標的型攻撃に対するセキュリティ教育を自動化する訓練システムの評価

徳地達哉　塩田智基　池尻圭佑　後藤田中　喜田弘司

香川大学

1. はじめに

近年標的型攻撃の被害が拡大しており 2018 年の時点では，6000 件以上の被害が発生している[1]．また，2015 年 5 月には日本年金機構が標的型攻撃の被害にあい，個人情報が約 125 万件流出した[2][3]．標的型攻撃の対策には，個々のセキュリティに対する意識の底上げが必要不可欠である．そこで我々は，標的型攻撃に対するセキュリティ教育を自動化する訓練システム(以下本システムと称する)の研究を行っている[4][5]．本稿では，本システムの有用性や需要をアンケートにより評価した．

2. 課題

現在のセキュリティ教育は，ウイルスメールの例を Web 教材で提示して注意喚起を行う手法が一般的である．標的型攻撃は日々進化するため従来の手法では以下の課題が挙げられる．

課題① 最新の標的型攻撃に追従した教材を人が作るためコストが高い

課題② 定期的に講義を受けなければ最新の標的型攻撃に対応することが難しい

また，これまでにも訓練システムを利用した教育手法は存在したが，システムを利用していても大多数が手動で動作しているため以下の課題がある．

課題③ 継続して訓練を行うことが難しい

これらの課題を克服することが標的型攻撃の対策として重要なものになると考えている．

3. 本システムの概要

本システムは日常的に行っているメール処理に訓練メールを紛れさせ，その訓練メールで行われた処理を解析し，その解析結果を利用して教育を行う．

3.1. 課題の解決

課題①は，訓練メールを受講者の受信メールをもとに自動生成することで教材を作る必要がなくなり解決する．課題②，課題③については，受講者が日常的に行っているメール処理の中で，訓練を行わせることで講義形式の教育を行う必要がなくなり解決する．

3.2. システムの構成

システムの構成(図 1)は，利用者，教師，メールシステム，本システムから成る．ここでの利用者は，受講者のことを指す．メールシステムは，利用者が日常的に利用するメールの送受信をするサーバである．本システムは以下の 3 つの機能がある．

(1) メールシステムから利用者の受信メールを受け取り，訓練メールを生成する

(2) メールシステムを介して訓練メールを利用者に送信する

(3) 利用者が訓練メールに対して行った処理を解析し，利用者にその結果を提示する

また本システムは，利用者に案内メールを送信することで解析結果を確認させるように促す．

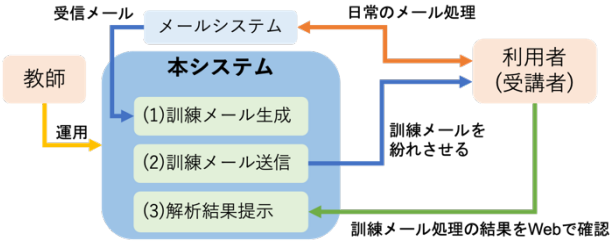

図 1 システム構成図

3.3. 訓練の流れ

訓練は日常的にメール処理を行っている利用者を対象とする．訓練の流れを以下に示す．

① 利用者は本システムに登録する

② 本システムから訓練メールが送信されるため，利用者はその訓練メールを処理する

③ 本システムは利用者が訓練メールに行った処理を解析し，利用者はその解析結果を確認し学習を行う

利用者は②と③を継続的に繰り返し訓練する．

4. システムの評価

4.1. 評価の目的

本システムの有用性や需要，利用者の対策意識とメール処理の傾向を知ると共に要件を明らかにする．

4.2. 評価の方法

まず，本システムの概要をデモしながら説明し，その直後にアンケートを実施した．回答者は，オープンキャンパスの訪問者 10 名であり，それぞれ，会社員 1 名，大学技術職員 1 名，学生 5 名，無職 1 名，高校生 2 名であった．

4.3. アンケートの内容

アンケートの内容(表 1)は，本システムについて

“System Evaluations of a Training System to Automate Security Education for Countermeasures Against Targeted Attacks”
Tatsuya Tokuchi, Tomoki Shiota, Keisuke Ikejiri, Naka Gotoda, Koji Kida
Kagawa University

