Vol.2019-GN-108 No.15
Vol.2019-SPT-33 No.15
2019/5/10

Cognometric方式画像認証のユーザ設定に関する調査

石井 健太郎[1,a)]

概要：本研究では，ワンタイム図形生成に基づく Cognometric 方式の画像認証手法を提案している．提案手法では，正規のユーザが知る認証図形群生成ルールに基づいて，ワンタイムの正解図形とダミー図形を生成して画面に提示する．被認証者は，提示された図形群の中から正解図形を選ぶことによって認証を受ける．画面には都度生成された図形が提示されるため，ショルダーハッキングが行われた場合であっても正解の手がかりをつかみにくいことが期待できる．まず提案手法の基本手法について，1 名の実験参加者が認証を受けている場面をもう 1 名の実験参加者がショルダーハッキングを行う評価実験を行ったところ，ショルダーハッキングを認めているにも関わらず，多くの認証図形群生成ルールにおいて高い本人パス率と他者拒否率を示した．一方で，同じルールカテゴリのルールを体験したことがある実験参加者は，未体験の実験参加者に比べて非正規に認証を受けられることが示された．そこで，この課題への対策として発展的手法を導入し，その設定についてのユーザの好みを探るべくユーザスタディを行った．

Study on User Preferences of Cognometric Image-based Authentication

1. はじめに

通常のパスワード/パスコード認証やスマートフォンで見られるパターンロック認証では，何らかの方法で他者がパスワード/パスコードやパターンを取得すると，不正認証を受けることができてしまう．また，これらの認証手法では，入力の位置からパスワード/パスコードやパターンを推測することが可能であり，認証場面のショルダーハッキングにより他者が不正認証を受けるための情報を取得することが容易である．

本研究では，この問題の低減を目指して，ワンタイム図形生成に基づく Cognometric 方式の画像認証手法を提案している [1]．認証時には都度生成された図形が提示されることが提案手法の特徴であり，ショルダーハッキングが行われても，他者が次に認証を受けるときには異なる図形が提示されるため，正解の手がかりをつかみにくいことが期待できる．提案手法では，あらかじめ決められた認証図形群生成ルールに基づいて，ワンタイムの正解図形とダミー図形を生成して画面に提示する．認証図形群生成ルールを知る被認証者は，都度生成された図形であっても正解図形を選ぶことができる．

本論文では，まず先行研究 [1] で提案した基本手法について，ショルダーハッキングへの耐性を調べる評価実験の手順と結果をまとめる．また，先行研究 [1] の発展的手法についても，どのような設定をユーザが好むかを調査するためのユーザスタディを行う．

2. 関連研究

通常のパスワード認証のような文字の記憶と比較して，人間の画像再認能力は高いとされており，このことを利用した画像認証手法は記憶負荷が通常のパスワード認証手法よりも低いと考えられている．本研究でも用いている画像そのものを選択する Cognometric 方式の画像認証としては，Déjà Vu が提案されている [2]．Déjà Vu では，コンピュータで生成した画像から 5 枚の正解画像をあらかじめ決めておき，認証は 25 枚の提示画像の中から 5 枚の正解画像を選択することによって行う．しかし，ユーザとは無関係で意味のない画像を用いているため，記憶負荷低減の効果が限定的である可能性がある．

そこで，ユーザが自身で正解画像とダミー画像を登録・追加できる仕組みも提案されている．あわせ絵 [3], [4] は，そのような仕組みを持つ認証システムであり，個人のエピソードに基づく再認しやすい画像を認証に用いることができる．また，ダミー画像の登録を検索エンジンの画像検索

[1] 専修大学
Senshu University, Kawasaki, Kanagawa 214–8580, Japan
[a)] kenta@pc.fm.senshu-u.ac.jp

Vol.2019-GN-108 No.15
Vol.2019-SPT-33 No.15
2019/5/10

を用いることによって自動化することで，正解画像の登録のみを必要とする画像なぞなぞ認証も提案されている [5]．

しかし，以上までの手法は，提示されている画像が正解画像そのものであるため，ショルダーハッキングが行われてしまうと，他者が不正に認証を受けることが容易である．本研究は，Cognometric 方式の画像認証においてもショルダーハッキングによる不正認証を防ぐ手法を扱う．

