金融系ウェブサイトにおける認証画面デザイン分析：デザインメトリクスとユーザ認知

シュウ インゴウ[1,a)]　坂本 一仁[3]　飯島 涼[1,2]　櫻井 悠次[1]　森 達哉[1,2]

概要：フィッシング詐欺に対する対策として，ウェブサイトやブラウザは様々な対策を講じている．例えば，ユーザの重要な情報資産を管理するウェブサイトではフィッシングに対する注意喚起として，バナーや注意書きなどの手法によって，ユーザにフィッシング詐欺のリスクを気が付かせるためのデザインを採用している．しかしながらそのような目的に叶うデザインを実現する一般的な指針はこれまでのところ存在しない．また現在採用されているデザインが実際に注意喚起を促すものとして有効なものであるかは明らかではない．本研究は，上述した問題の解決に向けたファーストステップとして，金融系ウェブサイトを対象とした調査分析により，以下の Research Question (**RQ**) に取り組む．**RQ1**: 金融系ウェブサイトの認証画面のデザインはどのようなものが存在するのか．**RQ2**: それらのデザインに対するユーザの認知はどのようなものか．本研究ではウェブサイトの認証画面のデザインを特徴づける「デザインメトリクス」として，「空白率」，「文字数」，「色の情報エントロピー」を採用し，収集した認証画面の分析を行った．また，収集したログイン画面に対してユーザスタディを実施し，画面に対するユーザの認知を調査した．この結果，認証画面のデザインにおいては，文字数を減ずることにより，ユーザはシンプル，あるいは使いやすいと感じることが明らかになった．すなわち，闇雲にセキュリティ警告の文字を提示することは，ユーザの注視を引きつけるにはかえって逆効果であることが示唆された．

Analyzing the Design of User Authentication Pages of Financial Websites: Design Metrics and User Perception

Yunao Zhou[1,a)]　Takahito Sakamoto[3]　Ryo Iijima[1,2]　Yuji Sakurai[1]　Tatsuya Mori[1,2]

Abstract: Websites and browsers have developed various countermeasures against phishing scams. For example, websites that manage valuable information assets of users adopt a design to let users be aware of the risk of phishing scams using banners and cautionary statements as a warning against phishing. However, there has been no general guidance to achieve such a design. Also, it is unclear whether the design currently in use is effective. As the first step toward the address the problem shown above, this study addresses the following Research Question (**RQ**) through the analysis of financial websites and user survey. **RQ1**: What is the design of the authentication screen for financial websites? **RQ2**: What is the user perception of these designs? In this study, we adopt "blank rate," "number of characters," and "information entropy of color" as the "Design Metrics," which characterizes the design of authentication page of the website. Besides, we perform an online survey to assess the user perception on the login screens collected from the online banking sites. Our analyses revealed that the user tended to feel that a login screen was simple or easy to use when the number of characters is few. The result implies that presenting a large number of letters for the security warning is not effective in attracting users' attention.

1. はじめに

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サービスとなった．2016 年の情報通信

[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.)
[a)] zhouyunao@nsl.cs.waseda.ac.jp

白書によれば，オンラインバンキングの利用率は 41.1%にのぼり，またオンラインショッピングの利用率は 79.9%にのぼる [14]．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．その代表的な手口はフィッシングサイトを用いたアカウント情報の窃取である．具体的には電子メールや SNS の書き込みを利用して偽のウェブサイト（フィッシングサイト）に誘導することにより，利用者のユーザー ID，パスワード，クレジットカード番号などの重要な情報を不正に入手する手口を指す．トレンドマイクロ社の「年間セキュリティラウンドアップ」 [12] の報告によると，2018 年にフィッシングサイトに誘導された国内ユーザ数は前年比で約 2.5 倍に急増しており，フィッシング詐欺の脅威は日々拡大を続けているのが現状である．

