鳥取大学におけるマルウェア対策（電子メール）

Malware prevention included in e-mail at Tottori University

本村真一 †, 宮田直輝 †, 大森 幹之 †

Shin-ichi Motomura†, Naoki Miyata†, Motoyuki OHMORI†

motomura@tottori-u.ac.jp, miyata@tottori-u.ac.jp, ohmori@tottori-u.ac.jp

鳥取大学総合メディア基盤センター †
Center for Information Infrastructure & Multimedia, Tottori University†

概要

メール経由でのマルウェア拡散が増えており、鳥取大学（以下、「本学という」。）においても 2016 年頃から多数のマルウェアが届いている。本学では以前からトレンドマイクロ社製 InterScan Messaging Security Virtual Appliance （以下、「IMSVA」という。）をメール対策のため導入していた。ここでは、本学の状況及び 2016 年以降に実施した IMSVA の対策やその効果について報告する。

キーワード

マルウェア, 電子メール, 入口対策

1　はじめに

セキュリティ対策においてマルウェアへの対策は重要な意味を持つ。本学においても以前から 2 つのマルウェア対策を行っている。一つはメールに対するものであり、メールを中継するサーバとして IMSVA を導入している。IMSVA はメールに添付されたマルウェアへの対策だけでなく、フィッシングメールなどメールを介する様々な攻撃に対処するものである。二つ目はエンドポイントに導入するトレンドマイクロ社製ウイルスバスター コーポレートエディション（以下、「Corp.」という。）である。本学では Trend Micro Campus Agreement for Endpoint（以下、「TMCA」という。）を契約し、教職員のみならず学生のコンピュータに対しても Corp. の導入を可能としている。IMSVA はその前身である InterScan シリーズを含めると 2003 年以前から導入していた。TMCA は 2014 年からの導入であるが、教職員向けには 2005 年から Corp. を導入していた。しかしながら、IMSVA や Corp. により検出されたマルウェアに関する確認作業などはこれまであまり行っていなかった。それというのも、マルウェアに感染したエンドポイントの特定を IPS で行なっていたためである。本学ではその他のセキュリティ対策として、マカフィー社製 Intru Shield という IPS を導入し、ラック社の JSOC に運用を委託していた。IPS では学外からの不正アクセスだけでなく、学内から学外への不正アクセスがあった場合も JSOC から通知を受けており、JOC による分析によってマルウェアに感染していると考えられるエンドポイントを特定し対応を行なってきた。

表- 1: JSOC からの通知件数

年度	全通知件数	学生（感染元）	学生以外（感染元）
2013	56	47	9
2014	45	40	5
2015	22	13	9
2016	35	16	19

状況が変わったのは 2016 年度になってからである。表 1 に攻撃が成功していると JSOC にて判断された近年の通知件数を示す。そのほとんどがマルウェアに感染しているものである。2016 年度に学生以外の感染が急増し、文部科学省から報告を求められるようになった。マルウェア感染による影響、情報漏洩の有無、感染原因の調査、再発防止策の実施など対応負荷が急増した。特に 2016 年 5 月から 7 月にかけて、ばらまき型メールに

よる感染が4件続けて発生したことが大きい。下記はその一例のメール本文であるが、添付されている zip 内のファイルをユーザが実行することでマルウェアをダウンロードし感染した。

■お届け予定日時
6 月 30 日 時間帯希望なし※お届け予定日時につきましては、ゴルフ・スキー・空港宅急便（施設宛）の場合、プレー日（搭乗日）を表示しております。
■品名：**********
■商品名：宅急便
■ご依頼主：
■伝票番号：xxxx-xxxx-xxxx ヤマト運輸株式会社

マルウェア感染時の対応負荷を軽減するため、予防やより早期の発見に取り組むことが重要となった。最近のマルウェアの感染経路の多くがメールであったことから、まずは IMSVA による対策を見直した。ここでは、本学で実施した対策及びその効果について紹介する。