Cognometric 方式の画像認証においては，正解画像そのものではなく不鮮明化した画像をチャレンジ画像として提示することで，ショルダーハッキングの影響を低減する手法が提案されている [6]．元画像を知らない他者には，チャレンジ画像を見ても元画像を特定することが難しい．しかし，この方式は元画像を特定されなくても，困難ではあるが不鮮明化画像からレスポンスが推定できてしまう可能性が指摘されている [7]．これに対して，この手法を Locimetric 方式の画像認証に応用して，同じチャレンジ画像に対して，指定の部位を変化させることで異なるレスポンスを生成させる手法も提案されている [7], [8]．本研究は，毎回異なるチャレンジ画像が提示される点において前者の提案と異なる．また，本研究の提案手法では画像そのものを選択する Cognometric 方式を用いており，そのために Locimetric 方式よりも認証時のレスポンス生成が容易であることが期待できる点で後者の提案と異なる．

3. ワンタイム図形認証の基本手法

本節では，提案手法であるワンタイム図形生成に基づく画像認証手法のうち，基本手法の概要を述べる[*1]．

3.1 図形生成基本アルゴリズム

提案手法で生成されるワンタイム図形は，正解図形もダミー図形も本節で述べる図形生成基本アルゴリズムによって生成される．**図 1** は，この図形生成基本アルゴリズムによって生成された 9 つの図形の例を示している．図形生成基本アルゴリズムは，Miyashita らの図形生成手法 [9] を参考にしてアレンジしたものである．

図形生成基本アルゴリズムの手続きを以下に示す．いずれの操作もランダムに選ばれるパラメータがあり，それにより毎回異なる図形が生成される．

(1) ランダムな数の頂点を持つ正多角形を用意する．
(2) 隣接した頂点を結んだ線分の中点に新しい頂点を作成し，図形の中心から新しい頂点までの距離が増加または減少するように，新しい頂点をランダムな距離だけ移動させる．（**図 2**; 各頂点の移動距離は同一である．）
(3) (2) をランダムな回数繰り返す．
(4) (3) までの操作で生成された多角形をランダムな色で塗りつぶす．

[*1] 詳細については，先行研究 [1] を参照のこと．

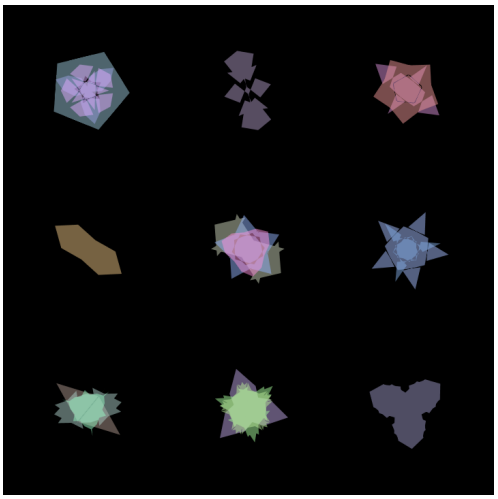


図 1 図形生成基本アルゴリズムによって生成された図形
Fig. 1 Shape patterns generated by the basic algorithm.

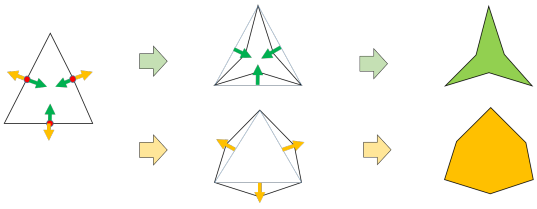


図 2 中点の移動による変形
Fig. 2 Edge middle point deformation.

