Vol.2018-CSEC-83 No.19
2018/12/14

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

小野木 祐太[1,a)]　宮本 大輔[1,b)]

概要：現代社会において、電子メールの普及とともになりすましメールが問題となっている。なりすましメールからエンドユーザの安全を守る技術に関して様々な研究が行われているが、これを利用する人間が確認を怠るようなことがあれば、忽ち危険な状態に晒されてしまう。このような人的要因を軽減するために、メールソフトにはインジケータを用いて、エンドユーザに安全性を検証した結果を提示する機能がある。しかし、メールインジケータの視認性や分かりやすさには不明瞭な点が多い。これらの特性を調べるために、既存のメールインジケータと異なる特性を持つ 2 種類のメールインジケータを設計し、ユーザがなりすましメールの判定をする際の視線情報を用いて分析を行う。その結果、視認性の高いインジケータには、画面の左側に表示するインジケータや、アイコンと文字と色で構成されるインジケータ、表示領域の拡張をするインジケータは視認性が高い傾向が確認された。また、判読性の高いインジケータの特徴は、画面の左側に表示するインジケータや、アイコンと文字と色で構成されるインジケータが該当した。可読性の高いインジケータの特徴は、判読性が高く凝視時間割合や凝視回数が小さくなるものである。

キーワード：なりすましメール, セキュリティインジケータ, メール認証, セキュア UI, 視線認識

Yuta Onogi[1,a)]　Daisuke Miyamoto[1,b)]

1. はじめに

現代社会において、電子メールは手軽なコミュニケーションツールとして広く普及しており、日々膨大な量の通信が行われている。このような状況から、サイバー犯罪者にとっては、メールが最も狙いやすい攻撃経路となっている。メールを利用して攻撃を行う場合、特定の人物や組織になりすましてメールを送る「なりすましメール」がある。

なりすましメールには、送信者の名前を、特定の個人や有名ブランドであるかのように見せかけ、メールに添付されたマルウェアを開かせるものや、悪意のあるサイトに誘導するフィッシング攻撃、企業から金銭を騙し取る BEC(Business Email Compromise) などがある。このようなサイバー攻撃に対して、送信ドメイン認証や電子署名、伊藤によるメーラーフィンガープリントを用いた研究 [6] など対策が提案されてきたが、攻撃の報告は毎年増加する一方である。

この原因としては、技術的要因だけでなく人間の精神状態が影響する人的要因も考えられ、ストレスなどの精神的負荷の高まりが過失を起こしやすくするとされている [1]。フィッシング攻撃に関しては、セキュリティ知識の不足が原因と言われている [2]。このような人的要因によるセキュリティインシデントを軽減するために、メールソフトにはインジケータを用いて安全性の検証を行った結果をエンドユーザに提示する機能がある。インジケータは安全性を保証するだけでなく、様々な要件定義があり、詳細は 3.1 節で述べる。しかし、メールインジケータのインターフェースの視認性や分かりやすさの有効性については不明瞭な点が多い。

この特徴を調べるため、本研究では様々な種類のメールインジケータを用いた視線分析の実験を行い、ユーザがメールの真贋判定をする上で、メール画面のどこに重要と感じる要素があるのかを調査する。また、ウェブインジケータのデザイン設計に関する研究を元に、本研究では 2 種類のメールインジケータを設計し、既存のメールインジケータと比較することで、それぞれのインジケータのユーザーインターフェースの有効性の特徴について言及する。

2. 関連研究

この章では、メールインジケータを作るにあたって参

[1] 奈良先端科学技術大学院大学 情報科学研究科
サイバーレジリエンス構成学研究室
NAIST, Icoma, Nara 630–0192, Japan
[a)] onogi.yuta.oq6@is.naist.jp
[b)] daisu-mi@nc.u-tokyo.ac.jp

© 2018 Information Processing Society of Japan

図 1　調査に用いるウェブインジケータの形状一覧

図 2　3 種類に選定したウェブインジケータの形と色

考にしたウェブインジケータの研究を 2.1 節に述べ、現在メールで使われているインジケータを 2.1.1 項に述べる。

2.1　ウェブで使われるインジケータ

ブラウザのウェブインジケータの研究は、2000 年代半ばに盛んなに行われていた。当初は、URL バーだけでなく、ブラウザの右下など複数の領域に表示していたが、現在では URL バーだけの表示となっている。

ユーザがウェブインジケータの意味を完全には理解していない場合が多いため、専門的知識を持たない一般のユーザでも理解できるウェブインジケータを設計しなければならない。

また、インジケータの設計要件として、最低でも接続しているウェブサイトが安全か否かを判別する警告だけでも伝える必要がある。Google Chrome を使用しているユーザを対象に、オンラインベースの企業向け市場調査サービスである Google Consumer Surveys(GCS) を利用して調査し、ユーザが分かりやすいと感じるウェブインジケータの組み合わせを調査したものに、A.P.Felt らの研究 [3] がある。この研究では、8 種類のアイコン形状 (図 1)、5 種類の表示色 (黒/青/緑/橙/赤)、7 種類の説明文をウェブインジケータの調査に用いる構成要素とし、その中から安全性を示す指標に最適な 3 種類 (安全/不明/危険) のインジケータの組み合わせを提案している。最初に選定したのは図 2 に表す 3 種類のアイコン形状と表示色による組み合わせである。それぞれに対応する 7 種類の説明文を以下に示す。

