Vol.2017-HCI-172 No.21
2017/3/7

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

山田恭平[†1] 小倉加奈代[†1] ベッド.B.ビスタ[†1] 高田豊雄[†1]

概要：近年，セキュリティ意識の低さからフィッシング攻撃を回避できないユーザが多い．フィッシングサイトは，正規サイトからデザインを流用している場合が多く，見た目でサイトの真偽を判断することが困難である．特に，スマートフォンユーザは，画面サイズによるユーザインタフェースの制約のため，フィッシング攻撃を回避できない傾向が強い．本稿では，スマートフォンユーザに向けたフィッシング攻撃対策としてスマートフォンの画面サイズの制約を考慮したセキュリティ意識を向上させるスマートフォン警告ダイアログを実装し，その有効性を検証する．

キーワード：スマートフォン，フィッシング，警告ダイアログ，ユーザインタフェース

A Study of Alert Dialog to Raise Security Awareness Considering Restriction by Screen Size of Smartphone

KYOHEI YAMADA[†1]KANAYO OGURA[†1]
BHED. B. BISTA[†1]TOYOO TAKATA[†1]

Abstract: In recent years, many users cannot protect themselves from phishing attacks due to their lack of security awareness. Phishing sites often use design or appearance of legitimate sites. In many cases, it is difficult to judge the authenticity of a site from its appearance. Especially, smartphone users tend to be unable to avoid phishing attacks because of the interface which is restricted by the screen size. This paper implements an alert dialog to raise security awareness of phishing attacks for smartphone users by considering the restriction of screen size of smartphone. Furthermore, the paper verifies the effectiveness of the design of the alert dialog.

Keywords: Smartphone, Phishing, Alert Dialog, User Interface

1. はじめに

近年，セキュリティ意識の低さからフィッシング攻撃を回避できない利用者が多い[1]．フィッシングとは，金融機関 (銀行やクレジットカード会社) などを装った電子メールを送り，住所，氏名，銀行口座番号，クレジットカード番号などの個人情報を詐取する行為である．電子メールのリンクからフィッシングサイトに誘導し，そこで個人情報を入力させる手口が一般的に使われている[2]．フィッシングサイトは，正規サイトからデザインを流用している場合が多く，見た目だけで判断することが困難である[3]．特にスマートフォンユーザは，画面サイズによるユーザインタフェース（以下 UI）の制約のため，フィッシング攻撃を回避できない傾向が強い[4]．Web ブラウジング時の一般的なフィッシング攻撃を回避するための対策として，ウェブサイトの URL や SSL 証明書の確認などがあげられる[5]．また，アドレスバーに表示される鍵マークなど接続するサイトの安全性を一目で確認できる指標も存在する．一方，スマートフォンに限ると，画面サイズの制約により，アドレスバーを含むサイトの表示内容の確認が容易ではないため，前述のフィッシング攻撃回避対策の効力は十分ではない．

また，スマートフォン契約数は年々増加し，2019 年には 1 億を突破することが見込まれている[6]．契約数の増加に伴い，今後スマートフォンユーザがフィッシング攻撃を回避できない状況がさらに増えることが予想される．よって，スマートフォン利用時のフィッシング対策が重要となる．

そこで本稿では，スマートフォンの UI の制約を考慮したセキュリティ意識を向上させるスマートフォン警告ダイアログを実装し，その有効性を検証する．フィッシング攻撃を単に回避させる警告ではなく，セキュリティ意識を向上させる警告により，ユーザ自身の判断によるフィッシング攻撃の回避を可能とする．なお本稿では，フィッシング攻撃回避へとつながる行動である「ウェブサイト上から情報を送信する前に，送信するかどうかを安全性の面から再考する」ことをセキュリティ意識の向上と定義する．

2. 関連研究

Maurer ら[7]は，ユーザの悪質サイト判定の研究として，PC による Web ページ閲覧時の入力フォームに対する警告ダイアログ表示の有効性を実験により検証した．この研究で実装された警告ダイアログは，入力フォームに，パスワードやクレジットカード番号のような重要情報が入力され

†1 岩手県立大学
Iwate Prefectural University

た際に表示されるものである. この警告ダイアログにより，ユーザが自ら入力した情報の重要性を再考することで，フィッシング回避につなげる．実験の結果，実装した警告ダイアログにより，ユーザは，入力情報の重要性を自覚し，入力情報を送信するか否かを再考する行動が確認され，セキュリティ意識の向上に有用であることがわかった. また，この警告ダイアログは, PC 利用歴が浅いユーザやセキュリティ知識が低いユーザにも有効であることが確認された.

