電子メールにおける情報セキュリティのリテラシ調査システム

A System to Check the Literacy of Information Security for E-Mail

森田 浩平[*1], 松本 慎平[*1], 岩井 健吾[*1]
Kohei MORITA[*1], Shimpei MATSUMOTO[*1], kengo IWAI [*1]
[*1] 広島工業大学情報学部
[*1] Faculty of Applied Information Science, Hiroshima Institute of Technology
Email: {b214205, s.matsumoto.gk, b212013}@cc.it-hiroshima.ac.jp

あらまし: 現在，電子メールは規模に関わらずあらゆる組織において必須のコミュニケーションツールとなっているが, その反面, 電子メールからのマルウェア感染, それに伴う情報漏洩事例は増え続けている．さらに，攻撃ツール・ドキュメントの充実や攻撃者の技術力の向上により，情報漏洩のリスクは高まる傾向にある．セキュリティリテラシを高めるための啓蒙活動やセミナーは各所で積極的に推進されているが, セキュリティ教育の受講者は, 情報漏洩が起こった実際の状況を想像することが難しい. したがって，研修内容に対して他人事のように感じてしまう傾向にあるため，セキュリティ漏洩に対する危機感を自覚させることは容易ではない. そこで本稿では，電子メール利用における情報セキュリティのリテラシを調査でき，教育利用が可能なシステムを開発する．本システムの対象利用者は，電子メールにおけるセキュリティを学ばせたい者である．本システムは，実際の攻撃を想定したメールを対象利用者に対して自動送信し，対象利用者のメールに対する反応を記録できる．本システムは，情報セキュリティのリテラシを調査できると共に，実データを収集できるため，現実感溢れるセキュリティ教育の展開に寄与できる．
キーワード: 電子メール，情報セキュリティリテラシ，マルウェア，情報漏洩，セキュリティ教育

1. はじめに

近年インターネットの普及に伴い，電子メールは個人・業務利用はもちろんのこと，あらゆる組織において，関係者間の情報共有や外部との協働を行う際の必須のコミュニケーションツールとなっている．また，電子メールはデータ(ファイル)共有に最も利用されている手段であり，数年前の時点で業務データの 7･8 割が電子メール添付でやり取りされていると報告されている(1)．このように電子メールの重要度が高まるにつれ，電子メールは，スパムメール，ウィルスなど外部からの脅威を受け続けている．ウィルスは，電子メールによって感染及び拡散するケースが最も多く，電子メールによるウィルスの感染の割合は IPA におけるコンピュータウィルスに関する届出件数の実に約 98%を占めていると報告されている(2)．電子メールを使った攻撃技術は巧妙化し続けており，日々新たな攻撃手法が出現している．

こうした中，電子メールのセキュリティは重要視されており，電子メール利用者のセキュリティに関する意識を高め組織の内部情報や知的財産権を保護するため，セキュリティリテラシを高めるための啓蒙活動やセミナーは各所で積極的に推進されている．しかしながら，電子メールでのマルウェア感染による企業の内部情報漏洩は後を絶たない(3)．その大きな理由として，セキュリティ教育の受講者に情報漏洩が起こった実際の状況を想像させることが難しいため，情報漏洩に対する危機感を自覚させることは容易ではないからであると考えられる(4). 一方で, 標的型攻撃は情報セキュリティ上の大きな脅威となっていることから(5)，情報漏洩は各自の身近な問題であることを実体験から自覚させることが重要ではないかと考えられる．そのためには，セキュリティ学習対象者のリテラシに適した現実感溢れるセキュリティ教育を実施するためには，学習者のセキュリティに関するリテラシを自然な形で容易に調査できるような仕組みが必要ではないかと考えられる．

そこで本稿では，電子メール利用における情報セキュリティのリテラシを自然な形で容易に調査でき，セキュリティ教育に展開可能なシステムを開発する．提案システムの対象利用者は電子メールにおけるセキュリティを学ばせたい者であるため，年齢や職業問わず提案システムを適用可能である．提案システムは，実際の攻撃を想定したメールを対象利用者に対して自動送信し，対象利用者のメールに対する反応を記録できる．具体的には，利用者プロファイルの近さ，漏洩事例の多さや攻撃手法の巧妙さの 2 種類の要素から標的型攻撃メールの難易度を設定し，各難易度のメールに対する対象利用者の反応を記録することができる．ここで得られた記録から電子メールの情報セキュリティリテラシの動向を調査すると共に，実データに基づいたセキュリティ教育の実践に活用できる．

2. 標的型攻撃メール

標的型攻撃メールは，主として特定の組織や人に送信されるものであり，機械的な分類が難しい．また，メール受信者が不審を抱かないよう巧妙な手口を駆使しているため，本物のメールと勘違いする可能性が高い．標的型攻撃メールの発見は，利用者各自の情報セキュリティリテラシに強く依存する．

標的型攻撃メールに対するセキュリティリテラシ向上を目的とした取り組みが報告されている[6,7]．これら先行研究から，標的型攻撃メールに対する意識を高めるためには，実状況を想定した調査や教育が不可欠であると考えられる．

