回答候補画像の追加と正解画像の集中配置による再認式画像認証の安全性改善と操作負担抑制

森 康洋 †　　高田 哲司 †

† 電気通信大学
182-8585 東京都調布市調布ケ丘 1-5-1
m1110146 @mail.uec.jp and zetaka @computer.org

あらまし 本研究では，再認式画像認証の安全性を改善する手法として次の 2 手法を提案する．1) 認証回答時の回答候補画像を増やす．2) 正解画像の配置に一定の条件を課す．これらの手法により記憶負担を増やすことなく安全性向上を実現するととに，それにともなう操作負担増にも配慮した再認式画像認証を提案する．この提案に基づきプロトタイプシステムを実装し，利用可能性と操作負担に関して被験者による評価実験を実施した．その結果，正解画像の条件付き配置については操作負担の抑制に効果があること，ならびに 100 枚の画像群から 4 枚の正解画像を選択するのに平均 12 秒で操作可能なことが明らかになった．

Realizing Better Security in Recognition-based Image Authentication by both Increasing candidate images and Conditional layout of secret images

Yasuhiro Mori†　　Tetsuji Takada†

†The University of Electro-Communications.
1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
m1110146 @mail.uec.jp and zetaka @computer.org

Abstract In this paper, We propose two ideas to improve security level of recognition-based image authentication without increasing operational burdens to users: 1) increasing candidate images in an answering screen, 2) placing a condition on an answer image layout. These ideas realize security-level improvement of recognition-based image authentication and minimize related operational burden to users. We implement a prototype system based on the ideas and evaluate usability and operational burden of the proposed system with subjects. From the result of the evaluation, the conditional layout of answer images has an effect to suppress operational burden. Moreover, a user can pick up four answer images in average 12 seconds from one hundred images.

1　はじめに

画像を秘密として応用する個人認証には大きく 3 つのカテゴリーがある [1].

- 図画再生 (drawmetric)
- 手がかり付き想起 (cued-recall)
- 再認 (recognition)

これらはどれも知識照合型個人認証手法であり，既存手法における記憶負担を改善しうる手法と

して様々な研究が試みられている．これら 3 手法の中でも再認による画像認証は，記憶負担の効果が最も期待できる手法だと考えられている [2]．その理由は，回答入力時に回答候補画像が表示されるため，表示画像と利用者の記憶との相互作用により以下の効果が期待できるからである．

- 視覚記憶の優位性
- 回答を思い返す可能性 (Deja vu 効果)

一方，再認手法は他の手法と比較して安全性が低くなる傾向にある．回答方法は複数の回答候補の中から正解を選択する手法になるため，理論的な安全性，すなわち総あたり攻撃への安全性は「認証画面における回答候補の画像数」と「正解画像の枚数」に依存することになる．

そこで本研究では，再認式画像認証の利点を可能な限り維持するため，正解画像の枚数を変更せず，回答候補の画像数を増やすことにより安全性を向上させる手法について考察を行った．またその考察に基づきプロトタイプの実装を行うとともに被験者による評価実験を行った．本論文では，その改善手法と評価結果について報告する．

2 回答候補画像数の増加による安全性改善

再認式画像認証の理論的安全性，すなわち総当たり攻撃への安全性を改善する手法には以下の 3 つが考えられる．

a) 正解画像の枚数を増やす
b) 回答順序を秘密の一つとする
c) 回答候補画像の数を増やす

上記の手法のうち a),b) は，安全性改善につながるものの利用者の記憶負担を増加させることにもなる．一方 c) は，回答入力時に認知・操作負担を増加させる懸念があるものの，秘密情報には変化がないため記憶負担の増加にはならない．この考察から，項目 c) の「回答候補画像の数を増やす」という手法を基本とする再認式画像認証の改良を試みた．

