「マルチメディア，分散，協調とモバイル
(DICOMO2018) シンポジウム」 平成30年7月

Webページ閲覧履歴に基づく スマートフォン端末向け画像認証システム

飯澤 悠介[1]　中村 嘉隆[2]　稲村 浩[2]

概要：スマートフォン端末の普及が増加しており，不正利用・情報漏洩の危険性から端末の不正利用対策が重要となっている．現行のスマートフォン端末には利便性と安全性の間にトレードオフの問題が存在するため，画像認証と履歴情報を用いた認証を複合させ，履歴情報から画像を選出する認証を行う．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画像として用いる，利用者の注視継続率が最も高い Web ページを正解画像，正解画像を検索した際の検索キーワードの検索結果から未閲覧の Web ページを不正解画像としたをシステムを提案した．実験では正解画像 1 枚と不正解画像 9 枚の提示画像群から正解画像を選択する認証実験を行い，全体の認証率が 67%という結果で低い結果となった．選択時間が全体で平均 16.9 秒，認証成功のみでは平均 14.8 秒という結果を得た．注視継続率は不正解画像との峻別が可能な正解画像を選択できており，失敗する原因として閲覧時間，正解画像と酷似したレイアウト・内容の不正解画像が影響していることがわかった．また，選択時間においては関連研究よりも長く，利便性を低下させる可能性があることがわかった．

Image based authentication system using Webpage browsing history for smartphone device

YUSUKE IIZAWA[1]　YOSHITAKA NAKAMURA[2]　HIROSHI INAMURA[2]

1. はじめに

近年，スマートフォン端末やタブレット端末など、タッチパネルを有した携帯端末，特にスマートフォン端末の普及が増加している．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．スマートフォン端末はその形状や機能性ゆえに，ネットワークに接続可能な環境であれば，不特性多数の人々が存在する飲食店や電車などの公共交通機関でも端末操作を行う傾向がある．このような状況では，覗き見によって端末の認証操作に用いるパスワード等の情報を他者に知られ，端末を不正利用される危険性も増大する．また，スマートフォン端末では個人に結びつく情報を多く保存していることから，情報漏洩の危険性も大きい．そのため，端末の不正利用対策が重要となる．

一般的なスマートフォン端末の不正利用対策として画面ロック機能がある．端末起動時に既定の認証行為を行うことによってユーザ認証を行う．現在主流な認証方法には，生体認証，英数字を用いたパスワード認証や数字を用いた個人識別番号 (PIN:Personal Identification Number) などを含めた固定式パスワード認証がある．

生体認証は，利用者の虹彩や顔，指紋など身体的特徴の情報をあらかじめ端末に登録し，認証時に端末の各種センサから取得した生体情報と照合して個人識別を行うことで利用者の認証を行う．現在のスマートフォン端末では指紋認証が主流となっており，指紋センサのスマートフォン端末への搭載普及率は 2018 年で 2/3 を超えると予想されている [2]．一般的に認証装置に認証対象部位である指を読み取らせるのみであるため，利便性は高いといえる．しかし，成長や受傷などによる認証対象部位の損傷・変化や手袋やマスクなど認証対象部位を覆う装着物の影響で認証が不可能となる場合がある．一方，固定式パスワード認証は，利用者が前もって定めたパスワードを登録しておき，認証

[1] 公立はこだて未来大学大学院システム情報科学研究科
[2] 公立はこだて未来大学システム情報科学部

時に利用者に該当パスワードを入力させ，登録パスワードとの照合を行うことで認証を行う技術である．固定式パスワード認証では，パスワードの定め方によって，認証の安全性・利便性が変化する．高い安全性を求めた場合，無意味な文字列の羅列や長い文字列，特殊記号と大文字を含めたパスワードなど複雑なものを用いることになる．複雑なパスワードは利用者の記憶負担を増加させるため，パスワードの再現が困難になるなど，利便性に問題が生じることが多い．また，利便性を求めた場合，文字列のパスワード，同じ文字のみのパスワードが用いられる傾向にある．単純なパスワードは推測が容易であるため，情報量が減少して総当たり攻撃への強度が低下することに加えて，タッチパネルの残留物からの推測や覗き見などによりパスワードが漏洩し，端末の不正利用につながる危険性があるなど，安全性に問題が多い．このように利便性と安全性の間にはトレードオフの関係があるといえる．

