Vol.2017-GN-102 No.8
Vol.2017-SPT-23 No.8
2017/5/12

ユーザのフィッシングサイト回避能力と心理特性との関係性の検討

小倉加奈代[†1]

概要：フィッシング被害の現状を見ると，現状の技術では，犯罪者が編み出す新しい手口に対応することが難しいことから，技術のみでの防止対策には限界があると考えられる．従来の自動検知をはじめとした技術に加え，ユーザ自身によるフィッシングサイト検知能力を高めることで，新しい手口に対する検知精度も向上し，フィッシング犯罪を防止できる可能性が高まることが期待できる．また，フィッシングサイトか否かの判断と同様の行動である安全性やリスク認知に関して，批判的思考態度が大きく影響することが食品リスクや放射線リスクを対象とした調査から明らかとなっている．そこで本研究では，ユーザ自身によるフィッシングサイト検知能力向上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回避能力とユーザの心理特性として，批判的思考態度尺度，認知的熟慮性-衝動性尺度の 2 つの尺度を用いた調査を実施し，その結果により，フィッシングサイト回避能力とユーザの心理特性との関係性を検討する．

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

An Examination of the Relation between Phishing Threat Avoidance Behavior and Psychological Traits of Users

KANAYO OGURA[†1]

Abstract: In this paper, I conduct a questionnaire survey among about 50 university students to investigate the factors and function of phishing threat avoidance behavior in relation to critical thinking attitude and reflective cognitive attitude. Other researchers proved that critical thinking attitude affected scientific literacy and knowledge of food-related risk and radioactivity risk. I deduce from this fact that critical thinking attitude also affect security-related risk as web pages and mails authenticity verification. On basis of the gathered data, I examine the relation between knowledge and avoidance behavior of phishing and psychological factors.

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

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，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搾取する犯罪である．この犯罪を防止するためには，ユーザが偽メールであることに気づくか，誘導された先が偽サイトであることに気づく必要がある．フィッシング犯罪を防止するために，偽メール・偽サイト検知技術開発研究，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的研究が盛んに行われている．偽メール・偽サイト検知研究では，機械学習，視覚的類似性，ブラックリストを用いた自動検知技術開発研究が数多く行われている[1]．加えて，市販のウイルス対策ソフトの一機能として偽メール・偽サイト判定機能をもつソフトが多く存在する．しかし，攻撃者側は，利用している手口がフィッシングとして認知されると，例えば，メールの内容を旬である出来事を盛り込んだ内容に書き換えることでメールの信憑性を高めるというように犯罪手口の精錬を行う．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，「いたちごっこ」の関係から抜け出せないのが現状である．犯罪事例を用いた教育的研究については，成果として IPA 等セキュリティ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，犯罪手口を変えているため，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．

本研究では，従来の検知技術だけに頼るのではなく，ユーザの心理特性や行動特性を考慮した偽メール・偽サイトに気づきやすくするための注意喚起を主とした検知支援を行い，技術とユーザ自身の能力の両面からのフィッシング犯罪防止を最終目標と設定する．本稿では，第一段階として，ユーザ自身によるフィッシングサイト検知能力向上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回避能力とユーザの心理特性として，批判的思考態度尺度，認知的熟慮性-衝動性尺度の 2 つの尺度を用いた調査を実施し，その結果により，フィッシングサイト回避能力とユーザの心理特性との関係性を検討する．

2. 関連研究

批判的思考(critical thinking)とは，雑多な情報の中から適切な情報を選択し，正しい答えを導きだすために，物事を客観的に捉え，多面的・多角的に検討する思考のことであ

