シスコ セキュリティ ソリューション導入事例

佐賀市教育委員会

教員と児童生徒の PC を未知の脅威から守るため クラウドと連携するマルウェア対策ソフトを導入

製品 & サービス

- Cisco Advanced Malware Protection（AMP）for Endpoints

課題

- 教職員および児童生徒が利用する PC 端末に対する、マルウェア感染へのより強固な対策
- シグネチャを用いるウイルス対策製品では検知できない標的型攻撃やゼロデイ攻撃への対策

ソリューション

- クラウド上のセキュリティ基盤と連携して世界トップの検知率を持つ Cisco AMP を導入し、PC 端末のマルウェア対策を強化

結果～今後

- PC を安全に利用できる環境を維持し、ICT を活用した教育を市内の小中学校で展開
- 教職員のセキュリティに対する意識を高め、児童生徒の模範となるよう努める

佐賀市教育委員会は、市内の小中学校 53 校で ICT を活用した教育を推進しています。PC や電子黒板などの端末を用いたわかりやすい授業の実現、インターネットを通じた多様な情報の収集と発信といった実践的な学びを通して、児童生徒の学習意欲と理解度を高めると共に、これからの国際社会で必要とされる情報活用力を育んでいます。

Cisco AMP はクラウド上に蓄積される最新の情報と常に照合して脅威を判定するという新しい仕組みで、標的型攻撃やゼロデイ攻撃への備えを万全にできる点を評価しました。

―― 佐賀市教育委員会 こども教育部 学校教育課
ICT 利活用教育係 主幹 兼 係長　石橋 秀昭 氏

佐賀市教育委員会では、すべての小中学校の普通学級と特別支援学級に電子黒板を配備しており、デジタル化が進む教材への対応や教員の自作教材の活用などで多くの実績を上げています。また、いくつかの学校はモデル校としてビデオ会議システムも導入済みで、国内や海外の学校との交流を積極的に行っています。

佐賀市教育委員会 こども教育部 学校教育課 課長の中村祐二郎氏は次のように話します。

「インターネットで社会とのつながりが増し、自分が住んでいる市や町に留まらず、日本全国、そして世界の情報に直接触れることができるのは児童生徒にとって大きなメリットです。また、今はモデル校で行っているオーストラリアの学校との交流授業は、国際化に対応した教育という点でも意義があります。山間部の小規模な学校では外部との交流がどうしても少なくなってしまうのですが、ビデオ会議システムを生かして海外の学校とつながり、子供たちが本当に生き生きと発言して学んでいる姿を見ると、自分に自信を持って成長していく上で大きな効果があると実感します。このビデオ会議システムの導入と運用はシスコにも協力いただいており、このノウハウを市内の各校に広げていくことで佐賀市全体の成果にも結びつくと期待しています。」

佐賀市教育委員会 こども教育部 学校教育課 ICT 利活用教育係 指導主事の行徳武彦氏は、各校で導入してきた ICT 設備の活用度はとても高く、教職員の業務にも効果が出ていると話します。

「電子黒板、書画カメラ、デジタル教科書はほとんどの授業で使われていて、使わない日はないほどです。教員の授業の準備のしやすさやデジタル教材をどこでもすぐ使える便利さが好評でした。PC 教室にはモニタ部分を外してタブレットのように使えるハイブリッド型の PC を導入しています。今後、活用事例を増やしていきたいと思っています。」

佐賀市教育委員会
こども教育部 学校教育課
課長
中村 祐二郎 様

佐賀市教育委員会
こども教育部 学校教育課
ICT 利活用教育係
指導主事
行徳 武彦 様

佐賀市教育委員会
こども教育部 学校教育課
ICT 利活用教育係
主幹 兼 係長
石橋 秀昭 様

佐賀市教育委員会
こども教育部 学校教育課
ICT 利活用教育係
加々良 哲 様

※NSS 侵害検出テストでシスコが再度首位を獲得
http://www.cisco.com/c/m/ja_jp/offers/sc07/amp-analyst-report/index.html

課題

佐賀市教育委員会は 2011 年（平成 23 年）頃から各校への PC 導入を本格的に進め、電子黒板は 2013 年（平成 25 年）から 2015 年（平成 26 年）の 2 年間で導入を完了しました。ただ、各校の導入のタイミングは異なっており、インターネットへの接続環境も個別に構築していたため、セキュリティ対策の強度や内容が不揃いであることが課題となっていました。そこで、PC 端末の更新時期を迎えた 2016 年（平成 28 年）に各校のシステム環境を再構築し、セキュリティ対策も一元的に行えるよう改めました。これに合わせて PC 端末のマルウェア対策を強化しています。

