Vol.2019-SPT-32 No.22
2019/3/8

従業員に対する安全な SNS の利用方法についての教育用ゲームの効果検証

萩谷 文[†1] 稲葉 緑[†1]

概要：従業員が個人的に利用するソーシャルネットワーキングサービス（SNS）で公開した情報が、企業・組織へのセキュリティ攻撃に活用される危険性が提示されている。このような危険性に対して企業・組織が取り得る対策の 1 つとして、従業員に対する SNS の安全な利用方法の教育が挙げられる。また、具体的な利用方法を教えることに加え、従業員の安全な SNS を利用しようとする意識を高めることが必要であると推察された。我々は今回、この教育に活用するプログラムを試作した。SNS の利用方法に関する既存の解説書から学習内容を選定し、その内容をゲーム形式で表現した。本研究では、学習内容をテキスト形式で学んだ条件と、ゲーム形式で学んだ条件とで SNS の利用に対する意識の変容に違いがみられるか比較した。実験の結果から、ゲーム形式で学んだ条件の方がテキスト形式学んだ条件に比べ、安全な SNS 利用に対する意識が高まることを示した。

キーワード：情報セキュリティ意識、企業内教育、ゲーム、SNS

Study on effects of the serious game to learn how to use SNS safely for employees

AYA HAGIYA[†1] MIDORI INABA[†1]

Abstract: Information that employees post in their private use of SNS (social networking service) has been reported to be risks for security attacks against corporations or organizations. One of the measurements against these risks would be the education of the employees about how to use SNS safely. However, it has shown that many employees are reluctant to learn security and that their information security awareness are considerably low. Therefore, we developed the serious game to teach proper usage of SNS with fun and to increase their information security awareness. The learning contents were selected from the textbook about safe usage of SNS, such as what information is safe to share and how to select their privacy setting. We created the serious game to learn the same contents. The aim of this study is to find out facilitating effects of the serious game on the information security awareness about safe use of the SNS. We performed an experiment to compare these effects in learning between using the textbook and the serious game. Results showed that the learning using the serious game more increased the information security awareness than that using the textbook.

Keywords: Information security awareness, Corporate education, Serious game, SNS

1. はじめに

企業、組織が実施する情報セキュリティ対策の 1 つに、従業員に対する教育がある。従業員の行動に潜む脆弱性を狙うサイバー攻撃から組織のシステムを守るためには、従業員一人ひとりの情報セキュリティに資する行動（以下、「情報セキュリティ行動」と言う）が必要である。ただし、情報セキュリティ担当者が、従業員一人ひとりの行動を統制することは不可能である。そこで組織は、教育によって従業員の情報セキュリティ行動に対する意識を高めることを目指す。

しかし、情報セキュリティについて学ぶことは困難であるとのイメージが持たれているとの報告がある。このようなイメージが情報セキュリティに関する学習を妨げる可能性を打破するため、ゲーム形式を導入した教育プログラムが開発されている[1, 2, 3, 4, 5]。例えば、会田ら[3]はセキュリティ双六「セキュろく」を提案した。エンターテイメント性の高いボードゲームで、「ウイルス感染」「フィッシング詐欺」に遭遇した際の初動などについて学ぶことを主とする。彼らは教育プログラムにゲーム形式を導入したことで、従業員らが楽しんで取り組むことを可能とし、苦手意識の払拭に効果があったと示した。また、藤田ら[1]は、楽しみながら強度の高いパスワードを覚えさせる事を目的として、ゲーム形式でのコンテンツを提案している。「クリアしたい」「高得点をとりたい」という意欲を、高い情報セキュリティタスクの達成に変換し、ユーザが日常生活においてゲームで遊んでいるうちに、強度の高いパスワードの記憶を促進する結果を報告した。

このように従業員の積極的な情報セキュリティに対する学びを促すゲーム形式の教育プログラムが提案されてきた中で、解決されていない課題もある。従業員らは、情報セキュリティ対策は情報システム担当者が実施すればよいと考え、積極的に情報セキュリティ行動をとらない場合が

†1 情報セキュリティ大学院大学
Graduate School of Information Security INSTITUTE of Information Security

