標的型攻撃に対する報告を確実に行うための リマインダ機能を有した対話エージェントの開発

徳地 達哉 [1)], 池尻 圭佑 [1)], 塩田 智基 [1)], 米谷 雄介 [1)], 後藤田 中 [1)], 大野 真伯 [1)], 山下 俊昭 [1)], 小野 滋己 [1)], 八重樫 理人 [1)], 藤本 憲市 [1)], 林 敏浩 [1)], 今井 慈郎 [1)], 最所 圭三 [1)], 喜田 弘司 [1)]

1) 香川大学

s17t248@stu.kagawa-u.ac.jp

Development of a Dialogue Agent with Reminder Function to Ensure Reporting Against Targeted Attacks

Tatsuya Tokuchi [1)], Keisuke Ikejiri [1)], Tomoki Shiota [1)], Yusuke Kometani [1)], Naka Gotoda [1)], Masanori Ono [1)], Toshiaki Yamashita [1)], Shigemi Ono [1)], Rihito Yaegashi [1)], Kenichi Fujimoto [1)], Toshihiro Hayashi [1)], Yoshiro Imai [1)], Keizo Saisho [1)], Koji Kida [1)]

1) Kagawa Univ.

概要

近年、標的型攻撃の対策は緊急課題と言える。大学では、セキュリティ管理者や教職員だけで組織内のすべてのインシデント情報を把握することは難しいため、学生の力を借りる必要がある。しかしながら本学では、学生からの報告はほとんどあがっていない。本研究では、セキュリティ管理者に報告する訓練及び実際の窓口に利用できるリマインダ機能を有した対話エージェントを提案し、それを実現するためのシステムを開発した。開発したシステムを導入することで得られる報告件数の増加によるメリットとシステム面のメリットを利用者に伝えることで、システムの継続利用が可能となり、報告件数の長期的な増加に繋がる効果が期待できる。

1 はじめに

近年、標的型攻撃の被害が拡大しており、深刻な問題となっている。2019 年 10 月には、首都大学東京教員のパソコンが標的型攻撃によって、ウイルスに感染し、当該パソコンからメールアドレスが窃盗される事件が起こるなど、大学機関での被害も多く発生している[1]。

標的型攻撃の対策には、フィルタリングサービスやウイルス対策ソフトなどを利用したシステム上の対策と、組織の人に対する教育による対策がある[2]。システム上の対策だけでは、脆弱性が狙われることが多く、防ぎきれない。そのため、教育の重要性は高まっている。

教育による標的型攻撃の対策では、「メールを怪しいと判断したら開封しない」、「開封して、怪しければ、添付ファイルや記載リンクをクリックせずに破棄する」など、構成員が攻撃メールに騙されないことに加えて、「メールを怪しいと判断したらセキュリティ管理者に報告する」など、組織の感染拡大を防ぐ行動が必要である。しかし、現在の教育では、前者のみを目的として実施している場合がほとんどである[3]。

そこで本稿では、セキュリティ管理者に報告をする訓練及び、実際にセキュリティ管理者との窓口に利用できるリマインダ機能を有した対話エージェントを提案し、システムとしての試作の開発について述べる。

2 報告の課題

大学では、セキュリティ管理者や教職員だけで組織内のすべてのインシデント情報を把握することが難しい。大学には学生がおり、彼らの力を借りることで攻撃を探知する目が大幅に増加し、それにより組織全体の被害回避能力の大幅な向上が期待できる。しかしながら本学では、学生からの報告はほとんどあがっていない。香川大学情報メディアセンターの職員にヒアリング調査した結果、

3 つの心理的障壁があることがわかった。
障壁1.　誰かわからない人に連絡しづらい
障壁2.　どんな場面で報告していいかわからない
障壁3.　習慣化されていない(面倒だと感じる)

3 コンセプト

3.1 アイデア

我々は、報告先が人であることを意識させないことで障壁 1 を低減することができると考えた。その実現方法として学生とセキュリティ管理者の間を取り持つ対話エージェント(以下エージェントと称する)を提案する。

また、エージェントから学生に報告を促すアクションを取ることで報告する場面の提供、報告の習慣化に繋がり、障壁 2、3 を低減することができると考える。本研究では、報告を促すための方法をリマインダとして実現する。加えて障壁 3 に関して、学生のメール離れが問題となる。本学での現在の報告は、メールと Web サイトのフォームでする。しかし、手軽なチャットツールの普及により、近年の学生のメール離れが進んでいる。そこで我々は、近年の学生が得意であるチャットツールを用いることで、簡単に利用できるエージェントとする。

