Vol.2020-SPT-36 No.42
2020/3/2

エンドユーザはフィッシングサイトを見破ることができるか？ 視線追跡装置と半構造化インタビューを用いたユーザ行動分析

シュウ インゴウ[1,a)]　森 啓華[1]　櫻井 悠次[1]　坪根 恵[1]　飯島 涼[1,2]　阿曽村 一郎[1,5]　坂本 一仁[4]
島岡 政基[3]　森 達哉[1,2,6]

概要：巧妙なフィッシングサイトに対する有望な対策として，ブラウザ上でセキュリティ指標（例えば鍵マークや証明書情報など）を表示することにより，ユーザのリスク認知を高める試みがなされている．また，ユーザに対して適切な教育を施すことにより，リスク認識力が高まることが期待される．しかしながら，これらのアプローチがユーザのフィッシングサイト認知に与える影響は，必ずしも自明ではない．本研究はユーザによるフィッシングサイト認知において事前知識やセキュリティ指標に関する教育が与える影響を一貫的に理解することを目的とし，以下の Research Questions (RQ) を掲げる．**RQ1**: 「フィッシングサイトに対する事前知識やセキュリティ教育により，ユーザの行動はどのように変化するか？」**RQ2**: 「ユーザは何を根拠としてフィッシングサイトを認知するのか？」本研究では，正規のサイトおよびフィッシングサイトを模した架空のフィッシングサイトを 7 つ用意し，ユーザ実験を行う．25 名の実験協力者にそれらのサイトへのログインを促し，その際のユーザの視線をアイトラッキングを用いて計測する．また，上記実験とセットで行うユーザへの教育と半構造インタビューを通じ，ユーザがとった行動とフィッシングサイトの認知状況を詳細に調査する．実験の結果，ブラウザ上で「セキュリティ指標」として表示されている「ドメイン名」,「鍵マーク」及び「証明書」の認知度は低いこと，セキュリティ教育を施すことにより，ユーザの行動（視線）はフィッシングサイトの認知に対して有効な方向に変化するものの，必ずしもすべてのフィッシングサイトの検知にはつながらないことを明らかにした．

キーワード：フィッシングサイト，認知，ユーザスタディ，視線追跡，半構造化インタビュー

Can End-Users Detect a Phishing Site? An Interactive User Behaviour Study Through the Eye Tracking and Semi-Structured Interviews

Abstract: As the countermeasures against phishing sites, browser vendors have developed several security indicators such as address bar display and secure lock icon. In addition, it is expected that the users' ability to understand security risks of phishing attack may rise by giving the appropriate education to the user. However, the impact of these approaches has not been well understood in a consistent manner. In this study, we attempt to consistently understand the effect of user's prior knowledge and security education on the users' awareness of phishing site. This work poses the following Research Questions (RQs). **RQ1**: *How does user behavior change due to prior knowledge and education for phishing sites*? and **RQ2**: *How do users recognize phishing sites?* In this study, we prepare legitimate/fake websites for carrying out user experiments. We recruit 25 participants to study how they behave when they log in to these sites. During the experiments, we monitor their gaze using an eye tracking device. The behavior of the user and the recognition levels of the phishings site are studied through the interactive education programs and semi-structured interviews. As a result, we found that may of participants were not familiar with the security indicators shown on a browser. We also found that by providing prior risk recognition and security education, the behavior of the user changed in an effective direction for detecting the phishing sites, but the change did not lead to the increase in the attack detection rate.

Keywords: Phishing Site, Perception, User study, Eye Tracking, Semi-structured interview

1. はじめに

今日，オンラインバンキングやオンラインショッピングは我々の日常に欠かせない．2016 年の情報通信白書によれば，オンラインバンキングの利用率は 41.1%，オンラインショッピングの利用率は 79.9%にのぼる [13]．その一方で，これらのオンラインサービス利用者を狙う犯罪が増えている．偽の Web サイト (フィッシングサイト) を用いたアカウント情報の不正入手が代表的な手口である．トレンドマイクロ社の「2019 年上半期セキュリティラウンドアップ」 [11] の報告によると，フィッシング詐欺による攻撃は現在も継続して発生しており，2019 年上半期にフィッシングサイトに誘導された国内利用者数は過去最大規模の 200 万件を突破している．

そのようなフィッシングによる被害を軽減するため，これまで様々な対策が提案および実装されてきた．サーバ証明書（以後，単に証明書と呼ぶ）による Web サイトの真正性認証や，法的実在性が確認された組織のみに発行される EV（Extended Validation）証明書の導入はその主な例である．さらに，ユーザに対しては，不正アクセスに対する認知を高めるための様々な「セキュリティ指標」 (security indicator) がブラウザによって提供されている．例えばオンラインバンキングサイトなどのセンシティブなデータを扱う Web サイトにログインする際には，ブラウザのアドレスバー上に表示されている「ドメイン名」が正規サイトと同一であるかを確認することが重要である．また，Web サイトとの通信が TLS によって保護されているかは「鍵マーク」の有無によって確認できる．さらに進んだ情報源として，「公開鍵証明書」に記載された情報を Web サイトの真正性の判断根拠として利用することが可能である．

