愛知県田原市役所 様

標的型攻撃やウイルス感染を早期に検知し、被害を最小化
脅威侵入後を見据えた対策で、市民サービスの安全を守る

愛知県の南東部、渥美半島に田原市は位置します。三河湾、太平洋、伊勢湾と、三方を海に囲まれた温暖な気候を活かし、野菜や果物などの近郊園芸農業が盛んで、農業産出額は市町村別で全国1位を誇ります。また工業の分野でも、三河港臨海工業地帯田原地区を中心に様々な製造業が生産拠点を構えており、製造品出荷額も全国有数の地域です。

課　題

- インターネットの出入口や職員利用端末への対策をすり抜けて、新種のマルウェアが侵入
- 大きな被害にならなかったが、調査のため一部のネットワークを自主的に6日間制限した

効　果

- 当社エキスパートのログ解析により、脅威の侵入が把握でき、月次レポートの結果から庁内ネットワーク状況を可視化
- 異常検知時の即時通報により、初動の強化とお客様の工数削減に貢献

導入サービス	FUJITSU Security Solution ウイルスふるまい検知サービス
導入の目的	ネットワークに潜む脅威の早期検知、侵入後の迅速かつ的確な対応
採用のポイント	初期投資の抑制と運用負荷を軽減し、既存資産も有効活用できる

■ お客様の課題

侵入を100%防ぐことが困難な未知の脅威に、どのように対応するべきか

現在、自治体のIT活用において避けては通れないテーマがセキュリティです。「自治体情報システム強靭性向上モデル」といった総務省主導の対応はもちろん、インターネットの出入口やエンドポイントを中心に、ファイアウォール、IPS、スパムメール対策、ウイルス対策ソフトなど、田原市独自でも、様々な対策を講じてきました。

しかし2016年6月、職員が受信した攻撃メールの添付ファイルを開き、PCがウイルス感染するインシデントが発生しました。市民サービスには直接の影響はなかったものの、情報漏えいなどの被害が起きていないか確認できるまで、5日間にわたって自主的に一部のネットワークを停止させました。

この際、インシデント原因究明をトレンドマイクロ株式会社（以下、トレンドマイクロ社）へ依頼し、その調査で「Deep Discovery Inspector™（以下、DDI）」の効果を実感して頂きました。「調査の結果、原因がオンラインバンキングを狙った未知のマルウェアだと判明しました。ゼロデイ攻撃など、侵入を100%防ぐことが困難な未知の脅威に対し、どう対応するべきかという課題を突きつけられました」と田原市の小久保氏は振り返ります。

愛知県田原市役所
総務部情報システム係
課長補佐兼係長
小久保 高 氏

■ 導入のポイント

既存資産も有効活用し、脅威に対して、早期の気付き・対処できる仕組みづくりへ

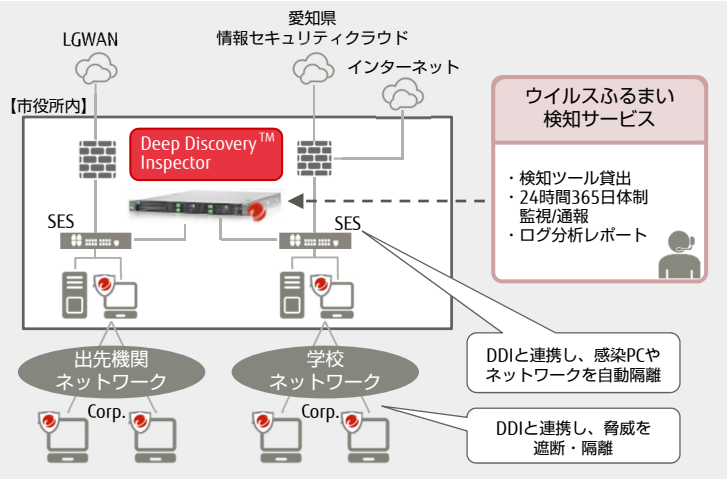
田原市は脅威を検知するセンサーにDDIを導入、他の製品と連携させ、被害を最小限化する仕組みを構築しました。同市は、庁内ネットワークをアライドテレシス株式会社（以下、アライドテレシス社）の機器で構築しています。DDIはSDN（Software Difined Network)を実現する同社の「Secure Enterprise SDN（以下、SES）」と連携し、DDIが不審な通信を検出した場合、事前に設定したポリシーに基づき関連端末やネットワークセグメントを自動で隔離・遮断を可能としました。

他にもDDIは、既に端末のウイルス対策に導入していたウイルスバスター™ コーポレートエディション（以下、Corp.）と連携し、パターンファイルで検知できない脅威をクライアント側で検知・隔離が可能となりました。これらの仕組みにより、同市は脅威検知時の一次対応、および被害の局所化を図りました。

「ウイルスふるまい検知サービス」を採用

DDIの導入にあたり、「ウイルスふるまい検知サービス」は、セキュリティセンターによる24時間365日体制の監視やレポーティング、検知後の対処まで、トータルで支援します。DDIからのアラートで危険度の高いものだけをセンターで判断し、通報を行うため、お客様の運用負荷軽減が実現できました。

また、これらの運用とDDIの機器レンタルを月額サービスとして利用し、初期投資を抑えることにも成功しました。特に自治体は、リソース不足で専任担当者の配置が難しく、数年単位で異動があり、ノウハウの蓄積が難しい現状です。負担を増やさず、安全性が高まると高評価を頂いています。



■ 導入効果

現在、外部接続のあるインターネット系ネットワーク、及びLGWAN上の約1,300台の端末がDDIの監視対象です。市庁舎と支所の出先機関、市立小中学校で教員が利用する端末も含まれます。

「ネットワーク制御のアライドテレシス社、セキュリティのトレンドマイクロ社、運用の富士通エフサスと、各スペシャリストの密接な連携によって、より強固なセキュリティ対策が確立できました」と同市を長く支援するNTT西日本の鈴木氏は語ります。

「インターネット接続は、愛知県の情報セキュリティクラウドを経由し、閉域網であるLGWANも安全性が高いといわれますが、それでも100%安心とは言い切れません。どこまでも万全を期すことが、我々のミッションです」と、小久保氏の力強いお言葉が印象的でした。

NTT西日本 名古屋支店
ビジネス営業本部
SE担当 主査
鈴木 祐司 氏

■ 今後の展望

「田原市のセキュリティにおける今後のテーマは、職員一人ひとりのセキュリティリテラシー向上です」と、小久保氏は続けます。安全な市民サービスを提供するために、最新技術を活用し、システム全体でセキュリティを向上した同市の取り組みは、他の自治体にとって非常に有効なリファレンスとなることでしょう。

お客様情報

愛知県田原市役所 様

所在地	｜	愛知県田原市田原町南番場30-1
市長	｜	山下 政良
職員数	｜	656人（2017年4月1日現在）
URL	｜	http://www.city.tahara.aichi.jp/

「ウイルスふるまい検知サービス」詳細は、以下よりアクセスをお願いします。
»» http://www.fujitsu.com/jp/fsas/solutions/business-technology/security/detection/index.html

2017年12月

株式会社富士通エフサス

〒211-0012 神奈川県川崎市中原区中丸子13-2野村不動産武蔵小杉ビルN棟
お問い合せ 0120-860-242　http://www.fujitsu.com/jp/fsas/

●お問い合わせ