Web トラフィック検査のためのサンドボックスの運用結果について

吉田 和幸 [1)], 吉崎 弘一 [1)], 安徳 恭彰 [2)]

1) 大分大学 情報基盤センター
2) 大分大学 医学情報センター

yoshida@oita-u.ac.jp

Operation Result of the Sandbox Checking Web Traffic

Kazuyuki Yoshida [1)], Koichi Yoshizaki [1)], Yasuaki Antoku [2)]

1) Information Technology Center, Oita University
2) Medical Information Center, Oita University

概要

大分大学では、2017 年 3 月の基盤情報システムの更新に合わせてサンドボックス装置を導入した。これにより、従来のファイアウォールによる保護に加えて Web アクセスにより侵入する可能性がある malware を検知することが可能になった。本稿では、導入後 6 か月の運用状況（検知結果）について報告する。

1 はじめに

インターネットからのマルウェアの侵入を防ぐための入り口対策は重要である。大分大学では、ファイアウォール等によるセキュリティ対策に加えて、2017 年 3 月の基盤情報システムの更新[1]に合わせてサンドボックス装置(FireEye NX7500 Essential)を導入し HTTP でダウンロードされる実行形式ファイルの検査を行うようにした。本稿では、半年間のサンドボックスの運用の状況を報告するとともに、サンドボックスの有効性について考察する。

2 従来のセキュリティ対策

大分大学は、5 学部、5 研究科からなり、学生約 6000 人、教職員数約 1900 人の規模である。

学内 LAN におけるセキュリティ対策の中心は、2015 年 4 月に導入したファイアウォール(Forti-Gate 1500D)である[2]。本ファイアウォールにより、「学外から学内(Inbound)」,「学内から学外(Outbound)」の両方向のトラフィックを監視し、TCP Flood 攻撃、scan 攻撃等を検知、遮断し、Web ページのアクセスに関しては、URL の分類、レーティングに基づいて、許可／遮断を決定している。ファイアウォールでは stream 型の簡易なウィルス検査を行っている。

メールに関しては、ファイアウォールで行う簡易なウィルス検査に加えて、メールゲートウェイで送信元メールサーバのレーティング情報などを用いて spam 判定を行い、その後、メールサーバでウィルス検査を行っている[3,4]。さらに PC に取り込まれたときに PC のウィルス対策ソフトウェアで添付ファイルのウィルス検査が行われる（表 1）。

これに対して、Web ページからファイルをダウンロードするときは、そのページの URL のレーティングのチェック行い、ダウンロードされるファイルに対してはファイアウォールでは、簡易なウィルス検査を行っているが、十分ではなく PC のウィルス検査に大きく依存していた(表 2)。

3 サンドボックスの導入

Web からダウンロードするファイルを検査する装置として、サンドボックスを導入した（表 2）。サンドボックスは、ダウンロードされているファイルを取り込み、内部の隔離された環境で仮に実行してみて、そのふるまいを確認することでマルウェアを検知する。そのため、未確認のマルウェアを検出することも可能である。今回導入した装置は、隔離された実行環境として Windows 環境とともに Mac OSX 環境も持っている。

表 1. メールの多段防御対策

装置等	対策
Firewall	Inbound/Outbound port 25 Block (IP25B/OP25B) Mail Gateway が送受信するメールのみ通す
Mail Gateway	spam 対策　(Greylisting, S25R, SPF 他)
Mail Server	添付ファイルのウィルス検査
PC	添付ファイルのウィルス検査, C&C サーバとの通信の検知・遮断

表 2. Web の多段防御対策

装置等	対策
Firewall	Inbound port 80 Block (IP80B)(Web サーバ宛の通信のみ通す) Outbound は、フリー
	URL のレーティング
Sandbox (新規)	ダウンロードファイルを隔離環境で実行，ふるまい検査, C2 サーバとの通信の検知
PC	ダウンロードファイルのウィルス検査 C2 サーバとの通信の検知・遮断

