社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (56)
2006／7／21

画像記憶のスキーマを利用した認証方式の拡張
－手掛かりつき再認方式－

山本 匠[1] 原田 篤史[2] 漁田 武雄[3] 西垣 正勝[4]

1 静岡大学情報学研究科 〒432-8011 静岡県浜松市城北 3-5-1

2 静岡大学理工学研究科 〒432-8011 静岡県浜松市城北 3-5-1

3 静岡大学情報学部 〒432-8011 静岡県浜松市城北 3-5-1

4 静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市城北 3-5-1

E-mail: nisigaki@inf.shizuoka.ac.jp

あらまし 我々は，一見すると無意味に見える不鮮明な画像をパス画像とすることにより，覗き見攻撃に耐性を有する「画像記憶のスキーマを利用した認証方式」を既に提案している．しかし本方式は，視認性の低い不鮮明化画像を利用しているため，ユーザがパス画像の選択に要する時間が長くなるという問題を残していた．一方，本方式においては，スキーマを持たない攻撃者に対してパス画像に関する情報を言語で伝えても，攻撃者はその意味を理解できないという実験結果が得られている．そこで本稿では，パス画像を思い出すにあたっての手掛かりとなる言語情報を認証時に提示することによって，本方式の改善を図る．手掛かり情報はスキーマを有する正規ユーザにのみ伝わり，正規ユーザの認証負荷のみを軽減することができると期待される．本稿では手掛かりの提示による利便性向上への寄与と覗き見攻撃への影響を，基礎実験を通じて検証する．

キーワード 画像認証，スキーマ，不鮮明化画像，覗き見攻撃，手掛かり

An Improvement of User Authentication Using Schema of Visual Memory
－An extension of the system using hint－

Takumi Yamamoto[1] Atsushi Harada[2] Takeo Isarida[3] and Masakatsu Nishigaki[4]

1 Graduate School of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan

2 Graduate School of Science and Engineering, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan

3 Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan

4 Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan

E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract We have already proposed an user authentication system using "unclear images" as pass-images, in which only the legitimate users can understand their meanings by viewing the original images corresponding to the unclear pass-images. These unclear images are meaningless for illegal users. Hence it is difficult for illegal users to remember the unclear pass-images, even though they observe the legitimate users' authentication trial. In addition, the previous study has shown that it is not easy for illegal users to guess the meaning of the unclear pass-image even if a brief explanation of the pass-image is given with words. However, the system has a drawback that less visibility of unclear images can impede the legitimate users to recognize their pass-images, which will require a longer time for the authentication. Therefore we enhance our authentication system by giving a brief explanation of the pass-image as hint. It is expected that the hint is helpful only for the legitimate user, since illegal users can not understand the hint as confirmed in the previous study. This paper verifies the availability of the modified system through basic experiments.

Keyword Image authentication, Schema, Unclear image, Observing Attack, Hint

1. はじめに

現行のユーザ認証方式は，汎用性と利便性の高さからパスワード方式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画像認証方式が注目されている．

しかし，画像認証方式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であった．また，パスワード認証ではパスワードの漏洩が問題となるが，画像認証においても依然として，画像の意味や内容を言葉で教えることによって認証を通過するのに十分な情報を他人に伝達することができてしまう[1]．

上記で挙げた問題の解決を目標に，我々は，画像記憶を利用することで正規ユーザの記憶負荷を軽減しつつも，第三者が他人のパス画像を覗き見ても記憶負荷軽減の効果を得ることができず，かつ，正規ユーザが認証情報を他者に伝達することが難しい「スキーマを利用したユーザ認証方式」（以下，基本方式と呼ぶ）を既に提案している[2]．詳細は2章で述べるが，基本方式は従来の画像認証方式に比べて覗き見攻撃やパス画像の漏洩への耐性向上を果たしており，本人認証に関しても高い認証成功率を維持している．

しかし，基本方式では，視認性の低い画像を認証用の画像とするため，正規ユーザが当該パス画像を認識するまでの時間が延び，その結果認証に要する時間が長くなるという問題を残していた．認証に時間がかかることで，ユーザビリティが低下することに加え，覗き見攻撃者にパス画像をさらす時間が長くなるなどの悪影響が生じてしまう．

