FireEye®

サンドボックス型脅威解析システム
FireEye NX7500 Essential | 導入事例

User's Profile

国立大学法人 大分大学 様

国立大学が標的型攻撃対策に次世代型サンドボックスを導入
サンドボックス回避型マルウェアも高精度に検知し
拡大が予測される教育機関への高度なサイバー攻撃にも対応

ポイント

- 検証機による評価でバックドア通信を多数発見し効果を実証
- ネットワーク全体の見直しとアカデミックパッケージの適用で予算内導入を実現
- 誤検知率やグレー判定が少なく検知後の切り分けが容易なため小人数での運用も可能に
- Mac OSにも対応した網羅性の高い攻撃検知システム

国立大学法人 大分大学

名　　称：国立大学法人 大分大学
所 在 地：〒870-1192
　　大分市大字旦野原700番地
導入時期：2017年2月
U　R　L：http://www.oita-u.ac.jp/

2003年10月に旧大分大学と大分医科大学が統合して設立。大分県の中心部に位置する旦野原、挾間、王子の3つのキャンパスに5学部・5研究科と、教育学部附属学校園、医学部附属病院などを有する県内唯一の国立大学。知の拠点としての機能と地域医療や福祉の高度化で地域活性化に貢献。2016年には44年ぶりの学部新設となる福祉健康科学部を開設し、時代や社会のニーズを踏まえた教育研究組織の改革に向けた歴史的な一歩を踏み出した。

国立大学法人 大分大学
学術情報拠点 副拠点長
（情報基盤センター）
教授 工学博士
吉田 和幸 氏

国立大学法人 大分大学
学術情報拠点
（情報基盤センター）
准教授 博士（理学）
吉崎 弘一 氏

教育機関へのサイバー攻撃急増がサンドボックス導入を後押し

国立大学法人 大分大学（以下、大分大学）の学術情報拠点 情報基盤センターは、旦野原（だんのはる）キャンパスに拠点を置き、挾間キャンパスにある医学情報センターと緊密に連携を取りながら、大分大学における全学的な学術情報基盤の基幹組織として学術情報の整備・充実とその高度化を進める組織だ。教育・研究の進展を図る学術情報拠点の中で、大学の基盤情報システム（情報システムおよび情報ネットワーク）を統括し、学生や教職員の利用を多方面で支援している。

情報基盤センターが管理するキャンパスネットワーク（学内LAN）は、6年ごとに大規模な更改を行っており、前回の2011年に続き、今回は2017年2月28日に更新を完了した。その中で、今回ひときわ注目を集めたのが最先端のサンドボックスの導入だった。

「標的型攻撃の脅威が大きな話題になる中、メール経由の攻撃に対してはメールサーバにて添付ファイルのチェックやスパム対策などを行ってきましたが、Web経由で怪しいプログラムが入って来る場合は途中で何も防御できない状態でした。歴史の古い旦野原キャンパスの情報基盤センターのネットワーク構成が学内にグローバルアドレスを配布した状態で運用しているためプロキシサーバを導入することが難しかったからです」。そう当時の状況を語るのは、大分大学学術情報拠点（情報基盤センター） 副拠点長 教授 工学博士の吉田和幸氏だ。

キャンパスネットワークのファイアウォールにはURLフィルター機能が入っているため、ブラックリストに載ったURLへのアクセスは拒否されるが、高度に偽装された悪意のあるURLやWebの脆弱性を突く攻撃を検知する術がなく、学内の端末にウイルスが侵入してしまう可能性があり、PCのウイルスチェックで防ぐしかない状況だったという。

「情報基盤センターがサンドボックス導入を検討した大きな要因は、近年増加している学校ネットワークへの不正アクセスや、標的型攻撃を起因とする情報漏えい事件の発生でした」と吉田氏は打ち明ける。今後拡大が予測される教育機関に向けた高度なサイバー攻撃に対して、より高度なセキュリティ対策が必要となる。その対策のひとつが高性能なサンドボックスの活用だったことも決断を後押しした。

複数のセキュリティベンダーを厳選 FireEyeに決定した3つのポイント

吉田氏は、東京で開催される国内最大規模ICT展示会にも足を運び、さまざまなセキュリティベンダーの情報を積極的に収集する中で、マクニカネットワークスが提供する次世代の脅威対策ソリューション「FireEye」に注目した。FireEyeの優位性について次の3つが挙げられたという。

1つ目は総合的な検知力。独自の仮想実行エンジン「MVX」（Multi-vector Virtual eXecution

engine）は、ファイルベースの解析ではなくトラフィックフローをマルチに解析し、サイバー攻撃のコンテキスト全体を高精度に把握するとともに、誤検出のアラートを最小限に抑えつつ、疑わしいコンテンツのインライン分析をリアルタイムで実行する。

2つ目は運用の容易性。不正な外部通信を自動ブロックするため運用負荷を大きく軽減できる。3つ目は導入実績。グローバル、日本国内ともにサンドボックス市場での圧倒的な導入実績は大きな安心材料となった。

