Vol.2022-IOT-58 No.4
2022/7/12

悪性メール提示による脅威認識がセキュリティ対策意欲へ与える影響の分析と啓発利用への検討

藤原 晴[1,a)]　敷田 幹文[1,b)]

概要：セキュリティインシデントが年々増加傾向にあり企業や機関でも情報漏洩等の被害が発生している．インシデント原因の過半数はシステムのみでは保護しきれない人的ミスが発端となっており，リテラシー教育を重視する組織も増えている．しかし，インシデント発生件数は年々増加しており十分な効果が出ているとは言い難くより効果的に啓発を行っていくことが重要となっていると言える．そこで，本研究ではヒューマンファクタに着目しユーザに対して数種類のフィッシングメールサンプルを精巧さに基づき段階的に提示した際のユーザのセキュリティ対策行動に対する意識への影響を分析することで，ユーザの脅威への認識とセキュリティ対策への意欲の関連性を示し，セキュリティ対策行動の促進を狙った啓発の実施において有用であるかの検討を行った．

The analysis of impacts of threat perception patterns on security awareness and consideration for educational use

Haru Fujiwara[1,a)]　Mikifumi Shikida[1,b)]

Abstract: The number of security incidents has been on the increase every year, and companies and institutions have been suffering from information leakage and other damages. The majority of incidents are caused by human errors that cannot be protected by the system alone. It is therefore important to raise awareness more effectively. Therefore, in this study, we focus on the human factor and analyze the effects on user's awareness of security measures when several types of phishing mail samples are presented to users in stages based on their sophistication, and show the relationship between user's threat awareness and their willingness to take security measures. We examined the usefulness of this method in the implementation of educational activities aimed at promoting security countermeasure behaviors.

1. はじめに

セキュリティインシデントが年々増加傾向にありその中でも公的な組織や企業を装ったメールやメッセージによって悪性なサイトへ誘導を行い個人情報を騙しとるフィッシングが増加しており，個人・組織を問わずに被害が発生している [1]．フィッシングをはじめとして様々なセキュリティインシデント発生原因の過半数は人的ミスであることから，システム的な保護のみに留めず各ユーザに対して啓発を行っていくことの重要性が叫ばれ，実際にリテラシー教育にコストをかける組織が増加していることからも伺える [2][3]．セキュリティインシデント対策としてナッジによってユーザにインシデント発生への注意を促す手法やセキュリティ対策行動に関連するヒューマンファクタの定義を行うといったように，システムではなくユーザ自身に注目した様々な研究や検討が行われているが，根本的な対策案として組織内で規定されたインシデント対策事項の遵守や環境整備を結論の一つとしてあげているものが多い [4][5]．

そこで本研究ではオンラインアンケート上にて悪性メールイメージの提示を複数回行い，啓発の実施にあたっての資料の提示方法がユーザに与える影響を分析することによってセキュリティ対策行動を促進するのに有用であると

[1] 高知工科大学
Kochi University of Technology
[a)] 255116p@gs.kochi-tech.ac.jp
[b)] shikida.mikifumi@kochi-tech.ac.jp