また，ESET 社[4]による調査では，PC ユーザよりスマートフォンユーザのほうがリンクをみるとすぐにアクセスする傾向が高いことが指摘されている．これは，小画面化に伴う UI の制約により，スマートフォンによる Web ブラウジングでは，Web サイトの真偽を判断しにくいため，フィッシング攻撃に遭いやすいことを示している．また，この調査では，スマートフォンユーザは，PC ユーザよりもセキュリティ知識が低いため，フィッシング攻撃の被害者になりやすいことも報告された．この対策として，前述のセキュリティ知識が低いユーザにも効力を発揮した Maurer らの警告手法を，スマートフォンユーザに適用することが有効であると考えられる．しかし，Maurer らの手法をスマートフォンに適用するには，スマートフォンの画面サイズを考慮した UI 設計はもちろん，過剰な表示による馴化について考慮する必要がある. 警告ダイアログに対する馴化は，警告内容を読まなくなるといった状況を引き起こす可能性があり，対策が必要である.

3. スマートフォン向け警告ダイアログ

本研究では，スマートフォンによる Web サイト閲覧時の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の入力時に，警告ダイアログを表示することにより，入力情報の重要性を自覚し，入力情報を送信するか否かを再考することでフィッシング攻撃を回避することを目指す. そのために, 前章で説明した Maurer らの警告ダイアログをスマートフォン向けに改良し，その有効性を評価，検証する．警告ダイアログは，独自にブラウザを開発し，その一機能として実装した. 警告ダイアログの概要は以下である.

Step1: ユーザが Web サイトの入力フォームに文字列や数字列を入力する際に，入力情報の種類を特定し，入力情報がパスワード，クレジットカード番号の場合に警告ダイアログ（図 1）を表示する.

Step2: ユーザは，警告ダイアログの内容から閲覧中のサイトが信頼できるサイトか否かを判断する.

Step3: Step2 の結果からユーザは，信頼できる場合には警告ダイアログ上の「送信ボタン」, 信頼できない場合には「拒否ボタン」を押す.

Step4:「送信ボタン」を押した場合，そのまま警告ダイアログが閉じられ，ページ操作が可能となる.「拒否ボタン」を押した場合，閲覧ページから離れ，1 つ前のページに戻る.

図 1 警告ダイアログ
（左：安全なサイト，右：危険性のあるサイト）
Figure 1 Alert Dialog (Left: Secure, Right: Insecure)

3.1 警告ダイアログの実装と処理手順

警告ダイアログの実装方法は，まず，Android 専用ブラウザを実装し，その一機能として追加した．警告ダイアログは，実装ブラウザ上での Web ページ閲覧時に動作する.

警告ダイアログが表示されるまでの処理手順は，以下である.

手順 1 : 開発したブラウザで Web ページ閲覧中，Web ページのソースより入力フォームの種類を特定する.

手順 2 : 手順 1 の結果，入力フォームの Input type がパスワード型であることが特定された場合，または，クレジットカード番号と判断された場合に警告ダイアログを表示する.

手順 3 : 警告ダイアログには,「送信する」,「拒否する」の 2 種類のボタンが用意されており，ユーザが「送信する」を押した場合には, 警告ダイアログが閉じられ，そのまま Web ページの操作が可能となる.「拒否する」を押した場合には，閲覧中の Web ページから離れ，1 つ前のページまで戻る処理を実行する.

なお，本研究では，Maurer らとほぼ同一の警告ダイアログ表示手順を採用するが，以下が本研究で新たに追加した点である.

・「拒否する」ボタンを押した場合に，閲覧中の Web ページから離れる.

・「送信する」または，「拒否する」のボタンを押すまでは警告ダイアログを閉じることができない.

・警告ダイアログが表示される際の背景の暗転機能を無効にする.

