セキュリティとユーザビリティ特集
個人認証におけるセキュリティとユーザビリティ

産業技術総合研究所 - 高田 哲司

ヒューマンインタフェース学会誌 Vol.9, No.1, 2007 - Revised version

1 なぜ個人認証はかくも厄介か?

最近では，何をするにも個人認証を通じて自分が誰であるかを証明する必要があると言っても過言ではないであろう．しかし，これがとても面倒な作業であることは，多くのユーザが実感するところである．ならば「簡単にできる個人認証を考えればよいではないか!」と思うのだが，なぜか「この認証は簡単だし安全!」と実感できるような個人認証システムに出会わないのも事実である．

単に操作を簡単化するだけならば，その実現は不可能ではないだろう．しかし個人認証の難しい点は，安全性を維持したままで，その行為を簡単にしなければならない点である．それは正規のユーザ “だけ” を可能な限り正確に識別し，他のユーザを排除しなければならないというのが個人認証の目的だからである．

広く利用されている個人認証手法は，一定の安全性を担保している．しかし，ふと考えてみると，これを疑問に思うことがある．既存の個人認証システムは，その安全性が維持されるための前提条件として「認証システムの意図した通りにユーザがシステムを利用すること」であることは周知の事実である．しかし，これは見方を変えると，システムは単に入力値と既定値の照合をするだけで，安全性を担保するための負担は，すべてユーザ側で負担して下さい．と言っているように受け取れるからである．これこそが，既存の個人認証の問題点であり，だからこそ個人認証はこうも厄介なのではないだろうか? と考える．

個人認証システムの安全性を確保するためにユーザに課される要件を，パスワード認証を例に考えると以下のものがある．

- 推測が困難で，辞書に載っておらず，数字や特殊文字を含んだ，一定の長さ以上のパスワードを生成し，使用せよ
- パスワードは正確に記憶し，忘れてはならない
- 認証時にはパスワードを一文字も間違えずに正確に思い出し，かつ入力せよ

ほぼすべてのユーザにとって，これらの要件を確実に行うことは極めて困難であろう．つまり既存の認証システムは,「システム自体は単純なシステムとして実装し，安全性を確保するために必要だが，その実行が難しいことはユーザの負担にしてしまおう」というシステムに見えるのである．

技術の進歩が進む一方で，多くの読者はいろいろな場面で 4 桁数字による暗証番号認証を現在も使用していると推測する．その危険性が数多く指摘されているにもかかわらず，4 桁数字による暗証番号認証がいまだに広く利用されているのはなぜだろうか? 暗証番号認証と同等またはそれ以上の安全性を保証する個人認証システムを実現することは難しいことではない．パスワード認証ならば，4 文字のパスワードと仮定しても 4 桁暗証番号より高い安全性を実現できる．しかし利便性という観点で考えるとどうだろうか? 答えは No である．つまり，暗証番号認証が広く利用されている理由は，暗証番号認証と同等の安全性と利便性を兼ね備えた認証方法が他に存在しないからだと言えるのではないだろうか?

これと同じ論理は，最近普及が進みつつある IC カードや生体情報を利用した個人認証にも適用可能だと考える．これらの認証手法が普及した理由は，その手法によって保証される安全性が向上したから普及し始めているのではなく，利便性が向上したからである．つまり，これらの認証手法は，既存の認証手法における問題の 1 つである「記憶」の問題を “排除” することができるからである．

以降では，知識照合型認証において安全性と利便性を考慮した手法として提案されている画像認証について概要を説明し，既存の画像認証の問題を改善する手法として個人の所有する写真を使用した個人認証システム「あわせ絵」を取り上げ，その安全性と利便性に関する特徴を紹介する．また既存の個人認証の問題を整理し，その改善のために望まれる研究の方向性を明確にする．

2 新しい知識照合型認証: 画像を利用した認証手法

画像を用いた認証手法が近年注目されている．それは安全性と利便性を両立しうる新たな認証手法として見込まれているからである．画像認証には，想起手法 (recall-based) と再認手法 (recognition-based) という二つの手法がある．

