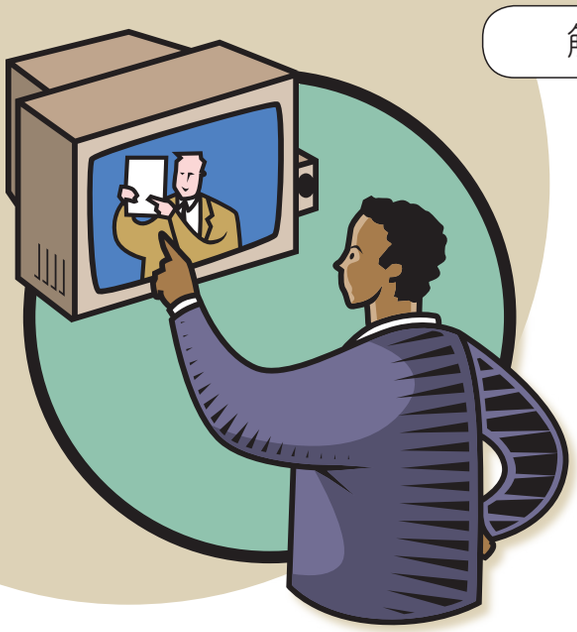
解　説



画像を用いた個人認証手法

小池英樹　電気通信大学
koike@acm.org

増井俊之　産業技術総合研究所
masui@pitecan.com

高田哲司　産業技術総合研究所
zetaka@computer.org

現在の情報社会において，個人認証手法として一般的なのは4桁PINや英数字パスワードといった文字列パスワードである．その安全性の根拠は組合せの数であるが，実際には人々は記憶を容易にするため簡単な文字列を選択する傾向が強い．またキーボードによる文字入力はユビキタス環境において使いやすいとはいえない．これに対し，画像を用いた認証手法が研究開発されている．本人しか知り得ない記憶情報を鍵として使用することによる安全性の高さ，記憶負荷の低さ，入力の容易さといった利便性の高さがその特徴である．本稿では，画像認証の概要，システム例，利点と問題点などについて解説する．

既存の個人認証手法

現在の情報社会において，個人認証の重要性が増している．従来の銀行ATMの利用やコンピュータへのログインに加え，携帯電話，各種Webサービスなど，さまざまな局面で個人認証が求められる．こうした個人認証手法は，所有物方式，バイオメトリクス方式，知識記憶方式の3つに大別できる．

所有物方式とは，物理的な鍵，入退室カード等，特定の物を所有することで認証を行う方式である．本方式の問題点は，この「鍵」を紛失，あるいは盗まれる可能性があり，その場合，これを取得した第三者の使用を防ぐことができないことである．したがって，銀行のATMカードなどでは本方式と知識記憶方式を組み合わせて使用するのが一般的である．

最近注目を集めている認証手法にバイオメトリクス方式がある．これは，指紋，掌紋，声紋，虹彩，静脈パターンなど各人に固有の生体情報を認証に使用する手法である．所有物方式のように物を持ち運ぶ必要がなく，紛失する恐れもない．知識記憶方式のように秘密情報を忘れる心配もない．さらに知識記憶方式，特に文字列パスワード方式のようにキーボード入力を必要としないため，コンピュータ操作に慣れた人以外でも比較的簡単に使用できる．

一方，バイオメトリクス方式の問題点としては，まず第1に誤認証の問題があげられる．たとえば，指紋認証の場合，手が荒れている等の何らかの理由で本人の認証に失敗するケース(本人拒否)と，本人以外，たとえば偽造された指紋により認証を突破されるケース(他人受容)がある．第2の問題は，認証の鍵として使用される生体情報の変更ができない点である．たとえば，何らかの理由で鍵として登録してある指紋情報が盗まれ，これを偽造されたとしても，唯一無二の生体情報であるがゆえにこれを変更することはできない．また生体情報を登録するという心理的抵抗感，認証デバイスの大きさ等の問題点もある．

知識記憶方式とは，ある秘密情報を記憶させ，認証の際にそれを正しく入力できるかどうかで認証を行う手法である．代表的なものには銀行ATMの4桁PINや，計算機ログインのための英数字パスワードがあり，各種Webサービスなど現在の情報システムにおける最も一般的な認証手法である．

