修士論文

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

2018 年 10 月 22 日

奈良先端科学技術大学院大学
情報科学研究科 情報科学専攻

本論文は奈良先端科学技術大学院大学先端科学技術研究科に
修士 (工学) 授与の要件として提出した修士論文である。

小野木　祐太

審査委員：

門林 雄基　教授　（主指導教員）
笠原 正治　教授　（副指導教員）
安本 慶一　教授　（副指導教員）
池田 和司　教授　（副指導教員）
奥田 剛　准教授　（大阪大学）

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

内容梗概

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おり、ユーザはこの技術を利用してメール送信者の真贋性を確認することができる。しかし、ユーザが確認が行わないような人的要因による過失が起こると危険な状態に晒されてしまう。このような過失を防ぐために、メールインターフェース上にはインジケータが実装されており、なりすましメールに気付きやすいユーザ環境が提供されている。しかし、インジケータの視認性や分かりやすさの有効性には不明瞭な点が多い。本研究では、この有効性を調べるために、既存のメールインジケータと異なる構成要素を持つ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取得する被験者実験を行う。この実験では、ユーザの視線情報を元に、凝視率、最初の凝視時間、凝視時間割合、凝視回数の4つのパラメータを取得し、視認性と分かりやすさを分析する。また、ユーザアンケートの調査により、インジケータの可読性の評価を行う。実験の結果から、視認性が高いインジケータの特徴には、メール画面の左側に表示されること、危険性を認識しやすいアイコン、文字、色の3要素で構成されることが確認された。判読性が高いインジケータについても、危険性を認識しやすいアイコン、文字、色の3要素で構成される時に最も高い評価を示した。可読性については、判読性が高く凝視時間割合や凝視回数が小さくなる時に高く評価できることが確認できた。追加の考察として、ユーザが今までにセキュ

*奈良先端科学技術大学院大学 情報科学研究科 情報処理学専攻 修士論文, 2018年10月22日.

リティ教育を受けたかどうかが、視線分析の結果に影響するかを調べた。セキュリティ教育を受けてない人は送信者情報に注目を置く傾向があり、セキュリティ教育を受けた人は、本文の凝視時間割合が高く、本文中に含まれる URL を早く見つける傾向が確認できた。

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, ユーザインタフェース, 視線分析

Visibility Analysis of Email Security Indicators based on Gaze Tracking*

Yuta Onogi

Abstract

Email spoofing, e.g., phishing email or business email compromise, has become a serious threat with the mainstream usage of email in our society. Various countermeasures have been developed for protecting end users by allowing them to check the authenticity of the email senders. However, end users are still vulnerable as they can misjudge the alerts raised by the countermeasures, which would lead them to commit crucial mistakes. In order to prevent such faults, security indicators have been implemented on modern mail user interfaces, making spoofed emails easier to notice. Nonetheless, to the best of my knowledge, the effectiveness of the indicators visibility and perspicuity are still unsatisfactory. In this thesis, I conducted a set of experiments where I introduced 2 components to exiting security indicators and explored their effectiveness by using gaze tracking while assessing the credibility of emails by users. During the experiments, I used 4 parameters – "Percentage Fixated," "First Fixation Duration," "Ratio of Fixation Duration," and "Fixation Count" – for analyzing the effectiveness of the indicators. After the gazing experiments, users evaluated the legibility of the indicators. The results showed that email indicators that are displayed in the left side of the e-mail forms tend to have a higher visibility. Additionally, indicators which information contents are composed of icons, texts and colored areas were

*Master's Thesis, Department of Information Processing, Graduate School of Information Science, Nara Institute of Science and Technology, October 22, 2018.

more efficient to help end users recognize security risk. Indeed, our evaluation showed that the aforementioned types of indicators performed better in regards to legibility. The evaluation showed also that the combination of a high legibility and a low ratio of fixation duration or less fixation count allowed all the indicators to perform better in regards to readability. Furthermore, I investigated whether the level of security education of the end users affected the results of the gaze tracking analysis. The investigation showed that the users who did not receive security education tend to check the name of the sender of the email and their address. In contrast, the users with security education tend to gaze the email body and rapidly find URLs from the message.

Keywords:

Spear-phishing e-mail, Security Indicator, E-mail authentication, UI, Gaze Tracking

目 次

目 次

表 目 次

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いる一方で、サイバー犯罪者にとって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する手法には、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」があり、フィッシング対策協議会 [1] によれば被害件数は毎年増加を続けている。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。フィッシング攻撃の例として、会員制のウェブサービスや有名企業を騙って ID やパスワードなどの会員情報を抜き取るものや、インターネットバンキングを偽ってクレジットカード情報を抜き取るものがあり、会員情報や利用規約の変更を理由に悪意のあるサイトに誘導するための偽の URL を本文中に記載することでその攻撃を行う。BEC の例としては、最高経営責任者 (CEO) や最高財務責任者 (CFO) になりすまして送金を指示するものがある。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、ウィルス対策ソフトウェア、メーラーフィンガープリントを用いた伊藤の研究 [2] など、エンドユーザの安全を守る技術に関する様々な対策が研究されてきたが、攻撃の報告は毎年増加する一方である。

セキュリティインシデントに対する被害の要因には、セキュリティの技術的要因だけでなく人的要因が考えられ、人間の精神状態やセキュリティ知識の不足が影響する [3]。人間の精神状態として、ストレスなどの精神的負荷の高まりは過失を起こしやすい環境を発生させる。また、フィッシング攻撃の被害は、セキュリティ知識の不足が原因となっており [4]、なりすましメールに関しても同様のことが言える。

このような人的要因による過失を軽減するために、メールインターフェース上にはインジケータが実装されており、なりすましメールに気付きやすいユーザ環境が提供されている。しかし、インジケータの視認性や分かりやすさの有効性は十分な議論が行われておらず、不明瞭な点が多い。これらの有効性を調べるため、本研究では様々な種類のメールインジケータを用いて、ユーザがなりすましメール

の真贋判定を行う際の視線情報を取得する被験者実験を行う。メールインジケータには、既存手法に加えて、ウェブインジケータの研究を元に作成した既存手法が持たない構成要素を持った 2 種類のものを用いる。これらのインジケータを用いたユーザの視線検知の実験により、インジケータの有効性とユーザがメール画面のどこに重要と感じる要素があるかを考察する。

本論文の構成について述べる。2 章では、なりすましメールの対策手法やユーザインターフェース、インジケータに関する関連研究について述べる。3 章では、メールインジケータの要件定義と、分析に用いる新たなメールインジケータの設計、視線分析実験によりメールインジケータの有効性について考察する。4 章では、追加の考察としてセキュリティ教育の有無が実験の結果に影響されるかを調べた結果とその特徴について言及を行い、本手法の問題点と今後の課題について分析する。最後に 5 章で本研究で得られたメールインジケータのインターフェースに関する研究のまとめを行う。

2. 関連研究

この章ではメールインジケータの有効性を調べるために、より良いユーザインターフェースの設計とインジケータの関連研究について述べる。2.1 節ではユーザインタフェースの関連研究を、2.2 節ではウェブインジケータの関連研究、2.3 節では既存のメールインジケータを、2.4 節ではメールインジケータの関連研究を述べる。

2.1 ユーザインターフェースの関連研究

ユーザの過失を減らすためには適切なユーザインターフェースを提供しなければならない。なりすましメールにおいて、なりすまし検知の対策手法を導入することで、ある程度の精度で判別ができるが、ユーザがこの意味を正しく理解しなければその効果は発揮できない。

Norman は認知科学の分野で「7 つのデザイン原則」を提唱しているが、インターフェースに適用すると以下のように定義できる [5]。

1. 発見可能性
   ユーザは目で見ることによって、装置の状態とそこでどのような行為が行えるかを判断できる。

2. フィードバック
   フィードバックとは、ユーザの要求に対してシステムが動いていることを知らせる手段である。その手段は視覚的な表現に限ったことではなく、音によるフィードバックも有効である。

3. 概念モデル
   概念モデルはモノがどのように動くのかの説明であり、通常は簡素化されている。デザインは理論と制御感に繋がるように、システムの良い概念モデルを作るのに必要な情報を伝える。概念モデルは、発見可能性と評価の両方を向上させる。

4. アフォーダンス
   アフォーダンスとは、対象となる物とそれを利用する主体 (ユーザ) との間に「どのような行為が可能か」という関係のことを示す。インターフェースにおいては、目に見えるアフォーダンスはモノを操作する時に強力な手がかりを提供するが、知覚されないアフォーダンスは存在しないのと同義である。望ましい行為を可能にするために適切なアフォーダンスを提供しなければならない。

5. シグニファイア
   シグニファイアとは、ユーザに適切な行動を促すためのデザイン上の手がかりのことである。アフォーダンスをユーザが知覚し、その意味を理解するにはシグニファイアが重要な鍵となる。インターフェースに関しては、その属性 (形状、材質、色など) がユーザに対して、どのような機能を持っているのかを発信するシグニファイアを持っていると考えることができる。例えば、ウェブ上で使われるボタンのインターフェースには「クリックすることができる」というアフォーダンスが存在しているが、ボタンのデザインを凸型にしたり枠で囲うデザインであるシグニファイアを使うことで、過去

の経験則からユーザはその意味を知覚しやすい環境となる。効果的にシグニファイアを利用することによって、発見可能性を確かなものにし、フィードバックが理解可能な形で伝えられる。

6. 対応付け
   対応付けとは、操作手段とその動きという 2 つのものの間で、現実世界に及ぼす結果の間の関係のことである。自然な対応付けを行い、マニュアルやラベルが無くても操作できるような設計をすべきである。

7. 制約
   「できないこと」を明確にすることによって、デザインの有効性を単純化し、エラーを最小限に抑えることができる。制約は以下の 4 つに分類できる。

   - 物理的制約
     物理的に規定されるもの。
   - 意味的制約
     状況や外界への知識に依存するもの。
   - 文化的制約
     文化的慣習に基づくもの。
   - 論理的制約
     論理的な推測に基づくもの。

また、物理的世界に働きかけて何らかの目的を果たそうとする時に要求される処理の段階を表したモデルとして、Norman は「行為の 7 段階モデル」を提唱している [5]。なりすましメール判別におけるインジケータのデザインを設計する場合に、ユーザの行為は次のように考えることができる [2, 5]。

1. 目標の設定
   何らかの行為を行うための目標を定める。即ち、メールを確認し、内容に合わせて処置を決定する行為 (返信、保留等) である。

2. 操作意図の形成
   目標を達成するためにどのような操作が必要になるかを考える。即ち、受信メールを開いて、内容を確認する行為である。

3. 操作系列の生成
   必要な操作の順序を考える。即ち、受信メール一覧を表示し、未読メールを選択後、内容を確認するまでの順序を考える行為である。

4. 操作の実行
   生成した操作系列を実行する。

5. 結果の知覚
   実行した結果を知覚する。即ち、インジケータの存在を認識する行為である。

6. 結果の解釈
   知覚した情報を解釈する。即ち、インジケータの正確な意味を理解する行為である。

7. 結果の評価
   解釈した情報を元に目標が達成できたかを評価する。即ち、インジケータの認知的負荷の軽減が達成できたかを評価する行為である。

なりすましメールにおいて、操作の実行までの段階ではユーザの精神状態が影響することはないが、操作の実行を終えた後の 3 つの段階において攻撃の被害に遭遇する危険性がある。インジケータの視認性が悪い場合、ユーザはなりすましメールの危険性を知覚できないため、次の段階の結果の解釈で正規メールと誤った解釈をしてしまう。そのため、インジケータには視認性の高いインターフェースが求められる。しかし、正確な意味を知覚できても、その意味が正しく理解できなければ添付ファイルや悪性の URL などを誤ってクリックしてしまう可能性がある。そのため、インジケータは正確な意味の伝達ができる設計でなければならない。最後の段階として、結果の解釈を行う上でユーザに認知的負荷をかけるのは、優れたユーザインタフェースとは言えない。ユーザに正確な意味を伝える

