Vol.2017-MBL-85 No.19
Vol.2017-ITS-71 No.19
2017/11/15

利用者の Web ページ閲覧挙動を用いたスマートフォン端末向け認証方式の検討

飯澤悠介[†1]　中村嘉隆[†1]　稲村浩[†1]

概要：現在，スマートフォン端末には他者の不正利用を防ぐため，固定式パスワードやパターン認証，生体認証が主に導入されている．しかし，固定式パスワード，パターン認証での利便性と安全性はトレードオフの関係であるため利用者への記憶の負担，ショルダーハッキングなどの恐れがある．また，生体情報は不変であることから偽造によって認証を突破される恐れがあり，利便性はあるが安全性に不安がある．本研究では，利用者の Web ページ閲覧挙動を用いたスマートフォン端末向け認証方式の検討を行う．個人的体験であるブラウザ閲覧行為から，最も注目した Web ページを閲覧挙動から抽出し，人間が認識しやすい画像という形で提示することで利便性と安全性の両立を実現する．

キーワード：ブラウザ，閲覧挙動，スマートフォン端末，知識認証，個人認証

1. はじめに

近年，スマートフォン端末が急速に普及している．総務省の調査[1]によると，個人のスマートフォン端末保有率は 2011 年時点で 14．6%であったのに対し，2016 年は 56.8%と約 4 倍に上昇していることから，スマートフォン端末は我々の生活の一部になっていると言える．スマートフォン端末には様々な個人情報が保存されているため，他者の端末不正利用による情報漏洩の危険もあり，不正利用を防止する仕組みが必要となるなど，スマートフォン端末自体のセキュリティに対する重要性も増してきている．

スマートフォン端末の端末保護方法としては，利用者があらかじめ設定しておいた英数字からなる文字列を入力させる「固定式パスワード認証」を用いた認証手法や，画面上の複数の点について利用者があらかじめ決めておいたたどり方を再現させる「パターン認証」を用いた認証手法が主流である．これらの端末保護方法は，高い安全性を求めた場合には認証操作が複雑化する傾向があり，設定したパスワードやパターンを再現することが困難になって利用者の記憶負担が増加する．利便性を求めた場合には，認証操作が単純化する傾向があり，画面の残留物からの認証動作の推測や認証動作を背後から他者が覗き見し，その行動を再現することで認証を突破するショルダーハッキング等で容易に他者の不正利用を許してしまうことがある．このように利便性と安全性はトレードオフの関係にあるといえる．

一部のスマートフォン端末には身体の部位を利用した生体認証が導入されている．生体認証は記憶の必要がなく，紛失・盗難の心配もないため，利便性が高い． しかし，パスワードやパターンのように自由な変更が不可能であるため，認証に用いる生体情報が一度流出すると，他者の不正利用を防ぐことが困難になる．例えば，スマートフォン端末における指紋センサは搭載普及率が 2018 年で 2/3 を超えると予想されている[2]ものの，指紋情報をデジタルカメラ等で撮影された指の写真から復元する技術[3]をもとに，シリコン等で作成した偽指[4][5]や，導電性インクで印刷した指紋 [6] など，入手した指紋情報を実体化して使用するような技術も登場してきているため，生体認証の安全性に対する脅威となっている．

本研究では利便性と安全性の両者を満たしたスマートフォン端末向け認証方式の実現を目的とする．利用者の負荷を減らしつつ，安全な認証を実現することで，スマートフォン端末の不正利用の危険性を軽減することが期待できる．

2. スマートフォン端末における認証

本章ではスマートフォン端末における認証方式の利便性と安全性について考察する．

2.1 利便性

スマートフォン端末に多く搭載されている固定式パスワード認証やパターン認証は再生型と呼ばれる記憶した内容を再現する想起方法を利用した認証方法である．利用者はスマートフォン端末を使用する際に記憶した英数字列やパターンを再現する必要があるため，煩雑さを感じる．そのため，複雑なパスワードを設定しない傾向があると考えられる．これに比べ，生体認証は再生型の煩雑さがほぼなく，認証機器に登録部位を接触させるだけで簡単に認証できる．しかし，登録部位の状態や接触位置の違いによって何度も認証を求められることがあり，不快感を覚える場合もある．これらから，スマートフォン端末における利便性は利用者に認証における記憶の負担を低減し，なおかつ確実な認証を行う必要がある．