これらの問題に対応するため，本研究では利便性と安全性を両立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．

2. 関連研究

2.1 画像認証

生体認証，固定式パスワードとは異なる個人認証として画像を用いた画像認証が研究されている．画像認証とは，画像を認証成功となる秘密情報として扱う個人認証手法である．画像認証の基本的な手続きを図 1 に示す．認証画面で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む提示画像群を提示し，その中から利用者が適切な画像を選択した場合は認証成功，それ以外の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 [7].

(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」[8] と呼ばれている．この効果により，画像認証はパスワード認証に対して，記憶負担の面で優位性があるといえる．また画像認証の特徴として，再認方式であるという点が挙げられる．ここで示す再認とは，提示画像群から正解画像かどうかを判断する行為である．再認方式を用いた認証は，固定式パスワード認証のようなパスワードを手がかりなしで想起し，利用者自身が入力する再生方式よりも容易であるとされている．画像認証を用いている「Deja Vu」[10] では，提示された複数の幾何学模様の人工画像がの中から，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. 認証時には不正解画像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」[11] 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．

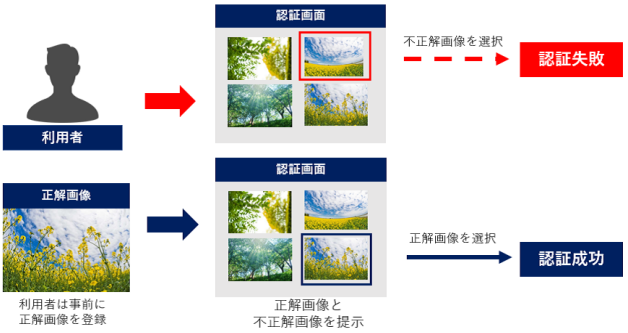

図 1 画像認証の基本的な認証方法

2.2 履歴情報を用いた認証

個人認証には利用者の履歴情報を用いた認証も研究されている．履歴情報には昨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だけではなく，センシングデバイスなどから自動記録されるライフログも含む．履歴情報の特徴として，日常生活の中で常に変化が発生し，他者が正確に取得することも困難であることが挙げられる．認証においては新しい履歴情報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可能性がある. 履歴情報を用いた認証の 1 つとして電子メールの履歴を用いた認証 [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利用者が選択することで認証を行っている．安齋ら [12] はパスワードなどの認証情報を忘れたり，認証時に規定数間違えた際の代替認証方式であるフォールバック認証にスマートフォンの利用履歴を用いて動的に認証質問を行う手法を提案している．例えば，利用者のアプリの利用履歴から 1 週間の中で最も使用したと思われるアプリ 3 つを選択するといった出題を行う．また，Ngu ら [6] 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．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．

3. 画像と履歴情報の複合認証

画像認証は，利用者が登録する対象を文字列等から画像とする事で記憶の負担軽減，想起の容易さ，認証の手軽さから利便性に対する効果が高い．しかし，利用者による提示画像群に登録する画像の準備，登録作業が必要であり，利用者に負担を強いる可能性がある．そこで，履歴情報から画像を取得することで，自動的な画像の準備・登録が行

えると同時に本人の履歴情報は他者が事前に知る事は困難であるため，前もって盗み取られる心配はない．加えて，履歴情報の更新に伴い，画像も更新することで同じ画像を使い続ける事がなくなるため，安全性の向上が可能となる．したがって，利便性と安全性を両立させるため，本研究では履歴情報と画像の再認を複合させた認証方式を提案する．この複合認証をスマートフォン端末を対象に用いることとする．この複合認証を行う上で生じる課題とそれに対するアプローチ，提案システムについて述べる．