佐賀市教育委員会 こども教育部 学校教育課 ICT 利活用教育係 主幹 兼 係長の石橋秀昭氏は次のように話します。

「教職員と児童生徒が使う PC のほかに、各校に校務用サーバがあり、以前はこれらが直接インターネットにつながる状態でした。ファイアウォールの設置などセキュリティも意識はしていましたが、53 校すべてに高機能な製品を設置するとなるとコスト負担は大きくなってしまいます。そこで校務サーバの仮想化による統合と合わせてインターネット接続環境も 1 つにまとめ、ゲートウェイレベルの対策をしっかり行える構成にしたのです。このほかに、ユーザ認証や USB メモリの利用規定なども大幅に強化しています。

PC 端末の対策としては、これまでもウイルス対策ソフトを用いてきましたが、昨今の標的型攻撃やゼロデイ攻撃に対応するため、定義ファイルに依存しない別のソフトウェアも導入して、万全を期したいと考えたのです。」

コストは抑えながらも
最大のセキュリティ確保を目指しました。

ソリューション

Cisco AMP で防御力の向上と、万一の際の追跡調査を可能に

Cisco Advanced Malware Protection（AMP）for Endpoints は、マルウェアの検出とブロック、継続的な分析やアラート発行などを実現します。標的型攻撃や未知の脅威、ゼロデイ攻撃から端末を保護する製品として豊富な実績を持ち、第三者機関の調査でもマルウェアの検知率は 3 年連続で世界トップ※と評価されています。

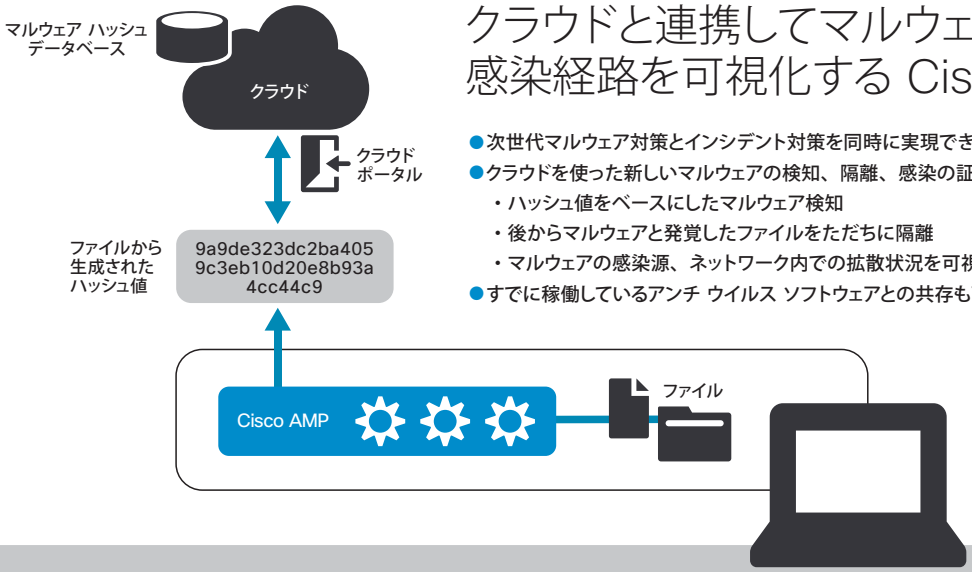
今回 Cisco AMP を採用した理由を、石橋氏は次のように話します。

「理由は大きく 2 つあります。1 つは、従来のウイルス対策ソフトウェアでは検出することができない標的型攻撃やゼロデイ攻撃への対策を実現するためです。もう 1 つは、不幸にもマルウェアに感染してしまった端末が出てきた場合に、Cisco AMP ならマルウェアの侵入経路や実際の影響、データの流出といった事象を追跡調査することができるからです。感染を防ぐことが第一ですが、もし感染してしまった場合、その後の対応も重要かつ大変ですので、その部分を Cisco AMP が補ってくれることを期待しています。実際の運用はシステムの再構築を担当した地元のパートナー企業と一緒に行っていますが、導入を終えてから現在までマルウェア感染もなく、安心しているところです。」

Cisco AMP は、シスコがクラウド上に持つ世界最大級のセキュリティ情報基盤と連携して常に最新の情報と照合しながらネットワーク上の脅威を判定します。その時点でマルウェアとは判別されなくても一度検査したファイルのハッシュ値をクラウド上で記録しておき、後の分析や情報の追加でマルウェアと判定されたときに、該当のファイルを迅速に隔離する仕組みを備えています。これが高い検知率を支えており、従来のウイルス対策ソフトとは根本的に考え方や機能が違う点を佐賀市では高く評価しています。