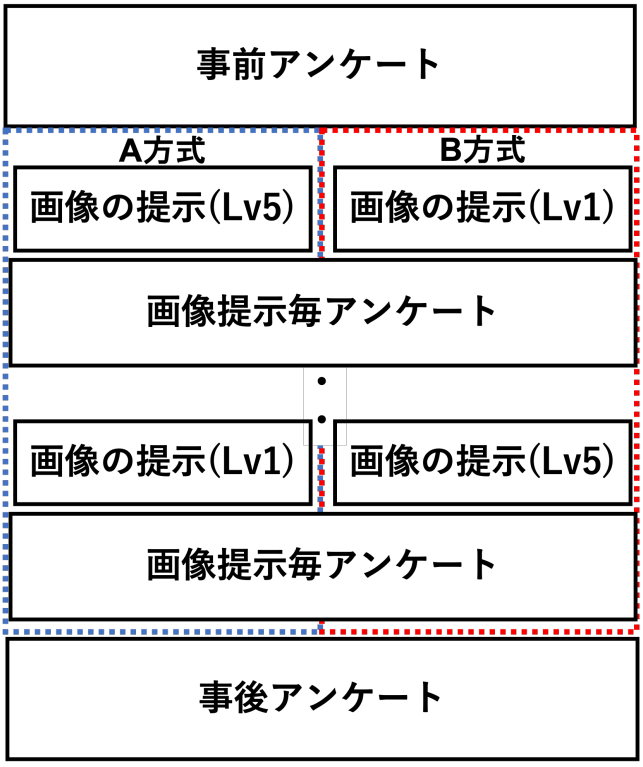

図 1 アンケート構成図

考えられる要素を示すとともに, 実際に啓発手法へ適用することを前提として検討を行う. メールイメージの提示にあたっては先行研究 [6] において, 比較的簡単な課題と困難な課題を順に実施した際に簡単な課題を先に実施した方が最終的に当事者意識が高まる可能性が示唆されたことに着目して悪性メールの精巧さに基づいて並び替えたメールイメージを順に提示している.

2. 調査内容

2.1 調査概要

本研究では 5 種類のフィッシングメールの画像を順に提示した際の印象についてのアンケートをオンライン形式で実施した. メール画像の提示前と各メール画像の定時毎, 全てのメール画像の提示後に質問事項を提示した. 提示するメール画像はフィッシングメールにおいてユーザが注目する要素 [7] に基き, フィッシング (アンケート上では詐欺メールと表記) か否かの判別のしやすさが異なるように設計した. 実験参加者は判別難度が高い方からメール画像を提示される A 方式と低い方から提示される B 方式のいずれかの形式で, アンケートに回答するように振り分けを行い実施した (**図 1**).

2.2 調査条件

2.2.1 実験参加者

- クラウドソーシングサイト登録者: 197 名
  - A 方式: 97 名
  - B 方式: 99 名

2.2.2 メール画像内容

本論文ではフィッシングであるか, そうでないかの判別のしづらさを「レベル感」と定義する.

本実験ではレベル感を 5 段階に分けてメール画像を用意している. このなかで最も判別のしやすいメール画像を Lv1, 判別しづらいものを Lv5 と表記する. アンケートにて提示した画像の構成要素を Lv5 のものを例として**図 2** に示す. 各画像の詳細な説明は以下の通りである.

- Lv1 のメール
  - ① 適当な文字の羅列をメールアドレスに設定
  - ② ロゴを挿入しない
  - ③ URL をベタ書き
  - ④ 謙譲語を含めず, 誤字脱字を含める
- Lv2 のメール
  - ① 適当な文字の羅列をメールアドレスに設定
  - ② ロゴを挿入しない
  - ③ URL をベタ書き
  - ④ 謙譲語を含めず, 不自然な送り仮名を含める
- Lv3 のメール
  - ① 適当な文字の羅列をメールアドレスに設定
  - ② ロゴを挿入しない
  - ③ URL を隠す
  - ④ 謙譲語を含めない
- Lv4 のメール
  - ① 企業名と適当な羅列を組み合わせたメールアドレスを設定
  - ② ロゴを挿入
  - ③ URL を隠す
  - ④ 謙譲語を含める
- Lv5 のメール
  - ① 実際に企業が利用しているアドレスに似せたアドレスを設定
  - ② ロゴを挿入
  - ③ URL を隠す
  - ④ 謙譲語を含める

2.2.3 アンケート内容

実施したアンケートは原則 5 点評価法を用いている. 各質問の目的と提示箇所の内訳の一部を以下に示す.

事前の脅威認知度の確認

- 詐欺メールについて誰かに相談したことがある (事前)

メール画像提示による脅威認知度の確認

- 詐欺メールの作成・送信には知識が必要だと思う (事前/事後)