また、FireEyeはセキュリティベンダーとして世界で初めてAppleのMac OSにも対応し、Microsoft Windowsと同様に、Appleのプラットフォームに対してもAPT（高度かつ継続的な攻撃）やゼロデイ攻撃、標的型攻撃を特定し、マルウェアのアウトバウンド通信を阻止できる機能を提供することも高く評価した。「大学内にはWindowsユーザが多いものの、特に医学部においてはMacユーザの比率が比較的多く、Mac OS対応は既に必要な要件となっていました」（吉田氏）

2016年6月に、マクニカネットワークスからFireEyeの検証機を借り、キャンパスネットワーク内に配置してポートミラーで3週間ほど評価を実施。その結果、学内で既存のセキュリティ対策をすり抜けた攻撃が多数検知され、バックドア通信が27回も見つかったことから、FireEyeの効果が実証されることとなった。

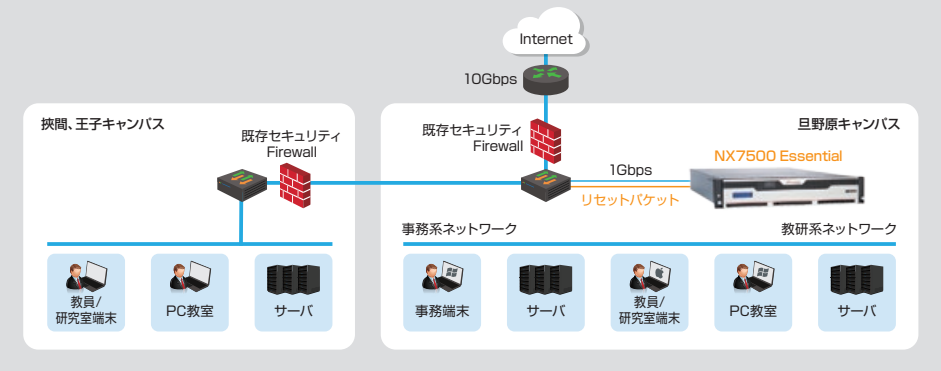
検証に携わった、大分大学学術情報拠点（情報基盤センター）准教授 理学博士の吉崎弘一氏は、「FireEyeのユーザインターフェースは直感的な操作が可能なほど容易で、マニュアルを特に参照しなくてもアラートの箇所を確認し、どんな内容のアラートなのかを把握することができました。使いやすく、簡単に使えると感じました」と当時を振り返り感想を述べる。

検証終了後、7月の報告会を経て、FireEyeを導入するための要求仕様書を策定し、ネットワーク更改プロジェクトの入札要件に加えることが決定した。

アカデミックパッケージを適用し厳しい予算内での導入を実現

製品導入にあたり一番の問題は予算だった。当初はサンドボックス導入に当てるコストを少なく見積もっていたため要求仕様に残せるか厳しい見通しだった。それも、ネットワーク全体の予算を見直すことである程度の予算幅を捻出するとともに、ファイア・アイが国公私立の教育機関（大学、大学院、高等学校および小中学校）を対象とした標準ライセンスより大幅に安価なアカデミックパッケージの提供を2016年11月から開始する予定があり、それを前倒しする形で適用したため予算内導入が実現した。

一方、他大学の管理者と定期的に情報交換をするという吉崎氏は、多くの大学がAPTへの有効な対抗策としてサンドボックスの必要性を感じてはいるものの、予算が捻出できずに導入を断念しているケースも多いという。「もっとサンドボックスの活用を大学全体のリスク管理に直結する施策として前向きに議論するべきですね。単独での予算獲得が難しい場合は、今回当大学がトライしたようにネットワーク機器全体の調達で試算してみるなど、導入を可能にする方法はあると思います」



サンドボックス回避型マルウェアもMVXエンジンで高精度に検知

導入モデルは「FireEye NX7500 Essential」。それを含めた新キャンパスネットワークは2017年3月1日に本稼働を開始した。FireEyeの監視範囲は全キャンパスの学生約5700名と、教職員約1900名を対象とする大規模なものとなっている。具体的には、FireEyeが攻撃を検知するとアラートメールが情報基盤センターの担当メンバー全員に通知され、すぐさまIPアドレスを確認し、その端末の使用者を特定してファイアウォールを停止し、本人に電話かメールで通知して、アクセスを遮断するという流れだ。そして、疑いのあるURLを全学に通知して被害が拡大するのを防ぐ。C&Cサーバとのコールバック通信を迅速に検知し、遮断することが期待できるようになった。「最近のマルウェアの中にはサンドボックスの仮想環境を敏感に判定するものも登場し、一般的な仮想環境の中ではマルウェアが自ら動きを潜めてしまうため検知できないという問題も起きているようです。しかし、FireEyeはサンドボックスを回避するようにプログラムされたマルウェアも高精度に検出できるMVXを搭載しているため、巧妙なサイバー攻撃も検知し、安心してユーザにネットワークを利用してもらうことができます」と吉田氏は評価する。

さらに吉崎氏は、「大学のようなオープンな環境でネットワークをセキュアに管理するためには、運用に手間をかけないことも必要になります。FireEyeは検出精度が高いため誤検知率やグレー判定が少なく、白・黒をはっきりつけてくれるので、検知後の切り分けに手間がかかりません。管理者が小人数でも運用しやすいことに魅力を感じました」と続ける。

この大分大学のFireEye導入は、今後情報セキュリティ体制の強化に取り組む多くの教育機関への模範となるべきものではないだろうか。

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