- 緑色の鍵アイコンに対応する説明文
  ”https”, ”Private”, ”Secure”, ”Safe”, ”Encrypted”, ”Secure and private”, ”Secure site”
- 黒色の丸アイコンに対応する説明文
  ”http”, ”Not private”, ”Not secure”, ”Not safe”, ”Not encryped”, ”Not secure, not private”, ”Site not secure”
- 赤色の三角アイコンに対応する説明文
  ”http”, ”Not private”, ”Not secure”, ”Not safe”, ”Not encryped”, ”Not secure, not private”, ”Site not secure”

これらを元に GCS でユーザ調査をして、選ばれたのが以下の組み合わせである。

- 緑色の鍵アイコンに対応する説明文→”Secure”
- 黒色の丸アイコンに対応する説明文→”Not secure”
- 赤色の三角アイコンに対応する説明文→”Not secure”

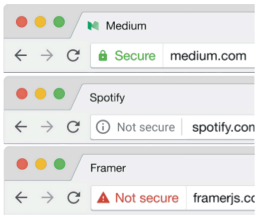

図 3　A.P.Felt らが提案するウェブインジケータ

図 4　電子署名で使われるメールインジケータ

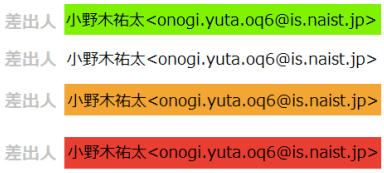

図 5　DKIM Verifier の背景色強調機能 [DKIM Verifier(S)]

この組み合わせに対して、表示する位置など更に調整を加えることで、最終的な提案手法として選出したのが図 3 の組み合わせである。しかしながら、この論文では Not secure を黒色から灰色に変更した理由が書かれておらず、調査の実態についても記載がなされていない。

2.1.1　メールで使われるインジケータ

この項では、既存のメールインジケータの機能や特徴について紹介する。

(1) Thunderbird 上で使われるセキュリティ技術とメールインジケータ

- 電子署名
  S/MIME は Thunderbird に標準搭載しているセキュリティ技術であり、PGP については Thunderbird アドオンである Enigmail をインストールすることで使用可能になる。いずれの機能も同じメールインジケータを使用しており、安全と危険を示す 2 種類のものがあり、その一覧を図 4 に表す。図 4 において、左側のメールのアイコンが安全を示すメールインジケータ、右側のメールのアイコンに × マークが入ったものが危険を示すメールインジケータである。
- DKIM Verifier[4]
  Thunderbird 上で DKIM を実装した機能を持つアドオンである。メールインジケータとしては差出人の背景色強調機能 (図 5, 以降 DKIM Verifier(S) と表記する)、DKIM ヘッダの表示 (図 6, 以降 DKIM Verifier(H) と表記する)、ステータスバーのアイコン表示機能 (図 7, 以降 DKIM Verifier(S.B) と表記する) を持つ。それぞれの図において、上から順に、有効な署名 (安全)、署名情報なし (安全でない)、未署名か一時的なエラー、無効な署名 (危険) である状態を表している。
- Thundersec[5]
  Thundersec は、DNSBL(DNS-based Blackhole List)、

© 2018 Information Processing Society of Japan

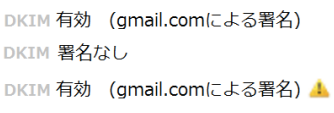

図 6 DKIM Verifier の DKIM ヘッダー表示機能 [DKIM Verifier(H)]

図 7 DKIM Verifier のステータスバーアイコン表示機能 [DKIM Verifier(S.B)]

図 8 Thundersec で使われるメールインジケータ

図 9 M.F.R. で使われるメールインジケータ

RBL(Realtime Blackhole List(RBL)、DKIM、SPF を実装した Thunderbird アドオンである。メールインジケータとしては、図 8 のような通知バーによる表示を行う。図 8 において、上が安全な状態を示す通知バー、下が危険な状態を示す通知バーとなっている。

(2) メーラーフィンガープリントを用いた研究 (以降 M.F.R と略す)

M.F.R で使われるインジケータでは、図 9 のようにメッセージヘッダ中央部に大きなアイコンの表示をする。図 9 において、それぞれのインジケータは左から順に、安全、不明、危険なセキュリティ状態を示す。

2.2 問題分析

ユーザがメールの真贋判定をできない原因として、既存のなりすましメールの対策手法を用いても、その真贋判定に資する情報を表示するユーザインタフェースの問題があるのではないかと考えられる。また、メールインジケータをどのように設計するかは、不明瞭な点が多く、この特性を調べるために特徴の異なるメールインジケータを作成し、分析する。

