# １つの秘密情報で複数の安全性を提供しうる個人認証

高田 哲司[1]　森 康洋[1,†1]

**概要**：本論文では，１種の個人認証手法で，かつ１つの固定値による秘密情報で複数の安全性を提供しうる個人認証を提案する．個人認証が提供する安全性を変更するには，一般に秘密情報を変更する手法が用いられる．しかし，そのアプローチは利用者に負担をかける方法であり，望ましいものとは言いがたい．これに対して本研究では，利用者が記憶する秘密情報は変更せずに，回答候補数を増やすことでその安全性を可変とする．そしてこの手法は画像を用いることで可能であり，従来の記号による秘密情報では実現が困難なことについても議論する．またこの提案手法が「利用状況に応じた個人認証」に適した個人認証であり，安全性が高いけれども利用頻度は高くないシーンでの個人認証としても利点のある手法であることについても議論する．

**キーワード**：個人認証，二要素認証，画像認証，リスクベース認証，利用状況に応じた認証

# Stretchable Image-based Authentication enables to provide Multi-level Security with One Fixed Credential

Tetsuji Takada[1]　Yasuhiro Mori[1,†1]

***Abstract:*** In this paper, we propose an image-based user authentication that could provide multi-level security with one fixed credential. Generally, there are two approaches to improve a security of a user authentication: 1) use an alternative or an enhanced credential, 2) use more than one verification schemes sequentially. However, it is undesirable approaches because they put an additional operation load to users. On the other hand, our scheme enables to change a security level flexibly while a user just answers one fixed credential by a same operation. This authentication scheme makes use of the fact that we could prepare numerous variations of image than a symbol-based information such as characters or numbers. We also discuss that the proposed scheme is suitable for following two user authentication scenes: (1) "Context-dependent (Risk-based) User Authentication", and (2) frequency of use is low but it needs a high-level security.

***Keywords:*** Image-based User Authentication, Two-factor Authentication, risk-based authentication

## 1. はじめに

携帯端末の普及にともない，IT システムの主たる利用形態は計算機から携帯端末になり，その利用シーンは多様化した．またシステムの利用方法も Web ブラウザだけでなく，専用のアプリケーション (アプリ) を通じて利用する形態も増えつつある．

この状況において，IT システムのサービス内容または機能に応じてアクセスレベルを柔軟に設定できることが望ましいと利用者が考えていることが明らかになっている．Hayashi らの論文 [2] によると，携帯端末で利用するアプリに対し利用者が希望するアクセスレベルがアプリによって異なることが明らかにされている．一例を紹介する．携帯電話で画面ロックを利用している人に対し，端末内にインストールされているアプリの希望する利用形態を次の 3 カテゴリーから選択してもらう調査を行った結果，**表 1** の結果となった．

[1] 電気通信大学
The University of Electro-Communications
[†1] 現在，(株) ソリトンシステムズ
Presently with Soliton Systems K.K.

**表 1** アプリに適したアクセスモデルの分類結果

| Category | Median value |
|---|---|
| Always Available | 35% |
| Split | 20% |
| After Unlock | 45% |

1) 常時利用可能で良い (Always Available)
2) 一部の機能は画面ロック解除時のみ，それ以外の機能は常時利用可能で良い (Split)
3) 画面ロック解除時のみ利用可能 (After Unlock)

この結果から言えることは，現状のアクセス制御モデルが利用者の望む状況とは異なっている点である．現状のアクセス制御は，All-or-Nothing モデルである．つまり，個人認証を通じてサービスにログインすれば許可されているすべての操作が可能だが，ログインしていなければ，いかなる操作もできない．つまり IT システムのアクセス (利用) 制限はアプリ単位や機能単位ではなく，端末単位またはサービス単位になっている．

柔軟なセキュリティモデルを必要としているもう１つの例として「リスクベース認証」がある．システムの利用シーンの多様化により，IP アドレスなど利用環境に基づくアクセス制御が困難になりつある．この状況に対し，利用シーンに関する様々な情報を基に操作者の「正規利用者らしさ」を算出し，その値が低い場合には検証情報を増やすことで，より確実なユーザ認証を行う手法である．「正規利用者らしさ」の算出には時空間情報 (移動履歴) を用いるものや，端末内の複数のセンサー値に基づく状況情報 [4] を活用する方法などが提案されている．

アクセスレベルまたは検証レベルを柔軟に設定可能にするためには，複数の安全性を提供可能な検証システムが必要となる．ここで「検証システム= 認証システム」とすると，より高い安全性を提供しうる認証システムが必要となる．一般に個人認証の安全性を強化する方法は以下の２つのアプローチになると考える．

(a) 秘密情報の情報量を増やす
(暗証番号を 4 桁から 6 桁へ，パスワードの文字数と文字種を増やす)
(b) 複数の認証システムを併用する
(複数の認証手法の直列接続)

