Computer Security Symposium 2017
23 - 25 October 2017

私的な連想情報の再認による個人認証と安全性評価

山岸 伶[1]　高田 哲司[1]

概要：再認方式の個人認証は秘密情報保持の点で利点がある一方で，回答候補が視認できるため推測攻撃に脆弱であるという問題があった．この状況を改善しうる再認式個人認証として，本研究では「既知の私的な連想情報」を秘密として用いる認証手法を提案する．この提案に基づき，10 個の単語群から 4 つの単語ペアを秘密として回答するプロトタイプシステムを実装し，被験者による評価実験を実施した．その結果，実用面において二週間間隔での利用でも秘密情報保持に支障なく利用できること，また推測による攻撃に対しても 70 試行までの推測攻撃には安全であることが明らかになった．

キーワード：個人認証，再認方式，推測攻撃，私的連想，安全性と有用性

Recognition-based User Authentication with Associated Information for the Users and the Usability Evaluation

Rei Yamagishi[1]　Tetsuji Takada[1]

Abstract: Recognition-based authentication has an advantage in memorability. However, it has vulnerability to guessing attacks because the answer candidates are shown by the system. In this paper, we propose the authentication that uses associated information for users as a secret. Based on this proposal, we implemented a prototype system whose secret is defined as four associations for the user from ten words. We evaluated the system through usability and guessing attacks experiments by subjects. We find that a user is available it after two weeks and it has security against guessing attack of 70 attempts.

Keywords: User Authentication, Recognition-based Authentication, Guessing Attacks, Association of Information, Security and Usability

1. はじめに

パスワードをはじめとする知識照合型個人認証は，実装の容易さなどの理由から現在も広く利用されている．一方，知識照合型個人認証には，記憶可能性と推測攻撃耐性のトレードオフが存在している．ここでの有用性は記憶可能性，入力時間とする．安全性は推測攻撃，総当たり攻撃，逆総当たり攻撃，覗き見攻撃，汚れ攻撃，フィッシング攻撃に対する耐性とする．例えば，意味のある文字列で構成された短いパスワードは記憶可能性が高い一方，総当たりや推測攻撃耐性が低い．意味のない文字列で構成された長いパスワードは，総当たり攻撃や推測攻撃耐性が高い一方，有用性が低い．

記憶可能性を向上させる手法として，再認方式の個人認証が提案されている．再認方式の個人認証は，秘密情報でなく秘密情報の入力方法の一つであり，回答候補群 (秘密情報とそれ以外の囮で構成される) から正しく秘密情報を選択する手法とする．再認方式の個人認証は以下の利点を持つ．

- 秘密情報を忘却していても，正解となる秘密情報を見ることで想起の手助けとなる (記憶可能性が高い)．
- 提示された情報から秘密情報を直接選択する回答方法が多く，入力操作が簡単になるという傾向がある (文字入力しない)．
- 認証画面に提示される回答候補群がユーザによって異なるため，フィッシング攻撃がパスワードと比較して

[1] 電気通信大学
The University of Electro-Communications

困難である．

その一方で，再認方式の個人認証は秘密情報が認証時に提示されるため，攻撃者も秘密情報の手がかりを得ることができる．したがって，再認方式の個人認証は特に推測攻撃耐性が低いという問題点がある．

本研究では，「既知の私的な連想情報」を秘密情報として，再認方式の利点である記憶可能性を低下させずに推測攻撃耐性の高い個人認証を目指す．「既知の私的な連想情報」は，自分が秘密情報登録以前から知る「2 つの情報 (単語) の関連」で定義される．提案する手法は再認方式の個人認証であるため，ユーザは解答候補群 (情報のペア) から「既知の私的な連想情報」を選択する．

提案する個人認証の記憶可能性と推測攻撃耐性を評価するために，プロトタイプを実装して，被験者による 2 つの評価実験を実施した．

- 記憶可能性評価実験: 被験者が秘密情報の登録と一定期間を開けて認証を行い，提案手法の記憶可能性を評価した．また，認証時間も測定した．
- 推測攻撃耐性評価実験: 被験者同士がお互いの秘密情報を推測することで提案手法の推測攻撃耐性を評価した．

また，評価を行なっていない有用性や安全性についても定性的な議論を行う．

2. 関連研究

関連研究として，「再認方式の画像認証」，「関連を秘密情報とした個人認証」と「パスワードに対する推測攻撃の評価実験」に関する研究について述べる．

2.1 再認方式の画像認証

再認方式は，秘密情報のことでなく，解答候補群から秘密情報を選択する手法をさす．そのため，再認方式の個人認証は秘密情報自体も記憶可能性が高いものが利用される．多くの再認方式の個人認証は秘密情報として画像を用いる (以下，画像認証とする)．これは画像が文字と比較して記憶するのが容易という性質を持つためである．

再認方式の画像認証は秘密情報に画像を用いて記憶可能性を向上させる一方，依然として推測攻撃耐性が低い．これは回答候補群の画像とユーザの趣味嗜好に基づいて，攻撃者が秘密情報を推測する可能性があるためである．この問題を背景として，推測攻撃耐性を向上させる秘密情報を持つ再認方式の画像認証が研究されている．以下では，推測攻撃耐性の向上に取り組んだ再認方式の画像認証として 2 つの関連研究について述べる．

