偽ECサイト被害撲滅のためのセキュリティ学習システム

Security Learning System to Eliminate Damage from Fake EC Sites

薄井百花† 宮治裕†
UsuiMomoka† MiyajiYutaka†
†青山学院大学 社会情報学部
† School of Social Informatics, Aoyama Gakuin University.

要旨

近年，偽 Web サイトの詐欺被害は年々増加しており，深刻な社会問題になっている．情報技術が急速に進歩している現代において，テストを行いながら，擬似的な偽の web サイトを見分けるポイントや偽サイトの特徴を学習するシステムは，Web サイト詐欺被害の解決手段になると考えられる．本論文では，偽 Web サイトによる詐欺被害を未然に防ぐことを目的としたセキュリティ学習システムを提案する．評価実験では，学習システムを実験参加者に体験してもらい，そのアンケート調査と学習前後に行ったテストの正答率，アイトラッカーでの分析によってシステムを評価した．

1. はじめに

近年，ネットショッピングやオンラインバンキングは我々の生活に欠かせないものとなっている．令和 3 年の情報通信白書[1]によれば，インターネットショッピングの利用率は 73.4%，オンラインバンキングの利用率は，28.1%にのぼる．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．フィッシング対策協議会[2]によれば, 令和 4 年中のフィッシング報告件数は前年から 44 万 2328 件増え，96 万 8,832 件（前年比で 84.0%増加）と，右肩上がりで増加している．トレンドマイクロ社の 2023 年上半期の動向から注目すべき 3 つのサイバー脅威[3]によると，フィッシングメール（電子メール）経由の誘導とスミッシングと呼ばれる SMS 経由の誘導に加えて，Web 検索，一般サイト上の広告，SNS 上の広告など，いわゆる不正広告からネット詐欺への誘導が顕著化している．

ユーザが詐欺被害を受けないようにするためには，ユーザに対する教育が必要不可欠である．Dhamja らが行ったフィッシングサイトを検知させる実験では，実験協力者の 23%はアドレスバーやステータスバーなどのブラウザベースの手がかりを見ていないこと，40%のユーザは，フィッシングサイトを誤答していることが示された．[4]Stuart E らが行った研究では，HTTPS の表示が消えても，ウェブサイトを訪れる人々は個人情報を提供する意欲には影響がなく, ウェブサイトの認証マークがなくなっても, 97%の参加者が個人情報を入力し続けたことが示された．[5]Kirlappos らは上述の両論文の問題を受け，ユーザーのフィッシング・サイト検出能力を向上させるためには，技術的なフィッシング対策に加え，効果的な教育が必要であると説いている [6].

ユーザに対するセキュリティ教育の課題がある上，フィッシングメールや SMS だけでなく，Web 検索，一般サイト上の広告，SNS 上の広告など，不正広告によるネット詐欺が増加しているためそれらの対応も必要である．

本研究の目的は，過去の研究から得られた知見および警視庁などの公的機関が提供する情報を基盤としたセキュリティ学習システムを開発し，ユーザーがフィッシングサイトを識別し，対処策を学ぶ支援を提供することである．ネット詐欺への誘導が顕著化している現状において，フィッシングメールや，SMS 以外からのアクセスにおいても, 偽 web サイトを見分ける知識や見方を身につけることが望ましいことは明らかである．したがって，今回のセキュリティ学習システムは，偽ショッピングサイトを見分ける学習に焦点を当てた．

2. 詐欺サイト学習システム

本システムは，学習サイトとテストをベースとした Web アプリケーションである．ユーザは，PC を用いてシステムを利用する．システムは図 1 のように，学習前テスト，学習，学習後テストの 3 つのフェーズにわかれている．アプリケーションのフロントエンドには，3 つのフェーズともに React のフレー

ムワークである Next.js と CSS のフレームワークである Tailwind を用いて作成した.

学習前・学習後テストフェーズでは，図 2 の例のようにショッピングサイトが表示され，怪しいと思う点をクリックできるようになっている. そのほかに怪しい項目があれば記述できるようになっている. 特に URL については，なぜ怪しいと思ったのか記述する項目がある. クリックした項目や記述はローカルストレージに保存され，評価の際には Google スプレッドシートにローカルストレージのデータを取り込み，正答率を分析できるようにしている.