フィッシング詐欺をユーザに気付かせる対策は，主としてブラウザによる対策とウェブサイトによる対策に分けることができる．前者の一例は Domain Highlighting (DH) と呼ばれる手法である．DH はブラウザーのアドレスバーに表示される URL 内のドメイン部分を強調して表示する仕組みであり，Chrome，Firefox などの主要なブラウザで実装されている．ユーザがブラウザのアドレスバーを確認し，正規のサイトとフィッシングサイトのドメイン名を区別でき，かつ DH によりフィッシングに利用されるドメイン名が強調されれば，ユーザが詐欺に気がつくことが期待される．しかしながら，Xiong ら [11] および Lin ら [4] の研究によれば，DH は有効ではないことが示唆された．後者のウェブサイトによる対策としては，フィッシング詐欺に対する喚起等の記載があげられる．例えば図 1 に示すように，ユーザの重要な情報資産を管理する金融系ウェブサイトではフィッシングに対する注意喚起として，バナーや注意書きなどの手法によって，ユーザにフィッシング詐欺のリスクを気が付かせるためのデザインを採用している．しかしながら，フィッシング詐欺防止の目的に叶うデザインを実現する方法論はこれまでのところ存在しない．また，現在採用されているデザインが実際に注意喚起を促すものとして有効なものであるかは明らかではなく，サイトの利便性や真贋性判断にネガティブな影響を与えることも予想される．

本研究は以上で示した議論に基づき，日本の金融系ウェブサイトを対象とした認証画面の基礎的な調査分析を実施する．本研究で設定する Research Question (**RQ**) は以下の通りである．

- **RQ1**: 金融系ウェブサイトの認証画面のデザインはどのようなものが存在するのか．
- **RQ2**: ユーザは認証画面のデザインに対してどのような認知を示すのか．

RQ1 に答えるため，国内金融系ウェブサイト 905 件を調査した結果，206 のユニークな認証画面のスクリーンショットを収集することができた[*1]．これらの認証画面は，オンラインバンキングやクレジットカードサービスにアクセスするための，必要な認証を提供する目的で用いられているものであり，ユーザのセキュリティ行動に影響を与えると考えられる．206 のスクリーンショットを分析し，認証画面の「デザインメトリクス」を算出する．ここにデザインメトリクスとは，画面のデザインを特徴づけると考えられる要素である．本研究では，デザインメトリクスとして，画面を構成する空白率，文字数，色の情報エントロピーを採用する．分析の結果，画面の文字数は小さなものから大きなものまで幅広く分布していたのに対し，画面の空白率は高いウェブサイトが多いことがわかった．また，認証画面には写真や，色のグラデーションにより，高いエントロピーを持つウェブサイトが 2 割ほど存在することがわかった．

図 1　注意喚起が掲載された認証画面の例
Fig. 1　Sample of login page that attached warnings

また，**RQ2** に答えるため，収集した認証画面から 206 枚を用い，ユーザが認証画面に対しどのように認知するかを調査した．585 名の参加者に認証画面に対する認知として，「シンプルさ」および「使いやすさ」についてアンケート調査をした．この結果，「シンプルさ」と「使いやすさ」は強い正の相関を持つこと，認証画面中の文字数はユーザが認知する「シンプルさ」と「使いやすさ」に対して正の相関を持つこと，および空白率はユーザが認知する「シンプルさ」と「使いやすさ」に対する相関が低いことが明らかになった．すなわち，認証画面のデザインにおいては，文字数を減ずることがユーザの認知としてシンプルさや使いやすさの向上につながることが示唆された．これは，闇雲に多数の警告文を提示することは，かえって逆効果であることを示唆している．

本論文の構成は以下の通りである． 2 章では，金融ウェブサイトの認証画面収集方法，ならびに収集したスクリーンショットに対して，ウェブサイトの「デザインメトリクス」を分析した結果を示す． 3 章では，得られたスクリーンショットに対するユーザの認知を調査した方法と結果を

[*1] 調査対象とした金融系ウェブサイトにはユーザがログインするサービスを提供しないものも多数含まれていた．

示す．4章では，本研究の制約事項ならびに倫理的配慮について論じる．5章で関連研究をまとめ，6章で結論を述べる．

2. 認証画面のデザインメトリクス

本章では，**RQ1**—金融系ウェブサイトが採用している認証画面デザインの解明—に取り組む．国内金融サービスのウェブサイト905件を対象に，ログイン画面の画像を収集し，デザインメトリクスの観点から国内に存在するログイン画面の特徴を分析する．

2.1 認証画面の収集方法

国内の金融系ウェブサイトとして，Alexa [1] のカテゴリ: 「Top/World/Japanese/ビジネス/金融サービス」にリストされた，905のウェブサイトを調査対象とする．事前調査としてこれらの金融サービスのサイト構造をマニュアルで分析し，下記の特徴を確認した．

