Vol.2022-SPT-46 No.7
2022/3/7

フィッシングメールが人を欺く要因

閻鳳 [1]　馬遠 [2]　藤波努 [3]

概要：フィッシング被害が年々増加し，多くは SMS や電子メールを用いた誘導事件である．人間の心理を突くフィッシングメールが読み手をいかに欺くのかを調べる必要がある．本研究では，フィッシング協会のフィッシングメール事例を素材として，メッセージの受け手がメールの危険度を判断する過程の視線を計測した．また危険度の判断を聴取した. そして,視線データと聞き取り調査の結果に基づいて, 信頼感あるいは危機判断に影響する要因を分析した．実験参加者は文章の論理性，文書の書き方などに注目し，判断の手がかりとなるポイント，すなわちメッセージ送信者のメールアドレスやメッセージに含まれるリンク先にあまり関心を示さなかった．これらがセキュリティ教育の弱みを示唆するものと考える．トラストに関するセキュリティ教育に有効な方法を考える必要がある．例えば,最初に模擬攻撃を行い，直後に問題点を指摘し，最後正しい対応策を教えるシミュレーション教育などが考えられる．

キーワード：フィッシングメール，危機判断，セキュリティ教育，視線計測

Deceiving Factors of Phishing Mail

FENG YAN[†1]　YUAN MA[†2]
TSUTOMU FUJINAMI[†3]

Abstract: Property harm caused by phishing has been increasing in recent years, which most cases, those security-threatening information guide people to use SMS and email. Accordingly, there is a demand to discover hidden factors in phishing emails that deceive readers psychologically. In this study, we observed readers' eye-movement responses regarding their judgments about the existence of risk in given email messages. We utilized the phishing email instances of the Phishing Association as materials. Also, we collected self-reports from subjects about the judgment of potential risk in degrees in short interviews that followed each judging trial. We analyzed factors that influence the sense of trust with results from eye-movement data and interview recorders. We found that subjects in the experiment preferred to assign attention to areas that involve logical connections and writing styles rather than more critical elements for judging the risk as helpful clues, namely senders' email addresses and enclosed links. This work suggests weaknesses in security education. Our results reflect the necessity to consider an effective method for security education on trust. A typical process could be, for instance, designing a simulation education program that first demonstrates a simulated attack, then highlights the critical points immediately, and finally educates a related countermeasure as the end.

Keywords: Phishing mail, Crisis judgment, Security education, Gaze measurement

1. はじめに

近年，フィッシング詐欺は急増し，身近なセキュリティリスクになっている．独立行政法人情報処理推進機構（IPA）がとりまとめた「情報セキュリティ 10 大脅威 2020」[1]においても，個人向け脅威の第２位に「フィッシングによる個人情報の詐取」が挙げられている．個人被害だけでなく，荒金・塩野入・金井(2007)[2]によれば，フィッシングが企業に損害を与えたり、サービスレベルを低下させたりするといった被害をもたらし，さらにブランドイメージを失墜させ、顧客の離散を招く可能性があると指摘している．またフィッシング対策協議会発表した『フィッシングレポート 2021』[3]によれば，2021 のインターネットバンキングの不正送金被害の多くは, SMS や電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口によるものである. 2020 年はフィッシング情報の届け出件数が，前年と比較して著しく増加した（図 1）．金融機関や Amazon，楽天のなりすまし送信が多く報告されている．

このような状況に対処するため，高橋・猪俣(2018) [4]は機械学習を用いてヘッダ情報を学習し，フィッシングメールを識別する方法を提案したが，高い識別率を実現できなかった．精度を向上させるには，サンプル数を増やすなどの継続的努力が必要である．

フィッシングメールとは，なりすましメールなどを介して，ターゲットのカード情報やパスワードなどの個人情報を窃取する犯罪手法のことである．メールでユーザの不安を煽るなど，個人情報の入力を誘導するのは一般的な手段である．

1 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology (JAIST)
2 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology (JAIST)
3 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology (JAIST)

