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

高田哲司[†] 小池英樹[††]

複数画像から正候補を選択する方式による画像認証が知識/記憶照合による認証方式の人間に起因する問題点を改善する方法として注目されている．しかしその一方で，システムが提供する画像のみを使用している，記憶すべき画像の枚数が多い，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．そこで本研究では画像登録と利用通知という機能を導入するとともに「照合すべき画像が提示画像群に存在しない」という事象を意図的に導入することで，既存の画像認証における問題点を改善する方法を提案する．これによりユーザの記憶に対する負担を軽減可能にするとともに，画像認証に対する攻撃への安全性を確保することも可能になる．この提案に基づき，我々が開発したカメラ付き携帯電話の利用を対象とした画像認証システム「あわせ絵」についても紹介する．

Awase-E: the Method Enables an Image-based Authentication to be More Secure and Familiar for Users with Providing Image Registration and User Notification

Tetsuji Takada[†] and Hideki Koike[††]

We propose the method that makes image-based authentication to be more secure and familiar to users. We introduce a novel image-based authentication system, called “Awase-E”, based on the methods. Current image-based authentications have some problems: using artificial images, necessary for memorizing some but not a few images and presenting password images at all time. In order to improve them, we introduce “image registration” and “notification to users” into image-based authentication. It makes possible to reduce the load to human memory and build a security against some types of attacks.

1. はじめに

アカウント/パスワードによる認証方法の問題を改善する方法として画像を用いた認証方式（以降，画像認証と呼ぶ）が提案されている[1)]．この認証方式は既存の知識/記憶による認証方式において最大の問題点であった「人間に起因する問題」に着目し，その改善方法を提案したものとして注目を集めている．人間に起因する問題とは，認証における安全性を維持するために人間にとって不得意であり，簡単には遂行できない作業を強制している点である．具体的にいうと「意味のない文字列を記憶しなければならないとともに，認証時にはそれを間違いなく完全に思い出せなければならない」ということである．画像認証は，認証時に人間が行うべき行為を「文字列を思い出す」から「画像を認識する」という行為に変換することにより，ユーザに課される記憶負担を軽減し，その問題の改善を可能にしている．

しかし提案されている画像認証は，いくつかの問題が残されている．そこで本論文では，既存の画像認証の問題点を整理するとともに，それらの問題を改善する方法として「画像登録」と「利用通知」という枠組みを導入するとともに「照合すべきパスワード画像が含まれない」という画像提示法を利用する方法を提案する．さらに我々は，この提案を基にカメラ付き携帯電話での利用を対象として開発した画像認証システム「あわせ絵」について紹介する．

本論文では，2章で画像認証とその問題点を整理するとともに，それらに対する改善方法を提案し，3章ではその提案を基にカメラ付き携帯電話での利用を対

† 電気通信大学サテライトベンチャビジネスラボラトリ
Satellite Venture Business Laboratory, University of Electro-Communications
†† 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, University of Electro-Communications

象として開発した画像認証システム「あわせ絵」について紹介する．4 章では，考察として提案方法の利点，安全性，今後の課題について述べる．

2. 画像認証の問題点とその改善法

2.1 知識/記憶に基づく認証方式と画像認証

認証とは，ある操作を実行する際にその操作者が該当操作を行う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方法に基づき 3 種類に分類できる（**表 1**）．

この中で「知識/記憶による方法」は他の 2 つの方法と比較して利点も多く[5),6)]，現在も多方面で利用されている．しかしその一方で，この方法には大きな問題がある．それはユーザである人間にとって，その実行が容易ではない行為を強いることである．それが結果として認証システムの安全性を損なうような種々の行為をユーザにさせてしまう原因となっている．このような問題の解決を試みたのが Deja Vu[1)]（**図 1**）に代表される正候補選択方式による画像認証である．画像認証と呼ばれる認証方式はほかにも提案されているが[8)]，以降，本論文で画像認証とは上記の方式に基づく画像認証を指すものとする．

本方式による画像認証は画像をパスワードとして利用し（以降，パスワード画像という），複数提示された画像の中から事前に決定しておいたパスワード画像を選択することで認証を行う．これによりパスワード情報の記憶ならびに想起を容易にするとともに望ましくないパスワードを使用不可能にする，さらに認証時の作業を簡易化するなどの利点が得られ，結果として人間に起因する認証システム上望ましくない行為の回避を可能としている．

2.2 画像認証における問題点

画像認証は記憶/知識による認証方式の問題点を改善しうる方法である．しかし，画像認証には以下にあげるような問題点が残されている．

1 つめはユーザとは無関係な人工画像[2)]の利用である．人間にとって画像は文字列よりもその記憶や想起が容易であるという特性を持つ．しかし既存の画像認証は，認証システムが一方的に提供するユーザとはなんの関係のない画像を利用している．これでは画像とはいえ，ランダムなパスワードの使用を強制されている状況と同様であるといえ，前述の利点を享受できているとはいえない．

2 つめはパスワード画像の追加や変更が困難なことである．既存の画像認証は画像の追加を許していなかったり，その方法がユーザにとって容易でなかったりすることが多い．また意味のない画像を利用しているため，パスワード画像の決定は容易ではなく，またその記憶に対する負荷も大きい．したがってパスワード画像は更新されにくい状況にあるといえる．