- トップページに認証画面を持つサイトが存在する．
- 1つのサイト上に複数の認証画面を持つものがある．
- 認証画面にたどり着くまで複数回のクリックを要するサイトがある．

以上の特徴を踏まえた上で，サイト内を巡回し，認証画面のスクリーンショットを取得するクローラを作成した．クローラはSeleniumおよびHeadless Chromeによって実装した．認証画面の効率的な収集を実現するため，クローリングには再帰型の深さ優先探索を用いた．

ある1サイトを対象とした認証画面探索手順をアルゴリズム1に示す．アルゴリズム内で用いる認証画面判定，および探索リング判定の文字列パターンをXPathによって定義した．それぞれを表1, 2に示す．探索ページにおいて，表1のs_1のパスワード入力欄と判定できる基準によって，ログインフォームが存在すると判定できれば，そのページのスクリーンショットを取得する．スクリーンショットのサイズとしては，モニタ解像度シェアが高い [1920*1080] を選定した [7]．認証画面ではないと判定した場合，そのページ内で表2の判定基準によって認証画面と推測できるリンクを検出し，そのリンクにアクセスして認証画面の判定を繰り返す．l_1はaタグにおいてログインに関する文字列の存在，l_2およびl_3は親要素がaタグのspanタグ，impタグにおいてログインに関する文字列の存在を判定する．理想的には，各サイトの全てのページを探索し，認証画面を抽出すべきであるが，1サイトあたりの探索時間が大きくなること，サイトに過度な負荷をかけてしまうことを考慮し，トップページから深さ3リンクまでの探索とした．

2.2 収集結果

905の金融系ウェブサイトに存在する認証画面を探索した結果，226枚の認証画面のスクリーンショットを自動収集することに成功した．金融系ウェブサイトの中にはユーザがログインを必要とするような認証画面が存在しないものも多く，サイト数よりも少ない認証画面の取得数となった．また，サイトによっては個人向け，法人向けのように複数の認証画面を持つサイトもいくつか確認された．

認証画面の分析を行うにあたり，自動収集した226枚の認証画面の画像のうち，重複や非認証画面のスクリーンショットを手動で判別し，20枚を除去した．最終的には206枚の異なる認証画面デザインを持つ画像の収集に成功した．

表 1 認証画面判定の文字列パターン
Table 1 Patterns of detecting login page.

	XPath
s_1	//input[@type=“password”]

表 2 探索リンク判定の文字列パターン
Table 2 Patterns of detecting next link.

	XPath
l_1	//a[contains(text(),“ログイン”)]
l_2	//span[contains(text(),“ログイン”)]/parent::a
l_3	//img[contains(@alt,“ログイン”)]/parent::a

アルゴリズム 1 サイト内における認証画面の探索手順

```
page ← “https://top.example.com/”
loginPatterns ← [s1]                                  ▷ 表1参照
linkPatterns ← [l1, l2, l3]                           ▷ 表2参照
procedure ExtractLoginPage(page)
    html ← request.get(page)
    if loginPatterns ∈ html then
        screenshot(page)                              ▷ スクリーンショットを取得
    else
        links ← getLinks(html, linkPatterns)
        for all link ∈ links do
            page ← link                               ▷ 新しいページを指定
            return ExtractLoginPage(page)
```

2.3 デザインメトリクス

クローリングによって自動収集した206の認証画面に対し，デザインメトリクスの観点から分析を行う．前述したように，本研究で採用したデザインメトリクスは，文字数，空白率，および色の情報エントロピーの3つである．以下にそれぞれの詳細を示す．

2.3.1 文字数

1番目のデザインメトリクスは文字数である．文字はウェブページにおいて不可欠な要素であり，画面における文字の量の多さは視覚的認知に大いに影響すると考えられる．例えば，認証画面中に非常に多数の文字が存在すれば，ユーザーは注視すべき場所を見失うと考えられる．ウェブ画面上の文字数の集計は自明ではない．なぜなら動的なウェブサイトでは，単純にHTML中のテキスト要素を集

(a)グレースケール画像　　(b)2値化画像(しきい値=220)

図 2　認証画面のグレースケール化と 2 値化の例
Fig. 2　Sample of grayscale and binary images

計することが困難である．また，テキストデータではなく，画像で重要なメッセージを表示するケースも少なくない．こうした問題を解決するために，本研究では光学文字認識 (以後，OCR．) 技術を用い，認証画面のスクリーンショットから文字を抽出・集計するアプローチをとる．OCR として，オープンソースの OCR プログラム tesseract [9] を採用し，文字数を集計する．本研究の目的としては，得られた文字数に関する厳密性は求めない．したがって，本研究では, 検出された文字の正確性検証は割愛する．

