令和 4 年度

修士学位論文

セキュリティ対策行動を促す啓発手法の提案と評価

Promotion of Security Awareness: Proposal and Evaluation of Enlightenment in an Opportunity for Voluntary Security Action

1255116　藤原 晴

指導教員　敷田 幹文

2023 年 2 月 27 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報学コース

要 旨

セキュリティ対策行動を促す啓発手法の提案と評価

藤原 晴

近年, 悪性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傾向にある. フィッシングをはじめとしたセキュリティインシデントの発生原因は人間の不注意や社内ルールの不遵守に起因する人的ミスが過半数を占めているのが現状であり, システム的な保護のみならずシステムを操作するユーザ自身に対して啓発を行い対策知識と意欲を高めることが重要視されている. そこで本研究では, 組織・企業のように幅広い層のユーザが混在する環境においてもフィッシング被害防止のための対策を促す啓発手法を提案・評価することを目的とした. ヒューマンファクタに着目したセキュリティ演習方式を設計し比較することで, 対策意欲の向上に有効な要素とユーザ特性との関連を分析すると共に演習実施から一定期間をおいての追跡調査により定着度を評価した結果, 比較した演習方式は演習直後のみ対策意欲を比較的高める方式と演習直後の対策意欲の高まりは劣るが, 定着度については高い評価の方式といったように一長一短であることが分かった. このことから, 各演習方式が有効に作用する場面を例示し, 啓発を行う状況によって使い分けることが最適であるとすることで, 最終的な啓発手法の提案とした.

キーワード　ヒューマンファクタ, フィッシング, 情報セキュリティ, セキュリティ啓発

Abstract

Promotion of Security Awareness: Proposal and Evaluation of Enlightenment in an Opportunity for Voluntary Security Action

Haru Fujiwara

In recent years, the number of phishing attempts that lead users to malicious websites and cheat them of their personal information has been on the increase. security incidents, including phishing incidents, are caused by human errors due to human carelessness and non-compliance with company rules, and it is important not only to protect the system but also to educate the users themselves to increase their knowledge and promotion of security awarness. Therefore, the purpose of this awaraness is to propose and evaluate a method to promote anti-phishing measures even in an environment with a wide range of users such as an organization or a company. By designing and comparing security training methods focusing on human factors, we analyzed the relationship between factors effective in improving motivation to take countermeasures and user characteristics, and evaluated the degree of retention through a follow survey after a certain period of time from the implementation of the training. As a result, it was found that the compared training methods have one advantage and another disadvantage, such as the method that relatively increases the motivation to take countermeasures only immediately after the exercise and the method that is less effective in increasing the motivation to take countermeasures immediately after the training, Based on this, we have proposed a final method of raising awareness by giving examples

of situations in which each training method works effectively, and by assuming that it is optimal to use each method depending on the situation in which the awareness-raising is to be conducted.

key words Human Factor , Phising, Information Security, Security Awareness

目次

図目次

図目次

表目次

第 1 章

はじめに

近年、セキュリティインシデントは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いる. フィッシングによる被害は個人・組織を問わず発生しており, IPA による注意喚起や協議会を設置しての対策が講じられている [1][2]. 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はシステム上の問題よりもシステムを扱う人間の不注意や社内ルールの不遵守等の人的ミスが過半数を占めている. このことから, システム的な保護のみに留めずシステムを操作するユーザに対して啓発を行っていくことが重要視されており, ユーザのリテラシー教育にコストをかける組織は被害数に伴い年々増加している [3][4].

しかし, セキュリティインシデント対策として組織が保護すべき情報とその利用形態は千差万別であることから, 画一的な啓発や演習による知識教育を実施しても中長期的な効果は期待しづらい側面がある. そのため, 根本的なセキュリティインシデント対策案として組織内で規定されたインシデント対策ルールの遵守や環境整備を行うことを結論の一つとしてあげているものが多い [5][6] . したがって, セキュリティ啓発においては具体的な対策知識の習得よりもインシデントの脅威を認識させ対策ルールを遵守するといったセキュリティ対策意欲を高めることに着目することが望ましい.

そこで本研究では, 企業組織のように幅広いリテラシーレベルのユーザが混在するグループ全体のセキュリティ対策意欲を高める手法を提案・評価することを目的として, ヒューマンファクタ (以下:HF) に着目したセキュリティ演習を実施することで対策意欲の向上に有効な要素とユーザ特性との関連を調査し, セキュリティ対策意欲を高める啓発手法の提案と評

価を行った.

2 章ではセキュリティ演習を攻撃者と被害者双方の立場から実施した際の演習結果とアンケート回答の違いから, セキュリティ啓発において有効な HF の分析を行った. 次に 3 章では有効と考えられる HF を中心として設計した演習の実施順による違いが対策意欲に与える影響をユーザ特性に着目し分析することで, 幅広いリテラシーレベルに対応し対策意欲を高める啓発手法を提案した. そして, 4 章では演習実施から 2 週間後に同一ユーザに対して追跡調査を実施することにより, 提案した手法による啓発効果の定着が見れるかを評価した. さらに 5 章では啓発手法の提案・評価によって得られた HF とユーザ特性に対する知見から, 啓発手法を考えるうえで参考となる事柄について議論を行った.

第 2 章

関連研究

2.1　非情報分野におけるインシデント発生防止策

情報分野は比較的, 若い分野であることからノウハウを基にしたインシデント発生の抑制についての検討が十分に行われていない現状を受けて, 航空宇宙分野や医療分野のようにインシデントの発生が人命に関わることからヒューマンエラーの抑止について検討が進められている分野から情報分野のインシデント防止に活かそうという取り組みがある [7]. 漫然と繰り返し行われる注意喚起の特徴とその効果が薄れ形骸化していくメカニズムとその対応策を論じたものや [6][8], インシデントの発生は前提としてリスクマネジメントを発生時の被害軽減や発生確率の低減に着目して行ったものもある [9]. インシデント防止は組織単位で行うものであるとし, 航空機内で起こり得る状況と対応行動が持つ意味を多角的に説明した研究もあり [10], フィッシング対策には無数に検討の余地が残されていることが示唆されており, リスク低減を意識した啓発方針の参考とすることが可能である.

2.2　フィッシング対策へのヒューマンファクタの援用

セキュリティ対策に有効な HF を検討した研究は数多く存在する. 分析にあたってはあらゆる分野の HF に対する文献を収集し組織単位での対策策定, フィッシング攻撃が成功してしまう際の要素などについて分析し, 自然な形式での演習の有効性について論じている研究などがある [11]. これに加えて, 教育機関や企業が組織内での啓発や対策設計に落とし込む検討が行われている [12][13][14]. また, ユーザの特性による影響にも着目してより多くの環

境でも適用可能な対策モデルを検討した研究も存在する [15][16]. なかにはいくつかの HF に基づいた演習を実施し HF の作用について分析を行っている研究もあるが, 攻撃者視点での演習から中長期的な定着度までを評価したものはない.

第 3 章

セキュリティ対策意欲を促進するヒューマンファクタの分析

3.1　攻撃者視点を認知させる実験

フィッシングをはじめとして, サイバー攻撃には被害や攻撃者の姿が不透明であるという特徴がある．これは攻撃者を過度に恐れ自身の対策を無意味と感じたり, 被害リスクを矮小化するといった考えに陥らせ, セキュリティ対策行動に負の影響を与えている．そこで, 啓発演習においてよく用いられる本物のメールとフィッシングを見分ける演習に加えて, フィッシングを行う攻撃者を体験する演習を実施することで, 攻撃者視点を認知させることが対策意欲に与える影響を演習成績とアンケートにより分析する．3.2 節では本実験の調査方式を説明する．そして, 3.3 節では調査結果について説明し, 3.4 節で啓発手法を提案する上で有用となる可能性がある要素について考察を行う．

3.2　調査方式

本調査ではフィッシングメールを題材として演習を実施した．演習では図 3.1 に示すように, 演習の前後と節目でアンケート調査を行い分析を行った．実施する演習はフィッシングの被害者と攻撃者を想定した 2 種類を用意した．どちらの方式を先に実施するかで A 方式 (被害者側→攻撃者側) と B 方式 (攻撃者側→被害者側) に, 人数が均等となるように分類している．また, 各演習が終了した時点で演習結果に基づいたフィードバックを適宜行い, 第 2

3.2　調査方式

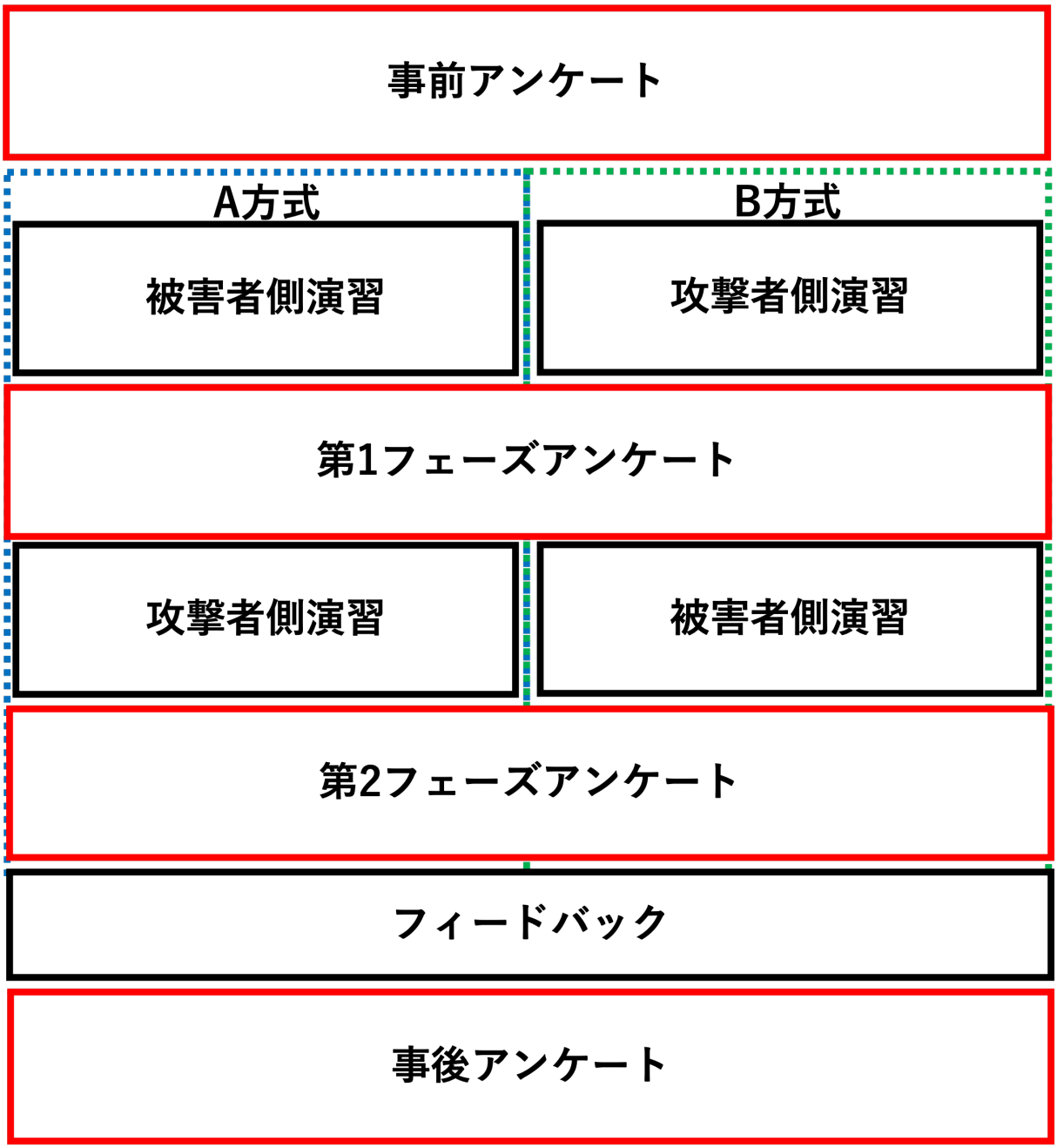

図 3.1　実験の流れ

フェーズアンケート終了後に, 被害者側演習結果について詳細にフィードバックを行った.

3.2.1　調査条件

3.2.1.1　被験者

- 大学生: 8 名
  - 非情報系学生: 4 名
  - 情報系学生 1 年: 2 名
  - 情報系学生 2 年: 2 名

3.2.1.2　演習内容

- 攻撃者側
  - 選択肢によって穴埋めを行うことで, フィッシングメールを作成可能なツールを用いて 3 種類のメールを作成) し監督者へ送信を行う.
  - 選択肢は単語等 (例: 受信者の呼び名 ユーザ様) ではなく, 入力内容の考え方 (誰にでも当てはまる名称で書く) から選択してもらうとで, 攻撃者の思考をイメージするように促すことで無効感の軽減を狙っている.
  - 自身が作成したメールが, 実際に届いている様子を確認した後に, アンケートに回答.
- 被害者側
  - Gmail の実験用アカウントに用意した 22 通のメールサンプルを, フィッシングメールとそうでないものに振り分けてもらう.
  - サンプルはフィッシング対策協議会で公開されている事例を参考に作成 [2].
  - メールファイルの編集を行うことで, ”送信元”を任意に変更した状態で配置しフィッシング対策として有名な, 送信元を確認する行動が有効となるように設定.
  - 振り分け後, 「フィッシングメールを正しいと誤って判断した数」と「フィッシングメールと誤って判断した数」のみを監督者から聞きアンケートに回答.

3.2.1.3　アンケート内容

本実験で実施したアンケートは原則 5 点評価法を用いて各フェーズで質問する共通質問を 15 問, 特定のフェーズだけで質問する固有質問を 5 問用意した. 調査目的別の内訳の一部を以下に示す.