想起手法とは，画像内の特定位置を秘密情報として利用する方法である．画像の内容を利用して秘密情報とする位置を決定することにより，秘密情報の記憶が容易になると

いう手法であり，代表的な製品として visKey[1] がある．図 1 は，visKey の認証画面例である．イルカが三匹写っている写真であるが，この例では，三匹のイルカの口先を秘密情報として定義しており，ユーザは事前に決定した順序にしたがい，いるかの口先をスタイラス等で選択することで認証を行う．また特定位置のかわりに，画像をマス目状に分割し，その中の特定マスを選択させるという手法 [4] もある．

Figure 1: visKey の認証画面例

一方，再認手法とは，画像そのものを秘密情報として使用する手法であり，認証画面に複数の画像を提示し，その画像群の中から，事前に決定しておいた画像を選択することで認証を行う手法である．著名なシステムとしては Deja Vu[3] がある．このシステムでは，認証画面に 20 枚の画像が提示されるので，その中から事前に決定しておいた 5 枚の画像を順不同で選択することで認証を行う手法である (図 2)．

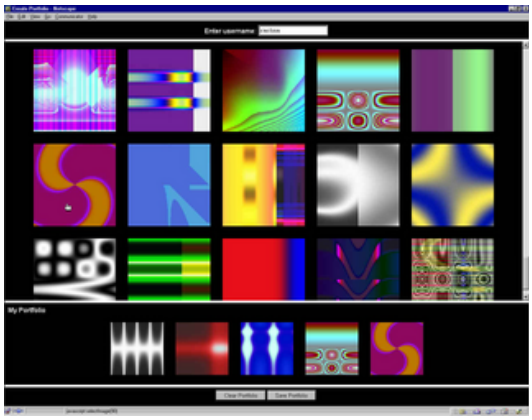

Figure 2: Deja Vu の認証画面例

Deja Vu の著者らは，既存の知識照合型認証の問題に対し，以下に挙げるような改善が必要であると指摘している．

1. システムは，ユーザが秘密情報を常に正確に思い出せると仮定すべきでない．そのかわりに，認識に基づく方法にすべきであろう
2. ユーザが，脆弱なパスワードを選択できないようにすべきである
3. システムは，秘密情報を書き止めたり共有することを困難にすべきである

そこで Deja Vu では，上の項目 1. に対する具体的方法として，正確な想起に基づく認証から，一度見たことのある画像の識別による認証手法を提案し，また項目 2,3. に対する具体策として，数式により生成される抽象画を画像認証に使用する方法を提案している．これらの提案により，認証手法は「事前に決定したパスワードを正確に思い出し，かつ一文字も間違えることなく入力する」という行為から，「一度見たことのある画像を画像群の中から探し出し，選択する」という行為，すなわち “想起 + 入力” から “認識 + 選択” になる．これにより，以下に挙げる利点が得られる．

- 記憶負担の軽減
  秘密情報を画像にすることにより，視覚記憶を利用することが可能となり，結果として記憶負担の軽減が見込まれる．
- 想起補完の可能性
  一度見たことのある画像は，仮にそれを忘れていたとしても，それを再び見たときに「この画像/風景は以前に見たことがある」と思い出すことがある．いわゆる既視感 (Deja Vu 効果) を認証における記憶補完の仕組みとして取り込むことが可能になる．
- 脆弱なパスワードの使用不能化
  秘密情報に抽象画を使用することにより，脆弱なパスワード，すなわち第三者によって推測されやすいパスワード画像の使用を排除することが可能になる．
- メモや共有の困難化
  秘密情報は抽象化された画像に限定されているので，その特徴を記述するのが困難になり，結果として秘密情報のメモや共有が困難になる．
- 操作の簡易化
  画像を選択するだけで認証が可能になり，キーボードによる入力が不要となる．PDA や携帯電話でも容易に操作可能になる．

