O-002

ばらまき型攻撃メールにおける本文特徴による攻撃メール検知方法の一検討
A Study on Detection Method of Attack Mail by Mail Body Characteristic in Indiscriminate Mail Attacks

弥田 紘一† 齊木 あずさ† 佐々木 昌樹†
Koichi Yata Azusa Saiki Masaki Sasaki

1. はじめに

近年，特定者に向けてマルウェア感染を誘発する攻撃メールよりも不特定多数に偽装メールを送り付ける「ばらまき型攻撃メール」が増加している．ばらまき型攻撃メールとは，マルウェア感染などを目的に，広く多くの組織に送付されるメールである．例えば特定企業の社員全員に同一内容のメールを送る，特定の銀行に口座を持つ一般ユーザに同じ内容のメールを送る等である．このメールにはオフィスアプリケーションなどにマクロ実行機能を備えたファイルが添付され，ファイルを開くとマルウェアがダウンロードされ，マルウェア感染する可能性がある．

ばらまき型攻撃メールは巧妙化しているため，受信者によるチェックでは攻撃メールの判断がしにくく防ぎきれないという課題がある．

2. 先行技術

先行技術として，迷惑メールの判定のため，過去にやり取りされた複数のメールについての各メールのメールデータからメール情報（送信元 IP アドレス，メールアドレスドメイン，SPF レコード）を抽出し，メール判定リスト（ブラックリスト又はホワイトリスト）を作成し，迷惑メール判定を行う方法がある． [1]

3. 課題

しかし，この技術ではメールデータが偽装されていない場合，メール判定リストで検知する事ができるが，攻撃メールの場合は，正規サーバを利用して送信されたように偽装することが多いため，メールデータが偽装された場合，検知できない．

4. 提案方法

そこで本研究では，メールヘッダではなくメール本文を使用したばらまき型攻撃メールの検知方法について検討する．

4.1 システム構成

提案システムの構成図を図 1 に示す．

・攻撃メール判定サーバ
　メール端末より不審メールと判断され、不審メール通報された不審メールのメール本文について，半角英数記号の文字を削除したデータのハッシュ値を算出しブラックリスト（不審メール通報リスト）に登録する．メール端末が新たにメールを開封したときに開封したメールが攻撃メールかの判定要求を受けた時に攻撃メール判定要求結果を返す．また，通報された不審メールが攻撃メールと管理者が判断した場合は不審メール通報リスト内で今回該当する不審メールに攻撃メールフラグを付加する．
・メール端末
　ユーザが不審メールと判断した場合に通報する不審メール通報，受信したメールが攻撃メールかの判定を攻撃メール判定サーバに行ったもらうため攻撃メール判定要求を行う．
・ゲートウェイ
　異なるネットワーク間を接続する．
・メールサーバ
　メール送受信の管理を行う．
・メール端末（攻撃者）
　メール端末 1～n に攻撃メールを送信する．

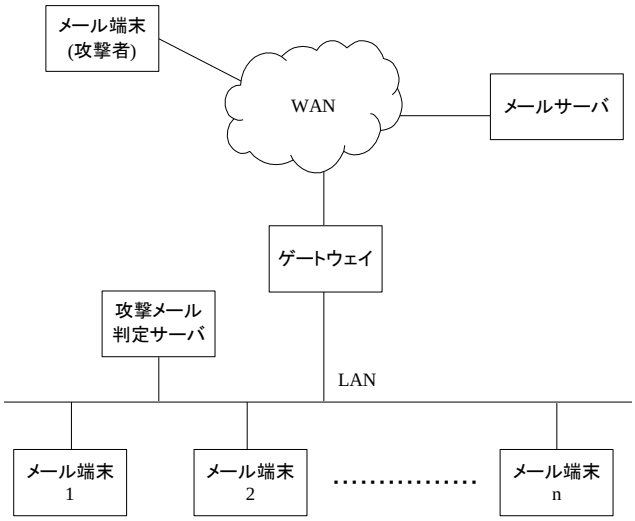

図 1　全体構成図

4.2 動作手順

動作手順を図 2 に示す．ここでは，不審メール通報リストにリスト登録がないところから開始する．

1. メール端末（攻撃者）は各メール端末 1～n に攻撃メールを送信する．(a)
2. メール端末 1 がメール開封動作を行うと同時にメール本文から半角英数記号の文字を削除したデータのハッシュ値を算出し，攻撃メール判定要求を行う．(b)

†株式会社ナカヨ 事業戦略本部 情報技術研究所
Information Technology Laboratory, Corporate Strategy Division, NAKAYO, INC.

