似顔絵認証: 情報認知の個人差を用いた記憶照合型個人認証への推測攻撃に対する安全性向上策の提案

益尾 文里† 高田 哲司†

†電気通信大学
182-8585 東京都調布市調布が丘 1-5-1
masuo @ az.inf.uec.ac.jp and zetaka @ computer . org

あらまし 記憶照合型個人認証への攻撃方法の１つに推測に基づくパスワード破りがある．辞書攻撃や類推攻撃はその一例と言えよう．この攻撃への対策として我々は「情報認知の個人差」を秘密情報に応用した認証手法を提案する．この対策方法により，攻撃者が複数回の推測を成功しないと秘密情報の特定ができなくなり，結果として推測攻撃に対する安全性が向上する．このアイデアに基づき似顔絵を秘密情報とした認証システムを実装し，利用可能性と安全性に関して被験者による評価実験を実施した．

A Countermeasure for a Password Guessing Attack in Knowledge-based User Authentication by a Personal Difference in Information Recognition

Fumisato Masuo† Tetsuji Takada†

†The University of Electro-Communications
1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, JAPAN
masuo @ az.inf.uec.ac.jp and zetaka @ computer . org

Abstract Password cracking is a practical issue in knowledge-based user authentication. Especially password guessing attack, such as dictionary attack, is a major methods in this type of attack. To counter this type of attack, we try to apply “a personal difference in information recognition” to a user authentication. This makes password guessing more hard because attackers have to guess a victim’s secret more than one times. In this paper, we use a deformed portrait as a secret in a user authentication. In this system, attackers have to succeed two guesses in order to impersonate a victim: 1) Whose face is a secret?, 2) How a face is illustrated to a portrait? We implemented a prototype authentication system and conducted a user study to evaluate memorability of a secret and security level to a guessing attack.

1 はじめに

本論文では記憶照合型個人認証に対する脅威の一つである「推測攻撃」に対する対策手法として「情報認知の個人差」を応用した認証手法を提案する[1].「情報認知の個人差」とは，特定の情報をどう認知し解釈するかは人によって異なるということを指す．この仕組みを個人認証

[1]第一著者は大学を卒業し，現在民間企業に勤務．本論文中では研究実施時の所属にて記載

の秘密情報に応用することにより，個人認証における秘密情報の推測可能性を低減する手法を提案する．また提案する手法に基づいてプロトタイプシステムを実装し，それを用いて個人認証システムとしての継続利用可能性と推測攻撃に対する安全性について被験者実験を実施した．以降、本論文では 2 章で推測攻撃について述べ，3 章でその対策として情報認知の個人差の応用について説明する．4 章では本研究で実装した認証システムについて説明し，5 章で実装システムによる被験者実験について述べる．6 章で実験結果や今後の課題について考察する．

2 記憶照合型個人認証における推測攻撃

記憶 (知識) 照合型個人認証には様々な攻撃方法が存在する．本論文では個人認証システムそのものに対する攻撃方法に着目し，認証システムで利用される通信経路上での盗聴やマルウェアによる秘密情報の窃盗，ソーシャルエンジニアリングによる秘密情報の聞き出しなどを検討対象外とし，パスワードクラッキング (パスワード破り) に注目する．パスワードクラッキングには以下の 3 つの手法が知られている．

1. 総当たり攻撃 (brute-force attack)
2. 辞書攻撃 (dictionary attack)
3. 類推攻撃 (guess attack)

これら 3 つの攻撃方法のうち，総当たり攻撃を除く残りの 2 つは推測攻撃と考える．類推攻撃とは，認証システム利用者の様々な属性や趣味、所有物に関する情報を秘密情報として使用していると想定し，それらの情報に基づく文字列をパスワード候補として攻撃，すなわちログインを試みる方法である．この攻撃方法で用いられる秘密情報候補の代表的な例としては攻撃対象者の生年月日や電話番号，自宅/職場等の居室番号，好きな有名人の姓名等が考えられる．これらはまさに個人情報に基づく推測攻撃であると言える．

一方、辞書攻撃とは認証システム利用者が自然言語における一般的な単語を秘密情報として使用する傾向があることを利用し，辞書に掲載されている単語やそれらの単語の組み合わせ，単語を基にしたいくつかの手法による小変更を施した単語等をパスワード候補として攻撃を行う手法である．とある Web サイトから漏えいしたパスワードを調査した結果 [1] によると，一部の利用者は “Password”,“princess”,“rockyou” といった単語や単語列を秘密情報にしていたことが明らかになっている．また Yahoo のサービスから漏えいした 45 万件ものアカウント調査 [2] でも同様の結果が得られている．これらの事実から，推測に基づく攻撃手法が無作為に生成するパスワードで攻撃するよりも，攻撃成功率が高いことは明らかであり，この性質を応用し，パスワード辞書を利用した攻撃用ツールも存在する [3, 4].