3. 視線分析技術を用いたメールインジケータの視認性分析

この章では、メールインジケータの要件定義として、本研究を行う上での前提条件とあるべき姿について述べた後に、メールインジケータの視線分析をするための手法や、その結果から分かる特徴についてまとめる。

3.1 インジケータの要件定義

この節ではインジケータの要件定義について説明する。インジケータの要件定義は、セキュリティ面とインターフェース面に分けて考えることができる。本研究では、セキュリティ面の要件が満たされているものとして、インターフェース面の視認性と分かりやすさの特徴を調べるための分析をする。

- セキュリティ面

(1) 提示される情報の正確性

インジケータはセキュリティ技術により検証した結果が提示されるものであるが、この内容は正しく判別した結果を表示しなければならない。メールインジケータは危険度別に 4 種類 (安全/不明/危険/その他警告) に分類することができるが、その他警告は使われる事例が極めて少ないため、3 種類 (安全/不明/危険) を対象とする。

(2) インジケータの偽装について

なりすましメールの文面が限りなく正規のメール文面に近い形となっているように、インジケータのデザインが普及すれば、攻撃者は正規のものを使用して攻撃を行おうとする。そのため、インジケータは偽装しにくいデザインで設計しなければならない。

- インターフェース面

(1) 提示される情報の視認性

ユーザがインジケータの存在を認識できなければ、インジケータとして効果を示すことはできない。そのため、インジケータをユーザが認識しやすい場所や、認識しやすい大きさに設計する必要がある。

(2) 提示される情報の分かりやすさ

インジケータが安全性の情報を提示しても、その意味が理解されないことがある。そのため、インジケータの提示する内容はユーザにとって分かりやすく (判読性が高く)、その意味を素早く理解できる (可読性が高い) ものでなければならない。

(3) 提示する情報の表示空間

使用するデバイスによっては、インジケータを表示するための空間が十分に確保できない場合がある。そのような限られた領域においても、効果的なインジケータを設計しなければならない。

3.2 本研究で新たに設計するメールインジケータ

2.1 項で述べた、A. P. Felt らの提案手法を参考に真贋性を示すメールインジケータとして次のような設計を行った。

- アイコン形状

A. P. Felt らの提案手法と同じ形状にした。具体的には安全を示す形状を南京錠、不明を示す形状を丸型のエクスクラメーションマーク、危険を示す形状を三角のエクスクラメーションマークを使用する。

- 色

A. P. Felt らの提案手法では、不明を示す色が灰色であるとした論拠が乏しく、確実な成果としては、黒色がユーザの主観的評価が高いという結果が出ていた。その他は市場調査に基づいた評価を行っていたため、本提案手法では安全を示す色が緑色、不明を示す

© 2018 Information Processing Society of Japan

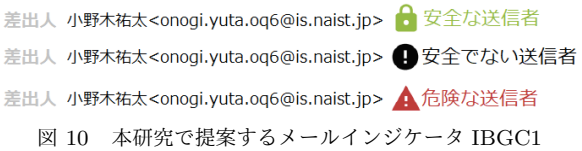

図 10　本研究で提案するメールインジケータ IBGC1

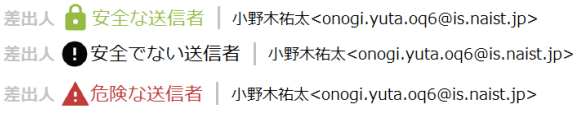

図 11　本研究で提案するメールインジケータ IBGC2

色が黒色、危険を示す色が赤色を採用する。

- 文字

  A. P. Felt らの提案手法では、安全を示す言葉として”Secure”、不明と危険を示す言葉が”Non secure”であったが、本研究では、日本人が使うメールを想定するので、日本人が分かりやすいと感じる言葉を選ぶ必要がある。そのため、安全を示す言葉を”安全な送信者”、不明を示す言葉を”安全でない送信者”、危険を示す言葉を”危険な送信者”とした。

ウェブインジケータでは URL バーの左に表示するのが一般的であるが、メールインジケータにおいてはそれぞれの手法によって表示場所が異なるため、どの表示場所が効果的かを調べる必要がある。そのため、表示する場所を変えたメールインジケータセットを 2 つ作成した。差出人情報の左側に表示するセットを Indicator Based Google Chrome Pattern1(IBGC1) として図 10 に、右側に表示するセットを Indicator Based Google Chrome Pattern1(IBGC2) として図 11 に表す。

3.3　実験

この節では、メールインジケータのユーザーインターフェースの有効性についての特徴を調べるために視線分析実験を行い、視認性と分かりやすさの観点でそれぞれの特徴をまとめる。