ための情報は十分になければならないが、その情報量が多すぎたり、認識に時間がかかるような設計であってはならない。

2.2 ウェブで使われるインジケータの関連研究

ブラウザのウェブインジケータは、2000 年代半ばに盛んに研究が行われていた。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ウェブインジケータを表示していたが、現在では URL バーだけの表示となっている。

ユーザは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、最低でも現在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。

ユーザに受信したメールの安全性や危険性を知らせる方法として、パッシブインジケータとアクティブインジケータの 2 つがある [6]。パッシブインジケータはユーザのタスクを遮らずに警告を行えるインジケータである。パッシブインジケータの有効性については、EV SSL(Extended Validation Secure Sockets Layer) を評価した研究がある。この研究では、EV SSL 証明書を使った Web サイトは通常の SSL を用いた Web サイトよりも、Web サイト所有者の情報を発見しやすくなったという結果が示されている。しかし、一方で Wu らの研究 [7] や Egelman らの研究 [8] では、フィッシング詐欺からユーザを守るには、パッシブインジケータはアクティブインジケータよりも効果的でないとしている。2 つの研究で比較に用いたパッシブインジケータは、アドレスバーや文字の色付け、文字列、マークによる警告である。

Whalen らの視線追跡データを収集した調査 [9] によれば、南京錠のアイコンは相互作用なしに一般的に見られることが確認されている。しかし、EV 証明書のインジケータはユーザにほとんど見られていない。Sobey らによれば、Firefox の EV SSL 証明書のインジケータについて、全てのユーザが気が付かない結果が出ている [10]。また、Jackson ら [11] によれば、Internet Exporer 7.0 の EV SSL 証明書のインジケータは、ピクチャ・イン・ピクチャ攻撃やホモグラフ攻撃に対して、悪性サイトかどうかを判別するのに効果がない特性がある。ピクチャ・イン・

ピクチャ攻撃とは、本物のウェブサイトを偽装するために、ウィンドウを覆い隠し、下にあるコンテンツを隠す手法である。一方、ホモグラフ攻撃は、URL のテキストを本物のサイトに酷似させることで偽装し攻撃を行う手法である。ホモグラフ攻撃の例を以下に示す。

- G**0**OGLE.COM
  全角アルファベットの O の代わりに数字の **0** を混ぜて偽装
- googl**I**e.com
  半角アルファベットの l の代わりに全角アルファベットの **I** を混ぜて偽装
- **rn**icrosoft.com
  m の代わりに **r** と **n** の 2 つを混ぜて偽装

図 1 Pan らによる SSL 証明書が有効でない時のインジケータ

図 2 Pan らによる SSL 証明書が有効な時のインジケータ

Pan ら [12] は Firefox で使われる SSL 証明書のインジケータを Norman のデザイン原則に基づいて、図 1 と図 2 のように設計した。既存の SSL 証明書は、URL バーの左側にボタンとして表示されるが、ユーザにクリックされる可能性は低い。明示的なクリック表記を持つボタンはクリックされる可能性が高い [13] ため、Pan らの手法ではインジケータに CLICK というラベルのインジケータを加えている。インジケータのアイコンは、インジケータの機能とデザインの対応付けが適切に行えるメタファーを使うべきであるとして、南京錠のデザインを採用している。メタファーとは一般には隠喩のことであるが、ユーザが理解しやすい物に例えて、インターフェースを直感的に操作できるようにするものである (例:自宅のアイコ

ン ⇒ ホームページを開く操作)。南京錠の色が、灰色の時はウェブ接続に SSL が使われていない (安全でない) 状態を示し、金色の時は SSL が使われている (安全な) 状態を示す。

このインジケータの被験者実験の結果では、インジケータのサイズの大きさから既存のインジケータより注目を集めたが、ほとんどクリックはされることはなかった。また、CLICK という文字はクリック操作を促すウイルスのような振る舞いに誤解される可能性もあり、Secure、web、information などの文字が適切である可能性があると言及されている。

アイコンと色と警告文の 3 つを用いたウェブインジケータの研究として、A.P.Felt らの研究 [14] がある。この研究では、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) を利用して調査を行い、ユーザが理解しやすいインジケータを提案している。具体的には、8 種類のアイコン形状 (図 3)、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対象の構成要素とし、その中からウェブサイトの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。

図 3　A.P.Felt らが調査に用いたウェブインジケータの形状一覧

図 4　A.P.Felt らが 3 種類に選定したウェブインジケータの形と色

最初に選定したのは図 4 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”

これらを元に再度 GCS でユーザ調査を行い、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”

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 5 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。

2.3 メールで使われる既存のインジケータ

この節では、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 Thunderbird で使われるメールインジケータの紹介を行う。

- 電子署名
  S/MIME[15] は Thunderbird に標準搭載しているセキュリティ技術であり、PGP[16] については Thunderbird アドオンである Enigmail をインストール

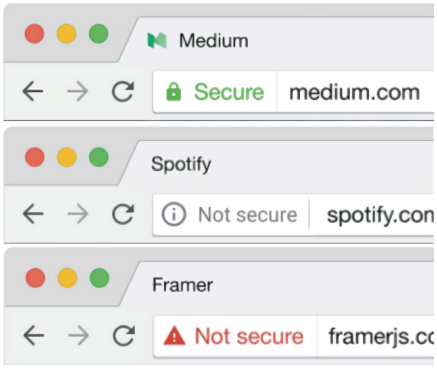

図 5　A.P.Felt らが提案するウェブインジケータ

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 6 に表す。図 6 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。

図 6　電子署名で使われるメールインジケータ

- DKIM Verifier[17]
  Thunderbird 上で DKIM[18] 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 7、以降 DKIM Verifier(S) と表記する)、DKIM ヘッダの表示 (図 8、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 9、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[19]

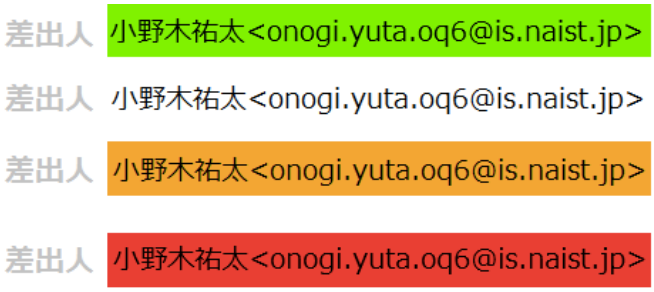

図 7 DKIM で使われる背景色強調のメールインジケータ [DKIM Verifier(S)]

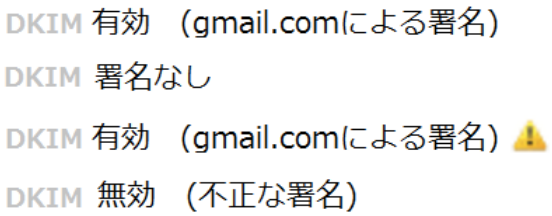

図 8 DKIM で使われるヘッダのメールインジケータ [DKIM Verifier(H)]

図 9 DKIM で使われるステータスバーのメールインジケータ [DKIM Verifier(S.B)]

Thundersec は、DNSBL(DNS-based Blackhole List)、RBL(Realtime Blackhole List(RBL)、DKIM、SPF[20] 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 10 のような通知バーによる表示を行う。図 10 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。

図 10　Thundersec で使われるメールインジケータ

2.4　メールで使われるインジケータの関連研究

メールで使われるインジケータについて、送信者の顔写真を用いた研究と画像を用いた研究を紹介する。

メールインジケータに送信者の顔写真を用いた研究として Waterhouse[21] がある。Waterhouse では、送受信者が SNS の友人の関係にある時に暗号化メールのやり取りができ、図 11 のようなインターフェースでセキュリティ状態の表示を行っている。PGP で暗号化された安全なメッセージを開いた時には、2 つのインジケータの表示を行い、送信者の名前と顔写真を表示するインジケータと、安全を示す文字を表示するインジケータがある。それぞれのインジケータの背景色は緑色で強調される。危険なメッセージの場合、危険を示す文字のインジケータのみの表示としている。このメールシステムでは、実在する人物の名前と写真を偽装した SNS アカウントを使ってメールを送ることでなりすましが可能ではあるが、送信者と受信者の共通の友人の数が一定数以下となる場合に、公開鍵を信用しないような仕組みが議論されている。

また、画像を用いたインジケータに伊藤の研究 [2] がある。この手法では、2.1 節で述べた「行為の 7 段階モデル」を元に、存在の認識、正確な意味の伝達及び人的負荷の軽減を考慮した図 12 のようなインジケータ (以降 M.F.R と表記する) を設計している。M.F.R では、正確な意味の伝達と認知的負荷を軽減するために

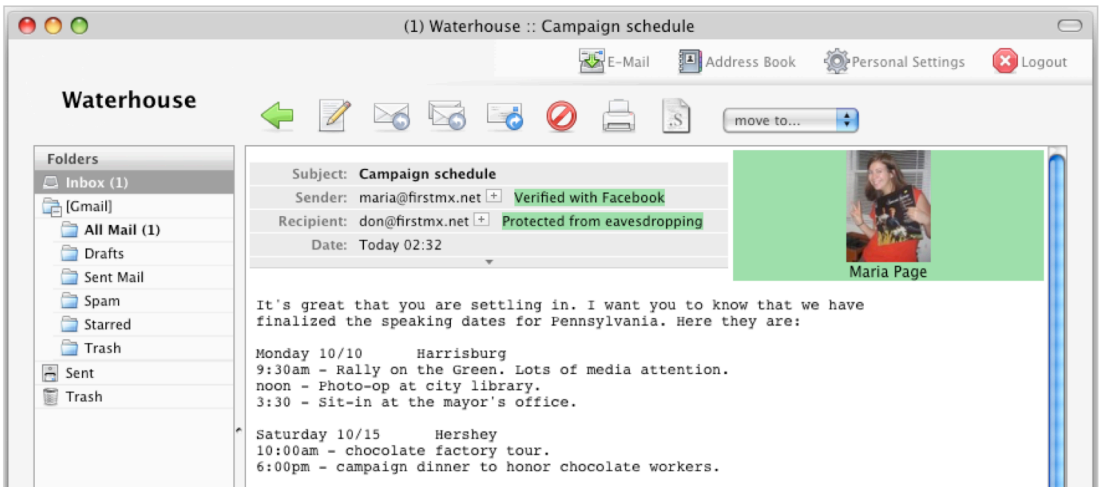

図 11　Waterhouse のメールインターフェース

図 12　伊藤が提案するメールインジケータ (M.F.R)