1 つ目の閲覧中の Web ページから離れる理由は,「拒否ボタン」を押した時点で,その Web ページに滞在する理由がなく,早急に離れるためである.2 つ目の警告ダイアログを閉じることをできないようにした理由は，いずれかのボタンを押さずに警告ダイアログが閉じられることを防ぐためである．3 つ目の理由は，背景の暗転機能による画面の制約を緩和させるためである.

3.2 警告ダイアログの内容

警告ダイアログには閲覧中のサイト及び入力フォームに関する以下 3 つ（図 1 の①～③に対応）が表示される．なお，①の入力情報の特定方法は次節で説明する.

① フォームに入力された情報の種類（パスワード/クレジットカード番号）
② 現在訪れているサイトの暗号化情報の有無
③ 現在訪れているサイトのドメイン名

なお，②は，「暗号化」ではなく「保護」と表現することで，セキュリティ知識レベルの低いユーザが単語の意味を理解できない状況を防ぐ．また，図 2 のように特定された情報の種類に応じたアイコンを警告ダイアログの右上に表示する

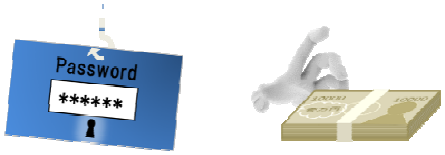

図 2　入力情報の種類を示すアイコン
(左：パスワード，右：クレジットカード番号)
Figure 2　Icons of Input Type
(Password or Credit Card Number)

3.3 入力情報の種類の特定方法

入力フォームに入力された情報の種類はそれぞれ以下の方法で特定する．

- **パスワードの場合**

閲覧中のページの HTML ファイルから入力フォームのタイプを解析し，フォームの入力形式がパスワード形式の場合，入力された情報をパスワードとする．

- **クレジットカード番号の場合**

クレジットカード番号の検査ディジット生成アルゴリズムである Luhn アルゴリズムを使用する．入力フォームに数字列が入力され，その数字列に対してフォーカスを合わせた場合に取得し，Luhn アルゴリズムに流す.Luhn アルゴリズムの適用例を以下に示す．

（例）「30569309025904」
(1)数字列の奇数番目の数字を 2 倍する．
6 0 10 6 18 3 0 9 0 2 10 9 0 4
(2)総和を求める．なお，2 倍した後 2 桁の数字となった場合はそのまま足さずに 1 桁目の数字と 2 桁目の数字を足す．
6+0+1+0+6+1+8+3+0+9+0+2+1+0+9+0+4=50
(3)　(2)の解が 10 で割り切れた場合，クレジットカード番号とみなす．この例では合計が 50 であり 10 で割り切れるため，クレジットカード番号と判断する．

3.4 警告ダイアログのデザイン

ウェブサイトの暗号化情報を警告ダイアログの背景色を変えることで直感的に安全/危険であることを伝える．落合ら[8]は，日本の安全色 6 色および対比色 2 色の潜在危険の程度を評定するため，日本人学生を対象として日本の安全色に対するリスク認知について検討した．その結果，赤が最も潜在危険度が高く，緑や青が最も潜在危険度が低いことが示された．これは赤が「危険」の存在を表す色として最も適していることを意味する．この結果を参考に，実装する警告ダイアログの背景色は，暗号化されているサイトの場合には，明度高めの緑を使用し，暗号化されていないサイトで表示する警告ダイアログには，明度やや暗めの赤を適用することとした．また直感的な判断を促進するため，保護の有無について図 3 のアイコンを利用することとした．

文字の大きさは，現在訪れているサイトの信頼性判断の重要な材料となる暗号化情報とドメイン名に対し，フォントサイズを大きくすることで強調し，暗号化されていないサイトへの情報送信は「非推奨」であることを伝えるために，送信ボタンに「非推奨」表示を追加する．また可読性を考慮し，暗号化されているサイトでは文字色は黒を使用し，暗号化されていないサイトでは白を使用する．