本実験で用いるメーラーは、普及率が高いことと、アドオンやプラグインの導入により開発しやすい環境であることから「Thunderbird」を用いる。Thunderbird のバージョンは 52.9.1(MAC OS 版) である。また、視認性分析に用いる視線認識装置は、23 インチ型モニターと視線認識装置の一体型の製品の「Tobii Pro TX300」である。この視線認識装置では、ユーザがモニターから数十 cm 程度離れた位置の椅子に座った状態でモニターを見つめることで、視線検知を行う。

調査に用いるメールインジケータは、2.1.1 項で述べたメールインジケータに加えて、本研究の提案手法のメールインジケータを使用する。

3.3.1　視認性分析に用いるメール文面

メール文面の設計として、視線認識装置が認識しやすいように差出人、件名、宛先、本文の文章を標準設定よりも大きくし、文字の行間も広くなるようにした。

図 12　視線位置の初期化

本文は、執筆者の元に届いた正規のメールと、フィッシング対策協議会 [7] に報告されたなりすましメールの 2 種類を用いて、個人情報やセキュリティの観点から一部に改変を加えたものを使用した。

メール文章と使用するメールインジケータの安全性 (安全/不明/危険) の組み合わせはランダムに設定した。つまり、安全を示すメールインジケータであっても、メールの文章は正規メールとなりすましメールの 2 通りが存在する。これは、文章の正規性に関係なく、ユーザはメールインジケータを見て判断するのかを調査するためである。

3.3.2　視線の初期化

メール画面を連続して見る時、人間の視線は直前に見た画面の視線位置を引き継いでしまう為、次のメール画面に遷移する前に、視線情報をリセットする必要がある。これを行うため、図 12 のような画像を、メール画面が遷移する前に挟むことで視線を中央に戻せるようにした。

3.3.3　被験者の募集

視認性分析の実験に参加した被験者の詳細を以下に示す。

- 被験者の条件

  日本語で構成されたメールについて送信者のなりすましを判定する必要があるので、普段から日本語のメールを使っている日本人を対象とする。

- 被験者の詳細

  2018 年 10 月 16 日 (水)〜2018 年 10 月 19 日 (金) の間、奈良先端科学技術大学院大学の先端科学科情報科学領域の日本人の学生と職員の 17 名を対象とした。

3.3.4　実験手順

前項の被験者に対して、以下の手順で実験を行う。

(1) 実験方法の説明

被験者に実験開始から実験終了までの実験手順、また以下のような実験を行う上での注意点を説明をする。

- 顔の位置がキャリブレーションした位置からずれてしまうと正しい計測ができなくなるため、その旨を伝える。
- 送信者のなりすましを判定してもらうため、慎重になりすぎないように、なるべく普段通りに見て欲しい旨を伝える。
- 実験中に笑ったり目を細めてしまうと視線認識装置が視線を正しく検知できなくなることがあるので、その旨を伝える。

(2) キャリブレーション

本実験に用いる視線認識装置は、角膜に近赤外線を照射し、眼球の動きを映像解析することにより、「どこ

© 2018 Information Processing Society of Japan

を・どのように」見たのかを計算することができる。実際には、赤色のボールが画面内のあらゆる場所を動き回る画面があり、それを目で追跡することで、瞳孔点と反射点、2 点の位置関係と、選ばれた眼球の 3D モデルを元に、専用のアルゴリズムを用いて眼球の向きを算出する。キャリブレーション結果が誤差の少ない状態を示す緑色の状態になったら、視線認識の誤差が少ない状態 (60cm 先であれば直径 1cm 程度、腕の長さほど先であれば親指の爪の大きさぐらいの精度) となるので、次の実験実施フェーズに移る。

(3) 実験実施

- サンプル画面

  メール画面の送信者のなりすまし判定を行う画面は、サンプル画面からスタートする。その理由は、メール画面に慣れていなかったり、実験手順を正確に把握できていなかった場合に、最初のメール画面とそれ以降の画面で、認識する時間や視線行動に差ができるのを防ぐためである。

- メール画面の視線認識

  被験者にメール画面を見せて、送信者のなりすまし判定 (○/△/×) を 20 秒以内に口頭で答えてもらい、その内容を記録する。○が信頼できる正規の送信者、△ がどちらともいえない送信者、× が危険な送信者 (なりすましメール) を表す。判定ができた時点で次のメール画面に進み、全 16 画面に対して同様の内容を記録する。この 20 秒というのは、おおよその人がメール 1 通あたりに割く時間の上限であると想定して決定した。全 16 画面の送信者の真贋性判定が終わったら、次のアンケート評価のフェーズに移る。

(4) アンケート評価

アンケート評価を行う前に、被験者に対して本実験でメールで使われた全てのメールインジケータの意味を説明し、被験者がメールインジケータの意味を理解できたら以下に示す判読性を調べるためのアンケートに記入してもらう。アンケート用紙には、実験で使われたメールインジケータの画像を全て記載する。被験者は、この画像と以下の文面を読んで評価を行う。

今回の実験で使われたセキュリティ警告の一覧を以下に記載しています。それぞれのセキュリティ警告がどれくらい使いやすいと感じるか、5 段階 (1〜5) で意味が分かりやすいほど高得点で評価してください。

