あわせ絵: 登録と通知による画像認証方式の強化法

高田　哲司[1]　　小池　英樹[2]

電気通信大学 サテライトベンチャビジネスラボラトリ[1]
電気通信大学大学院 情報システム学研究科[2]

画像を用いた認証が記憶照合による認証方式の人間の記憶に起因する問題点を改善する方法として注目を集めているが，その一方で人工的な画像の利用や記憶すべき画像数の多さ，照合時にパスワードとなる画像が必ず提示されるなどの問題が残されている．そこで本研究では登録と通知というインタフェースを画像認証に導入するとともに「照合すべき画像が存在しない」という事象を認証方法にて意図的に利用することにより，それらの問題点を改善する方法を提案する．またこの提案に基づきカメラ付き携帯電話を対象とした画像認証システム “あわせ絵” について紹介する．

Awase-E: making image-based authentication to be secure and less load of memory providing image registration and user notification

Tetsuji TAKADA[1]　and Hideki KOIKE[2]

Satellite Venture Business Laboratory
University of Electro-Communications[1]

Graduate School of Information Systems
University of Electro-Communications[2]

This paper describes about image-based authentication system called “Awase-E”. Image-based authentication like “Deja Vu” are watched by many people because it has a potential abilities to improve the problems caused by a human. On the other hand, such authentication system still have left some problems: It uses randomly generated images, Users have to memorize some but not a few images, Password images are displayed in each authentication attempt. In this research, we propose the method to make image-based authentication to be more secure and less load of memory. One is to integrate image registration and user notification into image-based authentication. The other is that it intentionally makes use of the situation as “there is no password images” in authentication attempt. We introduce new image-based authentication “Awase-E” that is supposed to use with cellular-phone with digital camera.

1. はじめに

新たな認証方法として画像を用いた認証方式☆が提案されている．この認証方式の特徴は「人間の記憶に関する問題」に着目し，その改善を試みている点である．記憶による認証の問題点は「意味のないパスワード情報を記憶し，かつ必要に応じてそれを完全に思い出さなければならない」という人間にとって困難な行為を強いていることである．画像認証は「文字列を思い出す」から「画像を認識する」という行為にすることで認証時に人間に必要とされる行為を簡易化し，その問題の改善を行っている．

しかし既存の画像認証はいくつかの点で問題が残されているため，その実用化が進んでいないと考えられる．そこで本論文では画像認証における問題点を整理するとともに,「通知」と「登録」というインタフェースを認証システムに追加することによる改善方法を提案する．さらにこの提案に基づきカメラ付き携帯電話を対象とした画像認証システム「あわせ絵」について紹介し，最後にあわせ絵の利点，安全性および今後の課題について考察を行う．

☆ 以降，画像を用いた認証方式を画像認証と呼ぶ

2. 画像認証の問題点とその改善法

認証とはある行為を行う者が正当な権利を持つ者であることを確認するための技術である．既存の認証方法は照合情報に基づき，1. 所有物による認証 (IC Card，鍵)，2. 知識/記憶による認証 (アカウント+パスワード，暗証番号)，3. 生体情報による認証 (指紋，虹彩，筆跡) の三種類に分類できる．画像認証は知識/

記憶による認証の一つであるが，この認証方法の他の方法と比較した時の利点は以下の通りである．

所有物による認証と比較した場合

- パスワードとなる情報が容易に変更可能
- 紛失の心配がない
- 複製による危険が少ない

生体情報による認証と比較した場合

- パスワードとなる情報が変更可能
- 心理的抵抗感がない
- 利用不可能な人は極めて少ない
- 経年変化/欠損による利用不能の可能性がない

しかしアカウント/パスワードに代表されるこの認証方式の問題点は，なんらかの情報を記憶し，かつそれを必要に応じて思い出さなければならないことである．しかし人間にとってこの作業は容易なことではなく，それゆえに記憶しやすい文字列を使用したり，パスワードを書き留めてしまうなどの問題を引き起こしている．画像認証は照合情報として画像を使用することによって記憶が容易，提示されれば思い出しやすいといった人間の記憶特性を利用可能にし，前述の問題を回避可能にしている．また照合時の行為が “思い出す” から “認識する” になることで，画像自体を正確に思い出す必要がないという利点も得られている．