ここで既存の再認式画像認証には大きく 3 つの手法があり，以下のように分類することができる．ここで正解画像の枚数を 3 枚，認証画面における回答候補の画像数を 9 枚 ($= 3 \times 3$) と仮定した場合の総あたり攻撃への安全性も併記する．

i) `mStage-1Choice`:
9 枚から回答 1 枚を選択．それを 3 回行う
(安全性：$1/9 \times 1/9 \times 1/9 = 1/729$)
ii) `1Stage-mChoice-wo/Order`: 9 枚から回答 3 枚を順不同で選択 (それを 1 回行う)
(安全性：$3/9 \times 2/8 \times 1/7 = 1/84$)
iii) `1Stage-mChoice-w/Order`: 9 枚から回答 3 枚を既定順序通りに選択 (それを 1 回行う) (安全性：$1/9 \times 1/8 \times 1/7 = 1/504$)

ここで回答候補の画像数を増やすということは，9 枚と仮定している画像数を増やすことである．この際，方法 i) は回答候補画像群を複数用意する必要があるため，回答候補の画像数を増やすとシステム利用開始時に多くの画像が必要となる．方法 ii), iii) は画像 9 枚で認証可能になるのに対し，方法 i) は 27 枚の画像が必要になり，また画像枚数を増やせば増やすほど大きな差になる．よって手法 i) よりは ii), iii) の手法で提案方法による改良を試みることが望ましいと言える．一方，ii) と iii) の方法を比較すると，安全性に大きな違いがある．ゆえに方法 iii) の方が望ましいと言える．これにともない，前述の考察で b)「回答順序を秘密の一つとする」手法は記憶負担を増やすことになるため改良法としては対象外としていたが，安全性確保のため導入することとする．

ここで回答候補の画像数を増やした際の効果について一例を示す．手法 iii) において仮に回答候補の画像枚数を 9 枚 (=3×3) からおよそ 2.5 倍の 25 枚 (=5×5) に増やしたとする．すると利用者が記憶保持する秘密情報は変化しないまま，ランダム回答が正解となる確率は 1/504 から 1/303,600 と，おおよそ 1/600 になる．

理論的には上記の通り，記憶負担を追加せずに安全性の改良が可能になる．しかし，ここで２つの問題が発生する．

r1) 機器による制約，特に画面内に表示可能な画像枚数
r2) 操作および認知負担の増加

これらの問題を制約として捉え，これらの制約のもとで妥当と考えうる負担増加に抑制しつつ，回答候補の画像数を増やす方法を検討する．

2.1 画像提示方法

ここで機器制約として機器画面内に一度に表示可能な画像数を 20 枚 (=5 行 ×4 列)，回答候補の画像数を 100 枚と仮定する．また正解画像は 4 枚で秘密情報は順序付きとする．またタッチパネルを装備した認証端末を想定する．これらの条件のもとで利用者に認証画面を提示する方法として，正解画像をランダムに配置することを前提に以下の 2 つの方法を考えた．

提示案 1) 1 グリッド
横 4 列，縦 25 行の縦長の画像グリッドを作成し，利用者は縦方向にスクロールすることで回答画像群を閲覧する．

提示案 2) 複数グリッド
回答候補画像群を画面内に一度に表示できる 20 枚の画像グループに 5 分割し，それぞれを画像グリッド化する．これらの画像グリッドはフリック操作で切り替え回答画像を閲覧する．

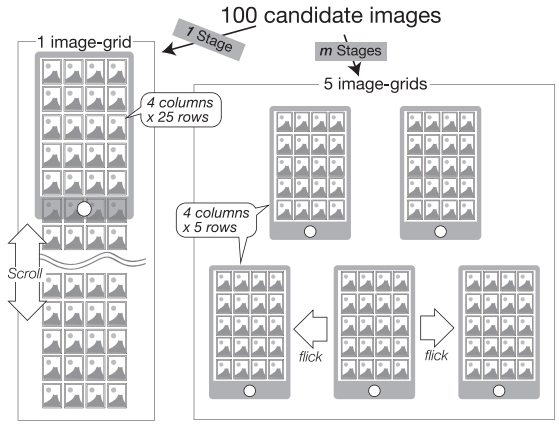

図 1: 2 つの画像提示方法

ここで正解画像をランダム配置にすると，利用者はすべての正解画像が見つかるまで回答候補画像を閲覧し，正解画像を見つけ出す必要がある．これは操作・認知負担を増大させることになり，回答候補画像の数が増えるとともにその負担も比例して増えることが予想されるため，軽減策があるべきである．そこで我々は正解画像の集中配置を提案する．正解画像をランダムに配置するのではなく，認証端末が一度に表示できる範囲内にすべての正解画像を配置する方法である．この規則により，正解画像が 1 つ見つかればその周辺に他の正解画像も存在することになり，正規の利用者にとっては正解画像の探索が容易になる．