一方，この文字列パスワード方式については，従来から多くの問題点が指摘されてきている．次章ではその問題点について述べる．

文字列パスワードの問題点

第1の問題点は安全性に対する疑問である．文字列パスワード方式ではパスワード文字列の組合せの数の大きさが安全性の根拠となっている．たとえば4桁PINの場合10^4=10,000通りの組合せがある．しかし，これは第三者がランダムに4桁数字を入力した場合，偶然当たる確率が10,000分の1だと言っているに過ぎない．実際にはユーザは，0000, 1234, 9999 といった簡単な数字か，生年月日，電話番号といった本人に関係する番号を選ぶ傾向にあり，実際に使用されるパスワード空間は理論的パスワード空間よりはるかに小さい．

長いパスワードを利用する場合，組合せの数はより大きくなるが，今度はユーザが長いパスワードを憶えられなくなる．結果として簡単な文字列を選択して辞書攻撃等によって破られるか，難しい文字列を選択して憶えきれずにメモをとり第三者に漏洩するという事態が生じる．

さらに文字列パスワードの場合，使用するシステムが異なっても同じパスワードを使用する傾向にある．理由はシステムごとに異なるパスワードを記憶するのが大変，あるいは個々の情報システムとパスワードの関係を記憶するのが大変だからである．結果として，1つの情報システムの認証を突破されると他のシステムの認証も突破される可能性が高くなる．

文字列パスワードの第2の問題点はその利便性の低さである．計算機の専門家が使うシステムのようにキーボードが標準装備されている場合は長いパスワードの入力は大きな問題にならないが，非熟練者が使う場合やユビキタス環境においては，文字入力は決して容易な作業ではない．これに対し，銀行ATMや携帯電話は誰でも使いやすいようにキーの数を最小限にしている．この場合，4桁PINのような単純で安全性の低い数字列を入力するのは簡単だが，長い英数字を入力するのは多くのユーザにとって受け入れがたいものになる．

つまり，4桁PINのように短いパスワードは記憶，入力も比較的容易であり，実装も容易かつ装置も小型だが，その安全性は低い．一方，長いパスワードは組合せ数は大きいが，記憶，入力ともに困難で，装置の小型化も難しい．

画像を用いた個人認証

近年，文字列パスワード方式に代わる新しい知識記憶方式の認証手法として，画像を用いた認証手法が注目されている．以下ではこの画像を用いた個人認証手法に焦点をあて，文字列パスワードとの比較，システムの紹介，その利点と問題点を述べる．

◉特徴

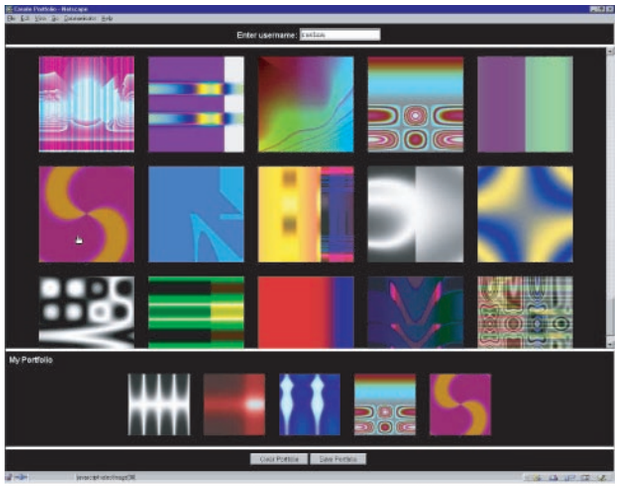
画像認証(Image-based authentication)とは，1枚あるいは複数の画像を提示し，これに対するある質問に答えさせることで認証を行う知識記憶型認証手法である．

その一般的な特徴としては，文字列パスワードのように秘密情報を正確に記憶する必要がなく，提示された画像を見て，考え，あるいは思い出して，質問に答えればよい．もし秘密情報を忘れた場合でも，提示された画像を見ることで思い出すことが可能となる．第2の特徴は，メモや口頭での伝達が困難だという点である．従来の文字列パスワードは紙に書いたり，言葉で伝えるのが容易であり，結果としてパスワード漏洩が起こりやすいという脆弱性を持つ．これに対して，画像パスワードは，パス画像をあえてプリンタ出力したり，メール等で添付しさえしなければ，一般に文字列パスワードに比べ他人への伝達が困難である．第3の特徴は，必ずしもキーボード入力を必要としないことである．文字列パスワード方式ではキーボードが必要となる．しかし，一般の人々は必ずしもキーボード入力には慣れていない．また，携帯電話等，物理的に十分なキー数を確保できない場合，その入力は非常に不便である．これに対し，画像選択方式では，画像を選択するだけなので，マウスやタッチパネル，あるいは携帯電話のように少ない数のキーボードでも簡単に使用できる．