対策行動への意欲確認

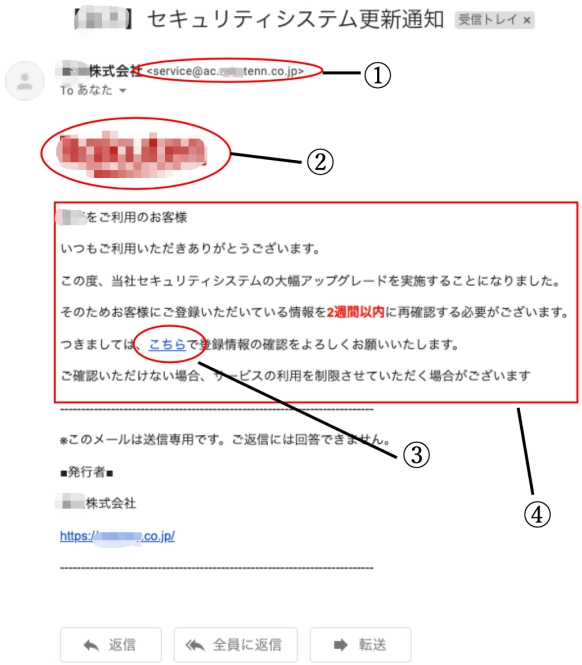

図 2　提示メール画像のイメージ

- 詐欺メールに騙されないためには知識が必要だと思う (事前/事後)
- 詐欺メールへの対応に関してのルールが自分には必要だと思う (事前/事後)
- 詐欺メールへ対応することは面倒だと感じる (事前/事後)
- 詐欺メールを目にした際に本アンケートを思い出すと思うか (事後)

メール画像への印象確認

- 画像のメールは信頼できるか (画像提示毎)
- 画像のメールの体裁は自然か (画像提示毎)

リテラシーへの自信の確認

- メールの体裁を見れば詐欺メールを見分けられると思う
- リスト (アンカーテキスト, フィッシングサイト, メールヘッダ等) のキーワードへの理解度

3. 調査結果

本章ではアンケートについて, メール画像提示前と後に着目した 1 標本と方式間の 2 標本について比較した結果を示すことで, 実験参加者の特性と方式による傾向をそれぞれ述べる.

3.1 脅威提示パターンがユーザに与える影響の分析

両方式ごとに事前アンケートと事後アンケートの回答結果を**図 3** に示す.

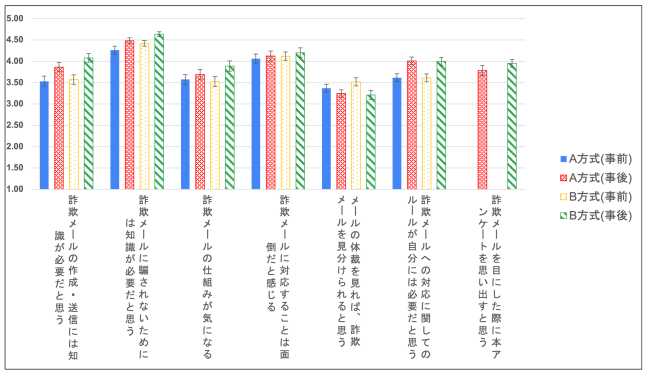

図 3　事前・事後アンケート比較

両方式とも事前アンケートと事後アンケート間でほとんどの共通質問に有意差が見られ ($p < .05$), 脅威体験が方式を問わずに実験参加者へ影響を与えていることが伺えた. 特に「詐欺メールを見た際にアンケートを思い出すか」については方式間でも有意差 ($p = .037$) が見られ, B 方式の実験参加者の方が対策行動への意欲を問う質問に対して高い点数の回答を行う傾向が見られた.

対して, 「詐欺メールに対応することは面倒だと感じる」については実施前後, 方式間ともに有意差が見られず脅威体験による影響は発生していないことがわかる.

3.2 ユーザ特性が対策意欲の変動傾向に与える影響の分析

アンケートの回答結果からユーザの分類を行った. 分類に用いた質問は「詐欺メールについて誰かに相談したことがある」, 「キーワードへの理解度」の 2 種類である.

フィッシングに関して他人に相談したことが 1 度でもあるかないかでアンケート実施前からの脅威認知の有無を評価し, 事前の「脅威認知あり」と「脅威認知なし」に分類した.

キーワードへの理解度についてはリストアップしたキーワードについて「誰かに説明できる」(4 点), 「なんとなく理解している」(2 点), 「聞いたことはある」(1 点), 「全くわからない」(0 点) の選択肢からの回答を実験参加者ごとに合算することで, 主観的なリテラシーへの自信度を算出し相対評価によって「自信あり」,「普通」,「なし」に分類した.

3.2.1 リテラシーへの自信度による比較

キーワードへの理解度の質問にてリテラシーへの自信度で実験参加者を分類した際の回答結果を**図 4** に示す.

「詐欺メールを見た際にアンケートを思い出すか」については, 方式間で「自信なし」と「自信あり」にそれぞれ有意傾向 ($p = .056, p = .053$) が見られた. このとき, 「自信なし」の実験参加者群は A 方式「自信あり」の実験参加者群では B 方式の方が高い点数をつける傾向が見られた.