しかしその一方で画像認証には以下に述べるような問題が残されている．

一つは無意味な画像を利用していることである．Deja Vu[1] では人工的に作成されるランダムアート画像 [2] を照合画像に用いている．そのため画像とはいえ人間にとっては意味のない情報であり，文字列の場合と同様にその記憶や認識が容易でないという問題を抱えることとなる．したがって画像の利用による利点を半減させることになる．

また記憶すべきパスワード画像数の多さも画像認証の利点を半減させる問題である．画像認証はその安全性を確保するため複数枚の画像を使って認証を行う．しかし，この画像枚数が多いとユーザの記憶への負担が増加し，人間に起因する問題を誘発する恐れがある．

次の問題点はパスワード画像の追加が困難であり，その変更も容易でないことである．既存の画像認証は認証システムが持つ画像のみを利用しており，画像の追加を許していない．したがってパスワード空間としての全画像数は拡大しないことになる．また，システムが提示する画像の中からパスワード画像を選択しなければならないため，パスワード画像の更新が行われにくいと考える．画像認証によりパスワード画像作成の手間は減るものの，その決定には手間がかかるからである．具体的には，画像を閲覧する必要があるために時間が必要となることや，提示される画像はユーザにとってなんらかの関連を持った画像ではないため，どれをパスワード画像にするか迷うことが考えられるためである．

最後の問題は照合時にパスワード画像が必ず提示されることである．画像認証は “認識” による照合のため，パスワード画像が照合時に必ず提示される．しかし，これが Intersection 攻撃といった新たな脅威を生じさせる原因となっている．Intersection 攻撃の詳細は 4.2 章で述べる．

2.1 改善方法

本節では前述の問題点を改善するために三つの提案を行う．

一つめは現実世界の写真を画像認証で利用可能にする．これは人間の記憶に対する負担を軽減するために必要である．人間は視覚的情報の記憶に長けているが，中でもエピソード記憶と呼ばれる自分の体験/経験に基づくものが最も忘れにくく，かつ思い出しやすいと言われている [3]．したがって，画像認証の利点である人間の記憶に対する負担軽減を実現するためには，そのような特性を持ちやすい写真の利用を可能にすることが望ましいといえる．

二つめは「照合時に必ずパスワード画像が提示される」という原則をなくすことである．つまり，認証システムは照合時に「パスワード画像が含まれない」という事象を意図的に発生させる．これにより画像認証に対する攻撃への安全性を確保する．

三つめはユーザが記憶すべき画像数を可能な限り少なくすることである．これにより写真の利用とあわせてユーザの記憶に対する負担を軽減する．

これらの提案は人間の記憶に対する負担を軽減することに主眼が置かれている．記憶照合による認証の問題点は，人間の記憶に対する負担の大きさに起因しているため，これを最優先に改善することが必要であると考えたからである．しかしそれにともない安全性が損なわれては認証としての意味がなくなる．そこで我々は以下の認証方法を提案する．

1 回の認証は 4 回の照合作業からなる．それら 4 回の照合がすべて正解であった場合に認証成功とする (図 1)．

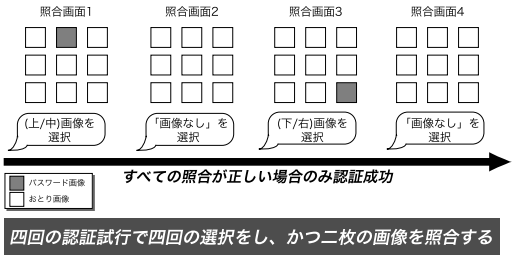

図 1　あわせ絵における認証方法

各照合では 9 枚の画像が提示され，その中には最大で 1 枚のパスワード画像が含まれる．つまりパスワード画像が含まれない場合もある．またおとり画像，パスワード画像ともに提示される位置はランダムであり，

またおとり画像は提示される画像もシステムによってランダムに決定される (図 2).

