SCIS 2020 2020 Symposium on
Cryptography and Information Security
Kochi, Japan, Jan. 28 – 31, 2020
The Institute of Electronics,
Information and Communication Engineers

ブラウザの閲覧履歴に基づく Web ページのスクリーンショットを利用した画像認証における実用性の検討

Evaluation of Practicality in Image Based Authentication Using Screenshots of Web Pages Based on Browsing History

飯澤悠介 * 中村嘉隆 † 稲村浩 †
Yusuke Iizawa Yoshitaka Nakamura Hiroshi Inamura

あらまし スマートフォンの普及に伴い，不正利用による個人情報の閲覧・流出の危険性が懸念されている．現行の個人認証手法である知識による認証にはトレードオフ，身体的特徴による認証には不変なデータであるが故の複製等の問題があるため，不変なデータを利用せず，安全性を保持した認証が必要である．本研究では，行動履歴であるブラウザの閲覧履歴を利用して Web ページのスクリーンショットを取得し，それらを秘密情報とした画像認証を提案した．利用者がブラウザで閲覧した Web ページを正解画像，未閲覧の Web ページを不正解画像として混在させて提示することにより，利用者のみが知りえる情報を利用した秘密情報を更新可能な認証が可能となる．本稿では，日常利用を想定した実験と推測攻撃に対する耐性の検証を行った．日常利用を想定した実験の結果，ブラウジングから 1 時間後，5 時間後，24 時間後以降の間隔の認証は高い認証成功率で認証可能であることを示した．推測攻撃は，利用者の情報を利用しない場合と利用する場合の両方を行い，どちらの場合も攻撃者による正解画像の推測は困難であることがわかった．

キーワード 画像認証，行動履歴認証，Web ページ，スクリーンショット，個人認証

1 背景

近年のスマートフォンの普及は著しく，先進国ではスマートフォン所持率が 2018 年で平均 76 %となっている [1]．スマートフォンは，e-コマース・電子メール・ソーシャルネットワークなど様々なオンラインサービスにアクセスするための重要なモバイル機器として位置づけられつつある．加えて，QR コード決済環境の普及により，決済アプリを利用する場面も増えている．これらのサービス利用のためにユーザ情報やパスワードを端末内に保存する機会が多くなっている．また，端末ストレージの大容量化に伴い，写真や知人の連絡先，スケジュール等の様々な個人情報が端末内に保存されるようになってきており，端末へのアクセスに関するセキュリティが課題となりつつある．

スマートフォンはその特性から，ネットワーク接続可能な状況であればどのような場所も操作される．そのため，不特定多数の人々が存在する公共の場での利用が多くなることが想定され，端末の盗難等により端末内部のデータへアクセスされる危険も高まる．前述のように端末内部データには個人情報も多く含まれるため，端末の盗難が，QR コード決済アプリの不正利用や個人情報の暴露などにつながる危険性が高くなる．そのため，盗難時にも端末内データの安全性を確保するために，端末利用に際して高いセキュリティ強度をもつ利用者認証手法を備える必要がある．

スマートフォンの個人認証手法として、「本人の知識による認証」と「本人自身の特徴による認証」の 2 つが一般的に利用されている．

「本人の知識による認証」は，PIN(Personal Identification Number)，文字列パスワード認証，パターン認証など利用者が任意で秘密情報を設定する認証手法を指す．この認証手法は，スマートフォンの安全性を重視すると，十分な強度である複雑な秘密情報を設定する必要がある．これによって覗き見攻撃や推測攻撃など，利用者の行動を観察・把握して攻撃する手法への安全性は向上するが，記憶負担の増加および煩雑な認証操作を必要とする．反対に単純な秘密情報を設定した場合，記憶負担が少なく，

* 公立はこだて未来大学大学院システム情報科学研究科, 北海道函館市亀田中野町 116 番地 2, 116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, Japan.
† 公立はこだて未来大学システム情報科学部, 北海道函館市亀田中野町 116 番地 2, 116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, Japan.

