PROTECTORS
STORIES

CrowdStrikeお客様事例

岐阜県中津川市教育委員会

セキュリティ専門家不足でも運用を持続可能に「ほぼ何もしなくていい。安心して任せられる」

AVだけではエンドポイントは守りきれない 検知できても判断と対応ができない

岐阜県中津川市は、美濃三河高原の西にあり、豊かな自然に囲まれた中核都市だ。銘菓「栗きんとん」や「からすみ」、高原で栽培されるミネラル豊富な野菜、飛騨牛などの畜産業、伊勢神宮の御用材も産出する林業、歴史を伝える宿場町や苗木城跡など、実に多彩な魅力にあふれた市だ。また2027年にはリニア中央新幹線の岐阜県駅が市内に設置されることになっており、交通アクセスの整備や企業誘致が活発に進められている。

中津川市が教育で重視しているのは「よりよいひとりだち」。これは同市教育振興基本計画で定められている。方針には「生活・学習における基礎基本の習得とたくましい子の育成」と定め、知識と知恵を身につけて生きぬく力を育むようにしている。重点には教科指導、ICT教育、特別支援教育、教育相談の取り組みのほかにも、すご技中津川プロジェクトや岐阜サマーサイエンススクールなど特色ある教育活動もある。

近年マルウェアやランサムウェアの脅威が高まっている。中津川市や同教育委員会では、致命的な被害をもたらすセキュリティインシデントに見舞われたことはないものの、国内ではランサムウェア被害の報告が相次いでいる。2022年7月には、ある地方自治体の教育委員会の公務ネットワークがSSL-VPN装置からの侵入でランサムウェア攻撃を受け、同地域の小中学校が持つ児童・生徒のデータが暗号化されて閲覧不能となるインシデントが起きた。それも夏休みに入る直前だ。公務支援システムや教職員用のパソコンが利用できなったため、現場では紙の資料からデータを復旧したり、手書きで通知表を作成したりするなどの対応に追われた。その脅威の状況から、中津川市役所 教育委員会事務局 教育企画課 小川 大貴氏は「人ごとではない」と危機感を抱いていた。

中津川市の教育委員会および教育現場のICT環境で管理する端末は約700台。ネットワークには標準的な境界型のセキュリティ対策を施し各端末に従来型のアンチウイルス（AV）を導入し、どちらも最新版となるように更新していた。10年以上この運用を続けていた、かつてなら十分だったかもしれない。しかしサイバー攻撃が高度化する今となっては不十分だと小川氏は懸念を抱いていた。「各種セキュリティ調査レポートによると、シグネチャ型のアンチウイルスで防御できるものは半分もない、検知すらできないと言われています」と話す。それより少ないと指摘する調査結果もある。検知を高めるためにAVはNGAV（次世代型アンチウイルス）に、さらに不審なふるまいの検知や対処を行うEDR（Endpoint Detection and Response）へとセキュリティ対策を高度化していく必要があった。

課題はもう1つある。検知後の対応だ。小川氏は「検知できたとしても、我々（市の職員や教職員）は専門家ではないので、どう対応すべきか分かりません」と話す。教育委員会ではセキュリティ担当は未経験者が引き継ぐことが多い。昨今の高度化した攻撃では何をしたらいいのか分からずお手上げとなってしまうのは目に見えていた。何か危険な兆候を検知した時、すぐに分析して判断できる専門家が必要だった。

セキュリティ認証や 第三者機関の製品評価レポートから クラウドストライクを選定

中津川市ではエンドポイントのセキュリティ対策強化として、まずは従来型のAVに加えNGAVとEDR機能を必須条件とした。加えて小川氏は「両製品がセットで提供されていること」を重視した。個別のソリューションの組み合わせでは、別々の管理画面を監視することになり「（分析や対応の）スピードが落ちてしまう」と

業種
地方公共団体

所在地
岐阜県中津川市栄町1-1
にぎわいプラザ4階

岐阜県中津川市教育委員会

岐阜県東濃にある中津川市は、長野県に隣接した位置にある。地理的には美濃三河高原にあり、北部や南部に山地が多く分布している。付知峡や乙女渓谷、また馬篭宿、落合宿、中津川宿といった中山道の宿場町、苗木城跡など歴史ある地域でもある。名産品には「栗きんとん」や「五平餅」などがある。リニア中央新幹線が開通すれば岐阜県駅が中津川市内に設置される予定だ。総人口は約7万5000人（2023年7月末）。面積は676平方キロメールで、琵琶湖とほぼ同じ大きさに相当する。

https://www.city.nakatsugawa.lg.jp/pe/education/kyoikuiinkai/index.html

導入サービス

- CrowdStrike Falcon Complete™ CrowdStrike Falcon Completeに含まれるコンポーネント
  - CrowdStrike Falcon Prevent™ 次世代アンチウイルス（NGAV）
  - CrowdStrike Falcon Insight XDR™ EDR
  - CrowdStrike Falcon OverWatch™ プロアクティブな脅威ハンティング
  - CrowdStrike Falcon Discover™ IT資産管理
  - CrowdStrike Falcon Complete TeamによるMDR（Managed Detection and Response）サービス

