FireEye®

標的型サイバー攻撃対策
FireEye | 導入事例

User's Profile

静岡県富士市 様

富士市

名　　称：富士市
所 在 地：〒417-8601
　　静岡県富士市永田町1丁目100番地
導入時期：2015年12月
U　R　L：http://www.city.fuji.shizuoka.jp/

1966年11月、旧富士市、吉原市、鷹岡町が合併して誕生。2016年には市制施行50周年を迎えるため、2017年3月までかけて市内各所で記念行事が行われる。また、2013年に富士山が世界文化遺産に登録されたことから、その南に位置する同市も観光に注力しており、Webサイトなどを通じて国内外にその魅力をアピールしている。

総務部 情報政策課
課長
深澤 安伸 氏

「FireEye FXシリーズ」を中核とした検疫ソリューションにより、ネットワーク間におけるファイルの安全なやりとりを実現。ネットワークの分離に対応。

ポイント

- FireEye独自の仮想実行エンジン「MVX」がファイルのふるまいを解析
- 指定フォルダにアップロードされたファイルを解析、結果に応じてファイルを自動振り分け
- ファイルの安全なやりとりを実現することで、ネットワーク分離の要求に対応

マイナンバー制度のスタートにあたりサンドボックス型セキュリティの導入が必須に

静岡県東部に位置し、富士山と製紙の街として知られる富士市は、かぐや姫伝説の地としても有名である。2016年は、2市1町が合併し同市が誕生してから50周年にあたるため、これを記念してさまざまなイベントが執り行われる予定だ。

これまで積極的にITの活用に取り組んできた。同市は、住民基本台帳、税金、福祉などの個人情報を扱う「基幹系」と、財務や人事など内部業務システムを利用するための庁内LAN系（LGWAN）およびメールやWebなどで利用するインターネット系の2つを扱う「情報系」を同一の環境で運用していた。しかし、2016年1月からスタートするマイナンバー制度へ対応するにあたり、同市はさらなるセキュリティ強化の検討を開始した。

マイナンバーは第一級の機密情報であり、万が一にも漏えいは許されない。そこでどんな対策をとればよいのかが問題となる。2014年に総務省が発表した「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」には、「基幹系と情報系のネットワークを同一環境で運用している場合、マルウェア対策としてサンドボックス装置を導入すること」とあり、また、地方公共団体情報システム機構の「地方公共団体の中間サーバやソフトウェアに関するシステム設計書」にも、「共用環境で庁内LAN接続をしている場合はサンドボックスの導入が必須」と明記されていた。そこで同市は検討を重ねた上、インターネットの入口／出口対策に対応したサンドボックス型の標的型サイバー攻撃対策「FireEye NXシリーズ」の導入を決定した。

ネットワーク分離という要求に応えるため検疫ソリューションの導入を検討

しかしその後、事態は急転する。総務省の自治体情報セキュリティ対策検討チームによる報告「新たな自治体情報セキュリティ対策の抜本的強化に向けて」の中で「3層からなる対策」の提言がなされ、マイナンバーを利用する基幹系と、業務システムを利用する庁内系、メールやWebを利用するインターネット系の3つのネットワークを分離し、庁内系とインターネット系でやりとりする際にはウイルス感染の恐れがない無害化通信を図るようにという指針が発表された。これについて富士市総務部 情報政策課 課長の深澤安伸氏は「なにせ突然の話でしたので、私たちも驚きました。万全なセキュリティ体制を築くために各ネットワークを分離しなさいという指針はもちろん理解できますが、単純に分けただけでは業務の利便性が大幅に落ちてしまいます。そこで、ネットワーク間でファイルを安全にやりとりできる仕組み、具体的にはメールに添付したファイルや、インターネットからダウンロードしたファイルを、ウイルス感染がないことを確認してから庁内系へと移す検疫ソリューションが必要と考えました」と当時を振り返る。

そこで同市は、すでに採用が決まっていたFireEye NXシリーズの販売元であるマクニカネットワークスに相談したところ、「FireEye FXシリーズ」を検疫ソリューションとして活用することを提案された。

