voices

CrowdStrike 導入事例

高知県庁

高知県庁6,500台の業務端末を守るのは AIと振る舞い検知で未知の攻撃も防ぐ CrowdStrike Falconプラットフォーム

高知県 Kochi Prefecture

県民サービス向上や県内産業振興のため デジタル活用を推進、セキュリティは必須に

緑濃い森林と青い海の国 高知県。北は四国山地で愛媛県、徳島県に接し、南は太平洋に面して扇状に突き出した地形を持ち、恵まれた自然環境の中で、豊かで変化に富んだ風土が形勢されている。この土地に生まれ育つ高知の人々は自由かつ豪快な気風で知られ、男性は「いごっそう」、女性は「はちきん」と呼ばれる。また、坂本龍馬がそうであるように、土佐人はアイデアも豊かなら行動力もあり、こだわりのある園芸作物や産業技術を始め、「よさこい祭り」「日曜市」など個性豊かな地域の文化を発展させてきた。

この高知県の行政機関である高知県庁では、令和元(2019)年度からデジタル化の取り組みをスタートした。当初は「高知県行政サービスデジタル化推進計画」と高知県庁内を対象とする内容、そして令和3(2021)年からはこれを県全体へとカバー範囲を広げ、より総合的な「高知県デジタル化推進計画」としてバージョンアップした。そこで掲げられているのは、「県民サービスの向上」「デジタル技術を活用した課題解決と産業振興」「行政事務の抜本的な効率化」という3つのVisionだ。高知県 総務部 デジタル政策課 主幹 山端 桂祐氏は、バージョンアップの背景を次のように語る。

「行政だけをデジタル化しても、高知県全体のデジタル水準は向上しません。逆に民間事業者の仕事や個人の手続きが紙のまま残ってしまったら、かえって仕事が増えてしまいます。また、県民の皆さん誰もが、デジタル化の恩恵を受けられるような形にもしなくてはいけません。高知は一つの家族、われわれにはみんなで一緒にデジタル力を底上げしていきたいという思いがあります。デジタル化推進計画でも特に意識しているのは、デジタルを活用することで、本県の多くの部分を占める中山間地域においても、安心して、より豊かに住み続けられる環境を創っていくということです」

高知県のような地方公共団体の情報システムは、大きく3つの系統から構成される。「個人番号利用事務系システム」「LGWAN接続系システム」「インターネット接続系システム」がそれらだ。総務省は「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和4年3月版)」において、この3システムのありように、α、β、β'という3つのモデルを示している。モデルによって対策すべき情報セキュリティが異なり、α→β→β'の順に、より厳格な技術的対策、組織的・人的対策が必要になる。現在、地方公共団体の情報システムは、それぞれが方法を選択して運用されている。

「今日、民間ではSlackやGoogle Workspaceなどがコミュニケーションやコラボレーションシーンで当たり前のように利用されていますが、高知県庁では現在、このようなインターネット上の資源がうまく活用できません。使えたとしても非常に手間がかかります。庁内からは『県内事業者や県民の皆さんと協創、協業するためにこういうツールを使いたい』という声が上がっています。そのためにβ'も見据えた検討もしています。」

既存アンチウイルスソフトに 感じていた3つの課題

デジタル活用の推進には、セキュリティ対策が欠かせない。エンドポイント端末のセキュリティ対策のひとつ、基本中の基本といえるアンチウイルスソフトに関して、デジタル政策課は大きく3つの課題を感じていた。

1つめは、新しいタイプの攻撃が増大し、シグネチャ型の製品ではもはや十分に対抗できないという点だ。隣県でのランサムウェア被害の話を耳にしており、もはや対岸の火事ではないことを認識していた。マルウェアの形態などではなく、ふるまいで検知できる必要があると考えた。

2つめは、職員の使用感である。既存のアンチウ

業種

地方公共団体

所在地

高知県高知市丸ノ内1丁目2番20号

高知県庁

四国の南部に位置する高知県は、美しく豊かな緑と黒潮打ち寄せる変化に富んだ海岸線に恵まれた土地だ。面積は約7,104平方キロメートルで四国四県では一番広く、森林面積は約83%を占める。あわせて、坂本龍馬や吉田茂など、数多くの先人・偉人を輩出してきた歴史と風土がある。高知県庁は高知県の行政機関で、「高知県はひとつの大家族やき。」をキャッチフレーズに、同県全体を「高知家」という家に見立て、あたたかくて人懐こい県民性をアピールするとともに県内産業の振興を推し進めている。