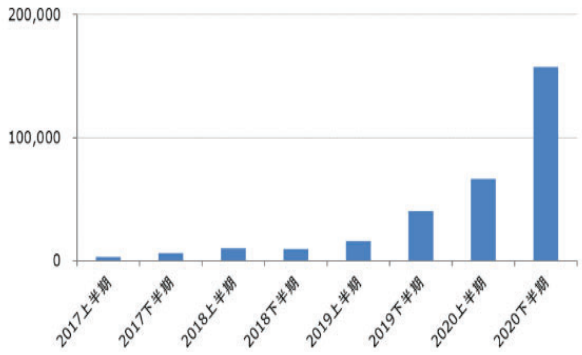

図 1　国内のフィッシング情報の届け出件数

それ故，フィッシング被害を防ぐために，人間の心理を突くフィッシングメールが読み手をいかに欺くのかを調べる必要がある。

本研究では，メールの信頼度を判断する実験を実施し，判断過程の視線を計測し，判断理由を聞き取り調査した．眼球運動のデータをもとに，危険判断に影響する要素を分析し，聞き取り調査などから得られた情報を参照しつつ考察する．

2. 実験方法

2.1 被験者

23 歳から 29 歳までの大学院生 35 名（このうち男性 21 名，女性 14 名，中国留学生 23 名，日本語母語話者 12 名）実験参加者は全員裸眼または矯正で正常な視力である．

2.2 実験手順

実験手順は図 2 のように設計した．

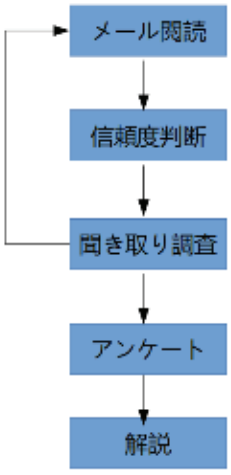

図 2　実験手順

聞き取り調査

被験者は実験材料となったメールのスクリーンショットを「信頼度が低い一信頼度が高い」を 1 から 5 まで，五段階で評価する．加えて，判断理由を聞き取り調査した．調査では，主に判断理由（信頼できる箇所，不安を感じる箇所），対応策を聴取した．

聞き取り調査アンケート

アンケートでは，個人情報とフィッシングメールを認識する際の判断軸などについて質問した．

解説

図のような手順を終えた上で，実験結果に関して短く解説する．解説の内容は，実験参加者の判断状況とフィッシングに関する認識に基づいて，主に当実験参加者の判断の誤りの提示と判断の手がかりとなるポイントの紹介である。

2.3 実験材料

素材として、Jigsaw (Google)[5]から提供したフィッシングクイズとフィッシング対策協議会[6]から公表したフィッシング被害事例を主体として編集できたメールのスクリーンショット合計 15 件を用いた。

2.4 視線計測

Tobii 光トポグラフィーを用いて注視箇所と滞留時間を計測した。

3. 実験結果

木村(2013)[7]はメールの構成要素の「差出人」「件名」「本文」「添付ファイル」について，心理的要因[8]に則った偽装方法を指摘した．そのゆえ，本研究では，人間の性質を利用してある行動へと誘導する心理的要因（返報性，コミットメントと一貫性，社会的証明，好意，権威，希少性）に沿った言葉要素，メール情報要素，加えて聞き取り調査からまとめた判断に影響する要素に基づく，メール内容における人間の危険判断に影響する要素の AOI（Area of Interest）を定めた．

本研究における実験素材により，危険判断に影響する要素を特定し，実験素材の 15 のメールのスクリーンショットに対する，各メールの中で異なった要素（AOI）の区別を検討する．

例として AOI を色付きの図 3 をあげる。

具体的なデータを分散分析し，結果により，有意である時等分散検定の結果により，有意確率 p<0．01．そのため Dunnett T3 を選んで多重比較し，分析した結果を以下の表 1，表 2，表 3 にまとめた：