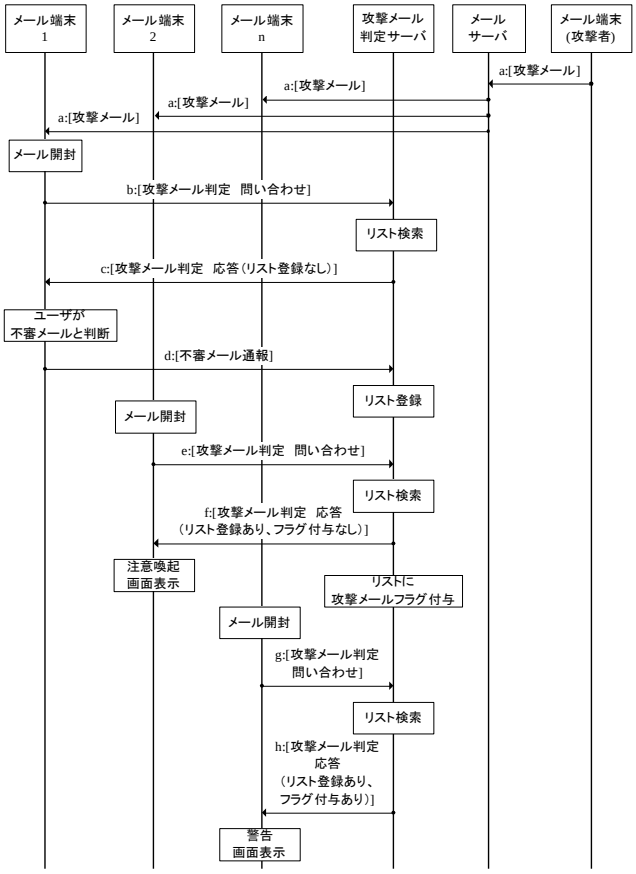

図 2　動作手順

3. 攻撃メール判定サーバは不審メール通報リストから同一のハッシュ値があるかどうかチェックし，攻撃メール判定結果（リスト登録なし）をメール端末 1 に送信する．(c)
4. メール端末 1 は判定結果「リスト登録なし」を受け取り，メールの開封処理を行う．メールを開封したメール端末 1 のユーザが不審メールだと判断し，不審メールを攻撃メール判定サーバに通報する．(d)
5. 攻撃メール判定サーバはメール端末 1 より通報された不審メールの通報日時，通報者，通報端末名，件名，メールサイズとともに，メール本文を抽出して，半角英数記号の文字を削除したデータのハッシュ値を算出したものを不審メール通報リストに登録する．
6. メール端末 2 がメール開封動作を行うと同時にメール本文から半角英数記号の文字を削除したデータのハッシュ値を算出し，攻撃メール判定要求を行う．(e)
7. 攻撃メール判定サーバは不審メール通報リストから同一のハッシュ値があるかどうかチェックし，攻撃メール判定結果（リスト登録あり，攻撃メールフラグなし）をメール端末 2 に送信する．(f)
8. メール端末 2 は判定結果「リスト登録あり，攻撃メールフラグ付与なし」を受け取る，この時点では攻撃メールフラグの付与がなく，攻撃メールの判断が付かないため，注意喚起画面を表示する．
9. ここで管理者が不審メール通報で受けたメールを攻撃メールと判断し，不審メール通報リストに攻撃メールフラグを付与する．
10. メール端末 n がメール開封動作を行うと同時にメール本文から半角英数記号の文字を削除したデータのハッシュ値を算出し，攻撃メール判定要求を行う．(g)
11. 攻撃メール判定サーバは不審メール通報リストから同一のハッシュ値があるかどうかチェックし，攻撃メール判定結果（リスト登録あり，攻撃メールフラグあり）をメール端末 n に送信する．(h)
12. メール端末 n は判定結果「リスト登録あり，攻撃メールフラグ付与あり」を受け取る．攻撃メールフラグの付与があるため，警告画面を表示する．

5. まとめ

本研究では，メール本文を使用したばらまき型攻撃メールの検知方法について検討した．

攻撃メール判定サーバは，通報された不審メールのメール本文について，半角英数記号の文字を削除したデータのハッシュ値を計算したものをブラックリストとする．そして，攻撃メール判定要求に対する結果を返すことで攻撃メールを防ぐことができる．この方法を用いるとメール本文からハッシュ値を抽出するためメールデータを偽装されていても，検知できる．

この他の案として攻撃メール判定サーバは通報された不審メール（HTML 形式）のメール本文について，タグの部分を抽出し，アドレスを削除したデータのハッシュ値を計算したものをブラックリストとする．そして，攻撃メール判定要求に対する結果を返すことで攻撃メールを防ぐことができる．

これにより攻撃メールの特徴として HTML の骨格の部分だけを残すので，同じメール形式の攻撃メール（リンククリック者を特定するために個別の URL を用いた亜種やフィッシング詐欺目的の URL を用いた亜種）も検知できる．

また，

・検知精度を上げる方法としてハッシュ値の計算に添付ファイル名や件名を追加する．
・サーバの負荷を軽減する方法として，攻撃メール判定サーバは各メール端末に不審メール通報リストを配信し，メール端末はリストで攻撃メールか否かをチェックし，リストになかったら攻撃メール判定サーバに攻撃メール判定問い合わせをする．
・管理者として攻撃メールをいち早く判断する方法としてメール開封時だけでなく，メール受信時も検知する．
・メール端末での処理を無くし，サーバで完結させる方法として攻撃メール判定サーバをメールサーバに組み込む．

という内容も考えている．

参考文献

[1] 澤谷　雪子, 窪田　歩,“メール情報抽出装置，メール判定リスト作成装置，メール情報抽出方法，メール判定リスト作成方法およびコンピュータプログラム.” 特開 2016-71728.