個人認証システム「あわせ絵」の安全性と利便性に関する評価実験

高田哲司[†] 大貫岳人[††] 小池英樹[††]

本論文では，写真を用いた個人認証システム「あわせ絵」の安全性と利便性に関して行った評価実験について述べる．あわせ絵はユーザの秘密情報として写真を用い，かつ提示選択方式という手法を採用することで，知識照合型認証方式の安全性と利便性の改善を目指したシステムであるが，その主張を実証する評価実験が行われていなかった．そこで我々は，その両面に関して客観的な度合いを知るために被験者による評価実験を行った．実験結果から，利便性については暗証番号やパスワード，そしてランダム画像と比較しても写真の方が長期記憶が可能であり，かつ認証の使用頻度が低くても安定して認証を行い続けられることが明らかになった．さらに，秘密情報を更新しても，その認証成功率が低下しにくい特性を持つことも明らかになった．一方，脆弱性に関しては，本手法に特有の攻撃に対して脆弱であることが確認された．そしてその脅威の度合いは，既存の認証と比較しても無視できない程度であることが明らかになった．

A User Evaluation Study about Security and Usability of Awase-E

Tetsuji Takada,[†] Takehito Onuki[††] and Hideki Koike[††]

In this paper, we describe about user experiments about Awase-E. We implemented a web-based prototype system of Awase-E. Using this system, quantitative user experiments on usability and vulnerability were conducted. From the results of these experiments, it was clearly shown that photos are easy to memorize and recall over a long period of time, and people do not confuse their pass-images between old and new one after updating it. It was also show that, however, the Awase-E is vulnerable in typical attack methods for this kind of authentication scheme. The experiments on vulnerability showed that what are the vulnerabilities and how vulnerable they are.

1. はじめに

様々な個人認証が提案されている中で，画像を用いた認証方式が注目を集めている．それは知識照合型認証の欠点である「秘密情報の保持」に関する欠点を改善しうる可能性を持つためである．そこで我々は，写真を秘密情報として用いた個人認証システム「あわせ絵」[1)] を提案した．しかし，論文 1) では認証手法の提案とその理論的な安全性を述べるにとどまり，実際にその主張が妥当なものかを示す評価実験を行っていなかった．そこで我々は，システムを実装し，それを用いて長期間における認証の遂行可能性と指摘されている攻撃手法による脆弱性評価実験を行った．本論文では，この評価実験とその結果について述べ，かつそれに対する考察を行い「あわせ絵」における今後の課題を明確にした．

以降 2 章ではあわせ絵について簡単に概要を説明し，3 章では実際に行った長期記憶実験と攻撃実験の双方について，その実験方法，結果および考察を述べる．4 章ではこれらの実験結果を総括するとともに今後の課題について述べ，5 章では同種の認証手法に対して評価を行っている関連研究について述べる．

2. あわせ絵の概要

あわせ絵[1)] とは，秘密情報としてユーザが撮影した写真を使用することを前提とし，かつ照合方法として提示選択方式という手法を採用した個人認証方式である．秘密情報とはユーザ自身が正規のユーザであることを証明するための情報を意味し，既存の認証でいう暗証番号やパスワードがそれに相当する．あわせ絵の秘密情報は写真であるため，我々はそれを「パス画像」

† 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
†† 電気通信大学大学院
University of Electro-Communications

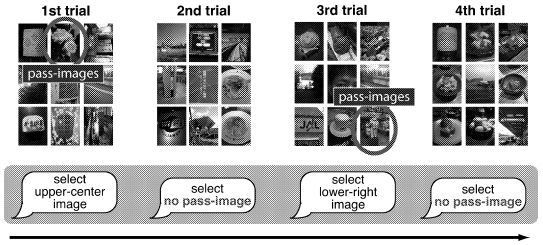

図 1 あわせ絵の認証手順
Fig. 1 Authentication sequence of the Awase-E.

と呼ぶことにする．また提示選択方式とは，回答候補を画面に提示し，その中からユーザの秘密情報を選択させるという照合方法のことを指す．あわせ絵の認証手順を具体的に説明する（**図 1**）．

あわせ絵では 1 回の認証行為において 4 回の照合作業を行う．各照合画面には 9 枚の写真が提示される．この中にはユーザのパス画像が 0 枚か 1 枚含まれる．認証をするユーザは，パス画像が含まれている場合にはそれを正しく選択し，ない場合には「パス画像なし」という回答をする．4 つの回答すべてが正解であった場合，ユーザを正規のユーザとして認証するという仕組みである．

我々は「あわせ絵」の利便性と安全性を具体的にするため，被験者による評価実験を行った．利便性に関しては，以下の 2 点を評価対象とした．

(1) 長期記憶の可能性
(2) 操作時間

また安全性に関しては，この種の認証方法に特有な攻撃として推測攻撃と抽出攻撃による攻撃実験を行った．実験に際して我々は，Web アプリケーションとして暗証番号，パスワード，そしてあわせ絵方式による認証システムを実装し，実験に用いた．ランダム画像と写真による認証実験は，どちらもあわせ絵方式による認証方法を用いた．その双方の実験における違いは，使用した画像種が異なることである．

3. 利便性に関する実験

我々は，あわせ絵の利便性を評価する実験として，ユーザがどれだけの間，秘密情報を記憶し続けることができ，その結果として認証に成功し続けられるかという実験を行った．

3.1 実 験 方 法

本実験は 2 つの被験者グループを対象にして実験を行った．1 つめの被験者グループは，講義を受講している大学院学生 35 名で，その内訳は男性 33 名/女性 2 名である．これは講義の出欠確認の一環として行ったものである．もう 1 つの被験者グループは，研究室に所属する学生 10 名で，全員 20 代男性である．

表 1 各認証手法における秘密情報の定義
Table 1 The definition of secret in each authentication method.