上述のように，ユーザがフィッシングサイトを認知するための技術的なメカニズムとしてセキュリティ指標が整備されている一方で，それらの指標を適切に使いこなすためには，ユーザに対する教育が必要不可欠である．Dhamja らは 2006 年にユーザにフィッシングサイトを検知させる実験を行い，22 人の実験協力者の内 23%はアドレスバーやステータスバーを見ていないこと，およびユーザがフィッシングサイトを誤答した割合は 40%にのぼることを報告している [3]．Kirlappos らは上述の問題を受け，フィッシング対策におけるセキュリティ教育の必要性，特にセキュリティ指標をユーザが正しく理解することの重要性を説いている [4]．同文献では，フィッシング対策に特化した教育プログラムの作成・評価を実施した研究事例として PhishGuru [5] を紹介しているが，PhishGuru を用いた教育から 4 週間後に実施した実験では，参加者の 17.5%が依然としてフィッシングサイトに重要な情報を入力したことが報告されており，さらなる改善の余地があることが指摘されている [5]．

本研究はこれら過去の研究で得られた知見を基盤とし，ユーザがフィッシングサイトを認知する上で，「ユーザの事前知識」および「セキュリティ指標にフォーカスした教育」が与える効果を理解することを目的とする．これらのフィッシングサイト認知に影響を与える要因は個別に調査・研究がなされてきたが，著者らの知る限りすべての要素を一貫的に調査した研究事例は存在しない．本研究の Research Questions (RQ) は以下の通りである．

RQ1:「フィッシングサイトに対する事前知識やセキュリティ指標に関する教育により，ユーザの行動はどのように変化するか？」

RQ2:「ユーザは何を根拠としてフィッシングサイトを認知するのか？」

上記の **RQ** に答えるため，本研究では著者らが用意した偽サイトを含む 7 つの金融サイトの認証画面を用いた半構造化インタビュー形式のユーザ実験を実施する．さらに，ユーザがフィッシングサイトへ誘導されるリスクを認知した後，およびセキュリティ指標の意味を理解した後の行動変化を計測するため，アイトラッキングシステムを用いて実験参加者の視線追跡データを収集する．

本研究で得られた主要な発見は以下の通りである．

1) ユーザはフィッシングサイトへ誘導されるリスクを認知した際にアドレスバーを注視する傾向にあるが，フィッシングサイトに不信感を持つユーザは多くない．
2) フィッシングサイトを判断する根拠としてコンテンツに着目するユーザは多いが，正しい判断を行ったユーザは少ない．
3) 鍵マークおよび EV 証明書に関する知識を得たユーザはフィッシングサイトに対する不信感を高める．
4) セキュリティ指標に関する教育を受けた後，ユーザの視線は正しい場所を注視するように変化するものの，必ずしもフィッシングサイトの検知にはつながらない場合がある．

本論文の構成は以下のとおりである．2 章では実施したユーザ実験の手順について述べ，その結果を 3 章に示す．4 章では本研究の制限事項とユーザ実験に関する研究倫理と今後の展望を述べ，5 章では関連研究をまとめる，6 章にて本論文のまとめを行う．

2. ユーザ実験の概要

2.1 実験セットアップ

視線測定環境

[1] 早稲田大学 (Waseda University)
[2] 情報通信研究機構 (NICT)
[3] セコム株式会社 (SECOM CO.,LTD.)
[4] 株式会社 DataSign (DataSign Inc.)
[5] みずほ銀行 (Mizuho Bank, Ltd.)
[6] 理化学研究所 革新知能統合研究センター (RIKEN AIP)
[a)] zhouyunao@nsl.cs.waseda.ac.jp

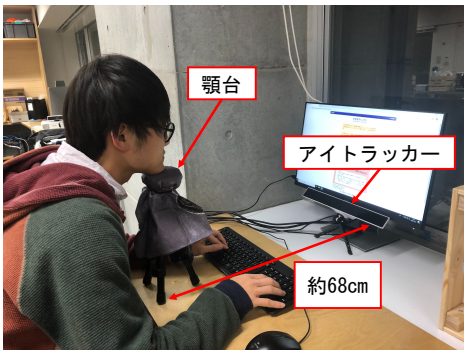

図 1　実験環境の外観 (写真は著者によるシミュレーションの様子)

実験には Dell 23 インチ LCD モニタ (S2319HS) と．Windows10 を搭載したパーソナル・コンピュータを用いた．ウェブサイトへのアクセスには Chrome のシークレットモードを使用した．参加者の視線の計測のため，赤外線強膜反射法による視線計測装置（60Hz；GP3 Eye Tracker，Gazepoint）を使用した．視線を正確に計測するため，三脚に備え付けた自作の顎台を用いて参加者の顔の位置を固定した．参加者と視線計測装置 (以下アイトラッカー) の距離は約 68cm となるよう調整した．実験環境の外観を図 1 に示す．アイトラッカーを用いて，参加者の視線の座標と，その座標での視線停留時間を測定した．

対象ウェブサイト

本研究ではユーザ実験のため，7 つのウェブサイト認証画面を用いる．そのうち 3 つは正規サイトであり，残りの 4 つは正規サイトの画面を完全にコピーしたフェイクサイト（擬似的なフィッシングサイト）である．ウェブサイトの概要を表 1 に示す．また各ウェブサイトにおける認証画面のアドレスバーを図 2 に示す．T1，T2，T3 は実際に運用されている正規サイトである．実験は 4 フェーズから構成され，フェーズ 1 とフェーズ 2 のタスク 1 は 5 サイト (F1，F2，F3，F4，T1)，フェーズ 2 のタスク 2，フェーズ 3，フェーズ 4 では 7 サイトすべてを用いた．自己署名証明書を導入した F1 は，近年増加している無料の証明書を用いるフィッシングサイトを模したものである [1].