しかし，これらのアプローチはどちらも利用者の負担を増やすことになる．(a) は秘密情報の記憶負担を増やすことになる．この負担増は多くの利用者にとって受容するのが困難なのが現状である．したがって望ましいアプローチとは言い難い．(b) は二要素認証が該当する．記憶負担を増やさないようにするため，所有物や One-Time Password によって検証要素を増やす手法が用いられている．しかし，この方法でも操作負担や機器所持の負担は増える．したがってこのアプローチも望ましい手法とは言いがたい．

これらの議論をふまえると，以下の特徴を備える個人認証手法が望まれていると言える．

i) 秘密情報の記憶保持負担増を抑制しつつ，安全性向上を可能にする
ii) 複数の認証手法の組み合わせでなく，単一の認証手法で安全性向上を可能にする

そこで本研究では，単一の秘密情報で安全性を柔軟に可変可能な認証手法として再認式画像認証を用いた実現方法を提案する．提案手法のポイントは，秘密情報以外のおとり回答の数を増減することで利用者が記憶する秘密情報を変更することなく提供する安全性を柔軟に変更可能にする点にある．またこの提案手法は画像を利用しているから実現が容易であり，数字や文字といった記号情報を用いた場合には限界があることについても言及する．

以降，本論文では 2 章で利便性を損なわずに安全性を可変化する方法について議論し，画像を用いることによりその実現が可能なことについて述べ，3 章で提案する安全性を伸長可能な画像認証について説明する．4 章では考察として，提供しうる安全性について明らかにするとともに，利用状況に応じて安全性を提供しうる個人認証の実現に関して議論する．

## 2. 利便性を損なわずに安全性を変更する方法

ランダム攻撃に対する個人認証の安全性は式 (1) で表すことができる．

$$Security\ level = (\frac{1}{m})^{n} \tag{1}$$

4 桁の暗証番号認証であれば，(m, n)=(10, 4) であり，アルファベット (大小文字) による 8 文字のパスワードであれば (m, n)=(52, 8) として安全性を計算することができる．この 2 変数のうち，変数 $n$ は秘密情報の文字数に該当する．したがって，この数字を増やすと秘密情報の情報量が増加し，結果として記憶負担が増えることになる．したがって変数 $n$ を変更することで認証システムが提供する安全性を変更する方法は望ましい方法とは言いがたい．

一方，変数 $m$ は秘密情報を構成する基本情報 1 つあたりのバリエーション数である．暗証番号であれば，数字のバリエーション数であり ($m = 10$)，アルファベット (大文字+小文字) であれば ($m = 52$) となる．この値は秘密情報のバリエーション数を決定する一要素であるため，秘密情報作成時には選択肢の数として影響を及ぼすと考えるが，決定後の秘密情報の記憶負担に対する影響はないと言える．したがって，この値を変更することで提供する安全性を柔軟に変更可能な認証システムの設計を試みる．

ここで変数 $m$ の値を柔軟に変更できるかについて考察すると，記号情報による秘密情報である限り，容易ではないと言わざるをえない．理由は，記号のバリエーション数は基本的に固定だからである．数字なら 10 種類，アルファ

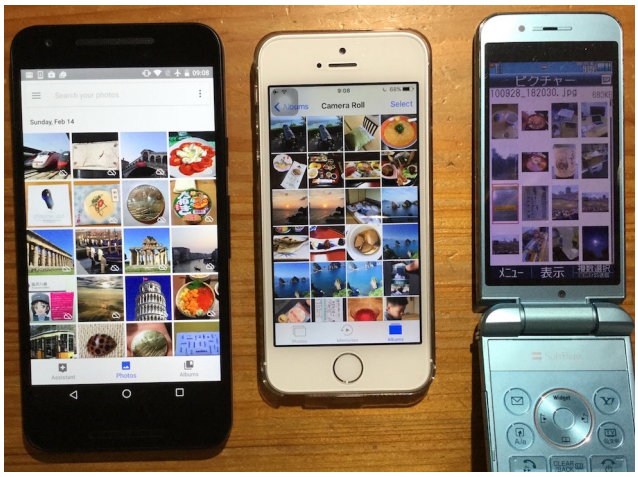


**図 1** 携帯端末におけるアルバムアプリの表示画面

ベットなら 26 種類という具合である．この値を減らすことは可能だが，それは安全性の低下を導くだけであり，安全性の高い認証手法の実現はできない．バリエーション数の多い記号として「漢字」や「絵文字」の適用も考えられる．しかし，その記号に慣れ親しんでいて活用できるユーザ層が一部に限られる点と，数字やアルファベットと比較しても，秘密情報として利用される記号に偏りが発生する懸念があるといった点が問題となる可能性がある．そこで本研究では画像の利用を提案する．

