O-011

# 受信済みメールに対するばらまき型攻撃メール検知方法の一検討
# A Study on Indiscriminate Attack Mail Detection Method for Received Mail

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

## 1. はじめに

近年，特定者に向けてウイルス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が増加している．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防ぎきれない課題がある．

## 2. 先行技術

先行技術として，前回攻撃メール判定サーバについて発表した．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、攻撃メールと人為的に判定され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して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ヘッダを偽装されていても，検知できる． [1]

## 3. 課題

しかし，この技術ではブラックリストの作成前に，このブラックリストに掲載されているばらまき型攻撃メールをすでに受信しているメール端末について，その対策を考慮していない．

## 4. 提案方法

そこで本研究では，ばらまき型攻撃メールをすでに受信しているメール端末について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．

・不審メール検出サーバ
　複数のメール端末が受信したメールのなかから不審メールを検出し，メール端末毎に，所定のパターン情報と受信メールのメール ID に紐付けて蓄積し，ばらまき型攻撃メールあるいはその可能性があると判断されたメールについて，メール端末毎に，メール端末に対応付けられて蓄積された所定のパターン情報のなかから検索し，パターン情報に紐付けられているメール ID を，メール端末に通知する．

・メール端末
　メール端末毎に，受信メールのメール本文中の文面により定まる所定のパターン情報を，この受信メールのヘッダ情報に含まれているメッセージ ID 等の固有のメール ID に紐付けて不審メール検出サーバに送信し，不審メール検出サーバよりばらまき型攻撃メールあるいはその可能性があると判断されたメールについて，不審メール検出サーバより通知されたメール ID により特定されるメールに対して注意喚起を表示する．

・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．

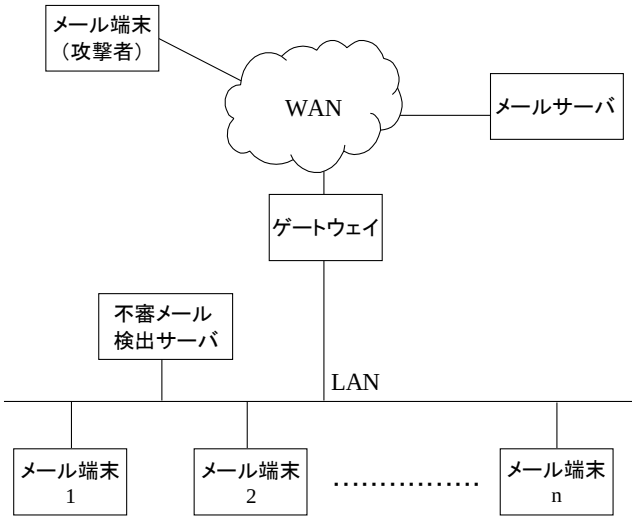


図 1　全体構成図

### 4.2 動作手順

動作手順を図 2 に示す．ここでは，不審メールリスト（ばらまき型攻撃メールの可能性があると人為的に判断されたリスト）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 1～3 にばらまき型攻撃メールを送信する (a) .
2. メール端末 1～3 が受信したメールのメール本文からパターン情報の抽出と電子メールのヘッダ情報に含まれているメッセージ ID をメール ID に設定し，不審メール検出サーバに送信する (b,c,d) .
3. つぎに，不審メール検出サーバは，メール端末 1～3 のそれぞれから受信したパターン登録依頼に含まれている所定のパターン情報を，電子メールの開封状態（ここでは「未開封」）とともに，このパターン登録依頼に含まれているメール ID に紐付けて，該当するメール端末 1～3 のパターン情報リストに登録する．また，ばらまき型攻撃メールの可能性があると人為的に判断された電子メールがないか不審メールリストから，メール端末 1～3 のそれぞれから受信したパターン登録依頼に含まれている所定のパターン情報を検索する．不審メールリストに登録さ

†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.