◉システム例

DhamijaらはDeja Vu[4), 5)] と呼ばれる画像認証システムを開発している（図-1）．ユーザはシステムが自動的に生成する幾何学模様の中から5枚を指定しておく（以降，パス画像と呼ぶ）．認証時にはこの5枚を含む25枚の画像が，5×5の格子上のランダムな位置に提示され，ユーザは5枚のパス画像を正しく選択することで認証が成功する．認証の強度は25枚から5枚を選ぶ組合せ，つまり，${}_{25}C_5$=10,626通りとなり，4桁PINの組合せ数，10,000通りとほぼ同程度となっている．Deja Vuの問題点の1つは自動生成された幾何学模様が記憶しにくいことである．文字列パスワードと異なり，パス画像を正確に記憶する必要はなく，提示された画像を見て思い出せばよいのだが，その長期記憶可能性に関しては疑問が残る[11)]．

PassFaces[14)] はパス画像として人間の顔を使用する．システムが準備した顔写真の中から，ユーザはあらかじめ5人の顔をパス画像として登録しておく．認証画面（図-2）には1枚のパス画像を含む9枚の顔が表示され，この中から登録したパス画像を選択する．パス画像とし



http://www.sims.berkeley.edu/~rachna/dejavu/

図-1　Deja Vuの画面例．
パス画像として登録してある5個の図を選び出す．

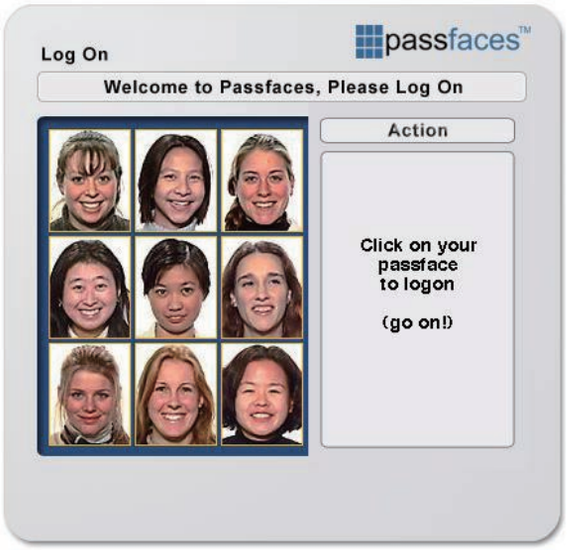


図-2　PassFacesの画面例．あらかじめ指定してある人の顔をクリックする．同様の操作を5回繰り返す．

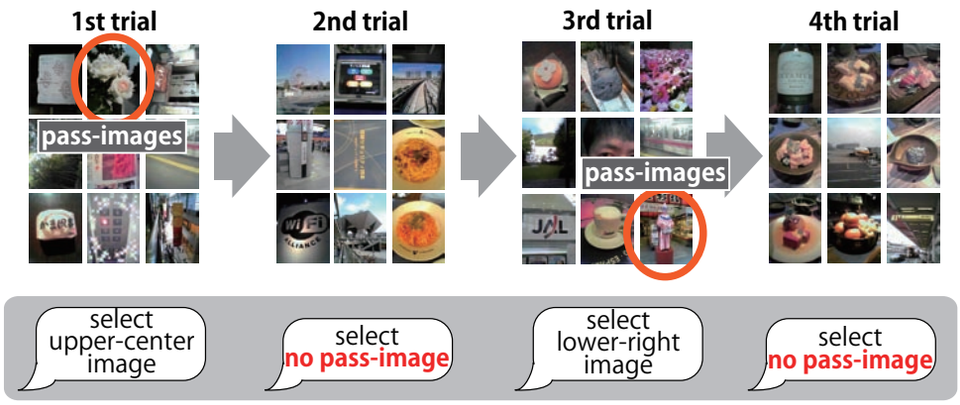


図-3　あわせ絵の認証画面例．あらかじめ指定したパス画像がある場合は対応する'1'から'9'のテンキーを，ない場合はテンキーの'0'を押す

て顔を利用する利点は，人間は人の顔に非常に敏感であり，一度見た顔の認識が非常に得意だという点，および異なる顔の区別が得意だという点が挙げられている．

Peringらはユーザ自身の撮影した写真をパス画像として利用するシステムを提案している[13]．ユーザ自身が撮影した写真はユーザの体験に基づく記憶（エピソード記憶）と関連し，それ以外の画像に比べて，忘れにくいというのがその理由である．ただしPeringらの手法はユーザのPCにある写真を母集団とするため，攻撃者にこれら写真集合を見られた場合，認証を破られやすいという脆弱性を持つ．

Jansenらのシステム[7]やニーモニック認証[18]もこうした画像選択方式の1つである．