Dhamija らによって，Deja Vu[1] という再認方式のグラフィカルパスワードが提案されている．この認証では 25 枚の抽象画から秘密情報としている 5 枚の抽象画を順不同で選択する．Deja Vu は推測を困難にする代わりに，記憶可能性を低下させている．記憶可能性に関する評価実験では一週間後に 10%の人が秘密情報を忘却していた．推測攻撃に関してはシステムが画像の候補を生成するため推測攻撃に耐性を持つが，評価実験を行っていないため確かではない．

Hayashi らは Use Your Illusion[2][3] を開発した．これは，画像を油絵のようにぼかす加工をすることで推測攻撃耐性を向上させるというものである．Hayashi らはこの手法の記憶保持実験と推測攻撃実験を行った．その結果，Use Your Illusion の記憶可能性は高い一方で，推測攻撃耐性が低いことがわかった．登録から 2 日後，1 週間後，4 週間後でも 100%のユーザが秘密情報を記憶可能であった．その一方で加工した画像に対して 10 回の試行で知人が攻撃をした場合，15 人中 1 人攻撃に成功することが明らかになった．

2.2 関連を秘密情報とした個人認証

関連を用いることで秘密情報を思い出しやすいという利点が存在する．これは認知心理学の研究の成果である単純に 1 つの事柄の想起と比較して 2 つの関連した事柄を想起する方が容易である [4] という成果に基づいている．以下では，関連を秘密情報とした個人認証について述べる．

Smith によって単語の関連を用いた手法 [5] が提案されている．単語のペアを複数登録し，ペアのうち片方が秘密情報となる．認証時には登録したペアの中からランダムで秘密情報でない方の単語が一つ提示され，それと関連した秘密情報の単語を解答する．例えば，「山」と「川」(秘密情報) をペアとして登録した場合，システムが「山」を表示し，ユーザはその単語を手掛かりにして「川」と入力する．Smith によると 6 ヶ月後経過しても 94%の被験者が手掛かりを見て関連する単語を想起し，18 ヶ月経過後も多くの被験者が単語を想起できた．一方で，Smith の手法に対して Pond らが再調査 [6] を行った．その結果，秘密情報の登録から 2 週間経過した際に 65%のユーザしか秘密情報を想起できなかったと示した．

2.3 パスワードに対する推測攻撃の評価実験

パスワードに対する推測攻撃耐性測定法は，2 種類あると Melicher ら [7] は分類している．一方は推測攻撃のシミュレーションによる手法で，もう一方は統計的手法 [8] である．Melicher らは，統計的手法がサンプル数を大量に必要とするため困難とし，ニューラルネットワークを用いた推測攻撃のシミュレーション手法について述べた．そこでは，クラウドソーシングによる収集や漏洩したパスワードを用いて，推測モデルを作成し，10^{25} 回の試行回数のシミュレーションを行った．その中でデータセット内のパスワードが何%推測可能かについて議論している．

パスワードに対する推測攻撃耐性の測定は多くの試行回

数を用いたシミュレーションが行われている．その一方で，新たに提案される個人認証の多くは研究室内実験を行うことで推測攻撃に対する強度を測定しているため，試行回数が限られている．新たに提案される個人認証も，推測攻撃耐性実験の際に，より多くの試行回数を必要だと考える．

3. 提案手法

3.1 提案手法のコンセプト

2.1 節で，再認方式の個人認証において記憶可能性と推測攻撃耐性のトレードオフが残っていることを示した．Deja Vu は記憶可能性が低い代わりに推測攻撃耐性が高く，Use Your Illusion は推測攻撃耐性が低い代わりに記憶可能性を向上させている．このトレードオフを解消し，記憶可能性と推測攻撃耐性を両立した個人認証の提案を目指す．

本研究では，1) 入力手法:再認方式，2) 秘密情報:「既知の私的な連想情報」の個人認証を提案する．1) の再認方式は秘密情報の想起を助けて記憶可能性を向上させる手法であるが，推測攻撃耐性に問題がある．この問題を解決するために 2) の「既知の私的な連想情報」を秘密情報とする．「既知の私的な連想情報」が高い推測攻撃耐性を持つ根拠を説明する前に，秘密情報の詳細を説明する．

以下で秘密情報について説明する．1 節でも述べたが，「既知の私的な連想情報」は，a) ユーザが秘密情報の登録以前から知る (以下，既知情報とする)，b)「2 つの情報 (単語) の関連」で定義される．例を挙げると，印象的な悪夢で「公園」に「虎」が出たというものがあれば，その夢を見た人の中では「公園」と「虎」の関連が「既知の私的な連想情報」となる．また，「地下鉄」で「時計」を失くした経験があれば，「地下鉄」と「時計」の関連が「既知の私的な連想情報」となる．a) の既知情報はユーザが秘密情報登録以前から知る情報であるため，記憶負担を軽減することができる．ただし，秘密情報であるため辞書に載っているような関連ではなく「私的な」情報に限定した．b) の 2 つの情報の関連は例のような「地下鉄」と「時計」であり「地下鉄」単体や「時計」単体でなく，その 2 つが関連していることである．以下では，2 つの情報「A」,「B」が関連していること (ペアであること) を「A-B」と表現する．秘密情報は関連と定義されため，「A-B」の「-」が秘密情報である．