3 推測攻撃対策: 情報認知の個人差の応用

推測攻撃が成立しないようにする方法は 2 つあると考える．一つは秘密情報の推測を無意味にする方法である．具体的な方法としては認証システムが秘密情報を無作為に決定し，認証利用者にその利用を強要する方法がある．別の言い方をすれば，個人認証における秘密情報を利用者に決定させない方法である．この方法ならば，秘密情報と認証利用者の属性情報や人間の行動傾向との間にはなんの関連もなくなるため，秘密情報の推測行為は無意味となる．

しかしながら，この対策方法は推測攻撃に対する安全性が改善する一方で，記憶保持にかかわる利便性を阻害する方法でもある．無作為に決定された秘密情報を確実に記憶し，必要に応じてその秘密情報を正確に想起することが可能な人間は少数派であろう．したがって，この対策方法は現実的な手法ではないと言わざるを得ない．

もう一つの改善方法は，秘密情報の推測をより困難にする方法である．

なぜ認証利用者は自身の属性情報から類推可

能な情報を秘密情報に割り当てるかというと，記憶保持のためである．人間は記憶した事柄同士を関連付けて記憶しており，これを連想記憶と呼ぶ．この能力を個人認証における秘密情報の記憶に応用して記憶保持に努めている．それゆえ人は「秘密情報⇒息子の誕生日⇒ 0824」というように類推により推測されやすいが記憶保持は可能な情報を秘密情報として設定する傾向にある．

この考察から記憶照合型個人認証において推測攻撃が成立する原因は，秘密情報の記憶保持のために利用者がしている工夫にあると言える．しかし記憶照合型個人認証は，利用者が秘密情報を記憶することが大前提である．よって記憶保持の観点から秘密情報は利用者が設定するという特性は維持しつつ推測攻撃への安全性を高める方法を模索した．そして，その一方法として秘密情報の特定に複数回の推測が必要になる秘密情報の利用を考えた．

認証方法を複数回の問いと回答による構成にすれば，秘密情報の特定に複数回の推測が必要になる．しかし，これは記憶負担や認証操作の面で負担が増えるため望ましくない．望ましいと考える秘密情報は，正規の認証利用者にとっては単に秘密情報を記憶するだけだが，攻撃者にとっては 1 回ではなく複数回の推測が成功しないと秘密情報の特定が困難な特性を持つものである．また攻撃者が秘密情報を推測する際，その候補となる選択肢が多いことが望ましい．例えば「漢字一文字とその書き順」が秘密情報だとする．この場合，攻撃者はどの漢字が秘密情報か? という第一段階の推測では十分な数の選択肢があるが，第二段階の推測である “書き順” では，多数の人が既定の書き順を秘密情報にしてしまう可能性が高く，選択肢が十分あるとは言いがたい．

そこで本研究では「情報認知の個人差」の応用を考えた．「情報認知の個人差」とは，ある情報を人間が知覚した際，その情報をどのように認知したかは個人差がある．という特性のことを指す．例としては「ロールシャッハ・テスト」が挙げられる．このテストは視覚による情報認知の個人差を人格分析に利用したものである．これと同様の事象は視覚だけでなく聴覚や味覚でも起こりうる．この中で本研究では個人認証の秘密情報として「似顔絵」を選択した．理由は 2 つあるが，それらはどちらも前述の特性を満たしうると考えたからである．まず 1 つめは情報認知の個人差が生じ，かつ個人差による選択肢数が多いという点である．似顔絵ならば同一人物を対象としても，その人物を各個人がどう認知し、似顔絵としてどう抽象化するかによって様々な似顔絵が作成されうると考えたからである．2 つめは記憶保持の観点から望ましいと考えたためである．人間は人間の顔を記憶するための特別な能力を持つことが知られており [7]，その能力を活用した記憶照合型個人認証システム [8] も存在する．このことから，記憶保持の実行可能性はあると考えている．

