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

2009－DPS－138（16）
2009－CSEC－ 44（16）
2009／3／5

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

小島 悠子[1]，山本 匠[2,3]，西垣 正勝[2,4]
[1] 静岡大学大学院情報学研究科〒432-8011 静岡県浜松市城北3-5-1
[2] 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
[3] 日本学術振興会特別研究員（DC1） 〒432-8011 静岡県浜松市城北3-5-1
[4] 科学技術振興機構, CREST 〒432-8011 静岡県浜松市城北3-5-1
E-mail: nisigaki@inf.shizuoka.ac.jp

あらまし

人間の画像認識能力の高さを用いた画像認証方式が注目を集めている．しかし，多くの画像認証方式は覗き見攻撃に脆弱であり，覗き見攻撃に強い方式が望まれる．覗き見攻撃耐性を向上させる方式として，攻撃者に認証情報が一意に特定されないよう認証情報の入力を曖昧にする方式が提案されている．しかし，既存の曖昧入力方式は画像群を空間的に配置する方法となっているため，広い空間の中からパス画像を探し出すことが困難という問題があった．そこで本稿では，常に同じ位置にパス画像と囮画像を配置することで，広い空間の中からパス画像を探し出すというユーザの探索負荷を軽減する．そして，認証の都度変化する「あみだくじ」を画像群上に配置することによって，パス画像を起点に毎回異なる「経路」を辿ってレスポンスを生成させることでワンタイム性を追加し，覗き見攻撃耐性の維持を図る．基礎実験を行い提案方式の有効性を確認する．
キーワード 画像認証，CHC方式，利便性，覗き見攻撃耐性，あみだくじ

A study on image-based authentication with usability and shoulder-surfing resistance

Yuko Kojima[1], Takumi Yamamoto[2,3], Masakatsu Nishigaki[2,4]
[1] Graduate School of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
[2] Graduate School of Science and Technology, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
[3] Research Fellow of the Japan Society for the Promotion of Science (DC1), 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
[4] Japan Science Technology and Agency, CREST, 3-5-1 Johoku, Hamamatsu, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract

Although image-based user authentication systems have gotten a lot of attention recently to reduce the burden of memorizing password, they are usually vulnerable against shoulder surfing attacks. To overcome this problem, shoulder-surfing resistant image-based authentications with indirect-image-selection had been proposed. However, these schemes have problems that "it is difficult for authorized users to find out their pass images among a wide space", because a large number of images are randomly arranged in authentication window to implement indirect-image-selection. Therefore, this paper proposes to fix the placement of pass-images and decoy-images at every authentication, in order to eliminate user's burden to find out pass-images. To realize that, we tries to introduce the concept of a "AMIDA-lottery" into image-based authentication. By using the lottery, we can produce different response at every authentication trials, and thus its shoulder surfing resistibility will be maintained. We conduct fundamental experiments to estimate the feasibility of the proposed scheme.
Keyword image-based authentication, CHC (convex-hull-click) scheme, usability, shoulder-surfing resistance, AMIDA-lottery

1. 背景

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方式においては，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．この問題の対策の一つとして，攻撃者に認証情報が一意に特定されないよう認証情報の入力を曖昧にする方

式が提案されており，その代表的なものとしてSobradoらの方式[3, 4]がある．しかし，この方式は認証の都度ランダムに配置される大量の画像群の中からパス画像を探し出す方式となっているため，パス画像の探索負荷が問題となっていた．そこで本稿では，常に同じ位置にパス画像と囮画像を配置することで，ユーザの探索負荷を軽減する．そして，認証の都度変化する「あみだくじ」を画像群上に配置し，パス画像を起点として毎回異なる「経路」を辿ってレスポンスを生成させることでワンタイム性を追加し，覗き見攻撃耐性の維持を図る．すなわち提案方式は，何の手掛かりも無しに毎回異なる場所にあるパス画像を探し出す「探索負荷」に比べ，常に同じ場所から毎回異なる経路を辿る「追跡負荷」のほうが人間にとって容易であることを利用した画像認証方式となっている．