あることが指摘されている[7, 8, 9, 10]。このような従業員に情報セキュリティ行動を実行させるためには、「自分が情報セキュリティ対策に取り組まなくてはならない」との従業員の認識（以下、「自分事認識」と言う）を喚起することが重要であると考えられる。提案されたゲームや漫画を使った教育プログラムには、情報セキュリティに関する知識を習得するほかに、自分事認識を高めることを目的としてディスカッションが含まれている例がある[3, 4]。有効性が期待される一方、自分事認識を喚起するには不十分である側面もあると推測される。例えば、第一に、集合的なディスカッション形式によるアプローチでは、客観的な事象の理解を促進しても、自分自身がその被害に遭遇することを認識できない心理（否認）[10]を解消することは難しい。この否認を減少させるためには他者との知識の共有とは別に、自分の行動を振り返り、見つめ直す機会を提供する必要があると考えられる。第二に、被害者目線での脅威体験や、情報セキュリティインシデント対応シナリオ体験によるアプローチでは、従業員自身の行動が脅威を誘発する要因となり、インシデントに繋がる可能性を実感させることは難しいという点である。

著者らは、これらの問題点を解消し、自分事認識を喚起させる工夫として、攻撃者目線で客観的に自分自身を捉え直させる視点に着目した。また、この視点を学習者に対して容易に提示するために、ゲーム形式を採用した。このような教育プログラムは、萩谷・稲葉[11]でも報告している。この際、従業員への情報セキュリティ教育に携わる教育担当者へインタビューを実施し、ニーズの高い教育内容を複数選定した。その中から「適切なパスワード利用」を選んで教育プログラムを作成し、検討した。この研究を展開し、今回は、ニーズの高い教育内容の一つとして挙げられた「SNS への適切な情報投稿およびセキュリティ設定」を取り上げる。

以上のように本研究では、SNS への投稿およびセキュリティ設定について、上述した攻撃者目線を従業員に提供するゲーム形式の教育プログラムを作成した。また、その自分事認識を高める効果について、テキスト形式の教育プログラムと比較した。

2. 教育プログラムの設計・作成

2.1 教育内容

既に多くの企業や組織において、SNS へ業務情報や個人の特定が可能となる情報を投稿してはいけないという内容の情報セキュリティ研修が実施され、従業員らは、SNS へ企業や組織に関する情報や、自分自身の個人情報を投稿することに注意を払っている[12]。しかし、実際にはセキュリティ設定の操作方法に不明点があるまま利用していたり、自分の意図しない文脈や写真から、意図しない情報開示が行われていたりする実態が指摘されている[13]。「SNS への業務情報投稿」という非セキュリティ行動に対して教育する内容は、SNS のセキュリティ設定に関する知識と、注意を払うべき SNS への投稿内容に関する知識とする。

2.2 教育用テキストプログラム

SNS に関する教育用テキストでは、TrendMicro 社から提供されている教育用サイト[14, 15, 16]より、前節にて選定した教育内容に該当する知識項目を抜粋し、テキストにまとめた。取り組みやすさを損なわないように、早くとも 5 分程度、じっくり読めば 10 分程度の量となるように調整した。表記は文字のみで、絵や図はない。内容は以下のとおりである。

1） SNS で不用意な仕事の話は控えよう
・業務上知り得た知識を明かす
・取引先との懇親会や、社内行事、業務行動の写真を勝手に公開する
2） 安全なネット利用の心得
・ネットで安易に個人情報を公開しない
・セキュリティ設定に細心の注意を払う
・発信前に内容を見直す

2.3 教育用ゲームプログラム

プログラムはα）ゲームフェーズとβ）解説フェーズから構成される。易しいストーリーに沿って教育内容を学べるよう、アンデルセン童話「雪の女王」をベースとしたゲームおよび解説を作成した。テキストプログラムと同様、全編通して 10 分程度の所要時間となるように設計した。

α）ゲームフェーズでのおおよそのストーリーは下のとおりである。

・登場人物は、雪の女王、男の子、男の子と仲良しの女の子である。男の子はスマートフォンおよび SNS を使っていた。
・雪の女王は男の子をさらい、男の子のそれまでの記憶を消してしまう。
・雪の女王はおもちゃ代わりに新しいスマートフォンを男の子に与えた。また、限られた内容のみ投稿することを条件に、新しい SNS アカウントを作ることを許可した。