一方，基本方式においては，スキーマを持たない攻撃者に対してパス画像に関する情報を言語で伝えたとしても，攻撃者はその意味を理解することはできないという実験結果が得られている．つまり，例えば認証画面とともに，パス画像の意味を言語で与えたとしても，パス画像に対するスキーマを持たない攻撃者はそれを有効に利用することはできないと予想できる．

そこで本稿では，パス画像を思い出すにあたっての手掛かりとなる言語情報を認証時に提示することにより，本方式の改良を図る．改良方式では，正規ユーザは，手掛かりによって認証時の再認および想起が促進され，認証時間の短縮と記憶負荷のさらなる軽減が期待できる一方，攻撃者はこの手掛かりを活用できない．

改良方式の詳細は3章で述べる．そして，改良方式のプロトタイプ実験システムを実装し，基礎実験によって有効性の検証を行った結果を4章に示す．さらに，5章で今後の改良指針を示し，6章で本稿をまとめる．

2. 画像記憶のスキーマを利用した認証方式

2.1. コンセプト

本章では，画像記憶のスキーマを利用した認証方式の基本方式について説明する．詳細については文献[2]を参照されたい．基本方式は，既存の画像認証方式における覗き見攻撃や，正規ユーザによる意図的な認証情報の（言葉による）漏洩の脅威を軽減することを目的としている．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，基本方式では，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（以下，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（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[3]．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，無意味な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してもらうようにする．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」[4]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構造」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フィルタを通して認識しており，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．

2.2. 不鮮明化画像の生成手順

認証に使用する画像について説明する．本方式では，多数の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)と，$I(x,y)$ に対してモザイク化などの不鮮明化処理を施した画像 $O(x,y)$（以下，不鮮明化画像と記す）を使用する．以下に，今回提案システムで採用した不鮮明化処理の手順を簡単に説明する．

【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して，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 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．なお，乱数のシードには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なっている．

【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，$I''(x,y)$ を重み $w(0 \leqq w \leqq 1)$ の加重平均によって重ね合わせ処理を行い，画像 $O(x,y)$ を得る．

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

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．

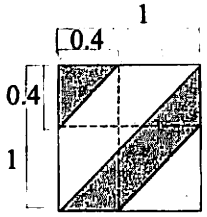

図 1　不鮮明化処理における DCT 係数の変更範囲

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化画像の例を図 2 に示す．図 2 左はオリジナルのカラー画像(予稿の印刷上はモノクロ)であり，図 2 右は不鮮明化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．

図 2　画像の不鮮明化処理

2.3. 基本方式の手順

基本方式の登録・認証の手順を以下に示す．

● 登録フェーズ

【Step1】システムは，オリジナル画像の一覧をユーザに提示する．

【Step2】ユーザはシステムが提示したオリジナル画像の中から，パス画像にしたい画像を選択する．

【Step3】システムは，ユーザが選んだオリジナル画像と，それを不鮮明化した画像をユーザに提示する．ユーザはこれらの画像を納得がいくまで見ることが可能である．

【Step4】ユーザは，Step2 の不鮮明化画像をパス画像として登録する．

【Step5】Step1～Step4 を繰り返し行い，既定の枚数の画像をパス画像として登録する．

● 認証フェーズ

【Step1】システムは，ユーザのパス画像をランダムに 1 枚選び，かつ，ユーザのパス画像以外の不鮮

明化画像をランダムに規定の枚数分選択する．そして，それらの画像を，ランダムな順番に並びかえて認証画面に表示する．

【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選ぶ．

【Step3】Step1～Step2を既定の回数だけ繰り返し，そのうちの一定回数以上，ユーザがパス画像の選択に成功すれば認証成功とする．

要求される認証強度に応じて，登録するパス画像の枚数，認証フェーズで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．

2.4. 基本方式の有効性と課題

基本方式は，既存の画像認証方式（オリジナル画像を利用する方式）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[2]．