以下，2章でCHC方式を紹介し，その問題を挙げる．3章で提案方式の詳細を述べ，基礎実験によってCHC方式と提案方式の比較検討を行った結果を4章に示す．5章で両方式を考察し，6章で本稿をまとめる．

2. 既存方式(CHC方式)

本章では，著者らが注目したSobradoらの方式[3, 4](以降，CHC方式と記す)を紹介し，本方式の課題を示す．CHC方式では，認証システムからのチャレンジとして，多数のアイコン(以降，キャラクタと呼ぶ)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パスキャラクタを画面の中から探し出し，パスキャラクタ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）．

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」という曖昧な形で返すため，覗き見攻撃者にパスキャラクタが一意に漏洩しない．

しかし，既存方式では，総当たり数を確保するために大量の囮キャラクタを用意した上で，覗き見攻撃耐性を確保するためにキャラクタの配置を毎回ランダムに変化させる必要がある．このような方法では，広い空間の中に敷き詰められた多数のキャラクタの中からパスキャラクタを探し出すことは，ユーザにとって非常に手間のかかる操作となる．

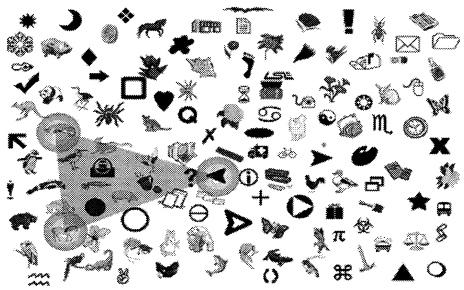

図1　文献[3]の認証画面例

3. 提案方式

3.1. アプローチ

本章では，パスキャラクタと囮キャラクタを毎回ランダムに配置することで曖昧入力を実現するというCHC方式に対し，キャラクタ群を常に同じ位置に配置して探索負荷を抑えつつ，認証の都度変化する「あみだくじ」をキャラクタ群上に配置し，ユーザにパスキャラクタを起点として毎回異なる経路を辿ってレスポンスを生成させる方式を提案する．

登録フェーズでは，ユーザに自分のパスキャラクタとパスアルファベットを記憶してもらう．認証システムは，パスキャラクタと多数の囮キャラクタをランダムに配置するとともに，その上にあみだくじを表示する．パスアルファベットは，あみだくじの各列と列の間（以降，区間と呼ぶ）に割り当てられる．認証フェーズでは，ユーザは，パスキャラクタを起点として，パスアルファベットが表示されている区間（以降，パス区間と呼ぶ）に向かってあみだくじを辿る．パス区間に辿り着いた時点の横線の上部に付記されている数字がレスポンスとなり，その数字を入力することにより認証が行われる(図2)．パス区間に辿り着く前にあみだくじの上端または下端に到達した場合には，そこに付記されている数字がレスポンスとなる(多くの場合，あみだくじは上から下へ辿ることになっているが，今回の方式では，下から上に辿ることもある)．

ここで重要なことは，あみだくじの概観，すなわち，画面上のキャラクタ群およびアルファベットの位置は常に同じであるということである．よって，ユーザは登録フェーズにて，パスキャラクタの位置についても覚えてしまって良い．これに対し，あみだくじの横線の有無および横線の上部に付記される数字は認証の都度ランダムに変化する．あみだくじには，横線が1本追加・削除されるだけで経路が変化するという性質があるため，画像群やアルファベットが固定されていてもレスポンスは毎回変化する．

