利便性と安全性を兼ね備えた画像認証方式の実現

静岡大学　博士論文

利便性と安全性を兼ね備えた画像認証方式の実現

2010年6月

大学院 自然科学系教育部

情報科学専攻

山本　匠

論文要旨

インターネットの爆発的な普及に伴い，ネットワークおよびコンピュータシステムが社会に深く浸透し，組織内において情報システムを活用して業務やサービスを管理・遂行することが当然のこととなってきている．しかし一方で，マルウェアの蔓延や個人情報漏洩などのセキュリティインシデントが激増しており，被害に遭った場合の損失や社会的影響も甚大になってきている．このような背景から，組織内の機密データに対する不正アクセスや，それに伴うデータ破壊や情報流出などを防止するために，システム利用者の権限に応じたアクセス制御を徹底する必要があり，そのための個人認証の確実な実施が重要となっている．

現在最も普及している個人認証は，汎用性と利便性の高さからパスワードが主流となっているが，人間にとって長くランダムな文字列を記憶することは容易ではない．そのため，人間の画像認識能力の高さを利用して記憶負荷を軽減させる再認型の画像認証方式が注目されている．しかし，画像認証においては，毎回の認証時にパス画像がディスプレイ上に表示されるため，認証時の覗き見攻撃に対して脆弱となる．この問題に対し，現在までに，画像認証をワンタイム化する方法と攻撃者の画像認識を妨害する方法が提案されている．前者の方式では，画像認証の Challenge&Response 化（以降，C&R と略記する）が試みられている．しかし，チャレンジとレスポンスの両者を観測することができる攻撃者に対して安全性を担保するには複雑な計算によってチャレンジからレスポンスを生成する必要があり，ユーザに高い作業負荷を与えてしまう．一方，後者の方式は，覗き見をする攻撃者にとってパス画像の記憶が困難となるように，不鮮明化画像（モザイク化等の不鮮明化処理を施した一見無意味な画像）をパス画像として使用する認知心理学的なアプローチである．人間は画像の記憶に優れているという特性を有するものの，それは有意味な画像を記憶する場合に限ってのことであり，無意味に見える画像を記憶することはやはり難しい．ゆえに，他人のパス画像（不鮮明化画像）を覗き見て記憶することは，攻撃者にとって困難な作業となる．しかし，たとえ不鮮明な画像であっても認識すること自体は不可能ではないため，カメラで盗撮しておいた不鮮明化画像と同じものを選ぶという攻撃には脆弱性が残る．最近は ATM への盗撮カメラ設置の事件も発生していることから，カメラ撮影を用いた覗き見にも一定レベルの耐性を有することが望まれる．

さらに，従来の画像認証においては，パス画像を隠すために利用される囮画像（認証画面にパス画像と共に表示される複数の画像）を適切に更新していくことも重要な課題の 1 つと言われている．正規ユーザにとって馴染みの無い新しい囮画像を適切に用意することができなければ，画像認証の安全性や正規ユーザの利便性の低下につながってしまう．

以上をまとめると，画像認証には，「覗き見の問題」と「囮画像の問題」の 2 つの本質的な課題が残されており，現在までのところ正規ユーザの負荷を抑えたまま両課題を克服した研究は確認されていない．そこで本研究では，画像の記憶・再認の優位性は残したまま，両課題を同時に解決する新しい画像認証の実現を目指す．その際，人間の計算能力の限界に鑑みるに，計算量的な安全性を礎とする暗号学的なアプローチによって画像認証を改良することは基本的に困難であると考えられる．このため本研究では，認知心理学的な観点からのアプローチ，すなわち，不鮮明化画像の特長に着目して研究を進めていく．

本研究で行った具体的な3つの取り組みを以下に示す．

1．覗き見攻撃への取り組み

a) 言語手がかり付き再認方式（RVC方式）

正規ユーザにm枚のパス画像を記憶させた上で，1回の本人認証にあたってn枚（m＞n）のパス画像を用いて認証を行うという対策によって，再認型画像認証を拡張する（以降，m-n対策と呼ぶ）．この結果，カメラを用いた覗き見であっても，攻撃者がパス画像を特定するためには複数回の覗き見が必要となる．ただし，パス画像の増加にともなうユーザの負荷増大を緩和する工夫なくしては，その導入は難しい．そこで，正規ユーザのみが効果的に利用可能な手がかりを認証時に与えることで，ユーザの負荷を軽減する．

b) 暗示・応答型画像認証方式（Q&R方式）

再認型画像認証のC&R化を試みる．ただし，人間の計算能力には限界があるため，チャレンジからのレスポンス生成に暗号計算が必要となる通常のC&R型認証を適用することは不可能である．そこで，チャレンジの意味を隠すというアプローチを採ることによって，簡素なレスポンス生成処理を採用した場合であっても，あるレベルの安全性が担保される暗示・応答（Q&R）型画像認証を実現する．カメラを用いた覗き見であっても，攻撃者はチャレンジの意味が分からず，パス画像の特定が困難となる．

2．囮画像の潤沢な用意への取り組み

a) 囮画像の自動生成（ADG方式）

囮画像の自動生成を検討する．あらかじめ大量の囮画像を端末に保存しておいたり，ネットワークを介して囮画像をその都度ダウンロードしたりするのではなく，シーズとなるわずかな情報から，正規ユーザにとって馴染みの無い囮画像を数多く出力する方式を実現する．

各方式のプロトタイプシステムを実装し，10名の被験者の協力のもと実験を行い提案方式の評価を行った結果，RVC方式およびQ&R方式においては，正規ユーザの負荷増大を極力抑えつつ，カメラ撮影を含むより強力な覗き見にもある程度の耐性を持たせることが確認できた．ADG方式においては，ある程度の実用性レベルで，囮画像とパス画像の識別が攻撃者には困難で正規ユーザには容易な，囮画像の自動生成法を実現することに成功した．実験結果を踏まえ，利便性および安全性の観点から本研究と関連する既存研究との比較検討を行い，本研究の優位性を検証している．また，3方式（RVC方式，Q&R方式，ADG方式）を同時に導入した場合におけるメリット・デメリットを整理・確認し，今後の課題および展望を示した．

目次

1章　序論

インターネットの爆発的な普及に伴い，ネットワークおよびコンピュータシステムが社会に深く浸透し，組織内において情報システムを活用して業務やサービスを管理・遂行することが当然のこととなってきている．法律の面では，不正アクセス禁止法[MET1]や電子署名法[MET2]，個人情報保護法[CAO]などの整備も進みつつあり，いよいよ情報システムはビジネスや生活に必要不可欠なインフラとなった．しかし一方で，コンピュータウィルスの蔓延や，Web ページの改ざんやサービス妨害（DoS）攻撃，個人情報漏洩などのセキュリティインシデントが激増しており[CER][NPO]，被害に遭った場合の損失や社会的影響も甚大になってきている[CSI]．このような背景から，組織内のシステム上に存在するデータの安全性を維持することの重要性は増大の一途をたどっている．組織内の機密データに対する不正アクセスや，それに伴うデータ破壊や情報流出などを防止するためには，システム利用者の権限に応じたアクセス制御を徹底する必要があり，そのためにも個人認証を確実に実施することが肝要である．

現在，最も普及している個人認証方式は，パスワードや暗証番号のような文字や記号を用いた古典的な認証方式である．コンピュータ登場のはるか以前より「合言葉」という形で行われてきた認証形態が，1960 年代にタイムシェアリングシステムが登場して1台のコンピュータを複数のユーザにより共用するという運用が導入された時点でパスワードとして利用されるようになり，現在に至るまで使用され続けている．最近では組織の建物や業務スペースへの出入りや，機密度の高い計算機へのアクセスなどに，指紋や虹彩などを利用する生体（バイオメトリクス）認証[Set02]や，IC カード[MOI00]，認証トークン[SW][SID]，乱数表[TMD]などの個人の所有物を利用した認証方式も採用されはじめている．しかしながら，個々の情報端末におけるログイン認証や，銀行 ATM の認証，Web ページ上のサービスの認証などでは，特別なハードウェアを必要としないパスワードや暗証番号のような文字や記号の記憶を利用する認証方式が依然として主流である．

このように実装の容易さと高い汎用性を有するパスワード認証であるが，認証方式として完全であるというわけではなく，むしろ大きな欠点を伴っていることが多くの研究により指摘されている．2 章で詳しく記述するが，その主要な原因は，できるだけ長くランダムな文字や数字の組み合わせを設定するほどパスワードの安全性が増すのに対し，本来，人間は長い文字列や記号列を正確に記憶することが得意ではないことにある．すなわち，攻撃者による推測が困難で安全なパスワードであるほど，ユーザにとっては記憶しにくいというトレードオフが存在する．そのため，ユーザは長くランダムなパスワードを設定することや，定期的に新たなパスワードを覚えなおすことに対する記憶負荷の大きさに苦痛を感じている．実際，平易なパスワードを設定してしまっているユーザは少なくなく，また，複雑なパスワードを設定していたとしても，多くのユーザがそれを紙に書き留めておいたり，様々な環境で同一のパスワードを使いまわしたりする傾向

があることが知られている[FH07]．そのようなパスワードは，辞書攻撃やソーシャルエンジニアリング[1]などに対して脆弱であり，システムのセキュリティレベルを低下させる原因となっている．

この問題の解決に向け，文字や記号の代わりに画像を用いて認証を行う方式が多数提案され，注目されている．人間の画像の記憶に関する能力は，文字や記号等の言語的記憶に比べて優れていることが認知心理学における長年の研究から知られている[She67][PRS68] [Nic68][NRW76][Par97]．また，再生型の想起に比べて，再認に関する人間の能力は顕著である[Nie93]．このため，認証時にディスプレイ上に複数枚の画像が提示され，ユーザがその中に含まれている自身のパス画像を正しく選出することによって認証を行う再認型の画像認証方式が特に有望視されている．

しかし，再認型画像認証においては，毎回の認証時にパス画像がディスプレイ上に表示されるため，認証時の覗き見攻撃に対して脆弱となる．正規ユーザの認証操作を数回（最悪の場合 1 回）覗き見られるだけで，攻撃者に認証情報（パス画像）が特定されてしまう恐れがある．この問題の対策として，現在までに，画像認証をワンタイム化する方法[SB02][WWS06][JN06][Ta08][HNE08][KYN07][KYN08][YKN09]と攻撃者の画像認識を妨害する方法[HIM05][HCD07]が提案されている．

画像認証をワンタイム化する方法においては，ネットワーク認証プロトコルで利用されている Challenge & Response 型認証方式[2]（以降，C&R と略記する）に倣い，画像認証を C&R 型に改良するための研究が行われている．しかし，人間は複雑な計算は不得手であるため，パスワードと乱数（チャレンジ）をハッシュ化[3]してレスポンスを返すことは不可能である．Sobrado らの方式[SB02][WWS06]は，pass-object を頂点とした凸包内部を選択させることで，比較的良好な C&R 型画像認証方式を実現している例といえるが，非常に多数のアイコンの中から pass-object を探し出す必要があり，ユーザにとってチャレンジに対するレスポンスを生成することは容易なことではない．Roth らの方式[RPF04]は，認証情報に付与されているグループ情報を回答させるというアイデアによって，レスポンスの生成に対するユーザの負荷を軽減させることに成功しているが，その代わりに，認証情報の入力回数が激増してしまう．

---

[1] ソーシャルエンジニアリングとは，「平凡な善人のふりをして他人に接近し，その人を騙すテクニック」のことである．「社会の仕組みや人間関係を操り，悪用する」ことで，重要な情報（パスワードやそのヒントとなる情報）を盗み出すことができる[MS03]．例えば，ゴミ箱の中に捨てられているメモを集めたり，コンピュータ管理者になりすましてユーザからパスワードや関連する情報を聞き出したりすることで．パスワードが盗まれる．

[2] ユーザはサーバに認証要求をする．サーバはランダムな文字列 C をユーザに送る．ユーザは受け取ったランダムな文字列 C を，サーバとユーザとで共有する秘密の情報 K に依存する逆計算困難な関数 $F_K(\cdot)$を使って変換し，その結果 $R=F_K(C)$をサーバに返す．サーバも自ら $F_K(C)$を計算し受け取った R と照らし合わせる．$F_K(C)=R$ であれば認証成功．そうでなければ認証失敗となる．暗号プロトコルでは通常 $F(\cdot)$はハッシュ関数である．

[3] あるデータを一定の大きさのデータ（ハッシュ値）に変換する関数のことである．一方向性と衝突困難性を有する．

一方，攻撃者の画像認識を妨害する方法は，覗き見をする攻撃者にとってパス画像の記憶が困難となるように，モザイク化等の不鮮明化処理を施した一見無意味な画像をパス画像として使用するというアイデアに基づいている[HIM05][HCD07]．正規ユーザにのみ不鮮明化画像に対するオリジナル画像を見せ，スキーマ（オリジナル画像と不鮮明化画像の間の認知構造的なリンク）[Bre99]を学習させることにより，正規ユーザは不鮮明化画像を有意味な画像として認識できるようになり，パス画像（不鮮明化画像）を容易に記憶することができる．人間は画像の記憶に優れているという特性を有するものの，それは有意味な画像を記憶する場合に限ってのことであり，無意味に見える（意味を言語化できない）画像を記憶することはやはり難しい[Mat83][OT01]．ゆえに，他人のパス画像（不鮮明化画像）を覗き見て記憶することは，攻撃者にとって困難な作業となる．しかし，スキーマを獲得していなくても，不鮮明化画像を認識すること自体は不可能ではない．よって，カメラで盗撮しておいた不鮮明化画像と同じものを選ぶという攻撃には脆弱性が残る．最近は ATM への盗撮カメラ設置の事件も発生している[ITN05]ことから，カメラ撮影を用いた覗き見にも一定レベルの耐性を有することが望まれる．

以上のように，従来の覗き見攻撃を考慮した画像認証方式は，その安全性と利便性の面で課題を残している．

加えて，パス画像を隠すために利用される囮画像（認証画面にパス画像と共に表示される複数の画像）を適切に用意することも，画像認証における重要な課題の 1 つと言われている．例えば，毎回の認証で常に同じ囮画像のセットを利用してしまうと，攻撃者が認証画面中の画像一枚一枚に当たりをつけ，「その画像を選択して認証に失敗したならば，その画像はパス画像ではない」というように，パス画像の候補が徐々に絞られていく問題（Exhaustive 攻撃と呼ばれる）がある．

また，複数の画像の中から自分が記憶したパス画像を選択する再認型の画像認証方式においては，過去にパス画像もしくは囮画像として用いた画像を囮画像にしたり，自分が撮影した写真のように自分にとって馴染みの深い画像を囮画像としたりすると，結果的に正規ユーザは認証画面中のすべての画像に対して再認を起こすことになり，パス画像の認識に混乱をきたす可能性があると言われている[DP02]．そのため，囮画像にはなるべく正規ユーザが再認を起こさない，つまり，正規ユーザが見たことのない画像を使うことが望ましい．

これらの問題を解決するために，毎回の認証ですべての囮画像を一新する，つまり，一度囮画像として利用した画像は以降の認証では囮画像として利用しないという方法が考えられる．しかしこの場合は，今度は，認証の度に必ず表示される画像がパス画像であるということが推測されてしまう（Intersection 攻撃と呼ばれる）ことになる．

以上より，ある一定枚数の囮画像は前回の認証から引き継ぎ，残りの囮画像は正規ユーザが見たことの無い全く新しい画像を用いるという折衷案が適切と考えられるが，残念ながらこの方法にも依然として，どのようにして新しい囮画像を追加すればよいのかという問題が残る．あらかじめ大量の囮画像を端末に保存しておいたり，ネットワーク

を介して自動的にダウンロードするなどの方法も考えられるが，実装や運用の観点からはストレージや通信量に関してはその使用を可能な限り抑えたいというニーズがある．

このように，従来の画像認証の研究のほとんどにおいて，正規ユーザにとって馴染みの無い囮画像の潤沢な用意について，未解決のまま残されていた．

以上をまとめると，画像認証には，以下の 2 つの本質的な課題が存在する．

イ) 覗き見の問題

覗き見攻撃に対して脆弱である．

ロ) 囮画像の問題

囮画像の用意およびその更新が難しい．

本研究では，以下の取り組みによって，画像の記憶・再認の優位性は残したまま，上記の 2 つの課題を同時に解決することのできる新しい画像認証方式の実現を目指す．

1. 覗き見攻撃への取り組み

a) 正規ユーザに m 枚のパス画像を記憶させた上で，1 回の本人認証にあたって n 枚（m＞n）のパス画像を用いて認証を行うという対策によって，再認型画像認証を拡張する（以降，m-n 対策と呼ぶ）．この結果，カメラを用いた覗き見であっても，攻撃者がパス画像を特定するためには複数回の覗き見が必要となる．ただし，パス画像の増加にともなうユーザの負荷増大を緩和する工夫なくしては，その導入は難しい．そこで，正規ユーザのみが効果的に利用可能な手がかりを認証時に与えることで，正規ユーザの負荷が少ない m-n 対策を実現する．

b) 再認型画像認証の C&R 化を試みる．ただし，人間の計算能力には限界があるため，チャレンジからのレスポンス生成に暗号計算が必要となる通常の C&R 型認証を適用することは不可能である．そこで，チャレンジの意味を隠す（正規ユーザ本人にしかチャレンジを理解することができないようにする）というアプローチを採ることによって，簡素なレスポンス生成処理を採用した場合であっても，あるレベルの安全性が担保される暗示・応答（Q&R）型画像認証を実現する．カメラを用いた覗き見であっても，攻撃者は（チャレンジおよびレスポンスを覗き見ることはできるが）チャレンジの意味が分からず，パス画像の特定が困難となる．

2. 囮画像の潤沢な用意への取り組み

a) 囮画像の自動生成を検討する．あらかじめ大量の囮画像を端末に保存しておいたり，ネットワークを介して囮画像をその都度ダウンロードしたりするのでは

なく，シーズとなるわずかな情報から，正規ユーザにとって馴染みの無い画像を数多く出力する方式を実現する．

人間の計算能力の限界に鑑みるに，計算量的な安全性を礎とする暗号学的なアプローチによって画像認証方式を改良することは基本的に困難であると考えられる．そこで本研究では，上記の 3 つの解決方針を実現するにあたって，認知心理学的な観点からのアプローチ，すなわち，不鮮明化画像[HIM05]の特長に着目して研究を進めていく．なお，本論文では，これら 3 つの方法をそれぞれ独立した観点から議論していくが，本研究の最終目標は，それぞれを併用することによって，安全性と利便性を両立した画像認証方式を実現することにある．そこで，本論文の最後で，現時点でそれぞれの方式を同時に導入した場合の状況について触れ，今後の研究の方向性と課題を確認する．

以降の本論文の構成は次のとおりである．

2 章において，本研究の関連研究として，パスワード認証および画像認証をさまざまに拡張することで，その安全性の向上や記憶負荷の軽減を図った既存研究を多数取り上げ，それぞれの特徴および課題についてまとめる．その上で，関連研究に対する本研究の位置付けを明確に示す．

3 章では，本研究において重要な役割を持つ不鮮明化画像を用いた「画像記憶のスキーマを利用した認証方式[HIM05]」を説明する．当該研究の基本アイデアは，人間の認知の特性である画像記憶に関する「スキーマ」[Bre99]をうまく利用することで，正規ユーザには記憶しやすいが，それ以外の他者には記憶が困難となるようなパス画像を認証に利用することにある．これを実現するために，有意味なオリジナル画像に対して不鮮明化処理を施すことによって作成された，一見すると無意味に見える「不鮮明化画像」をパス画像として利用する．

4 章では，画像認証における(イ)の課題（覗き見の問題）に焦点を当て，不鮮明化画像を用いた認証方式に対して m-n 対策の導入を試みる．m-n 対策は正規ユーザが記憶すべきパス画像の枚数（m 枚）を増加させることになるが，「パス画像を思い出すにあたっての手がかりとなる情報を認証時にヒントとして提示する（言語手がかり付き再認方式）」ことによって，その記憶負荷の低減を図る．ここで，「スキーマを持たないユーザは，オリジナル画像に関する言語手がかりを与えられたとしても，不鮮明化画像の意味を類推することが困難である」という不鮮明化画像の特長が巧みに利用されている．実験により，提案方式の利便性（正規ユーザの記憶負荷）や安全性（認証率およびなりすまし成功率）について評価を行う．

5 章では，画像認証の(イ)の課題（覗き見の問題）へのもう 1 つの取り組みとして，画像認証の C&R 化を試みる．ただし，人間の計算能力の限界に鑑みるに，チャレンジからのレスポンス生成に暗号計算が必要となる通常の C&R 型認証を適用することは不可能である．そこで，「スキーマを持たないユーザは，不鮮明化画像の意味を類推するこ

とが困難である」という特長を有する不鮮明化画像をチャレンジとして利用し，簡素なレスポンス生成処理を採用した場合であっても，不正者にはパス画像が容易には推測できない方式を提案する．正規ユーザ本人のみに隠れたチャレンジを伝えるというアプローチによって認知心理学的に C&R 型認証の安全性を担保する本方式を「暗示・応答（Q&R）型画像認証方式」と名付ける．実験により，提案方式の利便性（正規ユーザの記憶負荷）や安全性（認証率およびなりすまし成功率）について評価を行う．

6 章では，画像認証の(ロ)の課題（囮画像の問題）に焦点を当て，囮画像の自動生成を試みる．ここで，「簡素な画像処理によって，オリジナル画像と不鮮明化画像の間のスキーマを切断することが可能である」という不鮮明化画像の特長を活用し，正規ユーザにとって馴染みの無い囮画像を自動的に大量に生成する方法を提案する．実験により，生成された囮画像が利便性（囮画像が正規ユーザのパス画像の記憶・想起を阻害することはないか）および安全性（不正者がどの程度囮画像を識別可能か）の面でどのような影響を与えるのかについて評価する．

7 章では，4~6 章における方式や実験結果を踏まえ，それぞれの方式を同時に導入した場合の総合的な考察を行う．また，覗き見攻撃以外にも想定される各種攻撃方法，および，囮画像の用意以外のその他の諸問題に関して考察を加える．そして，関連の深い既存研究との比較を行い，本方式の特徴と利点を明確にする．

最後に，8 章において本論文の成果と今後の課題についてまとめる．

2章　従来研究

個人認証方式は，1) 個人の所有物に基づく方式，2) 個人の生体的な特徴に基づく方式，3) 個人の記憶に基づく方式，に大別される．パスワード認証方式や，本研究が取り上げる画像認証方式は，個人の記憶に基づいた方式である．本章では，まず，それぞれの認証方式の区分における，長所と短所を簡潔にまとめる．その後，パスワード認証方式や画像認証方式など，本研究の関連研究について，各方式の特徴や問題点について整理し，本研究との差異について述べる．

2.1　各種認証方式

2.1.1　個人の所有物に基づく方式

ユーザが所有する認証用デバイス（古くは自宅の鍵から，磁気カード，乱数表[TMD]，認証トークン[SW][SID]（図 2-1），IC カード[MOI00]など）に含まれる認証情報を，専用の読み取り装置などを通して認証システムへ入力することにより，個人認証が行われる方式である．

図 2-1　RSA セキュア ID　ハードウェアトークン

出典：　http://www.rsa.com/japan/products/securid/SID_DS_0911-J.pdf

一般的な長所は次の事項が挙げられる．

- 認証情報を記憶する必要がなく，記憶負荷が無い
- 認証情報を他者に推測される危険性が少ない
- 乱数生成器や計算能力を搭載した認証トークンや IC カードを用いる場合には，ワンタイムパスワードを生成できる

一方，短所は次のようになる．

- 特別なハードウェアデバイスを所持しておく必要がある
- 認証用デバイスを紛失・破損する可能性がある
- 認証用デバイスの盗難，複製，情報読み取り（スキミング）によって認証情報が漏洩する可能性がある

認証用デバイス自体は比較的安価である場合が多い．最も大きな利点はユーザの記憶負荷が無いことであるが，盗難などによるなりすましの脅威や，常に認証用デバイスを所持しておく必要があるという利便性の低さが大きな課題である．また，携帯電話やスマートフォンなどにおいては，アクティベーションのために特殊なデバイスを別途所持することは理にかなっておらず，携帯端末用の認証としては応用しづらい．

2.1.2 個人の生体的特徴に基づく方式

ユーザ個人の身体に関する生体情報を特別な読み取り機器で測定することで，あらかじめ認証システムに登録してある生体情報と照合し，個人認証を行う方式である[Set02]．利用される生体情報には，指紋[JHB97]，虹彩[Dau04]，顔[Kan01][Neo]，静脈[FUJ][HIT]，DNA[IT01]などの静的な情報や，声紋[Shi84]，筆跡（署名）[Nal99]，なぞり書き[NUY09]，キーストローク[MRW99]，生体反射[NA06][NO07][AYT09]などの動的な情報がある．

図 2-2　指静脈システム

出典：　http://www.hitachi-media-el.co.jp/products/fvu.html

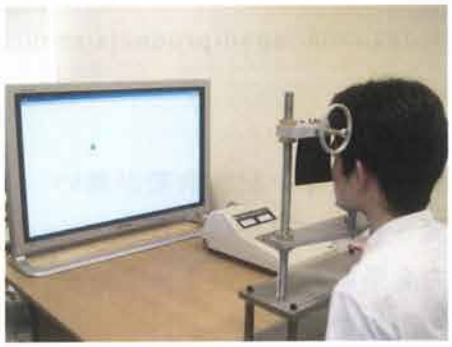


図 2-3　生体反射型認証[NA06]

一般的な長所としては，次の事項が挙げられる．

- 認証情報を記憶する必要がなく，記憶負荷が無い
- 特別なハードウェアデバイスを所持する必要がなく，利便性が高い

一方，短所としては以下のことが指摘されている．

- 生体情報を測定するため，高価な読み取り機器が必要である
- 身体的な不調，病気，怪我，汚れ，照明，未対応などによる本人拒否の可能性が小さくない
- 本人拒否率（FRR）と他人許容率（FAR）がトレードオフの関係となる
- 残留指紋など，生体情報の漏洩しやすさの問題がある
- 生体情報の取り換えが非常に困難
- 写真，模型，訓練などによる生体情報の偽造や模倣[Mat01][MHS04]が可能である
- プライバシ情報を扱うことによる精神的抵抗感がある

その他の問題として，入国時に指名手配犯や強制退去歴のある外国人の指紋データベースと照合する指紋認証システムをすりぬけるために，指紋の手術をした事例が発生している[AFP09]．また，生体情報は人体と密着しているため，犯罪に巻き込まれた場合に生体認証に使用している部位を切断あるいは摘出されて持ち去られる危険性がある．これは映画や物語の中だけの話ではなく，実際に，指紋認証システムが搭載された高級車を盗むために運転手の指が切断されるという事件が起こっている[ITP05]．指紋認証，虹彩認証，顔認証，静脈認証など技術的には実用レベルに達している方式も多く，記憶の負担もデバイスの所持も必要ないという非常に高い利便性のため，徐々に普及しだしているが，まだ乗り越えるべき課題は多い．

2.1.3 個人の記憶に基づく方式

個人の記憶に基づいた方式は，パスワードや暗証番号などの認証情報をユーザが暗記しておき，その認証情報を認証システムに入力することによって個人認証が行われる方式である（図 2-4）．一般的に，次のような長所が挙げられる．

図 2-4　パスワード認証の例

- 認証情報がユーザの頭の中にあり，簡単には盗むことができない
- 特別なハードウェアを必要としないため，実装が容易で利便性が高い

一方，以下のような短所が存在する．

- 認証情報を忘却するリスクがある

・ 入力の際に認証情報を覗き見されるリスクがある
・ 認証情報を他人と共有することができる

どの認証方式にも一長一短があるが，現在，実装の容易性や高い汎用性から最も広く普及しているのは，パスワード（暗証番号も含む）などの文字／数字列の記憶に基づく認証方式である．しかし，パスワード認証方式については，多くの研究者によってその問題点が多数指摘されている（2.3 節参照）．

2.2 画像認証に関する研究の重要性と意義

本論文では，高い普及率と認知度を持つ記憶に基づく認証方式のなかでも，特に画像を認証情報（パスワード）として利用する認証方式に主眼を置き，その主要な問題点を解決することによって，利便性と安全性を両立する認証方式の実現を目指す．

ここで，2.1 節で記述した 3 つの認証方式の中から個人の記憶に基づく認証に注目する理由は，その普遍性に拠っている．本人性およびユーザの利便性という観点では，個人の生体情報に基づく認証方式に分があるだろう．現在，多くの大学や企業が生体認証技術の研究開発に力を注いでおり，その普及に対する期待も大きい．しかし 2.1.2 節で述べたように，生体情報は残留指紋の採取や，顔や虹彩の写真撮影などによって容易く漏洩する．近年では静脈など，漏洩しにくい生体情報を利用する方式も登場しているが，実際の認証システムで使用されている読み取り装置と同様の機器をドアノブ等に密かに（あるいは偽の認証システムとして堂々と）設置することや，正規サイトを装ったフィッシングサイト[4] を作成しそこにユーザを誘き寄せることによって，秘密裏にユーザの認証情報を取得されてしまう可能性は否定できない．一度漏洩してしまった生体情報を変更するためには，外科手術などを行わない限り，別の生体情報の利用に切り替えることが必要となる．指紋認証の例であれば，別の指の指紋を登録しなおすことも可能だが，それでも変更できる回数は手指の本数に応じた 10 回に限定されてしまう．また最近では，相次ぐ個人情報漏洩事件や個人情報保護法の施行によってプライバシ情報の保護に関するユーザの意識が高まっている．生体情報から人種や健康状態などのプライバシ情報を類推することも可能であると報告されている[Si06]．生体情報の漏洩はプライバシ保護の観点からも深刻であり，強度の個人情報である生体情報を登録する必要のある生体認証に対するユーザの抵抗感も無視できない．一方，所有物に基づく認証においては，認証用デバイスの携帯の不便さや紛失，盗難の危険性がつきまとう．また，携帯電話やスマートフォンなどにおいては，機器のアクティベーションのために特殊なデバイスを別途所持することは理にかなっておらず，携帯端末用の認証としては応用しづらい．これ

[4] フィッシングとは，インターネットバンキングサービスやオンラインショッピング等を提供する正規サイトを模倣したサイトを作成し，そこへ利用者を誘導して正規サイトと勘違いさせることで不正に個人情報やクレジットカード番号，各種サービス利用のための ID・パスワード等の重要な情報を詐取することであり，フィッシングサイトとは，フィッシングの目的に作られた不正なサイトのことである．

らに対し，記憶を利用する認証方式では，ユーザの記憶を外部の機器などから読み取ることは現在の技術では不可能であり[5]，万一，パスワードが漏洩してしまった場合にもユーザがパスワードを変更するだけで復旧が可能である．そのため，入国審査のように個人の身元確認がプライバシや利便性よりも優先される場合を除き，記憶に基づく認証が望まれる状況は非常に多いと予想され，その利便性および安全性を改善することは大きな意義があると考える．

また，特に画像認証に注目する理由は，タッチパネルディスプレイのように実装が容易で，高齢者でも簡単に操作が可能な機器によって構築できるシステムの需要が高くなっているという事実に拠る．例えば，銀行の ATM や駅の券売機などをはじめとして，タッチパネルディスプレイを利用するシステムが既に至るところに普及している．先述の生体認証システムを実装するにあたっては，生体情報を読み取るための装置が別途必要になるのに対し，パスワード認証システムであれば最低限の PC 環境（PC 本体＋ディスプレイ＋キーボード）にて構築可能であり，さらに画像認証システムは機器本体にタッチパネルディスプレイさえあれば実装が可能である．そのため，銀行 ATM[6]などにも新たな機器を追加するコストを要することなく画像認証を導入することができる．携帯電話をはじめ，様々な機器に液晶ディスプレイが搭載されることが一般的になっていることから，付加的な機器によるコストが発生せず，ディスプレイを見ながら直感的な操作で認証が可能となる方式は非常に使用価値が高いと考えられる．特に，一人一台の時代に突入した携帯電話やスマートフォンなどの携帯端末は今後，様々なサービスのキーアイテムになってくると予想されるが，携帯端末のような小型で安価なデバイスには，サイズが大きいキーボードや高価な生体認証の読み取り装置を実装することは難しい．一方，画像認証方式は，携帯端末の液晶ディスプレイを利用しながら簡単なキー操作だけで認証を行うことができるために有力な選択肢となり得る．

本論文では以降，画像認証方式の改善について検討を重ねていくが，まずは次節より，パスワード認証方式の現状の問題点およびパスワードを拡張する様々な方式を調査することを通じ，記憶に基づく認証における画像認証方式の位置付け，既存の画像認証方式および未解決問題などを明確にしていく．

2.3 パスワード認証方式の問題点

パスワード認証は，実装の容易性や高い汎用性から，広く普及している．しかし，その反面，パスワード認証は大きな欠点を伴っていることが多くの研究により指摘されている [MT79][AS88][FK89][Kle90][Spa91][AS99][Wu99][Sch01][Geh02][Ric03][FH07]．

---

[5] ただし，ユーザを脅迫して自白を強要することや，パスワード情報の入力過程を覗き見るなどのソーシャルエンジニアリング[MS03]によってパスワード情報を盗み出される可能性はある．

[6] 東京三菱銀行や駿河銀行などでは静脈認証機能付きの ATM が導入されているが，もちろん ATM 一台当たりのコストは高い．

その主要な原因は，できるだけ長くランダムな文字や数字の組み合わせを設定するほどパスワードの安全性が増すのに対し，本来，人間は長い文字列や記号列を正確に記憶することが得意ではないことにある．すなわち，攻撃者による推測が困難で安全なパスワードであるほど，ユーザにとっては記憶しにくいというトレードオフが存在する[Sch01]．そのため，ユーザはパスワードを忘れないようにするために，以下のような行動をとる傾向にあることが知られている．

- 短く，単純なパスワードを設定する
- パスワードに名前や誕生日など個人に関する情報を含める
- 一度パスワードを設定すると長期にわたって変更しない
- 様々な環境で同一あるいは少数のパスワードを使いまわす
- パスワードを紙に書き留める

以上のような行動を取るユーザのパスワードは，辞書攻撃やパスワードの推測，ソーシャルエンジニアリングなどに対して非常に脆弱である[FK89][Kle90][Wu99]．そこで，パスワード認証システムを安全に運用するために，多くの技術書では「1〜2 か月ごとにパスワードを変更する」あるいは「パスワードは 8 文字以上で，大文字と小文字を用いて英数字や記号を無作為に織り交ぜる」などの対策を推奨している[HBH98][SSM01][Ori02]．企業ではシステム管理者によって，強制的なパスワードの定期更新や，脆弱なパスワードを検出するプログラム[MT79][FK89]を用いた検査が実施されている場合も多い．しかし，そのようなユーザの記憶の限界を考慮しない非現実的な対策は，結果として多くのユーザに「パスワードを紙に書き留める」という行動を促すことにつながってしまっている[AS88][AS99]．これらのセキュリティレベルを低下させるユーザの行動を抑制するためには，一般にはユーザに対する教育や訓練が必要である[AS99]と言われている．しかし，たとえコンピュータを熟知し，セキュリティに関する教育を受けていたとしても，ユーザは利便性を優先し，上記のような行動を行うという調査結果[DP02]も得られている．パスワード認証の問題点の大部分は，人間の許容範囲を超えた記憶能力への要求に端を発しており，運用や教育のみによって解決できるものではない．さらに，昨今は様々な場面でパスワード認証を要求されることが多くなっていることや，コンピュータの計算能力の向上，ボットネット[7]やクラウド・コンピューティング[8]等の分散計算機リソースの登場によって総当り攻撃の脅威が増していることなどから，これに

---

[7] ボットネットとは，悪意のある攻撃者によって乗っ取られた脆弱な PC やサーバによって構成された計算機ネットワークのことである．攻撃者によって遠隔地からインターネットを経由で，ボットネットに指令が渡り，スパムメールを送信したり，DDos 攻撃を実行したり，各種の攻撃に利用される．

[8] 「ローカル・マシンやリモート・サーバ・ファームではなく，グローバルにアクセス可能な分散されたリソースの集合体を利用するコンピューティング」とする IBM の定義[COM07]がわかりやすく，従来のコンピュータ利用は，ユーザ（企業，個人など）がコンピュータのハードウェア，ソフトウェア，データなどを，自分自身で保有・管理していたのに対し，クラウド・コンピューティングでは「ユーザはインターネットの向こう側からサービスを受け，サービス利用料金を払う」形になる[Sa10]．

耐え得るためにより長く複雑なパスワードを設定しなければならなくなっており，ユーザの記憶への負担に拍車が掛っている状況にある[DP02][Geh02].