これらの利点は，知識照合型認証における安全性改善だけではなく，利便性の改善も実現していることに疑いの余地はない．これに対し，想起手法による画像認証では，秘密情報である画像内の場所を正確に記憶し，認証時にはそれを正確に思い出す必要があり，記憶負担の点で考える

と，再認方式ほどの負担軽減は困難であると推測する，また画像そのものが秘密情報ではないため，想起補完の可能性は再認方式よりも低いと推測される．さらに認証操作は画像内の特定位置を指し示さなければならないため，画像そのものを選択をするよりも手間がかかるとともに，どの程度の正確さを位置選択に要求するかという点で照合判定にゆらぎが残ることにもなる．よって利便性の改善という意味では，想起手法よりも再認手法の方が上回っていると言えるだろう．よって本稿では，以降，再認手法の画像認証に絞って話をすすめる．

しかし，Deja Vu には大きく 2 つの疑問点が残されている．1 つは使用される画像が抽象画であるため，記憶負担の軽減ならびに想起補完の可能性という点で疑問が残るという点であり，もう一つは，Deja Vu では 5 枚の抽象画を秘密画像として記憶しなければならないが，それは多くのユーザにとって実行可能なのだろうかという疑問である．これらの疑問は，どちらも秘密情報が抽象画であることに由来している問題である．

3 自分の写真を使用した画像認証システム「あわせ絵」

Deja Vu のよい点を生かし，さらなる安全性と利便性の向上を目指した再認手法による個人認証システムとして，あわせ絵 [5] を提案している．あわせ絵とは，ユーザ自身が撮影した写真を使用することを想定した画像認証システムであり，携帯電話での利用を想定し，既存の暗証番号認証と同等の安全性と利便性の実現を目指したシステムである．

本手法の特徴は大きく 2 つある．1 つは，認証に使用する画像として，ユーザ自身が撮影した写真を使用することである．これは 2 つの点で利便性向上を可能にする．1 つは，記憶負担を軽減することである．これは単にその記憶負担を軽減するというだけでなく，ユーザがすでに知っているものを秘密情報として使用することにある．つまり，あらためて記憶する必要がないものを秘密情報として使用可能にすることでその記憶負担を軽減可能にするものである．2 つめは，“Deja Vu” 効果を最大限利用可能にするためである．自分が撮影した写真とは，その場面/風景に対してなんらかの興味を持ち，そして自ら能動的に写真を撮ったからこそ残されている記録である．よって記憶に残っている可能性は，突然使用することになった抽象画よりも意識に残っている可能性は高いと推測する．よって既視感による記憶補完の効果も Deja Vu の時より高いと考えられる．さらに安全性の点でも利点がある．それは秘密情報更新時におけるユーザの負担軽減が見込まれることである．自分の撮影した写真を使用することにより，新しいパスワード画像の選択が容易になると推測され，またもし気に入った写真がなければ，その場で適当な写真を撮影し，それを使用することも可能である．また更新したパスワード画像も自身で撮影した写真であるため，自分とはなんの関係もない抽象画よりも記憶に残っている可能性は高く，また秘密情報更新による新旧秘密情報の混乱を回避可能にする効果も期待できる．

もう 1 つの特徴は「パスワード画像がない」という回答を導入していることである．あわせ絵では，パスワード画像を一枚も含んでいない照合画面を意図的に提示し，その際にはこの回答をユーザに明示的に行わせるものである．これにより利便性向上と利便性を損なわずに安全性改善を可能にしている．詳細は後で説明する．

あわせ絵の認証方法について説明する (図 3)．まずはじめにユーザは，事前に自分のパスワード画像を複数枚決定しておく．あわせ絵認証は，1 回の認証行為が 4 つの照合画面から構成される．各照合画面には 9 枚の画像と「パスワード画像なし」の 10 個の回答が用意されており，この各照合画面にはパスワード画像が 1 枚か 0 枚含まれている．よってユーザは，照合画面の状況に応じて次のように回答しなければならない．照合画面内に自分が事前に決定しておいたパスワード画像が存在する場合は，パスワード画像を選択する (図 3 1st/3rd stage)．照合画面内にパスワード画像が存在しない場合は「パスワード画像なし」と回答する (図 3 2nd/4th stage)．すべての回答が正解であれば，認証者を正規のユーザとして認証する．という仕組みである．

