

ユーザのサイト真偽判断行動と思考特性との関係性の検討

小倉加奈代^{†1}

概要: 本稿では、フィッシング犯罪に対し、ユーザの判断行動に関わる心理特性とユーザへの攻撃回避能力との関係を明らかにするために実施した調査のうち、サイトの真偽判断実験とその実験協力者を対象とした心理特性のうちの思考に関わる質問紙調査結果について報告する。今回は、思考特性として、物事を客観的に捉え、多面的・多角的に検討する思考である批判的思考態度尺度、判断を下すまでにじっくり進捗に考えるか、早急に結論を下すかの判断プロセスに関わる認知的熟慮性-衝動性尺度、物事を経験に基づき一般化しようとする認知的構造欲求尺度を用い、サイト真偽判断テスト結果との関係を検討する。

キーワード: フィッシング, リスク認知, 批判的思考態度, 認知的熟慮性-衝動性, 認知的構造欲求

An Examination of the Relation between Verifying Authenticity of Websites and Thinking Traits of Users

KANAYO OGURA^{†1}

Abstract: This paper examines a result of the relation between verifying authenticity of websites which consist of real Facebook and thinking traits based on a questionnaire survey. This questionnaire survey consists of "Critical Thinking Attitude" which signifies that we think objectively, multidirectionally and multilaterally, "Cognitive Reflection-Impulsivity" which means that we conclude carefully or without reflection or too soon, and "Cognitive Need for Structure" which means that we generalize based on our experience as thinking traits.

Keywords: Phishing, Risk Perception, Critical Thinking Attitude, Cognitive Reflection-Impulsivity, Cognitive Need for Structure

1. はじめに

フィッシング犯罪とは、犯罪者が正規の企業や組織になりすました偽メールを送信し、正規サイトを模した偽サイトへ誘導して、アカウント ID、パスワード、クレジットカード番号や暗証番号といった個人情報を入力させ窃取する犯罪である。一般的には、偽メールで、偽サイトへ誘導し、偽サイトに重要情報を入力し、それを犯罪者が窃取するプロセスを経る。フィッシング対策協議会の調査報告[1]によると、届出件数としては、国内フィッシング情報件数、フィッシングサイト件数は 2014 年に達し、2015 年度からは減少傾向にある。しかし、警察庁の発表[2]によると、フィッシングによる不正送金は約 30 億と被害額は巨額であり、年々わずかではあるが被害額は増大している。このことから、依然として、被害は拡大傾向にあり、フィッシング犯罪への対策は重要課題の 1 つであるといえる。

フィッシング犯罪防止のためには、(1)ユーザが、偽サイトに誘導する段階（主に偽メールであること）で気づく、(2)誘導先サイトが偽サイトであることに気づく、(3)偽サイトであることに気づかなかつたとしても個人情報を入力・送信しないことを選ぶことが必要となる。このために、偽メール・偽サイト検知技術の開発研究から個人情報入力・

送信時の警告に関する研究、犯罪事例を用いてユーザのセキュリティ意識や知識を高める教育に関する研究と多様な研究が存在する。一方で攻撃者側は、犯罪手口が世間に広まると、手口を精練し、新たな手口を考案する。その結果、犯罪者とフィッシング対策技術および犯罪を取り締まる側はたちごっこの関係から抜け出せないのが現状である。

本研究では、検知技術だけに頼るのではなく、ユーザ自身のリスクに対する感度を高めることによるフィッシング犯罪防止を模索する。この「リスクに対する感度」として、「必要以上に考えない」、「あらゆる選択肢をよく検討した上で結論を下す」といった人の考え方のくせや好みに関わる心理・思考特性が多かれ少なかれ影響すると考えられる。本稿では、ユーザ自身のフィッシング回避行動につながる「リスクに対する感度」に貢献する要素を明らかにするために、フィッシングサイトか否かの判断実験と認知判断傾向に関する心理特性測定尺度である、批判的思考態度尺度、認知的熟慮性-衝動性尺度、認知欲求尺度、認知的構造欲求尺度の 4 つの尺度を用いた質問紙調査を実施し、その結果により、サイト真偽判断行動とユーザの思考特性との関係性を検討する。