3 つめは記憶すべきパスワード画像数の多さである．画像認証ではその多くが安全性を確保するため複数枚の画像を照合することで認証を行う．しかし，記憶すべき画像の枚数が多くなればなるほど，画像とはいえ，それらすべての記憶が困難になる．結果として既存のパスワードによる認証と同様の問題を生じさせる恐れがある．

最後はパスワード画像を提示することに起因する問題の存在である．画像認証が既存のパスワード認証と異なる点は，認証時に照合する情報が必ず提示されるという点である．これは “Intersection Attack” と呼ばれる脅威を生じさせることが知られており，なんらかの対策が必要である．Intersection Attack の詳細は 4.2 節で述べる．

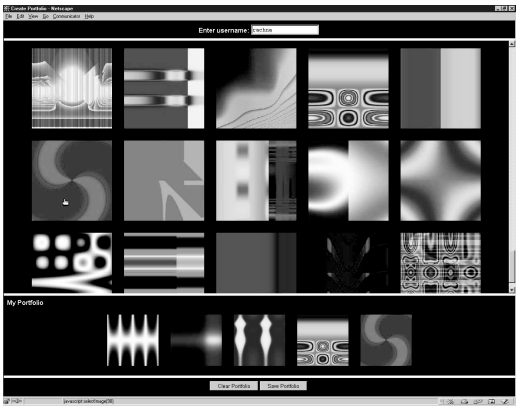
2.3 画像認証の問題を改善する 4 つの提案

前節の考察をふまえ，我々は画像認証における問題点を改善するための 4 つの提案を行う．

1 つめは利用可能な画像の制約を撤廃することである．これは画像を利用することによる人間の記憶負担軽減の利点を最大限享受可能にするためである．人間

表 1 認証方法の区分
Table 1 The three major authentication methods.

方法	例
所有物による方法	IC Card，鍵
知識/記憶による方法	アカウント + パスワード，暗証番号（PIN）
生体情報による方法	指紋，虹彩，筆跡



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

図 1 Deja Vu の画面イメージ
Fig. 1 A screen image of Deja Vu.

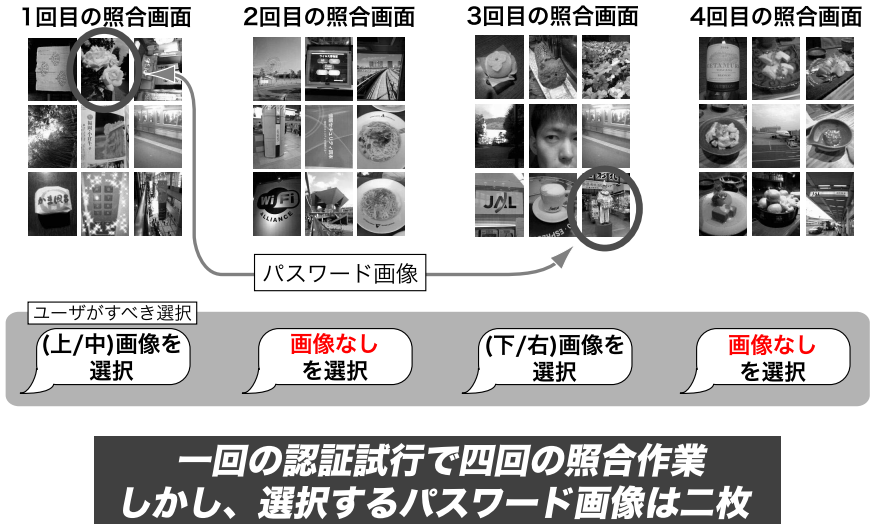


図 2 あわせ絵の認証方法（N = 4，P = 9）
Fig. 2 Detailed authentication method in Awase-E.

は画像などの視覚的な情報を記憶する能力に長けているが，画像であればなんでもよいというわけではない．さらに人間は，エピソード記憶と呼ばれる自分の体験に基づいた情報が最も忘れにくく，かつ思い出しやすいといわれている[5]．この特性を画像認証で利用するため，現実世界の写真を利用可能にすることが望ましい．したがって画像認証に使用する画像を特定の画像種に限定しないことが必要であると考える．

2 つめは認証システムで使用する画像をユーザが登録可能にすることである．これも前述のエピソード記憶に基づく画像を画像認証で利用可能にするために必要である．そのためにも画像登録は，ユーザ自身で簡単に実行可能であることが必要条件となる．

3 つめは「認証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が照合時に提示する画像群の中にパスワード画像が 1 枚も含まれないという組合せを故意に発生させることである．これにより特定の攻撃法に対する安全性を確保する．

4 つめはユーザが記憶しなければならないパスワード画像数を削減可能にすることである．これもユーザの記憶に対する負担を軽減するために必要である．

これらの提案を実現させ，かつ認証における安全性を確保するため，我々は以下のような認証方法を提案する（**図 2**）．

1 回の認証は **N** 回の照合作業からなる．認証は **N** 回の照合作業がすべて正解であった場合にのみ認証されるものとする．各照合作業では，画面に **P** 枚の画像が提示される．この **P** 枚の画像の中に最大で 1 枚のパスワード画像が含まれるものとする．いいかえると，パスワード画像が 1 枚も含まれない場合もある．また提示される画像の位置はパスワード画像およびおとり画像ともにランダムである．つまりパスワード画像が決まった位置に表示され続けるということはない．なお “おとり画像” とは照合時に提示される画像のうち，パスワード画像でないものを指す．ユーザは各照合段階で提示された画像を認識し，その中に自分が事前に決定しておいたパスワード画像が含まれていればその画像を選択し，パスワード画像が含まれていなければ「パスワード画像なし」を選択する．