提案手法は 1 つの情報 (「A」,「B」) でなく，各情報 (「A」と「B」) が関連しているかどうかを秘密情報とした．この秘密情報は関連を秘密情報としているため，1 つの情報を秘密情報にする場合と比較して他人が推測するのは困難だと考えた．2.2 節にあげた関連を秘密にする認証手法は「A」に関連する「B」を入力でする必要があり，「関連」自体でなく「関連する情報 (単語)」を秘密情報にした点で異なる．我々の知る限りでは，1 つの情報 (「A」,「B」) でなく，その関連 (「-」) を秘密情報としている個人認証は他にない．

以上で説明してきた 1) 入力手法:再認方式，2) 秘密情報:「既知の私的な連想情報」を組み合わせて，多くの回答候補群から「既知の私的な連想情報」を選択する個人認証を提案する．具体的には，「A-B」,「A-C」,「B-C」のような回答候補群中から「既知の私的な連想情報」(既知情報である関連「-」) を選択する．選択する際にユーザはその関連が既知情報かどうかを判断基準に再認できるため，記憶可能性が高いと考える．

3.2 プロトタイプシステム

本研究では「既知の私的な連想情報」を秘密情報とした再認方式の個人認証のプロトタイプシステムを iPad2 に実装した．プロトタイプシステムでは 1) 回答候補群の提示，登録の仕方を工夫し，2) 秘密情報や回答候補に制限を加えた．

回答候補群の提示方法としては「A-B」,「A-C」,「B-C」といった候補の表示方法でなく，「A」,「B」,「C」各情報をシステムが表示する．この情報からユーザは，その組み合わせ「A-B」,「A-C」,「B-C」であると解釈し，秘密情報を選択する．この方法によって同じ単語を重複して提示しなくていいため，画面に表示する単語の数を軽減することができる．そのため，タブレットの小さな画面でも利用可能であると考えた．また，回答候補が提示されているため，再認方式を保っている．同様に，秘密情報の入力の登録の際には単語を入力することで，ペア (回答候補群) ができるという利点がある．また，登録の際には秘密情報に利用する単語以外も登録することができ，この秘密情報とは関係のない単語を囮情報と呼ぶ．この囮情報は，攻撃者による推測を困難にするため，ペア情報を構成する単語となんらかの関係がある単語であることが望ましい．

プロトタイプシステムにおいて，回答候補は 10 単語からなるペアとし，秘密情報は名詞 4 ペアに限定した．これは 4 章の評価実験において，条件 (入力に必要な数など) に差が生じないためである．

3.2.1 秘密情報設定

秘密情報設定手順について説明する．

(1) 秘密情報の作成: 既知の私的な連想情報による単語ペアを 4 ペア作成する．この際，別のペアに同一の単語を使用してもよい．秘密情報の定義は，3.1 節を参照のこと．
(2) ユーザ名の登録
(3) 単語群の登録: 10 個の単語をシステムに登録する．登録する単語は，すべて名詞でなければならない．(1) で作成したペア情報を構成する単語数は 10 個未満となる．そのため，不足分は任意の単語を追加で登録する．
(4) ペア情報登録: プロトタイプシステムを利用して，ペア情報を秘密情報として登録する．(2) で登録した単語を画面に表示する（図 1 左）．この画面では，登録さ

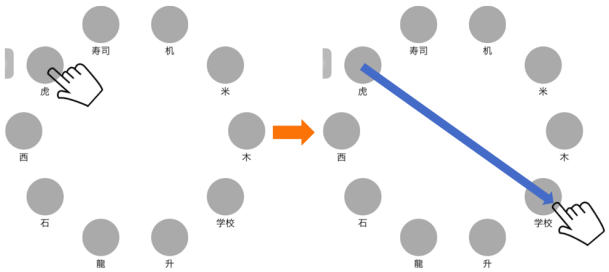

図 1 プロトタイプシステムの関連の登録, 認証画面

れた各単語は灰色の円オブジェクトとして表示され，各オブジェクトの直下に各単語がラベルとして表示される．ペア情報の登録は，ペアを構成する円オブジェクト同士を線で結ぶ操作で行う（図 1 右）．この際，どちらの単語を始点とするかは不問とする．秘密情報は「ペア（組み合わせ）」であり，順不同なためである．さらに，4 組のペア情報の入力順序も不問である．

3.2.2 認証手順

認証手順は以下の通りである．

(1) ユーザ名の入力

(2) 秘密情報入力: 認証画面 (図 1 左) で 4 組のペア情報を入力する (4 ペアの入力順は不問)．認証画面は 3.2.1 節で述べたペア情報画面と同一で，ペア情報の入力は 3.2.1 節で述べた「ペア情報の入力」と同じ操作で行う（図 1 参照）．なお認証画面における単語の配置は，認証行為のたびにランダム配置される．誤入力の許容回数は銀行 ATM の規則と同様に，2 回まで許容される．3 回連続で解答に失敗した場合，認証失敗となる．