次に「詐欺メールに対応することは面倒だと感じる」に

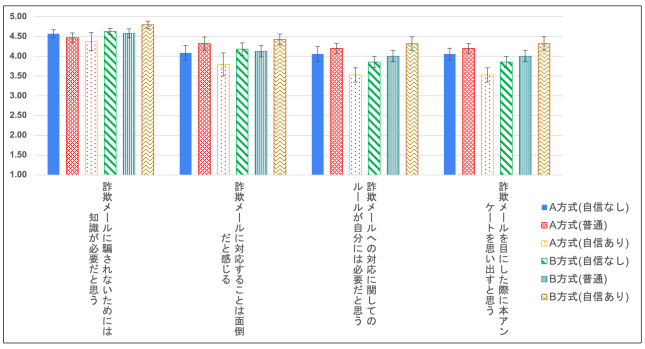

図 4 リテラシーへの自信度による比較 (事後アンケート)

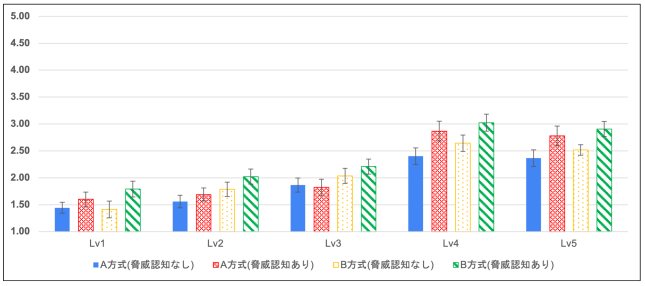

図 5 メールへの印象

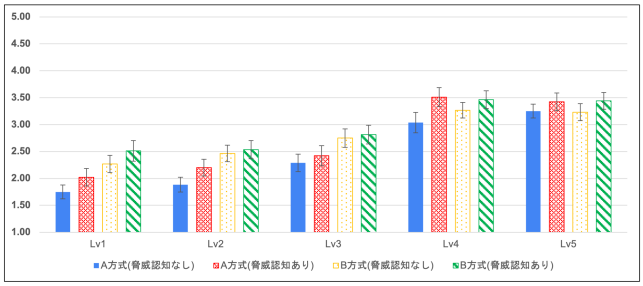

図 6 メールの体裁は自然か

ついては, 3.1 節にて実験参加者の分類を行っていない条件では有意差は全くなかったが, 「自信あり」の実験参加者群間で有意傾向 ($p = .059$) が見られ, 脅威提示パターンがユーザの対策行動を行うための物理的, 心理的な手間を感じる度合い (コスト感) に影響を与える可能性が示唆された.

そして, 「詐欺メールに騙されないためには知識が必要だと思う」と「詐欺メールへの対応に関してのルールが自分には必要だと思う」は「自信あり」の実験参加者群間で有意差 ($p = .028, p = .003$) が見られ, どちらも A 方式の実験参加者群が他条件の実験参加者群と比較しても低い点をつけていることがわかる.

3.2.2 脅威認知の有無による比較

アンケート実施前からの脅威認知の有無で実験参加者を分類した際の各メール画像提示後の質問に対する回答結果を**図 5** と**図 6** に示す.

「メールへの印象」については, Lv2 と Lv3 の画像にて「脅威認知あり」の実験参加者群間で有意傾向 ($p = .073, p = .066$) が見られ, レベル感の低いメール画像は提示の仕方次第で事前に脅威を認知しているユーザに対して影響を与える可能性が示唆された.

次に「メールの体裁は自然か」については, Lv1 と Lv2 の画像にて「脅威認知なし」の実験参加者群間で有意差 ($p = .014, p = .006$), Lv3 で有意傾向が見られた ($p = .053$). 加えて「脅威認知あり」の実験参加者群間で Lv1 の画像でのみ有意傾向 ($p = .055$) が見られた. 事前の脅威認知の有無に関わらずレベル感の低いメールに対して, B 方式の実験参加者はメールの体裁は自然であると比較的評価しているがレベル感が高くなるにつれて条件間での点数の差が小さくなっていることがわかる.