セキュリティ対策行動に対する意欲を調査

- あなたはフィッシングメールに正しく対応できると思いますか (事前, 1・2 フェーズ)
- 誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか? (1・2 フェーズ, 事後)

無効感の調査

- あなたはフィッシングメールに正しく対応できると思いますか (事前, 1・2 フェーズ)
- フィッシングメールを作成し送りつけるのは簡単だと思いますか (事前, 1・2 フェーズ)
- 攻撃者は技術力があると思いますか (事前, 1・2 フェーズ)
- 攻撃の素性は想像できますか (事前, 1・2 フェーズ)

当事者意識の調査

- 被害者はしっかり者だと思いますか (事前, 1・2 フェーズ)
- 被害者はリテラシーが高い人だと思いますか (事前, 1・2 フェーズ)
- 被害者の年齢層はいずれだと思うか (事前, 1・2 フェーズ) ※ 1:小中学生 2: 高校生 3:大学生 4:大人 5 お年寄り
- 今日学んだ、知ったことを”明日”も覚えていると思いますか? (事後) ※来週, 来月, 来年も調査
- 忘れたとして、実際にフィッシングメールを見たら今日学んだ、知ったことを思い出すと思いますか? (事後)

表 3.1　被害者側演習の成績

方式	フィッシングに引っかかった数	誤った破棄
B	6	3
B	4	4
A	2	6
A	2	7
A	2	10
B	2	3
B	1	7
A	0	7

脅威認知の確認

- 詐欺メール (フィッシングメール) を受け取ったことはありますか (事前)

3.3　調査結果

3.3.1　被害者側演習の結果と分類の設定

各フェーズにおいて, 実施した被害者側の演習成績の内訳を表 3.1 に示す. 本調査ではフィッシングメールを正しいとしたもの. つまりは「フィッシングに引っかかった数」を重大度が高いとして, 標準誤差範囲を上回る人をリテラシーが「低い」, 標準誤差を下回る人をリテラシーが「高い」, それ以外の人を「普通」に分類した.

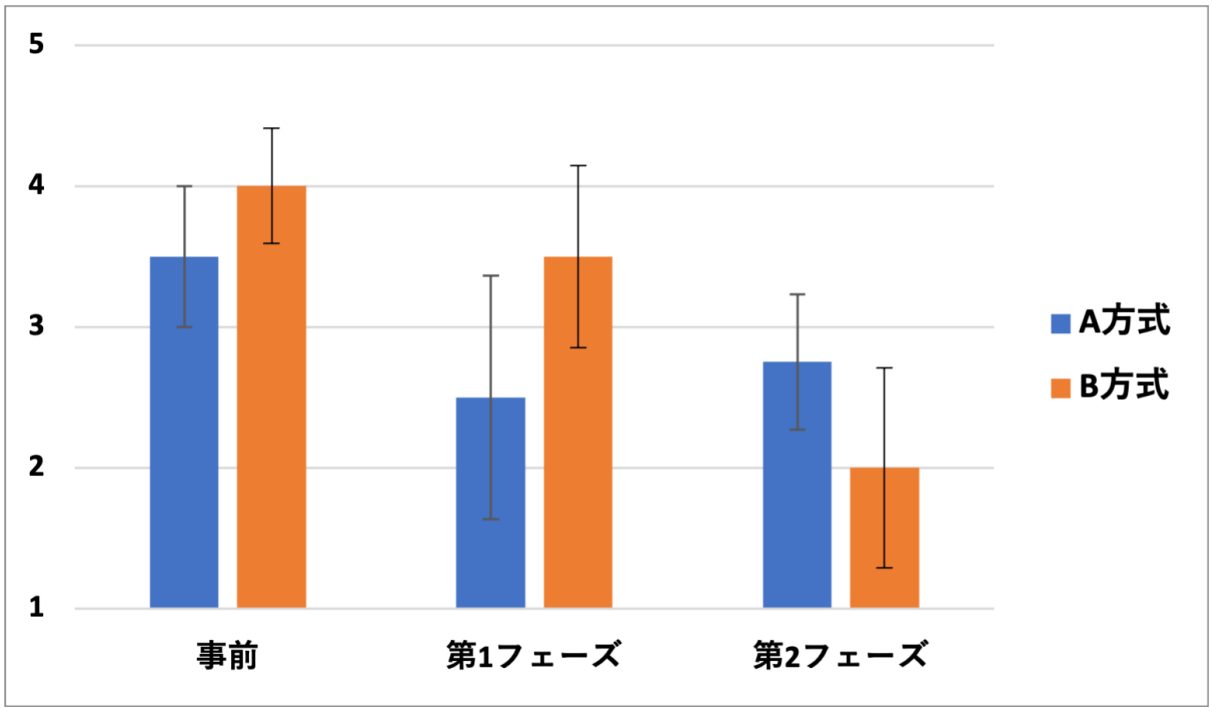

図 3.2　「あなたはフィッシングメールに正しく対応できると思いますか」に対する回答 (方式比較)

3.3.2　セキュリティ対策行動に対する自信の分析

「あなたはフィッシングメールに正しく対応できると思いますか」についてのアンケート結果を図 3.2 に示す. 両方式ともに第 1 フェーズ後は, フィッシングへ対応することへの自信が低下する傾向が見られ, 特に被害者側の演習を行った A 方式の低下が顕著であることがわかった. また, 攻撃者側の演習を実施した際には比較的自信の低下が小さい, または自信が増加していることが伺えた.

3.3.3　無効感の分析

次に, 「攻撃者は技術力があると思いますか」についてのアンケート結果を図 3.3 に示す. B 方式の第 1 フェーズ後に攻撃者への評価が半分以下になっていることから, 明らかに無効感が小さくなっていることが確認できた. しかし, 最終的には方式による差はなくなり演習実施前とも大きな差はないことがわかる. また, A 方式では大きな変動が演習を通して見られなかった.

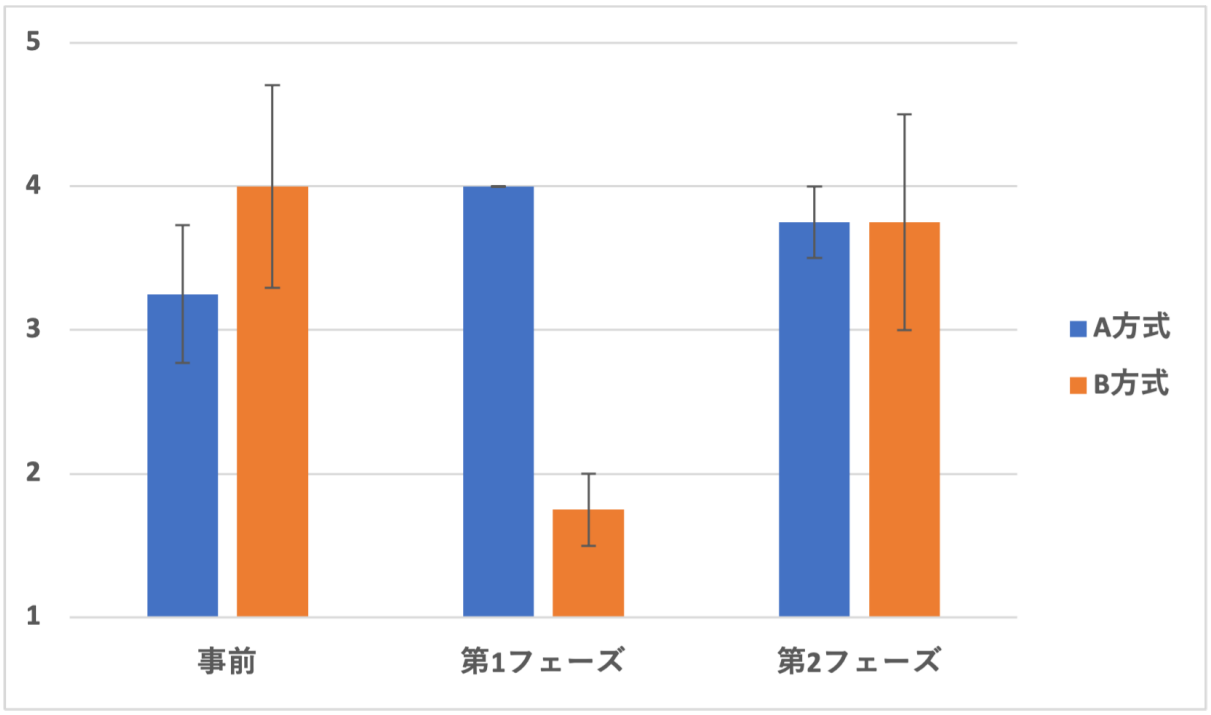

図 3.3　「攻撃者は技術力があると思いますか」に対する回答 (方式比較)

3.3.4　セキュリティ対策行動に対する意欲の分析

「誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか」についてのアンケート結果を図 3.4 に示す. 方式に関わらず第 2 フェーズにかけて, 他人への共有を行うことへ意欲的となっていることがわかる. しかし, 事後アンケート前に行ったフィードバックによる影響は確認できなかった.

次に, 「忘れたとして, 実際にフィッシングメールをみたら今日学んだ, 知ったことを思い出すと思いますか？」についてのアンケート結果を図 3.5 に示す. B 方式の方が顕著に高くなる傾向がみられることから, 比較的強く印象に残っていることが伺える.

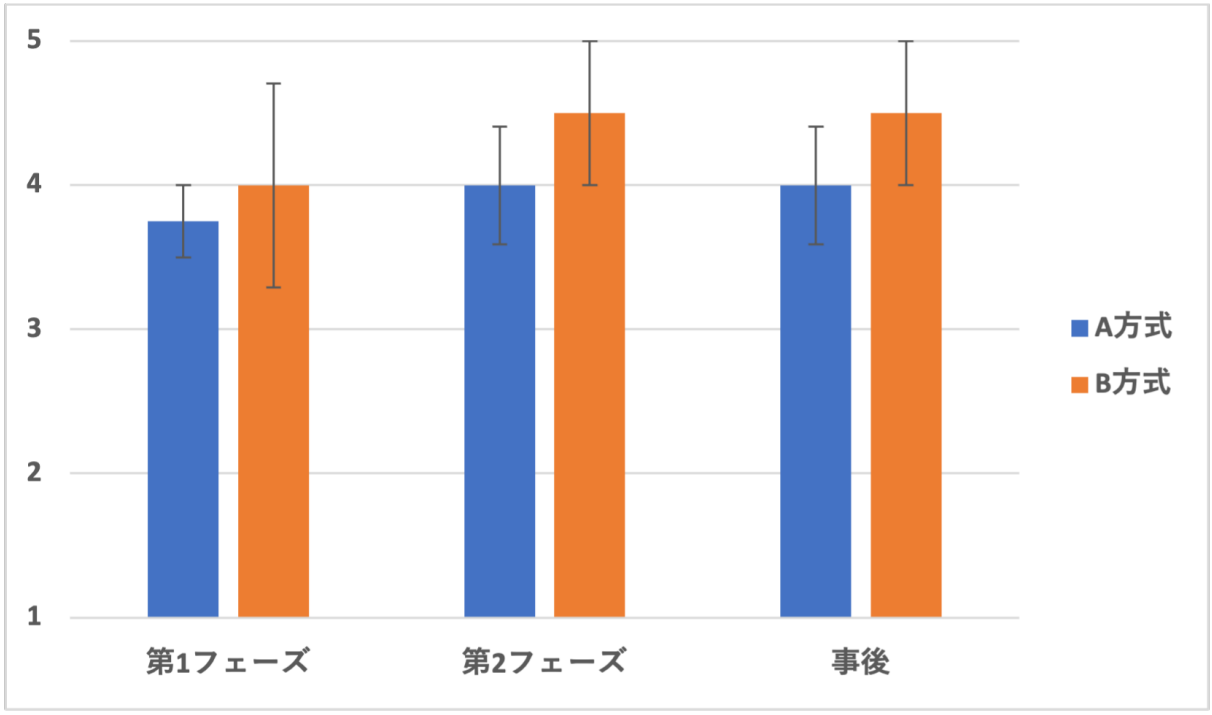

図 3.4 「誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか」に対する回答 (方式比較)

3.4 考察

3.4.1 無効感軽減が対策意欲へ与える影響

図 3.3 より両方式ともに被害者側の演習を行った際に, 対応への自信が低下していることが伺える. しかし, 誤差が攻撃側演習を行った際よりも大きくなる傾向がみられた. このことから, 被験者の特性が影響したと考えられる. そこで演習成績によって被験者を分類したグラフを図 3.6, 図 3.7 に示す.

図 3.6, 図 3.7 より両方式共に成績が「高い」に分類される被験者は, 演習を通しての自信の低下が比較的小さいこと, 攻撃者側の演習を行うことは無効感軽減に大きく影響することはなく, 後に脅威を認知した際の自信低下が大きくなることが伺えた. このことからユーザが元々認知していた脅威と演習を通して認知した脅威との差異が無効感の増減に影響を与える可能性が示唆された. これに加えて「誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか」を成績によって分類したグラフを図 3.8, 図 3.9 に示す.

