FireEye®

標的型サイバー攻撃対策
FireEye | 導入事例

User's Profile

東京都北区 様

標的型サイバー攻撃による情報漏えいを未然に防ぐため、FireEyeを選択
ゼロデイ攻撃の増加に伴う強固なセキュリティ対策を実現

東京都北区

名　　称：東京都北区
所 在 地：〒114-8508
　　東京都北区王子本町1-15-22
導入時期：2015年6月
U　R　L：http://www.city.kita.tokyo.jp/

東京都23区の北部に位置し、東西約2.9km、南北約9.3kmの面積20.59平方キロメートルの区域に総人口約33万人が暮らす特別区。荒川、隅田川、石神井川、新河岸川の4つの河川が流れる豊かな水辺空間と、桜の名所たる数多くの公園、23区内最多の11駅を抱えるJRや地下鉄、都電など区内のほぼ全域が駅まで徒歩圏内という交通利便性が特徴で、平成11年度からは「子ども」「元気」「花とみどり」「安全・安心」をキーワードにした4つの重点戦略に基づく区政運営を行っている。

東京都北区
区民部区民情報課
区民情報主査
菊池 亜紀子 氏

東京都北区
区民部区民情報課
（電子区役所担当）
主任主事
杉田 義和 氏

ポイント

- これまで見えていなかった脅威を具体的に把握することが可能に
- 本当に危険な脅威のみアラートがあがるため運用しやすい
- 初動対応をネットワーク監視サービスと連携することで、情報漏えいを即時ブロック

情報系ネットワークの更改を機に標的型サイバー攻撃への対応を強化

東京都23区の北端に位置し、荒川を隔てて埼玉県と接する北区は、隅田川、石神井川など区内を流れる4つの河川が豊かな水資源を恵み、古くから伝統工芸や消費材生産業が発達した文化都市だった。江戸幕府末期に滝野川反射炉が設営されたのを端緒に、明治期から昭和中期に至る近代には用水供給が可能な地理を活かした紡績業や製紙業、食品製造業などが発展。その日本の近代産業振興を支えた歴史と文化遺産をベースとして、現在も最先端技術や次世代の製品開発を担う独創的な中小企業が多く立地する。またその創意工夫の精神は区政を担う北区役所のIT化戦略にも通じるところが多い。

東京都北区 区民部区民情報課 区民情報主査の菊池亜紀子氏は、IT化の経緯と課題について次のように語る。「北区は他の自治体に比べ比較的早期にIT化を進めてきた歴史があります。情報セキュリティにおいてもログイン時の生体認証や持ち出し制御による情報漏えい防止などを先駆けて導入し、高いレベルで強固なセキュリティ対策を行ってきました。昨今は自治体を狙った標的型サイバー攻撃が急増しており、それをどう防ぐかが大きな課題となっています。そのため、庁舎内の情報系ネットワークの全面更改を機に標的型サイバー攻撃への対応をさらに強化しようと考えたのです」

北区役所には、住民記録、税等の情報を管理・運用を行う基幹系システムと総合行政ネットワーク（LGWAN）、インターネットに接続する情報系ネットワークの2つが存在するが、情報系を管轄する電子区役所部門は2015年度に情報系ネットワークの大規模な更改を行なった。東京都北区 区民部区民情報課（電子区役所担当） 主任主事の杉田義和氏は、近年の高度化・多様化するサイバー攻撃を危惧していたという。

「ゼロデイ攻撃の脅威が日々増加する中、かねてより市場で顕在化してきていた情報漏えいへの懸念から、2014年夏前より標的型サイバー攻撃の対策を検討していました。従来、北区が導入してきたアンチウイルスソフトは検知内容が不明確で、特にヒューリスティックスキャン機能による誤検知の割合も多く、本来防ぐべき標的型サイバー攻撃の脅威をどのように検知して情報漏えいを防げばいいのかという点を重視し、新たなセキュリティ製品の選定を行おうと考えました」

総務省が示した未知のマルウェア対策サンドボックス装置の有効性

当初は次世代ファイアウォールやIPS製品も検討していたが、最も注目したのが当時マイナンバー制度施行にあたり総務省から発行された「“地方公共団体における情報連携プラットフォームに係る中間サーバ・ソフトウェアの設計開発作業の請負”システム方式設計書」（ガイドライン）が示した、共用環境ネットワーク利用時におけるセキュリティ対策だった。そこには、未知のマルウェア対策として「サンドボックス装