図 3 暗号化の有無を伝えるアイコン
Figure 3　Icons Secure or Insecure

3.5 馴化対策

馴化とは，ある刺激が繰り返し与えられることで，その刺激に対して鈍感になり,反応が徐々に見られなくなっていく現象のことである[9]．よって，警告ダイアログが出現する状況を多く経験すると，警告内容を読まない状況が起こる可能性があり，そのため対策が必要である．Maurer らの研究では，ユーザが一度でも信頼できると判断したサイトでは警告ダイアログを表示しないようにホワイトリストを利用した．しかし，この方法では，警告ダイアログが複数回表示されることは変わらないため馴化対策として不十分である．Anderson ら[10]は，fMRI(磁気共鳴機能画像法)を用い，被験者に 560 枚のソフトウェアのウィンドウやセキュリティ警告を見せ，警告時の脳への影響を調査した．その結果，同じ警告を何度も見ることで注意力が大幅に低下することを明らかにした．また，Anderson らは，有効な馴化対策手法として警告ダイアログの色・形・文言を毎回変化させるような表示形態の多様性がセキュリティ警告の馴化対策に有効であることを示している．さらに，警告ダイアログを左右に揺らすアニメーションが最も有効であることを示した．

本研究の馴化対策では，Anderson らの知見を利用し，警告ダイアログの色・形・文言を変化させる多様な警告方法を取り入れることで馴化を防止する．実装の際には，暗号化されていないサイトで表示する警告ダイアログには左右に揺らすアニメーションを適用する．また，スマートフォンの振動を利用した物理的な刺激を与えることで危機感を煽る．

図 4 アニメーションを取り入れた警告ダイアログ動作例

Figure 4　Alert Dialog with Animation

3.6 警告ダイアログの表示位置

対象サイトが暗号化されている場合は，画面下部に表示し，暗号化されていないサイトでは，画面上部に表示する．暗号化されているサイトで画面下部を利用する理由は，(1)文字を入力する場合にキーボードが表示される部分で必ず目を通す領域であり，キーボードと警告表示位置が被り，画面サイズの小ささによる UI の制約を更に損なわない領域であること，(2)ウェブサイトを遮られることによるストレスを軽減するための 2 つである．また，暗号化されていないサイトで画面上部を利用する理由は，「注視していなかった領域からの刺激は，ユーザの注意を引くことに適している」という周辺視野の原理[11]を利用し，フォームに入力するために画面下部のキーボードに注視していた視線に対し，注視していなかった画面上の領域へ視線を移動させることで警告ダイアログに注視させるためである．

4. 実験

本章では，実装した警告ダイアログがフィッシング攻撃回避対策として機能するかを評価する．そのために，主に以下 2 つについて検証する．

(1) 警告ダイアログによりフィッシングを回避できるか
(2) 警告ダイアログにより「ウェブサイト上から情報を送信する前に，送信するかどうかを安全性の面から再考する．」というセキュリティ意識の向上が起こるか

4.1 実験手順

情報系学部に所属する大学生 17 名（男 16 人，女 1 人）を被験者とし，以下の手順で実験を行った．次節よりそれぞれの手順を説明する．

(1) 警告ダイアログ表示ブラウザの操作方法説明
(2) ログイン実験
(3) 事後アンケート

4.2 警告ダイアログ表示ブラウザの操作方法説明

まず，実装した警告ダイアログ表示機能を有するブラウザの使用方法について，サンプルを含めて説明する．サンプルは，ログイン実験で使用するログインページである．説明では，著者がサンプルのリンクをタップし，ログイン画面が表示されるまでの流れを被験者に実演した．

4.3 ログイン実験

実験課題は，実装した警告ダイアログ表示機能を有するブラウザ上で，著者が用意したログインページ 5 つに対し，順番にログインするという内容である．被験者がパスワードを入力する際に，警告ダイアログが表示され，その際に，「送信する」,「拒否する」ボタンのいずれかを押す．なお，想定する 5 つのログインページの真偽と表示する警告ダイアログの種類を表 1 に示す．5 つのうち 4 つは正規サイトであり，表示される警告ダイアログの内容は図 1 左同様に，サイトの暗号化を示すアイコンがあり，背景色が緑で安全性の高いサイトを示す内容である．残りの 1 つは不正サイトであり，表示される警告ダイアログの内容は，図 1 右同様に，サイトの暗号化がなされていないことを示すアイコンがあり，背景色が赤で危険可能性のあるサイトを示す内容である．