この方法は上記の提示案 1, 2 のどちらにも適用できる．秘密情報空間について考察する．集中配置を提示案 2 で実施した場合，5 組の画像グリッドの 1 つに正解画像をすべて埋め込むことになる．すると，秘密情報の取りうる数は正解画像が含まれる画像グリッドを選択し (5 通り)，その後，既定の順序通りに正解画像を選択する (20×19×18×17 通り) ことになる．したがって結果としては 581,400 通りとなる．

一方，提示案 1 で本提案を適用すると提示案 2 の計算における 1 段階目の選択数 5 通りが 22 通りに変化する．したがって結果としては 2,558,160 通りとなる．またこの場合，回答を順不同としても回答の取りうる数は 106,590 通りとなり，4 桁暗証番号による個人認証の 10 倍程度の安全性を持つこととなる．

3 Group & Photo Choice 認証

これまでの議論にもとづき実装した再認式画像認証 “Group & Photo Choice 認証”(G&PC 認証) について述べる．

3.1 秘密情報設定手順

G&PC 認証の秘密情報設定手順について説明する．

1) 利用者は **N** 枚の画像を準備する．これを認証システムに登録する．
2) 登録画像の中から秘密とする画像を **M** 枚設定する．この設定作業において，回答順序も指定する．

上記の変数 $\mathbf{N}$,$\mathbf{M}$ は，保護対象とするシステムが要求する安全性に応じて決定する．本論文では，以降 $(\mathbf{N}, \mathbf{M}) = (100, 4)$ として議論を進める．$\mathbf{N}$ を 4 とした理由は，4 桁暗証番号との比較を行うためである．回答候補数 $\mathbf{M}$ の数値について決定根拠はないが，枚数が多い方が望ましい状況において現実的に準備可能な画像枚数としてこの数値を選択した．

3.2 回答手順 (認証操作)

G&PC 認証における回答入力手順は以下の 2 ステップからなる (図 2(b) 参照)．

- 回答画像候補から画像群を絞り込む (Group choice)
- 絞り込まれた画像群から正解画像を選択する (Photo choice)

Step 1) 回答候補画像の絞り込み
G&PC 認証では，1 段階の回答として 100 枚の回答候補群から 20 枚の画像群に絞り込む．2.1 節で述べた 2 つの提示法について，回答方法を説明する．

提示法 1 では縦スクロール操作で画像群を閲覧し，画面内にすべての正解画像が表示される状態にして回答 (確定) する．提示法 2 では機器画面内に一度に表示可能な 5 つの画像グリッドをフリック操作により切り替えて閲覧する．正解画像が含まれる画像グリッドを探し出し，その画像グリッドの画面に表示した状態で回答 (確定) する．

なお両提示方法において画像グリッドを横 4 列とした理由は 2 つある．1 つは，正解画像 4 枚すべてを画像グリッド内の横一行内に配置可能にするためである．もう 1 つはスマートフォンや折りたたみ式携帯電話の写真閲覧アプリで多く用いられている表示列数であり，一般的にも妥当な数だと言えるからである．

Step 2) 正解画像の入力
Step 1 により回答候補画像は 20 枚に絞り込まれ，認証機器の画面内にすべて表示された状態となる．Step 2 での回答は 2 章で述べた `1Stage-mChoice-w/Order` 手法による回答と同じになる．つまり，絞り込まれた 20 枚の画像の中から正解画像 4 枚を既定の順序通りに選択することである．