ここから女の子は、いなくなった男の子を探し始める。学習者（従業員）は、女の子の立場を追体験する。
・女の子は、あるきっかけで、男の子のものらしいアカウントを特定し（図 1）、フォローすることで追跡を開始する。
・そのアカウントへの投稿内容（メッセージや写真など）から、女の子は様々な場所を訪ねたり人々に話を聞いたりして、男の子の居場所に関する証拠を積み上げていく。
・証拠に基づき、女の子は男の子の居場所を探し当て、助ける。

β）解説フェーズでは、女の子が男の子に対し、なぜ彼を雪の女王から助けることができたのかについて解説する

（図 2)。男の子の投稿ひとつひとつを取り上げ、①なぜ男の子のアカウントであると特定できたのか、②追跡する際

図 1　ゲーム画面例（男の子の投稿）

Figure 1　Example of the page of the game (Boy's tweet).

図 2　ゲーム画面例（解説画面）

Figure 2　Example of the page of the game (Explanation).

は、投稿内容の文脈、写真のどの部分に注目したのか、③どういったセキュリティ設定が脆弱であり、どういった設定であれば有効であったのか、の 3 点を示した。

3. 評価

3.1 目的

提案手法のゲーム形式での教育プログラムと、統制条件として用意したテキスト形式での教育プログラムにて、同じ教育内容をそれぞれ表現し、実験協力者らに実施させた。情報セキュリティ意識の中の、自分事認識にアプローチするためには、ゲーム形式のもつメリットが有効に作用するのではないかと仮定する。情報セキュリティ意識の向上を評価するために「情報セキュリティ意識アンケート」と「危険性認識テスト」を用意した。ゲーム形式、あるいはテキスト形式によって、教育プログラム実施前後の差分にどのような違いがあるのか確認することを目的とする。

3.2 方法

実験協力者は人材派遣会社を通して募集した 20 代から 50 代の男女 34 名である。1)企業または組織に勤めている方であること、2)Twitter あるいは Facebook アカウントを持っていることの 2 点を参加条件として提示した。協力を得た 34 名を年齢、男女比についても均等になるように配慮しつつ、17 名ずつ 2 グループに割り当てた。1 つのグループにはテキストで、もう 1 つのグループにはゲームによって SNS に関するプログラム学習を求めた。

実験全体の冒頭にて、（1）SNS の利用状況アンケート、および、（2）情報セキュリティ意識アンケートを実施した。その後、（3）SNS 危険性認識テストを実施した。このテストに続いて、学習プログラムに取り組んでもらった。最後に、再度（3）のテスト、（4）プログラムに関するアンケートを実施した。

（1）利用状況アンケート

このアンケートでは、実験協力者が現在どのように SNS アカウントを管理しているのか、日常的に困っていると感じることはないかを調べるために全員に対して行った。

①お使いの SNS は Twitter と Facebook のどちらですか？
②①の SNS をおおよそいつから使い始めましたか？
③①の SNS を現在、どのくらいの頻度で起動させますか？
④①の SNS を現在、どのくらいの頻度で自分から情報を投稿していますか？
⑤全部でいくつ SNS アカウントを持っていますか？
⑥SNS を使われている目的は何ですか？
⑦SNS を使うにあたって困っていることはありますか？「ある」を選んだ方は、どういった内容で困っていますか？
⑧SNS にはどのような内容を投稿されていますか？
⑨ご自身の現在使われているアカウントで、誰が SNS に載せた内容を見られるようになっているのか知っていますか？

（2）情報セキュリティ意識アンケート

質問項目は、5 分類、全 11 項目にて作成した。

A. 情報セキュリティに関する認識を確認する質問
①情報セキュリティとは何か知っていますか。
②あなたが普段行っている情報セキュリティのための行動を教えてください。
③情報セキュリティのための行動は、すべての人が自分自身で行う必要があると思いますか？上記でそう思った理由を自由に書いてください。
④情報セキュリティに関する事故やトラブルについて知っていますか？「知っている」を選んだ方は、例えばどういった内容でしょうか。
⑤ご自身の会社にはセキュリティに関する規定やポリシー、ルールがありますか？「ある」を選んだからは、その内容について知っていますか？