また認証利用者と攻撃者との秘密情報に対する負担は非対称になりうると考えている．認証利用者の作業は，秘密情報にする人物を決定し，その人物の似顔絵を作成して記憶することである．特定人物の似顔絵を記憶するだけであり，秘密情報が複数になるわけではないので，既存の記憶照合型個人認証と比較して大幅に記憶負担が増えるわけではないと考える．一方，攻撃者にとっては二段階の推測に成功しないと秘密情報が特定できなくなるため推測攻撃の難易度が高くなる．一段階目の推測は，認証利用者が秘密情報にしている人物を推測することであり，二段階目の推測は，秘密情報にしている人物の似顔絵を推測することになるからである (図 1)．つまり，仮に認証利用者の趣味や人間関係等か

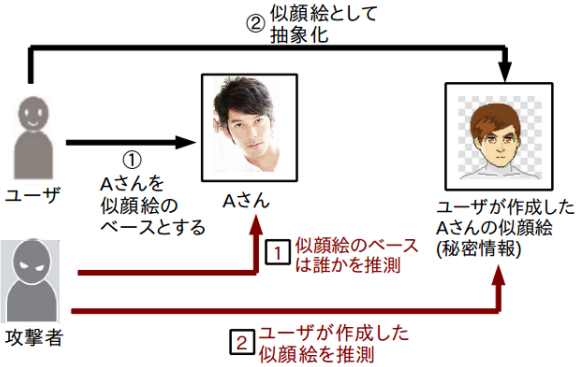

図 1: 推測攻撃の困難性

ら秘密情報にしている人物が特定できたとしても，さらにその人物の似顔絵を推測しなければ秘密情報の特定にならない．したがって，単に秘密情報である人物を推測するよりも推測攻撃による安全性が向上することになる．

4　似顔絵認証システム

本研究では，3 章の考察を基に似顔絵を用いた個人認証システムを実現した．本章では実装した個人認証システムについて述べる．

個人認証の秘密情報に似顔絵を用いるとはいえ，認証のたびに似顔絵を描かせるのは認証時間が長くなるため現実的ではない．また認証のたびに秘密情報として設定した似顔絵と一定の確度で同じ似顔絵を描画できる人は一部の人に限られるであろう．とはいえ推測攻撃に対する安全性向上の観点から認証画面において多種多様な似顔絵が作成できることが望ましい．そこで本研究では，犯罪者の手配写真を作成する際に用いられるモンタージュ手法を認証手法とした．つまり目，はな，くち、髪型など顔の各パーツについて多種多様な似顔絵パーツを用意し，それらの組み合わせにより秘密情報である似顔絵を再現する方法である．図 2 に実装した似顔絵認証の認証画面を示す．

この画面はユーザ名を入力すると表示される．画面内には「りんかく」「髪型」「まゆげ」「目」「はな」「くち」の 6 つの部位について，それぞれ 5 つの選択肢を提示している．認証利用者は，それぞれの部位について，利用者自身が事前に設定した似顔絵を再現するよう各部位の選択肢から 1 つづつ選択する．選択された各パーツにより構成される似顔絵は画面左上の欄に合成されて表示されるので，認証利用者が選択肢による似顔絵が確認可能となっている．全ての部位に関する選択肢を選択し終わったら，画面左上にある「認証完了」ボタンを押す．このボタンによって検証処理が実施され，事前に設定した似顔絵と一致したら認証成功となる．