3.1 提示画像の準備

画像認証には認証時に選択すると認証成功となる正解画像と認証失敗となる不正解画像の 2 種類の画像群を用意する必要がある．これらの画像群は利用者の記憶の鮮明さが求められるため，利用者の自発的行動による履歴情報に基づくものが望ましい．記憶と画像の結びつきが最も強固であると考えられる履歴情報としては，スマートフォン端末内に保存されているカメラ機能で撮影した写真が挙げられる．しかし，端末で撮影した写真には利用者の交友関係や活動場所等，個人情報に当たるものも多く含まれてしまうため，そのまま認証に用いた場合は他者への個人情報漏洩の危険が大きい．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スマートフォン端末内の履歴情報から選出して提示する必要がある．

3.2 正解画像の選出

利用者が選択すると認証成功となる正解画像は，関連研究 [10][11] では利用者自身の画像登録作業によって決定されている．正解画像の画像登録作業を行うことによって，認証時の正解画像の想起が容易になるが，利用者に対し，正解画像の準備・登録作業を必要とする．これの作業は利用者にとって心理的な負担となるため，正解画像の変更に対する煩わしさから，正解画像が長期間変更されずに，覗き見攻撃などで他者に突破される可能性がある．したがって，正解画像は利用者の登録作業の負担が小さいものであることが重要である．

3.3 不正解画像群の選出

利用者が画像認証を行うためには，不正解画像となる画像群の登録が必要である．関連研究 [10][11] では利用者が登録した画像群の中から選択した正解画像以外を不正解画像としている．不正解画像は他者が判別不可能にするための囮であるため，正解画像より大量の画像が必要となる．利用者は大量の画像を収集するし，登録する必要があるため，不正解画像の変更も頻繁には行わない可能性がある．画像の変更が行われない場合，認証時に同一画像が頻繁に提示されることになる．その結果，正解画像の推測が可能となり安全性が低下する．また，不正解画像と正解画像を認証画面に提示したとき，利用者が認証操作時において迷いが生じ，認証に時間がかかる可能性がある．したがって，利用者にとって正解画像と峻別しやすい不正解画像群の収集の検討が必要となる．

4. アプローチ

4.1 提示画像の準備に対するアプローチ

端末内で認証時に使用可能な画像候補として，ダウンロード画像や他アプリ操作時のスクリーンショットなどがある．ダウンロード画像にはメッセージアプリなどによる個人的な内容に関するものによって取得する画像が存在する可能性があり，利用者の個人情報に関わる危険性が高い．一方，アプリ操作時のスクリーンショットは対象アプリを限定することによって利用者の個人情報とは無関係な画像が抽出可能である．特に，標準インストールされているブラウザでの Web ページ閲覧操作から得られるスクリーンショット画像の特徴としては以下のものがある．

(1) ブラウザによる Web ページ閲覧は利用者の自発的行為であるため，個人に特化した画像となる
(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，スクリーンショット画像のみから該当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) 個人アカウントに紐付いたサービスでないならば，専用アプリよりブラウザを用いて閲覧している時間のほうが長い [5]

インターネット上に膨大な数が存在するため，認証のための提示画像の候補が枯渇することはない．また，ブラウザ閲覧履歴に記録された URL を用いることで，利用者に追加の作業を必要とせずに画像の登録が可能である，さらに，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記載されているため，利用者のみに閲覧済みの情報を提示することで，認証時の Web ページ想起に効果的であると考える．本研究ではブラウザの閲覧履歴に着目し，Web ページそのものを 1 枚の画像として捉え，スクリーンショットを画像と定義し，提示画像群に登録する．

4.2 正解画像の選出に対するアプローチ

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ものが存在する [4]．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 ページを閲覧時に画面に親指を接触させ

る動作を行わせる．この動作を行っている間は利用者がスマートフォン端末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する．これにより，利用者の負担を最小限に閲覧時の注視状態を取得可能となり，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が可能になる．スマートフォン端末での Web ページ表示時間と画面接触時間から注視の度合いを算出し，最も高い値が想起しやすい画像であると考えた．本研究では，Web ページの表示時間と親指の画面接触時間から利用者の注視の度合いを示す注視継続率を求め，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．