ここで「パスワード画像なし」回答の導入による利点について説明する．まず利便性について述べる．本回答の導入により，ユーザが記憶すべきパスワード画像の枚数は削減可能となる．あわせ絵のように，4 回の照合画面がある場合は 4 枚のパスワード画像が必要と考えられるが，あわせ絵では本回答の導入により，ユーザの所有するパスワード画像が 4 枚未満でも認証することが可能となり，結果として記憶負担を軽減することが可能となる．ただし，認証において 1 枚のパスワード画像も使用しないという事例だけは安全性の観点から禁止している．

次に利便性を損なわずに安全性改善が可能という点について説明する．一般にブルートフォース攻撃に対する安全性を増すためには秘密情報を増やす必要があるが，あわせ絵ではこの回答の導入により，ユーザが持つべきパスワード画像の枚数を増やすことなく，ブルートフォース攻撃に対する安全性を向上させることが可能である．それは一回の認証における照合回数を増やすことで実現される．現在の照合回数は 4 回だが，これを 5 回にすれば，その安全性は $1/10,000$ から $1/100,000$ となる．しかし，増えた照合分の回答には「パス画像なし」回答を用いることができるため，ユーザは自分のパスワード画像を増やす必要がない．結果として，利便性を損なうことなく安全性を向上させることを可能にしていると言える．

次に被験者によるあわせ絵認証の評価実験 [6] について述べる．この実験では，まずはじめにユーザが所有する写真から 4 枚の写真を持ち込んでもらい，それをパスワード画像として設定した後，プロトタイプシステムを利用して認証方法を学習させた．以降，その日を起点として，2,4,8,16,18 週間後に再度認証実験を行った．なお 16 週目の認証実験の後，ユーザのパスワード画像を強制的に変更させた．つまり 18 週目の実験では，0 週目に設定したパスワード画像とは異なるパスワード画像で認証実験を

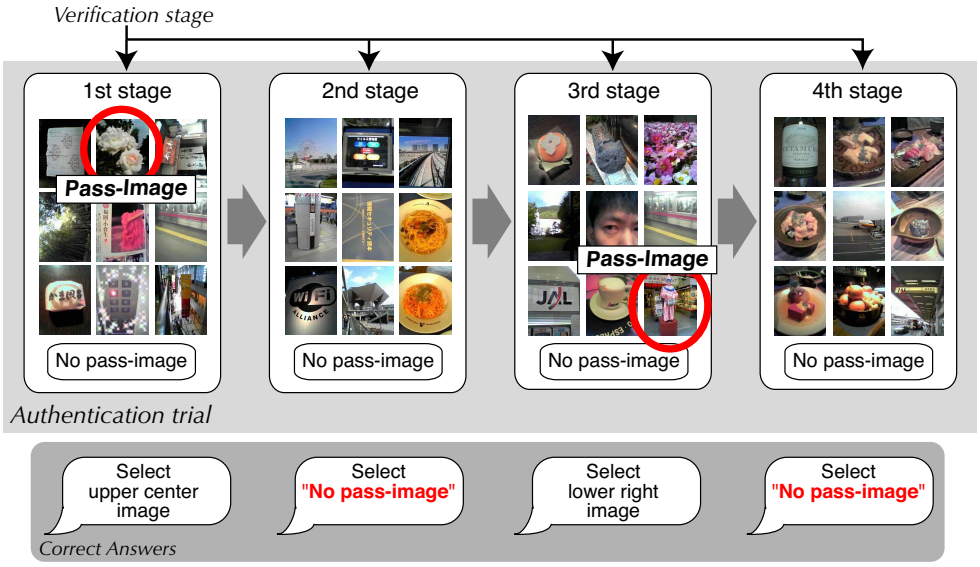

Figure 3: あわせ絵の認証方法

行なったことになる．なおこれと同じ実験を，4 桁数字の暗証番号，6 文字以上の文字列パスワード，そして認証手法はあわせ絵だが，認証に使用した画像種は写真ではなく Deja Vu で使用されていたような抽象画を使用した手法でも行った．被験者は大学院学生で男性 10 名である．各実験では 3 回まで試行を許可した．つまり 3 回試行しても認証に成功しなかった場合は認証失敗とした．図 4 は，本実験の手順を時系列に表したものである．