4. 考察

4.1 啓発におけるレベル感設定の重要性

図 5 と図 6 より, 完成度の低いメール画像から順に提示される B 方式の実験参加者群に Lv1 から Lv3 のメール画像に対して比較的高い点数をつける傾向にあることが伺えたが, Lv4 以降のメール画像に対しては方式による有意な差は見らなかった. これは A 方式の実験参加者群はレベル感の高いメール画像を先に提示されていたことから相対的にレベル感の低いメール画像に対して懐疑的となったのに対して, B 方式は比較対象が現在提示されているメール画像よりもレベル感が低いものとなっていたことによって, 提示される順番が両方式において同じ Lv3 のメール画像に対しても有意傾向が見られ, A 方式の実験参加者群よりも高い点数をつける傾向にあった可能性がある. 加えて, 先述の傾向は実験参加者の分類を行っていない場合とリテラシーへの自信度によって実験参加者を分類した場合でも同様に確認された. 以上より, 啓発においてインシデント事例や資料を提示する際にコスト感や無効感と呼ばれる「攻撃者に対しての偏見から自発的な対策行動を無意味であると感じる」という要素の高まりを危惧しレベル感の低い資料提示のみに止めると, かえって啓発がユーザにインシデントリスクを軽視させるリスクを高める可能性が示唆された.

4.2 資料の提示方法がセキュリティ対策行動意欲に与える影響

図 3 より, 方式を問わずアンケートを通してのメール画像の提示を通してユーザ意識に有意な影響を与えることが示され, 方式 B の実験参加者群の方が高い点数をつける傾向にあった. これは A 方式はレベル感の高いメール画像から提示し最後に 1 番レベル感の低い画像が提示され, B 方式はこの逆順であることから B 方式群の実験参加者の方がフィッシングへの脅威を感じた印象が強く残っており意欲的になった可能性がある.

しかし, 単に最後に提示されたメール画像のレベル感だけが実験参加者の意欲に影響を与えたわけではなく, 数種

表 1 詐欺メールを見た際に本アンケートを思い出すと思うか (事前実験)

	平均	標準誤差	p 値
A 方式	3.80	0.88	0.875
B 方式	3.82	0.10	

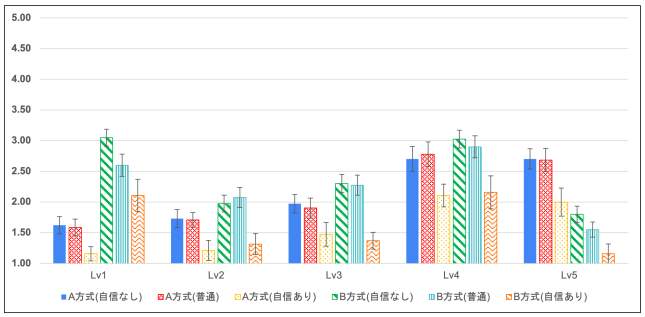

図 7 メールへの印象 (リテラシー自信度)

類のメール画像を順に提示したことが関連している可能性がある．本実験を実施するにあたって事前にレベル感の低いメール画像と高いメール画像 2 枚を用いての実験を A 方式 119 名, B 方式 100 名で実施した結果を**表 1** に示す．

表 1 より 2 枚のメール画像を用いて実施したアンケートにおいては全く有意差はないことがわかる．また，「本実験の方がユーザの対策意欲を高める」という対立仮説に基づいて片側検定を行うと B 方式間で有意傾向 ($p = .079$) が見られた．このことから段階的にレベル感を上げながら資料を提示することが脅威体験を通してユーザにより強い印象を与えたと言える．悪性メールの提示数を増やすことで方式間に有意傾向が生じた要因として考えられるのは, 実験参加者個々人のリテラシーレベルとの合致である．セキュリティ対策行動をユーザが実施するにあたっては様々な要因が関連してくる [8]．その 1 つとしてユーザの ICT 理解度が挙げられ, それに基づいて情報提供や啓発を実施することが対象ユーザのセキュリティ対策行動の促進につながると分析し主張を行った研究がある [9]．そこで「メールへの印象」リテラシーへの自信によって実験参加者を分類し比較を行った結果を**図 7** に示す．

図 7 より「自信なし」と「自信あり」実験参加者群には全体的に差が生じていることが伺える．このことから本実験においても実験参加者間で ICT 理解度には差異が存在していることがわかり, 本実験では提示するメール画像を増やしたことによってリテラシーレベルと合致する実験参加者が多くなり対策意欲に影響を受ける人数も増えたため方式間で有意差が現れた可能性がある．

4.3 脅威体験パターンとユーザ特性に着目した啓発利用への検討

ユーザにセキュリティ対策行動を促す際には数多くのヒューマンファクタについて考慮し設計を行うことが望ましい．本節では本実験にて得られた知見とセキュリティ対策意欲に影響を与えると考えられている無効感と関心と定義された「情報セキュリティが社会において必要であると感じる度合い」といったヒューマンファクタに着目して啓発利用への検討を行う．