2.3.2　空白率

2 番目のデザインメトリクスは，画面の空白部分の割合，すなわち「空白率」である．画面の空白部分はロゴや文字などコンテンツ以外の背景部分であり，画面デザインを特徴付ける．画面全体が画像や文字で覆われていれば，空白率は小さくなり，結果としてユーザーとしてはどこに注視すればよいか，わかりにくくなると考えられる．実際のウェブサイトでは，背景を完全な白色（RGB 値が {255,255,255}）にしている場合は多くない．そのような状況を踏まえ，画像をグレースケールに落とし，更にしきい値を決め，2 値化を行うアプローチを採用する．

図 2 に，あるウェブサイトの認証画面をグレースケールに変換した画像，更にしきい値を 220 として 2 値化した画像を例示する．このしきい値は他の画像の結果も踏まえ，経験的に決定した数値である．

2.3.3　色の情報エントロピー

3 番目のデザインメトリクスは，認証画面中で使われる色の情報エントロピーである．画像を構成する各ピクセルに対し，それぞれが 8 ビットで表現される RGB 値を得る．ある RGB 値 $i \in \{1, \ldots, N\}$ $(N = 2^{24})$ に対し，その RGB 値の画像中における生起確率を p_i とする．情報エントロピーは $p_i > 0$ となる i に対し，$-\sum_{i=1}^{N} p_i \log p_i$ を計算することで得られる．文字数と同様，色の情報エントロピーが極端に高いと，ユーザーは真に注視すべき箇所を見失う可能性があると考えられる．

2.4　デザインメトリクスの分析結果

デザインメトリクスそれぞれの累積相対度数分布を図 3 に示す．まず文字数に関して，画面内文字数が 1500 字以下となったものは 206 枚の認証画面のうち約 80%であった．文字量の分布に偏りは見られなかった．それに対し，空白率は全体的に高くなる傾向があり，206 枚のうち 201 枚の画像で空白率は 0.5 を超えた，特に，そのうち 90 枚の画像は空白率が 90%から 95%の間に集中した．空白率が特に高いものは，認証画面としての要素より，認証とは直接関係ない背景を多く含んでいるという特徴がある．一方，色の情報エントロピーの分布は全体の 75%は 0.08 から 2.37 のデータ域に集中した．残りの 25%の認証画面の中写真や色のグラデーションが存在するパターンが多い．

3.　認証画面の認知に関するユーザスタディ

本章では，**RQ2**—ユーザの認証画面デザインに対する認知— を明らかにするためのユーザスタディを実施する．前章で収集した 206 枚の認証画面スクリーンショットを対象に，オンラインサーベイにより，画面のデザイン性に関する評価を行う．

3.1　ユーザスタディの設計

認証画面に対するユーザの基本的な認知を測定するため，本稿では視覚的な認知を測る「シンプルさ」，および実際にログイン操作を行うことを仮定した操作性に関する認知を測る「使いやすさ」を主要な設問とした．下記にそれぞれの設問の詳細を示す．

- 「シンプルさ」の設問
  「ログイン画面のデザインはシンプルですか」という設問を用意し，参加者に「ごちゃごちゃ」から「シンプル」まで 5 段階のリッカート尺度によって，回答を取得した．この設問は認証画面デザインに対する視覚的な認知を評価することを目的とした．
- 「使いやすさ」の設問
  「ログイン画面は使いやすそうであると思いますか」という設問を用意し，実験参加者に「使いにくい」から「使いやすい」まで 5 段階のリッカート尺度によって，回答を取得した．この設問は認証画面デザインに対する操作性・機能性を評価することを目的とした．

また，上記のユーザスタディと同時に，下記の 2 点の調査を実験参加者に依頼した．

- ログインフォームの有無
  認証画面に対して「ログインフォームはありますか」という設問を用意し，「あり」，「なし」の回答を取得した．本稿では認証画面において最初に表示される