2.2　ユーザ実験のデザイン

フィッシングサイトを目の前にしたユーザの行動と，行動を決定する要因を明らかにするため，以下のようなユーザ実験を実施した．実験は 2020 年 1 月に行い，参加者は学校内のアルバイト募集掲示板を通して募集した．参加条件として「オンラインバンキングアカウントを所有していること」，「裸眼またはコンタクトの着用で普段コンピュータを操作すること」を提示した．ユーザ実験を始める前に，実験目的と収集データの使用方法を参加者に伝え，研究同意を得た．次に基本情報に関するアンケートを行った後，4

*1　金融機関の特定を避けるため，文中ではドメイン名は example.co.jp (TLD は適宜実態に合わせる) で表記する．

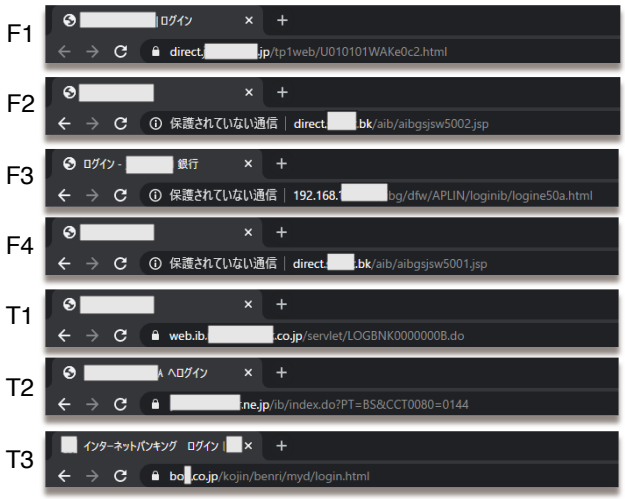

図 2　各ウェブサイト（認証画面）のアドレスバー

つのフェーズによって構成される実験を行い，最後に半構造化インタビューを行なった．実験協力者の集中度を低減させないよう，実験は全体で 45 分以内に終わるよう設計した．4 フェーズからなる実験の意図は以下のとおりである．フェーズ 1 ではフィッシングサイトに関する情報は一切開示せず，ユーザは普段通りログインを試みる，フェーズ 2 ではフィッシングサイトを含むことを開示した上で，参加者自身の保持する知識で不正サイトの判別を行う．フェーズ 3，フェーズ 4 ではそれぞれセキュリティ指標に関する教育を受けた上でユーザの行動がどのように変化するかを調査する．教育は代表的なセキュリティ指標であるドメイン名，鍵マーク，公開鍵証明書に関して，事前に準備した資料*2 を用いた．

以下では実験を構成する一連の流れを示す．

■基本情報のヒアリング

はじめに，参加者の基本情報に関するヒアリングを行う．具体的には，年齢や性別などのデモグラフィックス，コンピュータやネットバンキングの利用経験についてヒアリングする．

■フェーズ 1 (リスク認知なし)

参加者が「通常時」に認証画面を利用する際の行動に焦点を当てる．参加者は予めブラウザ上のタブで開いてある 5 つの認証画面 (F1，F2．F3，F4，T1) にアクセスし，事前に渡したアカウントとパスワードを用いてログインする．アクセスは F1，F2．F3，T1，F4 の順に行う．これらの 5 つのサイトの内，正規サイトは 1 つであり，他はいずれも擬似フィッシングサイトであるが，参加者にはその事実は開示しない．タスク中に外部からの誘導などを避けるため，参加者に対するアドバイス等は一切行わない．アカウント情報の入力後，認証画面から次にページに遷移したら，すぐにタブを閉じるように指示する．

*2　https://www.dropbox.com/s/s8f9vp4m2mvovpc/hint.pdf?dl=0

表 1　実験に用いたウェブサイトの概要

ラベル	金融機関	真贋	証明書	備考*1
F1	A 銀行	偽	あり（自己署名証明書）	サブドメインを構成する文字列を一部改変 (direct.xx-bank.example.co.jp → direct.example.co.jp)
F2	B 銀行	偽	なし	TLD を変更 (example.co.jp → example.bk)，広告バナー削除
F3	C 銀行	偽	なし	ドメイン名の部分を (プライベート)IP アドレスに変更
F4	B 銀行	偽	なし	TLD を変更 (example.co.jp → example.bk)
T1	D 銀行	正規	あり (EV 証明書)	-
T2	E 銀行	正規	あり (EV 証明書)	証明書の主体は銀行のドメイン名ではなく，業務委託企業の所有ドメイン名
T3	F 銀行	正規	あり	-

■フェーズ 2 (リスク情報の開示)