B. 情報セキュリティ教育の必要性を確認する質問
⑥情報セキュリティについての知識を持つことは必要だと思いますか？

C. 情報セキュリティ教育における意識の有効性を確認する質問
⑦情報セキュリティについての知識を持つことができれば、

情報セキュリティのための行動をしたくなると思いますか？上記でそう思った理由を自由に書いてください。

D. 情報セキュリティ教育の完全性を確認する質問

⑧情報セキュリティの知識を持つことで（④番の）トラブルは無くなると思いますか？上記でそう思った理由を自由に書いてください。

E. 情報セキュリティ教育よりも技術の有意性を確認する質問

⑨十分なセキュリティ技術があれば、ご自身が情報セキュリティについて知る必要はないと思いますか？

⑩インターネットプロバイダ（NTT,docomo,au,ソフトバンクなど）が十分に情報セキュリティのための対策をすれば、ご自身が情報セキュリティについて知る必要はないと思いますか？

⑪会社や組織の情報セキュリティ担当者が十分に情報セキュリティのための対策をすれば、ご自身が情報セキュリティについて知る必要はないと思いますか？

（3）SNS 危険性認識テスト

SNS 危険性認識テストは、教育プログラム実施前後に実施した。様々な場面における SNS 投稿を 5 種類見せ、それぞれ安全かどうかを 5 点評価法（1,とても安全である、2,まあまあ安全である、3,どちらともいえない、4,あまり安全ではない、5,安全ではない）で回答させた。各問は、下のメッセージと図 3 にある写真とが組み合わされている。

①「取引先で出していただいたお茶菓子が、本当においしかった！ありがとうございます。」

この問は、安全な SNS 投稿とした。教育内容では「業務上知り得た知識の公開は控える」「写真に含まれる情報にも注意を払う」といった知識が提示されているが、この投稿はそのどれにも該当しない。より「安全である」と回答した場合、危険性の認識が高いことを示す。

②「年末になると、やっぱり忙しいですね。今日はまだまだ残業です。愛用のタンブラーで、ほっと一息。」

この問は、教育内容のうち、注意を払うべき「意図しない情報開示」に分類されるものである。「写真に含まれる情報」の中に業務情報と思われる設計図が載っている。より「安全ではない」と回答した場合、危険性の認識が高いことを示す。

③「今日も一日中、係長の怒鳴り声。会議に 5 分遅刻した社員に対して、30 分以上説教していました。こんな会社だってわかっていたら入社しなかったのに。早く転職したいです。」（写真無し）

この問は、教育内容のうち、注意を払うべき「一社会人として控えるべき仕事の自慢、愚痴」に分類されるものである。より「安全ではない」と回答した場合、危険性の認識が高いことを示す。

④「なんと！私はついに大きな仕事をします！会社が水面下で交渉を続けてきていた､マレーシアでの水道整備事業をたった今当社が落札！私は来月から視察も兼ねてマレーシア駐在です。マレーシアに詳しい人、ぜひいろいろ教えてください。特に、ごはん事情とゴルフ事情をお願いします！」

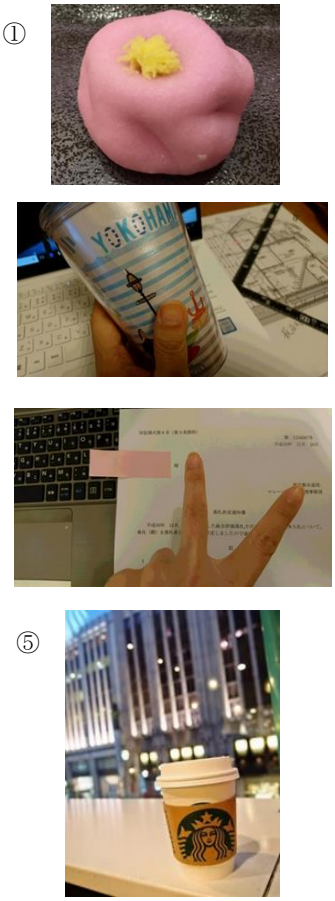

図 3　SNS 危険性認識テストに使用した写真

Figure 3　Pictures used in the SNS risk recognition test

この問は、SNS 教育内容のうち、「業務上知り得た知識を明かす」という望ましくない行動に分類されるものである。より「安全ではない」と回答した場合、危険性の認識が高いことを示す。