なお本システムで使用している顔の各部位のパーツ画像は「似顔絵イラストメーカー」という Web サービス [5] から利用許諾頂いた上で使

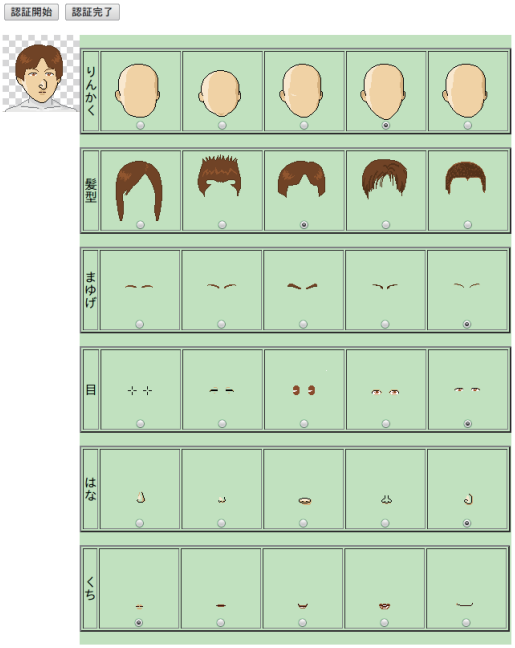

図 2: 似顔絵認証: 認証画面

表 1: 各部位のパーツ画像数

部位	りんかく	髪型	まゆげ	目	はな	くち
画像数	30	91	29	83	36	59

用している．そのため各部位のパーツ画像総数は表 1 に示す通りばらつきがある．図 2 の画面例では各部位に対する選択肢数はそれぞれ 5 つだが，この選択肢数は各部位で同一数にするという条件を置くのであれば 29 個まで増やすことが可能である．これは認証に求められる安全性に応じて変更することが可能である．

なお本システムにおいて秘密情報の似顔絵を構成するパーツ画像以外の選択肢として表示される画像を「おとり画像」と呼ぶことにするが，このおとり画像は秘密情報である似顔絵を構成するパーツ画像以外の画像群からランダムに選択した．

5　評価実験

本章では 4 章で述べた実装システムを使用して実施した被験者による評価実験とその結果について述べる．

5.1 評価実験概要

評価実験では，以下の 2 つの点を評価した．

- 実験 A) 利用可能性
  既存の認証手法とは異なる認証方法なので，一般の利用者が継続して認証処理可能かについて評価する．
- 実験 B) 安全性
  推測攻撃への安全性向上が意図通り実現されているかについて実際に攻撃を実施して評価する．

各実験における被験者の構成は表 2 の通りである．なお被験者は 40 代の被験者 1 名をのぞき全て男性である．

表 2: 被験者の構成

実験種別	20 代	30 代	40 代	50 代	合計
実験 A	3	2	1	1	7 名
実験 B	5	2	1	1	9 名

実験 A の実施方法について説明する．まず始めに各被験者に認証における秘密情報として似顔絵を決定してもらった．似顔絵は Web サービスである「似顔絵イラストメーカー」[5] を使用して作成させた．この時点では当該 Web サービスが提供するすべてのパーツ画像を利用可能とし，似顔絵作成の自由度は高くした．したがって被験者にとっては自身で決定した人物になるべく似通った似顔絵が作成できるように配慮した．

次に認証を実施させた．認証処理は 4 章で述べた通りである．一回の認証実験では 3 回までの試行を認めた．つまり 2 回までの認証失敗は許容し，3 回連続で失敗した場合を認証失敗とした．これは既存の銀行 ATM と同じ条件である．また一定の空白期間のあとでも認証可能かを調査するため，図 3 のタイムラインに従い、8 日間にわたり 3 回の認証実験を実施した．

また認証画面として 2 つの設定による画面を実験 A では利用した (表 3)．したがって理論的な安全性，すなわちランダムに選択した回答が正解となる確率は表 3 より Interface 1 が $22^3 = 10,648$ より 1/10,648 となり，Interface 2 では

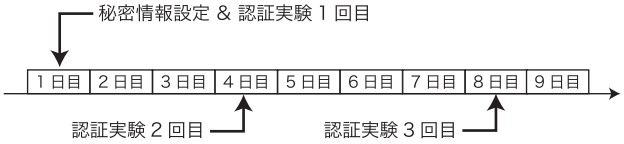

図 3: 実験 A におけるタイムライン

表 3: 実験 A における 2 つの認証インタフェース

	Interface 1	Interface 2
顔の部位数	3	6
部位毎の選択肢数	22	5

$5^6 = 15,625$ なので 1/15,625 となる．これは 4 桁暗証番号による個人認証の安全性と同等以上になることを基準として画面構成を決定したためである．