3. 調査用システム構築

構築した調査用システムは，実際の攻撃を想定したメールを対象利用者に対して自動送信し，対象利用者のメールに対する反応を記録できるものである．システム構成は，FreeBSD 10.1 を OS とし，Web サービスは Apache 2.4.10，SMTP サービスは Postfix 2.11.5，IMAP3/POP3 サービスは Dovecot 1.2.17 で提供される．また，メールクライアントとして Thunderbird 31.7.0 を利用した．

本研究では，利用者プロファイルの近さ，漏洩事例の多さや手法の巧妙さの 2 種類の要素から標的型攻撃メールの難易度を設定し，メール文面を作成した．各要素の難易度は 4 段階で定義されている．よって，計 16 種類のメールが対象利用者に任意の間隔と任意の順番で送信される．ただし，一日あたり 0~2 通を送信数とした．

利用者プロファイル要素の難易度(個人情報に近ければ近いほど難易度が高いと定義)：
Lvl 1: 心当たりのない通知を記述したメール文面
Lvl 2: ユーザ登録を行っていたウェブサービスの情報が漏洩した場合を想定したメール文面で，興味を惹かれる内容．
Lvl 3: 所属大学が所数する情報が漏洩した場合を想定したメール文面
Lvl 4: 指導教員が所有する情報が漏洩した場合を想定したメール文面

手法の巧妙さ(文献[8]に基づき難易度を定義)：
Lvl 1: 差出人(署名)と from ドメインが異なる
Lvl 2: 日本語の不自然さがある(簡体や繁体が用いられているなど)
Lvl 3: メール本文に表示されている URL が通常と異なっている．
Lvl 4: ファイル拡張子やアイコンが偽装されている．

架空のユーザアカウントは 13 種類，ドメインは 6 種類用意し，Postfix 上でバーチャルドメインを構築した．送付されたメールに対しては，メールに返信したか，URL をクリックして Web サーバにアクセスしたか，添付ファイル(word)を開いたか，添付ファイル(exe)を実行したか，の 4 種類の情報を取得できるようにしている．なお， word には Web ビーコンを仕込んでおり，受信者が開封すると用意した Web サーバにアクセスする仕組みとなっている．また，exe は C#(.NET)で作成し，実行すると word 同様に用意した Web サーバに GET リクエストを送信するもので，レベル 2-4 における exe に関してはアイコンと拡張子(ファイル名)が偽装されている．

from: matsumoto@matsumoto-s.pw
Subject: ゼミ旅行

ゼミ旅行についての資料を送ります。
資料の内容は編集を有効にすると確認できます。
よろしくお願いします。

word 添付

図 1　メール文面の一例 (利用者プロファイルのレベル 4，手法の巧妙さレベル 2)

4. 実験結果及び考察

情報学を専攻する大学 4 年生及び大学院 1 年生 15 名を被験者として実験を開始させた．本稿執筆の段階では実験中であるが，現在までに，利用者プロファイルのレベル 3，4 に対して反応する被験者がおり，標的型メールに対する耐性の低さが浮き彫りとなった．とりわけ，普段からメールに対して真面目に返信を行う学生が顕著に反応していた．ただし，学生の何名かは指導教員にメールについて直接確認するものがいた．対策として，実際に対面する機会にメールの件を確認する習慣をつけること，また，ウェブメールの GUI ではいくつかの情報が非表示になっていることから，この点について，教育の場で注意深く教授すべきであることを確認した．以上は，提案システム無しでは得られなかった知見である．

5. おわりに

本稿では，電子メール利用における情報セキュリティのリテラシを自然な形で容易に調査でき，セキュリティ教育に展開可能なシステムの概要と，現在の時点までに得られている実験結果の一部を紹介した．実験結果の詳細及び構築したシステムの動作例は当日発表で紹介する．

参考文献

(1) ダウジャパン株式会社, メールによる情報漏洩を防止するための Outbound メールの制御機能，SPAM WATCHER Outbound ホワイトペーパー (2009).
(2) 独立行政法人情報処理推進機構, 大企業・中堅企業の情報システムのセキュリティ対策〜脅威と対策〜, 分冊 5 (2007).
(3) 株式会社ラックサイバーグリッド研究所, 日本における標的型サイバー攻撃の事故実態調査レポート, Cyber GRID View, Vol.1, pp.1-35 (2014).
(4) 独立行政法人情報処理推進機構, 標的型攻撃メールの傾向と事例分析 (2013).
(5) 総務省，情報通信白書平成 25 年版 (2013).
(6) 木村壮太, メール攻撃危険予知訓練システムの開発, 情報処理学会研究報告, Vol.2013, No.4, pp.1-6 (2013).
(7) 伊藤史人，高見澤秀幸，佐藤郁哉，標的型攻撃メールの予防対策，学術情報処理研究，No.16, pp.100-110 (2012).
(8) 独立行政法人情報処理推進機構，IPA テクニカルウォッチ「標的型メールの例と見分け方」(2014).