URL:https://www.pref.kochi.lg.jp/

導入製品

- CrowdStrike Falcon Prevent™ NGAV(次世代アンチウイルス)

導入時期:2022年7月

イルスソフトは、毎週水曜日の午前中にシグネチャのアップデートが起動する設定になっていた。また、職員は月に一度フルスキャンを行うことにもなっていた。しかし、どちらも動き出すとPCが重くなる。水曜日午前中はPC利用を避けるとの声も聞こえ、効率の阻害要因であった。

3つめは、ガバナンスの問題だ。アンチウイルスソフトのPCへのインストールは、職員自身が手動で行うことになっていた。そのため、対象業務端末へのインストール作業が迅速かつ確実にできているとは言えなかった。

次期導入製品・サービスではこのような課題を解決すべく、2022年に訪れる既存セキュリティ製品の保守期間終了を前に、2021年春ごろから広く市場調査を行った。

多数の評価項目が盛りこまれた仕様書をクリアできたのはクラウドストライク製品

シグネチャに依存しないもの、というのは当初から山端氏の考えにあった。他の候補要件は、様々なベンダーから話を聞きながら探っていった。約10種類の製品・サービスを見ていく中で、評価すべき項目を表１のように絞り、仕様書に記述した。

シグネチャ非依存	端末への導入容易性
端末負荷の軽さ	運用負荷軽減の工夫
新しい技術の搭載	第三者機関の評価
コスト	3OS対応（Win,Mac,Linux）
将来的な拡張性	

表１：デジタル政策課が次期アンチウイルスソフト選定で掲げた評価項目

2022年4月上旬、一般競争入札が行われた結果、選定されたのはクラウドストライクの次世代アンチウイルスCrowdStrike Falcon Preventだった。山端氏はこの結果について次のように語る。

「PCにインストールするのは軽量のセンサーで、Active Directoryから直接配布できるため、対象業務端末に抜け漏れなく入れることができます。稼働による業務への影響を感じない上に、フルスキャンが不要になるのは非常に大きいです。また、AIを駆使したふるまい検知により、新しいタイプの脅威にも立ち向かえます。

Falcon Preventは、第三者機関での格付けも高く、最も信頼したのは数十の製品・サービスを対象としているAV-Comparativesでの評価です。そこで常にしっかりと評価されていることは心強く思いました。さらに、CrowdStrike Falconプラットフォームからはライセンスを追加購入するだけで、別エージェントをインストールすることなくEDRが利用できるようになるという点も、今後、ネットワークがオープンになるβ'モデルへの移行を行うとなった場合にもセキュリティの担保をスムーズに行えると思いました。価格が予算内に収まったことにも満足しています」

デジタル政策課では、2022年5月から実際に導入しての内部評価を開始した。デジタル政策課の業務端末での動作検証の後、「LGWAN接続系システム」にアクセスする端末に追加導入、計380台で試験導入を実施した。年内には全てに導入を完了させる予定である。日々の運用は事業委託会社が担っており、一定のアラート情報についてデジタル政策課に連携する運用を想定している。

脅威対策が強化されただけでなく業務効率は向上、運用コストも削減

Falcon Prevent導入により、高知県庁では高度化する脅威に対峙できる体制が整いつつある。使用感という観点でも、先行利用している庁内職員からは好評で、あまりに静かなため「ほんとうにウイルスソフトが入っているんですか？」という声が届くほどだ。

さらに、導入してから気がついたメリットというのもある。クラウドストライク製品はクラウドネイティブでクラウドから提供されているため、管理サーバなどが一切不要である。既存製品の管理サーバに対する運用保守は不要となり、その管理保守を外部委託していた分のコスト削減にもつながったのである。中山間地域でも安心して豊かに暮らせる社会の実現を最重要テーマに掲げる高知県庁は、CrowdStrike Falconプラットフォームでセキュリティを担保し、デジタル活用推進への道を進んでいる。

高知県
総務部 デジタル政策課 主幹
山端 桂祐 氏

POINT

- 県全体のデジタル力を底上げする「高知県デジタル化推進計画」を支えるセキュリティ
- AIと振る舞い検知を活用した次世代AVで強固なセキュリティを実現
- EDRも見据え、将来の拡張性ある製品を選択
- クラウドネイティブ、管理サーバ不要となり、保守費用のコスト削減
- 対象業務端末6,500台の脅威対策強化が実現予定

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/**