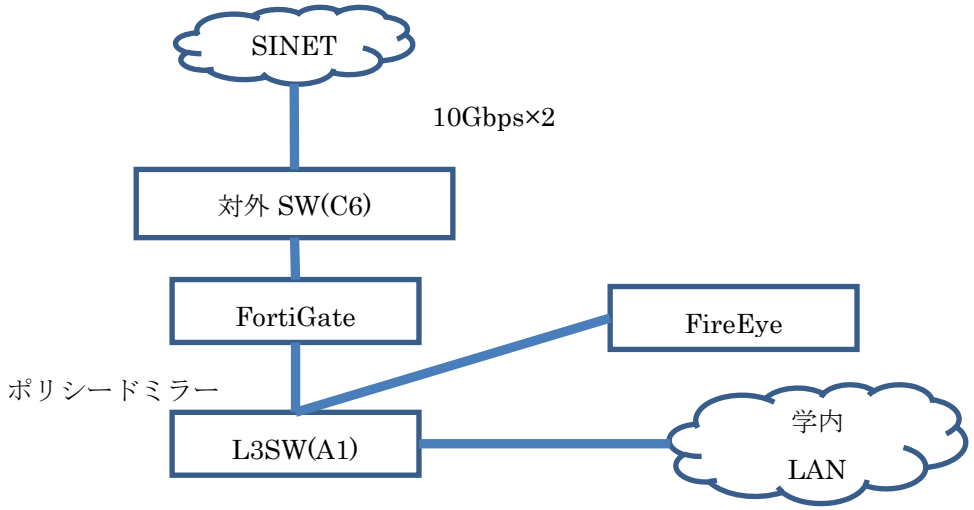

図 1．システム構成図

ファイアウォールの学内 LAN 側のインタフェースと接続する LAN スイッチのポートをミラーして、サンドボックス装置の検知用インタフェースに送っている。サンドボックス内の仮想環境で動作させるのは、80 番ポート、8080 番ポートの http で通信される実行形式ファイルであるが、侵入した Malware と C2 サーバとの通信を検知する機能も持っているので、すべての TCP トラフィックと UDP の DNS トラフィックをミラーしている(図 1)。