文献[2]では覗き見攻撃者（実験実施者の認証作業を横で見ていた被験者）にとって非常に有利な条件である2択認証システム*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，基本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．さらに，9択認証システムによって4ターンの認証を行う方式**にて同様の実験を行ったところ，本人認証率をほぼ100%に保ったまま，覗き見攻撃によるなりすまし成功率を26%にまで下げることができたという結果が得られている．

文献[2]では，パス画像の情報を他人に言語情報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た．攻撃者にパス画像の情報***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，基本方式の認証成功率は74%であった．さらに，9択認証システムによって4ターンの認証を行う方式における実験では，認証成功率を0%に抑えることができている．

一方，文献[2]の実験からは，基本方式は視認性の低い不鮮明化画像をパス画像として用いているため，正規ユーザが自分のパス画像を認識するまでの時間が延び，その結果認証に要する時間が長くなるという問題も浮き彫りとなった．特に9択認証システムにおいては，本人認証にかかる時間は各ターンで平均10数秒となるという実験結果が得られており，正規ユーザにストレスを感じさせてしまうかもしれない．また，認証に時間がかかることで，覗き見攻撃者にパス画像をさらす時間が長くなるなどの悪影響も生じるだろう．基本方式を実用化するためには，正規ユーザが認証時に自分のパス画像（不鮮明化画像）を再認するにあたっての迷いを減らし，素早く認証できるようにする工夫が必要である．

ここで，基本方式における言語によるパス画像漏洩の実験から，言語でパス画像の内容を伝えたとしても，不鮮明化画像に対するスキーマを持っていない攻撃者には正しくその情報が伝わらず，これをなりすましに活用することは難しいという結果が得られていた．そこで次章では，不鮮明化画像を用いた画像認証システムが有するこの特性を巧みに利用することにより，基本方式の改良し，認証時間を改善していく．

3. 改良方式

本章では，基本方式における認証時間を短縮するために改良方式を提案する．改良方式では，基本方式に，パス画像を想起させる手掛かりを認証画面に提示するという拡張を加える．手掛かりには，パス画像に対応するオリジナル画像の意味を言語で表現した文を用いる．例えば，犬の写真を不鮮明化したものがパス画像であった場合には，「犬の画像を選択してください」といったメッセージを，パス画像の選択画面と一緒に表示する．この手掛かりの提示によって，正規ユーザはパス画像の意味を容易に想起でき，パス画像を素早く選択できるようになる．特に，ユーザに多数のパス画像を記憶させるような認証方式では，手掛かり情報により現在のターンで再認を求められているパス画像を特定することができるため，ユーザは囮画像の中からどのパス画像を探せばよいのかがわかる分，囮画像の中からパス画像を見つける作業が容易になり，認証時間が大きく短縮されると考えられる．

ここで，画面に提示される手掛かりは正規ユーザだけでなく，第三者（覗き見攻撃者）にも与えられることになるが，基本方式を評価するにあたって行ったパス画像漏洩の実験[2]より，パス画像に関する情報を言

---

* 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．

** ユーザは4枚のパス画像を記憶する．認証画面に提示される画像は，4枚のパス画像の内の1枚と囮画像8枚の計9枚である．ユーザはこの中から正しいパス画像を選択する．これを，それぞれのパス画像に対し，4回繰り返す．4回とも正しいパス画像を選ぶことができたユーザを正規ユーザとして認証する．

*** 文献[2]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．

語で与えただけでは，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ことが確認されている．よって，認証時に言語による手がかりを提示することで，覗き見攻撃者によるなりすましの成功率を増大させることなく，正規ユーザによるパス画像の想起を容易にすることができると予想される．

改良方式では，登録フェーズの Step3 ならびに認証フェーズの Step1 において，当該パス画像とともにそれに対する手掛かり情報が同時に提示される．図 3，図 4 及び図 5 に，改良方式における登録フェーズと認証フェーズの表示画面をそれぞれ示す．