4. 評価実験

本研究では，提案する個人認証手法の記憶可能性と推測攻撃耐性を検証するため，被験者による評価実験を行った．本章で，評価実験について，実験方法とその結果を示す．

4.1 記憶可能性評価実験

提案手法をユーザが利用可能か調査する目的で，被験者による記憶可能性評価実験を実施した．記憶可能性評価実験では，プロトタイプシステムを通じて認証成功率を測定した．また，5 節で議論するために操作時間についても測定した．

4.1.1 実験方法

本節では，実験手順について述べる．

(1) 事前準備: 実験目的とプロトタイプシステムについて説明を行い，秘密情報をプロトタイプシステムに登録した．秘密情報を登録後，登録した秘密情報の再確認とシステムの操作に慣れてもらう目的で，認証に 3 回成功するまで認証練習を行わせた．

(2) 1 回目実験: (1) の認証練習を終了してから 15 分後に，1 回目の認証実験を行なった．

(3) 2，3 回目実験: 1 回目の実験終了後，X 週間間隔を空けて 2 度認証実験を実施した．

表 1 各実験での認証成功数

条件	1 試行	2 試行	3 試行	失敗
Group1-Exp1	7	0	0	0
Group1-Exp2	6	0	1	0
Group1-Exp3	7	0	0	0
Group2-Exp1	12	0	0	0
Group2-Exp2	11	1	0	0
Group2-Exp3	12	0	0	0

表 2 各実験での認証時間 (単位は sec.)

条件	平均値	標準偏差	最小値	中央値	最大値
Group1-Exp1	14.53	3.60	9.50	14.42	20.58
Group1-Exp2	25.51	17.36	12.75	17.49	57.92
Group1-Exp3	17.37	6.06	12.32	15.62	30.72
Group2-Exp1	14.27	3.18	9.21	13.87	19.91
Group2-Exp2	26.26	10.52	16.38	22.23	47.38
Group2-Exp3	20.21	7.61	11.97	17.71	37.44

本実験では被験者を 2 つのグループに分けた．1 つは X=1 と（Group1 とする），もう 1 つは X=2 とした（Group2 とする）．このように実施した目的は記憶保持について比較検証を行うためである．

被験者は 19 名 (男性 15 名，女性 4 名) であり，Group1 が 7 名，Group2 が 12 名とした．

4.1.2 実験結果

記憶可能性に関する実験結果を認証成功率として示す．認証成功数と，認証成功時の試行回数を表 1 に示す．なお表中の条件列に記載されている文字列”Exp”の右の数字は，何回目の実験かを意味している．結果，全ての被験者が 3 回の試行回数以内に認証した．一方，1 回の認証試行で認証成功しなかった事例は，2 例だけであった．

操作時間に関する結果を表 2 に示す．まず全体として，操作時間の平均は 19.94 秒であり，標準偏差は 1.33 秒となった．また中央値と平均値の関係を見ると，Group1，2 ともに中央値のほうが小さく，被験者の多くは平均時間よりも操作時間が短いことがわかる．一方，実験回数ごとの操作時間の変化だが，どの条件でも認証時間は Exp2 > Exp3 > Exp1 という順で長かった．

4.2 推測攻撃耐性評価実験

提案手法の秘密情報を他者が容易に推測可能かを調査する目的で，被験者による推測攻撃耐性実験を実施した．2.3 節で述べたように，パスワードのような既存手法に合わせて，多くの試行回数を検証する必要があると考える．一方で，研究室内実験では攻撃者が実際に秘密情報を推測して入力するため試行回数が限られていた．そのため，本推測攻撃耐性実験では，新たに研究室内実験でも多くの試行回

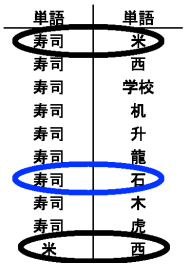

図 2 推測攻撃用紙

数に相当する推測を行った．

4.2.1 実験方法

「記憶可能性実験で被験者が作成した秘密情報」を別の被験者が攻撃者として推測するという方法で実施した．攻撃者と被攻撃者の関係によって攻撃成功率が変化すると予想されるため，以下の 3 つのグループに分類して実験を実施した．

- Group-A: 同研究室のメンバー間での推測
- Group-B: 同サークルのメンバー間での推測
- Group-C: 知人でない間での推測 (被攻撃者は Group-B と同じ)

このグループ分けにより，以下の 2 点の検証が可能になる．(a) 攻撃者と被攻撃者が知人かどうかで攻撃成功率が異なるか (b) 知人であっても，その関係性によって攻撃成功率が異なるか

実験方法は，以下に述べる手順で行なった．攻撃者は被攻撃者の秘密情報の候補となる全 45 ペアから疑わしいと考える 16 ペアを図 2 のように選択した．(秘密情報となっているのは 4 ペア) また，攻撃者は疑わしいと考えた 16 ペアにも最も疑わしい第 1 候補の 4 ペア，次に疑わしい第 2 候補の 4 ペアといった 4 段階の順位をつけた．(図 2 のように色で分けた) 実験環境は，現実の攻撃環境を考慮し以下の条件で実施した．

