# パターン定義に要する対応期間の調査に基づく セキュリティ製品の妥当性点検

小野 滋己[1)], 後藤田 中[1)], 米谷 雄介[1)], 青木 有香[1)], 八重樫 理人[1)], 藤本 憲市[1)]
林 敏浩[1)], 今井 慈郎[1)], 最所 圭三[1)]

1) 香川大学

jyohosenm@jim.ao.kagawa-u.ac.jp

# Validity Check of Security Products based on Survey of Response Period Required for Pattern Definition

Shigemi Ono [1)], Naka Gotoda [1)], Yusuke Kometani [1)], Yuka Aoki [1)], Rihito Yaegashi [1)],
Ken'ichi Fujimoto [1)], Toshihiro Hayashi [1)], Yoshiro Imai [1)], Keizo Saisho [1)]

1) Kagawa University

**概要**

情報セキュリティマネジメントにおいて、組織に沿ったセキュリティ対策の状況確認・有効性の確認は必要不可欠である。本学では、予算・運用形態等の制約の中で、導入した製品の妥当性点検の試みを行っている。近年の標的型攻撃に重点を置き、本学のファイアウォールで監視されるメール、また Web からのダウンロードファイルを対象に、サンドボックスにおいて新種・亜種と思われる検知マルウェアのハッシュ値に着目した。本研究では、同一のハッシュ値を持つパターンファイルに定義として反映される期間について、本学で全学導入しているアンチウイルスソフト（他社製品群を含む）を対象に調査し、その妥当性点検に活用した。

## 1 はじめに

標的型攻撃によるセキュリティの脅威が増す中で、大学組織が情報セキュリティを維持・確保するために、人的、物理的、技術的、組織的なセキュリティ施策を体系的に取り組む情報セキュリティマネジメントが欠かせない。限られた予算・リソースの中で、あらゆる脅威にすべて対処することは困難であり、自組織に沿ったセキュリティ対策の状況確認し、導入した製品等の有効性を確認することは必要不可欠である。

こうした状況の中、ファイアウォール、エンドポイント等多層の各セキュリティ施策に対し、相原らは、リスク等に応じてこれらに対するコスト比重を検討する手法を提案している[1]。一方で、こうした考えに基づき予算配分した後の製品検討について、市場調査に基づき行われるベンダー評価や製品評価等を参考にすることは可能であるが、自組織に迫る具体的な脅威に基づいて、導入検討・更新検討を行うことは難しい。例えば、そうした評価に関する対策用の検体データであれば、

・取り扱われる言語や地域圏（例：欧米、日本）
・機関特性（官公庁・大学等の高等教育機関/企業）

等が、合致しているか各社の公開データに基づき検証を行うことは困難である。だが、他社との比較も行いながら、導入した製品が十分な性能を維持できているか、予算・運用形態などの制約の中で導入する、もしくは導入した製品の妥当性について経営層や内部の情報セキュリティ関係者に点検の結果を示すことは、重要な活動といえる。

そこで、本学では、標的型攻撃に添付されやすい新種・亜種のマルウェアに対する対策として、本学のファイアウォールで監視されるメール、また Web からのダウンロードファイルを対象に、導入済みのサンドボックスにおいて新種・亜種と思われる検知マルウェアのハッシュ値に着目した。本研究では、同一のハッシュ値を持つパターンファイルに定義として反映される期間について、本学で全学導入しているアンチウイルスソフト（他社製品群を含む）を対象に調査し、アンチウイルスソフトの妥当性点検に活用したので、その仕組み、および調査方法について紹介する。

## 2 新種・亜種による標的型への対応要件

### 2.1 サンドボックスの導入経緯とその機能制約

本学では、医学部附属病院における端末のウイルス感染によるインシデント発生後、こうした標的型攻撃に対する脅威に強い警戒感を持って訓練等の対応を行っている[2]。その一環として、ファイアウォールの拡張機能として、サンドボックスも導入した。

ファイアウォールに組み込まれた一般的なサンドボックスでは、ゼロデイ攻撃であった場合に、仮想化領域等保護された環境において、新種・亜種のマルウェアとしての判定・検知に一定の時間を要する。構成員を多く抱える組織の実環境としては、この判定が出るまで、通過を滞留させる設定は現実的ではなく、結果として、初回に届いた新種マルウェア添付のメールは、検知されるまでの間、同機能をそのまま通過することになる。このため、未然かつ完全にブロックすることは難しい。

### 2.2 多層防御としてのアンチウイルスソフト

一方で、サンドボックス機能で、ブロックに至る時間までに通過した受信メールや Web からのファイルダウンロード操作に基づくマルウェア感染をいかに防ぐかが鍵となる。本学では、包括契約に基づき、学生を含む全構成員にアンチウイルスソフトを配布しており、このパターン定義更新に要する対応期間が短いほど、同ファイルの開封・実行動作の検知が可能となり、感染リスクを減らすことが可能と考えた。

### 2.3 それぞれの位置づけと役割について

渋谷らは、亜種の収集・分析を行い、その機能の変化の解明結果から標的型対応の難しさと検体に基づく分析の重要性を示唆している[3]。新種・亜種のマルウェアを意識した場合に、我々は、サンドボックスは、自組織への脅威としての対策用の検体データを収集することが可能である点に着目した。仮に、それがゼロデイ攻撃であった場合でも、アンチウイルスソフトのパターン定義ファイルの更新が早ければ、脅威を低減できると考えた。