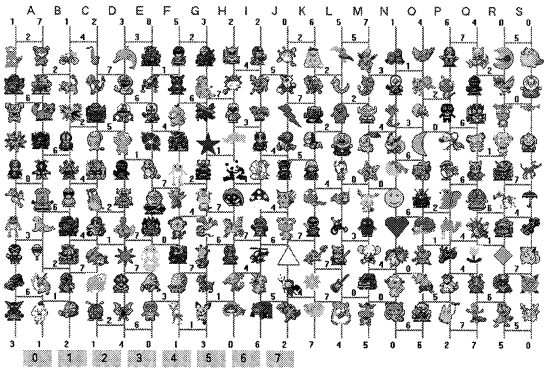

図2　提案方式の認証画面の例

3.2. 認証方式

提案方式の登録フェーズおよび認証フェーズの具体的な手順を説明する．

● 登録フェーズ

【Step1】認証システムはユーザにキャラクタ一覧とアルファベットのリストを提示する．

【Step2】ユーザはパスキャラクタとして用いたいキャラクタ1体と，アルファベット1文字を選択する．

【Step3】認証システムは，パスキャラクタと囮キャラクタをランダムにM行×N列に配置し，その上にあみだくじを提示する．あみだくじの各区間の上部には左から右へ昇順にアルファベットが，あみだくじの横線の上部にはランダムな数字が付記される．

【Step4】ユーザは自分が選択したパスキャラクタの位置およびパスアルファベットを記憶する．

【Step5】認証システムはパスキャラクタとパスアルファベットを秘密情報として登録する．また，すべてのキャラクタの表示位置も記憶する．

● 認証フェーズ

【Step1】システムは，登録フェーズにてユーザに提示したあみだくじを表示する．キャラクタ群およびアルファベットは毎回同じ配置だが，あみだくじの横線の配置およびそれに付記される数字は認証ごとにランダムに変化する．

【Step2】ユーザは，パスキャラクタを起点としてパス区間に向かってあみだくじを辿る．例えば図3の例では，パスキャラクタから上に辿ると右に，下に辿ると左に進む．この場合，パス区間に近づくようにあみだくじ辿るためには，パスキャラクタから上に辿ることになる．また，図4の例では，パスキャラクタから上に辿っても下に辿っても右にしか進めない．このような場合は，パスキャラクタが上端に近い場合は下へ，下端に近い場合は上端へたどることとする．パス区間に到達した時点の横線に付記されている数字がレスポンスとなる．パス区間に到達することなくあみだくじの上端または下端に到達した場合は，その時点の横線に付記されている数字をレスポンスとする．

【Step3】ユーザが正しいレスポンスを入力することができれば認証成功とする．

パスキャラクタ数，囮キャラクタ数，認証フェーズにおけるターン数や，横線の上部に付記される数字の範囲は，要求される認証強度に応じて定められる．

4. 実験

CHC 方式および提案方式のプロトタイプシステムを実装し，認識負荷および覗き見攻撃耐性を基礎実験を通じて評価する．なお，本実験の被験者は本学情報学部学生5名である．

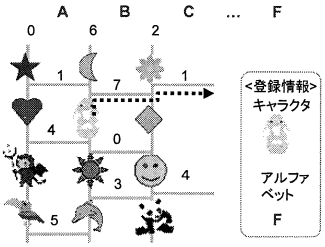

図3　あみだくじを辿る様子の例1

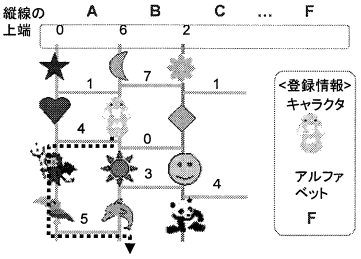

図4　あみだくじを辿る様子の例2

4.1. CHC 方式に対する予備実験

提案方式では，CHC 方式と同等の覗き見攻撃耐性を確保しつつ認識負荷を低下させる方式を目指している．そこで，両方式の攻撃耐性と認識負荷を公正に評価するためには以下に記載する項目のバランスを考慮する必要がある．

①記憶負荷…ユーザが記憶する秘密情報の量．記憶する情報量が増える(記憶負荷が増える)ほど，攻撃耐性は向上する．

②入力選択肢数…攻撃者がランダムにレスポンスを入力した際に認証に成功する確率の逆数．

③覗き見攻撃耐性･･･認証操作をビデオカメラで盗撮された場合，何回の盗撮に耐え得るか．以降では特に断りのない限り，「覗き見攻撃耐性」とはビデオカメラによる盗撮を意味する．