- 攻撃対象の秘密情報は推測攻撃実験の利用を知らされずに作成された (被攻撃者は秘密情報作成後に推測攻撃実験への参加を依頼された)．
- 攻撃者に攻撃対象アカウント (被攻撃者) が誰かを通知した．
- 被攻撃者の情報を集めるために，攻撃者に Web ページ閲覧を許可した．

今回の手法を用いることで，被験者の入力を少なくし，1,820 回の攻撃パターンの試行に相当することができた．本来であれば，実際に攻撃者がシステムを操作して，認証試行回数が攻撃回数となる．4 ペアを 1 回選択することで 1 回の攻撃試行になり，もう一度 4 ペアを選択することで 2 回目の攻撃試行ができる．その一方で，今回の手法は 45 ペアから 16 ペアの選択で多くのの攻撃試行ができる．具体的に，以下のような攻撃試行に相当していることがわかる．第 1 候補として 45 ペアから 4 ペア選択することは 1 回の攻撃試行に相当する．第 2 候補では新しく選択した 4 ペアと第 1 候補の 4 ペアを合わせた 8 ペアの中から 4 ペア選ぶ組み合わせが，${}_8C_4 = 70$ 通りあるそのため第 2 候補では，70 回の攻撃試行に相当する．同様に第 3 候補までででは 495 回，第 4 候補では 1,820 回の攻撃思考を行うことができる．

表 3 推測攻撃耐性実験の被験者数と総攻撃数

条件	被験者数	1 人あたりの攻撃回数	総攻撃数
Group-A	7	6	42
Group-B	8	7	56
Group-C	6	8	48

表 4 攻撃の成功率と推測された被験者

条件	攻撃成功数	攻撃成功率 (%)	推測された被験者名
Group-A	4	9.52	sub1(3),sub2(1)
Group-B	3	5.36	sub8(1),sub9(2)
Group-C	3	6.25	sub8(1),sub10(2)

本実験に参加した被験者は 21 名 (男性 16 名，女性 5 名) であり，3 グループのそれぞれに属する被験者人数は，表 3 の「被験者数」列に示している．また「総攻撃数」列に各グループにおいて実施した攻撃数を示している．Group-A,B は，各被験者がグループ内の他のアカウントを攻撃するので，被験者 (攻撃者) 数を n とすると，攻撃数 u は u=n(n-1) となる．また Group-C は各被験者が Group-B のアカウントを攻撃するので 6 被験者× 8 被攻撃者=48 攻撃となる．

4.2.2 実験結果

各グループにおける攻撃の成功率を表 4 に示す．Group-A の攻撃成功率が 9.52%であり，Group-B の攻撃成功率は 5.36%であり，Group-C の攻撃成功率は 6.25%である．各グループの攻撃成功率について，カイ二乗検定を行ったところ，3 グループ間に統計的有意差はなかった ($\chi^2(2)$=0.60, p=0.74 > 0.05)．同様に，2 グループごとにカイ二乗検定を行った場合も，Group-A と Group-B 間に統計的有意差はなかった ($\chi^2(1)$=0.54, p=0.46 > 0.05)．Group-B と Group-C 間にも統計的有意差はなかった ($\chi^2(1)$=0.03, p=0.85 > 0.05)．これらの結果から，今回の実験条件においては，攻撃者と被攻撃者の関係が推測攻撃の成功率に影響しない，という結果になった．

推測成功件数と推測された秘密情報の被験者との関係を表 4 に示す (カッコ内の数字は特定された件数)．この表を見て分かるのは，推測に成功された被験者 5 名だが，そのうち 1 回しか推測されなかった被験者 (sub1) は 1 名のみであった．この結果から，秘密情報を推測された被験者は，複数の第三者から推測される可能性が高いことが示唆されている．

次に，攻撃成功事例が，攻撃試行時のどの段階で成功したかを表 5 に示す．第 2 候補までででの攻撃成功例はなく，第 3 候補で 2 グループで 3 例，第 4 候補で全グループにお

表 5　推測に成功した数と特定した候補

条件	第 1 候補	第 2 候補	第 3 候補	第 4 候補
Group-A	0	0	1	3
Group-B	0	0	0	3
Group-C	0	0	2	1

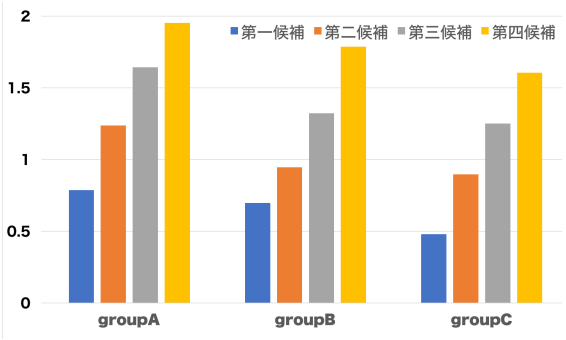

図 3　各候補での特定ペア数の平均

いて 7 例の攻撃成功例が見られた．

秘密情報となっているペアを特定した数の平均を各候補に分けて図 3 に示す．各攻撃において選択したペアが正しい秘密情報と一致した数 (特定した数) の和を攻撃数で割ったものである．第 4 候補での特定ペア数に対して，グループ間での結果に統計的有意差は見られなかった ($\chi^2(8)$=6.28, p=0.62 > 0.05)．

