4F-02

ソーシャルエンジニアリング攻撃に対応する情報セキュリティ行動への誘導手法の検討

今田　寛†　　大坐畠　智‡　　山本　嶺‡　　加藤　聰彦‡

電気通信大学†‡

1. 背景

ソーシャルエンジニアリングとは、社会の仕組みや人間関係を操り、悪用する技術のことであり、人間は情報セキュリティの最も弱い部分であると言われている [1]。フィッシング攻撃は、信頼できる会社や団体・個人などになりすますことで、ユーザから情報を詐取しようとする攻撃であり、人間の弱点を利用したソーシャルエンジニアリングの一種である。APWG の調査によれば、2019 年第 3 四半期に APWG が検出したフィッシングサイトの総数は 266,387 で、第 2 四半期の 182,465 から 46%増加しており、2016 年後半以降最も高いレベルとなっている [2]。

情報セキュリティにおいて、フィッシング攻撃など人間の選択や行動によって引き起こされる問題は人間的要素と呼ばれる。人間的要素における対策は、必要な場面で実際に望ましい選択や行動しなければ効果はない。そこでユーザに対し、望ましい選択や行動をするよう促す方法が検討されている。望ましい選択や行動をするよう促す方法として、防護動機理論を用いた情報セキュリティ行動の動機付けや、ナッジ理論を用いてより良い選択や行動を強制せず自発的に行うよう促す方法などが検討されている [3]。

恐ろしい、退屈だ、といったセキュリティに関する否定的な感情が効果を低下させているという報告 [4]があることから、場面によっては恐怖喚起により動機付けを行う防護動機理論の応用では逆効果となる場合が存在する可能性が考えられる。

ナッジを長期的に使用すると、選択をナッジに頼るようになり、プライバシーとセキュリティの価値に対する認識を低下させ、ナッジのない新しい脅威を過小評価する可能性が指摘されている [5] [6]。これより、望ましい選択や行動を促す手法の適した場面の検討及び場面に適した新たな手法の検討が必要だと考えられる。

本研究では、フィッシング攻撃をはじめとした情報機器が関連するソーシャルエンジニアリング攻撃への対策としての望ましい選択や行動を促す手法の適した場面の検討及び場面に適した新たな手法の検討を行う。

2. 関連研究

2.1. 防護動機理論

深田 [7]によれば、脅威アピールとは、脅威(threat)の危険性を強調して受け手を脅すことによって、その脅威に対処するための特定の対処行動(coping behavior)の勧告(recommendation)に対する受け手の受容を促進させようと意図された説得的コミュニケーションのことである。防護動機理論は脅威アピールに分類される。

Rogers [8]によれば、脅威アピールには（a）イベントの有害性の大きさ。（b）適応行動が実行されない場合、または既存の行動の性質に変更がない場合に、イベントが発生する条件付き確率。（c）有害な刺激を軽減または除去する可能性のある対処応答の可用性と有効性。の 3 つの重要な刺激変数があるとしている。

2.2. ナッジ

Richard ら [9] [10]は、行動経済学の応用として、強制することなく自発的に望ましい選択をする

Inducing information security behavior for social engineering attack
†IMADA Hiroshi The University of Electro-Communications
‡OHZAHATA Satoshi The University of Electro-Communications
‡YAMAMOTO Ryo The University of Electro-Communications
‡KATO Toshihiko The University of Electro-Communications

ように促す「ナッジ」という理論を提案した。「ナッジ」とは、注意や合図のために人の横腹を特にひじでやさしく押したり、軽く突いたりする [10]ものであり、選択を禁じることも、経済的なインセンティブを大きく変えることもなく、人々の行動を予測可能な形で変える選択アーキテクチャーのあらゆる要素 [10]のことである。

2.3. 防護動機理論とナッジの統合

Briggs ら [3]は防護動機理論とナッジの統合について言及している。Bavel ら [11]はナッジに防護動機理論を適用することを試みている。実験では、高い効果が得られている一方で、防護動機理論による脅威アピールを用いた場合に実験を完了しないドロップアウトが脅威アピールを用いた場合において最も多いという結果になっている。

3. 提案方式

防護動機理論による脅威アピールは高い効果が得られる一方、ユーザの感情に配慮する必要があると考えられる。また、ナッジは選択を禁じることも、経済的なインセンティブを大きく変えることもなく、人々の行動を予測可能な形で変えることができる一方で、新しい脅威を過小評価する可能性が考えられていることから、場面によって逆効果となる可能性が考えられる。情報セキュリティ行動が要求される場面において、感情を考慮して適切な手法を使い分けることにより、効果を向上させることができると考えられる。場面に応じたユーザの感情を考慮するためには、場面ごとのユーザの感情と行動について調査する必要がある。

本研究では、情報システムを使用するユーザの感情および行動について調査し、場面ごとに適した情報セキュリティ行動への誘導手法を検討する。コンピュータ使用時の表示内容および操作履歴の記録を行う実験を実施する。実験の結果からセキュリティに関する行動が増減する原因について分析し、望ましい選択や行動を促す手法の適した場面の検討及び場面に適した新たな手法の検討を行う。

4. 今後の予定

セキュリティおよびフィッシング攻撃に関する知識・認識・その対策ツールに関するアンケート調査を行う。アンケートの結果からユーザの属性・知識・習熟度ごとの選択や行動の傾向を分析し、実験の方針を検討する。

参考文献

[1] K. Mitnick, W. L. Simon: The art of deception: controlling the human element of security, Wiley, (2001).

[2] APWG: Phishing Activity Trends Report 3rd Quarter 2019, APWG, (2019).

[3] P. Briggs, J. Debbie , C. Lynne: Behavior change interventions for cybersecurity., Academic Press, pp. 115-136 (2017).

[4] J. M. Haney , W. G. Lutters: "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security, USENIX, (2018).

[5] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri , Y. Wang: Nudges for privacy and security: Understanding and assisting users' choices online., ACM Computing Surveys (CSUR) , Vol50, No3, (2017).

[6] L. Bovens: The ethics of nudge., Preference change, Springer, Dordrecht, pp. 207-219(2009).

[7] 深田博己: 説得と態度変容—恐怖喚起コミュニケーション研究—, 北大路書房, (1988).

[8] Rogers , R. W.: A protection motivation theory of fear appeals and attitude change1, The journal of psychology, Vol91, No1 , pp. 93-114(1975).

[9] H. T. Richard , R. S. Cass: Nudge: Improving decisions about health, wealth, and happiness., (2008).

[10] リチャード・セイラー, キャス・サンスティーン , 遠藤真美: 実践行動経済学 健康、富、幸福への聡明な選択, 日経 BP, (2009).

[11] R. van Bavel, N. Rodríguez-Priego, J. Vila , P. Briggs: Using protection motivation theory in the design of nudges to improve online security behavior, International Journal of Human-Computer Studies, Vol123, pp.29-39(2019).