日本人の文化的制約を考慮した設計を行っている。安全を示すインジケータは、作業現場で安全を意味するものとして用いられることから「緑の十字」の画像を使用し、不明を示すインジケータは疑問を表すものとして「疑問符」の画像を、危険を示すインジケータは交通機関で危険性の注意を促す色として使われる「黄色」を、画像には毒性を示す「ドクロ」を使っている。形については、セキュリティ状態を区別するためにそれぞれを分けているが、文化的制約は用いられていない。

また、M.F.R. では存在の認識を効果的なものにするために、インジケータの表示位置を認知するための自然な対応付けができるような設計を行っている。M.F.R. ではメール送信者の認証結果をユーザに伝えるのが目的であるので、送信者情報を強調することが自然な対応付けである。このことから、送信者ヘッダにインジケータの表示を行っている。しかしながら、送信者ヘッダには他にも表示領域が存在していることから、この表示場所が最適であるとは言えない。

インジケータの認識はユーザのストレスに影響される。伊藤 [2] によれば以下のような特性が確認されている。ストレスが多いユーザはメールを確認する際の時間的制約があることにより、認知的負荷の少ないインジケータを好み、通知バーなどの文字の内容を読まない傾向がある。

また、図のようなセキュリティ状態の保証する範囲が限定的なものについては、ユーザがその危険性を理解するために、範囲に応じてインジケータの表示を変えるべきである [2]。

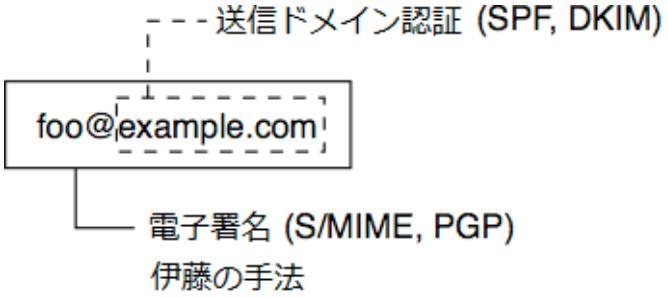

図 13 セキュリティ状態の保証する範囲について

2.5 問題分析

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メールインジケータの存在が認識できない (視認性が悪い) 場合や、正確な意味が把握できない (判読性が悪い) 場合には対策手法の効果は発揮されない。また、メールインジケータは認知的負荷が小さくなる (可読性が高くなる) ように設計しなければならない。これらの条件を満たすメールインジケータについて、その有効性は十分に議論されておらず、不明瞭な点が多い。このゆうクオ性を調べるために、本研究では、既存のメールインジケータが持つ構成要素と異なるものを作成し、分析した結果をまとめる。

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有効性についてまとめる。

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。

- 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を検証した結果を提示するが、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セキュリティ状態別に 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の効果を示すことはできない。そのため、ユーザがインジケータを認識しやすい場所や、認識しやすいデザインに設計する必要がある。
2. 提示される情報の理解しやすさ
   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。

本研究では、インジケータの視認性と理解しやすさの有効性を調べるのが目的であるため、セキュリティ面の要件は満たされているものする。

3.2 新たに設計するメールインジケータ

メールインジケータの視認性や分かりやすさの有効性を調べるために、既存のメールインジケータが持たない構成要素のメールインジケータを設計する。2.2 項で述べた、実際に Google Chrome で採用された A. P. Felt らの提案手法を参考に以下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、ここで設計するメールインジケータでは安全を示す色が緑色、不明を示す色が黒色、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したいので、文化的制約として日本人が分かりやすい文言を選ぶほうが効果的である。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。メールインジケータは送信者の真贋性を表すインジケータであることから、表示場所について差出人情報の近くに表示を行うのが自然な対応付けと言える。そのため、そのため差出人情報の近くに表示を行う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 14 に、右側に表示するセットを Indicator Based Google Chrome Pattern2(IBGC2) として図 15 に表す。

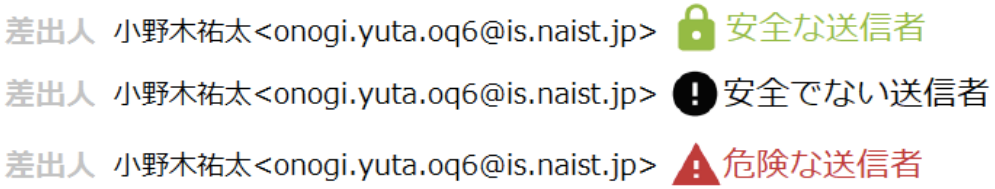

図 14　本研究で提案するメールインジケータ IBGC1

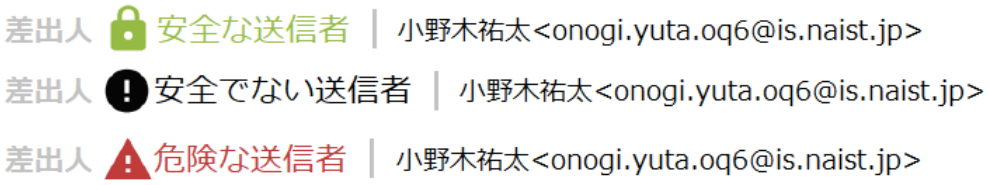

図 15　本研究で提案するメールインジケータ IBGC2

3.3　実験

この節では、メールインジケータのユーザインターフェースの有効性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性をまとめる。

図 16　本実験で用いる視線認識装置「Tobii Pro TX300」

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、図 16 のような 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、2.4 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、標準の設定では視線認識装置の誤差が大きいため、差出人や件名、受信者などのメール要素の個々を識別するのが困難であった。そのため、視線認識装置が認識しやすいように差出人、件名、宛先の文字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。

本文については、執筆者の元に実際届いた安全な正規メールと、フィッシング対策協議会 [22] に報告された危険ななりすましメールの 2 種類を使い、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真贋性 (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。実際に使用するメール画面は全 16 画面で、それぞれの画面を付録の図 28 〜図 43 に表す。

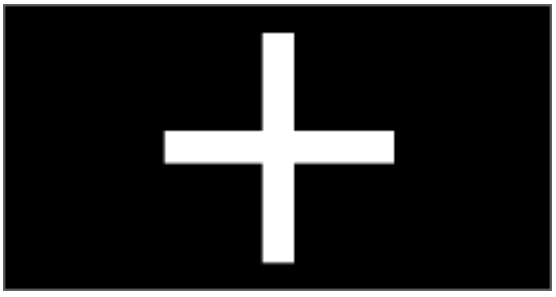

図 17 視線位置の初期化

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、一度視線情報をリセットする必要がある。これを行うため、図 17 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

視認性分析の実験を行うために集める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の真贋判定を行うため、日本人を対象とする。
- 被験者の詳細
  1. 1 回目の調査 2018 年 5 月 19 日 (土) に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で行われるオープンキャンパスに参加する日本人学生に対して、実験の趣意の同意が取れた 4 名を対象とした。
  2. 2 回目の調査 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) となるので、実験の実施に移る。

3. 実験実施

- 視線認識実験の誤差

  実際に、キャリブレーション結果が緑色の状態において、どの程度の誤差が生じるのかを計測するために、図 18 に表したような画面を被験者に見せ、①→②→ … →⑨までそれぞれ 1、2 秒程度見つめてもらう。

  これにより、数字の位置と実際に観測された視線認識位置にどれくらいの誤差が生まれるのかを検証できる。

- サンプル画面

  メール画面において送信者の真贋判定を行う画面は、サンプル画面 (図 19) からスタートする。その理由は、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、送信者の真贋判定 (○/△/×) を 20 秒

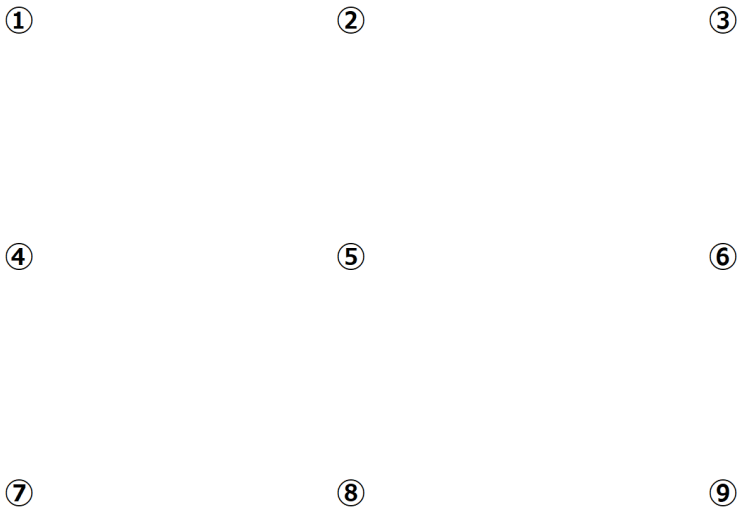

図 18　視線認識精度を調べるための画像

図 19　サンプル画面

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アンケートに記入してもらう。アンケートの対象者は、3.3.3 項の 2 回目の募集で集まった被験者 17 名である。アンケート内容については次節にて説明を行う。

3.3.5 アンケート内容

この項では、被験者実験後に被験者が記入を行うアンケート内容の詳細を述べる。

1. メールインジケータの分かりやすさ

   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。

2. メールインジケータの重要度

   ユーザにとってのメールインジケータの重要度を調べるために、以下のような文面を記載した。

   本実験で、送信者のなりすまし判定 (○/△/×) にあたって、セキュリティ警告を何%くらい判断材料として考慮に入れましたか。

3.3.6 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

   視線認識装置の「Percentage Fixated」で計測されるパラメータである。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

   視線認識装置の「Time to First Fixation - seconds」で計測される最初に凝視されるまでにかかった時間を表すパラメータである。　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。凝視が一度もされなければ、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してしまうと本来よりも高い評価をつけることになってしまう。そのため、この場合につける悪い評価として、被験者がなりすまし判定にかけた合計時間を適用することで、パラメータの調整を行った。

3. 凝視時間割合

   視線認識装置の「Total Fixation Duration - seconds」で計測されるパラ

メータに対して、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

視線認識装置の「Fixation Count」で計測されるパラメータである。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 [23]。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。

3.3.7 被験者の選別

被験者の中には、キャリブレーションの結果が緑色であるにも関わらず、視線認識精度の低い人が複数人見られた。1 回目の調査では 4 人全員が、2 回目の調査では 17 人の内、4 人がこれに該当した。視線認識精度の低い人の一例を図 20 に表し、認識精度の高い人の一例を図 21 に表す。これらの図は図 18 の画面を被験者が見たときの視線情報を表すヒートマップである。

本実験で用いるヒートマップは凝視時間割合の大きさに応じて色付けしたものであり、図 22 のように、緑色が凝視時間割合が小さい凝視点を示し、黄色、赤色と変色するにつれて、この割合が大きくなる注視点の集合図となっている。視線認識精度の高い人の例では数字とほとんど重なるように凝視点が分布しているのが確認でき、視線認識精度が低い人は数字から少し離れた点に凝視点がずれてしまっているのが確認できる。

