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　２ 年　 ６ 月 ２２ 日現在

機関番号：２１２０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ０１０２５

研究課題名（和文）人間の心理・行動特性に着目したフィッシング犯罪防止対策に関する研究

研究課題名（英文）Study on AntiPhishing based on Human Psychological Traits and Behavior

研究代表者
小倉　加奈代（Ogura, Kanayo）

岩手県立大学・ソフトウェア情報学部・講師

研究者番号：１０４３２１３９

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究の目標は，ユーザの心理・行動特性を考慮し，技術とユーザ自身の能力向上の両面からフィッシング犯罪を防止することであった．
技術的アプローチとしてWebサイトの表層的特徴量とURL評価サービスに機械学習アルゴリズムを適用した検知手法を提案し，その有効性を確認した．また，検知支援技術として，スマートフォンの一般ユーザが見落としやすい暗号化情報等の注意喚起を促す警告ダイアログを設計し，その有効性を確認した．さらに，ユーザの能力面のアプローチとして，動画コンテンツによる擬似的訓練に基づいた標的型学習教材と第三者視点での防御能力を高める学習教材を作成し，学習効果を確認した．

研究成果の学術的意義や社会的意義
本研究では，悪性サイト検知時でも，アクセスを自動遮断せずに，ユーザ自身が検知結果を熟慮した上で最終的な行動を選択することを想定している．現在，高精度でフィッシングサイトの自動検知が可能であるが，攻撃者は新たな手口を見つけ出し，検知困難なサイトを次々と生み出すため，技術が新たな悪性サイトに対応できない場合，ユーザ自身の検知・回避が必要である．この点で本研究成果の検知支援技術によりユーザ自身の悪性サイトに対する検知感度であるセキュリティ意識を高めることができる点が特色であり，学術的意義として主張できる点である．また，これによりフィッシング犯罪減少に貢献できる点で社会的意義を主張できる点である．

研究成果の概要（英文）：Our goal of this study is to devise methods to avoid phishing by technology and user’s competence based on psychological and behavioral traits.
As technical approaches, we proposed two detection methods. A method was to use surface feature of websites. The other method was to apply machine learning algorithm to results of scoring services of web sites. We confirmed these proposed ways were usefulness. In addition, as a detection support technology, we designed a warning dialog that alerts smartphone users to call attention to important information for figuring safety of web sites and proved this effectiveness. Moreover, as an approach of user's ability, we programed a learning material for advanced persistent thread based on simulated training with video contents and a learning material that enhances the defense ability from a third person's perspective. We verified that these materials raised a learning effect.

研究分野：ヒューマンコンピュータインタラクション

キーワード：フィッシング　ソーシャルエンジニアリング　表層的特徴量　URL評価サービス　警告ダイアログ　標的型攻撃学習教材

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

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，犯罪事例を用いて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．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，既存研究および市販のソフトには，ゼロデイ攻撃という脆弱性修正のためのセキュリティパッチ提供前を狙った攻撃に弱いこと，犯罪者側が，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．

また，偽サイト検知について，近年，急速に普及しているスマートデバイスについては，自動検知技術も含め，偽サイト検知に関する研究は，申請者の知る限りではまだ多くないのが現状である．スマートデバイスの場合，PC と比較するとディスプレイサイズが小さく，Web ブラウジングの際に，可読領域が狭まるために，PC 利用時と比較すると，ブラウザのインタフェースデザインやユーザのブラウジング行動パタンの異なる点が多い．

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．

２．研究の目的

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日常的なくせのような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目指す．

３．研究の方法

本研究では，研究課題(1)として，フィッシングメールやフィッシングサイトの判断に人間の心理や行動特性が影響するのかを調べるため，フィッシングサイト・メールの真偽判断行動とユーザ特性との関係性を実験・質問紙調査を実施し，検討した（研究テーマ(1)）．また，技術面からのフィッシング防止手法として，研究課題(2) Web サイトの表層的特徴に着目した検知手法，既存のサイト安全性評価ツールを利用した検知手法を提案し，その有効性を評価した．さらに，研究課題(3)として，前述の検知技術をより効果的に伝え，ユーザ自身のフィッシングサイトやメールそのものへのセキュリティ意識を高める警告ダイアログを設計し，その有効性を評価した．そして研究課題(4)として，ユーザのフィッシング回避能力を高めるため，ユーザ特性に考慮した学習教材を試作し，学習効果を評価した．