記憶の負荷以外の問題点としては，パスワードを入力する過程の覗き見攻撃（ショルダーハッキング）の問題[And94]や，正規ユーザ本人が認証情報を漏洩させる場合が往々にしてある[Ric03][ITE04]ことが挙げられる．特に後者に関しては，近年，その被害額が甚大になっているソフトウェア等の不正コピー[TS03][BSA05]において，組織内や友人間におけるソフトウェアのカジュアルコピーなど，正規ユーザ本人からの認証コード（シリアルナンバーなど）の漏洩が大きな問題となっている[Ric03][ITE04]．銀行ATM の暗証番号などを家族で共有しているケースも多いだろう．多くのユーザがパスワードの共有のしやすさを「機能の 1 つ」と認識しているという調査結果[DP02]は，ユーザが気軽にパスワードを他人と共有してしまいがちであることを示している．このように，文字や数字をベースとしたパスワード方式では，パスワードを書き下しておいたものを読まれたり，電子メールや電話などを用いてパスワードを教えたりすることによって，簡単かつ正確にパスワードを他人と共有できてしまうことが，セキュリティ上の問題点となる．

2.4 パスワード認証方式の強化に関する既存研究

パスワード認証方式を拡張したり，文字以外の情報を利用したりすることで，安全性や記憶の容易性を向上させようとする研究は，これまで盛んに行われており，既に様々な方式が提案されている．本節では，本研究に関連するこれらの既存方式を取り上げ，その特徴や問題点をまとめる．

2.4.1 パスワード方式を強化する手法

Manber や Reinhold は，乱数等を用いることにより，推測が困難なパスワード（パスフレーズ）を生成する方法を提案している[Man96][DW]．これらの方式の目的は主に他者に推測されにくいパスワードを生成し，その記憶方法を提供することにある．しかし，記憶方法そのものが不正者に漏洩したり，ユーザ間で共有されたりしてしまった場合には，耐性が著しく低下する．

荒川らは，複数個のパスワード入力装置を用意し，入力装置の色や位置に関する情報を付加情報としてパスワードに組み込むことで，総当たり数の増加と入力操作の覗き見攻撃の危険性を緩和することを意図した方式を提案している[ATS03]．この方式もパスワードの記憶負荷の問題を解決するものではなく，人間的要因に関する課題を残している．

2.4.2 画像情報などの記憶に基づく認証方式

パスワード方式におけるユーザの記憶負荷の大きさの問題を解決するために，文字や記号の代わりに画像情報を利用して認証を行う方式が多数提案され，注目されている．

人間にとって画像の記憶は文字や記号等の言語的記憶に比べて優れており，加齢の影響も受けにくいことが認知心理学における長年の研究から知られている[She67][PRS68][Nic68][NRW76][Par97]．特に，認証時に提示される複数の画像中に含まれる自身のパス画像を正しく見つけ出すことで認証が行われる方式では，画像記憶の優位性に加え，画像の再認によってパス画像が想起されるという効果を利用することができる．文字や画像の想起に関して，再認課題（対象を見て思い出す課題）は再生課題（対象を見ずに思い出す課題）に比べて顕著に優れており[Nie93]，加齢による衰えが非常に少ないという特徴があり，再認課題では 20 歳代から 60 歳代の間でも成績の下降が見られない（成績の下降が見られても再生課題に比べて顕著に緩やかである）という実験結果が得られている [SR66][Rab84]．すべての認証情報を正確に入力する必要のある認証システムにおいては，細部を記憶しなくてもよい再認方式を用いることで，ユーザの記憶負荷を大きく抑えることが可能であり，ユーザの振る舞いに起因するセキュリティレベルの低下を軽減できることが期待される．さらに，画像認証方式はマウスやスタイラスペン，タッチパネルディスプレイ等の操作が簡便な入力機器で実装することが可能であり，高いユーザビリティを持つことが特徴である．

しかし一方で，通常の画像認証方式には「毎回の認証時にパス画像がディスプレイ上に表示されるために，認証行為を覗き見されてしまうと，パス画像が漏洩する危険性がある」という画像の再認による認証を行うが故の欠点が存在する．従来の文字のパスワード認証においても覗き見攻撃（ショルダーハッキング）の問題[And94]は指摘されているが[SYK09]，パスワードに対しては「********」のように入力された文字を隠して表示することにより，少なくともディスプレイを覗き見る攻撃に関しては無効化できる．一方，画像の「再認」をベースとする方式では，そのような対策は不可能である．すなわち，画像の使用は，正規ユーザの記憶負荷を低減すると同時に，攻撃者に対しても覗き見た他人のパス画像を記憶することを容易にしてしまう．そのため，従来の文字を用いたパスワード認証と比較して，画像認証方式における覗き見攻撃の脅威は大きく，ユーザにとって記憶しやすいパス画像ほど覗き見攻撃が容易であるというトレードオフを解消するまでには至っていない．

また，パスワードは他人と共有されやすいという問題に対しても，パスワードを画像に変えるだけでは十分な対策とはならない．文字よりも曖昧性の高い画像を利用することによって，パス画像の内容を一意的に伝えることは困難になるが，画像の意味内容を言葉にして伝えるだけでも，認証を通過させるに十分な情報を漏洩させることは可能であろう．また正規ユーザの情報（趣味・嗜好など）からパス画像が推測される可能性（Educated-Guess 攻撃[9]と呼ばれている）も少なくない．

---

[9] 犬好きであれば犬の画像を，車好きであれば車の画像を，白い猫を飼っていれば白い猫の画像をパス画像としている可能性が高いなど，正規ユーザ本人の情報を元に，パス画像を推測攻撃のことである．

パス画像を隠すために利用される囮画像（認証画面にパス画像と共に表示される複数の画像）を適切に用意することも，画像認証における重要な課題の 1 つと言われている．例えば，毎回の認証で常に同じ囮画像のセットを利用してしまうと，攻撃者が認証画面中の画像一枚一枚に当たりをつけ，「その画像を選択して認証に失敗したならば，その画像はパス画像ではない」というように，パス画像の候補が徐々に絞られていく問題（Exhaustive 攻撃と呼ばれる）がある．

また，複数の画像の中から自分が記憶したパス画像を選択する再認型の画像認証方式においては，過去にパス画像もしくは囮画像として用いた画像を囮画像にしたり，自分が撮影した写真のように自分にとって馴染みの深い画像を囮画像としたりすると，結果的に正規ユーザは認証画面中のすべての画像に対して再認を起こすことになり，パス画像の認識に混乱をきたす可能性があると言われている[DP02]．そのため，囮画像にはなるべく正規ユーザが再認を起こさない，つまり，正規ユーザが見たことのない画像を使うことが望ましい．

これらの問題を解決するために，毎回の認証ですべての囮画像を一新する，つまり，一度囮画像として利用した画像は以降の認証では囮画像として利用しないという方法が考えられる．しかしこの場合は，今度は，認証の度に必ず表示される画像がパス画像であるということが推測されてしまう（Intersection 攻撃と呼ばれる）ことになる．

以上より，ある一定枚数の囮画像は前回の認証から引き継ぎ，残りの囮画像は正規ユーザが見たことの無い全く新しい画像を用いるという折衷案が適切と考えられるが，残念ながらこの方法にも依然として，どのようにして新しい囮画像を追加すればよいのかという問題が残る．あらかじめ大量の囮画像を端末に保存しておいたり，ネットワークを介して自動的にダウンロードしたりするという方法も考えられるが，実装や運用の観点からはストレージや通信の使用を可能な限り抑えたいというニーズがある．

2.4.2.1 図形的な形状や位置情報を認証に利用する方式

Jermyn らや Microsoft では，PDA やタブレット上のグリッドで分割された領域に，スタイラスペン等を用いて図形を描き，どのグリッドをどの順番で通過したかという情報を取得して個人認証を行う方式を提案している[JMM99][MC03]．また，同様の考え方に基づき，規則正しく配列されたボタンの入力順序を，図形的なパターンとして記憶して認証に利用する方式[CSE][PAT]が実用化されている．これらの方式では，認証用情報を図形的に記憶することで，画像記憶の優位性を利用することができるが，認証方法が図形の再生課題に基づいており，再認を利用する方式ほどの記憶負荷の軽減は期待できない．実際，手書きの図形を用いる方式[JMM99]に関する評価では，ストローク数（画数）が多くなると文字のパスワードよりも再生の正確性が低くなるという結果が得られている[GHS02]．実際に導入された場合，パスワード認証の問題と同様に，覚えやすいパターン（対称なパターンなど）ばかり選択される可能性があるという問題も指摘されている[TO04]．

鹿島の研究[Kas00]，blonder の特許[Blo96]，商用製品の visKey [VK]や V-go [VGO]などでは，画面に表示されている画像内の複数の位置情報をパスワードとして設定し，それらの位置をあらかじめ登録した順序で選択（マウスクリックやスタイラスペンで選択）することで認証が可能となる方式を提案している．認証時には，ユーザは画面に表示された画像を手がかりとして，自らが設定した位置を思い出して選択することができる．ただし，画像中の位置やその順序を思い出すタスクは再生課題に相当し，再認課題ではない．また，位置情報を利用する方式については，ユーザは特徴的なポイントを選びがちであり，実質的な総当りパターン数は少なくなってしまうことが多い[RA04]という問題も指摘されている．

2.4.2.2 写真やイラスト画像の再認を利用する認証方式

写真画像をパス画像として登録し，認証時に複数枚提示される画像の中からパス画像を選び出して選択できれば認証成功となる方式[ACC02][Mas02][PSL03][JGK03][WP]が提案されている．これらの方式は，人間が得意とする画像の再認課題を利用することで，ユーザの記憶負荷の軽減を実現するものである．実際に，写真の再認を利用する認証は暗証番号（PIN）やパスワードの再生よりも記憶負荷が低いという実験結果が得られている[DP02]．図 2-5 に，文献[PSL03]における認証システムの表示例を示した．

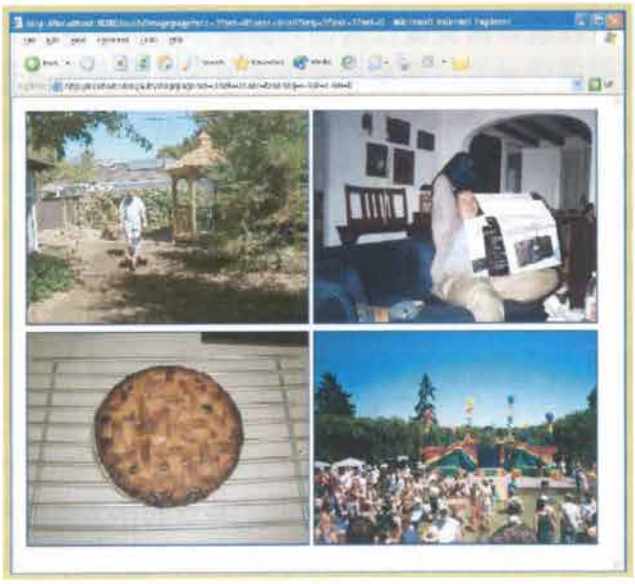


図 2-5　写真の再認を利用する画像認証方式の例

出典：　http://www.cs.cmu.edu/~15-821/CDROM/PAPERS/pering03.pdf）

IP イノベーションズは，あらかじめ特定の画像を登録しておき，認証時に複数枚現れる画像の中から登録画像を探し出し，登録画像の上に記されている数字列をワンタイムパスワードとして入力する方式を提案している[VEN05]．パスワードの入力方法に工夫が見られるが，登録画像を知られてしまうと安全性が無くなるため，登録画像となる写真画像をパス画像とした再認方式の認証システムと同様のシステムと捉えることができ，

その長所や短所もそれに準じる．また一度認証作業（入力した文字列と文字列に対応する画像）を完全に覗き見られてしまうと，登録画像が漏洩してしまうという課題がある．

PassFace[PF]は，パス画像として人間の顔写真の再認を利用する．この方式は，人間は画像の記憶が得意であるが，特に人間の顔を記憶して再認することに優れている[Bru90][YMN93]という点に基づいており，さらなる記憶負荷の軽減を図っている．

ニーモニックガード[MNE]や Pointsec[PMT]などは，写真やイラスト画像などをパス画像として設定し，認証画面上に表示される多数の画像の中から複数のパス画像を正しい順番で選択することによって認証を行う機能を含んでいる．ユーザがパスワードを選択する際に，各パス画像の内容を盛り込んだ文章を作成して記憶することを推奨している点が特徴である．例えば，「女性」「飛行機」「コーヒー」「本」という順番でパス画像を選択する場合，「花子は，飛行機の中でコーヒーを飲みながら読書をして時間をつぶした」という文章やストーリーを作成して記憶する．これは，イラスト画像の画像的記憶に加えて，パスフレーズ的な文章やストーリーの意味情報の記憶を併用することで，パス画像の記憶負荷を軽減することを図っており，いわゆる記憶術を用いた方式といえる．

合わせ絵[TK02]も写真画像をパス画像として用いる方式であるが，カメラ付き携帯電話等でユーザ自身が撮影した写真画像をパス画像として登録することを特徴としている．自分自身で撮影した写真を用いることによって，パス画像の想起がさらに容易となることが期待される．なお，ニーモニックガード[MNE]も同様にユーザ自身に馴染みがある写真等の好みの画像をパス画像として登録する機能を含んでいる．

上記の方式に共通している点は，写真やイラスト等の意味のある画像の再認を利用すること，および，パス画像の選択や登録方法を工夫することによって，ユーザの記憶負荷の軽減に注力していることである．しかし一方で，認証時の覗き見攻撃や，パス画像の意味を言語によって漏洩される問題に対して耐性を有する方式ではない．また，囮画像の問題についても未解決のままになっている．

2.4.2.3 人工画像の再認を用いた画像認証方式

Dhamija らは，乱数を引数とするランダムな計算方法によって生成された，抽象的な幾何学模様の人工画像[Bau]をパス画像として用いる方式を提案している[PS99][DP02][KHM02]．認証時には複数の人工画像の中からパス画像を再認して選び出す方法を用いており，ユーザの記憶負荷を軽減している．図 2-6 に，Dhamija らの認証システム[DP02]の例を示す．

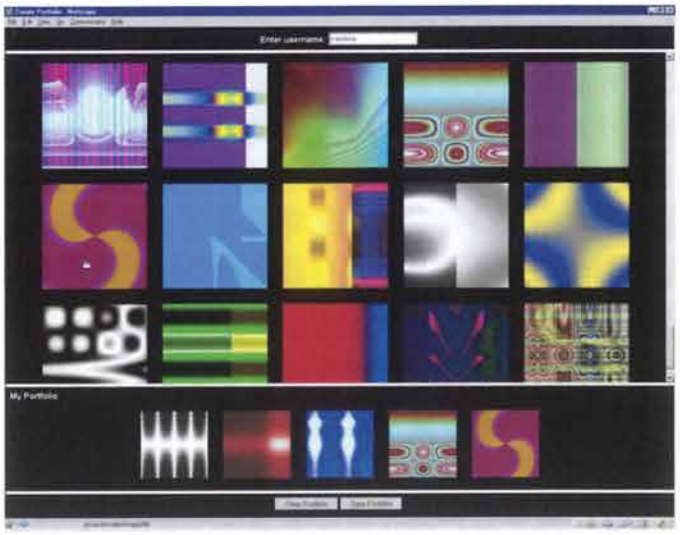


図 2-6　人工画像の再認を用いた認証システムの例 (Deja Vu)
出典　http://people.ischool.berkeley.edu/~rachna/dejavu/

人工画像を使用する方式の特有の利点として，人工画像のもとになる乱数を保存しておけば人工画像そのものを保存しておく必要がなく，認証システムのストレージ容量を節約できることが挙げられる．また，乱数を変えれば別の異なる人工画像を得ることができ，無限に人工画像を生成することができる．そのため，囮画像の問題を解決している方式であるといえる．

さらに，正規ユーザ本人からのパス画像の漏洩に注目し，抽象的な画像を用いることで，紙に書き留めることや，他者にパス画像の特徴を正確に伝達することを困難にすることを意図している．しかし，実際に他者への漏洩が困難になるかどうかに関する評価は，Dhamija らの論文において行われていない．人工画像にも，円・四角形・直線といった幾何学的な形状情報，形状の色情報や位置情報などが含まれており，それらを言語化して伝えることは比較的容易であることから，なりすましに十分なレベルのパス画像の情報が漏洩する可能性は残ると考えられる．また，覗き見攻撃に関する対処も課題である．

2.4.3　ユーザの既知情報に基づく認証方式

新たに認証情報を記憶するのではなく，既にユーザが持っている知識を利用する認証方式[ZH90][Smi87]が提案されている．Zviran らの方式では，ユーザが自分で作成した質問とその回答をシステムに登録しておき，認証時に画面に表示される質問（あらかじめユーザが登録した，既定の事実や知見に基づく質問）に正答した場合に正規ユーザであると認証される[ZH90]．この仕組みは，すでに複数の WEB サイト[YAH][WLI]などで，ユーザがパスワードを忘れてしまった場合への備えとして導入されている．また Smith の方式では，ある単語 A からユーザが連想する他の単語 A'を登録しておき，認証時に提示される単語 A に対応する単語 A'をユーザが正しく回答できれば認証成功とな

る[Smi87]．これらの方法は，ユーザの既知情報を利用できるために，認証のために新たに記憶しなければならない情報がなく，ユーザの記憶負荷は少ない．ただし，答えを入力する際の覗き見攻撃に耐性がなく，正規ユーザを知っている者による推測攻撃に対して課題がある．

Spector らの方式では，ユーザがあらかじめ「犬を連れて弁当とお茶を持って遊びに出かけた」といった文章を認証システムに登録しておき，ユーザは認証時に再び同じ意味をもつ文章の入力を要求される[SG94]．例えば「動物を連れて弁当とお茶を持って遊びに行った」と入力したとすると，認証システムが文章を解析し，「何という動物を連れていましたか？」という質問をしてくるので，「犬」と正しく回答することができれば認証に成功するという方式である．ユーザはその文章の持つ意味を記憶しておけば，文章の一字一句を正確に記憶する必要がないため，通常のパスフレーズ方式よりも記憶負荷を軽減できる．ただし，この方式は言語情報における再生課題に基づくものであり，再認を利用するものではない．また，認証情報を入力する際の覗き見攻撃への耐性もない．

西垣らの方式[NKT06]では，ユーザが日々の生活で経験する個人的なイベント情報を認証システムに蓄積する．認証システムがその情報に準拠した質問を生成し，当該ユーザがその質問に正答できるか否かによって認証が行われる．当該研究では，ホームコンピューティング環境が実現されていると仮定した場合，ユーザが日常に視聴しているTV 番組名をホームサーバ（認証システム）が取得しており，ユーザの帰宅時には「昨日 20:00 から観た TV 番組はなんですか？」という質問に正答することができればドアを開錠する，というような仕組みを提案している．ユーザは認証情報を記憶しておく必要がなく，自分の生活に密着した情報を利用できることで記憶の負荷が軽減されている．また，認証情報は日々更新されてゆくため，ワンタイムパスワードのような効果があり，覗き見攻撃にもある程度の耐性がある．ただし，個人情報を認証に用いるためにプライバシ情報漏洩の問題があることと，特に身近な人物にとっては正答の推測が可能であることが課題である．

2.4.4 その他の人間の特性を利用する方式

2.4.4.1 人間の画像認識能力の高さを利用する研究

CAPTCHA[ABH03]は，歪曲やノイズの付加によって難読化された文字や絵を見ても，その対象物を正しく認識できる人間の高度な認識能力を利用するという点が不鮮明化画像を利用した画像認証と関連している．図 2-7 に CAPTCHA によって生成された文字列の例を示す．

図 2-7　CAPTCHA システムー「grae」という文字列

出典　http://www.captcha.net/cgi-bin/gimpy-r

難読化された文字列を正確に読み取ってシステムに入力することで認証が行われる方式であり，複数の大手企業が Web 上のサービスの安全性向上のために CAPTCHA や同種の仕組みを導入している[YAH][MSN]．ただし，この方式の目的は，人間による web アクセスとコンピュータプログラムによる攻撃とを弁別し，近年大きな問題となっているスパムメール[SYM04]やスパムブログ[10] [SOU]，ボット（bot）[IPA]等のマルウェアによる活動を防止することであり，人間同士を識別するための認証を扱うものではない．また，CAPTCHA の導入が進むことによって，視覚障害者がサービスを享受できなくなることが社会的な問題として指摘されだしている[CNE04][Ono05][W3C03]．これは，当該研究のみにとどまらず，画像や図形などの視覚的情報を用いる認証方式全体の問題でもある．

2.4.4.2　経験による想起の容易さを利用する認証方式

花井らは，人間の得意な画像の認識・識別能力に加え，過去に解いたことのある問題に再度直面した際に以前より速く解くことができるという，人間の経験を活用する能力の高さを利用した方式を提案している[HNY04]．この研究は，多数の紛らわしい人物たちの中から，ある特定の人物を探し出すというパズル絵本の「ウォーリーを探せ」[Han00]より着想を得ている．図 2-8 に，当該研究の登録フェーズにおける画面表示の例を示す．

[10] スパムブログとは主に，ニュースサイト等からの文章の引用や組み合わせにより自動的に作成されたブログ，アフィリエイトの収入を目的としたアフィリエイトリンクアンカーのみを大量に貼り付けたブログ，アダルトサイトや出会い系を目的としたブログ等，機械的に作成されたブログのことを指す．

図 2-8　「ウォーリーを探せ」を模した認証システム画面

登録フェーズにおいて，ある特定のキャラクタを選んで，そのキャラクタを多数の類似したキャラクタ群の中から選びだすというパズル問題を解いておく．その後，認証フェーズにおいて，登録フェーズと全く同じ配置のパズル問題を制限時間以内に解けるかどうかで個人認証が行われる．正規ユーザは登録フェーズにおいて一度パズルを解いた経験があるため，認証フェーズでは素早く正解のキャラクタを探し出し，答えを入力することができる．正規ユーザ以外は，たとえ正解のキャラクタを推測できたとしても，初見でパズル問題を制限時間内に解くことは困難である．当該研究はまだコンセプト提案の段階にあり，課題は多いものの，人間の経験による想起の容易性を利用してユーザの記憶負荷軽減を意図している点が独創的である．ただし，覗き見攻撃や，言葉による認証情報の漏洩に対する耐性は備えていない．また本方式においても，囮画像（囮キャラクタ）の問題が未解決のままとなっている．

2.4.5　覗き見防止を考慮した認証画面

攻撃者による覗き見を防止する対策として，商用に広く販売されている狭可視角化フィルタ（プライバシフィルタ）[TOH]を認証用ディスプレイに装備することが考えられる．これは簡便で効果的な方法であるが，横からの覗き見は防止できても後ろからの覗き見までを防ぐことができない．

また，2 枚のスライドシートを重ね合わせると文字や画像が浮かび上がる VSS[NS94]を利用する文献[KI96]の方式は，後ろからの覗き見にも効果がある方式であるが，認証情報を復号するためのスライドシートを常に所持しておく必要があり，利便性の面で問題が残る．

ヘッドマウントディスプレイ[SHI]のように物理的に一人しか画面を見ることができないハードウェアを用いて認証用ディスプレイを実装することも可能だが，そのような機器は現在でも高価であり[WRP]，個々の情報端末への導入は困難であろう．また，専用のメガネを着用しないとディスプレイ上の表示を見ることができない PPT（Picture Protect Technology）ディスプレイ[PPT]においては，同じ PPT 専用メガネを所有する人物によって画面表示を見られてしまうという問題が指摘されている[TNS04]．また，携帯電話やスマートフォンなどの携帯端末用の認証システムへの応用はしづらい．さらに，本方式は物理的に覗き見を防止する対策であるため，囮画像の問題の解決を目的としたものではない．

2.4.6 覗き見攻撃に対する既存の画像認証方式

覗き見攻撃に対する耐性を有する記憶に基づく認証方式の研究も進められている．現在までのところ，大きく分けて以下の 4 つの方式が知られている．

1. C&R 型画像認証方式 [SB02][WWS06][RRF04]
2. パス画像更新型認証方式 [JN06][Ta08]
3. 画像認識妨害型認証方式 [HIM05][HCD07]
4. チャレンジ隠蔽型 C&R 画像認証方式 [SCH08]

以下では，上記の 4 種類の方式について概説し，問題点を挙げる．

2.4.6.1 C&R 型画像認証方式（Challenge & Response 型画像認証方式）

C&R 型画像認証の代表的な方式として Sobrado らが提案する方式[SB02][WWS06]がある．Sobrado らの方式では，チャレンジとして，システムから多数のアイコンがランダムに配置された画面が提示される．ユーザは，あらかじめ登録しておいた複数の pass-object（3 つ以上）を画面の中から探し出し，pass-object を頂点とした凸包内部を選択することでレスポンスを返す（図 2-9）．

ユーザからのレスポンスを「凸包の内部」という曖昧な形で返すため，覗き見攻撃者に凸包を構成する pass-object が一意に漏洩しない．しかし，正規ユーザにとって多数の object（アイコン）の中から特定の pass-object を探し出す作業は容易なことではなく，認識負荷の点で問題を残している．また，pass-object は意味のある画像であり，画像の意味内容を言葉にして伝えるだけでも，認証を通過させるに十分な情報を漏洩させることは可能である．

本方式においても従来の画像認証同様，正規ユーザの趣味・嗜好から pass-object が推測される恐れがあり，囮画像（囮の object）の問題も未解決のままとなっている．

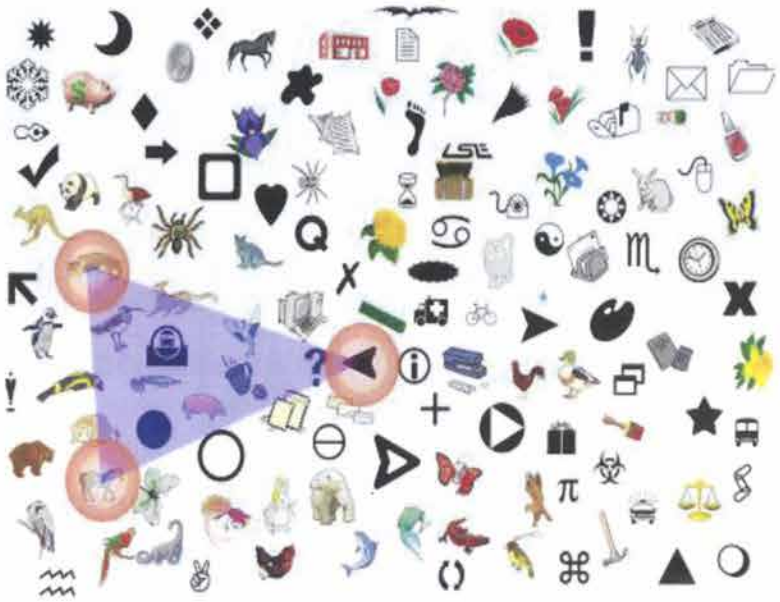


図 2-9　Sobrado らの認証システム[SB02]の認証画面

一方，Roth らが提案する方式[RRF04]では，認証情報に付与されているグループ情報を回答させるというアイデアによって，レスポンスの生成に対するユーザの負荷を軽減させることに成功している．Roth らの方式では，認証時には 0～9 までの数字が並べられた画面が表示される．各数字の背景は白もしくは黒のどちらかの色でランダムに塗られており，それによって各数字がどちらの色のグループに含まれるのかが示されている．ユーザは自分の暗証番号の数字の背景色が白なのか黒なのかを答える（図 2-10）．これを各桁につき 4 回行う（4 桁暗証番号であれば計 16 回もの問答を繰り返す）．ユーザが色を答える度に画面上の数字の背景色はランダムに塗り直される．

暗証番号を記憶している正規ユーザはレスポンス（背景色）を容易に返答することが可能である．しかし，レスポンスの選択肢が限られる（白と黒の 2 択）ので，十分な総当り数を確保するためには問答を繰り返す必要があり，入力回数が激増してしまう．また，記憶しやすい番号列が設定され易いという暗証番号本来の問題は解決されない．

本方式は暗証番号の代わりにパス画像を用いることで，記憶負荷を抑える方式へと拡張することも可能であろうが，従来の再認型の画像認証同様，パス画像の言葉による漏洩や囮画像の用意について課題が残る．

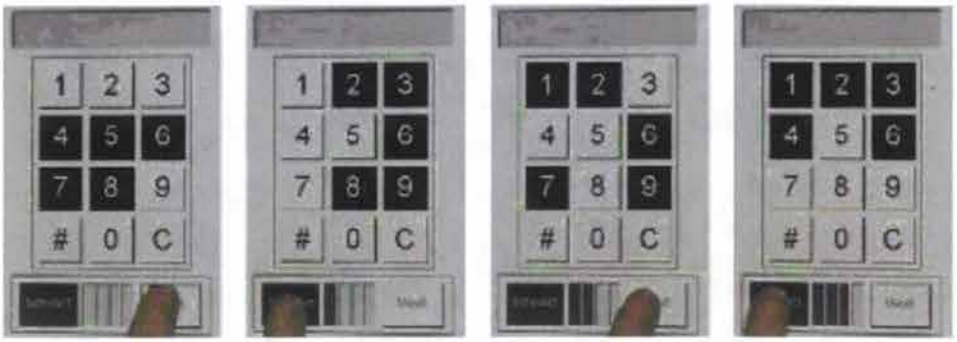


図 2-10　Roth らの認証システム[RRF04]の認証画面の例

2.4.6.2　パス画像更新型認証方式

パス画像更新型認証方式は，セキュア ID[SID]のように認証情報を毎回更新するタイプのワンタイム画像認証方式である．しかしながら，画像認証においてパス画像を毎回覚え直すことはユーザにとって大きな負荷になってしまう．そこで，徐らはストーリーづけによる記憶補完（ニーモニック）を導入することによって，パス画像更新時の記憶負荷を軽減しようと試みている[JN06]（図 2-11）．しかし，ストーリーによる記憶負荷軽減の効果が十分でないこと，および，パス画像更新の度にストーリーを考えること自体がユーザの負荷となることなどの問題が残る．また本方式においても従来の画像認証同様，正規ユーザの趣味・嗜好からパス画像が推測される恐れがあり，囮画像の問題も未解決のままとなっている．

図 2-11　徐らの認証システム[JN06]の認証画面の例

fakepointer[Ta08]では，パス画像の短期記憶を活用することで記憶負荷を抑える工夫をしている．fakepointer は暗証番号の各桁をパス画像（背景画像）に合わせることによ

って認証が行われる（図 2-12）が，認証の度にパス画像が変更される．ここでパス画像は，時間的・空間的に異なる通信路（例えば，ユーザ固有の携帯端末）を介して，認証操作の直前にユーザに送られてくる．すなわち，ユーザがパス画像を記憶していなければいけない時間は，パス画像が届いてから認証操作を行うまでの短期間のみとなる．しかし，パス画像の具体的な取得方法に疑問が残る上に，パス画像の短期記憶の負荷が本当に低いかどうかに関する実験や評価もなされていない．

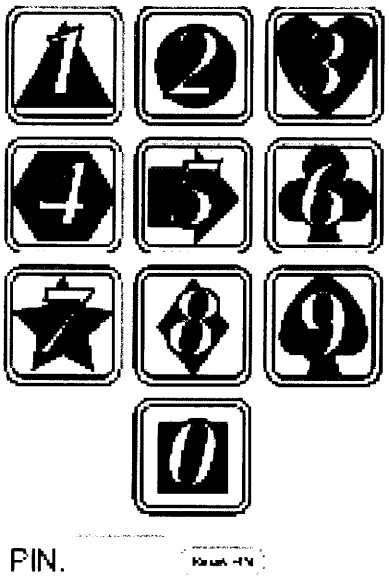


図 2-12　fakepointer [Ta08]の認証画面の例

2.4.6.3　画像認識妨害型認証方式

画像認識妨害型認証方式としては，原田らの不鮮明化画像を用いた方式[HIM05]とHayashi らのぼかし画像を用いた方式[HCD07]が知られている．

不鮮明化画像を用いた方式（以降，不鮮明化画像方式と呼ぶ）は，覗き見や推測をする攻撃者にとってパス画像の記憶や推測が困難となるように，モザイク化等の不鮮明化処理を施した一見無意味な画像（図 2-13 右）をパス画像として使用するというアイデアに基づいている[HIM05]．正規ユーザにのみ不鮮明化画像に対するオリジナル画像（図 2-13 左）を見せ，スキーマ（オリジナル画像と不鮮明化画像の間の認知構造的なリンク）[Bre99]を学習させることにより，正規ユーザは不鮮明化画像を有意味な画像として認識できるようになり，パス画像（不鮮明化画像）を容易に記憶することができる．さらに，不鮮明な画像の利用は，パス画像の内容を言葉で伝えることを困難にし，正規ユーザの情報（趣味・嗜好など）からパス画像を推測することを難しくするという効果もある．

