様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２６ 日現在

機関番号：３２７２１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ０５０１３

研究課題名（和文）ヒューマンエラーに対するアプローチのフィッシング詐欺被害防止教育への応用

研究課題名（英文）Application of the human error approach to phishing fraud prevention education

研究代表者
稲葉　緑（Inaba, Midori）

情報セキュリティ大学院大学・その他の研究科・准教授

研究者番号：８０４１９０９３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究は第一に、フィッシングメールが正しく判別される際の、メールに関する初期の気づきが獲得されるメカニズムを調べた。フィッシングメールへの気づきにはメタ認知スキルが、詐欺メールの中でも判別の難易度が高いとされる標的型攻撃メールには証拠に基づく客観的な思考傾向が貢献することを明らかにした。
また、初期の気づきに関する重要性等の説明を加えた提案形式のプログラムを試作し、これが標的型攻撃メールに対する誤った反応を抑制する効果を評価した。従来形式の教育プログラムと比較した結果、従来形式よりは効果が確認されたものの、十分に効果があると言える程度には達しなかった。

研究成果の学術的意義や社会的意義
初期の気づきがフィッシングメールへの判別を左右するとの報告がある一方、この気づきについての知見はほとんどみられていない。本研究ではこの気づきに影響する要因を示し、気づきのメカニズムを明らかにすることに貢献した。
また、標的型攻撃メールへの反応を防ぐための従来形式の教育プログラムについては以前からその効果の小ささが報告されており、今回もそれを支持する結果が確認した。しかし、提案形式のプログラムにも十分な効果は確認できなかった。ただし研究成果を総合的にみることで、教育プログラムをどのように改善すべきかの具体的方向性を把握することができた。

研究成果の概要（英文）：The study first investigated the mechanisms by which individuals can acquire intuitions when correctly identifying phishing emails. Metacognitive skills were found to contribute to the intuitions about phishing emails. Moreover, the evidence-based objective reasoning tendency was found to contribute to intuitions about targeted attack emails and the correct identification of these emails.
In addition, this study developed the proposed educational program that focused on explaining the importance of acquiring the intuitions to prevent individuals from responding to the targeted attack emails. The experiment was conducted to compare its effectiveness with the conventional educational program. As a result, the proposed program was appeared to be more effective than the conventional program, but not to the extent that it could be said to be sufficiently effective.

研究分野：実験社会心理学

キーワード：フィッシングメール　標的型攻撃訓練　教育　メタ認知スキル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

年々増加するフィッシング詐欺による被害の改善を目指し、研究業界では当該被害を防ぐための教育プログラムが検証されてきた。その一つが、フィッシングメールが不正を目的としたメールであると判別する力を高めるものである。しかし、これらのプログラムは実験内でのメールの真偽性を判断するテストの成績を向上させても、実際のメールコミュニケーション場面での適切な判断を促す効果は確認されていない。

本研究は、フィッシングメールの中でも精巧に作成されたものに対して不正なメールであると気づくメカニズムを明らかにすることを目的とした。また、この気づきに関するスキルの向上に効果的な教育プログラムを示すことを目指した。

２．研究の目的

フィッシングメールを不正なメールであると気づくためには、客観的事実、および、正規のメールが有する特徴との不一致を認識する必要がある。この不一致への認識を本研究では「初期認識」と呼ぶ。この初期認識を促進する要因を明らかにし、また、初期認識獲得に有効な教育プログラムを示すことを目的とした。

この研究は3つの研究工程から構成される。以降、研究工程ごとに記述する。

(1) 本研究では不一致への初期認識の中でも「独自認識」に焦点を当てた。独自認識とは、メールの受信者自身に独特の事実との不一致への初期認識である。例えば、ユーザ自身の過去および今の状況との比較，あるいは，自身が所属する組織の既定等との比較によって生じる不一致への初期認識である。特に精巧に作成されたフィッシングメールの判別成功に独自認識が寄与する事例について報告されている。しかし、この独自認識の獲得を難しくする要因についての研究は多く存在する一方、何によって促進されるのかについての研究はみられない。これを明らかにすることを(1)の目的とした。

(2) (2)からフィッシングメールの中の1種である標的型攻撃におけるメール（以降「標的型攻撃メール」という）に、さらに対象を絞り込むこととした。標的型攻撃は情報資産等の盗難等を目的とした組織を対象としたサイバー攻撃の1つである。組織の従業員が標的型攻撃メールを不正なメールと気づけずに正規のメールとして反応することで、標的型攻撃の進捗が可能になる。フィッシングメール同様、標的型攻撃メールの適切な判別にも初期認識が寄与すると予測されたが、このメカニズムについては明らかにされていない。これを明らかにすることを(2)の目的とした。