この「パスワード画像なし」という選択肢を導入することにより，照合回数を維持したままユーザが覚えるべきパスワード画像枚数を減らすことが可能になる．また各照合においてパスワード画像を最大で 1 枚しか提示しない理由は，携帯端末などからの利用も考慮したものである．つまり照合時に提示できる全画像枚数（**P** 枚）を増やせないという条件の下で，第三者が偶然によりパスワード画像を正しく選択してしまう確率を下げるためである．なお本認証方法では，各ユーザのパスワード画像の枚数は 1 枚以上という制約の下で可変とする．

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で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の利用を前提にした理由は大きく 2 つある．

1 つは入力方法が貧弱である携帯電話や PDA に適

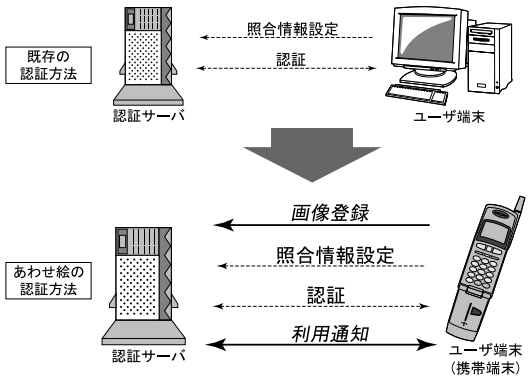


図 3 あわせ絵の機能群と既存の認証方法との比較
Fig. 3 The four modules on "Awase-E" and in comparison with current authentications.

した認証方式だと考えるからである．これらの機器の入力デバイスは，テンキーや非常に小さなキーボードであるため，快適かつ適度な速度で文字入力を行えるとはいえない．この状況において既存のアカウント/パスワード認証はきわめて使いにくいといえる．しかし画像認証の場合，ユーザに必要とされる行為は「文字入力」から「画像選択」になるため，これらの機器でも容易に操作可能となるからである．

もう 1 つはカメラ付き携帯電話の普及により，ユーザは自身の知識や体験に基づく写真を取得し，かつそれをその場ですぐに他の計算機へ送付することが容易に実行可能だからである．これによりエピソード記憶となるような画像の取得と，そのような画像の認証システムにでの利用が容易に実現可能だからである．

そこで我々は画像認証システム "あわせ絵" を開発した．これは既存の認証方式に実装されている「照合情報設定」と「認証」の 2 機能に「画像登録」と「利用通知」の機能を組み合わせたものになる（**図 3**）．なお「照合情報設定」とはパスワード情報を決定する行為であり，「認証」とは実際に認証をする行為である．

「画像登録」とは認証システムに画像を "追加登録" する機能である．つまり認証システムに画像を登録するためのインタフェースであるといえる．この機能によりユーザはいつでも任意の画像を認証システムに登録することができる．登録された画像は，パスワード画像およびおとり画像として照合時に利用される．

「利用通知」とは画像登録や認証試行の発生およびその結果，ならびに照合情報設定の各行為が発生したことをユーザに通知する機能である．つまりユーザに利用状況を通知するインタフェースであるといえる．本機能では，能動的通知と受動的通知の 2 種類の通知方法を提供する．能動的通知は認証システムからユーザに能動的に通知する方法であり，通知対象の行為が発生するたびにその旨をユーザに E-mail で通知する．受動的通知は，ユーザからの要求に従い過去の利用履歴を提供する方法であり，現在時刻より過去一定期間における利用履歴を Web ページとして提供する．

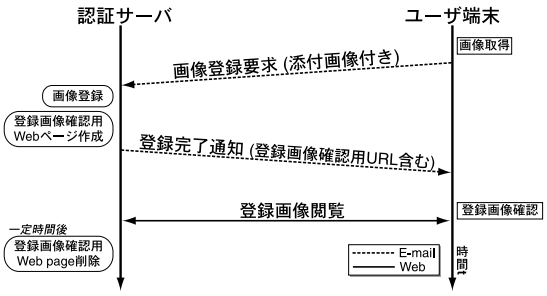


図 4 画像登録の処理詳細
Fig. 4 Process flow about image registration.

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認証するユーザの操作端末とのサーバ/クライアント構成になる．また本システムはサーバ/クライアント間のやりとりに Web ページと E-mail の双方を用いる．また Web による両者間の通信は暗号によって保護され，その盗聴は困難であるとする．以下ではあわせ絵における 4 大機能についてより詳細に説明する．

画 像 登 録

画像登録とは認証時に提示される画像を認証サーバに追加登録する機能である（**図 4**）．この機能は E-mail を用いて行われる．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その画像が認証サーバに追加登録される．

なお本処理は処理が正常に行われたことを知るための確認作業が必ず発生する．画像登録が正常に処理され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自身の端末で見ることができる．これは 2 つの点で重要である．

1 つは登録した画像が自分の携帯端末上でどのように見えるかを実際に認証で使用する前に確認するためである．照合作業時に提示される画像は縮小された画像となる．また照合作業時の画像がユーザの持っていた画像の印象とは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見ておくことは重要である．

もう 1 つは登録した画像を事前に見て「印象づけて」おくことである．これはパスワード画像としての利用を前提とした場合に画像の記憶ならびにその想起

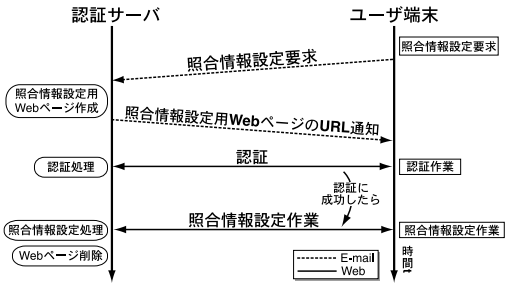


図 5 照合情報設定処理の詳細
Fig. 5 Process flow about setting a password image.