注視点のずれがメール画面でどのような影響を与えるのかを示すために、今回の被験者全 21 名の視線認識結果結果の一例 (図 23) と前述の 8 名を除いた 13 名の視線認識結果の一例 (図 24) で比較を行う。

被験者全員の結果 (図 23) では、送信者のなりすましを判定する時の特徴として、「差出人と件名」、「メールインジケータと件名」に繋がる連続的な凝視として強い反応が確認できるが、視線認識精度の高い人のみの結果 (図 24) では、差出人とメールインジケータのそれぞれの強い凝視に留まっている。つまり、本来

図 20　視線認識精度が低い人の視線情報

図 21　視線認識精度が高い人の視線情報

図 22　ヒートマップの見方

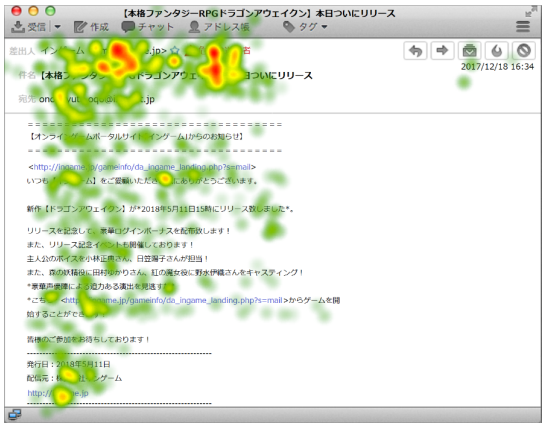

図 23　視線認識精度の低い人を含むメール画面上の視線情報の例

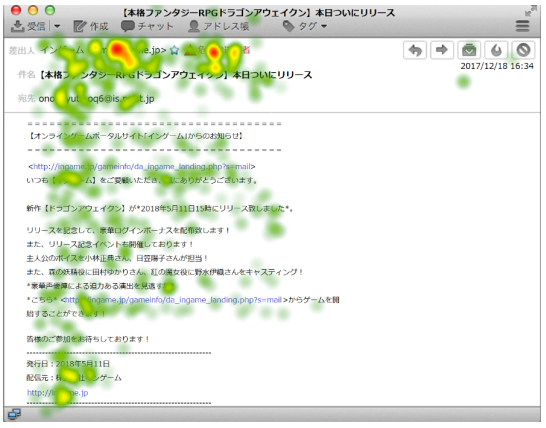

図 24　視線認識精度の低い人を除いたメール画面上の視線情報の例

であれば差出人やメールインジケータを凝視した場合に、認識精度の悪い人がいれば、隣接する要素である件名の凝視をしたと誤認識してしまうことになる。

メールヘッダ領域には送信者名や送信者アドレス、件名、宛先、インジケータなど様々な要素があり、隣接する上下の要素間での距離が特に短くなっているため、認識精度の低い人で誤認識が発生しやすい。

視線認識精度を調べる画像においてはこのメールヘッダ領域に該当する場所が①〜③である。

このような状態では、どのメール要素の凝視かを正確に測定することができないため、①〜③の注視点のズレが、視線認識精度を隣接するメール要素 (例えば送信者名と件名) の間の余白の大きさ (36px) 以下となるように被験者の選別を行った。そして、この被験者を視線認識精度の高かった人として、精度の高かった人のみの結果 (13 名分) を用いて分析を行う。

3.3.8 実験結果

前項の被験者の選別を踏まえた実験結果として、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 44〜図 51 に表す。3.3.6 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 52〜図 67 に表す。それぞれ、横軸がメールインジケータの種類、縦軸が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は図 55、図 59、図 63、図 67 に表すが、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。

アンケート結果については分かりやすさのアンケート結果を図 25〜図 27 に示す。アンケートは視線認識精度の良し悪しの影響がないため、17 人分のデータを記載する。

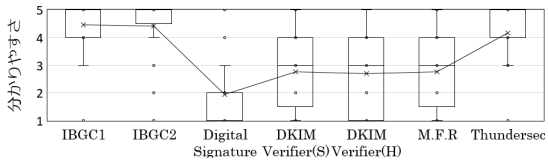

図 25 インジケータの分かりやすさ (安全) - アンケート結果

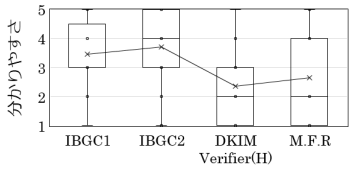

図 26 インジケータの分かりやすさ (不明) - アンケート結果

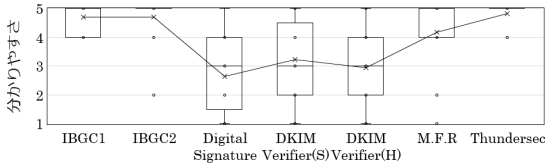

図 27 インジケータの分かりやすさ (危険) - アンケート結果

表 1 なりすまし判定の一致率

インジケータの判定	IBGC1	IBGC2	DigitalSignature	DKIM Verifier	M.F.R	Thundersec
安全	87	76	24	59	47	76
不明	12	12		12	18	
危険	59	65	24	65	82	59

3.3.9 実験の分析と考察

この項では、前項の結果から分析したメールインジケータの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。尚、本研究では統計的な有意差を求める有意水準に 5%を採択し、比較検討を行う。また、比較を行う際の 2 つの標本のいずれかに正規性が認められない (Shapiro-Wilk の正規性検定) ことが確認されたため、ノンパラメトリックな検定である MannWhitney の U 検定で有意差検定を行う。

1. メールインジケータの分かりやすさ (判読性)

   判読性は危険性を認識しやすい「アイコン、文字、色」の 3 要素で構成されるか、「アイコン、色」の 2 要素で構成される時に高い評価を示した「アイコン、文字、色」の 3 要素で構成されるインジケータについては、図 25〜図 27 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。一方で、「アイコン、色」の 2 要素で構成される M.F.R の危険を示すインジケータの結果 (図 27) も高い評価となっている。同手法における安全、不明を示す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 2 要素で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、全体的に判読性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可能性が高い。このような分かりにくいインターフェースは、改善の余地があると言える。

2. 凝視率

   凝視率はメール画面の左側に表示される特徴を持つ場合が一番高い評価となり、危険性を認識しやすい「アイコン、文字、色」の 3 要素で構成される特徴を持つ場合においても良い結果を示している。図 64〜図 66 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内、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 (図 30) 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、安全と不明を示すインジケータのメール画面 (図 28、図 29) では、それぞれ 40 文字、41 文字と文字数が多いため、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、危険性を認識しやすい「アイコン、文字、色」の 3 要素での構成で、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 52〜図 54 を確認してみると、危険性を認識しやすい「アイコン、文字、色」の 3 要素で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 つの特徴を持つ IBGC2 と Thundersec の間には有意差がなかった。安全を示すインジケータにおいて、IBGC2 と Thundersec の有意差検定を行った結果 ($W=96.5$, $p=0.555(\geq 0.05)$) より有意差はないことが確認された。同様に、危険を示すインジケータの有意差検定を行った結果 ($W=116$, $p=0.112(\geq 0.05)$) より有意差はないことが確認された。

次に、メール要素全体の結果 (図 59) 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 59 を確認すると、ヘッダ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結果を示したが、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条件を考える。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、凝視率が高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、凝視率が高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、危険を示すインジケータにおいて IBGC2 の方が良い結果となった。凝視時間割合の結果 (図 58) を確認すると比較すると、Thundersec が一段と高い数値を示しており、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。具体的な比較については、IBGC2 と Thundersec の有意差検定を行った結果 ($W=31$, $p=0.00507(<0.05)$) より有意差はないことが判明した。そ

れぞれのインジケータの文字数について、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 59) 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傾向が確認された。IBGC1(図 44) と IBGC2(図 45) を比較すると、IBGC1 よりも IBGC2 の方が全ての状態で広範囲に赤の凝視点が出ていることから、この傾向が確認できる。

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 49 から分かるように凝視が全くされなかった。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、ステータスバー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 48) より、緑色と黄色の凝視点が多く、強い凝視反応を示す赤色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されにくいため、ユーザはその意味を考えながら読んだが、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て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。

6. DKIM Verifier(s) について

DKIM Verifier(s) の背景色強調機能は、なりすましメールの真贋判定において重要な送信者情報を強調しているため、送信者情報のもつ注目度などのインジケータのパラメータと単純に比較することはできない。前述の結果より、送信者情報は背景色が強調されていなくても、早い段階で凝視が行われ、凝視率や凝視時間割合、凝視回数も高い結果が得られている。そのため、送信者情報を強調したものと強調してないものに分けて結果の比較を行う。図71〜図74は背景色強調の機能について4つのパラメータを用いて性能比較を行ったものである。サンプル数を少しでも多く増やすために、強調なしのデータは、視認性分析実験に用いた全16画面の内、安全と危険の背景色強調を除いた14画面分のデータを用いている。

背景色強調機能により、緑色は最初の凝視時間を早める効果が確認できたが、赤色については確認できなかった。図71の最初の凝視時間について、緑色と強調なしの有意差検定を行った結果 ($W=138$, $p=0.0219(<0.05)$) では有意差が確認できたが、赤色と強調なしの有意差検定の結果 ($W=1197$, $p=0.212(\geq 0.05)$) では有意差が確認されなかった。このことから、今回の被験者のユーザ群においては、赤色よりも緑色の方が視認性が高いということが言える。

一方で凝視時間割合と凝視回数は強調なしと比べると、強調したことにより値が小さくなったように見えるが、前述の結果から、この結果は文字数にも影響される要素のため、今回の結果から正確な比較を行うことはできない。具体的な文字数を比較してみると、送信者名と送信者のアドレスの文字数 (ピリオドを含む) の合計が、DKIM Verifier(s) の安全のメール画面では23文字、危険のメール画面では25文字であるのに対して、それらを除くメール画面の平均で30文字となっている。背景色強調による凝視時間割合と凝視回数の差異を正確に言及するためには、送信者情報が平均で

ある 30 文字程度となるように設定した上で分析をしなければならない。

7. なりすまし判定の結果

   インジケータの表示と被験者のなりすまし判定がどの程度一致したかの一致率について表 1 に表す。アンケートから得られたインジケータの重要度は 57.9%であり、一致率がこれを上回る評価が得られれば、インジケータとしての効果がある程度発揮できていると判定できる。

   一致率を見てみると、安全を示すインジケータではIBGC1、IBGC2、DKIM Verifier、Thundersec が、危険を示すインジケータでは IBGC1、IBGC2、DKIM Verifier、M.F.R、Thundersec がこの数値を超えた。

   しかしながら、不明を示すインジケータではどれも 20%を下回る低い評価となった。インジケータの不明を示す状態を考えると、インジケータからなりすまし判定ができなかった状態であるので、ユーザの取るべき好ましい姿は、本文やその他のメール要素からなりすましを判定することである。この中に、なりすましメールと思うような怪しい要素を一つでも発見したら危険と判定し、そのような要素が一つもなければ安全と判定するのが正しい行為であるので、一致率が低くなったと考えられる。

8. インジケータの大きさについて

   インジケータの大きさとして、大きいものを使うほど、凝視率と最初の凝視時間は高い評価になるのは当然である。極端に言えば、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。本実験で用いたそれぞれのインジケータの大きさを表 2 に表す。