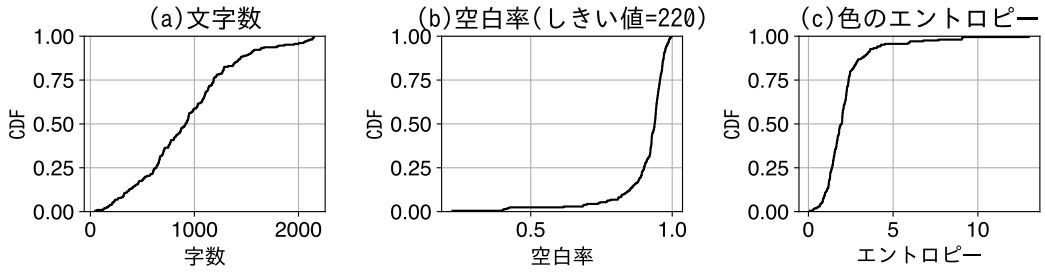

図 3 デザインメトリクスの累積相対度数分布
Fig. 3 Cumulative relative frequency distributions of design metrics

表 3 参加者のデモグラフィックデータ ($N = 585$)
Table 3 Demographic data of participants ($N = 585$).

項目	属性	人数
性別	男性	328
	女性	257
年齢	18, 19 歳	4
	20 代	79
	30 代	214
	40 代	175
	50 代	89
	60 代以上	24
職業	社会人	570
	学生	15
コンピュータ	5 年未満	34
経験年数	5 以上 10 年未満	87
	10 年以上	464
オンラインバンキング	有り	451
アカウントの有無	無し	134

[1920*1080] 区画をユーザが認知する部分として評価しているが，この部分にログインフォームがない場合の，ユーザ認知への影響を評価することを目的としている．

- **詐欺に関する警告の個数**
  認証画面に対して「詐欺に対する警告の個数はいくつですか」という設問を用意し，「0 個」から「4 個」まで，更に「5 個以上」という 6 つの選択肢を設け，回答を取得した．警告の個数におけるユーザ認知への影響を評価することを目的としている．

実験期間は 2019 年 8 月であり，実験参加者の募集はクラウドソーシングサービスのランサーズ [3] を利用した．アンケートは，SurveyMonkey [8] を利用し，収集した．実際のアンケート項目や画面インターフェースの詳細は紙面の制限上割愛する．

3.2 参加者統計

206 の認証画面に対して，1 アンケートにつき 10 または 11 の認証画面を割り当て，合計 20 のアンケートを準備した．1 アンケートは最大 30 名の実験参加者を募集し，最大 600 名が参加を可能とした．ランサーズの機能上，それぞれのアンケートに対する同一参加者の重複回答を防止することが難しい．そのため，我々はランサーズのユーザ名を確認し，重複回答を除く 585 名の回答を分析に利用した．本実験では，1 アンケートにつき 108 円の報酬を支払っている．

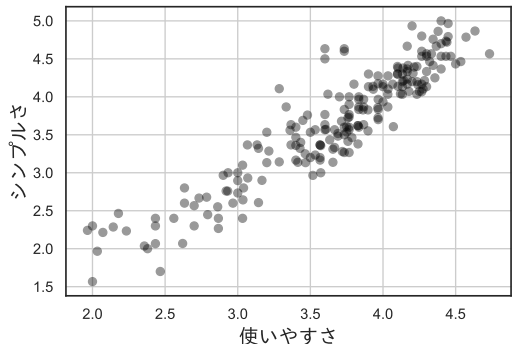

図 4 「シンプルさ」と「使いやすさ」のスコアの相関
Fig. 4 Correlation between simplicity and usability.

参加者 585 名のデモグラフィックデータを表 3 に示す．参加者男女比は 328 対 257 で，男性参加者がやや多い結果となった．職業に関しては社会人が多く，570 名が参加し，残りの 15 名は学生であった．また参加者のうち，「少なくとも 5 年以上コンピュータを利用している」と答えた人は 500 人以上であった．更にオンラインバンキングのアカウントを持つ参加者が 451 名で大半を占め，金融系ウェブサイトの認証画面を経験したことがある参加者が多いと推測できる．

3.3 ユーザスタディの結果

206 の認証画面に対して，1 画面につき最大 30 名の実験参加者によって，計 585 のアンケート結果を収集した．1 画面につき「シンプルさ」および「使いやすさ」の 5 段階リッカート尺度の結果が最大 30 存在するが，どちらも度合いが連続的な間隔尺度として解釈できる．本項では，「シンプルさ」および「使いやすさ」を間隔尺度として扱い，1 画面毎にそれぞれの平均値を算出し，その平均値をスコア

(a)「シンプルさ」スコアが最も低い認証画面(1.567)

(b)「シンプルさ」スコアが最も高い認証画面(5.000)

図 5「シンプルさ」の結果
Fig. 5 Results of Simplicity.