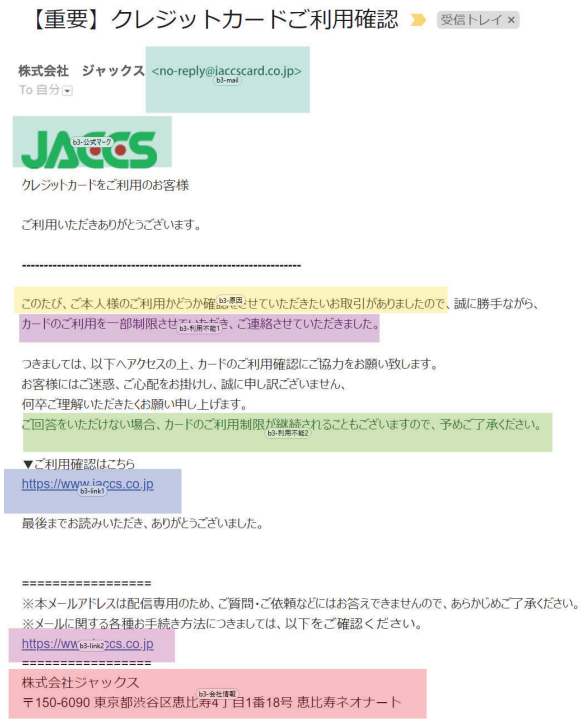

図 3　AOI の例

表 1 実験結果の分析(1)

メール番号	1	2	3	4	5
含む要素	言葉不自然2、コミットメントと一貫性2、権威、Link2	メールアドレス、Link、添付ファイル	メールアドレス、原因、コミットメントと一貫性2、権威2、Link2	メールアドレス、言葉不自然、催促、署名、Link	言葉不自然、緊急、原因、Link
分散分析結果	有意	有意	有意	有意	有意
分散分析データ	F(7)=25.545, p<0.01	F(2)=21.337, p<0.01	F(7)=7.348, p<0.01	F(4)=12.324, p<0.01	F(4)=22.210, p<0.01
Dunnett T3分析結果（有意）	権威と原因、権威と言葉不自然	メールアドレス、Link、添付ファイル三つの要素	権威（会社情報）と原因、権威（会社情報）とコミットメントと一貫性	メールアドレスと催促	原因とすべての要素、言葉不自然と緊急以外の要素

表 2　実験結果の分析(2)

メール番号	6	7	8	9	10
含む要素	メールアドレス、言葉不自然、重要、原因、Link	メールアドレス、権威2、Link	メールアドレス、好意、権威、署名、添付ファイル	誤字、催促、原因、コミットメントと一貫性、権威、Link	メールアドレス、希少性3、原因、Link
分散分析結果	有意	有意	有意	有意	有意
分散分析データ	F(4)=7.865, p<0.01	F(3)=7.099, p=0.05	F(4)=2.880, p=0.024	F(5)=22.544, p<0.01	F(5)=21.828, p<0.01
Dunnett T3分析結果	原因とメールアドレス以外の要素	linkとすべての要素	原因と好意、好意と署名	linkと権威以外の要素、権威とlink以外の要素、原因とすべての要素	原因とすべての要素、linkとメールアドレス

表 3 実験結果の分析(3)

メール番号	11	12	13	14	15
含む要素	メールアドレス、Link	メールアドレス、原因、催促、権威2、Link2	メールアドレス、返報性2、権威、Link	メールアドレス、原因、コミットメントと一貫性2、権威、Link	メールアドレス、コミットメントと一貫性、権威、Link
分散分析結果	有意	有意	有意	有意	有意
分散分析データ	F(1)=21.528, p<0.01	F(6)=7.036, p<0.01	F(4)=25.139, p<0.01	F(5)=4.990, p<0.01	F(3)=45.801, p<0.01
Dunnett T3分析結果	メールアドレスとlink	メールアドレスと原因、メールアドレスと催促	メールアドレスと権威、メールアドレスと返報性	linkと原因	コミットメントと一貫性

4. 考察

4.1 信頼感(危機判断)に影響する要因を分析

4.1.1 AOI の分析と考察

全メール要素を分析した結果有意で，同じメール（文書）の中で，異なる要素が人間の危険判断にさまざまな影響を及ぼす．送信理由の影響は有意であり，その平均値(図 4)は他の有意要素を上回る．Link は有意だが，有意性の平均値は他の要素より低い．また，好意，権威などポジティブな要素は有意だが、リスクを示したネガティブな要素（不自然など）より有意性の平均値は低い．

