自動生成した標的型メールを用いた訓練用メール配信システムの開発

徳野 響　五味 悠一郎

本研究の目的は「自作標的型メールを学習させた訓練用標的型メールの自動配信システム」を構築し, 企業が標的型メール訓練を積極的に行うことができる状況をつくることで社会のセキュリティ意識を向上させ標的型メール被害を減少させることである. 先行研究ではマルコフ連鎖と多重マルコフ連鎖を用いて自作標的型メールを基に訓練用標的型メールを自動生成するシステムを開発した. しかし, 自動生成した訓練用標的型メールを配信するシステムは開発されておらず, 開発した訓練用標的型メール自動生成システムを用いた標的型メール訓練を行うことができない状況である. そこで本稿では自動生成した標的型訓練用メールを自動配信するシステムを開発し, 自作標的型メールを学習させた訓練用標的型メールによる標的型メール訓練を行うことを可能にした.

1　はじめに

サイバー攻撃の 1 つとして, 標的型攻撃がある. 標的型攻撃による機密情報の窃取は, IPA の情報セキュリティ 10 大脅威に 2016 年から 9 年間連続で選出されており, 優先的に対策を行うべき攻撃の 1 つである [1]. 標的型攻撃において標的組織のネットワークへの初期侵入時にメールを用いて行われる攻撃手法を標的型メール攻撃という. 標的型メールは, 情報窃取等を目的として, ごく少数または多数ながら特定された範囲のみに対して送られ, 利用者の PC をマルウェアに感染させることを目的としている. 特徴としては, 送信者の詐称や添付ファイル等を開かせるための件名, および本文の細工などが見られる.

標的型メール攻撃への対策の 1 つとして, 標的型メール訓練が挙げられる. しかし, 標的型メール訓練を行うサービス費用の問題から, 企業が標的型メール訓練を積極的に行えない状況にある. また, サービスを利用する以外の方法として, 独自に標的型メール訓練環境を用意することが考えられるが, 技術的な知識やノウハウが求められるため困難である場合が多い. そこで, 標的型メールを基に自作した標的型メール（以降, 自作標的型メールとする）を用いた標的型メール訓練システムを開発し, 企業が簡単に標的型メール訓練を行える状況を作ることで問題解決を図る.

本稿では, 自作標的型メールを用いた標的型メール訓練システムを利用可能にするために, 自動生成した標的型メールを配信するシステムを開発した.

2　準備

本稿で用いる用語や先行研究について説明する.

2.1　URL パラメータ（クエリストリングパラメータ）

Web プログラム呼び出しの URL の中に含まれるパラメータのことである [2].URL の後ろに”?”（クエスチョンマーク）を挟んで, パラメータ名とパラメータの値が”=”（イコール）で結ばれる形で記述される.Web アプリケーションに対して URL パラメータで値を渡すことで, 値に応じた処理を行うことが可能である.

Concurrent Operations on Splay Trees.
Yuichiro Gomi, 日本大学理工学部, College of Science and Technology, Nihon University.
Hibiki Tokuno, 日本大学理工学部応用情報工学科, Department of Computer Engineering, College of Science and Technology, Nihon University.

2.2　訓練用標的型メール自動生成システム

当研究室において, マルコフ連鎖を用いた訓練用標的型メール自動生成システム（以降, メール自動生成システムとする）を開発した [3]. この研究では,『IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」』やセキュリティ企業が実例として提供している標的型メールを参考に, 自作標的型メールを作成してメール文章の自動生成を行った. 形態素解析された自作標的型メールを基に, マルコフ連鎖によるメール文章の自動生成を行うことで, 時間を要さず極めて短い時間で訓練用標的型メールの生成を可能にしている. マルコフ連鎖を用いた訓練用標的型メール文章生成は Google Colaboratory 上で行い, 形態素解析によって判定された固有名詞 (人名や組織名および地域など) を伏字で出力する仕様であった. メール自動生成システムによって, 生成したメール文章の例を図 1 に, メール自動生成システムのシステム構成図を図 2 に示す.

行政執行法人　×××　〇〇と申します。
それ故、〇〇オリンピックの記事の掲載を予定しております。
平素より格別のご指摘をお伺いしたく、質問内容を添付ファイルにまとめさせていただきました。
お忙しいところ、恐れいりますが、ご連絡させて頂きました。
ご検討いただきますよう、ご連絡させて頂きました。

図 1　マルコフ連鎖を用いて自動生成したメール文章

図 2　マルコフ連鎖を用いた訓練用標的型メール自動生成システム構成図

3　訓練用メール配信システム

本稿では, マルコフ連鎖により自動生成した標的型メールを配信するためのシステム（以降, メール配信システムとする）として, メール配信機能とクリック者検知機能を開発した.