(a)「使いやすさ」スコアが最も低い認証画面(1.965)

(b)「使いやすさ」スコアが最も高い認証画面(4.733)

図 6「使いやすさ」の結果
Fig. 6 Results of Usability.

として分析を行う．「シンプルさ」と「使いやすさ」のスコアの相関を図 4 に示す，ユーザ認知の 2 つの指標は強い正の相関を持つことが確認でき，相関係数は 0.924 である．

3.3.1 認証画面に対するユーザ認知

206 の認証画面に対する「シンプルさ」および「使いやすさ」のスコアからユーザ認知における顕著な結果を示す．「シンプルさ」の設問に対する特徴的な認証画面を図 5 に示す．図 5 (a) は「シンプルさ」の 5 段階リッカート尺度

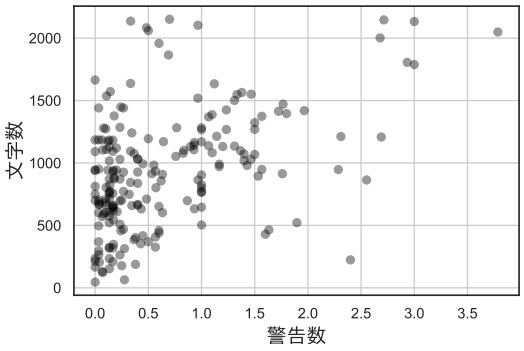

図 7 文字数と警告数の相関
Fig. 7 Correlation between characters and warnings.

において最も低いスコア（1.567）となった認証画面である．画像な文字などの情報量が多く，またログインフォームは他の要素よりかなり小さく，画面の一番上に配置されている．図 5 (b) は「シンプルさ」の 5 段階リッカート尺度において最も高いスコア（5.000）となった認証画面である．画面中央にログインフォームがあり，他の要素は少量である．

「使いやすさ」の設問に対する特徴的な認証画面を図 6 に示す．図 6 (a) は「使いやすさ」の 5 段階リッカート尺度において最も低いスコア（1.965）となった認証画面である．この認証画面は，ログインフォームが画面の枠外にあり，実際ユーザがこの認証画面を利用する際は，一度スクロールする必要がある．図 6 (a) は「使いやすさ」の 5 段階リッカート尺度において最も高いスコア（4.733）となった認証画面である．ログインフォームは画面の真ん中に設置され，他の要素も少ない．

ログインフォームの有無に対する結果として，認証画面の表示区画（[1920*1080]）にログインフォームが完全に含まれない画面が 7 画面 (3.4%) 存在した．7 つの画面における最もスコアが高いものであっても，「シンプルさ」のスコアは 2.567 であり，「使いやすさ」のスコアは 2.700 である．共に全体の平均スコア 3.655 と 3.656 を下回っているため，ログインフォームが画面区画にない場合，ユーザ認知にネガティブな影響を与えることが示唆される．

詐欺に対する警告の個数に対する結果として，警告が 1 つでも含まれている認証画面は 45 (21.8%) であった．また，警告が 3 つ以上のものが 3 (1.5%) あり，3 つのうち「シンプルさ」が最も高いスコアは 2.629 であり，「使いやすさ」が最も高いスコアは 2.703 である．これらも共に全体の平均スコア 3.655 と 3.656 を下回っており，警告の個数はユーザ認知にネガティブな影響を与えることが予想される．また，警告の個数と文字数の関係を図 7 に示す．警告の個数と文字数も正の相関（相関係数：0.451）を示しており，警告の個数が増えると文字数が増えることが示唆される．

表 4　デザインメトリクスとユーザ認知の相関係数
Table 4　Correlation coefficients of design and user perception.