前述の攻撃手法に脆弱になる．PC のパスワードを単純に設定する傾向 [2] があるため，スマートフォンでも同じ傾向があると考えられる．スマートフォンは，持ち運び可能な小型モバイル機器であるため，端末の認証操作は不特定多数の人間が混在する場所で行われる．そのため，覗き見攻撃や推測攻撃への耐性のある複雑な秘密情報を用いつつ，記憶負担や認証操作負荷を最小限にするような認証手法が必要となる．

「本人自身の特徴による認証」は，生体認証と呼ばれている．指紋，虹彩，顔など身体的特徴を秘密情報として設定する認証手法を指す．現在のスマートフォンには主に指紋認証が多く導入されている [3]．指紋認証は認証機器に認証対象部位を接触させることで，事前に登録した利用者の指紋データと照合し，利用者を識別する．指紋認証は秘密情報の入力動作が「接触」という最小限の動作だけであり，利便性が高い．反面，不変であるデータを利用するという問題がある．採取した指紋による指紋の複製 [4] や「DeepMasterPrints」と呼ばれる様々な人物の指紋になりすませる手法 [5] も存在するため，不変であることがセキュリティリスクになりうる．したがって，身体的特徴に替わりうるような，利用者の特徴を表すデータを利用した認証手法を利用する必要がある．

本研究では，不変な身体データを利用せず，安全性を保持した新たな個人認証手法の提案を目的とし，ブラウザの閲覧履歴に基づいた Web ページのスクリーンショットを利用した認証手法を提案した．この認証手法について日常利用を想定した認証可能性および推測攻撃への耐性について検証した．長時間利用しない期間を設けても 1 日単位であれば認証可能であり，推測攻撃にも耐性があることを示した．

2　関連研究

2.1　画像認証

記憶負荷の低減、認証操作負荷の低減を基本とした個人認証手法として、画像認証が研究されている．画像認証の基本的な手続きを図 1 に示す．個人認証のたびに，利用者に対して正解画像と囮となる複数枚の不正解画像を含んだ提示画像群を認証画面で提示する．その中から適切な画像を選択した場合は認証成功，それ以外の場合を選択した場合は認証失敗となる．画像には人間の記憶に対して以下のような効果がある [6].

1. 文章と比較して記憶可能な量が多い
2. 文章と比較して画像の記憶保持期間が長い

このように文章に比べて画像に対する記憶が優れていることは「画像優位性効果」[7] と呼ばれている．この効果により，画像認証は「本人の知識による認証」に対して，記憶負担の面で優位性があると言われている.「Deja Vu」[8] では，提示された複数の幾何学模様の人工画像の中から，5 枚を正解画像として登録し，これを用いた認証を行っている. 個人認証時には、不正解画像群と正解画像がランダムに提示され，5 枚の正解画像を正しく選択することで認証成功とする．しかし，意味を持たない幾何学模様の人工画像では記憶が困難であることから，Deja Vu を発展させた「あわせ絵」[9] が考案されている．この「あわせ絵」は人工画像の代わりに，カメラ付き携帯端末で撮影した写真を利用している．利用者が経験した画像を用いるという形で，最も忘れにくく，思い出しやすいエピソード記憶の考えを取り入れている．しかし、画像認証を行うためには、利用者が事前に大量の画像を収集し、登録する手続きが必要になるため，この一連の手続きが利用者への負担となる．

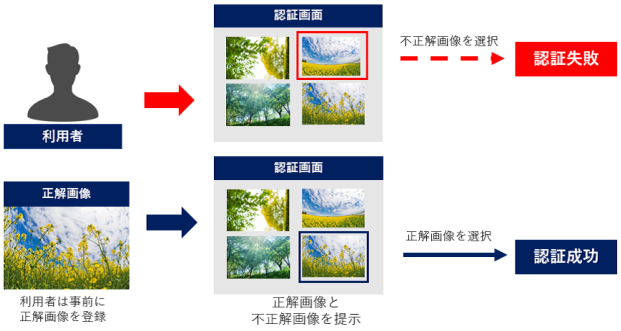

図 1: 画像認証の基本的な手続き

2.2　行動履歴認証

不変なデータを利用しない個人認証手法として，スマートフォンのセンサ情報によって利用者の行動履歴を取得し，この情報を元にして暗黙的な個人認証を行う研究がある [10][11]．しかし，行動を基にした個人認証は周囲の環境，利用者の状態に大きく左右される場合がある．そこで，前日の朝食や訪れた店舗の情報等，利用者の主観的な経験情報を明示的に提示して個人認証を行う行動履歴認証の研究が行なわれている．明示的な行動履歴の特徴として，日常生活の中で常に変化が発生するため，他者が正確に行動履歴を取得することが困難であることが挙げられる．認証においては新しい行動履歴を適切に選択することで変化する認証情報として利用できる. 明示的な行動履歴を用いた認証の 1 つとして電子メールの履歴を用いた認証 [12] 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利用者が選択することで認証を行っている．また，Ngu らは利用者が頭や胸ポケットに着用したカメラデバイスなどで，日常を利用者目線で記録した映像を用いて認証を行う「PassFrame」を提案した [13]．記録した映像から代表的な場面を抽出し，利用者の時間的な情報に関する暗