^{†1} 岩手県立大学
Iwate Prefectural University

2. 関連研究

2.1 フィッシング犯罪対策

フィッシング犯罪対策として、偽メール・偽サイト検知技術の開発、個人情報入力・送信時の警告の試み、犯罪事例を用いたユーザのセキュリティ意識や知識を高める教育コンテンツの開発と多様な方向性での対策が存在する。偽メール・偽サイト検知技術としては、機械学習、視覚的類似性、ブラックリストを用いた検知技術の開発研究が数多く行われている[3]。加えて、市販のウイルス対策ソフトやブラウザでは、偽メール判定やサイトの安全性判定機能をもつ製品が多く存在する。しかし、前述のように、手口が広まると、犯罪者側は、検知技術の脆弱性をついた新たな手口を考案するため、検知技術側が新たな手口に対策できていなければ対応することが困難である。個人情報入力・送信時の警告に関する研究としては、パスワードやクレジットカード情報などの重要個人情報入力・送信時に、警告ダイアログを表示することにより、情報送信のリスクを再考させ、結果的にセキュリティ意識の向上に貢献する種の研究[4][5]が存在する。しかし、これらの研究には警告に対する馴化の問題がある。犯罪事例を用いた教育コンテンツの開発や運用としては、警察庁、IPA等の団体や企業から教育コンテンツが数多く提供されている。しかし、前述のとおり、犯罪者は日々、犯罪手口を変えるため、事例ベースのコンテンツでは、犯罪の現状に追いつかない可能性が高い。

2.2 リスクと思考に関わる心理特性

リスク理解、リスク対処行動と思考に関わる心理特性との関係の解明を試みた研究として、楠見らの研究がある。楠見ら[6]は、福島第一原発事故後の放射能リスク理解に批判的思考態度がどのように影響するかを調査した。その結果、批判的思考態度はメディアリテラシーを向上させることを通して、知識や自発的な情報収集を促進し、リスク対処行動に影響を及ぼしていることがわかった。フィッシング判定も放射能リスク理解と類似するプロセスであると考えられるため、フィッシングに関わるリスク理解、対処行動にも批判的思考態度が影響する可能性がある。さらに楠見ら[7]は、食品の安全性やリスク認知を支える食品リスクリテラシーには情報に素早く反応するのではなく時間をかけて反応する熟慮的認知スタイルを土台とした批判的思考態度が影響すると説明している。

また、詐欺犯罪のリスクと心理特性との関係を試みた研究として鈴木の研究がある。鈴木[8]は、振り込め詐欺について分析し、物事を経験に基づき一般化しようとする認知的構造欲求の高い群は振り込め詐欺の被害を受けやすいことを明らかにした。フィッシングも振り込め詐欺と同じく

詐欺であるため、認知的構造欲求に関して同様の傾向を示す可能性があると考えられる。

3. 実験・調査方法

本稿では、フィッシング犯罪実行の2つのプロセス、(1)偽メールによる偽サイトへの誘導、(2)偽サイト内での重要個人情報の窃取のうち(2)に焦点をあてる。そのため、サイトの真偽判断や重要情報の入力・送信場面の危険性判断と、ユーザのPC・スマートデバイスの習熟度やセキュリティに関係する知識、考え方のくせに関係する心理特性との関係性を検討する。具体的には、サイトの真偽判断と情報の入力・送信場面の危険性判断については、実フィッシングサイト画面を用いた判定実験を実施した。PC・スマートデバイス習熟度、セキュリティに関係する知識と心理特性については、IPAの調査や企業や団体が提供しているセキュリティレベルチェックとして実在する質問項目および、心理測定尺度を用いて調査を実施した。