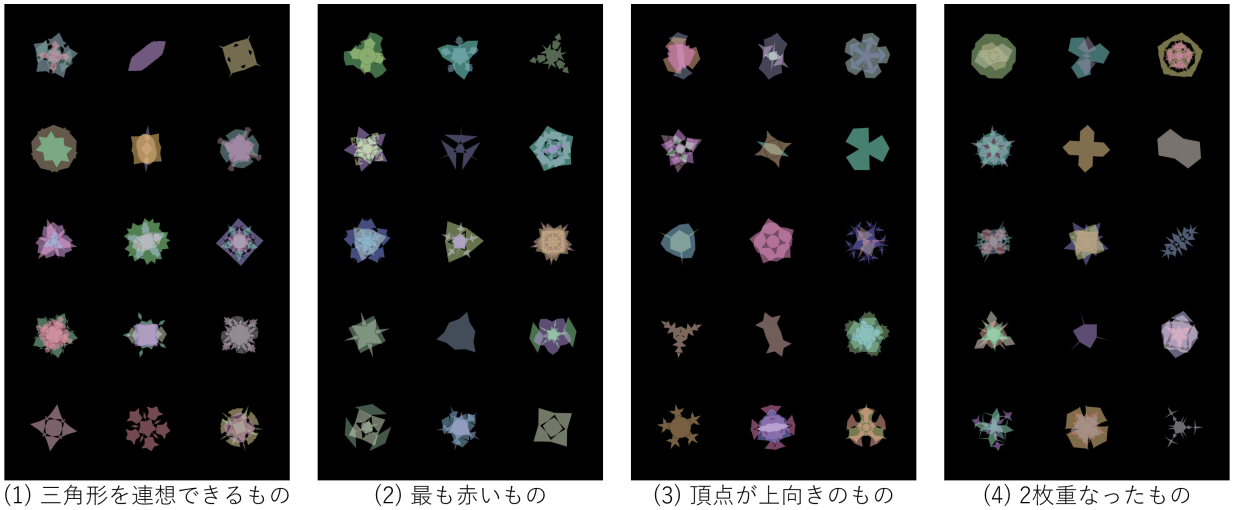
(5) 図形の中心を軸にランダムな角度だけ回転させる．
(6) (5) までの操作で生成された図形を一定の透明度でランダムな枚数だけ重ね合わせる．

3.2 認証図形群生成ルールと正解図形・ダミー図形の生成

図形生成基本アルゴリズムをもとにして，正解図形とダミー図形の組み合わせを生成する認証図形群生成ルールを定義する．ここで言う正解図形とは被認証者が認証時に選ぶべき図形であり，ダミー図形とは認証時に選ばざるべき図形である．したがって，認証図形群生成ルールが持つべき特徴として，ルールを知る者には正解図形をダミー図形から見分けることができることと，ルールを知らない者には正解図形からルールを推測できないことの 2 つがある．後者の特徴は，正解図形を選択する場面をのぞき見られても，他者が認証を受けることを防ぐために必要となる．

本研究では，認証図形群生成ルールは，3.1 節の図形生成基本アルゴリズムのパラメータを制限することで定義する．例えば，図形生成基本アルゴリズムではランダムであった初期多角形の頂点の数のパラメータを，正解図形の場合は 3 に固定し，ダミー図形の場合は 3 以外のランダムとすることによって認証図形群生成ルールを定義する．この方法によれば，原理的には図形生成のランダムパラメータが重複しない範囲で認証図形群生成ルールを定義することができる．図形生成基本アルゴリズムのランダムパラメータ

Vol.2019-GN-108 No.15
Vol.2019-SPT-33 No.15
2019/5/10



(1) 三角形を連想できるもの　(2) 最も赤いもの　(3) 頂点が上向きのもの　(4) 2枚重なったもの

図 3 4 つのカテゴリそれぞれの認証図形群生成ルールによって生成された図形群と直感的なルールの解釈．図形群は 1 つの正解図形と 14 のダミー図形を含む．図形生成基本アルゴリズムを知らなくても，直感的なルールの解釈のみで正解図形を見分けられる．また，ルールによる図形群の大きな差異はない．

Fig. 3 Shape patterns generated by the generation rules and interpretations of the generation rules. Each set of shape patterns includes one correct answer and 14 dummy answers. Users do not necessarily need to know the basic generation algorithm. There is no big difference among the sets of shape patterns.