また各 Interface で使用した顔の部位だが，Interface 1 では顔の部位として「髪型，目，まゆげ」を使用し，Interface 2 では Interface 1 の部位に加えて「鼻，口，輪郭」を使用した．Interface 2 の認証画面例は図 2 と同一である．各 Interface において，それらの顔部位を選択した理由について述べる．顔の形態特徴を自由記述を日本人と英国人に対して実施した研究結果 [6] がある．その結果，どちらの国民においても程度の差はあれ顔の特徴として記述した部位の上位 3 つは「髪型，目，まゆ」であった．この結果を参考にし，Interface1 では「目，髪型，まゆげ」を使用し，Interface 2 ではそれに加えて「鼻，口，りんかく」を選択した．なお実験 A では 7 名の被験者を Interface 1 に 3 名，Interface 2 に 4 名とグループ分けして実験を行った．

つづいて実験 B の実施方法について説明する．実験 B では本論文の第一著者を被攻撃者とし，各被験者に攻撃者としてなりすまし攻撃を実施させた．具体的には Interface 2 の認証システムを使用し，被験者に第一著者の似顔絵を 3 回推測させた．なお各被験者と被攻撃者との間柄は，同一研究室内の同級生，アルバイト先の社員そして第一著者の両親であり，すべての被験者は第一著者の顔を良く知る人物達である．被験者の人数と年齢構成は表 2 で示した通りであり，性別は 40 歳代の被験者を除いて全員男

性である．また認証画面に提示する顔パーツ画像は全被験者で同一画像群を使用した．

5.2 実験結果

まず始めに実験 A の結果について述べる．8 日間にわたる 3 回の認証実験の結果は表 4,5 の通りになった．それぞれの Interface による認証実験において若干数の試行失敗があるものの，すべての被験者が 3 回までの試行で認証に成功した． またこの実験での興味深い結果として，認

表 4: 実験 A - Interface 1 の認証結果

被験者	1回目 (1日目)	2回目 (4日目)	3回目 (8日目)
20代	1回目 × 2回目 ○	1回目 × 2回目 ○	○
40代	○	○	○
50代	1回目 × 2回目 ○	1回目 × 2回目 ○	1回目 × 2回目 × 3回目 ○

表 5: 実験 A - Interface 2 の認証結果

被験者	1回目 (1日目)	2回目 (4日目)	3回目 (8日目)
20代	○	○	○
20代	1回目 × 2回目 ○	1回目 × 2回目 ○	○
30代	○	○	○
30代	○	○	○

証失敗時の選択ミスが特定の部位に偏っていた点である．Interface 1 による実験 (表 4) での合計 6 回の認証失敗はすべて「まゆげ」の選択ミスであり，Interface 2 による実験 (表 5) での 2 回の認証失敗はすべて「鼻」の選択ミスであった．

次に認証成功時の所要時間を被験者別の折れ線グラフで示す．図 4 は Interface 1 の被験者 3 名分の 3 回の認証実験における認証成功時の所要時間の推移を表している．図 5 は，Interface 2 における認証成功時の所要時間の被験者別推移を示す． 3 回目の認証実験における所要時間の平均値で比較すると，Interface 1 が 39.0 秒，Interface 2 が 22.5 秒となった．

