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

2008－CSEC－42（36）
2008／7／25

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

山本 匠[1, 3]　漁田 武雄[2]　西垣 正勝[1, 4]

[1]静岡大学創造科学技術大学院 〒432-8011 浜松市中区城北 3-5-1
[2]静岡大学情報学部 〒432-8011 浜松市中区城北 3-5-1
[3]日本学術振興会特別研究員（DC1）
[4]科学技術振興機構，CREST

E-mail: f5745037@ipc.shizuoka.ac.jp, isarida@inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

あらまし　本稿では，一見すると無意味に見える不鮮明な画像を活用することで，暗示・応答型画像認証方式（Que and Response 型画像認証方式）という新しいコンセプトの Challenge & Response 型画像認証方式を提案する．本方式は，システムから提示されるチャレンジそのものを攻撃者から隠すことで，レスポンス生成の方法が単純であっても，覗き見に対する安全性を確保することが可能であると考えられる．これにより，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つの特長を有する画像認証方式が実現可能である．基礎実験を通じ，本方式の実現可能性を評価する．

キーワード　画像認証方式，不鮮明化画像，スキーマ，覗き見攻撃，暗示・応答

Proposal of a Cue & Response Based User Authentication Using Unclear Image

Takumi YAMAMOTO[1, 3]　Takeo ISARIDA[2]　and　Masakatsu NISHIGAKI[1, 4]

[1]Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011, JAPAN
[2]Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Naka, Hamamatsu, 432-8011, JAPAN
[3]Research Fellow of the Japan Society for the Promotion of Science (DC1)
[4]Japan Science Technology and Agency, CREST

E-mail: f5745037@ipc.shizuoka.ac.jp, isarida@inf.shizuoka.ac.jp, nisigaki@inf.shizuoka.ac.jp

Abstract　We have recently 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 unauthorized users. Hence it is difficult for unauthorized users to remember the unclear pass-images, even though they observe the legitimate users' authentication trial. In this paper we propose a new type of Challenge & Response based image authentication by using a feature of unclear image, which we call as "Cue & Response (Q&R) based image authentication". In this authentication, it is expected that even simple calculation of a response can achieve high robustness against observing attackers by hiding a challenge (cue) from unauthorized users. By doing this, only a legitimate user can respond to a randomly changing cue properly while unauthorized users are prevented from impersonating with limited amount of observing attacks. We conduct fundamental experiments to study the availability of the proposal Q&R image authentication system.

Keyword　image-based user authentication, unclear image, schema, observing attack, cue & response

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[1，2]が注目されている．しかし，再認型の認証となる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．この問題の対策としては，画像認証方式をワンタ

イム化する方法[3-6]と認知心理学的に攻撃者の画像認識を妨害する方法[7]に大別される．

前者に対しては，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（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）をハッシュ化してレスポンスを返すというようなことは不可能である．Sobrado らの方式[3]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言えるが，やはり，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[4]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低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．

また，セキュア ID [8]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も提案されている[5,6]．ただし，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，徐らの方式[5]ではニーモニックを導入することによって，fakepointer2 [6]では画像の短期記憶を活用することによって，それぞれ記憶負荷を抑える工夫をしているが，その記憶負荷は依然として大きい．

一方，後者の方法では，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をパス画像として使用する方法が提案されている[7]．正規ユーザにのみ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）[9]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，パス画像を容易に記憶することができる．しかし，不鮮明化画像の認識は困難ではあるが不可能ではないため，パス画像をワンタイム化，または定期的に変更できると望ましい．

以上のように，前者の C&R 型画像認証方式には，安全性や利便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り，後者の不鮮明化画像認証方式には，認証情報にワンタイム性を追加したいという要望がある．そこで本稿では，両者を融合することによって，より効果的な画像認証方式を実現することを目指す．

具体的には，不鮮明化画像の特徴[10]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．チャレンジそのものを攻撃者から隠すことができれば，レスポンス生成の方法が単純であっても，覗き見に対する安全性を確保することが可能であると考えられる．本稿では，このような非明示的（暗示的）なチャレンジを「キュー」と呼び，本方式を暗示・応答（Cue and Response：Q&R）型画像認証方式と呼ぶこととする．

2. 覗き見攻撃に対する既存の画像認証方式

覗き見攻撃に耐性を持たせることを目的とした画像認証方式を以下の 4 つ分けて，それぞれを簡単に説明し，課題を示す．

2.1. C&R 型画像認証方式

代表的な方式として Sobrado らが提案する方式[3]がある．この方式では，チャレンジとして，システムからの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 1）．