は，初期多角形の頂点の数・頂点追加時の移動距離・頂点追加の回数・色・回転角度・図形の重ね合わせ枚数の 6 つである．

検討の結果 [1]，初期多角形の頂点の数・色・回転角度・図形の重ね合わせ枚数の 4 つを認証図形群生成ルールの定義に用いることとした．用いるランダムパラメータによってカテゴリ分けすると，以下のような 4 つのカテゴリのルールを定義でき，それぞれのパラメータの特徴により，合計 12 の認証図形群生成ルールを定義できる．**図 3** に，4 つのカテゴリから 1 つずつ代表して，認証図形群生成ルールにより生成された図形群を示す．

カテゴリ 1　正解 : 初期多角形の頂点の数が n，ダミー : 初期多角形の頂点の数が n 以外，ルールは 4 種類あり n は $\{2, 3, 4, 5\}$ のいずれかをとる

カテゴリ 2　正解 : RGB 色空間の要素のうち c が最も大きい，ダミー : RGB 色空間の要素のうち c 以外が最も大きい，ルールは 3 種類あり c は $\{R, G, B\}$ のいずれかをとる

カテゴリ 3　正解 : 回転角度が θ，ダミー : 図形の回転角度が θ 以外，ルールは 2 種類あり θ は $\{\pi/2, 3\pi/2\}$ のいずれかをとる（画面座標系の偏角の定義により $\theta = \pi/2$ は下向き・$\theta = 3\pi/2$ は上向きとなる）

カテゴリ 4　正解 : 図形の重ね合わせ枚数が n，ダミー : 図形の重ね合わせ枚数が n 以外，ルールは 3 種類あり n は $\{1, 2, 3\}$ のいずれかをとる

直感的には，以上のルールによって生成される正解画像は，以下のように解釈できる．したがって，これは重要なことであると考えるが，プログラムの内部構造やパラメータの種類を知らないユーザでもルールを把握することができる．また，カテゴリやルールによる認証図形群の大きな差異はない（図 3）．

カテゴリ 1　{ 二角形, 三角形, 四角形, 五角形 } を連想できるもの（ただし，二角形は便宜的な呼びかたであり線分を意味する）

カテゴリ 2　最も { 赤い, 緑の, 青い } もの

カテゴリ 3　頂点が { 下向き, 上向き } のもの

カテゴリ 4　多角形が { 1 枚, 2 枚, 3 枚 } 重なったもの

4. 基本手法の評価

3.2 節の認証図形群生成ルールを組み込み，認証のユーザインタフェースを追加した認証アプリケーションを，Android スマートフォンに実装して評価実験を行う．このアプリケーションでは，画面上に 15 の図形が提示され，被認証者がそれらのうちの 1 つを選択するのを待ち受ける．図形の選択を行うと，画面が切り替わり別の 15 の図形が提示される．このプロセスを 4 回繰り返すと終了するようなアプリケーションである．各画面では，認証図形群生成ルールに基づいて生成された 1 つの正解図形と 14 のダミー図形が含まれており，すべての画面で正解図形を選択できれば認証される．

表 1　ルールごとの認証成功率 (%)
Table 1　Authencication rates for each generation rule.

	二角形	三角形	四角形	五角形	赤い	緑の	青い	下向き	上向き	1 枚	2 枚	3 枚	全体
正規	100.0	88.9	100.0	100.0	94.4	94.4	94.4	98.1	94.4	94.4	72.2	83.3	92.8
非正規	25.9	37.0	22.2	11.1	5.6	16.7	5.6	11.1	7.4	33.3	22.2	22.2	17.1

表 2　ルールごとの正答率 (%)
Table 2　Correct answer rates for each generation rule.

	二角形	三角形	四角形	五角形	赤い	緑の	青い	下向き	上向き	1 枚	2 枚	3 枚	全体
正規	100.0	96.3	100.0	100.0	97.2	98.6	98.6	99.5	98.6	98.6	93.1	94.4	98.0
非正規	44.4	50.0	30.6	38.9	21.5	34.7	27.1	21.3	21.8	48.6	41.7	30.6	32.6

4.1　実験手順

実験は 2 名 1 組の実験参加者を招いて行う．1 名の実験参加者が正規の被認証者役となり，もう 1 名の実験参加者はショルダーハッキングを行う非正規の被認証者役となる．

認証図形群生成ルールを変えて 6 セッションの評価を繰り返すこととし，2 名の実験参加者を A,B とすると，A → A → B → B → A → B の順で正規の被認証者役を行い，もう一方が非正規の被認証者の役を行うというように，実験の最中に正規・非正規の役割は交代して実験を行う．この順序としたのは，最初の 2 セッション・中間の 2 セッション・最後の 2 セッションについて，本認証システムの事前知識に関して異なる条件でのデータを取得するためである．