3.3.5 実験で取得したいパラメータについて

視認性を評価するために、本実験で取得したいパラメータは以下の 4 つである。まず最初に、これらのパラメータで使われる凝視の定義をする。凝視とは、視線認識装置が被験者の視線情報として認識した画面上の注視点について、前後のサンプリング点を比較した時に、予め定義された最小距離以下の移動に留まる場合か、特定の速

図 13 IBGC1 のヒートマップ

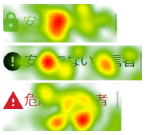
図 14 IBGC2 のヒートマップ

図 15 DigitalSignature のヒートマップ

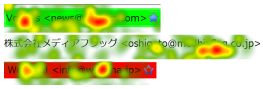
図 16 DKIM Verifier(S) のヒートマップ

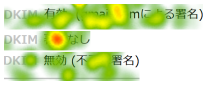
図 17 DKIM Verifier((H) のヒートマップ

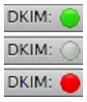
図 18 DKIM Verifier((S.B) のヒートマップ

図 19 M.F.R. のヒートマップ

度以下で移動した場合に「凝視」と定義する。即ち、視線が比較的静止した状態となっている時に凝視していると判定する。視線追跡装置の凝視を検知するためのフィルターには Tobii Studio で定義される I-VT filter の初期設定 (Velocity threshold = 30 degrees/sec, Windows length = 29ms, Minimum fixation duration = 60 ms) を用いた。

(1) 凝視率

指定したエリア要素に対して、凝視した人数の平均の割合を指す。インジケータは視認されなければ全くの効果を示さないため、視認性において、凝視率は一番重要なパラメータである。

(2) 最初の凝視時間

ユーザはインジケータを早く視認できるほど、危険性の早期発見につながるので、インジケータの視認性は高いと評価できる。そのため、このパラメータ値は小さいほど高い評価ができる。凝視が一度されなければ、この値は∞となり通常は値は算出できないが、この時の結果を除外するのではなく、悪い評価をすべきである。そのため、被験者がなりすまし判定にかけた合計時間が凝視がされなかった場合の時間となるようにパラメータの調整を行った。

(3) 凝視時間割合

指定したエリア要素の凝視時間の合計をメール画面全体の凝視時間の合計で割った値である。

(4) 凝視回数

指定したエリアの凝視回数の合計値を示す。ユーザがなりすまし判定をする上で特定領域の凝視回数は、他の領域よりも重要であることを示す [8]。凝視時間割合や凝視回数が高くなると、なりすまし判定にかけた時間的コストが高くなったことを示すので、ユーザにとって重要に感じた要素である一方で、可読性の悪いインターフェースとも評価できる。

3.3.6 実験結果

この項では認識精度の悪かった被験者 4 人を除いた 13

© 2018 Information Processing Society of Japan

図 20　Thundersec のヒートマップ

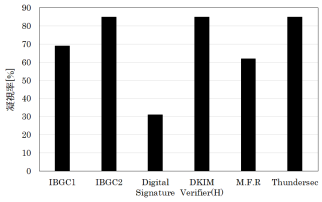

図 21　凝視率 (安全を示すメールインジケータ)

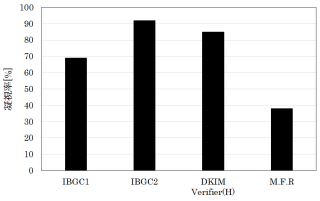

図 22　凝視率 (不明を示すメールインジケータ)

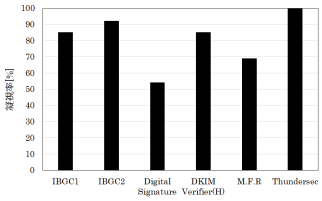

図 23　凝視率 (危険を示すメールインジケータ)

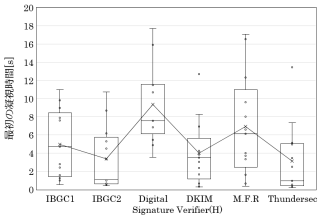

図 24　最初の凝視時間 (安全を示すメールインジケータ)

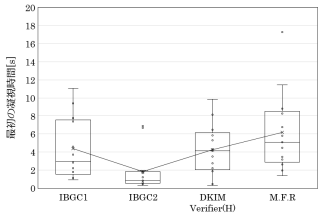

図 25　最初の凝視時間 (不明を示すメールインジケータ)

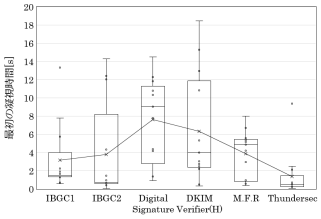

図 26　最初の凝視時間 (危険を示すメールインジケータ)