黙的な知識を用いて認証を行っている．明示的な行動履歴認証は，利用者の個人情報に結び付きやすいため，それらの情報に繋がらない適切な行動履歴を用いる必要がある．

3 行動履歴に基づく画像認証

3.1 アプローチ

画像認証に備わる記憶負担の軽減と行動履歴認証に備わる知識による認証の安全性を複合させ，双方の利点を活かす．

スマートフォン利用時において得られる行動履歴には Web ページ閲覧履歴，アプリ利用履歴，動画像撮影履歴等がある．このうち，アプリ利用履歴や動画像撮影履歴は情報そのものに個人情報が多く含まれるため，認証時に秘密情報として用いることは適切ではない．一方，多くの Web ページは公開を前提としたものであるため，ある種の個人的な Web ページやセンシティブな履歴を排除することで，Web ページ閲覧履歴の情報を認証に用いることができる．また，閲覧履歴情報から画像を選出するため，画像認証における正解画像の登録を不要にできる．このことから，Web ページ閲覧履歴に基づく画像を用意し，画像認証に用いることとした．

Web ページ閲覧履歴に基づく画像として，Web ページ内に埋め込まれている画像が考えられる．しかし，Web ページ内の画像を利用者が必ず閲覧しているとは限らず，埋め込み画像の量によって想起が困難になる可能性がある．また，画像が埋め込まれていない Web ページも存在するため，その Web ページが正解画像の対象となると，秘密情報としての画像を抽出できないことが考えられる．そこで，Web ページのスクリーンショットを画像として利用する．スマートフォンの標準ブラウザを使用して Web ページの閲覧操作を実行したときに取得できるスクリーンショットには，次の利点がある．

1. 自発的に閲覧した Web ページを利用可能
2. 文章や Web ページのレイアウトが含まれるため，利用者の想起の補助となる
3. 基本的に画像を含まないあらゆる Web ページに対しても確実に画像として取得することが可能

3.2 課題

Web ページ閲覧履歴に基づく画像認証のアプローチを行うには，選定した情報に基づく認証のための正解画像および不正解画像の選出方法が課題となる．

認証時に利用する画像は利用者が鮮明に記憶していることが求められるため，受動的な閲覧ではなく，自発的な閲覧に基づくものが望ましい．また，利用者自身に深い関係がありながら，利用者の特定は難しい履歴情報から選定する必要がある．

認証時の正解画像は．利用者が記憶から正しく想起することが可能である必要がある．関連研究 [8][9] では，利用者自身が正解画像を登録する作業が必要であるため，正解画像の想起が容易である．しかし，閲覧履歴情報から正解画像を取得する場合，利用者が画像登録作業を行わないため，利用者は認証画面に提示されて初めて正解画像を目にすることになる．そのため，閲覧履歴から利用者の記憶にはっきり残っているような正解画像の選出が必要である．

一方，不正解画像は，利用者にとっては正解画像と峻別しやすくなっていることが必要である．関連研究 [8][9] では利用者が登録した画像群から正解画像として登録したもの以外を不正解画像として用いている．利用者は正解画像を意図的に登録しているため，正解画像と不正解画像との峻別は容易である．しかし，閲覧履歴情報に基づく選出を行う場合は，正解画像と同様認証画面に提示されて初めて目にするため，正解画像と類似した不正解画像の場合は認証成功率の低下や認証操作時間の増大などが考えられる．したがって，不正解画像としては，利用者の記憶内で正解画像と大きな相違があるような画像を用意する必要がある．また，他者から見た場合には正解画像と不正解画像に差がないような画像を用意する必要もある．

4 提案手法

4.1 正解画像選出

利用者に負担をかけず，各 Web ページの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手法が存在する [14]．Web ページの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，利用者が注視していた可能性が高いといえる．そのため，利用者が想起し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，Web ページ閲覧時に画面に親指を接触させる動作を行っている間は利用者がスマートフォンの画面に表示された Web ページに注視しているとした．画面に親指を接触させた時間を画面接触時間と定義し，画面接触時間の長い Web ページを選出することで, 利用者の負担を増大させずに Web ページが取得可能となる．また，ブラウザ閲覧を行いながら自動的に正解画像を選ぶことも可能になる．スマートフォンでの Web ページ表示時間と画面接触時間から注視の度合いで

ある注視継続率を以下の式で算出する．

$$\text{注視継続率} = \frac{\text{閲覧時間 (ms)}}{\text{Web ページ表示時間 (ms)}}$$

利用者がブラウザを終了するまでに閲覧した Web ページから、最も高い値を持つ Web ページを最も注視して閲覧したものとみなし，Web ページのスクリーンショットを取得して正解画像とする．