ただし、この目的には多数のデータが必要であり、標的型攻撃メールを実際に受信し、さらに正しく判別したことを自身で知る参加者のデータを多数収集することは困難であると予測された。そこで、多くの組織が実施している標的型攻撃訓練メール（標的型攻撃メールを模した訓練用メールを配信する訓練）に着目し、この訓練用メールを受信したことがある個人を対象とした調査を実施した。

(3) 実際的なコミュニケーション場面における標的型攻撃メールへの反応を抑制することに有効な教育プログラムは示されていない。本研究では、先行研究や既存の資料などに基づく従来形式のプログラムの効果を改善するものとして、初期認識、特に独自認識の重要性やその認識の持ち方についての解説を追加した提案形式のプログラムを試作した。そのうえで、標的型攻撃メール訓練を含む実験を実施し、提案形式のプログラムが従来形式のプログラムよりも、訓練用メールへの反応を抑制する効果が高いとの仮説を評価した。また、(2)で収集した初期認識に寄与する要因についてのデータも本実験の参加者から収集し、訓練用メールへの反応についての考察を展開した。

３．研究の方法

全ての研究は人を対象とした調査・実験に関する日本心理学会等の倫理規程に従って計画され、本研究者の所属機関における倫理委員会の承認を得た上で実施された.

(1) 450人を対象としたWebアンケート調査を実施した。調査参加者には過去にフィッシングメールを判別したときのことを想起するよう依頼し，判別のきっかけになった各種の初期認識について聞いた。そのほか、初期認識に影響し得ると予測された要因を評価するための質問への回答を依頼した。このような回答データを使用し、各種の初期認識をきっかけにフィッシングメールを判別した経験の有無を目的変数とするロジスティック回帰分析を実施することで、各初期認識を促進する要因を明らかにすることとした。

(2) 標的型攻撃メール訓練を実施する企業に所属し、訓練用メールを受け取ったことがある1065 人を対象とした Web アンケート調査を実施した。このうち 715 人は訓練用メールを不正なメールあるいは訓練用メールとの判別に成功した個人であった。残りの 350 人は、訓練用メールの判別に失敗した経験を持つ個人であった。調査では、訓練用メールを判別成功および失敗したときのことを想起し、そのときの初期認識や、メールの特徴などについて尋ねた。また、この判

別や初期認識に影響し得る要因を評価するための質問にも回答してもらった。
(3) 企業に勤務する20代から50代までの社会人52人（予備実験12人、本実験40人）を対象とした実験を実施した。実験はZoomおよびメールを使って行った。実験は①メールによるアンケート回答、②Zoomにおける教育プログラム学習とテスト、③メールによるアンケート回答の3段階で実施した。①では参加者にメールを送り、そのメールにはアンケート調査に回答するためのファイルを添付した。このアンケート調査では、(2)で使用した質問等についての回答を依頼した。②では従来形式あるいは提案形式の教育プログラムを視聴・参加してもらった後、正規および不正のメール画面を表した刺激を判別するテストを受けてもらった。③のメールは標的型攻撃訓練メールに相当するものであった。②のZoomの際に説明したアンケート内容とは異なるアンケートを送り、また、メールアドレスは実験前に参加者に示した正規のメールアドレスおよび①のアドレスとは異なっていた。回答期限までにアンケートへの回答がない、あるいは、事前に伝えておいた別の方法で実験者や人材派遣会社に問合せがあった場合に、教育プログラムの標的型攻撃メールに対する反応を抑制する効果があるとみなした。