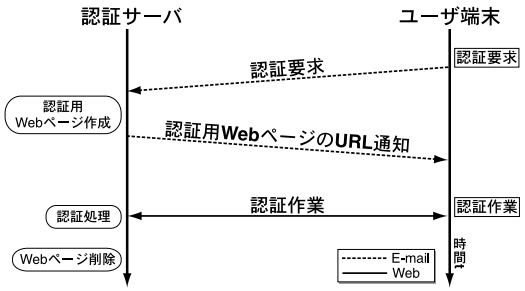


図 6 認証処理の詳細
Fig. 6 Process flow about authentication.

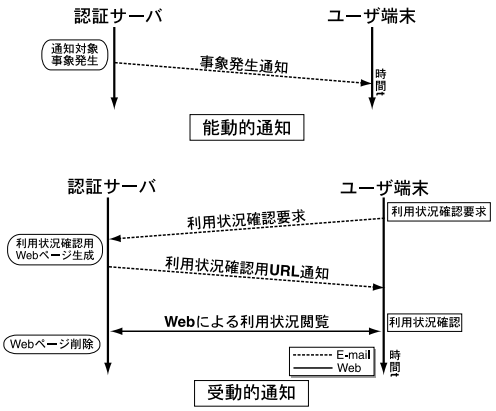


図 7 利用通知処理の詳細
Fig. 7 Process flow about user notification.

を支援するために必要な作業である．また本機能により，第三者が正当なユーザになりすまして画像を登録したことを知ることも可能になるという利点もある．なおこの目的のために生成された確認用 Web ページは，安全性確保のため一定時間後には自動的に削除される．

照合情報設定

照合情報設定とは，認証サーバに登録されている画像群から自分のパスワード画像を決定する機能である（**図 5**）．

この作業は E-mail と Web ページの双方を用いて行う．なお第三者によるなりすましを防ぐため，この作業を行う前に事前にユーザ認証を行うことは必須事項とする．認証に成功すると，認証サーバに登録されている画像がユーザに提示されるので，ユーザはその中から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は，2 つの条件にて制約を課すことが可能である．1 つは自分が登録した画像のみを提示する方法であり，もう 1 つは登録時刻に基づき，最近登録した画像から順に提示していく方法である．

認　　証

認証とは実際に認証を行う機能である（**図 6**）．

この作業は Web ページと E-mail の双方を用いて行う．認証を行おうとするユーザは，まずはじめに認証サーバへ認証要求の E-mail を送付する．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，そのリンクによって指定された Web ページへアクセスしてはじめて実際に認証作業を始めることになる．なお，あわせ絵におけるアカウント名は E-mail アドレスを用いており，認証要求によって送られてくる E-mail から抽出している．したがって認証時にアカウント名を入力する必要はない．

認証方法は 2.3 節で説明した方法であるが，携帯電話での利用を念頭におき，照合時に提示される画像の全枚数（$= \mathbf{P}$）は 9 枚としている．照合作業で各ユーザは，自分のパスワード画像を選択するか「パスワード画像が含まれていない」という選択肢を選択する．このような照合を複数回繰り返し，すべての選択が正しければ認証されることになる．

利 用 通 知

通知とは画像登録，照合情報設定ならびに認証が行われたことを正当なユーザに通知する機能である（**図 7**）．

利用通知の対象となっている事象は以下のとおりである．これは単に認証試行の発生を通知して不正行為の発生を知るだけでなく，その不正行為の結果をも調査可能にするとともに，認証にかかわる多くの事象をユーザに通知することによって，自身に対する脅威の存在を認識するとともに，より早い段階での対応を可能にする．

- 画像登録
- 照合情報設定
- 認証試行の発生（認証作業の始まり）
- 認証結果（認証が成功したか失敗したか）

- 受動的利用通知（Webページによる利用状況確認）

通知は Web ページと 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 2 つの方法が用意されている．能動的通知は E-mail を用いて行われ，通知対象である行為が発生するたびにその旨を当該ユーザに E-mail で通知する．受動的通知は Web ページを用いて行われ，ユーザの要求に応じて現在時刻から過去一定時間前までのすべての通知対象行為の発生履歴を Web ページとして提供する．

4. 考　　察

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

4.1 利　　点

画像認証システム「あわせ絵」には大きく 2 つの利点がある．

1 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ことである．この利点は画像認証で使用する画像種の制約の撤廃と，認証のためにユーザが覚えるべき画像数の削減可能化によるものである．これらにより既存の画像認証よりもユーザの記憶への負担を軽減可能にしており，結果として人間に起因した認証における種々の望ましくない行為の回避が可能になる．なお写真の利用とその安全性については 4.2 節で述べる．