3.1 サイト真偽判断実験

3.1.1 実施時期

2016年10月に、著者が担当する講義、応用心理学(岩手県立大学ソフトウェア情報学部選択科目、開講学年1年生)の時間内に実施した。なお、本実験は、質問紙調査の実施時期とは異なる。

3.1.2 実験対象者

前述の応用心理学受講者106名が実験に参加した。しかし、本稿の分析対象は、本実験と後述する質問紙調査の両方に参加した80名(男性61名、女性19名、学年内訳は1年生68名、3年生11名、4年生1名)とした。

3.1.3 実験概要

本実験では、実在するサイト画面を8種類用意し、対象者に「入力フォームに個人情報を入力してもよいと思うか、思わないか」を判断させる課題を用意した。

3.1.4 対象サイト画面

使用するサイト画面のブランドは、対象者のサイト認知度が結果に影響する可能性を考慮し、Facebook[a]に統一した。また、サイト真偽に関係する知識の有無が結果に影響する可能性を考慮し、ブラウザのURLや暗号化表示を使用するサイト画面には一切表記しないこととした。使用するサイト画面は、高橋ら[9]の評価実験での誤検出サイトのうち、模倣元サイトとデザインがかけ離れた実在する偽サイト7種類と正規サイト1種類の合計8種類である。なお、偽サイトの7つは、PhishTank[b]に報告されているサイトである。

3.1.5 実験手続き

実験は、全対象者一斉に以下手順で実施した。

手順1: 実験承諾書および回答用紙を対象者へ配布

a Facebook: <https://www.facebook.com/>

b PhishTank: <https://www.phishtank.com/>

手順 2：対象者へ実験内容説明として以下手順を確認

- (1)これから 8 つのサイト画面をスクリーンに表示
- (2)個人情報を入力してもよいと思う場合は○
- (3)個人情報を入力しないほうがよいと思う場合は×
- (4)可能な限り理由も明記
- (5)各サイト画面は 2 分間表示
- (6)回答を後から見直すことはできない

手順 3：サイト画面を表示し、対象者は配布された回答用紙に回答を記入(8 回繰り返す)。

手順 4：対象者は、回答用紙を裏返し、裏面のアンケートに回答。なお、アンケートの内容は以下 4 つである。

- ・ PC 習熟度 (レベル 1～レベル 4 のうち 1 つを選択)
- ・ Facebook の利用状況 (1:未経験～4:頻繁に利用)
- ・ Facebook 利用時の使用媒体 (PC/スマホ/タブレット/その他 (複数回答可))
- ・ 「フィッシング」という用語の理解度 (1:全く知らない～4:知識を持っており、自分で対象ができる)

3.2 質問紙調査

3.2.1 実施時期

2016 年 12 月に、Web 上に回答フォームを用意し、調査対象者が好きな場所、好きな時間に取り組む形態とした。調査データの取り扱いに関する説明は回答開始前に対象者全員に対し紙面を配布し、口頭で説明した。Web 回答フォームの冒頭に、実験承諾に関する設問を用意し、調査データの取り扱い方法に承諾できない場合には、「承諾しない」の回答を選択することで、回答が終了する。また、本調査は、短縮 URL に関わる調査[10]、人間の脆弱性を利用したシナリオに関する調査[11]として実施した。

3.2.2 調査対象者

3.1.2 項と同様の 80 名である。

3.2.3 質問項目

本調査で分析対象とした質問項目は以下 6 つである。

- (1) PC/スマートデバイスの習熟度レベル
- (2) セキュリティ知識レベル
- (3) 批判的思考態度尺度
- (4) 認知的熟慮性-衝動性尺度
- (5) 認知欲求尺度
- (6) 認知的構造欲求尺度

なお、3.2.1 項のとおり、本調査には、短縮 URL に関わる設問、人間の脆弱性を利用したシナリオに関わる設問が含まれていたが、本稿では分析対象としない。

(1) PC/スマートデバイス習熟度レベル

IPA が実施した 2015 年度情報セキュリティの脅威に対する意識調査[12]の PC 習熟度およびスマートデバイス習熟度の設問を利用した。PC およびスマートデバイス習熟度レベルの設問では、回答者に、表 1 および表 2 に示すレベル 1 からレベル 4 の説明のうち、自身のスキルレベルに最もあてはまるものを 1 つ回答することを求めた。