秘密情報の基本構成情報に画像を用いることで，上述の問題が回避可能になる．写真の利用により，基本構成情報におけるバリエーション数の制約はなくなる．したがって，前述の式 (1) における $m$ の値域の制約がなくなるため，目標とする認証システムの実現が可能となる．また写真を用いることにより，既存の記号情報を用いた秘密情報の場合と比較して，特定の画像が多くのユーザの秘密情報として使用される懸念，つまり，秘密情報に利用される画像が偏る可能性も低減可能になると考える．さらに個人認証に利用する画像をユーザがシステムへ持ち込み可能にすることにより，利用者ごとに秘密情報の母集団が異なることになる．これはセキュリティ向上にもつながると考える．すべてのユーザが同一母集団から秘密情報を設定して利用すると，どうしても多くのユーザが秘密情報として使用する傾向のある画像が発生する．これは「多くの利用者が使用する傾向にある秘密情報 (=画像) で多数のユーザアカウントに対してなりすましを試みる」という攻撃を可能にしてしまう．秘密情報を決定する母集団をユーザ毎に異なるものにすることは，上記の攻撃を困難化することになると考える．また画像を秘密情報に用いることで人間の視覚記憶を活用可能なため，記憶負担に配慮した個人認証にもなる．

これらの理由から，画像を個人認証に応用することにより，前章で述べた目標の (i)(ii) を実現する個人認証を提案する．

## 3. 安全性が伸長可能な画像認証

本章では，安全性を柔軟に変更可能な画像認証について説明する．前章で述べた通り，提案手法は画像そのものを秘密情報として利用する．したがって，再認手法による画像認証をベースとする．再認式画像認証の場合，複数ある回答候補画像の中から自分の秘密情報である画像を選択することで回答を入力する．その際，秘密情報である画像以外の画像が「不正解用の回答候補」として必要となる．提案手法ではこの不正解用の画像数を変更することで，個人認証が提供する安全性を柔軟に変更可能とする．なお以降では秘密情報である画像のことを「パス画像」，不正解用の画像のことを「おとり画像」と呼ぶ．

したがって，おとり画像が増えるにしたがい，多くの画像を閲覧し，そしてその中からパス画像を発見して選択できるユーザ・インタフェースが必要となる．そこで本研究では，スマートフォンにおけるアルバムアプリのユーザ・インタフェースの仕組みを流用する．カメラ付き携帯端末の普及により，アルバムアプリの利用経験があるユーザは少なくないと想定する．そういったユーザは，大量の画像閲覧における操作に習熟しており，新たな個人認証の利用における学習負担を抑制しうると考えるからである．

本提案では，以下の設計要素を既存のアルバムアプリから流用する．

(x) 縦スクロールのみによる画像閲覧操作
(y) 画像の表示サイズ

一方，流用しないのは以下の要素である．

(z) 画像の配置 (レイアウト)

画像の提示方法は縦スクロール操作だけで全画像が閲覧できるよう縦長のグリッド表示とする．個々の画像の表示サイズは「画像グリッド 1 行に画像 4 枚」を基準とする．iOS，Android，第三世代携帯電話のアルバムアプリを調査したところ，調査した範囲において画面が比較的小さい端末ではこの数は共通であり，画面の物理サイズには非依存であった (**図 1**)．よって本研究では 1 行内の画像数は 4 とした．この決定により画像グリッドの列数は固定化されたため，おとり画像の画像数に応じて画像グリッドの行数が増える，つまり縦方向に長くなることになる．一方，画像の配置は既存のアルバムアプリが時系列順で固定配置である傾向にあるが，本研究における個人認証ではランダム配置とする．

ただし，パス画像を画像グリッド内に単純ランダム配置すると認証回答時のパス画像探索負担が大きくなる．特に回答候補画像の数が増えるにしたがい，つまり画像グリッドが大きくなるにつれ，多数の回答候補画像の中からパス画像を探索しなければならず，負担が大きくなることが懸念される．この負担増加を抑制する仕組みとして，別のパ

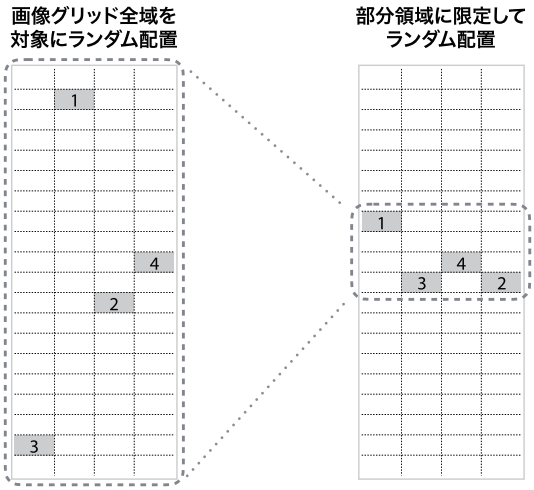


**図 2** パス画像の配置:グリッド全域と部分小領域

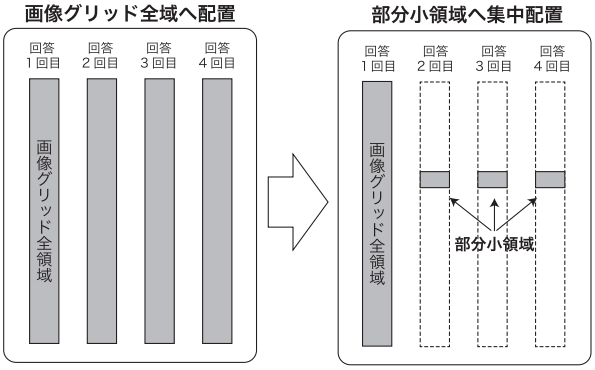


**図 3** 配置方法の変更によるパス画像探索領域の縮小

ス画像配置方法を提案する．それはパス画像の配置領域を「縦長画像グリッド内の部分小領域内に制限する」方法である (**図 2**).