3.4 考察

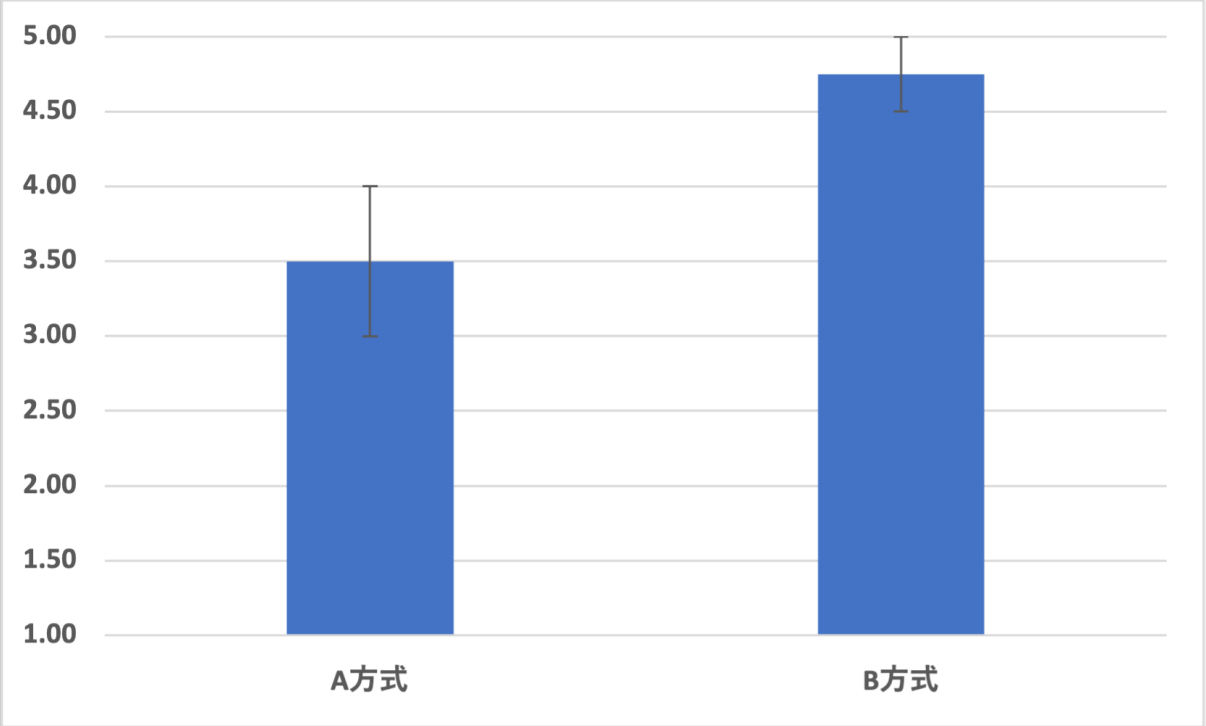

図 3.5 「忘れたとして, 実際にフィッシングメールをみたら今日学んだ, 知ったことを思い出すと思いますか？」に対する回答 (方式比較)

図 3.8, 図 3.9 より, A 方式は「低い」に分類される被験者のみが他者へ共有することへの意欲が高まっており対策へ前向きとなっていることが伺える. それに対して B 方式がどの成績分類においても他者へ共有することへ意欲的になっていることが伺える. このことから, 無効感が高まって自信が低下しているにも関わらず対策意欲が高まっているといえる. これは無効感よりも有意に対策意欲に影響を与える HF である「関心」(情報セキュリティが社会において必要だと感じる度合い)[17] が自信の低下により高まったからであると考えられる.

以上より, 無効感を軽減することを狙った攻撃者視点の演習が, 対策意欲に与える影響は小さいといえる. ただし, 脅威を認知した際に関心を高めるのには効果的であり, 特に情報セキュリティへの関心が低いユーザの対策意欲を高めるのに有用であると考える.

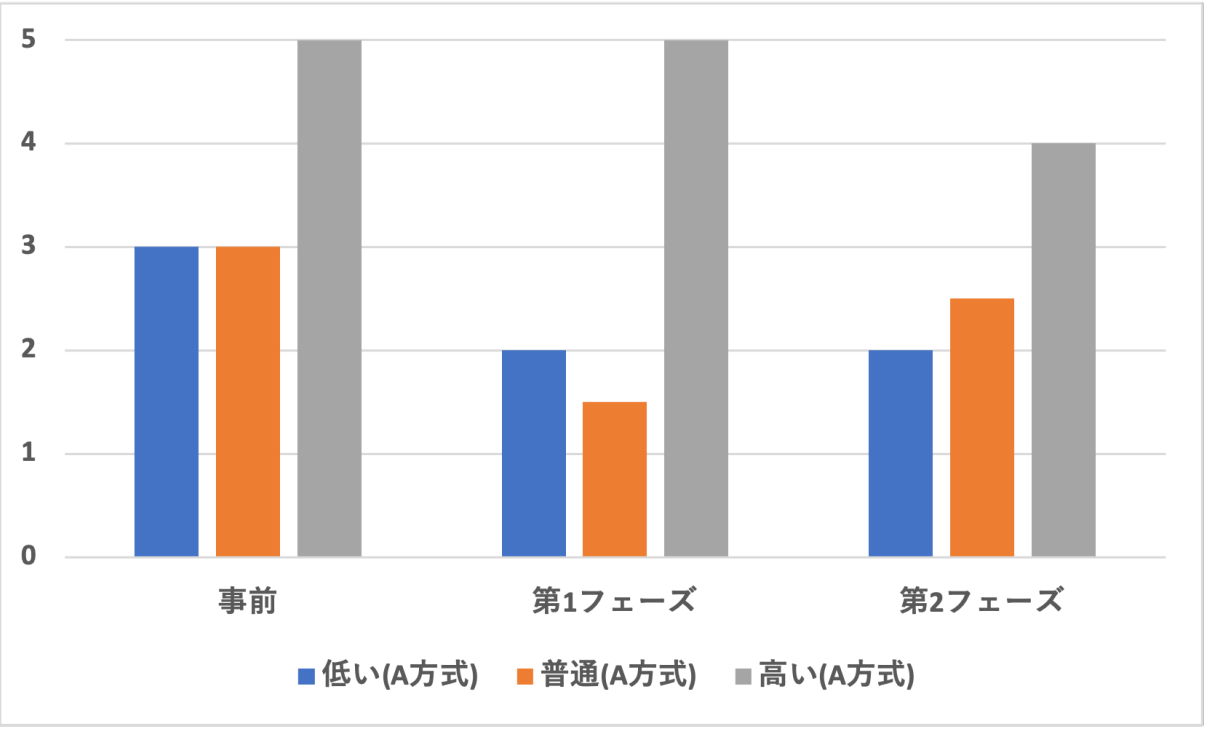

図 3.6 「あなたはフィッシングメールに正しく対応できると思いますか」に対する A 方式の回答 (成績比較)

3.4.2 脅威体験による当事者意識の変化

図 3.2, 図 3.4, 図 3.5 より B 方式の方が, 被験者自身は演習による学びの定着度が高いと感じており, 対策行動に比較的意欲的であることがわかる. そして, 図 3.3 をみると B 方式で演習を実施し, 攻撃者側の演習を先に行った場合に攻撃者に対しての恐怖心が顕著に小さくなっていることから, 無効感が軽減されていることもうかがえる. しかし, 図 3.1 から分かるように B 方式の方が演習の成績が比較的悪くなっていることから, 攻撃者側演習によって攻撃手法のイメージを非常に簡略化された形で学んだことで, 脅威を過小評価してしまい当事者意識が希薄になった可能性がある. これにより攻撃側演習で主に取り上げた, フィッシングを行うにあたってのメールの題材や文面の構成に対して, 大きく意識が削がれてしまうことで送信元などへの注意が薄れ, 被害者側演習の成績に影響を与えた可能性が考えられる [6].

以上より, 本実験のように事前知識がほとんどないユーザに対して攻撃者のイメージを簡

3.4 考察

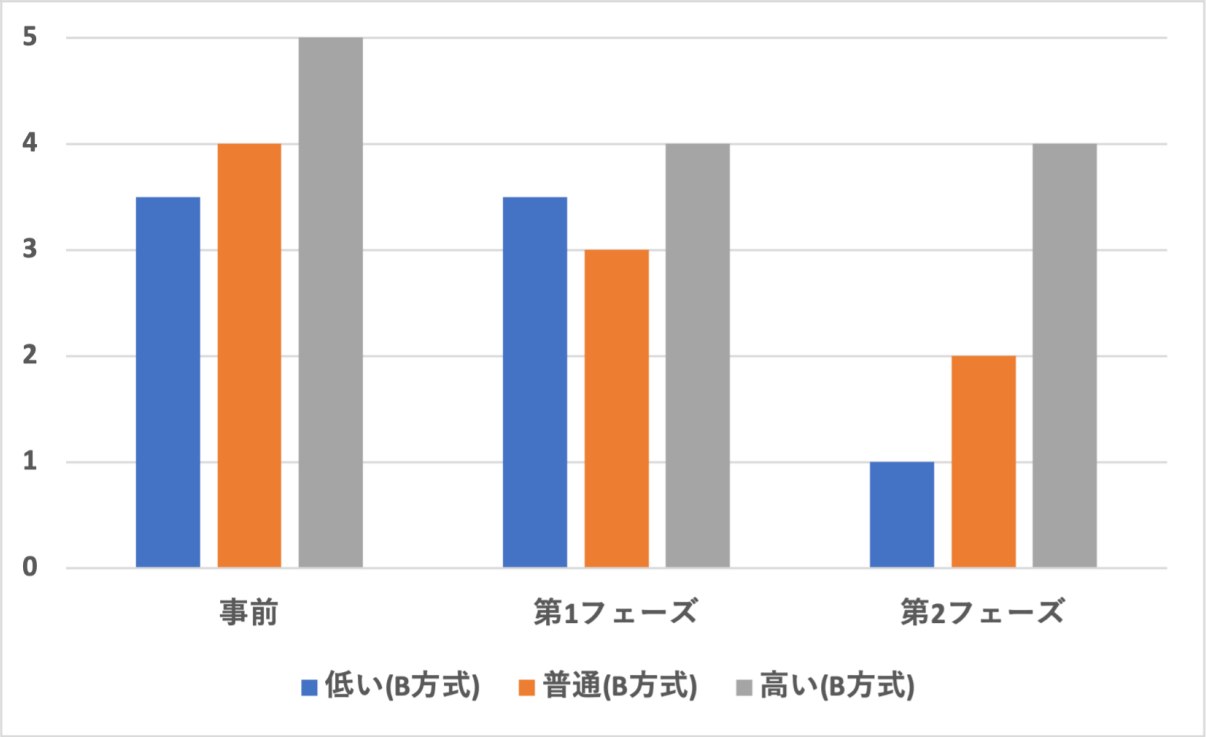

図 3.7 「あなたはフィッシングメールに正しく対応できると思いますか」に対する B 方式の回答 (成績比較)

潔に伝えた場合には, 無効感は軽減されるが当事者意識が薄れてしまう可能性が示唆された. 前節において脅威体験の機会を与え脅威を認知させることで関心を高め, 対策意欲に正の影響を与えるとした. しかし, 本研究で注目した HF ーの他にもコスト感やベネフィット (主観的な行動に対するコストとその見返りの関係性) に関する多数の要素, 現状維持バイアス (現状に不満や疑問を感じていないと, 多少の異変を感じたとしても自身の中で辻褄を合わせる傾向), 確証バイアス (人は自分の背景要因に沿った事柄が記憶に残りやすい傾向) などが存在する [18][19]. これらにも着目し演習の実施や分析を行うことで, 当事者意識の高まりを評価するのに適した演習の設計も可能となると考えられる.

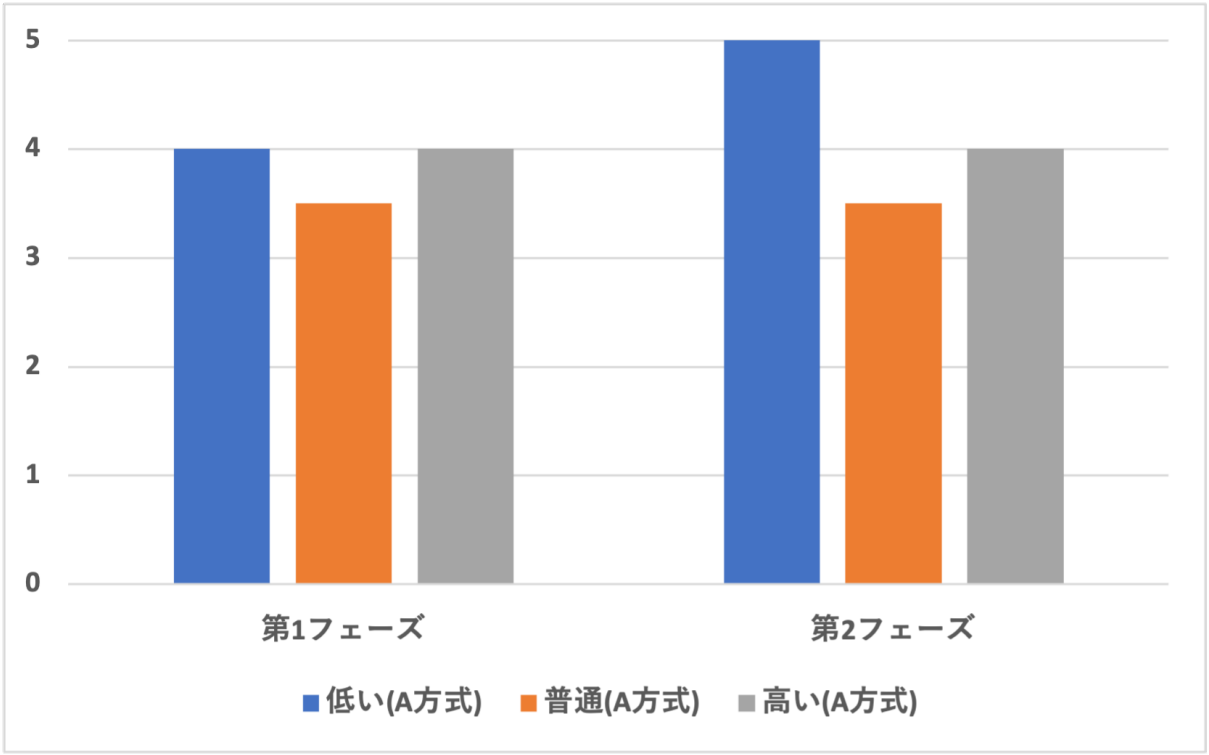

図 3.8　「誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか」に対する A 方式の回答 (成績比較)