ログインに必要なパスワードは，著者が用意した．実験で使用したログイン画面の 1 つを図 5 に示す．実験では，被験者は，前述のログインページにアクセスし，パスワードを入力する．パスワード入力時に警告ダイアログが表示され，被験者は，内容を読んだ後に入力したパスワードを送信するか否かを判断し，送信する場合には「送信する」ボタン，送信しない場合には「拒否する」ボタンを押す．ログイン自体は警告ダイアログで情報の送信を許可しない限りログインできないようブロックした．

なお，実験では，各ログインページで表示された警告ダイアログの表示時間，入力した認証情報の送信許可/拒否に関わるボタンに対する行動履歴を取得する．警告ダイアログの表示時間を取得する理由としては，被験者の注意を引きつけられたかを測る指標として使用するためである．

表 1　実験時の各ログインページと警告ダイアログの種類

Table 1　Experiment Setting

	ページ真偽	警告ダイアログ
P1	真	安全（図 1 左）
P2	真	安全（図 1 左）
P3	真	安全（図 1 左）
P4	真	安全（図 1 左）
P5	偽	危険（図 1 右）

図 5　実験で使用したログイン画面の例

Figure5　Example of Login Screen Used In Experiment

4.4 事後アンケート

事後アンケートとして，被験者はフィッシング攻撃の認知度，スマートフォン習熟度，警告ダイアログ使用時の行動に関する設問に回答する．フィッシング攻撃認知度と，スマートフォン習熟度の項目は IPA による調査[12]を参考に作成した. 警告ダイアログ使用時の行動に関する設問は，警告ダイアログをどの程度読んだのか，提示された警告ダイアログによって入力情報の送信を再考したかといった警告ダイアログ表示時の行動と，警告ダイアログ使用に関する感想について回答する形式である．

5. 実験結果

5.1 フィッシング攻撃回避に対する警告ダイアログの効果

警告ダイアログによるフィッシング攻撃回避の効果を確認するために，各ログインページで警告ダイアログが表示された際に，各被験者が「送信する」,「拒否する」ボタンのどちらを押したかを表 2 に示す．フィッシングサイトの想定であるログインページ 5 については，警告ダイアログの「拒否する」ボタンを押した被験者は全被験者 17 名中 14 名（約 82%）であった．なお，ログインページ 1〜4 番目の安全なサイトを示す警告ダイアログ表示時に,「拒否する」ボタンを押した被験者も 4 割から 5 割弱存在した.

表 2　送信/拒否ボタンを押した人数 (N=17)
（P1〜P5 はログインページ番号，真/偽はページの真偽）
Table2　The Number of Subjects Sending/Refusing Button

	送信ボタン	拒否ボタン
P1（真）	10 人	7 人
P2（真）	9 人	8 人
P2（真）	11 人	6 人
P4（真）	11 人	6 人
P5（偽）	3 人	14 人

5.2 セキュリティ意識向上の対する警告ダイアログの効果

1 章で述べたように，本研究の目標は，単にフィッシング攻撃の回避だけではなく，セキュリティ意識の向上により，ユーザ自身の判断によるフィッシング攻撃の回避能力を高める警告ダイアログを実現することである．ここでいう「セキュリティ意識の向上」について本研究では,「ウェブサイト上から情報を送信する前に，送信するかどうかを安全性の面から再考する」ことと定義している.「送信するかどうかを再考する」場合，警告ダイアログの表示時間が長くなること，警告ダイアログの内容をよく確認することが予測できる．そこで，警告ダイアログによるセキュリティ意識の向上の効果を確認するために，各被験者の警告ダイアログの平均表示時間を表 3 に，事後アンケートの「警告ダイアログをどの程度読んだか」の設問回答状況を表 4 に,「情報の送信を考えるか」の設問の回答状況を表 5 に示す.

表 3 警告ダイアログの平均表示時間
Table 3　Average Time of Displaying Alert Dialog

	平均表示時間
P1（真）	10.953 秒
P2（真）	3.258 秒
P3（真）	1.914 秒
P4（真）	1.853 秒
P5（偽）	9.815 秒

表 4 警告ダイアログを読んだ程度の設問回答状況
Table 4　The Number of Subjects Reading Alert Dialog

	全部	一部	なし
P1（真）	6 人	9 人	2 人
P2（真）	4 人	10 人	3 人
P3（真）	5 人	9 人	3 人
P4（真）	5 人	9 人	3 人
P5（偽）	7 人	8 人	2 人

表 5　警告ダイアログによる情報送信再考設問回答状況
Table 5　The Number of Subjects Considering Whether Subjects Send Personal Information or Not.