4.2 不正解画像選出

不正解画像は, 利用者にとって正解画像と峻別が可能であり，他者にとっては区別が困難であることが重要である．注視継続率の低い閲覧済みの他の Web ページを不正解画像として用いた場合，正解画像・不正解画像に選出された Web ページの内容によっては，利用者が正解画像・不正解画像を混同するおそれがある．したがって，記憶の混乱を防止し，正解画像との明確な峻別を行うために，不正解画像として未閲覧 Web ページの画像を提示する．本研究では検索キーワードとの意味的距離に基づいた不正解画像選出手法を提案する．正解画像として選出された Web ページを閲覧した時の検索キーワードに対し，Word2Vec[15] と学習済み日本語モデルを利用することで，正解画像の検索キーワードと意味的に離れたキーワードを発見する．この過程により，正解画像と異なる検索キーワードを用いて不正解画像を選出することで，正解画像との明確な峻別が容易になると考えられる．Word2Vec は，文の集合を入力とし，注目単語の近傍に現れる単語から注目単語のベクトル表現を学習する．正解画像選出で用いるキーワードと不正解画像選出で用いるキーワードをそれぞれ異なるキーワードにすることで，正解画像と不正解画像の内容が類似することによる記憶の混乱を防ぐ．選出手法の流れを図 2 に示す．本研究では白ヤギコーポレーションが提供している学習済み日本語モデル [16] を利用した．正解画像として選出された Web ページを閲覧した際の検索キーワードを入力とし，学習済みの日本語モデルと Word2Vec を利用して，検索キーワードを入力として Cos 類似度を求め，意味的な距離が離れたキーワードを一定数取得する．それぞれのキーワードの検索結果からランダムに 1 件ずつ URL を取得する．その後，それぞれの URL から Web ページのスクリーンショットを取得する．

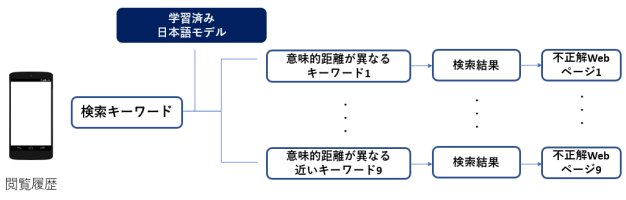

図 2: 検索キーワードとの意味的距離に基づいた不正解画像選出手法

5 日常利用を想定した実験

日常利用のモデルケースを想定して，1 日にブラウザの閲覧から認証までの間に間隔を設けてからの認証を行い，1 日単位の認証が可能かの実験を行った．日常利用のモデルケースとして，職場や学校などの私用スマートフォン禁止時間帯後の認証と起床後の認証を想定した．スマートフォンの利用時間帯のピーク時が，7-8 時台，12 時台，17 時台，22 時台 [17] である事から，ブラウザの閲覧が終了してから認証を行うまでの時間間隔を 1 時間後，5 時間後，24 時間後以降と設定した．24 時間後以降の場合，被験者に認証時間は設定せず，自由な時間に認証を行った．全被験者の時間帯ごとの認証成功率から，スマートフォン操作不可だと考えられる一般的な勤務・授業時間帯の間隔をあけても認証可能であること，全被験者の時間帯ごとの確信度と認証成功数から，利用者自身が高い確信度をもって正解画像を認識していることを評価する．

5.1 実験方法

被験者は 22 24 歳の大学生と大学院生で，男性 4 名，女性 1 名の計 5 名である．以下の実験手順を被験者 1 人に対して行った．

1. 被験者は初めに検索するキーワードを 3 つ決める．条件として，被験者が興味を持っているキーワードかつ学習済み日本語モデル内にキーワードが存在するとした．

2. 1. で決めた 3 つのキーワードごとに 10 分間ブラウジング

3. X(1 時間後，5 時間後，24 時間後以降) の間隔ごとに正解画像 1 枚、不正解画像 9 枚の認証画面を提示して認証操作

4. それぞれの時間帯の認証操作ごとに，確信度 (5:最も自信がある 1:最も自信がない　の 5 段階評価) とその理由をアンケートに回答

閲覧に利用したスマートフォンを表 1 に示す．正解画像の選出に必要な注視継続率の算出は実験者が作成したブラウザアプリケーションで行った．不正解画像 Web ページの選出，正解画像と不正解画像のスクリーンショット取得は PC で処理を行った．認証画面の提示は正解画像 1 枚，不正解画像 9 枚の合計 10 枚の提示画像群を俯瞰して見られるような形で被験者に送信した．それぞれの提示画像に番号が振られており，被験者は正解画像だと思う画像の番号とその理由を作成したフォームに回答する形で行った．