４．研究成果
(1) 本稿では、フィッシングメール判別に独自認識の１つ「知っている個人・社員や関係がある企業からのメールであったが，そのような内容のメールが自分に届くことは無いと思った」がきっかけとなった経験がある個人と、無い個人とを比較した結果について示す。この独自認識は、先行研究からフィッシングメールの判別成功に寄与するものとして抽出されたものである。分析結果は、この独自認識をきっかけとして判別した個人ほど、フィッシングメールについての学習経験を持ち、コントロールスキルが高いことを示した（表１の上矢印)。様々なフィッシング対策向けの教材や解説の中で，自身との関連性についてよく考えるよう推奨されていることが独自認識を促しているのかもしれない．また，フィッシング詐欺について知ることで，フィッシングメールへの意識が全体的に高まったことが寄与している可能性もある．
　一方のコントロールスキルとは、メタ認知のうちの１つの構成スキルである。メタ認知とは、我々が学習したり判断したりするときに情報を理解したり、自分自身について振り返って考えたり、これらの思考をコントロールする能力のことを指す。本研究では事前の分析により、メタ認知のコントロールスキルを、自身の現在の状況を認識したり過去と照らし合わせたりするスキルと定義した。本研究が焦点を当てた独自認識を持つためには，自身に関する現在や過去を想起したり考えたりする活動を要すると想定していた。このような独自認識に上述したコントロールスキルが有効であることは妥当であると考えられる。
(2) 本稿では分析結果２つを示す。１つ目は、訓練用メールの判別に独自認識の１つ「本文や件名に書かれていた内容に心当たりがなかった」が寄与した経験の有無による個人の違いを明らかにした分析の結果である。この独自認識をもって訓練用メールを判別した参加者には、「証拠に基づく客観的な思考傾向」という特性が高い特徴がみられた。また２つ目の結果は、訓練用メールの判別に失敗したことが無い個人と、失敗したことがある個人とを分ける要因についての分析結果である（表 2)。判別に成功している個人は、証拠に基づく客観的な思考傾向が高く、また、訓練用ではない実際の標的型攻撃メールを受け取った経験を持つという特徴がみられた。
　いずれでも確認された証拠に基づく客観的な思考傾向は、批判的思考の一側面である。批判的思考は、自分の考えているプロセスを意識的に見つめ、目的に照らし合わせて判断や行動を決める思考傾向とされる[1]。独自認識や判別成功を促進した当該要因は、判断しようとしていることが自身の思考や感覚だけでなく客観的な根拠に照らし合わせて妥当であるかという点に意識を向けやすいとされる傾向である。ただし、この思考傾向が、メールに含まれる不一致への初期認識のうち独自認識以外、例えばメールアドレスが正規のものではないといった不一致への初期認識に貢献するとの結果は得られていない。ここから１つの可能性として、この思考傾向はメール処理時に、自身に関する現在や過去についてのエピソード等の詳細な記憶に依拠することが多い可能性を考える。ただし、日常的な記憶力は判別に顕著に寄与していないことが示されたため（表 2)、能力というよりも意識の向けやすさにおける違いであると解釈できる。
　また、１点興味深い結果とみられるのが、「熟慮的思考傾向」が訓練用メールの判別失敗を助長する要因として抽出されたことである。熟慮性は情報を収集し、判断する際に分析的に、また、論理的に問題を解決することを好む傾向とされる[2]。先行研究では、メールの真偽性について熟考すると迷い、真と判断しやすくなるとされる[3]。拙速な判断が望ましいとは思われないが、先行研究と合わせて考えても、単純に熟慮を求めることよりも初期の気づきを可能とすることが判別には有効である可能性が考えられる。
(3) 本稿では方法(3)③の訓練用メールへの反応を中心に記載する。予備実験で従来形式の教育プログラムを学習した参加者は全員、③のメールに回答期限までに反応した。すなわち判別失敗割合が 10 割であった。複数の先行研究で報告されている標的型攻撃メール訓練への判別失敗者の割合は 3 割程度に留まる。この差を踏まえて予備実験の方法を見直し、教育プログラムを更新

したほか、訓練用メールの判別に関する難易度を下げた。しかし本実験でも結果は変わらず、全員が判別に失敗した。ただし、提案形式の教育プログラムを学習した参加者も、判別成功者は 20 人中 2 名のみであった。

続いて、(2)で使用した質問項目への回答を分析したところ、提案形式で学習した判別に成功した 2 人の証拠に基づく客観的な思考傾向は、失敗した 18 人に比べて高かった（6 点満点で平均 5.5 vs. 3.4)。ただし、データ数の偏りにより統計的分析は行えていない。一方、従来形式で学習した参加者の中に当該思考傾向が高い個人は存在したが、これらの個人は訓練用メールの判別には失敗した。

提案形式による学習者の方が若干は訓練用メールの判別に成功した。しかしこの結果が、従来形式に比べて提案形式のプログラムの方が訓練用メールへの反応を抑制する効果が高いとの仮説を支持するものとまでは言えないと考える。本研究の結果の特徴として、先行研究に比べて訓練用メールへの判別失敗確率が極めて高いことが挙げられる。その理由として訓練用メールの判別の難易度が非常に高いものであったことがある。参加者は③のメールが届くものと待ち構えている状況で、本文上に表示される名前は以前と同じ差出人から訓練用メールを受け取った。このように見た目の相手やタイミングが合ってしまうと、内容に目を向けにくくなり、そのために自身が過去に聞いた内容との違いに気づくことも難しくなったと考えられる。実験終了後に判別に失敗した参加者から寄せられた感想でも、訓練用メールに対して全く違和感を持たなかったという声が聞かれ、学習プログラムの効果の限界が示された。

また、判別成功者が少ないため分析には至らなかったが、独自認識の獲得を促進し得る要因「証拠に基づく客観的な思考傾向」が訓練用メールへの反応の抑制にも貢献し得るとの示唆を得た。ただし、この思考傾向が高くても、従来形式のプログラムを学習した参加者は訓練メールに反応した。ここから、提案形式の教育プログラムは、当該思考傾向が高い個人が非常に難易度の高い標的型攻撃メールに反応しないことを促進することには効果がある可能性も考えられる。しかし、当初にこのような思考傾向を持たない個人が客観的な視点でメールを判別することを可能にするものではなく、この課題については引き続き検討する必要がある。

＜引用文献＞

[1] 平山＆楠見 (2004) 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, 186-198.

