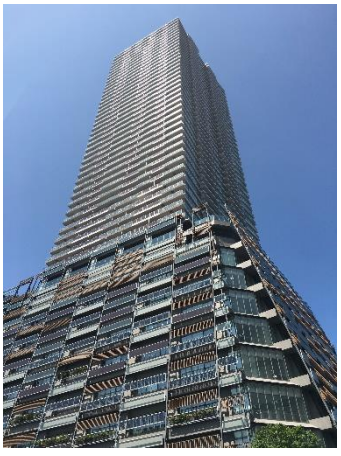
FFRI yarai analyzer 導入事例

豊島区役所様

Automated Malware Analysis System

現庁舎移転のタイミングで庁舎内のシステムを洗い直し、区民の窓口業務を守るため、移転後から有人による24時間365日体制に

豊島区では都市づくりの基本構想において区の将来像を『未来へ　ひびきあう、人　まち・としま』と掲げ、平和の希求、人権の尊重、住民自治の実現を基本的な理念とし、さまざまな人と共に生き、共に責任を担う協働・協創のまちづくりを推進しています。この将来像を実現するため、豊島区に住み、働き、学び、訪れるすべての人と共に地域づくりを推進していく姿勢として「1.あらゆる主体が参画しながら、まちづくりを実現していく」「2.安心して住み続けられる、心のかよいあうみどりのまちを創造する」「3.魅力と活力にあふれる、にぎわいのあるまちをめざす」「4.伝統・文化と新たな息吹が融合する文化の風薫るまちをめざす」の4つの柱を示しています。



豊島区役所庁舎

豊島区 政策経営部 情報管理課には、セキュリティ、システム、基盤の各グループがあり、外部業者に委託しているヘルプデスク担当と窓口担当と協働しながら豊島区における行政情報推進等を行っています。

豊島区役所は、2015年5月に現庁舎へ移転しました。移転前よりウイルス対策ソフト、PCの認証、IPSやIDSなどの不正侵入検知・防御システム、標的型メール訓練等でセキュリティ対策と、全職員に対してセキュリティに関するルールや知識の周知の徹底を行ってきましたが、より強固なセキュリティ対策を行うべく、移転が決まってから庁舎内のシステムを洗い直し、移転後に有人による24時間365日体制で、各メーカーやベンダーが構築した庁内のシステムやネットワークを一元的に管理・運用・保守を行う統合運用管理サービスの利用をスタートさせました。

導入の背景・経緯
移転前にできていなかった、より強固なセキュリティ対策の実現

現庁舎への移転にあたり、移転の2～3年前からは庁舎内のシステムの洗い直しにとどめ、移転のタイミングで実現させたい、新たなセキュリティ対策の計画を推進してきました。

「毎朝8時半には窓口業務が動いている必要があります。土日も開庁している区民の窓口業務をしっかりと守るべく、有人での24時間365日体制は必須でした」(秋山氏)

「移転前、ログ管理や通信をすべて見るフォレンジックはまだできていませんでしたが、今後は必要になるだろうと考えていました」(芝崎氏)

「未知マルウェア対策としてサンドボックスを利用した製品も、これからは利用していくべきと移転前から考えていました」(木本氏)

そこで有人による24時間365日体制で統合運用管理サービスの利用を移転後から開始することになりました。統合運用管理サービスの一環である「FFRI yarai analyzer（以下、yarai analyzer）」は、パケットキャプチャ製品（トーテックアメニティ社「NetRAPTOR」）との連携や、未知マルウェア検出に優れたエンジンにより仮想環境上で動的解析が可能であるという点で、まさに豊島区が移転前から求めていた、新たなセキュリティ対策の要望を満たすセキュリティ製品として評価されました。

導入の効果
メール経由のマルウェアを庁舎内で解析、結果を迅速に報告

日頃のセキュリティに関する啓発活動の成果などもあり、各職員の意識も高まり、職員からメール開封前に「怪しいメールが届いているが、大丈夫か？」といった問い合わせが情報管理課に入るようにもなってきましたが、メール経由のマルウェアの監視は優先事項となっていました。

豊島区では現在、メール添付ファイルのマルウェア検査に活用するため、yarai analyzerをパケットキャプチャ製品（NetRAPTOR）と連携して利用しています。現庁舎への移転以降、何件かのマルウェアの検出がありましたが、統合運用管理サービスのヘルプデスク担当が検出後すぐに庁舎内でyarai analyzerで解析し、情報管理課に迅速に報告を上げることができました。

「解析の結果、いずれも幸いなことに事故につながるようなマルウェアではありませんでした。仮に今後、深刻なマルウェアが発生した場合でも、外部に依頼することなく、スピーディーに庁舎内で解析できるようになったため、移転前に比べてセキュリティレベルが上がっていると感じています」（木本氏）

今後の展望
よりセキュリティレベルと効率を上げるyarai analyzerの運用方法を検討

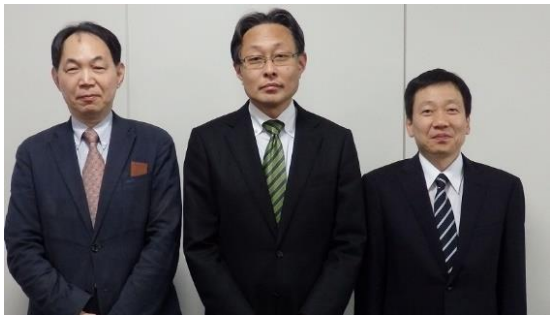
2015年の日本年金機構の情報漏洩事故を受け、総務省は各自治体に2017年7月までに下記2点の実施を求めています。

●「自治体情報システム強靭性向上モデル」に基づき、LGWAN(統合行政ネットワーク)接続系とインターネット接続系のネットワーク分離
●市区町村が個々に持っているインターネットの接続口を都道府県レベルに集約し、セキュリティレベルの向上を図る「自治体情報セキュリティクラウド」の実施

豊島区も現在、上記の運用手順の作成にあたっています。

「セキュリティ対策に関して総務省や都からの通達に合わせた対応を行っていくだけでなく、豊島区自身で気が付いたことも積極的に進めていく予定です。ICTは日々進化しており、各セキュリティ製品の機能も増えています。予算はもちろんのことですが、セキュリティ脅威の現状とICTの進化を合わせて考え、豊島区のセキュリティ対策にはどこが足りないのか、どこを強化すべきか、各製品のすみ分けについても常に考えています 」（芝崎氏）

豊島区は今後、東京都のセキュリティクラウドを利用していくことになるため、都のセキュリティクラウドを利用した場合に、よりセキュリティレベルと効率の上がるyarai analyzerの利用方法を検討していきたいとのことです。



(右から)豊島区 政策経営部 情報管理課
情報担当係長(基盤グループ) 木本 隆氏、
情報管理課長　秋山 直樹氏、
情報担当係長(課長補佐) 芝崎 良彦氏

製品・サービスについてのお問い合わせは
株式会社ＦＦＲＩ
〒150-0013
東京都渋谷区恵比寿1-18-18　東急不動産恵比寿ビル4階
TEL：03-6277-1811　E-mail：sales@ffri.jp
本製品に関する情報はインターネットでもご覧いただけます。
http://www.ffri.jp/

Ver 2.00.01
2017年6月現在