標的型攻撃メールの対策（1）

－ メールシステムログの見える化 －

矢野孝三(*1), 大塚秀治(*1), 千葉庄寿(*1), 熊谷将也(*2)

*1 麗澤大学 情報教育センター
*2 富士通株式会社

yano@reitaku-u.ac.jp, ohtsuka@reitaku-u.ac.jp, schiba@reitaku-u.ac.jp
kumagai.masaya@jp.fujitsu.com

概要： 本学では、教職員用メールシステムを狙ったフィッシングメールによる攻撃を継続的に受けている。従来、システム管理者がこのような攻撃を把握するためには、受信したユーザからの通報を受けケースごとにアクセス制御を行う方法しかなく、能動的に対応することが困難であった。本研究ではメールログをリアルタイムに解析して、過去に受信した攻撃メールの特徴と一致するものを検出するシステムを開発する。これまで受信した攻撃メールの特徴について検証を行い、本システムが必要とする機能を検討して開発を行った。

キーワード： セキュリティ，標的型攻撃メール

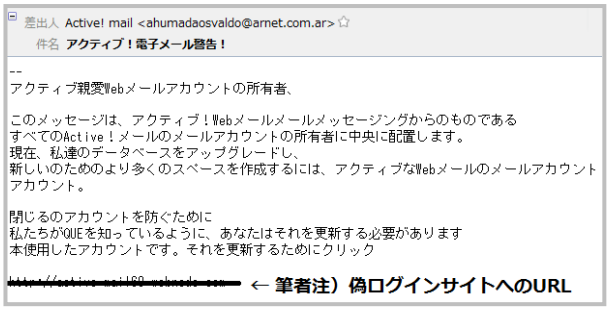
1. 背景

本学では 2013 年頃から、教職員を狙ったフィッシングメールによる攻撃を受けており、現在も攻撃が継続している状況である。フィッシングメールの内容は、本学の教職員用のメールシステムである TransWARE 社の Active!mail に攻撃者がなりすまし、メールの容量が制限を超えている旨の警告をユーザに送信するものである。メールには外部 URL のリンクが記載されており、アクセスすると偽のログイン画面が表示される。TransWARE 社によると、そこにログインしたユーザの ID とパスワードは攻撃者に取得され、システムに侵入するために利用されるとの説明がなされており[1]、実際に教員ユーザのアカウントが乗っ取られる被害も発生している。この攻撃への対応として、本学ではウェブや文書による注意喚起を行っており、ユーザから図 1 に示すような攻撃メールの受信報告があれば、本文中の URL をプロキシサーバに登録してアクセス禁止にすることで、アカウントの乗っ取りを未然に防ぐ対処も行なっている。

しかし、これらの攻撃メールは不特定多数のユーザにランダムに送信される上、受信したユーザが必ずしも報告するとは限らず、システム管理者が全てを把握することは困難である。また、前述した攻撃以外にも、様々な標的型攻撃メールによる情報漏洩事件が社会問題化しており、組織としての対応が喫緊の課題となっている。

2. 研究の目的

本研究では、メールシステムのログをリアルタイムに解析し、指定したパターンに一致するメールを管理者に通知するシステムを開発する。本学がこれまで受信した攻撃メールの特徴から、本システムに必要な機能を検証し、標的型攻撃メールに対応する手段の一方策として発展させることを目的とする。


差出人 Active! mail <ahumadaosvaldo@arnet.com.ar>
件名 アクティブ！電子メール警告！

--
アクティブ親愛Webメールアカウントの所有者、

このメッセージは、アクティブ！Webメールメールメッセージングからのものである
すべてのActive！メールのメールアカウントの所有者に中央に配置します。
現在、私達のデータベースをアップグレードし、
新しいのためのより多くのスペースを作成するには、アクティブなWebメールのメールアカウント
アカウント。

閉じるのアカウントを防ぐために
私たちがQUEを知っているように、あなたはそれを更新する必要があります
本使用したアカウントです。それを更新するためにクリック

[redacted] ← 筆者注）偽ログインサイトへのURL

図 1 受信した攻撃メールの例

このメールは本学や TransWARE 社、および Active!mail とはまったく関係のないフィッシングメールである。管理者になりすまして、ユーザに容量増加を促し、偽のログイン画面へ誘導しようとしている。よく読めばフィッシングメールであることは容易に判断できるが、誘導されてしまうユーザはゼロではない。

3. システム設計の方針

本学でこれまでに受信したフィッシングメールの多くは以下の特徴を持っている。

- ・差出人のアドレスは学外ドメインである
- ・差出人の名前にメールシステムの名称を含む
- ・件名に「警告」「メンテナンス」等の語句を含む
- ・複数の学内メールアドレスに同時に送信される