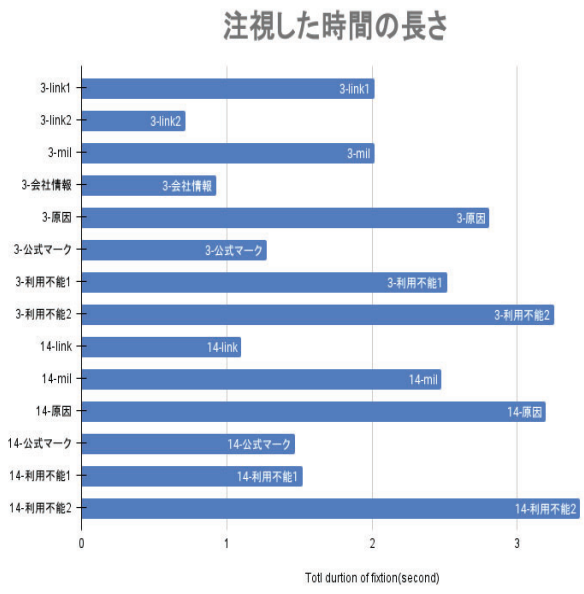

図 4　AOI に注視した時間の長さ(一部)

以上の分析結果に基づき，危険性判断に影響する要因を分析する．

まず，送信理由は有意の場合が多く，平均値が高い理由

は，原因(物事の論理性)が人間の危険判断に影響するためと推測する．なぜなら，判断理由を聴取したところ，送信理由の論理性またはネット上でのやりとりに関する標準的作法に照らし合わせて危険性を判断する被験者が全体の2/3 に達したからである．

また，Link は有意だが，平均値は他の要素より低い。理由は，Link から推測できる送信元と送信者のメールアドレスが一致しないという特徴があるため，それがフィッシング判断の手がかりとなり，決定的な証拠となる．しかしこの点は実験参加者に重視されなかった. 特に Link を見る回数が極めて少なかった，それゆえ，Link とメールアドレスは危険度判断にあまり影響しないと思われる．

最後にポジティブな要素はネガティブな要素と同じく有意だが, 平均値は低い。この点について北島(2013)[9]は，安全をハザードとリスクから定義し，危険度判断の第一，二因子は「非常に恐ろしいリスク」と「未知のリスク」であると指摘した．それゆえ，フィッシングメールという潜在的なリスクの危険度判断に対して，好意，権威などポジティブな要素より，不安を招くネガティブな要素の影響が大きいと推測される．

以上により，理由(物事の論理性)とネガティブの要素が人間の危険判断に大きく影響し，Link とメールアドレス危険判断にあまり影響しないと結論づける．

4.1.2 ヒートマップの分析と考察

また AOI の面積は様々であり、評価困難なので，並行して表示されているメールの文面に対する視線データを集計し，ヒートマップを作成した．

ヒートマップにおける視線が集中している箇所の特徴をまとめると，人間の危険判断要点は以下の 4 点にまとめられる．

(1) (用語，書き方で)内容が不自然である
(2) 送信理由が論理性を欠く
(3) 誤字など明確な間違いが含まれている
(4) 内容が現実とかけ離れていて信じられない

以下では，実際のヒートマップ例を上げて説明する．

ヒートマップでは、緑，黄色，赤の順で、視線が集中し，注視した時間が長かったことを示す．

図 5 のように表現が不自然なところ､たとえば｢あなた｣，さらに理由を確認する箇所がより頻繁に注視されている．これらの箇所が危機判断に強く影響しているものと考えられる．

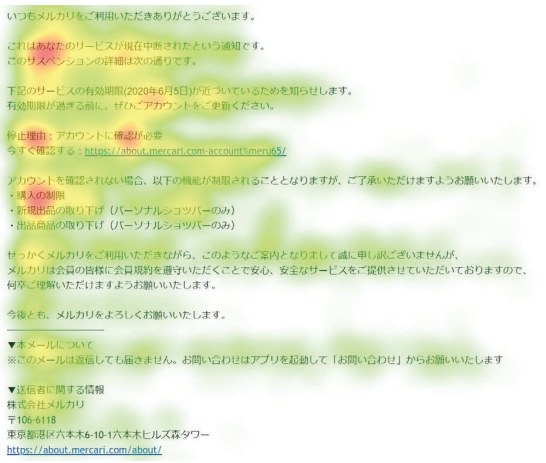

図 5 ヒートマップ(1)不自然と理由確認

または図 6 のように、誤字「ぷ」と「直ちにご登録のうえ」など、誤りや対応を不自然に急かすところが注目される．誤字と不自然な催促の表現があるので、この公式メールの信頼度が低いと判断する．