表 1: 実験用スマートフォン

Device name	VAIO Phone A VPA0511S
OS	Android 6.0.1
External dimensions	77.0 mm x 156.1 mm x 8.3 mm
Display size	5.5inch
Resolution	1080 x 1920

5.2 実験結果

被験者ごとの認証結果を表 2 に示す．認証結果から，5 日間の認証成功率が被験者 1,2,4,5 は 100%，被験者 3 が 93%と高い認証成功率を維持している結果となった．各時間間隔ごとの確信度と認証結果の度数を図 3 に示す．どの時間間隔の場合も被験者は 5，4 と高い確信度で正解画像を選択できていることがわかった．しかし，5 時間後の確信度が 1 で認証成功の場合と，各時間間隔にど中程度の確信度である 3 で認証を成功している場合が見られた．また，低い確信度で失敗の場合が見うけられた．

表 2: 被験者ごとの認証結果

	Day1			Day2			Day3			Day4			Day5		
	1	5	24	1	5	24	1	5	24	1	5	24	1	5	24
被験者1	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
被験者2	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
被験者3	S	S	S	S	S	S	S	S	S	S	S	S	S	S	F
被験者4	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
被験者5	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

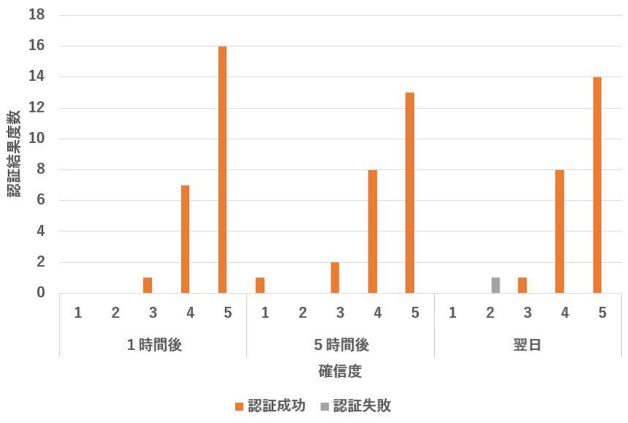

図 3: 各時間間隔ごとの確信度と認証結果の度数

5.3 考察

5 日間を通して，1 時間後，5 時間後，24 時間後以降で高い認証成功率と確信度を維持出来ていた点から，スマートフォンの操作を行わない時間帯を経た後でも認証成功が可能であり，1 日単位の認証は問題なく利用できると考える．

低い確信度と中程度の確信度で認証成功していた場合，被験者のアンケートでの回答から，確信度 3 では類似画像の出現や，消去法で選んだと回答があった．これらの回答から，正解画像の記憶があいまいであったとしても，未閲覧の検索キーワードを利用する不正解画像選出により，選択の補助的効果が生まれていると考えられる．例えば，正解画像がすぐにわからない場合，被験者自身が調べる可能性が低い画像を内容やスクリーンショット内の画像，タイトル等で判断することで，正解画像へ導くという効果である．これは，不正解画像選出で重視した正解画像との峻別が大きく影響していると推測．確信度 1 に関しては，選択理由が「はっきり覚えており，他の画像を見た覚えがない」と回答しているため，確信度の記入ミスの可能性が考えられる．低い確信度で失敗している場合，実験以外で閲覧した Web ページと混同したという回答が得られた．今回は実験用のスマートフォンを利用しため，被験者自身が所持するスマートフォンで閲覧した Web ページが影響してしまったと考えられる．今回の状況を日常生活で考えた場合，自分のスマートフォン以外のスマートフォンでブラウザの閲覧を何度もする状況は限られるので，異なるスマートフォンで閲覧した内容と混同するという影響は少ないと考える．

6 推測攻撃への耐性実験

6.1 個人認証が直面する脅威

スマートフォンのロックスクリーンに搭載する個人認証はセキュリティを強固にする必要がある．特に，利用者以外の人物の攻撃に耐性がなければならない．本研究において，利用者以外の人物が行うと考えられる攻撃手法として Intersection 攻撃，Observation 攻撃，推測攻撃，Blute-Force 攻撃の 4 つが考えられる．