認証手法	秘密情報
暗証番号	4 桁数字
パスワード	6 文字以上の任意の英数文字列
ランダム画像	抽象的な画像 4 枚
あわせ絵	本人撮影による写真 4 枚

表 2 長期記憶に関する評価実験の実験条件
Table 2 The conditions of both long-term memory experiments.

被験者	講義受講者	研究室メンバー
人数	男性 33 名 / 女性 2 名	男性 10 名
ランダム画像の画像母集団	100 枚	100 枚
あわせ絵の画像母集団	140 枚 (=35 名 x 4 枚)	1240 枚 (=(10 名 x4 枚)+1200 枚)
実験実施期間	0, 2, 4, 8 週目	0, 2, 4, 8, 16 週目
試行した認証種別	各被験者はあわせ絵と残りの 3 種の認証のうちの 1 つ 計 2 種	各被験者が 4 種すべてを実施
秘密情報設定時の周知	周知した	周知なし

この 2 つの被験者グループに対し，あわせ絵認証のほかに比較対象として暗証番号，パスワードそしてランダム画像による認証を行った．なおランダム画像による認証は，手法そのものはあわせ絵認証と同一であるが，秘密情報として写真のかわりにランダム画像を用いたものである．各認証方式における秘密情報の定義は**表 1** のとおりである．

各認証方式における秘密情報の選択は，表 1 の条件を満たす範囲内で被験者の自由とした．ランダム画像については，Deja Vu [2] で使用しているランダムアートと同種の画像を主観的判断に基づき 100 枚収集し，それを画像母集団として使用した．被験者はこの母集団の中から好きな画像を 4 枚選択し，それを秘密情報とした．また，あわせ絵については各被験者が所有している写真の中から秘密情報として使用したい写真を 4 枚提供してもらい，それを秘密情報として設定した．

次に，講義受講者による実験と研究室メンバによる実験の実験条件の違いについて説明する（**表 2**）．実験条件の違いは 4 点ある．1 つめは，あわせ絵認証における画像母集団の画像構成である．講義受講者による実験では，各被験者が秘密情報として提供した写真のみで画像母集団を構成しており，結果として 140 枚（$= 35 \times 4$）の写真である．一方，研究室メンバによ

る実験では，被験者により提供された写真に著者の写真を 1,200 枚追加して画像母集団を構成した．その理由は，被験者による写真のみでは画像母集団が小さすぎることと，あわせ絵が想定している利用状況と同様の状況で評価を行いたいという意図があったためである．想定している利用状況とは，多くのユーザが画像母集団を共有しており，画像母集団はユーザから提供された多くの画像からなるという状況である．

2 つめの違いは実験実施期間である．講義受講者と研究室メンバによる実験実施期間の差は，秘密情報設定後 16 週間後の実験実施の有無である．これは講義の都合上，16 週目の実験が実施できなかったためである．

3 つめの違いは，各被験者が実施した認証種別とその数である．研究室メンバによる実験では，4 種類すべての認証方法を実施した．しかし，講義受講者による実験は，あわせ絵と残りの 3 種の認証手法のうちいずれか 1 つ，合計 2 種類の認証のみを実施した．認証方法の割当て方法は，被験者を 3 つのグループに分類し，それぞれのグループにあわせ絵と残りの 3 つの認証手法のうちの 1 つを割り当てた．

最後の違いは，秘密情報設定時の周知の有無である．講義受講者による実験では，秘密情報設定時に「認証を行えば認証に失敗しても出席とする．だが，秘密情報はなるべく忘れないような情報を設定せよ」という周知を行った．一方，研究室メンバによる実験では周知を行わなかった．

なお，すべての被験者にとって画像を用いた認証を行うのは初めての経験であった．また実験期間中に被験者が我々に無断で各認証システムを利用することは不可能である．実験手順は以下のとおりである．まず初めに各認証システムとその使い方について簡単に説明を行い，その場で各認証の秘密情報設定を依頼した．秘密情報設定後に，秘密情報ならびに認証方法の確認もかねて，一度認証を行ってもらった．これが 0 週目，すなわち秘密情報設定直後の実験としている．その後は上述した期間経過ごとに再度認証を試みてもらった．

3.2 実験結果

講義受講者による実験結果

図 2 は講義受講者による利便性実験の結果である．横軸は認証手法と経過時間，縦軸は認証成功率を表している．この結果から暗証番号とあわせ絵は，秘密情報設定から 8 週間経過した後でもほとんどの被験者が認証に成功するという結果になった．しかし，その一方で，パスワードとランダム画像による認証は，8 週間後にはおよそ 25%の被験者が 3 回試行しても認証に失敗するという結果になった．

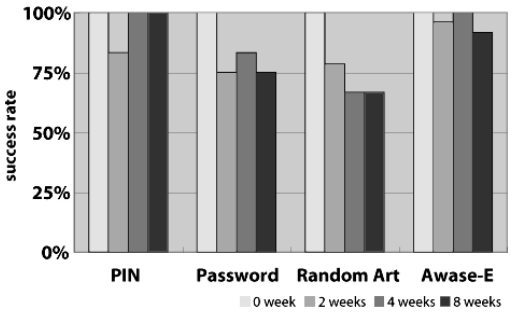

図 2 講義受講者による利便性評価実験
Fig. 2 Long-term memory evaluation with students in class-room.

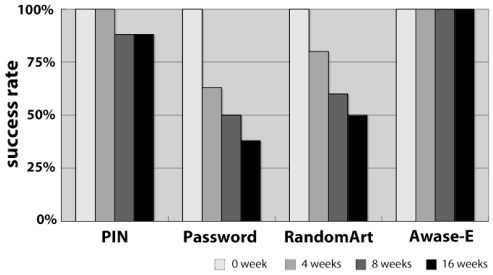

図 3 研究室メンバによる利便性評価実験
Fig. 3 Long-term memory evaluation with lab's students.