2 IMSVA の活用

IMSVA はマルウェア対策だけでなく、RBL 及びメール本文の URL 判定を含んだ迷惑メール対策を実現する製品であるが、2016 年度までは RBL とマルウェア対策のみを利用していた。現在とは異なり、2011 年頃までは迷惑メールの数が現在の 4 から 5 倍程度も多く、メール対策において RBL の占める割合が大きかったためである。また、マルウェア対策もパターンファイルを用いた検索という基本的な設定で運用していた。これはより積極的にマルウェアを検出する動作を行なった場合、false positive が増加することが予想され、これを避けていたためである。しかしながら、false positive の増加を許容してでも感染のリスクを減らすため、より積極的な対策を行うこととした。

2.1 スマートスキャン

トレンドマイクロ製品におけるマルウェアの検索方法には従来型スキャンとスマートスキャンの 2 種類の方法がある。従来型スキャンはパターンファイルをクライアントに配置し検索する方法である。スマートスキャンはパターンファイルの大半をスキャンサーバに配置し、クライアントとスキャンサーバの両方で検索する方法である。両方式の大きな違いとして、パターンファイルの更新頻度が挙げられる。従来型スキャンは概ね 1 日に 1 回の更新に対して、スマートスキャンは概ね 1 時間に 1 回である。マルウェアへの対応の迅速さが 24 倍になっていると言える。

IMSVA は以前からスマートスキャンに対応しており本学でも利用していたが、バージョン 9.0 まではスキャンサーバの接続に失敗すると従来型スキャンに切り替わってしまい、その後手動でスマートスキャンに変更する必要があった。2017 年 4 月 20 日にリリースされたバージョン 9.1 からスマートスキャンだけで運用できるオプションが提供されたことで、マルウェアへの対応の迅速さが損なわれないようになった。

表- 2: スマートスキャンの効果例 1

マルウェア名	HTML_PHISH.AUSEDN
受信日時	2017 年 7 月 14 日 02 時 55 分
従来型	2017 年 7 月 14 日 06 時 10 分
スマートスキャン	2017 年 7 月 13 日 17 時 37 分

表- 3: スマートスキャンの効果例 2

マルウェア名	JS_VALYRIA.DLA
受信日時	2017 年 7 月 24 日 20 時 31 分
従来型	2017 年 7 月 25 日 05 時 45 分
スマートスキャン	2017 年 7 月 24 日 17 時 37 分

表 2、3 に、本学に届いたマルウェアがスマートスキャンにより検出された例を示す。これらについては、従来型スキャンのパターンファイルでは検出が間に合わなかったものが、スマートスキャンパターンファイルでは駆除できた。なお表の時間は全て日本時間である。また、パターンファイルのリリース日時は最新のパターンファイルのみ公開されているため、当方でパターンファイルのリリース情報を取集し保存している。

2.2 実行形式ファイルと Office ドキュメントのマクロの削除

2016 年に発生したばらまき型メールによる感染は、メールに添付されていたファイルを実行したことによるものであった。この再発防止策として、2016 年 8 月 29 日から IMSVA により実行形式ファイルを削除してから配送している。IMSVA では、COM、EXE、DLL、Java バイトコード、自己解凍型圧縮ファイルについては拡張子に関係なく検出できるが、Javascript などのスクリプトファイルやショートカットなどは対応していないため、これらについては拡張子により検出している。削除対象に設定している拡張子の詳細は、本学総合メディア基盤センターの Web ページ（http://www.center.tottori-u.ac.jp/services/euq/quarantine/）に記載している。なお、これらは圧縮ファイルに含まれていても検出される。

本対策実施後しばらくの間は、添付メールを介したマルウェア感染を JSOC で検知されることはなかったが、メールに添付されていた Excel ファイルのマクロを有効にすることでマルウェアをダウンロードし感染するインシデントが発生した。本インシデントが発生した 2017

表- 4: 実行形式ファイル及びマクロ削除の効果

	全削除数	false positive	false positive 率	実削除数	全体に占める割合
パターンファイル	94	0	0%	94	10%
実行形式ファイル	627	22	4%	605	65%
マクロ	379	114	38%	235	25%
合計	1,100	136		934	100%