2.2 安全性

利便性を求めて認証に単純な固定式パスワードを利用した場合，ショルダーハッキングや利用者個人から得られる情報から推測する推測攻撃で認証を突破されることがある．

†1 公立はこだて未来大学 システム情報科学部

ⓒ 2017 Information Processing Society of Japan

また，パスワードに利用される文字列はメモなど他の媒体に書き写す，口頭で伝えることが出来るので，他者がその情報を詐取する機会がある．パターン認証では，認証時にたどった軌跡が，埃や皮脂などによって画面の残留物として顕著に現れることが多く，パターンの推測が容易であり，認証を突破される可能性がある．生体認証については，認証部位を偽造したり，同等の特徴量を示すもので複製したりすることによって認証システムを欺き，認証が突破される可能性がある．

3. 既存技術

利便性と安全性の両者を満たす可能性のある個人認証手法へのアプローチとして画像を用いた認証と記憶を用いた認証研究が行われている．

3.1 画像認証

画像は単語や文章に比べて覚えられる量が多く，記憶できる期間が長いという特徴がある．このような特徴は画像優位性効果と呼ばれている．この効果を利用した認証方法が画像認証である．画像認証の場合は提示された画像群から正解画像を選ぶ再認型が多い．再認型は，想起する内容があらかじめ提示されるので，想起対象の手がかりなしで想起する再生型よりも容易であるとされている．画像認証の基本的な手続きを図 1 に示す．　スマートフォンの端末認証において画像認証を使用するメリットとしては，画像優位性効果により記憶が容易であり，固定式パスワードやパターンを再現する再生型よりも，設定したものを選択するだけの再認型の方がスピーディかつ利用者の負担が少なくなるという，利便性に関するものが挙げられる．

再認を用いた画像認証の研究として代表的なシステムである「Déjà Vu」[7]は，登録時に複数の人工画像が提示され，数枚を正解画像として登録し，認証時にはダミー画像と一緒に提示され，正解画像を正しく選択することで認証可能とする．Déjà Vu を発展させたものが「あわせ絵」[8]である．合わせ絵は正解画像とダミー画像を携帯端末に保存されている画像を登録して提示することで，人工画像よりも想起を容易にしている．

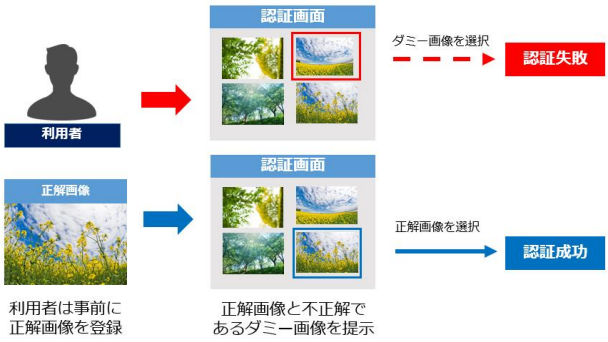

図 1 画像認証の手続き

3.2 人間の記憶を用いた認証

人間が長期的に維持できる記憶には「意味記憶」と「エピソード記憶」がある．意味記憶は「クジラは哺乳類である」，「カエルは両性類である」など，覚えようとして覚える知識の事を指す．エピソード記憶は，昨日受けた講義や昨日の夕食などの個人の体験，経験を指す．このエピソード記憶は忘れにくいため認証に用いた場合も利便性を確保できる．また他者が知ることは困難であり，生活していくことで常に変化するため，これを認証に用いることで安全性も確保できると考えられる．

エピソード記憶を用いた認証研究としてメールの履歴を用いた認証[9]がある．電子メールの本文を提示し，最近受信したものか過去に受信したものかを選択する．また，エピソード記憶と意味記憶の両方を用いた認証方法[10]も提案されている．

3.3 スマートフォン端末に用いる際に生じる問題

画像認証と人間の記憶を用いた認証を組み合わせることでスマートフォン端末に用いることで利便性と安全性の両立が可能である．一方，その際に生じる問題として 3 つ挙げられる．