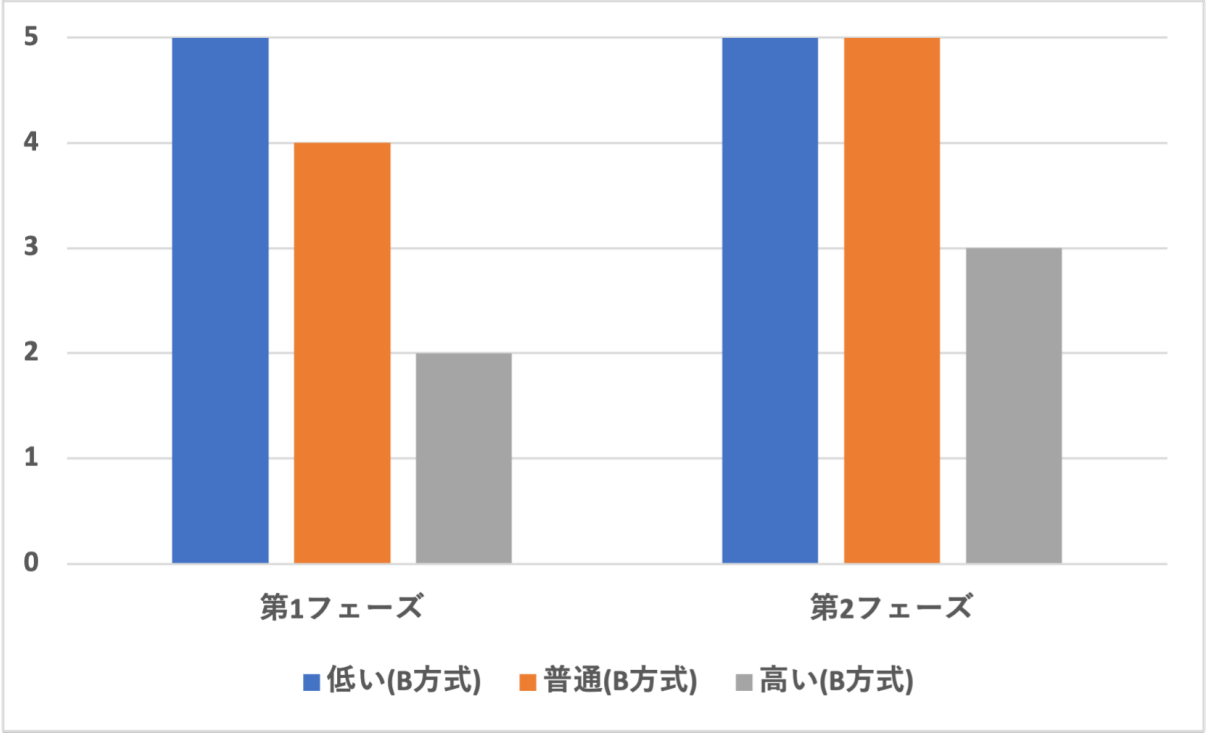

図 3.9　「誰かに今日の体験で学んだ, 知った, 気づいたことを共有したいと思いますか」に対する B 方式の回答 (成績比較)

第 4 章

教材提示パターンがセキュリティ対策意欲に与える影響の分析

セキュリティ啓発において攻撃手法を実際に試行することで、攻撃者の思考への理解を深め対策へ活かそうという取り組みが行われている。しかし, この手法は妥当な情報倫理と知識を有したユーザが高度な知識と技術を有する指導者の管理下において実施することが望ましいとされており, これらの要件を満たしつつ, 定期的に啓発を実施することが困難な組織も少なからず存在する. そこで, 従来の被害者側の立場を想定した演習を基本として, 教材を数種類用意する. これをグループごとにパターンを変更して提示し, アンケート調査を行うことで, 提示パターンがセキュリティ対策意欲に与える影響をリテラシーレベルごとに分析する. 4.1 節では本実験の調査方式を説明する. そして, 4.2 節では調査結果について説明し, 4.3 節で幅広いリテラシーレベルのユーザを対象とした啓発手法を提案する上で有用となる可能性がある要素について考察を行う.

4.1 調査方式

本調査では 5 種類のフィッシングメールの画像を順に提示し, メールへの印象を問う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 [20] に基づいており, フィッシング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低い方から順に, メール画像を提示する A

方式と高い方から順に, 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 4.1).

4.1.1　調査条件

4.1.1.1　回答者除外条件

Web アンケートの特性上, 不誠実な回答が行われた可能性が存在する. そのため本調査では 5 点評価方式の質問全てに同じ値で回答した被験者を除外している.

4.1.1.2　実験参加者

- クラウドソーシングサイト登録者: 196 名
  - A 方式: 99 名
  - B 方式: 97 名

4.1.1.3　メール画像内容

本実験では判別難度を 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 4.2 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

4.1.1.4　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.

事前の脅威認知の確認

4.1　調査方式

- 詐欺メールについて誰かに相談したことがある (事前)

無効感を推測する質問

- 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

- 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 (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

4.2　調査結果

本節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.

4.2.1　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 4.3 に示す.

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 ($p = 0.037$) が見られ, A 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.

4.2.2　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.

4.2.2.1　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 4.4 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 ($p = 0.056, p = 0.053$) が見られた. このとき, 「自信なし」の実験参加者群は B 方式「自信あり」の実験参加者群では A 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 ($p = 0.059$) 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 ($p = 0.028, p = 0.003$) が見られた.

4.2.2.2　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 4.5 と図 4.6 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 ($p = 0.073, p = 0.066$) が見られ, 判別難度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 ($p = 0.014, p = 0.006$), Lv3 で有意傾向が見られた ($p = 0.053$). 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 ($p = 0.055$) が見られた. 事前の脅威認知の有無に関わらず判別難度の低いメールに対して, A 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判別難度が高くなるにつれて方式間での点数の差が小さくなっていることがわかる.

4.3 考察

4.3.1 啓発における演習難度設定の重要性

図 4.5 と図 4.6 より, 完成度の低いメール画像から順に提示される A 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 B 方式の実験参加者群は判別難度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判別難度の低いメール画像に対して懐疑的となったのに対して, A 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判別難度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, B 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の高まりを危惧し判別難度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.

4.3.2 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 4.3 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がユーザの対策への関心に有意な影響を与えることが示され, A 方式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 B 方式は判別難度の高いメール画像から提示し最後に 1 番判別難度の低い画像が提示され, A 方式はこの逆順であることから A 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判別難度だけが実験参加者の意欲に影響を与

表 4.1 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	3.82	0.10	0.875
B 方式	3.80	0.88	

えたわけではなく, 数種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判別難度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 100 名, B 方式 119 名で実施した結果を表 4.1 に示す.

表 4.1 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がないことがわかる. ここで, 「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 A 方式間で有意傾向 ($p = 0.079$) が見られた. このことから段階的に判別難度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 [18]. 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た研究がある [16]. 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 4.7 に示す.

図 4.7 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 理解度による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.

4.3.3 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 HF 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 HF に着目して啓発利用への検討を行う.

4.3.1 項においてユーザへ判別難度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判別難度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. これは判別難度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, 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 [17].

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判別難度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判別難度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, 4.3.2 項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判別難度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, 判別難度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判別難度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, 幅広いリテラシーの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.