４．研究成果

研究課題(1)フィッシングサイト・メールの真偽判断行動とユーザ特性との関係性の分析

本課題では，フィッシング犯罪実行のプロセスである，フィッシングメールによるフィッシングサイトへの誘導の成否判定実験を実施し，合わせて 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・認知特性に関する質問紙調査を 2016 年度から 2018 年度の 3 年間で約 300 名の大学生を対象に実施した．

フィッシングメールによる誘導実験では，メールのシナリオに着目し，人間の脆弱性[1]と考えられている返礼，義務感，譲歩，希少性，権威，言質と一貫性と行為，コンセンサスと社会的証明を利用した標的型メール攻撃シナリオを 6 種類作成し，それぞれのシナリオを読んだ後の行動を複数用意し，実験協力者に選択してもらった．フィッシングサイトの審議判定実験では，実在する SNS の正規ログイン画面とフィッシングログイン画面を 8 種類用意し，実験協力者にログインのための入力フォームに個人情報を入力するかしないかを判断してもらった．実験と合わせて実施した質問紙調査では，(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を利用した．

実験および質問紙調査の結果，フィッシングメールの成否得点については，認知的熟慮性-衝動性との間に弱い正の相関（「深く物事を考えるほうだ.」のような物事を判断する際の認知傾向が高いほど，メールによる攻撃を回避できる能力が高い傾向にある），認知欲求尺度との間に弱い負の相関（「常に頭を使わなければ満足しない」のような考えることへの動機づけ得点が低いほど，メールによる攻撃を回避できない傾向にある）があることを確認した．さらに，シナリオのうち，希少性に関するシナリオでは，認知的構造欲求尺度の構造欠如に関する反応が強いとフィッシングメールを受け入れる傾向がやや強いこと，返礼・義務感・譲歩およびコンセンサスと社会的証明に関するシナリオでは，認知欲求が高いとフィッシングメールを受け入れる傾向が

やや強いことがわかった．また，サイトの真偽判定得点については，スマートフォンの習熟度レベルとの間に弱い正の相関があることを確認した．

研究課題(2) Web サイトの表層的特徴に着目した検知手法およびサイト安全性評価ツールを利用した検知手法を提案と評価

フィッシングサイトの検知技術の 1 つとして，Web サイトの表層的特徴に着目した検知手法を提案した．この手法では，対象となるサイトのドメインをホワイトリストと照合し，照合しない場合に，Web サイトのキャプチャ画面から画像局所特徴量を算出し，その結果と，事前に構築するデータベース画像との照合の結果，フィッシングサイトを検知する手法である．提案手法を実在する Web サイトを利用し，評価した結果，フィッシングサイトを約 9 割の精度で検知することができ，本手法の有効性を確認した．

また，短縮 URL を含めたサイトの URL を対象に複数の Web サイトの安全性評価ツール結果を統合したサイトの安全性提示手法を提案した．この手法では，既存の Web サイトの安全性評価ツールの評価結果に対し，線形回帰，SVM，ロジスティック回帰，ナイーブベイス，ランダムフォレスト，多層パーセプトロンの訓練あり機械学習アルゴリズムを適用し，対象サイト URL がフィッシングサイトを含めた悪性サイトか否かを判定する手法である．本手法を実在する良性サイト・悪性サイトのリストから作成した評価データにより性能評価した結果，いずれのアルゴリズムでも 100%に近い精度で判定可能であることを確認した．また，実在するフィッシングサイト URL を利用した評価データにより性能評価した結果，ランダムフォレスト，多層パーセプトロンを利用した場合に約 8 割の精度で良性サイト・悪性サイトの判定が可能であることを確認した．

研究課題(3)ユーザ自身のセキュリティ意識を高める警告ダイアログを設計と評価

前述の研究課題(2)の検知結果を確実に伝えるとともに，検知結果をユーザ自身が再吟味し，自身のフィッシングサイトに対する感度を高めるようなセキュリティ意識を高めることを可能とする警告ダイアログを 2 種類設計し，その有効性を確認した．なお，いずれの警告ダイアログともに，フィッシングにより漏洩することが多いパスワードやクレジットカード番号といった重要な個人情報入力時に表示するものとした．