参加者に対し，不正サイトが含まれることを開示する．これにより，参加者がリスクを認知した際にどのように行動が変化するかを観察する．参加者はフェーズ 1 で利用した 5 つのサイトに同順にアクセスしログインする．アクセス中のサイトが偽物だと判断したら, そのサイトへのログインを中止することができる. これをタスク 1 とする．次に，参加者は 7 つの認証画面について信頼度を回答する．各々のサイトに対して「どの程度信頼できると思いますか」という問に対し,「全く信頼できない」から「とても信頼できる」の 5 段階リッカート尺度で回答する.F1， F2．F3，T1，F4，T2，T3 の順に評価をする．これをタスク 2 とする．参加者の負担を減らすため，5 つの認証画面 (F1，F2，F3，F4，T1) ではタスク 1 とタスク 2 を同時に行なった．

■フェーズ 3 (セキュリティ指標の簡易教育)

フェーズ 3 の開始前に，参加者の知識レベル確認を行う．ブラウザのアドレスバーに表示された URL，および URL の横に表示された鍵マークの意味に関する理解度を確認した後，予め用意した解説資料を読んでもらうことにより，参加者に対する教育効果を得た．資料を読み終えた後，参加者は 7 つのサイトすべての認証画面をブラウザ上で閲覧し，5 段階リッカート尺度で「信頼度」を回答する. フェーズ 3 では参加者はログインは行わず，フェーズ 2 のタスク 2 と同順にアクセスする．

■フェーズ 4 (セキュリティ指標の詳細教育)

フェーズ 4 では，さらに詳細な技術情報の教育を実施した上で，参加者の行動変化を観察する．特に 2019 年に実施された Chrome の仕様変更により EV 証明書の組織名表示がアドレスバーからなくなった事実に着目する．「証明書」と「EV 証明書」についての理解度を確認した上で，予め準備した資料を読んでもらう．資料を読み終わった後，参加者は 7 つのサイトすべての認証画面をブラウザ上で閲覧し，5 段階リッカート尺度で「信頼度」を回答する. フェーズ 4 では参加者はログインは行わず，フェーズ 2 のタスク 2，フェーズ 3 と同順にアクセスする．

■半構造化インタビュー

フェーズ 1 から 4 が終了した後，実験中の思考や行動，普段の行動に関して半構造化インタビューを行なう．インタビューでは実験で用いた認証画面のデザインのシンプルさや使いやすさに関する感想，普段オンラインバンキングを使用する時の行動 (アクセス方法，機密情報の入力方法，注意書きを読むか)，EV 証明書の表示方法の変更に関する動向，セキュリティ指標の利便性，その他気がついたこと等に関して質疑応答を実施する．

表 2　実験参加者の使用デバイスとブラウザ ($N = 25$)

項目	属性	人数
金融機関利用時のデバイス	スマートフォン	20
	タブレット	3
	コンピュータ	18
普段使うブラウザ	Chrome	20
	Safari	11
	Firefox	6
	IE	3
	Edge	1
用意した認証画面の利用	任意 1 種類	14
	任意 2 種類	5

3. 実験結果

3.1 参加者統計

大学内のアルバイト募集掲示板を利用して，25 名の参加者を募集した．参加者は男性 15 名，女性 10 名で男性の参加者が多かった．22 名は 20–29 才，残り 3 名は 18–19 才であった．また理工学部の参加者が最も多く 7 名で，続いて文学部，教育・総合科学部と参加者の専攻は幅広かった．コンピュータ経験年数が 5 年未満であった参加者は 8 名，5 年以上 10 年未満の参加者は 9 名，10 年以上の参加者は 8 名であった．コンピュータに慣れ親しんだ参加者が多かった．

参加者が普段使用しているデバイス，ブラウザに関する情報を表 2 に示す．普段「Chrome」を使うと答えた実験参加者は 25 人中 20 人であり，「Safari」,「Firefox」など他のブラウザを使う参加者数は半数以下だった．今回用意した認証画面のうち任意の 1 サイトを利用している参加者は 14 名，任意の 2 サイトを利用している参加者は 5 名であった．一部の参加者は本実験で用いる金融機関の認証画面に馴染みがあると考えられる．

3.2 リスク認知および教育の効果

本研究の **RQ1** に対し，事前知識として不正サイトに対するリスクを認知すること，およびセキュリティ指標に関する教育を受けることによって，ユーザの行動にどのよう

図 3　フェーズ 1 (リスク認知無し) における視線停留時間ヒートマップ．対象ウェブサイトは (F1，F2，F3，F4，T1)

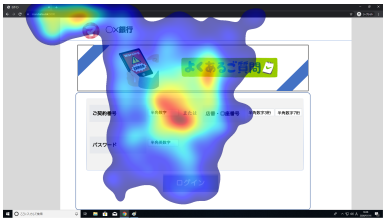

図 4　フェーズ 2 (リスク認知有り) における視線停留時間ヒートマップ．対象ウェブサイトは (F1，F2，F3，F4，T1)