しかし，スキーマを獲得していなくても，不鮮明化画像を認識すること自体は不可能ではない．よって，カメラで盗撮しておいた不鮮明化画像と同じものを選ぶという攻撃

には脆弱性が残る．最近は ATM への盗撮カメラ設置の事件も発生している[ITN05]ことから，カメラ撮影を用いた覗き見にも一定レベルの耐性を有することが望まれる．

図 2-13　原田らの認証システム[HIM05]で用いられる不鮮明化画像（右）とそのオリジナル画像（左）の例

Hayashi らの方式では，油絵処理によってぼかした画像（図 2-14 の右）をパス画像として利用する[HCD07]．正規ユーザはパス画像登録時にオリジナル画像（図 2-14 の左）を見ることができ，これによって，ぼかし画像であっても容易にその意味を認識することが可能となる．オリジナル画像を知らない攻撃者にはぼかし画像からその意味を類推することが困難である．

この研究の基本アイデアは，原田らの不鮮明化画像方式[HIM05]と同等であり，人間の認知の特性である画像記憶に関するスキーマを活用することで，正規ユーザには記憶しやすいが，それ以外の他者には記憶が困難となるようなパス画像を認証に利用することにある．ただし，本方式は，覗き見攻撃が脅威となりにくい小型の携帯端末用の認証システムとして研究が進められており，小さなディスプレイを利用した際のパス画像の認識性の改善と，携帯端末が攻撃者に拾得された際のパス画像の漏洩に対する耐性の向上に主眼が置かれている．このため，特に覗き見攻撃耐性について考慮した方式とはなっていない．

図 2-14　Hayashi らの認証システム[HCD07]で用いられるぼかし画像（右）とそのオリジナル画像（左）の例

また両手法においても．従来の画像認証と同じく囮画像の用意の問題が未解決のままとなっている．

2.4.6.4 チャレンジ隠蔽型 C&R 画像認証方式

Sasamoto らの方式[SCH08]は，チャレンジそのものを秘密の通信路を介してユーザに提示することで，ビデオカメラによる複数回の撮影に対しても高い耐性を実現している．認証時にはディスプレイから与えられる明示チャレンジ（visible challenge）と触覚デバイスから与えられる隠蔽チャレンジ（hidden challenge）とからレスポンスを生成する．隠蔽チャレンジは触覚デバイスを介してユーザの掌によって知覚される．触覚デバイスはユーザの掌によって隠されており，隠蔽チャレンジは外部からは見えない．このため，覗き見（ビデオカメラによる撮影）によって取得可能な情報（明示チャレンジとレスポンス）だけでは，正規ユーザになりすますことは困難である．

しかし Sasamoto らの方式では，チャレンジの隠蔽を実現するために特殊な装置（触覚デバイス）を必要とする（図 2-15）．また，一般的な触覚デバイスにおいては一度に多くの情報量のチャレンジをユーザに送信することは難しく，覗き見攻撃への耐性を落とさずに十分な総当たり数も確保するためには，多数回の問答を繰り返す必要がある．

図 2-15　Sasamoto らの認証システム[SCH08]

2.5 既存方式のまとめと本研究の位置付け

上記のように，従来の記憶に基づいた認証方式に関する研究は，ユーザの記憶負荷をいかに軽減するかという目的に注力したもの[JMM99][MC03][PSL03][Kas00][Blo96][VK][VGO][Bru90][YMN93][MNE][PMT][SGP][DP02][ZH90][Smi87][SG94][NKT06]や，覗き見攻撃への耐性改善にのみ注力するもの[SB02][WWS06][JN06][RRF04][SCH08][Ta08][HNE08][KYN07][KYN08][YKN09][WWS06]がほとんどであり，パス画像の共有のし易さ，趣味・嗜好からのパス画像の推測のし易さ，囮画像の潤沢な用意などの問題を同時に解決する方式となっていない．また，覗き見攻撃への耐性改善に注力した方式であっても，特別なデバイスやチャネルを前提としたり，正規ユーザに複雑な処理を必要としたりするものがほとんどであり導入の負荷が高い．

そこで，本論文では，画像の記憶・再認の優位性は残したまま，上記の課題を克服した新しい認証方式の実現の目指す．その際，人間の計算能力の限界に鑑みるに，計算量的な安全性を礎とする暗号学的なアプローチで認証方式を改良することは基本的に困難であると考えられる．そこで本研究では，認知心理学的な観点からのアプローチ，特に不鮮明化画像[HIM05]の特長に注目して，研究を進めていく．

本研究では，覗き見の問題に対して，手がかり付き再認を利用した認証方式の改良，および，「暗示・応答」という新しい概念に基づく認証方式の提案を行い，その有効性を検証する．また，囮画像の問題に関しては，囮画像の自動生成の手法を示し，その性能について評価を行う．

3章　不鮮明化画像方式：画像記憶のスキーマを利用した認証方式

本章では，本研究において重要な役割を担っている不鮮明化画像方式[HIM05]について説明する．当該研究の基本アイデアは，人間の認知の特性である画像記憶に関する「スキーマ」[Bre99]をうまく利用することで，正規ユーザには記憶しやすいが，それ以外の他者には記憶が困難となるようなパス画像を認証に利用することにある．これを実現するために，有意味なオリジナル画像に対して不鮮明化処理を施すことによって作成された，一見すると無意味に見える「不鮮明化画像」をパス画像として利用する．

3.1　コンセプト

画像認証方式にとって覗き見攻撃が脅威となるのは，正規ユーザのみならず覗き見攻撃者にとっても画像の記憶は容易であるからである．すなわち，認証画面にパス画像そのものが表示されるため，正規ユーザによる認証時の画像選択を覗き見られると，攻撃者にパス画像を容易に記憶されてしまう．そこで，本方式では，覗き見をする攻撃者にとってパス画像の記憶が困難となるように，モザイク化等の不鮮明化処理を施した一見無意味な画像（不鮮明化画像）をパス画像として使用する．人間は画像の記憶に優れているという特性を有するものの，それは有意味な画像を記憶する場合に限ってのことであり，無意味に見える（有意味化が困難な）画像を記憶することはやはり難しい[Mat83][OT01]．ゆえに，他人のパス画像（不鮮明化画像）を覗き見て記憶することは，攻撃者にとって困難な作業となる．

ただし，無意味に見える画像を記憶することは正規ユーザにとっても困難であるため，正規ユーザにのみ，パス画像の登録時に不鮮明化処理を施す以前の有意味なオリジナル画像を見せ，当該画像に不鮮明化処理を施したパス画像と合わせて記憶させるようにする．不鮮明化画像にはオリジナル画像の特徴がある程度残されているため，オリジナル画像を見ることによって，正規ユーザは不鮮明化画像の中にオリジナル画像の持つ意味を見出せるようになる．この結果，正規ユーザは不鮮明化画像を有意味な画像として認識できるようになり，パス画像を容易に記憶することができる．

これは，不鮮明なパス画像に対するスキーマを正規ユーザに学習させていることに相当する．ここでスキーマとは，人間が外界からの情報を知覚した際に無意識のうちに蓄積している「その情報をどのように認識・記憶したかという知識の枠組み」を意味する認知心理学用語である．人間は外界から得られる情報を，無意識のうちに，常時スキーマという枠組みを用いて認識しており，ひとたび不鮮明化画像に対するスキーマを学習すれば，それ以降に当該不鮮明化画像を見た場合にも，スキーマを活用することによって簡単にその意味を再認識することが可能になる．

スキーマを認証に利用することで，不鮮明化処理を施したパス画像であっても正規ユーザは容易にこれを記憶でき，一方，スキーマを学習していない覗き見攻撃者には他人のパス画像を記憶することが困難であるという認証方式が実現できる．ここで重要なこ

とは，正規ユーザ以外には，不鮮明化処理を施したパス画像からオリジナル画像の意味が類推できないようにすることである．つまり，他のユーザには当該パス画像に対するスキーマを学習させないようにする必要がある．

3.2 不鮮明化画像の生成方法

本節では，本研究で用いた不鮮明化画像の生成方法について概説する[11]．本研究における不鮮明化画像の生成方法は不鮮明化画像方式の研究[HIM05]で紹介されている方法である．

写真画像などの有意味なカラー画像 $I(x,y)$（以下，オリジナル画像と記す）を用意し，$I(x,y)$ に対してモザイク化などの画像処理を施した不鮮明化画像 $O(x,y)$ を作成する．以下に，詳細な不鮮明化処理の手順について記述する．

● 不鮮明化処理アルゴリズム

STEP0. 300×300 ピクセルの 256 色カラー画像 $I(x,y)$ を用意する．

STEP1. $I(x,y)$ をモノトーン化した後，ヒストグラム均一化処理を施し，明るさおよびコントラストを調整した画像 $I'(x,y)$ を得る．

STEP2. $I'(x,y)$ に対し，6×6 ピクセルブロック単位でモザイク化処理を行い，画像 $I''(x,y)$ を得る．各ブロックは，ブロック内の平均輝度で一色にぬりつぶされる．

STEP3. $I''(x,y)$ のモザイク処理された各ブロックを 1 画素とみなした画像 $M(k,l)$ (50×50 ピクセル)に対して，二次元 DCT 処理を行う．今回は簡単のため画像全体を 1 ブロックとして DCT を行った．

STEP4. STEP3 で得られた DCT 係数の低周波成分および中～高周波成分の値にノイズとなるデータを与える．今回のシステムでは，図 3-1 におけるグレーの範囲に対応する DCT 係数に，-100～100 の値をランダムに代入し，DC 成分は 0 とした．その後，IDCT 処理によって画像 $M'(k,l)$ を得る．今回のシステムでは，乱数のシードに常に同じ値を設定し，同じ画像に対しては常に同じ不鮮明化画像が作成されるようにした．

STEP5. $M'(k,l)$ の 1 画素を 6×6 サイズのブロックに伸長し，元画像の大きさに戻した後，再びヒストグラム均一化の処理を行って画像 $I'''(x,y)$ を得る．

STEP6. $I'''(x,y)$ に対して，$I''(x,y)$ との重み $w(0 \le w \le 1)$ の加重平均による重ね合わせ処理を行い，画像 $O(x,y)$ を得る．

$$O(x,y) = wI''(x,y) + (1-w)I'''(x,y), \quad \forall (x,y)$$

---

[11] ただし，不鮮明化画像方式における第一の目的は，スキーマをうまくコントロールすることによって，正規ユーザにのみ記憶が容易な不鮮明化画像を作成して認証に利用する方式を提案することにあるため，本節で示す不鮮明化画像の作成方法はあくまで一例である．

今回のシステムでは，w=0.3 とした．

STEP4 における DCT 係数の操作による画像の劣化の程度には画像ごとに大きな差がでるため，STEP4 では比較的大きく画像を壊しておき，STEP6 の処理によってオリジナル画像の特徴を補完してバランスをとっている．STEP4 において各画像に応じて適切な DCT 係数の調整が行えれば，STEP6 の処理は必要ない．それでも極端に認識しにくい画像あるいは極端に認識しやすい画像が作成される場合は，手動でこれを除外することとする．

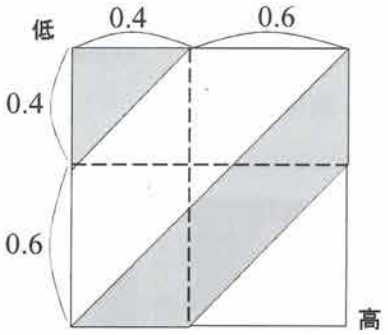
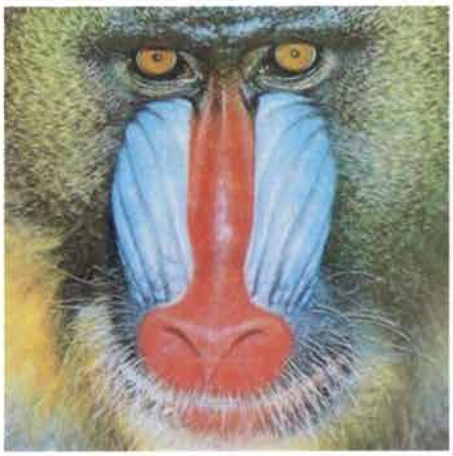
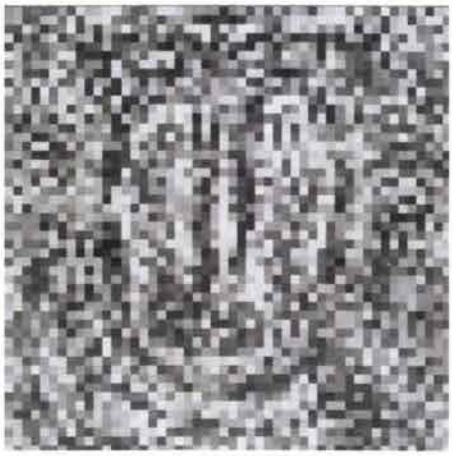


図 3-1 不鮮明化処理における DCT 係数の変更範囲

上記の手順に従ってオリジナル画像から得られる不鮮明画像の例を図 3-2 に示す．図 3-2 の左側の画像はカラーのオリジナル画像であり，図 3-2 の右側は不鮮明処理後の画像である．不鮮明化画像は，オリジナル画像と比較して，モザイク化や DCT 係数の操作によって大きく情報量が削減されているが，ある程度の特徴が残されていることが見てとれる．

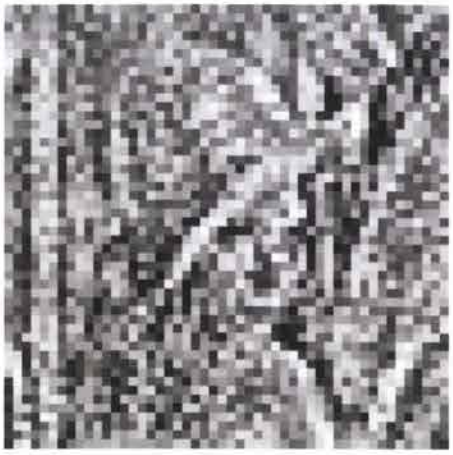


(a)　オリジナル画像



(b)　不鮮明化画像

(a)　オリジナル画像



(b)　不鮮明化画像

(a)　オリジナル画像

(b)　不鮮明化画像

図 3-2　不鮮明化画像の例

3.3 基本的な認証手順

不鮮明化画像方式におけるパス画像の登録フェーズおよび認証フェーズの基本的な手順は以下のとおりである.

● 登録フェーズ

STEP1.認証システムはユーザに複数のオリジナル画像を提示する.

STEP2.ユーザはパス画像として用いたい画像を選択する.

STEP3.認証システムは，ユーザが選択した画像に対応する不鮮明化画像をユーザに提示する.

STEP4.ユーザは，オリジナル画像と不鮮明化画像を比較しながら記憶する.

STEP5.ユーザが納得すれば，認証システムは当該不鮮明化画像をパス画像として登録する.

● 認証フェーズ

STEP1.認証システムはユーザに対して，当該ユーザのパス画像を含む複数枚の不鮮明化画像をランダムに選び，規則正しく並べて提示する. (図 3-3)

STEP2.ユーザは，提示された不鮮明化画像の中から，自身のパス画像を探し出す.

STEP3.ユーザが正しい位置（画像）を選択することができれば認証成功とする.

要求される認証強度に応じて，パス画像の枚数，認証時に提示される不鮮明化画像の枚数，認証フェーズにおける選択の繰り返し回数（ターン数）などが定められる. 不鮮明化画像をパス画像として用いることを除くと，根本的には 2 章で述べた既存の画像の再認を利用する認証方式と同様の手順である.

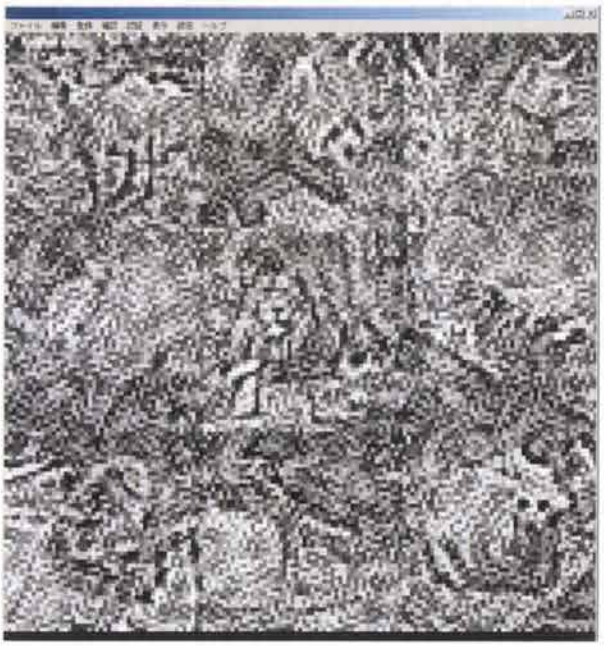


図 3-3　9 択認証システムにおける認証画面の例

3.4 不鮮明化画像方式の有効性と課題

不鮮明化画像方式は，既存の画像認証方式（オリジナル画像をパス画像として利用する再認型画像認証方式）と比べ，正規ユーザの認証成功率を高く維持したまま，攻撃耐性についても有望な結果を残している[HIM05].

文献[HIM05]の 4.1 節では，不鮮明化画像方式における本人認証率について調査を行っている．当該認証実験では，ユーザが登録するパス画像は 4 枚である．認証時には，9 枚の画像の中から 1 枚のパス画像を選択する操作を 4 ターン繰り返し，4 回連続でパス画像の選択に成功したときのみ認証成功とする．システムは，1 ターン目の認証画面を用意するにあたり，登録した 4 枚のパス画像の中から 1 枚をランダムに選ぶ．同時に，パス画像以外の不鮮明化画像の中からランダムに 8 枚を選び，計 9 枚の不鮮明化画像をランダムな配置で表示する．2 ターン目の認証画面においては，残りの 3 枚のパス画像の中からランダムに選ばれた 1 枚が，9 枚の不鮮明化画像の中に含まれることになる．3 ターン目は残り 2 枚のパス画像のいずれかが，4 ターン目は最後に残ったパス画像が選ばれ，それぞれ 9 択の認証画面が構成される．このように，9 枚の不鮮明化画像の中には，いずれかのパス画像が必ず 1 枚だけ含まれるようになっている．当該実験では，パス画像登録日から 1 日後，8 日後に，ほぼ確実に被験者は本人認証に成功していることが報告されている．8 日後に一回だけ認証に失敗したケースがあったが，失敗をした被験者からの聞き取り調査からは，9 択の中にパス画像と似た画像が登場したために，うっかり誤選択してしまったが，選択後すぐに失敗に気づいたということであった．このように，不鮮明な画像を利用しても，ユーザの画像の記憶や識別に対する負荷が少ないことが確認できる．

一方，攻撃耐性については，覗き見攻撃者（実験者の認証行為を横で見ていた実験参加者）にとって非常に有利な条件である 2 択認証システム[12]を用いて覗き見実験が実施されているが，既存の画像認証方式のなりすまし成功率が 100%であったのに対し，不鮮明化画像方式ではなりすまし成功率を 90%に下げることができている．また文献[HIM05]では，パス画像の情報を他人に言葉で伝えることができるかどうかを測るパス画像漏洩の実験も実施されている．攻撃者にパス画像の情報[13]を言葉で与えた上で，2 択認証システムによる認証試行を行わせたところ，既存の画像認証方式の認証成功率が 100%であったのに対し，不鮮明化画像方式での認証成功率は 74%であった．囮画像の枚数を増やすことによって，これらのなりすまり成功率は更に低下するものと考えられる．

---

[12] ユーザは 1 枚のパス画像を記憶する．認証画面に提示される画像は，パス画像と囮画像 1 枚の計 2 枚である．パス画像を選択することができたユーザを正規ユーザとして認証する．

[13] 文献[HIM05]では動物の画像を不鮮明化したものをパス画像として用いたため，「動物の種類（例：犬）」，「正面か，横向きか」，「全身か，一部か」，「座っているか，立っているか」に関する情報を攻撃者に言葉で伝えた．

このように，不鮮明化画像方式は，正規ユーザの記憶負荷を低く抑えながら，覗き見攻撃や言葉によるパス画像の漏えいに対する耐性についても有望な結果を残している．しかしながら，不鮮明化画像方式では，毎回の認証におけるパス画像は常に同じものが使われる方式となっているため，攻撃者が覗き見した認証画面の中のパス画像がなりすましの際の認証画面にも必ず表示されることになる．不鮮明な画像であっても，同じパス画像を毎回の認証で用いている限り，攻撃者にそれを覚えられる可能性が残る．同じ理由で，カメラで盗撮しておいた不鮮明化画像と同じものを選ぶという攻撃に対しても脆弱性が残る．また，不鮮明化画像方式においても，囮画像の問題は未解決のままとなっている．

4章　言語手がかり付き再認方式
（RVC 方式：Recognition with Verbal cue）

本章では，正規ユーザに m 枚のパス画像を記憶させた上で，1 回の本人認証にあたって n 枚（m＞n）のパス画像を用いて認証を行うという対策によって，不鮮明化画像方式の拡張を図る（以降，m-n 対策と呼ぶ）．この結果，カメラを用いた覗き見であっても，攻撃者がパス画像を特定するためには複数回の覗き見が必要となる．ただし，パス画像の増加にともなうユーザの負荷増大を緩和する工夫なくしては，その導入は難しい．そこで，正規ユーザのみが効果的に利用可能な手がかりを認証時に与えることで，正規ユーザの負荷が少ない m-n 対策を実現する．

4.1　コンセプト

覗き見攻撃耐性の強化のためには，認証の度異なるパス画像セットを利用できることが望ましい．そこで本方式では，正規ユーザに m 枚のパス画像を記憶させた上で，1 回の本人認証にあたって n 枚（m＞n）のパス画像を用いて認証を行うという運用（m-n 対策）を導入する．しかし，正規ユーザに一回の認証に必要なパス画像の枚数よりも多くのパス画像を記憶させることは，正規ユーザの負荷の増大につながる．そのため，m-n 対策の導入に対してはユーザ負荷増大の緩和対策が必須となる．

そこで本方式では，パス画像を思い出すにあたっての手がかりとなる言語情報を認証時に提示する（RVC 方式：Recognition with Verbal Cue）ことにより，m-n 対策を導入したときのユーザ負荷の増大を抑制する．RVC 方式では，スキーマを有する正規ユーザは，手がかり情報によって認証時の再認および想起の促進が期待される．ここで，画面に提示される手がかりは正規ユーザだけでなく，覗き見攻撃者にも与えられることになる．しかし，不鮮明化画像の特長を評価した実験（文献[HIM05]の 3.4 節）から，不鮮明化画像であれば，覗き見攻撃者にパス画像の内容を言葉で伝えた場合であってもパス画像の推測成功率を低下させることができるという結果が得られている．この不鮮明化画像の特長から，認証時にパス画像に対する手がかり情報を言葉で与えたとしても，攻撃者にはその情報を有効に活用できないことが予想できる．

手がかり情報の使用に関しては，不鮮明化画像の研究[HIM05]の今後の課題の中で簡単に触れられてはいたものの，覗き見対策のための方法として考えられていたわけではなく，不鮮明化画像方式におけるユーザの画像認識負荷の軽減を目的としたものであった．本研究における RVC 方式は，m-n 対策と組み合わせることで，ユーザの画像記憶負荷および画像認識負荷の軽減を果たしつつ，不鮮明化画像方式の覗き見攻撃耐性を効果的に向上させることを狙っている．

4.2 認証方式

本節では，RVC 方式の認証手順を簡単に紹介する．基本的な手順は不鮮明化画像方式の認証手順と同じである．異なる点は，m-n 対策が導入されている点，および，パス画像のヒントが言語手がかりによって与えられる点である．

● 登録フェーズ

STEP1. 認証システムはユーザに複数のオリジナル画像を提示する．

STEP2. ユーザはパス画像として用いたい画像を選択する．

STEP3. 認証システムは，ユーザが選択した画像に対応する不鮮明化画像をユーザに提示する．同時に，それに対する手がかり情報もいっしょに提示される．手がかり情報としては，例えば動物の画像の場合，「犬」や「猫」といった言語情報が手がかりとして与えられる．

STEP4. ユーザは，オリジナル画像と不鮮明化画像を比較しながら記憶する．

STEP5. ユーザが納得すれば，認証システムは当該不鮮明化画像をパス画像として登録する．

STEP6. ユーザが m 枚のパス画像を覚えるまで STEP1～STEP5 を繰り返す．

● 認証フェーズ

STEP1. 認証システムはユーザに対して，当該ユーザのパス画像を含む複数枚の不鮮明化画像をランダムに選び，規則正しく並べて提示する．同時に，現在表示されているパス画像に対する言語手がかりも一緒に提示する．

STEP2. ユーザは，与えられた言語手がかりを元に，現在表示されているパス画像を絞り込んだ上で，提示された不鮮明化画像の中から，自身のパス画像を探し出す．

STEP3. STEP1～STEP2 を n 回（m＞n）繰り返し，すべてのターンでユーザが正しい位置（画像）を選択することができれば認証成功とする．

要求される認証強度に応じて，パス画像の枚数，認証時に提示される不鮮明化画像の枚数，認証フェーズにおける選択の繰り返し回数（ターン数）などが定められる．登録画面例を図 4-1 および図 4-2 に，認証画面例を図 4-3 に示す．

現在認証画面に表示されているパス画像に対する手がかり情報が提示されることにより，正規ユーザにのみ効果的にパス画像の想起・再認が促され，パス画像を容易に選択することが可能となっている．攻撃者が正規ユーザの認証を覗き見たとしても，次の認証で同じパス画像が現れるとは限らず，カメラを用いた覗き見であっても，パス画像を特定するためには複数回の覗き見が必要となる．本方式は正規ユーザが記憶すべきパス画像の枚数が増えるほどその効果が期待される．

なお，図 4-4 に示すように，オリジナル画像を用いた従来の画像認証方式に手がかり情報を与えた場合は，攻撃者に答え（パス画像）を教えていることと等しく，認証方式として成立し得ない．本改良が，不鮮明な画像だからこそ実現する，画期的な方式であることに注目されたい．図 4-5 に RVC 方式の概観を示す．

図 4-1　登録画面（不鮮明化画像表示時）

図 4-2　登録画面（オリジナル画像表示時）

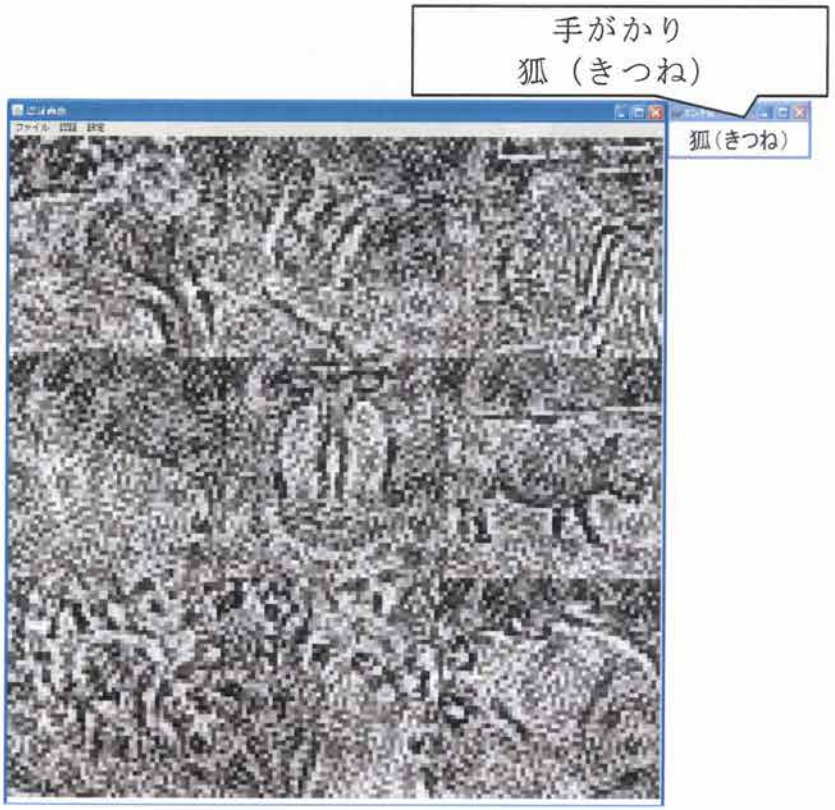


図 4-3　認証画面

図 4-4　認証画面（オリジナル画像）

図 4-5　RVC 方式の概観

4.3　RVC 方式の評価実験

RVC 方式の有効性を，実験により評価する．被験者は本学情報系学部学生 10 名である．本実験に利用した画像は，様々な種類の動物が写っている背景つきの写真画像 80 枚である．実験に用いた動物の写真画像はインターネット上で公開されている画像などから収集した．なお，本論文の図中に示した写真画像は，著作者により自由な使用が認められている画像である．

4.3.1　本人認証実験

m-n 対策の導入（正規ユーザに m 枚のパス画像を記憶させた上で，1 回の本人認証にあたって n 枚（m＞n）のパス画像を用いて認証を行う）によって増大されるユーザの負荷が，手がかりの提示によってどの程度抑えることができるのかについて，本人認証率および認証時間の比較を通じて検証する．不鮮明化画像方式における認証実験は，文献[HIM05]の実験結果を引用する．また，比較のために，RVC 方式から手がかりの提示を除去したシステム（不鮮明化画像方式に m-n 対策のみを導入した方式．以下，比較方式 1 と呼ぶ）を構築して，RVC 方式と合わせて認証成功率および認証時間について調査する．

● **実験環境**

RVC 方式：

正規ユーザが記憶すべきパス画像の枚数は 10 枚である．認証時には，9 枚の画像の中から 1 枚のパス画像を選択する操作を 4 ターン繰り返し，4 回連続でパス画像の選択に成功したときのみ認証成功とする．すなわち，m＝10，n＝4 である．システムは，1 ターン目の認証画面を用意するにあたり，登録した 10 枚のパス画像の中から 1 枚をランダムに選ぶ．同時に，パス画像以外の不鮮明化画像の中からランダムに 8 枚を選び，計 9 枚の不鮮明化画像をランダムな配置で表示する．画面に表示される不鮮明化画像 1 枚の大きさは 300×300 pixel である．2 ターン目の認証画面においては，残りの 9 枚のパス画像の中からランダムに選ばれた 1 枚が，9 枚の不鮮明化画像の中に含まれることになる．3 ターン目は残り 8 枚のパス画像のいずれかが，4 ターン目は残り 7 枚のパス画像のいずれかが，9 枚の不鮮明化画像の中に含まれることになる．このように，9 枚の不鮮明化画像の中には，いずれかのパス画像が必ず 1 枚だけ含まれるようになっている．認証画面の横には，現在表示されているパス画像に対するヒントとなる言語手がかりが表示される．言語手がかりは，パス画像に写っている動物の種類の名前（例：犬，馬など）とした．図 4-3 が RVC 方式における認証画面例である．

比較方式 1：

正規ユーザが記憶するパス画像は 10 枚である．認証時には，9 枚の画像の中から 1 枚のパス画像を選択する操作を 4 ターン繰り返し，4 回連続でパス画像の選択に成功したときのみ認証成功とする．すなわち，m＝10，n＝4 である．言語手がかりは表示されない．図 3-3（図 4-3 における手がかり情報を削除したもの）が比較方式 1 における認証画面例である．

不鮮明化画像方式：

不鮮明化画像方式の研究[HIM05]で用いられた実験環境である．正規ユーザが記憶するパス画像は 4 枚である．認証時には，4 枚の画像の中から 1 枚のパス画像を選択する操作を 4 ターン繰り返し，4 回連続でパス画像の選択に成功したときのみ認証成功とする．すなわち，m＝4，n＝4 である．言語手がかりは表示されない．図 3-3（図 4-3 における手がかり情報を削除したもの）が不鮮明化画像方式における認証画面例である．

● **実験方法**

10 名の被験者を，5 名ずつ 2 グループに分け，それぞれ実験群 A，実験群 B とする．実験群 A では RVC 方式→比較方式 1，実験群 B では比較方式 1→RVC 方式，という順番で認証実験を行う．以下では実験群 A を例にとり，実験手順を示す．

STEP1. 実験初日に登録フェーズを行い，10 枚のパス画像を登録し，記憶してもらう．

STEP2. 登録日から 1 日後，8 日後に，RVC 方式による認証実験を実施する．RVC 方式で利用するパス画像の手がかりは，パス画像に写っている動物の種類の名前（例：犬，馬など）とした．

STEP3. 被験者には各認証実施日に 5 回ずつ RVC 方式による認証実験を行ってもらい，認証成功率，認証時間を測定する．パス画像の選択に迷ったときには，少しでも答えに近いと思う画像を選択させた．

STEP4. RVC 方式の 8 日後の認証実験の後，登録フェーズを行い，RVC 方式の実験で利用した 10 枚のパス画像とは異なる画像 10 枚を，パス画像として再登録し，記憶してもらう．

STEP5. 登録日から 1 日後，8 日後に，比較方式 1 による認証実験を実施する．比較方式 1 では，パス画像に対する手がかり情報は提示されない．

STEP6. 被験者には各認証実施日に 5 回ずつ比較方式 1 による認証実験を行ってもらい，認証成功率，認証時間を測定する．パス画像の選択に迷ったときには，少しでも答えに近いと思う方を選択させた．

● **実験結果**

表 4-1　本人認証実験の結果

			不鮮明化画像方式 [HIM05] (m＝4，n＝4，手がかり＝無)		比較方式 1 (m＝10，n＝4，手がかり＝無)		RVC 方式 (m＝10，n＝4，手がかり＝有)	
			1 日後	8 日後	1 日後	8 日後	1 日後	8 日後
認証成功率			50/50 (100%)	49/50 (98%)	45/50 (90%)	41/50 (82%)	50/50 (100%)	49/50 (98%)
ターン毎の選択成功率			200/200 (100.0%)	199/200 (99.5%)	195/200 (97.5%)	189/200 (94.5%)	200/200 (100.0%)	199/200 (99.5%)
ターン毎の回答時間	選択失敗を含む	平均（秒）	8.26	7.10	10.82	16.46	6.44	7.64
		標準偏差（秒）	11.68	8.78	13.25	28.75	6.38	11.49
		最短値（秒）	1.19	1.06	1.64	0.20	1.50	1.30
		最長値（秒）	56.50	67.13	91.06	272.98	49.13	104.53
	選択失敗を含まない	平均（秒）	8.26	6.80	9.69	14.05	6.44	7.15
		標準偏差（秒）	11.68	7.72	10.92	20.87	6.38	9.22
		最短値（秒）	1.187	1.062	1.641	1.313	1.5	1.30
		最長値（秒）	56.50	66.50	81.34	174.06	49.13	103.58