研究室メンバによる実験結果

図 3 は研究室メンバによる利便性実験の結果である．表示方法は図 2 と同様である．この実験でも，暗証番号とあわせ絵による認証は，秘密情報設定より 16 週間後であっても 9 割近くの被験者が認証に成功する結果となった．特にあわせ絵では 16 週間後の実験でも認証成功率は 100%であった．しかし，ランダム画像による認証では 50%の被験者が 16 週間後には認証不能になり，パスワードにいたっては 60%の被験者が認証不能になるという結果となった．

なお研究室メンバによる実験では，追加で 2 つの測定を行い，興味深い実験結果を得た．1 つは認証成功時の試行回数である．

図 4 は，認証成功時の試行回数を表すグラフである．つまり，被験者が実験において認証に成功したのは何回目の試行であったかを表すものである．このグラフから，今回の実験ではランダム画像と写真による認証では 3 回目の試行で認証に成功した事例が存在するが，その一方で暗証番号やパスワードによる認証では 3 回目の試行で認証に成功した例はないという結果となった．

もう 1 つの測定は，秘密情報の更新による認証成功率の変化である．研究室メンバに対しては，16 週間

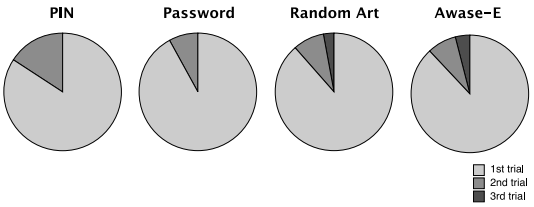

図 4 認証成功時の試行回数
Fig. 4 A number of trials until an authentication succeeds.

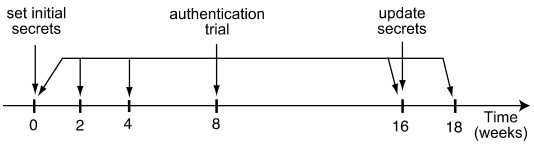

図 5 研究室メンバを対象とした実験の時間と作業の関係
Fig. 5 Time line of a usability evaluation experiment for lab's members.

後の認証実験後，さらに以下のような手順で追加実験を行った．

(1) 16 週間後の認証実験後，すべての認証方法の秘密情報を強制的に変更させた．
(2) さらに 2 週間後（実験開始から 18 週間後），再度，認証実験を行った．

なお，この際も秘密情報の決定は，以下の条件を満たす範囲内で被験者の自由とした．

- 既定の条件（表 1）を満たすこと
- 今まで使用してきた秘密情報とは異なること

研究室メンバに対する実験と時間の流れを図示すると**図 5** のようになる．

図 6 は，秘密情報の更新前後における認証成功率の変化を表したグラフである．図中にはそれぞれの認証方法に対し 2 つの棒グラフがあるが，左側の棒グラフは秘密情報の初期設定後 2 週間後の認証成功率を表し，右側の値は 16 週目の秘密情報更新より 2 週間経過後の実験における認証成功率を表している．両者の値は，どちらも秘密情報設定後 2 週間後の値であるが，それ以前に異なる秘密情報を使用していた場合と，そうでない場合という差がある．

この実験結果から，暗証番号とパスワードによる認証は秘密情報の更新によって認証成功率が下がったが，ランダム画像と写真による認証では認証成功率が下がらないという結果を得た．

3.3 考　　察

図 2，3 の実験結果から，あわせ絵はこれらの認証手法の中で最も高い認証成功率を得ることのできる手法だといえるだろう．また，その高い認証成功率は，

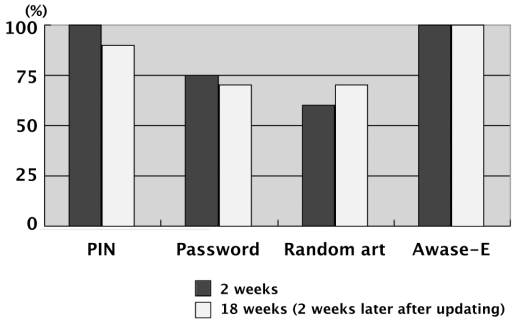

図 6 秘密情報の更新による認証成功率の変化
Fig. 6 An authentication success rate before and after updating secrets.

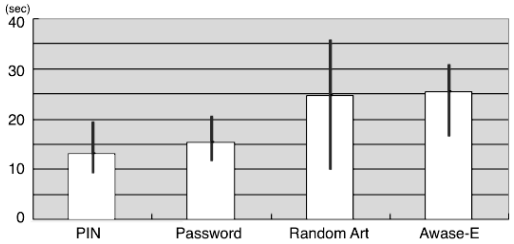

図 7 各認証方法における認証時間
Fig. 7 An authentication process time in each authentication schemes.

秘密情報設定後 16 週間を経ても保持されるという結果を得た．このことから秘密情報に写真を使用し，それを提示選択方法で照合する手法は，秘密情報の長期記憶/想起を可能にし，かつ高い認証成功率を長期間維持可能にする認証方法であるといえる．

また今回の実験では，実験における空白期間が最短で 2 週間という設定であった．この間隔は一般に使用されている認証の使用頻度と比較しても低頻度であるといえるだろう．このような状況下でも，安定して高い認証成功率を維持できるという事実は，あわせ絵の特筆すべき特徴であり，ユーザにとって記憶負担の少ないことを示す 1 つの指標であると考える．

次に認証時間について考察する（**図 7**）．認証時間の平均値はあわせ絵認証が 24.6 秒，ランダム画像による認証は 25.4 秒と画像認証の 2 手法でほぼ同程度であった．ただし，そのばらつき度合いは両者で大きく異なり，ランダム画像による認証は，あわせ絵による認証よりもばらつきが大きく，両者で 2 倍程度の差があった．