れていない場合は，パターン登録依頼の送信元のメール端末 1～3 に対する応答処理は実施しない．

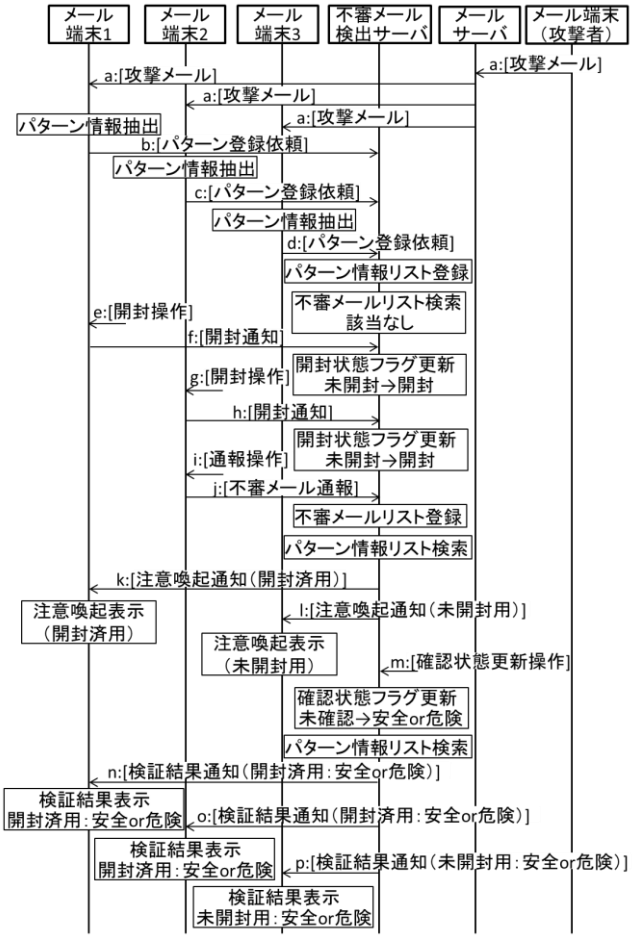


図 2　動作手順

4. メール端末 1 は開封操作をユーザより受け付け(e), 開封した電子メールのメール ID を含む開封通知を不審メール検出サーバに送信する(f) .
5. 不審メール検出サーバは，メール端末 1 からの開封通知を受信すると，メール端末 1 のパターン情報リストに登録されている開封状態を「未開封」から「開封済」に更新する．
6. 同様に，メール端末 2 もメール端末 2 のパターン情報リストに登録されている開封状態を「未開封」から「開封済」に更新する(g,h).
7. つぎに，メール端末 2 が，ばらまき型攻撃メールの可能性があるとする通報操作をユーザより受け付けると(i),メール端末 2 は，この電子メールを不審メールに設定して，不審メールおよびこの不審メールのメール ID を含む不審メール通報を不審メール検出サーバに送信する(j).
8. 不審メール検出サーバは，メール端末 2 からの不審メール通報を受信すると，メール端末 2 のパターン情報リストを参照し，この不審メール通報に含まれているメール ID に紐付けられたパターン情報を特定する．そして，特定した所定のパターン情報およびこの不審メール通報に含まれている不審メールは，検証による確認状態（ここでは「未確認」）を示すフラグ（以下，確認状態フラグ）とともに不審メールリストに登録する．
9. 不審メール検出サーバは，該当するメール端末 1，3 のパターン情報リストから，不審メールリストに登録した所定のパターン情報を検索できたならば，この所定のパターン情報に紐付けられて不審メールリストに登録されている確認状態が「未確認」であることを確認して，この所定のパターン情報に紐付けられて該当するメール端末 1，3 のパターン情報リストに登録されている開封状態に応じた注意喚起メッセージを生成しメール端末 1，3 に送信する(k,l).
10. メール端末 1，3 は，不審メール検出サーバからの注意喚起通知を受信すると，この注意喚起通知に含まれているメール ID により特定される電子メールの件名，差出人，宛先，受信日時等の諸情報を特定し，これらの諸情報を，注意喚起通知に含まれている注意喚起メッセージとともに表示する．
11. この不審メールが安全か危険かを管理者が判断し，確認状態更新操作を，管理者より受け付けると(m), 不審メール検出サーバは，確認状態フラグを「未確認」から「安全」あるいは「危険」に更新する．
12. 不審メール検出サーバは，すべてのメール端末 1～3 のパターン情報リストから，確認状態フラグに対応付けられて不審メールリストに登録されている所定のパターン情報を検索し，パターン情報リストに登録されている開封状態と，この所定のパターン情報に紐付けられて不審メールリストに登録されている確認状態フラグが示す確認状態（「安全」または「危険」）に応じて検証結果メッセージを生成し送信する (n,o,p) .
13. メール端末 1～3 は，不審メール検出サーバから検証結果通知を受信すると，この検証結果通知に含まれているメール ID により特定される電子メールの件名，差出人，宛先，受信日時等の諸情報を特定し，これらの諸情報を，検証結果通知に含まれている検証結果メッセージとともに表示する．

## 5. まとめ

本研究では，受信済みメールに対するばらまき型攻撃メール検知方法について検討した．

不審メール検出サーバは，受信メールのメール本文中の文面により定まる所定のパターン情報を，受信メールのメール ID に紐付けて蓄積する．ばらまき型攻撃メールあるいはその可能性があると判断されたメールについて，蓄積されたパターン情報のなかから検索し，メール端末に通知する。

メール端末は，不審メール検出サーバから通知されたメール ID により特定されるメールに対する注意喚起を表示する．

これによりばらまき型攻撃メールあるいはその可能性があると判断される前に，このメールをすでに受信しているメール端末に，このメールに対する注意を喚起することができる．

参考文献

[1] 弥田紘一, 佐々木昌樹, 齊木あずさ, “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”, 第 17 回情報科学技術フォーラム, 2018 年 9 月 19 日