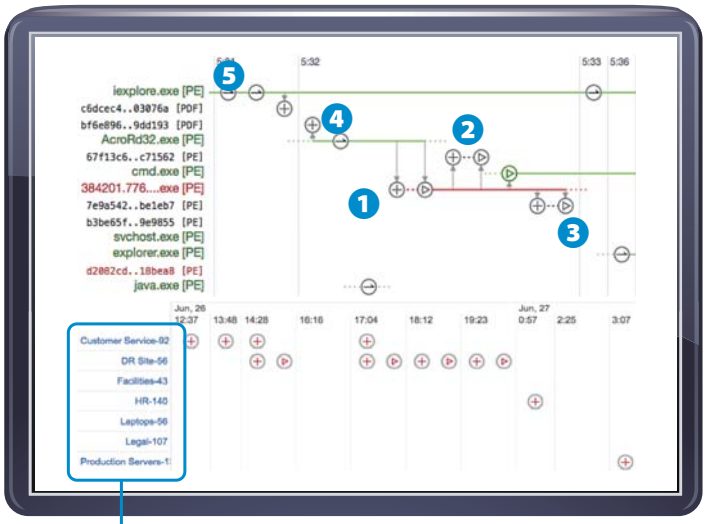
佐賀市教育委員会 こども教育部 学校教育課 ICT 利活用教育係の加々良哲氏は次のように話します。

「これまでの定義ファイルを突合させるタイプのウイルス対策ソフトのようにフルスキャンを何度もくり返す必要がなく、軽快に動作して PC やユーザの負荷を軽減します。これは大きな差があると思います。」



クラウドと連携してマルウェアの感染経路を可視化する Cisco AMP

- 次世代マルウェア対策とインシデント対策を同時に実現できるソリューション
- クラウドを使った新しいマルウェアの検知、隔離、感染の証跡を提供
  - ハッシュ値をベースにしたマルウェア検知
  - 後からマルウェアと発覚したファイルをただちに隔離
  - マルウェアの感染源、ネットワーク内での拡散状況を可視化
- すでに稼働しているアンチ ウイルス ソフトウェアとの共存も可能



Cisco AMP は、デバイス トラジェクトリ※という仕組みを用いてマルウェアの感染経路を可視化し、原因の特定と必要な対策を早期に行えるようにします。

事象を可視化、把握する流れ

1. マルウェアが作られた
2. 3. マルウェアが何かファイルを作り出して実行した
4. アプリケーションが通信をした後マルウェアが作られ、さらにアプリケーションがそのマルウェアを実行した
5. Web ブラウザでどこかに通信した後、ファイルをダウンロードしてきた

【凡例】
- 赤――：マルウェア
- 緑――：正規のベンダーのファイル
- 黒――：現時点ではマルウェアとは判定されていないファイル
- ⊕ ファイルが作られた
- ▷ ファイルが実行された
- ⊖ ファイルが通信をした

※検知したマルウェアをインストールした元のファイルは何か、そのファイルがどこからダウンロードされたのか、ほかのファイルを作成していないかといったマルウェアの挙動をフライト レコーダーのように記録して、感染経路や原因を可視化する仕組み

結果～今後

佐賀市教育委員会は、今回採用したセキュリティ対策を適切に運用しながら、教職員と児童生徒が安全に、安心して ICT を利用できる学びの環境をさらに発展させていくことを目指します。現在は生徒の多くがスマートフォンなどのデバイスを所有、利用していることを踏まえ、授業の中でもセキュリティの大切さを教えていこうとしています。そして、その手本となるべく、教職員のセキュリティに対する意識をさらに高めるための取り組みも市および学校全体で進めていきます。

その他の詳細情報

Cisco AMP の詳細は、www.cisco.com/jp/go/amp を参照してください。

佐賀市教育委員会（佐賀市）

所在地　佐賀市役所　佐賀市栄町 1-1
規模　人口 234,591 人（男 110,514 人、女 124,077 人）
世帯数 98,230 世帯（平成 29 年 1 月時点）
URL　https://www.city.saga.lg.jp/

平成 17 年 10 月 1 日に佐賀市、諸富町、大和町、富士町、三瀬村が合併。その後平成 19 年 10 月 1 日に、川副町、東与賀町、久保田町と合併して現在の佐賀市となる。面積は 431.84 平方キロメートル。
古代肥前の国の行政府跡「肥前国庁」、佐賀城公園、佐賀城本丸歴史館などがあり、筑後川にかかる昇開橋や佐賀平野に広がるクリークや田園風景、有明海など素晴らしい環境に恵まれている。山間部にある観光りんご園、温泉、スキー場、沿岸部の干潟と個性的な動植物など観光面でも多様な魅力を有している。
平成 27 年 5 月に「東よか干潟」がラムサール条約湿地に登録。また平成 27 年 7 月には、日本初の実用蒸気船「凌風丸」が造られた「三重津海軍所跡」が世界文化遺産に登録された。

お問い合せ

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

1268-1703-00A-F