1 つ目は提示画像抽出の問題である．画像認証は正解画像とダミー画像の提示が必要である．それらの画像は利用者の負担の少ない認証が行えるよう，記憶に関連したものが望ましい．記憶と画像の結びつきが最も強いと考えられる対象は端末内に保存されている画像である．しかし，提示画像で使用してしまうと利用者の人相や交友関係，活動場所等の個人情報に当たる情報が認証を試みた他者に知られてしまう危険もある．近年はインターネット上にプライベート画像をアップロードすることに抵抗が少ない風潮にあるため，このような利用者の個人情報を含む画像やその手掛かりになる画像が端末内に保存されている可能性は高い．そのため，利用者自身に深い関係がありながらも利用者が特定されないような画像を抽出して提示する必要がある．また，利用者の想起を容易にするため，利用者自らが行った経験・体験として記憶に残っているような画像であることも考慮する必要がある．

2 つ目は正解画像とダミー画像の登録の問題である．あわせ絵[8]では利用者が自ら画像を登録する仕組みになっているが，電子メールで画像を送信し，専用 Web ページで管理するため，利用者に長時間の登録作業を必要とする．そのため，人間心理的に長期間画像が変更されない状況が発生しやすくなり，安全性が低下することがある．したがって，利用者にとって登録の負担が少ない画像登録方法の検討が必要となる．

3 つ目は正解画像の選出である．正解画像も利用者の登録動作によって決定されるため，正解画像が長期間変更されない状況が作られ，他者に突破される可能性がある．し

たがって正解画像も利用者の負担が少ない登録ができ，かつ利用者の記憶と強く結びついており，画像を正解画像であると容易に認識できるような画像の選択が必要となる．

4. アプローチ

4.1 提示画像抽出

本研究はブラウザを用いて提示画像を抽出する．スマートフォン端末で認証のために使用できる画像としてアプリケーションからダウンロードした画像やアプリケーション操作時のスクリーンショットなどが考えられる．しかし，ダウンロードした画像の中にはメッセージアプリケーションなど個人的な内容のやりとりをするものによって取得された画像が存在する可能性もあるため，利用者の個人情報につながらない画像のみを抽出することは困難である．一方，アプリケーション操作時のスクリーンショットは対象アプリケーションを限定することによって利用者に無関係な画像が抽出できる．ブラウザ操作から得られる画像の特徴としては以下のものがある．

1) ブラウザでのページ閲覧は自発的行為であり，個人に特化したものとなるため，利用者の経験・体験として記憶しやすい．
2) Web ページは基本的に不特定多数のインターネット利用者に公開されているため，画像からスマートフォン端末利用者を特定することは困難である．
3) 社会的ニュースサイトや旅行サイトなど，個人情報の表示を必要としないサービスは専用アプリケーションで閲覧する時間よりブラウザで閲覧する時間の方が長い[12].

これらの特徴から，認証用に提示する画像に適している画像を抽出する対象として適している．

4.2 画像登録

ブラウザ利用時に記録できる登録候補の画像として，Web ページの img タグで表示された画像や，画像検索で表示された画像があるが，本研究では Web ページそのものを一枚の画像として使用する．閲覧した Web ページにはコンテンツに関してのテキストや画像などの情報がすべて表示されており，ページをスクリーンショットとして表示し，手がかりを示すことで，利用者のページを「閲覧した」エピソード記憶とページで「理解した知識」である意味記憶の両方の効果が望め，想起に有利になる．

また，ブラウザを起動して閲覧を行うたびに正解画像，ダミー画像を含めた提示画像を変化させ，ワンタイムパスワードのようにすることでショルダーハッキングへの対策となる．

4.3 正解画像選出

ブラウザ操作時の Web ページのコンテンツへの利用者の Web ページ表示時間と親指の動作を利用した画面接触時間から得た最も高い注視継続率を指標として画像を選出する．Web ページ興味推定手法として利用者に負担をかけず，興味に関する情報を取得する暗黙的手法に Web ページの閲覧時間を用いたものが存在する[11]．Web ページ表示時間が長ければ長いほどそのページに対して興味があり，注視しているといえる．そのため，利用者の記憶に残りやすいと推測できる．

