様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ５ 月 ３１ 日現在

機関番号：１２６０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１８０

研究課題名（和文）視線分析による標的型攻撃メール対策システムの研究

研究課題名（英文）A Study of Prevention Systems against Targeted Email with Eye Tracking

研究代表者
宮本　大輔（Miyamoto, Daisuke）

東京大学・大学院情報理工学系研究科・准教授

研究者番号：９０６１２４５８

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：標的型攻撃メールに起因するサイバー攻撃が猛威を奮っている。本研究では、受信者がメールを閲覧した際の視線移動や眼球運動を分析し、受信者がどのような基準で標的型攻撃メールか正常なメールかの意思決定を行うか予測する手法を研究した。セキュリティ情報を表示するインジケータのインタフェースについて調査を行い、17名の被験者の視線を分析し、セキュリティインジケータを凝視する率、最初の凝視にかかった時間、凝視時間の割合、回数を性能指標として分析したところ、本研究で提案するインジケータ及び配置位置の有効性が示された。また、PC環境だけでなくスマートフォン環境でも有効性の検証を行った。

研究成果の学術的意義や社会的意義
近年はコンピュータを用いるユーザを狙ったサイバー攻撃が猛威を奮っている。特に標的型メール攻撃は、ユーザを悪性サイトに誘導するだけでなく、メールに添付されたマルウェアを誤ってユーザに開かせ、コンピュータをマルウェアに感染させようとする。標的型メールの文面は怪しい所がなく、ユーザはメールソフトのセキュリティインジケータを用いて対策を行う必要がある。本研究は、このインジケータがどのような設計であれば注意を引きやすいかを視線分析を用いて研究し、特定の部分を見るまで添付ファイルやメール本文のリンクをクリックできないソフトのプロトタイプ開発を行った。

研究成果の概要（英文）：The number of cyber threats that targets computer users with targeted email attacks are increasing. In this study, we analyzed eye movements when the users viewed an email, and studied a method to predict what criteria the recipient uses to make a decision about whether an email is a targeted attack email or a normal email. We conducted a survey for the interfaces of the indicator to display security information, and we analyzed the efficiency with 17 of subjects. The results showed that the rate of staring at the security indicator, the time it took for the first stare, the rate of stare time, and the number of times were analyzed as performance indicators, indicating the effectiveness of the indicator and placement position proposed in this study. We also verified the effectiveness of the system not only in the PC environment but also in the smartphone environment.

研究分野：サイバーセキュリティ

キーワード：標的型メール対策　サイバーセキュリティ　視線分析　情報システム　不正アクセス対策

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

特定の組織に属する人物から機密情報を搾取する「標的型攻撃」が深刻な脅威となっており、その中でも「標的型攻撃メール」への対策が急務とされる（参考文献[1]）。標的型攻撃メールは、メール受信者が不信を抱かないようなメール文面が書かれており、ウイルス感染の仕掛けが施された添付ファイルをクリックしたり、ウェブサイトへのリンクをクリックしたりする可能性が高い。さらに、不特定多数に送信される「バラマキ型メール」とは異なり、特定の人物のみを受信者としているため、セキュリティソフトの定義ファイルに登録されるよりも前にメールが受信できてしまう。この結果、受信者はセキュリティソフトを利用していても被害を防ぐことは難しい。

受信者に届いた標的型攻撃メールを見破るためには、メールに付随する電子署名の情報を確認する手法や、Sender Policy Framework (SPF, RFC4408)・DomainKeys Identified Mail (DKIM, RFC6376)のようなメールの送信者が正規のメールサーバを利用した情報を確認する手法が上げられる。この一方で、メールの受信者が情報そのものを知らなかったり、気づかなかったり、確認を怠ったりすることで標的型攻撃メールの被害を受ける可能性はある。

この一方で、研究代表者はフィッシングサイトの対策研究を行っている。フィッシングサイトも、標的型攻撃メールと同様に本物か攻撃かの見分けがつきにくい。我々の先行研究では、視線追跡カメラを用いて、ウェブサイトを閲覧するユーザが何から情報を得ているかを分析した。正しい判断を行うユーザはアドレスバーに記載される URL や SSL 証明書などのアイコンを表示している領域を見ているに対し、騙されやすいユーザはウェブコンテンツにもとづいて真贋判定を行う傾向が観測された。さらに、単に特定の箇所を眺め見るのではなく、眼球運動における凝視運動の時間及び回数を機械学習により分類したところ、ユーザが URL や SSL 証明書から情報を得ようと意図を持って閲覧しているか否か、そしてウェブコンテンツに騙されるか否かを高精度で推測可能なことがわかった。この結果を先行研究の知見を活用し、普通のメールや標的型攻撃メールを確認する受信者の視線を分析する。そして、視線分析と標的型攻撃メールの真贋判定の相関関係を分析し、受信者にとって正しい真贋判定を行いやすいメールクライアント（Mail User Agent、MUA）を調査し、標的型攻撃メールの対策システムの設計・実装及び評価を行う。