ただし，CHC 方式では「毎回位置や面積の変化する凸包の内部をクリックする」という方式の性質上，「②入力選択肢数」を理論的に求めることが困難である．そこで著者らは文献[5]に注目した．文献[5]では，入力を曖昧にすることにより覗き見攻撃に耐性を持たせる認証方式全般の覗き見攻撃耐性を理論的に求めており，入力選択肢数がSである認証システムの認証行為を1回覗き見られた場合，パス情報の候補が「パス情報の組合せ総数（例えばPINの場合は10,000通り）の1/S」に減少することが導出されている．そこで，今回実装したCHC方式のプロトタイム認証システムを用いて覗き見実験を実際にシミュレートし，1 回の認証行為の覗き見によってパス情報の候補がどれくらいに絞られるかを実験的に求めることとした．文献[5]の理論より，その逆数がCHC方式の事実上の入力選択肢数ということになる．

今回のCHC方式のプロトタイプでは，システムを簡

素にするため，図5のようにキャラクタを縦10体×横20体に整然と並べた．正規ユーザが記憶すべきパスキャラクタの数は3体，パスキャラクタと一緒に表示する囮キャラクタの数は197体とする．認証フェーズにて3体のパスキャラクタが縦一列に並ぶ配置，3体のパスキャラクタが形成する三角形が極端に細長くなる配置となった場合は全キャラクタの配置をやり直した．

今回の認証システムは，盗撮攻撃の機能についても実装してある．被験者は認証フェーズ(200体のキャラクタの中から登録キャラクタを探し，登録キャラクタを頂点とした凸包内部を選択する)を20回成功するまで繰返す．システムは，3体のキャラクタを任意に選択する．ユーザによる20回の認証試行の中で，ユーザがクリックした座標が一度でもそのキャラクタ3体を頂点とする三角形の内部から外れたならば，その3体のキャラクタは正しいパスキャラクタのセットではないことが判明する．これを，パスキャラクタ3体のすべての組合せ（200体のキャラクタから3体のパスキャラクタを選択する組合せ ${}_{200}C_3$ 通り）に対して繰り返し，パスキャラクタの組合せの候補を絞り込んでいく．以上の作業を20回(認証回数/人)×5人(被験者数)分行い，1回の盗撮攻撃によりパスキャラクタ3体の組み合わせの候補数が何分の一に絞り込まれるかの平均を求めた実験結果を表1に示す．「残存候補数の割合」は認証試行を1回盗撮された場合に，パスキャラクタ3体の組合せの候補が何分の一に絞り込まれるかという割合の逆数をとった値であり，これが入力選択肢数の実効値ということとなる．

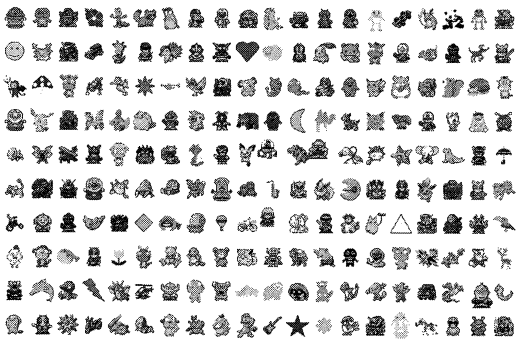

図5　実装したCHC方式の認証画面

表1　盗撮攻撃シミュレーション結果

被験者	1	2	3	4	5	平均
残存候補数の割合	11.0	6.4	7.0	6.8	10.0	8.24

表1より，今回の実験条件においては，CHC方式における1回の認証行為（パスキャラクタ3体によって構成される凸包の内部をクリック）は，8択の中から正しい回答を選択する入力操作とほぼ同等であることがわかった．よって，次節で用いる提案方式の認証システムでは，入力選択肢数を8に設定して実験を行ってゆく．

4.2. 認識負荷実験

4.2.1. 実験項目

CHC方式における秘密情報はパスキャラクタ3体であり，提案方式の秘密情報はパスキャラクタ1体とパスアルファベット1文字である．アルファベットを画像で代用することも可能であることを考慮すると，提案方式の秘密情報はパスキャラクタ2体分に相当する．そこで，今回の実験では秘密情報の数を両方式で合わせるために，提案方式においてはパスキャラクタ2体とパスアルファベット1文字を使用する方式（次項の方式1〜3に詳しく示す)についても検討することとする．