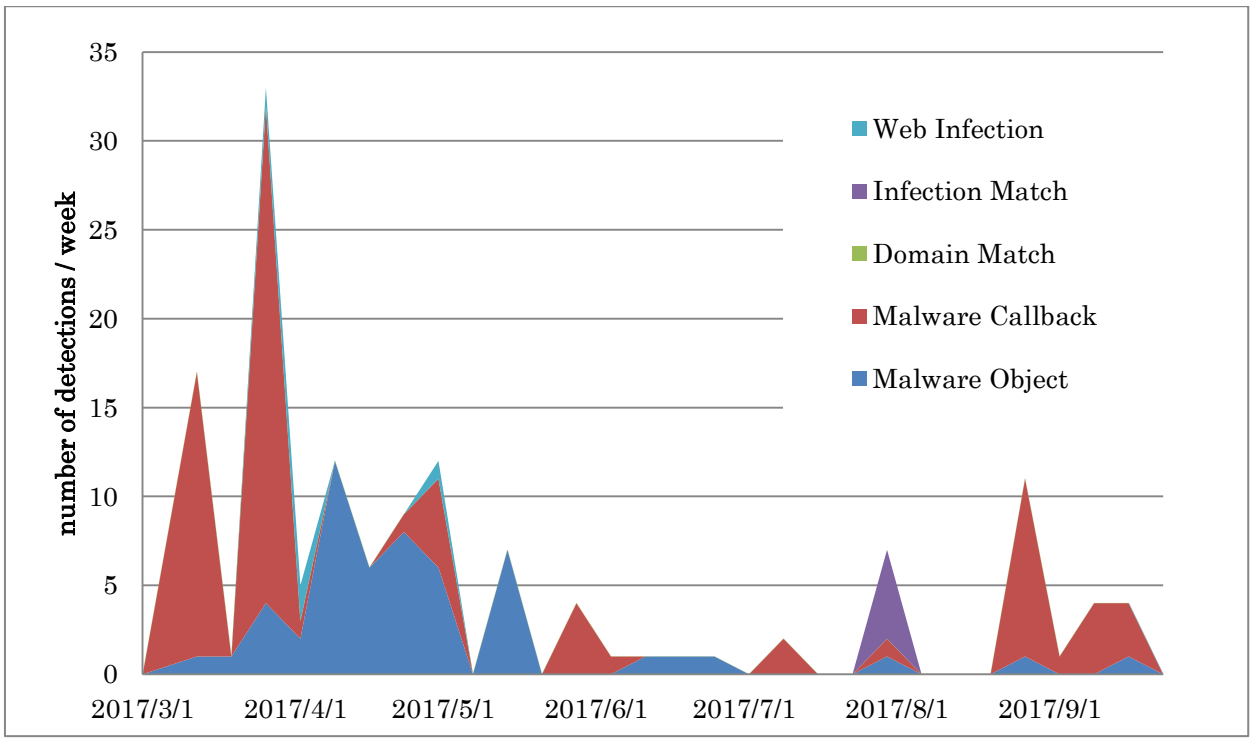

図 2. 検知数の推移

表 3. 検知数

Malware Object	Win	40	53
	Mac	4	
	非依存	9	
Malware Callback			77
Domain Match			0
Infection Match			5
Web Infection			4
Total			139

4 サンドボックスの運用状況

サンドボックスの導入以降、2017 年 9 月までの検知数を表 3 に、1 週間ごとの検知数の推移を図 2 に示す。サンドボックス(FireEye NX7500 Essential)は、以下の 5 つのアラートタイプで検知を行う。

1) Malware Object: マルウェアと思われる実行形式ファイルを検知した。
2) Malware Callback: C2 サーバへと思われる通信を検知した。
3) Domain Match: C2 サーバと思われる FQDN の DNS 問い合わせを行った。
4) Infection Match: 過去に報告実績のあるマルウェア感染を引き起こす攻撃が試行された。
5) Web Infection: web 経由での感染行為(Java, Flush player 等)が試行された可能性がある。

「Malware Object」が、サンドボックス内の仮想環境で実行し、不審な動作をした結果、検知されたものである。

表 3 より、Domain Match アラートは、検知されず、Infection Match アラート、Web Infection アラートは、数件検知された。大部分は Malware Object アラート、Malware Callback アラートである。これらのアラートは、情報基盤センター、医学情報センターで確認し、対処が必要であれば、利用者にダウンロードしたファイルの削除や、ファイルのスキャン等を要請している。

外部との通信を上り下りとも単一のポートへミラーしてサンドボックスに送っているので、Web トラフィックに乗って外から侵入してくる malware、内部から外の C2 サーバへの通信ばかりでなく、その逆も検知できる。学内の Web サーバに関して Malware Object の検知が 5 回、外から学内に向かう Malware callback アラートが 30 回検知された。Malware Object は、ファイルスキャンの結果、誤検知であった。Malware callback は、C2 サーバ探索のスキャンであり、

学内側の IP アドレスは未割当であった。

5　まとめ

2017 年 3 月に導入し、運用しているサンドボックス(FireEye NX7500 Essential)の設置と Malware 検知の状況にについて述べた。今後、誤検知の状況等をみながら自動遮断可能なものは、遮断するようにしていきたい。

参考文献

[1] 吉田：新基盤情報システムについて，Journal of IPCs，大分大学学術情報拠点(情報基盤センター・医学情報センター)，vol.37，pp.4-7，2017.
https://www.cc.oita-u.ac.jp/journal/vol.37.pdf

[2] 吉田：ファイアウォールの更新について，Journal of IPCs，大分大学学術情報拠点(情報基盤センター・医学情報センター)，vol.36，pp.4-5，2016.
https://www.cc.oita-u.ac.jp/journal/vol.36.pdf

[3] 吉田：情報基盤センターにおける spam 対策の現状，Journal of IPCs，大分大学学術情報拠点(情報基盤センター・医学情報センター)，vol.35，pp.2-4，2015.
https://www.cc.oita-u.ac.jp/journal/vol.35.pdf

[4] 松井 一乃，金高 一，加来 麻由美，池部 実，吉田 和幸：milter の組み合わせによる低配送遅延を目指した spam 対策メールサーバの設計と導入の効果について，情報処理学会論文誌，Vol.55，No.12，情報処理学会，pp.2498-2510，2014.