２．研究の目的

本研究では、受信者がメールを閲覧した際の視線移動や眼球運動を分析し、受信者がどのような基準で標的型攻撃メールか正常なメールかの意思決定を行うか予測する手法を研究する。PC 用、スマートフォン用及びウェブメーラなどのメールクライアントと、それらのセキュリティ情報の表示について調査し、受信者が真贋判定を行いやすいインタフェースを視線分析に基づいて分析する。具体的には、セキュリティ情報を表示する際に利用されるアイコンの色や形、文言を調査し、受信者が真贋判定を行いやすい MUA のユーザインタフェースを分析することで、セキュリティ情報へのアクセシビリティの高い MUA の設計手法を解明する。

また、視線分析に基づく標的型攻撃メール対策システムを実装し、実験を通じて有効性を検証する。さらに、セキュリティ情報を目視確認しない限り、メール文面のリンクや添付ファイルなどへの操作を無効にすることで、受信者にセキュリティ情報の目視確認の習慣を得させる手法について研究する。

３．研究の方法

本提案の研究計画は、(1) 標的型攻撃メールに関するデータ収集、(2) 参加者による実験の実施、(3) 実験結果の分析、(4) 標的型攻撃メール対策インタフェースの設計、(5) 研究成果の社会への展開、の 5 つの研究課題によって構成した。さらに課題ごとにサブ課題を設け、それぞれに研究を無理なく実施できるようなマイルストーンを設定した。

本研究では、まず標的型攻撃メールに関するデータ収集を行う。標的型攻撃メールの収集を行い、また、メールクライアントを調査し、メールの信頼性を高める機能の実装についての情況、画面についてサーベイを行う。クライアント PC にインストールするもの、スマートフォンのアプリとしてインストールするもの及びウェブメールアプリケーションが対象であった。さらに、意思決定に重要な影響を及ぼしていると思われる視線・眼球運動について調査した。また、データセットは生体情報を含むため、暗号化や秘匿化、匿名化などを施した上で、データの保存・保管を行う。このために必要な設計及び運用を行った。

次に実験に用いる標的型攻撃メールを安全に閲覧するシステムの設計及び実装を行い、実験計画書を作成する。また、実験の参加者に説明するための実験の趣意説明書、オープンデータセットについて公開する情報、公開しない情報についての説明書を作成した。趣意説明及びオープンデータセットについて十分な説明を行った上で、実験を実施し、視線情報及び真贋判定情報を

収集する。参加者は、単純にメールを閲覧し「正常なメールである」「標的型攻撃メールである」といった解答を行う。また、この結果について視線分析と標的型攻撃メールに騙されたかどうかを判定した。また、この知見に基づいた標的型攻撃メール対策の設計及び実装を行った。さらに、国際会議・国内研究会における論文発表の他、国際標準化提案を行う。

４．研究成果

17 名の被験者の視線を分析し、セキュリティインジケータを凝視する率、最初の凝視にかかった時間、凝視時間の割合、回数を性能指標として分析し、提案手法が高い性能であるという知見が得られた。また、質疑により危険な場合、安全な場合、安全性が不明な場合のわかりやすさも調べた。この結果、アイコン、色、文字を組み合わせ、かつ、メール画面の左側に表示する方が効果が高いという知見が得られた。また、大型のスクリーンを持つ PC 環境だけでなく、スマートフォン環境においても動作させるべく、スマートフォン用の Eye tracking を導入し本研究の基礎実験を行い、フィッシングメール及び攻撃についても視線分析によるアプローチが有効であることを確認した。また、以下の論文を出版した。

（論文誌）

1. Jema David Ndibwile, Edith Talina Luhanga, Doudou Fall, Daisuke Miyamoto, Gregory Blanc, and Youki Kadobayashi, “An Empirical Approach to Phishing Countermeasures through Smart Glasses and Validation Agents” IEEE Access, ISSN 2169-3536, DOI: 10.1109/ACCESS.2019.2940669, Vol. 7, pp.130758-130771, September, 2019.

（国際会議）

2. Jema David Ndibwile, Edith Talina Luhanga, Doudou Fall, Daisuke Miyamoto, Youki Kadobayashi , “A Comparative Study of Smartphone-User Security Perception and Preference towards Redesigned Security Notifications” In Proceedings of the 2nd African Conference on Human Computer Interaction (AfriCHI 2018), pp.17:1-17:6, December 2018.

（国内研究会）

3. 小野木 祐太, 宮本 大輔, “視線認識を用いたメールインジケータの視認性分析に関する研究
情報処理学会研究報告” CSEC 83(19), pp.1-8, 2018 年 12 月.

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Ndibwile Jema David、Luhanga Edith Talina、Fall Doudou、Miyamoto Daisuke、Blanc Gregory、Kadobayashi Youki	４．巻 7
２．論文標題 An Empirical Approach to Phishing Countermeasures Through Smart Glasses and Validation Agents	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 130758～130771
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2940669	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 小野木祐太，宮本大輔
２．発表標題 視線認識を用いたメールインジケータの視認性分析に関する研究
３．学会等名 情報処理学会研究報告
４．発表年 2018年

１．発表者名 Jema David Ndibwile, Edith Talina Luhanga, Doudou Fall, Daisuke Miyamoto, Youki Kadobayashi
２．発表標題 A Comparative Study of Smartphone-User Security Perception and Preference towards Redesigned Security Notifications
３．学会等名 The 2nd African Conference on Human Computer Interaction（国際学会）
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考