   このインジケータの大きさを用いて、効果的な設計が出来ていたかを検討する。安全を示すインジケータの中で、比較的視認性の高かった、IBGC2、DKIM Verifier(H)、Thundersec の大きさについて、IBGC2 を基準に考えてみると、DKIM Verifier(H) は 1.3 倍、Thundersec は 8.5 倍となり、Thundersec については大きく差がついていることが確認できる。DKIM Verifier(H) については、ユーザの分かりやすさの数値が低いことが影響して凝視時間

表 2 インジケータの大きさ [px]

インジケータの判定	IBGC1	IBGC2	DigitalSignature	DKIM Verifier(H)	M.F.R	Thundersec
安全	5643	6270	2856	7810	14161	53544
不明	7008	7616	–	3108	15129	–
危険	4988	5760	4047	5704	15694	53544

割合や凝視回数が高くなっていた。DBGC2 と Thundersec の間に凝視時間割合や凝視回数にそれぞれ大きな差がなかったことを考慮すると、IBGC2 は小さなインジケータながら、比較的視認性の高い評価を示したと言える。同様に危険を示すインジケータについて、Thundersec は IBGC2 の 9.3 倍の大きさとなるが、凝視時間割合や凝視回数の観点で Thundersec が高い評価を示したので、こちらに関しては、サイズを考慮してどちらが効果的であったかは言及できない。

4. 考察

4.1 セキュリティ教育が与える本実験の認識結果への影響について

本実験の結果が被験者のセキュリティ知識によって影響されるかを調べるため、ユーザがこれまでにセキュリティ教育を受けたかどうかで結果の分類を行う。セキュリティ教育については、学校の授業や会社の研修、講演会等でセキュリティ教育を受けたかどうかを対象とした。

インジケータの評価の差については、セキュリティ教育を受けた人のデータが 11 人分であるのに対して、セキュリティ教育を受けてない人のデータが 3 人分しかないため、特性についての言及ができない。そのため、メール画面を跨ぐ全体の分析であれば 3 人× 16 画面=48 のサンプル数となるので、特性の比較が行える。

メール画面全体の結果として、セキュリティ教育を受けてないユーザ群は、送信

者情報に比較的注目を置く傾向が見られた。図 81 と図 82 より、凝視率もセキュリティ教育を受けてないユーザ群の方が高い評価を得ている。また、送信者情報の最初の凝視時間 (図 75、図 76) について、有意差検定の結果 (W=1690, p=1.61E-3(<0.05)) から有意差は確認され、セキュリティ教育を受けたないユーザ群の方が送信者情報を早く見つける傾向があることが分かる。同様に、送信者情報の凝視時間割合 (図 77、図 78) や凝視回数 (図 79、図 80) に有意差検定を行った所、凝視時間割合 (W=3140, p=0.0232(<0.05)) と凝視回数 (W=3170, p=0.0183(<0.05)) に有意差が確認された。つまり、セキュリティ教育受けてないユーザ群の方が送信者情報を高い時間割合で、何度も見る傾向があることが分かる。

セキュリティを受けたユーザ群の特徴としては、本文の凝視時間割合が高く、本文中の URL を早く見つけ出す傾向が確認できた。本文の凝視時間割合 (図 77、図 78) について、有意差検定を行った結果 (W=3140, p=0.0232(<0.05)) より有意差は確認され、セキュリティ教育を受けたユーザ群の方が本文の凝視時間割合が高くなることが確認できる。同様に、URL の最初の凝視時間 (図 75、図 76) についても有意差検定を行った結果 (W=0.964, p=0.153(≥0.05)) より有意差が確認され、セキュリティ教育を受けたユーザ群の方が本文中の URL を早く凝視し始める傾向が分かる。本文中の URL は悪性サイトのリンクとなっている危険性があるため、これに早く気付けるためのセキュリティ教育の効果が一定量確認できた。

4.2 本手法の問題点

4.2.1 メガネを着用する人の特性

レーシック手術を受けた人や眼鏡をかけている人は、認識の精度が低く、今回のメール視認性分析の結果として使えない形となってしまった。こういう人達に向けて、今回使ったメール画面の要素同士が更に離れるようにデザイン修正すれば可能ではあるが、誤差を許容するためには要素同士の間隔を大幅に大きくする必要があり、そのような状態では通常のメール画面と違う形になり、視認性にも影響が出る恐れがある。

そこで普段から眼鏡を用いている人達の特徴を測るためには、ウェラブルメガ

ネを用いることで可能になると考えられる。ウェラブルメガネとして現在普及している製品には、 Google の Google Glass やソニーの Smart Eye Glass、東芝の Wearvue TG-1、テレパシージャパンの Telepathy Walker などがあり、視線検知が可能な製品には Tobii Pro Glasses2 や JINS MEME などがある。これらの視線検知が可能なウェアラブルメガネを利用することで眼鏡を使用する人の特徴も捉えられることができる。

4.2.2 本文のランダム性

メール画面を構成する要素であるメールインジケータとメール文面の組み合わせとして、通常のメールとなりすましメールの 2 種類をそれぞれのメールインジケータに対してランダムに割り当てたが、被験者毎にその組み合わせを変更することなく同じ組み合わせのものを用いている。完全なランダム性を持たせるには、メールインジケータだけでなく、すべての被験者に対してランダムな規則が必要になる。完全なランダム性が保証された環境で同じ実験を行えば、新しい結果とそこからわかる性質が得られると考えられる。

4.2.3 現実に則したデータの使用

実験に用いるデータは現実に則した値を使用すべきである。本実験で使用したメール文面は、正規のものと危険ななりすましメールの比率が 1:1 となるように設定したが、現実のデータを考えると、これよりも低い値となっているはずである。なりすましメールの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。なりすましメールの受信比率はユーザの精神状態に影響を与える要素であるので、これを適切な値に設定することで、より実用的な結果が得られると考えられる。

4.3 今後の課題

4.3.1 個人特性とユニバーサルデザイン

ユーザの個人特性には、年齢、性別、人種、文化、言語、国籍、能力の差、盲目や色覚異常などの障害有無などがあるが、それぞれの個人特性に合わせた制約を作ることで、個人に特化した有効性の高いインターフェースを作ることができる。本研究で新たに作成したメールインジケータは、文化的制約として、個人特性の中の「人種」を制限することで日本人に分かりやすい文言を加えることで有効性の高い結果を得ることができた。しかし、制約をより完全な形にするには、インジケータの文言だけでなく、形や色にも適用すべきである。A.P.Felt のウェブインジケータの研究では、ユーザ調査の属性としてアメリカ人の割合が高く、形や色にはアメリカ人の個人特性を持った文化的制約が可能性がある。日本人に効果的なインジケータを設計するためには、ユーザ調査を日本人に絞って行うべきである。

しかしながら、本来の理想からすれば、個人特性に依らず全ての人々に効果的なインターフェースとしてユニバーサルデザインを目指すべきある。日本においても、2020 年に東京オリンピックの開催に伴い「ユニバーサルデザイン 2020 行動計画」[24] の取り組みが行われており、ICT の分野においても情報のバリアフリーが期待されている。そのため、全ての人に効果的なメールインターフェースについて検討すべきである。

4.3.2 メール画面の大きさについて

本研究では、表示領域に余裕がある場合のメールインジケータの有効性を調べたが、メール画面の大きさによって視認性の特徴が変わる可能性がある。画面を広くすると、本文の右側に空白スペースが生まれ、画面中に表示されている文字の重心が中心よりも左に移動してしまうことにより、ユーザの注視点も左寄りとなる。表示領域に余裕のない画面においては、本文も右端まで表示される可能性が高くなり、重心が中央に近づいてくるので、今回の実験と異なる有効性が得られると考えられる。

メール画面の表示領域に余裕がない場合の例が、スマートフォンやタブレットなどのモバイル端末である。モバイル端末では、本実験で用いたような大きな視線認識装置は使えないが、モバイル端末に搭載されている前面カメラを用いて視線検知を行うことができる。通常のカメラを用いて視線検知をリアルタイムかつ高精度に行う研究に NEC の「遠隔視線推定技術」[25] がある。この視線検知技術では上下左右 5 度以内の誤差で視線検知が可能となっている。モバイル端末の前面カメラでの応用を考えると、ある程度画面に近づいて視線検知を行うことで、本実験と同様の視認性分析が行えると考えられる。

4.3.3 インジケータの凝視について

本研究では、インジケータの意味を理解するためには凝視されるべきという前提のもとに視認性の有効性を分析したが、この動作には必ずしも凝視を伴う必要がない場合が考えられる。

その例として考えられるのが、セキュリティに精通したユーザの場合である。セキュリティに精通したユーザの場合、一般のユーザと比べてインジケータの意味を知っている可能性が高く、その意味の理解も速く行えるはずである。本研究では、セキュリティ教育が与える影響について分析を行ったが、ユーザのセキュリティ知識には 0、1 で表せない多くの段階がある。実際にユーザの中には、セキュリティ教育を受けたが真面目に受けていないため実際には知識が得られていない人や、教育を受けてから長い年月が経ち内容を忘れてしまった人、セキュリティ教育を受けただけでなく更に勉強を重ねた人など異なるセキュリティ知識を持つ人が確認された。ユーザのセキュリティレベルを正確に反映するためには、セキュリティテストをユーザに受けてもらい、その点数に応じて分析を行うことで、より正確な影響を調べることができる。

その他の例として考えられるのが、インジケータを導入したメールシステムを長期に渡って利用した場合である。本研究では、メールインジケータを新しく導入する際に視認性を調べたことになるが、ある程度の期間を使用してメールインジケータに慣れた環境になると、有効性の結果が変わる可能性が高い。メールインジケータに慣れたユーザは、その意味を理解するための認知的負荷が小さくな

るため、判読性が高くなる。そのため、メールインジケータをしっかり見なくとも、その存在が認識できればセキュリティ状態が分かるようになる。

いずれのインジケータも凝視の特徴だけでなく、「サッカード」と呼ばれる短時間に高速な視線移動を繰り返すことで情報を取り入れる眼球運動の特徴を分析することで、直感的に認識できるインジケータを調べることができると考えられる。

5. 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有効性を調べるために、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た被験者実験を行った結果を分析することで、その有効性が明らかになった。その結果、視認性が高いインジケータの特徴には、メール画面の左側に表示されること、危険性を認識しやすい「アイコン、文字、色」の3要素で構成されることが確認された。判読性が高いインジケータについても、危険性を認識しやすい「アイコン、文字、色」の3要素で構成される時に最も高い評価を示した。可読性については、判読性が高く凝視時間割合や凝視回数が小さくなる時に高く評価できることが確認できた。追加の考察として、ユーザが今までにセキュリティ教育を受けたかどうかが、視線分析の結果に影響するかを調べた。セキュリティ教育を受けてない人は送信者情報に注目を置く傾向があり、セキュリティ教育を受けた人は、本文の凝視時間割合が高く、本文中に含まれるURLを早く見つける傾向が確認できた。

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有効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。

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] フィッシング対策協議会. フィッシングレポート 2017 普及が進むユーザ認証の新しい潮流. https://www.antiphishing.jp/report/pdf/phishing_report_2017.pdf (2018 年 10 月 21 日閲覧).

[2] 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. 修士論文, 奈良先端科学技術大学院大学 情報科学研究科, 2017 年 3 月.