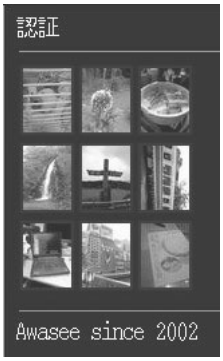

図 2　あわせ絵の認証画面

ユーザは各照合段階でパスワード画像を選択するか,「パスワード画像が含まれない」という選択をする．これにより照合回数を減らすことなく，ユーザが記憶すべき画像枚数を削減することが可能になる．また各照合段階でパスワード画像を最大で 1 枚しか提示しない理由は偶然による照合成功の確率を下げるためである．

なおこの認証方法では，各ユーザは最低でも 2 枚のパスワード画像を持つ必要がある．もちろんそれ以上の枚数のパスワード画像を設定することも可能である．

3. 画像認証システム: あわせ絵

我々は前章の提案を基にカメラ付き携帯電話の利用を前提とした画像認証システム「あわせ絵」を開発した．カメラ付き携帯電話を対象とした理由は，エピソード記憶になるような画像を取得でき，それを E-mail を用いて送付することが容易であることと，文字入力手段が貧弱であるため既存のアカウント/パスワード認証が使いにくいという点から別の認証手段が必要とされているからである．

あわせ絵では前述の改善法を実現するため，既存の認証方法に二つの「インタフェース」を追加する．既存の認証方法はパスワードを設定する「設定」と，実際に認証を行う「認証」の二機能により成り立っているが，あわせ絵ではこれに「登録」と「通知」というインタフェースを追加する (図 3).

「登録」とは認証システムに画像を追加登録するインタフェースである．これによりあわせ絵のユーザはいつでも任意の画像を認証時に使用する画像として登録することが可能になる.「通知」とは登録や認証，設定行為が発生したことをユーザに通知する機能である．これは UNIX 系 OS でネットワークを通じて計算機にログインした直後に最近のログインがいつどの計算機から発生したかを表示する lastlogin 機能と同じ目的を持つ (図 4).

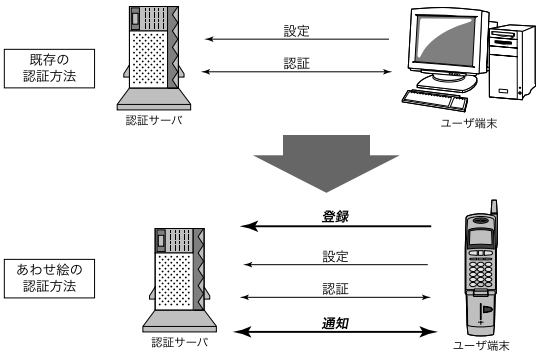

図 3　あわせ絵の機能群と既存の認証方法との比較

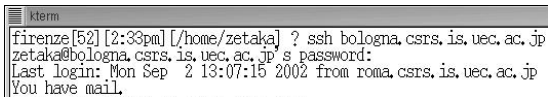

図 4　lastlogin の表示

3.1 システム構成

あわせ絵は認証処理を司る認証サーバと，ユーザの端末となる携帯電話のサーバ/ クライアント形式になる (図 5)．なお本システムは，サーバ/ クライアント間の通信に E-mail と Web を利用する．また Web による両者間の通信は暗号化された通信路によって保護され，その盗聴は困難であると仮定する．