な差があるかを調査する．

リスクの認知による行動の変化

アイトラッカーを用いることにより，参加者の視線を座標として収集できる．座標の時間的変化を解析することにより，画面上における停留時間を把握することができる．実験の進行上，各サイトの滞在時間にはばらつきが生じるため，単純に停留時間を比較することはできない．そこである座標に注視 (停留) した時間をそのサイトに滞在した時間で割ることによって正規化する．フェーズ 1，フェーズ 2 における 5 つの認証画面 (F1，F2，F3，F4，T1) での視線の平均停留時間を表したヒートマップを図 3 と図 4 に示す．図 3 から，参加者がリスクを認知していない場合，視線は主に認証画面のコンテンツ部分，特にアカウントとパスワードの入力欄がある画面中心部に集中したことがわかる．図 4 から，リスクを認知した参加者はコンテンツを幅広く見て判断していること，またブラウザのアドレスバーに着目してサイトの真贋性を判断していることがわかる．

教育有無による行動の違い

セキュリティ指標に関する教育前後の参加者の行動パターンを分析した．フェーズ 2，3，4 での 2 つの認証画面 (T2，T3) の視線の平均停留時間ヒートマップを図 5 に示す．フェーズ 2 は教育前，フェーズ 3，フェーズ 4 は教育後の参加者の行動パターンを表す．フェーズ 2 にて他 5 つの認証画面 (F1，F2，F3，F4，T1) に対するログイン試行を行なっているため，本分析では T2，T3 のみを分析対象とする．図 5 から，教育前 (フェーズ 2) はコンテンツやアドレスバーに視線が向いているが，ドメイン名/鍵前マークの教育を受けた後 (フェーズ 3) はアドレスバーにのみ視線が集まり，さらに証明書に関する詳細な教育を受けることで (フェーズ 4) アドレスバーのみでなく証明書が位置する場所に注視する時間が増えていることがわかる．

教育内容を事前に知っている人にとって，教育は各セキュリティ指標をリマインドする効果があり，知らなかった人にとっては新しい指標として認知させる効果があった．そのような効果により，アドレスバーを確認する時間が増えたと考えられる．フェーズ 3，4 ではフェーズ 1，2 と比較して，画面中央部に視線が集まる時間が短い傾向があった．フェーズ 1 からフェーズ 4 まで同じ認証画面を用いたため，実験が進むにつれて参加者が認証画面のコンテンツに見慣れたこと，あるいは真に注視すべきポイントが絞れるようになったことが要因と考えられる．

3.3　ユーザがフィッシングサイトを認知する根拠

本研究の **RQ2** に対し，ユーザの認知を決定する要因を半構造化インタビューにより調査した結果を示す．

セキュリティ指標の認知度

フェーズ 3，4 のはじめに，セキュリティ指標である「ドメイン名」，「鍵マーク」，「証明書」についての認知度を調査した．その結果，「ドメイン名」と「証明書」を「知らない」と答えた参加者はそれぞれ 17 名であった．また「鍵マーク」について「知らない」と答えた参加者は 11 名と少なかった．証明書がないウェブサイトのアドレスバーには「保護されてない通信」と表示される．これによって不安感を覚え，「鍵マーク」の知識を身に着けた参加者が多いのではないかと推測する．一方，「ドメイン名」は「URL」や「アドレス」などと間違えられることが多い．「証明書」に関して，昨年まで EV 証明書の発行先がアドレスバーに常時表示されていたが，その表示に気づいていた参加者はわずか 2 名で，認知度の低さを裏付ける結果となった．

同一認証画面における信頼度の変化

フェーズ 2，3，4 では，参加者は 7 つの認証画面に対して信頼度の評価を行った．評価は「全く信頼しない」から「とても信頼できる」の 5 段階リッカート尺度評価形式で行い，その結果を表 3 に示す．表 3 の評価の変化及び評価後のインタビューから，画面上で確認できるセキュリティ指標である「ドメイン名」，「鍵マーク」，および昨年画面上での表示がなくなった EV 証明書の「発行先」がユーザの判断にどのような影響を与えるか分析した．

まず，認証画面 F2，F3，F4 について述べる．3 サイトとも通信が暗号化されていないため「鍵マーク」がアドレスバーに表示せず，代わりに「保護されてない通信」という文言が表示される．そのため「鍵マーク」と「ドメイン名」の教育をしたフェーズ 3 にて，信頼度の評価は一気に下がった．「証明書」に関する知識が身についたフェーズ 4 では更に信頼度が落ちた．「鍵マーク」は視覚的に分かりやすく，インタビューでも頻繁に言及された．「ドメイン名」の文字列に違和感を覚える参加者はほとんどいなかった．