⑤「山手線が全線運休！新宿で足止めです。復旧まであと 1 時間とは…。仕方がないので、お茶をして待ちます。（仕事もしてるよ！）」

この問は、教育内容のうち、「写真情報、文脈から今あなたのいる場所が推測できる可能性がある」に分類されるものである。より「安全ではない」と回答した場合、危険性の認識が高いことを示す。

（4）プログラムアンケート

プログラムに関するアンケートは全 10 問から構成される。ゲーム形式の教育プログラムとテキスト形式の教育プログラムにて主語を変えて作問したが、質問内容に差はない。

①ストーリーは分かりやすかったですか？
②このゲーム／テキストは楽しかったですか？
③このゲーム／テキストで、なぜ SNS に安易に個人情報を載せてはいけないのか、わかりやすく理解することができましたか？
④このゲーム／テキストで、なぜ SNS のセキュリティ設定に注意を払わなくてはならないのか、わかりやすく理解することができましたか？
⑤このゲーム／テキストを身近な人に薦めたいと思いますか？
⑥あなたはこのゲーム／テキストを通じて、ご自分の SNS のセキュリティ設定が安全かどうか考えましたか？
⑦あなたはこのゲーム／テキストを通じて、ご自分の SNS のアップ内容を見直そうと思いましたか？
⑧あなたはこのゲーム／テキストを通じて、ご自分の SNS のセキュリティ設定を見直そうと思いましたか？
⑨今後、安全な SNS についてもっと知りたいという気持ちになりましたか？
⑩その他、お気づきの点、こうしたほうが良いのではという点がありましたら、自由に書いてください。

4. 結果

本稿では、プログラムアンケートの回答結果の一部について報告する。各問における評価をゲーム形式とテキスト形式とで比較した。使用した分析方法はマンホイットニー法である。③『このゲーム／テキストで、なぜ SNS に個人情報を載せてはいけないのか、わかりやすく理解することができましたか』、④『このゲーム／テキストで、なぜ SNS のセキュリティ設定に注意を払わなくてはならないのか、わかりやすく理解することができましたか』の問では、ゲーム形式の方が、テキスト形式よりも「理解できた」と回答される傾向が確認された(③図 4, 有意, p<0.005, ④図 5, 有意傾向, p=0.064)。次に、⑦『あなたはこのゲーム／テキストを通じて、ご自分の SNS のアップ内容を見直そうと思いましたか？』、⑧『あなたはこのゲーム／テキストを通じて、ご自分の SNS のセキュリティ設定を見直そうと思いましたか？』の問に対する回答結果について示す（それぞれ図 6, 7)。⑦の質問への回答では、ゲーム形式、テキスト形式の間に回答傾向の差は認められなかった。⑧については、テキスト形式よりもゲーム形式で「見直そうと思う」という回答傾向が強くみられた(有意, p<0.05)。

5. 考察

はじめに、『自分の SNS セキュリティ設定をみなおすか』の問において、ゲーム学習者の方がテキスト学習者より「そう思う」と回答した傾向が強くみられた点について考察する。利用状況アンケートにて、『SNS について困っていることはないか』という問に対し、「困っている」と回答した