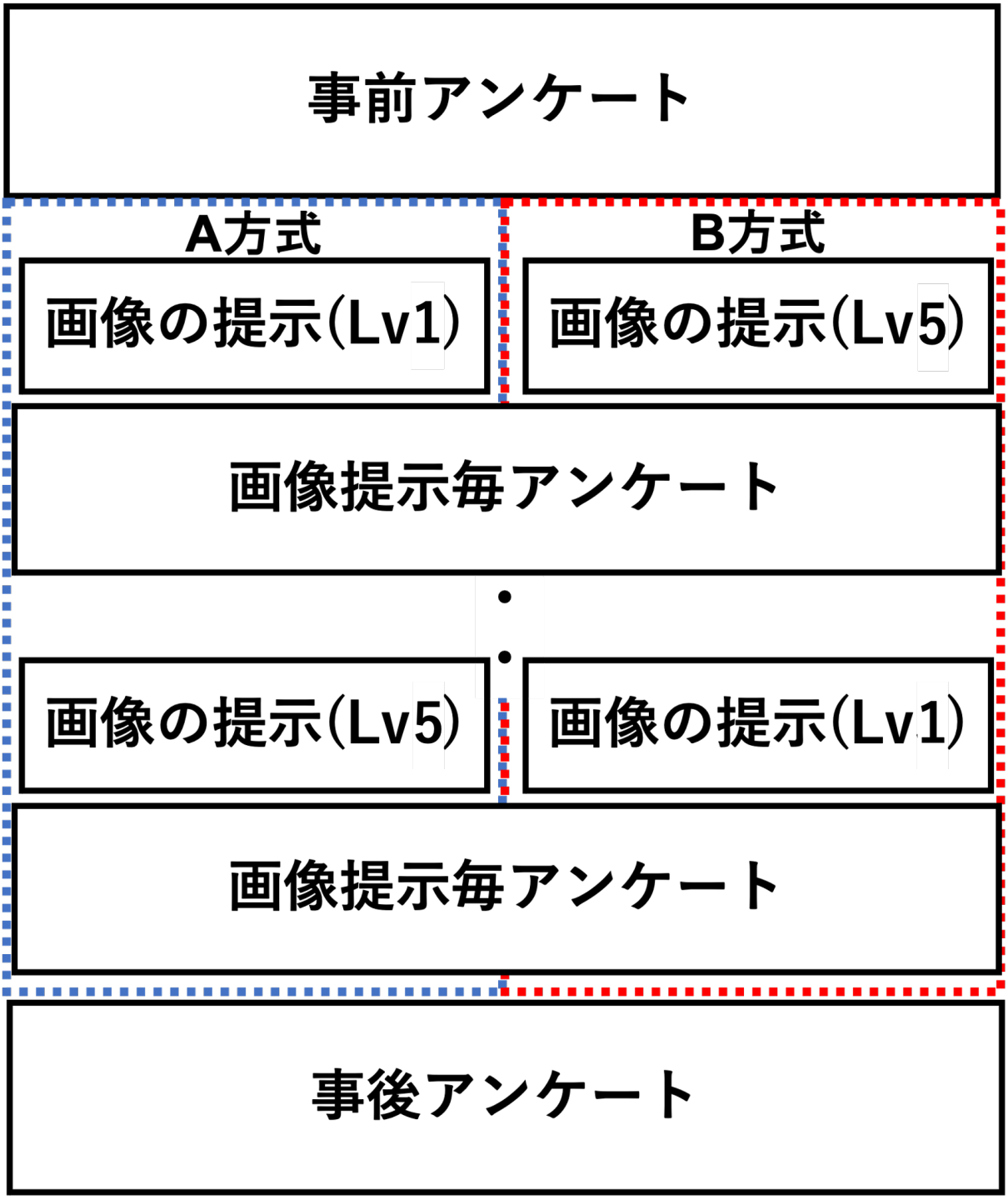

図 4.1　アンケート構成図

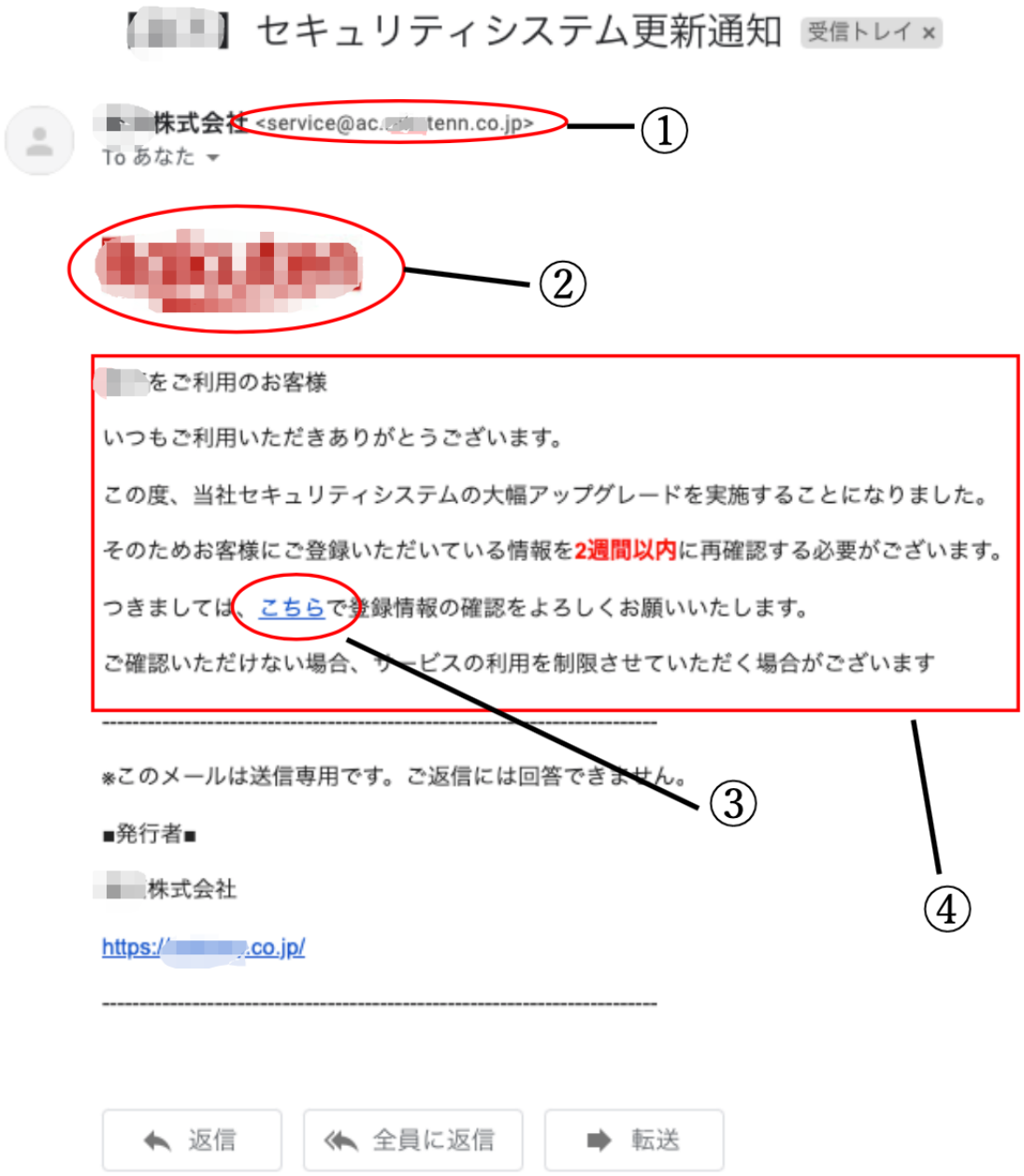

図 4.2　提示メール画像のイメージ

4.3 考察

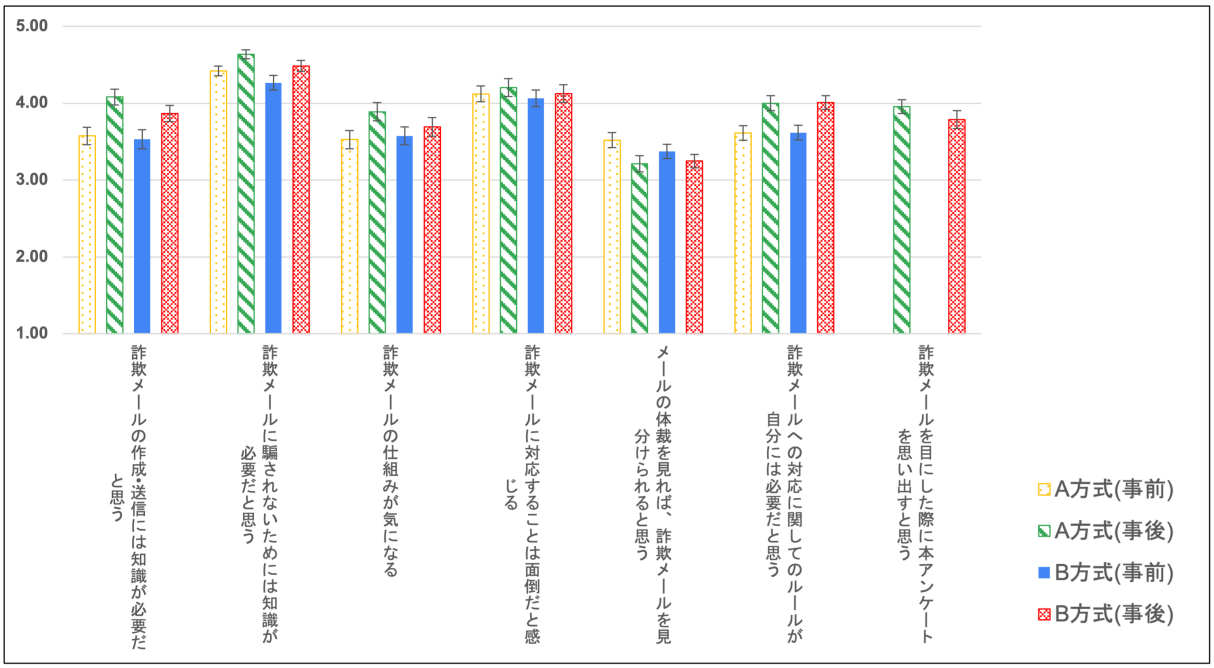

図 4.3　事前・事後アンケート比較

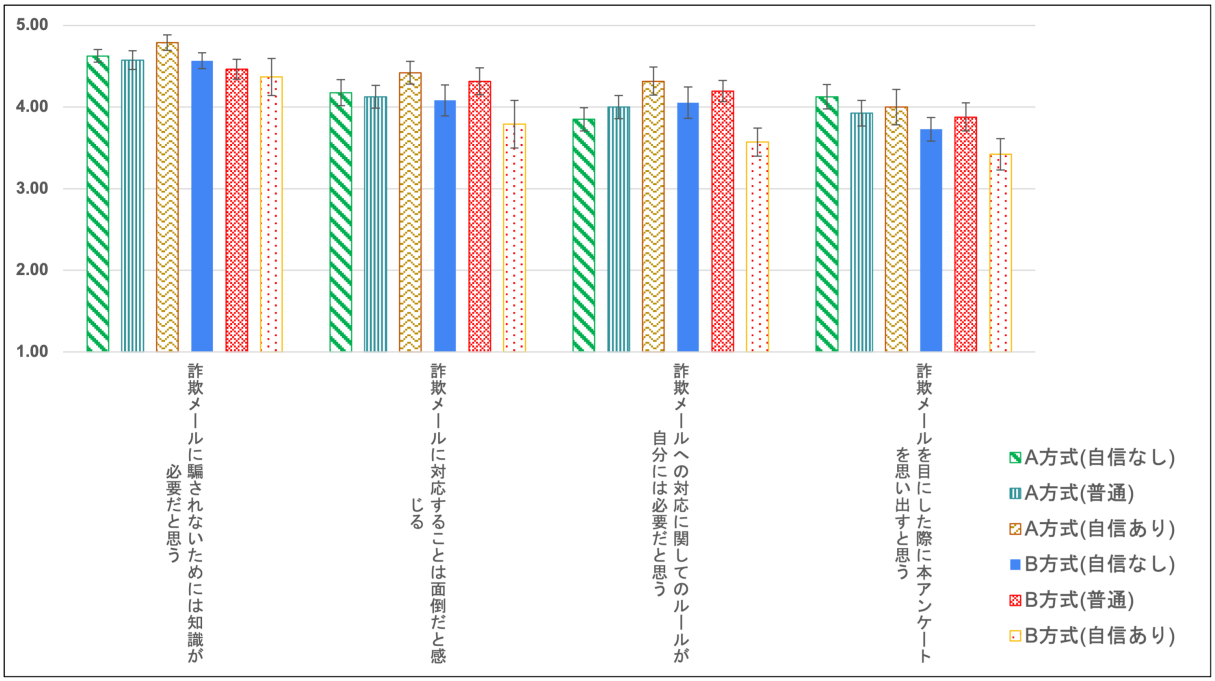

図 4.4　リテラシーへの自信度による比較 (事後アンケート)

4.3　考察

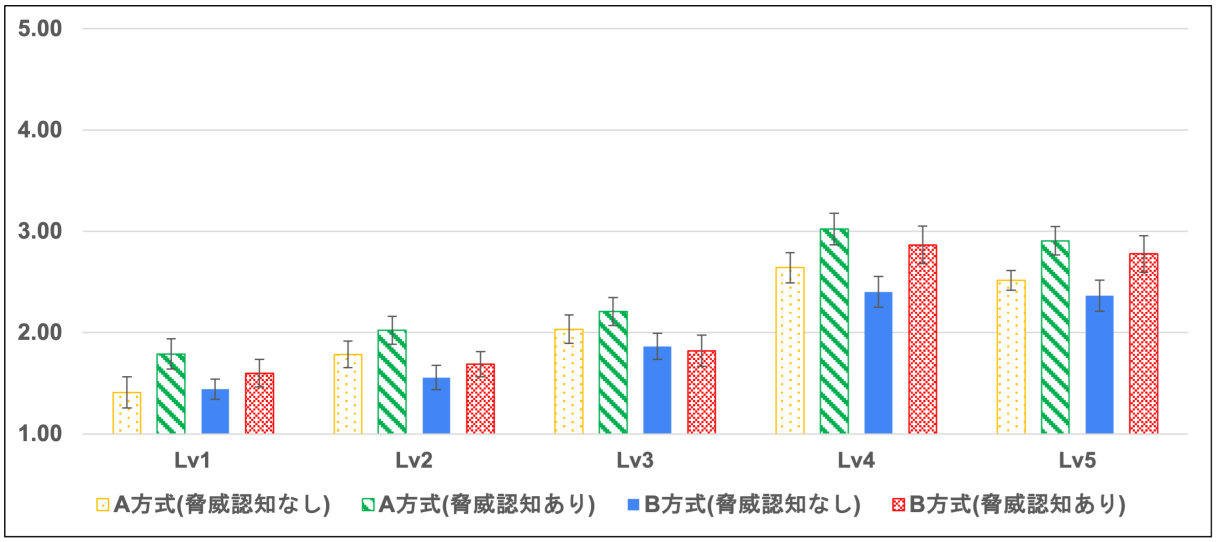

図 4.5　メールへの印象

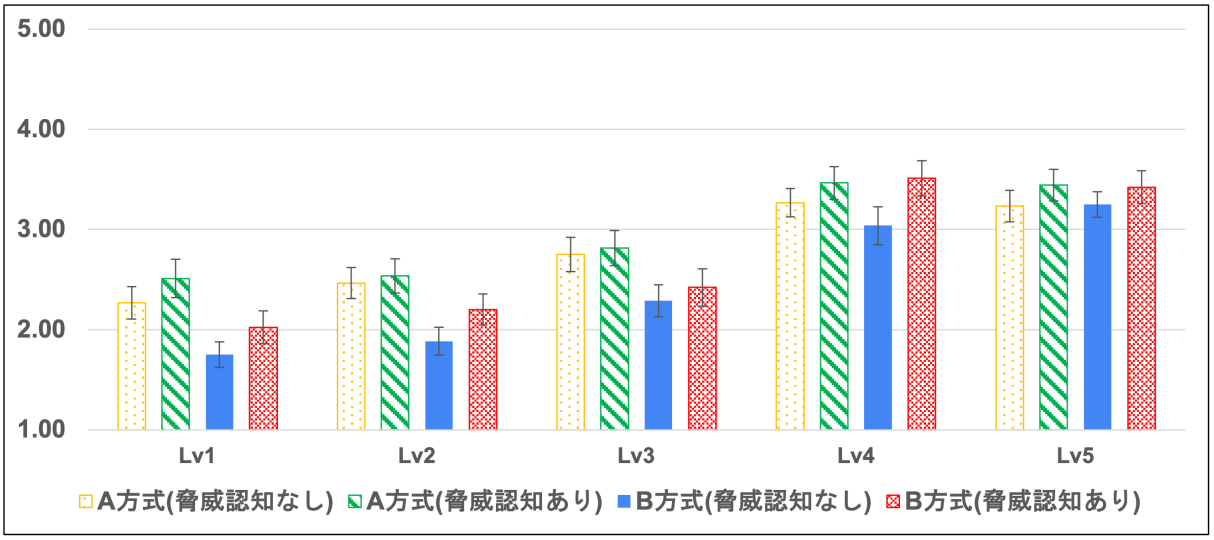

図 4.6　メールの体裁は自然か

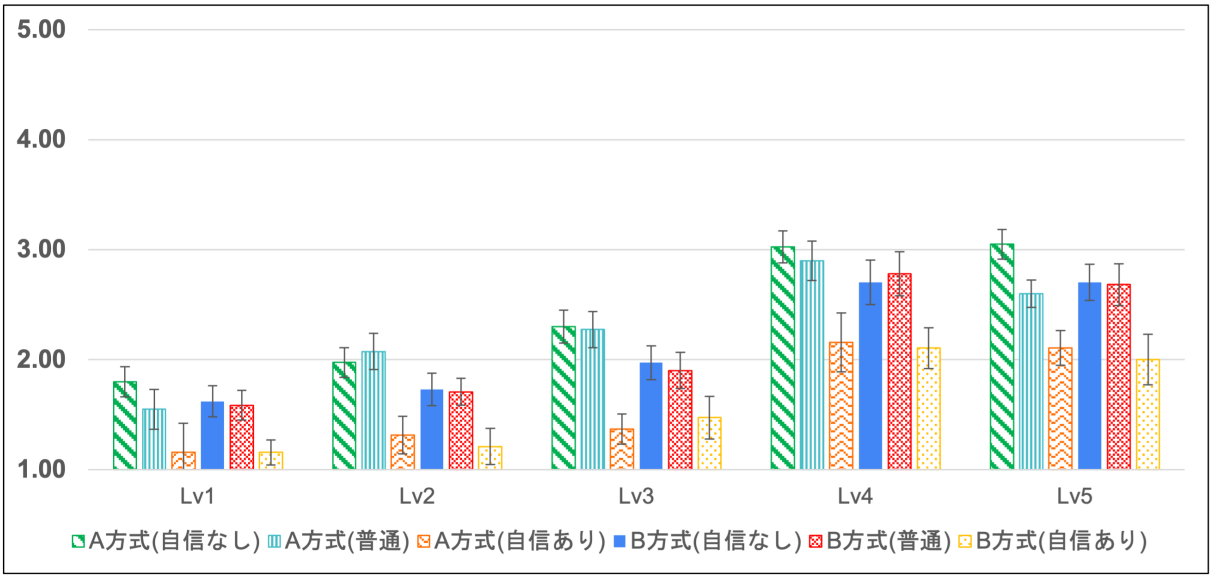

図 4.7　メールへの印象 (リテラシー自信度)

第 5 章

啓発の定着度評価

インシデントは業務中のヒューマンエラーが累積した結果として発生するとされている. これを防止する施策として社内ルールを定め, 啓発実施や社内通知を通して注意喚起を実施している. しかし, 攻撃は時期を問わずに行われる可能性があるのに対して, ユーザへの注意喚起を日常的に実施する体制を整えられていない組織は少なくない. また, 日常的に繰り返される事柄への関心は慣れるほど薄れていくという問題がある [6]. そこで, 演習と啓発を実施してから期間をおいて定着度を評価することで, 中長期的にインシデント防止のための留意事項をユーザに印象付けるのに有効な方式を示す. 5.1 節では本実験で実施した 3 つの演習方式と評価方法について説明する. そして, 5.2 節では調査結果について説明し, 5.3 節では結果を基に各演習方式の啓発定着傾向の違いについて考察を行う.

5.1 調査方式

本調査では, 4 章にて実施した, 判別難度が徐々に高くなる A 方式と徐々に低くなる B 方式に加えて, 一般的なフィッシング注意喚起資料に用いられる難易度 (Lv4) を常に提示する C 方式の演習を実施した. 本調査は期間をおいての 2 度にわたるアンケートを同じ被験者群に実施することで定着度評価を実現している (図 5.1).