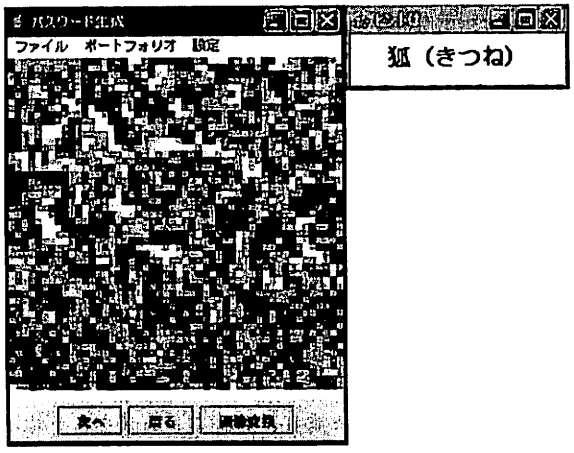

図 3　登録フェーズの Step3 の画面
（不鮮明化画像表示時）

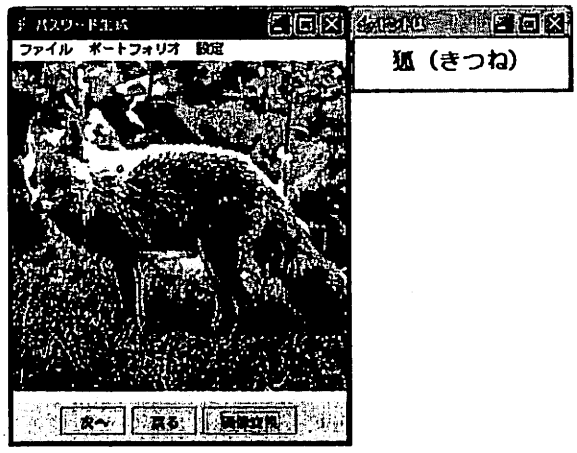

図 4　登録フェーズの Step3 の画面
（オリジナル画像表示時）

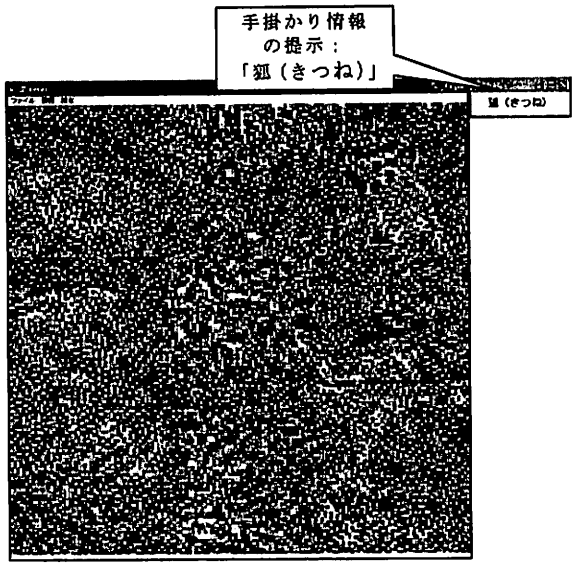

図 5　認証フェーズの Step1 の画面

登録フェーズにおいて，正規ユーザはパス画像（オリジナル画像と不鮮明化画像におけるスキーマ）とともに手掛かりとなる情報を記憶する．その後，認証フェーズにて，パス画像とともにその手掛かりが提示されることにより，正規ユーザにのみパス画像の想起が促され，正規ユーザは認証画面の中から自分のパス画像を容易に選択することが可能となっている．

4. 基礎実験

改良方式の利便性向上への寄与と覗き見攻撃への影響を，基礎実験を通して評価する．

利便性向上に関する評価においては，正規ユーザの認証成功率および認証時間を測り，基本方式との比較を行う．

覗き見攻撃に関する評価においては，なりすまし実験を実施し，パス画像に関する手掛かりが（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が攻撃耐性の低下につながらないか確認する．言葉による手掛かり情報の提示が，覗き見攻撃に対する大きな脅威とならないことは基本方式におけるパス画像漏洩の実験[2]から分かっているが，改良方式では，攻撃者が覗き見したパス画像の情報と，画面に提示される手掛かり情報を併せて活用できるため，基本方式に比べてなりすまし成功率が増大する危険性がある．このため，改良方式の安全性を再確認する．

4.1. 実験 1:認証実験

改良方式における，正規ユーザの認証成功率および

認証に要する時間を測定し，基本方式と比較する実験を行う．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，本稿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．