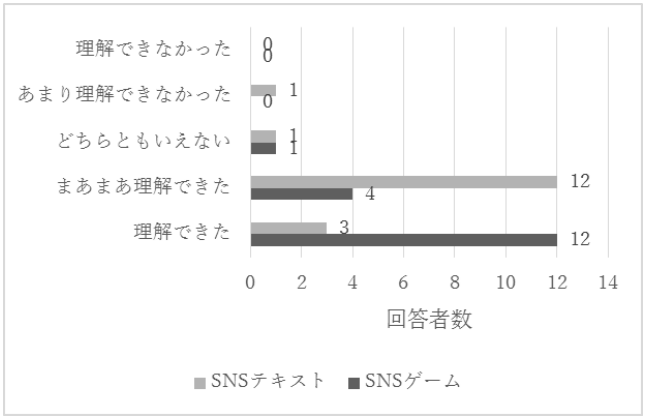

図 4　問③に対する回答
Figure 4　Responses to Q③

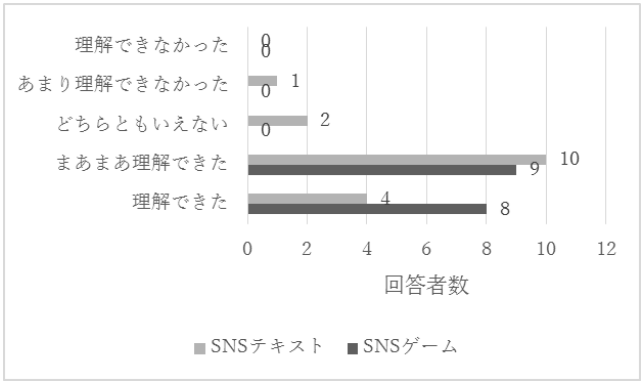

図 5　問④に対する回答
Figure 5　Responses to Q④

実験協力者の約半数が、SNS のセキュリティ設定について「困っている」と回答した。実験協力者らは、SNS のセキュリティ設定について「知りたい」と思っていたと解釈することができる。このような教育ニーズのある状態で、ゲーム学習とテキスト学習とを実施させた場合、テキスト学習よりもゲーム学習の方が、教育ニーズに応えることができたと解釈することができる。

次に、『なぜ SNS に安易に個人情報を載せてはいけないのか、わかりやすく理解することができましたか？』という問では、ゲーム学習者の方がテキスト学習者より有意に「理解できた」と回答した。利用状況アンケートから、SNS への投稿内容については、実験協力者らの間で日頃から注意が払われていた可能性がある。そのため、実験協力者らにとって、「なぜ安易に個人情報をアップしてはいけないのか」というトピックは大変興味深い項目であったと推測することができる。中でも「理解できた」とはっきり述べた回答に関しては、テキスト学習者では 2 割であるに対し、ゲーム学習者では 7 割に達する。また、テキスト学習者で「理解できた」と答えた 2 割の内、「自分の SNS アップ内容を見直すか？」で「そう思う」とはっきり回答したのは 2 割であり、一方、ゲーム学習者では先の質問で「理解できた」と答えた 7 割の内、「自分の SNS アップ内容を見直

