

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評価  
Evaluation of a Dialogue Agent to Promote Reporting of Targeted Attacks

川田 大斗<sup>†</sup> 徳地 達哉<sup>†</sup> 難波 夏貴<sup>†</sup> 米谷 雄介<sup>†</sup> 後藤田 中<sup>†</sup> 大野 真伯<sup>†</sup>

山下 俊昭<sup>†</sup> 小野 滋己<sup>†</sup> 八重樫 理人<sup>†</sup> 藤本 憲市<sup>†</sup> 林 敏浩<sup>†</sup>

最所 圭三<sup>†</sup> 喜田 弘司<sup>†</sup>

Yamato Kawata Tatsuya Tokuchi Natsuki Namba Yusuke Kometani Naka Gotoda Masanori Ono  
Toshiaki Yamashita Sigemi Ono Rihito Yaegashi Kenichi Fujimoto Toshihiro Hayashi  
Keizo Saisho Koji Kida

## 1. はじめに

近年、標的型攻撃の高度化に伴い、標的型攻撃を対象とした防御策であっても、単一の対策では防ぎきれないケースが増えている。そのため、多層防御を用いて対策する必要がある。

大学では、セキュリティ管理者(以下、管理者)や教職員だけで組織内に標的型攻撃メールが入ってきているか把握することは難しい。そこで、情報源となる監視の目を増やすために学生の力を借り、不審なメールを発見した際には管理者へ報告するという、内部対策の層を増やすアプローチを提案、そのシステムを開発している[1]。本稿では、開発したシステムを実験とアンケートにより評価する。

## 2. 報告の課題

### 2.1 課題と目標値の設定

現在の本学では学生からの報告はほとんど来ていないため、学生の報告率が低い事を課題とした。本学の報告先である香川大学情報メディアセンターへのヒアリングにより、学生同士のコミュニティを 5 人としたとき、1 人報告すれば十分と考えていることがわかった。そこで、報告率の当面の目標値は 20%以上とした。

### 2.2 課題の原因

著者らは、報告を躊躇する心理的障壁が課題の原因であると考えた。本研究では 3 つの心理的障壁を定義する。障壁 1 は面識がない管理者に報告することに抵抗があることである。特にウイルスに感染していると気付かなければ、本当に標的型攻撃メールなのかがわからない。このような場合、無駄な作業をさせてしまうのではないかと不安が生じ、より難しい。障壁 2 は報告するときに誰に何を伝えれば良いかわからないことである。障壁 3 は報告する作業が面倒ということである。例えばメールでの報告の場合、件名と本文を考え、硬い文章を書かないといけないという手間がかかるイメージがある。

### 3. 報告を促す対話エージェントの開発

前記の 3 つの心理的障壁を除去し、報告率を上昇させるために「対話エージェント」「リマインダ」「チャットツール」の機能を有するシステム[1]を提案・開発した(以下、本システム)。対話エージェントが学生と管理者の間に入

ることで障壁 1 を軽減し、自発的に報告できるようにする。リマインダは報告を促すメッセージで、誰に何を報告すべきかを伝えることで障壁 2 を軽減する。チャットツールはメールと比べて件名や本文のような決まった項目が無く、気軽に文章を送信することができ、障壁 3 を軽減する。

本システムはチャットツール Slack 上で動作する。ユーザは学生であり、管理者が設定したリマインダは、事前に指定された時間にエージェントを介して学生へ送信される(図 1 左側)。学生は本文を見て必要な情報を把握し、下の報告ボタンを押すと報告画面へ遷移して手間をかけずに報告ができる(図 1 右側)。報告画面はタイトルと本文が入力可能で、タイトルが空白の場合は本文の先頭となる。

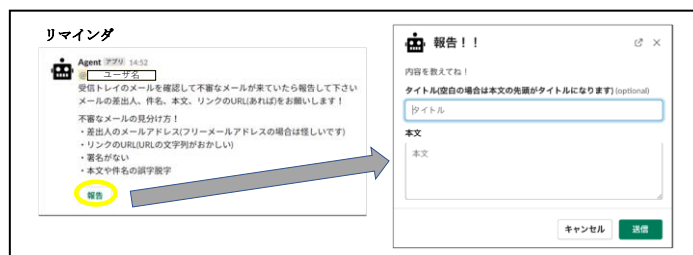


図 1 リマインダから報告画面へ

## 4. 評価実験

### 4.1 目的

本システムを利用することで、2.1 節の目標値が達成できるかを確認する。しかし、評価実験では期間が定められている点、実験用メールが送信されることがわかっている点から、実際の環境より報告率が高くなると予想される。そこで、目標値を「報告率 40%以上」とし、検証する。また、3 章で述べた「心理的障壁を除去することで報告率が上昇する」という仮説が正しいか検証する。

### 4.2 方法

評価実験は 2021 年 1 月 12 日～2021 年 1 月 25 日の 2 週間、香川大学の学生 20 名を対象に実施した。今回は、学生側の評価であるため、管理者役は著者らが担当した。メールでの報告(以下、従来手法)と比較するため、従来手法による報告と、本システムによる報告を 1 週間ずつ行った。その際、前の手法が次の手法に影響を与えることを考慮し、表 1 に示すグループに分け、報告手法の順番を入れ替えた。