● 実験方法

基本方式，改良方式のプロトタイプを実装し，これを用いて実験を行う．被験者は本学学生10名である．まず，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では基本方式，実験群Bでは改良方式を用いた認証実験を行う．両実験群の各被験者には，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．その後，登録日から1日後，8日後，29日後に認証フェーズを実施する．毎回の認証フェーズにおいては，9枚の不鮮明化画像の中から1枚のパス画像を選択するという作業(これを1ターンと呼ぶ)を4ターン行う．各ターンのパス画像はランダムに選ばれるが，1回の認証フェーズの異なるターンにおいて，同じ画像が2度以上現れることはない．すなわち被験者は，自分が覚えた10枚のパス画像（不鮮明化画像）のうちの4枚を，それぞれ9枚の画像の中からすべて正しく選択することができた場合に認証成功となる．実験群Bで利用するパス画像の手掛かりは，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．それぞれの場合において，被験者には5回ずつ認証フェーズを行ってもらい，認証成功率，認証時間を測定する．なお，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

実験群A･Bの各被験者について，1日後，8日後，29日後に5回ずつ行った認証フェーズに関して，認証成功率と平均認証時間（4枚のパス画像全てを選択し終えるのに要した時間の平均）を表1に示す．

表1より，基本方式に比べ，改良方式が認証成功率および1回の認証にかかった時間に関して良好な結果を得ていることがわかる．これは，手掛かりが提示されることにより，被験者は確実にパス画像の意味を想起することができるようになり，自分が記憶した10数のパス画像のうち，現在のターンで問われているパス画像がどれであるかを即座に確定することができるため，パス画像を素早く正確に選択できるようになった結果と考えられる．

表1　認証成功率と平均認証時間

	1日目		8日目		29日目	
	実験群A:基本方式	実験群B:改良方式	実験群A:基本方式	実験群B:改良方式	実験群A:基本方式	実験群B:改良方式
認証成功率(%)	100.0	100.0	88.0	100.0	88.0	100.0
4ターンの平均認証時間(秒)	33.6	25.7	75.3	21.0	45.4	21.5

4.2. 実験2:覗き見攻撃によるなりすまし実験

改良方式における，手掛かりの提示による覗き見攻撃者のなりすまし成功率に対する影響について検証する．実験2では，被験者に実験実施者（正規ユーザ）に対する覗き見攻撃を実施してもらう．

● 実験方法

実験1と同じ被験者（10名）で，基本方式と改良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．改良方式では，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掛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．

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．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．実験1と同様，9択認証システムによる認証を4ターン繰り返す．すなわち覗き見攻撃者は，覗き見をすることにより実験実施者が選択した4枚のパス画像（不鮮明化画像）を覚えた上で，それに続くなりすまし試行において，その4枚をそれぞれ9枚の画像の中からすべて正しく選択することができた場合に認証(なりすまし)成功とする．ただし，本実験が極端に難しいものにならないよう，実験2では正規ユーザ（実験実施者）が覚えるパス画像は4枚とした．これにより，直前に覗き見たパス画像がなりすましを行う際に必ず現れるようになっている（ただし，パス画像の現れる順番は変わる）．実験実施者は試行ごとに4枚のパス画像をランダムに変更しながら，各被験者に対し5回ずつのなりすましの試行をとり行う．

なお，実験1における「各ターンの平均認証時間（4枚のパス画像全てを選択し終えるのに要した時間の平均を，ターン数である4で割った時間）」が最大で20秒弱（実験群A：8日目）であることを鑑み，実験2の各ターンの覗き見時間，すなわち認証画面に画像が表示されてから実験実施者がパス画像を選択するまで

の時間を一律20秒とした．また，被験者が，パス画像の選択に迷った際には，少しでも答えに近いと思う方を選択させた．

● 実験結果

各被験者について，なりすましの成功率となりすましに要した時間を表2に示す．5回の試行のうち，4ターン連続してパス画像を選択することができた割合を「なりすまし成功率」，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を「各ターンの成功率」，1回のなりすまし（4ターン分のなりすまし）を行うにあたりパス画像を選択するのに要した時間の平均を「平均認証時間」とした．