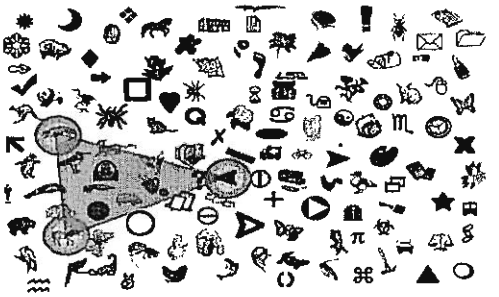

図 1　文献[3]の認証画面の例

この作業を複数回繰り返すことで認証の可否を判断する．ユーザからのレスポンスを「凸包の内部」というあいまいな形で返すため，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，多数の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．

一方，Roth らが提案する方式[4]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低減させることに成功している．この方式では，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）．これを各桁につき複数回行う．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．

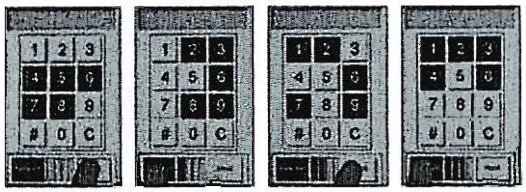

図 2　文献[4]の認証画面の例

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．

2.2. パス画像更新型認証方式

セキュア ID [9]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[5]（図 3）．しかし，ストーリ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．

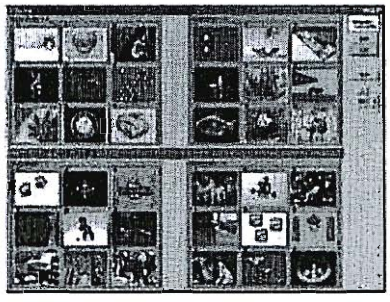

図 3　文献[5]の認証画面の例

一方，fakepointer2 [6]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．fakepointer2 は暗証番号をパス画像（背景画像）に合わせることによって認証が行われる（図 4）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．

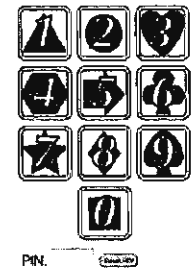

図 4　文献[6]の認証画面の例

2.3. 画像認識妨害方式

覗き見をする攻撃者にとってパス画像の認識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 5 右）をパス画像として使用する[7]．正規ユーザにのみオリジナル画像（図 5 左）を見せることにより，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[9]」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，ひとたび不鮮明化画像に対するスキーマを学習すれば，それ以降にその不鮮明化画像を見た場合に，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．

しかし，不鮮明化画像の認識は困難ではあるが不可能ではないため，（記憶負荷を増加させることなく）パス画像を定期的に変更できると望ましい．

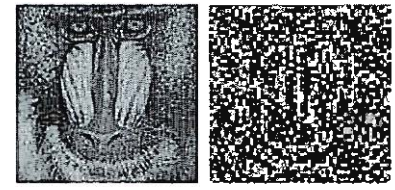

図 5　文献[7]で用いられる不鮮明化画像（右）とそのオリジナル画像（左）の例

3. Q&R 型画像認証方式

3.1. コンセプト

2 章で概説したように，既存の C&R 型画像認証方式には，安全性や利便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，画像認識妨害方式（不鮮明化画像認証方式）には，パス画像更新型認証方式のような記憶負荷の増加を生じさせることなく，何らかのワンタイム性を追加したいという要望がある．そこで本稿では，C&R 型画像認証方式と

画像認識妨害方式の両者を融合することによって，より効果的な画像認証方式を実現することを目指す．

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徴[10]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．

通常の C&R 型認証においては，攻撃者もチャレンジとレスポンスを観測することができるため，一方向性を有する複雑な計算によってチャレンジからレスポンスを生成しなければ，覗き見攻撃に耐えられない．これに対し，チャレンジそのものを攻撃者から隠すことができれば，レスポンス生成の方法が単純であっても，覗き見に対する安全性を確保することが可能であると考えられる．

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「非明示的」に提示される．本稿では，このような暗示的なチャレンジを「キュー」と呼び，本方式を暗示・応答（Cue and Response：Q&R）型画像認証方式と呼ぶ．

Q&R 型画像認証方式は，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有する，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．

3.2. 認識方式

文献[10]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徴[7]を活用し，認証時に言葉によってパス画像に関す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成功率を増大させることなく，正規ユーザの認証時の認識負荷を軽減する方式を提案している（図 6）．

