情報処理学会論文誌 Vol.57 No.12 2641–2653 (Dec. 2016)

秘密情報を変更せずに提供しうる安全性を柔軟に変更可能な再認式画像認証の提案

森 康洋[1,†1,a)] 高田 哲司[1,b)]

受付日 2016年3月10日, 採録日 2016年9月6日

概要：本研究では，秘密情報を変更することなく提供する安全性を変更可能な再認式画像認証を提案する．提案する画像認証方式では前記の特徴を実現するため以下の 2 つの工夫を施している．工夫 1）認証時の回答候補画像を増やす．工夫 2）システムにより規定される部分領域内に正解画像を集中配置する．手法 1 により秘密情報を変更することなく安全性向上を可能にし，手法 2 により安全性向上にともなう操作負担の増加を抑制可能にする．この提案に基づく画像認証の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，提案する認証方式の操作時間は 100 枚の回答候補画像から 4 枚の正解画像を選択するのに平均 15.2 秒という結果となり利用可能性に疑念がないこと，また正解画像の制約付き配置については操作負担増加を抑制しうる効果が確認された．

キーワード：個人認証，画像認証，再認式認証，安全性と利便性，リスクベース認証

Stretchable Image-grid Authentication: Additional Decoy Images and Conditional Layout of Answer Images Realize Secure Recognition-based Image Authentication

Yasuhiro Mori[1,†1,a)] Tetsuji Takada[1,b)]

Received: March 10, 2016, Accepted: September 6, 2016

Abstract: We propose two ideas to realize better security for a recognition-based image authentication: 1) adding more decoy images into an answer selection screen, 2) setting a condition for answer images layout. These ideas realize not only improving a security-level of the authentication scheme but also minimizing an additional load in a user operation. We implemented a prototype system based on the ideas and evaluated feasibility and operational load of the proposed system with subjects. From the result of the experiment, the conditional layout of answer images has an effect to suppress operational burden. Moreover, a user took sixteen seconds in average to pick up four answer images with an order from one hundred images.

Keywords: User authentication, Image-based authentication, Graphical password, Recognition-based image authentication, Security and Usability, Human-Factor, Risk-based authentication

1. はじめに

画像を秘密情報として扱う個人認証手法には大きく 3 つのカテゴリがある [1], [2].

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

個々のカテゴリにおけるシステム例としては，図画再生による手法は文献 [3], [4] が，手がかりつき想起による手法は文献 [11], [12], [13], [16] が，再認による手法は文献 [6], [7], [24], [30] などがあげられる．

これらの手法はどれも知識照合型個人認証であり，秘密

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[†1] 現在，民間企業勤務
Presently with Private Company
[a)] m1110146@mail.uec.jp
[b)] zetaka@computer.org

情報の記憶負担軽減のため画像を応用した手法である．これら 3 手法の中でも再認による画像認証は，記憶負担の軽減効果が最も期待できる手法だと考えられている．その理由は，回答入力時に回答候補画像が利用者に提示されるため，提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といわれている．

- 視覚記憶の優位性
- 忘れかけていた秘密を思い返す可能性（Déjà Vu 効果）

この特性を個人認証の改良に活用する方法は 2 つある．1 つめの方法は，この特性を素直に活用し，既存の個人認証と同程度の安全性を提供しつつ，秘密情報の記憶負担を軽減する方法である．文献 [8], [24] で提案されているシステムは，このアプローチに基づく事例であると考える．もう 1 つの方法は，既存の個人認証と同程度の記憶負担で，より安全性の高い個人認証を実現する方法である．画像を秘密として利用することにより記憶負担の軽減が期待できる．つまり既存の個人認証と同程度の記憶負担を維持する方針のもとに画像を秘密情報とした個人認証を設計すれば，結果として秘密情報量を増やすことが可能になる．これにより個人認証の安全性改善を実現する方法である．

しかし安全性向上を目指す後者の方法は，3 つの問題があると考える．1 つは，人間が秘密情報を保持するため追加可能な秘密情報量には上限がある点である．秘密情報の情報量が増えるに従い記憶負担が増すことは避けられず，現実的に可能な安全性向上には限界がある．2 つめの問題は，既存の個人認証と同等程度の記憶負担を実現するには慎重なシステム設計が必要となる点である．数字列や文字列と複数枚の画像の記憶負担をどう評価して同等な記憶負担と見なすかには議論が必要である．最後の問題は，理論上は既存の認証手法と同等程度の記憶負担として慎重に設計したとしても，利用者が実際に受ける印象や実質的な負担増加は理論と異なる可能性があるという点である．

そこで本研究では，再認式画像認証の利点である記憶負担軽減効果をなるべく損なうことなく安全性を向上しうる別の方法を提案する．その提案内容は，以下の 2 つである．

- 安全性向上を目的として，回答候補画像を増やす方法を採用する．その一方で秘密情報自体は既存の画像認証と同等程度にする．
- 操作負担の増加抑制を目的として，正解画像をシステムで規定する領域内に配置する．また既存の画像閲覧アプリにおける設計要素を流用する．

つまり「秘密情報には変更を加えず，正解ではない回答候補となる “おとり画像” の数を増やす」方法で再認式画像認証の安全性改善を試みる．ただし，このアプローチでは操作負担が増加する．この負担増加を抑制する方法として正解となる画像の配置方法を工夫する，という手法の提案となる．この提案に基づき，スマートフォン上で動作するプロトタイプシステムを実装して，利用可能性と操作負担の増加抑制に関する評価実験を実施した．

以降本論文では，2 章で再認式画像認証方式における安全性改善へ向けた提案内容について説明し，3 章では携帯端末向けに実装したプロトタイプについて述べる．4 章では．実装したプロトタイプシステムによる被験者実験について実験方法とその結果を述べ，5 章では提案手法の安全性と利用可能性・操作負担の増加抑制について議論する．

2. 回答候補画像の追加による安全性改善

本研究では再認式画像認証をベースとし，秘密情報の記憶負担を増やさずに回答候補画像数を増やすことで画像認証の安全性を改善しうる方法を提案する．本章では，この提案方法と設計理由について説明する．なお以降では，スマートフォンなど携帯端末による個人認証を前提として話を進める．理由は 2 つある．1 つめは改善の余地があるためである．スマートフォン向けの個人認証手法は限られており，個人認証の利用率も低い [14], [15]．このことから改善の余地があると考えるためである．もう 1 つは，機器制約が大きいためである．画面サイズや入力手法など機器による制約があるため，そういった状況下でも必要最小限の負担で実行できる個人認証手法が必要であると考えるためである．

個人認証が提供する安全性を向上させる方法の 1 つに秘密情報の情報量を増やす方法がある．暗証番号を 4 桁から 6 桁にする，パスワードを「8 文字以上」から「15 文字以上で数字を必ず含める」ように変更する，などはその一例である．しかしこのアプローチは，安全性向上のため記憶保持・回答操作の負担を利用者に強いる方法でもある．しかし，現実を省みると利用者の多くはすでに多くのサービスを利用しており，そのそれぞれで個人認証が必要とされる状況にある．つまり，個人認証を行うための秘密情報をあらたに記憶するだけの余裕がない状況にある [33]．したがって，可能であれば記憶負担を増やさずに安全性向上が実現できる方法が望ましい．

そこで本論文では「n_{all} 枚の画像を利用者に一度に提示し，その中から既定の正解画像 m_{all} 枚を既定の順番どおりに選択する」手法をベースとし，以下の 2 つの特徴を備える再認式画像認証を提案する．

- 安全性改善を目的として，回答候補画像数 n_{all} を増やせる手法とする．
- 操作・認知負担軽減を目的として，正解画像を回答候補画像群で構成される格子状領域の部分領域内に配置する．

以降では，上記 2 点の提案内容について説明する．

2.1 回答候補画像数の追加による安全性改善

再認式画像認証の仕組みを文章化すると，次のとおりとなる：「画像 n 枚からなる回答選択画面の中から m 枚の正

解画像を選択する．この行為を p 回繰り返し，選択した画像が既定の秘密画像と同一であれば認証成功とする」．これに加えて，1 回の回答選択画面で選択する正解画像枚数 m が複数枚（$m > 1$）である場合，正解画像の回答順序が検証対象の秘密情報か否かも設計要素（q）となる．したがって（n，m，p，q）の 4 つの設計要素があることになる．