これらの特徴は最初に受信が確認された 2013 年頃から、現在まで一貫している。しかし、攻撃の度にアドレス、件名、本文、URL が変わるため、メールシステムのスパムフィルタリング機能に個別登録して排除することは困難である上、通常の業務メールが誤検知されてしまう可能性も生じる。そこで、本研究では攻撃メールをシステムで排除することよりも、管理者がいち早く攻撃に気付いて、能動的に事態に対処することに重点を置く。開発するシステムでは、メールの差出人や件名に含まれる語句をチェックし、指定した特徴を持つメールが一定数配信された場合に、管理者への警告を行う機能を実装する。

4. システムの構築

4.1 システム概要

本システムは、管理サーバ、情報表示端末、監視対象(メールゲートウェイ)で構成される。管理サーバでは監視対象から syslog を取得し、解析した結果を DB に蓄積する。情報表示端末はブラウザでサーバに定期的にアクセスし、結果をウェブ画面で表示する。それぞれの機器の関連を表した概要を図 2 に示す。

4.2 メールシステムログの取得とデータの蓄積

本学ではメールシステムに Barracuda 社の Spam & Virus Firewall 600 を使用しており、学外と学内を繋ぐメールゲートウェイとして DMZ に設置している。メールゲートウェイが出力する syslog にはメールの送信者や件名が含まれており、管理サーバはこれらの情報をリアルタイムに取得する。管理サーバは送受信されるメールの情報を 1 件ずつ syslog から取得して、[日時], [送信者], [受信者], [件名]のデータを抽出する。これらのデータは、後述するキーワードと共に集計のため DB に蓄積される。DB には MySQL を使用し、処理プログラムは PHP によって実装している。

4.3 件名からキーワードの抽出

一般的にメールの件名は、複数の単語や文節から構成される短文であることが多い。本システムでは件名に含まれる語句を抽出するために、形態素解析[1]のソフトウェア「MeCab」を使用する。形態素解析によって名詞と判定された語句を、このメールのキーワードとして紐付ける(図 3 参照)。

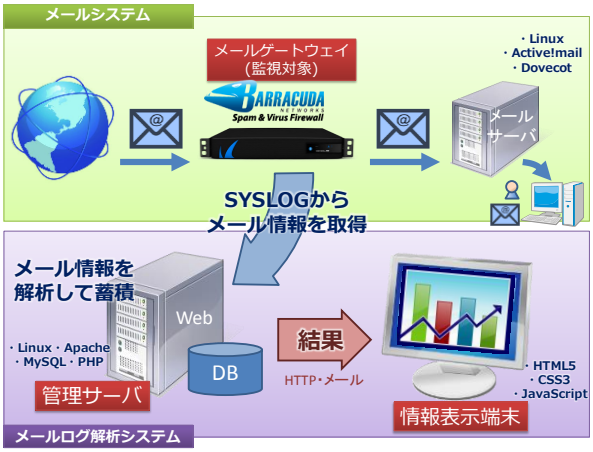


図 2 システム概要図

メールシステムは Barracuda 社の Spam & Virus Firewall 600 を使用しログは管理サーバに syslog で記録する。ログは管理サーバ上で MySQL を用いて DB 化される。処理プログラムは PHP で実装される。管理者への通知は HTML と JavaScript によって管理者用情報表示端末上に生成されるウェブ画面として提供する。

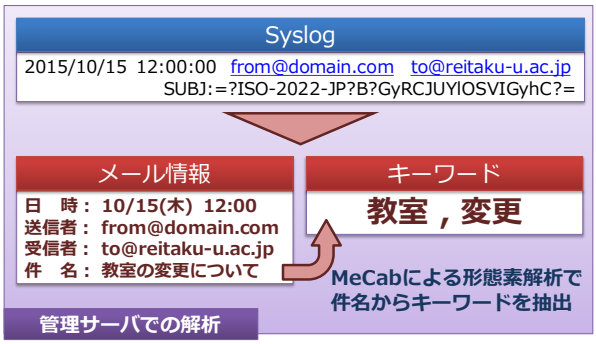


図 3 メールログの解析方法

メールログは MeCab による形態素解析によってキーワードに分解し、名詞と判定したものを当該メールと紐付ける。

図 4 情報表示画面（ウェブブラウザ上での表示例）

左側に受信メール情報が表示される。syslog から新たな受信メールを確認すると、スクロールして順次表示される。プライバシー保護のためアドレスのユーザ名は表示しない。右側はキーワードのランキングが表示される。管理者が指定したキーワードは色分けされ、攻撃パターンのキーワードが蓄積されていないか確認ができる。