実験結果を表 4-1 に示す．不鮮明化画像方式の結果は，文献[HIM05]の 4.1 節の実験結果の再掲である．表中，「認証成功率」は，各認証試行において認証に成功した（1 回の認証において，4 ターンのパス画像選択全てに成功した）割合である．「ターン毎の成功率」は，全 20 ターン（5 回の試行×4 ターン）のうち，パス画像の選択に成功したターン数の割合である．また，ターン毎のパス画像選択にかかった回答時間の平均，標準偏差，最短時間，最長時間，をそれぞれ「ターン毎の回答時間の平均」，「ターン毎の回答時間の標準偏差」，「ターン毎の回答時間の最短値」，「ターン毎の回答時間の最長値」として記した．なお，回答時間については，失敗した際の選択時間を含める場合とそうでない場合とに分けて示している．

1 日後，8 日後とも，RVC 方式の本人認証率は，不鮮明化画像方式と同様，100%を維持している．比較方式 1（手がかり無）の認証率が低下している事実より，手がかり情

報を用いることで，認証画面に表示されているパス画像に対するスキーマの想起が促進され，認証成功率の低下が抑えられたのだと推測できる．

回答時間については，RVC 方式は不鮮明化画像方式とほぼ同等であることが確認できる．一方，比較方式 1（手がかり無）ではその増加が確認できる．よって，手がかり情報により想起すべきスキーマが絞られ，囮画像の中からパス画像を見つける作業が容易になったのだと考えられる．

4.3.2 覗き見実験

攻撃者が正規ユーザの認証作業を覗き見たとしても，次の認証で同じパス画像が現れるとは限らないため，m-n 対策の導入が覗き見攻撃耐性を大きく向上させることは容易に想像ができる．しかし，RVC 方式では，m-n 対策の導入とともに，言語手がかりの提示を行っている．文献[HIM05]の 3.4 節の結果からもわかるとおり，攻撃者は言語手がかりを十分活用することはできないと考えられるが，言語手がかりの提示が覗き見攻撃の脅威をどれほど増加させてしまうかについて実験により確認する必要がある．

● 実験環境

RVC 方式：

正規ユーザが記憶するパス画像は 10 枚である．認証時には，2 枚の画像の中から 1 枚のパス画像を選択する操作を 1 ターンだけ行い，パス画像の選択に成功したときのみ認証成功とする．すなわち，m＝10，n＝1 である．システムは，認証画面を用意するにあたり，登録した 10 枚のパス画像の中から 1 枚をランダムに選ぶ．同時に，パス画像以外の不鮮明化画像の中からランダムに 1 枚を選び，計 2 枚の不鮮明化画像をランダムな配置で表示する．画面に表示される不鮮明化画像 1 枚の大きさは 300×300 pixel である．認証画面の横には，現在表示されているパス画像に対するヒントとなる言語手がかりが表示される．言語手がかりは，パス画像に写っている動物の種類の名前（例：犬，馬など）とした．図 4-6 が RVC 方式における 2 択の認証画面例である．

不鮮明化画像方式：

不鮮明化画像方式の文献[HIM05]の中の 3.3 節で用いられた実験環境である．正規ユーザが記憶するパス画像は 1 枚である．認証時には，2 枚の画像の中から 1 枚のパス画像を選択する操作を 1 ターンだけ行い，パス画像の選択に成功したときのみ認証成功とする．すなわち，m＝1，n＝1 である．システムは，認証画面を用意するにあたり，登録した 1 枚のパス画像とパス画像以外の不鮮明化画像の中からランダムに 1 枚を選び，計 2 枚の不鮮明化画像をランダムな配置で表示する．言語手がかりは表示されない．図 4-6 における手がかり情報を削除したものが不鮮明化画像方式における 2 択の認証画面例である．

2 択システムとした理由は，覗き見攻撃者に非常に有利な条件であっても本方式が有効であるかを測るためである．また，覗き見攻撃耐性に対する m-n 対策の影響と手がかり情報提示の影響を個別に評価するためには，不鮮明化画像方式に m-n 対策のみを導入した方式（4.3.1 節の実験における比較方式 1．本実験においては m=10, n=1，手がかり＝無），および，不鮮明化画像方式に手がかり情報の提示のみを導入した方式（以下，比較方式 2 と呼ぶ．本実験においては m=1, n=1，手がかり＝有）を対象とした覗き見攻撃実験についても実施すべきである．しかし，4.3.1 節の実験結果より，比較方式 1 は，本人認証成功率および認証時間において RVC 方式および不鮮明化画像方式に匹敵するパフォーマンスが得られないことが判明しているため，ここでは比較方式 1 に対する実験は省略した．また，比較方式 2（m＝1，n＝1，手がかり＝有）の覗き見攻撃成功率は，「不鮮明化画像方式（m=1, n=1，手がかり＝無）の覗き見攻撃成功率 P1」と「パス画像の内容を言葉で伝えた際の不鮮明化画像方式に対するパス画像の推測成功率 P2（文献[HIM05]の 3.4 節の実験結果より 0.74（74%））」を用いて 1－(1－P1)×(1－P2)によって試算できることから，ここでの実験は省略した．

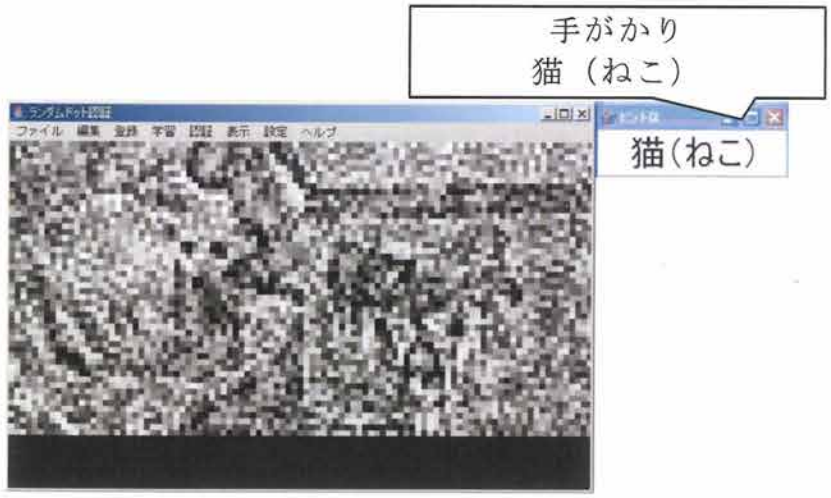


図 4-6　2 択の認証画面

● **実験方法**

4.3.1 節と同じ被験者（10 名）で，不鮮明化画像方式と RVC 方式のシステムを用いて実験を行う．10 名の被験者全員が両方式に対して覗き見によるなりすましを行う．RVC 方式では，被験者はパス画像の選択動作に加え，認証画面に提示される手がかり情報についても覗き見ることができ，なりすましの際に両者を併せて活用することができる．

以下に RVC 方式を例に攻撃実験の手順を示す．

STEP1. 各被験者は，実験実施者が認証フェーズを行う様子を，画面がよく見える位置から覗き見る（図 4-7）．
STEP2. その直後に，被験者には実験実施者へのなりすましを試みてもらう．
STEP3. 各被験者につき，同じパス画像セットについて 5 回ずつ認証試行を行ってもらった．

i 回目の認証試行で覗き見したパス画像が，i＋1 回目以降の認証試行で登場するケースが起こり得るので，認証試行の回数を重ねるほど被験者は有利になっていく．不鮮明化画像方式の文献[HIM05]を参考に，各認証試行において，被験者の覗き見時間は 5 秒に設定した．

なお STEP3 において，不鮮明化画像方式の実験[HIM05]では同じパス画像セットは用いず， STEP1~STEP2 を繰り返すたびにパス画像をランダムに変更している．そのため，RVC 方式における実験の方が攻撃者により有利な条件で実験を行っているといえる．

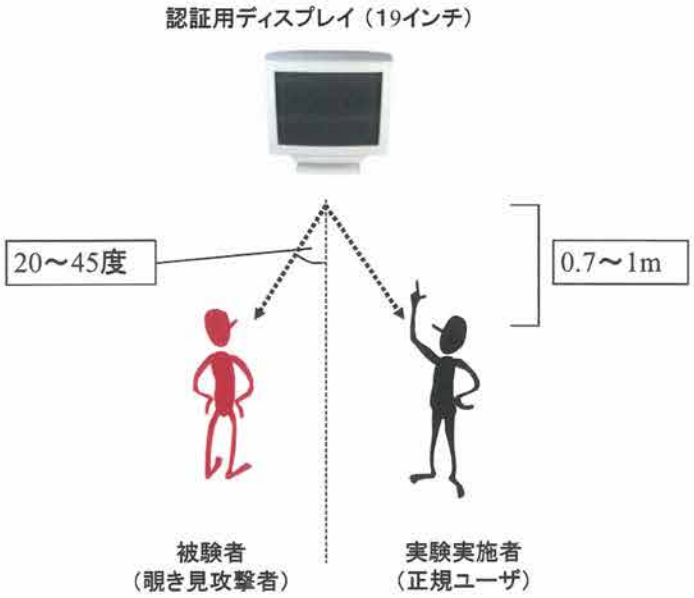


図 4-7　被験者と認証システムの位置関係

● **実験結果**

実験の結果を表 4-2 に示した．不鮮明化画像方式の結果は，文献[HIM05]の中の 3.3 節の実験結果の再掲である．表中，「成功率」は 10 人の各被験者につき 5 回ずつ行った認証試行の全体の成功率（なりすまし成功率）を表している．

表 4-2　覗き見によるなりすまし成功率

	不鮮明化画像方式	RVC 方式
成功率	46/50 (92%)	39/50 (78%)

比較方式 2 のなりすまし成功率が約 98%[14]と試算されることから，m-n 対策の効果によって RVC 方式のなりすまし成功率が不鮮明化画像方式のそれよりも 14%低く抑えられたことがわかる．

しかし，手がかりを与えず m-n 対策のみを導入する比較方式 1 におけるなりすまし成功率は，理論的には約 54%[15]の確率であり，手がかりの提示により，m-n 対策の効果がある程度薄れてしまっていることがわかる．このことからも今後は，手がかりの提示の工夫や，攻撃者が手がかりを全く活用できないような不鮮明化アルゴリズムの検討が必要であろう．

4.4　RVC 方式についての総合的な考察

4.4.1　利便性

m-n 対策の導入は，一回の認証に必要なパス画像の枚数よりも多くのパス画像を正規ユーザに記憶させるため，認証時のユーザの負荷が増大してしまう．しかし，RVC 方式では言語手がかりを活用することで，認証時のユーザの負荷を不鮮明化画像方式とほぼ同等レベルにまで抑えることができている．

同じ種類の動物に対しては同じ言語手がかりが与えられるシステムであるため，そのような場合には，ユーザが戸惑う可能性もある．パス画像ごと特徴的なラベルを正規ユーザ本人にタグ付けしてもらうことで，手がかりとパス画像との紐付けをより強固にすることも可能だと考えられる．

---

[14] 不鮮明化画像方式のなりすまし成功率 P1=0.92（92%），パス画像の内容を言葉で伝えた際のパス画像推測成功率 P2=0.74（74%）より 1－(1－P1)×(1－P2)を算出することができる．

[15] 覗き見直後に同じパス画像が現れる確率は 1/m（m は正規ユーザが記憶しているパス画像の枚数）であり，その時攻撃者は P1=0.92（92%：不鮮明化画像方式のなりすまし成功率）の確率でそのパス画像を選択することができると仮定すると，パス画像が表示されない時は，当て推量による回答しかあり得ないため，覗き見によるなりすまし成功確率は P1×1/m + 1/2 × (1-1/m) と計算できる．

4.4.2 安全性

m-n 対策は覗き見攻撃耐性への寄与は大きい．しかし，RVC 方式では，m-n 対策における記憶負荷を軽減するために，言語手がかりを認証時に提示する．文献[HIM05]の 3.4 節の結果からもわかるとおり，攻撃者は言語手がかりを十分活用することはできないものの，m-n 対策のみの導入を行った比較方式 1 における覗き見攻撃耐性の試算と比べ，覗き見攻撃耐性が劣化していることから，攻撃者は言語手がかりをある程度活用できていることがわかる．しかし，それでもなお RVC 方式に対する覗き見攻撃によるなりすまし成功率は，不鮮明化画像方式のそれよりも，14%も低い．よって，手がかり情報の提示をしたとしても，m-n 対策の導入効果が認められる結果が得られている．

また RVC 方式では，再認型画像認証において大きな問題である Exhaustive 攻撃や Intersection 攻撃に対してもある程度の効果が期待できる．

Exhaustive 攻撃とは，毎回の認証で認証画面中の画像一枚一枚に当たりをつけ，「その画像を選択して認証に失敗したならば，その画像はパス画像ではない」というように，パス画像の候補を徐々に絞っていく攻撃である．この攻撃に対して，認証画面に一度に複数のパス画像が表示されるような拡張を考えてみることにする．例えば，認証画面には 3 つのパス画像（「犬」「猫」「猿」）と 6 つの囮画像が表示されている．その際，言語手がかりは「猫」であったとし，攻撃者は「猫」以外のパス画像を選択して認証に失敗したとする．この時，従来の方式（既存の再認型の画像認証方式）であれば，攻撃者が選択した画像はパス画像ではないとして，パス画像の候補から除外することができる．しかし本拡張においては，攻撃者は囮画像を選択して失敗したのか，異なるパス画像（手がかりが指し示すパス画像以外のパス画像）を選択して失敗したのかまでは判断できないため，パス画像の候補を絞り込むことが困難になる．ただし，本拡張が利便性にどの程度影響を与えるのかについても評価が必要である．

Intersection 攻撃とは，毎回の認証で出現頻度の高い画像をパス画像の候補として徐々に絞っていく攻撃である．従来の方式（毎回同じパス画像が表示される方式）では，認証試行を 2，3 度見るだけで，常に認証画面に表示される画像はパス画像であると容易に特定することができる．一方 RVC 方式では，毎回同じパス画像が表示されるわけではないため，パス画像の特定には，より多くの認証試行を見る必要があり，Intersection 攻撃に対する耐性は増加すると考えられる．

まとめると，RVC 方式は不鮮明化画像方式と比べ，利便性（パス画像の想起・再認のし易さ）を同程度に保ったまま，覗き見攻撃（カメラ撮影を含む）などに対する耐性を向上させることができたといえる．

5章　暗示・応答型画像認証方式
（Q&R 方式：Cue & Response）

本章では，覗き見攻撃およびカメラ撮影を用いた攻撃にも一定レベル耐性を画像認証方式に持たせるためのもう一つの手段として，再認型画像認証の C&R 化を図る．ただし，人間の計算能力には限界があるため，チャレンジからのレスポンス生成に暗号計算が必要となる通常の C&R 型認証のスキームをそのまま画像認証に適用することは不可能である．そこで，チャレンジの意味を隠す（正規ユーザ本人にしかチャレンジを理解することができないようにする）というアプローチを採ることによって，簡素なレスポンス生成処理を採用した場合であっても，あるレベルの安全性が担保される暗示・応答（Q&R）型画像認証を構築する．カメラを用いた覗き見であっても，攻撃者は（チャレンジおよびレスポンスを覗き見ることはできるが）チャレンジの意味が分からず，パス画像の特定が困難となる．

5.1　コンセプト

2.4.6.1 節で示した従来の C&R 型画像認証方式には，その安全性を維持したまま，レスポンス生成処理を簡素にしたいという要望がある．一方，2.4.6.4 節で述べたように，Sasamoto らは物理的にチャレンジを隠すことで簡素なレスポンス生成を実現した方式を提案している．ただし，Sasamoto らの方式では，非常に特殊なデバイス（触覚デバイス）を必要とし，その実用性に疑問が残る．そこで本論文では，チャレンジの意味を隠す（正規ユーザ本人にしかチャレンジを理解することができないようにする）というアプローチを採ることによって，認知心理学的にチャレンジを隠蔽（正規ユーザ本人にしか伝わらないようにする）することで，特殊なデバイスを用いなくともレスポンス生成が容易な C&R 型画像認証を実現する．

具体的には，「不鮮明なパス画像に関する情報を言葉で与えただけでは，スキーマを持たない攻撃者はパス画像を特定するに足る情報量を得ることができない」という不鮮明化画像の特長[HIM05]を活用し，認証の度に異なる質問（チャレンジ）を正規ユーザのみが理解することができる形で提示する．本方式においては，認証の度に異なる質問が正規ユーザのみが知覚できる形で提示される．本論文では，このような暗示的なチャレンジを「キュー（Cue）」と呼び，本方式を暗示・応答型画像認証方式と表現する．本論文では，Q&R 方式（Cue & Response）と略記する．Q&R 方式は，正規ユーザであれば直感的な処理によってキューに対するレスポンスを生成することができ，かつ，攻撃者による有限回の覗き見に対する耐性を持つ，という 2 つの特長を有する C&R 型画像認証方式となっている．

5.2 認証方式

4 章では，「不鮮明なパス画像に関する情報を言葉で与えただけでは，スキーマを持たない攻撃者はパス画像を特定するに足る情報量を得ることができない」という不鮮明化画像の特長[HIM05]を活用し，m-n 対策導入時のユーザの負荷を，言語手がかりを認証時に提示することで軽減する方式（RVC 方式）を提案した（図 4-5）．

本章ではこのアイデアを拡張し，4 章で用いられた手がかり情報の提示を，正規ユーザのみにチャレンジ（キュー）を認識させる手段として利用する（図 5-1）．キューは，パス画像に対する部位情報を言語手がかりで示したもの（例：「左目」，「右耳」，「尻尾」，「左前足」等）であり，認証の度に変化する．ユーザは，囮画像に紛れているパス画像を見つけた上で，キューによって指示された部位に対応する場所をクリックすることによってレスポンスを返す．

スキーマを持たない攻撃者には，不鮮明化画像の意味を認識することは困難であるため，指示された部位に対応する場所を正しくクリックすることは容易なことではない．一方，不鮮明化画像の意味（スキーマ）を知っている正規ユーザであれば，指示された部位をクリックすることは容易である．キューにより指定される部位は認証の度に変化する（ある認証フェーズで「左耳」をクリックしている瞬間を覗き見られたとしても，次回の認証においては例えば「左前足」という指示に変わる）ため，覗き見攻撃に対する耐性も増加する．また，この方法は，パス画像選択の総当たり数を増やすことを可能にするというメリットもある．

図 5-1　言語手かがリによって選択する部位を

指示する認証方式の概観

しかし，この方法においては，例えば「左目」というキューに対する正規ユーザのレスポンスを覗き見ていた攻撃者は，「正規ユーザがクリックした場所の付近が，正規ユーザが認識している左目である」という情報を得ることができてしまう．攻撃者は，複数回これを繰り返すことにより，正規ユーザが認識する不鮮明化画像の全体像（例えば動物の写真画像の場合，顔，手，足，胴体の位置関係等）を認識することが可能かもしれない．

そのため，キュー（部位情報）を言語手がかりとして直接的に示すのではなく，別の不鮮明化画像中の部位としてユーザに暗示的に示す方法を採用する．以降，キューを示すために用いられる不鮮明化画像を参照画像と呼ぶことにする．

正規ユーザはパス画像登録時に，参照画像とそれに対応するオリジナル画像も一緒に記憶し，参照画像のスキーマを学んでおく．すなわち，パス画像に対するスキーマと参照画像に対するスキーマの両方を学習しておく．認証時には，システムはパス画像と複数の囮画像を認証ウインドウに提示する（図 5-2 左）．同時に，参照画像中の任意の部位（以降，パス部位と呼ぶ）を選び，その位置に目印をつけた形でこれを参照ウインドウに表示する（図 5-2 右）．参照画像のスキーマを有する正規ユーザは，参照画像中の目印からパス部位を認識することができる．また，正規ユーザはパス画像のスキーマも学習しているので，認証ウインドウの中からパス画像を見つけた上で，パス画像におけるパス部位をクリックすることが可能である．すなわち，参照画像上の目印によって提示されたパス部位が「右足」であったとすると，正規ユーザはパス画像の「右足」付近をクリックすることになる．

攻撃者は参照画像に対するスキーマを有していないため，参照画像上の目印を覗き見たとしても，その位置に何が映っているのかを類推することは容易ではない．さらに，攻撃者はパス画像に対するスキーマも持っていないため，正規ユーザのレスポンスを覗き見たとしても，クリックの位置に何が映っているのかを類推することも難しい．これにより，パス部位を攻撃者に理解できない形で正規ユーザにのみ提示することが可能となる．

パス部位の位置は，毎回の認証でランダムに決定される．参照画像上に目印として提示されるパス部位が毎回の認証のキューであり，ユーザによるパス画像上のパス部位のクリックがキューに対するレスポンスである．図 5-3 に提案方式（Q&R 方式）の概観を示す．

言語手がかりを用いる方式においては，覗き見によって得られたパス画像のパス部位と言語手がかりとの対応情報（例えば，「パス画像中の座標位置(X1,Y1)が眼」）から，攻撃者は「鼻は眼の下のあたりにある」，「顔の下に体がある」などというように，パス画像の構造を予想していくことが可能である．しかし参照画像を用いる方式では，攻撃者が覗き見によってパス画像と参照画像のパス部位の対応情報を得たとしても，それ

は「無意味に見えるもの」と「無意味に見えるもの」との対応付けでしかないため，そこから画像の構造を推測していくことは困難になる[16].

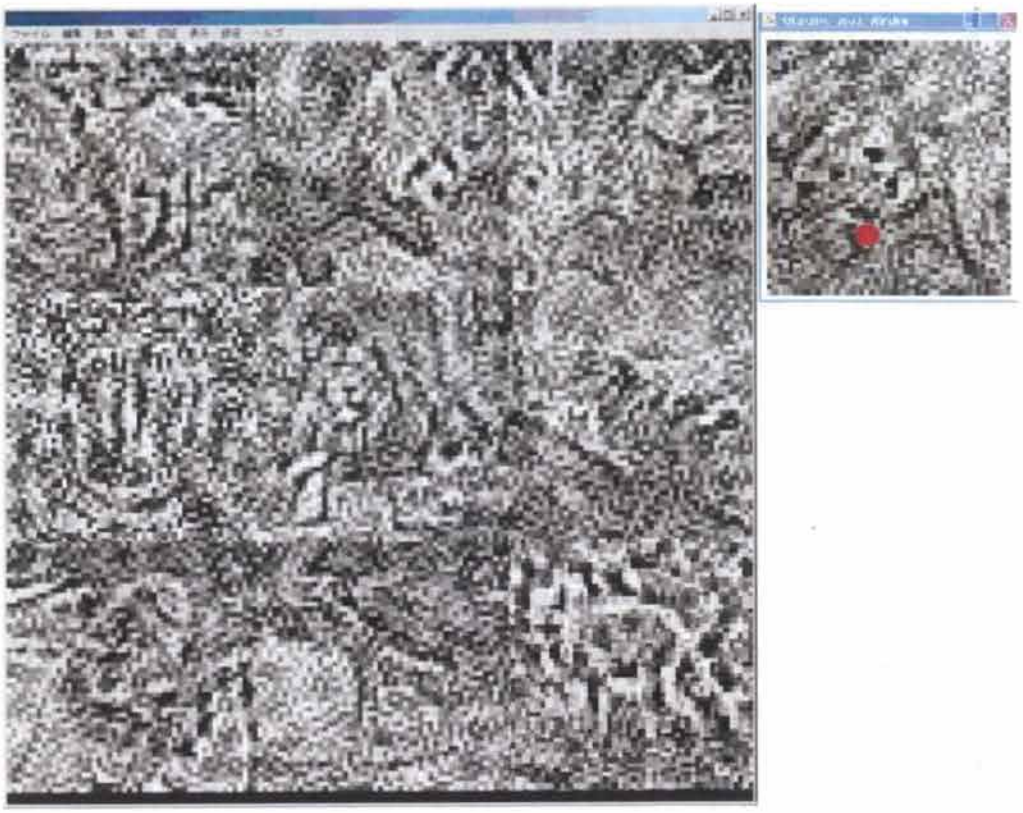


図 5-2　認証ウインドウ(左)と参照ウインドウ(右)の例
図の大きさの都合上，赤丸は実際のサイズより相対的に大きく記してある.

[16] 攻撃者が覗き見を繰り返すうちに，過去に表示されたチャレンジ（キュー）と同じチャレンジが提示された場合は，攻撃者がその時点で取得しておいたレスポンスをリプレイすることによって，なりすましが可能である．この攻撃に対しては，言語手がかりを用いる場合も参照画像を利用する場合も耐性はない.

図 5-3　提案方式（Q&R 方式システム）の概観

5.3　不鮮明化画像における部位情報の登録

スキーマは，正規ユーザが不鮮明化画像の意味を再認識するにあたっての大きな手がかりとなる．しかしそれは，「不鮮明化画像を見た際に，正規ユーザの頭の中に鮮明なオリジナル画像が再び蘇る」という現象が起こっているわけではないということに注意しなければならない．本来人間は不鮮明な画像やランダムドットのような画像を見た場合にも，無意味な点と点，線と線の間に何らかのまとまった関連を見つけ，そこに何らかの意味を見出そうとする性質を持っている[Mat83][17]．スキーマは，この「不鮮明化画像から意味を見出す作業」を後押しするものであり，「オリジナル画像を不鮮明化した際に失われた情報を修復し，正規ユーザの頭の中に鮮明なオリジナル画像を復元する」までの効力はないと著者は解釈している．

このため，画像によっては，オリジナル画像と不鮮明化画像とで正規ユーザが認識する部位の有無・位置・大きさが異なってくるようなケースが発生する．そこで本方式では，オリジナル画像上で認識される部位を用いるのではなく，不鮮明化画像をユーザに見せ，その中で「ユーザにとって部位として認識できる場所」を登録してもらうという方法を採る．

不鮮明化画像がまったく無意味な画像であった場合には，不鮮明化画像の中から部位として認識できる場所を見付け出す作業は人間にとって容易なことではない．しかし本方式においては，正規ユーザは，まずオリジナル画像と不鮮明化画像の両者を見てスキーマを獲得することにより，不鮮明化画像の中に意味を見出すことができている．よっ

[17] このような人間の認知の仕組みは，ゲシュタルト心理学派の研究者が提唱してきた，人間が個別の情報をより簡潔な意味を持つ全体的な情報として認識するという，いわゆるゲシュタルトの法則によって説明される場合もある．

て，登録フェーズにて不鮮明化画像の中の部位情報をシステムに回答することは正規ユーザにとっては大きな負荷にはならないと考えられる．

5.4 Q&R 方式の評価実験

提案方式の有効性を確かめるために基礎実験を行い検証する．本実験の被験者は本学情報学部学生 10 名である．実験で使用する画像も，不鮮明化画像方式[HIM05]のシステムに合わせ，様々な種類の動物が写っている背景つきの写真画像 100 枚とした．今回の実験では，被験者に記憶してもらう参照画像は 1 枚とした．

5.4.1 本人認証実験

正規ユーザにとって，参照画像から与えられるキュー（パス部位）を正しく認識し，パス画像中のパス部位を的確に選択することが可能かどうかを確認する．不鮮明化画像方式[HIM05]と比較し易いように，被験者に記憶してもらうパス画像の数は 4 枚とし，9 択（9 枚の画像の中からパス画像を探し出した後，キューに対応する場所を選択）×4 タ ーンの認証とする．

● 実験方法

登録フェーズ

全被験者には，それぞれ 4 枚のパス画像と 1 枚の参照画像を記憶してもらう．パス画像 4 枚と参照画像 1 枚は全て異なる画像である．また，実験で使用した全ての画像に対して，被験者自身に部位情報を登録してもらう．今回の実験では動物の写真画像を使用しているため，目，鼻，耳，右前足，左後足，胴体，尻尾などが部位として登録されることになる．ただし，被験者の手間を軽減させるため，まずは実験実施者が手動で部位を登録しておき，被験者にその位置・大きさを修正[18]してもらうようにした．図 5-4 のきつねと犬の画像に対し，実験実施者が登録した部位の例を図 5-5 および図 5-6 に示す．ただし，5.3 節で述べたように，被験者による部位情報の登録は（オリジナル画像ではなく）不鮮明化画像を見ながら行ってもらうことに注意されたい．このため，登録される部位情報は，オリジナル画像上で認識されるものとは異なり得る．

なお，図 5-5 および図 5-6 に付されている各部位の名称は，説明を分かりやすくするために記したものであり，実験の際に被験者には提示されない．また，図 5-6 の部位の名称には「(1)」，「(2)」というラベルが記されているが，図 5-6 の犬の画像において左の犬を犬(1)，右の犬を犬(2)としている．

[18] 実験実施者が前もって登録しておいた部位の中で，被験者が認識できないものがあった場合にはこれを削除したり，実験実施者が登録したもの以外に被験者が認識できる部位があった場合にはこれを追加登録したりすることも自由に許した．

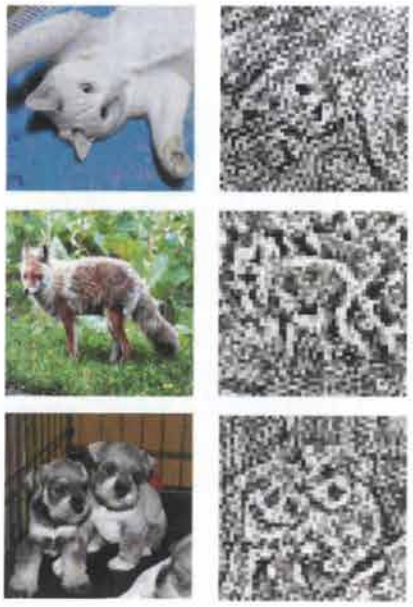


図 5-4　不鮮明化画像方式[HIM05]で用いられる不鮮明化画像（右）と
そのオリジナル画像（左）の例

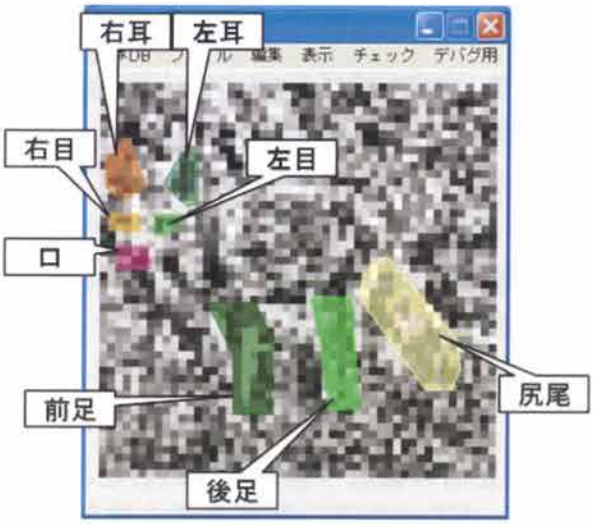


図 5-5　部位登録画面の例 1

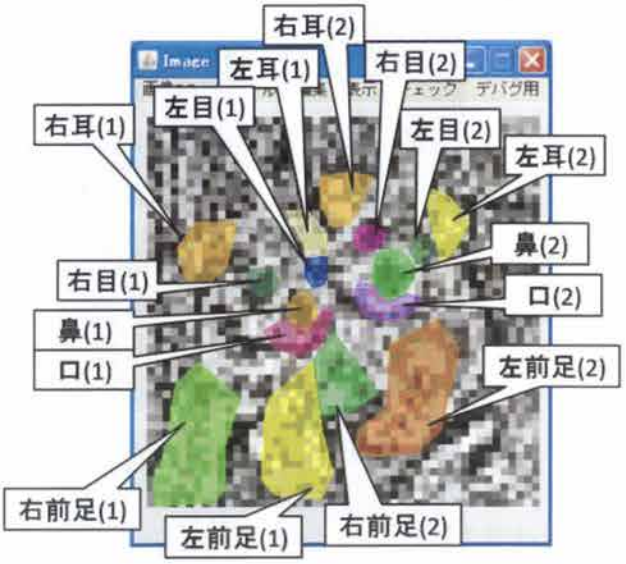


図 5-6　部位登録画面の例 2

認証フェーズ

STEP1. 認証時には，パス画像 1 枚と囮画像 8 枚が表示されている認証ウインドウ（図 5-2 左）と，参照画像 1 枚が表示されている参照ウインドウ（図 5-2 右）が被験者に提示される．

STEP2. パス画像，囮画像，参照画像のそれぞれの画像は全て，300×300 pixel の大きさで画面に表示される．参照画像上にはパス部位が赤い丸でプロットされる．参照画像上に表示されるパス部位は，部位の重心の位置に半径 3 pixel でプロットすることとした．

STEP3. 被験者は，参照画像中のパス部位（赤い丸）を認識し，認証ウインドウ中の 9 枚の画像の中から自分のパス画像を探し出した上で，パス画像上におけるパス部位を選択する．

なお，画像においては左右の概念（動物自身の右なのか，画像を見ている被験者から見て右側なのか）が曖昧になるため，今回の実験では左右の区別はしないこととした．また，画像の中に複数の動物が存在する画像においては，何番目の動物であるかを指示することは煩雑であると考え，今回の実験ではどの動物であるかは区別しないこととした．これを図 5-5，図 5-6 の例を用いて簡単に説明する．例えば，参照画像中のキュー（パス部位）が「左前足」であり，その際のパス画像が図 5-5 であった場合，被験者はパス画像（図 5-5）の中の「左前足」をクリックしても「右前足」をクリックしても認証される．また，参照画像中のキュー（パス部位）が同様に「左前足」であり，その際のパス画像が図 5-6 であった場合は，被験者はパス画像（図 5-6）の中の犬(1)の「左前足(1)」と「右前足(1)」，犬(2)の「左前足(2)」のどれをクリックしたとしても認証されることになる．

今回の実験では，登録される部位情報の数は 1 枚の画像あたり平均 8.2 箇所（標準偏差=2.13，最小値=5，最大値=16）であった．ただし，上記のように左右および動物の順序を区別せずにカウントした場合（例えば，「右前足」と「左前足」は合わせて 1 つと数えた場合）は，部位情報の数は 1 枚の画像あたり平均 5.6 箇所（標準偏差=0.88，最小値=4，最大値=7）であった．

パス画像を変えながらこの操作を 4 ターン行って，認証可否の判定を行う．キューとなるパス部位は，登録されている複数の部位情報の中から，ターン毎にランダムに選択される．

パス画像（および参照画像）登録日から 1 日後と 8 日後に，各被験者につき 10 回ずつ認証を行ってもらった．登録後，被験者は認証実験以外の場でパス画像，参照画像，および，それらのオリジナル画像を確認することはできない．