ここで既存の再認式画像認証手法を調査すると，その多くは以下にあげた 5 手法のうち，手法 (a)，(b)，(c) の 3 手法に分類される．

手法 (a)：$(m, p) =$ (1 枚, 複数回)
手法 (b)：$(m, p, q) =$ (複数枚, 1 回, 順序なし)
手法 (c)：$(m, p, q) =$ (複数枚, 1 回, 順序あり)
手法 (d)：$(m, p) =$ (1 枚, 1 回)
手法 (e)：$(m, p, q) =$ (複数枚, 複数回, 順序あり or なし)

手法 (a) の代表例としては PassFaces [30] や Awase-E [8]，手法 (b) の代表例は，Déjà Vu [6]，手法 (c) の代表例は，ニーモニックガード [31] があげられる．なお LockTile [32] は設定次第で手法 (b)，(c) のどちらでも利用可能である．一方，手法 (d) や (e) に基づく提案は著者の知る範囲において見受けられない．手法 (d) による手法が提案されていない理由は，回答操作負担を増やすことなく安全性を確保することが困難なためであり，手法 (e) による手法が提案されていない理由は，設計方法にも依存するが，手法 (a)，(b)，(c) と比較しても安全性の劣化，回答方法の困難化，記憶負担の増加が懸念されるためであると考える．

上記の手法分類で利用されている 3 つの設計要素（m，p，q）は，すべて秘密情報を規定する要素である．利用者が記憶すべき正解画像数 m_{all} は，$m_{all} = m \times p$ となり，また回答順序 q も検証対象であれば秘密情報となるからである．したがって，これらの数値を増やすことは記憶負担の増加につながる懸念があり，望ましいアプローチとはいいがたい．したがって値を変更して安全性改善について探求可能なのは，回答選択画面に提示される画像数 n だけとなる．本研究で安全性改善のアプローチとして回答候補画像を増やす手法を採用している理由はこれゆえである．

なお本アプローチは再認式画像認証との親和性が高く，一方で暗証番号やパスワードなど，記号情報による秘密情報を用いた個人認証では困難なアプローチであると考える．再認式画像認証は，画像そのものが秘密情報であり回答候補情報となる．したがって回答候補数を増やすことは容易である．しかし暗証番号やパスワードでは，回答候補数を増やすことに限界がある．暗証番号における回答候補数は数字の 10 種類のみであり，番号という前提をくずさずにこの種類数を増やすことはできない，パスワードも同様のことがいえる．仮に利用可能な文字種を「アルファベット大文字・小文字と数字」と仮定した場合 62 種類となり，これを増やすとしても増やせる数には限界がある．日本語の場合，平仮名や片仮名，漢字を許容することによりその種類数を増やすことは可能だが，入力方法の問題や言葉への慣れの問題など，日本語に習熟していないユーザの利用が困難になるという問題が発生する．よって，暗証番号やパスワードなど記号に基づく秘密情報を用いた個人認証では限界があり，再認式画像認証にとって親和性の高いアプローチであるといえる．

次に，いくつか存在する再認式画像認証手法の中で「n_{all} 枚の画像を利用者に一度に提示し，その中から既定の正解画像 m_{all} 枚を既定の順番どおりに選択する」手法，すなわち手法 (c) をベースとして選択した理由について述べる．なお文中の n_{all}，m_{all} を前述の手法定義の設計要素を用いて表すと以下のとおりとなる．

- $n_{all} = n \times p$
- $m_{all} = m \times p$

ここで（n_{all}，m_{all}）を同条件とした場合の手法 (a)，(b) の安全性について検討する．なおこの前提条件では手法 (c) は手法 (b) と同じ評価になることに注意されたい．ここで仮に $n_{all} = 100$，$m_{all} = 4$ と仮定して考えると，手法 (a) と手法 (b) では以下の設計条件になる．

- 手法 (a) による手法：(n, m, p)=(25 枚, 1 枚, 4 回)
- 手法 (b) による手法：(n, m, p)=(100 枚, 4 枚, 1 回)

すると，各手法によって提供される安全性は次のようになる

- 手法 (a) による安全性：
  $1/390,625 = (1/25)^4$
- 手法 (b) による安全性：
  $1/94,109,400 = (1/100 \times 1/99 \times 1/98 \times 1/97)$

この結果から，手法 (b) または (c) をベースにすべきであることが分かる．最後に回答順序 (q) であるが，安全性改善という点では回答順序ありが望ましいことは明らかである．なお回答順序なしの条件よりも記憶負担が高くなる懸念があるが，暗証番号やパスワードも数字や文字を既定の順番どおりに回答する手法であり，理屈上は既存の秘密情報と同様の条件であるといえる．したがって「回答順序あり」条件の採用が既存の個人認証と比較して著しく記憶負担を増やす方法とはいいがたいと見なし，本論文では $q =$「回答順序あり」として議論を進めていく．これらの理由から，我々は安全性改善手法のベース手法として手法 (c) を選択した．

しかしながら，回答候補画像を増やすアプローチは回答時における利用者の負担が増加する．回答選択画面の画像数が増えることにより，従来よりも多くの画像群の中から正解画像を見つけだし，回答操作を行う必要があるためであり，操作負担と認知負担が増えると予想される．さらにこの負担は回答候補画像数の増加に比例して増えることも予想される．そこで次節では，この負担増加を抑制するための提案について説明する．

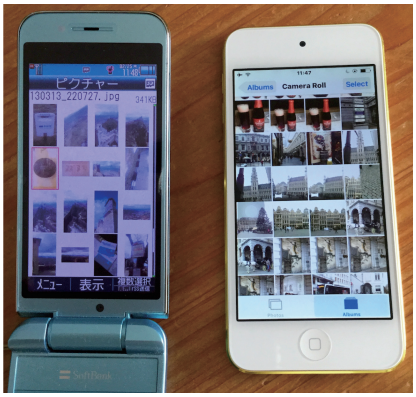

図 1 画像 4 列表示の例：3 G mobile phone/iPod touch (5th gen.)
Fig. 1 Example of 4 column picture display: 3 G mobile phone/Apple iPod touch (5th gen.).

2.2 正解画像の配置による認知・操作負担の抑制

本節では認知・操作負担軽減を目的とした正解画像の配置方法について，まず回答候補画像群の提示方法を説明し，次に正解画像をどのように配置することで認知・操作負担の増加を抑制するのかを説明する．

まずはじめに回答候補画像群の提示方法であるが，本研究では携帯電話での写真閲覧（アルバム）アプリの手法をそのまま流用する．つまり，多数の画像を縦長のグリッド配置として利用者に提示する．これは縦方向のスクロール操作のみで多数の画像を閲覧可能にするため，操作方法の単純化による負担軽減にも寄与すると考える．また携帯電話の利用者はこの操作方法に慣れ親しんでおり，画像閲覧行為において新たな操作方法に対する学習負担を利用者に課さない方法でもある．

また本研究では画像グリッドにおける 1 行の画像数を 4 枚とした．この数は，機器の画面サイズが比較的小さい第 3 世代携帯電話や Apple 社の iPod touch における写真閲覧アプリが，1 行に 4 枚の写真を提示している事例があり，それを踏襲したものである（**図 1**）．画像サイズは認知負担と操作負担に関係する．画像サイズを小さくすると多くの画像を一定領域の中に表示できるため画像閲覧のための操作は少なくなり負担は減るが，個々の画像の内容把握が困難になるため認知負担は増えると考える．しかし回答候補画像数を増やすという仮定のもとで画像サイズを小さくすると正解画像の探索を困難にすると考える．これは結果として正解画像を見つけにくくし，回答候補画像群を何度も閲覧する必要が生じることから操作負担も増えることになると推測する．したがって，既存の写真閲覧アプリと同等の画像サイズという設計とした．既存の仕組みと同等の仕組みを流用することにより，利用者に対する操作負担・認知負担を不用意に増やさないような配慮をしている．

次に正解画像の配置方法について説明する．

安全性の観点から考えれば，画像グリッド内に正解画像をランダムに配置する方法が望ましい（**図 2** 左）．しかし，

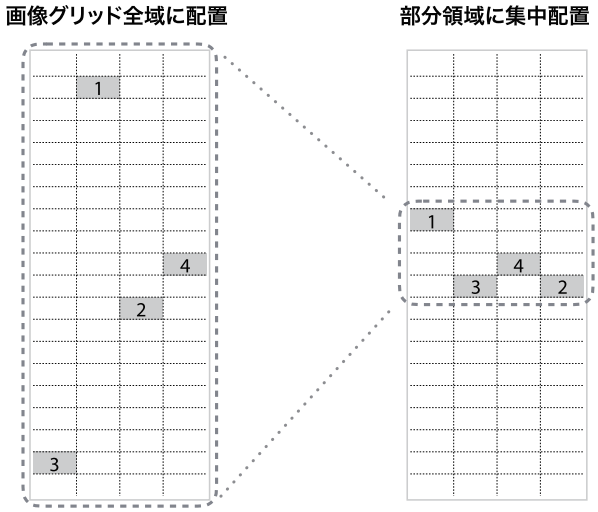

図 2 正解画像の配置法：全領域への配置と特定領域への集中配置
Fig. 2 Answer Image Layout: an entire region and a certain sub region.