Intersection 攻撃は，提示画像群の中に「正解画像が 1 枚存在する」という前提のもと行われる．複数回の認証行為で表示された画像の登場頻度や積集合を求めることで，正解画像を特定する攻撃である．Observation 攻撃は，利用者の認証行為を覗き見し，正解画像を特定する攻撃である．推測攻撃は，提示画像群の内容から正解画像を推測する攻撃である．特に，事前に入手した利用者の情報から，正解画像を推測する攻撃を Educated Guess 攻撃という．Blute-Foece 攻撃は，全ての画像の組み合わせで正解画像を推測する攻撃である．

本研究において，最も脅威となる攻撃手法として Educated Guess 攻撃が挙げられる．提示画像群として Web ページのスクリーンショットを利用するため，利用者の趣味や趣向が反映されやすくなっている．写真とは違い，文章，写真等多くの情報が 1 枚の画像に表示されるため，これまでの画像認証で用いられているような画像よりも情報量が多い．したがって，攻撃者により多くの情報を渡してしまい，利用者の情報と比較しやすくなっている．ゆえに，正解画像の推測が容易になっていると考えられる．Educated Guess 攻撃がどの程度通用するのかを検証

する必要がある．

6.2 実験目的

推測攻撃の耐性の実験は，攻撃者が窃取を想定した「利用者の情報を持っていない」シチュエーションと友人や近親者を想定した「利用者の情報を持っている (Educated Guess 攻撃)」シチュエーションの 2 つを行った．攻撃者が利用者の情報を持っていないシチュエーションでは，Web ページのスクリーンショットの内容の差異だけで正解画像を推測可能かを評価する．利用者の情報を持っているシチュエーションは，利用者情報を利用して Web ページのスクリーンショットから正解画像を推測可能かを示す．本手法において，推測攻撃の耐性と攻撃者が利用者のどのような情報を利用して攻撃を行うのかを検証する．

6.3 実験方法

本実験は，被験者ごとに行う前準備と攻撃者ごとに行う攻撃実験の 2 プロセスで構成される．

6.3.1 前準備

被験者は男子大学生 1 名，男子大学院生 2 名であった．被験者は最初，表 3 のアンケートに回答する．次に，検索キーワードには現在興味があり，学習済み日本語モデル内に存在するという制約を設けた上で，各被験者は各自が検索する検索キーワード 4 つを決定する．被験者はそれぞれの検索キーワードごとに 10 分間のブラウジングを行う．提案システムはこのデータをもとに，検索キーワードごとに正解画像 1 枚，不正解画像 9 枚を選出する．不正解画像は正解画像に対し Cos 類似度を 0.05 ずつ離したキーワードから得られる Web ページのスクリーンショットとする．最後に，正解画像 1 枚・不正解画像 9 枚を混在させた提示画像群を各検索キーワードごとに俯瞰できる形で作成する．

表 3: アンケート項目

質問	
名前	情報の入手方法
出身地	1日のインターネット利用時間
趣味	休日の過ごし方
1日の過ごし方	課題としている事，チャレンジしたいこと
よく閲覧するWebサイト	ブラウザの主な利用目的
最近の関心事	最近スマートフォンのブラウザを利用して調べたキーワードとその理由

6.3.2 攻撃実験

攻撃者は大学生 4 名で行った．まず利用者の情報を持っていないシチュエーションにおける攻撃について評価を行う．攻撃者に前準備で作成した正解画像 1 枚，不正解画像 9 枚の提示画像群を紙または PDF で提示する．攻撃者は，その中から正解画像だと思われる画像を推測し，選択する．その後，攻撃者は正解画像の選択理由をアンケートに回答する．アンケートの選択理由が勘であったら理由なしを選択，明確な理由がある場合は理由ありにその理由は記述する．この流れを被験者 1 人につき前準備で決定した 4 つの検索キーワードごとに行う．

次に，利用者の情報を持っているシチュエーションにおける攻撃について評価を行う．攻撃者に，被験者が回答したアンケート内容を被験者の個人情報として提示した．この個人情報は，被験者個人の特定による攻撃成功率の増加を避けるため，名前情報を削除している．次に，攻撃者に前準備で作成した提示画像群を提示する．攻撃者は，その中から利用者の情報を駆使して正解画像だと思われる画像を推測し，選択する．正解画像の選択回数は 1 回のみに定めた．その後，攻撃者は正解画像の選択理由をアンケートに回答した．アンケートは選んだ理由が勘であったら理由なしを選択，明確な理由がある場合は参考にした項目を複数回答可能で選択した．この流れを被験者 1 人につき 4 つの検索キーワードごとに行う．

利用者の情報を持っていないシチュエーションを終了した後，攻撃者に選択した画像が正解画像であるかの情報は与えなかった．したがって，その後の利用者の情報を持っているシチュエーションの正解画像の推測に影響がないよう実験を行った．