訓練と実際でシステムが異なると、心理的障壁が新たに発生することが予想されるため、どちらにも使用できるものを目指す。

3.2 エージェントの動作イメージ

図 1 に示すように、エージェントを介して学生とセキュリティ管理者との間でやり取りをする。

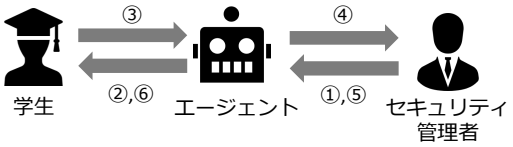

図 1 動作イメージ

報告プロセスについて図 1 を用いて説明する。始めに、セキュリティ管理者が学生に報告して欲しい内容をリマインダとして登録する(①)。エージェントは学生に一定周期でリマインダを送信する(②)。それに対し学生は、エージェントに報告する(③)。セキュリティ管理者は、学生の報告をエージェントから受け取り、対応する(④)。その対応はエージェントを経由して学生に伝えられる(⑤、⑥)。図 2、3 は、報告プロセスにおいて学生、セキュリティ管理者が利用する画面の例である。

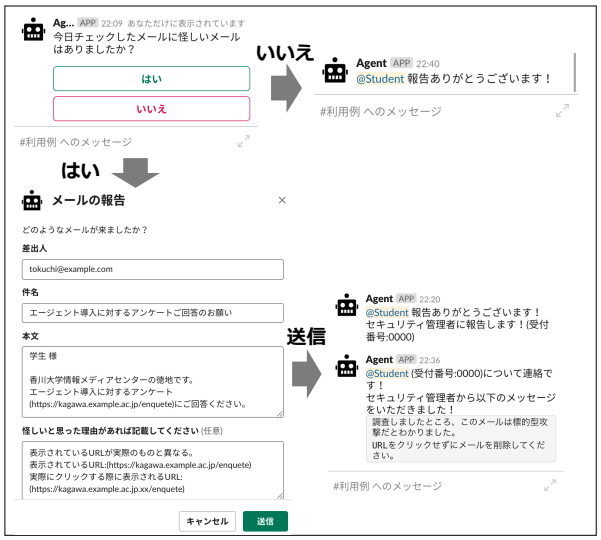

図 2 学生の利用画面例

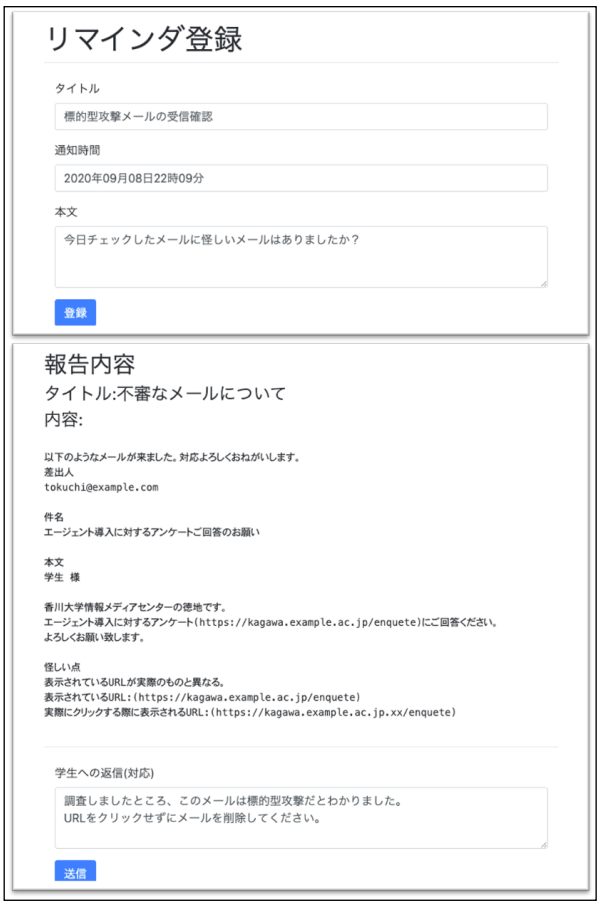

図 3 セキュリティ管理者の利用画面例

「エージェント導入に対するアンケートご回答のお願い」という件名の標的型攻撃メールが流行しており、本学の学生にそのメールが届いていた場合を想定する。セキュリティ管理者は、IPA などのサイトから流行の情報を発見する。セキュリティ管理者はこのメールが本学にも届いているのか確認したい。そこで、セキュリティ管理者は、リマインダとしてそのメールが届いているのかをエージェントを介して学生に問いかける。学生は、