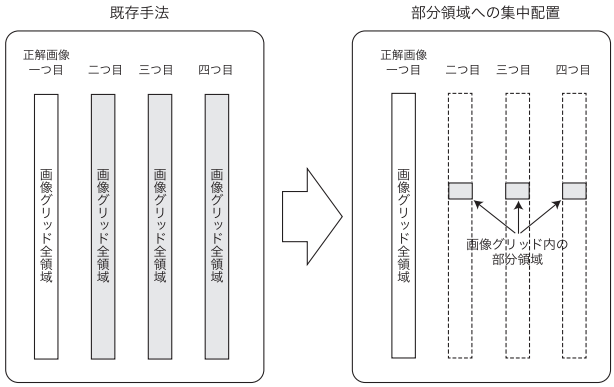

図 3 正解画像の探索領域の違い
Fig. 3 Difference of Search Area between two Answer Image Layouts.

利用者の視点から考えると，画像グリッド内から正解画像を既定の回答順番どおりに 1 つずつ探し出す作業が必要となり，正解画像の探索負荷が高くなるため望ましいとはいいがたい．また回答候補画像数が増えるに従い探索空間も拡大するため，安全性改善にともない利便性が低下するという望ましくない結果を招くことにもなる．

そこで我々は「画像グリッド内の一部である部分領域にすべての正解画像を集中配置する」方法を提案する（図 2 右）．この配置方法の利点は，正解画像を 1 つ見つけられれば他の正解画像を容易に発見可能にする点にある．正解画像を 1 つ見つけられれば，それ以外の正解画像はその周辺に存在するからである．言い換えると，この提案は正解画像の探索空間を縮小することでもある．これについて**図 3** を用いて説明する．仮に正解画像を 4 枚とすると，ランダム配置と集中配置における正解画像探索操作と探索領域は以下のようになる．

- ランダム配置：
  「画像グリッド全体」からの正解画像探索を 4 回（図 3

左）
- 集中配置：
  「画像グリッド全体」からの正解画像探索を 1 回と「部分領域」からの正解画像探索を 3 回（図 3 右）

ランダム配置の場合，各正解画像に対する探索空間は画像グリッド全体になる．一方，集中配置の場合は 2 つめ以降の正解画像は 1 つめの正解画像が見つかった場所の「周辺」に限定される．つまり 2 つめ以降の正解画像の探索領域が縮小され，画像グリッド全体を再度探索する必要がなくなるため，その探索負担は抑制されることとなる．

またこれらの配置手法における負担と画像グリッドの大きさとの関係に注目すると以下のようになる．
- ランダム配置：
  画像グリッドが大きくなるに従い探索負担も増加する．
- 集中配置：
  画像グリッドの大きさに影響を受けるのは 1 回目の正解画像探索のみ．2 つめ以降の正解画像探索は画像グリッドの大きさとは無関係．

よって集中配置手法における探索負担は，画像グリッドのサイズに依存しにくい仕組みであるといえる．回答候補画像を増やしたとしても，それに比例して探索負担が増えるのは「1 回目」の正解画像探索だけである．またここで注意してほしいのは「1 回目」の探索であり「1 つめの正解画像探索」ではない．つまり複数枚ある正解画像のいずれか 1 つを発見できれば，他の正解画像も周囲にあることになるため，その瞬間から探索領域は狭まることになる．したがって，2 回目以降の正解画像探索は画像グリッドの大きさには依存せず，最大でも部分領域の 2 倍程度の領域に限定される．したがって回答候補画像の増加による安全性改善が利便性低下に直結する仕組みではないと考える．

次に正解画像を配置する部分領域について説明する．部分領域は縦長画像グリッドの部分領域とし，本研究では認証機器の画面内に一度に収まる矩形領域と定義する．つまり部分領域は，認証機器の画面内に一度に表示可能な範囲となる．また縦スクロールのみによる画像閲覧操作を維持するため，部分領域の定義は縦方向の行数のみが可変値とする．1 行 4 列の画像グリッドのもと，4 列配置に基づく画像サイズを保持しつつ，認証機器の画面サイズに応じて適切な行数を決定する．これにより，すべての正解画像は認証機器の画面内に必ず表示されることとなる．これにより正解画像の探索を支援，すなわち認知負担の増加を抑制する．また正解画像を選択する際に画像グリッドをスクロールさせずにすべての正解画像を選択できるため，回答操作における操作負担の増加も抑制できる．

最後に，正解画像の配置方法におけるランダム性について述べる．提案手法では，配置方法に起因する安全性低下の懸念に対して，ランダム性を持たせることで安全性を確保する．提案手法では，回答画面構築の処理において以下の 2 つのランダム性が含まれる．

1) 画像グリッドから部分領域をランダムに決定する．
2) 正解画像を部分領域内にランダムに配置する．

これらのランダム性により，ある事象からすべての正解画像を特定しうるような逆変換や攻撃手法は成立しないと考えている．

なお正解画像の配置領域が部分領域に限定されることで可能となる攻撃手法に “Intersection 攻撃” がある．この攻撃方法は，認証時に提示された画像グリッドから部分領域として切り出し可能なすべての画像集合を対象に，同一領域内に配置された画像ペアを抽出し，記録・集積していく．もし認証試行のたびに画像グリッドの配置が変更されると仮定すると，認証試行を複数回繰り返して画像グリッドの配置を複数パターン取得し，そのそれぞれから画像ペアの抽出を行ってそれらの積集合をとることで，正解画像が特定可能になる．ただし，この方法により特定可能になるのは正解画像の集合だけであり，回答順序は不明なままとなる．したがって，攻撃者による “なりすまし” が正解画像特定後にすぐに成功するわけではない．しかし回答順序により確保可能な “場合の数” は少ないため，“Intersection 攻撃” を困難にするための対策は必要である．この対策の 1 つとしては，回答画面の画像配置は 1 度決定したら一定の期間が経過するまでは変更しない，といった仕組みが考えられる．

3. プロトタイプシステム

これまでの議論に基づく再認式画像認証 “Stretchable Image-Grid Authentication”（S-IGA）を Android アプリケーションとして実装した．本章では，このプロトタイプシステムについて説明する．

3.1 認証画面の構築

認証画面の構築，すなわち認証回答時に利用者に提示する画像グリッドの画像配置方法は 2.2 節での議論に基づき，以下の手順で行う．

Step 1） 画像グリッドから部分領域をランダムに決定する．

Step 2） **Step 1** で決定した部分領域内に正解画像をランダムに配置する．

Step 3） **Step 2** で配置されていない領域に “おとり画像” を配置する．

なお “おとり画像” とは正解画像ではない画像を意味する．また，S-IGA の基本条件を以下のとおり定義した．以降の議論ではこれらの条件を前提として議論を行う．
- 回答候補画像の総数（$=n_{all}$）：100 枚
- 正解画像の数（$=m_{all}$）：4 枚
- 部分領域：5 行 × 4 列の画像グリッド

n_{all} を 100 枚にした理由は 2 つある．1 つは著者らの知

る範囲において 3 桁枚数の回答候補画像による再認式画像認証の提案は存在せず，この条件における操作負担を検証することは 1 つの有用な目安を提供することになると考えるからである．もう 1 つの理由は，3 桁数値における最小値であり，仮に回答候補画像を利用者に用意してもらうとした場合でも実行不可能な数ではないと考えたためである．

m_{all} を 4 枚とした理由は，提案されている画像認証システムのいくつかが正解画像の枚数を 4 枚としており，また 4 桁暗証番号との比較も可能となるためこの条件とした．なお本研究では携帯端末として Nexus 5X [34] を利用した．この機器の画面サイズに適した部分領域として，1 行 4 列に基づく画像サイズを維持したうえで表示可能な行数として，今回は 5 行という条件設定を行った．