我々は実験前の仮説として「あわせ絵認証の認証時間は，ランダム画像による認証よりも短い．つまり写真の認識にかかる時間は，ランダム画像より短いであろう」と推測していた．しかし，結果は仮説とは異なる結果となった．

この理由として，被験者が照合画面に表示される写真を面白がって見入るという事態が発生したことがあげられる．本実験では，認証時間を測定している旨を被験者に事前に伝えなかった．これは，その旨を事前に通知することで，被験者に余計な配慮をさせないためであった．しかし，そのために被験者のうち数人は写真を見入ってしまい，結果として認証時間が本来測定したい作業時間よりも長くなるという事態をまねく結果となった．よって，あわせ絵の認証時間は本実験結果よりも短くなる可能性があると考えており，その検証は今後の課題である．なお暗証番号やパスワード認証の認証時間の平均値が 10 秒を超えている理由は，時間の経過とともに秘密情報の想起に時間がかかったためである．

ここで講義受講者と研究室メンバによる実験の差について考察する．2 つの実験結果における差は，パスワード認証の時間経過にともなう認証成功率低下の度合いである．この差を生じさせた原因は 3 つあると考える．1 つめは秘密情報設定時の周知の差である．講義受講者による実験では，秘密情報設定時に「忘れにくい情報を秘密情報とせよ」と周知をした．これにより，被験者は安易に忘れることのない情報を秘密情報として設定したため，結果としてパスワードによる認証成功率の低下が研究室メンバによる実験よりも少ない結果になったと考える．

2 つめは被験者 1 名あたりの秘密情報数の差である．講義受講者による実験でパスワード認証を行った被験者は，パスワード認証とあわせ絵認証の 2 種の認証方法のみを行った．しかし研究室メンバによる実験では，被験者は 4 種類すべての認証手法を行っていた．したがって被験者による記憶負担には明らかな差があり，それゆえ，パスワードは忘れられ，結果として研究室メンバによる実験ではパスワード認証の認証成功率が大きく低下することになったと考える．

最後の要因は被験者の技能による点である．図 3 を見て「パスワード認証による認証成功率がこんなに低下するとは思えない」と疑問を持つ人もいるかもしれない．こうなった理由は，研究室メンバによる実験の被験者のうちの数人は，日常的に使用しているパスワードを本実験では使用せず，新たに実験専用のパスワード文字列を生成し，秘密情報として設定していたためである．この被験者グループのメンバは，情報セキュリティに関する研究をしている学生であり，一般の学生と比較しても情報セキュリティに関する意識の高いメンバであった．それゆえ秘密情報の運用に関する意識が高く，複数の被験者が自然発生的に日常的に使用しているパスワードを実験では使用せず，新たに実験専用のパスワードを生成して使用していたのである．したがって，新たに生成されたパスワード文字列は時間の経過にともなって忘れられ，認証成功率は講義受講者によるパスワード認証の認証成功率よりも低下していったのである．

次に，研究室メンバを対象として行った追加実験について考察する．まず認証成功時の認証回数（図 4）に注目する．我々は，この結果を示唆に富む結果として見ている．この結果から，暗証番号やパスワードによる認証，すなわち想起入力型の認証方法では 2 回の認証試行失敗後，3 回目の試行で認証に成功することはなかった．しかし，ランダム画像や写真による認証，すなわち提示選択方式による認証方法は，どちらも 3 回目の試行で認証に成功する事例が存在したのである．これは回答候補が被験者に提示されることで，被験者が忘れかけていた秘密情報を想起した結果ではないかと推測している．つまり暗証番号やパスワード認証といった既存の想起入力方式では，忘れてしまった秘密情報を想起させる手段はほとんどないが，提示選択方式ならば試行を通じて秘密情報の想起を可能にし，結果として認証を可能にする効果があるという主張を裏付ける結果であると考えている．しかし，今回の実験だけでは被験者数も少なく，その効果を断定するには不十分といわざるをえない．この検証実験は今後の課題である．

また，別の興味深い結果として，秘密情報の更新による認証成功率の変化（図 6）があげられる．我々は実験前の仮説として「どの認証手法であっても，その認証成功率は更新前と比較して低下する．ただし，その低下の度合いが一番少ないのは写真による認証である」と推測していた．理由は簡単である．秘密情報の更新により被験者の記憶に新旧の秘密情報が混在することとなり，それが混乱を招いて新しい秘密情報での認証に失敗する被験者が必ず出現すると推測したからである．また，その影響は，知識照合型認証であれば認証方法には依存しないとも考えていた．

実験結果は，暗証番号とパスワードについては予想どおりの結果になった．しかしその一方で，ランダム画像と写真による認証は予想と反する結果になった．ランダム画像では認証成功率が上昇し，あわせ絵は成功率が変わらないという結果を得たのである．この結果は，画像を用いた提示選択型認証では，秘密情報を更新しても，それによって新旧の秘密情報によって混乱を生じ，認証成功率が下がるという傾向が少ないということを示すものだと考える．この特性の存在が確

かならば，知識照合型認証の問題を改善しうる好ましい特性であるといえる．

また，ランダム画像による認証成功率が秘密情報の更新後に改善された理由は，「これまでの実験経験から，ランダム画像の記憶保持が想像以上に困難であることを実感した．それをふまえて，秘密情報更新時には，きちんと覚えられるであろうランダム画像を選択した」という学習効果が発生していたことが実験後のインタビューによって分かっている．

4. 安全性に関する実験

次に我々は，あわせ絵の安全性に関する実験を行った．ここでは，すでに知られている攻撃による脅威がどの程度のものなのかを実際に確認するのが目的である．本論文では，写真による提示選択型認証の攻撃手法として知られている攻撃手法のうち，推測攻撃と抽出攻撃について実験を行った．抽出攻撃とは，多数の照合画面を集め，その画面に提示される各画像の出現頻度を求めることで，パス画像を発見する攻撃手法である．