†1 岩手県立大学
Iwate Prefectural University

る．また，批判的思考は，私たちの日常生活において，テレビを視聴し，書籍やインターネットから情報を集め，決定する際などに働いており，日常生活に必要なコミュニケーション能力を支えている．日常生活だけではなく学業，職業など幅広い場面で働く汎用的スキルである[2]．また，批判的思考プロセスを振り返りコントロールし，実行するかを決定することを支えているのが，批判的に考えようとする批判的思考態度である．楠見ら[3]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たことが明らかとなった．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，フィッシング回避行動に批判的思考態度が影響する可能性がある．

また，フィッシング被害に遭う場合，フィッシングメール内の URL をクリックする，フィッシングサイトのフォームに重要情報を入力，送信するといった行動を起こすことになる．この際に，じっくり考えて慎重であるか，早急に結論を下すか，人により判断を下すまでのプロセスである認知的熟慮性-衝動性[4]に違いがあると考えられる．実際，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考えられており[5]，フィッシング回避にも熟慮的認知スタイルが関係する可能性がある．

3. 調査方法

3.1 調査対象と手続き

岩手県立大学 1 年生全学部（看護学部，総合政策学部，社会福祉学部，ソフトウェア情報学部）対象の必修科目である情報リテラシー受講者 55 名（男性 32 名，女性 23 名）が対象である．なお，回答に欠損のあった 4 名は後の分析より除外した．

講義中に質問紙を配布し，調査を実施した．回答時間は，約 15 分であった．回答後，質問紙を回収した．調査実施期間は 2015 年 7 月中旬であった．

3.2 質問項目

以下 6 つについて質問表を作成した．詳細は次項より説明する．

(1) PC/スマートデバイスの習熟度レベル
(2) セキュリティ全般の知識レベル
(3) フィッシング対策に関する知識レベル
(4) 実在メールの真偽判定
(5) 批判的思考態度尺度
(6) 認知的熟慮性-衝動性尺度

3.2.1 PC/スマートデバイス習熟度

IPA が実施した 2013 年度情報セキュリティの脅威に対する意識調査[6]の PC 習熟度及びスマートデバイス習熟度の設問を利用した．PC 習熟度レベルの測定は，表 1 に示す 10 項目について「できる」ものにチェックすることを求め，チェック数によりレベル 1 からレベル 4 までの 4 段階にレベル分けする．スマートデバイス習熟度は，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当てはまるものを 1 つ回答することを求めた．

表 1. PC 習熟度レベルに関する質問項目

電子メールの送受信やウェブサイトの閲覧ができる
電子メールの送受信の設定ができる
パソコンにデータを保存したり，保存したデータを開いたりできる
ソフトウェアをインストールして使うことができる
コントロールパネルを開いて設定を変更できる
パソコンをインターネットに接続する設定ができる
パソコンのログオフ，シャットダウン，休止状態，スタンバイ（スリープ）の違いがわかる
パソコンの周辺機器（プリンタなど）を接続し，動作させられる
パソコンのパーツ（ハードディスクやメモリなど）の交換ができる
CD や DVD，Blu-ray などの外部メディアにデータをバックアップできる

表 2. スマートフォン習熟度レベルに関する質問項目

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

3.2.2 セキュリティ全般の知識レベル

トレンドマイクロ社が提供する「セキュリティ常識力検定」[7]を利用した．この検定は，不正プログラム，Web サイト閲覧時，無線 LAN，スマートデバイスを対象とした幅広い常識的な知識レベルを測定するための 7 つの設問で構成されている（表 5 参照）． それぞれの設問に対し「○」，「×」のいずれかで回答を求めた．

3.2.3 フィッシング対策に関する知識レベル

トレンドマイクロ社が提供する，「あなたの「だまされレベル」チェック」[8]を利用した．これは，フィッシングサイトの真偽判定に関わる常識的な知識を問う設問であり，ブラウザの暗号化を示す鍵マークの確認，アドレス欄の確認，

Vol.2017-GN-102 No.8
Vol.2017-SPT-23 No.8
2017/5/12

Web サイトそのもののプロパティ情報の確認に関する 5 つの設問から構成されている．図 1 のようなブラウザの画像に対し，フィッシングサイトである可能性が「高い」，「低い」のいずれかで回答を求めた．