3.2 利用方法

次にプロトタイプシステムにおける利用方法について説明する．

秘密情報の登録手順

S-IGA における秘密情報登録は以下の手順で行う．

- **N** 枚の画像を準備する．これを S-IGA システムに登録する．
- 登録画像から秘密情報とする画像を **M** 枚（ただし **M**<**N**）選択する．また回答順序も同時に指定する．

上記の変数 **M**，**N** 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されるものである．本プロトタイプシステムでは前述のとおり $(\mathbf{M}, \mathbf{N}) = (4, 100)$ とした．

回答操作手順

S-IGA における回答操作は「部分領域選択」と「正解画像の選択」からなる 2 段階の回答手順となっている．

(1) 部分領域選択：

S-IGA では 1 段階目の回答として（25 行 × 4 列）の画像グリッドから（5 行 × 4 列）の部分領域を選択する（**図 4** 左）．これは回答候補画像を 100 枚から 20 枚に絞り込むことに相当する．プロトタイプシステムでは機器画面内に表示される画像グリッドと部分領域の大きさは同一となっているため，直感的に部分領域の選択が可能となっている．なお利用者が選択すべき部分領域とは，すべての正解画像が含まれている部分領域である．ユーザは画像グリッドを上下にスクロールし，すべての正解画像が機器画面内に表示された状態にしてから画面下の OK ボタンを押下する．この操作により部分領域の選択が完了となる．

(2) 正解画像の選択：

前述の操作により，回答候補画像は 100 枚から機器画面内に表示されている 20 枚に絞り込まれた状態になっている．正解画像の選択は，既存の回答順序付き再認式画像認証（2.1 節の手法 (c)）と同様，この 20 枚の画像群から正解画像を既定の回答順序に従って選択し，最後に回答確定のため OK ボタンを押下する（図 4 右）．この操作により回答情報が認証システム側に送付され，秘密情報と同一値か検証される．回答された画像群と回答順序が既定の秘密情報と同一値であれば認証成功となる．

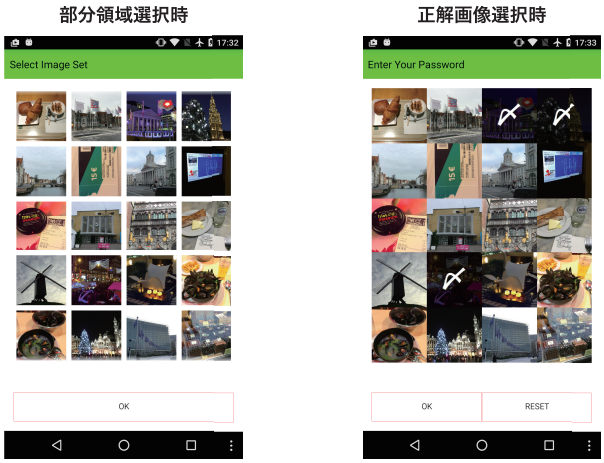

図 4 プロトタイプシステムの画面例
Fig. 4 Screen snapshots of the prototype system.

4. 被験者による評価実験

S-IGA の利用可能性と回答操作時における認知・操作負担増の抑制を検証するため，被験者による評価実験を行った．本章では評価実験の内容と結果について述べる．

4.1 実験目的

本評価実験の目的は，部分領域への集中配置により回答操作の負担が抑制されること，また現実的に利用可能性があることを示すことである．この目的のため，本実験では 4 つの設計条件による認証システムを用いて比較実験を行った．4 つの条件を**表 1** に示す．

各設計条件について説明する．表内の T3 条件が 3 章で述べてきた S-IGA の条件になる．また正解画像の配置を画像グリッド内の全領域内でランダムに配置する手法が T1 条件である．T2 条件は T1 条件と正解画像の配置方法が異なる手法であり，T4 条件は T3 条件と回答候補画像の閲覧方法が異なる手法となっている．正解画像の配置領域に関する条件はすでに 2.2 節で説明済みである．回答方法では，

表 1 被験者実験に用いた実験システムの設計条件
Table 1 System configurations for experiment systems.

条件	回答画像枚数	正解画像配置領域	スクロール方法	回答方法
T1	100	全領域	連続	直接回答
T2	100	部分領域	連続	直接回答
T3	100	部分領域	連続	二段階回答
T4	100	部分領域	ページ送り	二段階回答

すでに述べた 2 段階回答のほかに部分領域の選択を必要としない直接回答条件を用意し，スクロール方法では画像グリッドが 1 行ずつ連続スクロールする方法のほかに，部分領域をページとする単位で離散的にスクロールする離散的スクロールの条件を用意し比較評価を行った．つまり今回の条件では 25×4 の画像グリッドを 5 ページ分の 5×4 の画像グリッドに分割し，ページ単位でスクロールする方法で画像群の閲覧が可能なシステムで評価を実施した．T4 条件は T3 条件との比較で「離散的スクロール」の効果を見るため，T2 条件は部分領域への集中配置について T1 条件との比較で効果を見るために設けたものである．

4.2 実験方法

前節で述べた 4 条件によるプロトタイプシステムを実装し，被験者による評価実験を行った．被験者は 9 名，全員が大学研究室所属の学生で 20 歳代男性である．また被験者全員がスマートフォンの利用者で，かつ画像グリッド表示による写真閲覧アプリの利用経験者であった．なお実験では Android 端末として Nexus 5X（画面サイズは 5.2 インチ，解像度は 1,920 × 1,080 pixels）[34] を使用した．

なお本実験で使用した画像群は，著者所有の旅行時の写真 100 枚である．これらの画像をシステムに事前に登録し，システム側から画像を提供する形で実験を実施した．これらの写真は風景画や食べ物の写真が主であり，被験者に関係のある人物や被験者の所属組織などに関する写真は 1 枚も含まれていないことをここに一言添えておく．

実験手順は以下のとおりである．

1) 事前説明：実験手順と各認証方法の操作について事前説明を行い，秘密情報の設定を行った．

なお事前説明における実験システムの説明であるが，回答方法とスクロール方法は認証操作を行ううえで必要不可欠であるため，各被験者に事前説明した．一方，正解画像の配置方法については事前説明を行わずに実験を行った．つまり T3，T4 システムについては，2 段階回答であることから正解画像が部分領域に集中配置されることが自明である．一方，T1，T2 における正解画像の配置方法は被験者が知らない状態で実験を実施した．

2) 操作実験：プロトタイプシステムを用いて認証操作を実施させた．被験者への操作依頼内容は，各設定の認証手法ごとに「認証に 7 回成功するまで認証操作を繰り返して下さい」とした．実験結果はプロトタイプシステムを通じて計測しており，計測値は（操作時間，認証成否，回答情報）の 3 情報である．なお各認証手法の実験実施順はランダム化したうえで被験者に割り当てて実施させた．

3) アンケート調査：操作実験終了後に認証手法に関する主観評価をヒアリングする目的でアンケート調査を行った．アンケートでは正解画像探索，回答操作，認証時間，フラストレーションの 4 項目について 7 段階スケールによる回答を依頼した．各項目における値の割当ては，数値が小さい方が肯定的，大きい方が否定的となっている．つまり，フラストレーションの評価項目を例にとると，フラストレーションがきわめて小さい場合が評価値 1 で，フラストレーションがきわめて大きい場合が評価値 7 としている．

またあわせて，4 種の認証手法のどれかを暗証番号認証の代替として利用しなければならない，という状況を想定した場合にどの設計条件による認証手法を希望するかについて同着なしの条件で順位付けすることも行わせた．

表 2 各システム条件における認証操作時間
Table 2 Authentication time in four system configurations.

	T1	T2	T3	T4
平均 (sec)	28.04	14.64	15.19	10.44
標準偏差 (sec)	16.62	10.44	5.53	3.94
最長値 (sec)	82.81	62.52	30.77	20.63
中央値 (sec)	23.25	11.68	13.64	10.51
最短値 (sec)	7.80	5.12	7.76	3.96

表 3 各実験システムに対する主観評価
Table 3 Subjective evaluation of the operation in four auth. schemes.