の項目 (1〜4)と 被験者についての項目(5〜7)になっている．項目 1〜5 は 4 件法，項目 6 は 3 件法，項目 7，8 は自由記述で行った．

表 1 アンケートの内容

項目	質問内容
1	このシステムは便利だと思いましたか
2	自分のメール処理の傾向を知ることができれば，便利だと思いますか
3	自分が企業の社長だとして，会社にシステムを導入したいと思いましたか
4	このシステムで日常的に訓練を受けたら標的型メールに対応できると思いましたか
5	攻撃メールが来ても騙されない自信がありますか
6	メールのフォルダ分けは普段していますか
7	どのようなメールだと確実に開きますか
8	感想

5. アンケートの結果と分析

5.1. アンケートの結果

項目 1〜5 の結果を示す(図２)．項目 6 では，「はい」が 3 名，「いいえ」が 6 名，「メールを普段利用していない」が 1 名という結果になった．項目 7 では，「学校からのメール」，「仕事のメール」，「ゲームの通知」，「身内の不幸」などの回答があった．項目 8 では，「セキュリティ対策に今後役に立つと思った．」，「日常の生活に取り入れられていい研究だと思いました．」などの感想があった．

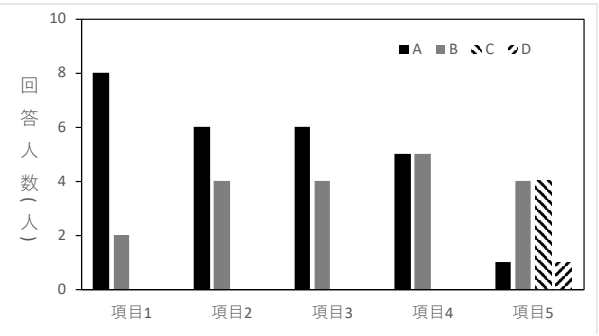

図 2 項目 1〜5 の結果

なお，図 2 の A，B，C，D は，項目 5 ではそれぞれ，「自信がある」，「少し自信がある」，「少し自信がない」，「自信がない」，その他の項目ではそれぞれ，「思う」，「少し思う」，「少し思わない」，「思わない」に対応している．

5.2. アンケートの分析

本システムの有用性に関して，項目 2 より，すべての人がメール処理の傾向を知ることが便利だと感じているため，傾向を求めることができる本システムの解析機能は有用性があるといえる．

本システムの需要に関して，項目 1 より項目 3 が「思う」と回答した人が少ないことについて調べると，多くの人が，2 つの項目で同様の回答をしていた．しかし，会社員の人は項目 1 では「思う」，項目 3 では「少し思う」と回答していた．よって，本システムには需要があるが，企業として運用するためには改良が必要であると考えられる．

普段のメール処理について，項目 7 より，所属している組織や普段利用しているサービスからのメールは開いてしまう傾向があると推測する．

メールのフォルダ分けを行っている人は，対策の意識が高いと推測し，項目 5 と 6 の相関を確認した．その結果，メールのフォルダ分けを行っている人は騙されない自信があることが多い．また，項目 6 より，メールのフォルダ分けを行っている人は少なかった．職業別に見ると，会社員と大学技術職員という企業で働いている人はフォルダ分けを行っている．一方，学生はフォルダ分けを行ってないことが多い．以上より，今回のアンケートでは，学生の比率が高かったため，このような結果になったと推測することができる．また，学生よりも社会人の方が，フォルダ分けを利用するなど，意識だけでなく行動での対策を行っている傾向が高いといえる．

6. おわりに

アンケートの結果と分析より，本システムが有用であることがわかった．今後は，メール処理の傾向分析と，実際に組織で運用してもらうことの 2 点を目標に研究を行っていく．

参考文献

[1] 警察庁, “平成 30 年におけるサイバー空間をめぐる脅威の情勢等について”, https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf, 2019/12/19

[2] 日本年金機構, ”不正アクセスによる情報流出事案に関する調査結果報告について”, https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.files/press0820.pdf, 2019/12/19

[3] 米谷雄介ら, 香川大学での標的型攻撃メール訓練の導入と改善点の検討, 学術情報処理研究 22 巻, 第 1 号, pp54-pp63, (2018)

[4] 塩田智基ら, “標的型攻撃に対するセキュリティ教育を自動化する訓練システムの提案”, 令和元年度電気関係学会四国支部連合大会論文集，pp183, (2019)

[5] 塩田智基ら, “標的型攻撃に対するセキュリティ教育を自動化する訓練システムの開発”, 大学 ICT 推進協議会 2018 年度年次大会論文集, pp298-pp302, (2019)