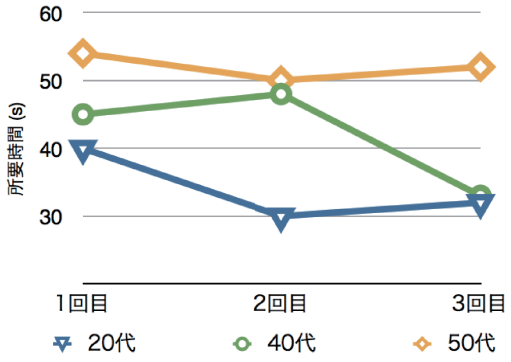

図 4: 認証成功時の認証時間の推移:Interface 1

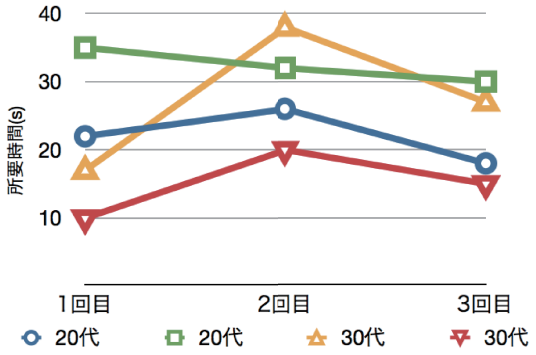

図 5: 認証成功時の認証時間の推移:Interface 2

次に実験 B の実験結果を述べる．実験 B では第一著者の似顔絵が秘密情報であるとわかっていることを前提とし，第一著者の Interface 2 による認証画面を利用して被験者に秘密情報を推測させた．実験では攻撃者 (=被験者) が推測した似顔絵と正解である似顔絵とを比較し，誤回答であった顔部位を記録した．実験結果を表 6 に示す．結果として 3 回の推測攻撃で秘密情報である似顔絵を正確に推測できた被験者は 0 人であった．この合計 27 回 (9 名 x 3 回) の推測攻撃において，各顔部位が誤回答として含まれていた回数を集計し，グラフ化したのが図 6 である．この結果から最も誤回答が多かったのは「まゆげ」であり,「髪型」については一度も誤回答がなかった．

表 6: 推測攻撃実験結果: 誤回答の顔部位

被験者	攻撃1回目	攻撃2回目	攻撃3回目
20代	まゆげ	まゆげ	まゆげ
	はな	はな	はな
20代	りんかく	りんかく	りんかく
	まゆげ	まゆげ	まゆげ
	目	目	
		はな	はな
	くち	くち	
20代	りんかく		くち
	まゆげ	まゆげ	まゆげ
	はな	はな	はな
20代	りんかく	りんかく	りんかく
	まゆげ	まゆげ	まゆげ
	目		目
	はな	はな	はな
		くち	くち
20代	まゆげ	まゆげ	まゆげ
	はな	はな	
30代	まゆげ	まゆげ	
	はな	はな	はな
	りんかく	くち	くち
30代		りんかく	
	まゆげ	まゆげ	まゆげ
	はな	はな	はな
	くち	くち	
40代	りんかく	りんかく	りんかく
	目		目
	くち	まゆげ	まゆげ
50代	りんかく		
	まゆげ		
	目	目	目
	くち	はな	はな

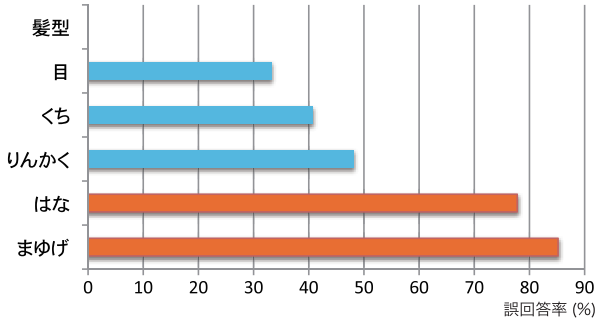

図 6: 顔の各部位毎の誤回答率

6 考察

6.1 実験結果について

実験 A の利用可能性について認証 Interface を 2 つ用意し被験者を分けて実験を実施した理由は，正規の利用者にとって部位数と選択肢数のどちらが多い方が認証成功率が高いかを検証するためであった．結果としては Interface 2，すなわち各部位の選択肢数が少ない方が正規利用者の認証失敗率が低かった．今回の実験では 2 種類の Interface で検証を行ったため，各部位の選択肢数が少なく，かわりに顔の部位数が多い認証画面の方が記憶負担を増大させず，また所要時間も短くなるという結果となった．しかし認証画面の構成として，理論的安全性，記憶可能性および所要時間に配慮しつつ「部位数」と「各部位の選択肢数」のよりよい構成法を追求するのは今後の課題の 1 つである．

実験 B の推測攻撃に対する安全性についてだが，似顔絵の推測に一人も成功しなかったのは予想外であった．実験条件は，以下に述べる通り攻撃者にとって優位な条件を設定したからである．1) 推測すべき似顔絵は第一著者の顔を素直に似顔絵化したものであり，推測を困難にするような工夫はしなかった．2) 被験者全員が第一著者の顔を良く知っており，それぞれが自信をもって似顔絵作成できる人達であった．3) Interface 2 の認証画面を利用し，顔の各部位の選択肢はそれぞれ 5 つに絞られていた．また図 6 より推測が困難な部位はその推測の困難さに応じてまゆげ，はなと目、くち、りんかくの 2 つのグループに分類されることもわかった．この結果から言えることは，提案手法により推測攻撃に対する一定の安全性は確保しうる可能性が高いと考えられる．