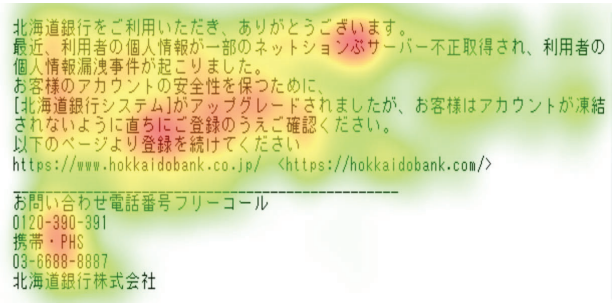

図 6 ヒートマップ(2)誤字と不自然

最後に図 7 のように，「失効した d ポイント」を「現金進呈」することは現実にはあり得ない，普段の生活でポイントを現金へ交換することはなく，信頼度が低いため，実験参加者が注目し，メールの危険判断に顕著な影響を与える．

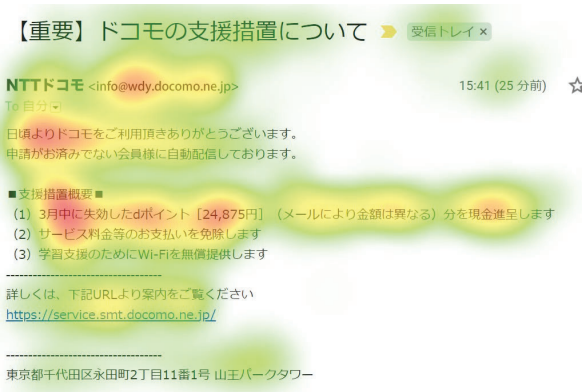

図 7 ヒートマップ(3)現実と離れて信じられない情報

今回の実験が「フィッシングメールが含まれて言う」という前提なので，実験参加者の選択は慎重になり，マイナス要因があったら判断に影響すると感じた．

ヒートマップにおける視線が集中している箇所の特徴をまとめると，人間の危険判断要点は AOI の分析結果と一致し、以上の分析を踏まえて理由(物事の論理性)とネガティブの要素が人間の(信頼度)危険判断に大きく影響すると結論づける．

4.2 人を欺く要因の分析

次には実験材料に対する評価による人を欺く要因を分析する．

今回実験は実験材料となったメールのスクリーンショットに対する「信頼度が低い—信頼度が高い」を 1 から 5 まで, 五段階で評価する. 評価した結果の平均値を計算し，4 に上回るのはメール 8 とメール 15 である。

以下図 8 と図 9 はメール 8 とメール 15 のヒートマップである。

図 8 メール 8 のヒートマップ

メール 8(図 8)における平均値はメールアドレスが間違っているグループでも 4．51 に達した．聞き取り調査の結果による，信頼感を与えるポイントは「文書の正しさ」と「添付ファイルあるだけなのでリスクなし」または「論理的に正しい」である．

メール 15(図 9)における平均値はメールアドレスが間違っているグループでも 4．52 に達した．聞き取り調査の結果による，信頼感を与えるポイントは「文書の正しさ」と「内容が充実し，見た目公式っぽい」「論理的に正しい」．

メール 8 とメール 15 の表現をまとめて，実験参加者たちはセキュリティ知識が不足ため，自分が持っているネット常識による判断する．それゆえ文書の正しさ，文面の充実さ，公式との類似は人間を欺く要因とする．

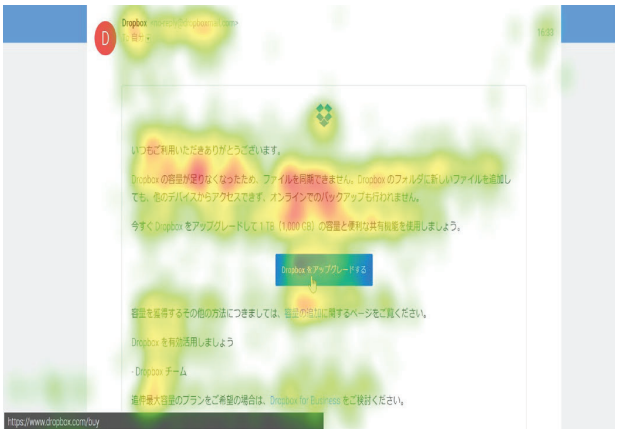

図 9 メール 15 のヒートマップ

4.3 聞き取り調査の分析と考察

このような現象が観察された原因を次のように推測する。行動経済学者のダニエル・カーネマン氏とエイモス・トベルスキー氏が提唱したプロスペクト理論[10]によれば，人は損を避けることを優先する傾向がある，また有利なときは安定を志向し、不利なときはリスクを回避する傾向が強まる．