高田と小池の「あわせ絵」[16),17)]は，携帯電話での使用を中心に考えた画像認証システムである（図-3）．各認証ステージでは9枚の写真が3×3の格子状に毎回ランダムに提示される．9枚中にはパス画像が1枚ある場合とない場合がある（ただし，認証プロセス終了までには最低1枚は現れる）．各画像の位置は携帯電話のテンキーの'1'から'9'に対応する．パス画像がある場合には対応するテンキーを押し，ない場合には'0'を押す．この認証ステージを複数回繰り返すことで認証が完了する．図-3の例ではN=4であり，「2,0,9,0」と押すことで認証が成功する．

このパス画像が出現しないケースというのはあわせ絵の特徴の1つである．PassFacesなどでは1画面に

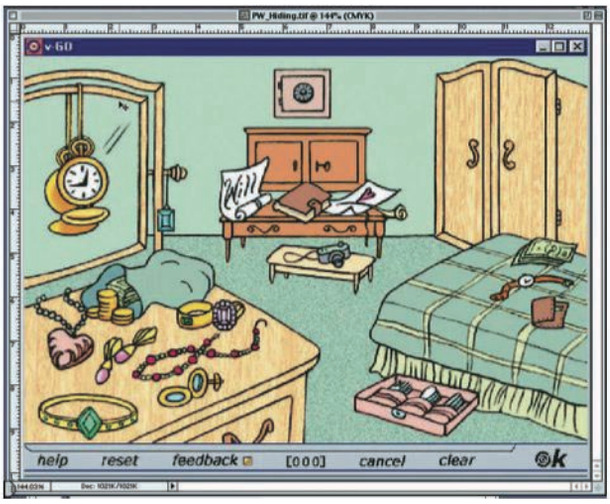


図-4 Passlogixの画面例．画面上のオブジェクトをあらかじめ指定した順番に選択する．

図-5 GATESCENEの画面例．左の食べ物と右のソフトキーボードを指定した順番に選択する．

必ずパス画像が表示されるが，パス画像の出現確率と他の画像の出現確率の差から，認証プロセスを何度か見ると第三者が容易にパス画像を推測できてしまう(Intersection攻撃)．あわせ絵ではパス画像を表示しない場合を設けることでこの問題に対処している．

あわせ絵の第2の特徴は，カメラ付き携帯電話と電子メールを利用したパス画像登録・変更の利便性の改善である．パス画像登録および変更には，カメラ付き携帯電話で撮影した写真を，電子メールに添付して認証サーバに送信する．ユーザは登録した自分の写真群の中からパス画像を指定する．こうしたパス画像更新の容易さは重要である．パスワードの定期的更新の重要性は情報セキュリティにおいてしばしば強調されているが，従来のシステムでは更新に手間がかかったり，更新後にパスワードを忘れることがあるため，励行されていない．これに対し，あわせ絵では簡単な操作でパス画像の更新が可能であり，かつ更新後にも忘れにくい．また，パス画像の登録時や認証時には確認の電子メールを送信することで，第三者による不正使用に気付くようにしている．

あわせ絵の第3の特徴は，携帯電話のキーボードに最適化したインタフェース設計である．携帯電話上でDeja Vuのように多くの画像を表示すると画面スクロールが必要となりキー操作が増える．このキー操作の数は利便性の1つの指標ともいえる．あわせ絵ではこれらを考慮し，1画面内の画像数は9枚に制限し，それぞれをテンキーに対応させた．