5. 考察

本章では，記憶可能性と推測攻撃耐性について議論する．また他の安全性，有用性について定性的に議論するとともに，今後の課題について述べる．

5.1 記憶可能性と推測攻撃耐性に関する考察

記憶可能性

短期記憶でも 1，2 週間間隔を 2 回あけた場合でも全ての被験者が認証に成功したことから，高い記憶可能性を持つことがわかる．特に，多くの被験者が 1 回の試行で認証に成功しており，再認方式であることをあいまって，低利用頻度でも秘密情報の想起を可能にしていると考える．この結果から，利用頻度が 1，2 週間に一度程度の利用形態でも，十分実用に耐えうる認証手法であると考える．

推測攻撃耐性

今回の実験で，最低限安全が確保されている試行回数について述べる．第 2 候補までの攻撃成功の例はなく，第 3 候補で 3 回の攻撃が成功することがわかった．第 2 候補は 2〜70 回の試行に相当し，第 3 候補は 71〜495 回の試行に相当する．したがって，攻撃にはじめて成功するのは 71〜495 回の試行で，最低限安全が確保されている試行回数は 70 回だということがわかる．推測に 70 回の試行が必要だということは，再認方式で既知情報を用いている手法として，十分な推測攻撃耐性が確保されていると考える．これは 1) 実験条件が攻撃者有利な状態であること，2) 他の再認方式の手法と比較しても推測攻撃が困難になっていること，3) 脆弱な秘密情報を考慮して確保された安全性であることが理由に挙げられる．実験条件は知人である攻撃者が秘密情報の候補を見て，被攻撃者に関して自由にインターネットを介して調査できる状態であった．そのため，攻撃者が被攻撃者についての知識を最大限活用できる状況であったと考える．また，「関連手法との比較」でも述べるが他の再認手法である Use Your Illusion の秘密情報が攻撃に成功された 10 回の試行と比較して，より多くの試行回数が必要となっている．最後に，秘密情報を推測された被験者は，複数の第三者から推測されていて，脆弱な秘密情報であったと示唆される．ユーザが自分で秘密情報を作る以上脆弱な秘密情報は作成されるという問題があるが，その脆弱な秘密情報でさえ 70 回の試行回数が推測に必要だという点は評価できると考える．

1,820 回の試行回数で特定されたペアについて考える．特定されたペアを考えることで，4 ペア全ての秘密情報を特定し攻撃に成功しなくても，3 ペアや 2 ペアの秘密情報を特定できた攻撃を考慮することができる．特定できたペア数の平均は Group-A: 1.95 ペア，Group-B: 1.79 ペア，Group-C: 1.60 ペアであった．一方で，ランダムに選択した場合は，1.42 ペア特定できる．これは，45 ペア内に 4 ペアの秘密情報が存在している場合，その中から 16 ペア選択した時に何ペアの秘密情報が存在するかを意味するため，(4/45) × 16=1.42 で求められた．比較すると，ランダムで選択した場合と各条件で特定できたペア数の差は最大で 0.52 ペアである．この結果，知識による推測はランダム選択と比較して 1 ペア以上増加していないことから，被験者に関する知識が推測する際に，回答候補が決定的な手がかりを与えていないことを示唆している．

次に，1,820 回の試行における攻撃成功率について述べる．1,820 回の試行における推測攻撃成功率は最大で 9.52%であった．2.3 節であげたパスワードに対するシミュレーションは多くの試行回数においてそれぞれ何%推測可能であったか評価している．サンプル数や条件が異なるため一概に比較できないが，結果としてパスワードよりも提案手法の推測攻撃成功率は高い．しかし，再認方式で記憶可能性が高く，回答候補が提示されている状態で 1,820 回の攻撃成功率が最大 9.52%(表 4 参照) であることは評価できると考える．

1,820 回の試行における攻撃成功率と間の差について述べる．各グループと攻撃成功率の関係に有意差はなかった．被攻撃者と攻撃者が知人である場合は推測に有利だと仮定していたが，攻撃者と被攻撃者の関係が推測攻撃の成功率に影響しないとわかった．また，有意差はなかったが，攻撃者と被攻撃者が知人同士である Group-B より知人でない Group-C の方が低い攻撃成功率を持つという結果も

あった．これは，「2 つの単語の関連」が知人であっても推測に有利に働かない秘密情報ということを示唆している．

関連手法との比較

実験の結果，提案手法は「秘密情報登録から 4 週間後の利用，2 週間間隔での利用でも秘密情報保持に支障なく利用できること」，「70 試行までは推測攻撃耐性を確保していること」がわかった．以下で，記憶可能性と推測攻撃耐性に関して関連研究との比較を行い，提案手法が記憶可能性と推測攻撃耐性について，利点を維持して，より記憶可能で推測攻撃耐性を持つ手法であることを示す．