<sup>†</sup>香川大学 Kagawa University

表1 被験者のグループ

期間	グループ1	グループ2
第1週(1月12日～1月18日)	従来手法	本システム
第2週(1月19日～1月25日)	本システム	従来手法

評価実験の流れは、被験者に評価実験資料を配布し、期間中に図2のような実験用メールを1週に2通送信した。資料では、実際の環境に近づくために研究の背景や目的は述べず、不審なメールの報告依頼と、本システムの使用方法を記載した。また、本システムでは1日に1度、図1で示したリマインダを送信した。評価実験終了後に、心理的障壁を除去できたか確認するため、アンケートを行った。

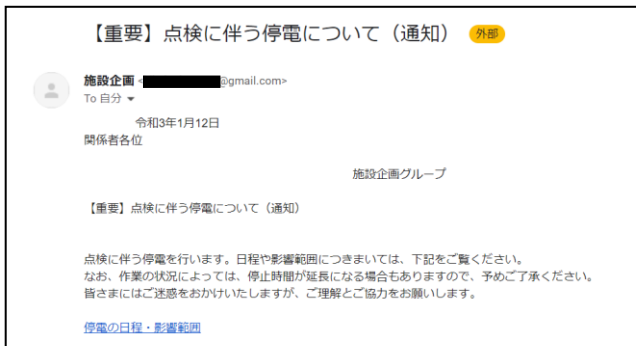


図2 実験用メールの例

### 4.3 結果

#### 4.3.1 報告率

報告率はグループ・報告手法ごとに、送信した実験用メール数と被験者の人数の2つの観点で集計する。実験用メール以外の報告は割合の計算の際には除外した。

本システムは、目標値40%以上を全ての集計で達成した。グループ1について、表2及び表3共に本システムが従来手法の2倍以上となっている。グループ2について、表2では従来手法が本システムを上回っている。

表2 送信した実験用メール数に対する報告率

	従来手法	本システム
グループ1	20%	45%
グループ2	50%	40%

表3 被験者の人数に対する報告率

	従来手法	本システム
グループ1	30%	60%
グループ2	60%	70%

#### 4.3.2 心理的障壁

質問1は「報告するときに言いづらさや抵抗感を感じないと思いますか」、質問2は「報告したときに感じたことはありませんか」である。

図3は、質問1を従来手法と本システムで分けて、5段階で集計した結果である。本システムの方が、障壁1にあたる抵抗感が少なくなっている。

表4は、質問2を従来手法と本システムで分けて、複数選択可能で集計した結果である。障壁2や障壁3に該当する選択肢は、本システムの方が感じた人が少ない。報告しなかった理由も同様に集計したが、迷惑メールに入っていたという回答が過半数であった。

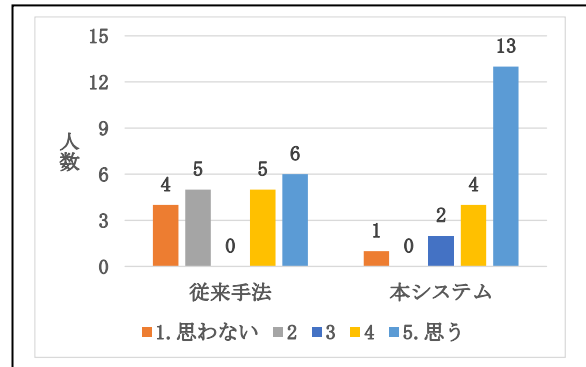


図3 質問1の結果

表4 質問2の結果

選択肢	従来手法	本システム
文章を作成する作業に面倒さを感じた	5件(36%)	1件(7%)
正式なフォーマットを検討しなければいけない作業に面倒さを感じた	5件(36%)	2件(14%)
メールが本当に実験用メールなのかわからず不安であった	3件(21%)	3件(21%)
報告する内容がわからなかった	3件(21%)	0件(0%)
リンクをクリックしてしまったことに対して後ろめたさがあった	0件(0%)	0件(0%)
迷惑メールに入っていた	9件(64%)	10件(71%)
特になし	3件(21%)	1件(7%)
その他	1件(7%)	1件(7%)

## 5. 考察

### 5.1 報告率について

表2及び表3のグループ1から、本システムの導入によって報告率が上昇する効果が十分に得られると考える。

グループ2の従来手法での報告率が表2のようになった要因として、第1週に本システムによる報告を行っていた影響が、第2週に出ている可能性がある。しかし、リマインダの効果は時間が経つと薄まるのが予想されるため、本システムは一時的な利用ではなく、本学の報告体制として継続して利用すべきだと考える。

### 5.2 心理的障壁について

図3から障壁1、表4から障壁2及び障壁3が、本システムによって除去できていると考える。

報告率とアンケート結果から、心理的障壁を除去することで報告率が上昇するという仮説は正しいと結論づけた。

#### 参考文献

- [1] 徳地 達哉, 池尻 圭佑, 塩田 智基, 米谷 雄介, 後藤田 中, 大野 真伯, 山下 俊昭, 小野 滋己, 八重樫 理人, 藤本 憲市, 林 敏浩, 今井 慈郎, 最所 圭三, 喜田 弘司, “標的型攻撃に対する報告を確実にする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”, 大学ICT推進協議会 2020年度年次大会論文集, WP-2, pp.459-462 (2020).