この方法は Intersection 攻撃[2] とは異なる攻撃手法であることに注意されたい．Intersection 攻撃とは，パス画像が照合画面に毎回必ず提示されることを悪用し，照合画面の積集合をとることで決定的にパス画像を特定する攻撃手法である．あわせ絵では照合画面を複数のステージに分割するとともに，パス画像が提示されない事象を導入することで，この攻撃に対する安全性を確保している[1]．

4.1 実験方法

推測攻撃に関する実験

推測攻撃の脅威を測るため，我々は 3 種類の実験条件を設定し，実験を行った．実験では，実際のシステムを用いずに，認証時の 4 つの照合画面を一度に俯瞰できる状況をつくり出したうえで，被験者（つまり攻撃者）にパス画像の推測を行わせた．これは現実的に攻撃者が作り出せる状況であり，なおかつ攻撃者にとって都合の良い状況でもある．そのため我々は，特定ユーザの認証で実際に画面に提示された 4 つの照合画面を印刷した紙を複数人分用意した（**図 8**）．なお推測実験のため，この実験シートに印刷されたすべての照合画面はパス画像を含んだ状態とした．また，その事実は実験前に被験者にも周知した．

この実験では，実験シートを被験者に見せ，その場で対象ユーザのパス画像を推測してもらうという方法で行った．被験者は 8 名で，全員男性 20 代の大学院生である．また推測対象者，すなわち “なりすまされる” ユーザも全員 20 代の男性で大学院生である．なお，回答に時間制限は設けていない．以下に実施した 3 種類の実験条件について述べる．

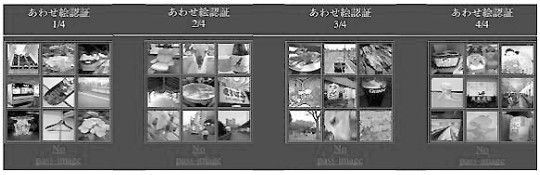

図 8 Educated guess 攻撃実験のための実験シート
Fig. 8 Virtual authentication screens for educated guess attack experiment.

- 推測実験 1
  推測対象者は同一研究室に所属するユーザであり，推測対象者と攻撃者は互いに知人である．また，被験者（攻撃者）には，この認証画面が誰のものかが伝えられる．ただし推測対象者のパス画像には一見すれば分かるような共通性はない．この条件のもとで，図 8 の実験シートを 5 枚（すなわち 5 名分）提示し，推測対象者のパス画像を推測させた．
- 推測実験 2
  推測対象者は，被験者にとって他人である．ただし，この実験では推測対象者のパス画像に一見すれば容易に見出せるであろう共通点がある．この条件のもとで実験シートを 2 枚提示し，推測対象者のパス画像を推測させた．
- 推測実験 3
  推測対象者は，被験者にとって他人である．また，この場合は推測対象者のパス画像に容易に見出せるような共通点もない．この条件のもとで実験シートを 2 枚提示し，推測対象者のパス画像を推測させた．

パス画像の共通性とは，ユーザのパス画像間に意味的または表象的な共通性があることを指す．例を示す．**図 9** は，実験に参加した 2 名のユーザのパス画像を 4 枚ずつ並べたものである．図中上段にある 4 枚の写真からはなんの共通性を見出せないが，下段の 4 枚の写真は，すべてビールの入ったグラスが写っている写真であることが一見して分かる．この下段のようなパス画像の場合を，パス画像に共通性があるという．推測実験 2 では，実験参加者のパス画像の中からなんらかの共通性があるものを主観的判断で選択し，それを用いて実験を行った．

抽出攻撃に関する実験

次に我々は，抽出攻撃の脅威を知るために実験を行った．実験条件は以下のとおりである．

図 9 パス画像の共通性—上段：共通性なし，下段：共通性あり
Fig. 9 A common attribute in pictures.

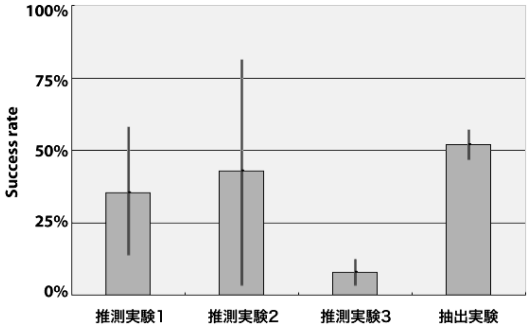

図 10 推測ならびに抽出攻撃実験の結果
Fig. 10 A result of attack experiments.

- 抽出実験
  推測対象者は被験者にとって他人であり，推測対象者のパス画像に容易に見出せるような共通性はない．この条件のもとで，推測対象者 1 名の認証 6 回分にあたる実験シート 6 枚を同時に俯瞰できるような形で提供し，パス画像を推測させた．なお，この実験で提供した実験シートの照合画像には，推測攻撃の実験とは異なり，パス画像が含まれていない照合画面も含まれている．

4.2 実験結果

図 10 は，推測ならびに抽出攻撃による実験結果である．

グラフは横軸が実験種別を表し，縦軸は推測成功率を表している．推測成功率の値であるが，パス画像一枚の推測に成功するごとに 25%の値を与えた．これはパス画像は全部で 4 枚であり，4 枚すべてのパス画像推測に成功した場合を推測成功率 100%とするためである．図 10 中の棒グラフは，その推測成功値を全被験者で集計した平均値を表し，棒グラフ上の線は各実験における推測成功率の最大および最小値を示している．

4.3 考　　察

まずはじめに，推測実験 1，2，3 に注目する．推測実験 1 の結果から，なりすまし対象が攻撃者の知人である場合，攻撃者はパス画像間に容易に分かるような共通性がなくても 4 枚のうち 1〜2 枚はパス画像を推測できるという結果となった．