---

1 形態素解析とはコンピュータを用いた自然言語処理のひとつであり、文を形態素（意味を持つ最小の単位）に分解し、品詞などの文法情報を付与することである。MeCab はオープンソースの形態素解析エンジンである。

4.4　情報表示画面

情報表示画面は PC やタブレットなど機器を問わずにアクセスできるよう、HTML と JavaScript によって生成されるウェブ画面として提供する。本画面ではリアルタイムの受信メール情報と、これまで受信したメールのキーワードを集計したランキングを表示する。画面の表示例を図 4 に示す。

4.5　攻撃メールの判定

管理者は攻撃メールの特徴として、アドレスに含まれるドメインや、件名に含まれるキーワードをシステムに登録する。さらに、しきい値を指定することで攻撃メールが一定数以上になると警告するように設定する。これは、一般的に攻撃メールは一件だけ送信されることはまれで、多数のユーザに同時送信されるという特徴があるためである。単発の正常なメールが偶然キーワードを含んでいた場合に、誤警報が頻発することを抑止する効果を持つ。

他に不特定多数に送信されるメールとして、外部のメールマガジン等があるが、身元が確かなものについては送信元アドレスをホワイトリストに設定できるようにした。安全性が明確なものは検出対象から除外することで、攻撃メールの検出率を向上させることが目的である。攻撃メールの検出フローを図 5 に示す。

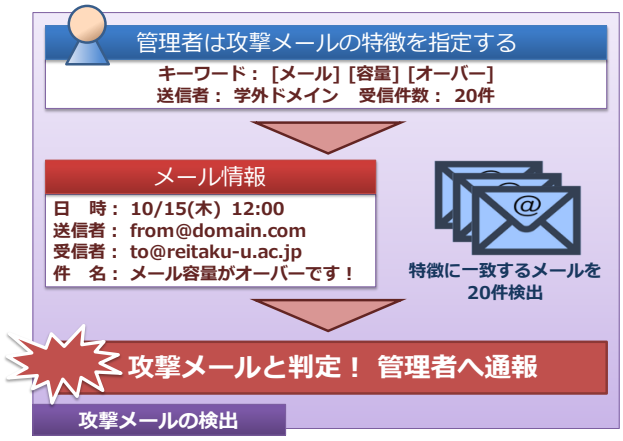


図 5　攻撃メールの検出フロー

管理者は攻撃メールの特徴から検知ルールを指定することができる。検知ルールは攻撃パターン毎に複数指定することも可能で、それぞれのルールについてしきい値を設定することができる。この機能でヒット率を向上させ、誤警報を抑止する。

4.6　管理者への通報

管理サーバは攻撃メールを一定数検出すると、管理者への通報を行う。通報にはあらかじめ登録したメールアドレスに対して警告メールを送信する。また、情報表示画面では検出したメール情報をポップアップ表示することで視覚的に周知を行う（図 6 参照）。

5.　システムの課題

現行のメールゲートウェイが出力する syslog からは、送信者名を取得することができない。前述したように本学に送信される攻撃メールについては、送信者名が固定パターンであることが多いため、送信者名を取得することができれば、検出率の向上に繋がるものと思われるが、現状では実現できていない。

また、近年の標的型攻撃メールでは、文書ファイルに偽装した実行可能ファイル（.exe 等）を実行させて、PC をウイルスに感染させるものが確認されている[2]。syslog からはメールに添付ファイルが含まれるかどうか取得できないため、検出パターンのひとつとして活用することができないという課題もある。

図 6　攻撃メール検知時の警報画面

攻撃パターンに合致するメールを規定数以上検知すると警報画面がポップアップ表示される。

6.　今後の展開

本稿を執筆している 2015 年 10 月現在では、システムの試験運用中であり、まだ本番環境への適用には至っていない。試験運用ではこれまで本学で確認された既知の攻撃メールの特徴を登録して、実際の攻撃メールを検知できるかどうかを検証するとともに、実際に攻撃行われた場合に、システム管理部門としてどのような対応を行うのか検討を行っている。

これまでは、ユーザからの通報によって攻撃メールを受信したことを把握し、注意喚起のウェブサイトや文書等を作成したり、フィッシングサイトの URL をアクセス禁止にしたりするなどの対応を行なっていた。しかし即応性に欠ける上、ユーザからの報告が無い場合は対応すること自体も不可能であっただけに、本システムによってより能動的なセキュリティ対策が実現することに期待したい。

参考文献

[1] TransWARE 社, Active!mail のユーザー様を狙ったフィッシングメールについて,
http://www.transware.co.jp/phishing/summary.html.

[2] 独立行政法人情報処理推進機構, IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」,
https://www.ipa.go.jp/files/000043331.pdf.