この提案により，パス画像の探索負担増を抑制できると考えている．ここで以降の議論では，パス画像を 4 枚と仮定する．画像グリッド全域にパス画像をランダム配置した場合，**図 3** 左にある通り，画像グリッド全域を対象にパス画像の探索を 4 回行う必要がある．つまり，この配置方法だと，画像グリッドが大きくなるにしたがい，パス画像の探索負担も比例して増えることになると言える．これに対して，配置領域を部分小領域に限定した場合，まず利用者は 4 枚のパス画像のうちのいづれか 1 枚を縦長グリッドの全領域から見つけ出す必要がある．しかし，パス画像を 1 つ発見した後は，発見したパス画像の周辺領域だけに限定して残りのパス画像を探索すればよいことになる (図 3 右)．したがって，2 回目以降のパス画像の探索領域は部分小領域に限定されることになる．これにより安全性向上のために画像グリッドが大きくなったとしても，その大きさに応じて探索領域が大きくなるのは 1 回目の探索のみとなる．つまりパス画像の探索負担増加を抑制できることになる．

これまでの議論により，提案手法には以下の 2 つの設定要素があることを説明した．

- おとり画像の画像枚数 $(= m)$
- パス画像の配置方法 (画像グリッド全域 or 部分小領域)

上記の 2 つ以外に，もう 1 つ「パス画像の回答順序」という設定要素を導入する．パス画像が複数枚の場合，その回答順序を個人認証における検証対象とするかを選択可能にするのである．検証対象の場合，秘密情報は「画像による順列」となり，検証対象外の場合は「画像集合」として既定の値と同一かが検証されることになる．この設定要素は個人認証が提供する安全性に影響する一方で，秘密情報の記憶負担を増やす懸念がある [5]．理由は，パス画像を記憶すると同時に，回答入力順序も記憶する必要が生じるからである．回答順序の記憶支援にストーリを作成して記憶する手法が知られているが，それでも負担になるという結果も報告されている [5]．ただし論文 [5] による実験条件は，システムが画像を提供した上での評価であり，その画像群も複数のカテゴリーに限定された画像をもとに行ったものであった．よって，それ以外の条件による画像での回答順序の記憶については未検証である．よってここでは，柔軟な安全性提供の可能性を残すため，この設定要素を取り入れる前提で議論を進める．

### 3.1 プロトタイプシステム

これまでの議論に基づき，個人認証システムのプロトタイプを Android スマートフォンのアプリとして実装した．なおこのプロトタイプは論文 [1] をベースに行ったものであり，特にユーザ・インタフェースの見た目は同一である．実装したプロトタイプシステムの認証画面例を**図 4** に示す．端末画面には 5 行 4 列の画像群が表示されているが，これらの画像は回答候補画像群の一部であることに注意されたい．つまり表示されている画像群の上下に，端末には表示されていない回答候補画像群が存在するという意味である．

プロトタイプシステムの操作方法は設定条件にかかわらず同一である．縦長グリッド状に配置された回答候補画像群の中から既定のパス画像を見つけ出し，選択 (回答) することである．ただし，パス画像の回答順序が秘密情報となっている場合は，既定の回答順にパス画像を選択する必要がある．

なおパス画像配置領域を部分小領域に限定する場合の部分小領域は，5 行 4 列の表示領域と定義した．これは被験者実験で使用した Android 端末である Nexus 5X の画面サイズにあわせたものである．列数 4 の理由はすでに述べた通りである．行数 5 の理由は，操作用ボタンの表示領域を除いた残りの画面領域で表示可能な最大画像数がこの大きさであったためである．部分小領域を端末画面に一度に表示される領域とした理由は，操作負担への配慮のためである．パス画像が配置される部分小領域が端末画面に一度に


**図 4**　プロトタイプシステムの認証画面例

表示可能ということは，すべてのパス画像を端末画面上に同時に表示できることを意味する．パス画像の選択操作をする前に，すべてのパス画像が端末画面上に表示されるよう事前にスクロール操作をしておけば，パス画像の選択操作をスクロールすることなく一度に行うことができ，操作負担の抑制につながると考えたためである．

なおこの部分小領域は，画像グリッド全領域の中からランダムに決定される．つまり，仮に画像グリッド全領域が 25 行 (=パス画像+おとり画像が 100 枚) である場合，そこから 5 行の部分小領域を決定する方法は 21 通りあることになる．

### 3.2　被験者による評価実験

提案する認証手法の利用可能性を明らかにするため，認証操作にかかる時間を被験者による実験で評価した．認証操作時間を利用可能性の指標とした理由は，回答候補画像数が増えるにしたがい認証行為に必要な時間が現実的に受け入れ困難と判断されるほど長くなる懸念があったためである．