Use Your Illusion と比較をする．Use Your Illusion は登録後 3 回の認証を求め，それは 2 日後と 1 週間後と 4 週間後であった．その結果，全ての被験者が認証に成功し，最大 3 週間間隔で 100%が記憶保持可能であった．Use Your Illusion と提案手法は認証間隔や回数が異なっていて一概に比較できない．Use Your Illusion は提案手法より長い最大 3 週間間隔をあけて認証していて，提案手法は Use Your Illusion と比較して認証回数 (認証頻度) が 1 回であるという差がある．しかし，ともに秘密情報登録 4 週間後の認証成功率が 100%であることから同等程度の記憶可能性だと考える．推測攻撃耐性に関しては，Use Your Illusion が 10 回の試行で 15 人中 1 人が攻撃成功したのに対して，提案手法は 70 回の試行までは推測攻撃に成功しなかった．この結果は，提案手法の方が高い推測攻撃耐性を持つことを示唆している．したがって，提案手法は Use Your Illusion の記憶可能性を維持しつつ，より高い推測攻撃耐性持つ手法であると考える．

Deja Vu と比較をする．Deja Vu の記憶可能性については，評価実験において 1 週間間隔で 90%が記憶保持可能であることが示された．提案手法と比較すると Deja Vu に関しては記憶保持できている被験者が 90%であったため，記憶可能性が提案手法と比較して低い．Deja Vu は推測攻撃の評価実験を行っていないため推測攻撃耐性は定かではなく，比較をすることができない．また，ユーザが画像を用意しないため推測攻撃耐性が高いという点もあるが，秘密情報にする画像はユーザが選択するため，好みの色や形で偏りが生じる可能性がある．したがって，提案手法は Deja Vu より高い記憶可能性を持つ手法であると考える．推測攻撃耐性については，定かではないが，Deja Vu においても推測攻撃が可能であることを示した．

5.2 その他の有用性と安全性

本節では，入力時間とその他の安全性 (総当たり攻撃，逆総当たり攻撃，覗き見攻撃，汚れ攻撃，フィッシング攻撃) について議論する．

入力時間

入力時間について考察する．ここでは Exp2，Exp3 の入力は想起が影響し人によってバラツキがあるため，もっともバラツキが少ない Exp1 の認証時間をシステムの入力時間として考える．よって，入力時間は平均値が 14.4 秒，中央値が 13.9 秒であった．入力時間は平均値より中央値の方が小さく，入力時間が他と比較して長い人がいることが示唆される．

次に関連研究の入力時間と比較する．評価実験における平均入力時間は Deja Vu が 32 秒であり，Use Your Illusion が 12.4 秒であった．したがって，提案手法と関連研究の入力時間は長い順に Deja Vu ＞ 提案手法 ＞　Use Your Illusion である．これは秘密情報がそれぞれ，Deja Vu: 5 枚の抽象画，提案手法: 単語の 4 ペア，Use Your Illusion: 3 枚の画像であったことから，入力に必要な操作の回数が理由だと考える．また，提案手法は認証の度に単語の配置が異なる (以下で説明する汚れ攻撃対策) ため，単語を探す時間が必要となるのも理由だと考える．他の手法比較して，提案手法は認証時間が短いと言い難いため，入力時間の短縮方法が今後の課題となる．

総当たり攻撃

次に，総当たり攻撃への安全性について考察する．プロトタイプシステムでは秘密情報の候補として，10 単語群がシステムに提示される．故に，作成可能な単語ペアの総数は ${}_{10}\mathrm{C}_2 = 45$ ペアである．ユーザはこの 45 ペアの中から 4 ペアを選択するため，選択可能な場合の数は ${}_{45}\mathrm{C}_4 = 148,995$ 通りである．よってランダムに入力した場合，認証に成功する確率は 148,995 の逆数であると言える．提案手法の場合の数は，認証システムとして実用化されている 4 桁 PIN の場合の数である 10,000 通りよりは高いため，利用可能な範囲であると考える．

逆総当たり攻撃

「逆総当たり」攻撃とその安全性について議論する．この攻撃は，多くのユーザが同一の秘密情報を利用していることを想定した攻撃である．多くのユーザが利用していると推測される 1 つまたは少数のパスワードを用い，多数のユーザに対して”なりすまし”を試みる．この攻撃方法では，各ユーザに対してなりすましを少数回しか試行しないため，規定回数以上認証に失敗すると認証不能となるアカウントロック機構も無意味である．

この攻撃方法に対する根本的な対策は，利用者が定義する秘密情報が同種のものに偏らないことである．これについて推測攻撃実験で攻撃対象とした 21 名の秘密情報を分析した．つまり，被験者が設定した秘密情報に重複がなければ，それは秘密情報の偏りがなく，結果として当該攻撃への安全性がある，と考えられるからである．解析結果は以下の通りとなった．

- 秘密情報の「単語ペア」単位での重複: なし
- 秘密情報に用いられた「単語」単位での重複: 210 単語中，20(9.5%) 単語が重複
- システムに登録された「単語」単位での重複: 210 単