認証画面 T2，T3 に関して，2 サイトともにフェーズ 2 では高い信頼度を得ているものの，フェーズ 3 では信頼

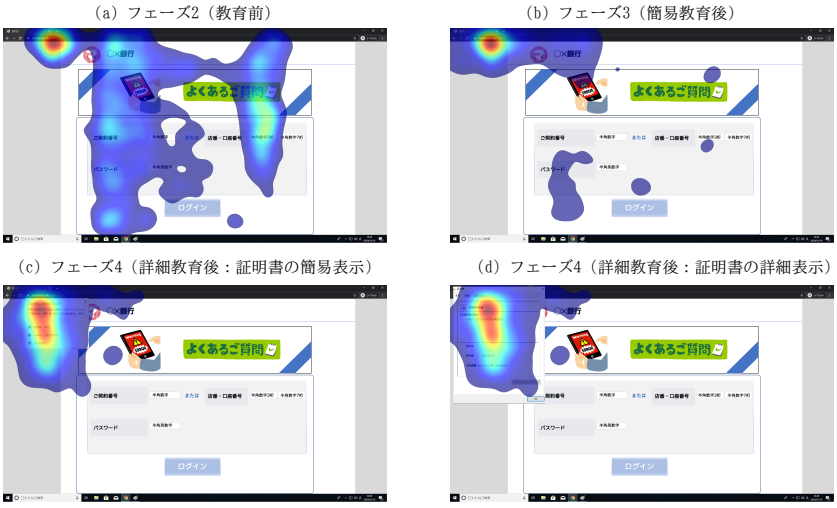

図 5 教育前後の視線停留時間ヒートマップの変化．フェーズ 4 では，証明書の内容を簡易表示したケース (c) と詳細表示したケース (d) に分類．対象ウェブサイトは (T2，T3)

度が落ちる結果となった．しかしフェーズ 4 でまた評価が回復した．インタビューでは，T2 のドメイン名 (金融機関の委託先企業が所有するドメイン名だが，金融機関名とも委託先企業名とも関連性が薄い) と T3 のドメイン名「bo<e>.co.jp[*3]」(bank of example の略語) に関して，金融機関の名称と異なる，あるいは関係性が見られないドメイン名で困惑したという回答が多く見られた．困惑の結果，フェーズ 2 より低い評価を回答した参加者が多かった．「証明書」の情報を受けた後 (フェーズ 4) では，「鍵マーク」をクリックし，証明書が「有効」であることを確認した上で評価を上げた参加者が大部分を占めた．

最後に認証画面 F1，T1 の信頼度の評価について考察する．T1 は正規サイトであり，ドメイン名や証明書を確認することで信頼度が高くなることは明らかである．一方で F1 は偽サイトだが，T1 と同様に実験 3，4 と徐々に信頼度が高くなった．理由として，参加者が「ドメイン名」と「証明書」を詳細に見ていなかった，あるいは理解できていなかったことが考えられる．

以上の知見から，「鍵マーク」の有無はユーザにとって判断が容易で，セキュリティ指標として有効であることがわかった．一方，「ドメイン名」については，正規サイトのドメイン名と比較することが困難なため，偽のドメイン名に気づくことも難しい．正規サイトが，金融機関の名称と関係が薄いドメイン名を使用している場合，ユーザに不安感を与える可能性がある．また，ユーザは「証明書」が「有効」かどうか確認することで，ウェブサイトが信頼できるか判断しており，証明書の詳細を自身で確認，理解することは難しかった．昨今のフィッシングサイトは証明書を導入していることが多いため，今回実験に参加した平均的なユーザの知識では，フィッシングサイトの判別に対して証明書は必ずしも役に立たないことが示唆される．

*3 <e>部分には実際の金融機関名の頭文字 (1 文字) が入る．

表 3 各フェーズにおけるウェブサイトに対する信頼度の評価平均

ウェブサイト	真贋	フェーズ 2	フェーズ 3	フェーズ 4
F1	偽	3.96	4.40	4.68
F2	偽	3.08	2.04	1.56
F3	偽	3.27	1.24	1.20
F4	偽	3.50	2.32	1.60
T1	正規	3.07	4.64	4.84
T2	正規	3.58	2.68	3.40
T3	正規	3.46	2.76	3.28

認証画面間の信頼度の比較

表 3 の T1 と T2 を比較すると，どちらも正規サイトかつ EV 証明書を導入しているにも関わらず，フェーズ 3，4 にて信頼度に差があることがわかる．T1 のドメイン名は “web.ib.example.co.jp” であり，かつ EV 証明書の発行先は “<Example> Bank,Ltd. [JP]” と認証画面上に記されている金融機関名と一致していた．しかし T2 のドメイン名は金融機関と無関係なものであり，このドメイン名は金融機関の委託先企業が所有しているものの企業名とも不一致だった．具体名は避けるが，例えれば Woodgrove 銀行が Adatum 社にサイト運営を委託しているものの，同社が所有するドメイン名は contoso.net であった，というようなものである[*4]．以上のことが要因となり，ドメイン名や証明書の教育を受けた参加者にとって，T2 は信頼度が下がる結果となったことが考えられる．このように EV 証明書を取得してサービスを運用している場合でも，ユーザから不信感を抱かれるケースがあることが明らかとなった．また，F2 と F4 の違いは広告バナーの有無のみであったが，信頼度にわずかな差が見られた．広告バナーが存在する F4 の認証画面の方が，フェーズ 2，3，4 すべてにおいて高い信頼度を得た．シンプルなデザインに不信感を抱

*4 Woodgrove 銀行，Adatum 社および contoso.net はいずれもマイクロソフト社が所有するサンプル用ドメイン名として知られている．https://ja.wikipedia.org/wiki/コントソ

