[ポスター発表] 研究報告

IMAP エージェントを用いた スレッド表示による不審メール警告システム

兵頭樹 [1]　山井成良 [1]　北川直哉 [1,†]

A Warning System for Suspicious Emails by Message Threading and IMAP Agent

1. はじめに

電子メールはコミュニケーション手段の一つとして社会に広く根付いており，重要な情報技術となっている．一方で電子メールは迷惑メールや標的型攻撃といった行為にも利用され，情報窃取などの犯罪行為による被害も発生している[1].

こうした悪質なメールに対して受信側が可能なセキュリティ対策としては，ブラックリストや機械学習による検出が一般的である[2]．不審な点を検出したメール（以下，不審メール）に対して受信側が取れる処置は主に二種類存在する．一つは不審メールの自動削除や隔離であり，こちらは多くのメールサービス事業者が実施している一般的な処置であるが，誤検出の際に重要なメールを見逃すリスクが存在する．もう一つは不審メールの存在をユーザに警告するものであり，誤検出の場合のリスクを軽減しつつユーザに注意を促すことが可能である．しかし既存の警告方法には，後述するような問題点が存在する．

本論文では既存の問題点を解決するため，MUA のスレッド表示機能と IMAP エージェントを利用して不審メールを警告するシステムを提案する．

2. 既存の不審メール警告方法の問題点

- 互換性・汎用性に乏しい

不審メールのヘッダへの“Keywords:”フィールドの付加[3]や，「ラベル」や「タグ」などのメールの自動分類機能の利用，あるいは MUA の拡張機能の利用[4]といった警告方法が提案されている．その他，警告メールを作成してそこに不審メールをファイルとして添付するといった方法が存在する．しかしこれらの方法は特定のメール環境でのみ利用可能であったり，あるいは一部の環境では利用不可であったりする問題が存在する．

- 不審メールの再検証不可

不審メールの件名への[スパム]等の語句の付加[5]や，本文への警告文の付加[4]により警告を行う方法が存在する．しかし主要な送信ドメイン認証技術の一つである DKIM では電子署名の作成にメール本文を参照し，また多くの場合件名も参照するため，上述の方法では元のメールを再検証する際に失敗する問題が存在する．

- 利便性の低下

隔離した不審メールを一定期間ごとにユーザへレポートする[5]ことや，隔離した後に警告メールを送信する[4]ことにより警告を行う方法が存在する．しかしこれらの方法ではメールが到着した際に即座にメールを確認できなかったり，隔離されたメールに返信等する際にメールボックスを移動する操作が必要となったりすることから利便性を損なう問題が存在する．

3. 不審メール警告システムの提案

3.1 提案システムの概要

MUA には，同じスレッド（一連の会話）に含まれるメールをメール一覧画面やメール表示画面でまとめて表示する機能を持つものが存在する．このスレッド表示機能を利用すると，メール一覧画面ではスレッド内で最新のメールが表示されるようになる．本論文ではこれを利用して，IMAP エージェント[6]を用いて新着メールを検査し，不審メールを発見した場合にはそのメールと同じスレッドになるように警告メールを作成しアップロードすることで，メール一覧画面で警告文を表示するシステムを提案する．提案システムの構成図を図 1 に示す．なお，スレッド表示機能が使えない場合，あるいは利用しない場合でも警告メールの受信時刻が不審メールの直後となるため，メール一覧表示でまとまって表示され，一定の警告効果が見込まれる．

1 東京農工大学
Tokyo University of Agriculture and Technology
† 現在，国立情報学研究所
National Institute of Informatics

3.2 提案システムの利点

提案システムの利点を以下にまとめる．

(1) OS 付属の MUA や Gmail 等の Web メールサービスといった現在主要な MUA[7]の多くはスレッド表示機能に対応しているため，導入可能性が高い．

(2) 元の不審メールを書き換えないため，メール転送の際に DKIM 検証に失敗することがない．

(3) 不審メール確認の際にはスレッドを遡るだけでよく，隔離先メールボックスへの移動といった操作を挟む必要がない．

(4) 単純に警告メールを送信する場合と比較して，スレッド表示機能を利用することでどのメールに対して警告メールが送信されたかが分かりやすくなるため，不審メールの認識性を高める効果を期待できる．