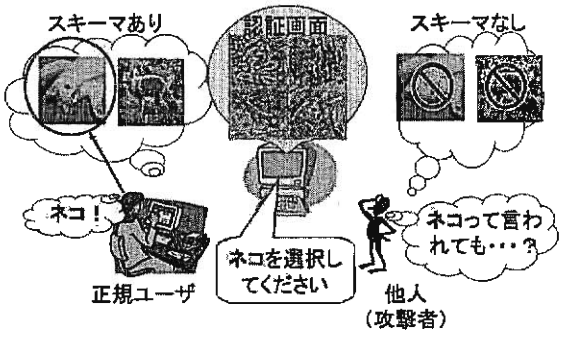

図 6　文献[10]の概観

本稿ではこのアイデアを拡張し，文献[10]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 7）．キューは，パス画像に対する部位情報（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難しい．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．キューにより指定す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，単純な覗き見攻撃にも耐性を有する．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．

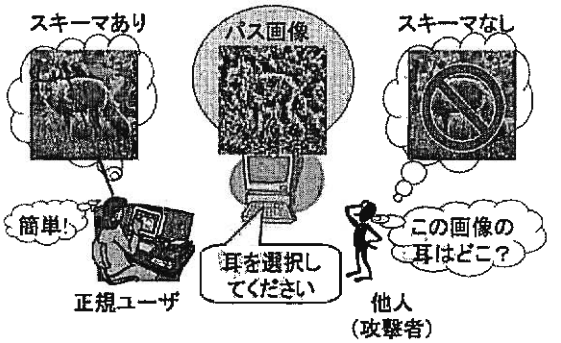

図 7　言語手がかりによって選択する部位を指示する認証方式の概観

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，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．

この問題を解決するために，本稿では，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 8 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 8 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困難である．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．

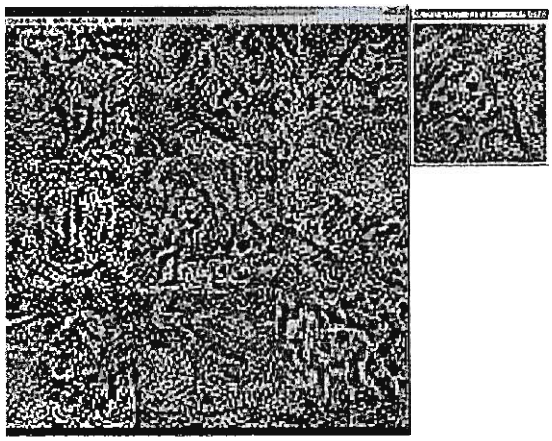

図 8 認証画面(左)と参照画面(右)の例

パス部位の位置は，毎回の認証でランダムに決定する．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 9 に提案方式(Q&R 型認証方式)の概観を示す．

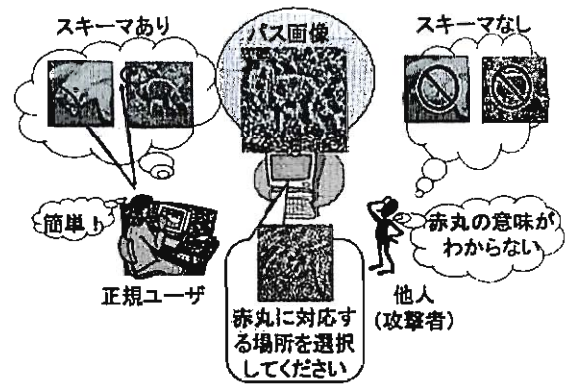

図 9　提案方式（Q&R 型画像認証システム）の概観

4. 基礎実験

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．

4.1. 本人認証実験

a)実験の目的

正規ユーザにとって，参照画像によって与えられるキュー（パス部位）を正しくに認識し，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．

b)実験方法

本実験の被験者は本学情報学部学生 5 名である．全被験者には，それぞれ 4 枚のパス画像と 1 枚の参照画像を登録してもらう．パス画像 4 枚と参照画像 1 枚はすべて異なる画像である．

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 8 左）と，参照画像 1 枚が表示されている参照ウインドウ（図 8 右）が被験者に提示される．参照画像上にはパス部位が赤い丸でプロットされる．

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．今回は，参照画像の赤い丸によって指示されたパス部位が「右足」であった場合，パス画像における「右足」と「左足」のどちらを選択しても正答とした．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ターンごとにランダムに選択される．

表 1 本人認証実験の結果

	部位の選択		画像の選択		ターン毎の平均回答時間
	認証成功率	ターン毎の成功率	認証成功率	ターン毎の成功率	
1日後	84.00%	96.00%	100.00%	100.00%	8.62
8日後	80.00%	94.50%	94.00%	98.00%	9.96