5.1　調査方式

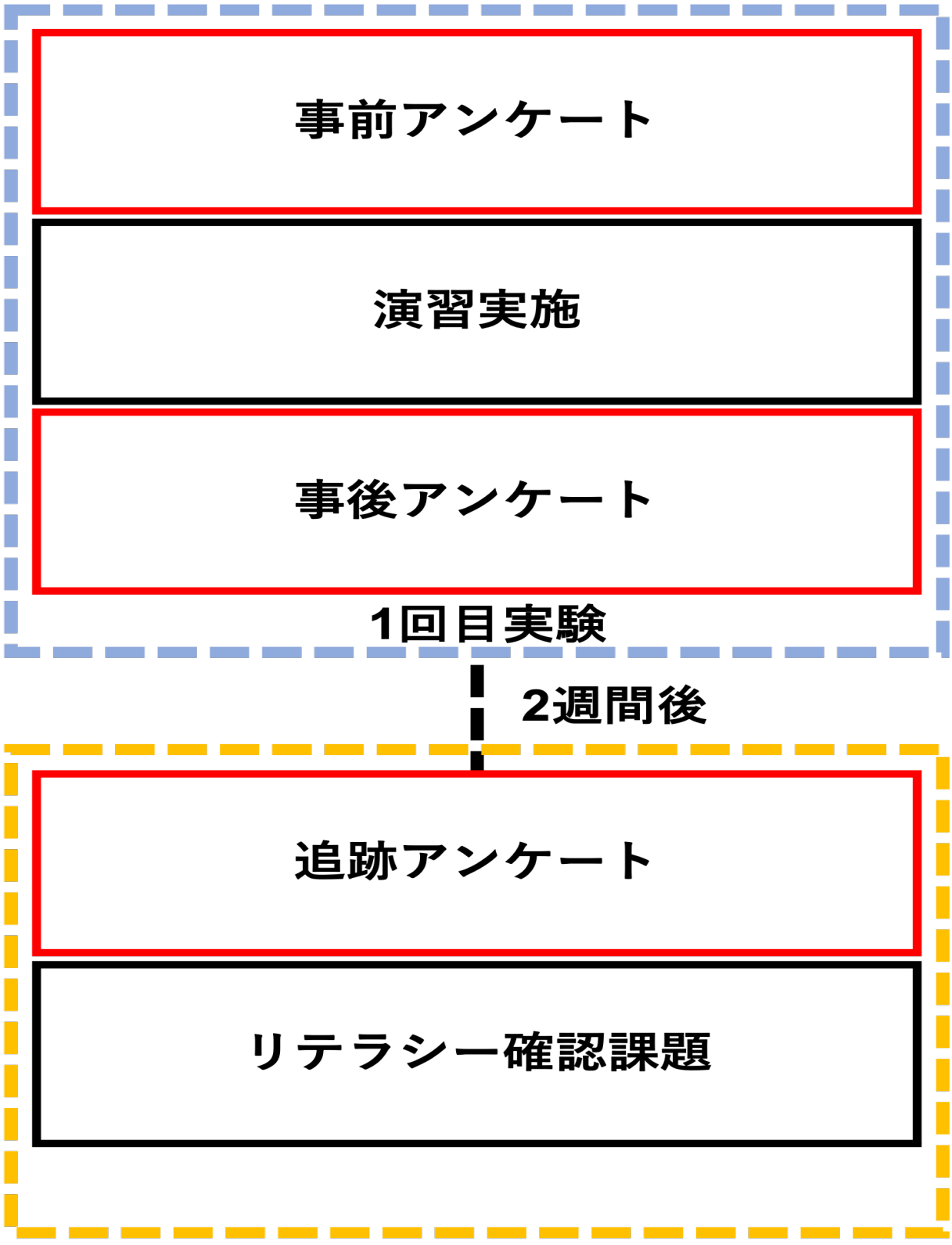

図 5.1　定着度評価アンケートスケジュール

5.1.1　調査条件

5.1.1.1　分析対象

- 2 回目アンケート回答者: 366 名　※不適切な回答を削除後の人数
  - A 方式: 136 名
  - B 方式: 110 名
  - C 方式: 120 名

5.1.1.2　メール内容

本実験では, 4.1 項で定義したメール内容をもとに提示を画像ではなく Web ページ上に提示している. Web ページ上で提示するにあたって変更する内容は以下の通りである.

- 被験者の利用経験があるサービスをモデルにメール提示
  - 国内で相当数のシェアを誇るサービスを 5 つから選択
- マスクされたリンクの内容
  - Lv3,Lv4: Lv1-Lv2 のマスクされる前のリンクを設定
  - Lv5: 実際のサービスのドメインに似せたリンクを設定

5.1.1.3　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.

啓発受講経験の確認

※ Q1 は YES(0), NO(1) の 2 択 Q1:詐欺メールに騙されないための説明を受けたことがある (事前/追跡)

無効感を推測する質問

Q2: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/追跡)

Q3: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/追跡)

Q4: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 (事前/事後/追跡)

対策行動への意欲確認

※ Q5,Q6 は YES(0), NO(1) の 2 択 Q5: 今月中にフィッシングを疑った頻度 (追跡)

Q6: 今月中にフィッシングメールを目にした枚数 (事前/追跡)

メールへの印象確認

- 画像のメールは信頼できるか (画像提示毎)

リテラシーへの自信の確認

- リスト (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 (事後)

5.1.1.4　回答者除外条件

Web アンケートの特性上, 不誠実な回答が行われた可能性が存在する. そのため本調査では以下に示す条件に該当する回答者を分析前に除外している.

- 5 点評価方式の質問全てに同じ値で回答
- マトリクス形式の問題に対して順列で回答
  - 6 つの要素に順位ずけを行う質問にて 1,2,...,5,6 と回答

また, 本実験では演習を自作ページ, アンケートを Google form で実施した. その際に実施した演習方式とアンケートの対応を取るために演習実施後にページへ表示する ID をアンケートへコピー&ペーストするように指示を行っていた. その結果, 総演習実施者 820 名に対してアンケート回答者が 545 名となっており ID の入力操作を行わず離脱したユーザ 276

名 (A 方式: 79 名, B 方式: 100 名 C 方式: 97 名) が除外されている．回答者と離脱者の「メールへの印象確認」に対する回答合計値の内訳は図 5.2, 5.3, 5.4 の通りである．

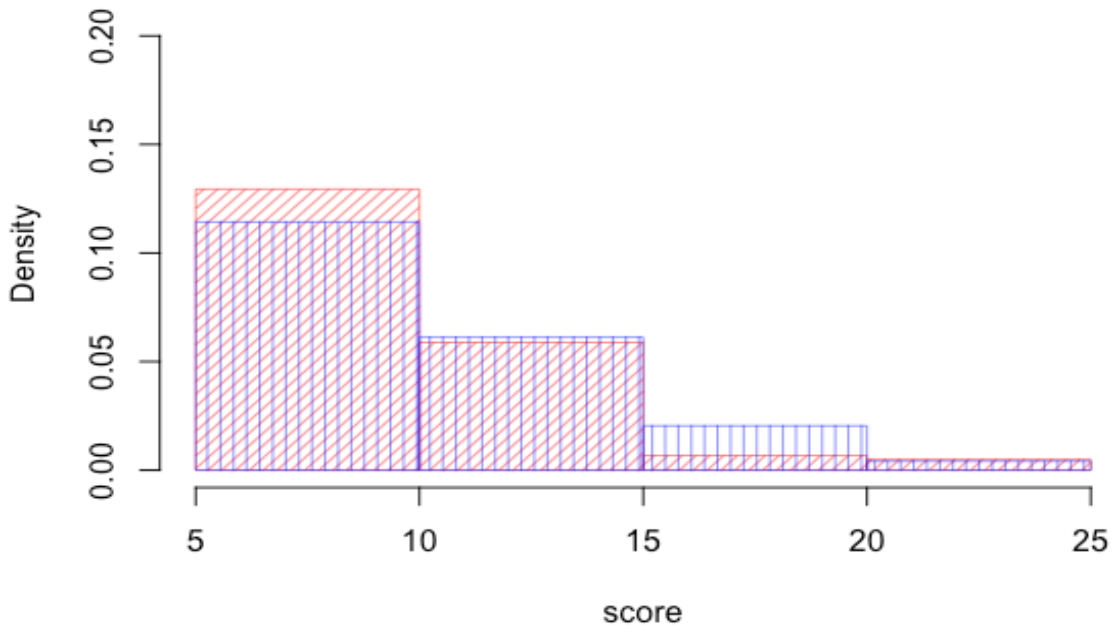

図 5.2　A 方式: 演習回答合計分布 (斜線: 参加者, 縦線: 離脱者)

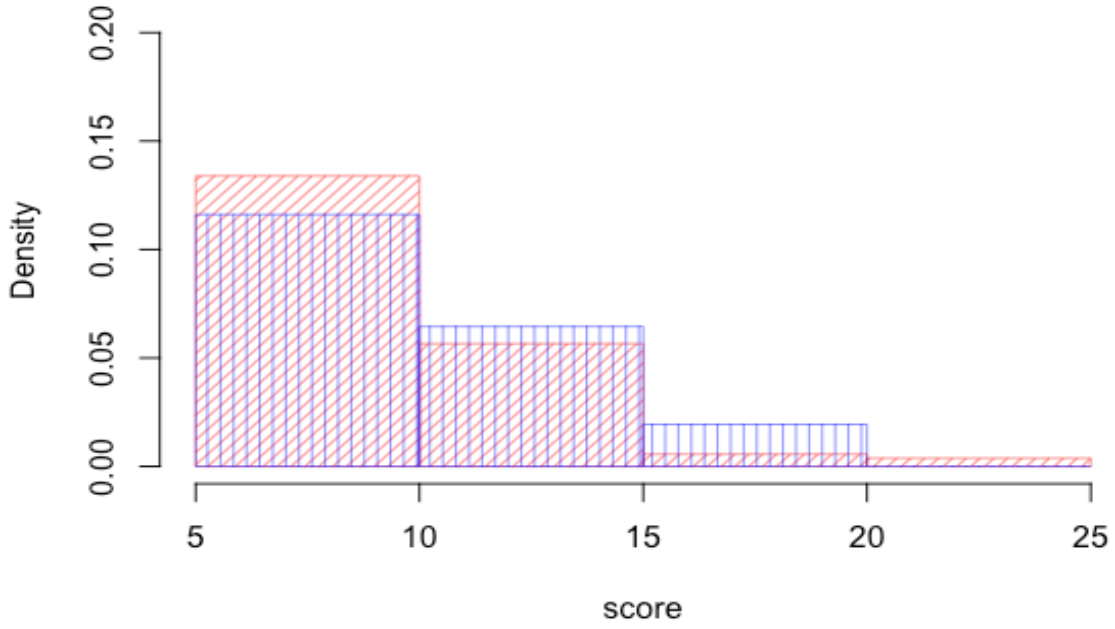

図 5.3　B 方式: 演習回答合計分布 (斜線: 参加者, 縦線: 離脱者)

5.1.1.5　リテラシー確認課題

2 回目実験の最後に図 5.5 のようなメール画像を提示し「このメールを目にした際に注目する箇所を順位づけて回答してくだい」を重複回答不可として回答させた. 図のうち A(メールアドレス), D(マスクされたリンク), F(リンクの中身) を, 優先順位 3 位以内で選択していた場合に得点として加算している. 点数は有効性に準じて以下の通りに設定した.

- メールアドレス: 2 点
- マスクされたリンク: 1 点
- リンクの中身: 3 点

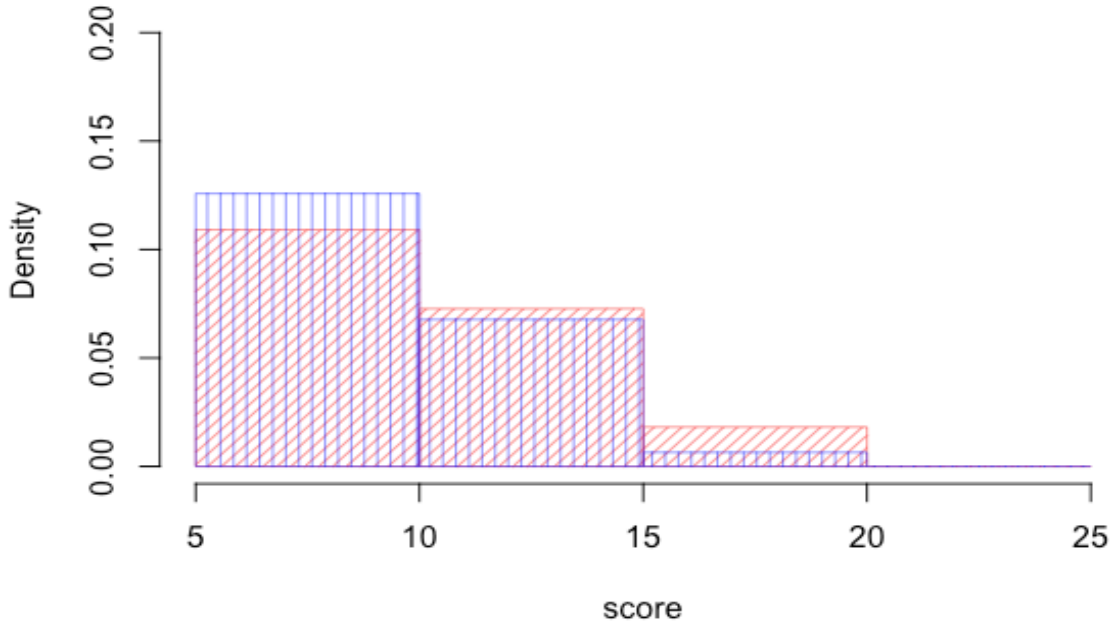

図 5.4　C 方式: 演習回答合計分布 (斜線: 参加者, 縦線: 離脱者)

5.2　調査結果

本節では事前アンケートから追跡アンケートにかけての回答推移を演習方式ごとに示すと共に追跡アンケートにて方式間での比較分析を行った結果を示す事で, 実験参加者の特性と定着度の関係を示す.

5.2.1　実験過程による推移分析

方式ごとに 2 つ以上のアンケートにて行った 5 点評価形式の質問の回答推移と検定結果を表 5.2.1 表 5.2.1 に示す. 方式に関わらず演習実施直後は回答が高めに遷移する傾向にあることがわかる. この時, 方式間で有意差はみられないが C 方式のみ Q2 において有意に高い回答を行っていることが確認できた. これが, 2 週間後の追跡アンケートとの比較となると以下に示すように方式ごとに異なる傾向を示した.