(5) ユーザがスレッド表示機能を利用しない/できない場合も，単純な警告メール送信システムとして動作する．また IMAP エージェントを利用することで，メール環境を限定せず提案システムを導入可能であるため，総じて汎用性が高い．

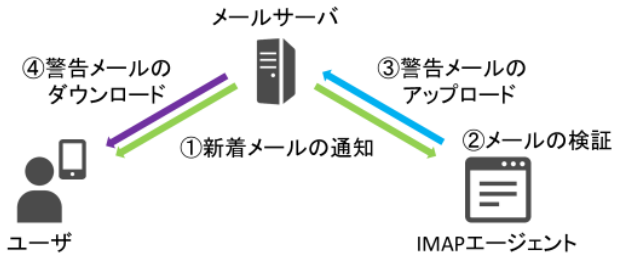

図 1　提案システムの構成

4. 不審メール警告システムの実装

提案する不審メール警告システムが実現可能であることを示すため，C#の IMAP クライアントライブラリを利用して提案システム（IMAP エージェント）を実装し，動作検証を行った．本節では実装したシステムの動作手順および検証結果について述べる．

4.1 システムの動作手順

1. IMAP エージェントはメールサーバに接続する．
2. 新着メールの通知が来るまで待機する．
3. 新着メールの内容を取得する．
4. 新着メールに不審な点が存在するか検査し，存在すれば次のステップに進む．存在しなければステップ 2 に戻る．
5. 新着メールのヘッダ情報を用いて，同じスレッドになるように警告メールをアップロードする．
6. 他に新着メールがあればステップ 3 に戻る．無ければステップ 2 に戻る．

4.2 システムの動作検証

実装したシステムをメールサーバに接続して動作検証を行った．本検証では提案手法の動作確認を目的として，検査は行わずに新着メールに対して無条件に警告メールのアップロードを行った．

動作検証の結果，Windows 10 標準メールアプリ他の主要な MUA で図 2 のように，提案手法の意図通りに警告文が表示されることを確認し，提案システムが実現可能であることを確認した．

図 2　Windows 10 標準メールアプリでの検証結果

5. おわりに

本論文では，MUA のスレッド表示機能と IMAP エージェントを用いることで既存方式の欠点を解消した不審メール警告システムを提案した．

今後の課題としては，警告メールがアップロードされる前にユーザが不審メールを開封してしまう場合や，大量の不審メールが届く場合など，実運用上で考えられるケースについて対応策の検討が必要であると考えられる．また，システムの効果の評価方法についても検討が必要であると考えられる．

参考文献

[1] 迷惑メール対策推進協議会, “迷惑メール白書 2018,” 2018-11-8. [オンライン]. Available: https://www.dekyo.or.jp/soudan/data/anti_spam/2018/HB18_00_all.pdf. [アクセス日: 2019-1-15].

[2] 田端利宏, “SPAM メールフィルタリング : ベイジアンフィルタの解説(情報のフィ ルタリング),” 情報の科学と技術, 第 56 巻, 第 10 号, pp. 464-468, 2006.

[3] 王建人, Natthamon Pongchanchai, 山井成良, 北川直哉, Vasaka Visoottiviseth, “ディスプレイネームをユーザ認証に利用したなりすましメール対策システムの試作,” インターネットと運用技術シンポジウム（IOT 2017）, pp.81-88, 2017 年 11 月.

[4] 福山雅深, 大岩美春, 山井成良, 北川直哉, “POP プロクシを用いた DKIM 検証システム の実装,” 情報処理学会研究報告, Vol.2015-IOT-28, No.2, 2015.

[5] 株式会社 NTT ぷらら, “機能詳細 | 迷惑メール振り分けサービス | ぷらら,” [オンライン]. Available: https://www.plala.or.jp/option/antispam/product/. [アクセス日: 2019-1-15].

[6] 横木健太, 山井成良, 王建人, 北川直哉, “電子メールの柔軟な処理を可能とする IMAP エージェント,” マルチメディア, 分散, 協調とモバイル(DICOMO 2018)シンポジウム論文集, pp. 1403-1406, 2018 年 7 月.

[7] Litmus Software, Inc., “Email Client Market Share Trends for the First Half of 2018,” 2018-7-13. [オンライン]. Available: https://litmus.com/blog/email-client-market-sharetrends-first-half-of-2018. [アクセス日: 2019-1-15].