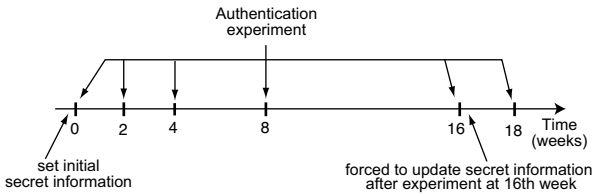

Figure 4: あわせ絵評価実験の時間軸表示

実験結果について述べる．まずはじめに秘密情報の記憶維持に関する評価を，認証成功率の時間経過で評価した．この結果，あわせ絵は 16 週間後の実験でも 3 回までの試行で全員が認証に成功する結果となった．しかしパスワードでは 50%の被験者が，抽象画による認証では 60%以上の被験者が 16 週目の実験で認証に失敗する結果となった．

次に 2 週目と 18 週目の認証成功率を比較した．これら 2 つの実験は，どちらも秘密情報を設定してから 2 週間後の実験である．しかし，18 週目の実験は秘密情報の更新後であり，ユーザは新旧双方の秘密情報により記憶に混乱を生じている可能性があることから，結果として認証に失敗すると想定して実験を行った．実験結果だが，暗証番号やパスワードでは予想通り 18 週目の認証成功率が 2 週目よりも低下した．しかし，あわせ絵では認証成功率が低下しないという結果になった．

最後に認証に成功した時の試行回数を調査した．その結果，あわせ絵では 3 回目の試行で認証に成功した例が少数ながら存在したのに対し，暗証番号やパスワードでは 3 回目の試行で認証に成功した例は一回もなかった．

これらの結果から，以下の結論が導き出せると言える．

- あわせ絵認証における秘密情報の記憶負担は暗証番号認証と同等レベルである
- あわせ絵認証では，秘密情報の更新による記憶の混乱を回避可能である
- あわせ絵認証では，数回の認証試行によって，忘れていた秘密情報の想起が可能になる

また認証操作は Deja Vu 同様，画像を選択するだけなので，暗証番号認証と同じ打鍵数で認証可能であり，文字入力は不要なため PDA や携帯電話でも容易に操作可能である．しかし，あわせ絵の唯一の問題は認証時間である．実験結果から，認証にかかる時間は平均で 24.6 秒となり，暗証番号認証と比較しておよそ 10 倍の時間がかかる結果となった．

また安全性に関しては，ブルートフォース攻撃，総当たり攻撃，推測攻撃および覗き見攻撃に関して暗証番号認証との比較を行った．詳細は紙面の都合で割愛するが，推測攻撃に対しては，どちらが脆弱であるか甲乙つけがたいものの，その他の三種の攻撃手法においては暗証番号認証よりも安全性が高いことが確認された．興味のある方は，論文 [6] を参照して頂きたい．

これらの結果から，あわせ絵認証は認証時間を除けば暗証番号認証と同等の利便性を確保しており，かつ暗証番号認証よりも安全性を高い認証手法であるといえる．ただし例外である操作時間に関しては，安全性を損なうことなく，認証時間短縮を可能にする手法を探求するのが今後の課題である．

最後に，これまでに紹介した論文以外で画像認証に関する論文をいくつか紹介する．論文 [7] は，既存の画像認証をサーベイした論文である．なお論文 [8, 9, 10, 11] は，画像認証の評価に関する論文である．興味のある方は参照して頂きたい．

4 よりよい個人認証に向けて

一般にセキュリティシステムでは，安全性と利便性は反比例すると言われている．図 5 はその概念図である．図中の曲線は，個人認証の現状を表しており，安全性の高い認証手法は利便性が低く，利便性の高い認証方法は安全性が低いということを示している．