推測実験 2 についても推測実験 1 と同様，1〜2 枚のパス画像の推測に成功するという結果となった．しかし推測実験 1 と異なる点がある．それは推測成功率のばらつきであり，その値域は推測実験 1 よりも大きくなった．興味深いのは，この実験における結果のほとんどが「パス画像がまったく推測できない」か「ほぼすべてのパス画像を推測できた」かのどちらかになったことである．この攻撃は，攻撃対象者の知識ではなく，画像の視覚的または意味的特徴に基づく共通点を見抜くことである．それゆえ，その成功率は攻撃者の能力，すなわち多数の画像から，なんらかの妥当な共通点を見出せるかどうかに依存しているといえる．よって，それに成功した者は，ほとんどのパス画像推測に成功し，できなかった者は，まったくパス画像を推測できなかったという結果になったと考えられる．

最後に推測実験 3 だが，この実験における推測成功率は，平均して 8%，最大でも 20%に満たないという結果となった．つまりほとんどの被験者が 1 枚の推測もできないという結果となった．

これらの結果を総合すると，以下のようなことがいえる．

- なりすまし対象者が攻撃者の知人であっても，その推測成功率は平均して 30%程度であり，攻撃されれば簡単になりすまされてしまうというほどの脅威ではない．
- パス画像の共通性による推測は，なりすまし対象者の知識に基づく推測の脅威と同等かそれ以上である．ただし，この攻撃の成否は，攻撃者の能力に大きく依存する．
- 推測攻撃による脅威を軽減するためには，パス画像に共通性を持たせないようにすべきである．

今回の推測実験において，実験条件にパス画像の意味的/表象的共通性の有無を考慮した理由は「パス画像になんらかの共通性がある場合，なりすまし対象者に対する知識がなくてもその推測は容易である」という仮説を評価するためである．これは Cognitive 攻撃と呼ばれており[11]，写真を使った提示選択型認証における脅威として指摘されている．我々は，本実験中に評価要素として組み入れ，その脅威の具体的評価を行った．

実験結果から，推測実験 1 と推測実験 2 について

は平均 1〜2 枚のパス画像推測に成功するという結果を得た．ただし，これらの実験における推測成功率は推測実験 3 と比較すると変動が大きく，最大値を見ると実験 1 では 50%，実験 2 では 75%を超えているが，最小値を見るとどちらも 25%を下回った．つまり攻撃者によってはパス画像の推測に 1 枚も成功しなかったという結果となっている．この実験結果は，攻撃の成否は攻撃者の知識や能力に大きく依存することを示す結果であると考える．

次に抽出攻撃について考察する．実験結果から分かるとおり，推測成功率の平均値はこれまでの攻撃実験の中で最も高い結果となり，平均で 52%であった．またその推測成功率は，攻撃者による変動が少ないという特徴も明らかになった．つまり認証 6 回分の照合画面群があれば，4 枚のパス画像のうち 2 枚は多くの攻撃者が推測に成功しうるということである．このことから，抽出攻撃による脅威は推測攻撃よりも大きいといえる．

これらの攻撃実験から，あわせ絵がこれらの攻撃に対して脆弱であり，その度合いは決して無視できるものではないことが分かった．しかし，それと同時に，即座になりすまされるほど脆弱な認証手法ではないことも明らかになった．

これらの攻撃による推測成功率は，1. 登録されているパス画像の共通性，2. 攻撃者が持っている推測対象者の属性情報，そして 3. 攻撃者自身の能力，に大きく依存しているといえる．したがって，この特徴を裏返せば，パス画像の決定時にユーザが注意すべき点が明確になる．これらに攻撃に対する安全性を高めるには，パス画像の選択において以下の点に配慮すべきである．

(1) 自分の属性情報に依存しない画像をパス画像として使用すべき．
(2) 容易に見出せるような共通性をパス画像に持たせない．

なお，これらの制約により，ユーザのパス画像に対する記憶負荷が増大するのではという意見があるかもしれない．これらの制約により，パス画像の選択に制限が生じるのは事実である．しかし，写真を使用しているため，上記の条件を満たす写真の生成および選択は，従来のパスワードよりも容易であると考える．写真ならば，上記の制約に該当しないような写真を自身の写真集の中から選択するか，または上記のような条件を満たす写真を撮影するだけでよいからである．また，その記憶負荷についても，写真であれば記憶のための意味付けや紐付けは意味のない文字列よりも容易であり，よってその記憶負担も無意味な文字列より増大するとは考えにくい．

これらの実験結果から，脅威の度合いは以下の関係があるといえる．

- 抽出攻撃 > 推測攻撃
- パス画像の共通性による推測攻撃 ≥ 知識による推測攻撃

5. 議　　論

これまでの実験結果を総括し，あわせ絵の利便性と安全性について議論するとともに今後の課題について述べる．

あわせ絵の利便性に関する実験は，これまでの主張を裏付ける望ましい結果が得られたと考える．長期記憶に関する評価では，4 カ月にわたる実験で利用頻度が少ない状況でも高い認証成功率を長期間維持できることが確認された．また認証成功時の試行回数の結果から，提示選択方式の認証方法の採用により，ユーザが忘れかけていた秘密情報を想起させる可能性についても示唆のある結果が得られた．さらに秘密情報の更新による認証成功率の低下についても，提示選択型認証方法では新旧の秘密情報による混乱は生じにくく，引き続き認証を行うことが可能という結果を得た．これらの結果は，あわせ絵による知識照合型認証の利便性向上を肯定する結果であると考える．