[3] 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 *Symposium on Cryptography and Information Security (SCIS) 2017*, 2017 年.

[4] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pp. 581–590, New York, NY, USA, 2006. ACM.

[5] D. A. ノーマン, 岡本明, 安村通晃, 伊賀聡一郎, 野島久雄. 誰のためのデザイン? 増補・改訂版 –認知科学者のデザイン原論. 新曜社, 2015.

[6] Jason Hong. The state of phishing attacks. *Commun. ACM*, Vol. 55, No. 1, pp. 74–81, January 2012.

[7] Min Wu, Robert C. Miller, and Simson L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pp. 601–610, New York, NY, USA, 2006. ACM.

[8] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pp. 1065–1074, New York, NY, USA, 2008. ACM.

[9] Tara Whalen and Kori M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, GI '05, pp. 137–144, School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 2005. Canadian Human-Computer Communications Society.

[10] Jennifer Sobey, Robert Biddle, P. C. Oorschot, and Andrew S. Patrick. Exploring user reactions to new browser cues for extended validation certificates. In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security*, European Symposium on Research in Computer Security (ESORICS) 2018, pp. 411–427, Berlin, Heidelberg, 2008. Springer-Verlag.

[11] Collin Jackson, Daniel R. Simon, Desney S. Tan, and Adam Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security*, pp. 281–293, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[12] Pan Shi, Heng Xu, and Xiaolong (Luke) Zhang. Informing security indicator design in web browsers. In *Proceedings of the 2011 iConference*, iConference '11, pp. 569–575, New York, NY, USA, 2011. ACM.

[13] Joanna McGrenere and Wayne Ho. Affordances: Clarifying and evolving a concept. In *Proceedings of the Graphics Interface 2000 Conference, May 15-17, 2000, Montr'eal, Qu'ebec, Canada*, pp. 179–186, May 2000.

[14] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 1–14, Denver, CO, 2016. USENIX Association.

[15] Sean Turner and Blake C. Ramsdell. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. RFC 5751, January 2010.

[16] Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880, November 2007.

[17] Philippe Lieser. DKIM Verifer. `https://addons.thunderbird.net/ja/thunderbird/addon/thundersec/` (2018 年 10 月 21 日閲覧).

[18] Murray Kucherawy, Dave Crocker, and Tony Hansen. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376, September 2011.

[19] Ilker Temir and Tim Sammut. ThunderSec. `https://addons.thunderbird.net/ja/thunderbird/addon/thundersec/` (2018 年 10 月 21 日閲覧).

[20] S. Kitterman. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208, April 2014.

[21] Alex P. Lambert, Stephen M. Bezek, and Karrie G. Karahalios. Waterhouse: Enabling secure e-mail with social networking. In *CHI '09 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '09, pp. 4099–4104, New York, NY, USA, 2009. ACM.

[22] フィッシング対策協議会. `http://www.antiphishing.jp/` (2018 年 10 月 21 日閲覧).

[23] Alex Poole, Linden J. Ball, and Peter Phillips. In search of salience: A response-time and eye-movement analysis of bookmark recognition. In Sally Fincher, Panos Markopoulos, David Moore, and Roy Ruddle, editors, *People and Computers XVIII — Design for Life*, pp. 363–378, London, 2005. Springer London.

[24] ユニバーサルデザイン 2020 行動計画. https://www.kantei.go.jp/jp/singi/tokyo2020_suishin_honbu/ud2020kkkaigi/pdf/2020_keikaku.pdf (2018 年 10 月 21 日閲覧).

[25] NEC. 遠隔視線推定技術. https://jpn.nec.com/physicalsecurity/technology/gaze_technology.html (2018 年 10 月 21 日閲覧).

付録

A. メールインジケータの有効性についての要約

本研究は、表示領域に余裕のあるメール画面場合に限定し、どのような特徴を持つインジケータが効果的であったかを簡潔に述べる。

1. 視認性が高いインジケータの特徴
    - メール画面の左側にあるに表示している
    - 危険性を認識しやすい「アイコン、文字、色」の 3 要素で構成される
2. 判読性が高いインジケータの特徴
    - 危険性を認識しやすい「アイコン、文字、色」の 3 要素で構成される時に最も高い
    - 危険性を認識しやすい「アイコン、色」の 2 要素で構成される時にも比較的に高い評価
3. 可読性が高いインジケータの特徴
    - 前提条件として判読性が高くなければならない
    - 凝視時間割合や凝視回数が小さくなる時に可読性が高く評価できる

表示領域に余裕のある画面では、本文の文字が左側に集約されることが多いため、インジケータの表示も左側の方が好ましく、視認性も高い特性が得られる。ヘッダの中央や差出人情報の右側に表示を行うインジケータについては、差出人や件名などの文字数が長さによっては、インジケータの表示位置が右側に移動し、視認性の低下に繋がってしまうことを考慮すべきである。

B. メール画面の一覧と結果の詳細データ

この章では、3.3 節で説明した視認性分析の実験で用いたメール画面の一覧と、実験結果である凝視時間割合のヒートマップの一覧と、3.3.6 項で述べた 4 つのパラメータを用いた分析結果の一覧を記載する。