	文字数	空白率	色の情報エントロピー
シンプルさ	0.739	0.179	0.279
使いやすさ	0.646	0.167	0.231

3.3.2　デザインメトリクスとユーザ認知の関係

図 3 で示したデザインメトリクス（認証画面の文字数，空白率，よび色の情報エントロピー）の結果と，ユーザスタディから得たユーザ認知（シンプルさ，使いやすさ）の結果の関係を図 8 に示す．図 8 (a) より，文字数は「シンプルさ」および「使いやすさ」との相関が強いことがわかる（相関係数 : 0.739, 0.646）．すなわち，認証画面内の文字数が多くなるにつれ，ユーザの視覚的な認知のしやすさ，操作性・利便性は低下することがわかる．さらに，警告の個数は文字数と関係しているため，フィッシング対策として注意喚起を多く掲載している認証画面は，ユーザに負荷を与えていることが示唆される．一方で，空白率および色のエントロピーとユーザ認知との相関はみられなかった．実際に，相関係数は 0.1〜0.3 程度であるため，それらが影響を及ぼすとは言い難い．各相関係数の詳細は表 4 に示す通りである．

4.　議論

4.1　制限事項

本研究では，認証画面の見た目の特徴として文字数，空白率，および色の情報エントロピーに着目した．空白率に関しては，画面中のどの範囲がユーザが着目するエリアであるかといった，実質的な空白率までは考慮できていない．また，画面におけるログインフォーム等の各要素の位置関係はスコープ外であった．これらの特徴を加味した上で，ユーザの認知を調査することは今後の課題としたい．また，ユーザスタディにおいては，特定のユーザによる回答が集中することを避けるため，注意書きにもそのことを明記した上で，参加者のアカウント名による重複チェックを行った．しかしながら，クラウドソーシングサービスの制限により，1 タスクにつき募集数の 30%までしか拒否できない制限があるため，最終的に 15 名の参加者が複数のタスクを実施する状況となった．この数は全体に対して十分に少ないと考えられるが，今後の調査においてはシステム的に重複制限ができる工夫を実現する必要があり，今後の課題としたい．

4.2　倫理的配慮

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．

5.　関連研究

フィッシング詐欺に関する研究は数多く存在する．既存のフィッシング詐欺防止や検知の中には，ウェブページの見た目に基づいた手法もいくつか存在する．Mao ら [5] はウェブページの CSS 様式に注目し，決定木を用いてフィッシングサイトを 90%以上正確に検知できるシステムを提案した．また Fu ら [2] は更に視覚的な角度から切り込んだ，ウェブサイトのスクリーンショットのうち，色合いを特徴量とした EMD ベースの識別機を使って，正規ページと偽ページを識別することに成功した．Shen ら [6] は，ウェブページに対するユーザの Saliency を定式化した．その中で，輝度やコントラクトだけでなく，位置，コンテンツそして，時間により Saliency に差が表れることが示された．

Chrome や Firefox などのブラウザに搭載した DH の機能性に対して，Xiong ら [11] と Lin ら [4] は疑問を呈した．両者は異なる視点からユーザスタディを実施し，参加者たちのアドレスバーに対する関心が高くないことを示した．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．

近年の研究として，Thompson ら [10] はブラウザにおける EV (Extended Validation) 表示，URL 表示に対する大規模なユーザスタディを行っている．彼らの結果においても，EV 表示や URL のハイライトに関してユーザの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．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 [13] が，新たな方向を模索する時期に来ていることが示唆される．本稿においては，認証画面における基礎的なユーザの認知を調査した．本稿の結果は，ユーザがフィッシングサイトに遭遇した場合の安全行動に対する新たな一助となることが期待される．

6.　まとめ

本研究は，フィッシング対策におけるウェブサイトデザインの有効性に着目し，日本の金融系ウェブサイトを対象とした調査分析を行った．ウェブサイトの画面デザインを特徴づけるデザインメトリクスとして，「空白率」，「文字数」，「色の情報エントロピー」を採用し，収集した認証画面の分析を行った．また，収集したログイン画面に対してユーザ調査を実施し，ユーザの認知として「シンプルさ」，および「使いやすさ」を調査した．実験の結果，ユーザが認知する「シンプルさ」と「使いやすさ」は強い正の相関