考える	少し考える	あまり考えない	考えない
8 人	6 人	2 人	1 人

表 3 から，想定がフィッシングサイトであるログインページ 5 において，その前までのログインページ 2〜4 と比較して 5 秒以上長い. なお, ログインページ 5 の表示時間は，ログインページ 2〜4 それぞれに対し，有意水準 1%で有意差が見られた．この結果について，被験者が，警告ダイアログの内容を確認し,「送信ボタン」,「拒否ボタン」のどちらを押すべきか検討している時間分であるという解釈も可能である．よって，フィッシングサイトの可能性がある警告ダイアログに，セキュリティ意識の向上につながる行動の喚起効果を有する可能性がある.

表 4 から，想定が正規サイトである場合，フィッシングサイトである場合と大きな違いはないが，フィッシングサイトの想定であるログインページ 5 について全被験者 17 名中 15 名（約 88%）が警告ダイアログの内容を程度に違うはあるにせよ読んでいることがわかった.

また，表 5 から，全被験者 17 名中 14 名（約 82%）が警告ダイアログによってパスワードの送信を再考したことがわかった．この結果からも警告ダイアログが，パスワード等の重要情報を送信する際に再考するというセキュリティ意識の向上につながる行動の喚起効果を有する可能性を示していると言える.

5.3 実装した馴化対策の効果

3.5 節で述べた通り，Maurer らの警告ダイアログは，馴化対策の点で不十分であるため，暗号化されていないサイトで表示する警告ダイアログには左右に揺らすアニメーションと物理的刺激として危機感を煽るための振動の 2 つを馴化対策として実装した．その効果を見るために，5.2 節で検討した各被験者の警告ダイアログの平均表示時間（表 3）を再度検討する．

表 3 を見ると，ログインページ 1 と 5 では，表示時間が 10 秒前後と他とくらべて長く，その他のページでは表示時間が 2,3 秒である．なお，ログインページ 5 と同様に，ログインページ 1 とログインページ 2～4 のそれぞれについて，有意水準 1%での有意差が見られた．ログインページ 1 では，はじめて警告ダイアログが表示され，すべての情報を読もうとすることにより表示時間が長くなったと推測できる．ログインページ 2～4 は，馴化が起こりログインページ 1 ほど警告ダイアログを読まなくなったと考えられる．ログインページ 5 では，極端に短かった表示時間が再び長くなった．これは，被験者が，ページ 2～4 では，警告ダイアログを十分に確認しなかったが，ログインページ 5 では十分に確認したことが考えられる．この結果から，適用した馴化対策が有効に働いた可能性を示していると言える．

5.4 警告ダイアログへの注視状況

5.2 節で事後アンケートの「警告ダイアログをどの程度読んだか」という設問の検討により，警告ダイアログの内容の確認状況を検討した．しかし，警告ダイアログのどの内容を確認しているかは検討していない．ここで，事後アンケートにおいて，警告ダイアログを全部もしくは一部読んだ被験者についての「どの部分を読んだか」の設問回答結果を表 6 に示す．

表 6　警告ダイアログを一部読んだ被験者の詳細
Table 6　The Number of Subjects Reading Contents Partly

	入力情報	暗号化情報	背景色	ドメイン
P1	3 人	4 人	6 人	2 人
P2	4 人	6 人	4 人	2 人
P3	4 人	5 人	4 人	2 人
P4	4 人	5 人	4 人	2 人
P5	3 人	6 人	6 人	3 人

表 6 より，5 つのページ間で特に違いは見られなかったが，全体としてみると，暗号化情報が他とくらべて読まれる傾向が高く，次に背景色に惹きつけられる被験者が多く，ドメイン名を読む人は他よりも少ないことがわかった．これは暗号化情報を「保護」と表現し，直感的な判断を促すために使用したアイコンが有効であったためと考えられる．逆にドメイン名は，読んでも理解できなかった被験者が多かったため，読まれる傾向が低かったと推測できる．