図 28 IBGC1(安全) のメール画面

図 29 IBGC1(不明) のメール画面

図 30 IBGC1(危険) のメール画面

図 31 Chrome2(安全) のメール画面

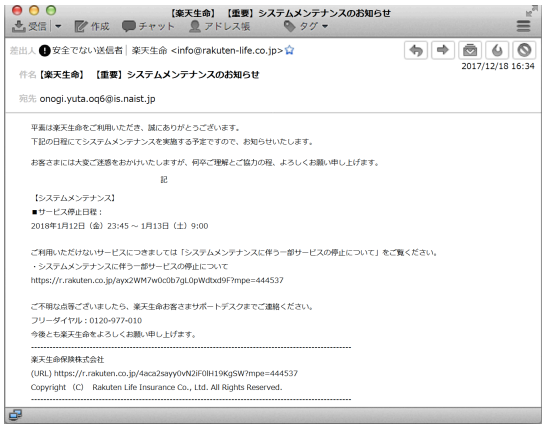

図 32 Chrome2(不明) のメール画面

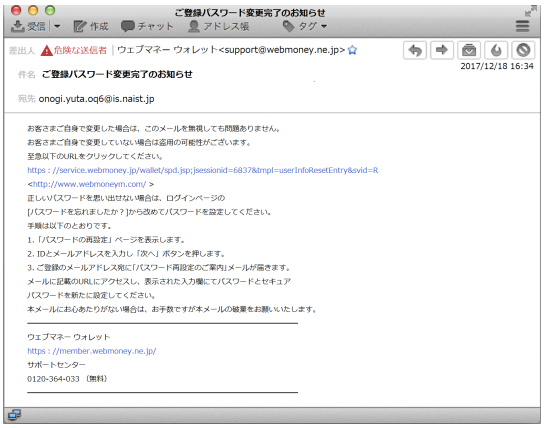

図 33 Chrome2(危険) のメール画面

図 34 S/MIME(安全) のメール画面

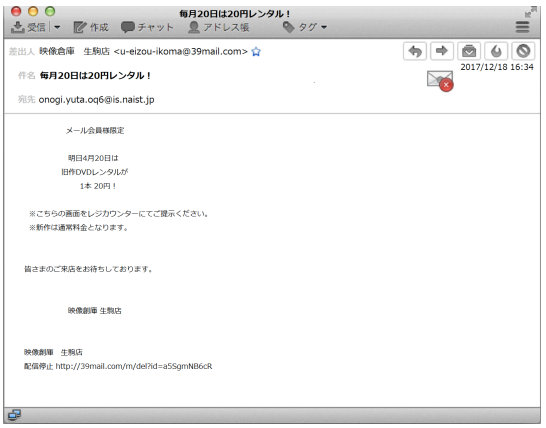

図 35 S/MIME(危険) のメール画面

図 36 DKIM(安全) のメール画面

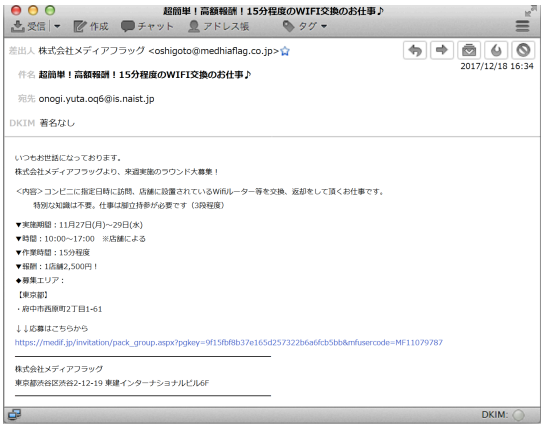

図 37 DKIM(不明) のメール画面

図 38 DKIM(危険) のメール画面

図 39 M.F.R.(安全) のメール画面

図 40　M.F.R.(不明) のメール画面

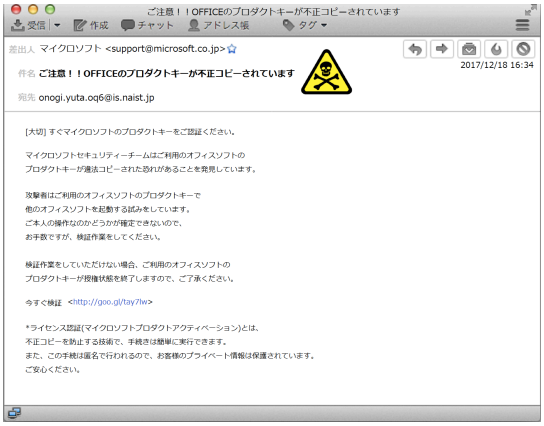

図 41　M.F.R.(危険) のメール画面

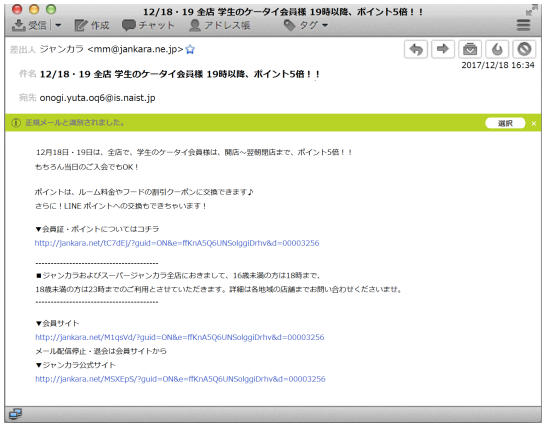

図 42　Thundersec(安全) のメール画面

図 43　Thundersec(危険) のメール画面

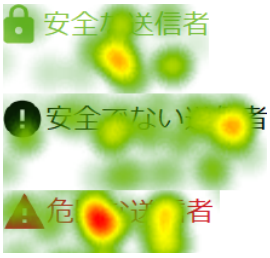

図 44　IBGC1 のヒートマップ

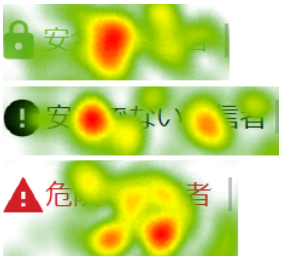

図 45　IBGC2 のヒートマップ

図 46　DigitalSignature のヒートマップ

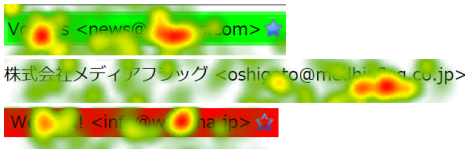

図 47　DKIM(S) のヒートマップ

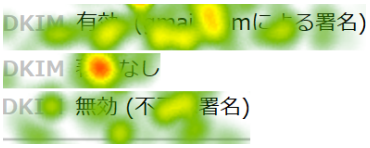

図 48　DKIM(H) のヒートマップ

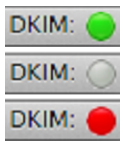

図 49　DKIM(S.B) のヒートマップ

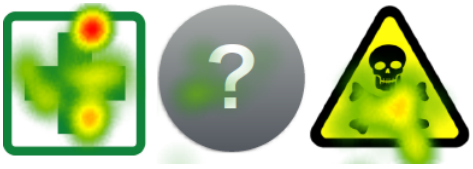

図 50　M.F.R. のヒートマップ

図 51　Thundersec のヒートマップ

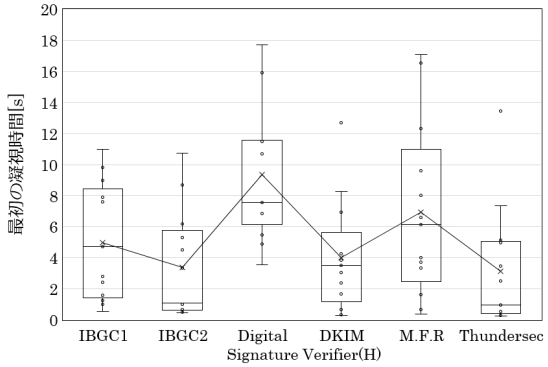

図 52 最初の凝視時間 (安全を示すメールインジケータ)

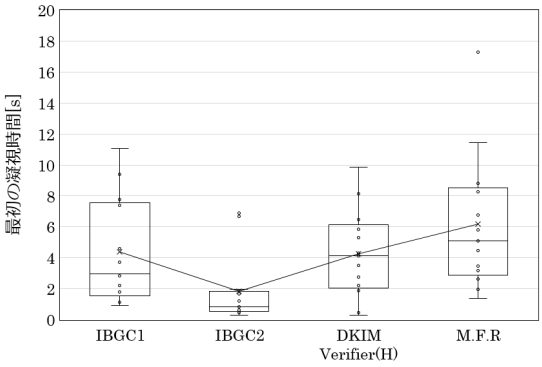

図 53 最初の凝視時間 (不明を示すメールインジケータ)

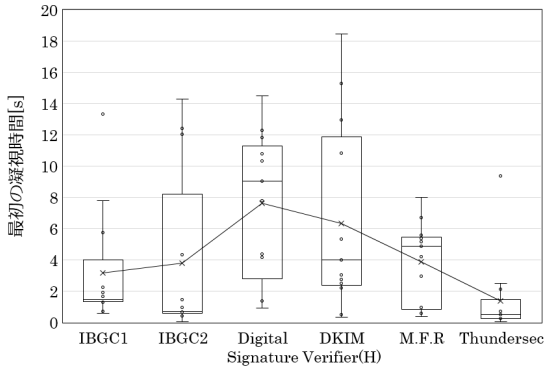

図 54 最初の凝視時間 (危険を示すメールインジケータ)

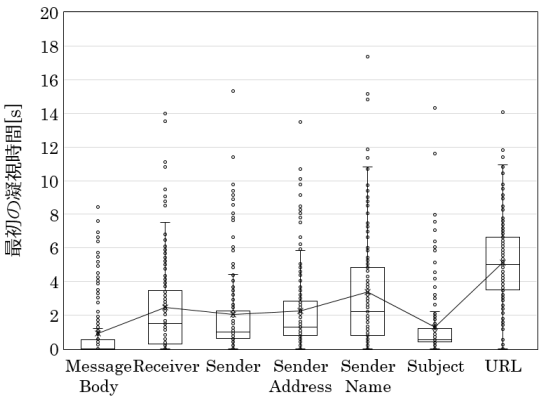

図 55 最初の凝視時間 (メール要素全体)

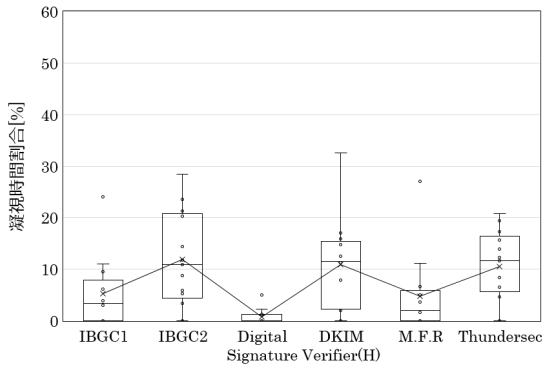

図 56 凝視時間割合 (安全を示すメールインジケータ)

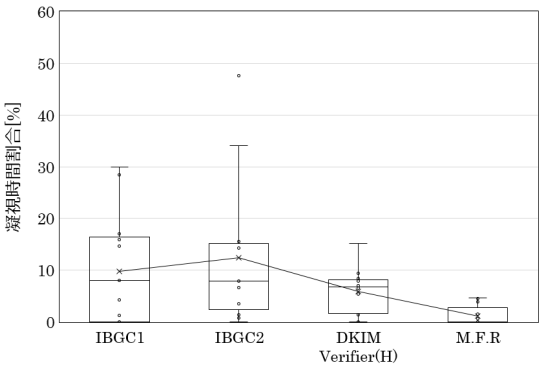

図 57 凝視時間割合 (不明を示すメールインジケータ)

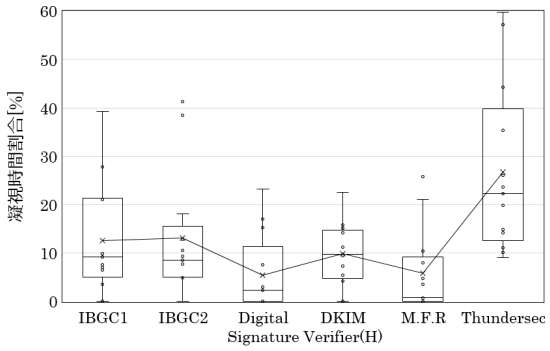

図 58 凝視時間割合 (危険を示すメールインジケータ)

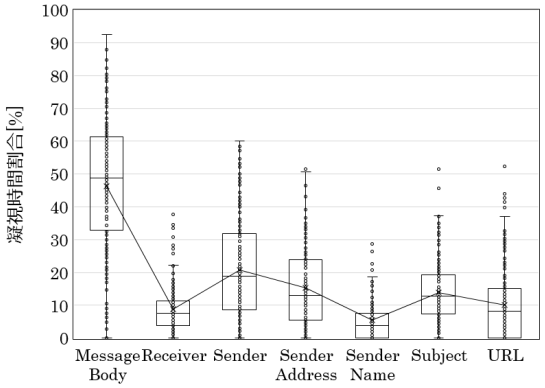

図 59 凝視時間割合 (メール要素全体)

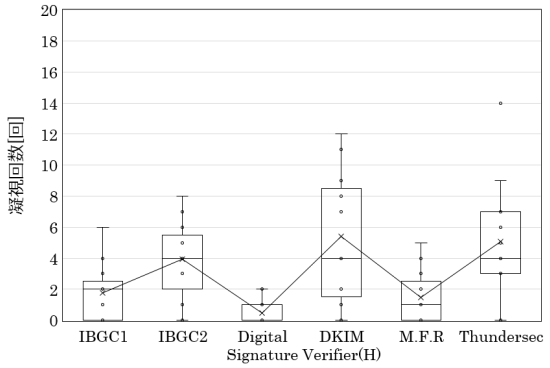

図 60 凝視回数 (安全を示すメールインジケータ)

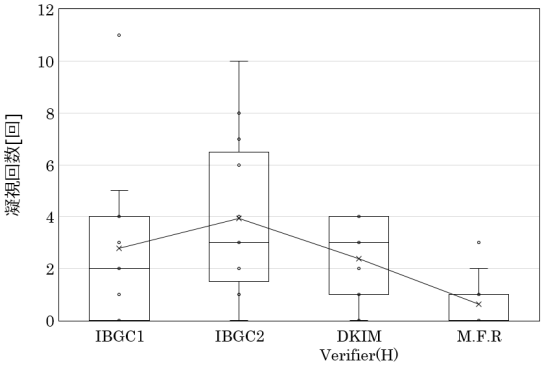

図 61 凝視回数 (不明を示すメールインジケータ)

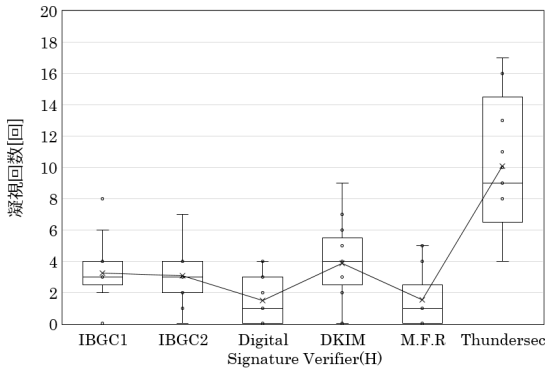

図 62 凝視回数 (危険を示すメールインジケータ)

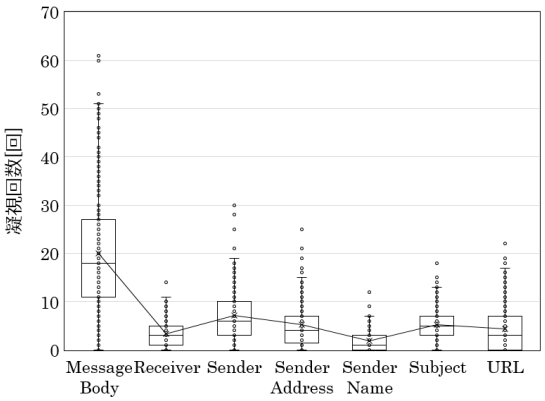

図 63 凝視回数 (メール要素全体)

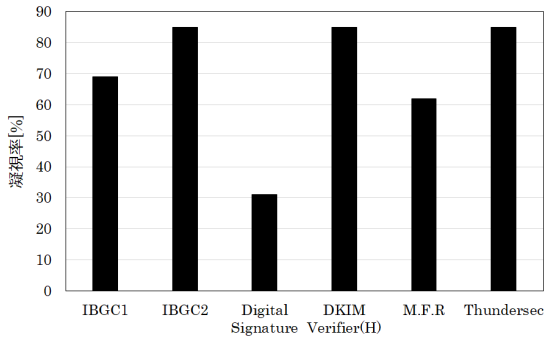

図 64 凝視率 (安全を示すメールインジケータ)