5.2　調査結果

図 5.5　提示メールイメージ

- A 方式
  - 全ての質問において有意差はみられないことから, 演習が印象に残っているとはいえない
- B 方式
  - Q2 が有意に高まる傾向がみられたことから, フィッシングに対して脅威を感じるようになった傾向がみられる
  - Q3 が有意に高まっていることから, ルールの必要性を感じ対策への意欲が高まっていることがわかる

表 5.1　各群の回答平均値 (事前:事後比較)

質問	演習方式	事前	事後	p 値
Q2	A	3.82	3.89	0.24
	B	3.75	3.84	0.22
	C	3.85	4.03	$p<0.001^{***}$
Q3	A	3.71	3.81	$0.052^{\dagger}$
	B	3.47	3.74	$p<0.001^{***}$
	C	3.67	3.90	$p<0.001^{***}$
Q4	A	3.21	3.71	$p<0.001^{***}$
	B	3.10	3.66	$p<0.001^{***}$
	C	3.36	3.85	$p<0.001^{***}$

$^{*}p<0.05$, $^{***}p<0.001$

- C 方式
  - Q2 が有意に高まることから, フィッシングに対して脅威を感じていることがわかる
  - Q4 が有意に高まる傾向にあったことから, 事前アンケートと演習が印象に残っていた傾向がみられる

5.2.2　追跡アンケートの分散分析

追跡アンケートについて,　リテラシー分類を行ったデータについて分散分析を行った結果を表 5.2.2 にそれぞれ示す. 本分析ではリテラシー確認課題で算出したスコアを基に被験者を 3 群に分類した. 分類は以下の通りである.

- Low: 0-1 点
- Mid: 2-3 点
- High: 4-6 点

表 5.2　各群の回答平均値 (事前:追跡比較)

質問	演習方式	事前	追跡	p 値
Q2	A	3.82	3.86	0.58
	B	3.75	3.93	$0.08^{\dagger}$
	C	3.85	4.03	0.02^{*}
Q3	A	3.71	3.68	0.69
	B	3.47	3.71	0.02^{*}
	C	3.67	3.81	$0.06^{\dagger}$
Q4	A	3.21	3.25	0.64
	B	3.10	3.33	0.02^{*}
	C	3.36	3.63	0.002^{**}

$^{\dagger}p<0.1$, $^{*}p<0.05$, $^{**}p<0.01$

Q2, Q3 に関してはどのリテラシー分類においても有意な差がなかったことから, 演習方式によってあるリテラシー層の無効感と関心に中長期的な影響を与える傾向は認められないことがわかる. 対して, Q4 は Low 群において有意傾向, Mid 群において有意差がみられた. この時, 一定の難易度でメール提示を行う C 方式が常に高い値を示していることがわかる. しかし, High 群において B 方式の平均値が高まったため有意差は確認されなかった.

5.2.3　演習実施が印象に残っている群のユーザ特性

定着度を評価するにあたって, 1 回目実験と演習が実施されてことが印象に残っている可能性が高い「演習実施が印象に残っている群」を本実験では以下の条件を満たす被験者として定義した.

- 追跡アンケートにて啓発受講経験を「あり」と回答
- 追跡アンケートにて Q4 に 4 以上で回答
- 追跡アンケートにて Q5 に対して疑う機会があったと回答

方式ごとに「演習実施が印象に残っている群」とそうでない群で比較検定を行った結果を表 5.2.3 に示す.

Q3 については, 方式に関わらず「演習実施が印象に残っている群」が有意に高い回答をする傾向が見られ, 関心との相関があることが伺えた. 対して, Q2 は B 方式でのみ有意差が見られたことから徐々に判別難度を下げていく演習は比較的, 中長期的に無効感を与えることが示唆された.

5.3 考察

5.3.1 メール注目箇所に基づいた定着度評価

メールの構成要素においてロゴは非常にユーザの注目を集めやすく [20], 昨今のフィッシングメールにおいては常習的に用いられている. そのため 1 回目実験で行った演習解説においてロゴの有無はメールの正当性を判断する要素として不適切であると示していた. 従って, 啓発内容が定着しているユーザとそうでないユーザで最も顕著に差が見られる要素であると考えられる. そこで, ロゴへの優先順位づけの傾向を演習方式で分類したものを図 5.6 に示す. 図 5.6 より, B 方式のユーザ群が比較的, ロゴへの優先度を低く設定しており, フィルタリングを行っていない方式のみの分類でも A - B 方式間に多重比較で有意傾向 ($adj.p = .056$) がみられた. これに加えて, 5.2.3 項にて設定した演習が印象に残っている群間のユーザにフィルタリングしたものを図 5.7 に示す. 方式間の差がより顕著にみられるようになっていることがわかり ($p = .029$, $\eta^2 = 0.09$), 多重比較で A - B 間に有意差 ($adj.p = .025$), B - C 間で有意傾向 ($adj.p = .087$) がみられた. 以上より, ステップダウン形式で演習を行う B 方式は啓発内容を定着させることに適していると言える.

5.3.2 C 方式と実験参加者分布の関連

定着度評価を行う本実験にて, 比較対象として追加した C 方式が追跡アンケートにおいて比較的, 高い対策意欲を示すことが表 5.2.2 より確認できた. また, グループ分類のみの表

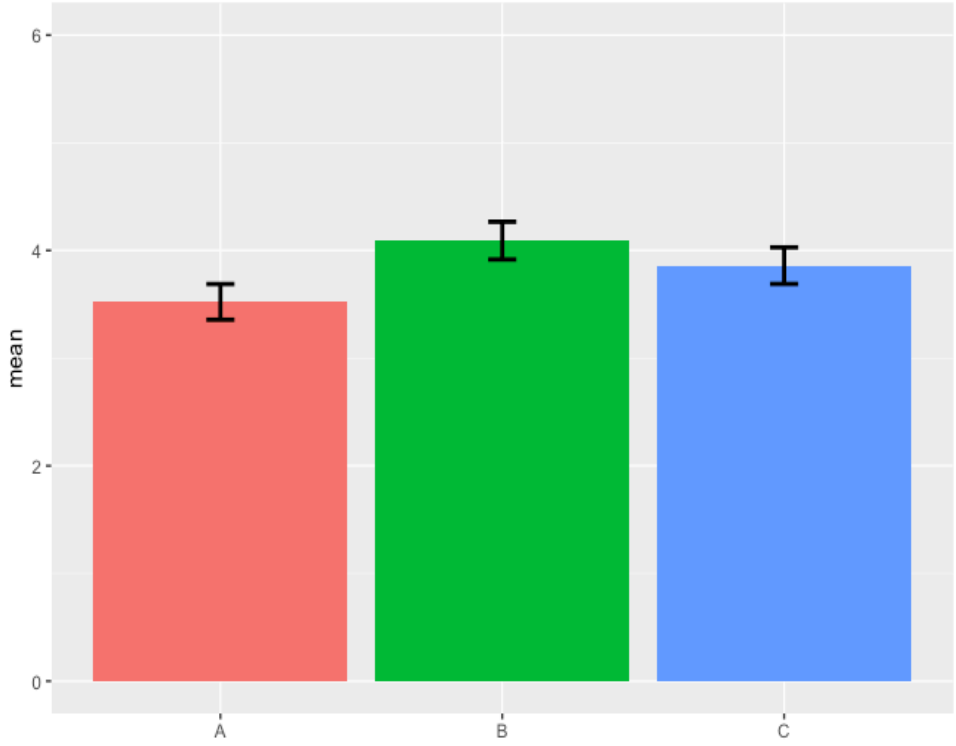

図 5.6　方式間: ロゴへの着目順位

5.2.1 からも同じ傾向が伺えた．このことから本実験の被験者群においては C 方式が対策意欲を保つのに有効だったと言える．

このようになった要因としては, 被験者層が限定されていたためであると考えられる．本実験では, 5.1.1.4 項で示したように相当数のユーザがアンケートを完了していなかった．

各方式の参加者と離脱者分類を行った演習スコア分布 (図 5.2, 5.3, 5.4) を見ると A, B 方式は離脱者が比較的高いスコアまで分布していることから, 「提示されたメールの多くを信用できると感じていたユーザ」が離脱者に多く含まれていたことがわかる．対して, C 方式は逆の分布を示す傾向にあることから「提示されたメールの多くを怪しいと感じていたユーザ」が離脱者に多く含まれていたことが分かる．そのため, 演習後に提示されたものがフィッシングであると開示された際に関心が高まるユーザが比較的多く含まれていた C 方式が全体的に高い対策意欲を示したと推測される．

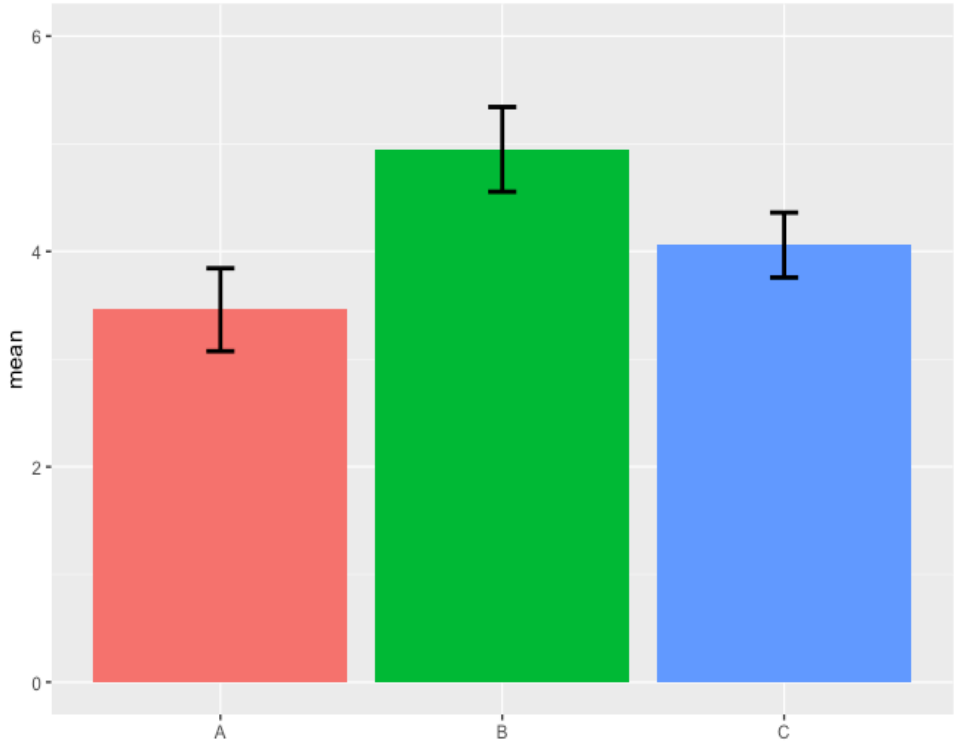

図 5.7　印象に残っているユーザ間: ロゴへの着目順位

表 5.3 Low 群比較

質問	演習方式	平均値	p 値
Q2	A(n=30)	3.90	0.44
	B(n=29)	3.69	
	C(n=16)	4.00	
Q3	A	3.50	0.60
	B	3.56	
	C	3.72	
Q4	A	3.00	0.09†
	B	3.25	
	C	3.55	

†p<0.1

表 5.4 Mid 群比較

質問	演習方式	平均値	p 値
Q2	A(n=77)	3.86	0.49
	B(n=62)	3.93	
	C(n=68)	4.03	
Q3	A	3.77	0.92
	B	3.75	
	C	3.81	
Q4	A	3.30	0.03*
	B	3.25	
	C	3.66	

*p<0.05

表 5.5 High 群比較

質問	演習方式	平均値	p 値
Q2	A(n=29)	3.86	0.34
	B(n=29)	4.07	
	C(n=26)	4.06	
Q3	A	3.65	0.42
	B	3.73	
	C	3.93	
Q4	A	3.38	0.47
	B	3.58	
	C	3.62	

表 5.6　演習実施が印象に残っている群の方式内比較

A 方式

質問	印象に残っている群	平均値	p 値	η ^2
Q2	TRUE(n=24)	4.00	0.407	0.005
	FALSE(n=112)	3.84		
Q3	TRUE	4.08	0.010*	0.047
	FALSE	3.60		

B 方式

質問	印象に残っている群	平均値	p 値	η ^2
Q2	TRUE(n=19)	4.26	0.040*	0.038
	FALSE(n=91)	3.86		
Q3	TRUE	4.15	0.012*	0.057
	FALSE	3.63		

C 方式

質問	印象に残っている群	平均値	p 値	η ^2
Q2	TRUE(n=34)	4.15	0.271	0.010
	FALSE(n=86)	3.99		
Q3	TRUE	4.09	0.017*	0.047
	FALSE	3.71		

$^{\dagger}p<0.1$, $^{*}p<0.05$

第 6 章

議論

6.1　演習方式の特徴に基づいた啓発手法の提案

本研究ではフィッシングに対するセキュリティ啓発において有効な HF 要素の分析を行い演習方式を 2 つ設計した．それらに 4.3.3 項にて比較対象として定義した演習方式を基に設計した C 方式も含めて定着度を評価することで, 3 つの方式には一長一短の特徴があることが確認できた．そのため, 1 つの優れた方式から啓発手法を提案するのではなく, 各方式の評価を基に適切な利用場面を示すことがセキュリティ対策行動を促す啓発手法の提案となると考える．

6.2　A 方式に適した利用場面

3, 4 章を通して, 演習直後に対策意欲を高めるには徐々に判別難度を高める A 方式を採用することがリテラシー自信度の影響を比較的おさえることにつながるため有効であるとした．しかし, 5 章において中長期的な視点で定着度の評価を行ったところ継続的に対策意欲を高める, 演習により与えた印象や啓発内容が他方式と比較して定着しているといったことは認められなかった．従って, A 方式はその場において幅広いユーザに対して脅威を認知させ対策意欲を高めたい場面で有効である．例えば, 講師がセキュリティ対策講習会を行う際などにデモ演習のような位置づけで実施すれば, 参加者の無効感を高めるが関心も高めることに繋がりその後の受講に対して意欲的とさせることが期待できる．

6.3　B 方式に適した利用場面

徐々に判別難度を下げる B 方式は 4 章までは演習直後はリテラシー自信度が高いユーザの対策意欲が有意に下がってしまうといった傾向が見られていたが, 定着度に着目して評価すると他方式よりも優れていることが高い効果を示しつつ確認された. 従って, B 方式は自習を通して留意点をユーザへ中長期的に意識させたい場面で有効である. 例えば, 各々が自身の都合に合わせて受講するようなオンライン研修において実施すれば, 研修内容の定着が期待できる. ただし, 本実験においては定着度を推測するのに適した「ロゴ」に着目することで方式間との差異を確認することができたが, 定着する留意点の傾向は不透明である. そのため, 定着させたい留意点を明確にして提示するなどして, 定着する可能性を高めることが重要となると考えられる.