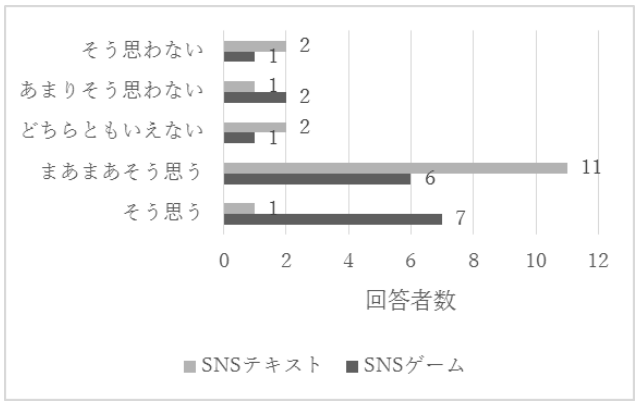

図 6　問⑦に対する回答
Figure 6　Responses to Q⑦

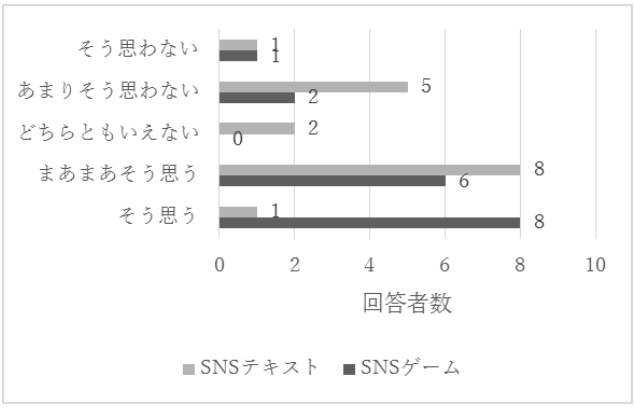

図 7　問⑧に対する回答
Figure 7　Responses to Q⑧

すか？」で「そう思う」とした回答は半数であった。

以上から、次のように考察する。まず、『個人情報を SNS に投稿してはならないということをわかりやすく理解できたか』の問において、ゲーム学習の方がテキスト学習より学習効果が出ている。さらに「個人情報を安易にアップしてはいけない」という理解した内容について、「SNS アップ内容を見直そうと思う」と、行動につなげる意図を示した実験協力者も、ゲーム学習者の方がテキスト学習者より高い割合を示した。実験協力者らは、ゲームでは、具体的なストーリー・文脈の中で危険な投稿内容、思い込みによるセキュリティ設定誤りなどの学びを得たと推測することができる。また、攻撃者の目線で、異なるアカウントからの SNS 投稿内容、異なる日付の SNS 投稿内容といったバラバラな情報を手繰り寄せ、つなぎ合わせて投稿している人物像をあぶりだし、その行動を予測するという疑似体験の機会を得た。これまでの自身の日常では思いもよらなかった攻撃者の存在を認識し、警戒心が高まった可能性がある。警戒心は、セキュリティ行動を促す重要な動機となることが期待できる。

なお、SPT 学会発表当日は、上述した以外の実験結果についても報告する。

参考文献

[1] 藤田真浩、山田眞子、西垣正勝　エンターテイメントを活用したセキュリティ強化：パスワード強化を組み込んだゲームの実装とその有効性　2016 年　情報処理学会論文誌 57 巻 12 号 pp.2711-2722
[2] 服部夢二、高田哲司　安全な秘密情報利用の動機付けを目的とした個人認証のゲーム化　2018 年　情報処理学会研究報告マルチメディア通信と分散処理(DPS) 2018-DPS-174 巻 15 号 pp.1-7
[3] 会田和弘　セキュろくキッズ～双六を用いた情報セキュリティ教育の試み　2014 年 関西学院大学リポジトリ　総合政策研究 pp.89-94
[4] Raghu Raman, Athira Lal, Krishnashree Achuthan　Serious Games based approach to cyber security concept learning : Indian context 2014 年 International conference on Green Computing Communication and Electrical Engineering(ICGCCEE)
[5] 山田眞子、藤田真浩、有村汐里、池谷勇樹、西垣正勝　エンターテイメントを活用したセキュリティ強化：ユーザ認証の強化を導くルーチンのゲームへの埋め込み　2014 年　コンピュータセキュリティシンポジウム 2014 論文集　2014 巻 2 号 pp.1230-1237
[6] 畑島隆、坂本泰久　情報セキュリティ不安全行動に対するテレワーク実施者の性向の分析　2017 年　情報処理学会論文誌 58 巻 12 号 pp.1912-1925
[7] 大友章司、意志があるのに実行しない心理～リスクを高める潜在的動機～ 2009 年　IPA 情報セキュリティと行動科学研究会
[8] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, Cate Jerram Determining employee awareness using the Human Aspects of Information Security Quetionnaire(HAIS-Q) 2014 年 Computer & Security Volume 42 pp.165-176
[9] 内田勝也、矢竹清一郎、森貴男、山口健太郎、東華枝　情報セキュリティ心理学の提案　2007 年　情報処理学会研究報告コンピュータセキュリティ(CSEC)2007 巻 16 号 pp.327-331
[10] 広田すみれ、増田真也、坂上貴之（編著）　心理学が描くリスクの世界　2008 年　慶應義塾大学出版会
[11] 萩谷　文、稲葉　緑　情報セキュリティ意識向上を目的とした企業内教育用ゲームの検討 ―パスワード強化を例に―　情報処理学会研究報告セキュリティ心理学とトラスト（SPT）2018-SPT-31 巻　12 号　pp.1-6
[12] 三上俊治　SNS における自己開示とプライバシー・パラドックス　2015 年　東洋大学社会学部紀要　53 巻 1 号 pp.65-77
[13] 太幡直也、佐藤広英　SNS 上での自己情報公開を規定する心理的要因　2016 年　パーソナリティ心理学会 25 巻 1 号 pp.26-34
[14] トレンドマイクロ「SNS で仕事がらみの投稿は慎重に」https://www.is702.jp/manga/1905/partner/12_t/ (2016/2/25 更新 2018/12/04 参照)
[15] トレンドマイクロ「ネットのコミュニケーションを安全に楽しむための「3 つの心得」（抜粋）https://www.is702.jp/special/2175/partner/12_t/（2017/7/20 更新 2018/12/04 参照）
[16] トレンドマイクロ「SNS からの情報漏えいを防ぐ 7 つのちぇっくぽいんと」（抜粋）https://www.is702.jp/special/3331/partner/12_t/　（2018/6/21 更新　2018/12/04 参照）