	T1	T2	T3	T4
探索負荷	6.33	3.56	3.89	1.67
操作負荷	4.67	2.33	4.00	2.33
認証時間	6.33	3.67	4.56	2.11
Frustration	5.89	3.44	4.78	2.22

表 4 代替認証手法としての利用希望ランキング
Table 4 Ranking of alternative authentication schemes instead of using PIN authentication.

	T1	T2	T3	T4
1 位	0	1	1	7
2 位	1	3	4	1
3 位	1	5	3	0
4 位	7	0	1	1

4.3 実験結果

まずはじめに操作時間の結果を**表 2** に示す．

結果から，T1 条件を除く 3 つのシステム条件では認証操作にかかる平均時間が 16 秒未満となった．また認証操作時間が最も短いのは T4 条件となった．なお被験者実験を通じて，合計で 252 回[*1]の認証試行を被験者に実施させたが認証に失敗する事象は 1 回も発生しなかった．

次にアンケート結果について紹介する．**表 3** に 7 段階スケールで主観的印象を評価した 4 項目の評価結果を示す．

最後に，携帯端末において暗証番号認証の代替として利用する場合，どのシステム設定による認証手法を希望するかに関する順位付け結果を**表 4** に示す．表 4 内の数字は

[*1] 4 種のシステム条件 × 7 回の試行 × 9 名の被験者

各手法を各順位に評価した被験者の人数を示している．

またこれらの実験結果から，正解画像の配置方法の差異に関して T1 と T2 条件を比較すると，T2 条件の認証時間は T1 条件のおよそ 1/2 となり，主観的評価も集中配置による方法のほうが全評価項目で T1 条件よりも負担が低いという結果になった．また画像グリッドのスクロール条件に関する差異について T3 と T4 条件を比較すると，T4 条件の認証時間は T3 条件のおよそ 2/3 となり，また主観的評価も T4 の方が T3 よりも全般的に負担が低く，特に T4 条件の探索負荷は T3 条件の半分以下という結果になった．

5. 考察

5.1 S-IGA による安全性改善について

提案する再認式画像認証 S-IGA の理論的安全性，つまりランダムに入力された回答が偶然正解となる確率（= 総当たり攻撃への安全性）について議論する．なお本節では 3 章での議論に基づく各種条件を前提に議論を進める．以下にその条件を再掲する．

- 正解画像の配置方法：集中配置
- スクロール方法：連続スクロール
- 回答方法：2 段階回答
- 回答候補画像数：100 枚
- 秘密情報：画像 4 枚+回答順序
- 画像提示領域：25 行 × 4 列の画像グリッド
- 部分領域：5 行 × 4 列の画像グリッド

S-IGA の安全性は 3.2 節の議論から 2 段階回答の各段階における選択肢数（= 場合の数）の積に依存する．つまり「部分領域選択」の選択肢数と「正解画像の選択」の選択肢数の積が認証手法としての安全性の分母になる．よって本節では，各回答段階の選択肢数を明らかにし，最後に認証手法としての安全性を明らかにする．

まずはじめに「部分領域選択」における選択肢数について検討する．この段階における場合の数は，25 行 ×4 列の画像グリッドから 5 行 ×4 列の領域を取り出す方法が何通りあるかに帰着する．S-IGA では画像グリッドと部分領域の列数が同一であることから縦スクロールしかしないため，単純に考えればこの数は 21 通りとなる．ただし，この数は正解画像が 5 行にわたって配置された場合の値であり，正解画像がそれよりも少ない行数内に配置された場合には，部分領域の決定方法が複数存在することになる．これについて図を用いて説明する．

図 5 の例では，部分領域 5 行のうちの 3 行に正解画像が配置された例を示している．この場合，図からも分かるとおり，すべての正解画像が表示されるように部分領域を決定する方法は 3 通りある．つまり部分領域の中に正解画像すべてを含める方法は複数あるのである．これを正解画像の配置状況に応じて整理すると以下のとおりになる．

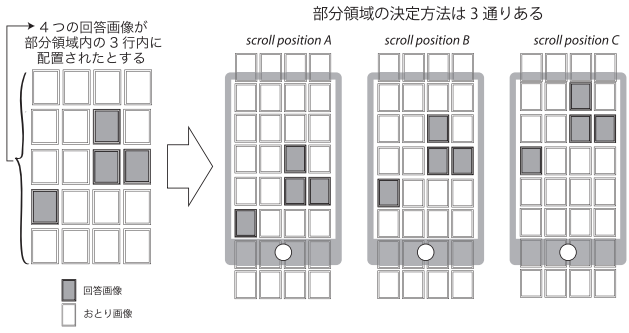

図 5 正解画像の配置状況と領域選択の関係

Fig. 5 Relation between an image grid extraction and answer image layout.

正解画像の配置行数 1 行 $\Longrightarrow$ 領域選択の方法 5 通り
正解画像の配置行数 2 行 $\Longrightarrow$ 領域選択の方法 4 通り
正解画像の配置行数 3 行 $\Longrightarrow$ 領域選択の方法 3 通り
正解画像の配置行数 4 行 $\Longrightarrow$ 領域選択の方法 2 通り
正解画像の配置行数 5 行 $\Longrightarrow$ 領域選択の方法 1 通り

よって，これが「部分領域選択」における選択肢数となり，その値は正解画像の配置状況に依存する．ここまでの議論をふまえたうえでこの段階における安全性を確率として表すと，分母は 21 となることから，上記の 5 状況に応じて（$\frac{5}{21}$，$\frac{4}{21}$，$\frac{3}{21}$，$\frac{2}{21}$，$\frac{1}{21}$）の値となる．

なお上記の計算は「連続スクロール」条件での計算である．離散的スクロールの場合の部分領域の選択肢数はページ数と等しくなり，4.2 節で議論した T4 条件の場合の選択肢数は 5 となる．つまり，部分領域の選択段階における安全性は，画像グリッドの全体サイズと部分領域のサイズの関係，ならびに正解画像の配置行数とスクロール方法に依存するといえる．

次に「正解画像の選択」段階における選択肢数について考察する．この回答段階における操作は，部分領域選択により決定された 20 枚の画像群の中から正解画像を既定の回答順に選択することである．したがって 20 枚から 1 枚，19 枚から 1 枚，18 枚から 1 枚，17 枚から 1 枚と 4 回画像選択を行うことから，回答選択肢の数は 116,280（$= 20 \times 19 \times 18 \times 17$）となる．つまり，この段階における場合の数は，秘密情報と部分領域に含まれる回答候補画像数に依存する．なお参考までに，秘密情報に回答順序を含まず，回答順は順不同でもよいとすると，とりうる選択肢数は，4,845（$= \frac{20}{4} \times \frac{19}{3} \times \frac{18}{2} \times \frac{17}{1}$）となり，回答順序ありの際の安全性の 1/24 となる．

これまでの考察をふまえ，実験システムにおける安全性を**表 5** に示す．この結果から，今回の評価実験で設定した 4 条件におけるシステムは「画像 4 枚による秘密情報」という既存の画像認証手法と同等程度の秘密情報を用いつつも，理論的安全性は高められていることが分かる．これにより，本研究の目的であった安全性改善が実現できたことになる．なお T2 条件の安全性を示していないが，これ

表 5 S-IGA の安全性
Table 5 Security level of S-IGA.