最初の 2 セッションでは，非正規の役割である B は，認証システムを利用したことがない状態でショルダーハッキングを行う．このとき，認証システムが認証図形群生成ルールに基づいて動作していること，あるいは，ルールが存在することも知らされない．

中間の 2 セッションでは，非正規の役割である A は，最初の 2 セッションで正規の役割を行う際に，認証システムが認証図形群生成ルールに基づいて動作していることを知らされるため，この中間の 2 セッションも何らかのルールに基づいて動作していることを知った状態でショルダーハッキングを行う．ただし，最初の 2 セッションと中間の 2 セッションで用いられるルールのカテゴリは異なるものを適用する．

最後の 2 セッションでは，非正規の役割である A または B は，これまでのセッションで認証システムが認証図形群生成ルールに基づいていることを知るとともに，自分が正規の被認証者として体験したルールと同じカテゴリでありパラメータは異なるルールのショルダーハッキングを行う．したがって，似たようなルールを体験済みの状態でショルダーハッキングを行うこととなる．

以上をまとめると，順に認証システム未体験/ルールがあることも知らされていない・認証システム体験済み/当該ルールカテゴリ未体験・認証システム体験済み/当該ルールカテゴリ体験済みの 3 つの条件を比較できるデータを取得することを意図している．以下では，それぞれ「システム未体験」条件・「ルールカテゴリ未体験」条件・「ルールカテゴリ体験済み」条件と呼び，この要因のことを「事前知識条件」と呼ぶこととする．

3.2 節で述べたどのカテゴリ・パラメータをどの順番で実験参加者に割り振るかは，実験参加者ごとにカウンターバランスをとって実施する．以下では，正規の被認証者役の実験参加者を「実験参加者（正)」・非正規の被認証者役の実験参加者を「実験参加者（非）」と呼ぶこととする．

各セッションについては，以下の手続きで実験を実施する．したがって，実験全体としては，以下の手続きを 6 回繰り返すこととなる．

(1) 実験者は実験参加者（正）へ認証図形群生成ルールを提示する．この際に，パラメータの説明は行わず，3.2 節で述べた直感的な説明のみを行う．
(2) 実験参加者（正）は認証アプリケーション利用の練習を 6 回行う．
(3) 実験参加者（正）は認証アプリケーション利用のテストを 3 回行う．その間，実験参加者（非）は実験参加者（正）のそばでショルダーハッキングを行う．
(4) 実験参加者（正）の 3 回のテストの終了後，実験参加者（非）は認証アプリケーション利用のテストを 3 回行う．

4.2　結果とデータ分析

26 組 52 名の実験参加者を招き実験を実施した．ただし，色覚異常を持つために実験を途中で中止したい旨を申し出た実験参加者が 2 名おり，その実験参加者が含まれる 2 組の中途データは除外した 24 組 48 名のデータを評価の対象とした．

評価対象の 48 名すべてにおいて，実験参加者（正）を 3 セッション・実験参加者（非）を 3 セッション行っているため，全体としては実験参加者（正）のデータを 144 セッション分・実験参加者（非）のデータを 144 セッション分取得した．実験参加者（正）も実験参加者（非）も，1 セッションあたり 3 回の認証試行を行い，1 回の認証試行につ

表 3　事前知識条件ごとの認証成功率 (%)
Table 3　Authencication rates for each experience condition.

	システム未体験	ルールカテゴリ未体験	ルールカテゴリ体験済み	全体
正規	92.4	93.8	92.4	92.8
非正規	11.8	13.9	25.7	17.1

表 4　事前知識条件ごとの正答率 (%)
Table 4　Correct answer rates for each experience condition.