6.4 実験結果

攻撃者が被験者の 1 つの検索キーワードで構成された提示画像群を推測する行為を“Phase”と表記した．図 4 に正解画像の選択理由なしを除いた被験者の Phase ごとの推測成功数をグラフで示す．被験者の情報を持っていない場合，攻撃者は選択した画像が正解画像である明確な理由を推測して認証成功した Phase はなかった．被験者の情報を持っている場合は，推測が成功している Phase があり，被験者の情報を持っていない場合と比較して推測成功数が増加している．

表 4 に利用者の情報を持っている場合のシチュエーションの全 Phase での攻撃結果を示す．被験ごとの 1 から 4 までの数値はそれぞれ Phase1 から Phase4 を表している．ここで，”S”が攻撃成功，”F”が攻撃失敗を表す．どの攻撃者も被験者の 4 つの Phase を全て推測し，認証成功することができなかった．また，被験者 3 の Phase2 については，すべての攻撃者が推測に成功していた．

図 5 に推測が成功した場合に攻撃者が利用した情報のアンケート結果である．趣味に関する情報を利用した場合が一番多く，次いで，最近の関心事，よく閲覧する Web サイトが用いられていた．

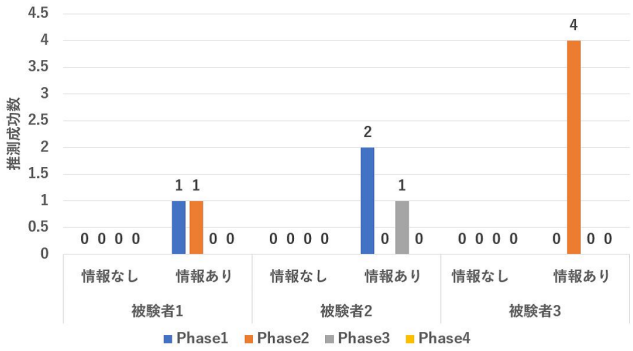

図 4: 被験者の Phase ごとの推測成功数

表 4: 攻撃者ごとの各被験者における攻撃結果

	被験者1				被験者2				被験者3			
	1	2	3	4	1	2	3	4	1	2	3	4
攻撃者1	F	S	F	F	S	F	F	F	F	S	F	F
攻撃者2	F	F	F	F	S	F	S	F	F	S	F	F
攻撃者3	F	F	F	F	F	F	F	F	F	S	F	F
攻撃者4	S	F	F	F	F	F	F	F	F	S	F	F

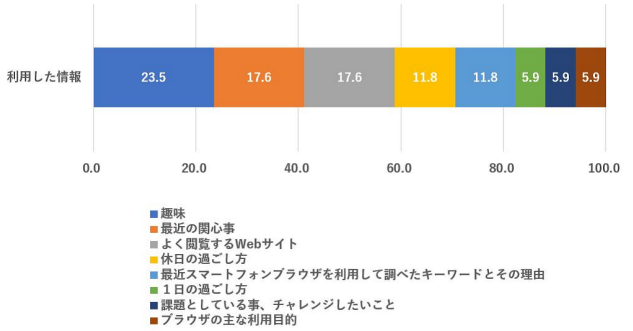

図 5: 攻撃者が推測に利用した情報の割合

6.5 考察

利用者の情報を持っていない場合，推測成功した回数は攻撃者全体で 0 回だったことから，本手法において，攻撃者は利用者の情報がなければ正確に正解画像を推測することは困難であると考えられる．一方，利用者の情報を持っている場合，正解画像を推測する場合が増加することわかった．このことから，情報をもとに推測することは可能であることが言える．しかし，正解画像を選択する操作を 4 回行う個人認証を行う (PIN と同等) を考えると，攻撃者が被験者のすべての Phase を正確に推測できる可能性は低いことが考えられ，認証の安全性に脅威を与えるほどの結果を得られない．また，利用者の情報を持っている場合，被験者 3 の Phase3 が全攻撃者が推測に成功している．この部分に関しては，被験者のアンケートの趣味に記述されていた内容と，正解画像の内容が一致していたためであった．今回の実験では，アンケートの内容は近親者や友人が知りうるう情報よりも詳細に記述されているため，利用者の人物像を深く知りうる人物による攻撃は成功する可能性があるものの，関係の薄い他者による攻撃に関しては攻撃成功の可能性は低くなると考えられる．推測成功時に利用した情報として，趣味，よく閲覧する Web サイト，最近の関心事があることがわかった．本手法の場合，正解画像の選出時にユーザが主観的によく閲覧する Web サイト，頻繁に検索されるキーワードを除外することで，攻撃者の推測を妨げることができると考えられる．趣味に関しては，利用者の興味を利用している限り，利用者の想起と密接しているため，完全に対策することは困難である．したがって，認証回数ごとに趣味によらない異なる意味に属するキーワードを用いて提示する必要があると考えられる．例えば，Phase1 で日常何気なく料理に関して調べた場合の提示画像群，Phase2 が興味のある本に関して調べた提示画像群という提示方法である．