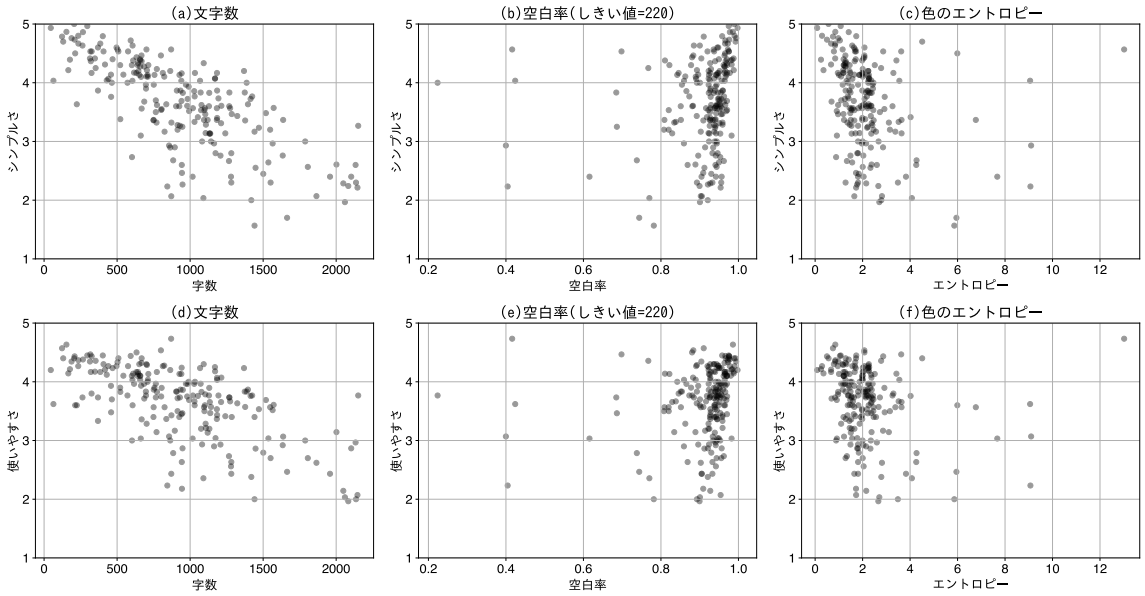

図 8 デザインメトリクスとユーザ認知の関係

を持つこと，認証画面中の文字数はユーザが認知する「シンプルさ」と「使いやすさ」に対して正の相関を持つこと，および空白率はユーザが認知する「シンプルさ」と「使いやすさ」に対する相関が低いことが明らかになった．すなわち，認証画面のデザインにおいては，文字数を減ずることがユーザの認知としてシンプルさや使いやすさの印象につながることが示された．これらの実験結果は，ウェブサイトのデザインにおいて，闇雲に多数のセキュリティ警告文を提示するアプローチは，かえって逆効果であることを示唆している．

本研究の最終的なゴールは，ユーザに対してユーザブルであり，かつ有効なセキュリティ警告を実現するウェブデザインのガイドラインを作成することにある．本研究で示したフレームワークと実験から得られた知見は，その最終ゴールに向けたファーストステップを与えたことに価値がある．本研究で割愛した他のデザインメトリクスがユーザ認知に与える影響を調査すること，さらに踏み込んだユーザビリティの調査，および調査の結果有効であることが判明したデザインを実際に作成し，評価することは将来の研究課題である．

参考文献

[1] Alexa: Top sites by category, `https://www.alexa.com/topsites/category/`. (参照 2019-08-22).

[2] Fu, A. Y., Wenyin, L. and Deng, X.: Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD), *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 4, pp. 301–311 (2006).

[3] Lancers: `https://www.lancers.jp/`. (参照 2019-08-22).

[4] Lin, E., Greenberg, S., Trotter, E., Ma, D. and Aycock, J.: Does domain highlighting help people identify phishing sites?, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2075–2084 (2011).

[5] Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A. and Liang, Z.: Detecting Phishing Websites via Aggregation Analysis of Page Layouts, *Procedia Computer Science*, Vol. 129, pp. 224 – 230 (2018).

[6] Shen, C. and Zhao, Q.: Webpage saliency, *European conference on computer vision*, Springer, pp. 33–46 (2014).

[7] StatCounter: Desktop Screen Resolution Stats Japan, `https://gs.statcounter.com/screen-resolution-stats/desktop/japan` (2019). (参照 2019-08-22).

[8] SurveyMonkey: `https://jp.surveymonkey.com/`. (参照 2019-08-22).

[9] tesseract ocr: `https://github.com/tesseract-ocr/tesseract`. (参照 2019-08-22).

[10] 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).

[11] 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).

[12] トレンドマイクロ：2018 年セキュリティラウンドアップ－騙しの手口の多様化と急増するメールの脅威，`https://resources.trendmicro.com/jp-docdownload-form-m113-web-2018-annualsecurityreport.html` (2018). (参照 2019-08-22).

[13] 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).

[14] 総務省：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).