1 種類目の警告ダイアログは，スマートデバイスの画面サイズの制約により，確認がおろそかになりがちな，スマートデバイスでの Web サイト閲覧時のサイトの暗号化情報やアクセスする URL を対象に，サイトの暗号化情報と URL 情報をもとに情報送信先の安全性を表示するものである（図 1）．設計した警告ダイアログを利用した実験により，偽サイトへの情報送信回避行動が確実に行われ，フィッシング回避に有効であること，情報送信前に再確認をするというセキュリティ意識の向上と取れる行動を確認することができた．

2 種類目の警告ダイアログは，1 種類目の警告ダイアログで，設計したダイアログに使い慣れると，表示内容の確認時間が短くなり，表示内容を確認しなくなるという馴化問題に対処するために，表示時にその都度，操作すべき方向（左右）が変化するスワイプ操作を導入した警告ダイアログを設計した（図 2）．この設計した警告ダイアログの利用実験を行い，前述の 1 種類目の警告ダイアログよりも利用回数が増えてもユーザの表示内容確認時間は長く，馴化が弱まることを確認した．

図 1：1 種類目の警告ダイアログ

図 2：2 種類目のスワイプ型警告ダイアログ

研究課題(4) ユーザ特性に考慮した学習教材の試作と評価

研究課題(3)で設計した警告ダイアログの利用を重ねるごとにセキュリティ意識が向上することを確認したが，直接的なフィッシング回避能力を高めることも重要であるため，ユーザ特性に考慮した 2 種類の学習教材を試作し，その学習効果を評価した．

1 種類目は，近年大きな脅威となっている特定の組織や人を対象とした標的型攻撃への回避能力を高めることを目的とした学習教材である．この教材は，近年セキュリティ教育においても人的対策として有効である事例が示されている学習者に模擬攻撃を体験させる訓練型の教材とし，

現実的なシチュエーションで，ユーザの身の回りの環境下での学習を可能にするために GBS 理論(Goal Based Scenario 理論)[2]を取り入れた Web コンテンツとして実現した（図 3）．本教材を利用した結果，特にセキュリティ意識の向上に関しての学習効果が高いこと，セキュリティやリテラシ知識の事前レベルが低い学習者でも理解しやすい教材であることが確認できた．

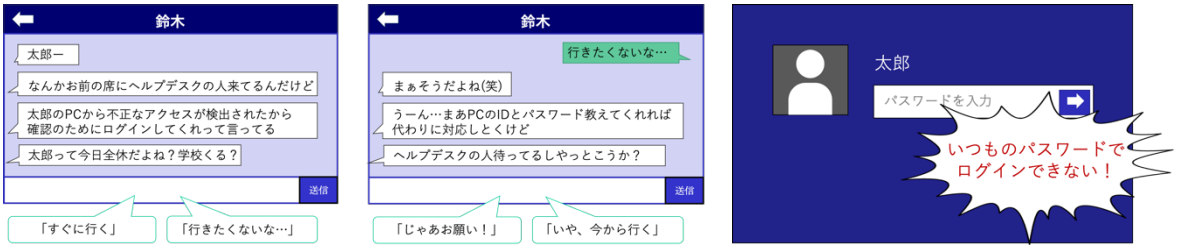

図 3：訓練型標的型攻撃学習教材（左，中央画面時では学習者が行動を選択する）

2 種類目は，セルマンの役割取得理論[3]を利用した情報セキュリティ全般の学習教材である（図 4）．この学習教材では，小学校高学年を学習対象者とし，第三者視点を取り入れることで，それぞれの事項に対する被害時の状況を含めた知識を深めることを目的としたものである．本教材を利用した結果，文字のみの既存の学習方法よりも学習効果が高いことが確認できた．また，インタビューより，「第三者の目線から学習することは意味がある」という意見が非常に多く，「小学生だけではなく親向けでもあるのでは」というような保護者からの好意的な意見が多く見られた．

図 4：セルマンの役割取得理論を利用した情報セキュリティ学習教材

＜引用文献＞

[1] Hadnagy, C., Social Engineering:The Art of Human Hacking, John Wiley & Sons, 2010.
[2] Collins, A., Goal-Based Scenarios and the Problem of Situated Learning: A Commentary on Andersen Consulting’s Design of Goal-Based Scenarios, Educational technology,34(9), pp.30-32, 1994.
[3] Selman R.L., Taking Another’s Perspective: Role-Taking Development in Early Childhood, Child Development, vol.42, pp.1721-1734, 1971.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計18件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 藤根麻羽，小倉加奈代，ベッド.B.ビスタ，高田豊雄
２．発表標題 複数の評価サービスの統合による短縮URLの安全性提示手法の提案
３．学会等名 平成30年度電気関係学会東北支部連合大会
４．発表年 2018年