4.3 不正解画像群の選出に対するアプローチ

利用者に未閲覧の Web ページを提示画像群として表示することで正解画像との峻別が容易になると考えられる．そのためには，検索キーワードに対する未閲覧 Web ページの URL 群を取得する必要がある．そこで，正解画像として選出された Web ページ URL の検索キーワードに対する検索結果から Web ページ URL 群を抽出する．図 2 を例にすると，利用者はブラウザ閲覧時に検索キーワード A，B，C を用いてそれぞれ検索し，Web ページを閲覧したとする．ここで検索キーワード B で閲覧した Web ページ群の中から正解画像が選出された場合，検索キーワード B を用いて未閲覧の Web ページを検索結果から選出する．検索結果を用いる場合，同一ドメイン名の Web ページが複数出力される場合がある．認証画面に同一ドメインの画像が提示された場合，酷似したレイアウト，内容である Web ページが含まれる場合があり，想起時に混乱する可能性がある．そこで，閲覧済み Web ページ URL 群からドメイン名を抽出し，抽出したドメイン名とドメイン名を含む URL を未閲覧 Web ページ URL 群から除外することで，利用者の想起時の混乱を防ぐことができると考えられる．以上から，本研究では利用者が閲覧済み Web ページと同一ドメインを排除した，正解画像を閲覧した際の検索キーワードから未閲覧の Web ページを不正解画像として選出する．

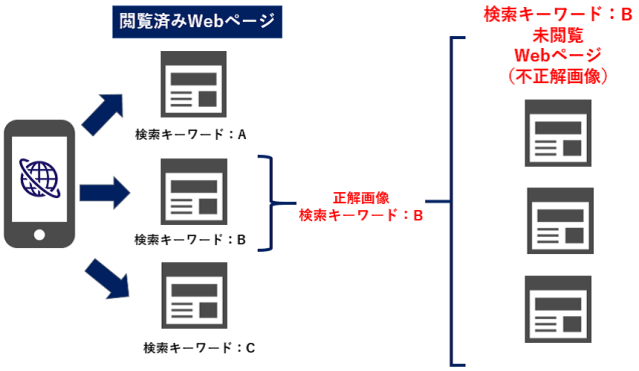

図 2 不正解画像に対するアプローチ

5. 提案システム

5.1 提案システム

提案システムを図 3 に示す．本研究はキーワード検索を経由した Web ページ閲覧しか対象としない．スマートフォン端末で起動したブラウザアプリで取得するデータは，閲覧した Web ページ URL，Web ページ表示時間，画面接触時間，注視継続率，検索キーワードである．この 5 種類のデータを BrowserDB に保存する．なお，同一 URL の Web ページが既に存在した場合は，注視継続率が最も高い Web ページ URL を登録する．BrowserDB から提示画像群取得システムが，正解画像となる注視持続率が最も高い Web ページ URL 1 つと不正解画像となる不正解画像となる未閲覧の Web ページ URL を 9 つ取得し，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する．正解画像・不正解画像は一定期間蓄積される．取得する URL は検索結果を除外する. 利用者がスマートフォン端末を起動すると提示方法に基づいて認証画面に蓄積された正解画像・不正解画像から選出した提示画像群が出現し，その中から正解画像を選択する試行を行う．認証画面表示ごとに提示画像群を変更し，認証成功した提示画像群は一定期間認証画面に表示されない．

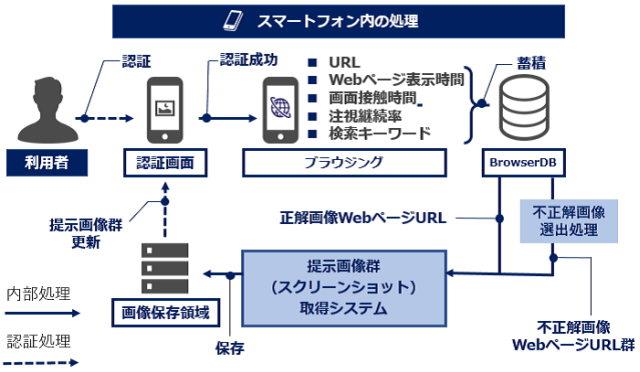

図 3 提案システム

5.2 注視継続率の算出

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．ここで Web ページ表示時間は Web ページのロード完了から Web ページの URL が変更されるまでとする．Web ページ p_i に対するロード完了時刻を sp_i，Web ページの URL 変更時刻を ep_i とすると Web ページ表示時間 rp_i は以下の (1) 式で求められる．

$$rp_i = ep_i - sp_i \tag{1}$$

Web ページ p_i に対する画面接触時間を求める．p_i を表示している時間内において親指が画面に触れてから離れるまでの時間を<t_{i1},t_{i2},⋯,t_{in}>，k を閲覧時間内の親指の接触