もう 1 つは「画像登録」と「利用通知」による認証システムの安全性強化である．

まず画像登録による安全性改善点について 2 点述べる．1 つはパスワード画像の更新頻度が向上すると考えられることである．画像登録が可能になることでユーザは好きな写真をパスワード画像として使用したいと思うようになると考える．つまり画像登録がユーザ自身によるパスワード画像の更新を動機づけるということができる．またこれによりパスワード画像の作成やその決定時間を短縮できるという利点も生まれる．これらは既存の知識/記憶による認証方法ではその実現がきわめて困難であった問題である．

もう 1 つは認証システムが持つ全画像数が増加することである．これは認証システムのパスワード空間が拡大することと等価であるといえ，結果として認証システムの安全性に寄与すると考えられる．画像認証は照合情報が画像であるため概念的には広大なパスワード空間を持つものの，実際には認証システムが保持する画像数に制約されていた．しかしあわせ絵では画像登録機能の導入により認証システムの持つ画像数は漸増するため，そのような問題は発生しないといえる．

次に利用通知による安全性強化点について述べる．それは「自身の権限が自分によってのみ利用されているかを自分自身で確認できる」ようになることである．つまり不正行為の有無を自分で確認できるようになるのである．

既存の認証システムは確率的な評価方法による安全性に依存し，上記のような事象に対する対策手段を提供してこなかった．そのため第三者によってなりすまされ，ユーザの権限が侵害されたとしてもユーザはそれを知ることすらできず，結果として第三者によって悪用され，なんらかのきっかけで後にそれを知るという好ましくない状況を作り出してきたといえる．

今日，認証システムにおける攻撃や悪用の検知をシステム管理者に依存するという行為はもはや現実的でないといえ[4]，今後は各ユーザに対してその手段を提供することが重要であるといえる．このことからあわせ絵の利用通知機能は上記の役割を果たしうる手段の 1 つとして重要であるといえる．

またこの機能は攻撃者に対する抑止力を発生させる効果を持つともいえる．第三者によるなりすまし行為は，その行為の成否にかかわらず正規のユーザに通知されることになる．正規ユーザはその通知と自身の行動記憶を擦り合わせれば，それが正当な利用か第三者による悪用かは即座に判断可能だからである．

なお最後に，本認証方式は特定のハードウェアや Operating System には依存していない．したがってカメラ付き携帯電話での利用を推奨しているが，E-mail と Web が使用できる計算機ならば本認証方法を利用することは可能である．

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．

確率的な安全性評価

本項ではあわせ絵の確率的評価に基づく安全性について，4 桁数字によるパスワード認証と比較する．比較のため，あわせ絵における照合回数（$= \mathbf{N}$）は 4 回とし，照合時の提示画像枚数（$= \mathbf{P}$）は 9 枚とする．

4 桁数字によるパスワードの場合，その組合せ数は $10^4 = 10{,}000$ 個となるためその確率は $\frac{1}{10000}$ となる．あわせ絵の場合は，選択肢が照合時に提示された画像 9 枚と「パスワード画像なし」のあわせて 10 個となり数字入力における場合と同等である．また照合回数も 4 回としているのでその組合せ数は $10^4 = 10{,}000$ 個となる．しかし，あわせ絵は最低 1 つのパスワード画像を持つという制約があるため，4 回の照合作業すべてにおいて「パスワード画像なし」という選択肢は

除外される．したがって組合せ数は 1 つ減って 9,999 個となり，その確率は $\frac{1}{9999}$ となる．この結果から，上記の条件によるあわせ絵の認証は，4 桁数字の入力によるパスワード認証とほぼ同等の安全性を持つといえる．

またあわせ絵では確率的評価を高めることが可能なのは自明である．それは照合回数（**N**）ならびに照合時の画像提示枚数（**P**）を増やすことが可能だからである．

写真の利用と安全性

本項では画像認証における写真の利用とその安全性について 4 つの点において人工画像と比較検討する．

1 つめは画像の認識ならびに想起の容易さである．これは写真のほうが好ましいといえ，認識についてはこれを裏づける評価結果も得られている[1)]．

2 つめは書き留めやすさである．この点について我々は，以下の 2 つの理由から大きな差はないと考える．1 つは言葉だけで画像が特定できるとは限らないことである．これは画像の意味や外見に依存すると思われるからである．もう 1 つは絵として「描き留める」ということが考えられるからである．つまり絵として描き留めたり，印刷してしまう可能性を考慮すると，この脅威に対する安全性に大きな差があるとは考えにくいからである．

3 つめは第三者による推測しやすさである．これは人工画像の方が好ましいといえる．写真を利用した場合，ユーザは自分になんらかの関連がある画像をパスワード画像として選ぶからである．これはそのユーザを知る第三者にとってもパスワード画像を推測しやすい状況を作り出すことになる．この問題に対する対策法は次項で述べる．

種々の攻撃法とその対策

本項では画像認証に対して行われると考えられる 4 種の攻撃方法とあわせ絵における安全性について議論する．

1 つめの攻撃手法は Brute-force 攻撃である．前述のとおり，あわせ絵は既存のアカウント /パスワードによる認証とほぼ同等の確率的な安全性を持つ．またあわせ絵における認証作業は，電子メールによる認証要求の送付から始まり，その返信にある URL の Web ページにアクセスすることによって認証作業を始められる仕組みになっている．したがって繰り返し認証作業を行うのは困難である．したがって Brute-force 攻撃が行いにくい仕組みとなっている．