表 1. PC 習熟度レベルの設問内容

レベル 1： 入門・初心者	設定等はお店でしてもらい、買った時のままにしている
レベル 2： 基本操作は習熟	メールを使ったり、ホームページを閲覧できる
レベル 3： 習熟	必要なアプリをインストールしたり、設定を変更したりして使える
レベル 4： 非常に習熟	PC を組み立てたり、トラブルが起きても自分で解決できる。

表 2. スマートフォン習熟度レベルの設問内容

レベル 1： 入門・初心者	設定等はお店でしてもらい、買った時のままにしている
レベル 2： 基本操作は習熟	メールを使ったり、ホームページを閲覧したりするのに支障がない
レベル 3： 習熟	必要なアプリをインストールしたり、設定を変更したりして使える
レベル 4： 非常に習熟	トラブルが起きても自分で解決できる

(2) セキュリティ知識レベル

トレンドマイクロ社が提供する、「ネット詐欺の手口と対処方法をクイズで確認 (4 問)」[13]および「セキュリティの常識をクイズでチェック！」(5 問)[14]を利用した。これは、実際のフィッシングの手口に関わる内容、Web サイトやスマートデバイス、Wi-Fi の利用に関わる内容であり、それぞれの設問に対し、回答者に、「はい」「いいえ」のいずれかで回答を求めた。

(3) 批判的思考態度尺度

平山ら[15]の批判的思考態度尺度 33 項目を利用した。本尺度は、「論理的思考への自覚」(13 項目、設問例「複雑な問題について順序立てて考えることが得意だ」)、「探究心」(10 項目、設問例「いろいろな考え方の人と接して多くのことを学びたい」)、「客観性」(7 項目、設問例「いつも偏りのない判断をしようとする」)、「証拠の重視」(3 項目、設問例「結論をくだす場合には、確たる証拠の有無にこだわる」)の 4 因子から構成されている。各項目について、回答者に「1:あてはまらない」から「5:あてはまる」の 5 段階での評定を求めた。

(4) 認知的熟慮性-衝動性尺度

滝間ら[16]の認知的熟慮性-衝動性尺度 10 項目を利用した。質問内容は、「深く物事を考えるほうだ。」、「用心深いほうだ。」のような物事を判断する際の認知傾向に関する設問である。各項目について、回答者に「1:あてはまらない」から「4:あてはまる」の 4 段階での評定を求めた。

(5) 認知欲求尺度

神山ら[17]の認知欲求尺度 15 項目を利用した。本尺度は、「常に頭を使わなければ満足しない」、「簡単な問題よりも複雑な問題のほうが好きだ」のような考えることへの動機づけを測定する尺度である。各設問に対し、回答者に「1:非常に当てはまらない」から「7:非常に当てはまる」までの7段階での評定を求めた。

(6) 認知的構造欲求尺度

鈴木ら[18]の認知的構造欲求尺度 10 項目を利用した。本尺度は「その場のルールがはっきりしないと嫌な気分になる」、「規則正しい生活は退屈だ」のような物事を経験に基づき一般化するかを測定する尺度であり、「構造に対する願望」と「構造欠如に対する反応」という2つの因子を持つ。各設問に対し、回答者に「1:非常に当てはまらない」から「7:非常に当てはまる」までの6段階での評定を求めた。

4. 結果と考察

3 章で説明したサイト真偽判断実験結果および質問紙調査の各回答結果について説明する。また、4.2 節以降、結果を検討するために、サイト真偽判定結果に関する分析、各心理特性結果に関する分析について説明する。