7 まとめ

本研究では，記憶負荷の低減，操作負荷の低減と不変データを利用しないことを目的に，ブラウザでの閲覧済み Web ページのスクリーンショットを利用した画像認証を提案した．この認証の課題として，正解画像の選出，不正解画像の選出があった．正解画像は利用者の注視継続率が最も高い Web ページのスクリーンショット画像を用いた．不正解画像の選出は，検索キーワードとの意味的距離に基づいた不正解画像選出手法を提案した．日常利用を想定した認証では，1 時間後，5 時間後，24 時間以降で高い認証成功率と確信度を維持していたことから，1 日単位の認証は問題なく利用できるとわかった．推測攻撃への耐性実験では，攻撃者は利用者の情報がなければ正確に正解画像を推測することが困難であることがわかった．また，利用者の情報を攻撃者が把握していたとしても，認証の回数を考慮することで安全性に脅威を及ぼす影響が得られないことが判明した．さらに，攻撃者は利用者の趣味の情報を主に活用しており，対策を行うことで更なる安全性向上に期待が持てることがわかった．

今後の課題として，Intersection 攻撃，Blute-Force 攻撃，Observation 攻撃などの攻撃に関する耐性の検証を行う．

参考文献

[1] Pew Research Center, ”Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally,” <https://www.pewresearch.org/global/2019/02/05/smart

phone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/> [2019-12-15].

[2] Splashdata, ”The Top 50 Worst Passwords of 2018,” <https://www.teamsid.com/100-worst-passwords-top-50/> [2019-12-15].

[3] statista, ”Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018 ”, <https://www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/> [2019-12-15].

[4] K. Cao A.K. Jain,”Hacking Mobole Phones Using 2D Printed Fingerprints,” MSU Technical Report, MSU-CSE-16-2, 2016.

[5] P. Bontrager, A. Roy, J. Togelius, N. D. Memon, and A. Ross, ”DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution,” Proceedings of the IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS2018), 2018.

[6] 高橋知世，北神慎司，宮代こずゑ，原田悦子，須藤智，“画像認証システムによる本人認証 (1) : 登録画像の選択に影響を及ぼす要因の検討”，情報処理学会研究報告，Vol.2012-SPT-3，No.1，pp.1-8，2012.

[7] 新美亮輔, 上田彩子, 横澤一彦，“オブジェクト認知 統合された表象と理解，シリーズ総合的認知”，勁草書房，Vol.2，pp.69-70，2016.

[8] R. Dhamija and A. Perrig,”Déjà Vu: A User Study Using Images for Authentication,” Proceedings of the 9th conference on USENIX Security Symposium(SSYM’00), pp.45-48, 2000.

[9] 高田哲司，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.2002-2012，2003.

[10] 味岡孝昇，梅澤猛，大澤範高，“暗証番号入力時の腕の加速度を用いた携帯端末向け個人認証”，Vol.2016-MBL-81，No.22，pp.1-6，2016.

[11] 山田健一朗，納富一宏，斎藤恵一，“スマートフォン操作時における行動的特徴量を利用した個人識別手法”，バイオメディカル・ファジィ・システム学会誌，Vol16，No.1，pp41-48，2014.

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

[13] N. Nguyen, and S. Sigg, ”PassFrame: Generating image-based passwords from egocentric videos”, Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017.

[14] 土方嘉徳，“利用者の好みをとらえ活かす-嗜好抽出技術の最前線- : 1. 嗜好抽出・情報推薦の基礎理論 1）嗜好抽出と情報推薦技術”，情報処理，Vol.48，No.9，pp.957-965，2007.

[15] T. Mikolov, I. Sutskever, K. Chen, G. Corrado, and J.Dean, ”Distributed Representations of Words and Phrases andtheir Compositionality”, Neural Information Processing Systems2013, pp.3111–3119, 2013.

[16] 株式会社白ヤギコーポレーション，“日本語 word2vec モデル” ，<https://github.com/shiroyagicorp/japanese-word2vec-model-builder>[2019-12-15].

[17] 総務省，“平成 30 年度 情報通信メディアの利用時間と情報行動に関する調査” ，<https://www.soumu.go.jp/main_content/000644166.pdf>[2019-12-15].