年 6 月 7 日の翌日から Office ドキュメントに含まれるマクロについても IMSVA で削除している。

これらの対策の効果を確認するため、2017 年 7 月 6 日から 8 月 3 日までの間にパターンファイルで検出したマルウェア、実行形式として検出したマルウェア、マクロとして検出したマルウェアを表 4 に示す。なお表中の false positive は、IMSVA のログ（送信元メールアドレス、送信先メールアドレス、件名等）を目視で確認し、正当な目的で送信されたと判断されるものを示している。表から実行形式ファイルの削除が最もマルウェアの駆除に有効なことが分かる。また、実行形式ファイルをメール添付しないことが周知されている、もしくはマナーとして定着しているためか false positive も少ない。一方、Office ドキュメントのマクロ駆除についてはマルウェアの駆除に有効である反面、false positive も多い。表 4 から、実行形式ファイル及び Office ドキュメントのマクロを削除することでマルウェアの 90%程度を駆除しており、IMSVA のパターンファイルでは 10%程度しか対応できていないと見ることもできる。ただし、フィッシング目的の URL が記載されたドキュメントなどはパターンファイルで駆除しており、パターンファイルによるスキャンが無駄なわけではない。

2.3 不審メールの隔離

IMSVA にはエンドユーザメール隔離と呼ぶ機能がある。この機能を用いることで、IMSVA により隔離されたメールを後ほどユーザが Web ページで確認して受信することができる。IMSVA では、スパムメール対策や本文に含まれる URL などから隔離すべきメールを判断している。フィッシングなどへの対策を目的としてとして、本機能についても 2016 年 10 月 3 日から有効にしている。

本機能の効果を確認するため、2017 年 7 月分のメールについて表 5 に集計を示す。IMSVA により不審メールと判断され隔離されたメールは、受信したメール全体の約 4%であった。そのうちユーザにより隔離が解除されたメールは約 1%であった。この数字を見ると適切に隔離しているようにも思えるが、ログや受信するメールなどから false positive 及び false negative があることが分かっている。筆者自身も必要でないと思われるメールの隔離解除は行わないため、実際には 1%より多くの false positive が発生していると考えられる。

表- 5: 実行形式ファイル及びマクロ削除の効果

全メール	1,927,644
RBL によるブロック	883,959
受信したメール	968,385
隔離したメール	40,214
隔離が解除された	381

3 未対応の脅威

IMSVA を積極的に活用することで、2016 年度以前と比較しメールを介した不正アクセスの脅威を減少させることができた。しかしながら、対応できていない脅威があることも分かっている。

3.1 Office ドキュメントの OLE オブジェクト

本学で確認しているのは 2017 年 6 月 13 日が初めてであるが、Javascript のコードを OLE オブジェクトとした Office ドキュメントが添付されたメールを受信している。この Office ドキュメントは、ユーザが開いたあとにドキュメント中のアイコン等をダブルクリックさせることで Javasript を実行させマルウェアをダウンロードする。IMSVA ではパターンファイルが対応していなければ駆除することができず、検体を Cuckoo Sandbox で検証してみたがマルウェアと判定することはできなかった。このようなユーザの操作を伴うものは、おそらく他のサンドボックス製品でも検出が難しいと思われる。他のマルウェアに比べてユーザの操作が多いためか、幸い今のところ本学では感染は確認されていない。

3.2 フィッシング

IMSVA はメール本文に含まれる URL をフィッシング対策の評価に利用している。トレンドマイクロ社では、Web レピュテーションと呼ぶ URL の評価を行った