しかし，その画面を利用者が本当に注視していたのかについては判断できず，利用者の記憶に残っていない画像が正解画像として選ばれる可能性もある．そこで，ページを閲覧する際にページを止める・読み進めるといった操作などをするために，画面に親指が接触する動作に着目する．これら動作を行っている間はコンテンツを注視していると考えられる．したがって，Web ページ表示時間と親指の画面接触時間から注視継続率を求め，注視継続率が最も高い Web ページのスクリーンショットを正解画像として選出する．

5. 提案手法

5.1 システム構成

システム構成を図 2 に示す．利用者が端末にインストールされたブラウザで閲覧を行う．Web ページを閲覧する度に取得した URL，Web ページ表示時間，画面接触時間，注視継続率をスマートフォン端末内のデータベースに蓄積する．利用者が端末を起動後，正解画像となる注視持続率が最も高い URL とダミー画像となる複数の URL を取得し，それぞれスクリーンショットを抽出，画像保存領域に保存し，認証画面に提示する．利用者は提示された画像群の中から正しく正解画像をタップすることが出来れば認証成功となる．認証成功後に web ページを閲覧した場合，提示画像群が更新され，正解画像，ダミー画像ともに閲覧した Web ページの情報に基づいて別の画像変化する．

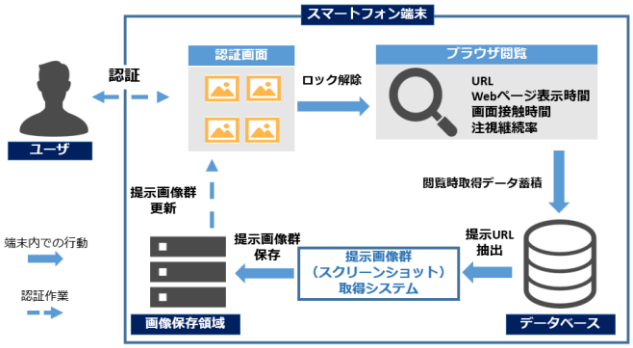

図 2 システム構成図

5.2 ブラウザによる Web ページ閲覧

ブラウザを用いて利用者のページ表示時間と画面接触時

間を記録し，注視継続率を算出する．利用者が閲覧する Web ページを<p_1，p_2，… p_n，>とする．

ページ表示時間は Web ページのロードが完了から URL が変更されるまでとした．Web ページp_iに対するロード完了時の Web ページ表示開始時刻をsp_i，遷移時の表示終了時刻をep_iとするとページ表示時間rp_iは以下の(1)式で求められる．

$$rp_i = ep_i - sp_i \quad \cdots(1)$$

Web ページp_iに対する画面接触時間を求める．p_iにおいて親指が画面に触れてから離れるまでの計測時間を<t_{i1}，t_{i2}，… t_{ik}，>とすると，画面接触時間tp_iは以下の(2)式で求められる．

$$tp_i = \sum_{j=1}^{k} t_{ij} \quad \cdots(2)$$

ページ表示時間rp_iと画面接触時間tp_iを用いて注視継続率gc_iは以下の(3)式で求められる．

$$gc_i = \frac{tp_i}{rp_i} \cdots \quad (3)$$

5.3 提示画像群の抽出

提示画像群である正解画像とダミー画像の抽出を行う．データベースへ問い合わせ，正解画像になる注視継続率が最も高い Web ページの URL とダミー画像になるランダムで選択された URL を選択する．その後，URL からそれぞれの Web ページのスクリーンショットを抽出する．

5.4 認証フェーズ

抽出したスクリーンショットを提示する．認証作業のイメージを図 3 に示す．利用者は提示された画像群の中からダミー画像を選択すると認証失敗し，正しく正解画像をタップすることで認証成功となりロックを解除できる．

