1T-03

標的型攻撃に対する訓練で利用されるメールを自動生成するシステムの提案

池尻圭佑　塩田智基　徳地達哉　本部建大　檜垣龍徳　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 年時点では,6000 件以上の被害が発生している[1]. 標的型攻撃メールは手口が巧妙化しており,その判別は難しくなってきている.近年の標的型攻撃メールは,標的とする企業と関連性の高い,実在する取引先に偽装して送信先に指定したり,添付ファイル名も業務に関係性があるものにしたりと見破るのは難しくなっている[2].標的型攻撃メールの対策は,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り,解決策のひとつは,セキュリティ教育を受けることである.しかし,前述のとおり,標的型攻撃メールは巧妙化しているため,個人が騙されやすいメールを用いて教育を行うことが必要である.

2 課題

現在のセキュリティ教育で利用されるメール(以下訓練メール)は,一般的に,被害が大きい標的型攻撃メールや自組織内で実際に見つかった標的型攻撃メールを模倣することで作られる.訓練メールを作成する人はその組織の IT やセキュリティの責任者であり,その組織内の部門の情報や個人の情報は全く知らない.一方,攻撃者は組織内の部門や個人の情報を何らかの方法で調査し,標的型攻撃メールを作成している.以上のように,攻撃者の手法のように組織内の部門や個人の情報を用いて訓練メールを作成する必要がある.

3 提案システム

3.1 課題の分析

我々は騙されたことを,以下のように定義する.

1. メールを開くこと
2. メールの添付ファイルをダウンロードすること
3. メール内のリンクを踏むこと

一般にこれらの操作をユーザが行うのは差出人を確認し,件名が適切であることを確認し,メールの内容が適切であることを確認できた後である.

差出人が何度もメールを交わしている相手である場合や件名に自組織の情報,例えば取り扱っている製品名が含まれている場合や,本文中に受信者の名前が含まれている場合は騙されやすい.

以上を踏まえ,我々は騙されやすいメールの特徴として3つの仮説を立てた.

1. 受信者が属している組織の情報(以下組織情報)が含まれているメールは騙される
2. 受信者の個人情報が含まれるメールは騙される
3. 受信者の知り合いからのメールは騙される

さらに過去に標的型攻撃メールのセキュリティ教育を受けたことがある受信者において,騙された訓練メールは,理由は不明だが,その受信者が騙されやすい特徴を持ったメールであると考えられる.すなわち,以下を 4 番目の仮説とした.

4. 過去に騙されたことのあるメールはもう 1 度騙される

3.2 システムのコンセプト

次に上記の仮説の下で課題を解決するための手法を述べる.攻撃者は受信者の情報を誰でもアクセス可能な受信者の組織のホームページから入手しているため,1 に関しては組織のホームページの情報を用いて訓練メールを生成する.攻撃者はウイルス等の何らかの手法を使って受信者のメールや SNS から受信者の個人情報(以下個人情報)や受信者とやり取りをしている知り合いの情報(以下知人情報)を入手しているため,2,3 に関しては受信者のメールや SNS の情報を用いて訓練メールを作成する.4 に関しては,セキュリティ教育は実施結果は何らかの方法でアーカイブされており,どういった訓練メールに対して受信者がどういう行動を行ったのか(以下訓練メールの結果)は残っている.この情報を使って訓練メールを生成する.

3.3 システムの構成

本システムは,データ解析部とモデル群とメール生成部から構成されている(図 1).先行研究の入出力(上部)に関しては 4 章で述べる.

データ解析部は,学習方法ごとにセキュリティ教育学習,ホームページ学習,SNS・メール学習の 3 種類からなる.

- セキュリティ教育学習(仮説 4 より):訓練メールの結果(4 章に示す)と訓練メール,標的型攻撃メールの件名と本文/訓練メールの特徴を学習したモデル
- ホームページ学習(仮説 1 より):組織情報/組織情報を学習したモデル
- SNS・メール学習(仮説 2,3 より):受信者の SNS・メールの情報/個人情報や知人情報を学習したモデル

以上の情報から各個人が騙されやすいメールの特

Proposal of a System to Automate Generation of Training Mail used in Education for Countermeasures Against Targeted Attacks
Keisuke Ikejiri, Tomoki Shiota, Tatsuya Tokuchi, Tatsuhiro Motobu, Tatsunori, Higaki, Naka Gotoda, Koji Kida
Kagawa University

徴を学習したモデルを作成する.

モデル群は,データ解析部で作られた学習モデルの集合である.モデルは,1 人の受信者に対しデータ解析部の学習方法の個数である 3 つずつ存在する.これらを利用して訓練メールの生成を行う.