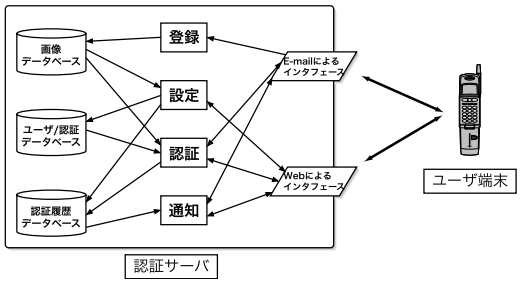

図 5　あわせ絵のシステム構成図

以下ではあわせ絵における四大機能についてその詳細を説明する．

登　　録

登録とは画像を認証システムに追加登録する機能である．これは E-mail を用いて行う．カメラ付き携帯電話で撮影した画像を E-mail に添付し，認証サーバに送付することで画像が認証サーバに登録される．

なお画像登録が完了すると，認証サーバから URL の書かれた E-mail が届く．この URL で指定された Web ページにアクセスすると自分が登録した画像を見ることができる．これは二つの点で重要である．

一つは登録した画像が自分の携帯電話上でどのように見えるかを確認するためである．認証時に携帯電話に表示される画像は縮小された画像になる．また撮影

時と認証時に表示される画像の印象が大きく異なることもありうる．これらを考慮し，登録した画像を認証時と同じ表示法で事前に確認しておくことは重要である．またパスワード画像として使用することを考えた場合，その画像を覚える必要があると同時に，仮に忘れたとして思い出せるように訓練しておく必要がある．これらの点から認証時と同じ表示法で事前に画像を見ておくことは重要である．

もう一つは，これにより第三者がなりすまして画像を登録したことを知ることが可能になることである．これにより，自分の権限が悪用されつつあるということをユーザ自身が知ることになる．

なお安全性確保のため，登録によって生成される確認用 Web ページは一定時間後に自動的に削除される．

設　　定

設定とはパスワード画像を認証システムが持つ画像群から決定する機能である．これは Web を通じて行われる．認証サーバに登録されている画像群からいくつかの画像が提示されるので，それを閲覧しながらユーザはパスワード画像を決定する．ユーザにパスワード画像の候補として提示する画像群は二つの方法で指定可能である．一つは自分が登録した画像のみを提示，もう一つは登録時間によるフィルタリングである．

認　　証

認証とは実際の認証行為をする機能である．これは E-mail と Web の双方を用いて行なう．ユーザはまずはじめに認証サーバへ認証要求の E-mail を送る．すると認証サーバから URL の書かれた E-mail が返信される．この URL は認証用 Web ページへのリンクであり，そこへアクセスして実際に認証作業を始めることになる．認証方法は 2.1 章で説明した方法である．

なおあわせ絵のアカウント名は E-mail アドレスとなっている．そのため認証時にアカウント名を入力する必要はない．

通　　知

通知とは登録，設定ならびに認証が行われたことを通知する機能である．これは Web と E-mail の双方を用いて行われる．通知には能動的通知と受動的通知の二つの方法がある．能動的通知には E-mail が用いられ，通知対象となる行為の発生後すぐに認証サーバがその旨を該当ユーザに通知する．受動的通知は Web を通じて行われ，現在時刻より一定期間前までのすべての該当行為の記録を閲覧することが可能である．

4. 考　　察

本章では画像認証システム「あわせ絵」における利点と安全性，そして今後の課題について述べる．

4.1 利　　点

あわせ絵における利点は大きく二つある．

一つはユーザの記憶への負担が最小限におさえられるという点である．

画像認証の利点は，認証時に必要とされる情報が覚えやすく認識が容易で，かつ思い出しやすくしたことである．これにより人間の記憶に対する負担を軽減し，人間に起因する認証の問題の回避を目指している．しかしその一方で，ランダムアートなど人工的な画像を使用し，複数枚の画像を記憶しなければならないなどの問題が残されていた．