また，実験後に行ったアンケートからも上述の結論を反映する回答が得られている．その一例として，ランダム画像が覚えやすかったと回答した被験者は 0 名であったのに対し，写真が覚えにくかったという被験者は 2 名だけであった．双方の画像種について「何枚まで記憶できそうか?」という問いへの回答は，ランダム画像が平均 3 枚となったのに対し，写真の場合は平均 6 枚という結果となった．これは同じ画像であってもその記憶負担は異なり，写真の方がその負担は少ないということを示すものである．

安全性についてであるが，あわせ絵に特有の攻撃手法による脅威は決して無視できないという結果となった．特に抽出攻撃については，パス画像の半数を推測可能にし，かつそれは攻撃者の能力に依存しないという特性が明らかになった．これらの攻撃手法に対する対策は必要不可欠である．

今後の課題は主に 2 つある．1 つはより一般的な評価実験を行うことであり，もう 1 つは安全性に対する対策手法を考案し，その対策方法による安全性の改善度合いを再評価することである．

今回の評価実験における問題の 1 つは，被験者の

属性情報が限定されていたことである．すべての被験者は大学院生で，その年齢は 20 代と限定されていた．また，そのほとんどが男性であるとともに，彼らの多くは情報セキュリティに興味を持っていたり，その分野の研究を行っている学生であった．これが実験結果にどのような影響を及ぼしたかは計りかねるが，一般ユーザによる評価結果と異なる結果となっている可能性は否定できない．したがって，様々な年代/性別/属性の被験者を募り，再度ユーザ評価実験を行う必要があると考えている．

また，今回の実験で明確になった脅威に対する対策は，あわせ絵の実用化に向けてその改良が必要不可欠な課題である．我々も含め，いくつかの研究によってこれらの脅威に対する改善方法が提案されている[1),4),5)]．しかし，今回の評価実験では，それらの対策方法を実験方法に採用しなかった．それは今後の研究の基礎として，あわせ絵における基本的な安全性を明確にするためである．すでに考案されている対策方法を実装し，それを用いた被験者による評価実験を行うのは今後の課題である．

6. 関 連 研 究

あわせ絵同様に画像を秘密情報として使用し，提示選択型認証を使った認証システムの評価を行った関連研究について取り上げる．

Deja Vu は，提示選択型認証を提案した認証手法として著名なシステムである．**図 11** は，Deja Vu の認証画面である．

この論文 2) では，Hash Visualization アルゴリズム[7)] を使って生成したランダムアート画像を秘密情報として使用し，25 枚の画像群の中から自分の秘密画像である portfolio 5 枚を順不同で選択することで認証する手法である．ランダムアートを秘密情報として採用している理由は，推測攻撃に対する安全性を確保するとともに，メモや口伝によるパス画像の漏洩を困難にすることで人的要因による脆弱性に排除するためである．

この論文では被験者による評価実験を行っている．被験者は 20 名（男性 11 名/女性 9 名）で本論文と同じく 4 種の認証手法を使って認証成功率と認証にかかった時間を測定し，その比較を行っている．しかし，この実験の問題点は，その評価期間が 1 週間と短いことである．ランダムアートによる秘密情報が本当に長期間記憶可能なのか，そしてそれが暗証番号やパスワードによる秘密情報よりも良い結果となるかは不明である．また，安全性に関しても特有の脆弱性の存在

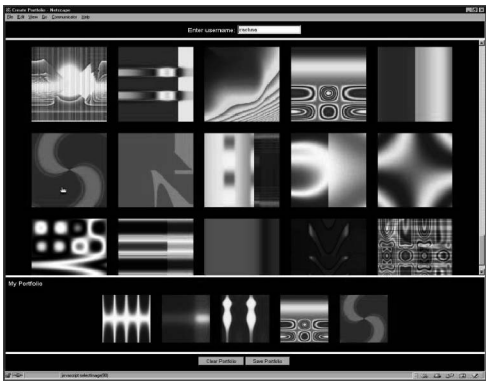

図 11 画像認証システム Deja Vu の認証画面
Fig. 11 A screen image of the Deja Vu system.

を指摘するとともに，それらに対する対策手法を提案してはいるが，その脅威の度合いを実際に評価してはいない．

Angeli らによる論文 9) は ATM での認証に注目し，数字の代わりとして写真を用いた認証を提案するとともに，その評価を行った論文である．その認証方法は 3 つ提案されており，方法 1，2 は，10 枚の写真群の中から 4 枚の写真を決められた順番で選択することで認証をする．双方の方法の違いは，方法 1 は秘密情報である写真の照合画面内の表示位置が固定で，方法 2 はランダムという設定である．方法 3 は 16 枚の写真群の中から秘密情報である写真 4 枚を順不同で選択する方法だが，秘密情報となる写真 4 枚は，事前に決めておいた 8 枚の母集団の中からシステムがランダムに選択して照合画面に提示する方法である．評価結果は方法 1 が最も良い結果となった．しかし，これは当然の結果であろう．方法 1 は既存の ATM の認証方法において照合画面に数字を表示する代わりに写真を用いただけであり，ユーザは写真を記憶しなくてもその表示位置さえ記憶すれば認証可能だからである．またこの論文の評価実験も実験期間は 1 週間と短く，それらの認証方法における長期記憶の可能性評価は明確ではない．また，攻撃実験による安全性評価は行っていない．

Pering らによる論文 11) は，通信データの盗聴や認証作業が覗き見られる環境下での認証方法として写真を用いた認証システムを提案している．この論文で提案されているシステムでは，照合画面に他人の写真 3 枚と自分の写真 1 枚の 4 枚が提示される．ユーザはその照合画面から自分の写真を選択する．この作業を 10 回繰り返し，すべての回答が正解であった場合に正規のユーザとして認証するという方法である．つまり照合画面から自分の写真を見つけ出し続けることで，