5.5 フィッシング攻撃認知度，スマートフォン習熟レベルと警告ダイアログ使用状況との関係

スマートフォン習熟度を表 7，フィッシング攻撃認知度を表 8 に示す．被験者のフィッシング攻撃認知度は，多くの被験者が「概要をある程度知っている」と回答し，「名前も概要知らない」と答えた被験者は一人もいなかった．

スマートフォン習熟度は，多くの被験者が，「習熟している(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)」と回答し，「入門・初心者(スマートデバイスの簡単な操作ならできる，設定等はお店にしてもらい，買った時のままにしている)」と回答した被験者は一人もいなかった．

スマートフォン習熟度で，「基本操作は習熟」と回答した被験者 4 人は，ログイン画面 1～4 では警告ダイアログの「送信する」ボタンを押し，ログイン画面 5 では，「拒否する」ボタンを押す傾向が見られた．これは，スマートフォン習熟度が比較的低い被験者でもおおむね正しい選択が行えていたことを示唆する結果であると言える．また，フィッシング攻撃認知度で，「名前を聞いたことがある程度」と回答した 4 人は，すべてのログインサイトで警告ダイアログの「拒否する」ボタンを押す傾向にあることが確認された．フィッシング攻撃認知度が比較的低い被験者は，警告ダイアログが表示されることで，予想以上に警戒心を抱き，警告内容に関わらず拒否をした可能性がある．

表 7　スマートフォン習熟度
Table7　Smartphone Skill

	合計人数
非常に習熟している	2 人
習熟している	11 人
基本操作は習熟	4 人
入門・初心者	0 人

表 8　フィッシング攻撃認知度
Table8　Phishing Attack Skill

	合計人数
詳しい概要を知っている	1 人
概要をある程度知っている	12 人
名前を聞いたことがある程度	4 人
名前も概要も知らない	0 人

5.6 警告ダイアログを使用した感想

事後アンケートの被験者の感想では,「ダイアログが表示されたとき,ページを離れなければならないと感じた」,「振動したのは良かった」,「ドメイン名が見えることでもう一度確認することができる」,「背景色に危険さを感じた」といった警告ダイアログのデザインが注意喚起の点で有効であったことを示唆する内容であった．しかし,「警告ダイアログの「送信」という表現がややこしい」,「パスワードマネージャと勘違いした」という意見も複数あった．

設計した警告ダイアログによって情報の送信を再考させることは実現できたが，その後の正しい選択をさせる点について改善の余地がある．

6. 考察

5 章の実験結果から，設計・実装した警告ダイアログがフィッシング攻撃回避対策としておおむね機能しており，重要な情報の送信を再考させる点にも有効であることが確認できた．しかし，ユーザに正しい行動を選択させる点について，正規のサイトへの情報送信の拒否率が比較的高いことから改善が必要である．

正規サイトへの情報送信の際に「拒否する」ボタンを押した原因として，本来のログイン時に表示されることのない警告ダイアログが出現したため不信感を覚えた可能性がある．また，被験者の感想から警告内容の意図が伝わっていなかった可能性も考えられる．さらに「送信の許可/拒否という表現がややこしい」というアンケートでの意見からデザインが一部不適切であったことが原因の 1 つとして考えられる．このような混乱を避けるため，図 6 のように情報の送信許可/拒否ボタンの表現変更を主としたデザインの改善によって正規サイトに対する情報送信を拒否する問題を解決するとともに，警告ダイアログへの信頼性の向上に取り組む必要がある．またフィッシングサイトへの情報送信の拒否率をさらに高めるために，例えば現行の警告ダイアログでは非推奨の行為としている暗号化されていないサイトへの情報送信の許可を行った場合，本当に送信を許可しても良いか再警告を施すなど，さらなる改善が必要である．

馴化対策の 1 つとして警告ダイアログに実装したアニメーション動作は，警告ダイアログの表示時間についてそれまでの表示時間よりも長くなったことから，有効であるといえる．この馴化対策は必要なタイミングで警告ダイアログに注意を引き付けることにおいて最も重要な対策であり，今後も必要である．本研究では，Anderson らの研究で最も効力があったとされる左右に揺らすアニメーションと物理的な刺激として振動を利用したが，多様な警告による馴化対策はとして他の対策を組み合わせることで，今以上の抑止効果を期待できるが，その場合，警告ダイアログの信頼性を損なわないよう設計を施す必要がある．警告ダイアログを毎回変化させることは警告ダイアログ自体への不信感へとつながる可能性がある．これはユーザの情報送信/拒否の選択やユーザビリティにも悪影響を与える可能性があるため，慎重に検討する必要がある．