そこであわせ絵では，認証時に使用する画像の制約をなくし，現実世界の写真を使用可能にした．これによりユーザはエピソード記憶に基づく画像を認証に使用することが可能になり，人工的でシステムから提示される画像よりもその記憶が容易になるとともに，思い出しやすくかつ忘れにくくなる．さらにあわせ絵では認証方法に「パスワード画像が存在しない」という事象を取り入れることでユーザが記憶すべき画像枚数を最小限にし，記憶への負担を軽減している．

このように人間の記憶に対する負担を軽減することで，既存の認証方式よりも人間に起因する問題を回避可能にしている．

もう一つは「登録」「通知」による画像認証の安全性強化である．

“登録” により画像認証の安全性は二つの点で改善される．一つは認証システムがもつ全画像数の拡大が見込めることである．これにより認証システムのパスワード空間は時間とともに拡大され，認証システムの安全性が強化される．画像認証は理論的には広大なパスワード空間を持つものの，現実的にはシステムが保持する画像枚数によって制約される．したがって提示されるおとり画像の数にも制約があった．しかしあわせ絵では登録機能によって画像を追加登録することができるので，全画像数は時間とともに増加する．したがってこのような問題は生じない．

もう一つはパスワード画像の更新頻度の向上が見込めることである．照合情報が画像になったことでパスワード情報の作成は楽になったといえる．しかし，これだけではパスワード画像の更新には至らないと思われる．しかし認証に写真が利用できることで，ユーザは写真を撮り，それを認証で使用したいと思うようになると考える．またユーザの多くは，いい写真が撮れた場合にはそれをパスワード画像として使用したいとも思うであろう．あわせ絵では登録と設定の機能を利用することでそれを簡単に実現できる．これにより既存の認証システムではその実現が困難であったユーザによる自主的なパスワード情報の更新が見込めるようになり，認証システムとしてもその安全性を強化することが可能になる．

一方 “通知” による画像認証の安全性から見た改善点は,「自分の権限 (アカウント) が自分自身によってのみ使われているかを自分で確認する手段」を与えたことである．既存の認証システムでは確率的な安全性に

ばかり依存し，なりすましが試みられているとか，なりすまされたという事象をユーザが知ることができず，またその方法を提供することもしてこなかった．そこで我々は認証システムのログに注目し，それをユーザに提示することで「ユーザに自身の権利を各自で管理/制御する方法」を通知という機能として提供した．これにより，あわせ絵の記録と自分の行動記憶と擦り合わせることで，なりすましや悪用の発生を各ユーザが自身で知ることが可能になる．このようにシステム管理者など一部の人間だけでなく，ユーザ自身に管理/制御手段を提供することはセキュリティシステムにおいて重要であると考える [4]．また一度でも認証に失敗するとそれが通知機能により正当なユーザに通知されるため，なりすましの試みを躊躇させるといった抑止力効果も期待できる．

また認証システムの評価も「確率的になりすましはほぼ不可能である」から「なりすましは可能である．しかしなりすましが成功するまでの間にユーザがその事実を知り，なんらかの対処ができる」という評価も可能になると考える．

4.2 安 全 性

ここではあわせ絵の認証システムとしての安全性について議論する

写真 vs. ランダム画像

ここでは安全性の観点から画像認証における「写真」と「ランダム画像」について比較検討する．

まずはじめに，記憶，認識ならびに思い出しやすさについて考える．これは写真のほうが好ましいことに疑いの余地はない．特に自身の経験や知識に関連した写真は仮に忘れていたとしても，ふと見た時に思い出しやすいと言われている [3]．また認識についても写真のほうが容易であるという実験結果も得られている [1]．

次は第三者による推測の容易さである．これはランダム画像のほうが好ましい．写真の場合，多くのユーザはその記憶が容易であるため，何らかのかたちで自分に関連のある写真を選んでしまう傾向がある．したがって容易には推測されないような画像を選択するようにユーザ教育を行う必要がある．