6.4　C 方式に適した利用場面

常に一定の判別難度となるようにメール提示を行う C 方式については 4 章のように厳密に提示条件を調整しての分析を行っていないため, 演習直後の対策意欲について正確に比較できているとは限らないが, 3 つの方式のなかで最も対策意欲を高めるのに有効であると考えられる. 定着度については, B 方式と比較すると具体的な留意点が定着しているとは言えないが, 期間をおいても演習の実施が印象に残っていると見られるユーザの比率は高く, 対策意欲も高い傾向にあった. しかし, 定着度評価の実験において発生した離脱者にリテラシーが低い層が多い傾向が見られたため, 4.3.3 項で仮定したようなユーザに適した判別難度に調整されていた可能性がある. そのため, 幅広いユーザ層が混在する環境においても本研究と同じ傾向の効果が期待できるとはいい難い. 従って, C 方式は演習を受けるユーザ群のリテラシー理解度がある程度予想することができ, 適宜提示するメールの判別難度を調整することができる管理者がいる場面で非常に有効であると考えられる. 例えば, 特定の部署などで対象となるユーザの傾向を理解している担当者が啓発を実施する際に効果が期待できる.

第 7 章

結論

近年, 増加傾向にあるフィッシング被害への対策としてヒューマンファクタに着目した演習方式を設計し比較分析を行い, 定着度を評価した. 結果として各演習方式にはそれぞれ一長一短の特徴があることが伺えたため利用場面に応じて, 適用する演習方式を変更することをセキュリティ対策行動を促す啓発手法として提案した.

本研究ではユーザ特性の中でもフィッシング対応についてより影響が大きいと考えられる, リテラシーに着目し幅広い層のユーザの対策意欲を高める演習方式を分析してきた. 本提案手法を用いることで幅広いユーザ層, 啓発場面において有効な啓発実施を可能とすることが期待されるが, より効果的な啓発とするには演習後の解説と補足が非常に重要となる. 啓発は対策行動への動機付けとなる演習とその内容に合致した解説を行うことで相乗効果が得られるとされている. 解説は含めるキーワードやレイアウト, 文量, 図表の有無, 用いる専門用語, 提示タイミング, 演習内容との関連度などユーザへ影響を与えると考えられる要素は多くある. これらを踏まえて本研究で示した各演習方式に適した解説方法を検討することでより完成度の高い啓発手法の提案へと繋がることが期待される.

謝辞

本研究を進めるにあたり, 多くの方々にご協力をいただきました. 特に指導教員である敷田幹文先生には, 学年主任であったことも鑑みると大学生活のすべて, 実に 6 年間にわたりお世話になりました. 研究活動をはじめとして, 就職活動などあらゆる場面にてご指導いただき高知工科大学の卒業生として社会に出ていけるまでに成長させていただきました. 心より感謝申し上げます. また, 学部時代から継続して副査をご担当くださり, 私が研究の方向性を見失うことなく根本となる主張ができるように助言をしてくださった, 福本昌弘先生と植田和憲先生のお二人にも厚くお礼申し上げます. さらに, 研究の考えを整理するにあたっての議論や発表練習に幾度となく付き合ってくれた同期の友人や研究室の後輩, 先輩の方々にも感謝を申し上げます. そして, セキュリティハッカソン SeckHack365 でトレーナーとして指導いただき, 研究についてもコメントを下さった国立研究開発法人情報通信研究機構の佐藤公信様, 同所属の安田真悟様, トレンドマイクロ株式会社の今佑輔様, チーム開発のメンバーにも深く御礼申し上げます. 最後に今日に至るまであらゆる面で支えてくれた母や祖父, 祖母, 叔父, 叔母, 従兄弟, 友人, 小中高の恩師の皆様に心より感謝を申し上げます.

参考文献

[1] IPA 独立行政法人情報処理推進機構. 安心相談窓口だより：ipa 独立行政法人情報処理推進機構. https://www.ipa.go.jp/security/anshin/mgdayori20210831.html. (Accessed on 12/26/2022).

[2] 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 01/2023).

[3] 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).

[4] 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 01/2023).

[5] 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).

[6] 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).

[7] 笠間貴弘, 安田真悟, 佐藤公信, 神薗雅紀, 小島恵美, 山口孝夫, 奈良和春. セキュリティインシデント対応に適したノンテクニカルスキルマップの提案. 情報処理学会研究報告, Vol. 32, No. 26, pp. 1–6, feb 2019.

[8] 谷口勇仁. 規則の形骸化の発生プロセス：不正のトライアングル理論に基づく検討. 經濟學研究, Vol. 67, No. 1, pp. 5–13, jun 2017.

[9] 河野龍太郎. 医療におけるリスクマネージメント. https://www.mlit.go.jp/common/001067785.pdf. (Accessed on 02/02/2023).

[10] 飯島朋子, 野田文夫, 桂司須藤, 村岡浩治, 船引浩平. CRM スキル行動指標の開発. 航空宇宙技術研究所報告, Vol. 1465, pp. 1–59, jul 2003.

[11] Giuseppe Desolda, Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. Human factors in phishing attacks: A systematic literature review. *ACM Comput. Surv.*, Vol. 54, No. 8, pp. 1–35, oct 2021.

[12] 中野佑輔, 田隈広紀. ナッジツールを用いた学生のセキュリティ意識向上の提案. 国際P2M 学会研究発表大会予稿集, Vol. 2020.Spring, pp. 285–291, 2020.

[13] 黒澤和人. 情報倫理とセキュリティの教育について〜一般情報教育の役割として〜. 研究報告コンピュータと教育, Vol. 139, No. 18, pp. 1–8, mar 2017.

[14] 畑島隆, 坂本泰久. 情報セキュリティ不安全行動に対するテレワーク実施者の性向の分析. 情報処理学会論文誌, Vol. 58, No. 12, pp. 1912–1925, dec 2017.

[15] 佐野絢音, 澤谷雪子, 山田明, 窪田歩. ユーザのセキュリティ対策行動における心理的な要因の影響分析と評価. 情報処理学会論文誌, Vol. 61, No. 12, pp. 1831–1844, dec 2020.

[16] 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.

[17] 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.

[18] 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*, pp. 1–10. Association for Computing Machinery, 2017.

[19] 一川誠. ヒューマンエラーの心理学. 筑摩書房, 2019.

[20] 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.

付録

Web ユーザを対象とした効果的なアンケート調査の実施

本研究では, Web 上のユーザを対象にアンケートを 3 度実施した. 対面形式とは比較にならない規模と回収速度が期待できる反面, 回答者の状況や特性を考慮する必要があるためアンケートの構成に留意することが非常に重要である.

回答者の知識レベルに依存しない形式

本研究では, 意図しない箇所で回答者の知識による差が生じることがないように留意した. 例えば, 「フィッシングメールを見たことがあるか」では「フィッシング」という用語を知らない回答者は正常な回答を行えない可能性が高まる. これを考慮して一般的な「詐欺メール」という用語に置き換えることで, 用語の知る知らないに関わらず同じ回答が得られるようにしている.

回答者の途中離脱の防止

対面形式とは異なり回答者の離脱についても考慮する必要がある. 本研究においても相当数のユーザが離脱するという事態が起こったが, 状況によっては偏ったユーザ層の回答が多く含まれる事になるため注意が必要である. 離脱の大きな要因としては「作業量の多さ」が挙げられる. Web 形式のアンケートは自身の発行したもの以外にも無数の候補が存在するため, 何十問にもわたる質問や進捗度の見えない構成, 難解な要求により回答者の負担が増加する. その兆しが見えると最後まで回答せずに離脱, 最悪の場合, デタラメな回答を行うといった可能性が高まる. これを予防するためには明確に知りたい事柄を厳選してアンケートに含める, 進捗度が目に見えて分かるような表現を含める (1/5 のような表現, フォームによっては進捗バーなどを設定する) と良いと考えられる.

不適切な回答者の削除

前項にて少し触れたが, web アンケートは報酬を伴うものが多いため, 質問文に目を通すことなく回答を繰り返すユーザが存在する可能性を考慮する必要がある.(無報酬で実施することも可能ではあるが, それに応じる回答者は一般的なユーザとは異なる点に留意する必要がある) 本実験で実施, 検討した不適切な回答者の削除方法を以下に示す.

- 質問文を読んで回答しているかを確認
  - 5 点評価方式の問題に対して, 全て 1(同じ値) で回答
  - 重複不可のマトリクス形式質問に対して, 順列 (1,2,3,4,5,6) で回答
  - 回答の開始から終了までの時間が極端に短い
  - ダミー問題 (2 と回答してください等) に正しく回答していない
- 矛盾する回答を行っていないかを確認
  -「詐欺メールを見たことがない」かつ「今月に詐欺メールを 10 通以上見た」と回答

また, 分布等で全体を俯瞰できる形式にデータを変換し説明がつかないようなデータ群が存在しないかを分析することも有用である. 見つかったデータを削除するのに妥当な説明が可能であれば, 論文や発表で明確に示すことを条件に削除することで見通しの良いデータ群となる場合がある.(考察の基となるようなデータである場合もあるので扱いに際しては熟考することが望ましい)

表 1　A 方式推移分析結果 (事前:事後比較)

A 方式 T 検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(事後)	−1.173	135	0.243	−0.101	0.069
Q3(事前)	-	Q3(事後)	−1.962	135	0.052	−0.168	0.062
Q4(事前)	-	Q4(事後)	−6.460	135	1.755×10^{-9}	−0.554	0.086

A 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	136	3.824	0.806	0.069	0.211
Q2(事後)	136	3.890	0.832	0.071	0.214
Q3(事前)	136	3.713	0.778	0.067	0.210
Q3(事後)	136	3.816	0.896	0.077	0.235
Q4(事前)	136	3.213	0.922	0.079	0.287
Q4(事後)	136	3.713	0.996	0.085	0.268

表 2　B 方式推移分析結果 (事前:事後比較)

B 方式 T 検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(事後)	−1.215	109	0.227	−0.116	0.085
Q3(事前)	-	Q3(事後)	−3.952	109	1.379×10^{-4}	−0.377	0.072
Q4(事前)	-	Q4(事後)	−6.468	109	2.903×10^{-9}	−0.617	0.098

B 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	110	3.745	0.882	0.084	0.236
Q2(事後)	110	3.836	0.883	0.084	0.230
Q3(事前)	110	3.473	1.002	0.096	0.289
Q3(事後)	110	3.736	0.915	0.087	0.245
Q4(事前)	110	3.100	0.986	0.094	0.318
Q4(事後)	110	3.664	0.951	0.091	0.260

表 3　C 方式推移分析結果 (事前:事後比較)

C 方式検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(事後)	−3.253	119	0.001	−0.297	0.071
Q3(事前)	-	Q3(事後)	−3.964	119	1.260×10^{-4}	−0.362	0.074
Q4(事前)	-	Q4(事後)	−7.345	119	2.807×10^{-11}	−0.670	0.085

C 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	120	3.850	0.827	0.075	0.215
Q2(事後)	120	4.025	0.667	0.061	0.166
Q3(事前)	120	3.667	0.863	0.079	0.235
Q3(事後)	120	3.900	0.760	0.069	0.195
Q4(事前)	120	3.358	0.896	0.082	0.267
Q4(事後)	120	3.850	0.847	0.077	0.220

表 4　A 方式推移分析結果 (事前:追跡比較)

A 方式検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(追跡)	−0.551	135	0.583	−0.047	0.096
Q3(事前)	-	Q3(追跡)	0.403	135	0.688	0.035	0.090
Q4(事前)	-	Q4(追跡)	−0.473	135	0.637	−0.041	0.081

A 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	136	3.824	0.806	0.069	0.211
Q2(追跡)	136	3.868	0.859	0.074	0.222
Q3(事前)	136	3.713	0.778	0.067	0.210
Q3(追跡)	136	3.684	0.849	0.073	0.231
Q4(事前)	136	3.213	0.922	0.079	0.287
Q4(追跡)	136	3.250	0.994	0.085	0.306

表 5　B 方式推移分析結果 (事前:追跡比較)

B 方式検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(追跡)	−1.800	109	0.075	−0.172	0.122
Q3(事前)	-	Q3(追跡)	−2.354	109	0.020	−0.224	0.113
Q4(事前)	-	Q4(追跡)	−2.425	109	0.017	−0.231	0.101

B 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	110	3.745	0.882	0.084	0.236
Q2(追跡)	110	3.927	0.786	0.075	0.200
Q3(事前)	110	3.473	1.002	0.096	0.289
Q3(追跡)	110	3.718	0.847	0.081	0.228
Q4(事前)	110	3.100	0.986	0.094	0.318
Q4(追跡)	110	3.327	0.879	0.084	0.264

表 6　C 方式推移分析結果 (事前:追跡比較)

C 方式検定

Measure 1		Measure 2	t	df	p	Cohen's d	SE Cohen's d
Q2(事前)	-	Q2(追跡)	−2.284	119	0.024	−0.209	0.105
Q3(事前)	-	Q3(追跡)	−1.876	119	0.063	−0.171	0.097
Q4(事前)	-	Q4(追跡)	−3.164	119	0.002	−0.289	0.100

C 方式回答

	N	Mean	SD	SE	Coefficient of variation
Q2(事前)	120	3.850	0.827	0.075	0.215
Q2(追跡)	120	4.033	0.709	0.065	0.176
Q3(事前)	120	3.667	0.863	0.079	0.235
Q3(追跡)	120	3.817	0.788	0.072	0.207
Q4(事前)	120	3.358	0.896	0.082	0.267
Q4(追跡)	120	3.625	0.821	0.075	0.226