増井らは，パスワード認証を行うシステムのフロントエンドとして画像認証を利用することができる「マイ認証」システムを提案している[10]．マイ認証システムでは，パスワードを要求するWebページが表示されると自動的にDeja Vuやあわせ絵のような画像認証システムが呼び出され，認証の成功／失敗に応じて正しいパスワードまたは誤ったパスワードがもとのWebページにペーストされるようになっている．この方法を利用すると，パスワードにもとづく任意のシステムにおいて画像認証システムを利用することができるため，画像認証を日常的に利用することができ，さまざまな画像認証システムの有効性の実証を行うことも可能になる．

上に紹介した，複数の画像から正しい画像を選ぶ方式のほかに，1枚の画像の特定部分を選択する方式の画像パスワードシステムも提案されている．

Blonder[3] は与えられた図の特定の位置を順番に選択することで認証を行うというアイディアを提案した．Passlogixはこのアイディアを基に画像認証システムを開発している[12]．図-4はその認証画面である．ユーザはあらかじめ任意のオブジェクト（例：時計，カメラなど）をある順番で選択し，認証時には正しい順番でこれらのオブジェクトを選択することで認証に成功する．

鹿島のGATESCENE[9] も同様に図中の特定のオブジェクトを順番に選択することで認証を行う．図-5はGATESCENEの画面例である．ユーザは画像中の特定の部分(例：リンゴ，ミカンなど)とソフトキーボードの数字をあらかじめ登録した順番で選択する．

PasslogixやGATESCENEでは画面上の選択可能なオブジェクトが限られている．結果として，パスワードとして使用できるシーケンスの組合せが少ない．これに対し，PassPoints[19] は，特定のオブジェクトにこだわることなく図の任意の位置を誤差2.5mmの範囲内で選択可能とした(図-6)．図において黒い正方形で表されている領域がユーザの登録した点であり，その順番が数字で示されている．ただし，実際の認証時にはこの正方形や数字は表示されない．

図-6　PassPointsの画面例．ユーザの選択した場所と順番が正方形と数字で示されている．認証時にはこれは表示されない．

図-7　CAPTCHAの画面例．

1枚の画像上での位置選択に基づくシステムの問題点の1つは，選択の位置および順番の長期記憶可能性である．特に表示画面はシステムが提供するものであるため，ユーザ自身のエピソード記憶は利用できない．したがって，ユーザ自身がなんらかのシナリオを作って，これらを憶える必要がある．

もう1つの問題点は，認証画面が毎回同じである点である．その結果，認証時における選択場所も毎回同じとなる．もしユーザが選択する位置を第三者に覗き見られると(shoulder surfing)，第三者はそのユーザに簡単になりすますことができるであろう．

画像，あるいは画像上の位置を記憶して認証を行う手法のほかにも，画像を用いた認証手法がある．

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)[1] は，図-7のようにわざと歪ませた字を画面上に表示し，これを答えさせる認証手法である．本システムの目的はシステムにアクセスしてきているのが人間か，自動化プログラムかを判定することである．人間ならば，この文字を読んで正しく答えることができるが，スパマーなどが利用する自動化プログラムではこれが難しい．大手ISPの中にはすでに採用しているところがある．

今後の課題

◉画像認証の安全性

画像認証は，文字列パスワードに比べ一般にブルートフォース攻撃，辞書攻撃，ソーシャルエンジニアリングなどの点で安全性が高いとされている[15]．ただし，以下のような特徴的な脆弱性を持っている．

その第1は，ユーザに関する知識を利用することでパス画像を予想する，いわゆるeducated-guess攻撃である．たとえば，あるユーザが旅行中の写真をパス画像として登録した場合，このユーザとその旅行先を知っている第三者は，写真を見て認証を破ることができる可能性が高い．

原田らはこの問題を解決するために，画像にフィルタ処理を施す手法を提案している[6]．彼らの手法は適当なディジタルフィルタや2枚の画像を重畳することで元画像を第三者にとって判別困難なものとする．一方，元画像を知っている本人は，このフィルタ処理された画像から元画像を思い出すのが容易であると述べている．

画像パスワードにおけるもう1つの特徴的な脆弱性は，パス画像と他の画像の出現頻度の違いを利用した，「intersection」攻撃である．たとえばPassFacesなどでは，各認証画面においてパス画像は必ず1つ出現するのに対し，他の画像は大量の画像からランダムに抽出されるため，パス画像以外の出現頻度はパス画像に比べて低い．その結果，何回かの認証フェーズを見れば，その出現頻度の差からパス画像が簡単に特定できてしまう．