表 4　フェーズ 2 における認証画面ごとのログインをした人数とその内低評価を行った人数

認証画面	F1	F2	F3	F4	T1
ログインした人数	22	16	16	20	17
低評価人数	4	5	6	5	5

く参加者がいたことを示している．

参加者の判断に影響を与えた要素

フェーズ 2 におけるインタビューの回答をもとに，認証画面の信頼度評価に影響する紛らわしい要素を調査した．まず，25 人中 7 人は偽サイトの判断基準として「コピーライトが新しいかどうか」に言及した．今回用意した 7 つの認証画面のうち，4 つのサイトでコピーライトが 2020 年になっていなかった．コピーライトはサイト内写真などの無断利用は禁止という表示であり，セキュリティ指標ではない．また「電話番号」などの問い合わせ先情報が充実しているかどうかを判断基準した参加者が 25 人中 6 人いた．他にも「アマゾンギフト券」や「対フィッシング詐欺ソフトウェアのインストールを促す広告」などのログインと関係のない内容の要素が参加者に不信感を与えた．

4. 議論

4.1 制限事項

実験参加者の視線データを観測するために使用したアイトラッカーは，角膜反射法を採用したモデルのため，計測データの精度は参加者の身体的特徴，実験環境 (光，距離，角度など) に影響される．実験の各フェーズ前にキャリブレーションを行ったが，視線データには固有のエラーが含まれる．実際，実験に参加した 25 名のうち 2 名の視線データは，終始狭い範囲内に留まっていたため，正確に計測できていないと判断し，分析から除外した．また実験は研究室内で行われ，参加者は事前に用意された環境を用い，実験を指揮した研究者立ち会いの元，認証画面へのログインタスクに取り組んだ．このような実験環境における振る舞いと，普段の行動に差がある可能性がある．

フェーズ 2 における実験参加者のターゲットサイトへのログインの有無と信頼度評価との関係性に着目すると，参加者の認知と行動に矛盾があった．表 4 に認証画面ごとにログインをした人数と低評価を行った人数を示す．低評価は信頼性の評価が 1 または 2 である場合を表す．表 4 から，ログインをしたにも関わらず低評価をつけた参加者がいることが分かる．たとえば F3 の認証画面にてログインをした参加者の内 6 名 (37.5%) が低評価をつけていた．低評価をつけた 6 名はインタビューにて認証画面のコンテンツまたはアドレスバーの表示に基づいてそのサイトが安全ではないと感じた上で，ログインを行ったと回答した．このような参加者の認知と行動に矛盾が生じた原因として，本実験において参加者は自分自身のアカウントではなく実験用のアカウントでログインを行ったため，認知したリスクを深刻に受け止めなかった可能性がある．

4.2 研究倫理

本研究におけるユーザスタディでは，早稲田大学が設置する研究倫理オフィスが定める「人を対象とする研究に関する倫理規程」および同オフィスが提供するフローチャートに則り，実験参加者に一切の不利益が生じることがないよう，慎重に実験を設計した．具体的には，実験参加は強制ではなく任意であること，参加者あたりの負荷や謝金のバランスを適切なものとしたこと，そして実験は匿名で行い，個人情報を一切収集しないことを遵守した．

本研究では実在するウェブサイトを参考として実験サイトを構築したが，構築したサイトはあくまでも本研究の目的のみに利用し，研究室内ネットワークからのアクセスに限定して実験を行った．また，実際の正規ウェブサイトを利用する場合は専門家に相談するとともに，ウェブサイトに対する負荷がかからないよう配慮した．その他，研究倫理への対応として，コンピュータセキュリティシンポジウム (CSS)2019 の「サイバーセキュリティ研究における倫理的配慮のためのチェックリスト」 [10] を参考とした．

4.3 今後の研究課題

利便性と信頼性の両立

本研究では認証画面のユーザビリティとユーザの認知との関係性に関する調査を行った．実験後のインタビューにおいて最もシンプルなサイトおよび最も使いやすいサイトを実験参加者に選ばせ，その理由を記録した．本研究において「シンプルさ」とは視覚的な認知を測る指標であり，「使いやすさ」は実際にログイン操作を行うことを仮定してその操作性に関して認知を測る指標である．前述した記録から多くの実験参加者が理想とする認証画面として「シンプル」または「簡素」なウェブページを例としてあげていたが，シンプル過ぎることを理由に信頼度評価を下げる参加者も一定数存在した．つまり，「シンプル」であるほどユーザビリティが向上する一方で，不審なサイトであると感じるユーザが増えることが示唆された．高いユーザビリティを確保しつつ，ユーザから信頼を得られる認証画面のデザインの作成は今後の課題である．

セキュリティ指標とユーザの理解度

本研究で実施したユーザ実験の結果，現状のユーザの知識レベルは高くない傾向にあることが判明した．参加者の多くはウェブサイト上のコピーライトや問い合わせ先の電話番号などのコンテンツに基づいて信頼性を評価しており，正しい判断を行えていなかった．さらに，セキュリティ指標についての教育を行った後でもフィッシングサイトであるかを見分けるのが困難なウェブサイトが存在することが明らかとなった．その顕著な例が，フィッシングサイトが無料で入手可能な証明書を使用していることを想定して用