図 1. フィッシング対策知識に関する図例[8]

3.2.4 実在メールの真偽判定

受信したメールの真偽判定を模擬的に行うための設問である．設問は，著者が過去に受信した著名なサービスや金融機関に関係するフィッシングメール及び，誤送信された正規メールを利用し，5 つの設問を作成した．全ての設問のメール内には URL が含まれている．回答者には，設問メールが詐欺である可能性が「高い」，「低い」のいずれかの回答を求めた．さらに，設問内の URL をクリックしてみようと「思う」，「思わない」のいずれかの回答を求めた．

3.2.5 批判的思考態度尺度

平山ら[9]の批判的思考態度尺度 33 項目を利用した．この尺度は，「論理的思考への自覚」(13 項目)，「探究心」(10 項目)，「客観性」(7 項目)，「証拠の重視」(3 項目) の 4 因子から構成されている．それぞれの因子の設問例を表に示す．各項目について「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，因子ごとに合計得点を算出した．

表 3. 批判的思考態度尺度の質問項目抜粋

論理的思考への自覚
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
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
いつも偏りのない判断をしようとする
証拠の重視
結論をくだす場合には，確たる証拠の有無にこだわる

3.2.6 認知的熟慮性-衝動性尺度

滝聞ら[10]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.」のような判断する際の認知傾向に関する質問である．各項目について「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．なお，この尺度では，全項目の合計得点が高いほど熟慮性が高いと判断する．

4. 結果と考察

4.1 結果

3 章で説明した 6 つの質問表のそれぞれの回答結果について述べる．

4.1.1 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 4 に示す．PC は，レベル 2（基本操作は習熟），スマートデバイスはレベル 3（習熟）の割合が高い．

表 4. PC/スマートデバイス各習熟度の人数 (N=51)

	PC	スマホ
レベル 1（初心者）	13.7%	3.9%
レベル 2	43.1%	19.6%
レベル 3	29.4%	58.8%
レベル 4（非常に習熟）	13.7%	17.6%

4.1.2 セキュリティ全般の知識

設問内容とそれぞれの正答率を表 5 に示す．また，得点分布を図 2 に示す．表 5 より設問 3 と設問 6 の正答率がそれぞれ 29.4%，11.8%と正答率の低かった．なお，全問正解者は 2 名であった．

表 5. セキュリティ全般知識の設問と正答状況

各設問内容（本文に省略箇所あり）	正答率(N=51)
問題 1：セキュリティソフトの利用期限が過ぎると新種のウイルスが現れた時に PC の感染を防げなくなることがある．	92.2%
問題 2：Windows でセキュリティ対策をする時は，「Windows Update」の機能を使ってアップデートを行うが，PC の全ソフトはこの機能でアップデートできる．	82.4%
問題 3：ショッピングサイトを開いた時，鍵マークが表示された．これは，このサイトが信頼できる事業者によって運営されていることを証明するものである．	29.4%
問題 4：最新情報を調べる時，検索サイトにキーワードを入力して検索し，検索結果上位にあるサイトをむやみにクリックするのは避けるべきである．	64.7%
問題 5：パスワードには，幾つかの英単語を組み合わせた文字列を設定すれば安全だ．	92.2%
問題 6:無線 LAN と PC 端末を無線で接続する時は，通信を盗聴されないように「WEP」という方式で暗号化すべき．	11.8%
問題 7：スマートフォンもウイルスに感染する危険性がある．	100%