● **実験結果**

実験結果を表 5-1 に示した．表中，「認証成功率」は，各認証試行において認証に成功した（1 回の認証において，4 ターンのパス部位選択全てに成功した）割合である．一方，「ターン毎の成功率」は，各認証試行時に行う 4 ターンのパス部位選択（9 択の不鮮明化画像の中からパス画像 1 枚を探し，その中のパス部位を選択するタスク）を独立にとらえ，1 ターン毎の成功率を表したものである．なお，今回はユーザの画像認識における曖昧性を吸収するために，登録されている各部位の領域境界から θ=10 pixel まで（領域境界から 10 pixel 未満）を選択成功範囲とした．表 5-1 は比較のために，θ={0,10,15,20}に対する認証成功率についても示した．「画像選択の成功率」は，パス部位の選択については無視し，パス画像の選択のみを考慮した認証試行として捉えた場合（不鮮明化画像方式[HIM05]のシステムに相当する）の認証成功率とターン毎の成功率を示してある．また，1 回の認証に要した時間の平均，標準偏差，最短時間，最長時間，をそれぞれ「認証時間の平均」，「認証時間の標準偏差」，「認証時間の最短値」，「認証時間の最長値」として記した．同様に，ターン毎のパス画像選択にかかった回答時間の平均，標準偏差，最短時間，最長時間，をそれぞれ「ターン毎の回答時間の平均」，「ターン毎の回答時間の標準偏差」，「ターン毎の回答時間の最短値」，「ターン毎の回答時間の最長値」として記した．なお，認証時間およびターン毎の回答時間については，失敗した際の選択時間を含める場合とそうでない場合とに分けて示している．

θ が大きくなるほど，本人拒否率は低下する（正規ユーザにとっては，おおよその場所をクリックすれば認証に成功する）一方で，他人受入率（どれがパス画像かを推定できた攻撃者が，パス画像をランダムにクリックした場合であっても認証に成功する可能性が高まる）が増加する．よって，パス部位を含む登録部位の面積は重要なセキュリティパラメータとなる．よって，表 5-2 に θ の値に対する登録部位 1 つ当たりの平均面積を示した．

表 5-1　本人認証実験の結果

			実験実施日			
			1 日後		8 日後	
			ターン毎の成功率	認証成功率	ターン毎の成功率	認証成功率
許容する誤差（領域境界からの pixel 数：θ）		0	93.75% (375/400)	78.00% (78/100)	92.75% (371/400)	76.00% (76/100)
		10	98.25% (393/400)	93.00% (93/100)	97.00% (388/400)	90.00% (90/100)
		15	98.25% (393/400)	93.00% (93/100)	97.25% (389/400)	91.00% (91/100)
		20	99.00% (396/400)	96.00% (96/100)	98.00% (392/400)	94.00% (94/100)
画像の選択成功率			100% (400/400)	100% (100/100)	99.75% (399/400)	99% (99/100)
選択失敗を含む	ターン毎の回答時間	平均（秒）	9.82		9.38	
		標準偏差（秒）	8.38		10.72	
		最短時間（秒）	2.30		2.16	
		最長時間（秒）	75.24		164.09	
	認証時間	平均（秒）	39.29		37.51	
		標準偏差（秒）	19.64		26.65	
		最短値（秒）	17.41		16.14	
		最長値（秒）	129.00		240.64	
選択失敗を含まない	ターン毎の回答時間	平均（秒）	9.72		8.75	
		標準偏差（秒）	8.29		7.05	
		最短時間（秒）	2.30		2.16	
		最長時間（秒）	75.24		62.27	
	認証時間	平均（秒）	38.89		34.35	
		標準偏差（秒）	19.39		16.78	
		最短値（秒）	17.41		16.141	
		最長値（秒）	129.00		112.20	

表 5-2　本人認証実験における登録部位 1 つ当たりの面積

		許容する誤差（領域境界からの pixel 数：θ）							
		θ=0		θ=10		θ=15		θ=20	
		パス画像	参照画像	パス画像	参照画像	パス画像	参照画像	パス画像	参照画像
A	A_M	2341.49	2089.61	4682.18	4239.15	6177.93	5618.82	7875.82	7190.45
	A_S	2359.59	1989.67	3455.03	2947.70	4035.46	3450.68	4632.20	3950.12
	A_R	2.60	2.32	5.20	4.71	6.86	6.24	8.75	7.99
B	A_M	3459.50	2855.80	6917.82	5793:50	9127.76	7679.06	11636.34	9826.94
	A_S	3757.49	2799.88	5832.79	4415.29	7023.27	5335.14	8308.71	6299.90
	A_R	3.84	3.17	7.69	6.44	10.14	8.53	12.93	10.92

A:部位の左右，ならびに，何番目の動物の部位であるかを区別した場合
B:部位の左右の区別や，何番目の動物の部位であるかといった区別は行わない場合
A_M：面積の平均[pixel^2]
A_S：面積の標準偏差[pixel^2]
A_R：画像面積に対する割合[%]

キューによって暗示されたパス部位を正しく認識し，パス画像上のパス部位を正確に選択できた割合は，1 日後，8 日後とも 90%以上であり，本方式の記憶負荷がそれほど高くないことが見て取れる．ただし，パス画像の選択だけであれば，両日ともほぼ 100%であるため，不鮮明化画像方式と比べ，正規ユーザの認証時の負荷が若干増大したことがわかる．また，表 5-1 と表 5-2 より，確かに，θ が大きくなるほど（パス部位として許容される領域の面積が大きくなるほど）本人拒否率が低下していることが確認できる．

認証負荷増大の問題を今後解決していくために，本実験における失敗の傾向について分析を行った．その結果を表 5-3 に示す．表 5-3 は，本人認証実験のターン毎における選択失敗の全てを，以下に示す失敗のケース毎（(A) ～(E))に分類し，各々の発生頻度を示したものである．

表 5-3　失敗の傾向

		1 日後の失敗の傾向	8 日後の失敗の傾向
失敗の傾向	A	3	10
	B	1	0
	C	2	0
	D	0	1
	E	1	1

(A)　パス部位の領域境界から 10pixel 以上の離れた位置を選択した
(B)　参照画像上のパス部位の認識を間違えた
(C)　登録されていない部位を選択した
(D)　パス画像そのものを忘れた
(E)　うっかりミス

(A)に分類された失敗は，パス画像の大まかな構図はスキーマを使って認識できるものの，時間が経過するにつれて当該部位から少し離れた別の場所が対応部位として認識されるようになってしまったことが原因である．本実験では認証可否についてのフィードバックを被験者に与えなかったが，実運用では，認証に成功した際に必要に応じて登録部位の位置を再度確認させるなどの対策が考えられる．

(B)に分類された失敗は，参照画像の記憶が曖昧であったために起こったと考えられる．特に，「目」と「耳」など互いに近くに配置され易い部位がキューとして提示された場合に，パス部位が「目」なのか「耳」なのかを被験者が混乱している傾向があった．画像によっては顔の部位が非常に密集している可能性がある．部位の密集具合に応じて密集している部位を 1 つの大きな部位に置き換えるなどの工夫が必要である（例えば，目，鼻，口の 3 つの部位を顔という 1 つの部位に置き換える）．

(C)に分類された失敗は，部位情報を登録する際に（実験実施者が前もって登録しておいた部位の中で）被験者自身が認識しにくいと感じた部位を登録から除外したにも関わらず，認証時には除外した部位を認識することができてしまい，部位の選択に混乱してしまったために起きた．この問題に対しても，被験者への認証可否のフィードバックや登録部位の再度確認などの対策が有効であろう．

(D)に分類された失敗は，不鮮明化画像方式においても共通の問題ではあるが，いかに不鮮明化画像を効率よく記憶してもらうかといった工夫が必要である．

なお，表 5-1 において，8 日目の「認証時間の最長値」が 240.64 秒と非常に長くなっているのは．この被験者が認証時にパス画像を見つけることができず，考え込んでしまったためである．

(E)に分類された失敗は，実験後に当該被験者から，キューの認識は正確にできていたのだが，パス画像中の部位を選択する際に，うっかり間違えて別の部位を選択してしまったと報告を受けたものである．

5.4.2 覗き見攻撃実験

攻撃者が過去に覗き見したキュー（参照画像上のパス部位）に対するレスポンス（正規ユーザがクリックした画像とその位置）の情報を用い，現在表示されているキュー（パス部位）に対するレスポンスを推測することが難しいかどうかを確認するために，認証試行を攻撃者に複数回覗き見されたことを想定した覗き見攻撃実験を行った．

なお，本方式においては，攻撃者がなりすましを行うにあたっては，(i) 9 択の認証ウインドウの中からパス画像を発見した上で，(ii) その中のパス部位を回答する必要がある．この内，(i)に関する攻撃実験については，正規ユーザの肩越しからの覗き見により，パス画像を特定する攻撃を仮定した実験が不鮮明化画像方式の研究[HIM05]の中で実施されている．そこで，本論文では(ii)に関する攻撃実験のみを行う．すなわち，パス画像についてはすでに不正者によって特定されてしまっていることを仮定し，その上で，パス部位の推測に関する攻撃成功率を測定する．

● 実験環境

本実験では，パス画像と参照画像のペア（2 枚 1 組）を被験者に提示する．攻撃者が過去に正規ユーザの認証試行を z 回（z=1,2,3）覗き見たこと（カメラで撮影したこと）を想定し，パス画像および参照画像上の対応する部位を任意に z 箇所選び，それぞれの画像上に丸印でプロットする．

パス画像と参照画像とで対応している部位同士は同じ色でプロットされ，z 箇所の部位は互いに異なる色（赤色以外）でプロットされる[19]．また，参照画像には，現在の認証に対するキュー（パス部位）が赤い丸印でプロットされる．攻撃者は，パス画像の中のパス部位（参照画像の赤丸の部位に相当する部位）を推測する．ここで，全ての丸印は，今回の認証システムに合わせ，部位の重心の位置に半径 3 pixel でプロットした．攻撃実験の画面の例を図 5-7 に示す．なお，図 5-7 に付されている各部位の名称は，本論文における説明を分かりやすくするために記したものであり，実験の際に被験者には提示されない．

[19] 例えば参照画像には左目しか写っていない場合などには，パス画像中の 2 つの部位（左目と右目）が参照画像中のパス部位（左目）と対応する．その場合，同じ部位は全て同じ色で表示される．

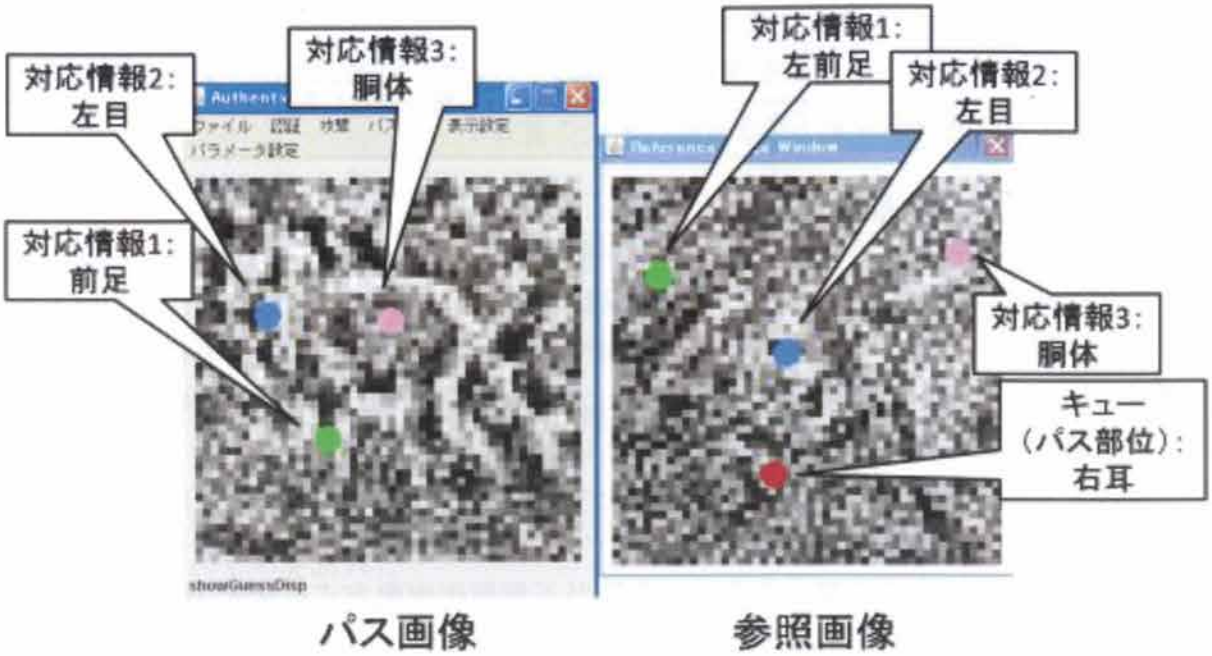


図 5-7　攻撃実験（過去の覗き見回数が 3 回）の例

図の大きさの都合上，丸印は実際のサイズより相対的に大きく記してある．

本実験では，5.4.1 節の本人認証実験のシステムに合わせ，4 枚のパス画像と 1 枚の参照画像を 1 組のパス画像セットとして攻撃を行った．すなわち，1 組のパス画像セットには，パス画像と参照画像のペアが 4 組（ただし，4 組のペアの参照画像は同一）含まれることになる．今回は，計 5 組のパス画像セットを用意した．5 組のパス画像セットの中には同じ画像は含まれていない．

5.4.1 節の被験者とは別の被験者 1 名に正規ユーザ役を引き受けてもらい，本実験で用いる全てのパス画像と参照画像（計 25 枚）に対して，5.4.1 節の認証実験のときと同じ方法で部位を登録してもらった．本実験における攻撃者役の被験者は，5.4.1 節の被験者 10 名と同じである．

● **実験方法**

以下に詳細な実験手順を示す．ここで，パス画像セット x に含まれる y 番目のパス画像を P(x,y) (x = 1～5, y = 1～4)とし，パス画像セット x の参照画像を R(x)と記す．

1) 実験システムは，画像セット 1~5 の中から 1 つの画像セット x をランダムに選ぶ．
2) 実験システムは，画像セット x に含まれる 4 枚のパス画像の中から 1 枚のパス画像 P(x,y)をランダムに選ぶ．
3) 実験システムは，パス画像 P(x,y)に含まれる部位の中から一つのパス部位 z1 をランダムに選ぶ．また，参照画像 R(x) に含まれる部位の中から z1 に対応するパス部位を探し，その部位の重心に赤い丸を記す．

4) 実験システムは，攻撃者役の被験者に P(x,y) と R(x) の組を提示する．参照画像 R(x) のパス部位の上には赤丸がプロットされている．

5) 被験者は，参照画像 R(x)上の赤丸（パス部位）をキューとし，パス画像 P(x,y)の中から対応するパス部位を推測し，マウスのクリックによりその位置を回答する．パス画像 P(x,y)上のパス部位 z1 をクリックできた場合には，覗き見成功と判定される．

6) 実験システムは，パス画像 P(x,y)の中に含まれる部位の中から z1 以外のパス部位 z2 をランダムに選び，その部位の重心に緑の丸を記す．また，参照画像 R(x)に含まれる部位の中から z2 に対応するパス部位を探し，その部位の重心に緑の丸を記す．

7) 実験システムは，攻撃者役の被験者に P(x,y) と R(x) の組を提示する．参照画像 R(x) のパス部位 z1 の上には赤丸がプロットされている．パス画像 P(x,y)と参照画像 R(x) の部位 z2 の上には緑丸がプロットされている．

8) 被験者は，参照画像 R(x)上の赤丸（パス部位）をキューとし，パス画像 P(x,y)の中から対応するパス部位を推測し，マウスのクリックによりその位置を回答する．被験者はパス画像 P(x,y)と参照画像 R(x)の緑丸の対応を，パス部位の推測に利用できる．パス画像 P(x,y)上のパス部位 z1 をクリックできた場合には，覗き見成功と判定される．

9) z1 および z2 以外のパス部位 z3 を追加し，6)-9)と同様の手順で攻撃実験を行う．部位 z3 の上には青丸が記される．

10) さらに，z1，z2，z3 以外のパス部位 z4 を追加し，同様の攻撃実験を行う．部位 z4 の上にはピンクの丸が記される．この時点で被験者に提示される画像例が図 13 である．

11) y を変え，3)~10)の攻撃実験を繰り返す．ただし，一度使用した y は選ばれない．3)-10)を 4 度繰り返した時点でパス画像セット x のパス画像 P(x,y)が使い尽くされる．

12) x を変え，2)~11)の攻撃実験を繰り返す．ただし，一度使用した x は選ばれない．2)-11)を 5 度繰り返した時点で 5 種類のパス画像セットが使い尽され，全ての攻撃実験が終了する．

● 実験結果

実験結果を表 5-4 に示す．表中，「成功率」は，各被験者がパス画像セット 5 組分の攻撃を行った攻撃試行全体の成功率（参照画像中のキューからパス画像中のパス部位を正しく選択できた割合）を表示された覗き見情報の数（z）ごとに示したものである．なお今回は，5.4.1 節の実験と同様，参照画像のキューによって指示されたパス部位が「右前足」であった場合，パス画像における「右前足」と「左前足」のどちらを選択しても正答とした．また，一枚の画像に複数の動物が写っている場合には，何番目の動物の「右前足」と「左前足」を選択しても正答とした．表 5-4 においても，領域の境界から θ pixel（θ ={0,10,15,20}）広げたときの成功率をそれぞれ示している．

表 5-4　覗き見攻撃実験の結果

		覗き見情報の数 z			
		0 個	1 個	2 個	3 個
成功率（領域境界から θ pixel までを境界範囲としたときの成功率）	θ =0	23.50% (47/200)	29.00% (58/200)	32.50% (65/200)	33.00% (66/200)
	θ =10	31.00% (62/200)	39.50% (79/200)	44.00% (88/200)	43.00% (86/200)
	θ =15	38.00% (76/200)	44.50% (89/200)	52.00% (104/200)	51.00% (102/200)
	θ =20	44.00% (88/200)	50.50% (101/200)	57.00% (114/200)	57.50% (113/200)

覗き見回数（z）が増加するにつれて攻撃成功率も増加していることが見て取れる．本人認証の実験にて設定した θ =10[pixel]の許容範囲に対して，覗き見情報無し（n=0）では約 3 割，覗き見情報 3 個（z=3）では約 4 割程度の攻撃成功率であった．

不鮮明化画像方式の文献 [HIM05]にて実施された 9 択×4 ターンの認証システムに対する攻撃実験において，攻撃者が覗き見によって 1 枚のパス画像を特定することに成功する確率は約 60%（9 択×4 ターンの認証システムにおけるターン毎の成功率）であることが報告されている．よって，「不鮮明化画像方式 [HIM05]の攻撃成功率」×「表 4 の攻撃成功率」により求められる提案方式の 1 ターンにおける攻撃成功率は，およそ 20～25%であると結論付けられる．パス部位という秘密情報が追加されている分，Q&R 方式の覗き見攻撃耐性は不鮮明化画像方式よりも当然高くなっている．

しかし，「覗き見情報無し（z=0）」であっても，攻撃者はキュー（パス部位）に対応する場所を 30%～40%の割合で選択することができてしまっている．これは，今回用いた不鮮明化画像の意味が攻撃者にある程度類推可能であったことを意味している．また，実験後のヒアリングの結果，多くの被験者が今回の実験で用いた画像の特徴を活用してパス部位を推定していたことが分かった．すなわち，今回は四足哺乳動物の写真画像を本実験に用いたため，被験者は画像の上部には動物の「頭」，画像の下部には動物の「足」がある可能性が高いといったことや，「目」，「耳」，「鼻」，「口」は比較的お互い近い位置関係にある可能性が高いといったことを仮定することで，パス画像と参照画像の部位を効率的に推測していた．

これらの問題に対応する手段として，画像における一般的な知識（画像の構造：画像の上部に頭があり，下部には足がある等）を崩した上で不鮮明化する方法が考えられる．例えば，歪めた画像を不鮮明化してパス画像や参照画像に用いてやれば，一般的な知識と歪められた画像の構造がマッチせず，攻撃者がパス画像や参照画像の内容を推測することを困難にすることができると考えられる．一方，正規ユーザは登録時に歪められた状態のオリジナル画像を見ることで，歪められたパス画像のスキーマを学習することができ，たとえ歪められていても正しくパス画像を認識することができると考えられる．

5.5 Q&R 方式についての総合的な考察

5.5.1 利便性

不鮮明化画像方式[HIM05]と比べ，Q&R 方式は若干認証時の負荷が増大していた．しかし，実験結果から得られた知見を元に大半の問題は解決可能であると考えられる．また，Q&R 方式の認証成功率は，登録日から 1 日後では 93%，8 日後では 90%程度であるが，カラー人工画像を使った従来の再認型画像認証方式[DP02]では 1 週間後の認証成功率が 90%程度（失敗ログインの割合が 10%）であることが報告されていることから，カラーの人工画像を使った方式と比べても Q&R 方式の記憶負荷はそれほど高いものではないと考えられる．

また，Sobrado らの C&R 型画像認証方式[SB02][WWS06]では，初心者向けの非常に単純化したシステム[20]を用いた場合に，認証情報登録日から 1 日目の認証成功率が 90.35%，認証成功時の認証時間の平均が 70 秒強（最短時間=24.08[sec]，最長時間=150.42[sec][21]）であったことが報告されている．一方，Q&R 方式においては，1 日目の認証成功率が 93 %，認証成功時の認証時間の平均は 40 秒弱（1 日目：最短時間=17.41[sec]，最長時間=129.00[sec]，8 日目：最短時間=16.14[sec]，最長時間=112.20[sec]）である．平均認証時間や認証成功率に鑑みると，Q&R 方式の認識負荷および作業負荷は Sobrado らの方式に比べ低いと考えることができる．

ただし．Q&R 方式の本人認証実験においては，被験者は認証情報の登録（パス画像と参照画像を記憶し，部位選択の練習を行う）に少なくとも 20 分程度の時間を要していた．そのため，他方式と比べ Q&R 方式は登録時におけるユーザの負荷が大きいと予想される．今後，認証情報の登録時間を短縮する工夫が必要である．

5.5.2 安全性

5.5.2.1 ランダムクリック攻撃（Brute force 攻撃）

従来の再認型画像認証方式[PSL03][DP02]も Q&R 方式も，複数の画像の中からパス画像を探し出すという点は同じである．簡単のために N 枚の画像の中から 1 枚のパス画像を選ぶ形の認証方式を想定すると，当て推量（ランダムクリック）による他人受け入れの（パス画像を選択する）割合は 1/N である．Q&R 方式では，1/N の確率でパス画像を見つけた後に，さらにパス部位を選択する必要があるため，その分，ランダムクリック攻撃の耐性が向上しているといえる．ここで，パス画像の面積を IA[pixel^2]，パス画像中の各部位の平均面積を MPA [pixel^2]と表わしたとき，パス画像がわかった上で，パス画像の中をランダムにクリックしてチャレンジに対応する部位を正しく選択できる確率

---

[20] 記憶している 5 個の pass-object の中から 3~5 個の pass-object がランダムに選択され，囮のアイコンと一緒に認証画面に表示される．認証画面には pass-object を含めて 43~112 体のアイコンが表示される．1 回の認証における問答の繰り返しは 5 回である．

[21] ただし認証に非常に時間を要した 1 人の被験者をアウトライヤとして実験結果から除いている．アウトライヤになった被験者は，2 番目に認証時間が長かった被験者の，2 倍以上認証に時間を要したと報告されている．

は，MPA/IA となる．すなわち，Q&R 方式における当て推量による他人受け入れの割合は，MPA/(N×IA)となる．

Man らの報告[MHM03]によると，Sobrado らの方式は画面の中心をクリックすれば非常に高い確率で正規ユーザになりすますことが可能であることが示されている．著者らもこれを確かめるために，Sobrado らの認証方式を単純なモデルに置き換え[22]，プログラムによりシミュレーションを行った結果，認証画面の中心をクリックすることで 3 割強の確率[23]で pass-object が構成する凸包内部が選択される結果となることがわかった．これはすなわち，Sobrado らの C&R 型画像認証方式における凸包内の選択という認証行為 1 回当たりのなりすまし成功率が約 30%であることを意味している．

Q&R 方式においては，パス画像 1 枚当たりのパス部位の平均面積は 7.69%（表 5-2）であることから，N=9 としたときの当て推量による他人受け入れの割合は，約 0.85%（(1/9)×(7.69/100)×100）となる．このことから．Q&R 方式におけるランダムクリック攻撃耐性は，Sobrado らの方式よりも約 30 倍程度強いことがわかる．

5.5.2.2 覗き見攻撃

Q&R 方式においては，攻撃者がなりすましを行うにあたっては，(i) 9 択の認証ウインドウの中からパス画像を発見した上で，(ii) その中のパス部位を回答する必要がある．よって，Q&R 方式における 1 ターンあたりの攻撃成功率は，「不鮮明化画像方式[HIM05]の攻撃成功率」×「4.2 節の表 4 の攻撃成功率」より求められ，その結果は約 20～25%であった．パス部位という秘密情報が追加されている分，提案方式の覗き見攻撃耐性は先行研究の不鮮明化画像方式よりも当然高くなっている．

Roth らが提案する C&R 型画像認証方式[RRF04]では，0～9 までの数字を白か黒かの 2 グループに分け，グループ情報を答えることで，攻撃者が一意に暗証番号を推測することを困難にしようとしているが，1 回の認証における一連の作業全てのスナップショットを撮られると暗証番号が一意に特定されてしまうという問題がある．入力をさらに曖昧化することによって，1 回の認証を覗き見られただけでは暗証番号を一意に特定することを不可能にした改良方式も提案されているが，その場合は総当り攻撃に対する安全性が低下してしまう．以上より，提案方式は Roth らの C&R 型画像認証方式と比べ，十分な安全性を有しているといえる．

Sobrado らの C&R 型画像認証方式[SB02][WWS06]では，3 つ以上の pass-object が構成する凸包内をクリックするという曖昧入力により，人間の目視に対しては高い覗き見攻撃耐性を確保している．しかし，小島らが行ったビデオ撮影を想定した覗き見に対す

---

[22] pass-object の数は 3 体に固定し，認証画面には pass-object を含め 66～100 体のアイコンがランダムな位置に整然と配置される．利便性と安全性を考慮すると凸包が小さすぎても大きすぎても問題となるため，認証画面の面積を S としたときに凸包の面積 T が S / 27 < T < S / 3 となるようランダムな位置に pass-object を配置している．

[23] pass-object を認証画面にランダムに配置する試行を 10000 回繰り返し，そのうち，pass-object により構成される凸包が認証画面の中心点を内包する割合を求めた．

る安全性の評価においては，Sobrado らの認証方式の簡易版プロトタイプシステム（3体の pass-object と 197 体の囮アイコンを 10×20 に整然に配置し，その中から探し出した pass-object を頂点とした凸包内部を選択するという作業が 1 回の認証行為となる）に対して，カメラ撮影を用いた 1 回の認証行為の覗き見によって pass-object の候補が約 1/8 に絞られること，および，8 回程度の覗き見により pass-object が特定されることが報告されている[KYN09]．一方，本章の実験で使用した画像に登録されていた部位情報の数は 1 枚の画像あたり（左右および動物の順序を区別せずにカウントした場合で）平均 5.6 箇所であるため，最低 6 回の覗き見によって 1 枚の画像の中のすべての登録部位が漏洩する可能性がある．5.5.2.1 節の考察を基に，Q&R 方式と Sobrado らの方式のランダムクリック攻撃耐性を比較すると，Sobrado らの方式において Q&R 方式 1 回あたりのランダムクリック攻撃耐性を確保するには，Sobrado らの方式による認証行為を 3～4 回繰り返す必要がある[24]．すなわち，Q&R 方式と Sobrado らの方式のランダムクリック攻撃耐性を同程度に合わせた場合，Q&R 方式による 3 回の認証が Sobrado らの方式による 9～12 回の認証に相当し，Sobrado らの方式においては覗き見耐性の限界（8 回程度の覗き見）に達してしまうことになる．ゆえに Q&R 方式は Sobrado らの方式と同程度以上の覗き見攻撃耐性を有していると考えられる．

Sasamoto らの方式[SCH08]は，チャレンジそのものを秘密の通信路を介してユーザに渡すことで，ビデオカメラによる複数回の盗撮に対しても高い耐性を実現している．しかし，特殊な装置（触覚デバイス）が必要となることから，Q&R 方式との比較対象からは外す．

5.5.2.3 部位に関する攻撃

Q&R 方式ではパス部位がキューとして暗示的に提示されるため，この情報が攻撃に利用される可能性がある．例えば，攻撃者が参照画像におけるパス部位（キュー）の意味を類推することができた場合，対応する部位を含んでいないと推測される画像は囮画像であると判断することができる．また，攻撃者が何らかの方法でパス画像の特定には成功している場合には，参照画像におけるパス部位（キュー）の意味を類推することができれば，その分，パス画像の中からパス部位を推測する作業は容易となるだろう．

不鮮明化画像の特徴を活用して，部位の位置を類推するという攻撃も考えられる．例えば，不鮮明化画像中に特徴的なエッジが認識できる場所は部位として登録されている可能性が高いかもしれない．

---

[24] 5.5.2.1 節より，Sobrado らの方式と Q&R 方式のランダムクリック攻撃耐性をそれぞれ 0.3（30%），0.0085（0.85%）とすると，Sobrado らの方式は，4 回繰り返して初めて Q&R 方式と同程度のランダムクリック攻撃耐性を持つことがわかる．
Sobrado らの方式を 3 回繰り返す：$0.3^3=0.027(2.7\%)$,
〃　　4 回繰り返す：$0.3^4=0.0081(0.81\%)$.

以上の問題は不鮮明化画像に起因するものであるため，不鮮明化処理の改善が対策の鍵となると考えている．

また，今回の実験で用いた認証システムでは，参照画像上に表示されるパス部位（キュー）は，部位の重心の位置に半径 3 pixel の赤い丸でプロットされる方式となっている．このため，キューのバリエーションは部位情報の登録個数と等しい値となる．よって，攻撃者が認証行為の覗き見を繰り返せば，すべてのキューとそれに対するレスポンスを収集することができてしまう．この問題に対しては，「認証が繰り返されるうちに同じ部位を再びパス部位として使用することになった際には，パス部位（キュー）を示す赤丸の位置を変更する」という対策が考えられる．パス部位（キュー）を示す赤丸は，正規ユーザが見た際にパス部位の領域を特定することができる位置であれば，パス部位の重心以外の位置に表示しても構わない．このような簡易な改良によって，キューのバリエーションを部位情報の登録個数よりもある程度増やすことは可能であるだろう．

6章　囮画像の自動生成
（ADG方式：Automatic Decoy image Generation）

本章では，画像認証の囮画像の問題に焦点を当て，囮画像の自動生成を試みる．ここで，「簡素な画像処理によって，オリジナル画像と不鮮明化画像の間のスキーマを切断することが可能である」という不鮮明化画像の特長を活用し，正規ユーザにとって馴染みの無い囮画像を自動的に大量に生成する方法を提案する．実験により，生成された囮画像が利便性（囮画像が正規ユーザのパス画像の記憶・想起を阻害することはないか）および安全性（不正者がどの程度囮画像を識別可能か）の面でどのような影響を与えるのかについて評価する．

6.1　画像認証における囮画像の問題

画像認証方式において，パス画像を隠すために利用される囮画像（認証画面にパス画像と共に表示される複数の画像）を適切に用意することは重要な手続きの1つである．毎回の認証で常に同じ囮画像のセットを利用してしまうと，攻撃者が認証画面中の画像一枚一枚に当たりをつけ，「その画像を選択して認証に失敗したならば，その画像はパス画像ではない」というように，パス画像の候補が徐々に絞られていく問題（Exhaustive 攻撃）がある．しかし，逆に，認証の都度，すべての囮画像を一新するようにすると，攻撃者が覗き見を繰り返すことによって，毎回の認証画面に必ず表示される画像がパス画像であると知られてしまう（Intersection 攻撃）．

以上より，ある一定枚数の囮画像は前回の認証から引き継ぎ，残りの囮画像は正規ユーザが見たことの無い全く新しい画像を用いるという折衷案が適切と考えられる．しかし，認証の都度，一定枚数の全く新しい囮画像を準備するにあたっては，以下の問題を考慮しなければならない．

1) ネットワークを介して毎回囮画像をダウンロードする場合

(ア)アクセス集中によるサーバ負荷および通信帯域消費の観点から，通信はできる限り抑えることが望ましい．

(イ)誰でもサーバから囮画像をダウンロードできるとした場合，攻撃者も囮画像の情報を用いて，他人のパス画像を絞り込むことが可能である．

2) 製品の工場出荷時に，あらかじめ大量の囮画像を記憶領域に保存しておく場合

(ア)ユーザ数が多い場合，製品ごとに異なる「大量の囮画像」を用意することは困難である．

(イ)すべてのユーザの製品に保存する囮画像が同じであった場合には，攻撃者は，自身が購入した製品に含まれている囮画像情報を用いて他人のパス画像を絞り込むことが可能である．

3) ユーザが撮影した写真を利用する場合

(ア)ユーザ自身が撮影した写真を囮画像とすると，パス画像と囮画像のどちらに対しても再認が引き起こされ，ユーザがパス画像の選択の際に混同する[DP02].