システム条件	安全性
T1 設定	1/94,109,400 (=1/100 x 99 x 98 x 97)
T3 設定	1/488,360 (=5/21 x 1/116,280) ～ 1/2,441,880 (=1/21 x 1/116,280)
T4 設定	1/581,400 (=1/5 x 1/116,280)
T3 設定 *(ただし回答順序なし)*	1/20,349 (=5/21 x 1/4,845) ～ 1/101,745 (=1/21 x 1/4,845)

は T3 条件と同一と見なすことができる．理由は 2 つある．「部分領域選択」回答の有無が T2 条件と T3 条件の差であるが，回答の有無自体は安全性に関係がないのが 1 つめの理由である．もう 1 つの理由は，部分領域の回答有無以外の条件は T2 と T3 で同一であり，回答操作も実質的に同じになるためである．

なお表 5 下部に，T3 条件において秘密情報に「回答順序を秘密情報に含まない」場合の安全性もあわせて示している．この結果から，今回の設計条件であれば回答順序を秘密情報に含めなくても，4 桁暗証番号認証よりは安全性の高い認証手法になることが明らかである．

なおこれらの結果自体は，そうなるような仕組みを導入した結果であり，当然の結果といえる．しかしここで重要な点は，この安全性改良を既存の画像認証で用いられている秘密情報と同等の秘密情報で実現したことにある．前述したが，知識による個人認証において安全性を向上させる一般的な方法は，秘密情報の仕様を変更し，その情報量を増やす方法である．4 桁の暗証番号を 6 桁にするというのがその一例である．しかしこの方法は，一般に秘密情報の維持負担増と入力操作の負担増を利用者に強いることになる．これに対して提案手法は，画像は多数の回答候補を用意することが可能であるという再認式画像認証の仕組みを活用することで秘密情報を変更することなく安全性改善を可能にし，かつそれにともなう操作負荷の増加を抑制する工夫を施したことが，既存の改良方法と異なる点であると考えている．なお操作負担の増加抑制に関する評価については次節で議論する．

5.2 利用可能性と操作負担の増加抑制について

本節では提案した S-IGA の利用可能性について，認証時間と被験者による主観的負荷評価について議論する．

認証時間については，以下の 3 点が評価実験から明らかになったといえる．

- 正解画像の集中配置による手法の認証時間は 16 秒未満．
- 正解画像の部分領域への配置は全領域への配置と比較して認証時間が約 1/2 に短縮．
- 2 段階回答は直接回答と比較して認証時間の標準偏差が小さい．

S-IGA の認証時間は，100 枚の候補画像から 4 枚を選択するという条件で 16 秒未満となり，また状況によっては 10 秒未満で操作が可能なことも表 2 の最短認証時間から明らかとなった．また本実験の被験者は，提案手法をはじめて利用したばかりであるため，認証手法への慣れが進むことで操作時間の短縮も見込めると考える．これらの結果から，S-IGA は 4 桁暗証番号認証よりも高い安全性を提供する個人認証手法としてその利用可能性が疑問視されるものではないと結論づける．

なお最長認証時間に注目すると，T1，T2 条件の認証時間はともに 60 秒を超えている．これは画像グリッド全領域内に正解画像がランダムに配置されていると理解し，その状況で正解画像 4 枚を探索するのにかかった最長認証時間である．これに対して集中配置が自明な T3，T4 条件では最長認証時間が約 31 秒であり，T1，T2 条件と比較すると 1/2 以下の認証時間となっている．このことから部分領域への集中配置は操作時間の長期化を抑制しているといえる．つまり，部分領域への集中配置は認知・操作負担の増加を抑制できていると結論づける．

また認証時間の最短値と最長値の間で認証時間に 4～12 倍程度の差が生じている．この理由は，正解画像の配置が探索時間に影響するためである．S-IGA では正解画像の配置がランダムに行われるため，配置状況によってはスクロールをまったくせずに正解画像を選択可能な場合もあれば，部分領域の探索に時間がかかる場合もありうるためである．

なお参考までに T1 条件において回答候補画像数を 100 から 50 枚に変更した場合の平均と最長認証時間は，それぞれ 12.27 秒と 39.79 秒となった．この認証時間は，T3 条件のそれと同等程度の値であり，その一方で理論的安全性は T3 条件よりも高い安全性（1/5,527,200（$= \frac{1}{50\times49\times48\times47}$））となる．T1 条件は回答候補画像の追加のみしか導入していないため S-IGA とはいいがたい．しかし再認式画像認証の利点を応用すれば，様々な安全性を妥当な利便性とともに提供できるという一例であると考える．

5.3 被験者による主観評価

提案手法に対する実験被験者の主観評価について議論する．正解画像の探索負荷については，画像グリッド全領域が配置対象の T1 条件と部分領域のみが配置対象の T2，T3，T4 条件で評価が分かれる結果となった．また部分領域への集中配置に基づく 3 手法でも，スクロール方法の違いにより主観評価が異なる結果となった．これらの結果から，被験者が感じる正解画像の探索負担は全領域への配置よりも部分領域に集中配置した方が少なく，またスクロール方法にも依存することが明らかになった．

操作負荷については，(T2, T4) と (T1, T3) の 2 グルー

表 6 既存研究との比較
Table 6 Comparison table of recognition-based image authentications.

	n	m	p	回答候補画像数 ($n \times p$)	正解画像枚数 ($m \times p$)	解答順序	安全性	操作時間 (sec)
Awase-E [8]	10	1	4	40	4	-	1/9,999	24.6
VIP1 [7]	10	1	4	40	4	-	1/10,000	17*2
VIP3 [7]	16	4	1	16	4	なし	1/1,820	21*2
Déjà Vu [6]	25	5	1	25	5	なし	1/53,130	32
Photographic Authentication [24]	4	1	10	40	10	-	1/1,048,576	16*2
Use Your Illusion [10]	27	3	1	27	3	なし	1/2,925	12.4
ニーモニックガード [31]	36	4	1	36	4	あり	1/1,413,720	-
LockTile（回答順序あり）[32]	16	4	1	16	4	あり	1/43,680	-
LockTile（回答順序なし）[32]	16	4	1	16	4	なし	1/1,820	-
S-IGA（T3）	100	4	1	100	4	あり	1/2,441,880	15.19

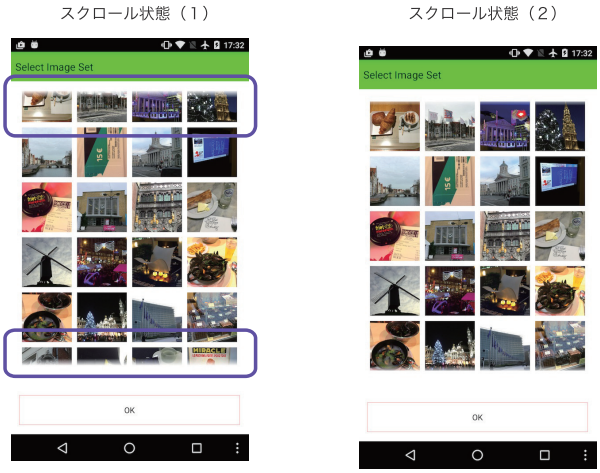

図 6 部分領域選択における操作性
Fig. 6 Operability issue in selecting sub region.

プに評価が分かれた．操作負荷の評価は，回答方法とスクロール方法の差異に起因すると考えるが，著者らの推測と異なったのは T3 条件の方が T2 条件よりも負担が大きいと評価された点である．これについて被験者にヒアリングしたところ，回答方法に起因していることが明らかになった．それは 2 段階回答における「部分領域選択」で，部分領域がきちんと位置あわせされるようスクロールを微調整しなければならない，と被験者の一部が思っていたためであった．**図 6** を用いて説明する．被験者は部分領域選択において，図 6 中のスクロール状態（1）では回答はできず，必ずスクロール状態（2）にする必要があると考えていた．そのため精緻なスクロール操作が求められると理解し，操作負担が大きいと評価していた．なお実際にはスクロール状態（1）で OK ボタンを押下すると，スクロール状態（2）のような状態にシステムが自動補正する仕組みとなっており，精緻なスクロール操作は実際には不要である．これを被験者が理解すれば，操作負担における T3 システムの評価は改善すると推測する．

次は認証時間に対する主観的評価である．これはシステム測定による操作時間（表 2）の結果とおよそ一致している．異なっている点は，T2 と T3 の認証時間は平均値を見ると実測値はほぼ同等であるのに対し，被験者による印象では T3 の方が長い時間が必要であると評価されている点である．両条件の差異は回答方法であり，T3 条件では 2 段階の回答が必須という事実が，認証時間を長いと感じさせる原因になっていると推測する．

最後に各条件のシステムが被験者に与えるフラストレーションについて述べる．著者らの仮説は T1 > (T2, T3) > T4 として T2 と T3 のフラストレーションに大きな違いは出ないと推測していた．しかし，実際には T1 > T3 > T2 > T4 となった．繰返しになるが，T2 と T3 条件の差異は回答方法であり，この評価結果も前述同様に 2 段階回答の操作性問題が被験者にフラストレーションを与えていると考える．

これらの評価結果から，T3 条件における 2 段階回答の「部分領域選択」に問題があり，それに起因する否定的評価が表出していることが明らかになった．したがって部分領域選択における操作性を改善する必要があるといえる．なお T2 条件と T3 条件の安全性は同等であることから，利用者の負担になる 2 段階回答を破棄して直接回答とすることが望ましいともいえる．