4.1 サイト真偽判断実験結果

本実験の回答形式は 3.1.5 項で述べたように、「個人情報を入力してもよいと思う場合は○」、「個人情報を入力しないほうがよいと思う場合は×」とした。正解・不正解の判定は、個人情報を入力してよい場合は、「正規サイト」と判断した場合、個人情報を入力しないほうがよい場合は、「偽サイト」と判断した場合として各設問の正解と照合し、正解・不正解を判定した。

全 8 問の正解率を表 3 に、得点分布を図 1 に示す。正解率が 80%後半の設問が複数ある一方で、28.8%と著しく低い設問も存在した。正解率が著しく低かった問 6 のサイト画像を図 2 に示す。

表 3. サイト真偽判断実験各設問正答率

	正解率(%) (N=80)
問 1	77.5
問 2	65.0
問 3	87.5
問 4	72.5
問 5	88.8
問 6	28.8
問 7	67.5
問 8	93.8
全平均	72.7

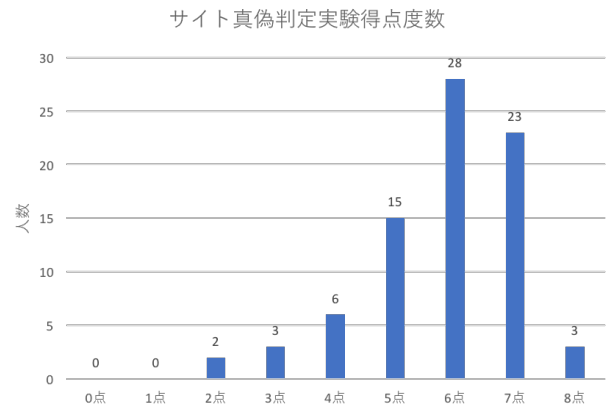


図 1. サイト真偽判定実験得点分布

(N=80, Ave.=5.81, SD=1.28)

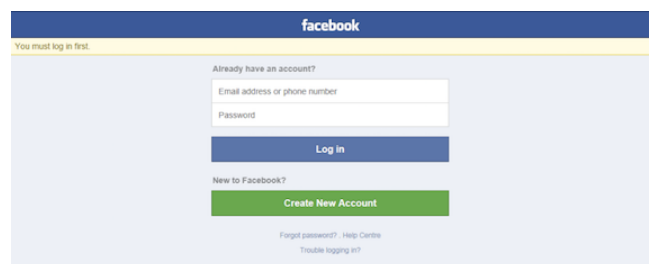


図 2. 問 6 (正解率の著しく低い設問) のサイト画像

4.2 質問紙調査結果

4.2.1 PC/スマートデバイス習熟度

PC とスマートデバイスの習熟度レベルの回答結果を表に示す。PC, スマートデバイスいずれも初心者レベルの回答者はごく少数であった。

表 4. PC/スマートデバイス各習熟度割合 (N=80)

	PC	スマホ
レベル 1 (初心者)	1.3%	3.8%
レベル 2	46.3%	3.8%
レベル 3	37.5%	67.5%
レベル 4 (非常に習熟)	15.0%	25.0%

4.2.2 セキュリティ知識

全 9 問の正答率を表に示す。全設問の平均正答率が 84.4%, 平均得点が 7.6 (9 点満点) であり、図 3 の分布からもセキュリティ知識レベルの高い回答者が比較的多かったといえる。

表 5. セキュリティ全般知識の設問と正答状況

	正解率(%) (N=80)
問 1	76.3
問 2	85.0
問 3	93.8
問 4	60.0
問 5	83.8
問 6	93.8
問 7	97.5
問 8	93.8
問 9	76.3
全平均	84.4