被験者 12 名で，内訳は男性 11 名/女性 1 名，全員が 20 歳代の大学学部または大学院生である．また被験者全員がスマートフォンの利用者で，かつアルバムアプリの利用経験者でもあった．実験で利用した携帯端末は Nexus 5X(画面サイズは 5.2 インチ，画面解像度は 1920×1080 pixels) を使用した．

今回の実験では 3 つの設定条件で実験を行った．実験で用いた認証システムの設定条件を**表 3** に示す．実験手順は以下の手順で実施した．

**Step 1) 事前説明**: 実験実施前に実験内容と認証システムの操作方法を説明し，実機による認証操作を最低 3 回行わせ，操作方法を確認させた．操作方法の説明は「再認式画像認証の基本操作と回答候補画像が縦長のグリッド状に配置されており，縦スクロールで画像群を閲覧できる」という説明にとどめ，配置方法の条件については説明しなかった．

**表 3**　被験者実験により評価した設定条件

| 条件 | 回答候補画像数 | 配置領域 | 回答順序 |
|---|---|---|---|
| Cond1 | 50 | 全域 | あり |
| Cond2 | 100 | 部分小領域 | あり |
| Cond3 | 100 | 全域 | あり |

なおパス画像は 4 枚の画像を順序付きで記憶するものとし，実験実施前に 50 枚の写真の中から被験者に自由に選択させた．50 枚の画像は著者側が用意した画像であり，著者所有の海外旅行時に撮影した写真群を利用した．

**Step 2) 操作実験**: プロトタイプシステムを用いて被験者に認証操作を実施させ，システムを通じて認証成否と操作時間を測定した．被験者には各設定条件の認証システムで 7 回認証に成功するまで繰り返し操作を実施させた．なお実験時において，これから操作する認証システムの回答候補画像枚数およびパス画像の配置領域に関する設定状況は被験者に明らかにせず，問われても回答はしなかった．

**表 4**　認証操作時間

| 条件 | 最小値 | 平均値 | 標準偏差 | 中央値 | 最大値 |
|---|---|---|---|---|---|
| Cond1 | 4.71 | 11.91 | 5.94 | 10.29 | 39.79 |
| Cond2 | 5.12 | 7.41 | 9.50 | 11.54 | 62.52 |
| Cond3 | 7.80 | 25.98 | 15.55 | 20.75 | 82.81 |

(数値の単位は全て second)

実験結果を**表 4** に示す．平均値に注目すると，100 枚の画像群からランダムに配置されたパス画像 4 枚を既定の回答順に選択する条件でも認証操作時間は 30 秒未満という結果となった．また部分小領域に配置した場合には，操作時間が 26 秒台から 7 秒台に短縮されうることも明らかになった．なお提案手法の認証操作時間は，パス画像の配置状況に応じて大きく変動せざるをえない面があることに注意する必要がある．また今回 3 種の設定条件による個人認証システムを 12 名でそれぞれ 7 回づつ，合計 252 回の認証操作を試みてもらったが，認証に失敗する事象は 1 回も発生しなかった．

## 4.　考察

### 4.1　提供しうる安全性

本節では，提案手法によって提供可能な複数の安全性について議論する．提案手法における設定要素は以下の 3 項目になる．

i) 回答候補画像の枚数 （パス画像の枚数+おとり画像の枚数の意．$n$ とする）

**表 2**　提供しうる安全性

**Table 2**　Possible Security Level of the Proposed System in Some Configurations

| | 画像枚数 | 配置領域 | 回答順序 | 回答バリエーション数 | 計算式 |
|---|---|---|---|---|---|
| 条件 a | 52 | 部分領域 | - | 8,721〜43,605 | $=(\frac{9}{5}\times\frac{20\times19\times18\times17}{4\times3\times2\times1})\sim(9\times\frac{20\times19\times18\times17}{4\times3\times2\times1})$ |
| 条件 b | 52 | 全域 | - | 270,725 | $=_{52}C_4=(\frac{52\times51\times50\times49}{4\times3\times2\times1})$ |
| 条件 c | 52 | 部分領域 | あり | 209,304〜1,046,520 | $=(\frac{9}{5}\times(20\times19\times18\times17))\sim(9\times(20\times19\times18\times17))$ |
| 条件 d | 52 | 全域 | あり | 6,497,400 | $=_{52}P_4=(52\times51\times50\times49)$ |
| 条件 e | 100 | 部分領域 | - | 20,349〜101,745 | $=(\frac{21}{5}\times\frac{20\times19\times18\times17}{4\times3\times2\times1})\sim(21\times\frac{20\times19\times18\times17}{4\times3\times2\times1})$ |
| 条件 f | 100 | 全域 | - | 3,921,225 | $=_{100}C_4=(\frac{100\times99\times98\times97}{4\times3\times2\times1})$ |
| 条件 g | 100 | 部分領域 | あり | 488,376〜2,441,880 | $=(\frac{21}{5}\times(20\times19\times18\times17))\sim(21\times(20\times19\times18\times17))$ |
| 条件 h | 100 | 全域 | あり | 94,109,400 | $=_{100}P_4=(100\times99\times98\times97)$ |

ii) パス画像の配置領域 （全域 or 部分小領域）

iii) パス画像の回答順序 （順序あり or 順不同）

なお，以下の仮定をおいて議論を進めることとする．

1) パス画像は 4 枚

2) パス画像を制限配置する際の部分小領域は 5 行 4 列

3) 回答候補画像数 $n$ は (52, 100) の 2 条件とする

これらの仮定により，3 つの設定要素についてそれぞれ 2 条件を用意し，合計 8 通りの条件設定が可能になる．これらの条件において，入力可能な回答バリエーション数，つまり偶然入力した値が正解になる確率の逆数を**表 2** に示す．この値が大きいほど，当該設定条件による認証システムは安全性が高いということになる．