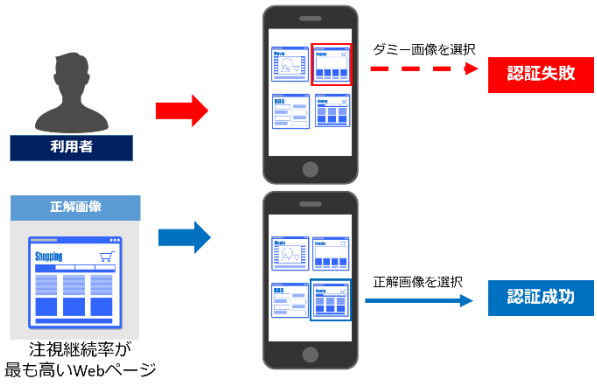

図 3 認証作業のイメージ

6. プロトタイプアプリケーションの実装

本研究では提案手法を基に，利用者が想起する正解画像と注視継続率から得られた正解画像が一致するかを確認するため，プロトタイプアプリケーションの実装を行った．データを取得するため，ブラウザの基本機能「戻る」「次へ」「ホーム」のみを備え，ページ表示時間計測，タッチ時間計測，注視持続率算出機能を組み込んだブラウザの作成を行った（図 4）．

プロトタイプのシステム構成を図 5 に示す．計測したページ表示時間と画面接触時間から注視継続率を求め，スクリーンショットサーバのデータベースへデータを送信する．データベースから注視継続率が最も高い Web ページの URL とランダムに抽出された URL を取得する．抽出する際，検索結果画面は除外し，URL が同じものが複数存在した場合，最も注視継続率が高い URL を取得した．その後，ページ上部から 320×568 のサイズでスクリーンショットを取得し，ブラウザ画面に提示画像群を表示する．

図 4 実験用ブラウザ

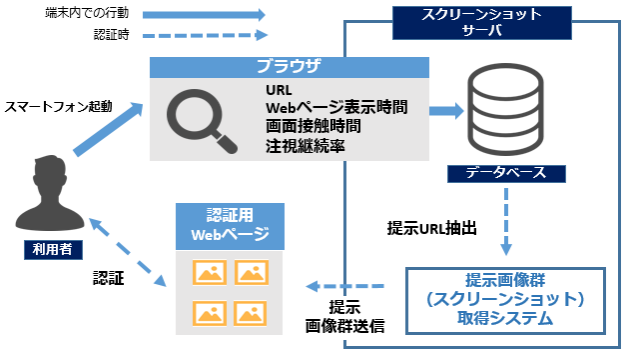

図 5 プロトタイプの構成

7. 基礎実験

認証成功には想起する正解画像を一定の時間経過後の認証時に記憶していることが必要となる．基礎実験として客観的な注視継続率という計測方法で選択した正解画像が，利用者の主観的な想起した正解画像と一致するか調査する．

7.1 実験方法

被験者はスマートフォン端末のブラウザアプリの扱いに習熟した本学システム情報科学部の男子学生 5 名(A~E)である．被験者全員に表 1 の端末を用いて実験を行ってもらった．典型的なスマートフォン操作過程を記録するため，被験者にまずキーワードを決めてもらい，それに基づく検

ⓒ 2017 Information Processing Society of Japan

索操作を 10 分間行わせた．そして，以下の指示を守るよう教示し，キーワードに関する内容の Web ページ閲覧を 10 分間行ってもらった．

・ロード終了後に閲覧を行う
・Web ページのコンテンツを注視する際は画面に親指を接触させたまま注視する

10 分後，閲覧を終了してもらう．その後，正解画像 1 枚ダミー画像 3 枚が表示される Web ページに作成された画像群提示画面へ移ってもらい，最も注視した画像を選択してもらった．この一通りの動作を被験者 1 人に対して 3 セッション行ってもらった．

表 1 実験端末

使用端末	SONY Xperia Z5 SO-01H
OS	Android 6．0
サイズ	146 ㎜×72 ㎜×7.3 ㎜
ディスプレイサイズ	5.2 インチ

7.2 実験結果

被験者ごとの成功数を表 2 に示す．全被験者合わせて 5 回正解し，10 回失敗する結果となり，注視継続率と Web ページの関連付けがうまく行われていないと言える．特に被験者 D に関しては 1 度も正解画像を選択することがない結果となった． 図 6 に成功した被験者ごと，図 7 に被験者 A から C，図 8 に被験者 D から E の失敗したセッションの Web ページ表示時間，画面接触時間，注視継続率を示す．線で囲っている画像は被験者が選択したものである．被験者が正解したセッションの正解画像は Web ページ表示時間，画面接触時間共にダミー画像よりも高い傾向にある．失敗時の特徴として 2 つ挙げられる．1 つ目は Web ページ表示時間，画面接触時間共に低いにも関わらず注視継続率が最も高い画像が正解画像として選ばれた場合には失敗が多いことである．その際，Web ページ表示時間が長い画像が選択されていることが多く見られた．2 つ目は，注視継続率に差があるが，Web ページ表示時間，画面接触時間が正解画像とほぼ同値のダミー画像を選択する場合が多いことである．