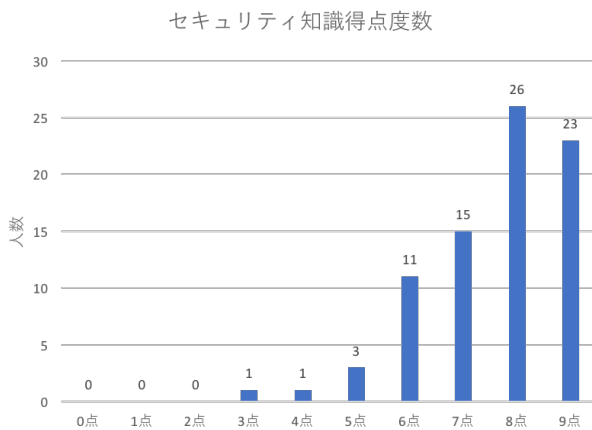


図 3. セキュリティ知識得点分布
 (N=80, Ave.=7.6, SD=1.31)

4.2.3 批判的思考態度尺度

批判的思考態度尺度の「論理的思考」、「探究心」、「客観性」、「証拠重視」の各因子の得点平均と標準偏差を表 6 に示す。なお、平山ら[15]の大学生 426 名の 4 因子 33 項目の平均値は、論理的思考 37.1, 探究心 37.9, 客観性 23.9, 証拠重視 10.3 であった。

表 6. 批判的思考態度尺度因子平均と標準偏差
 (N=80, 5 件法)

	平均	標準偏差	平均/項目
論理的思考(13 項目)	38.83	7.91	2.98
探究心(10 項目)	37.14	6.14	3.71
客観性(7 項目)	24.91	3.74	3.56
証拠重視(3 項目)	11.31	2.15	3.77
全因子	112.2	15.18	3.40

4.2.4 認知的熟慮性-衝動性尺度

認知的熟慮性-衝動性尺度の平均値を表 7 に示す。

表 7. 認知的熟慮性-衝動性尺度得点平均と標準偏差
 (N=80, 4 件法)

	平均	標準偏差	平均/項目
熟慮性 (10 項目)	27.38	4.65	2.74

4.2.5 認知欲求尺度

認知欲求尺度の平均値を表 8 に示す。

表 8. 認知欲求尺度得点平均と標準偏差
 (7 件法, N=80)

	平均	標準偏差	平均/項目
認知欲求 (10 項目)	57.38	13.43	3.83

4.2.6 認知的構造欲求尺度

認知的構造欲求尺度の平均値を表 9 に示す。

表 9. 認知的構造欲求尺度得点平均と標準偏差
 (6 件法, N=80)

	平均	標準偏差	平均/項目
認知的構造欲求 (10 項目)	31.84	6.14	3.18

4.3 サイト真偽判断実験結果の分析

4.3.1 サイト真偽判断得点別の分析

サイト真偽判断得点により下位群 (5 点以下, 26 名), 中位群 (6 点, 28 名), 上位群 (7 点以上, 26 名) の 3 群に分け, 質問紙調査の各設問の平均値を比較した。その結果, スマートデバイス習熟度($F(2,77)=3.57(p<.05), \eta^2=.09$)について, 上位に行くほど, それぞれの習熟度レベルが高くなる傾向があることを確認した。

4.3.2 サイト真偽判断設問別の分析

サイト真偽判断の全 8 問について正解群, 不正解群に分け, 質問紙調査の各設問の平均値を比較した。その結果, 問 2 の批判的思考-客観性因子($t(78)=3.14 (p<.01), d=0.75$)と批判的思考-証拠因子($t(78)=2.09(p<.05), d=0.5$)について, 問 7 のスマートデバイス習熟度($t(78)=2.09(p<.05), d=0.51$)について, 正解群の得点, レベルのほうが高くなる傾向があることを確認した。

図 4 に問 2 のサイト画像を示す。この設問で, 正規サイトに該当する回答を選択し, 不正解となった回答者の選択理由を分析した結果, 「Facebook の”F”のマークがあるから」, 「見たことのある画面だから」, 「よく見るマーク/画面に似ているから」と自分自身が過去に見た経験に基づき判断が下されている可能性が高いことがわかった。一方, 偽サイ