しかし，この問題も「登録」と「通知」により改善可能であると考える．登録によりそのユーザの情報によって推測される画像の候補がたくさん存在するようになれば，パスワード画像を推測することができても特定することは困難になるからである．また万が一なりすまされても，通知により迅速にその事実を知ることができ，なんらかの行動を起こすことが可能である．したがってこれらの機能により「なりすましをほぼ不可能にする」という観点から「数回の試行ではなりすましが成功されないようにする」という見方もできるようになる．

三つ目は書き留めやすさである．これは双方ともに同レベルであると我々は考える．写真のほうが文書として書き留めやすいと考えられるが，これはあくまで画像の内容に依存したことであると考える．また書き留めによるパスワード画像の漏洩はおとり画像の提示法にも依存するといえる．パスワード画像が花の写真である場合，同時に提示されたおとり画像がすべて似たような花や草木の画像にすることで書き留め情報によるパスワード画像の特定を困難にすることも可能であると考えられるからである．

画像認証の場合はむしろ文書による書き留めよりも絵としての “描き留め” による脅威のほうが大きいと考える．この場合は一般的に写真よりもランダム画像のほうが簡単である．またパスワード画像を印刷してしまうことを考えると，その容易さは画像の内容に依存しない．これらの問題を回避するためにも簡単に覚えられ，かつ忘れても思い出せるようにすることが大事であるといえる．

最後は画像種の分散化と集約化である．相反する二つの特性だが，どちらも画像認証には必要な特性であると考える．分散化はパスワード空間が広大になるようにするとともに，おとり画像の多様化のためにも必要となる．集約化は認証時にパスワード画像と類似した画像の存在がなりすましの成功を困難にするという点で必要となる．

これも写真のほうが好ましいと考えられる．ランダム画像は，ランダムとはいえある規則に基づいて作成されている以上その種類には限界があると考えられる．しかし写真にはそのような制約がない．また集約化についても写真にはある特定の撮影パターンが存在したり，多くの人がよく撮影する風景なども存在するため類似した画像が十分得られると考えられるからである．

種々の攻撃法とその対策

画像認証でおこりうる攻撃は四種類ある．それは Brute-force 攻撃，Educated Guess 攻撃，Observation 攻撃，Intersection 攻撃である．本節ではこれらのうち Educated Guess 攻撃と Intersection 攻撃について述べる．

Educated Guess 攻撃とは，あるユーザに関する情報を持つ第三者がその情報をもとにパスワード情報を推測することでなりすましを行おうとするものである．この攻撃は写真を用いた画像認証における大きな脅威であることに疑いの余地はない．

これに対しあわせ絵では登録と通知によりその改善が可能であることは “写真 vs. ランダム画像” の節で述べた．しかしこの方法でも限界はある．そこで推測によるパスワード画像の特定が困難になるような画像提示法を行う必要がある．具体的には，照合時に提示されるおとり画像群にパスワード画像と意味的にも絵的にも類似した画像を必ず提示する．これにより推測によるパスワード画像の特定をより困難にする．このように確率的にではなく，人為的な攻撃にもその安全性を確保できるような枠組みを考えていく必要がある

が，これは今後の課題である．

Intersection 攻撃とは画像認証に特有の攻撃で「パスワード画像が照合時に必ず提示される」という前提を悪用する攻撃である．この攻撃の脅威は以下のような状況を想像すると理解できる．もしすべてのパスワード画像が一回の認証試行で表示され，かつおとり画像が次の認証試行ですべて入れ替わるという状況下では二回の認証試行の画像群を取得するだけで，パスワード画像が特定できることになる．

これに対しあわせ絵では安全性を確保している．なぜならばあわせ絵では「パスワード画像が含まれない」という事象を意図的に利用しているため Intersection 攻撃の前提となる条件が成立しないためである．しかし，これと同様の目的で照合時の提示された各画像の出現頻度を求めることでパスワード画像を絞りこむことが可能になる．そこで我々は優先度付きおとり画像群の生成を提案する．これはパスワード画像の数倍程度の枚数の画像を選択し，これらの画像を優先的におとり画像として提示することで，おとり画像の出現頻度をパスワード画像と同程度にし，Intersection 攻撃によるパスワード画像の特定を困難にする方法である．この機能はシステムが自動で画像群を生成し提示していくことが望ましいが，どのような画像を選択したらよいかは今後の課題である．