そのメールを怪しいと思っていたが確証が持てずに放置していた。エージェントからのリマインダにより確証を得て、届いていることをチャットツールで報告した。このとき、チャットツールの操作に慣れているため、その場で簡単に返信として報告することができた。届いた報告をセキュリティ管理者は確認し、メールのリンクをクリックしないよう、エージェントを介して学生に指示した。

4 システムの試作

4.1 システムの機能と要件

エージェントを以下の 3 つの基本機能を持つシステム(以下本システムと称する)として開発する。

リマインダ機能：今までに報告された攻撃についての被害等の報告すべき内容をリマインダとして登録する。そのリマインダを指定した日時に学生に通知する。

報告機能：学生からの報告を受け取り、セキュリティ管理者に送る。それへの対応をセキュリティ管理者から受け取り、学生に送る。また、予想できる報告は、本システムが直接対応する。例としては、訓練時の想定された報告や、今までに学生から多く寄せられた報告などがある。

シナリオ進行機能：セキュリティ管理者が作成したシナリオに沿って、学生と本システムが対話する。シナリオは学生が実施したいタイミングで開始することができる。

これらの機能は並列に動いており、お互いに干渉することはない。また、学生の情報をセキュリティ管理者が正しく処理するために、学生の登録をしなければ機能が呼び出されないように制限をかける。そのため、上記の基本機能の他に学生登録機能を実装する。

要件として、学生と対話する部分は、苦手意識をなくす工夫が必要であり、セキュリティ管理者が操作する部分は、大量の報告が来ると予想されるため、視認性を高めることが求められる。

4.2 システムの構成

本システムは 3 つの要素で構成される(図 4)。

学生インタフェース部：チャットツールとして、学生との対話によるコンテンツを提供する部分。学生インタフェース部では、学生が苦手意識を感じない媒体を採用することが求められる。LINE や Microsoft Teams、Slack などの候補があると考えている。本稿の試作では Slack API [4]を用いた Bot により実装した。Slack は大学機関で実際に導入された事例のある媒体であるため、試作として適していると考えた[5]。

データ管理部 : データの保存や取出しをする部分。API としてデータを独立させることで、各部の依存をなくすことができる。学生情報(学籍番号、名前)に、学生インタフェース部の媒体ごとのユーザ ID(以下媒体固有学生 ID と称する)を紐付けることで、複数の媒体の併用が可能となる。本稿の試作では、媒体が Slack であるため、媒体固有学生 ID は Slack の User ID となる。

管理者インタフェース部：セキュリティ管理者がデータ管理部の情報を閲覧することや、学生に提供するコンテンツを登録する部分。チャットツールでは、大量の情報に対する視認性を高めることは難しいため、UI を自由に決めることができる Web ページとして実装した。

本システムでは、マイクロサービスアーキテクチャ[6]を採用している。このアーキテクチャを用いることで、各部でのメンテナンス性、機能の拡張性を向上させることができる。また、各部の依存をできるだけ減らすことで、各部ごとに技術を自由に変更、拡張することができる。

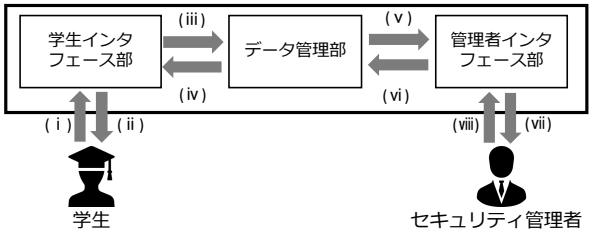

図 4 システム構成図

4.3 システムの各機能の処理

各機能の詳細な処理について説明する(図 4)。

4.3.1 学生登録機能

学生が学生インタフェース部に学生情報を送信する(ⅰ)。その情報に学生インタフェース部で媒体固有学生 ID を加え、データ管理部で保存する(ⅲ)。

4.3.2 リマインダ機能

リマインダ登録処理：セキュリティ管理者が管理者インタフェース部にリマインダ情報(タイトル、通知日時、送信する学生の学籍番号、本文)を送信する(ⅷ)。その情報をデータ管理部で保存する(ⅵ)。

リマインダ送信処理：登録されているリマインダ情報は、学生インタフェース部のポーリング処理によって監視されており(ⅳ)、リマインダの通知日時が来ると学生インタフェース部でリマインダとして送信する(ⅱ)。

