Case Study REPORT

PFU a Fujitsu company

NO.40

～ サイバーセキュリティソリューション ～

標的型サイバー攻撃対策支援サービスで行政ネットワークの安全性向上を実現

豊川市役所様

膨大な住民情報を保有する地方自治体にとって、情報セキュリティの確保は重要な課題。近年では総務省が自治体情報システムの強靭化対策を打ち出すなど、より一層の取り組みが求められている。こうした中、愛知県・豊川市では、PFUの「標的型サイバー攻撃対策支援サービス」を新たに導入。独自の脅威検知技術と24時間・365日の監視体制、分析・対処支援などのサービスを活用することで、セキュリティのさらなる強化を実現している。

自治体クラウド導入を契機にセキュリティの強化に着手

愛知県南東部に位置し、本宮山麓と三河湾の豊かな自然環境に恵まれた豊川市。豊川稲荷の門前町として古くから栄え、東洋一といわれる豊川市海軍工廠が建設されたことでも知られる同市は、現在も東三河地域の拠点都市として発展を続けている。

また、同市の大きな特長の一つが、情報セキュリティへの取り組みに力を入れている点だ。豊川市役所　企画部情報システム課　白井秀和氏は「平成24年度に庁内端末のシンクライアント化を実施したほか、二要素認証などの技術もいち早く取り入れて情報の安全な活用を進めてきました」と説明する。

こうした取り組みの一環として今回実施されたのが、いわゆる「インターネット分離への対応」だ。総務省では各自治体に対し、庁内ネットワークの3分割や自治体情報セキュリティクラウドの構築を求めている。同市でもこれに対応すべく、庁内のインターネット系業務を自治体情報セキュリティクラウドに移行することとなった。

ただし、ここで課題となったのが、新たな環境にふさわしいセキュリティ体制をいかに確立するかという点だ。白井氏は「情報システム課では、行政だけでなく市全体のネットワークを担当しています（教育委員会等）。セキュリティクラウドに載る庁内のデータは守れても、個人情報を取り扱う教育委員会は置き去りということでは問題ですので、我々の管理下にあるネットワークの安全を全て守れる環境を目指したいと考えました」と振り返る。

高い検知能力と手厚い支援がソリューション選定の決め手に

同市ではこのような課題を解決すべく、今後の情報セキュリティを担うソリューションの選定に着手。まず目を付けたのが、サンドボックス機能を搭載したアプライアンス製品だ。「これに関しては、単一のネットワークしか監視できない点がネックとなりました。各セグメントに個別に機器を設置するのでは、導入費用が高額になる上に管理もバラバラになってしまう。また、ネットワーク内部の通信状況を監視する製品なども候補に挙がりましたが、これも実際に脅威を検知した際の対応などはサポート外のため、採用には至りませんでした」と白井氏は説明する。

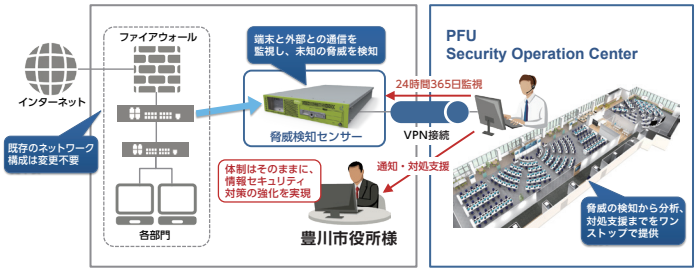
セキュリティインシデントへの対応には高度な専門知識が求められるため、一般企業や自治体内部の要員だけで対処するのは困難な面がある。様々な脅威を確実に検知できるだけでなく、いざという時にエキスパートの支援が受けられることも、同市にとっても非常に重要な要件だったのだ。

こうした点をクリアできるソリューションとして、新たに導入されたのが、PFUの「標的型サイバー攻撃対策支援サービス」だ。ここでは、PFU独自開発の標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」を搭載したセンサーを活用し、未知のマルウェアによる攻撃もリアルタイムに検知。加えて、PFUのSOC(Security Operation Center)による24時間・365日体制の監視も行われる。さらに、万一脅威が発見された場合には、インシデントの分析を行った上で、その後の対処行動も

＜お客様概要＞

名　　称 ： 豊川市
面　　積 ： 161.14㎢
人　　口 ： 18万3264人(2017年12月1日現在)
公 式 H P ： https://www.city.toyokawa.lg.jp/
市 概 要 ： 本宮山麓、豊川、三河湾の豊かな自然に恵まれた地方自治体。市内には商業施設も多く暮らしやすいことから、年々人口も増加している。豊川稲荷といなりずしをモチーフにした市公認のゆるキャラ「豊川市宣伝部長いなりん」も高い人気を獲得している。