	システム未体験	ルールカテゴリ未体験	ルールカテゴリ体験済み	全体
正規	97.6	98.4	98.1	98.0
非正規	28.8	25.2	43.9	32.6

き 4 回の正解図形の解答試行を行うため，全体としては，144 セッション・432 認証試行・1728 解答試行のデータを，実験参加者（正）と実験参加者（非）の両方について取得したこととなる．ルールカテゴリはカウンターバランスをとって均等に配分したため，4 つのカテゴリそれぞれについて，36 セッション・108 認証試行・432 解答試行のデータを取得した．ルールカテゴリによって，とりうるパラメータの数は異なりルールの数も異なるため，カテゴリ 1 の初期多角形ルールは，それぞれ 9 セッション・27 認証試行・108 解答試行のデータを取得し，カテゴリ 2 の色空間ルールとカテゴリ 4 の重ね合わせ枚数ルールは，それぞれ 12 セッション・36 認証試行・144 解答試行のデータを取得し，カテゴリ 3 の回転角度ルールは，それぞれ 18 セッション・54 認証試行・216 認証試行のデータを取得した．事前知識条件別には，3 条件それぞれについて，48 セッション・144 認証試行・576 解答試行のデータを取得した．

4.2.1　認証成功率・正答率

まず，**表 1** に，ルールごとの認証成功率として認証試行に対して成功した割合を示す．どのルールもおおむね似たような傾向を示しており，ショルダーハッキングを自由に許しているにもかかわらず，実験参加者（正）と実験参加者（非）の認証成功率は大きく異なっていた．全体として見れば，3 度連続でショルダーハッキングが行われることは，通常利用よりも正規の被認証者に厳しい条件であると考えられ，その条件下で実験参加者（正）と実験参加者（非）の認証成功率が大きく異なっていることは，提案手法が一定の効果を上げていることを示していると言える．

ルールを個別に見ると，実験参加者（正）に関しては，カテゴリ 4 の重ね合わせ枚数ルールの 2 枚と 3 枚において，ほかと比べて低い認証成功率であった．このことは，2 枚重ね合わせと 3 枚重ね合わせの認証図形群生成ルールが，やや本人にも解きにくいルールであることを示唆している．実験参加者（非）に関しては，カテゴリ 1 の初期多角形ルールの三角形とカテゴリ 4 の重ね合わせ枚数ルールの 1 枚において，ほかと比べて高い認証成功率であった．このことは，初期多角形が三角形と 1 枚重ね合わせの認証図形群生成ルールが，やや盗まれやすいルールであることを示唆している．

以上についてより詳細に調べるため，ルールごとの正答率として解答試行に対して正解した割合を検討する．**表 2** に示すとおり，100.0%である場合を除き，正答率は認証成功率よりも高い値となっているが，これは認証成功が 4 回の正答の AND 条件となっているためであり，すべての認証試行ですべて正答かすべて誤答でない限りは原理的にそのようになる．このようにしてみると，初期多角形が三角形と 1 枚重ね合わせの認証図形群生成ルールは，依然としてほかと比較して高い値であるが，その差は認証成功率ほど大きくない．無作為に選んだ場合に偶然正解してしまう確率は 1/15 であるので，正答率のチャンスレベルは 6.7%である．実験参加者（非）の正答率がチャンスレベル 6.7%と同等であるかの二項検定を行ったところ，いずれのルールもチャンスレベルとは有意差が認められた ($p < 0.01, g = 0.146 \sim 0.433$)．この結果は，統計的には実験参加者（非）があてずっぽうで回答していたのとは異なることを意味している．したがって，ルールによって程度の差はあるが，実験参加者（正）の解答試行から，ルールを認識できなかった認証試行においても実験参加者（非）がルールの可能性を絞り込めていることがわかる．

次に，**表 3** に，事前知識条件ごとの認証成功率を示す．実験参加者（正）に関しては，事前知識条件によらず同様にルールの直感的解釈を教示されるため，事前知識条件間に差はない．実験参加者（非）に関しては，システム未体験条件・ルールカテゴリ未体験条件よりも，ルールカテゴリ体験済み条件のほうが認証成功率が高くなった．カイ二乗検定を行ったところ，条件間の認証成功率に有意差が認められた ($p < 0.01, V = 0.162$)．このことは，提案手法においては，同様のルールを体験したことのあるショルダーハッカーは，認証図形群生成ルールを認識しやすいことを示している．**表 4** に示す事前知識条件ごとの正答率においても，同様の結果が得られている．カイ二乗検定を行ったところ，条件間の正答率に有意差が認められた ($p < 0.01, V = 0.173$)．

表 5　ルールごとの平均解答時間 (msec.)
Table 5　Average answer times for each generation rule.