実験参加者たちは安全・有利な場面にあると理解しているので，損を避けることを優先する傾向があり，安定志向になる．ゆえに，不安を感じるメールは放置し，実際の業務に支障がないなら無視することが多いだろう．

リスクを避けるので、実験参加者たちは判断の手がかりとなる箇所、すなわちメッセージ送信者のメールアドレスやメッセージに含まれるリンク先に注意を払わず、Link をクリックしない傾向があると推測する。しかし、危険度が正しく判断できない懸念から不安を感じた参加者が全体の 4/5 に達した．

聞き取り調査の結果に基づいて、信頼度の判断を２，4（信頼度はやや低い，信頼度はやや高い）と答え方が多くて，「確信できない」，「自信がない」，「完全にフィッシングメール/安全のメールと判断する決定的な証拠がない」，「怪しいほうが多い」「判断する手がかりがないので無視したい」などの声も出た．

以上のフィードバック，文書の正しさ，文面の充実さ，公式との類似さは人間を欺く要因になること，判断の手がかり-Link とメールアドレスへの注意不足，どちらもセキュリティ教育が不足している証拠と考える．

同時に，内田勝也(2012)[11]から，正しい情報を提供しても安全・安心と考えてくれないことが多いので，信頼関係の確立が重要ということを提示された．それゆえ，現代社会における多発しているフィッシングメール詐欺を防ぐため，どのようにすれば利用者たちに安心・安全な感じを与え，信頼関係を構築するか．これは考えすべき問題だと考える．今回の実験に基づいて，フィッシング詐欺に防ぐた

め，同時にユーザに安心・安全な感じを与えため，トラストに関するセキュリティ教育に有効な方法を提案する．

提案した教育方法は，今回実験と似ている形式である．詳しく説明すると，最初に模擬攻撃を行い，直後に問題点を指摘し，最後正しい対応策を教えるシミュレーション教育などが考えられる．

以下で今回の実験参加者の感想の一部(表 4)を参照して，この方法を提案する理由を説明する．

表 4 実験参加者の感想(一部)

	実験参加者の感想（一部）
1	面白い実験でした。ありがとうございました。
2	メールの数が多くなるとどんどん怪しいと感じるようになりました。実際に普段のメールに紛れていたり、就職活動に関係するようなメールだと引っかかってしまうかもしれないと思いました。あとは、大学や施設でセキュリティの研修、説明をうけるより、この実験をするほうがもっと効果がある気がします！
3	フィッシングメールについての実際の確認方法について最後に教えていただけたのでとても満足です。
4	勉強になりました。
5	これまで注目されていなかった細かい点について説明されたので、今後の生活で役に立つと感じました。
6	電子メールの内容と書式より、電子メールアドレスの正確さにもっと注意を払う必要があることを勉強できました。
7	このテーマに関する研究は実用的に重要であり、人々が予防に対する意識を高めるための良い参考資料となります。
8	フィッシングサイトについて新たに理解させていただきます。今後は、フィッシングサイトに騙されないように注意を払う必要があります。

以上の感想により，現在学校あるいは会社にあるただの座学セキュリティ教育と単純な訓練は生活での実用性が低いことを発見した．今回の実験参加者全員は入学の時に座学セキュリティ教育を受けた(フィシングメール対応あり)，所属する学校も定期的標的型メール攻撃の訓練を実施する．しかし，今回実験の実験参加者から，以前のセキュリティ教育からフィシングメールにおける危機判断の手がかりを把握した方は予備実験に含めて，42 人の中で 2 人しかない．

一方で今回の実験を通じて，実験参加者たちは実験からフィッシングメール判断の手がかりとなるポイントを勉強できたし，今後の生活中に利用できると感じた．フィッシングメールに詳しくなく，いつも不安を感じる状態より，これからフィッシングメールがあっても判断できるような自信があるため，安心・安全な感じが生じるようなフィードバックがある．