<導入イメージ>



支援。これにより、セキュリティの専門要員が不在の場合でも、効果的に情報の安心・安全を守れるのだ。

「ネットワーク内部における怪しい通信などをしっかりと見張れる上に、専門スタッフによる人的なサポートも受けられる点を高く評価しました」と白井氏は語る。

約3400台の端末を監視
安心感も大幅に向上

今回導入された標的型サイバー攻撃対策支援サービスは、2017年3月より本番運用を開始。市役所や出先拠点などで利用されている行政用端末約1200台に加えて、市内の小中学校などに設置された約2200台の教育用端末も監視対象となっている。

サービスの導入にあたっては、ネットワークのどの部分にセンサーを配置するか、かなり慎重に検討したとのこと。白井氏は「大規模環境を一元的に監視できるのが標的型サイバー攻撃支援サービスの良さなので、できるだけ抜け・漏れなく監視できる場所にセンサーを置きたかった。ただし、これさえ決まってしまえば、後の作業にさほど苦労はありませんでした。センサー自体はスイッチのミラーポートにつなぐだけですから、既存のネットワークに大きな改修を加える必要もありません」と語る。

万一、PFUのSOCが脅威の活動を検知した場合には、勤務時間内であれば情報システム課のグループウェアに、勤務時間外であれば職員の携帯電話にそれぞれ通知が行われるとのこと。白井氏は「脅威検知の第一報に続いて、調査・解析結果が第二報として届きますから、その内容を受けてこちらで対処行動を取る形になります。エンドポイント対策用のウイルス対策ソフトなどももちろん導入はしていますが、それだけでは本当にネットワーク内部が安全な状態かどうか確証が持てない。しかし、標的型サイバー攻撃対策支援サービスによる常時監視が行われるようになったことで、安心感は格段に向上しましたね」と語る。

通常とは異なる活動を
実際に検知したケースも

標的型サイバー攻撃支援サービスの導入後、データが流出するようなインシデントは実際に発生はしていません。事前のアラート検知は日々報告ありますが、直ぐに処置するような案件ではない。しかし、その効果を実感する場面も決して少なくはないという。

「たとえば以前、県のセキュリティ脆弱性診断を受けた際に、センサーからアラートが上がったことがあります。この時はオンサイト診断を行うために、脆弱性チェックツールをネットワーク内部で走らせていたのですが、これをセンサーが異常な行動として検知したのですね。何らかのデータがインターネットへ出て行ったわけではなく、まだネットワーク内部で活動している段階でも、怪しい通信をしっかりと察知できたことは非常に心強い。実際に、システム同士の横の通信もチェックしていることが確認できたのは、我々にとっても大変いい経験になりました」と白井氏は語る。また、標的型サイバー攻撃支援サービスで提供される月次レポートなども、庁内ネットワークの安全性を確認する上で役立っているとのことだ。

とはいえ、攻撃者の手法も年々巧妙化しているだけに、同市では今後も引き続きセキュリティ強化に取り組んでいく考えだ。「最近ではAI技術を活用した対策なども注目されていますので、PFUにもぜひ今後のトレンドを踏まえた先進的なソリューションを期待したいですね」と展望を語った。

ネットワーク内部の通信から脅威を検知
その後の対処行動もエキスパートが支援

PFUの「標的型攻撃対策支援サービス」は、自前の取り組みだけでは難しい高度なセキュリティ対策を可能にするサービスです。マルウェア自体の特性やふるまいではなく、ネットワーク内部の通信状況から攻撃プロセスを見出す独自の標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」を活用。また、SOCによる24時間・365日監視に加えて、インシデント分析、対処支援なども行います。これにより、高度な専門知識を持つセキュリティ人材が不在の場合でも、情報インフラの安心・安全を守ることができます。

お問い合わせ先

株式会社 PFU

■横浜本社
〒220-8567 横浜市西区みなとみらい4-4-5 横浜アイマークプレイス ☎(045)305-6000

■北海道支店 ☎(011)242-2212
■東北支店 ☎(050)3786-2204
■北陸支店 ☎(050)3819-9160
■東海支店 ☎(052)202-0871
■関西支店 ☎(06)6152-8153
■九州支店 ☎(050)3819-9180

http://www.pfu.fujitsu.com/

2017年12月 J-040 ALL30S