図 10 部位登録画面の例

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．

なお，被験者には画像を登録する際，パス画像 4 枚と参照画像 1 枚全てに対し，図 10 のような形でそれぞれの部位についても登録してもらった．

今回の実験で使用した画像は，様々な種類の動物が写っている背景つきの写真画像 100 枚である．

c)実験結果

実験結果を表 1 に示した．表中，「部位の選択－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，「部位の選択－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．「画像の選択－認証成功率」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施行を考えた時，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．一方，「画像の選択－ターン毎の成功率」は，各認証試行時に行う 4 ターンのパス画像選択（9 択の不鮮明化画像の中からパス画像 1 枚を選択するタスク）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．

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を「ターン毎の平均回答時間」として示した．

d)考察

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 日後ともおおむね 80%であることが見てとれる．画像の選択だけであれば，1 日後が 100%，8 日後が 94%であるため，暗示・応答型の仕組みを導入することで，正規ユーザの認証における負荷が増大したことがわかる．認証負荷増大の問題を今後解決していくためにも，本稿では本実験における失敗の傾向について分析を行った．失敗の傾向について分析した結果を表 2 に示す．

表 2 は，本人認証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，それらケース毎に失敗の数を示したものである．

(A) パス部位の領域境界から数ピクセル（1，2 ピクセル）ずれた位置を選択

(B) パス部位の領域境界から数十ピクセル（10～30 ピクセル）ずれた位置を選択

(C) パス画像中の登録部位（又はその付近）を選択してはいるが，それがパス部位ではない

(D) パス画像中の指示された部位を選択してはいるが，その領域が部位として登録されていない

(E) 選択した画像自体パス画像ではない

表 2 選択失敗の傾向について

失敗の種類	(A)	(B)	(C)	(D)	(E)	合計
1 日目	1	5	1	1	0	8
8 日目	1	1	2	3	4	11

(B)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，部位の位置等の細かな情報をスキーマから正確に認識することができなかったために起こったと考えられる．不鮮明化画像のスキーマからオリジナル画像を想起し細かな部位の位置を正確に認識することができるよう，スキーマの学習に工夫を取り入れていく必要があるだろう．

また，(A)と(B)については，登録されている部位にある程度のマージンを持たせる（θ ピクセル以内であ

れば選択成功として認める）ことで，認識のあいまいさによる入力のばらつきを吸収することができると考えられる．さらに，部位登録時にユーザに認証テストを行ってもらい，選択がばらつき易い部位やばらつき難い部位を推定し，ばらつき易い部位であればθを大きく，ばらつき難い部位であればθを小さく設定することで，ユーザに適したパス画像セットを用意することができると考えられる．

(C)に分類された失敗は，参照画像の記憶があいまいであったために起こったものであると考えられる．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にあった．また，参照画像は常に認証ウインドウの横に表示されているため，登録時に注意深く記憶していなかったと報告した被験者もいた．登録時にパス画像だけでなく参照画像に対しても確実にスキーマを学習させる必要があるだろう．

(D)に分類された失敗は，パス画像に部位を登録する際，適切に部位を登録しなかったために起こったものであると考えられる．パス画像の部位登録時に，登録可能な部位にも関わらず登録しなかったため，認証時に自分がどこを部位として登録したのかわからなくなり，結果的に選択に失敗したという事例がこのケースに含まれる．この問題に対しては，ユーザに登録可能な部位全てに対して適切な形式で部位を登録してもらうことで対応可能であると考えられる．

(E)に分類された失敗は，パス画像自体の選択を失敗したために起こったものである．被験者からは，本実験の前に行った別の実験で記憶したパス画像が本実験の囮画像としても用いられていたため，パス画像の選択に混乱をきたしたという報告があった．この問題に対しては，ユーザにとって馴染みの深い画像や以前にパス画像として使った画像を囮画像として用いないといった運用により対応することができると考えられる[1]．本実験結果を踏まえた上で，本認証方式の認証成功率改善についての検討を今後行っていく予定である．

4.2. 覗き見攻撃実験

a)実験の目的

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）の情報と，現在表示されているキュー（パス部位）とから，認証をパスするために十分な情報を得ることが困難であれば，提案方式が有限回の覗き見に対しても耐性を有していると考えることができる．これを確認するために，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．

b)実験方法

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 n 回（n=1,2,3）覗き見たことを想定し，パス画像および参照画像上の対応する部位を任意に n 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，n 箇所の部位は異なる色でプロットされる．また，参照画像には，現在の認証に対するキュー（パス部位）も異なる色の丸印でプロットされる．ここで，すべての丸印は，部位の重心の位置に半径 10 ピクセルでプロットすることとした．攻撃実験の画面の例を図 11 に示す．