表 2 被験者ごとの成功数

		被験者				
		A	B	C	D	E
セッション	1	失敗	成功	失敗	失敗	失敗
	2	失敗	失敗	失敗	失敗	失敗
	3	成功	成功	成功	失敗	成功
成功数		1	2	1	0	1

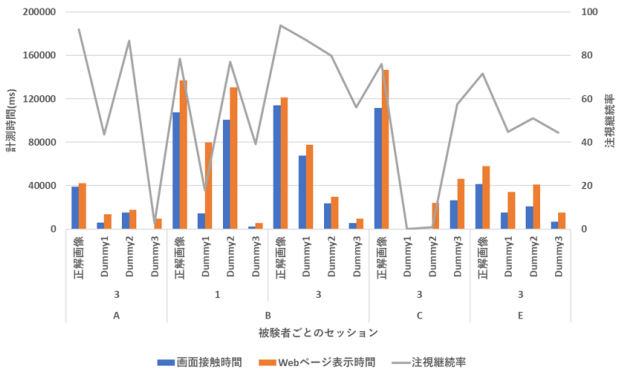

図 6 被験者ごとの成功時データ

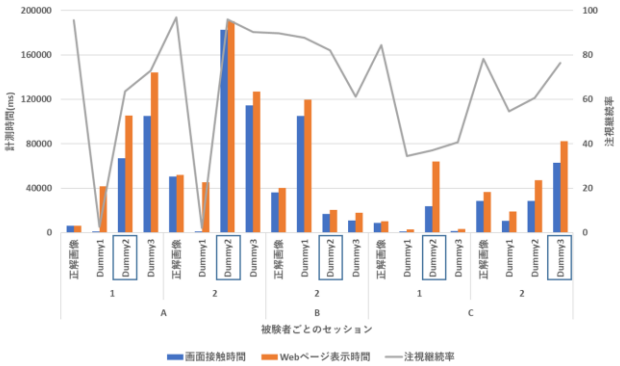

図 7 被験者 A-C の失敗時データ

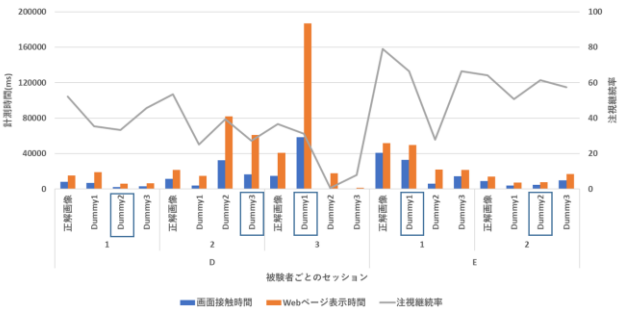

図 8 被験者 D – E の失敗時データ

8. 考察

Web ページ表示時間，画面接触時間共に低いにも関わらず注視継続率が最も高くなっている場合が存在する．これは，被験者は画面を注視しているが，短時間であったため注視継続率が高いものの，Web ページ表示時間が長い他の画像の方が記憶に残ってしまったと考えられる．失敗時に被験者が選択した画像も Web ページ表示時間が長い画像が多い．したがって，Web ページ表示時間は Web ページの注視に関する重要な特徴であるといえる．そのため，一定時間以下の表示時間の Web ページを正解画像候補から除外することや，Web ページ閲覧の際の利用者の行動特徴を用いることで，正解画像と記憶の関連付けを強化・改善する必要がある．