計算方法について説明する．まず (配置領域，回答順序) = (全域，あり) と (全域，なし) の 2 条件についてだが，これは回答候補画像群からパス画像を既定の順序で 1 つづつ選択する方法と，回答順序を検証せず回答画像群を集合とみなして検証することから，その回答バリエーション数はそれぞれ ${}_nP_4$ と ${}_nC_4$ になる．

次にパス画像の配置領域が部分領域の場合について説明する．この条件の場合，回答操作は実質的に以下の 2 段階になると考える．

- 1 段階目: 画像グリッド全域から部分小領域を決定する
- 2 段階目: 部分小領域からパス画像を選択する

したがって，これらの各段階で取りうるバリエーション数の積が最終的な回答バリエーション数になる．この 2 段階のうち後者の 2 段階目の計算については，配置領域が「全域」の場合の計算と同様であり，部分小領域が 5 行 4 列であることから $n=20$ になるだけである．したがって回答順序が「あり」の場合，2 段階目の回答バリエーション数は ${}_{20}P_4$ であり，回答順序が検証対象外の場合は ${}_{20}C_4$ となる．

次に 1 段階目の回答バリエーション数について説明する．この数はパス画像のレイアウト状況に依存し，本節でおいた前提条件では 5 種類の値を取りうる．この理由について説明する．

パス画像の部分小領域への配置はランダムである．この配置を「パス画像を 5 行 4 列の部分小領域のうち，何行の列にわたって配置されたか？」という観点で考えると 5 通りのパターンがありうることになる．1 行内に 4 つのパス画像すべてが配置される場合から，4 つのパス画像が 5 行に分散して配置されることもありうるからである (**図 5**)．

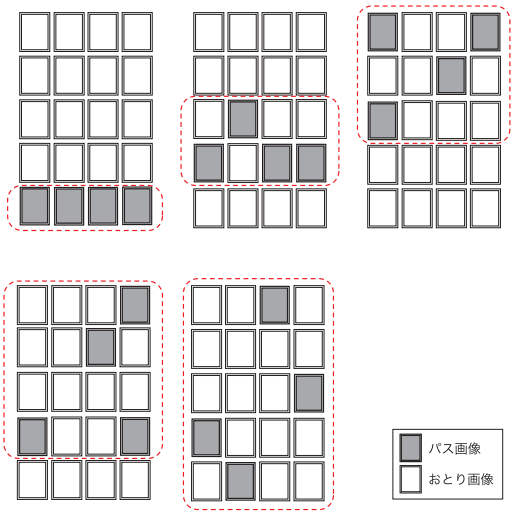


**図 5**　部分小領域へのパス画像の配置方法 (5 パターン)

この「パス画像が配置された領域」が完全に含まれるように部分領域を決定する方法が何通りあるかを考えると，(1,2,3,4,5) の 5 通りになる．

- 最小：1 通り
  (パス画像が 5 行にわたって配置された場合)
- 最大；5 通り
  (パス画像 4 枚すべてが 1 行に配置された場合)

**図 6** は，パス画像が 3 行にわたって配置された場合に，部分小領域の取りうる方法は 3 通りあることを示している．

一方，画像グリッドの全領域から部分小領域を選択する方法が何通りありうるかは列数が 4 で同一であることから，両者の行数がわかれば求められる．$n=100$ の場合，全域は 25 行で部分小領域は 5 行なので 21 通り，$n=52$ の場合，全域は 13 行なので 9 通りとなる．このバリエーション数を $p$ とすると，これまでの議論から 1 段階目の回答バリエーションは，$(\frac{p}{5},\frac{p}{4},\frac{p}{3},\frac{p}{2},\frac{p}{1})$ の 5 通りとなる．これゆえ表 2 において配置領域が “部分領域” である場合の回答バ