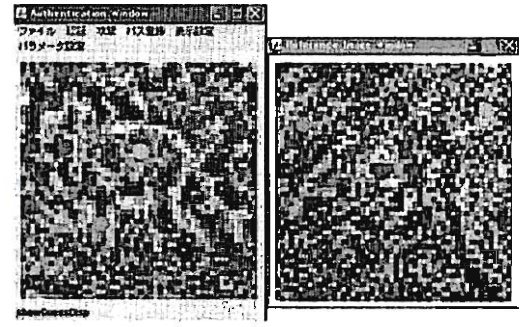

図 11　攻撃実験（過去の覗き見の回数が 3 回）の例

本実験では，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，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．4.1 節の被験者の 1 人に，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，4.1 節の認証実験のときと同じやり方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，4.1 節の被験者 5 人の中から，パス画像セットに対して部位の登録を行ってもらった被験者を除いた 4 人である．

c)実験結果

実験結果を表 3 に示す．表中，「成功率」は，各被験者につきパス画像 5 セット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（n）ごとに示したものである．なお今回は，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「右足」であった場合，パス画像における「右足」と「左足」のどちらを選択しても正答とした．

d)考察

覗き見情報 n=0～3 個において，おおむね 30%弱の割合で選択に成功していることが見てとれる．攻撃者

表 3　覗き見攻撃実験

成功率			
覗き見情報　0 個	覗き見情報　1 個	覗き見情報　2 個	覗き見情報　3 個
26.25%	28.75%	25.00%	30.00%

に非常に有利な条件（パス画像 1 枚と参照画像 1 枚のみを表示する攻撃実験環境）ではあるものの，約 3 回に 1 回の割合でパス部位の選択に成功してしまっている．そのため，本稿では，攻撃者が推測によく使っていた推測方法を分析し，今後の改良につなげる．

被験者がよく用いていた部位の推測方法として，実験で用いた画像の特徴を活用した方法がある．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．

このような攻撃に対応する手段として，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）を崩す方法が考えられる．例えば，歪めた画像を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．

今回の攻撃実験では，覗き見情報の数（n）に関係なく，覗き見成功率がほぼ一定であるという結果が得られた．もしこれが，覗き見の有無が攻撃成功率に影響しないという事実に起因するものであるのならば，本 Q&R 型画像認証方式は覗き見攻撃によって認証情報が漏れることがないということを意味することになると考えられる．これについては今後早急に調査していく予定である．

また，覗き見情報が 2 個のとき，成功率が若干ではあるが下がっていることが見てとれる．これは攻撃者が，与えられた覗き見情報により，パス部位の推測を惑わされたのではないかとも考えることができる．これを活用することで，攻撃者に間違った推測を促すようなキュー（パス部位）の提示方法を実現することができるかもしれない．これについても，今後の課題として検討していきたい．

5. まとめと今後の課題

本稿では一見すると不鮮明な画像の特徴を活用することで，Q&R 型という新しいコンセプトに基づくワンタイム型の認証方式を提案した．提案方式は，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 つの特長を有する画像認証方式となっている．ただし，現在のところ，正規ユーザの負荷および攻撃耐性の面で課題を残しているため，実験結果から得られた情報を元に提案方式の改善を行っていく予定である．

謝　辞

本研究は一部，（財）セコム科学技術振興財団の研究助成を受けている．

文　献

[1] R Dhamija, A Perrig, “Deja Vu: A User Study Using Images for Authentication”, 9th USENIX Security Symposium, pp.45-58, 2002.

[2] 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.

[3] L.Sobrado, J.-C.Birget, “Graphical passwords”, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol.4, 2002. http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm

[4] V. Roth, K. Fischer, and R. Freidinger, “A PIN entry method resilient against shoulder surfing”, In Proceedings of ACM CCS’04, pp.236-245, 2004.

[5] 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 年 3 月．

[6] 高田哲司，“fakePointer 2：個人認証における覗き見攻撃への安全性を向上させるユーザインタフェースの提案”，暗号と情報セキュリティシンポジウム（SCIS2007），電子情報通信学会 情報セキュリティ研究専門委員会，2007 年 1 月

[7] 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.

[8] RSA Security Inc., “RSA SecurID”, http://www.rsasecurity.com/node.asp?id=1156（2008 年 7 月確認）

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

[10] 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-34-56，pp.411-418，2006 年 7 月．