それゆえ，現行している座学セキュリティ教育と単純な訓練より今回提案した教育方法:模擬攻撃直後に問題点を指摘し，正しい対応策を教えるシミュレーション教育は実際に効果があると感じた．

5. おわりに

本稿では，アイトラッカーで計測した視線データを用いて，フィッシングメールが人を欺く要因を考察し，フィッシングメールの危険判断に対する影響は検討した．視線データは Fixation の持続時間を使って分析した．結果による，メールの危険判断に対するユーザはより安定傾向があるため，理由(物事の論理性)とネガティブの要素(用語，書き方など内容の不自然，誤字など明確の間違い，現実とかけ離れるなど)の影響が大きい．また文書の正しさ，文面の充実さ，公式との類似は人間を欺く要因とする．

また実験参加者の判断の手がかりとなるポイント，すなわちメッセージ送信者のメールアドレスやメッセージに含まれるリンク先にあまり関心を示さなかった．これらがセキュリティ教育の弱みを示唆するものと考える．

近年，フィッシング被害が年々増加している．本実験に参加した 35 名の実験参加者の中でも，実際にフィッシングメールに個人情報を獲得された経験があった人は 2 人がいる．フィッシングがあるという予告がある場面で，実験を参加する参加者たちもフィッシングメールを見つけかねる．そのゆえ，幅広くフィッシングに関する防犯教育が必要と考えられる．本研究における，実験後の短い解説も，「勉強になった」，「役に立つ情報」などのフィードバックをもらった．そのゆえ，フィッシングに関する防御知識は難しくないが，効果あり教育が足りないと考える．今回実験のように最初に模擬攻撃を行い，直後に問題点を指摘し，最後正しい対応策を教えるシミュレーション教育の効果が期待できると考えられる．

今後の課題としては，まず実験参加者の数量による制限があるので，今後国籍を比率して分析も必要と考える．次に，今回の実験材料は，フィッシング実例が多いので，100%安全のメールが欠く．また，「各種類のメールにおける，危険判断に影響が深い要素が違う」という傾向があるため，より全面的に各種類のメールと対照して検討する必要があると考える．最後に，今回の実験背景は「フィッシングメールを判断する」ので，実験参加者がリスクを重視し，実験結果を大きく影響する．今後はフィッシングメールの前提なし，日常生活と近づく実験する必要があると考える．

謝辞 本研究を進めるにあたり，多くの方々のご指導とご支援をいただいた．この機会に感謝の気持ちを伝えたいと思うまた，実験にご協力をいただいた実験参加者の皆様にも深く感謝を申し上げる．

参考文献

[1] 令和 2 年版情報通信白書 第 4 節 5G 時代のサイバーセキュリティ
[2] 荒金陽助・塩野入理・金井敦(2007)「フィッシング詐欺によるブランドへの影響に関する考察」情報処理学会研究報告 2007-EIP-36(2)
[3] フィッシング対策協議会(2021)「フィッシングレポート 2021」
[4] 高橋昌士・猪俣敦夫(2018) 「機械学習を用いた巧妙なフィッシングメールの識別方法の検討」情報処理学会研究報告 Vol.2018-IOT-43 No.13
[5] Jigsaw (Google) phishing quiz https://phishingquiz.withgoogle.com/?hl=ja,(参照 2021-07-27).
[6] フィッシング対策協議会,事例公開一覧 https://www.antiphishing.jp/news/database/,(参照 2021-11-06).
[7] 木村壮太(2013)「メール攻撃危険予知訓練システムの開発」情報処理学会研究報告 Vol. 2013-CSEC-63 No4 2013/12/9
[8] 内田勝也 et al.「 情報セキュリティ心理学の提案」情報処理学会研究報告,CSEC,2007(16),327-331,2007-03-01
[9] 北島洋樹(2013) 「3．4 安全・安心」『感性工学ハンドブック―感性をきわめる七つ道具』朝倉書店,2013,pp.187-201
[10] 『ダニエル・カーネマン 心理と経済を語る』,友野典男・山内あゆ子共訳,楽工社,2011 年
[11] 内田勝也(2012)「情報セキュリティ心理学~人的側面からの情報セキュリティ~」,情報の科学と技術 62 巻 8 号,336〜341(2012)