4.3.3 報告機能

報告送信処理：学生が学生インタフェース部に報告する(ⅰ)。その報告を報告情報(報告内容、報告日時、対応済みフラグ、報告した学生の学籍番号)に加工して、データ管理部で保存する(ⅲ)。

報告提示処理：セキュリティ管理者が報告情報を見るときは、管理者インタフェース部が API によりデータ管理部から報告情報を取得して(ⅴ)、セキュリティ管理者に提示する(ⅶ)。

報告対応処理：セキュリティ管理者が管理者インタフェース部に、報告情報への対応を入力する(ⅷ)。その対応を報告対応情報(報告内容、報告した学生の学籍番号、対応内容、対応日時、送信フラグ)に加工して、データ管理部で保存する(ⅵ)。その報告対応情報は、学生インタフェース部のポーリング処理によって監視されており(ⅳ)、未送信の報告対応情報がある場合、学生インタフェース部で学生に送信する(ⅱ)。

4.3.4 シナリオ進行機能

シナリオ登録処理：セキュリティ管理者が管理者インタフェース部にシナリオ情報を送信する(ⅷ)。その情報をデータ管理部で保存する(ⅵ)。

シナリオ提供処理：学生が学生インタフェース部に対してシナリオを呼び出す行動をとったときに(ⅰ)、データ管理部からシナリオ情報を取り出し(ⅳ)、学生インタフェース部が学生にシナリオとして提供する(ⅱ)。

5 期待できる効果の考察

5.1 システムの継続利用に向けての課題

報告件数は長期的に増加しなければ意味がないため、本システムは、継続的に利用してもらう必要がある。そこで、利用者(学生とセキュリティ管理者)に、本システムを導入することで得られるメリットを伝えることが重要となる。メリットには、報告件数の増加によるものと本システムによるものがある。次節以降では学生とセキュリティ管理者の立場からこれらについて考察する。

5.2 学生のメリット

報告件数の増加によるメリットには、「セキュリティ管理者が公開する情報が増え、攻撃を回避できる可能性が上がる」、「セキュリティ管理者からの対応が受けられるため、被害の侵食を阻止することができる」の 2 つが考えられる。

本システムによるメリットには、「時間を気にせずに報告することができる」、「セキュリティ管理者からリマインダで情報が入ってくるため、自分で Web ページ等を利用してインシデント情報を収集する必要がなくなる」の 2 つが考えられる。

5.3 セキュリティ管理者のメリット

報告件数の増加によるメリットには、「保有する情報が増えることにより、被害が出る前に周知ができる」、「感染者を即座に見つけて対応することで被害の拡大を阻止することができる」、「報告を分析することにより、今後の訓練の方針を定めることができる」の 3 つが考えられる。

本システムによるメリットには、「自動返信を行うことでセキュリティ管理者の負担を軽減できる」、「学生に直接情報を伝えることができる」の 2 つが考えられる。

6 おわりに

本システムを用いることで、今まで実施されていなかった、セキュリティ報告の訓練を行うことができる。また、従来のメール訓練と本システムを組み合わせることで、より実践的な訓練となる。予め想定される報告をデータ管理部に登録しておくことで、エージェントが自動返信を行い訓練と実際の窓口としての併用が可能となる。

今後、「心理的障壁の除去」の評価で本システムの効果を確認したあと、「本システムの継続的利用」の評価で効果の持続を確認する。

参考文献

[1] 公立大学法人首都大学東京、“首都大学東京におけるパソコンのウイルス感染について”、https://www.tmu.ac.jp/extra/download.html?d=assets/files/download/auth/press/press_20191101.pdf、(参照日：2020/09/09).

[2] 総務省、“標的型攻撃への対策”、国民のための情報セキュリティサイト、https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/07.html、(参照日：2020/09/07).

[3] 独立行政法人情報処理推進機構(IPA)、“標的型攻撃メール訓練の目的と活用 ～効果を上げる方法～”、https://www.ipa.go.jp/files/000053336.pdf、(参照日：2020/09/07).

[4] Slack API、https://api.slack.com、(参照日：2020/09/07).

[5] 近畿大学、“全学用 Slack のサービス開始について”、https://kudos.kindai.ac.jp/cms/news_maintenance/3085、(参照日：2020/09/07).

[6] James Lewis、Martin Fowler、“Microservices”、https://martinfowler.com/articles/microservices.html、(参照日：2020/09/15).