トに該当する回答を選択し、正解となった回答者の選択理由を分析した結果、大半の理由は、「英語でよくわからないから」、「説明文が少なくよくわからないから」と決めてとなる根拠がないことであった。このことから、正解となった回答者群は判断を下すために証拠を重視し、さらにできるだけ多くの証拠を必要とすることが推測できる。批判的思考態度尺度の客観性因子に属する「物事を見るときに自分の立場からしか見ない(逆転項目)」、「一つ二つの立場だけではなく、できるだけ多くの立場から考えようとする」という設問、証拠因子に属する「結論を下す場合には確たる証拠の有無にこだわる」という設問と、正解群、不正解群の判断理由がある程度一致しており、これが批判的思考態度尺度の設問の回答結果に反映されていると考えられる。



図 4. サイト真偽判断実験問 2 のサイト画面

4.4 質問紙調査項目の分析

質問紙調査項目のうち、PC 習熟度レベル、スマートデバイス習熟度レベルは、レベル低群(レベル 1,2)とレベル高群(レベル 3,4)の 2 群に、それ以外の項目は 3 群に分け、T 検定および分散分析を実施した。その結果、どの項目についても有意傾向が見られなかった。

4.5 全設問間の関係性の分析

サイト判断実験の得点、PC 習熟度レベル、スマートデバイス習熟度レベル、セキュリティ知識得点、認知欲求尺度、認知的構造欲求、批判的思考態度の論理的・探究心・客観性・証拠の 4 因子、熟慮性-衝動性尺度それぞれの得点の各指標間の相関係数を算出した。その結果、サイト真偽判断得点に対しては、PC 習熟度レベル、スマートデバイス習熟度のみ正の相関が見られた。

5. まとめと今後の課題

本稿では、ユーザ自身のフィッシング回避行動につながる「リスクに対する感度」に貢献する要素を明らかにするために、サイトの真偽判断実験と認知判断傾向に関する心理特性測定尺度である、批判的思考態度尺度、認知的熟慮性-衝動性尺度、認知欲求尺度、認知的構造欲求尺度の 4 つの尺度を用いた質問紙調査を実施し、その結果により、サイト真偽判断行動とユーザの思考特性との関係性を検討した。その結果、サイト真偽判断実験総合得点群別の各調査項目の平均得点比較から、得点が上位になるほど、スマートデバイスの習熟度レベルが高い傾向にあることが確認できた。また、サイト真偽判断実験結果と各調査項目との関係性の分析から、サイト真偽判断には、PC 習熟度レベル、スマートデバイス習熟度レベルが関係していることが確認できた。加えて、サイト真偽判断実験の設問別の正解・不正解 2 群の各調査項目の平均得点比較から、一部の設問について、批判的思考態度の客観性因子、証拠因子の得点が、正解群のほうが高い傾向を示すことが確認できた。

サイト真偽判断実験の各設問の判断結果を検討したところ、一部の理由の記述に「外国語のサイトを使いたくないから」、「個人情報をネットに上げたくないから」、「利用する価値を感じないから」といった自身の価値基準により真偽の判断を下していた回答者がいることがわかった。また、実験の全てのサイトが日本語以外の言語であり、「かいてある言葉がわからない」、「英語が読めない」といった言語の問題により実験者側が測定したい行動がとられておらず、使用するサイト、回答の引き出し方に問題があることがわかった。今回の実験では、サイトの真偽判断と、重要情報の入力・送信のフェーズが混在していたため、今後は、2 つのフェーズを分割した実験設計をする必要がある。

また、今回使用した思考に関する心理特性以外にも、例えばリスクテイキング尺度のような「リスクに対する感度」を測定するのに有用な尺度がある可能性があり、本稿で使用した尺度の関係性をより適切な実験で再確認することと合わせて、他の尺度の利用も検討する必要がある。

謝辞 本研究は JSPS 科研費 16K01025 の助成を受けたものである。また、本稿の実験および質問紙調査データの収集に際し、高橋啓伸氏、藤根麻羽氏、八藤後茉央氏にご協力・ご尽力いただきました。心より感謝申し上げます。