回数とすると，画面接触時間 tp_i は以下の (2) 式で求められる．

$$tp_i = \sum_{j=1}^{k} t_{ij} \tag{2}$$

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

$$gc_i = \frac{tp_i}{rp_i} \tag{3}$$

5.3 不正解画像選出処理

不正解画像となる Web ページ URL 選出までの処理を示す．初めに注視継続率が最も高い Web ページ URL と付随する検索キーワードを正解画像として BrowserDB から取得しする．不正解画像とあなる未閲覧 Web ページ URL を選出するまでの流れを図 4 に示す．正解画像 Web ページ検索キーワードと同一の検索キーワードを用いて，BrowserDB から閲覧済み Web ページ URL を抽出する．次に，正解画像の検索キーワードの検索結果から不正解画像候補として規定した個数の Web ページ URL を抽出する．同一検索キーワードの閲覧済み Web ページ URL と検索結果から抽出した不正解画像候補の Web ページ URL のドメイン名を比較し，同一ドメイン名の Web ページ URL は不正解画像候補に残さない．一連の処理で残った不正解画像候補の Web ページ URL からランダムに 9 個の Web ページ URL を抽出し，スクリーンショットを取得する．

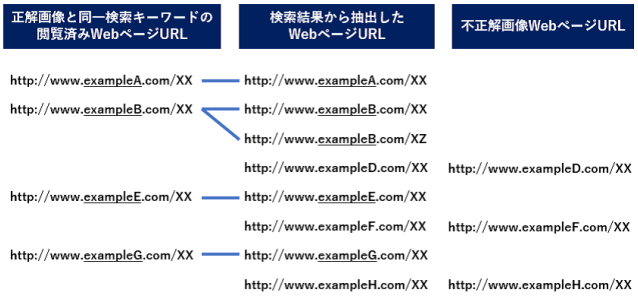

図 4 同一ドメイン名削除による不正解画像 Web ページ選出

5.4 提示方法

スマートフォンにおける画像の提示方法を図 5 に示す．認証時には画像の内容を確認することが必要である．提示画像枚数は正解・不正解画像合わせて 10 枚だが，スマートフォン端末の画面に提示することは困難である．提示画像群として Web ページのスクリーンショットを表示させるため、利用者が画像の内容を視認可能なサイズで提示させなければならない．そこで，画面上部に画像を表示し，画面下部に親指でスライドするためのスライドバーを配置する．画像の切り替えは，スライドバーをスライドさせるようにして移動させることで行える．表示されている画像が何枚目かを把握する為，スライドバー上部に数字を表示する．選択は提示画像をタップすることで行う．この提示方法により，素早い画像の視認が可能となり，10 枚の提示画像群を利用者が視認できる画像サイズで表示することが可能となる．

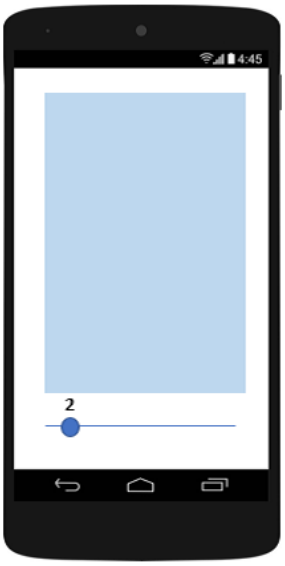

図 5 認証画面の提示方法

6. 実験

6.1 実験目的

提案システムについて，注視継続率を基準とした正解画像選択の有用性について対人実験を用いた評価を行った．本実験は各認証試行ごとに，1 枚の正解画像と 9 枚の不正解画像の計 10 枚を提示する．このときの各画像の注視継続率，閲覧時間，および画像群表示から正解画像選択までの認証時間によって評価する．