また，周辺視野の原理を利用した表示位置については，暗号化されていないサイトで表示する警告ダイアログを画面上部に表示するため，画面サイズの制限をさらに大きくし，被験者に不快感を与える懸念があった．しかし，本実験では，多くの被験者が警告内容に目を通しており，不快に感じるなどの意見も上がらなかったため不快感を与えることなく，注視させることを実現できたと考える．

図 6　警告ダイアログのデザイン改善例
Figure 6　Redesigned Plan of Alert Dialog

7. おわりに

本研究では，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を設計・実装し，その有効性を検討した．その結果，警告ダイアログによってフィッシング攻撃の回避に役立つことが確認され，セキュリティ意識向上につながる行動である情報の送信を再考させることにおいても有効であることが確認できた．また馴化対策や，警告ダイアログに注視させるための表示位置や，アニメーション動作についても有効であることが確認できた．

しかし問題点として，正規サイトへの情報送信の拒否率が比較的高いことがあげられる．これについては，今後，警告ダイアログ上の「送信する」,「拒否する」ボタンの表現に問題があることがアンケートから確認できたため，送信許可/拒否ボタンの表現変更を主としたデザインの改善によって正規サイトに対する情報送信を拒否する問題を解決するとともに，警告ダイアログへの信頼性の向上に取り組む．

また，本稿では，パスワードとクレジットカード番号のみを対象としたが，フィッシング攻撃によって盗まれる重要な情報はこれだけにとどまらない．今後，対象とする情報を追加することで，対応できる範囲を広げ，フィッシング攻撃対策としての有用性をさらに高めるための改良を進める．

謝辞 本研究は，JSPS 科研費 16K0126 の助成を受けたものである．

参考文献

[1] HARBOR BUSINESS Online:ネットのセキュリティ意識:世界 16 か国 1 万 8000 人への調査で日本が最下位に,入手先 http://hbol.jp/66173（参照 2016-6-16）
[2] フィッシング対策協議会:フィッシングとは,入手先 https://www.antiphishing.jp/consumer/abt_phishing.html(参照 2017-2-6).
[3] Canon キャノン IT ソリューションズ株式会社 ESET SPECIAL SITE:マルウェア情報局,入手先 http://canon-its.jp/eset/malware_info/term/ha/002.html(参照 2017-2-6).
[4] S. Bortnik: Why do phishing attacks work better on mobile phones?, Welivesecurity,2011.入手先<http://www.welivesecurity.com/2011/01/20/why-do-phishing-attacks-work-better-on-mobile-phones/>(参照 2016-6-16).
[5] フィッシング対策評議会:フィッシング対策の心得,入手先 https://www.antiphishing.jp/consumer/attention.html(参照 2017-2-6).
[6] MM 総研:「スマートフォンの市場規模の推移・予測(2014 年 4 月)」,入手先 https://www.m2ri.jp/news/detail.html?id=111(参照 2016-12-14).
[7] M.E. Maurer, A. D. Luca, S. Kempe: Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness, In Proc. of the Seventh Symposium on Usable Privacy and Security, pp.1-13, 2011.
[8] 落合信寿,齋藤美穂:日本人学生における安全色のリスク認知,日本色彩学会誌,Vol. 29 No.4,pp.303-311,2005.
[9] 心理学用語集 Psychological Term:馴化の定義.入手先 http://psychoterm.jp/basic/learning/05.html(参照 2016-7-22).
[10] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, A. Vance: How Polymorphic Warnings Reduce Habituation in the Brain—Insights from an fMRI Study, In Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp 2883-2892,2015.
[11] S. Weinschenk(武舎広幸,武舎るみ,阿部和也訳):続インタフェースデザインの心理学,オライリージャパン, p.320,2016.
[12] 独立行政法人情報処理推進機構:2015 年度情報セキュリティの脅威に対する意識調査-調査報告書,入手先 https://www.ipa.go.jp/security/fy27/reports/ishiki/(参照 2016-12-2).