## 3 製品の妥当性の点検方法

### 3.1 対象検体のデータ収集とハッシュ値の扱い

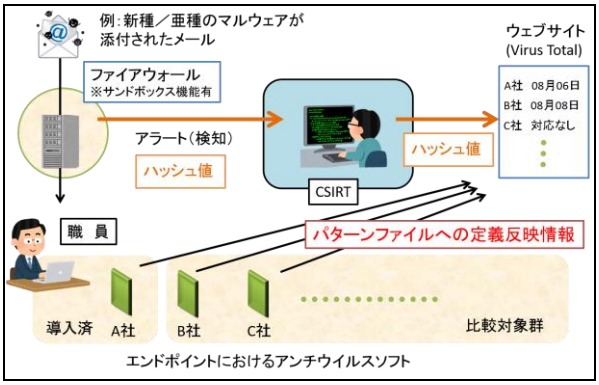


図 1 検体のハッシュ値と定義反映情報の取得

図 1 は、標的型攻撃がメールの添付ファイルを用いて行われた際にファイアウォールのサンドボックス機能が、それを検知し、システム管理者側へ通知し、定義反映情報を取得するまでの流れを示している。サンドボックスにおいて、アラート（検出）が行われた際に、そのハッシュ値を図 2 に示す VirusTotal[4] のフォームに入力する。ViruTotal では、入力されたハッシュ値に基づき、Virus Total が検体を提供している各社のアンチウイルスソフトの対応状況を一覧として確認できる（図 3）。多くのベンダーに提供されているが、本学では、全学導入している製品も含み主要な各社のみピックアップして、対応状況を確認する。なお、サンドボックスからのアラートには、全てハッシュ値が付けられているわけではなく、本研究の点検では、値が付けられたもののみを点検の対象としている。


図 2 Virus Total の日本語トップページ

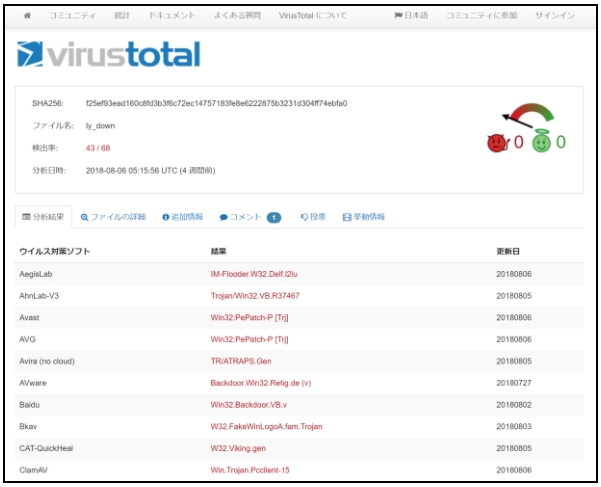


図 3 Virus Total における各ベンダー対応一覧

### 3.2 アンチウイルスソフトの対応点検について

本学では、初回のアラートにおいては、CSIRT の担当者が VirusTotal も含めて情報収集を行うため、その際に、定義反映を確認できるが、その後の対応期間(例えば、数時間単位での定義反映)については、細かく調査するのではなく、他の業務を兼ねる担当者に負担ない範囲内で一定の期間をおいて再度調査を行っている。定義反映に関する具体的な項目は、以下である。

・サンドボックスで検知された時点でのパターン定義の存在（有／無）
・後日確認時における定義の存在（有／無）
・誤検出ではないか？（偽陽性を検出）

サンドボックスのアラート時に、パターンファイルに定義が反映されていない製品については、後日、再度パターン定義がなされたかどうかの確認を行っている。また、後日確認を行い、例えば、1 社のみが、対応を行っていた場合は、偽陽性の可能性もあると判断し、その点も評価の参考とする。

### 3.3 導入・更新にあたっての他の点検項目

本稿では、標的型を意識し妥当性の点検を中心に述べているが、本学ではアンチウイルスソフトは年度ごとに更新の検討を行っており、他の視点も重視しながら、最終的にどの製品にするか点検・更新を行っている。代表的な他の項目の例としては、以下のような内容があげられる。

・予算に対する製品価格
・ライセンス形態（包括契約の有無等）
・インストール方法等のマニュアル更新の負荷

これらから、最終判断は総合的であり、必ずしも、もっとも対応が良い製品が導入・更新されるとは限らない点に留意されたい。

## 4 おわりに

本稿では、本学で導入したファイアウォールのサンドボックス機能を用いて、検知マルウェアのハッシュ値に着目した。各社のアンチウイルスソフトにおいて、同一のハッシュ値を持つパターンファイルに定義として反映される期間の調査に基づき、妥当性点検の一つの要素として、取り扱った。ただし、近年では、同製品群について、パターンマッチングによらない動的ヒューリスティック検出である「振る舞い検知」機能の強化を図る製品も増えており、そうした点の性能評価は今回対象としていない。その動向も見極めながらより良い点検に結び付けていきたいと考えている。また、定義として反映される期間については、人手ではなく、機械的に収集することも検討している。

## 参考文献

[1] 相原遼、石井亮平、佐々木良一、イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用、情報処理学会論文誌、Vol.50、No.3、pp.1082 – 1094、2018.

[2] 米谷雄介、後藤田中、小野滋己、青木有香、宮﨑凌大、八重樫理人、藤本憲市、林敏浩、今井慈郎、最所圭三、香川大学での標的型攻撃メール訓練の導入と改善点の検討、第 22 回 学術情報処理研究集会論文集、2018. (採録済)

[3] 渋谷健太、久山真宏、佐藤信、三村聡志、松本隆、佐々木良一、標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発 －標的型攻撃マルウェアの解析と亜種の予測－、マルチメディア，分散協調とモバイルシンポジウム 2016 論文集、pp.1081-1086、2016.

[4] VirusTotal、https://www.virustotal.com/ja/ (参照日：2018 年 09 月 03 日)