Vol.2017-GN-102 No.8
Vol.2017-SPT-23 No.8
2017/5/12

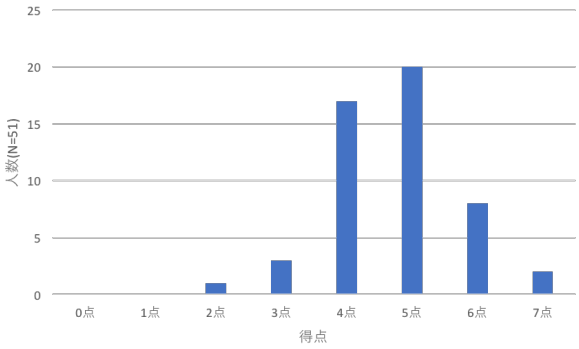

図 2. セキュリティ知識設問得点分布 (Ave.=4.73, SD=0.99)

4.1.3 フィッシングに関わる知識レベル

設問の内容概略とそれぞれの正答率を表 6 に示す. また, 総得点の分布を図 3 に示す. 28 名(54.9%)が全問正解であった.

表 6. フィッシングに関わる設問正答率

各設問内容（ポイント）	正答率(N=51)
問題 1：鍵マーク	86.3%
問題 2：鍵マーク	72.5%
問題 3：URL	92.2%
問題 4：URL	68.6%
問題 5：プロパティ	88.2%

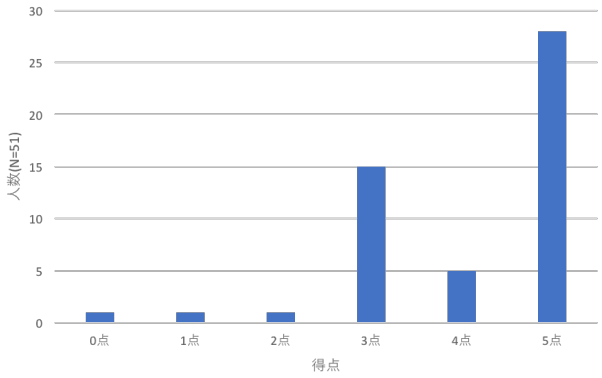

図 3. フィッシングレベル得点分布(Ave.=4.08, SD=1.19)

4.1.4 実在メールの真偽判定

設問の内容概略とそれぞれの正答率を表 7 に示す. また, 得点分布を図 4 に示す. 表 7 より設問 3,4 の正規メールに対する正答率が 41.8%, 29.1%と低めであった. これらは現実的に誤答したとしても実害はほぼないが, 設問 1,2,5 のフィッシングメールに対する正答率も 65.5%, 76.4%, 81.8%と中程度であった. なお, 全問正解者は 5 名であった.

表 7. メールの真偽設問正答率

各設問内容（ポイント）	正答率(N=51)
問題 1：フィッシング	65.5%
問題 2：フィッシング	76.4%
問題 3：正規（誤送信）	41.8%
問題 4：正規（誤送信）	29.1%
問題 5：フィッシング	81.8%

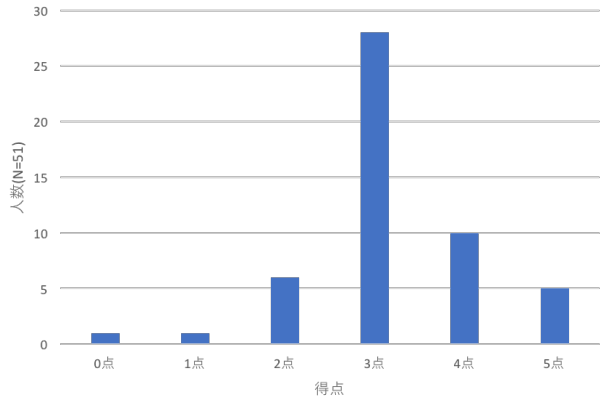

図 4. メール真偽設問の得点分布(Ave.=3.18, SD=0.96)

また, この設問では, メール内にある URL をクリックしてみようと「思う」,「思わない」についても回答を求めた. 結果を表 8 に示す. クリックしようと「思う」を選んだ回答者の多くは, メールそのものを正規メールと判定した上でクリックしようと思うと回答していたが, 設問 1, 設問 2 でそれぞれ 1 名ずつメールを詐欺メールであると判定しているにもかかわらずクリックしようと思うと回答していた.