参考文献

- [1] フィッシング対策協議会：レポート2016の掲載～世界に広がるフィッシング対策の輪～（オンライン），入手先<https://www.antiphishing.jp/report/pdf/phishing_report_2016.pdf>，(accessed 2017.6.13)
- [2] 警察庁：平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について（オンライン），入手先<https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf>，(accessed 2017.6.13)
- [3] Khonji, M. Iraqi, Y. and Jones, A., Phishing Detection: A Literature Survey, IEEE Communications Surveys and Tutorials 15 (4), pp.2091-2121, 2013.
- [4] M.E. Maurer, A. D. Luca, S. Kempe: Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness, In Proc. of the Seventh Symposium on Usable Privacy and Security, pp.1-13, 2011.
- [5] 山田恭平, 小倉加奈代, ビスタ・B・ベッド, 高田豊雄, スマートフォンの画面サイズによる制約を考慮したセキュリティ意識向上のための警告ダイアログの検討, 情報処理学会研究報告ヒューマンコンピュータインタラクション(HCI), 2017-HCI-172, no.21, pp.1-8, 2017.
- [6] 楠見孝, 三浦麻子, 小倉加奈代. 食品放射能リスク認知に及ぼす批判的思考態度と高次リテラシー：震災後の市民パネル調査データによる検討(2), 日本社会心理学会第53回大会発表論文集, p.372, 2012.
- [7] 楠見孝, 平山るみ. 食品リスク認知を支えるリスクリテラシーの構造-批判的思考と科学リテラシーに基づく検討-, 日本リスク研究学会誌 23(3), pp.165-172, 2013.
- [8] 鈴木護：恐怖喚起アピールの視点による振り込め詐欺の被害過程及び被害防止対策に関する研究，2009年度～2010年度科学研究費補助金若手研究(B)研究成果報告書（2012），（オンライン）入手先<<https://kaken.nii.ac.jp/ja/file/KAKENHI-PROJECT-21730510/21730510seika.pdf>>(accessed 2017.6.13)
- [9] 高橋啓伸, 小倉加奈代, Bhed Bahadur Bista, 高田豊雄, 画像局所特徴量を利用したフィッシングサイト検出手法の実装と評価, コンピュータセキュリティシンポジウム2016 (CSS2016) 論文集, 3B4-3, 2016.
- [10] 藤根麻羽, 小倉加奈代, 高田豊雄, バハドゥール ベッド. 人間の脆弱性を利用した標的型攻撃への防御手法の検討, 情報処理学会第79回全国大会論文集, 5W-04, 2017.
- [11] 八藤後菜央, 高田豊雄, バハドゥール ベッド, 小倉加奈代. 人間の脆弱性を利用した標的型攻撃への防御手法の検討, 情報処理学会第79回全国大会論文集, 5W-05, 2017.
- [12] 独立行政法人情報処理推進機構：2015年度情報セキュリティの脅威に対する意識調査，入手先<<https://www.ipa.go.jp/files/000050002.pdf>>（参照 2016-12-23）
- [13] トレンドマイクロ：ネット詐欺の手口と対処法をクイズで確認，入手先<http://www.is702.jp/special/1725/partner/12_t/>（参照 2016-12-23）
- [14] トレンドマイクロ：セキュリティの常識をクイズでチェック！，入手先<http://www.is702.jp/special/1902/partner/12_t/>（参照 2016-12-23）
- [15] 平山るみ, 楠見孝. 批判的思考態度が結論導出プロセスに及ぼす影響, 教育心理学研究, 52, pp.186-198, 2004.
- [16] 滝間一嘉, 坂元章. 認知的熟慮性-衝動性尺度の作成-信頼性と妥当性の検討, 日本グループダイナミクス学会第39回大会論文集, pp.39-40, 1991.
- [17] 神山貴弥, 藤原武弘：認知欲求尺度に関する基礎的研究, 社会心理学研究, 6(3), pp.184-192, 1991.
- [18] 鈴木公基, 認知的構造欲求尺度の試み, 筑波大学心理学研究, 第21号, pp.135-149, 1999.