人分の視線分析結果と 17 人分のアンケート結果について示す。それぞれのメールインジケータ毎に対する凝視時間割合のヒートマップを図 13〜図 20 に表す。3.3.5 項で述べた 4 つのパラメータから評価したときの結果を図 21〜図 31 に表す。横軸がメールインジケータの種類、縦軸がそれぞれのパラメータに対応する単位を示す。図中の × のプロットは平均値を示し、それぞれのプロットを繋ぎ、折れ線グラフとして表示している。メール要素全体の結果についてはその特性が分かりやすく表れていたものとして、最初の凝視時間を図 30 に、凝視時間割合を図 31 に表す。横軸の Sender Address は送信者情報のアドレス部分、Sender Name は送信者情報の送信者名のみの評価を示し、URL は本文中に含まれる URL のみの評価を表す。また、Sender, Sender Address, Sender Name はインジケータと切り離して、純粋なメール要素としての評価をしたいので、DKIM Verifier で背景色強調がされていた要素の値は含めずに算出した。　分かりやすさのアンケート結果を図 32〜図 34 に表す。18 人分のデータを記載する。

3.3.7　実験の分析と考察

(1) メールインジケータの分かりやすさ (判読性)

判読性はアイコン+色+文字の 3 つで構成されるか、アイコン+色の 2 つで構成される時に高い評価を示し、メール画面の左側に表示するものがより良い結果と

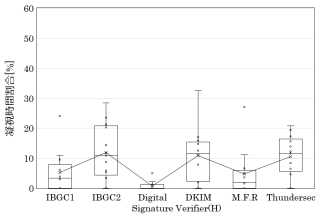

図 27　凝視時間割合 (安全を示すメールインジケータ)

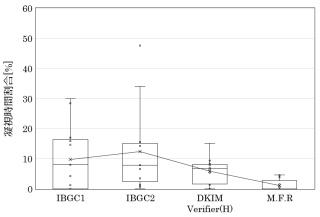

図 28　凝視時間割合 (不明を示すメールインジケータ)

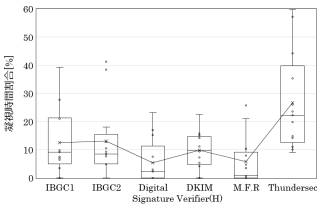

図 29　凝視時間割合 (危険を示すメールインジケータ)

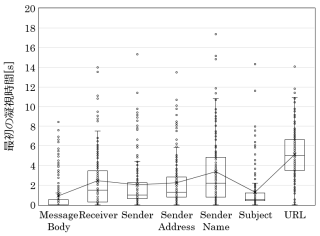

図 30　最初の凝視時間 (メール要素全体)

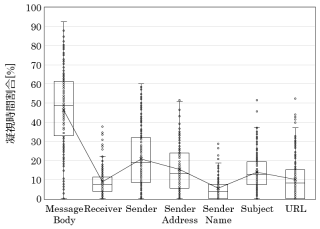

図 31　凝視時間割合 (メール要素全体)

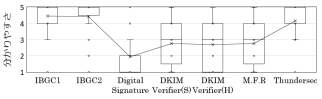

図 32　インジケータの判読性 (安全)

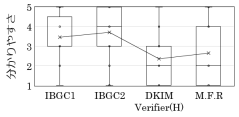

図 33　インジケータの判読性 (不明)

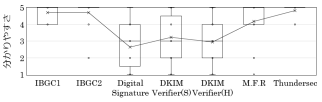

図 34　インジケータの判読性 (危険)

なった。アイコン+色+文字の 3 つで構成については、図 32〜図 34 より、この特徴に該当するインジケータである IBGC1, IBGC2, Thundersec が高い数値を示している。その中でも、IBGC1 と IBGC2 を比較すると、全ての状態 (安全/不明/危険) で画面の左側に表示する IBGC2 の評価が高くなっている。一方で、アイコン+色の 2 つから構成される M.F.R の危険を示すインジケータの結果 (図 34) も高い評価となっている。同手法における安全、不明のインジケータでは高い評価を得られなかったが、デザイン次第ではアイコン+色の構成においても分かりやすい設計が可能ということが分かる。

また、不明を示すインジケータでは安全と危険を示すインジケータと比べて、全体的に分かりやすさの評価が低くなっていることから、安全性が保証されない「不明」という状態がユーザにとって理解されにくいのではないかと推察できる。このような分かりにくいインターフェースこそ、改善の余地があると言える。

(2) 凝視率

メール画面の左側に表示するものが凝視率の高い評

価に最も影響し、アイコン+文字+色の 3 つで構成される特徴を持つ時も良い結果を示している。図 21〜図 23 を見てみると、前者の特徴と一致する IBGC2, DKIM Verifier(H), Thundersec が 80%以上で高い数値を示している。表示領域に余裕のある画面では、左側に情報が集中することが多いため、インジケータもこれに合わせて左側に表示する方が好ましいことが分かる。また、後者の特徴を持つ IBGC1, IBGC2, Thundersec も比較的高い数値を示している。