表 8. URL をクリックしようと思う割合

各設問内容	クリック(%)	詐欺+クリック
問題 1:フィッシング	11.8%	2.0%（1 名）
問題 2:フィッシング	15.7%	2.0%（1 名）
問題 3:正規(誤送信)	35.3%	0
問題 4:正規(誤送信)	17.6%	0
問題 5:フィッシング	5.9%	0

4.1.5 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 4 つの因子ごとの得点の平均と標準偏差を表 9 に示す. 平山ら[9]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. この結果と比較すると, 本稿の回答者群は, 探究心が低く, 客観性が高いことがわかる.

表 9.　批判的思考態度尺度 4 因子平均と標準偏差(5 件法)

	平均	標準偏差	平均/項目
論理的思考(13 項目)	37.98	7.97	2.92
探究心(10 項目)	34.25	6.64	3.43
客観性(7 項目)	25.29	3.74	3.61
証拠重視(3 項目)	10.63	1.45	3.54

4.1.6　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 10 に示す.

表 10. 認知的熟慮性-衝動性尺度の平均と標準偏差(4 件法)

	平均	標準偏差	平均/項目
熟慮性(10 項目)	27.24	4.50	2.72

4.2　考察

本節では，フィッシング回避に直接的に関係するセキュリティ知識レベル，フィッシング知識レベル，メールの真偽判定と心理特性として取り上げた批判的思考態度，認知的熟慮性との関係について考察する.

4.2.1　批判的思考態度，認知的熟慮性-衝動性との関係性の検討

PC 習熟度, スマートデバイス習熟度, セキュリティ知識, フィッシング知識，メール真偽判定，クリック行動，危険性がある場合のクリック行動，批判的思考態度の 4 因子，認知的熟慮性-衝動性の各指標間の相関係数を算出した（表 11）. その結果, PC 習熟度と認知的熟慮性の間に負の相関，セキュリティ知識と批判的思考態度尺度の論理的思考，客観性の間に負の相関，フィッシング知識と論理的思考，客観性，認知的熟慮性の間に正の相関，危険だと思う場合のクリック行動と熟慮性の間に負の相関が見られた.

4.2.2　熟慮群，衝動群間の差異の検討

2 章で説明したように，認知的熟慮性-衝動性尺度は，尺度得点が高いほど熟慮性が高く，尺度得点が低いほど，衝動性が高いこととなる．ここで，尺度得点の中央値 28 を基準として，回答者を熟慮群（29 点以上，19 名），中位群（28 点，7 名），衝動群（27 点以下，25 名）の 3 群に振り分けた．さらに，3 群ごとにセキュリティ知識，フィッシング知識，メール真偽判定，クリック行動，危険判断時クリック行動の平均得点を図 5 に示す．なお，それぞれの設問の得点平均について分散分析を行った結果，全てについて有意傾向が見られた(p<.05)．各設問のうち，特にクリック行動，危険時のクリック行動について，衝動群の得点が他の群よりも高く，衝動性が高い場合，クリック行動を取りやすい可能性がある.