2 つめは Observation 攻撃である．この攻撃は認証作業をのぞき見し，パスワードとなっている画像を知る方法である．あわせ絵では画像をキー入力で直接選択可能にするとともに，画像選択時には候補画像群がまったく見えない画面構成にするという対策を行う．後者の対策方法には 2 つの実現法を考えている．1 つは 1 画面内に提示画像群表示領域とあわせ絵選択領域が存在するものの，それらの間に意図的な空白領域を作成し，機器の画面表示領域では双方の表示領域を同時に閲覧できないようにする方法である．もう 1 つは 2 つの表示領域を独立した画面として構成する方法である．これらはユーザが使用する端末機器に応じて使いわけるものとする．またプライバシーフィルタの利用といった物理的な対策も有効であると考えている．

3 つめは Educated Guess 攻撃である．これは特定ユーザに関する情報を持つ第三者がその情報を使ってパスワード画像を推測し，なりすましを成功させる攻撃である．あわせ絵におけるこの脅威への対策は画像登録により実現されている．画像登録によりユーザが登録した画像は時間とともに増加する．すると照合時にはユーザによって登録された画像が複数枚出現するようになる．このため既知の情報に基づきパスワード画像を推測したとしても，複数の画像がそれに該当し，1 つの画像に絞りこむことが困難になると考えられるからである．

さらに我々はもう 1 つの対策法として画像提示法を利用した手法を提案する．それは提示画像群にパスワード画像と意味的または内容的に類似した画像を意図的に提示する方法である．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．

最後は Intersection 攻撃である．この攻撃はこの方式の画像認証に特有のもので「パスワード画像が必ず提示される」という前提を悪用したものである．認証試行を繰り返し，提示された画像群の積集合を求めるとパスワード画像が特定できるという攻撃方法であり，極端な条件の場合，2 回の認証試行でパスワード画像が露呈する．

あわせ絵はこれに対する安全性を確保している．なぜならば照合時に「パスワードが含まれない」という事象を意図的に利用することで，この攻撃成立の前提条件が成立しないようにしているからである．またこれと類似した攻撃方法に出現頻度抽出によるパスワード画像の同定攻撃が考えられる．これに対し我々は「優先度付きおとり画像群の作成」という対策手法を提案する．この方法はパスワード画像の数倍程度の枚数のおとり画像を用意し，それらを優先的におとり画像として照合時に提示する．それにより，それらの出現頻度を意図的にパスワード画像と同程度にすることで，

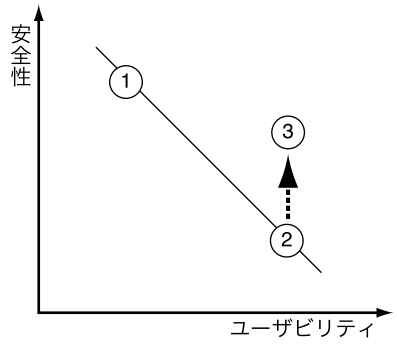


図 8 安全性とユーザビリティ
Fig. 8 The relation between safety and usability.

そのような攻撃によるパスワード画像の特定を困難にする．

安全性とユーザビリティ

一般にセキュリティと利便性，つまりユーザビリティは相反するものであると認識されており，認証に関する人為的問題の原因もそこにある．

既存のセキュリティシステムは**図 8** の ① または ② の状態であるといわれてきた．① の状態は安全であるが利便性の低い状態であり，② は利便性は高いが安全性は低いという状態である．この両者はけっして両立せず，反比例グラフとして表されていた．しかしあわせ絵ではユーザの負担軽減に主眼を置き，既存のセキュリティシステムにユーザインタフェースを提供することで，③ の状態のように利便性を損なうことなく安全性を高めることを可能にした．

このように安全性を損なうことなく，人的問題点に注目してユーザがより安全にセキュリティシステムを使用可能にするようなインタフェースを提供することは重要である．なぜならば，これによってユーザの権利をユーザ自身で管理/制御可能にするからである．つまり一部のシステム管理者やシステムの仕組みによってその安全性を保証して “もらう” のではなく，各ユーザにもその安全性を維持し監査できるようにする仕組みを提供することが重要なのである．あわせ絵は認証システムという分野においてこの概念[4]を導入したシステムとして有用であるといえる．

4.3 動作環境の必要要件

本システムを運用するために必要な動作環境は，既存の認証システムと比較してかなり高い要件になる．ここではファイルシステムサイズ，データ転送量，認証サーバへの負荷について考察する．

まずファイルシステムサイズについて述べる．あわせ絵では認証時に必要な画像を保持するために大容量のファイルシステムが必要となる．現在のプロトタイプに基づき試算をする．画像 1 枚のファイルサイズが平均 5 Kbyte になるため，ユーザ数を 100 万人とし，各ユーザが 30 枚の画像を登録可能にした場合，150 Gbyte もの容量を持つファイルシステムが必要となる．

次に 1 回の認証行為で必要となるデータ転送量について試算する．既存のアカウント/パスワード方式では多く見積もっても 1 Kbyte には及ばないと考えられる．これに対しあわせ絵では認証方法を以下のような条件で試算する．1) 携帯電話を通じて認証を行う．つまり画像は認証サーバで縮小される．したがって，画像 1 枚あたりのファイルサイズは 5 Kbyte から 1 Kbyte に削減される．2) 4 回の照合作業をもって 1 回の認証とする．つまり 9 枚の画像と認証用 Web ページ本体を最低 4 回ダウンロードすることになる．この認証用 Web ページのファイルサイズは，プロトタイプの実装で 1 Kbyte である．したがって照合作業 1 回あたりのダウンロードデータ量は画像 9 枚と認証用 Web ページで合計 10 Kbyte となる．これを最低でも 4 回ダウンロードすることになるので，1 回の認証で必要なデータ転送量は最低で 40 Kbyte となり，既存のアカウント/パスワード方式の 40 倍以上となる．