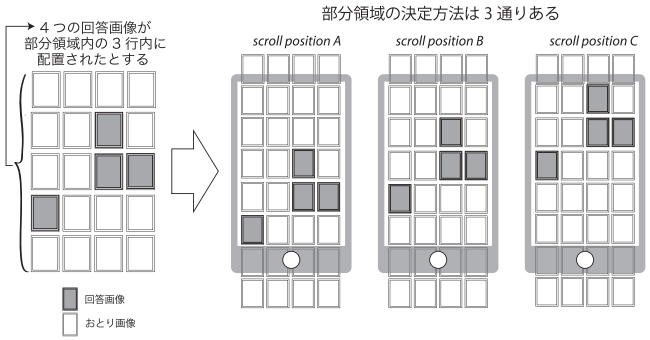


**図 6**　パス画像配置のための部分小領域の決定法

リエーション数は値に幅がある表記となっている．

これらの結果から提案手法における３設定要素でそれぞれ２条件を決定して運用すると，以下の値域にわたる安全性を１つの秘密情報で，かつ１つの認証手法で提供することが可能となる．

$$\frac{1}{8,721} \leq Security\ level \leq \frac{1}{94,109,400} \qquad (2)$$

### 4.2　利便性へのインパクト

本研究で提案した再認式画像認証は，(回答候補画像の枚数，パス画像の配置領域，パス画像の回答順序) という３つの設定要素を可変にすることで提供しうる安全性を柔軟に変更可能にした．重要なことは，この利点を１つの秘密情報で，かつ１つの認証手法として実現している点にある．

秘密情報は「回答順序付きの画像 4 枚」だけであり．認証システムにおける安全性の変更により秘密情報が変更されたり，追加されることはない．これは安全性向上に対する利用者の秘密情報維持負担の増加抑制に寄与すると言える．言い方を変えると，安全性の高い個人認証の導入に対する心理的障壁を下げる効果が期待できるとも言える．

また提案手法は認証手法としては再認式画像認証という１つの手法であり，その操作方法は提供しうる安全性の値を問わず同一操作である．また携帯端末におけるアルバムアプリの設計条件をユーザインタフェースとして取り入れているため，当該アプリのユーザであれば，違和感なく提案手法を利用可能であると考えている．また再認識画像認証の仕組みは単純であり，その理解に対する学習負担も低いと考える．これらの特徴も，前述同様，安全性の高い個人認証の導入に対する心理的障壁を下げる効果につながりうると考えている．

認証操作時間については，表 2 における条件 g,h と条件 d(厳密には条件に若干の違い (回答候補画像数 50≠52) がある) の 3 条件による測定を行った．その結果，条件 d,g については平均で 12 秒以下，早い場合には 5 秒前後で認証操作を完了することが可能であることが示された．これらの条件については，日常生活で利用する個人認証として，暗証番号認証よりも安全性が高く，利用者負担の増加が抑制された個人認証として受容されうると考えている．条件 h においては，平均で 26 秒となった．この操作時間では，日常生活での使用は現実的ではないと見るべきだろう．しかし，求められる安全性は高いが，その利用頻度は低いという認証シーンがあれば，この結果でも受容される可能性はあると考えている．

認証操作時間としては上記の評価となるが，ここで注意して欲しいのは，今回評価した条件はすべて「回答順序あり」条件であり，また 3 条件のうち 2 条件はパス画像の配置領域が「全域」である．これらの条件設定は，各設定要素において利用者への負担が大きいと推測される条件である．したがって他の条件では，今回の認証操作時間よりも短縮される可能性があることを指摘しておく．

### 4.3　利用状況に応じて対応可能な “柔軟な個人認証” へ

利用状況に応じたアクセス制御や個人認証が必要とされている．利用者視点では，利用する IT システムのサービス内容に応じて安全性を柔軟に設定したいという要望があることは 1 章で述べた．攻撃防御の視点ではリスクベース認証を例に挙げた．携帯端末のセンサー値などコンテキスト情報を用いて “正規利用者らしさ” を算出し，その値に応じて必要な検証レベルを柔軟に変更する個人認証である．この方法により，正規利用者を受け入れつつも，攻撃者による不正行為を困難にする認証手法である．

これらのアイデアは「利用状況に応じて正規利用者であることの検証レベルを動的に変更する」ということである．ただしそのレベルの変更方法に議論が偏っており，実際にどういう検証手法を利用するかについては 1 章で述べた２つのアプローチのどちらかの適用するにとどまっている．これらのアプローチによる手法は，安全性向上の代償として利用者への負担を増大させるため，検証レベルの動的変更による手法を利用することに対する障壁になっていると考える．

ここで考えたいのは，利用状況やサービス内容に応じてセキュリティレベルを変更するのは，攻撃者による悪用を困難にするためである．そのために検証レベルの高い個人認証をシステムに適用し，それに付随する負担を攻撃者に負わすことについては異論がないだろう．しかし，正規利用者にもその負担を負わせることは望ましいことではない．つまり本来あるべき理想は，攻撃者が攻撃を成功させるために必要なコストを高くしつつも，それにおける正規利用者の負担は不変であるか必要最小限の負担増になっていることである．この点から「複数の認証システムを併用する」も「秘密情報の情報量を増やす」の２つのアプローチを見ると，どちらも攻撃者と正規利用者の双方に負担を負わすことで攻撃成功率を低くするものであり，理想的な対策とは言い難い．

これに対して提案手法は，提供しうる安全性の変更を可能にしつつ，秘密情報の記憶負担や操作負担は低く抑制さ

れたシステムとなっている．一方，攻撃者に対しては安全性向上にともない回答選択肢が増えるため，パス画像の特定や推測に対する負担は増えることとなる．これらのことから，提案手法は上記の理想に近い個人認証システムであると考える．