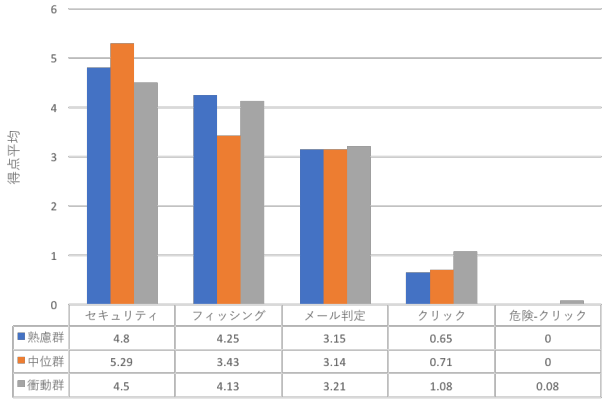

図 5. セキュリティ知識等の各群別の平均得点

5.　まとめ

本稿では，ユーザ自身によるフィッシングサイト検知能力向上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回避能力とユーザの心理特性として，批判的思考態度尺度，認知的熟慮性-衝動性尺度の 2 つの尺度を用いた調査を実施し，その結果について検討した．その結果，セキュリティ全般の常識的な知識と批判的思考態度のうちの論理的思考，客観席と負の相関，フィッシング対策に関わる知識と論理的思考，客観性，認知的熟慮性と正の相関が見られた．このことから，批判的思考態度が，フィッシング回避の知識と関わることが示唆された．また，フィッシング回避に関係する行動と心理的特性として，熟慮性の高いユーザと比較して，衝動性の高いユーザがメールやサイトの真偽にかかわらずクリック行動を取りやすい可能性が示された.

今後は，さらに多くの調査結果をもとに分析を進めるとともに，今回の調査とは異なる年代のユーザを対象とした調査を実施する予定である．さらに，すでに実施済みであるソーシャルエンジニアリングに関わるシナリオを取り入

表 11. フィッシング回避に関わる能力と心理特性に関する指標間の相関係数(N=51) (*:p<.05, **:p<.01)

	PC	スマホ	セキュリティ知識	フィッシング知識	メール真偽	クリック嗜好	危険-クリック嗜好	論理的思考	探究心	客観性	証拠重視
PC											
スマホ	.554**										
セキュリティ知識	.001	-.175									
フィッシング知識	-.106	-.014	-.299*								
メール真偽	-.294*	-.173	-.134	.211							
クリック嗜好	.201	.33*	-.41**	.076	.006						
危険-クリック嗜好	.242	.168	.056	-.013	-.037	.168					
論理的思考	.178	.273	-.303*	.392**	-.13	.208	-.014				
探究心	.091	-.007	-.236	.261	.137	.088	-.008	.262			
客観性	-.029	.025	-.29*	.313*	.121	.171	-.232	.42**	.636**		
証拠重視	.079	.142	-.084	.142	.257	-.046	-.018	.373**	.16	.081	
熟慮性	-.456**	-.132	-.043	.28*	.14	-.275	-.348*	.165	-.054	.21	-.014

れた調査[11]の結果と組み合わせた分析・考察を行う予定である．

謝辞 本研究はJSPS科研費16K01025の助成を受けたものである．

参考文献

[1] Khonji, M. Iraqi, Y. and Jones, A., Phishing Detection: A Literature Survey, IEEE Communications Surveys and Tutorials 15 (4), pp.2091-2121, 2013.
[2] 楠見孝. 良き市民のための批判的思考（特集 批判的思考と心理学），心理学ワールド(61), pp.5-8, 2013.
[3] 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.
[4] 滝聞一嘉．認知的熟慮性−衝動性が他者の判断への接触傾向に及ぼす効果，日本グループダイナミクス学会第38回大会発表論文集，pp.81-82, 1990.
[5] 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.
[6] 情報処理推進機構, 2013年度情報セキュリティの脅威に対する意識調査, http://www.ipa.go.jp/files/000035983.pdf（最終閲覧日 2017/4/4）
[7] トレンドマイクロ, インターネットセキュリティナレッジ「セキュリティ常識力検定　7つの問題で学ぶ，ネットの安全対策」，http://www.is702.jp/special/982/partner/12_t/（最終閲覧日 2017/4/4）
[8] トレンドマイクロ，あなたの「だまさレベル」チェック，https://www.is702.jp/special/phishing/00001/index.html（最終閲覧日 2017/4/4）
[9] 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.
[10] 滝聞一嘉，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.
[11] 八藤後茉央，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.