一方，認証負荷に関しては，CHC方式ではキャラクタ群の中から3体のパスキャラクタを探し出すという探索負荷がユーザにかかるのに対し，提案方式ではあみだくじを辿るという追跡負荷がユーザに課せられることになる．そこで今回の実験では，CHC方式においてはユーザがパスキャラクタ3体を探し出して凸包の内部をクリックするまでにかかる時間，提案方式においてはパスキャラクタからパス区間まであみだくじを辿ってレスポンスを入力するまでにかかる時間を調査し，両者を比較評価する．

4.2.2. 実験方法

a) CHC方式

前節にて実装した認証システムを用い，5人の被験者に対して10回の認証試行を実施してもらった[1]．

b) 提案方式

以下に示す3方式の認証システムを実装し，それぞれに対し，5人の被験者に10回の認証試行を実施してもらった．3方式とも，画面上の全キャラクタの配置は図5のCHC方式と同様に縦10体×横20体とした．すなわち，各列と列の間の区間の数は19であり，ここにA〜Sのアルファベットが付される．あみだくじの横線の総数は100本である．今回の入力選択肢数は8に設定することとしたため，横線の上部に付記する数字の範囲は0〜7となる．なお，登録フェーズにおいては，方式の確認を兼ね，被験者の納得がいくまで認証フェーズの練習を行うことを許した．また，順序効果を考慮し，各被験者には方式1〜3をランダムな順番で実施してもらった．

<方式1>

正規ユーザが記憶すべきパスキャラクタの数を1体，パスキャラクタと一緒に表示する囮キャラクタの数を199体とする．被験者は登録フェーズにて1体のパスキャラクタと1文字のパスアルファベットを記憶する．認証フェーズでは，パスキャラクタを起点としてパス区間に向かってあみだくじを辿り，パス区間に辿り着いた時点の横線に付記されている数字を回答する．

[1]実際には，前節で行ったCHC方式の入力選択肢数を測定するための20回の認証試行のうち，最初の10回を本項の実験データとして使用した．

〈方式 2〉

正規ユーザが記憶すべきパスキャラクタの数を 2 体，パスキャラクタと一緒に表示する囮キャラクタの数を 198 体とする．被験者は登録フェーズにて 2 体のパスキャラクタと 1 文字のパスアルファベットを記憶する．認証フェーズでは，まず 1 体目のパスキャラクタを起点としてパス区間に向かってあみだくじを辿り，パス区間に辿り着いた時点の横線に付記されている数字を回答する．次に，2 体目のパスキャラクタを起点として同様の操作を行う．すなわち，8 択の回答を 2 回繰り返す．

〈方式 3〉

正規ユーザが記憶すべきパスキャラクタの数を 2 体，パスキャラクタと一緒に表示する囮キャラクタの数を 198 体とする．被験者は登録フェーズにて 2 体のパスキャラクタと 1 文字のパスアルファベットを記憶する．あみだくじの横線には，0〜7 の数字に加え，A〜S のアルファベットも付記される．認証フェーズでは，まず 1 体目のパスキャラクタを起点としてパス区間に向かってあみだくじを辿り，パス区間に辿り着いた時点の横線に付記されているアルファベットを知る．このアルファベットが 2 回目のあみだくじの「ゴール区間」となる．すなわち，2 体目のパスキャラクタを起点としてゴール区間に向かってあみだくじを辿り（図 6），ゴール区間に辿り着いた時点の横線に付記されている数字を回答する．

各方式におけるパラメータを表 2 にまとめる．表中，NA はアルファベットの種類（あみだくじにおける区間の数），NC は画面に表示されるキャラクタの総数，PA はパスアルファベットの数，PC はパスキャラクタの数，N は秘密情報 PA と PC の組合せの候補数（CHC 方式においては ${}_{NC}C_{PC}$，提案方式においては ${}_{NA}C_{PA}\times{}_{NC}P_{PC}$），S は入力選択肢数である．