またこれらの利点を備えた個人認証が，１つの個人認証手法として実現されていることによる利点も２つある．１つは，導入にかかるコストが低い点である．再認式画像認証の仕組みはシンプルでありその理解は容易である．また，安全性の改良によって秘密情報や認証操作は変化しないため，安全性を向上した個人認証を利用させる際に学習コストも発生しない．見た目上変更されるのは，認証回答時に提示される画像グリッドの大きさだけである．

もう１つは継続利用可能性である．利用状況に応じて認証手法が切り替わると仮定すると，複数の個人認証手法において利用頻度の低い個人認証が発生する．利用頻度が低くなると，結果として当該認証手法の操作方法や秘密情報を忘却する恐れが出てくる．つまり，いざ必要な場面になった時，正規利用者もシステムやサービスを利用できないことになる．よって既存のリスクベース認証では，そういった懸念によって可用性が損なわれることを回避するため，所有物や生体情報による認証，または One-time password などで追加認証を行っている．しかし，これらの手法は専用機器や秘密情報の常時保持や認証手法の習得といった負担が増えることは避けられない．これに対して提案手法は，検証する安全レベルにかかわらず，秘密情報も操作方法も同一であり，変更はない．つまり検証レベルの高い個人認証が使用される頻度が低いとしても，検証レベルの低い状態で日常的に利用していれば，秘密情報や操作方法の忘却は発生する可能性はないと言える．結果として可用性が損なわれる可能性が低い，つまり継続利用可能性の高い個人認証であると言える．

## 5. おわりに

本研究では，提供する安全性を柔軟に変更可能な個人認証を提案した．安全性を変更するためには，(1) 秘密情報を変更または追加する．または (2) 複数の認証手法を組み合わせる，のどちらかの方法が主に用いられている．しかしこれらのアプローチは，安全性向上を可能にする一方で，秘密情報保持や認証操作に関する負担を増加させるものであり，利用者にとっては受容しがたい改良方法であると言える．

そこで本研究では画像の多様性を応用し，回答選択肢のうち秘密情報ではない “おとり画像” の数を増やすことにより，利用者に対する負担増加を必要最小限に抑制しつつ，安全性の向上を可能にする個人認証手法を再認式画像認証として実現した．１つの秘密情報で，かつ１つの個人認証手法でありながらも，それが提供する安全性を柔軟に変更可能にする手法は，上記の２つのアプローチとは異なる新たな改良手法の提案になると考えている．また提案手法の秘密情報と操作方法は，安全性の改良前と改良後で変化せず同一であるため，安全性の高い個人認証を利用者が必要としたとき，その導入/利用に対する負担および心理的障壁が低い手法であるとも言える．この利点は，利用状況やサービス内容に応じて本人確認における検証レベルを柔軟に変更する上で有益であり，その実現に資する手法であると考えている．

本論文では被験者による評価実験を 3 条件のみでしか行っていないが，今後は未評価の各条件でも評価を行い，各設計条件における認証操作時間，すなわち利便性についての影響を明らかにしていく予定である．またあわせ絵 [8] の「パス画像なし」回答や，SWIPASS[7] の「Fake image」やスワイプ操作など，利便性に影響を与えずに安全性をより柔軟に変更可能にする設計要素の追加を検討していく予定である．

**謝辞**　評価実験に協力頂いた学生諸氏に感謝する．また貴重な余暇の時間を割いてシステム実装に尽力いただいた第二著者の森氏に感謝する．

### 参考文献

[1] 森康洋，高田哲司：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，コンピュータセキュリティシンポジウム (CSS’ 15), pp.787-794, (2015).

[2] 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, In Proc. of the 8th Symp. on Usable Privacy and Security (SOUPS ’12), (2012).

[3] 今澤貴夫，小池英樹，高田哲司：GPS データを用いた位置認証システムとその停留点算出方式, コンピュータセキュリティシンポジウム（CSS ’08），(2008).

[4] R., Oriana, Qin, C., Strauss, K., and Lymberopoulos, D.: Progressive authentication: deciding when to authenticate on mobile phones, Proc. of the 21st USENIX Security Symposium, pp.301-316, (2012).

[5] D., Davis, F., Monrose, and M. K. Reiter, On User Choice in Graphical Password Schemes, 13th USENIX Security Symposium, (2004).

[6] R., Dhamija, and A., Perrig, and M. K. Reiter, Déjà Vu: A User Study Using Images for Authentication, 9th USENIX Security Symposium, (2000).

[7] Kosugi, M., Suzuki, T., Uchida, O., and Kikuchi, H.: SWIPASS: Image-Based User Authentication for Touch Screen Devices, Journal of Information Processing, Vol.24, No.2, pp.27-236, (2016).

[8] Takada, T., and Koike, H.: Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images, Int’l Conf. on Mobile Human-Computer Interaction (MobileHCI ’03), (2003).

[9] (株) シマンテック，「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⟩ (2016.08.10).