4D-05

ユーザがメールを確認する際の自動行動の調査

今田　寛†　　大坐畠　智†　　山本　嶺†　　加藤　聰彦†

電気通信大学大学院情報理工学研究科情報学専攻†

1. はじめに

人間は情報セキュリティの最も弱い部分(weakest-link)であると言われている[1]。最近では計算機のセキュリティは高度化し攻撃が難しくなっているが、それを使う人間についての問題は解決しておらず、未だに人間の弱点を突く攻撃は行われている。人間の弱点を突く攻撃の代表的なものとして、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フィッシング攻撃(phishing attack)がある。フィッシング攻撃など人間がセキュリティに影響を及ぼす場面では、人間の行動が問題となる。人間の行動には自動的な部分と非自動的な部分がある。行動の自動的な部分については意識や意図の範囲外であることがあり[2]、自身によるコントロールが難しいことから、対策が困難である。

フィッシング攻撃への対策は、教育や注意喚起など意識を重視した対策が検討されてきた。しかし、人間の行動には自動的な部分が存在することから、意識など非自動的な部分だけの対策では不十分である。そのため、フィッシング攻撃についても自動行動の観点から検討が必要である。自動行動の一種に習慣がある。フィッシング攻撃と習慣の関係についてはいくつかの検討が行われている。しかし、人間が行動する限り、習慣以外の自動行動が起こる可能性も考えられる。そこで本研究では、ユーザがメールを確認する際に自動行動を起こすのか、またどのような自動行動が起きるのかについて調査する。

2. 関連研究

2.1. 自動性

バージ[2]によれば、自動性の定義と診断の方法には外部から観測できる特徴ベースのものとメカニズムベースのものが考えられるが、メカニズムベースによる方法では現在提案されているメカニズムについて決定的な証拠がないことから、自動性を、外部から観測できるいくつかの特徴に分解し、各特長が観測できる程度によって漸進的に自動性を診断する方法が現実的であると述べている。

自動性の特徴として、非意図性（その行為は意図せず起こしたものかどうか）、目標独立性（その行為は目標と関係なくおこしたものかどうか）、統制不可能性（行為を変更、停止、回避しようとする目標があっても、変化、中断、防止が生じないかどうか）、自律性（非意図的で統制不可能な行為かどうか）、純粋に刺激駆動（純粋に刺激が原因の行為かどうか）、無意識性（合意に至った定義がない）、効率性（最小の注意資源の消費で済むかどうか）、迅速性（過程の持続時間が短いかどうか）が見いだされている。

2.2. フィッシングと行動

人間の行動を分析し、フィッシング攻撃との関係について検討を行う研究は以前より行われてきた。

Paul[3]は、ユーザの馴化と感作およびフィッシングに関する行動モデルを検討している。これはユーザの慣れとフィッシング攻撃の成功との関係については検討を行っているが、慣れ以外の自動行動との関連については検討を行っていない。

Kun ら[4]は、人間の行動の結果であるマウスの動きと人間がフィッシングメールを認識しているかどうかの関係について調査しており、マウスの動きが遅いことはフィッシングメールの認知度が高いことがわかっている。これは人間の行動の外部から観測できる特徴について検討した研究であり、マウスが動く速度などは効率性や迅速性などの自動性の特徴との関連が考えられる。しかし、この研究では自動性の特徴や自動行動との関連については検討を行っていない。

また、[5], [6]の研究では、ユーザの行動分析に視線追跡を用いている。宮本ら[5]は、ブラウザ上でのユーザの行動を視線追跡を用いて分析し、アドレスバーの URL と関連するセキュリティ情報の確認を習慣づけるシステムを構築している。シュウら[6]は、フィッシングに対する事前知識とユーザの行動の関係、ユーザが何を根拠にフィッシングサイトを認知するかについて、視線追跡装置と半構造化インタビューを用

Investigating user's automatic behavior in e-mail checking
†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