最後に認証サーバへの処理負荷の増大であるが，あわせ絵の処理はユーザからの要求に応じて動的に Web ページを作成するだけであるため，現時点では目立った処理負荷の増大は認められない．ただし処理負荷については，多数のユーザが利用する環境を構築し運用評価を行うことが必要であり，今後の課題である．

これらの要件は実装によって大きく変動する可能性がある．また実装以外にもハードウェアの利用やシステム構築時の工夫によりその改善や特定の問題の回避が可能になる可能性もある．よって実環境における評価の必要性とともに，実運用に向けたシステム要件の策定は今後の課題である．

4.4 関 連 研 究

関連研究について述べる．Deja Vu [1]は，正誤候補が提示された中から正候補を選択するという画像認証を提案した論文として著名である．この論文とあわせ絵の差異についてはこれまで述べてきたとおりであるが，あわせ絵は Deja Vu に存在する問題点に着目し，その改善法を提案するとともに安全性とユーザビリティの両立を実現したという点で大きく異なる．Angeli らの論文[3]では Deja Vu の枠組みに対して写真を適用し，ATM のインタフェースを想定して評価実験を行っている．しかし Deja Vu の問題点については注目していない．勝田らの論文[7]では，Deja Vu [1]の枠組みを

Web 上に実現するとともに，携帯端末での利用とシングルサインオンを考慮に入れた実装を行っているが，Deja Vu に存在する問題点には注目していない．國米の論文[6]も 2 次元バーコードを利用し，その応用例について述べているものの，それは Deja Vu の枠組みと同じである．また Deja Vu の問題点には注目していない．鹿島の論文[8]は，安全性強化には組合せが重要であることに注目し，パスワードの安全性を強化するために画像を導入し，その特定位置をパスワードの一部として利用したシステムである．したがって我々の意味する画像認証とは異なり，画像を利用した認証方式の安全性強化法であるといえる．よって一概に比較ができないが，この手法も安全性は向上するものの，人的問題の改善は図られておらず，安全性とユーザビリティの両立にはなっていないといえる．

次に本論文で提案した改善方法と関連する研究についてふれ，その差異について述べる．

「画像登録」について述べる．鹿島の論文[8]や商用製品[9]でも “ユーザの好みの画像をパスワード画像として設定できる” とあり，同等の機能を持つ既存のシステムは存在する．しかし，それらとあわせ絵の画像登録は異なる．それはあわせ絵の画像登録はインタフェースとして実装されていることであり，ユーザによる画像登録を簡単に実行可能にしていることと，画像登録機能により登録した画像が必ずパスワード画像になるものでないという点で異なる．画像登録が簡単に行えることは正候補選択方式による画像認証における安全性の向上のために重要である．画像を登録するという行為は，おとり画像数の増加やパスワード画像の更新，画像認証におけるさらなる安全対策の実現のための基礎となっているからである．

また他のシステムでは，“可能” という記述だけでその詳細な記述がないため推測ではあるが，インタフェースとしては実現されていないと推測される．よって画像登録には付加的な作業が必要となり，あわせ絵における画像登録ほど簡単には実行できないと考える．また既存のシステムでは，画像登録とパスワード画像更新は同一視されている．したがって画像登録の際には認証が必要になるとともに，それがパスワード画像になることからユーザに「登録する画像を忘れてはいけない」という観念をいだかせることになる．これらは結果としてユーザに画像登録を躊躇させるという悪循環を生むことになる．これは既存のパスワード認証において「ユーザがパスワードを更新しない」という人的問題を画像認証に内在させることになる．これに対しあわせ絵の画像登録は，単に画像を認証システムに登録するだけであり，それに対してユーザに何らかの負担を強いることはない．これらのことから，あわせ絵の画像登録は既存システムの “好みの画像を使用可能” とは大きく一線を画すものであるといえる．

次は「利用通知」である．これも既存の発明[10]で提案されている不正行為の通知方法と同等であると考えられる．この発明における不正行為の通知方法とは次のとおりである．ユーザがネットワークを通じて商品購入要求を行うと，安全な通信路を使ってユーザの端末にワンタイムパスワードを送付してくるというものである．つまり本人でない第三者がなりすまして商品購入要求を行うと，商品購入要求をしていない正規ユーザにワンタイムパスワードが送付されてくることからそれは正規ユーザの知るところとなる．というものである．しかし，あわせ絵の利用通知は以下の 2 点で上記の方法とは異なる．

1 つは所有物に依存しないということである．上記の方法では通知先がユーザの特定端末に限定されている．したがってその端末が盗難，紛失，破損した場合は不正行為の発生を知ることができなくなる．これに対しあわせ絵では同様の処理を実現している能動的通知のほかに受動的通知も行っており，所有物（もしくは通知先）には依存していない．したがって前述のような不測の事態になったとしても利用通知は利用可能である．また利用通知は，本来の認証行為とは独立して機能するため，仮に何らかの不都合により正規ユーザとして認証できなくなったとしても利用通知は利用可能であり，その逆もまた真である．