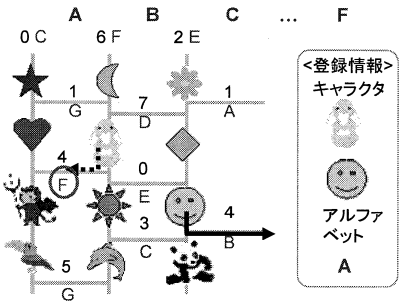

図 6　方式 3 の認証画面

表 2　各方式のパラメータ

	NA	NC	PA	PC	N	S
CHC 方式	-	200	-	3	1313400	8.24
方式 1	19	200	1	1	3800	8
方式 2	19	200	1	2	756200	64
方式 3	19	200	1	2	756200	8

4.2.3. 実験結果

認証実験の結果を表 3 に示す．入力選択肢数の観点からは，方式 2 は他方式 2 回分の認証試行と同等であるため，方式 2 の認証時間を 2 分の 1 に換算したものが「方式 2'」である．

表 3　認証時間（単位[秒]）

被験者	1	2	3	4	5	平均
CHC 方式	31.7	10.9	11.5	13	22	17.9
方式 1	4.5	8.7	3.7	5.0	3.3	5.0
方式 2	21.1	10.0	17.5	16.0	11.7	15.3
方式 2'	10.6	5.0	8.8	8.0	5.8	7.7
方式 3	15.6	19.8	18.9	14.7	13.7	16.5

表より，方式 1 の認証に要する時間は CHC 方式の約 1/3 である．方式 2（方式 2'）の認証に要する時間は CHC 方式の約 1/2 である．また，方式 3 の認証にかかる時間は CHC 方式と同等であることが見て取れる．

4.3. 盗撮攻撃実験

4.3.1. 実験の目的

4.1 節，4.2 節で得られた実験結果をもとに，CHC 方式および提案方式が何回の覗き見攻撃に耐え得るのかを評価する．今回の覗き見はビデオによる盗撮を想定している．

4.3.2. 実験方法

a) CHC 方式

4.1 節にて実装した認証システムを用い，5 人の被験者に対して 20 回の認証試行を実施してもらった[2]．各被験者に 20 回分のデータをランダムな順番で選択し，パスキャラクタ 3 体の組合せが一意に特定されるまでの盗撮回数を求める．

b) 提案方式

4.1 節にて実装した CHC 方式に対する盗撮攻撃の機能と同様の機能を，4.2 節にて実装した提案方式に対する認証システムにも実装し，5 人の被験者に対して 20 回の認証試行を実施してもらった[3]．

システムは，方式 1 に対しては 1 体のキャラクタと 1 文字のアルファベットを任意に選択し，当該キャラクタを起点として当該アルファベット区間まであみだくじを辿り，レスポンスを予想する．ユーザによる 20 回の認証試行の中で，ユーザが実際に入力したレスポ

[2]実際には，4.1 節で行った CHC 方式の入力選択肢数を測定するための 20 回の認証試行のデータをそのまま流用した．

[3]実際には，4.2 節の実験の時点で実験システムには既に盗撮攻撃機能が実装されており，4.2 節にて行われた被験者当たり 10 回の認証試行のデータについては，本実験のデータとして流用した．残りの 10 回の認証試行については，被験者の負担を軽減するために，実験実施者が各被験者の登録情報を用いて認証を代行することによって収集した．

ンスが一度でもシステムが予想したレスポンスと外れたならば，そのキャラクタとアルファベットは正しいパスキャラクタとパスアルファベットの組合せではないことが判明する．これを，パスキャラクタとパスアルファベットのすべての組合せ（${}_{NA}C_{PA}\times{}_{NC}P_{PC}$ 通り）に対して繰り返し，パスキャラクタとパスアルファベットの組合せの候補を絞り込んでいく．方式 2 および 3 の盗撮攻撃についても同様である．