6.1.1 実験用システム構成

評価実験にあたって，データ収集用に図 6 のような閲覧データ取得ブラウザアプリケーションを実装した．対象とする OS は Android であり，ブラウザ内で利用する検索エンジンは Google 検索である．このアプリケーションは，閲覧した Web ページ URL 取得機能，Web ページ表示時間計測機能，画面接触時間計測機能，注視継続率算出機能，検索クエリ抽出機能を備えている．このアプリケーションを用いた実験用システムの構成を図 6 に示す．Web ページ閲覧の進行によって Web ページが遷移するたびに，サーバ上の BrowserDB に各データを送信する．提示画像群取得システムにおいて，取得した URL から Web ページのスクリーンショットを取得し，ローカルフォルダに保存する．この際，スクリーンショット画像のサイズは 320x568 ピクセルとしている．提案システムでは実際には図 3 のようにすべての処理をスマートフォン内で完結させているが，実験用システムでは実験の進行上，取得した画像の蓄積や，

認証画面の表示は PC 上で行う (図 7)．認証画面で被験者に認証動作を行ってもらい，各認証試行について，使用した画像の情報とともに認証成功・認証失敗をラベル付けした情報を蓄積していく．

図 6　実験用ブラウザアプリケーション

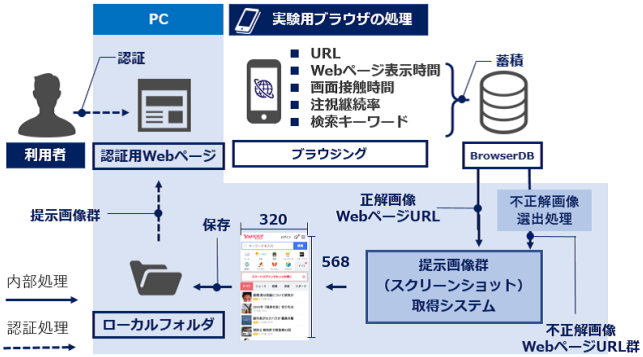

図 7　実験用システム構成図

6.2　実験方法

閲覧する Web ページの種類をある程度限定するために，被験者にはそれぞれ検索に用いるキーワードを用意させる．このキーワードを用いて検索することから Web ページ閲覧を開始してもらい，「Web ページのロード完了をもって閲覧開始とする」，「閲覧時には必ず画面に親指を接触させる」，「閲覧終了時には親指を離す」という条件のもと，Web ページ閲覧を 10 分間行わせる．10 分間の閲覧終了後に現れる認証画面において，閲覧した記憶が最も鮮明な画像を選択させる．この作業を被験者 1 名に対し 3 セッションずつ行わせる．なお，セッションごとに画像選択にかかわる蓄積データをクリアすることで，セッションごとの特徴データを取得する．

6.3　実験結果

表 1 のように，被験者 5 名による全 15 試行のうち，10 試行で認証に成功，5 試行で失敗という結果が得られた．図 8 に各 Web ページの注視継続率と提示画像群の表示から画像選択完了までの画像選択時間の関係を示す．全試行についての平均画像選択時間は 16.9 秒である．認証成功した試行については平均画像選択時間より短い時間で選択が完了しているものが多い．次に各 Web ページの注視継続率と Web ページの閲覧時間の関係を図 9 に示す．認証失敗した試行の多くは注視継続率は高いものの，閲覧時間が短くなっている．