そこで，本研究では，あらかじめ大量に囮画像を用意したり，ネットワークを介して自動的に囮画像を取得したりする方法とは別のアプローチにより新しい囮画像（正規ユーザにとって馴染みの無い画像）を取得する方法を検討する．本章では，不鮮明化画像の特長に着目し，従来の写真や絵（オリジナル画像）を利用する画像認証方式では実現不可能な方法で，囮画像を生成する方式（ADG 方式：Automatic Decoy image Generation）を提案する．

6.2 コンセプト　不鮮明化画像の特長を利用した囮画像の生成

はじめに，図 6-1 の不鮮明化画像を見てもらいたい．

図 6-1　不鮮明化画像の加工例

図 6-1 の不鮮明化画像は図 3-2（最上段）の不鮮明化画像を時計回りに 90 度回転（今後特に断りが無い限り，時計回りを回転方向の基準とする）させた画像である．既に 3 章で図 3-2（最上段）のオリジナル画像とそれに対応する不鮮明化画像を見ているにも関わらず，図 6-1 の不鮮明化画像の意味（何が映っていて，どのような状態になっているかなど）を類推することは難しかったのではないだろうか．このように，不鮮明化画像にある細工を加えた場合，あたかも加工前の元の画像とは全く無関係な画像のように知覚される．言い換えると，「簡素な画像処理によって，オリジナル画像と不鮮明化画像の間のスキーマを切断することが可能である」という特長が不鮮明化画像にはあり，その特長を活用すれば，正規ユーザが記憶しているパス画像や正規ユーザにとって馴染みの深い画像からでも，正規ユーザがパス画像との混乱をきたすことの無い囮画像を生成することが可能だと考えられる．一方，図 6-2 のようにオリジナル画像に対して同様の加工を行った場合，明らかに加工された画像だと認識できてしまい，これを囮画像として利用することはできないことに注意されたい．

画像の加工により囮画像を生成する方法（以下，囮画像生成法と呼ぶ）を不鮮明化画像方式に導入するという改良を加えることにより，ADG 方式は従来の画像認証方式における囮画像の用意に関する問題を解決することができると期待される．

図 6-2　図 6-1 に対するオリジナル画像

6.3　ADG 方式における囮画像の生成手順

囮画像はパス画像を紛れさせるために用いられるものであるため，囮画像（囮画像生成法により作成された不鮮明化画像．以下，加工不鮮明化画像と呼ぶ）とパス画像（オリジナル画像を不鮮明化処理することにより得られる不鮮明化画像．以下，自然不鮮明化画像と呼ぶ）は両者の区別がつかないようになっていないといけない．すなわち加工不鮮明化画像は，自然不鮮明化画像らしさを十分保持している必要がある．

本論文では，動物を被写体とした写真を実験に用いている．そのため，動物の身体全体が写っている画像であれば，画像の下半分に足があり，画像の上半分に頭部があり，画像の中心に胴体があるという構造を持つものが多い．また，動物の顔のアップが写っている画像であれば，上半分に目があり，下半分に口があるという構造を持つものが多い．著者らが行った事前調査から，実際に多くの被験者が，これらの構造に注目することによって加工不鮮明化画像と自然不鮮明化像の識別を試みていた．そこで今回は，上記の構造を崩さない不鮮明化画像を「自然不鮮明化画像らしさを有する画像」と考えることとする．

これを考慮すると，例えば図 6-1 に示した「回転」は，（写真の撮り方にもよるが）一般に画像の構造を崩すことになるため，囮画像を作成するための加工には適さないと考えられる．そこで以下では，動物の写真を前提とした上で，「自然不鮮明化画像らしさを有する囮画像」の作成が比較的期待できると考えられる 3 種類の囮画像生成法を示す．

1)　囮画像生成法 1

囮画像生成法 1 は，図 6-3 のように 2 枚のオリジナル画像 A と B のそれぞれ上半分と下半分をつなげる方法である．2 枚のオリジナル画像を組み合わせた後に，不鮮明化処理を施して加工不鮮明化画像を得る．上下の画像の境界部分の不整合を整えるために，境界部分にはグラデーション処理を適応する．本手法で作成した加工不鮮明化画像の例を，不鮮明化処理前の画像とともに図 6-4 に示す．

図 6-3　囮画像生成法 1

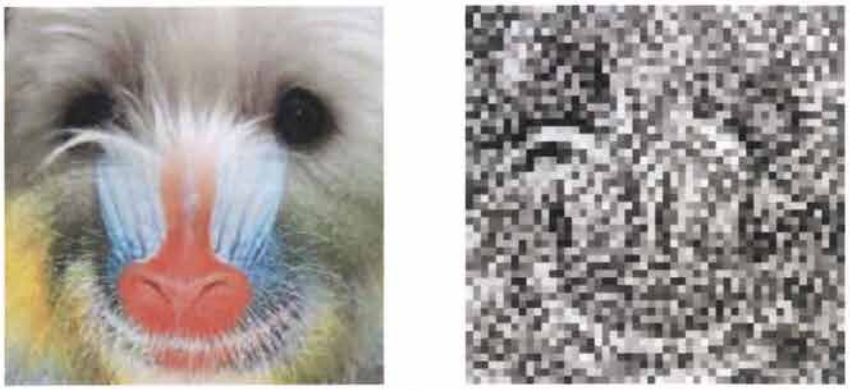


図 6-4　囮画像生成法 1 による加工不鮮明化画像例

2) 囮画像生成法 2

図 6-1 に示した「回転」は，画像の雰囲気を大きく変化させるには効果的だと考えられる．しかし，前述のとおり，「回転」単体だけでは，自然不鮮明化画像らしさを大きく崩すと考えられる．そこで「回転」により画像の雰囲気を大きく変化させた後に，自然不鮮明化画像らしさを補完する方法を考える．具体的には，図 6-5 のように正立したオリジナル画像 B に回転したオリジナル画像 A を同じ割合で重ね合わせる方法である．2 枚のオリジナル画像を重ね合わせた後に，不鮮明化処理を施して加工不鮮明化画像を得る．オリジナル画像 A の回転角度は 90 度，180 度，270 度の 3 種類である．回転したオリジナル画像 A により不自然さが増大するが，正立したオリジナル画像 B を重ね合わせることで「自然不鮮明化画像らしさ」を補うことが可能だと考えられる．本手法で作成した加工不鮮明化画像の例を，不鮮明化処理前の画像とともに図 6-6 に示す．

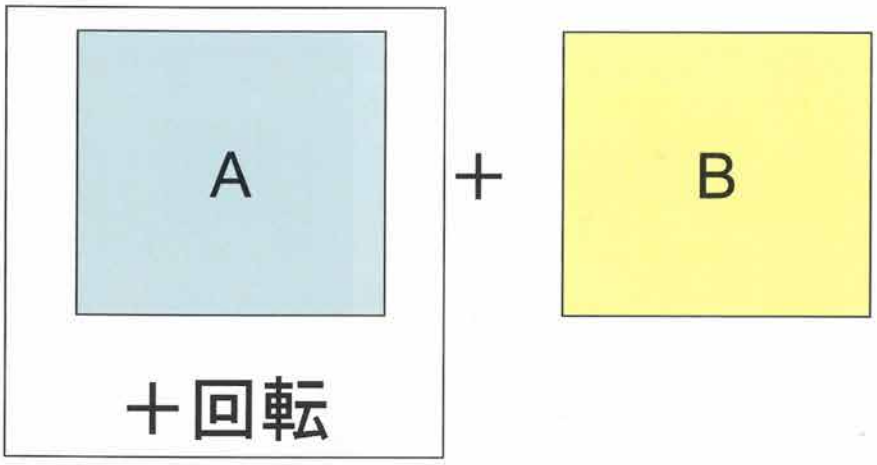


図 6-5　囮画像生成法 2

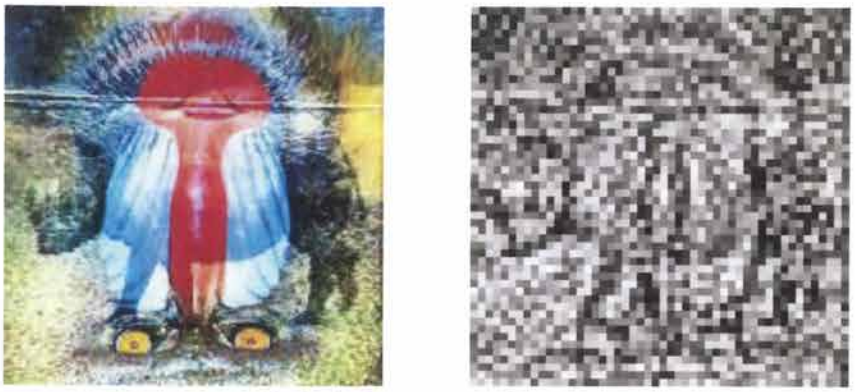


図 6-6　囮画像生成法 2 による加工不鮮明化画像例

3)　囮画像生成法 3

囮画像生成法 3 は，図 6-7 のように囮画像生成法 1 と囮画像生成法 2 を併用した方式である．すなわち，囮画像生成法 1 の要領で 2 種類のオリジナル画像を作成し，その 2 種類を囮画像生成法 2 の要領で重ね合わせる．最後に不鮮明化処理を施して加工不鮮明化画像を得る．本手法で作成した加工不鮮明化画像の例を，不鮮明化処理前の画像とともに図 6-8 に示す．

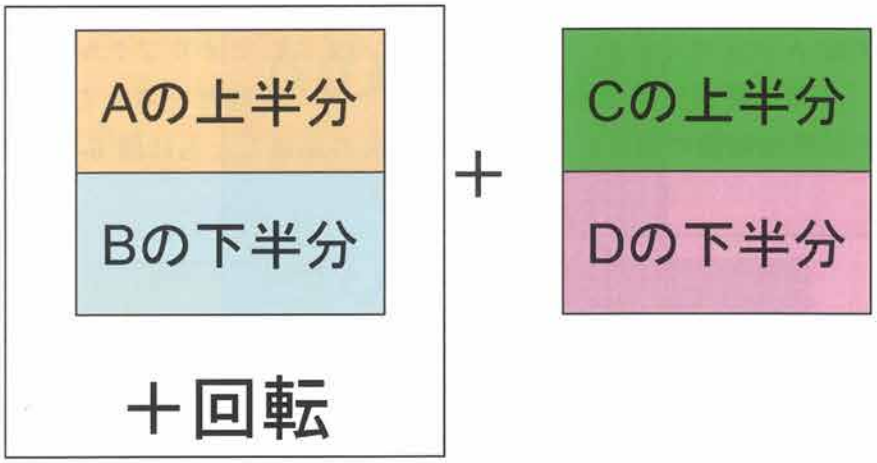


図 6-7　囮画像生成法 3

図 6-8　囮画像生成法 3 による加工不鮮明化画像例

なお，図 6-4，図 6-6，図 6-8 の加工不鮮明化画像の作成に用いたオリジナル画像を図 6-9 に示す．

図 6-9　加工不鮮明化画像の作成に用いたオリジナル画像

6.4　ADG 方式の評価実験

ADC 方式により生成された囮画像の有効性を確かめるために実証実験を行う．攻撃者には，囮画像（加工不鮮明化画像）とパス画像（自然不鮮明化画像）の見分けが困難で，正規ユーザには容易にできるようでなければならない．被験者は本学情報系学部学生 10 名である．本実験に利用した画像は，様々な種類の動物が写っている背景つきの写真画像 80 枚である．

6.4.1　識別実験

囮画像生成方法 1~3 により作成される加工不鮮明化画像が自然不鮮明化画像らしさをどの程度保持しているのか識別実験によって評価する．被験者が加工不鮮明化画像と自然不鮮明化画像とを切り分けることができなければ，自然不鮮明化画像らしさを十分保持した加工不鮮明化画像を生成することができたといえる．

● **実験方法**

本実験システムは，被験者に，2 択の認証画面を提示する（図 6-10）．2 枚の内，どちらか 1 枚が自然不鮮明化画像であり，もう 1 枚が加工不鮮明化画像である（両画像の位置は毎回ランダムに変わる）．被験者は 2 枚の画像の中で自分が直感的に自然不鮮明化画像だと思うものを選択する．囮画像生成法 1 に対する識別実験を例に採り，具体的な実験手順を以下に示す．囮画像生成法 2 および 3 の識別実験も同様の手順で実施される．

STEP1. 5 枚のオリジナル画像 1~5 を用意する．

STEP2. 全てのオリジナル画像 i を不鮮明化し自然不鮮明化画像 pass(i)（i=1~5）を作成する．

STEP3. 全てのオリジナル画像 i に対し，i 以外の 4 枚のオリジナル画像を用い囮画像生成法 1 により作成され得る全ての加工不鮮明化画像の画像セット decoy(^i,1)（i=1~5）を生成する[25]．

STEP4. 1~5 の中から一つの数字 k をランダムに選ぶ．

STEP5. decoy(^k,1)の中から任意に 1 枚の加工不鮮明化画像を選び，これと自然不鮮明化画像 pass(k)による 2 択の識別実験を行う．

STEP6. k を変え，STEP4，STEP5 の識別実験を繰り返す．ただし，一度使用した k は選ばれない．識別実験を 5 回繰り返した時点で，5 枚全ての自然不鮮明化画像が尽くされ，実験 1 セットが終了となる．

STEP7. オリジナル画像 1~5 を一新し，STEP2~STEP6 を計 4 セット繰り返す．すなわち，各被験者は囮画像生成法 1 の識別実験につき 2 択の選択を 20 回 繰り返す．

被験者は識別実験を始める前に，各囮画像生成法において加工不鮮明化画像がどのように作成されているのかを図を用いて詳細に説明される．

[25] 例えば decoy(^4,1)は，オリジナル画像 4 以外のオリジナル画像 1，2，3，5 を用いて囮生成画像法 1 により生成され得る加工不鮮明化画像の全てを表す．すなわち，オリジナル画像 A の上半分とオリジナル画像 B の下半分の組合せによって得られる加工不鮮明化画像を d(A,B)と表すとすると，decoy(^4,1)={d(1,2), d(1,3), d(1,5), d(2,1), d(2,3), d(2,5), d(3,1), d(3,2), d(3,5), d(5,1), d(5,2), d(5,3)}である．

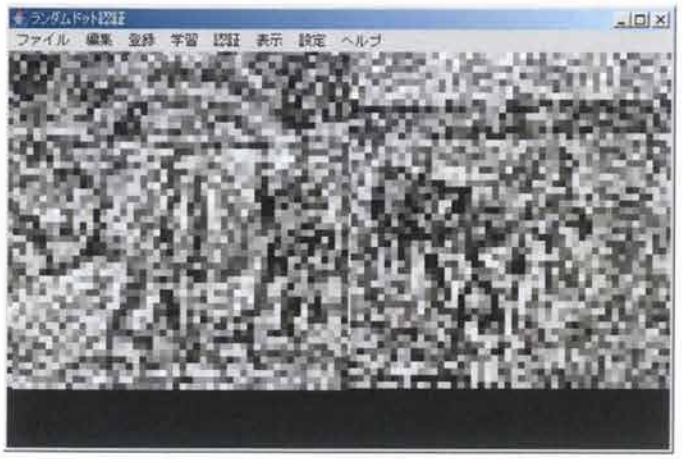


図 6-10　2 択の認証画面

● **実験結果**

実験の結果を表 6-1 に示した．表中，「識別成功率」は 10 人の各被験者につき 20 回ずつ行った各囮画像生成法に対する識別試行の全体の成功率（2 択の画面の中から自然不鮮明化画像を正しくを選択できた割合）を表す．

表 6-1　識別実験の結果

	囮画像 生成法 1	囮画像 生成法 2	囮画像 生成法 3
識別 成功率	117/200 (58.50%)	121/200 (60.50%)	115/200 (57.50%)

全ての生成法において，被験者は 60%前後の割合で自然不鮮明化画像と加工不鮮明化画像との違いを認識していることが見てとれる．被験者が完全に当て推量で回答した場合の識別率が 50%であるため，囮画像生成法 1~3 によって作成された加工不鮮明化画像は概ね自然不鮮明化画像らしい画像となっていると考えてよいと判断できる．

ただし，識別が 50%で成功するケース（被験者が完全に当て推量で回答する場合を意味する）を帰無仮説として，各生成法における識別成功率に対して t 検定を行った結果，囮画像生成法 1~3 それぞれの有意確率は $p=0.0634$，$p=0.0109$，$p=0.0119$ となり，囮画像生成法 1 以外の 2 つの生成法において $p<0.05$ で有意差（5%有意）が見られた．よって，少なくとも囮画像生成法 2,3 によって生成された加工不鮮明化画像は，攻撃者にパス画と囮画像とを切り分けるヒント（情報）を幾分与えてしまっていることがわかる．これは，自然不鮮明化画像と加工不鮮明化画像との差を利用した推測攻撃が ADG 方式の脅威となる可能性を意味する．

6.4.2 本人認証実験

本節では，パス画像から生成される囮画像を使用しても本人認証率が劣化することがないかを本人認証実験により確認する．正規ユーザにとって馴染みの深い画像（パス画像）から生成された囮画像を用いて，6.3 節で提案した囮画像生成法 1~3 によって生成された囮画像が正規ユーザの認証にどの程度影響を与えるか調査する．パス画像から生成された囮画像が正規ユーザにとって十分馴染みの無い囮画像になるのであれば，認証端末に必要な情報はパス画像となり，運用の面でも非常に優れた画像認証方式の実現が期待される．

● 実験方法

囮画像の用意の方法を除けば，本実験システム（ADG 方式）の設定は不鮮明化画像方式の文献[HIM05]の中の本人認証実験と全く同一である．すなわち，正規ユーザが記憶するパス画像は 4 枚であり，9 択の認証フェーズ（認証画面中にパス画像 1 枚と囮画像 8 枚が提示される）を 4 ターン行って 1 回の認証とするシステムを用いる（図 6-11）．

ターン毎に 4 枚のパス画像の中から 1 枚がランダムに重複無く選ばれ認証画面に表示される．パス画像と共に表示される 8 枚の囮画像は，現在表示されているパス画像以外の 3 枚のパス画像のオリジナル画像から，6.4.1 節と同じ方法で生成される．ただし，6.4.1 節の実験では，囮画像生成法 j（j=1~3）ごとに囮画像セット(decoy(^i,j))を用意したが，本実験では，3 つの囮画像セットを 1 つにまとめた囮画像セット{decoy(^i, 1) + decoy(^i, 2) + decoy(^i 3)}の中から各 8 枚の囮画像を選出する．

パス画像登録の後，1 日後と 8 日後に，各被験者につき 5 回ずつ認証を行ってもらう．なおパス画像登録後，被験者は認証実験以外の場でパス画像やオリジナル画像を確認することはできない．

図 6-11　9 択の認証画面例

● **実験結果**

実験結果を表 6-2 に示した．不鮮明化画像方式の結果は，不鮮明化画像方式の文献[HIM05]の 4.1 節の実験結果の再掲である．表中の用語は 4.3.1 節と同じである．

表 6-2　本人認証実験の結果

			不鮮明化画像方式 [HIM05]		ADG 方式	
			1 日後	8 日後	1 日後	8 日後
認証成功率			50/50 (100.0%)	49/50 (98.0%)	46/50 (92.00%)	47/50 (94.00%)
ターン毎の選択成功率			200/200 (100.0%)	199/200 (99.5%)	194/200 (97.0%)	196/200 (98.0%)
ターン毎の回答時間	選択失敗を含む	平均（秒）	8.26	7.10	20.60	17.67
		標準偏差（秒）	11.68	8.78	21.03	18.12
		最短値（秒）	1.19	1.06	2.33	2.34
		最長値（秒）	56.50	67.13	177.86	144.99
	選択失敗を含まない	平均（秒）	8.26	6.80	19.88	17.45
		標準偏差（秒）	11.68	7.72	20.37	18.04
		最短値（秒）	1.187	1.062	2.33	2.344
		最長値（秒）	56.50	66.50	177.86	144.99

実験結果から，たとえ，本人がスキーマを有しているパス画像（本人にとって馴染みの深い画像）から囮画像を生成したとしても，正規ユーザは自分のパス画像を高い確率で認識できていることが確認できる．しかし，不鮮明化画像方式よりも成功率が若干低下していること，および，回答に倍以上の時間を要していることを考えると，パス画像を元に囮画像生成法 1~3 を用いて生成された加工不鮮明化画像を囮画像として用いることは，正規ユーザの認識負荷の増加につながってしまったことがわかる．

6.5　ADG 方式についての総合的な考察

6.5.1　利便性

ADG 方式によってパス画像から囮画像を生成する方法に対しては，不鮮明化画像方式よりも認証成功率が若干低下していること，および，回答に倍以上の時間を要している

ことから，利便性の面での改良が必要である．正規ユーザの認識率の低下と所要時間の増大は，3 種類の囮画像生成法によって生成された加工不鮮明化画像中に，加工前の不鮮明化画像の特徴がある程度再認可能な状態で残っていたことが原因だと考えられる．この対策として，囮画像生成法のアルゴリズムに加工前の不鮮明化画像の特徴が大きく崩れるような処理が有効だと考えられる．例えば，歪曲処理を使えば，エッジの連続性を失うことなく，画像全体に変化を持たせることができる．また，パス画像中に含まれる再認を引き起こしやすい部分に加工（回転，拡大縮小，歪曲）などを加えるなどをすることで，馴染みのある画像からでも再認を引き起こしにくい囮画像を作成できるのではないかと期待できる．ただし，これらの加工が，6.3 節の「自然不鮮明化画像らしい構造」を崩さないことや，本当に再認を引き起こしにくいのかについては，今後調査が必要である．

また，パス画像だけから囮画像を生成するのではなく，馴染みの無い画像も囮画像生成に用いることで，正規ユーザにとって馴染みの無い加工不鮮明化画像を容易に生成することができると考えられる．ただし，6.1 節からもわかるとおり，あらかじめ全く新しい画像（馴染みの無い画像）を用意しておくことに関しては注意が必要であり，できるだけ小数の馴染みの無い画像からでも多種多様な加工不鮮明化画像が生成できるような工夫が必要であろう．今後より効果的に多種多様な加工不鮮明化画像を生成する方法についても検討していきたい．

6.5.2 安全性

ADG 方式はあくまでも囮画像の自動生成に焦点をおいた方式であり，覗き見攻撃，ランダムクリック攻撃，Educated-Guess 攻撃，Intersection 攻撃，Exhaustive 攻撃等，従来の画像認証方式における脅威への耐性向上を目指したものではない．そこで本節では，囮画像を自動生成するがゆえの脅威についてのみ議論する．

6.4.1 節の識別実験では，自然不鮮明化画像と加工不鮮明化画像が約 60%の確率で識別できてしまっている．そのため自然不鮮明化画像と加工不鮮明化画像との差を利用した推測攻撃が脅威となってくるだろう．さらに，この推測攻撃と従来からある脅威を組み合わせることで，より効率的にパス画像を推測していく攻撃も考えられるだろう．そのため，識別成功率をできるだけ 50%に近づける工夫が必要である．

現行の囮画像生成法の質が不十分であった原因として，「自然不鮮明化画像らしさを有する画像」の定義についての検討が不十分であったことが大きな要因だと考えられる．本論文での「自然不鮮明化画像らしさを有する画像」の定義は，6.3 節で述べているように「動物の身体全体が写っている画像」と「動物の顔のアップが写っている画像」の 2 パターンの画像にしか焦点を当てていない．これらのパターンに該当する画像は少なくないが，例えば「動物の身体全体が写っている画像」の中でも，「複数の動物の身体全体が写っている画像」もあれば，「一頭の動物の身体全体しか写っていない画像」もあるだろう．同様に，「複数の動物の顔のアップが写っている画像」もあれば，「一頭

の動物の顔のアップしか写っていない画像」もあると考えられる．また，写っている動物達の身体の大きさやカメラからの位置関係によっては，「身体全体が写っている動物や顔のアップが写っている動物が混在した画像」もありうると考えられる．今後はより多種多様なパターンの画像にも対応することができるよう「自然不鮮明化画像らしさを有する画像」の定義をより幅広く，より具体的に検討し，ADG 方式を改良していく必要がある．

また，画像の中の対象（顔や体）に注目するのではなく，画像の空間周波数［DG04］の高低に注目することで，細々した画像やそれ以外の画像（おおまかな画像）に分類し，それぞれに適した囮画像生成法を適応することができるかもしれない．これらについては今後の課題として検討をしていく予定である．

7章　総括的な考察

7.1　3方式のパフォーマンスと併用

本節では，本論文で論じてきた3種類の方式（RVC方式，Q&R方式，ADG方式）における本人拒否率（FRR）と攻撃成功率（ASR）について検討する．なお，本論文では，これら3種類の方法をそれぞれ独立した観点から議論してきたが，本研究の最終目標は，それぞれを併用することによって，利便性と安全性を両立した画像認証方式を実現することにある．そこで，本節で，現時点でそれぞれの方式を同時に導入した場合の状況について触れ，今後の研究の方向性と課題を確認する．4章～6章で行った各方式に関する実験の結果を，FRRとASRについてまとめたのが表7-1である．

表7-1　本人拒否率と他人受入率

	FRR（9択4ターン）		ASR（2択1ターン）
方式	1日後	8日後	覗き見攻撃
不鮮明化画像方式 [HIM05]	0%	2%	92% (46/50)
RVC方式（言語手がかり付き再認方式）	0%	2%	78% (39/50)
Q&R方式（暗示・応答型画像認証方式）	7%	10%	36.80%[26]
ADG方式（囮画像自動生成方式）	8%	6%	96.60%~96.84%[27]

RVC方式では，正規ユーザにm枚のパス画像を記憶させた上で，1回の本人認証にあたってn枚（m＞n）のパス画像を用いて認証を行うm-n対策により，カメラ撮影を用いた覗き見攻撃に対しても一定レベルの耐性を持たせることを目指した．ただし，m-n対策の導入は記憶すべきパス画像の枚数の増加をともなうため，正規ユーザのみ効果的に利用可能なヒント（パス画像に関する言語手がかり）を認証時に与えることで，正規ユーザの負荷増大を抑制した．その結果，不鮮明化画像方式とFRRを同等に保ちながら，攻撃者に非常に有利な2択システムにおいてASRを14%低下させることに成功した．

Q&R方式では，不鮮明化画像の特徴を効果的に利用することによって画像認証のC&R化を図り，カメラ撮影を用いた覗き見にも耐性を有した方式の実現を目指した．チ

[26] Q&R方式における覗き見攻撃の実験は，パス画像が特定されたことを想定した環境で実施されている．すなわち，どの方式よりも攻撃者に有利な条件で攻撃実験が実施されている．
[27] 不鮮明化画像方式におけるなりすまし成功率 P1＝0.92（92%），自然不鮮明化画像と加工不鮮明化画像の識別成功率 P2＝0.575～0.605（57.50~60.50%）とすると，ADG方式におけるなりすまし成功率は，1-(1-P1)(1-P2)と試算できる．

ャレンジの意味を隠す（正規ユーザ本人にしかチャレンジを理解することができないようにする）というアプローチを採ることによって，簡素なレスポンス生成処理を採用した場合であっても，あるレベルの安全性が担保される暗示・応答（Q&R）型画像認証の構築を達成した．Q&R 方式は，C&R 化の導入により，不鮮明化画像方式や RVC 方式よりもさらに ASR を低減することを可能にした．しかし，Q&R 方式の FRR は若干ではあるが他の方式よりも高い．この原因の多くは 5.4 節の実験結果から得られた知見を元に解決可能であると考えられるが，画像中の細かい部位の情報を使えば使うほど，認証方式が再認課題から再生課題（もしくは再構成課題）に近づいていきユーザの負荷は増大していくと予想される．そのためスキーマを持つ正規ユーザが細かな部位までも正確に想起できるような不鮮明化アルゴリズムの検討も必要になるだろう．

ADG 方式はあくまでも囮画像の自動生成に焦点をおいた方式であり，FRR や ASR を低下させることを目的にしたものではない．しかし，生成される囮画像（加工不鮮明化画像）が自然不鮮明化画像と見分けがついてしまう場合（識別率が 50%から外れる場合）は ASR が増加し，生成される囮画像がパス画像の不鮮明化画像と混同しやすい場合は FRR が増加することになる．ASR の観点からは，現状では自然不鮮明化画像と加工不鮮明化画像の識別率が約 60%であるため，自然不鮮明化画像と加工不鮮明化画像との差を利用した推測攻撃が不可能ではない状態となっている．今後は囮画像生成法のさらなる改善が必要である．FRR の観点においては，パス画像から作った囮画像を利用した場合は，正規ユーザの誤認識および認識負荷の増加につながってしまっている．これに対しては，実際の運用時においては，パス画像だけから囮画像を生成するのではなく，正規ユーザにとって馴染みの無い画像（未知画像）からも囮画像を生成するなどの工夫が必要になると考えられる．

ここで 3 方式の併用について議論する．RVC 方式と Q&R 方式はどちらも覗き見攻撃耐性が高い方式であるため，併用することによってさらに覗き見攻撃への耐性が向上すると期待される．しかし Q&R 方式の利便性（認証成功率および回答時間）は RVC 方式のそれと比べると低い．RVC 方式の利便性は残したまま，より高い攻撃耐性を持たせるには，各種パラメータ（RVC 方式における m と n，Q&R 方式における部位の数や閾値 θ など）を適切に調整した上で両方式を併用していく必要があるだろう．一方，ADG 方式とその他の 2 つの方式との併用に関しては，ADG 方式における囮画像生成法がまだ不十分なため（識別成功率が 60%前後），加工不鮮明化画像（自動生成された囮画像）の特徴を利用した推測攻撃により，ASR が増大する可能性が高い．そのため，本研究の今後のステップとしては，まずは，Q&R 方式におけるユーザの負荷の軽減および囮画像生成法の精度の改善に焦点をおいた解決策の検討が急務となるだろう．

以降では本研究全体の課題とその改善策について簡単に議論していく．個々の対策については各章にて既に議論しているため，共通の課題およびその対策についてのみ議論する．

7.2 利便性を改善する方法

Q&R 方式や ADG 方式（パス画像のみから囮画像を生成する場合）では FRR が低下している．また，両方式においては認証にかかる時間が増加しているためにユーザビリティの低下が懸念される．また，Q&R 方式や RVC 方式においては，画像のタグ付け（部位の登録や画像に対してラベルを付与するなど）を認証情報の登録時に行ってもらう必要がある．この作業は登録時の利便性を損ねてしまう．そこで本節では，ASR を増加させることなく FRR やユーザビリティを改善するための方法を検討する．

7.2.1 ユーザに馴染みが深い画像の利用

合わせ絵[TK02]などで採用されている方法と同様に，ユーザが自分で撮影した写真をパス画像として登録することで，ユーザは自分に関連が深い画像を利用することができるため，パス画像の想起をさらに容易にすることが可能であると考えられる．例えば，老齢のユーザであっても，孫の写真など，愛着や馴染みが深い画像をパス画像として用いることができるため，認証をより高い精度で素早く通過できるようになることが期待される．この方法を採用する際に問題となるのは，ユーザの言動やまわりの環境から，当該ユーザのパス画像を推測される可能性がある点と，パス画像が漏洩した際にプライバシ情報の漏洩につながる恐れがある点である．しかし，写真やイラスト画像をそのまま使用する方式とは異なり，本研究のパス画像は不鮮明化されているため，上記の問題は発生しにくく，ASR の増加やプライバシ情報の漏洩には繋がらないと考えられる．ただし，孫の写真をパス画像として使用する例では，たとえオリジナル画像を見ることはできなくとも，ユーザの家族や近隣の住人といった被写体（孫）の容姿や仕草を見慣れている人々はその情報をスキーマとして用いることで，当該ユーザのパス画像を特定することが可能かもしれない．実際にこの方法を採用した場合の，FRR の低減効果や，ユーザにごく身近な人物を仮定した被験者による ASR の実験を行う必要があるだろう．

7.2.2 画像のタグ付け

Q&R 方式では，登録時にパス画像のタグ付け（「左前足」，「右前足」などの登録）が必要である．また RVC 方式においても，パス画像の手がかりを表示するために，画像に対してタグ（手がかり）を登録する必要がある．しかし，タグ付け作業は正規ユーザにとって面倒な作業である．それゆえ，あらかじめタグ付けされた画像を扱うことも検討していくべきである．

この課題に関しては，reCAPTCHA[REC]を代表とする human computation の研究分野の技術の活用が考えられる．reCAPTCHA とは，有害なプログラムを除外する為の CAPTCHA を人間に解かせる一方で，人間に「別の問題」も解いてもらうことで，人間の能力をより有効に活用していくシステムである．「別の問題」の例として，OCR（Optical Character Reader）で読み取れなかった書籍等の文字列を解読することなどがある．例えば reCAPTCHA のサイト[REC]では，CAPTCHA 画像と reCAPTCHA 画像を

ユーザに同時に提示し，CAPTCHA 画像で有害プログラムを除外し，reCAPTCHA 画像で書籍のスキャニングを自動的に行うことが試みられている（図 7-1）．

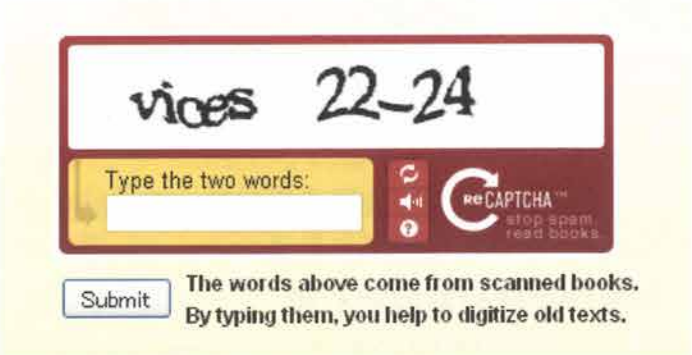


図 7-1　reCAPTCHA の例[REC]

reCAPTCHA 以外には，自動的に画像にタグ付けを行う技術の利用が考えられる．その一手法である PeekaBoom では，「場所当てゲーム」を通じて，画像のタグ付けを行う[ALB06]．このゲームでは，インターネットを介して 2 人（PEEK と BOOM）が対戦ゲームを行う．

今，BOOM が PEEK に対してクイズを出すとする．BOOM は「鼻」を答えとしたクイズを PEEK に与えようとしている（BOOM は PEEK に「鼻」と答えてほしい．）．BOOM は「鼻」が写っている画像を PEEK に送る．PEEK は送られてきた画像から BOOM の期待する答えを推測し回答する．BOOM は，PEEK の回答が正しければ正解と答え，間違っていれば答えの部位付近（鼻付近）に印を付けてヒントを与える（図 7-2）．PEEK はヒントを使ってさらに答えを推測する．このように，場所当てゲームを通じて，画像のタグ付けを自動的に行っていくのである．

PeekaBoom を利用することで，タグ付けされた多くの画像を自動的に収集すること（図 7-3）が可能であり，Q&R 方式や RVC 方式における登録時の手間を省くことができると期待される．

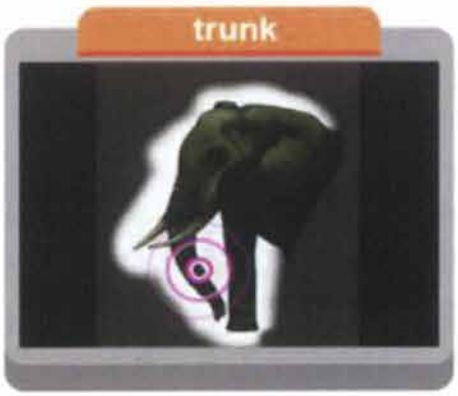


図 7-2　PeekaBoom で画像の部位のタグ付けを行う例（象の鼻）[ALB06]

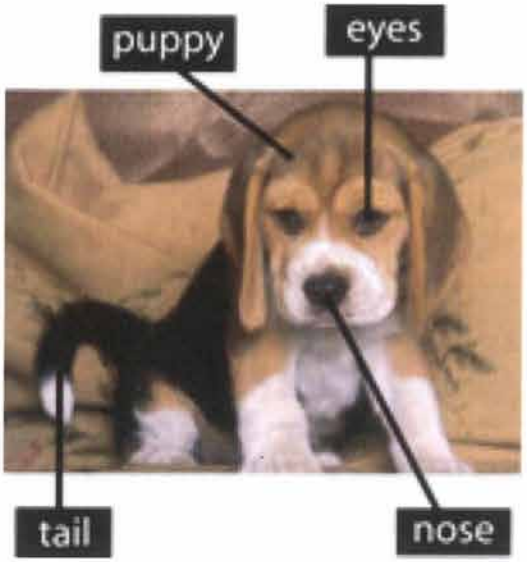


図 7-3　PeekaBoom で部位のタグ付けをされた画像の例（犬）[ALB06]