置」の有効性がうたわれていた。
杉田氏は、「ゼロデイ攻撃にはシグネチャで検知できない問題があります。サンドボックス製品ならば怪しいふるまいのものを疑似環境で実行させ脅威を検知できます。近年増えているWeb経由の標的型サイバー攻撃にも対応可能だと考えました」と話す。
サンドボックスの選定基準として、1）運用のしやすさ、2）脅威の可視化、3）初動対応のしやすさの3つを重視した。システムを運用するために常駐するベンダーや、北区のシステム担当者が見ても検知内容がすぐに理解しやすい製品が望ましかったと杉田氏はいう。そこで、代表的な2製品に絞り実践的な評価を行った。その1つが、マクニカネットワークスの提供する「FireEye NXシリーズ」（以下、FireEye）だった。
2014年10月に、検証のため2製品とも実機を取り寄せ、2週間にわたり同一条件・同一ポジションで本番環境に近い形での評価を行った。その試験運用を踏まえて具体的な運用も含めて検討した結果、最終的にFireEyeが選定された。
「試験運用中にもいくつかの脅威を検知しました。別製品は2週間で1000件以上ものアラートが上がり、その内容確認から始めなければなりませんでした。一方で、FireEyeのアラートは10件弱、さらに独自の仮想実行環境でマルウェアがどのような挙動をしているのかを動的に分析し、本当に脅威となるものだけに絞り込むため、対応の優先順位が判断しやすく、時間との勝負の標的型サイバー攻撃にも有効に働くと考えました」と杉田氏は述べる。
管理画面では分析結果のサマリ情報と詳細情報が時系列で表示され、どのような侵入方法を試みようとしたのかが整理された形で可視化されるため、管理者として把握しやすかったという。「PoV（Proof of Value：導入前検証）レポートも明確で、検証過程で感じた疑問にもマクニカネットワークスの担当SEが逐一解説してくれた上に、その内容も理路整然としていて、信頼性も感じました」（杉田氏）

FireEyeで通信トラフィックを監視し防御の難しいWeb経由の攻撃にも対応

2015年6月にFireEyeを導入し、2015年7月に本運用を開始した。北区役所の職員用端末と学校の教職員が利用する校務支援システムにつながる端末の合計約3400台をFireEyeが守っている。
具体的には、FireEyeで常にWeb通信トラフィックを監視し、脅威が検知されるとアラートが管理者に飛び、どの端末で何が起きているのかを迅速に把握するとともに、端末を使用しているユーザに連絡。一方で、同様の感染を防ぎ、また感染した端末のC&Cサーバへのコールバック通信を防ぐために、ログから得られる通信先情報を元にネットワーク機器で通信を遮断。感染の疑いのある端末は、即座にネットワークから隔離し、調査・対応を行う。また、MVX（仮想実行エンジン）内で疑わしい通信を実際に再現し、発生した事象を詳しく解析しながら、FireEyeの管理画面上でインシデントを詳細に確認してレポートするという流れだ。各機器のログ情報を組み合わせ、検知元となったWebサイトを特定することもできる。また、端末は、マルウェア感染の有無に関わらずディスク自体を交換している。
北区役所では標的型メール攻撃に対する訓練を2015年から定期的に行っており、怪しいメールが来た場合はすぐに報告するよう職員に周知されている効果もあって標的型メール攻撃での被害はない。しかし、FireEyeの本稼働後、月1 ～ 2件ほど攻撃を検知している。いずれもWeb経由の攻撃だ。
菊池氏は、「標的型メール攻撃に対しては訓練のおかげで職員の警戒心は高いのですが、Web閲覧によるマルウェア感染を意識して防ぐことは容易ではありません。FireEyeを導入したことによって、防御の難しいWeb経由の標的型サイバー攻撃も防ぐことができるようになりました」と評価する。
杉田氏は、FireEyeの効果に注目する。「どの端末が、いつ、どこから攻撃を受けているのか、さらにどの端末が感染していてC&Cサーバと通信を行っているのかが容易に把握できるため、評価通りの効果が得られたと満足しています」

社会全体のセキュリティレベル向上に役立つFireEye

FireEyeを導入した意義について菊池氏は「マルウェアを検知した場合に改ざんされたWebサイトの管理者へ注意喚起を行うことも出来ます。私たちがセキュリティレベルをあげることで、社会全体のセキュリティレベルをあげることにも繋がると思います」と語る。
2017年度からは基幹系ネットワークと総合行政ネットワーク（LGWAN）に接続する情報系ネットワークを接続し、マイナンバー運用に必要な連携を行う必要がある。また、総務省から「自治体情報システム強靭性向上モデル」に基づく庁内ネットワークの再構成も要請されている。
菊池氏は、今回のプロジェクトを振り返り、「マクニカネットワークスにはFireEyeの評価段階から疑問や運用の不安に対して的確にサポートしていただき、知見の深さを感じました。」杉田氏は「今後北区が取り組むセキュリティ強化に向けた新たな挑戦においても、引き続きプロフェッショナルな助言を期待しています」と希望する。
その思いに応えるため、マクニカネットワークスは持てる知見を動員し弛みない改善を目指す北区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
西日本営業所　TEL.045-476-2010 FAX.045-476-2060
〒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