4.3 今後の課題

あわせ絵における今後の課題について述べる．

一つは携帯電話の盗難/悪用時に対する対策である．あわせ絵は記憶による認証方法のため，携帯電話が盗難/悪用されたとしてもそれがすぐになりすましにはつながらない．しかし携帯電話にパスワード画像が保存されていた場合，そこからパスワード画像が漏洩する可能性がある．この脅威に対する対策は基本的にユーザ側でしか実施できない．使わない時はキーロックをする，パスワード画像を携帯電話内に保存しない，または他の多数の画像とともに保存しておくなどの対策が望まれる．

一方，あわせ絵としては通知機能によって携帯電話を紛失したとしても，Web を通じて自分の権限の利用状況を知ることは可能である．しかし，なりすまし発見後のことが考慮されていない．なりすまし発見後にユーザが取るべき対処法についても今後考察していく必要がある．

もう一つはパスワード画像の推測をより困難にする画像提示法の考案である．あわせ絵では Deja Vu[1] で提案されている方法を基に「選択すべき画像はない」という事象を導入し，記憶すべき画像数を増加させずに “なりすまし” を困難にした．しかし画像認証に特有の攻撃に対する安全性を増すためにはさらになんらかの対策を行う必要がある．

我々は 4.2 章で Educated Guess 攻撃ならびに Intersection 攻撃について述べた．Intersection 攻撃に対しては優先度付きおとり画像群を提案し，Educated Guess 攻撃に対してはパスワード画像と意味的にも絵的にも類似した画像を提示法をその対策として提案した．今後はこれらの実現に向けて考察を進めていく必要がある．

5. おわりに

本研究では，既存の画像認証システムの問題点を整理し，それらの問題を改善しうる方法を提案した．そしてその提案に基づき，カメラ付き携帯電話を対象とした画像認証システム「あわせ絵」を開発した．

本研究では画像認証に「登録」と「通知」というインタフェースを加えることで実世界の任意の写真を認証システムで利用できるようにするとともに，認証システムにおける各ユーザの利用状況をユーザ自身で確認可能にした．さらに，認証時の画像提示法において「パスワード画像が存在しない」という事象を意図的に発生させることにより，画像認証に特有の攻撃方法に対する安全性を確保するとともに，人間の記憶に対する負担の軽減を実現した．

今後の課題は携帯電話の盗難/悪用時の対策と第三者によるパスワード画像の推測をより困難にするような仕組みについて考察を進めていく予定である．

参考文献

1) R. Dhamija and A. Perrig: Deja Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, pp. 45–58, Aug, (2000).
2) A.Perrig and D.Song: Hash Visualization: a New Technique to improve Real-World Security, In International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC), (1999).
3) 増井 俊之: インターフェイスの街角 (43) – 明るい認証システム, UNIX MAGAZINE, (株) アスキー, Vol. 16, No. 7, pp. 185–189, July, (2001).
4) 高田哲司, 小池英樹: ログ情報視覚化システムを用いた集団監視による不正侵入対策手法の提案, 情報処理学会論文誌, Vol.41, No.8, pp.2216-2227, (2000).
5) 國米 仁: 記憶照合による個人認証手法 (囮混在秘匿方式), コンピュータセキュリティシンポジウム 2000 (CSS 2000), pp. 213–218, Oct, (2000).
6) 勝田亮, 平石広典, 溝口文雄: グラフィックパスワードを用いた Web 個人認証システムの設計, 情報処理学会コンピュータセキュリティ研究会研究報告 2002-CSEC-16, Vol. 2002, No. 12, pp. 91–96, Feb, (2002).