導入時期：2023年4月

懸念したためだ。また検知後の課題を考えると、EDRの運用を専門家に任せることができるMDR（Managed Detection and Response）が追加であると望ましいと考えた。

数あるセキュリティ製品のなかから「NGAVとEDRが必須、可能ならMDR」で選定を進め以下の条件を示した。

- 「教育情報セキュリティポリシーに関するガイドライン」に示されているクラウドサービス利用の際の第三者認証等の活用に示されている認証評価を得ていること
- 運用コストが低いこと、我々が手をかける必要がほぼないこと
- NGAVとEDRを1社がまとめて提供できること、可能であればMDRも同社で提供できること
- 予算内であること

最終的には2社の中から、MDRも含め、クラウドストライクを選択した。機能的な着眼点は、シングルエージェントで動作が軽くエンドポイントに大きな負荷を掛けないこと、サーバーの運用保守を不要とするクラウドネイティブであること、後からUSB制御など他のセキュリティ機能の追加を簡単に行うことができる拡張性があることなどである。「素人目で見た時には、2社の製品は同じかなと思いました。最終的には、拡張性と第三者機関の評価がクラウドストライクを後押ししました。」と小川氏は話す。

導入を決定したのが2023年2月、実際に運用を開始したのは同年4月からだ。小川氏は「当初は2024年度からにしようと思いましたが、意外にもとんとん拍子に運びまして『導入できるなら早いほうがいい』と2023年度から導入することになりました」と話す。

自動分析と専門家がしっかり判断し運用
24時間356日、監視と対応を任せられる

導入後の効果について小川氏は、特に運用面からコメントを寄せた。「ほぼ何もしなくてもよくて、安心して任せられます。端末やサーバーへのエージェントの展開サポートも、全てMDRのサービスに含まれておりお任せできましたので、本当に簡単でした」と話す。

何かあった際、サーバー、端末それぞれにどう対処するかを事前に決めて運用は開始された。緊急時は、クラウドストライクが提供しているネットワーク隔離の機能を利用し、該当端末の隔離を即行うようにMDRにお願いしてあるという。LANであれば感染した等問題のある端末のLANケーブルをぬけばいいが、wifiを利用している環境であれば、依頼するにも、どう対処したら良いかわからない人もいる。製品とMDRによる運用監視・対応の力が合わさり、組織のセキュリティを支える体制が整った。

運用開始後は、レポートメールに目を通せば必要な項目が通知されているので、わざわざ管理用のダッシュボードを開くことはほぼないという。

「恐らく、我々がダッシュボードを見ても分からないと思います。しかしクラウドストライクのMDRなら、自動分析と専門家でしっかり判断しますし、24時間356日監視・対応できます。学校では部活などで休日にも端末を使用することがあり、その時に何かが起こっても、我々だけでは対応しきれません」（小川氏）

現時点（導入後4ヶ月）まで、致命的なアラート発報やインシデントは起きていない。また事前にどのような条件でどのような対応を行うかの取り決めがあるため、緊急時にはすぐに必要な対処がなされる安心感がある。

セキュリティ運用の展望について、小川氏は次のように述べる。「セキュリティは多層防御が必要で、エンドポイントは全体の一部ではありますが、これでエンドポイント保護はかなりレベルが高いものを導入できました。今後はゼロトラストの考え方に基づき、ネットワークでもSASEを採用検討するなどさらなるセキュリティ強化を進めていきます」

中津川市役所
教育委員会事務局
教育企画課
小川 大貴 氏

POINT

- 従来のシグネチャ型アンチウイルス（AV）だけでは昨今のサイバー脅威に対抗できないため、次世代型AVとEDRを導入
- コスト、認証、第三者機関のセキュリティ製品評価レポートからクラウドストライクを選択
- クラウドストライクによるMDRを導入したことで、セキュリティ未経験の担当者でも運用を持続可能
- CrowdStrike Falcon®製品モジュールとMDRによる24時間365日の運用監視・対応の力が合わさり、組織のセキュリティを支える体制が整った

CROWDSTRIKE

we stop breaches

クラウドストライク合同会社
お問い合わせ: **http://crowdstrike.jp/contact-us/**