[2] 宮川ら (2010) 情報活用の実践力に対する熟慮・衝動的認知スタイルの影響, 日本教育工学論文誌, 34(Suppl.), 33-36.

[3] Wang et al. (2012) Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email, IEEE Transactions on Professional Communication, 55(4), 345-362.

表 1 (1)ロジスティック回帰分析結果

説明変数		回帰係数	標準誤差	*p* 値	オッズ比 (95%信頼区間) Exp(B)	下限	上限	影響
メタ認知	メタ認知的知識	0.154	0.07	0.02	1.17	1.02	1.33	↑
	コントロール	-0.05	0.08	0.515	0.95	0.81	1.11	
コミュニケーション	自己抑制	-0.02	0.05	0.71	0.98	0.90	1.07	
	曖昧さ耐性	0.03	0.07	0.62	1.03	0.91	1.18	
	暗示的	0.08	0.06	0.191	1.09	0.96	1.23	
ビッグファイブ	外向性	-0.02	0.05	0.653	0.98	0.88	1.08	
	協調性	-0.13	0.07	0.08	0.88	0.76	1.02	
	勤勉性	0.27	0.06	<.001	1.31	1.16	1.47	↑
	神経症的傾向	-0.05	0.06	0.41	0.95	0.85	1.07	
	開放性	0.09	0.06	0.15	1.09	0.97	1.22	
情報セキュリティ	被害経験有無	-0.25	0.25	0.31	0.78	0.48	1.27	
	学習経験有無	1.37	0.32	<.001	3.95	2.13	7.32	↑
	対策実施割合	0.12	0.43	0.78	1.12	0.49	2.60	
人口統計的	年齢	0.016	0.01	0.13	1.02	1.00	1.04	
	性別	-0.56	0.27	0.037	0.57	0.34	0.97	↓

※ 学習経験有無は、要因「学校や会社における学習経験の有無」を投入した場合の分析。

表 2 (2)ロジスティック回帰分析結果

		回帰係数	標準誤差	*p* 値	オッズ比	影響
仕事環境	IT系職業	-0.23	0.14	0.11	0.80	
	メール受信頻度	0.09	0.06	0.13	1.09	
学習経験有無	会社研修	0.21	0.19	0.26	1.24	
	学生時	-0.27	0.22	0.24	0.77	
	新聞・テレビ	0.03	0.18	0.86	1.03	
	インターネット	0.29	0.17	0.10	1.33	
	ガイドブック等	-0.06	0.20	0.75	0.94	
	友人・知人	-0.17	0.31	0.57	0.84	
リスク認知・経験	本物受信経験	0.34	0.16	0.04	1.40	↑
	訓練用判別への自信	-0.48	0.16	0.00	0.62	↓
	本物判別への自信	-0.11	0.16	0.48	0.89	
	受信予測	0.00	0.08	0.95	1.00	
ビッグファイブ	外向性	-0.25	0.08	0.00	0.78	↓
	協調性	-0.09	0.09	0.35	0.92	
	勤勉性	-0.09	0.09	0.33	0.91	
	神経症的傾向	-0.04	0.10	0.71	0.97	
	開放性	-0.05	0.09	0.54	0.95	
労働価値観	自己実現	-0.11	0.14	0.41	0.89	
	同僚への貢献	-0.06	0.11	0.60	0.95	
	金銭	0.07	0.09	0.40	1.08	
批判的思考	論理的思考	0.07	0.12	0.56	1.07	
	証拠に基づく客観性	0.35	0.13	0.01	1.43	↑
その他認知特性	記憶力	-0.09	0.09	0.33	0.91	
	熟慮性	-0.27	0.10	0.01	0.77	↓
	メタ認知スキル	0.31	0.18	0.09	1.37	
パーソナルスペース	友人・同僚	0.00	0.00	0.94	1.00	
	全く知らない人	0.00	0.00	0.40	1.00	
人口統計的	性別	-0.37	0.17	0.03	0.69	↓
	年齢	0.00	0.01	0.82	1.00	

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 稲葉　緑
２．発表標題 フィッシングメール内の不一致に対する気づきを促進する要因
３．学会等名 コンピュータセキュリティシンポジウム2022
４．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	稲葉　啓太 (Inaba Keita)		

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関