6.2 関連研究

推測攻撃の脅威は Social Networking Service の普及とともに拡大しつつある．単語ではなくなんらかのフレーズの頭文字を接続したパスワードを使用したとしてもインターネットから得られるフレーズを基に辞書を作成した結果，40 万個のパスワード辞書で調査対象のフレーズベースのパスワードの 4 研究がある [9]．このように従来安全だと言われていた秘密情報でも今後は推測による攻撃が可能になる可能性がある．

また似顔絵を用いた個人認証の研究事例としてCOMPASS[10]がある．この認証システムは人の似顔絵を秘密情報とした画像認証システムであり，顔そのものが認証画面に提示されるため，推測攻撃に対する対策にはなっていない．

7 おわりに

本論文では，記憶照合型個人認証に対する推測攻撃に着目し，その攻撃を困難にする方法として「情報認知の個人差」を応用した対策方法を提案した．この特性を利用することにより，攻撃者は秘密情報を特定するために複数回の推測を成功させる必要が生じるためである．この提案に基づき，好きな人物の似顔絵を秘密情報としモンタージュ形式による認証システムを実装した．さらにそのシステムを用いて被験者による評価実験を実施した．その結果，8日間にわたる認証実験では被験者全員が3回までの試行で認証に成功した．また推測攻撃実験では，攻撃者にとって有利な条件にしたにもかかわらず一人も似顔絵の推測に成功しなかった．これらの結果から，推測攻撃の困難な記憶照合型個人認証手法として有望であると言える．

今後はより詳細な被験者実験を実施しつつ，秘密情報の記憶負担と推測攻撃への安全性の双方をよりよいバランスで実現しうる認証画面の構成を模索する必要がある．また単なる似顔絵ではなく感情などの要素も秘密情報に取り込み推測困難性をさらに改善する方法についても検討を進める予定である．

謝辞

本研究の遂行にあたり，Webサービス「似顔絵イラストメーカー」の顔パーツ画像の研究利用を快く許諾して下さったAbiStudio株式会社の阿比留様に感謝致します．

参考文献

[1] Imperva: “Consumer Password Worst Practices” (online), 入手先 <http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf> (参照 2012-08-10)

[2] Anders Nilsson: “Statistics about Yahoo leak of 450.000 plain-text account” (online), available from <http://blog.eset.se/statistics-about-yahoo-leak-of-450-000-plain-text-accounts/> (accessed 2012-08-10)

[3] Openwall: “John the Ripper password cracker” (online), available from <http://www.openwall.com/john/> (accessed 2012-08-10)

[4] Foofus Advanced Security Services: “Medusa Parallel Network Login Auditor” (online), available from <http://www.foofus.net/ jmk/medusa/medusa.html> (accessed 2012-08-10)

[5] AbiStudio.com: “似顔絵イラストメーカー” (online), available from <http://illustmaker.abi-station.com/> (accessed 2012-08-10)

[6] 吉川左紀子，益谷 真，中村 真 (編): 顔と心 - 顔の心理学入門 -，pp.222-245，サイエンス社 (1993).

[7] 角南 典生: “顔の記憶は特別扱い” (online), available from <http://www.kyoukaikenpo.or.jp/13,85393,109,670.html> (accessed 2012-08-10)

[8] Passfaces Corp.: “Passfaces: Two factor authentication for the Enterprise” (online), available from <http://www.realuser.com> (accessed 2012-08-10)

[9] Cynthia K., Sasha R. and Lorrie F.C.: Human selection of mnemonic phrase-based passwords, Proc. of the 2nd symposium on Usable privacy and security (SOUPS ’06), ACM, pp.67-78 (2006).

[10] 横田可奈子，米倉達広: COMPASS(COMmunity Portrait Authentication SyStem) の評価, インタラクション 2006, 情報処理学会, available from <http://www.interaction-ipsj.org/archives/paper2006/pdf2006/interactive/paper0125.pdf> (accessed 2012-08-10)