メール生成部は,過去の訓練メールと標的型攻撃メールを入力にモデルを用いて訓練メールを生成する.過去の訓練メールなどの単語を編集することで個人ごとに騙されやすい訓練メールを生成することができる.図 2 は,メール生成部に入力される標的型攻撃メールの 1 例(上部), モデルから得られる騙されやすいメールの頻出単語や差出人リストの例,メール生成部から出力される訓練メールの例である.宅配便を装った標的型攻撃メールに騙される人は少なくなっている.モデルから得られる頻出単語や差出人リストを利用し,出力として,例えば,大学関係者の場合,入試の採点結果の確認メール,企業関係者の場合,製品の見積もり結果の確認メールが生成される.過去に騙されなかった訓練メールから各ユーザが騙されやすい訓練メールを生成することもできる.

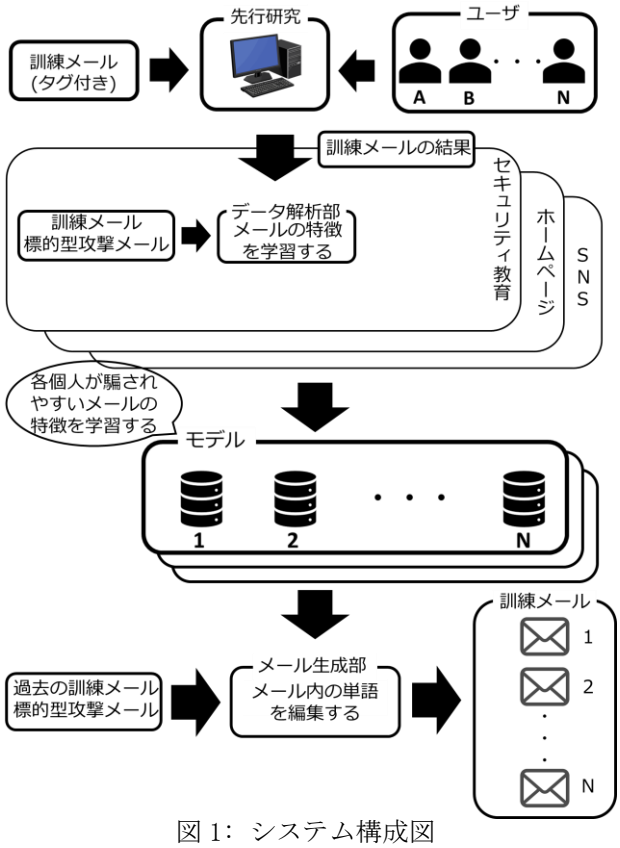

図 1: システム構成図

4 先行研究システムとの連携

セキュリティ教育から教育結果を得るための 1 例として先行研究[4][5]を利用する.先行研究システムは,訓練メールを用いて複数人のユーザにセキュリティ教育を行う(図 1).この先行研究システムから各ユーザの訓練メールの結果を受け取り,データ解析部でメールの特徴を学習する.

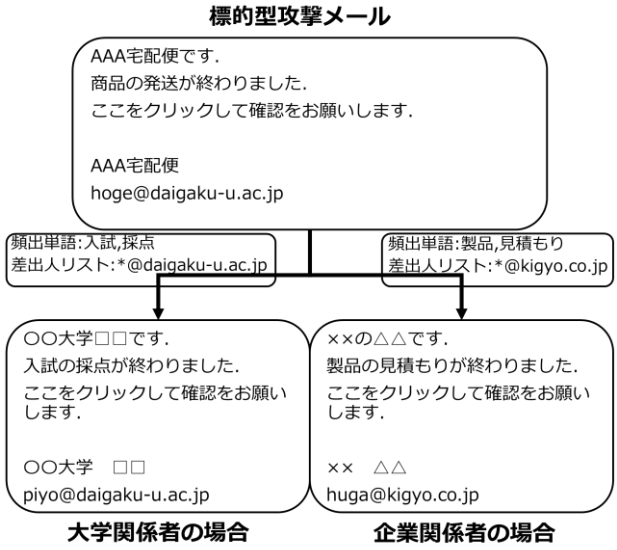

図 2: 訓練メールの生成例

参考文献

[1] 警視庁,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 年 3 月 7 日

[2] 標的型メールとは？巧妙化する手口とその対応方法, https://eset-info.canon-its.jp/malware_info/special/detail/190725.html,2019 年 7 月 25 日

[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,p54-63,2019 年 12 月 19 日

[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,16(1) - 2019 年 9 月 19 日

[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,p298-p302,2019 年 12 月 19 日