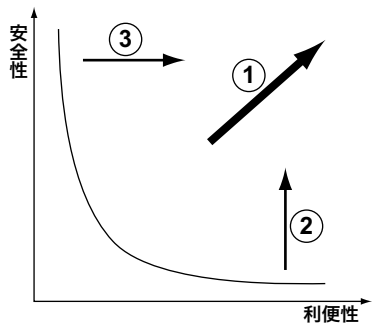

Figure 5: 個人認証における安全性と利便性の関係

この図で考えると，個人認証の理想は図中の矢印 1 のように，安全性と利便性をより高いレベルで両立させることである．しかし，その実現は容易ではない．そこでその足がかりとして，既存の手法と同等の利便性を保証しつつ，より高い安全性を実現する手法の探求 (矢印 2) や，同等の安全性を保証しつつ，より高い利便性を実現する手法の探求 (矢印 3) が望まれている．あわせ絵は，矢印 2 の一例であると言えよう．

よりよい個人認証の実現に向けて，その改善が望まれる知識照合型認証の問題点を整理すると，以下のような問題点が残されている．

1. 秘密情報の生成とその安全性
   ユーザが脆弱なパスワードを使えないようにする仕組み，ならびに脆弱なパスワードであることをユーザに知らせる仕組みを提案する必要がある．One-Time Password は，脆弱なパスワードを使えないようにするという意味で，この技術の一例であると考えることができる．SECUREMATRIX[15] のように，ある規則からパスワードを生成させるといった製品や，秘密情報の生成を簡単化するために”なぞなぞ”を使った手法の提案 [16] もあるが，これらもこの問題に対する改善策と言えよう．

2. 秘密情報の記憶
   秘密情報の記憶負担を軽減する方法を考案する必要がある．画像を使った画像認証はその一例であり，他の手法としては日常の生活記録を認証に応用する手法 [17] が提案されている．

3. 秘密情報の安全性と記憶可能性
   前述の 2 つの問題のバランスを考慮しなければならない．反比例すると言われている秘密情報の安全性と記憶可能性を両立可能にする新たな手法を探求する必要がある．

4. 秘密情報の入力
   キーボードによる秘密情報の入力は手間がかかる．またユビキタス環境の普及にともない，キーボードが利用不能な環境での認証も配慮する必要もある．これにともない新たな秘密情報の入力方法が望まれており，ジェスチャー [12] や人の振る舞いを応用した認証 [18] も提案されている．また秘密情報の入力については，実世界における覗き見という問題があり，その対索も必要となる．この問題に対してもユーザインタフェースによる改善策がいくつか提案されている [19, 20, 21].

5. 多数の秘密情報の管理
   Web サービスの普及にともない多くのパスワードが必要となり，その管理が問題になりつつある．既存の Web ブラウザにはパスワードマネージャがあり，またシングル サイン オンという技術も既に確立しているが，利便性が高く，かつ安全な秘密情報の管理手法に関する探求も行われている．論文 [22] は，Phishing 攻撃に対する対策手法の提案であるが，クライアントサイドの実装だけで複数サービスに対するパスワードの生成とその管理を容易にする手法としても注目に値する手法である．

6. アクセシビリティ
   認証システムは，誰でも使用可能であることが望まれる．健常者ではない方でも利用できるようなインタフェースや認証手法を探求する必要がある．

これらの項目を見ると，すべての項目がなんらかの形でユーザと関わりのある問題であると言える．つまり個人認証における問題点とは，利便性に関する問題ばかりであると言っても過言ではない．1 章でも述べたが，現状の個人認証システムは，安全性担保のための負担を過度にユーザに依存していることであり，その負担を軽減するようなシステムや手法の開発は急務である．そのためにはセキュリティ分野の研究者だけではなく，ユーザインタフェースや認知心理学などヒューマンファクターを扱う幅広い分野の研究者による貢献が必要であることに疑いの余地はない．

本稿をきっかけとして，より多くの研究者が個人認証の諸問題に目を向け，研究対象として興味を持って頂ければ幸いである．

References

[1] visKey, SFR SOFTWARE, http://www.sfr-software.de/cms/EN/pocketpc/viskey/, site accessed at Dec 20, 2006.