ここで IBGC1 の 3 つのインジケータのうち、危険を示すインジケータだけが凝視率が高くなった理由について考える。IBGC1 では送信者情報の右側にインジケータの表示するため、送信者情報の文字列が長くなるほど、インジケータの表示も右にずれて表示されることになる。危険を示すインジケータのメール画面における送信者情報は 17 文字で中央よりも左側にインジケータが表示されたが、安全, 不明の画面ではそれぞれ 40 文字,41 文字と長くなっているため、どちらも画面の右側の表示となってしまった。これが影響して凝視率が悪くなってしまったと考えられる。中央より右側で表示するインジケータは他にも M.F.R や DigitalSignature が該当し、これらは全て凝視率が低い結果となっていることから、インジケータの表示位置として右側は好ましくないということが分かる。

(3) 最初の凝視時間

最初の凝視時間の評価が高い特徴としては、アイコン+文字+色の構成で、メール画面の左側に表示をし、インジケータのサイズが大きいものが、これに該当した。図 24〜図 26 を確認してみると、アイコン+文字+色で構成される特徴を持つ IBGC1, IBGC2, Thundersec が高い評価となり、メール画面の左に表示する IBGC2, DKIM Verifier(H), Thundersec についても高い評価を示した。これらの 2 つの特性をもつ IBGC2 と Thundersec を比べた時、Thundersec の方が良い結果を示したが、Thundersec は IBGC2 の 8.5 倍 (安全を示すインジケータ)、もしくは 9.3 倍 (危険を示すインジケータ) となってる。大きなインジケータを使うほど視認しやすいのは当然のことで、例えば、画面全体の大きさのインジケータを用いれば、凝視率は必ず 100%になり、最初の凝視時間は 0 秒となる。凝視率にはこのサイズ差が大きな影響を及ぼさなかったが、最初の凝視凝視にはその差が大きく影響し、Thunderec の方が良い結果を示した。

次に、メール要素全体の結果 (図 31) を見てみると、なりすまし判定をする順番として、まず本文が一番最初に凝視され、続いてヘッダー部 (Receiver や Sender,Subject など)、最後に本文に戻って URL 等の細かい要素の確認をしているユーザの特徴が分かる。しかしながら 3.3.2 項で述べたように、メール画面が切り替わる際に、視線位置を中央に戻す画像を見せるため、なりすまし判定が始まった瞬間の視線位置も中央となり、これは本環境のメール画面における本文の場所に相当するので、本文の凝視が一番早くなるのは必然とも言える。

インジケータの最初の凝視時間の数値は 5 秒以内か、悪くても 7 秒以内に凝視されるように設計すべきである。このように言及したのは、図 31 を確認すると、ヘッダー部の全ての要素の凝視開始時間はおおよそ 5 秒以内、URL などの本文詳細はおおよそ 7 秒以内に行われる結果となっており、視認性の高いインジケータで文字だけの要素より早く視認できるからである。

(4) 凝視時間割合と凝視回数

どちらの結果も似たような特性を示したが、これらのパラメータを用いて可読性を評価するために以下のことを考える。

凝視時間割合の結果から可読性を評価するための条件は、判読性 (アンケート結果) の評価が高く、凝視率が近い数値となることである。判読性の評価が低い時には、ユーザがインジケータの意味を理解できないため、凝視の有無は関係なく判読性も低い評価となる。そのため、前提条件として判読性は高くなければならない。また、凝視時間割合は小さい程、一見可読性が高そうに思えるが、凝視率が低い場合にもこの値が小さくなってしまう。そのため、凝視率が近い数値のものについて比較を行うことができる。

この条件を用いて、凝視率が高く判読性が高評価であるインジケータ (IBGC2, Thundersec) の判読性の比較を行った結果、IBGC2 の方が良い結果となった。それぞれの凝視時間割合の比較すると、危険を示すインジケータ (図 29) では Thundersec が飛び抜けて高い数値となっており、インジケータの意味を理解するためのコストが大きく発生していることが分かる。この時の文字数は IBGC2 が 8 文字であるのに対して、Thundesec は 45 文字となっており、この文字数の差が判読性に大きく影響したと考えられる。

メール要素全体の結果 (図 31) では、本文や送信者のアドレスが大部分の凝視時間割合を占める結果となり、なりすまし判定における要素であると言える。本文においては、全体の半分の時間を費やしていることから一番重要な要素であると言える。

(5) 凝視時間割合のヒートマップ

メールインジケータを表示する場所によって、凝視時間割合の凝視点に差があり、メール画面の右側のインジケータと比べると左側の方が強い凝視反応が発生しやすい特性が得られた。IBGC1(図 13) と IBGC2(図 14) を比較すると、IBGC1 よりも IBGC2 の方が全て

© 2018 Information Processing Society of Japan

の状態で広範囲に赤の凝視点が出ていることから、この特徴が確認できる。

ステータスバーにインジケータを表示する機能を持つ DKIM Verifier(S.B) については、図 18 から分かるように凝視が全くされていなかった。アイコンの色の変化も影響がなく、すべての状態において凝視されないということは、この領域は視認性の悪い場所ということになり、インジケータを表示するために相応しい場所とは言えない。