意をした，自己署名証明書を導入した偽サイト F1 である．3 章で述べたように，ユーザが証明書について十分に理解できていなかったことや，詳細に見ていなかったことなどが原因で F1 の信頼度評価は教育を行うほどに上がっていた．これは近年増加している HTTPS 化したフィッシングサイト [1] に対して，多くのユーザが騙されやすいことを示している．また，例え正規サイトであっても証明書の発行先がその金融機関名と異なる場合，多くの参加者がウェブサイトに対して不信感を抱いていた．したがって，今後はフィッシングサイトの判別に寄与するだけでなく，ユーザに広く認知される新たなセキュリティ指標の開発が不可欠である．

5. 関連研究

ブラウザ上における URL 表示や証明書の効用に関してこれまで様々な研究が行われてきた．アドレスバー上のドメイン名に注意を惹きつけることを目的として，現在主要なブラウザではドメインハイライティング（DH）が実装されているが，Xiong ら [9] と Lin ら [6] は異なる視点からその有効性を調査するためのユーザスタディを実施した．調査の結果，参加者たちのアドレスバーに対する関心は低く，大半のユーザーはいまだウェブコンテンツに基づいてページの真偽を判断するため，DH は期待通りの成果をあげていないことが示唆された．Sobey ら [7] と Biddle ら [2] はウェブサイトを信頼するかどうかの判断を行う際に証明書が果たす役割についてユーザスタディを実施した．調査の結果，証明書の有無は実験参加者の判断に大きく影響したが，EV 情報の有無は大きな変化を与えないことが明らかとなった．Thompson ら [8] はブラウザにおける URL 表示および EV 表示に対する大規模なユーザスタディを行った．彼らの結果においても，DH がユーザのウェブサイト利用に影響を与える結果は発見できなかったとしている．さらに，EV 表示に注意を向ける参加者は少なく，本来の役割を果たせていないという結論に至ったため，Chrome 77 以降ではアドレスバーから EV 表示が削除された．したがって，フィッシング詐欺におけるユーザの対策・啓蒙としてはアドレスバーを確認することが求められてきた [12] が，今後は新たな指標を模索する必要がある．

6. まとめ

本研究はフィッシングサイトを目の前にしたユーザの行動と，行動を決定する要因を理解することを目的として，実在するウェブサイトを模した擬似的なフィッシングサイトを用いたユーザ実験を行った．実験の結果，多くのユーザはリスクを認知した際にアドレスバーやコンテンツ (特にコピーライトや問い合わせ先) を注視する傾向にあるが，正しくフィッシングサイトを見分けられるユーザは少ないことが判明した．教育を受けた後には，フィッシングサイトへの不信感は高くなったが，一部のサイトではセキュリティ指標を有効に活用できずフィッシングサイトを正確に判別できない可能性があることを明らかにした．ユーザにとってフィッシングサイト判別を容易にするために，新たなセキュリティ指標，および利便性と信頼性を兼ね備えた認証画面デザインの研究開発が必要である．

参考文献

[1] APWG: Phishing Activity Trends Report 3rd Quarter 2019, https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf.
[2] Biddle, R., Van Oorschot, P. C., Patrick, A. S., Sobey, J. and Whalen, T.: Browser interfaces and extended validation SSL certificates: an empirical study, *Proc. of ACM CCSW*, ACM, pp. 19–30 (2009).
[3] Dhamija, R., Tygar, J. D. and Hearst, M.: Why Phishing Works, *Proc. of SIGCHI*, p. 581–590 (2006).
[4] Kirlappos, I. and Sasse, M. A.: Security Education against Phishing: A Modest Proposal for a Major Rethink, *IEEE Security & Privacy*, Vol. 10, No. 2, pp. 24–32 (2012).
[5] Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. and Pham, T.: School of Phish: A Real-World Evaluation of Anti-Phishing Training, *Proc. of SOUPS* (2009).
[6] Lin, E., Greenberg, S., Trotter, E., Ma, D. and Aycock, J.: Does domain highlighting help people identify phishing sites?, *Proc. of SIGCHI*, pp. 2075–2084 (2011).
[7] Sobey, J., Biddle, R., Van Oorschot, P. C. and Patrick, A. S.: Exploring user reactions to new browser cues for extended validation certificates, *ESORSI*, Springer, pp. 411–427 (2008).
[8] Thompson, C., Shelton, M., Stark, E., Walker, M., Schechter, E. and Felt, A. P.: The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators, *28th USENIX Security Symposium*, pp. 1715–1732 (2019).
[9] Xiong, A., Proctor, R. W., Yang, W. and Li, N.: Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages?, *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 59, No. 4, pp. 640–660 (2017).
[10] コンピュータセキュリティシンポジウム（CSS）2019 研究倫理委員会：サイバーセキュリティ研究における倫理的配慮のためのチェックリスト，http://www.iwsec.org/css/2019/ethics_list.html (2019). (参照 2020-01-05).
[11] トレンドマイクロ：法人システムを狙う脅迫と盗用 2019 年上半期セキュリティラウンドアップ，https://resources.trendmicro.com/jp-docdownload-thankyou-m144-web-2019-1h-security-round-up.html (2019). (参照 2020-01-05).
[12] フィッシング対策協議会：利用者向けフィッシング詐欺対策ガイドライン（2019 年度板），https://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf (2019). (参照 2019-08-22).
[13] 総務省：情報通信白書平成 28 年版，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nc132120.html (2016). (参照 2019-08-22).