ⓒ 2017 Information Processing Society of Japan

注視継続率には差があるが，Web ページ表示時間・画面接触時間ともに正解画像とほぼ同値のダミー画像を選択する場合がある点について，被験者に「どちらが最も注視した Web ページか」という記憶の混乱が生じ，成功数が下がったと推測できる．このことから，ダミー画像にも選択のための注視継続率に対する閾値を設け，閾値以下の URL を選択することで改善する可能性があると考えられる．また，被験者が 1 セッションの 10 分間に閲覧した Web ページ数が被験者全体の平均で 11 ページと少なかったため，注視継続率が近い Web ページが提示画像群に多く表示され，利用者の混乱を招いている可能性もある．この問題に対する改善策として，以前にブラウザを起動して閲覧した URL も蓄積していくことでダミー画像候補を増やす方法が考えられる．また別の方法として，閲覧した Web ページの URL とそのドメイン，検索画面で表示された数十件の URL とそのドメインを取得し，閲覧していないドメインと対応する URL をダミー画像として抽出する．この方法を用いることによって利用者は最も注視した正解画像と見たことのない Web ページのダミー画像を提示画面で見ることになるため，正解画像の判別が容易となり成功数が上がる可能性がある．

9. おわりに

本研究では利用者の Web ページ閲覧挙動を用いたスマートフォン端末向け認証方式の検討として，ブラウザを用いて利用者が最も注視した Web ページのスクリーンショットを正解画像とし，提示画像群からその正解画像を選択する方式を提案した．これによって，利用者の記憶の負担と登録の煩雑さの軽減ができるため，利便性を保つことができる．また，利用者のプライベートが特定されない画像選択や閲覧するごとに提示画像群が変化するため，安全性も保つことができる．

基礎的な評価実験として，被験者に調べたいキーワードについて Web ページを閲覧してもらい，その後自分が一番注視した URL のスクリーンショットを選択してもらった．結果として全体で 15 回中 5 回正解画像を選択でき，10 回が選択できない結果となり，認証としては低い結果となった．現在の提案手法の課題として注視継続率の見直しやダミー画像の選定方法の見直しが必要である．

今後の課題として，ダミー画像の選定方法に対する改善案の有効性の調査，注視継続率の算出式の見直しを行い，被験者を増やして評価を行う．また，スマートフォン端末での具体的な提示方法についても検討する．また，本提案手法についてのショルダーハッキングの具体的な攻撃に対する耐性の調査，および画像認証特有の攻撃である Educated Guess 攻撃， Intersection 攻撃などに対する調査，対策についても行う必要がある．

参考文献

[1] 総務省:平成 29 年版情報通信白書(オンライン), 入手先〈http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc111110.html〉(参照 2017-10-20)

[2] CREDIT SUISSE: Asia Semiconductor Sector, 入手先〈https://research-doc.credit-suisse.com/docView?document_id=x745069〉(参照 2017-10 - 21).

[3] Chaos Computer Club: Fingerprint Biometrics hacked again, 入手先〈https://www.ccc.de/en/updates/2014/ursel〉(参照 2017-10-15)

[4] Putte T.v.d., and Keuning, J.: Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, Proc.4th Working Conference on Smart Card Research and Advanced Applications(CARDIS2000), pp.289-303 (2001).

[5] Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Proc. SPIE, Vol.4677, pp.275-289 (2002).

[6] Cao, K., and Jain, A.K.: Hacking Mobile Phones Using 2D Printed Fingerprints, MSU Technical Report, MSU-CSE-16-2 (2016).

[7] Dhamija, R., and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, Proc.9th conference on USENIX Security Symposium(SSYM'00), pp.45-58 (2000).

[8] 高田司, 小池英樹：あわせ絵：画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法,情報処理学会論文誌, Vol.44, No.8, pp.2602-2612 (2003).

[9] 西垣正勝, 小池誠：ユーザの生活履歴を用いた認証方式 -電子メール認証システム,情報処理学会論文誌, Vol.47, No.3, pp.945-956 (2006).

[10] 花井將臣, 中村逸一, 吉田英樹, 曽我正和, 西垣正勝：経験による想起の容易さを利用した認証方式, 情報処理学会研究報告, Vol.2004, No.22(2003-CSEC-024), pp.193-198 (2004).

[11] 土方嘉徳: 嗜好抽出と情報推薦技術, 情報処理, Vol.48, No.9, pp .957-965(2007).

[12] 岩崎宰守: スマホのネット利用はアプリとブラウザに 2 極化～ニールセン調査, INTERNET Watch, 入手先〈https://internet.watch.impress.co.jp/docs/news/1048729.html〉(参照 2017-10-21).