１．発表者名 藤根麻羽，小倉加奈代，ベッド.B.ビスタ，高田豊雄
２．発表標題 複数のWebサイト安全性評価サービスを利用したURL評価手法の検討
３．学会等名 情報処理学会第31回セキュリティ心理学とトラスト(SPT)研究会
４．発表年 2018年

１．発表者名 小倉加奈代
２．発表標題 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
３．学会等名 情報処理学会研究報告セキュリティ心理学とトラスト(SPT)研究会
４．発表年 2017年

１．発表者名 小倉加奈代
２．発表標題 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
３．学会等名 情報処理学会研究報告セキュリティ心理学とトラスト(SPT)研究会
４．発表年 2017年

１．発表者名
八藤後茉央，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
Web動画コンテンツを利用した標的型攻撃対策訓練手法の提案

３．学会等名
平成29年度電気関係学会東北支部連合大会

４．発表年
2017年

１．発表者名
藤根麻羽，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
短縮URLにおける行先サイト安全性判断支援手法の提案

３．学会等名
平成29年度電気関係学会東北支部連合大会

４．発表年
2017年

１．発表者名
八藤後茉央，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
動画コンテンツによる擬似的訓練を可能とする標的型攻撃教材の開発

３．学会等名
情報処理学会第80回全国大会

４．発表年
2018年

１．発表者名
藤根麻羽，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
複数の評価サービスの統合による短縮URLの安全性提示手法の提案

３．学会等名
情報処理学会第80回全国大会

４．発表年
2018年

１．発表者名
高橋啓伸，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
画像局所特徴量を利用したフィッシングサイト検知手法の実装と評価

３．学会等名
コンピュータセキュリティシンポジウム2016（CSS2016）

４．発表年
2016年

１．発表者名
山田恭平，高田豊雄，ベッド.B.ビスタ，小倉加奈代

２．発表標題
セキュリティ意識向上のためのスマートフォン警告ダイアログの検討

３．学会等名
平成28年度電気関係学会東北支部連合大会

４．発表年
2016年

１．発表者名
吉田裕哉，小倉加奈代，ベッド.B.ビスタ，高田豊雄

２．発表標題
キーストロークダイナミクスを用いたメール作成者保護技術の提案

３．学会等名
平成28年度電気関係学会東北支部連合大会

４．発表年
2016年

１．発表者名
山田恭平，小倉加奈代，ビスタ・B・ベッド，高田豊雄

２．発表標題
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

３．学会等名
第172回情報処理学会ヒューマンコンピュータインタラクション研究会

４．発表年
2017年

１．発表者名
藤根麻羽，小倉加奈代，ベッドバハドゥールビスタ，高田豊雄

２．発表標題
短縮URLの安全性判断支援手法の検討

３．学会等名
情報処理学会第79回全国大会

４．発表年
2017年

１．発表者名
八藤後茉央，小倉加奈代，Bhed Bahadur Bista，高田豊雄

２．発表標題
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

３．学会等名
情報処理学会第79回全国大会

４．発表年
2017年

１．発表者名
小倉加奈代

２．発表標題
偽メール及び偽サイトの回避能力と思考特性との関係性

３．学会等名
2019年度電気関係学会東北支部連合大会

４．発表年
2019年

１．発表者名
小倉加奈代，門脇春麗

２．発表標題
スワイプ操作情報を利用したセキュリティ意識を高めるためのスマートフォン向け警告ダイアログの検討

３．学会等名
ヒューマンインタフェースシンポジウム2019

４．発表年
2019年

１．発表者名
藤根麻羽，小倉加奈代，ベッド.B.ビスタ，高田豊雄

２．発表標題
フィッシングサイトに対するWebサイト安全性評価サービスの統合手法の評価と検討

３．学会等名
2020年暗号と情報セキュリティシンポジウム(SCIS2020)

４．発表年
2020年

１．発表者名
Toyoo Takata, Kanayo Ogura

２．発表標題
Confront Phishing Attacks - from a Perspective of Security Education

３．学会等名
2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)（招待講演）

４．発表年
2019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
研究分担者	高田　豊雄 (Takata Toyoo) (50216652)	岩手県立大学・ソフトウェア情報学部・教授 (21201)	
研究協力者	高橋　啓伸 (Takahashi Hironobu)		
研究協力者	藤根　麻羽 (Fujine Mau)		