4.1 節においてユーザへレベル感の低いものから高いものの順に脅威認識が行われるようにすることでセキュリティ対策意欲の高まりが期待できることと啓発においてユーザにとってレベル感の低い資料のみを提示することは誤りであり, かえってインシデントリスクを高める可能性を挙げた．これはレベル感の低い資料による脅威体験は無効感を軽減し高いものは関心を高めているためであると考えられる．ユーザがインシデントへ脅威を感じて関心が高まると, それに伴い無効感も高まっている可能性が先行研究にて示唆されたが [6], 関心の方がユーザのセキュリティ対策意欲に与える影響が有意であるため結果的に正の影響を与えていると推測される [10]．

以上より, 意欲を高めセキュリティ対策行動を促進するには関心を高めることが効率的でありユーザにとってレベル感の高い資料による脅威認識を促すのが適しているといえレベル感の低い資料によって無効感を軽減する重要度は低いといえる．

しかし, 4.2 節において同様の脅威体験パターンを提供した場合にも ICT 理解度 1 つをとってもユーザに与える影響が異なることが示唆されたことから, 啓発の対象となるユーザ特性が統一されている状況である．もしくは, ユーザごとに適したレベル感を判断し提示資料を変動させることができるのでなければ, レベル感を複数段階に分けて簡単なものから順に提示することで, あるユーザにとってレベル感の低いものは無効感の軽減に作用し, 高いものは関心を高めることにつながることが期待できる．このことから, 様々なユーザが混在する状況であれば段階的に脅威認識を促すことが適しているといえる．

5. おわりに

本研究ではユーザにセキュリティ対策行動を実施する意欲を促進するのに有用な資料の提示方式を明らかとすることを目的として, クラウドソーシングサイト上でオンラインアンケートを実施した．悪性メール画像を判別のしやすさに基づいて, 簡単な順と困難な順で提示する 2 つの方式でアンケートを行った結果の比較をすることで, セキュリティ対策意欲をはじめとしたユーザへの影響を分析した．そして, 提案した提示方式とユーザ特性に着目して実際に啓発手法へ適用することへの検討を行った．

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 2022. https://www.antiphishing.jp/report/

phishing_report_2022.pdf. (Accessed on 06/2022).
[2] 内閣サイバーセキュリティセンター. 人材育成等に係る取組状況について. https://www.nisc.go.jp/pdf/council/cs/jinzai/dai17/17shiryou03.pdf. (Accessed on 06/2022).
[3] JNSA 調査研究部会. 国内情報セキュリティ市場 2020 年度調査報告. https://www.jnsa.org/result/surv_mrk/2021/data/report2020.pdf. (Accessed on 06/2022).
[4] 前田典幸, 曽根芙美子. ヒューマンファクターに係る企業内研修に関する調査と考察. http://www.inss.co.jp/wp-content/uploads/2017/03/2009_16J022_029.pdf. (Accessed on 06/2022).
[5] 宇宙航空研究開発機構. ヒューマンファクタ分析ハンドブック. https://sma.jaxa.jp/TechDoc/Docs/JAXA-JERG-0-018A.pdf. (Accessed on 06/2022).
[6] 藤原晴, 敷田幹文. セキュリティ対策行動を促すヒューマンファクターの分析. 情報処理学会研究報告, Vol. 2022-SPT-46, No. 6, pp. 1–6, 2022.
[7] 閻鳳, 馬遠, 藤波努. フィッシングメールが人を欺く要因. 情報処理学会研究報告, Vol. 2022-SPT-46, No. 7, pp. 1–7, 2022.
[8] Peter Mayer, Alexandra Kunz, and Melanie Volkamer. Reliable behavioural factors in the information security context. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17. Association for Computing Machinery, 2017.
[9] 澤谷雪子, 佐野絢音, 山田明, 窪田歩. 個人のインターネット利用におけるセキュリティ対策行動開始のきっかけの分析. 情報処理学会論文誌, Vol. 61, No. 12, pp. 1845–1858, 2020.
[10] 諏訪博彦, 原賢, 関良明. 情報セキュリティ行動モデルの構築—人はなぜセキュリティ行動をしないのか. 情報処理学会論文誌, Vol. 53, No. 9, pp. 2204–2212, 2012.