この問題に対しては，銀行ATMのようにある回数以上の認証を許可しないことである程度の解決はできる．しかし，今後はおとり画像として使用する画像母集団の選択方法など詳細な解析が必要である．

こうした画像パスワードに特有の脆弱性に関するより詳細な議論は文献4)，15)，16)を参考にされたい．

◉画像認証の利便性

画像認証は，文字列パスワードのようにキーボード入

力を必要としない，必ずしも正確にパス画像を記憶する必要はなく，見て思い出せばいいという点などにおいて，利便性が高まっていると考えられるが，以下のような問題点もある．

その第1は，パス画像の登録や変更にかかる時間と手間が挙げられる．Deja Vuなどのシステムではシステムが準備した画像集合を見て，その中からパス画像を指定するのに時間がかかる．Peringらのシステムのようにユーザの所有する画像を利用する場合には，その画像の登録にも時間がかかる．あわせ絵ではこの画像登録の手間を軽減する手法を提案しているが，一般に画像認証システムでは文字列パスワード方式に比べ，手間と時間を必要とするのは事実である．

また画像認証では文字列パスワードに比べて認証にかかる時間が長い．これは画像認証の場合，提示された画像集合の中からパス画像を探すのに時間がかかるからである．大貫らの実験[11]では，被験者がおとり画像に興味を持って見てしまうことが観察されている．

おわりに

画像認証は人間の画像認知特性を利用した新しい認証手法で，従来の文字列パスワードにおける安全性と利便性のトレードオフを改善することができる．今後は，長期記憶可能性に関するユーザスタディや，脆弱性に関するより詳細な分析，その解決が重要である．

参考文献

1) Von Ahn, L., Blum, M. and Langford, J. : Telling Humans and Computers Apart Automatically, Communications of the ACM, Vol47, No.2, pp.57-60 (2004).
2) Angeli, A. D., Coutts, M., Coventry, L. and Johnson, G. I.: VIP: a Visual Approach to User Authentication, Proc. of the International Working Conference on Advanced Visual Interface (AVI2002), pp.316-323 (May 2002).
3) Blonder, G. : Graphical Passwords, U. S. Patent 5559961 (1996).
4) Dhamija, R. and Perrig, A. : Deja Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, pp.45-58 (Aug. 2000).
5) Dhamija, R. : Hash Visualization in User Authentication, Proc. on Human Factors in Computing Systems (CHI2000), pp.279-280 (2000).
6) 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 (Aug. 2005).
7) Jansen, W., Gavrila, S., Korolev, V., Ayers, R. and Swanstrom, R. : Picture Password: A Visual Login Technique for Mobile Devices, NISTIR 7030 (2003).
8) Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. and Rubin, A. D. : The Design and Analysis of Graphical Passwords, 8th USENIX Security Symposium, pp.1-14 (Aug. 1999).
9) 鹿島一紀：画像の位置情報による本人認証方式の研究開発 画像パスワードGATESCENE，コンピュータセキュリティ研究会，Vol.2000, No.68 (June 2000).
10) 増井俊之，塚田浩二，高田哲司：マイ認証，インタラクション2006論文集，pp.25-26 (2006).
11) 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) (Jan. 2005).
12) Paulson, L. D. :Taking a Graphical Approach to the Password, Computer, Vol.35, pp.19 (2002).
13) Pering, T., Sundar, M., Light, J. and Want, R. : Photographic Authentication through Untrusted Terminals, IEEE Pervasive Computing, Vol.2, No.1, pp.30-36, (Jan.-Mar. 2003).
14) RealUser, www.realuser.com
15) Suo, X., Zhu, Y. and Owen, G. S.: Graphical Passwords: A Survey, Proc. of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE (2005).
16) 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 (Aug. 2003).
17) Takada, T. and Koike, H. : Awase-E: Image-based Authentication for Mobile Phones Using User's Favorite Images, Proc. of 5th Intl. Symposium, Mobile HCI 2003, Springer, pp.347-351(Sep. 2003).
18) MNEMONIC GUARD, Mnemonic Security Ltd., (2001), http://www.mneme.co.jp/
19) Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N. : PassPoints: Design and Longitudinal Evaluation of a Graphical Password System, Int. J. Human-Computer Studies Vol.63, pp.102-127 (2005) .

（平成18年4月10日受付）