3.1　メール送信機能

マルコフ連鎖によって自動生成されたメール文章を取得し, メールとして送信するスクリプトを開発した. このスクリプトは Google Drive 上の csv ファイルに, 訓練者の氏名やメールアドレスを入力して実行することで, 自動生成されたメール文章内の伏字を入力内容に置き換え, 対応したメールアドレスに自動生成したメール文章を送信する. メール送信時には訓練者ごとに個別の数値を設定し URL パラメータとして組み込んでいる. この URL パラメータは, 後述する URL クリック者検知機能に利用している.

3.2　URL クリック者検知機能

GCP(Google Cloud Platform) を利用して URL クリック者検知を行う Web ページを作成した. この Web ページはアクセス者の URL パラメータを取得し, CSV ファイルに保存する.URL パラメータに id と num の 2 つの値を設定することで,URL クリック者を判断可能にしている.

4　テスト方法と評価方法

開発したメール配信システムを使用し, 機能テストを行った. この機能テストでは, 5 つのメールアドレスに対して, URL クリック者検知機能をもつ Web サイト URL を含んだ自作標的型メールを, 各 60 通ずつの計 300 通送信した. また, 伏字となっている氏名を受信者ごとに置換した 300 通のメールがすべて正常に送信されたこと, およびメール文章に含まれる Web サイト URL をクリックした場合にメール受信者を識別する URL パラメータが記録されることを確認した.

メール配信システムにおける訓練対象者数の上限は 300 名としているため、機能テストでの送信メール数を 300 通とした. 各メールアドレスに氏名と対応した訓練用メールが送信されたことを確認するため, 送信先のメールアドレス数は, 現在使用している 5 つとした. 各メールアドレスにて, 正常に受信したメール文章の例を図 3 と図 4 に示す.

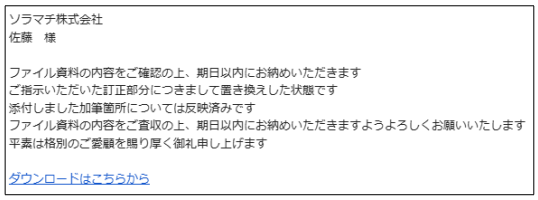

図 3　受信したメール文章 (氏名：佐藤)

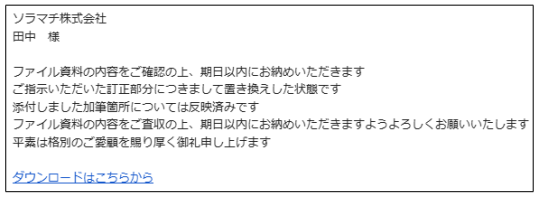

図 4　受信したメール文章 (氏名：田中)

5　結果と考察

メール配信システムにより, 300 通のメールを正常に送信することができた. また, 各メール文章に含まれる URL に対応した URL パラメータを, すべて記録できていることが確認できた. これらの結果から, 自動生成した標的型メールを用いた訓練用メール配信システムは, 実用に耐えうるといえる.

6　まとめと今後の課題

自動生成した標的型メールを用いた訓練用メール配信システムを開発した. 自動生成した標的型メールの送信, およびクリック者の検知を行うことができており, URL が含まれる自作標的型メールを用いた標的型メール訓練システムとして利用可能である. 一方, 添付ファイルを送信する機能がないため, このシステムでは, 添付ファイルをダウンロードさせる標的型メールに対する訓練は行うことができない.

今後の課題は, 添付ファイルを送信する機能を実装すること, および実際の環境でシステム動作を検証することである. これらの課題を解決することで, 自動生成した標的型メールを用いた訓練用メール配信システムとして, より実用的になると考える.

参 考 文 献

[1] 独立行政法人情報処理推進機構 (IPA): 情報セキュリティ10 大脅威 2024. https://www.ipa.go.jp/security/10threats/10threats2024.html, 参照 2024-08-03.

[2] 独立行政法人情報処理推進機構 (IPA): 第 5 章　3. コンテンツ間パラメータ対策. https://www.ipa.go.jp/archive/security/vuln/programming/web/chapter5/5-3.html, 参照 2024-08-03.

[3] 釜田諒大, 五味悠一郎: N 階マルコフ連鎖を用いて自動生成した訓練用標的型メールの比較と評価, 2023. 第 67 回日本大学理工学部学術講演会.