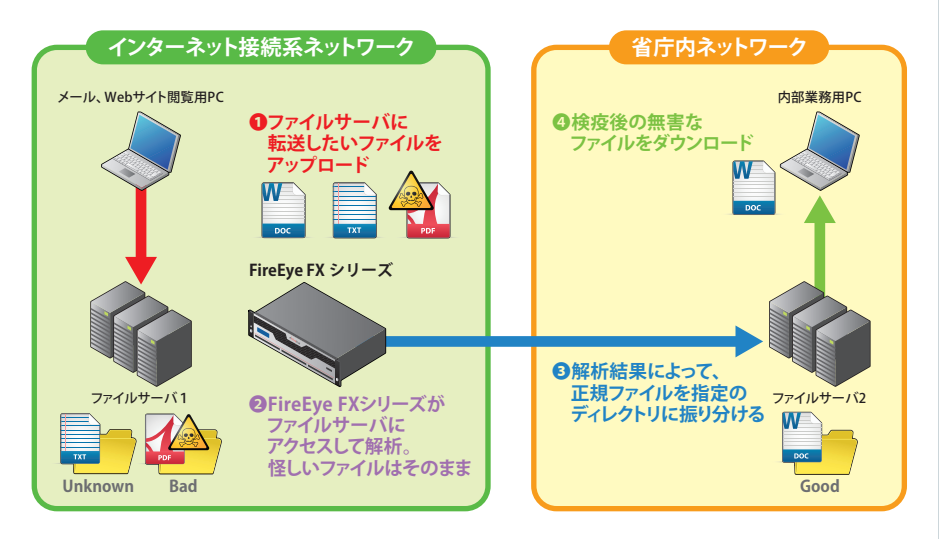
「シグネチャで検疫を行う製品も検討したのですが、未知の攻撃への対処という面で不安があり、サンドボックス製品の機能を使ってネットワーク間の安全なファイル転送を実現できないかと考えたのです。そこへFireEye FXシリーズの紹介を受け、そのファイル・コンテンツ・セキュリティ機能が今回の目的に合致すると判断し、採用を決定しました」(深澤氏)

検疫の仕組みのわかりやすさとかかる時間の短さを評価

富士市は2015年12月にFireEye FXシリーズを導入。庁内系ネットワークに配置し、そこからファイルサーバをスキャンするかたちで検疫を行っている。

検疫の具体的な流れは以下の通りだ。まず、ユーザがメールやWebサイト経由で取得したファイルは、インターネット接続系の「ファイルサーバ1」に格納される。FireEye FXシリーズはこれらのファイルを分析し、「Good(正常)」「Bad(危険)」「Unknown(不明)」の3段階に振り分ける。そしてGoodフォルダの中のファイルのみを「無害ファイル」として庁内系にある「ファイルサーバ2」へ移動し、最終的にユーザへと公開される。反対に、庁内系のシステムで作成されたファイルは、逆の経路をたどって外部に配信されることになる。

「FireEye FXシリーズによる検疫は、ファイルの入口と出口の2つを用意するだけでよく、仕組みが単純でわかりやすいのがいいですね。指定の場所にファイルを置くだけで自動的に検疫されるので、ユーザにもわかりやすい。通常のファイルサイズなら検疫にかかる時間もわずかですし、利便性が損なわれることもありません」(深澤氏)



独自の仮想実行エンジン「MVX」で未知の攻撃を防御

深澤氏は「FireEyeシリーズに搭載されている独自の仮想実行エンジン『MVX』は非常に優秀で、他のセキュリティ製品では検知できないような未知の攻撃まで防御でき、実際に何度も攻撃を止めています。また、検知した脅威がどの程度危険なものかを5段階で判定し、それを後から記録として見ることができるので、検証も簡単です」とその性能を評価する。

一般にサンドボックス製品の場合、誤検知や過検知が多発すると、担当者に過剰な負担がかかってしまうが、その点FireEyeは本当に危険な脅威のみアラートをあげるため、そういった心配はない。ただ、今後はセキュリティ対策が必要になる場面がさらに増えることが予想されるため、同市でもFireEye NXシリーズやFireEye FXシリーズから出力されるアラート情報を分析できる担当者の育成を進めていく予定だ。

「運用の流れがある程度フォーマット化されているFireEyeなら、短時間の教育で済むのではないかと考えています。また、攻撃フェーズがキーワードで簡単に確認でき、障害の切り分けも可能なので、セキュリティに詳しくない担当者でも状況判断がしやすいのではないでしょうか」(深澤氏)

FireEye FXシリーズの本格的な運用が始まるにあたり、同市ではマクニカネットワークスのサポートへ大いに期待を寄せている。「今回の導入では、検疫ソリューションが欲しいという依頼に対し、的確なタイミングで最適な提案をいただけました。実際に運用が始まれば、不具合への対応、検体の検査などでいろいろとご相談することになると思いますので、今後も継続的な支援をお願いします」(深澤氏)

その期待に応えるため、マクニカネットワークスは今後も富士市のセキュリティの取り組みを支援していく。

http://www.macnica.net/fireeye/

macnica networks

マクニカネットワークス株式会社

本社　〒222-8562 横浜市港北区新横浜 1-5-5
TEL.045-476-2010 FAX.045-476-2060
西日本営業所　〒530-0005 大阪市中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916 FAX.06-6227-6917