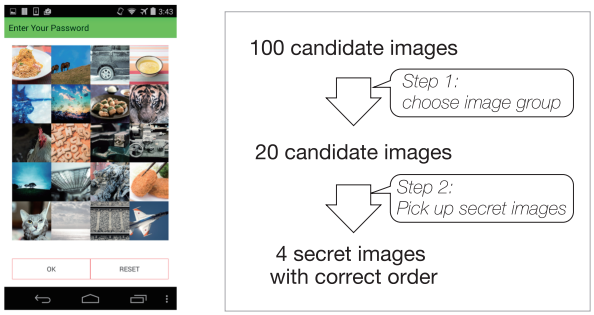

図 2: P&GC 認証のプロトタイプ画面と回答手順

4 評価

4.1 安全性評価

本節では G&PC 認証の安全性について考察する．なお認証手法における各種条件は 2.1 節冒頭での仮定と同一であるとする．提案手法の総当たり攻撃に対する安全性は，3.2 節で述べた Step 1 と Step 2 の回答選択可能数により決まる．そこで以降ではそれぞれの Step における総当たり攻撃への安全性について議論する．

まずはじめに Step 2 について考える．この Step では提示案にかかわらず 20 枚の画像から正解画像 4 枚を既定順序に従って回答することである．したがって安全性は，1/116,280 通りとなる (=1/20×1/19×1/18×1/17)．

次に Step 1 について考える．この Step では提示案 1, 2(2.1 節参照) によって回答可能数が異なる．まずはじめに提示案 2 について考える．提示案 2 では 100 枚の画像を 5 つの画像グリッドに分割している．したがって安全性はそれらの画像グリッドから 1 つを選択する行為になるため，1/5 となる．一方，提示案 1 では 100 枚の画像からなる 1 つ画像グリッドから 20 枚からなる画像グリッドを切り出す行為になる．この際，利用者の操作は縦スクロールなので，縦スクロールによる画像グリッドの切り出し可能数

が利用者の取りうる回答選択可能数となる．この数は 25 行のなかから連続した 5 行を選択することなので，その数は 21 となる．ただし，この数は正解画像の配置状況にも依存する．正解画像が 5 行にわたって分散配置されている場合スクロール位置の選択肢は 1 つだけである．しかしすべての正解画像が 1 行内に配置された場合，取りうるスクロール位置は 5 つとなる．正解画像の配置が nln 行に分散している場合，取りうるスクロール位置の数 ($numOfScrollPositions$) は以下の通りになる

$$\begin{aligned}
&\text{if } nln = 5 \text{ then } numOfScrollPositions = 1\\
&\text{if } nln = 4 \text{ then } numOfScrollPositions = 2\\
&\text{if } nln = 3 \text{ then } numOfScrollPositions = 3\\
&\text{if } nln = 2 \text{ then } numOfScrollPositions = 4\\
&\text{if } nln = 1 \text{ then } numOfScrollPositions = 5
\end{aligned}$$

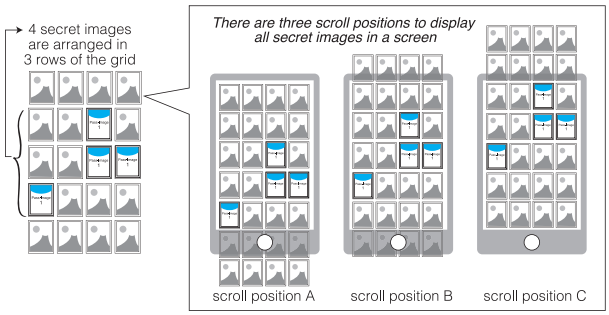

図 3: 正解画像の配置とスクロール位置の一例 (nls=3)

したがって提示案 1 における Step 1 の安全性は (worst case, best case) = (5/21, 1/21) の値域となる．これらの議論より，提案手法の総当たり攻撃に対する安全性は Step 1×Step 2 となることから以下のようになる．

表 1: GP&C 認証の安全性

画像提示条件	安全性
提示法 1 (Worst case)	1/488,360 (= 5/21 x 1/116,280)
提示法 1 (Bast case)	1/2,441,880 (= 1/21 x 1/116,280)
提示法 2	1/581,400 (= 1/5 x 1/116,280)

4.2 被験者による評価

被験者による提案手法の利用可能性と操作負担増に関する評価実験を実施した．なお以降の実験は，実験用端末として Android 端末である Nexus 5 (OS version 4.4.4) を用いて実施した．

4.2.1 利用可能性 (記憶保持)

提案手法では 4 枚の正解画像を順序付きで記憶保持する必要がある．この要件の実施可能性について被験者による評価実験を実施した．評価項目としては以下の 2 点とした．

1) システム提供画像とユーザ持ち込み画像による記憶保持能力に差が出るか?
2) 回答順序の決定時に「ストーリを作成して回答順序を決定せよ」とアドバイスすることで記憶保持能力に差が生まれるか?