表 1　被験者ごとの成功数

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

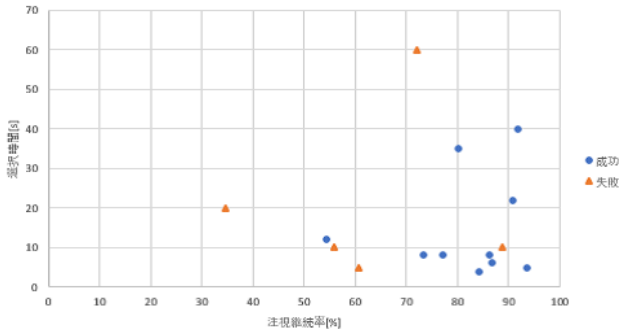

図 8　注視継続率と選択時間の関係

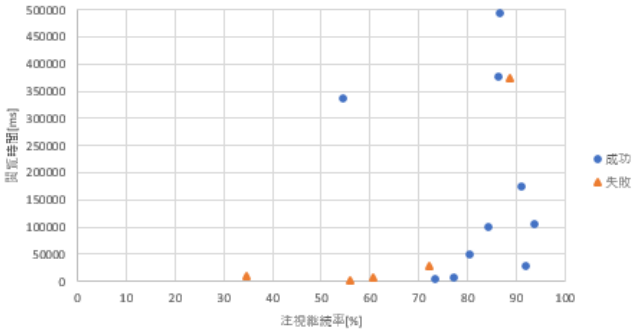

図 9　注視継続率と閲覧時間の関係

7.　考察

7.1　認証実験に関する考察

実験結果より認証が失敗した原因についての考察を行い，改善手法を探る．まず，図 8 の画像選択時間と注視継

続率の関係に着目する．正解画像となる Web ページについて鮮明な記憶が残っていた場合は迷いなく画像の選択に至ることから，画像選択時間は短くなる傾向があるといえる．注視継続率の高い画像群はおおむね画像選択時間が短く，認証も成功しているため，提案システムの画像選択基準は妥当なものであるといえる．一方，認証を失敗している試行については，注視継続率が高くても閲覧時間が極端に短いものが多い．これは閲覧時間が短いために画像が被験者の記憶に残りにくかったことが原因であると考えられる．これに対し，被験者全員に対してヒアリングを行った結果，画像の選択に迷いが生じた場合について，注視継続率以外の以下の 2 つの要因も影響を与えていることが判明した．(1) コンテンツの内容的に正解画像と酷似した不正解画像の出現 (2) コンテンツのレイアウト的に正解画像と酷似した不正解画像の出現，不正解画像には正解画像閲覧時に使用した検索キーワードから導出した Web ページを利用しているため，内容の似通った画像が選出される場合があったことが判明した．また，正解画像の選択時に，Web ページの見た目ではなく，コンテンツ内の文章を読んで選択していることも多く，条件 (1) が被験者の画像想起に影響を与えていることがわかった．また，認証成功時にも酷似した内容の画像が存在する場合は，画像選択時間がかかっていた．一方酷似したレイアウトの例としては，Web ページにリストビューが含まれている場合などである．このような場合，被験者は記憶上の閲覧済み Web ページ画像と，不正解画像をレイアウトから同一のものと判断してしまいがちなため，認証失敗に結びつきやすいといえる．また，検索キーワードが同一でレイアウトも酷似している場合は，Web ページの内容も酷似している傾向が強い．以上より，認証成功の精度をあげるためには，注視継続率に加え閲覧時間の閾値も設ける必要がある．また，酷似した内容・レイアウトの Web ページ画像が認証に影響を与えているため，不正解画像の選出時にこれらを排除する仕組みの導入が必要となる．評価実験では選択時間の全体平均が 16.9 秒，認証成功時に限った平均が 14.8 秒となっている．これについて関連研究における選択時間と比較評価する．「あわせ絵」は提示画像 10 枚から 1 枚選択する試行を 4 回繰り返した場合に平均 24.6 秒，「Deja Vu」は提示画像 25 枚から 5 枚選択する試行を 1 回行った場合に平均 32 秒，「PassFrame」は並べ替えによる画像配置手法の場合に平均 9.97 秒，画像選択手法の場合平均 3.42 秒である．現状では提案システムは選択にやや時間がかかっている傾向があるため，画像表示手法や選択手法の検討などを行い，選択時間の短縮を目指す必要がある．