凝視時間割合のパラメータ評価では高い値を示していても、高い凝視割合を持つ凝視点が少ないインジケータが確認された。DKIM Verifier(H) の結果 (図 17) より、緑と黄色の凝視点が多く、赤の凝視点が少ないことが確認できる。これはインジケータの意味が理解しにくく、その意味を考えながら読んでいたが、危険と判断する材料には至らなかったことを示している。不明を示すインジケータについては、アンケート結果より、判読性が特に悪い評価であったことから、他の 2 つのインジケータと比べと長く凝視されたと考えれる。

表示色が与える凝視の影響については、赤色が最も凝視されやすく、強い凝視を示す結果が得られた。先程のステータスバーのインジケータを除いて赤を基調としたインジケータには IBGC1, IBGC2, DigitalSignature, DKIM Verifier(S)、Thundersec などの危険な状態を示す時に使われており、すべてのインジケータで強い凝視反応が出ていることが確認できる。

4. おわりに

本研究ではメールインジケータの視認性と分かりやすさの特徴を調べるために、ユーザアンケートによる主観的評価と、ユーザがなりすましメールを判定する際の視線情報を用いて分析することで、その特性が明らかになった。視認性については、凝視率と最初の凝視時間で評価することができ、アイコン+文字+色の構成で、メール画面の左側に表示を行い、インジケータのサイズが大きいという特徴に該当するものが多いほど高評価が得られる特徴があった。分かりやすさの判読性については、アイコン+文字+色の構成が一番評価が高く、アイコン+色でもデザイン次第では高評価が得られる特徴が確認できた。可読性については、凝視時間割合や凝視回数を用いて一定量の比較ができ、判読性と視認性が高いインジケータに限定すると文字数の少ない IBGC2 が高評価が得られた。

今後の課題として、メール画面が小さくなった場合の調査や、ユーザのセキュリティ知識や精神状態が与えるインジケータの凝視への影響についての調査が挙げられる。

メール画面に余裕のある本想定環境では、画面の左側に本文の重心が寄った形となり、左側ほど視認性が高い結果となったが、メール画面が小さくなると、この重心が画面の中央に近づいてくるので、今回の結果とは異なる特性を示す可能性がある。

本研究におけるインジケータの凝視は、インジケータの意味を理解するために、少なくとも一度は凝視されるべきと考えて視認性の評価を行ったが、普段からインジケータをよく利用する人や、インジケータに関する知識がある人は、凝視の時間が一般のユーザに比べて短くなるため、新たな特性が得られる可能性がある。

インジケータはセキュリティインシデントとなる人的要因を緩和するためのツールであったが、インジケータを見るという行為自体にも精神状態が影響してしまう可能性もある。精神状態には、ストレスなどの精神的負荷の高まりだけでなく、なりすましメールの受信比率が影響する考えられる。受信比率が低くなると、ユーザはなりすましメールが少ないという安心感から判断を誤りやすく、逆の場合はなりすまし判定を慎重に行う可能性がある。現実のなりすましメールの受信比率は、情報漏えいによりメールアドレスが攻撃者の間で共有されていなければ低い数値となるはずである。このような現実に即した数値を使って特性を調べることができれば、実用的な結果が得られると考えられる。

謝辞 本研究を取り組むに当たり、本学情報科学領域の門林雄基教授、笠原正治教授、安本慶一教授、池田和司教授、大阪大学の奥田剛准教授、本学情報科学領域の妙中雄三准教授、樫原 茂助教、Doudou Fall 助教、東京大学の宮本大輔特任准教授には多大なるご指導を賜りましたこと、ここに厚く御礼申し上げます。研究を行う上で、本学サイバーレジリエンス構成学研究室の皆様に様々なご協力をいただき、深く感謝しております。

参考文献

[1] 宮本大輔. 認知心理学とサイバーセキュリティに関する一考察:視線分析の事例. In *SCIS 2017*, 2017 年.
[2] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, 2006.
[3] A. P. Felt, R. W. Reeder, A. Ainslie, et al. Rethinking connection security indicators. In *SOUPS*, 2016.
[4] Philippe Lieser. DKIM Verifer. `https://addons.thunderbird.net/ja/thunderbird/addon/thundersec`.
[5] Ilker Temir and Tim Sammut. ThunderSec. `https://addons.thunderbird.net/ja/thunderbird/addon/thundersec`.
[6] 伊藤俊一郎. セキュリティインディケータの改善によるなりすましメール対策の提案と評価. 電子情報通信学会 IPSJ-SPT 研究会, 2017 年 3 月.
[7] フィッシング対策協議会. `http://www.antiphishing.jp`.
[8] A. Poole, L. J. Ball, et al. In search of salience: A response-time and eye-movement analysis of bookmark recognition. In *People and Computers XVIII-Design for Life*, 2005.

© 2018 Information Processing Society of Japan