語中，27 単語 (12.9%) が重複

単語に重複が存在するものの，単語ペアとしての重複はなかったことは．当該攻撃への安全性に対する懸念は少ない可能性が示唆される．さらなる検証が必要だと言えるが，連想情報による秘密情報は，逆総当たり攻撃に対する安全性を確保しうる可能性があると考える．

覗き見攻撃

覗き見攻撃は，ユーザの秘密情報入力を攻撃者が覗き見ることで秘密情報を窃取する攻撃手法である．提案手法は覗き見攻撃耐性については考慮しておらず，脆弱なままである．この脅威に対する対策は今後の課題である．

汚れ攻撃（smudge attack)

汚れ攻撃は，タッチパネル上に残った操作痕跡から，秘密情報を特定する攻撃である．この痕跡により秘密情報が特定可能になる理由は，入力操作が常に同じなためである．汚れ攻撃耐性を確保するため，提案手法では単語の表示位置を認証試行のたびにランダムに変化させ，見た目上の入力操作を毎回異なるものにしている．この設計により，提案手法は逆総当たり攻撃に対する安全性を確保している．

フィッシング攻撃

フィッシング攻撃についても，既存の知識照合型個人認証と比較すると，攻撃しがたい認証手法であると考えている．パスワードなどの手法は全てのユーザが共通の入力画面を利用するため，フィッシングサイトを作成しやすい．一方，提案手法は認証画面に提示される解答候補群がユーザによって異なる．そのため攻撃者は，標的とするユーザの単語群を把握してから，そのユーザのためだけのフィッシングサイトを作成する必要がある．したがって提案手法は，フィッシング攻撃をパスワードなどの手法と比べて困難にする効果があると言える．

5.3 今後の課題

今後の課題として，プロトタイプにおける問題点の改善と，プロトタイプの拡張について述べる．プロトタイプにおける問題点とその改善に関する課題として二点述べる．1 つは入力時間の短縮方法の検討である．5.2 節で述べた通り，入力時間は短いとは言い難い．ここには一部の攻撃手法に対する安全性と入力時間とのトレードオフが存在するため，より良いバランスを実現しうる入力手法，または安全性対策を検討する必要がある．もう 1 つは覗き見攻撃である．現状の提案手法では，本脅威に対しては脆弱なままであり，対策を考えていく必要がある．

また，プロトタイプの拡張は以下の二点を検討する．

- 回答候補の情報種の多様化: 現在は文字で，かつ名詞の 1 単語であるが，今後はそれ以外の情報種の活用についても検討する．
- 連想情報の拡張: 現在は単語によるペア情報に限定しているが，それ以外の連想情報の利用 (例えば 3 情報によるグループ化) について検討する．

6. おわりに

本研究では秘密情報として「既知の私的な連想情報」を用いて，再認方式でありながら記憶可能性と推測攻撃耐性を両立する個人認証を目指した．プロトタイプシステムを実装して，記憶可能性と推測攻撃耐性について評価実験を行った．その結果，秘密情報登録 4 週間後の利用，2 週間間隔での利用でも秘密情報保持に支障なく利用できることがわかった．推測攻撃耐性については，より多くの攻撃試行が実現可能な手法を用いて，70 試行までは推測攻撃耐性を確保していることを示した．再認方式の関連研究と比較し，記憶可能性と推測攻撃耐性の利点を維持しつつ，より記憶可能で推測攻撃耐性を持つ手法であることを示した．また，最後に他の有用性や安全性についても議論を行った．今後の課題として，入力時間と覗き見攻撃耐性に関する問題の改善と，プロトタイプシステムの拡張 (情報種の多様化，連想情報の拡張) について検討していく．

参考文献

[1] Dhamija, R. and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, 9*th USENIX Security Symposium*, pp.4558 (2000).

[2] Hayashi, E. Christin, N. Dhamija, R. and Perrig, A.: Use Your Illusion: secure authentication usable anywhere, *Proc. 4th symposium on Usable privacy and security*, pp.35-45(2008).

[3] Hayashi, E. Hong, J. and Christin, N.: Security through a different kind of obscurity: evaluating distortion in graphical authentication schemes, *Proc. Human Factors in Computing Systems*(*CHI*'11), pp.2055-2064(2011).

[4] Bradshaw, G. and Anderson, J.: Elaborative encoding as an explanation of levels of processing, *Verbal Leading and Verbal Behavior*, Vol.21, Issue 2, pp.165-174(1982).

[5] Smith, S.: Authenticating Users by Word Association, *Computers & Security*, Vol.6, Issue 6, pp.464-470(1987).

[6] Pond, R. Podd, J. Bunnell, J. and Henderson, R.: Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates, *Computers & Security*, Vol.19, Issue 7, pp.645-656(2000).

[7] Melicher, W. Ur, B. Segreti, S. Komanduri, S. Bauer, L. Christin, N. and Cranor, L.: Fast, Lean, and Accurate:Modeling Password Guessability Using Neural Networks, 25*th USENIX Security Symposium*, pp.175-191(2016).

[8] Bonneau, J.: The science of guessing: analyzing an anonymized corpus of 70 million passwords, *Proc. 2012 IEEE Symposium on Security and Privacy*, pp.538-552(2012).