被験者ごとに 20 回分のデータをランダムな順番で選択し，パスキャラクタとパスアルファベットの組合せが一意に特定されるまでの盗撮回数を求める．

4.3.3. 実験結果

盗撮攻撃の実験結果を表 4 に示す．表 3 と同様，入力選択肢数の観点からは，方式 2 は他方式 2 回分の認証試行と同等であるため，方式 2 における盗撮に耐え得る回数を 2 倍に換算したものが「方式 2'」である．今回の実験では，提案方式において 20 回分の盗撮データ全てを用いてもパスキャラクタおよびパスアルファベットの候補を一意に絞り込むことができない場合が存在した．これは，実験データに偏りが生じたためであると考えられる．そこで，このような場合は，候補数の減少が収束した時点（それ以上候補が絞れなくなった時点，または，候補数が 1 桁にまで絞られた後，さらに 3 回分の盗撮データを用いて絞り込みを続けても候補が一意に絞られなかった時点）までの回数を掲載した．

表 4　CHC 方式において秘密情報を特定された回数

被験者	1	2	3	4	5	平均
CHC 方式	8.8	8.8	8.1	8.1	8.1	8.4
方式 1	4.5	4.5	5.1	9.4	4.7	5.6
方式 2	7	4.3	4.6	4.3	3.8	4.8
方式 2'	14	8.5	9.1	8.6	7.6	9.6
方式 3	8.6	9	10.1	7.1	7.7	8.5

実験結果より，方式 1 は約 5 回，CHC 方式と方式 2（方式 2'）および方式 3 は約 8 回程度の盗撮で登録情報（パスキャラクタおよびパスアルファベット）を一意に特定されることが分かる．

5. 考察

5.1. CHC 方式と提案方式の比較

4.2.3 の実験結果より，方式 2（方式 2'）の認証に要する時間は CHC の 2 分の 1 であり，4.3.3 の実験結果より登録キャラクタを特定される回数は同程度になることが分かった．したがって，方式 2（方式 2'）は CHC 方式の利便性を向上させつつ覗き見攻撃耐性を維持しているといえる．

今回の実験では，方式 3 と CHC 方式の間に差がみられなかった．これは，CHC 方式におけるパスキャラクタを探し出す探索負荷と方式 3 におけるあみだくじを辿る追跡負荷がトレードオフになっている可能性を示唆している可能性がある．

5.2. 提案方式間の比較

方式 2（方式 2'）は，4.2.3 および 4.3.3 の実験結果より利便性および覗き見攻撃耐性を有する方式と言える．

4.2.3 の実験結果より認証に要する時間の短さは方式 1，方式 2，方式 3 の順になる．方式 2 においては，方式 1 の操作が 2 回繰り返されている．しかし，なぜか，方式 2 の認証速度は方式 1 の 2 倍では収まらず，それ以上の認証時間がかかっている．この結果から，ユーザにとっては，方式 1 のようななるべく簡素な操作による認証が望ましいと言える．ただし，4.3.3 の実験結果より，方式 1 は盗撮耐性が低い．そのため，方式 1 は覗き見攻撃耐性よりも利便性を重視する環境での利用が望ましいと考えられる．

6. まとめ

本稿では，画像認証に「あみだくじ」のコンセプトを導入することにより，覗き見攻撃耐性を維持しつつ認識負荷の軽減を実現した．既存方式である CHC 方式と提案方式の実験システムを実装し，認証に要する時間および盗撮耐性を評価する基礎実験を行った．実験の結果からは提案方式の有効性が示された．今後は，被験者を増やして認識負荷実験および覗き見攻撃実験を行う予定である．

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．

参考文献

[1] R. Dhamija, and A. Perrig, "Deja Vu: A User Study Using Images for Authentication", 9th USENIX Security Symposium, pp.45-58, 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, and 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] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", In Proc. AVI'06, pp 177-184, 2006.

[5] 古原和邦，今井秀樹，"均等写像を用いた質問応答型直接個人認証方式ののぞき見攻撃に対するさまざまな安全特性について"，電子情報通信学会論文誌(A)，vol. J79-A，no.8，pp409-421，1991