著者らの仮説は「ユーザ選択画像で回答順序を自由に決定する方法が最も記憶保持が容易である」であった．

実験方法

20 枚 (=4 列 ×5 行) の画像群を実験端末の画面に表示し，被験者に順序付きで正解画像 4 枚を決定させた．この際の条件設定は表 2 の 2 条件とした．

表 2: 秘密情報設定における条件設定

条件名	画像種	順序決定の指示
mcond1	システム提供画像	ストーリ作成を指示
mcond2	ユーザ持ち込み画像	指示なし

被験者は 8 名で男女比は男性:女性=3:1，年齢は 20 歳代が 7 名，40 歳代が 1 名である．この被験者を 4 人づつ 2 分し，上記の 2 条件にランダムに割り当てて秘密情報を設定させた．なお実験に使用した画像群だが，mcond1 は著者が (食物，動物，建物，風景) の 4 カテゴリーからなる写真 20 枚を選択し実験させた．mcond2 の画像群は被験者に 20 枚の画像を持ち込むよう事前に指示し，その画像群を利用して秘密情報を設定させた．

実験は 14 日間にわたって実施した．0 日目に秘密情報を設定させ，その直後に 1 回目の認証実験を行った．そのあと 7 日後と 14 日後にそれぞれ認証実験を実施した．なお各回の認証実験では 6 回まで試行を認め，6 回までの試行で認証に成功しなかった場合「認証失敗」と判定した．測定値は認証成否 (2 値) と回答画像 (回答 4 画像と回答順序) である．これらの測定は実装したプロトタイプシステムを通じて実施した．

実験結果

表 3 は記憶保持の実験結果である．mcond1, mcond2 の両条件ともに 6 回までの試行で認証に成功しなかったケースが 1 回ずつ発生した．したがって認証成功率は両条件ともに 94.4%(= 17/18) となる．また成功はしたが 1 回の試行ではなく数回の試行の後に成功した事例が mcond1 で 1 件，mcond2 で 3 件あった．また誤回答の要因を調査した結果をまとめたものが表 4 である．

表 3: 記憶保持実験の実験結果

Subject name	mcond1 (system image)			mcond2 (user image)		
	0 day	*7 days*	*14 days*	*0 day*	*7 days*	*14 days*
Subject A	1	1	1	1	3 (image & order)	1
Subject B	1	1	1	1	1	1
Subject C	1	1	1	1	1	2 (image)
Subject D	1	2 (order)	1	1	1	1
Subject E	1	1	1	2 (image)	1	1
Subject F	1	failed (image & order)	1	1	failed (image & order)	1

表 4: 誤回答の要因調査

	mcond1	mcond2
正解画像誤り	2	5
回答順序誤り	1	0
双方誤り	4	5
誤回答合計	7	10

4.2.2 操作負荷

本研究では画像提示法として以下の提案をした．これらの設計による操作負担について被験者による評価実験を行った．

- 1 グリッド (提示法 1) or 複数グリッド (提示法 2)
- ランダム配置 or 特定領域に集中配置

著者らの仮説は「ランダム配置よりも集中配置，そして 1 グリッドよりも複数グリッドの方が操作負担は軽いと被験者は認識する」とした．

実験方法

この実験ではシステムが用意した 100 枚の画像を利用し，4 条件のシステムを用意して操作負担を比較した．用意した画像は Bing 画像検索でキーワード “image” で画像検索を行いヒットした画像の上位 100 件を用いた．秘密情報は 100 枚の画像から選択した 4 枚の画像とその回答順序である．

表 5: 操作負荷評価における個人認証システムの設定条件

システム名	画像Grid数	正解画像の配置	回答方法
S1	1	ランダム配置	直接回答
S2	1	集中配置 (被験者には非通知)	直接回答
S3	1	集中配置	2段階回答
S4	5	集中配置	2段階回答