学習テストフェーズでは，ユーザは偽サイトを見分ける場所や URL・証明書の見方を学習する. 見分けるポイントの指定には，ツアー系ライブラリである react-joyride[7]を用いた. 図 3 は学習システムの一部分である. ガイドに沿って実際にサイトのボタンを押していくことで偽サイトの見分け方を学習できるシステムにした.

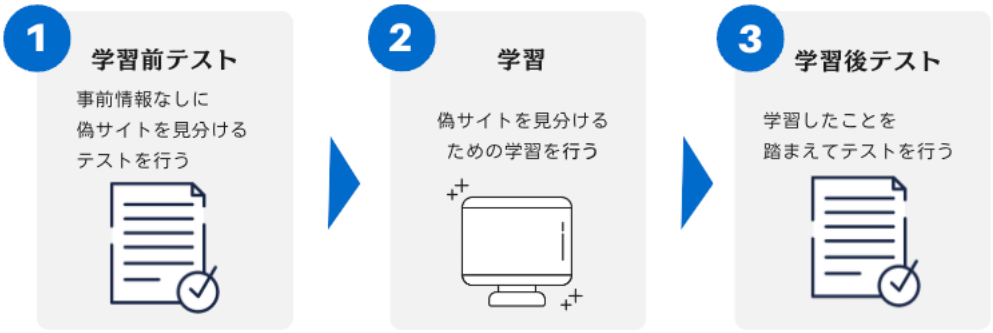

図 1　システムのフェーズ

図 2　テスト画面

図 3　学習画面のガイド

3. 実験

本システムの有効性を示すため，研究室内や学部内から，名の参加者を募集し評価実験を行った．実験は，アイトラッカーをつけた Windows の PC を用いて行った．

はじめに，実験参加者は，実験前アンケートに回答する．実験前アンケートの問 1 から問 4 は，参加者の基本情報に関するもの，問 5 から問 12 は PC や EC サイトの利用経験に関するもの，問 13 から問 17 は，現時点のセキュリティの理解度に関するものである．次に実験参加者は，提案システムを用いて学習前テストを受ける．学習前テストを受けている際には，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ようにする．学習前テストが終わった後，学習フェーズに移り，システムを用いて学習を実施する．学習が終わり次第，学習後テストを受け，最後に学習後アンケートに回答する．学習後アンケートは，問 1 から問 11 は，学習システムの満足度や，危機感や知識の向上に関するもの，問 12 から問 15 はキュリティの理解度に関するものである．

これらの結果と考察について発表する．

4. まとめ

本研究では，ユーザーがフィッシングサイトを識別し，対処策を学ぶ支援を目的とし，過去の研究から得られた知見および警視庁などの公的機関が提供する情報をベースとした，詐欺サイト学習システムを構築した．学習をする際に実際に偽サイトを見抜けない経験をするため，学習システムの評価をするために，システムには，学習前後のテストも組み込んだ．

評価実験は，学習システムの有用性を確かめるため，被験者のテストの正答率，アイトラッカーを用いた分析，アンケート結果を評価予定である．

参考文献

[1] 総務省,”情報通信白書令和 3 年度版”, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf (参照 2023 年 11 月 12 日)

[2] フィッシング対策協議会,”フィッシングレポート 2023” https://www.antiphishing.jp/report/phishing_report_2023.pdf (参照 2023 年 11 月 12 日)

[3] トレンドマイクロ社,” 2023 年上半期の動向から注目すべき 3 つのサイバー脅威” (参照 2023 年 11 月 12 日)

[4] Dhamija, R., Tygar, J. D. and Hearst, M.: Why Phishing Works, Proc. of SIGCHI, p. 581–590 (2006). (参照 2023 年 11 月 12 日)

[5] S.E. Schechter et al., “The Emperor’s New Security Indicators,” IEEE Symp. Security and Privacy, IEEE CS, 2007, pp. 51–65. (参照 2023 年 11 月 12 日)

[6] 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). (参照 2023 年 11 月 12 日)

[7] React Joyride，https://react-joyride.com/ (参照 2023 年 11 月 12 日)