2 つめは広範な情報提供である．上記の発明では不正行為の “発生” のみを通知するが，あわせ絵の利用通知はより広範な情報を通知する．これは不正侵入検知の分野でいわれている対策手法[4]のように，検知するだけでは対策として不十分であり，その後の調査や事後対処が重要だという立場に基づいている．あわせ絵では，認証行為の発生だけでなくその結果も通知する．これにより第三者によるなりすまし行為が発生し，その結果，認証に成功したか否かまで知ることができるようになる．これによりユーザは，即座に適切な対処を行うべきか，今は用心にとどめ，近いうちにパスワード画像を変更すべきといった事後対処の判断までが可能になる．また認証行為に基づく事象だけでなく，画像登録や照合情報通知といった事象も通知対象にしており，なりすましの準備行為や第三者が自分の認証履歴を閲覧していることも知ることが可能になっている．

このようにあわせ絵における利用通知は単なる不正

行為発生の通知だけではなく，不正行為に対する対策を行うために必要な情報を提供する機能として認証システムに必要な枠組みである点で既存の通知手法とは異なるといえる．

4.5 今後の課題

本節ではあわせ絵における今後の課題について述べる．

まずはじめに評価可能なシステム構築を行うとともに運用評価を行い，本論文で提案した理論が実際に成立することを定量的に評価する必要がある．その評価項目には認証システムの安全性のみならず，システム構成の必要要件やユーザビリティについても行う必要がある．

システム構成の必要要件とは，あわせ絵の運用を安定して行うために必要なシステム要件のことである．あわせ絵は既存の認証システムと比較しその要件が高くなることが見込まれるため，その見極めは必要であると考えている．

ユーザビリティは操作性，認証に必要な時間など使いやすさの面とパスワードとしての画像の覚えやすさ，想起の容易さといった人的要因についても評価する必要がある．特にあわせ絵によって導入された機能により新たに発生すると想定される問題の洗い出しとその評価を行うことは重要であると考えている．その一例としては，画像登録が容易になることで照合作業時にパスワード画像の判定に混乱を生じさせる恐れがあるということがあげられる．つまりユーザが頻繁に画像を登録し，パスワード画像を変更することで，照合時にはこれまで利用していた過去のパスワード画像が想起されてしまい，現在のパスワード画像が正確に判断できなくなる恐れがあるという問題である．

次は認証による権限の許諾を停止する手段の提供である．つまりユーザからの要求により，そのユーザの権限を完全に凍結する機能である．これは利用通知によってなんらかの不正行為や悪用が発覚したときの対策として必要であると考える．しかしこの機能そのものを第三者によって悪用される恐れもあるため，この機能の実行のために別の認証が必要になるという問題がある．つまり，認証システムの 1 機能のために，それとは別の認証が必要となるということである．したがって，その必要性の検討も含めて引き続き考察を行う必要があると考えている．

5. おわりに

本研究では，正候補選択方式による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する方法を提案した．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新たな画像認証システム「あわせ絵」を構築した．

本研究では画像認証に画像登録と利用通知の 2 機能を導入することにより，実世界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，認証システムの利用状況を各ユーザが自身で確認可能にした．さらに認証時における画像提示法に「パスワード画像が含まれていない」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．

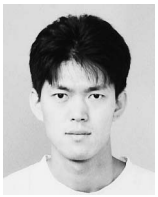
今後の課題は，第三者によるパスワード画像の推測をより困難にするような照合画像群の提示法についてさらなる考察をすすめるとともに，実運用による定量的評価を行うことである．

参 考 文 献

1) Dhamija, R. and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, *9th Usenix Security Symposium*, pp.45–58 (Aug. 2000).
2) Perrig, A. and Song, D.: Hash Visualization: a New Technique to improve Real-World Security, *International Workshop on Cryptographic Techniques and E-Commerce* (*CrypTEC*) (1999).
3) Angeli, A.D., Coutts, M., Coventry, L. and Johnson, G.I.: VIP: a visual approach to user authentication, *Proc. Working Conference on Advanced Visual Interface* (*AVI2002*), pp.316–323 (May 2002).
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) 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*, Vol.16, No.7, pp.185–189,（株）アスキー (2001).
6) 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).
7) 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 (2002).
8) 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（ゲートシーン），コンピュータセキュリティ研究報告，No.10, 情報処理学会 (July 2000).

9) モバイル端末の盗用/データ漏洩防止ソフト「ニーモニックガード」，有限会社ニーモニックセキュリティ(2001). http://www.mneme.co.jp/
10) 塩田岳彦，田中琢也：情報サービス提供方法，公開特許公報（特開 2002-32692），特許庁 (2002).
11) 田口浩平，小池英樹：位置情報を利用した本人認証，マルチメディア，分散，協調とモバイルシンポジウム（DICOMO2001），pp.458–465, 情報処理学会 (June 2001).
12) ZDNet News JAPAN：史上最悪のセキュリティホールはユーザのパスワード http://www.zdnet.co.jp/news/0205/28/ne00_password.html (May 28, 2002).

(平成 14 年 12 月 2 日受付)
(平成 15 年 6 月 3 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．現在に至る．情報視覚化の研究に従事．情報視覚化，情報セキュリティに関心を持つ．IEEE/CS，ACM 各会員．

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．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．