPPとほぼ変わらない現実的な価格で導入できる上に、猛威を振るうランサムウェアに備え、ロールバックによるデータの復旧機能を搭載していることに魅力を感じたという。

「EDRという新しい機能が追加され、より高いセキュリティが実現されるのであれば、それに越したことはないだろうと考えました」（長崎県教育庁 教育政策課 情報化推進班 参事 山田春仁氏）

加えて、それ以前からFortiGate、FortiMailやFortiAnalyzerといったフォーティネットのセキュリティ製品群を運用していたため、操作になじみがあり、安心感もあった。「この先、他のフォーティネット製品と連携することで、より大きな効果が期待できると判断しました」（中尾氏）

こうしたポイントを要求仕様に盛り込み、入札の末、FortiEDRの導入が決定した。

ただ実運用をにらむと、さらにいくつか確認すべきポイントがあった。一つは利便性との両立だ。「まず、県庁内にある学校と同様のネットワーク環境で検証用の端末を用いて検証したのに加え、実際に現場の数名に協力をいただき、学校の端末にインストールしてどのような挙動を示すか確認しました」（中尾氏）。この結果、誤検知や過検知なく、学校業務に必要なソフトウェアが動くことを事前に確認できた。

もう一つは展開手順だ。すべての学校を回ってインストールするのは非現実的であり、リモートでインストール作業を行えることも必須条件だったが、PoCを通じて迅速に展開できることも確認した。フォー

ティネットと密に連携しながら、約一ヶ月かけて行ったPoCを通していけるという手応えを持って本格導入を進めた。

基本的に脅威はブロック、わかりやすい管理画面で常時状況をチェック

長崎県教育庁では県立高等学校と特別支援学校、合わせて79校の校務ネットワークで教職員が利用するパソコンすべてと、各校に設置されている校務用サーバにFortiEDRを導入した。それまで利用していたウイルス対策ソフトのライセンス期限との兼ね合いで、2023年7月という年度途中のタイミングでの入れ替えとなり、決して余裕のあるスケジュールではなかったが、PoCでの検証通りスピーディに展開できた。

本土地区の学校にはリモートインストールによって配布した。残り約3分の1弱となる離島地区の学校については、別途保守業務を委託したシステムインテグレータの協力を得てオンサイトで展開していき、約1ヶ月間という短期間で約4,300台への導入が完了した。

運用を開始して数ヶ月。まず感じたのは管理インターフェイスのわかりやすさだ。全面的に日本語化されていることもあり、実際に管理作業に当たる常駐のエンジニアからの評判は上々だという。「私自身も業務時間中にちょくちょく管理画面をチェックしています。見やすく、ぱっと状況が頭に入ってくるので助かっています」（中尾氏）

これまで、学校の職員への連絡が必要になるほど深刻なインシデントやアラートは報告されていない。「確かに疑わしいものが検知されていますが、当初想定していたほど多くのアラートが出ているわけではありません。基本的にブロックされており、しっかり守ってくれていると考えています」（中尾氏）

また、悪意あるソフトウェアの状況だけでなく、端末で利用されているソフトウェアの状況を確認できるのも利点の一つだ。管理インターフェイスを開けば脆弱性のある古いバージョンのWebブラウザがどの端末で使われているかといった事柄をトップ画面上で一目で確認できるため、ガバナンスの観点でも有用だと感じている。

検知された事象などに関して不明なことがあれば、フォーティネットが提供する導入支援のベストプラクティスサービス（BPS）を通して確認し、その都度疑問を解消できている。「質問内容に対して非常に的確なアドバイスをいただけていますし、そのセッション中に浮かんだ疑問についても随時回答をもらい、生じた疑問点をすべてつぶしていけるため助かっています」（中尾氏）といい、運用は不安もなくほぼ軌道に乗り始めている。

利用者側にもメリットがあった。それまで利用していたウイルス対策ソフトでは、一週間に一度フルスキャンが動作し、その間、端末の動作が非常に重くなってしまっていた。FortiEDRでは、職員が意識するほど端末が遅くなる事態は起こらなくなっている。

FortiGateなどと連携し、自動的にブロックする運用も検討

長崎県教育庁では今後、FortiEDRと他のフォーティネット製品と連携させ、端末側で不正な通信を検知したらゲートウェイ側で自動的にブロックを行うといった運用も検討していく。「FortiGateなどと連携させるための設定はPoCの際に確認済みなので、一通り運用が軌道に乗ってから本格的に設定しようと考えています」（中尾氏）

複数のベンダーの製品を組み合わせる場合に比べ、「やはり同じメーカーの製品であれば、管理画面からちょっと設定するだけで簡単に連

長崎を一望する県庁の展望テラスにて、左から山田氏、中尾氏

携できます。運用を担う常駐エンジニアにとっても非常に助かり、楽になるソリューションだと考えています」と中尾氏は述べた。

将来的には、現時点では教務用と学習用、それぞれ一台ずつ用意して教職員が使い分けている端末を一本化していくことも想定しなければならない。さらに、校務系システムをデータセンターからクラウド上に移行することで、事前申請の元でリモートワークを許可していくことも考えられる。もちろん、教職員にとって最も大切なのは現場での授業だが、効率化できる部分は効率化していくことで、ワークライフバランス改善につなげていくこともできる。もちろん、それにはセキュリティがきちんと確保されることが大前提だ。クラウド移行も含め、ネットワークアーキテクチャ全体の青写真を描き、ソリューションを活用しながらゼロトラストセキュリティの考え方を取り入れるなど、予算の中で最適な仕組みを実現し、よりよい学びと学校業務の効率化を支援していく。

FORTINET
フォーティネットジャパン合同会社

〒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