7.2 安全性に関する考察

提案システムに対する他者からの攻撃方法として以下の 4 つが想定される．

(1) Educated Guess 攻撃
(2) 総当たり攻撃
(3) 覗き見攻撃
(4) Intersection 攻撃

Educated Guess 攻撃とは利用者に関する情報を基に，他者が認証画像を推測する攻撃のことである．提案システムでは，利用者本人が Web ページ閲覧時に検索に用いたキーワードを基に正解画像，不正解画像を決定しており，たとえ検索キーワードが漏れたとしてもどの Web ページをどれだけ閲覧したかの情報は取得できないため，他者による推測は非常に困難であり，Educated Guess 攻撃に対する耐性はあるといえる．

総当たり攻撃とはすべての画像選択パターンを試すタイプの攻撃である．提案システムでは提示画像 10 枚からの認証試行 4 回を想定しているため，総当たり攻撃に対して少なくとも PIN4 桁と同等の耐性を持つ．

覗き見攻撃とは他者が利用者の認証動作を覗き見て，その動作を再現することで認証を突破する攻撃である．提案システムでは認証の試行ごとに提示画像群全体を変更して，同一の正解画像・不正解画像を連続で出現させないようにしているため，覗き見攻撃に対しても耐性がある．

Intersection 攻撃とは，認証時に必ず正解画像が表示されることを利用した攻撃であり，提案システムでは現在のところ特に対応していない．しかし，正解画像が 1 枚も存在しない提示画像群に対し，利用者が「正解画像が存在しない」という選択をできるようにすることで，この攻撃を防ぐことができる可能性がある．

8. おわりに

本研究ではスマートフォン端末における固定式パスワードのトレードオフ問題を解決するため，画像認証と履歴情報を用いた認証を複合させ，履歴情報から画像を抽出して認証に用いる方式を検討した．この複合認証をスマートフォン端末に利用する際の課題として，提示画像抽出の準備，想起しやすい正解画像の選出，不正解画像群の選出の 3 つが考えうる．それぞれの課題解決アプローチとして，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画像として用いる，利用者の注視継続率が最も高い Web ページを正解画像，正解画像を検索した際の検索キーワードの検索結果から未閲覧の Web ページを不正解画像とする方法を提案し，これらのアプローチ手法を取り入れた複合認証システムの提案を行った．提案システムに対する評価実験として，正解画像 1 枚と不正解画像 9 枚の提示画像群から正解画像を選択する認証実験を行い，全体の認証成功率が 67%，選択時間が全体で平均 16.9 秒，認証成功のみでは平均 14.8 秒という結果を得た．注視継続率は不正解画像との峻別が可能な正解画像を選択できており，認証失敗する原因として閲覧時間と正解画像と酷似したレイア

ウト・内容の不正解画像の存在が判明した．また，選択時間において関連研究に及ばない場合があり，利便性の向上に工夫の余地があることがわかった．

今後の課題として，正解画像選出のための閲覧時間の閾値の決定，酷似したレイアウト・内容を持つ不正解画像選出への対策，選択時間の短縮，また各攻撃についての耐性の評価を行う必要がある．

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 2017-5-14）.

[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] Ngu Nguyen, and Stephan Sigg: PassFrame: Generating image-based passwords from ego-centric videos, Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp.4649 (2017).

[4] 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).

[5] 岩崎宰守:スマホのネット利用はアプリとブラウザに 2 強化 ニールセン調査, INTERNET Watch, 入手先 ⟨https://internet.watch.impress.co.jp/docs/news/1048729.htm⟩ （参照 2018-5-14）.

[6] Ngu Nguyen, and Stephan Sigg: PassFrame: Generating image-based passwords from ego-centric videos, Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp.4649 (2017).

[7] 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).

[8] 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, Vol.2, pp.69-70, 勁草書房 (2016).

[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] Rachna Dhamija, and Adrian Perrig: Dj Vu: A User Study Using Images for Authentication, Proceedings of the 9th conference on USENIX Security Symposium(SSYM'00), pp.45-58 (2000).

[11] 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).

[12] 安齊将之, 小倉加奈代, ベッド B. ビスタ, 高田豊雄, スマートフォンの利用履歴を用いたフォールバック認証の検討, 電気関係学会東北支部連合大会講演論文集 (2017).