比較した認証システムの 4 条件について説明する (表 5 参照)．画像グリッド数と正解画像の配置については 2.1 節で説明済みである．回答方法について説明する．G&PC 認証では回答を 2 段階にした (3.2 節参照)．これは表 5 における 2 段階回答を指すものであり，したがって S3 と S4 は G&PC 認証である．これに対し，設計上の選択肢として G&PC 認証の Step 1 を省略し，Step 2 による正解画像の直接回答による検証も可能である．それゆえ S1, S2 は比較対象として直接回答の条件とした．また S1 は正解画像の配置による比較のためランダム配置の条件とした．

被験者は 4 名で全員 20 歳代男性である．なお各被験者には 4 種の個人認証システムを 5 回認証成功するまで操作させた．実験は秘密情報を記憶した状態で実施し，秘密情報を忘れた場合

には秘密情報を再度記憶させた上で行った．4システムの実施順は被験者毎にランダムにしている．実験実施後，被験者に対してアンケートを実施し，認証に要した時間，正解画像探索の負担，システムの操作負担，フラストレーションの4項目について主観的評価を9段階で回答させた．また4つの提案システムと4桁暗証番号による個人認証の計5システムについて順位付けをすることを求めた．また認証時間をシステムを通じて計測した．

実験結果

まずはじめに対象4システムにおける認証時間を表6に示す．

表 6: 操作負担評価実験における認証操作時間

	S1	S2	S3	S4
平均 (sec)	16.5	11.0	11.6	8.1
最短値 (sec)	6.2	5.3	6.6	3.1
中央値 (sec)	12.1	9.3	10.1	7.7
最長値 (sec)	36.1	25.8	23.8	15.6
標準偏差 (sec)	8.99	5.61	4.46	3.50

次に評価対象4システムに対する被験者の主観的評価を表7に，評価対象4システムと4桁暗証番号認証の5種システムに対する順位付け結果を表8に示す．

5 考察

5.1 安全性について

G&PC認証の安全性については4.1節で述べた．2.1節冒頭の各種仮定を想定した場合，つまり正解画像は4枚で回答は順序付き，回答候補画像数は100枚で認証機器の画面には20枚の画像が一度に表示できるとした場合，総当たり攻撃への安全性は最悪の場合で1/488,360，最良の場合1/2,441,880となり4桁暗証番号による個人認証よりも安全性はおおよそ50〜240倍に改善される．この際，利用者が記憶することを要求される秘密情報は(正解画像4枚 + 回答順序)となる．これは既存の再認式画像認証における秘密情報の定義と同等であり，記憶負担だけ見れば安全性向上のために利用者に負担を追加するものではない．

表 7: 操作負担評価実験における被験者による主観的評価

	S1	S2	S3	S4
認証時間 (短い:1 - 9:長い)	7.25	3.25	5.25	4.75
探索負担 (軽い:1 - 9:重い)	7.25	3.50	3.00	1.75
操作負担 (軽い:1 - 9:重い)	3.50	2.25	3.25	3.25
Frustration (全く感じない:1 - 9:強く感じる)	4.00	1.75	3.50	3.00
合計	22.00	10.75	15.00	12.75

表 8: 評価4システムと暗証番号認証による使いやすさの順位付け

	1位	2位	3位	4位	5位	平均
S1	0	0	0	1	3	4.75
S2	0	2	1	1	0	2.75
S3	0	0	2	1	1	3.75
S4	1	1	1	1	0	2.50
PIN	3	1	0	0	0	1.25

またここで秘密情報から回答順序を除外した場合，正解回答が1通りから24通り (=4×3×2×1) に増えることから安全性は(最悪, 最良) = ($\frac{1}{20,348}$, $\frac{1}{101,745}$) となる．この結果から，回答順序を秘密情報から除外したとしても4桁暗証番号による個人認証と比較して，およそ2〜10倍の安全性があることになる．

5.2 操作負担について

記憶保持：利用画像種に関する2条件と回答順序へのアドバイスに関する2条件で構成される4条件のうち，2条件について被験者実験を実施した．認証成功率だけで見ると差はなく，7日間隔で2回認証を試みたがおよそ94%の認証成功率となった．被験者が少ないため，追実験は必要だが利用可能性は期待できるという結果となった．