5.4 既存研究との比較考察

既存の再認式画像認証手法と本論文での提案手法（T3 条件）を設計要素ならびに安全性，操作時間について比較した表を**表 6** に示す．なお操作時間は，平均値または中央値の値でシステムによって異なる．またハイフンは，該当データがない，または明確にされていないことを意味する．この結果から，正解画像枚数（$= m \times p$）が 4 枚という条件の複数の手法間で比較をしても，操作時間には既存の提案手法と同等程度でありながら，提供しうる安全性は

*2 グラフからの読み取り値．若干の読み取り誤差がある可能性あり．

今までの手法よりも高い安全性を提供可能にしていることが分かる．

一方，100 枚前後の画像を利用した画像認証の提案に，画像認証における覗き見攻撃対策のための研究がある．Yamamoto らの提案手法 [27] では回答候補画像数が 80 枚，Wiedenbeck らの提案手法 [26] では 43〜112 枚であり，提案手法と同等程度の数の回答候補画像数を用いた再認式画像認証を提案している．しかし，これらの手法の主たる目的は覗き見攻撃に対する安全性を確保することであり，正解画像を直接選択するかわりに，間接的に回答選択を行う手法となっている．したがって，本論文での提案手法と異なり，認証時間が長くなることと総当たり攻撃に対する安全性が低下するという問題をかかえている．したがって，多数の回答候補画像を利用する点では共通したアプローチであるものの，安全性改善の方向性が「覗き見攻撃」か「総当たり攻撃」なのかという点で異なっている．

なお画像認証が覗き見攻撃に対して脆弱になる傾向にあることはよく知られており，それゆえ画像認証における覗き見攻撃への対策手法が上記の 2 手法のほかにもいくつか提案されている [28], [29]．この状況に対し，S-IGA は総当たり攻撃への安全性については改善可能にした一方で，覗き見攻撃に対する安全性を確保できていない．この問題については，今後の課題である．

5.5 利用状況に応じた個人認証手法へ向けて

本論文で提案した S-IGA は，以下の 3 つの特性を同時に成立させる新たな認証手法であると考えている．

a) 秘密情報を変更せずに安全性を変更可能．
b) 秘密情報を変更しないため，その維持負担は不変．
c) 操作負担の増加は安全性改善と比例せず，抑制可能．

項目 a) は安全性の指標であり，項目 b), c) は利便性の指標である．知識照合型個人認証の改良とは，安全性と利便性の “より良いバランス点” を模索することであると著者らは理解している．この点において，上記 3 つの特性を同時に成立可能にしたことは新たなバランス点を実現したものと考える．理由は 3 つある．1 つめは，同一の秘密情報を利用したまま，安全性を変更可能にした点である．再認式画像認証は，回答候補情報が画像であるため多数の「おとり回答候補」を用意することが可能である．これを応用することで上記の利点を実現している．2 つめは，安全性の改善が利便性の低下に直結しない工夫の導入である．正解画像を画像グリッド内の部分領域内に集中配置することで，部分領域の特定時のみ画像グリッド全域を探索し，特定後は部分領域のみを対象に正解画像を探索すればよいからである．これにより操作負担の増加を抑制可能にしている．3 つめは，画像を秘密情報として利用することによる利用者負担の抑制である．数字や文字など記号情報のかわりに画像や写真を利用することにより，人間が持つ視覚情報の認識能力や記憶保持能力を活用可能とし，多数の回答候補画像の中から正解画像を探索したり，秘密情報を記憶保持したりする際の負担に関して，それらの負担増加を抑制する効果が見込める点である．

これらの特性は「利用状況に応じた個人認証」に適していると著者らは考える．リスクベース認証という仕組みが提案され，実用化されている [22], [23], [35]．この仕組みは個人認証時の行動プロファイルやデバイス環境などにより認証システムが利用者の「正規利用者らしさ」を評価し，正規の利用者ではないとシステムによって推測された場合には平時の個人認証のほかに追加の認証を課すという仕組みである．よってシステムの評価によっては，正規の利用者であっても複数種の個人認証を行い，自分が正規利用者であることをシステムに示す必要が生じる．これは概念としては妥当なものだと考えるが，仕組みとしては安全性向上の一方で，認証時の利用負担を増加させるものである．利用者は，つねに必要とはいえない複数種の個人認証手法を理解し，必要に応じて使用・操作できるようにしておく必要がある．

一方，リスクベース認証に適した個人認証には以下の 2 つの要件があると著者らは考える．

- 個人認証が提供する安全性をリスクに応じて変更できる．
- 正規利用者における個人認証の負担は，リスクにかかわらず不変もしくは最小限の負担増．

ここで重要なのは正規利用者と攻撃者への対応を別々に考える点にある．個人認証を通じて容易に “なりすまし” されないようするためには，安全性の高い個人認証を攻撃者に課するとともに，それに付随する負担を攻撃者に強いることについても異論はない．しかし，そのために正規利用者も攻撃者と同様の負担を強いられることは望ましいことではない．つまり，リスクベース認証の理想は，リスクに応じて個人認証が利用者に課する安全性を変更しつつも，攻撃者による攻撃成功へのコストを高くしつつ，かつ正規利用者の認証利用における負担は不変か必要最小限の負担増になっていることである．しかし，安全性確保のために複数の個人認証手法を組み合わせる手法を用いている限り，後者の要件を満たすのは困難であると考える．

これに対し，S-IGA はこれら 2 つの要件を満たしうる個人認証手法であると著者らは考える．安全性が変更可能であることは表 5 に示したとおりであり，リスクに応じた安全性の提供が可能である．一方，正解画像の集中配置により認証操作にかかる負担増加も抑制可能となっている．また秘密情報自体はシステムの設計条件にかかわらず不変であるため，秘密情報の維持負担は既存の画像認証と同等程度である．つまり正規利用者にとっては，必要な負担増のみでありながら，個人認証の安全性を可変化することが可能となっている．一方，攻撃者にとっては多数の画像群の

中から 4 枚の画像を既定の回答順序に従って回答できなければ “なりすまし” に成功できない．また回答候補画像数はリスクに応じて変更可能であり，画像枚数を増やすことで攻撃者がなりすましに必要なコストを高くすることも可能だからである．

そして何より重要な点は，これらの特性を 1 つの認証手法で提供できる点である．つねに使用するわけではない個人認証手法は，その秘密情報や操作方法を忘れる可能性がある．それゆえ既存のリスクベース認証では所有物認証や One-Time Password による追加認証を行っており．それゆえ秘密情報の保持に関する負担は無視できるようになっている．しかし，それでも個人認証に必要な機器・情報の所有や認証操作に関する負担は増加する．これに対して S-IGA では，S-IGA の設計条件をリスク評価に応じて動的に変更することで利用者に対する安全性を可変化できる．また安全性を可変にしても，新たに操作方法を習得したり，秘密情報を作成・保持するための追加負担はない．正規利用者が保持する秘密情報と認証操作方法は不変であり，リスク評価によらず同じ認証操作で同じ秘密情報を入力するだけである．またそれゆえに操作方法の忘却や必要な認証機器の欠落による追加認証が不能になるという懸念もない．これらの特徴はこれまでの個人認証手法にはない大きな利点であると考える．

6. おわりに

本論文では，知識照合型個人認証において再認式画像認証の安全性向上を可能にしつつ，認証時の負担増加を抑制しうる方法について議論し，再認式画像認証においては次の 2 つの仕組みを導入することがその実現を可能にする方法であることを述べた．手法 1）認証回答時の回答候補画像数を増やす．手法 2）正解画像を回答候補画像群内の部分領域に集中配置する．手法 1 により秘密情報の記憶負担を増やすことなく安全性向上を実現可能にし，手法 2 により安全性向上にともなう操作負担の増加を抑制可能にした．これらの提案に基づく個人認証システム “S-IGA” を Android アプリケーションとして実装し，被験者による利用可能性と操作負担の抑制効果について評価実験を行った．S-IGA の認証時間は，100 枚の画像から 4 枚の回答画像を既定の順序どおりに選択するという条件において平均 16 秒未満で操作可能であり，利用可能性に疑問を持たれる手法ではないことを明らかにした．また上記の秘密情報において 4 桁暗証番号認証よりも高い安全性を提供可能にすることを明らかにした．また提案手法における特徴である「秘密情報を変更せずに安全性を柔軟に可変化できる」点がリスクベース認証における個人認証手法として適していることについても議論した．