7.2.3　心地よいセキュリティ対策（エンターテイメント性の付与）

鈴木らは，CAPTCHA 導入時のユーザの利便性の低下を，従来とは異なるアプローチによって解決することを試みている[SYN09]．具体的には，人間にとって「心地良い（エンターテイメント性を有している）」CAPTCHA を構築することで，多少時間を要する方式であったとしても，煩わしさを感じさせない CAPTCHA を実現することを提案している．

その実現例の 1 つとして，4 コマ漫画を利用した CAPTCHA が示されている．4 コマ漫画の各コマをランダムに並べ替えて表示し，正しい順序を答えることができた者を人間として判定する（図 7-4）．4 コマ漫画のそれぞれのコマがランダムに並べ替えられていたとしても，人間であれば各コマの絵や台詞の意味を理解でき，各コマの順序をどのように並べたら面白いストーリーになるのかも類推することが可能である．そのため，4 つのコマを正しい順番に並べ替えることは人間にとっては容易に実行可能であると考えられる．

一方，コンピュータは，第一に，各コマの絵や台詞の意味を認識することが困難である．そして，たとえコンピュータの画像処理能力，言語処理能力が発達し，各コマの絵や台詞の意味を理解することができたとしても，「何がどうして面白いのか」というユーモアを理解することができない限り，コンピュータが 4 つのコマを正しい順番に並べ替えることは不可能である．特に，漫画の中には「暗黙の了解」や「場の空気」といった，明示的な会話となって現れない場面が往々にして存在するため，近未来の技術を持ってしても，そのような暗黙的な意味（ユーモア）までをも解するレベルの自動機械（マルウェア）を実装することは不可能に近いと考えられる．

そして，漫画を読むことは人間にとって楽しい（エンターテイメント性を有している）ため，4 コマ漫画 CAPTCHA であれば，正規のユーザが利便性の低下を感じることなく，心地良く（楽しみながら）チューリングテストを受けることができると考えられる．

図 7-4　鈴木らの CAPTCHA[SYN09]の認証画面例
（出展：左から 1 番目の図：文献[UE06]の p.25 の 4 コマ漫画の 1 コマ目，2 番目の図：同，p.25 の 4 コマ目，3 番目の図：同，p.25 の 3 コマ目，4 番目の図：同，p.25 の 2 コマ目）

鈴木らはエンターテイメント性という概念を CAPTCHA に適用しているものの，この考え方の利用が効果を発揮すると期待される範囲は CAPTCHA にとどまるものではなく，個人認証をはじめ様々なセキュリティ技術に応用可能であると考えられる．エンターテイメント性の付与による利便性の改善については，今後の重要な検討事項になっていくだろう．

7.3　その他の攻撃法

本研究はこれまでパス画像の覗き見攻撃に注目して論じてきたが，画像認証方式に対して行われ得る他の既存の攻撃法について，本節で検討する．

7.3.1　Educated-Guess 攻撃

Educated-Guess 攻撃は，特定のユーザの性格，言動，趣味，嗜好，周囲の環境などの情報を収集し，その情報をもとに当該ユーザのパスワードを推測してなりすましを試みる攻撃である[DP02]．例えば，「A さんは猫好きで有名だから，パス画像も猫の画像を含むに違いない」という要領でユーザ A のパス画像を推測する．また，表示される画像同士の関連性に注目し，同一ユーザに関連する画像であることを推測し，なりすましのための情報として利用することも考えられる[OTK05]．多くの画像認証方式では，自分の好きな画像をパス画像として登録する方式を採用しているため，Educated-Guess 攻撃が大きな脅威になる．ただし，本方式は不鮮明化画像をパス画像として用いるため，例えば「正規ユーザは猫をパス画像にしている」という知識のみではパス画像（不鮮明化画像）に対する正確なスキーマを得られず，正解のパス画像を選択することは困難であ

る．このことは 4.3.2 節の RVC 方式に対しての攻撃成功率の低さからも確認することができる．すなわち，不鮮明化画像を利用する本研究の認証方式においては，Educated-Guess 攻撃の危険性は他の方式よりも低いと考えられる．

ただし，5.4.2 節の Q&R 方式に対する攻撃実験では，動物画像の構図を仮定した上で，部位の意味（手，足，尻尾等）を類推することが攻撃者にある程度可能であるという結果が得られている．もし攻撃者が正規ユーザのパス画像の種類（例えば，動物）を Educated-Guess 攻撃により推測できたとした場合は，本方式に対する脅威となると考えられる．この問題に対しては，不鮮明化アルゴリズムを改良したり，画像を歪めたりすることによって画像の構造を崩した上で不鮮明化するなどの方策を検討する必要がある．

7.3.2 Exhaustive 攻撃と Intersection 攻撃

Exhaustive 攻撃とは，毎回の認証で認証画面中の画像一枚一枚に当たりをつけ，「その画像を選択して認証に失敗したならば，その画像はパス画像ではない」というように，パス画像の候補を徐々に絞っていく攻撃である．一方，Intersection 攻撃とは，毎回の認証で出現頻度の高い画像をパス画像の候補として徐々に絞っていく攻撃である．これらの攻撃に対しては，6.1 節で示したように，パス画像と囮画像の出現頻度を同等にすることである程度は耐性を持たせることができる．

また，Intersection 攻撃に対しては，認証画面中にパス画像が存在しないという選択肢を加えることで，必ずしも画面上にパス画像が出現するとは限らなくすることで対策することも可能である．ただし，不鮮明化画像を用いる場合は，正規ユーザであってもパス画像が画面に出現しているか否かを判断するのに相応の負担がかかると予想される．このため，正規ユーザの負荷への影響について実験により確かめる必要があるだろう．

7.4 アクセシビリティの問題

CAPTCHA[ABH03]においては，視覚障害者がサービスを享受できなくなるという Web アクセシビリティに関する課題が社会的な問題として指摘されだしている[CNE04][W3C][Ono05]．これは，CAPTCHA のみにとどまらず，画像や図形などの視覚的情報を用いる認証方式全体の問題でもある．

基本的に，視覚情報をユーザに提示して認証に利用する方式は，視覚障害者のアクセシビリティを確保することはできない．ただし，障害や先天的性質などによって特定のユーザがシステムの対象から外れてしまうことは，パスワード認証や生体認証などの他の認証方式でも必ず発生する問題である．アクセシビリティの問題は，単独の認証方式のみによって完全な解決が望める問題ではない．そのため，実際に業務やサービスのシステムを実装する際は，いくつかの性質が異なる認証方式を同時に採用し，その中からユーザに選択させるという運用でカバーするような現実的な対策が必要となるだろう．その場合，ユーザの利便性やアクセシビリティが向上する代わりに，認証システム全体

のセキュリティが最も強度の低い認証方式のレベルに低下してしまうことのないような対策が必要である[TMI03].

本研究は，画像の記憶を認証に利用することや，再認方式によって認証を行うことで，従来の文字の再生に基づくパスワード方式と比較して，加齢による記憶の衰えの影響を受けにくくなっていると期待できる．ただし，本論文の実験で協力してもらった被験者は全員 20 歳代であり，高齢者に対する実験データは得られていない．本研究で使用する画像は不鮮明化処理を行うことで通常の写真画像などに比べると認識の負荷が高くなっていると考えられる．さらに，Q&R 方式に関して言えば，画像の細かな部位の指定を必要とするため，再認課題から再生課題（もしくは再構成課題）に近づいている可能性もある．そのため，7.2 節に示した FRR やユーザビリティを改善する方法と併せて，高齢者のアクセシビリティに関して，今後さらに実験を行って確かめていく必要がある．

7.5 不鮮明化画像

本研究では，不鮮明化画像方式の文献[HIM05]の中で提案された不鮮明化アルゴリズムをそのまま採用し，新しい認証方式の実現を試みた．不鮮明化画像に関しては，文献[HIM05]の中でも議論されているが，以降では，本研究特有の課題について議論していく．

Q&R 方式において，「覗き見情報無し（z=0）」であっても，攻撃者はキュー（パス部位）に対応する場所を 30%～40%の割合で選択することができてしまっている．これは，今回用いた不鮮明化画像の意味が攻撃者にある程度類推可能であったことが原因と考えられる．実験後のヒアリングでも，被験者が実験で用いた画像の特徴を活用してパス部位を推定していたことが確認できている．すなわち，被験者は画像の上部には動物の「頭」，画像の下部には動物の「足」がある可能性が高いといったことや，「目」，「耳」，「鼻」，「口」は比較的お互い近い位置関係にある可能性が高いといったことを仮定することで，パス画像と参照画像の部位を効率的に推測していた．

この問題に対応する手段として，画像における一般的な知識（画像の構造：画像の上部に頭があり，下部には足がある等）を崩した上で不鮮明化する方法が考えられる．例えば，歪めた画像を不鮮明化してパス画像や参照画像に用いてやれば，一般的な知識と歪められた画像の構造がマッチせず，攻撃者がパス画像や参照画像の内容を推測することを困難にすることができると考えられる．ただし正規ユーザが，歪めた不鮮明化画像を長期の間，記憶することができるかについては，今後調査が必要である．

また，不鮮明化画像の特徴を活用して，部位の位置を類推するという攻撃も考えられる．例えば，不鮮明化画像中に特徴的なエッジが認識できる場所は部位として登録されている可能性が高い．特徴的なエッジを排除できるような不鮮明化アルゴリズムが必要ではあるが，それによって正規ユーザのスキーマの形成が阻害されてはならない．特徴的なエッジが無くとも，正規ユーザに認識が容易な不鮮明化アルゴリズムの検討が必要である．

7.6 関連方式との比較

本節では，本研究で着目した不鮮明化画像方式[HIM05]，写真を利用した最もオーソドックスな画像認証[PSL03]，人工画像を利用した画像認証[DP02]，画像認証の C&R 化を図った Sobrado の方式[SB02]，暗証番号の入力を C&R 化した Roth らの方式[RRF04]について，本研究の方式との比較に基づく考察を行う．それぞれ，「不鮮明化画像方式」，「写真画像方式」，「人工画像方式」，「CHC 方式(Convex Hull Click)」，「PEM 方式（Pin Entry Method）」と略記する．

これらの方式と本研究の方式（RVC 方式，Q&R 方式，ADG 方式，およびそれらの併用）を含めた 9 方式について，利便性と安全性について比較したものが表 7-2 である．なお，本節でいう利便性とは，認証情報を登録する際の負荷（登録時間，記憶容易性），認証時の負荷（認識容易性，作業容易性），および囮画像の用意の簡便性を意味する，安全性とは，覗き見攻撃，ランダムクリック攻撃，言葉による認証情報の漏洩，Educated-Guess 攻撃，Intersection 攻撃，Exhaustive 攻撃を意味する．

表 7-2　記憶負荷と安全性についての比較

		提案方式				不鮮明化画像方式	写真画像方式	人工画像方式	CHC 方式	PEM 方式
		RVC 方式	Q&R 方式	ADG 方式	総合					
利便性	記憶容易性	○	○	○	○	○	◎	○	◎	○
	登録時間	△	×	○	△	○	◎	○	△	△
	作業容易性	◎	○	○	○	◎	◎	◎	△	○
	囮画像の用意	△	△	○	○	△	△	◎	△	-
安全性	ランダムクリック攻撃耐性	△	◎	△	◎	△	△	△	×	△
	覗き見攻撃への耐性	○	◎	△	◎	△	×	×	◎	△
	言葉による漏洩への耐性	◎	◎	◎	◎	◎	×	○	×	×
	Educated-Guess 攻撃耐性	◎	◎	◎	◎	◎	×	○	×	×
	Intersection 攻撃耐性	○	○	△	○	△	△	△	○	○
	Exhaustive 攻撃耐性	○	○	△	○	△	△	△	○	○

● 記憶容易性

記憶容易性とは，認証情報の記憶のしやすさに関する指標である．Dhamija らの研究[DP02]において，人工画像よりも写真画像を用いるシステムのほうが，記憶が容易となることを示す結果が得られている．不鮮明化画像方式もまた，劣化した画像を利用してはいる分，オリジナルの写真画像を用いるシステムに比べて記憶容易性は低いと考えられる．本研究においても不鮮明化画像を用いており，4 章の実験結果から RVC 方式におけるユーザの記憶負荷は不鮮明化画像方式と同等程度であるといえる． Q&R 方式および ADG 方式においては，5 章および 6 章の実験結果から，記憶負荷および認識負荷の点で不鮮明化画像方式や RVC 方式よりも幾分劣化していることが分かる．ただし，その課題の多くは，実験により得られた知見を元に解決可能だと考えられ，RVC 方式に比べそれほど記憶負荷が高いというわけではないといえるだろう．CHC 方式はイラストや写真等のアイコンを利用しているため，写真画像方式と同様に記憶負荷は低いと考えられる．PEM 方式では 4 桁暗証番号を記憶し，それを正確に想起しなければいけないという点で，再生課題となっており，写真画像を使った方式に比べ記憶負荷は大きいといえる．

● **登録時間**

登録時間とは，認証情報の登録に要する時間である．再認型の画像認証方式に関してはパス画像を記憶するだけであるため，登録に要する時間は少ない．CHC 方式，PEM 方式は，多少複雑な方法を使って認証を行うため，ユーザが認証方式を理解するまでに時間を要すると考えられる．一方，RVC 方式はタグ情報（手がかり）を登録するための時間が，Q&R 方式には各部位の情報を登録するための時間がかかる．Q&R 方式においては，さらに，パス部位を正しく認識できるかを確認するためにある程度練習をする必要がある．

● **作業容易性**

作業容易性とは，認証時における認証情報（パス画像）の認識のし易さや認証作業の簡便さに関する指標である．従来の再認型画像認証方式は，複数の画像の中からパス画像を選択するだけであるため，作業自体は単純である．また不鮮明化画像や人工画像に比べるとイラストや写真は意味を認識し易い．一方，CHC 方式や PEM 方式では，大量のアイコンの中から自分のアイコンを探し出したり，単純な選択を多数回繰り返したりしなければならないため，作業容易性は低いといえる．Q&R 方式においても，複数の画像の中からパス画像を探す作業に加え，キューに対応する部位をパス画像の中から選択する作業が増える分，従来の再認型画像認証方式よりも作業が複雑になっているといえる．ただし，5.4.1 節の本人認証実験の結果（特に認証時間）からは，Q&R 方式は CHC 方式ほどの作業負荷の増大には至っていないと考えられる．ADG 方式においては，パス画像から作った囮画像を利用した場合，正規ユーザの認識負荷が増加する結果が得られている．しかし，パス画像だけから囮画像を生成するのではなく，正規ユーザにとって馴染みの無い画像（未知画像）からも囮画像を生成してやれば，囮画像が正規ユーザの認証作業に悪影響を与えることは少ないと考えられる．RVC 方式においては，正規ユーザに一回の認証に必要なパス画像の枚数よりも多くのパス画像を記憶させているが，4.3.1 節の本人認証実験の結果より，不鮮明化画像方式と同程度の認識負荷に抑えることができている．

● **囮画像の用意**

囮画像の用意とはユーザにとって馴染みのない新しい囮画像をどれだけ簡単に用意することができるかを示す指標である．囮画像の完全な自動生成を実現している方式は人工画像方式である．乱数を引数とするランダムな計算方法によって生成された抽象的な幾何学模様の人工画像は，乱数を変えれば異なる人工画像を無限に得ることが可能である．また，人工画像のもとになる乱数を保存しておけば人工画像そのものを保存しておく必要がなく，認証システムのストレージ容量を節約できることも利点である．人工画像方式に次ぐ方式は ADG 方式である．現段階では，攻撃者が加工不鮮明化画像の特徴を活用してパス画像と囮画像とを識別することができる可能性はゼロではない．また，パス画像のみから囮画像を生成した際に，正規ユーザの認識負荷が高まるという課題も残っている．しかし，これらの課題については考察で示した方法によりある程度は解決

することができると考えられ，人工画像方式に近いレベルの囮画像の自動生成も可能になると考えられる．PEM 方式においては，囮画像の概念は存在しない．その他の方式においては囮画像の問題を解決する方式はない．

● **ランダムクリック攻撃**

ランダムクリック攻撃については，複数の画像の中からパス画像を選択するような従来の再認型画像認証において，どの方式も大きな差はないと考えられる．囮画像の枚数や選択の繰返しを増やせば，ランダムクリック攻撃への耐性向上につながるが，利便性の低下は免れない．CHC 方式においては，画面の中心をクリックすれば 30%程度の確率で正規ユーザになりすますことが可能であることが示されており，従来の再認型画像認証よりも耐性が低いと考えられる．PEM 方式の安全性は暗証番号のそれと同等であるが，多くの問答の繰り返しが必要とされる．Q&R 方式においては，画像の選択に加え，画像の細かな部位の選択までも必要とするため，他の方式に比べるとランダムクリック攻撃への耐性が高いといえる．

● **覗き見攻撃**

覗き見攻撃については，従来の再認型画像認証方式である写真画像方式および人工画像方式は，覗き見攻撃に対して脆弱であることが，不鮮明化画像方式の論文[HIM05]の中で報告されている．不鮮明化画像方式は，従来の再認型画像認証方式よりも覗き見に頑強ではあるが，複数回の覗き見やカメラ撮影を用いた覗き見攻撃に対しては耐性を有していない．PEM 方式は，肉眼での覗き見は困難であるが，1 回の認証作業の全てをカメラで撮影された場合，暗証番号が一意に特定できてしまい，十分な耐性を有しているとは言えない．一方，RVC 方式，Q&R 方式，CHC 方式は複数回の覗き見に耐えることができ，覗き見攻撃耐性は他の方式よりも高い．

● **言葉による認証情報の漏洩**

正規ユーザからの言葉によるパス画像の漏洩への耐性に関しては，言語化のしやすさと，その意味内容の伝えやすさなどから，鮮明な写真やイラストを利用する写真画像方式や CHC 方式，および，暗証番号を利用する PEM 方式の耐性が最も低いと考えられる．人工画像方式は，抽象的な人工画像を用いることにより，正規ユーザからの言葉によるパス画像の漏洩に対する耐性の向上を図っているが，カラー／モノトーンを問わず 100%の確率で言葉による漏洩が成功するという結果が文献[HIM05]の中で報告されている．一方，不鮮明化画像を使う方式では，写真画像方式や人工画像方式と比べて，言語によるパス画像漏洩に対する耐性が高いことが，文献[HIM05]の実験により確認されている．そのため，不鮮明な画像を利用する不鮮明化画像方式および本研究における言葉によるパス画像の漏洩への耐性は高いと考えられる．

● **Educated-Guess 攻撃**

Educated-Guess 攻撃に関しても不鮮明化画像を使った方式は強い耐性を有している．オリジナル画像（スキーマ）を知らなければ，不鮮明化画像の意味を類推することは困難である．そのため，無意味に見える画像の中から，特定のユーザの性格，言動，趣味，

嗜好，周囲の環境などの情報を収集し，その情報をもとに当該ユーザのパス画像を推測しようとすることは難しい．また抽象的な人工画像を利用している人工画像方式においても，ある程度の Educated-Guess 攻撃耐性を有していると考えられる．

● **Intersection 攻撃および Exhaustive 攻撃**

人工画像方式，写真画像方式の代表的な方式や本研究は，「パス画像は固定であり，複数の囮画像の中から正しい画像を選ぶ」という認証の根本の方式は同じであるので，7.3 節で述べた Intersection 攻撃，Exhaustive 攻撃などによるパス画像の類推に対して本質的な脆弱性を有する．しかし，RVC 方式においては，4.4.2 節で述べたように m-n 対策と手がかりの活用の仕方によってはパス画像と囮画像の出現頻度をある程度調整することが可能なため，他の方式に比べると Intersection 攻撃や Exhaustive 攻撃への耐性を有しているといえる．また Q&R 方式，CHC 方式，PEM 方式においては，従来の再認型画像認証とは認証情報の入力方法が異なる分，Intersection 攻撃や Exhaustive 攻撃を実行しにくいと考えられる．

以上を踏まえると，総合的に判断して，本研究は有効性が高いと判断することができる．ただし，本研究で提案した 3 つの方式は依然として解決すべき点も多く，3 方式の併用に向け，十分な対応が必要であろう．

8章　結論

8.1　本論文のまとめ

本論文は，現状で最も普及しているパスワード認証方式において，人間的要因を軽視するがゆえに引き起こされる記憶負荷の高さに関する問題点を解消する方式として，近年多数の研究が試みられている画像認証方式に注目した．そして，画像記憶の優位性に加えて，一見すると無意味に見える不鮮明な画像の特長に注目することで，従来の画像認証方式で大きな課題となっていた以下の 2 つの課題を克服した新たな認証方式を実現することを目指し，研究を遂行した．

イ) 覗き見の問題
　覗き見攻撃に対して脆弱である．
ロ) 囮画像の問題
　囮画像の用意およびその更新が難しい．

2 章において，画像認証に関する本研究を行う重要性や意義について述べた後に，本研究の関連研究として，パスワード認証方式をさまざまに拡張することで，その安全性の向上や記憶負荷の低減を図った既存研究を多数取り上げ，それぞれの特徴および課題についてまとめた．（イ）と（ロ）の両課題を同時に克服した認証方式は存在しないことを示し，本研究の位置付けを明確にすることで，既存研究に対する本研究の独自性を明らかにした．

3 章では，本研究において重要な役割を持つ不鮮明化画像方式（画像記憶のスキーマを利用した認証方式）を紹介し，その有効性と課題を示した．不鮮明化画像方式は，人間の認知の特性である画像記憶に関する「スキーマ」をうまく利用することで，正規ユーザには記憶しやすいが，それ以外の他者には記憶が困難となるようなパス画像を認証に利用した方式である．これを実現するために，有意味なオリジナル画像に対して不鮮明化処理を施して作成された，一見すると無意味に見える「不鮮明化画像」をパス画像として利用している．

4 章では，画像認証における(イ)の課題（覗き見の問題）に焦点を当て，不鮮明化画像を用いた認証方式に対して m-n 対策の導入を試みた．m-n 対策は正規ユーザが記憶すべきパス画像の枚数（m 枚）を増加させることになるが，「パス画像を思い出すにあたっての手がかりとなる情報を認証時にヒントとして提示する」ことによって，その記憶負荷の低減を達成する RVC 方式を提案した．ここで，「スキーマを持たないユーザは，オリジナル画像に関する言語手がかりを与えられたとしても，不鮮明化画像の意味を類推することが困難である」という不鮮明化画像の特長が巧みに利用されている．実験により，RVC 方式の利便性（正規ユーザの記憶負荷）や安全性（認証率およびなりすまし成功率）について評価を行った．実験より RVC 方式は，不鮮明化画像方式と比べ正規

ユーザの負荷を同程度に抑えながら，覗き見攻撃（カメラ撮影も含む）への耐性向上を実現していることを確認した．

5章では，画像認証の(イ)の課題（覗き見の問題）へのもう1つの取り組みとして，画像認証の C&R 化を試みた．ただし，人間の計算能力の限界に鑑みるに，チャレンジからのレスポンス生成に暗号計算が必要となる通常の C&R 型認証を適用することは不可能である．そこで，「スキーマを持たないユーザは，不鮮明化画像の意味を類推することが困難である」という特長を有する不鮮明化画像をチャレンジとして利用し，簡素なレスポンス生成処理を採用した場合であっても，不正者にはパス画像が容易には推測できない暗示・応答（Q&R）方式を提案した．Q&R 方式では，チャレンジの意味を隠す（正規ユーザ本人にしかチャレンジを理解することができないようにする）というアプローチによって認知心理学的に C&R 型認証の安全性を担保しており．実験により，Q&R 方式の利便性（正規ユーザの記憶負荷）や安全性（認証率およびなりすまし成功率）について評価を行った． 実験結果から，Q&R 方式が従来の C&R 型画像認証に比べ，認証負荷を抑えつつ，同等以上の覗き見攻撃耐性（カメラ撮影も含む）を実現することを確認した．不鮮明化画像方式に比べると若干のユーザの負荷の増加が認められるものの，その原因の多くは実験で得られた知見を元に解決することが可能であると考えられる．

6章では，画像認証の(ロ)の課題（囮画像の問題）に焦点を当て，囮画像の自動生成を試みた．ここで，「簡素な画像処理によって，オリジナル画像と不鮮明化画像の間のスキーマを切断することが可能である」という不鮮明化画像の特長を活用し，正規ユーザにとって馴染みの無い囮画像を自動的に大量に生成する ADG 方式を提案した．実験により，生成された囮画像が利便性（囮画像が正規ユーザのパス画像の記憶・想起を阻害することはないか）および安全性（不正者がどの程度囮画像を識別可能か）の面でどのような影響を与えるのかについて評価した．実験結果から，ADG 方式で得られた囮画像は，攻撃者にとって概ね自然な囮画像になっていることが示された．その一方で，パス画像から生成された囮画像を認証に利用してしまうと，正規ユーザの認識負荷が幾分増大するという課題も見つかった．この問題については，パス画像からだけでなく，正規ユーザにとって馴染みの無い画像も囮画像の加工に加えることで，解決が可能であると考えられる．

7章では，4~6章における3つの方式（RVC 方式，Q&R 方式，ADG 方式）の特徴や実験結果を踏まえ，それぞれの方式を同時に導入した場合の総合的な考察を行った．また，覗き見攻撃以外にも想定される各種攻撃，および，囮画像の用意以外にも想定される利便性やアクセシビリティの問題などに関して考察を加えた．そして，本研究と最も関連の深い既存研究である，写真画像の再認を利用する認証方式，人工画像の再認を利用する認証方式，画像認証の C&R 化を行う Sobrado らの方式，暗証番号の C&R 化を行う Roth らの方式，および，不鮮明化画像の再認を利用する不鮮明化画像方式を対象として，本研究の3つの方式との比較検討を行い，本研究の方式の優位性を示した．

以上が，本研究で得られた成果である．

8.2 今後の展望

最後に，本研究の今後の展望について述べる．本論文では一般的なパソコン上で実装した実験システムを用いたが，本研究の適用範囲はパソコン用の認証システムに留まるものではない．銀行 ATM や駅の券売機などタッチパネルディスプレイが装備された機器であれば，容易に導入することが可能である．

また近年，iPhone や android 携帯を代表とするスマートフォン，kindle や iPad を代表とするタブレット型端末等，タッチパネルディスプレイを搭載した小型の携帯端末が急速に普及し始めている．チケット購入機能[ITD10]やクレジットカード機能[WWW10]など金銭のやり取りを携帯端末から実行することはもちろんのこと，ユーザの情報（位置情報，生体情報，声，趣味嗜好，個人情報等）を携帯端末のセンサで収集し，得られた情報から新しいサービスを展開することも次第に増えていくと考えられる．そのためユーザの情報を取り扱う携帯端末の安全性の確保は必須であり，セキュリティの第一関門である個人認証の高度化は急務といえる．しかし 2.2 節でも述べたが，所有物に基づく認証方式は，紛失・盗難の恐れがあるといった本質的な課題を解決しなければならない．また，持ち物（携帯端末）を守るために新たな持ち物（認証トークン）を持つことは理にかなっていない．個人の生体的特徴に基づく認証方式においては，生体情報自体が個人のプライバシ情報であるということや，認証情報そのものが漏洩しやすく，万が一漏洩した際に生体情報の変更が容易ではないという，本質的な課題が多く残っている．

本研究において著者が注目してきた画像認証は，何も所有する必要がなく，いつでも何度でも認証情報を変更することができるという個人の記憶に基づく認証方式の最大のメリットを持ち，かつ，記憶負荷が少なく，ディスプレイと簡易な入力装置さえあれば，容易に実装可能である．それゆえ，スマートフォンやタブレット端末等の小型の携帯端末用の個人認証方式として最も有力な候補になりうると考えられる．携帯端末はユビキタス社会を支えていく重要なツールである．安心安全なユビキタス社会を実現する 1 つの技術として，画像認証は広く利用されていくと期待している．本研究においても，ディスプレイや入力装置が小型のシステムでも利便性と安全性を十分確保できるよう，提案方式の各種パラメータを調整し，評価・検討を行っていく必要がある．

謝辞

本研究を進めるにあたり，指導教員として粘り強く，常に的確できめ細やかなご指導を賜り，常に励まし続けてくださった 静岡大学創造科学技術大学院 西垣 正勝 教授に心より御礼申し上げます.

本研究の立ち上げ当初より認知心理学の分野について懇切にご教授いただきました静岡大学情報学部情報社会科 漁田 武雄 教授に，感謝の意を表します.

副指導教員・博士論文審査委員として，私の博士論文に関して数多くのご助言を賜りました，静岡大学創造科学技術大学院 渡辺 尚 教授，海老澤 嘉伸 教授に，深謝申し上げます.

研究室の先輩であり，「画像記憶のスキーマを利用した認証方式」を提案し，本研究の礎を築いていただきました，三菱電機株式会社 情報技術総合研究所 原田 篤史 様に，在学中，的確なご支援・ご指導を賜りました．心より感謝いたします.

同じく，研究室の先輩であります，三菱電機株式会社 情報技術総合研究所 柴田 陽一 様に，在学中，厳しく的確なご指導を賜りました，深く感謝いたします.

認知科学の視点から，熱くご指導いただきました静岡大学創造科学技術大学院 竹内 勇剛 准教授に，心より御礼申し上げます.

携帯用認証方式「脳内認証」の共同研究開発を通じて，多くのご支援ご尽力をいただきました．株式会社リムコーポレーション 代表取締役 竹塚 直久様，代表取締役副社長 間淵 雅宏 様に，深謝申し上げます.

コンピュータセキュリティに関する学会・研究会等でいつも的確なご助言を賜りました東京電機大学 佐々木 良一 教授，創価大学 勅使河原 可海 教授，岩手県立大学 村山 優子 教授，東海大学 菊池 浩明 教授，東京工業大学 尾形 わかは 准教授，岡山大学 山内 利宏 准教授，東京理科大学 柿崎 淑郎 助教，に心より感謝申し上げます.

海外研修先で，本研究について的確なご助言を賜りました，UC Berkeley の Doug Tygar 教授に感謝の意を表します.

本研究を進める過程で貴重なご助言をいただきました株式会社日立製作所 システム開発研究所 高橋 健太 様，東芝ソリューション株式会社 加藤 岳久 様，日本電信電話株

式会社 NTT 情報流通プラットフォーム研究所　千田 浩司 様，間形 文彦 様，株式会社 KDDI 研究所　竹森 敬祐 様，株式会社インターネットイニシアティブ 須賀 祐治 様に，深謝の意を表します．

大学入学当初から，励まし指導し続けてくださった静岡大学情報学部情報社会科　西原 純 教授，同学科 Mordecai George Sheftall 准教授に心より感謝申し上げます．

研究活動および就職活動に関し多大なご配慮をいただきました．静岡大学大学院創造科学技術大学院　水野 忠則 教授，静岡大学情報学部情報社会科　市川 照久 教授に心より感謝申し上げます．

静岡県立掛川西高等学校時代の担任教諭であり，高校を卒業してからも温かく応援し続けてくださった，静岡県教育委員会文化課専門監　中山 正典 様に感謝の意を表します．

静岡県立掛川西高等学校時代のクラスメイトであり，同じ博士課程の学生として常に私を励まし心強い味方でいてくれた，首都大学東京　齋藤 仁 様に深く感謝いたします．

最後に，本研究を共に進めてきた仲間として，OB・OG を含めた西垣研究室の皆様に深く感謝いたします．

なお，本研究は科研費（No.20-6290）の研究助成を受けました．

参考文献

[ABH03] Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford: CAPTCHA: Using Hard AI Problems for Security, Advances in Cryptology, Eurocrypt 2003, pp.294-311, 2003.

[ACC02] Antonella De Angeli, Mike Coutts, Lynne Coventry and Graham L. Johnson: VIP: a visual approach to user authentication, Proceedings of the Working Conference on Advanced Visual Interfaces, AVI2002, pp.316-323, 2002.

[AFP09] AFPBB News 記事： 指紋手術し生体認証すりぬけ，国外退去中国人を逮捕，2009 年 12 月 7 日，http://www.afpbb.com/article/disaster-accidents-crime/crime/2672334/5008931 （2010 年 6 月 確認）．

[Aka95] 赤木 正人： カクテルパーティ効果とそのモデル化，電子情報通信学会誌，Vol.78，No.5，pp.450-453，1995.

[ALB06] Luis von Ahn, Ruoran Liu and Manuel Blum. Peekaboom: A Game for Locating Objects in Images, Proceedings of the SIGCHI conference on Human Factors in computing systems, CHI2006, pp 55-64, 2006.

[And94] Ross J. Anderson: Why Cryptosystems Fail, Communications of the ACM, Vol.37, No.11, pp.32-40, 1994.

[AS88] A.M.D. Alvare, E.E. Schultz Jr.: A framework for password selection, Proceedings of Unix Security Workshop II, pp.29-30, 1998.

[AS99] Anne Adams and Martina Angela Sasse: Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures, Communications of the ACM, Vol.42, No.12, pp.40-46, 1999.

[ATS03] 荒川 豊，竹森 敬祐，笹瀬 巌： 入力位置情報を付加したパスワード認証方式，情報処理学会研究報告，2003-CSEC-21，pp.35-40，2003.

[AYT09] 青山 真之，山本 匠，高橋 健太，西垣 正勝： 生体反射型認証－輻輳反射と眼球形状および両眼間距離を利用した認証方式の提案－，情報処理学会研究報告，2009-CSEC-44，pp.85-90，2009.

[Bau] Andrej Bauer: Gallery of random art,
http://www.cs.cmu.edu/~andrej/art/ （2010 年 6 月 確認）.

[Blo96] Greg E. Blonder: GRAPHICAL PASSWORD, United State Patent 5559961.

[Bre99] William F. Brewer: Schemata, In R. A. Wilson & F. C.Keil (Eds.), MIT Encyclopedia of the Cognitive Sciences, pp.729-730, 1999.

[Bru90] V. ブルース著，吉川 左紀子 訳： 顔の認知と情報処理，サイエンス社. 1990.

[BSA05] BSA： 昨年の日本の違法コピー率は１ポイント減の２８%～同損害額は約 1,900 億円と，依然として高水準～，2005 年 5 月 18 日，
http://www.bsa.or.jp/press/release/2005/0518.html （2010 年 6 月 確認）

[CAO] 消費者庁： 個人情報保護法令，
http://www.caa.go.jp/seikatsu/kojin/houseika/dai19/19siryou4-4.html （2010 年 6 月 確認）.