いたユーザ行動分析を行っている。

これまでの研究ではユーザによるフィッシングの検出やユーザがフィッシングを正しく分類できることに主眼が置かれており、ユーザが無意識に行っている行動とフィッシングへの引っかかりやすさとの関係についての議論は十分ではないと考えている。ユーザがフィッシングを認知するしないに関わらず、誤った行動を行ってしまう可能性についても検討が必要だと考えている。フィッシングメールがあるかないかにかかわらず、普段のメール利用についてどのような特徴が見られるか検討が必要だと考えられる。

2.3. フィッシングと自動性

Vishwanath ら[7]は、フィッシング詐欺につながる可能性のある認知的、前意識的、自動的なプロセスを説明するモデルを構築した。Link Attack と Attachment Attack について実験を行い、モデルの適合を確認した。

この研究では習慣に着目しているが、習慣以外の自動行動が被害にあう可能性を高めている可能性については検討していない。習慣以外の自動行動についても検討する必要があると考えられる。また、自動性の特徴に基づいて分析することで、フィッシングと自動性の関係をより理解することができると考えられる。

3. 調査方法

ユーザがメールを確認する際に自動行動を起こすのか、またどのような自動行動が起きるのかについて、ユーザがメールを確認する際の普段の行動を調査する。

はじめに、ユーザが普段のメール確認の際にどのような場面でどのような自動行動を起こす可能性があるか検討するため、メールを確認する際の普段の行動に関する質問紙調査を匿名で行う。この質問紙調査では、ユーザが普段どのようにメールを使用しているか、どのような経験をしているかについて調査する。年齢、性別、メールの使用頻度、メール使用の際の状況、メール使用時の行動、不審なメールの受信経験、ヒヤリハットの経験などを質問する。

次に、質問紙調査の結果から検討した、自動行動を起こす可能性のある場面やその自動行動の内容について、実際に起きるかどうか、またその他の自動行動が観測できないかを実験して確認する。

実験では、実際に普段通りのメール確認の操作をしてもらい、スクリーンレコーダーなどにより、表示内容、マウスカーソルの軌跡、クリック位置、入力内容などを記録し、その記録データから、操作の時間間隔、事前に定義した行動の回数、マウスカーソルの速度などを分析する。また、実験後には、自動性の特徴が見られるかを確認するために、操作時の周囲の状況、本人の状態など、操作内容に関してインタビューを行う。

4. まとめと今後の課題

ここでは、フィッシングへの引っかかりやすさと自動行動との関連の可能性について述べた。

今後は実験内容のより具体的な検討及び、実験を行い、ユーザがメールを確認する際に自動行動を起こすのか、またどのような自動行動が起きるのかについて検討を行う。

参考文献

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

[2] ジョン バージ: 無意識と社会心理学: 高次心理過程の自動性, ナカニシヤ出版, (2009).

[3] Watters P. A.: Why do users trust the wrong messages? A behavioural model of phishing, 2009 eCrime Researchers Summit, IEEE, (2009).

[4] Yu K., Taib R., Butavicius M. et al.: Mouse Behavior as an Index of Phishing Awareness, IFIP Conference on Human-Computer Interaction, Springer, Cham, vol. 11746, pp.539-548 (2019).

[5] Miyamoto D., Iimura T., Blanc G. et al.: Eyebit: Eye-tracking approach for enforcing phishing prevention habits, 2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS). IEEE, (2014).

[6] シュウ インゴウ, 森 啓華, 櫻井 悠次 ほか: エンドユーザはフィッシングサイトを見破ることができるか? 視線追跡装置と半構造化インタビューを用いたユーザ行動分析, 研究報告セキュリティ心理学とトラスト (SPT), 2020(42), pp.1-8 (2020).

[7] Vishwanath A., Harrison B., and Ng Y. J.: Suspicion, cognition, and automaticity model of phishing susceptibility, Communication Research, 45.8, pp.1146-1166 (2018).