表2より，改良方式と基本方式を比べると，なりすまし成功率は改良方式の方が若干増加しているものの，各ターンの成功率および認証に要する時間が両者でほぼ等しいことから，言語による手掛かりが，本方式の覗き見攻撃耐性を低下させることはないと考えることができるだろう．

表2　覗き見によるなりすまし成功率

	基本方式	改良方式
なりすまし成功率(%)	16.0	20.0
各ターンの成功率(%)	61.5	61.5
平均認証時間（秒）	60.2	62.9

4.3. 考察

認証実験の結果より，改良方式は，基本方式に比べ良好な結果となっていることがわかる．つまり，手掛かり情報の提示は，ユーザの記憶負荷を減らし，利便性を向上させることに寄与していることが確かめられた．

一方，覗き見によるなりすましの実験結果から，改良方式の覗き見攻撃に対する耐性は，基本方式とほぼ同等のレベルを維持していることが確認できた．なお，覗き見攻撃者のなりすまし成功率は20%となっており，不鮮明化画像を利用した画像認証方式においても5回に1回はなりすましが成功してしまう．しかし，オリジナル画像を利用した既存の画像認証方式においては，覗き見攻撃によるなりすましの成功率がほぼ100%であることを考慮すると，本方式の覗き見攻撃耐性の高さは相応のものであることがわかる．

5. 今後の改良

覗き見によるなりすましの実験結果から，改良方式で提示する手掛かり情報は，覗き見攻撃に対する大きな脅威とはならないと考えられる．しかし，5回に1回の割合で覗き見攻撃者によるなりすましが成功する．今後は，手掛かり情報や認証画面の提示方法を変更したり，手掛かりに代わる補助情報を提示したりすることにより，覗き見攻撃によるなりすましの成功率をさらに低下させるような工夫を検討したい．

なりすまし実験における実験後の聞き取り調査では，「自分なりに手掛かりが指し示している動物だと思われる不鮮明化画像を選択したのだが，推測が外れ，なりすましに失敗した」という声が多く聞かれた．よって，認証フェーズにおいて，「パス画像と同じ種類の動物が写っているオリジナル画像を不鮮明化した画像」をパス画像といっしょに表示することによって，さらに攻撃者を惑わせ，攻撃耐性の向上を図ることも可能ではないかと考えられる．例えば，パス画像が「きつねの写真を不鮮明化した画像」であった場合は，姿勢や向きが異なるきつねの写真を多数用意し，これらの不鮮明化画像を作成した上で，それらの不鮮明化画像とともにパス画像を認証画面に表示し，ここに「きつねを選択してください」という手掛かり情報を合わせて提示するようにする．

また，「きつねの左前足をクリックしてください」などといったように手掛かり情報を詳細化し，ユーザが正しいパス画像の中の正しい部位（この場合は左前足）をクリックできた場合のみ認証成功とするような方法も考えられる．スキーマを持たない攻撃者には，言葉による情報から不鮮明化画像の意味を推測することは困難である．まして，画像中の細かい情報（向き，姿勢，各部位の位置など）までを認識することは不可能に近いであろう．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にとっては，指示された場所（部位）をクリックすることは容易である．この方法は，ユーザの記憶負荷を大きく増加させることなく，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．さらに，手掛かりにより指定する部位を認証の度に変化させるようにすれば，ある認証フェーズで「左前足」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「尻尾をクリックしてください」という指示に変わるため，チャレンジ&レスポンス認証のようなリプレイ攻撃防止効果を得ることもできる．

これらの方式に対して，今後早急に，その有効性を検証していきたい．

6. おわりに

本稿では，正規ユーザの記憶負荷の増加を抑えつつ，覗き見攻撃耐性を強化した「スキーマを利用した画像認証方式」をベースに，手掛かり付き再認を利用する改良方式を提案した．さらに，改良方式の有効性を示すために，プロトタイプを実装し，本人認証および覗き見攻撃に関する基礎実験を行い，改良方式の有効性を示した．

参考文献

[1] 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 年．

[2] 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.

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

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