[CER] CERT/CC: CERT/CC Statistics, 1998-2005,
http://www.cert.org/stats/cert_stats.html （2010 年 6 月確認）.

[CNE04] CNET Japan ニュース： スパム封じか，視覚障害者の権利擁護か-揺れる画像認証テスト，2003 年 7 月 3 日，
http://japan.cnet.com/news/media/story/0,2000056023,20059708,00.htm （2010 年 6 月 確認）.

[COM07] Computerworld.jp 記事： IBM，クラウド・コンピューティングの導入支援構想を発表，2007 年 11 月 16 日，http://www.computerworld.jp/news/plf/87249.html （2010 年 6 月 確認）.

[CSE] 株式会社シー・エス・イー： SECURE MATRIX,
http://www.cseltd.co.jp/smx/index.htm （2010 年 6 月 確認）.

[CSI] CSI/FBI（米国）: Computer Crime and Security Survey, 2003.

[Dau04] John Daugman: How iris recognition works, IEEE Transactions on Circuits and Systems for Video Technology, Vol.14, No.1, pp.21-30, 2004.

[DG04] ディジタル画像処理編集委員会（監修）：ディジタル画像処理，画像処理教育振興協会(CG-ARTS 協会)，東京，2004.

[DP02] Rachna Dhamija and Adrian Perrig: Déjà Vu: A User Study Using Images for Authentication, Proceedings of the 9th conference on USENIX Security Symposium, Vol.9, pp.45-58, 2002.

[DW] Arnold G. Reinhold: Diceware, http://world.std.com/~reinhold/diceware.html （2010 年 6 月 確認）

[FH07] Dinei Florencio and Cormac Herley: A LargeScale Study of Web Password Habits, Proceedings of the 16th international conference on the World Wide Web, 2007.

[FK89] David C. Feldmeier and Philip R. Karn: UNIX password security - ten years later (invited), Lecture Notes in Computer Science, Vol.435, 1989.

[FUJ] 富士通株式会社 プレスリリース：世界初！非接触型手のひら静脈認証技術を開発，2003 年 3 月 31 日，http://pr.fujitsu.com/jp/news/2003/03/31.html （2010 年 6 月 確認）.

[Geh02] Edward F. Gehringer: Choosing Passwords: Security and Human Factors, Proceedings of the 2002 IEEE International Symposium on Technology and Society, ISTAS2002, pp.369-373, 2002.

[GHS02] Joseph Goldberg, Jennifer Hagman and Vibha Sazawal: Doodling our way to better authentication, extended abstracts on Human factors in computing systems, CHI2002, pp.868-869, 2002.

[Han00] Martin Handford 著，唐沢 則幸 訳：新ウォーリーを探せ！，フレーベル館，2000.

[HBH98] Arthur E. Hutt, Seymour Bosworth and Douglas B. Hoyt 著，佐野 美知夫 訳：ワイリーコンピュータセキュリティハンドブック，株式会社フジ・テクノシステム，1998.

[HIM05] 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.

[HIT] 株式会社日立製作所 ニュースリリース：開放型の指静脈認証技術，2004 年 3 月 1 日，http://www.hitachi.co.jp/New/cnews/040301.html （2010 年 6 月 確認）．

[HCD07] Eiji Hayashi, Nicolas Christin, Rachna Dhamija, and Adrian Perrig: Use Your Illusion: Secure Authentication Usable Anywhere, CMU CyLab Technical Report CMU-CyLab-07-011, 2007.

[SCH08] Hirokazu Sasamoto, Nicolas Christin and Eiji Hayashi: Undercover: Authentication Usable in Front of Prying Eyes, Proceedings of the 26th annual SIGCHI conference on Human factors in computing systems, CHI2008, pp.183-192, 2008.

[HNY04] 花井 將臣，中村 逸一，吉田 英樹，曽我 正和，西垣 正勝：経験による想起の容易さを利用した認証方式，情報処理学会研究報告，2004-CSEC-24-34，pp.193-198，2004.

[IPA] IPA：ボット対策について，http://www.ipa.go.jp/security/antivirus/bot.html （2010 年 6 月 確認）

[IT01] 板倉征男，辻井重男：DNA-ID を用いた DNA 個人情報管理システムの提案，情報処理学会論文誌，Vol.42，No.8，pp.2134-2143，2001.

[ITD10] ITmedia +D モバイル 記事：iPhone アプリで映画館のチケットを購入――my シアターのオンラインチケットサービス, 2010 年 6 月 18 日，http://plusd.itmedia.co.jp/mobile/articles/1006/18/news051.html (2010 年 8 月 確認).

[ITE04] ITmedia Enterprise 記事：チョコレートと交換でパスワードを教えた人，7 割を超える--英調査，2004 年 4 月，http://japan.cnet.com/news/sec/story/0,2000056024,20065583,00.htm （2010 年 5 月 確認）．

[ITN05] Itmedia News 記事：UFJ の ATM に隠しカメラ，2005 年 10 月，http://www.itmedia.co.jp/news/articles/0510/18/news025.html （2010 年 6 月 確認）

[ITP05] IT Pro Security 記事：【CRYPTO-GRAM 日本語版】バイオメトリクスの新たなリスク，2005 年 4 月 28 日，http://itpro.nikkeibp.co.jp/free/ITPro/Security/20050422/159969/ （2010 年 6 月 確認）．

[ITP10] ITmedia プロ 記事: スマートフォンで場所を選ばずクレジットカード決済――アスタリスクの「PitPay」，2010 年 7 月 2 日，http://www.itmedia.co.jp/promobile/articles/1007/02/news047.html （2010 年 6 月 確認）．

[JGK03] Wayne Jansen, Serban Gavrila, Vlad Korolev, Rick Ayers and Ryan Swanstrom: A visual login technique for mobile devices, NIST Report--NISTIR7030, 2003. http://csrc.nist.gov/publications/nistir/nistir-7030.pdf （2010 年 6 月 確認）．

[JHB97] Anil Jain, Lin Hong and Ruud Bolle: On-Line Fingerprint Verification, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.19, No.4, pp.302-314, 1997.

[JMM99] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin: The design and analysis of graphical passwords, Proceedings of 8th USENIX Security Symposium, pp.1-14, 1999.

[JN06] 徐 強，西垣 正勝：ニーモニックに基づくワンタイムパスワード型画像認証の実現可能性に関する検討，情報処理学会研究報告，2006-CSEC-32，pp.317-322，2006.

[TO04] Julie Thorpe and P. C. van Oorschot: Towards secure design choices for implementing graphical passwords, Proceedings of the 20th Annual Computer Security Applications Conference, pp.50-60, 2004.

[Kan01] 金子 正秀：顔による個人認証の最前線，映像情報メディア学会誌，Vol.55, No.22，pp.180-184，2001.

[Kas00] 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），情報処理学会研究報告，2000-CSEC-10，pp.121-127，2000.

[KHM02] 勝田 亮，平石 宏典，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，情報処理学会研究報告 2002-CSEC-16，pp.91-96，2002.

[Kle90] Daniel Klein: A survey of, and improvements to, password security, Proceedings of the USENIX Second Security Workshop, 1990.

[KI96] Kazukuni Kobara and Hideki Imai: Limiting the Visible Space Visual Secret Sharing Schemes and their Application to Human Identification, Advances in Cryptology, ASIACRYPT 1996, pp.185-195. 1996.

[KYN07] 小島 悠子，山本 匠，西垣 正勝：間違い探しを利用したワンタイムパスワード型画像認証の提案，情報処理学会研究報告，2007-CSEC-36，pp.375-380，2007.

[KYN08] 小島 悠子，山本 匠，西垣 正勝：手続き記憶を利用した再認型認証方式の検討，マルチメディア，分散，協調とモバイルシンポジウム 2008 論文集，pp.269-277，2008.

[KYN09] 小島 悠子，山本 匠，西垣 正勝：覗き見攻撃耐性と利便性を有する画像認証方式に関する一検討，情報処理学会研究報告．2009-CSEC-44．pp.91-96，2009.

[LN83] P.H. リンゼイ，D.A. ノーマン 著，中溝 幸夫，箱田 裕司，近藤 倫明 訳：リンゼイ／ノーマン 情報処理心理学入門 I －感覚と知覚－ 第 2 版，サイエンス社，1983.

[Man96] Udi Manber: A simple scheme to make passwords based on one-way functions much harder to crack, Computers & Security, Vol.15, No.2, pp.171-176, 1996.

[Mas02] 増井 俊之：インターフェイスの街角(49) -画像を使ったなぞなぞ認証，UNIX MAGAZINE, 2002 年 1 月号,
http://pitecan.com/UnixMagazine/PDF/if0201.pdf（2010 年 5 月確認）

[Mat01] 松本 勉：セキュリティ技術の弱点を発見したらどうしますか？，電子情報通信学会誌，Vol.84，No.3，pp.202-204，2001.

[Mat83] 松川 順子：ランダム図形の命名作用と再認，心理学研究，54，pp.62-65，1983.

[MC03] Microsoft Corporation: Let Me In: Pocket PC User Interface Password Redirect Sample, Microsoft Knowledge Base Article – 314989, July 2003,
http://support.microsoft.com/default.aspx?scid=kb;en-us;314989 （2010 年 6 月 確認）.

[MET1] 経済産業省：不正アクセス行為の禁止等に関する法律,
http://www.meti.go.jp/policy/netsecurity/fusei_access_law.htm （2010 年 5 月 確認）.

[MET2] 経済産業省： 電子署名及び認証業務に関する法律,
http://www.meti.go.jp/policy/netsecurity/digitalsign.htm（2010 年 6 月 確認）.

[MHM03] Shushuang Man, Dawei Hong and Manton Matthews: A shoulder-surfing resistant graphical password scheme - WIW, Proceedings of the International Conference on Security and Management, SAM2003, pp.105-111, 2003.

[MHS04] 松本 勉，平林 昌志，佐藤 健二： 虹彩照合技術の脆弱性評価（その３），
2004 年暗号と情報セキュリティシンポジウム論文集，SCIS2004，pp.701-706，2004.

[MNE] 株式会社ニーモニックセキュリティ： ニーモニックガード,
http://www.mneme.co.jp/neme/neme.html （2010 年 6 月 確認）.

[MOI00] 松本 隆明，岡本 龍明 編著，伊土 誠一 監修： 情報セキュリティ技術 第 5 章
IC カード，オーム社，2000.

[MRW99] Fabian Monrose, Michael K. Reiter and Susanne Wetzel: Password Hardening Based on Keystroke Dynamics, Proceedings of the 6th ACM conference on Computer and communications security, pp.73-82, 1999.

[MS03] ケビン・ミトニック, ウィリアム・サイモン, 岩谷 宏 訳： 欺術（ぎじゅつ）—
史上最強のハッカーが明かす禁断の技法，ソフトバンクパブリッシング株式会社，2003.

[MT79] Robert Morris and Ken Thompson: Password security: A case history, Communications of the ACM, Vol.22, No.11, 1979.

[NA06] 西垣 正勝，荒井 大輔，生体反射を利用した認証方式，情報処理学会論文誌，
Vol.47，No.8，pp.2582-2592，2006.

[Nal99] Vishvjit S. Nalwa: Automatic on-line signature verification, Proceedings of the Third Asian Conference on Computer Vision, Vol.I, pp.144-163, 1999.

[Neo] NeoFace：製品紹介: NEC:
http://www.nec.co.jp/soft/neoface/product/neoface.html （2010 年 6 月 確認）.

[Nie93] Jakob Nielsen: Usability Engineering, Academic Press, 1993.

[Nic68] Raymond S. Nickerson: A note on long-term recognition memory for pictorial material, Psychonomoic Science, 11, 58, 1968.

[NKT06] 西垣 正勝，小池 誠，田窪 昭夫：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.945-956，2006.

[NO07] 西垣 正勝，小澤 雄司，生体反射型認証：対光反射と盲点位置を利用した認証方式，情報処理学会論文誌，Vol.48，No.9，pp.3039-3050，2007.

[NPO] NPO 日本ネットワークセキュリティ協会: 2007 年 情報セキュリティインシデントに関する調査報告書，
http://www.jnsa.org/result/2007/pol/incident/2007incidentsurvey_v1.6.pdf （2010 年 6 月 確認）.

[NRW76] Douglas L Nelson, Valerie S Reed and John R Walling: Pictorical superiority effect, Journal of Experimental Psychology: Human Learning and Memory, Vol.2, No.5, pp.523-528, 1976.

[NS94] Moni Naor and Adi Shamir: Visual cryptograpy, Advances in Cryptology, Eurocrypt 1994, pp.1-12, 1994.

[NUY09] 西垣 正勝，梅本 功太，山本 匠：なぞり書き認証方式の提案とその認証精度に関する検討，画像ラボ，Vol.20，No.12，pp.14-21，2009.

[Ono05] 小野 束：画像認証方式の一評価実験，2005 年暗号と情報セキュリティシンポジウム予稿集，SCIS2005，pp.229-234，2005.

[Ori02] 織茂 昌之：情報セキュリティの基礎，日本理工出版会，2002.

[OT01] 太田 信夫，多鹿秀継 編著：記憶研究の最前線，北大路書房，2001.

[OTK05] 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，2005 年暗号と情報セキュリティシンポジウム予稿集，SCIS2005，pp.223-228，2005.

[PAT] SWIVEL: PATTern, http://www.swivelsecure.com/?page=turing（2010 年 6 月 確認）.

[Par97] Denise C. Park: Ageing and memory: Mechanisms underlying age differences in performances, Proceedings of the 1997 World Congress of Gerontology, 1997.

[PF] Real User Corporation: PassFace,
http://www.realuser.com/ （2010 年 6 月 確認）.

[PMT] Pointsec Mobile Technologies: Pointsec for Pocket PC, November 2002,
http://www.willcom-inc.com/ja/biz/solution/w-zero3/sol_list/pointsec/index.html
（2010年6月 確認）.

[PPT] 株式会社 SKR テクノロジー： PPT(PictureProtectTechnology)液晶ディスプレイ,
http://www.skr-tech.co.jp/2_11.HTML（2010 年 6 月 確認）.

[PRS68] Allan Paivoi, T.B. Rogers and Padric C. Smythe: Why are pictures easier to recall than words ?, Phychonomic Science, Vo.11, pp.137-138, 1968.

[PS99] Adrian Perrig, Dawn Song: Hash Visualization: a New Technique to improve Real-World Security, Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC1999, 1999.

[PSL03] 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.

[RA04] Karen Renauda and Antonella De Angelib: My password is here! An investigation into Visuo-Spatial Authentication Mechanisms, Interacting with Computers, Vol.16, No.6, pp.1017-1041, 2004.

[Rab84] Jan C. Rabinowitz: Aging and recognition failure, Jounal of Gerontology, Vol.39, No.1, pp.65-71, 1984.

[REC] reCAPTCHA: http://recaptcha.net/（2010 年 6 月 確認）

[Ric03] Richard E. Smith 著，稲村雄 監訳： 認証技術 パスワードから公開鍵まで，オーム社，2003.

[RRF04] Volker Roth, Kai Richter and Rene Freidinger: A PIN-Entry Method Resilient Against Shoulder Surfing, Proceeding of the 11th ACM conference on Computer and communications security, CCS2004, pp.236-245, 2004.

[Sa10] 佐々木 良一：クラウドと IT リスクに関する考察，情報処理学会研究報告，2010-CSEC-48，No.4，2010.

[SB02] Leonardo Sobrado and Jean Camille Birget: Graphical passwords, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (2010 年 6 月確認）.

[Sch01] Bruce Schneier 著，山形 浩生 訳：暗号の秘密とウソ，翔泳社，2001.

[Set02] 瀬戸 洋一著：サイバーセキュリティにおける生体認証技術，共立出版，2002.

[SG94] Yishay Spector and Jacob Ginzberg: Pass-sentence – a new approach to computer code, Computers & Security, Vol.13, pp.145-160, 1994.

[She67] Roger N. Shepard: Recognition memory for words, sentences, and pictures, Journal of Verbal Learning and Verbal Behavior, Vol.6, pp.156-163, 1967.

[SHI] 株式会社島津製作所：HEAD MOUNTED DISPLAY “Data Glass 2”, http://www.shimadzu.co.jp/hmd/ （2010 年 5 月 確認）.

[Shi84] 白井 克彦：音声と筆跡による個人認証技術，情報処理学会，Vol.25，No.6，pp.592-598，1984.

[SID] RSA Security Inc.: RSA SecurID, http://japan.rsa.com/node.aspx?id=1158 （2010 年 6 月 確認）.

[Si06] 清水 孝一: バイオメトリクス　−生体特徴計測による個人認証−，生体医工学，Vol.44，No.1，pp.3-14，2006.

[SYK09] 佐古 武志，吉田 隆弘，古原 和邦，今井 秀樹：ノートパソコンへのパスワード入力過程ののぞき見耐性について，2009 年暗号と情報セキュリティシンポジウム概要集，SCIS2009，pp264，2009.

[SL86] K.T.スペアー, S.W.レムクール 著, 苧阪 直行 訳： 視覚の情報処理―〈見ること〉のソフトウェア, サイエンス社, 1986.

[Smi87] Sidney L. Smith: Authentication users by word association, Computers & Security, Vol.6, No.6, pp.464-470, 1987.

[Spa91] Eugene H. Spafford: Preventing weak password choices, Proceedings of 14th NIST National Compter Security Conferense, pp.446-455, 1991.

[SOU] 総務省： “ブログの実体に関する調査研究の結果”, http://www.soumu.go.jp/iicp/chousakenkyu/data/research/survey/telecom/2008/2008-1-02-2.pdf （2010年6月 確認）.

[SR66] David Schonfield and Betty A. Robertson: Memory storage and aging, Canadian Jounal of Psychology, Vol.20, pp.220-236, 1996.

[SSM01] 白井 雄一郎, 白濱 直哉, 又江原 恭彦, 柳岡 裕美 著, 三輪 信雄 監修： インターネットセキュリティ 不正アクセスの手法と防御, ソフトバンク パブリッシング, 2001.

[SW] Secure Computing Corporation: SafeWord, http://www.aladdin.com/safeword/default.aspx （2010年6月 確認）.

[SYM04] 株式会社シマンテック： シマンテック, スパムメール実態調査でインターネットユーザの83.2 %がスパムメールを受信と発表, 2004年2月12日, http://www.symantec.com/region/jp/news/year04/040212.html （2010年6月 確認）.

[SYN09] 鈴木 徳一郎, 山本 匠, 西垣 正勝： 4コマ漫画CAPTCHAの提案, 2009年暗号と情報セキュリティシンポジウム概要集, SCIS2009, p.263, 2009.

[Ta08] 高田 哲司： fakePointer： 映像記録による覗き見攻撃にも安全な認証手法, 情報処理学会論文誌, Vol.49, No.9, pp.3051-3061, 2008.

[TK02] 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, 2002.

[TMD] 東京三菱銀行： 東京三菱ダイレクト ログイン方法，
http://www.web110.com/cyberacademy/ch15_3.html （2010 年 6 月 確認）．

[TMI03] 高橋 健太，三村 昌弘，磯部 義明，瀬戸 洋一： マルチモーダル生体認証技術の現状と逐次確率比検定によるアプローチ，ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会 第 1 回研究発表会予稿集，pp.19-26，2003.

[TNS04] 竹内 啓，西本 賢城，佐々木 良一： ディスプレイからの視覚的情報漏洩防止システムの開発，情報処理学会研究報告，2004-CSEC-25，pp.19-24，2004.

[TOH] 株式会社東芝： 視野角制御フィルタ，東芝レビュー，Vol.59，No.8，2004，
http://www.toshiba.co.jp/tech/review/2004/08/59_08pdf/rd2.pdf（2010 年 6 月 確認）．

[TS03] 土屋 範久 監修，佐々木 良一 他編著： 情報セキュリティ事典 第 7 章 不正コピー，pp.179-188，共立出版，2003.

[UE06] 植田 まさし：「新コボちゃん 8」，芳文社，2006.

[YAH] Yahoo! メール: http://mail.yahoo.co.jp/ （2010 年 6 月 確認）．

[VEN05] Venture Now（ベンチャーナウ）News 記事： IP イノベーションズ，画像利用のワンタイムパスワード技術販売開始，2005 年 7 月 19 日，
http://www.venturenow.jp/news/2005/07/19/1000_009996.html （2010 年 6 月 確認）．

[VGO] Passlogix: V-go，http://www.passlogix.com/ （2010 年 6 月 確認）．

[VK] SFR IT-ENGINEERING: visKey，
http://www.sfr-software.de/cms/EN/pocketpc/viskey/ （2010 年 6 月 確認）．

[W3C03] W3C: Inaccessibility of visually-oriented anti-robot tests problems and alternatives, W3C working draft5(2003),
http://www.w3.org/TR/2003/WD-turingtest-20031105/ （2010 年 6 月 確認）．

[WLI] Windows Live ID,
https://accountservices.passport.net/ppnetworkhome.srf?Lcid=1041 （2010 年 6 月 確認）．

[WP] ファルコンシステムコンサルティング株式会社： WisePoint, http://wisepoint.jp/index.html （2010 年 6 月 確認）.

[WRP] 株式会社 3Dwin： Wrap310, http://www.3d-win.co.jp/products_wrap310.html （2010 年 6 月 確認）.

[Wu99] Thomas Wu: A real-world analysis of Kerberos password security, Proceedings of the 1999 Network and Distributed System Security Symposium, 1999.

[WWS06] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado and Jean-Camille Birget: Design and evaluation of a shoulder-surfing resistant graphical password scheme, Proceedings of the working conference on Advanced visual interfaces, AVI2006, pp.177-184, 2006.

[WWN10] WirelessWire News 記事: スマートフォンを「おサイフケータイ」にする VISA と DeviceFidelity, 2010 年 5 月 18 日, http://wirelesswire.jp/Watching_World/201005180904.html （2010 年 6 月 確認）.

[YHI06] 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 画像記憶のスキーマを利用した認証方式の拡張－手がかりつき再認方式－，情報処理学会研究報告，2006-CSEC-34, pp.411-418，2006.

[YKN09] Takumi Yamamoto, Yuko Kojima and Masakatsu Nishigaki: A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection, Proceedings of the 2009 International Conference on Security & Management, SAM2009, pp.188-194, 2009.

[YMN93] 吉川 佐紀子, 益谷 真, 中村 真： 顔と心 ～ 顔の心理学入門, サイエンス社, 1993.

[ZH90] Moshe Zviran and William J. Haga: Cognitive Passwords: The key to easy access control, Computer & Security, Vol.9, No.8, pp.723-736, 1990.

著者発表論文

1. 学術雑誌等において発表した論文（査読あり）

First Author

- 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 不鮮明化画像が実現するスキーマを利用した画像認証方式の改良，日本セキュリティ・マネジメント学会誌，Vol.23，No.3，pp.17-29，2009．（研究論文）
- 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 画像記憶のスキーマを利用した認証方式の改良：ストーリーの利用による記憶負荷の削減，日本セキュリティ・マネジメント学会誌，Vol.23，No.3，pp.41-47，2009．（研究ノート）
- 山本 匠，漁田 武雄，西垣 正勝： 不鮮明化画像を利用した暗示・応答型画像認証方式の提案，情報処理学会論文誌，Vol.50，No.9，pp.2062-2076，2009．(研究論文)

Co-Author

- 西垣 正勝，臼井 佑真，山本 匠，間形 文彦，勅使河原 可海，佐々木 良一： 賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価，情報処理学会論文誌（研究論文）(現在投稿中).
- 原 正憲，長谷 巧，山本 匠，山田 明，西垣 正勝： スパムブログとアフィリエイトの関連性に関する一考察，情報処理学会論文誌，Vol.50，No.12，pp.3206-3210，2009．（テクニカルノート）

2. 国際会議で口頭発表した論文（査読あり）　下線は発表者を示す

First Author

- Takumi Yamamoto, Tokuichiro Suzuki, Masakatsu Nishigaki: A Proposal of Four-panel Cartoon CAPTCHA: The Concept, Proceedings of the International Workshop on Trustworthy Computing, TwC2010. (accepted, will be presented)
- Takumi Yamamoto, Yuma Usui, Fumihiko Magata, Yoshimi Teshigawara, Ryoichi Sasaki and Masakatsu Nishigaki: A Security Measure Selection Scheme with Consideration of Potential Lawsuits, Proceedings of the 2010 International Conference on Security & Management, SAM2010, (accepted, will be presented).
- Takumi Yamamoto, J.D.Tygar and Masakatsu Nishigaki: CAPTCHA Using Strangeness in Machine Translation, Proceedings of the 24th International Conference on Advanced Information Networking and Applications, AINA2010, pp.430-437, 2010.
- Takumi Yamamoto, Yuko Kojima and Masakatsu Nishigaki: A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection,

Proceedings of the 2009 International Conference on Security & Management, SAM2009, pp.188-194, 2009.

- Takumi Yamamoto, Atsushi Harada, Takeo Isarida and Masakatsu Nishigaki: Advantages of User Authentication Using Unclear Images －Automatic Generation of Decoy Images－, Proceedings of the 23rd International Conference on Advanced Information Networking and Applications, AINA2009, pp.668-674, 2009.
- Takumi Yamamoto, Atsushi Harada, Takeo Isarida and Masakatsu Nishigaki: Improvement of User Authentication Using Schema of Visual Memory:Exploitation of "Schema of Story", Proceedings of the 22nd International Conference on Advanced Information Networking and Applications, AINA2008, pp.40-47, 2008.
- Takumi Yamamoto, Atushi Harada, Takeo Isarida and Masakatsu Nishigaki: Improvement of User Authentication Using Schema of Visual Memory: Guidance by Verbal Cue, Proceedings of the 2007 International Conference on Security & Management, SAM2007, pp.58-64, 2007.

Co-Author

- Taiki Sakashita, Yoichi Shibata, Takumi Yamamoto, Kenta Takahashi, Wakaha Ogata, Hiroaki Kikuchi, and Masakatsu Nishigaki: A Proposal of Efficient Remote Biometric Authentication Protocol, Proceedings of the 4th International Workshop on Security, IWSEC2009, pp.58-64, 2009.
- Masakatsu Nishigaki, Takumi Yamamoto: Making Use of Human Visual Capability to Improve Information Security. ARES2009, pp.990-994, 2009.

3．国際会議でポスター発表した論文　下線は発表者を示す

First Author

- Takumi Yamamoto, Atsushi Harada, Takeo Isarida, Masakatsu Nishigaki: A User Authentication System Using Schema of Visual Memory, poster session in IFIPTM2010, 2010.

4．学術雑誌等又は商業誌における解説，総説

- Takumi Yamamoto, Atsushi Harada, Takeo Isarida, Masakatsu Nishigaki: A User Authentication System Using Schema of Visual Memory, IEICE Communications Society - GLOBAL NEWSLETTER, Vol.20, 2007.
- 西垣 正勝，梅本 功太，山本 匠：なぞり書き認証方式の提案とその認証精度に関する検討，画像ラボ，Vol.20，No.12，pp.14-21，2009.

5. 新聞での報道

- 「脳内認証」ゲームで体験，日経新聞（静岡版），2007 年 5 月 11 日.
- 情報漏洩防ぐ認証ソフト「販促用のゲーム開発」，日経産業新聞，2007 年 5 月 11 日.

6. 特許

- 出願番号：特願 2006 - 124336，出願人：株式会社リムコーポレーション，発明者：西垣 正勝，原田 篤史，山本 匠，発明の名称：情報端末及びこれを用いた画像認証方法，認証用画像の生成方法，提出日：2006 年 4 月 27 日

7. 口頭発表（査読無し）　下線は発表者を示す

First Author

- 山本 匠，漁田 武雄，西垣 正勝： 不鮮明化画像と言語手がかりを用いた Challenge&Response 型画像認証の実現に対する試み，映像メディア学会技術報告，pp.67-70，2009.
- 山本 匠，J. D. Tygar，西垣 正勝： 機械翻訳 CAPTCHA（その 2），コンピュータセキュリティシンポジウム 2009 論文集，pp.211-216，2009.
- 山本 匠，J. D. Tygar，西垣 正勝： 機械翻訳の違和感を用いた CAPTCHA の提案，情報処理学会研究報告，2009-CSEC-46，No.37，2009.
- 山本 匠，小島 悠子，西垣 正勝： 時間的曖昧入力方式による覗き見耐性画像認証方式，コンピュータセキュリティシンポジウム 2008 論文集，pp.157-162，2008.
- 山本 匠，漁田 武雄，西垣 正勝： 不鮮明化画像を利用した暗示・応答型認証方式の提案とその実現可能性，情報処理学会研究報告，2008-CSEC-42，pp.267-272，2008.
- 山本 匠，原田 篤史，漁田武雄，西垣正勝： 不鮮明化画像を利用した認証方式が有する特長－囮画像生成の容易性－，情報処理学会研究報告，2007-CSEC-38，pp.201-208，2007.
- 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 画像記憶のスキーマを利用した認証方式の改良 - 動画スキーマの利用 - ，コンピュータセキュリティシンポジウム 2006 論文集，pp.339-344．2006.
- 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 画像記憶のスキーマを利用したユーザ認証方式の拡張 - 手がかりつき再認方式 - ，電子情報通信学会技術研究報告，ISEC2006-40～71，pp.181-188．2006.
- 山本 匠，原田 篤史，漁田 武雄，西垣 正勝： 画像記憶のスキーマを利用したユーザ認証方式の実装，マルチメディア，分散，協調とモバイルシンポジウム論文集(II)，DICOMO2006，pp.949-952，2006.

Co-Author

- 高田 愛美，鈴木 徳一郎，山本 匠，西垣 正勝：視線誘導型なりすまし検知方式の検討（その 2），マルチメディア，分散，協調とモバイルシンポジウム論文集，DICOMO2010，(発表予定).
- 西垣 正勝，臼井 佑真，山本 匠,，間形 文彦，勅使河原 可海，佐々木 良一：賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価，マルチメディア，分散，協調とモバイルシンポジウム論文集，DICOMO2010，(発表予定).
- 鈴木 徳一郎，山本 匠，西垣 正勝：リレーアタックに耐性をもつ CAPTCHA の提案，情報処理学会研究報告，2010-CSEC-48，No.19，2010.
- 中澤 優美子，加藤 岳久，漁田 武雄，山田 文康，山本 匠，西垣 正勝：Best Match セキュリティ ～性格と本人認証技術に関するセキュリティ意識との相関に関する検討～，情報処理学会研究報告，2010-CSEC-48，No.24，2010.
- 渡邊幸聖，小田雅洋，山本匠，尾形わかは，菊池浩明，西垣正勝：曖昧性を含んだ多項式による特徴量関数を利用した非対称生体認証，2010 年暗号と情報セキュリティシンポジウム予稿集，SCIS2010，CD-ROM（論文 No.2F1-3），2010.
- 藤井裕樹，中澤優美子，安倍史江，山本匠，西垣正勝：痴漢冤罪対策の一方式の提案，2010 年暗号と情報セキュリティシンポジウム予稿集，SCIS2010，CD-ROM（論文 No.3E3-3），2010.
- 小田 雅洋，渡邊 幸聖，山本 匠，尾形 わかは，菊池 浩明，西垣 正勝：グラフ 3 彩色問題を用いた非対称生体認証方式に対する検討，映像メディア学会技術報告，pp.53-56，2009.
- 臼井 佑真，山本 匠，間形 文彦，勅使河原 可海，佐々木 良一，西垣 正勝：訴訟リスクを考慮した情報セキュリティ対策選定方式に関する検討，コンピュータセキュリティシンポジウム 2009 論文集，pp.105-110，2009.
- 高田 愛美，鈴木 徳一郎，山本 匠，西垣 正勝：視線誘導型なりすまし検知方式の検討，マルチメディア，分散，協調とモバイルシンポジウム論文集，DICOMO2009，pp.92-97，2009.
- 安倍 史江，山本 匠，西垣 正勝：人体通信による電子トリアージタグへの情報伝達：システムの実装，マルチメディア，分散，協調とモバイルシンポジウム論文集，DICOMO2009，pp.1849-1854，2009.
- 梅本 功太，山本 匠，西垣 正勝：なぞり書き認証方式の提案とその認証精度に対する本人特徴量と他人特徴量の寄与に関する検討，バイオメトリックシステムセキュリティ研究会，第 16 回研究発表回予稿集，pp.25-32，2009.
- 鈴木 徳一郎，山本 匠，西垣 正勝：4 コマ漫画 CAPTCHA の提案，2009 年暗号と情報セキュリティシンポジウム概要集，p.263，2009.

- 青山 真之，山本 匠，高橋 健太，西垣 正勝：生体反射型認証－輻輳反射と眼球形状および両眼間距離を利用した認証方式の提案－，情報処理学会研究報告，2009-CSEC-44，pp.85-90，2009.
- 小島 悠子，山本 匠，西垣 正勝：覗き見攻撃耐性と利便性を有する画像認証方式に関する一検討，情報処理学会研究報告，2009-CSEC-44，pp.91-96，2009.
- 長谷 巧，山本 匠，原 正憲，山田 明，西垣 正勝：アフィリエイトに着目したスパムブログ評価方式に関する検討，情報処理学会研究報告，2009-CSEC-44，pp.97-102，2009.
- 中澤 優美子，加藤 岳久，漁田 武雄，山田 文康，山本 匠，西垣 正勝：Best Match Security－性向とパスワード認証のセキュリティ意識との相関に関する検討－，情報処理学会研究報告，2009-CSEC-44，pp.43-48，2009.
- 小島 悠子，山本 匠，西垣 正勝：手続き記憶を利用した再認型認証方式の検討，マルチメディア，分散，協調とモバイルシンポジウム 2008 論文集，DICOMO2008，pp.269-277，2008.
- 小島 悠子，山本 匠，西垣 正勝：間違い探しを利用したワンタイムパスワード型画像認証の提案，情報処理学会研究報告，2007-CSEC-36，pp.375-380，2007.

8．表彰　　下線は発表者を示す

- Best Paper Award

  Takumi Yamamoto, J.D.Tygar and Masakatsu Nishigaki: CAPTCHA Using Strangeness in Machine Translation, Proceedings of the 24th International Conference on Advanced Information Networking and Applications, AINA2010, pp.430-437, 2010.
- CSS2008 学生論文賞

  山本 匠，小島 悠子，西垣 正勝：時間的曖昧入力方式による覗き見耐性画像認証方式，コンピュータセキュリティシンポジウム 2008 論文集，pp.157-162，2008.
- DICOMO2006 野口賞受賞

  山本 匠，原田 篤史，漁田 武雄，西垣 正勝：画像記憶のスキーマを利用したユーザ認証方式の実装，マルチメディア，分散，協調とモバイルシンポジウム論文集，DICOMO 2006，pp.949-952，2006.