本人であることを認証する方法である．

この論文では 8 名の被験者で評価実験を行い，被験者全員が認証に成功するとともに，その認証時間も平均 30 秒であったと述べており，その実用可能性は高いとしている．しかしながら，時間経過にともなう認証成功率の変化は評価していないため，その成功率が長期間維持可能かは不明である．

また，推測攻撃による攻撃実験も行っており，その推測成功率は照合画面単位で 60%の成功率であった．実際の認証はこれを 10 回繰り返すので，なりすましの可能性は低いと述べている．しかし，この実験では攻撃実験者と推測対象者の関係が明確ではなく，認証行為を攻撃者に数回見られていたという想定だけで行っている．したがって推測攻撃とはいいにくく，実際に推測対象者が攻撃者の知人であった場合はその推測成功率がより高くなる可能性があると考える．また，この認証方法でも抽出攻撃による脆弱性が存在しうるが，それに関する評価は行われていない．

7. おわりに

本論文では，写真を用いた個人認証システム「あわせ絵」の利便性と安全性に関して被験者による評価実験を行った．これらの実験結果は，限定的ではあるものの，この種の認証手法に関して示唆に富む結果を得た．

利便性に関する実験から，あわせ絵認証は，ユーザに対する秘密情報の記憶負担が少ないことが明確になったといえる．認証の利用頻度が少なくても長期間にわたって安定して認証可能であることが確認されるとともに，秘密情報を更新しても，新旧の秘密情報で混乱をきたし，認証不能になる可能性が少ないことが実験から確認された．これらは，既存の知識照合型認証における問題点を改善しうる特性であり，あわせ絵が知識照合型認証として望ましい特性を持っていることを肯定する結果であるといえる．

また，安全性に関する実験から，あわせ絵における推測攻撃ならびに抽出攻撃の脅威は無視できない程度の脅威であることが明らかになった．特に抽出攻撃はその脅威の度合いが推測攻撃よりも大きく，その対策は必要不可欠である．今回の実験結果を基に，それを克服するための対策法を模索していくのが今後の課題である．

謝辞 評価実験の被験者として評価実験に快く協力してくれた電気通信大学大学院情報システム学研究科小池研究室の学生諸氏，ならびに講義の出欠確認として評価実験に参加してくれた同大学大学院同研究科の学生諸氏に感謝する．

参考文献

1) 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).
2) Dhamija, R. and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, *Proc. 9th USENIX Security Symposium*, pp.45–58 (Aug. 2000).
3) 大貫岳人，高田哲司，小池英樹：画像認証システム「あわせ絵」の有効性実証のための評価実験，暗号と情報セキュリティシンポジウム SCIS2005 予稿集，Vol.I, pp.217–222 (2005).
4) 大貫岳人，高田哲司，小池英樹：写真を使った個人認証の脆弱性に対する改善策の提案，暗号と情報セキュリティシンポジウム SCIS2005 予稿集，Vol.I, pp.223–228 (2005).
5) 原田篤史，漁田武雄，水野忠則，西垣正勝：画像記憶のスキーマを利用したユーザ認証システム，情報処理学会論文誌，Vol.46, No.8, pp.1997–2013 (2005).
6) Tullis, T.S. and Tedesco, D.P.: Using Personal Photos as Pictorial Passwords, *Proc. Human Factors in Computer Systems* (*CHI2005*), pp.1841–1844 (2005).
7) Dhamija, R.: Hash Visualization in User Authentication, *Proc. Human Factors in Computing Systems* (*CHI2000*), pp.279–280 (2000).
8) Davis, D., Monrose, F. and Reiter, M.K.: On User Choice in Graphical Password Schemes, *Proc. 13th USENIX Security Symposium*, pp.151–163 (Aug. 2004).
9) Angeli, A.D., Coutts, M., Coventry, L. and Johnson, G.I.: VIP: a Visual Approach to User Authentication, *Proc.International Working Conference on Advanced Visual Interface* (*AVI2002*), pp.316–323 (May 2002).
10) Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D.: The Design and Analysis of Graphical Passwords, *Proc. 8th USENIX Security Symposium*, pp.1–14 (Aug. 1999).
11) Pering, T., Sundar, M., Light, J. and Want, R.: Photographic Authentication through Untrusted Terminals, *IEEE Pervasive Computing*, Vol.2, No.1, pp.30–36 (2003).
12) ニーモニックガード，(株) ニーモニックセキュリティ．http://www.mneme.co.jp/ (site accessed: May 5, 2006).

(平成 17 年 11 月 29 日受付)
(平成 18 年 6 月 1 日採録)

高田　哲司（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士課程修了．工学博士．同年電気通信大学サテライトベンチャビジネスラボラトリ研究員．2003 年ソニーコンピュータサイエンス研究所入所．2005 年産業技術総合研究所入所．現在に至る．情報視覚化，ユーザインタフェースおよび情報セキュリティに興味を持つ．IEEE/CS 会員．

大貫　岳人

2005 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士前期課程修了．修士（工学）．2005 年原田工業（株）入社，現在に至る．携帯電話や情報セキュリティ，個人認証に興味を持つ．

小池　英樹（正会員）

1991 年東京大学大学院工学系研究科情報工学専攻博士課程修了．工学博士．同年電気通信大学電子情報学科助手．1994 年同大学大学院情報システム学研究科助教授．2006 年同大学院情報システム学研究科教授．現在に至る．1994〜1996 年，1997 年 U.C. Berkeley 客員研究員．2003 年 University of Sydney 客員研究員．情報視覚化の研究に従事．特に視覚化へのフラクタルの応用，Perceptual User Interface，情報セキュリティへの視覚化の応用に興味を持つ．1991 年日本ソフトウェア科学会高橋奨励賞受賞．2000 年情報処理学会 DICOMO2000 最優秀論文賞．2001 年 IEEE VR2001 Honorable Mention for the Outstanding Paper Award 受賞．IEEE/CS，ACM，日本ソフトウェア科学会各会員．