[2] L.Sobrado and J.C.Birget,“Graphical passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm, site accessed at Dec 20, 2006.

[3] Rachna Dhamija and Andrian Perrig, Deja Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, 2000. http://www.ischool.berkeley.edu/ rachna/dejavu/ site accessed at Dec 20, 2006.

[4] Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers and Ryan Swanstrom, Picture Password: A Visual Login Technique for Mobile Devices, NISTIR7030, July 2003. http://csrc.nist.gov/publications/nistir/nistir-7030.pdf, site accessed at Dec 20, 2006.

[5] 高田哲司，小池英樹: あわせ絵: 登録と通知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, August 2003.

[6] 高田哲司，大貫岳人，小池英樹: 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，情報処理学会論文誌，Vol.47, No.8, pp.2602–2612, August 2006.

[7] Xiaoyuan Suo, Ying Zhu and G.Scott Owen: Graphical Passwords: A Survey, 21th Annual Computer Security Application Conference(ACSAC2005), pp.463–472, 2005.

[8] De Angeli, A., Coventry , L., Johnson, G., Renaud, K.: Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems, International Journal of Human-Computer Studies, 63 (1-2), pp.128–152. 2005.

[9] Darren Davis, Fabian Monrose ad Michael K. Reiter: On User Choice in Graphical Password Schemes, 13th USENIX Security Symposium, pp.151–164, 2004.

[10] Thomas S.Tullis and Donna P.Tedesco: Using Personal Photos as Pictorial Passwords, CHI2005 Late Breaking Results, pp.1841–1844, 2005.

[11] Trevor Pering, Murali Sundar, John Light and Roy Want: Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, Vol.2, No.1, pp.30–36, 2003.

[12] Shwetak N.Patel, Jeffrey S.Pierce and Gregory D.Dbowd: A Gesture-based Authentication Scheme for Untrusted Public Terminal, Symp. on User Interface Software and Technology(UIST 2004), pp.157–160, 2004.

[13] 國 米仁, 脅かされる本人認証「はびこる奇怪論理とその考察」, http://www.mneme.co.jp/data/thesis.html, site accessed at Dec 20, 2006.

[14] J.C.Birget: The Graphical Passwords Project, http://clam.rutgers.edu/ birget/grPssw/index.html, site accessed at Dec 20, 2006.

[15] 株式会社シー・エス・イー: SECUREMATRIX, http://www.cseltd.co.jp/smx/, site accessed at Dec 20, 2006.

[16] 増井俊之: インタフェースの街角 (43) - 明るい認証システム，UNIX Magazine 2001 年 7 月号, アスキー, 2001.

[17] 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, March 2006.

[18] デバイス・ユーザーの歩き方で ID 認証，フィンランドの技術研究センターが開発, ITPro, http://itpro.nikkeibp.co.jp/article/USNEWS/20051017/222871/, site accessed at Dec 20, 2006.

[19] A.Harada, T.Isarida, T.Mizuno and M.Nishigaki: A User Authentication System Using Schema of Visual Memory, Biologically Inspired Approaches to Advanced Information Technology，Second International Workshop BioADIT2006，pp.338-345, 2006.

[20] Desney S. Tan, Pedram Keyani and Mary Czerwinsky: Spy-resistant keyboard: more secure password entry on public touch screen displays, Proceeding of OZCHI 2005, 2005.

[21] Volker Roth, Kai Richter and Rene Freidinger: A PIN entry method resilient against shoulder surfing, In Proc. 11th ACM Conference on Computer and Communication Security, pp.236–245, Oct 2004.

[22] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh and John C Mitchell: Stronger Password Authentication Using Browser Extensions, Proceedings of the 14th Usenix Security Symposium, pp.17–32, 2005.