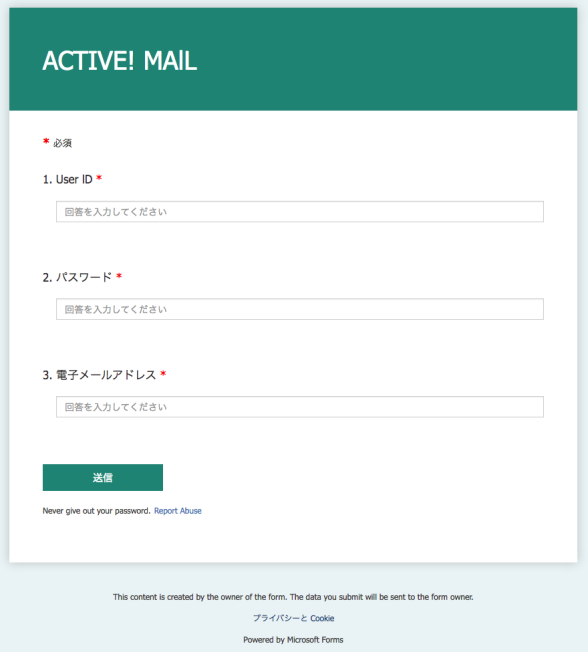

図- 1: フィッシング攻撃の例

データベースを保持しており、その内容は Site Safety Center（https://global.sitesafety.trendmicro.com/）から確認できる。しかしながら、Web レピュテーションでは未評価の URL を攻撃に利用されフィッシング被害にあっている。本学では多くの場合、フィッシングメールは複数のメールアドレスへ配信ており、本学総合メディア基盤センターから当該事案を学内へ通知するとインシデント発生の連絡を受けている。下記は最近の例であるが、このフィッシングメールには被害にあいやすい要素が 2 つ含まれていた。一つ目は、本学では Active!mail を利用していることから標的型的要素を含んでいたことである。二つ目は、図 1 にスクリーンショットを示しているが、サイトがマイクロソフト社の Web Form サービスであり、不正なサイトとしての判断が難しいものであった。これらのことから、約 200 通の配信に対して 5 件の被害が確認されている。

あなたのアクティブメール！ メールボックスがメールチームによって設定されたクォータ/リミットを超えました。
Web メールを再度有効にするまで、新しい電子メールを送受信できない場合があります。

検証するには、をクリックします。
https://forms.office.com/Pages/ResponsePage.aspx

3.3 クラウドサービス

本学での被害は確認していないが、Dropbox 等の広く利用されているクラウドサービスからマルウェアをダウンロードさせようとするメールを受信している。メール本文の URL に記載されていることもあれば、PDF などのファイルに記載されていることもある。このような攻撃に対しては、IMSVA を用いた対応策は現実的ではないと考えられる。

4 まとめ

近年増加しているばらまき型メールに対して IMSVA を活用した対策を行い、その効果が確認できている。しかしながら、メールを用いた攻撃への対策だけを取り上げてみても完全ではない。このようなメール対策を入口対策と呼ぶが、そもそも入口は他にも多くある。例えば、本学のメールサービスではなくプロバイダ等のメールサービスの利用、Web ブラウザによるダウンロード、PC や USB フラッシュメモリ等のデバイスの持込などがあげられる。メール対策の完全さを追求するよりは、Web Proxy サーバ導入等の出口対策を含めた別の方法との組み合わせを検討するほうが適切であると考えられる。

予防や早期発見の観点からは、ログの活用が今後は重要だと考えている。例えば、IMSVA により配信されたメールログと、当該メール利用者のエンドポイントのログを組み合わせて集計･分析することで、IMSVA をすり抜けた攻撃を補足し、他ユーザへの攻撃を未然に防ぐことができるかもしれない。このようなことを実現するために、トレンドマイクロ社製品では Connected Threat Defense（以下、「CTD」という。）と呼ぶシステム連携構成を実現している。これは、Trend Micro Control Manager（以下、「TMCM」という。）という統合管理ツールを用いることで複数の製品を連携させる。しかしながら、本学で試用した段階では目指す動作を実現できてない。一つには、TMCM に人やアカウントを識別する情報がないため、誰のメール、誰のエンドポイントという識別ができないことがある。他にも、これはセキュリティ製品全般に言えることであるが、検出される情報が過剰であるため適切に判断するためには何らかの処理が必要であった。そのため、CTD ではなく IMSVA や Corp. のログを独自に活用することを検討している。IMSVA ではバージョン 9.1 から syslog がサポートされたため、fluentd によりログの収集と整形を行い MongoDB で保存している。Corp. は外部へのログ出力をサポートしていないが、TMCM と連携させることで syslog 出力が可能となるため、こちらも同様のことを行っている。その他、認証サーバやネットワークスイッチについても MongoDB で保存しており、今後ファイアウォールなどのログと併せて集計・分析を行うことを検討している。