今後の課題であるが，正解画像の配置方法について別の手段で利用者の負担を過度に増大させずに認証時間を短縮可能にする方法がないか模索する予定である．また再認式画像認証において覗き見攻撃の脅威は無視できない．回答方法の工夫により，覗き見攻撃への安全性も確保可能にすべく改良を試みる予定である [36]．

謝辞 評価実験において被験者となっていただいた学生諸氏に感謝する．本研究は JSPS 科研費 JP26540055 の助成を受けたものです．

参考文献

[1] Gao, H., Jia, W., Ye, F. and Ma, L., A Survey on the Use of Graphical Passwords in Security, *Journal of Software*, Vol.8, No.7, pp.1678–1698 (2013).
[2] Suo, X., Zhu, Y. and Own, G.S.: Graphical Passwords: A Survey, *21st Annual Computer Security Applications Conference* (ACSAC) (2005).
[3] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D.: The Design and Analysis of Graphical Passwords, *8th USENIX Security Symposium* (1999).
[4] Syukuri, A.F., Okamoto, E. and Manbo, M.: A User Identification System Using Signature Written with Mouse, *3rd Australasian Conf. Information Security and Privacy* (*ACISP*), pp.403–441 (1998).
[5] 小池英樹，高田哲司，増井俊之：画像を用いた個人認証手法，情報処理，Vol.47, No.5, pp.479–484 (2006).
[6] Dhamija, R. and Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *9th USENIX Security Symposium*, pp.45–58 (2000).
[7] De Angeli, A., Coutts, M., Coventry, L., Johnson, G.I., Cameron, D. and Fischer, M.H.: VIP: A Visual Approach to User Authentication, *Proc. Working Conference on Advanced Visual Interfaces* (*AVI '02*), pp.316–323 (2002).
[8] Takada, T. and Koike, H.: Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images, *5th Int'l Symp. Human-Computer Interaction with Mobile Devices and Services* (*MobileHCI '03*), pp.347–351 (2003).
[9] Brostoff, S. and Sasse, M.A.: Are Passfaces more usable than passwords? A field trial investigation, *People and Computers XIV – Usability or Else!*, pp.405–424 (2000).
[10] Hayashi, E., Dhamija, R., Christin, N. and Perrig, A., Use your illusion: Secure authentication usable anywhere, *Proc. 4th symposium on Usable Privacy and Security* (*SOUPS '08*), pp.35–45 (2008).
[11] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N.: PassPoints: Design and Logitudinal Evaluation of a Graphical Password System, *Int'l Journal Human-Computer Studies*, Vol.63, pp.102–127 (2005).
[12] Chiasson, S., van Oorschot, P.C. and Biddle, R.: Graphical password authentication using cued click points, *European Symp. Research in Computer Security* (*ESORICS 2007*), pp.359–374 (2007).
[13] Chiasson, S., Forget, A., Biddle, R. and van Oorschot, P.C.: Influencing users towards better passwords: Persuasive cued click-points, *Proc. 22nd British HCI Group Annual Conference on People and Computers*, pp.121–130 (2008).
[14] Theriault, C.: Survey says 70% don't password-protect mobiles: Download free Mobile Toolkit, available from ⟨https://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/⟩ (accessed 2016-06-

10).
[15] Siciliano, R.: More Than 30% of People Don't Password Protect Their Mobile Devices, available from ⟨https://blogs.mcafee.com/consumer/unprotected-mobile-devices/⟩ (accessed 2016-06-10).
[16] Microsoft: Signing in with a picture password, available from ⟨https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password/⟩ (accessed 2016-06-10).
[17] Weinshall, D.: Cognitive authentication schemes safe against spyware, *2006 IEEE Symposium on Security and Privacy* (*S&P '06*) (2006).
[18] Gao, H., Liu, X., Dai, R., Wang, S. and Chang, X.: Analysis and evaluation of the colorlogin graphical password scheme, *5th International Conference on Image and Graphics* (*ICIG '09*), pp.722–727 (2009).
[19] Riva, O., Qin, C., Strauss, K. and Lymberopoulos, D.: Progressive Authentication: Deciding When to Authenticate on Mobile Phones, *21st USENIX Security Symposium*, pp.301–316 (2012).
[20] Davis, D., Monrose, F. and Reiter, M.K.: On user choice in graphical password schemes, *Proc. 13th USENIX Security Symposium*, pp.151–164 (2004).
[21] Hayashi, E., Das, S., Amini, S., Hong, J. and Oakley, I.: CASA: Context-aware scalable authentication, *Proc. 9th Symp. Usable Privacy and Security* (*SOUPS '13*), ACM (2013).
[22] Hayashi, E., Riva, O., Strauss, K., Brush, A.J.B. and Schechter, S.: Goldilocks and the two mobile devices: Going beyond all-or-nothing access to a device's applications, *Proc. 8th Symp. Usable Privacy and Security* (*SOUPS '12*), ACM (2012).
[23] Riva, O., Qin, C., Strauss, K. and Lymberopoulos, D.: Progressive Authentication: Deciding When to Authenticate on Mobile Phones, *Proc. 21st USENIX Security Symposium* (*USENIX Security '12*), pp.301–316, USENIX (2012).
[24] Pering, T., Sundar, M., Light, J. and Want, R.: Photographic Authentication Through Untrusted Terminals, *IEEE Pervasive Computing*, Vol.2, No.1, pp.30–36 (2003).
[25] Jansen, W., Gavrila, S., Korolev, V., Ayers, R. and Swanstrom, R.: Picture Password: A Visual Login Technique for Mobile Devices, *NISTIR 7030* (2003).
[26] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J.C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme, *Proc. Working Conference on Advanced Visual Interfaces* (*AVI '06*), pp.177–184 (2006).
[27] Yamamoto, T., Kojima, Y. and Nishigaki, M.: A Shoulder-Surfing-Resistant Image-Based Authentication System with Temporal Indirect Image Selection, *Proc. Int'l Conf. Security & Management*, pp.188–194 (2009).
[28] Sobrado, L. and Birget, J.C.: Graphical passwords, The Rutgers Scholar an Electronic Bulletin of Undergraduate Research, available from ⟨http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm⟩ (accessed 2016-03-01).
[29] 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.5, pp.1997–2013 (2005).
[30] Passfaces Corp.: Passfaces: Two Factor Authentication for the Enterprise (online), available from ⟨http://www.realuser.com/⟩ (accessed 2016-03-01).
[31] （株）ニーモニックセキュリティ：ニーモニックガード（オンライン），入手先 ⟨http://www.mneme.co.jp/mne/⟩（参照 2016-03-01）.
[32] （株）インフォファーム：LockTile 好きな写真で簡単セキュリティ（オンライン），入手先 ⟨http://www2.infofarm.co.jp/shalock/whats.html⟩（参照 2016-03-01）.
[33] （株）シマンテック/日本ベリサイン（株）：「個人・企業のパスワード管理」に関する意識調査結果のご報告，入手先 ⟨https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf⟩（参照 2016-06-10）.
[34] Google, Nexus 5X, available from ⟨https://www.google.com/intl/ja_jp/nexus/5x/⟩ (accessed 2016-02-25).
[35] Symantec Corp.: Symantec Validation and ID Protection Service (online), available from ⟨https://www.symantec.com/products/information-protection/validation-id-protection⟩ (accessed 2016-03-01).
[36] 森　康洋，高田哲司：スクロールとスライド操作による携帯端末向け個人認証，インタラクション 2015, pp.542–545 (2015).

森 康洋

2015 年電気通信大学情報理工学部総合情報学科卒業．在学中はモバイルシステム上での画像を用いた個人認証にかかる研究に従事．ソーシャルエンジニアリングにも関心がある．現在，民間企業勤務．

高田 哲司　（正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士後期課程修了．博士（工学）．2003 年ソニーコンピュータサイエンス研究所研究員．2005 年独立行政法人産業技術総合研究所情報技術研究部門研究員．2010 年電気通信大学大学院情報理工学研究科准教授，現在に至る．個人認証，ユーザブルセキュリティ，情報視覚化に興味を持つ．IEEE/CS 会員．