また興味深いのは，表4の誤回答の要因である．実験結果から「正解画像は記憶しているが，回答順序は忘れた」という要因の誤回答は両条件ともに少ないこと，またユーザが持ち込んだ

画像での認証 (mcond2) では，正解画像を誤ることによる誤回答が多いという結果となった．

認証時間：表 3 の結果から，平均時間を見ると G&PC 認証 (S3,S4) は，S1 よりも短時間で認証が完了している．S3, S4 と S1 を比較すると最短値では S3 よりも S1 の方が早い結果となっているが，これはランダム配置によって偶然にも正解画像の探索が容易な配置になったと考えられる．また S2 と S3 を比較すると最長値を除いて S2 の方が S3 よりも時間が短いという結果となった．これは直接回答の方が 2 段階回答よりも回答の手間が少なくなることが影響したと考えられる．

操作負担：表 4, 5 から被験者が感じた主観的操作負担は，負担が重いと感じられた順に (S1⇒S3⇒ (S2, S4)) となった．S1 の負担が重いと感じられた理由はランダム配置によるもとの言える．S3 は S2 と比較して回答方法以外に差はないのだが，被験者による主観的評価は大きく分かれる結果となった．表 4 のスコアからは認証時間とフラストレーションにより影響が大きいことが見てとれる．S2 と S4 は甲乙つけがたい結果となった．S4 が他の 3 手法と異なる点は画像グリッド数であり，操作においてフリックにより画像閲覧を 5 画面見ることで行える点である．これは操作・探索負担を低減すると仮定していたのだが，被験者による主観的評価では S4 の探索負担は低いものの，操作負担は軽いと評価されなかった．

6 おわりに

本研究では再認式画像認証の安全性向上を目指しつつ，それにともなう負担増を抑制可能な新たな改良方法として，選択肢の母集団である回答候補画像の数を増やす手法の提案を行った．この手法の最大の利点は，利用者が記憶保持する秘密情報が既存の再認式画像認証と変わらないまま，安全性向上を可能にする点である．また回答候補画像の増加にともない発生する操作・探索負担を抑制するため，縦スクロールまたはフリック処理による多数画像の閲覧方法と画像表示グリッドの一部に正解画像を集中配置する方法を提案した．またこれらの提案手法に関する操作負担について被験者による評価実験を行った．

今後の課題としては，次の 3 点を検討している．1) より多くの被験者による操作負担評価の追実験実施，2) 秘密情報作成時の負荷など他に評価すべき負担についての考察と評価，3) 安全性と操作負担とのバランスについて考察．これらを今後進めていく予定である．

参考文献

[1] Suo, X., Zhu, Y., and Owen, G.S.: Graphical Passwords: A Survey, 21st Annual Computer Security Applications Conference(ACSAC), (2005). URL: https://www.acsac.org/2005/papers/89.pdf

[2] Renaud, K., Mayer, P., Volkamer, M., Maguire, J.: Are graphical authentication mechanisms as strong as passwords?, Computer Science and Information Systems(FedCSIS), pp.837-844, (2013).

[3] Takada, T., Koike, H.: ”Awase-E: Image-Based Authentication for Mobile Phones Using User’s Favorite Images, Human-Computer Interaction with Mobile Devices and Services(MobileHCI), pp.347-351, (2003).

[4] Watanabe, K., Higuchi, F., Inami, M., Igarashi, T.: CursorCamouflage: multiple dummy cursors as a defense against shoulder surfing, SIGGRAPH Asia 2012 Emerging Technologies, (2012).

[5] Wiese, O., Roth, V.: Pitfalls of Shoulder Surfing Studies, Workshop on Usable Security (USEC), (2015). URL: http://www.internetsociety.org/doc/pitfalls-shoulder-surfing-studies

[6] 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”，情報処理学会論文誌，Vol.44，No.8，pp.2002-2012, (2003).

[7] (株) ニーモニックセキュリティ：本人認証ソフト ニーモニックガード, (オンライン) 入手先 <http://www.mneme.co.jp/index_net.html> (参照 2015-08-24).