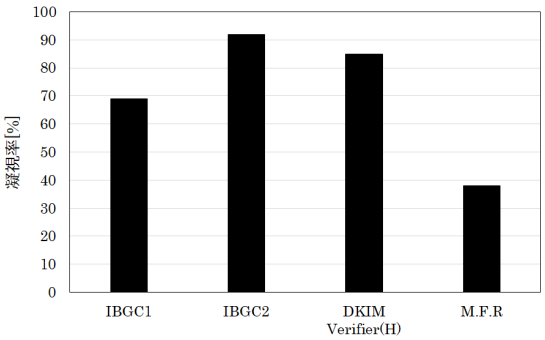

図 65 凝視率 (不明を示すメールインジケータ)

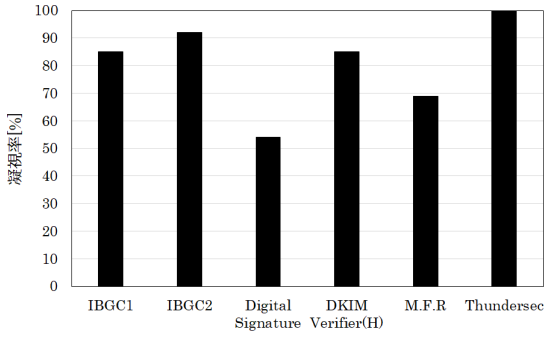

図 66 凝視率 (危険を示すメールインジケータ)

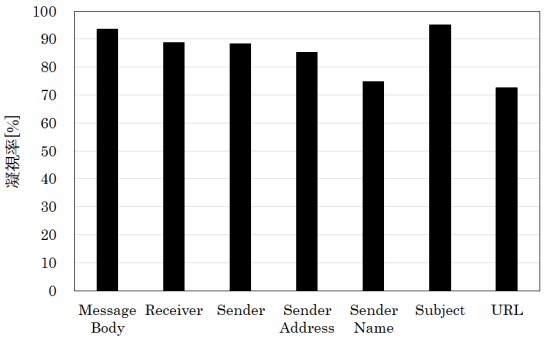

図 67 凝視率 (メール要素全体)

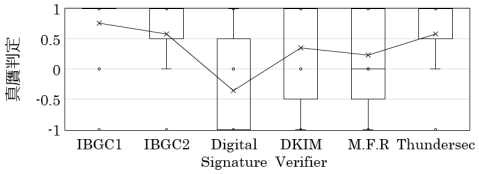

図 68 なりすまし判定 (安全)

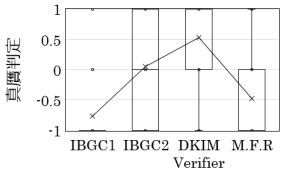

図 69 なりすまし判定 (不明)

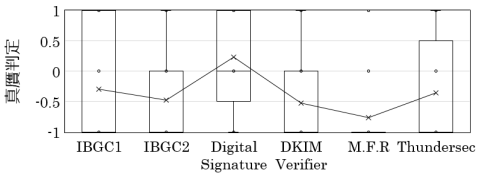

図 70 なりすまし判定 (危険)

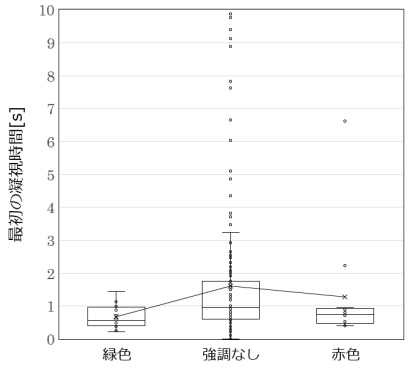

図 71 背景色強調による凝視開始時間の差

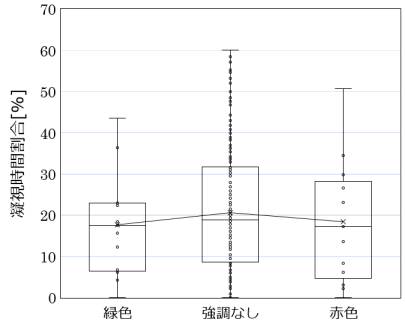

図 72 背景色強調による凝視時間割合の差

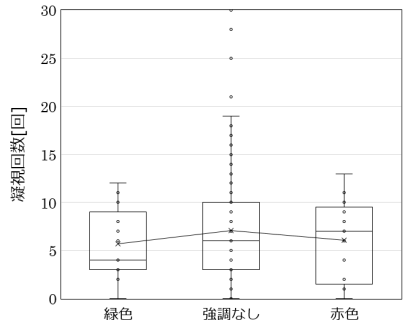

図 73 背景色強調による凝視回数の差

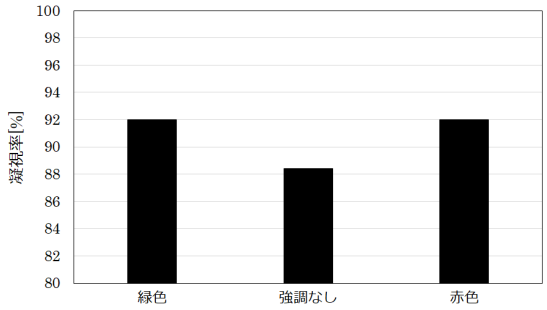

図 74 背景色強調による凝視率の差

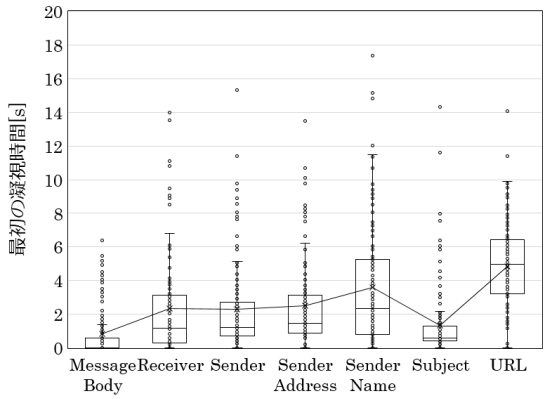

図 75 最初の凝視時間 (セキュリティ教育有)

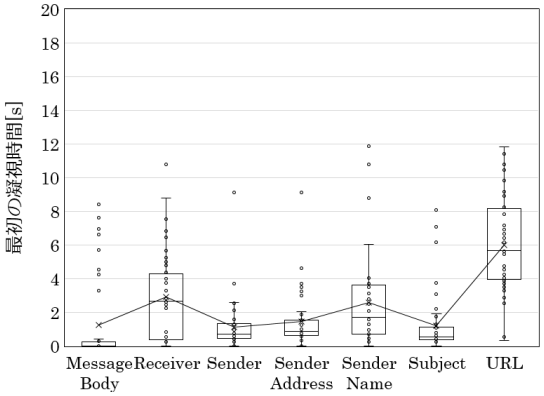

図 76 最初の凝視時間 (セキュリティ教育無)

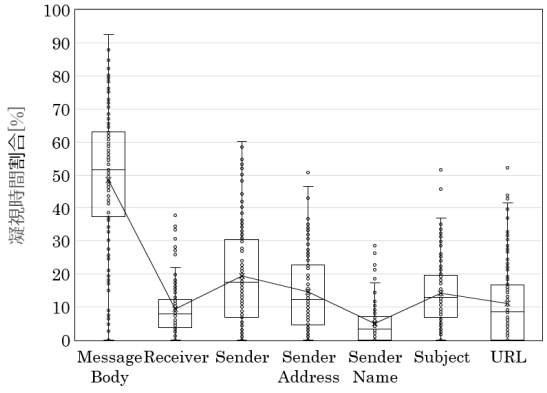

図 77 凝視時間割合 (セキュリティ教育有)

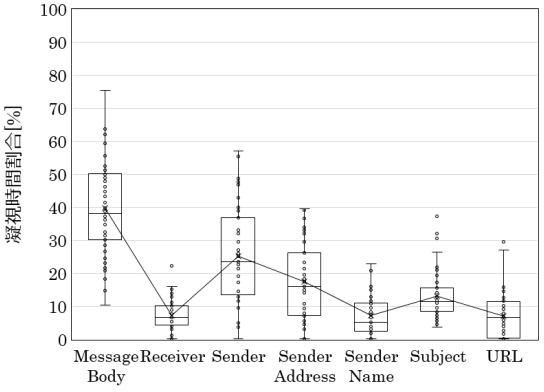

図 78 凝視時間割合 (セキュリティ教育無)

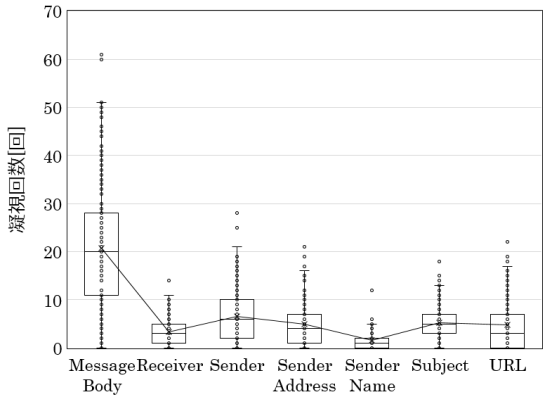

図 79 凝視回数 (セキュリティ教育有)

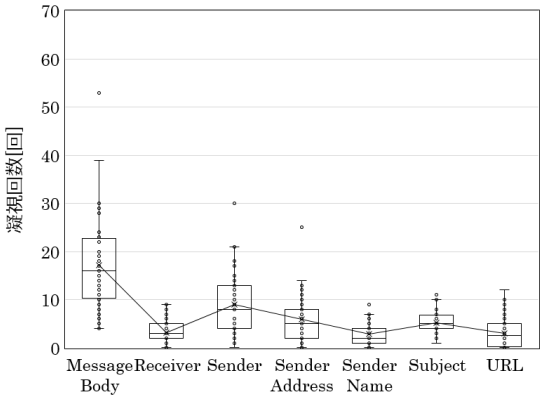

図 80 凝視回数 (セキュリティ教育無)

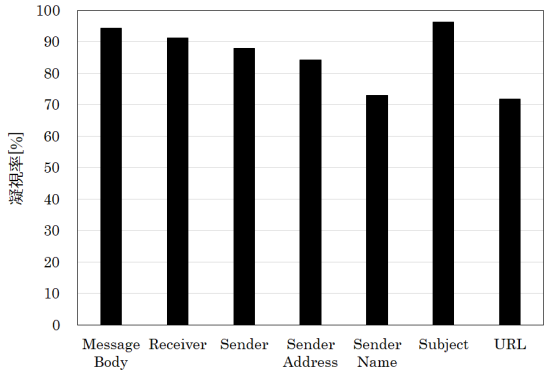

図 81 凝視率 (セキュリティ教育有)

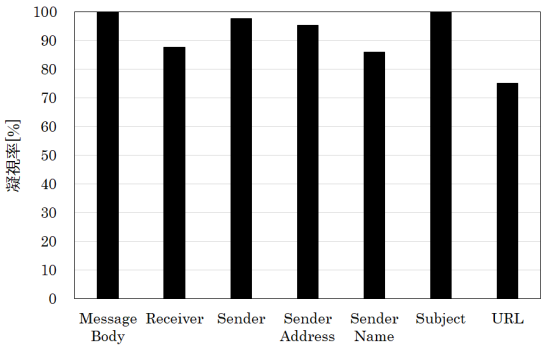

図 82 凝視率 (セキュリティ教育無)