	二角形	三角形	四角形	五角形	赤い	緑の	青い	下向き	上向き	1 枚	2 枚	3 枚	全体
正規	4109	5228	14995	6047	2939	4172	10879	6153	5079	3219	8431	9677	6535
非正規	9729	8577	10150	3605	7349	8548	9904	7029	10082	5975	16647	9339	8956

表 6　事前知識条件ごとの平均解答時間 (msec.)
Table 6　Average answer times for each experience condition.

	システム未体験	ルールカテゴリ未体験	ルールカテゴリ体験済み	全体
正規	6196	5629	7779	6535
非正規	8206	8800	9862	8956

4.2.2　解答時間

まず，**表 5** に，ルールごとの平均解答時間として認証図形群が提示されてからタップを行うまでにかかった時間の平均を示す．全体としては，実験参加者（正）のほうが実験参加者（非）よりも短い時間で回答している傾向が見られる．実験参加者（正）は認証を解くためのルールを知っているのであるから，解答時間が短くなることは理にかなっているが，それほど大きい差ではないことがわかる．

ルールを個別に見ると，二角形・赤い・緑の・1 枚といったルールで，実験参加者（正）が比較的すばやく回答しているが，全体的にばらつきが多く，平均するとそれほど差異がないと見受けられる．特に，カテゴリ 2 の色空間ルールにおいて，ルールを定義した際 [1] には，ほかのカテゴリに比べてすばやく回答できるであろうことを検討したが，青いのルールにおいてはそうではないことが示されている．一方で，カテゴリ内で比較すると，二角形や 1 枚のルールは，同じカテゴリのほかのルールと比べると単純な図形になることから，すばやく見分けやすいことが予想でき，その結果が現れているものと考える．

次に，**表 6** に，事前知識条件ごとの平均解答時間を示す．実験参加者（正）に・実験参加者（非）ともに，事前知識条件によって解答時間はあまり変化しておらず，事前知識よりもどの認証図形群生成ルールが用いられているかが解答時間に影響しやすいことを示唆している．

5.　ワンタイム図形認証の発展的手法

同じルールカテゴリのルールを体験したことがある実験参加者は，未体験の実験参加者に比べて非正規に認証を受けられることが基本手法の評価実験では示され，どのようなルールがあるかを知っているショルダーハッカーにどう対応するかという課題が明らかになった．このことに対しては，基本手法だけでは限界があり，対策が必要である．本節では，4 回のチャレンジにより認証されるプロセスにおいて，異なる認証図形群生成ルールを切り替えて用いる発展的手法を導入する [1]．

5.1　複数ルールの切り替え

ショルダーハッキングを行う者はどのルールが適用されているかを類推していることが考えられるため，ルールが認証プロセス中に切り替わることによってショルダーハッキングを行っている者の思考をそらすことができると考える．最も単純には，4 度の図形の選択における何度目の選択であるかによって適用するルールを決めておくことである．1 度目と 3 度目はルール A に基づき，2 度目と 4 度目はルール B に基づくというようにしてもよいし，4 度とも異なるルールを適用してもよい．また，ある認証プロセスにおいてルール A →ルール B →ルール C →ルール A と適用した場合は，次の認証プロセスにおいてはルール B →ルール C →ルール A →ルール B というように，順送りに繰り返すということも 1 つの手法として考えられる．この場合，認証に失敗することがあればルール A に戻るというような，ベースラインを担保する方法との併用も考慮する必要がある．

5.2　インラインルール通知

複数ルールの適用を事前に決められた順序で行うのではなく，ランダムに行うことも考えられる．その場合，何らかの方法で正規のユーザに適用されているルールを通知しなければならないが，これを提示されている図形によりインラインで行うことを考える．**図 4** は，インラインルール通知を実装した認証画面の例に説明を加えたものである．この例では，中央に提示された図形によってルールが通知される設定としており，そこに四角形を連想できる図形があることで，この画面の認証図形群生成ルールは四角形を連想できるものであることが通知される．

どの場所にルールが通知されるかは正規のユーザのみが知るとすると，非正規のユーザにはその図形がインラインルール通知であるのか，通常の正解図形・ダミー図形であるのかを見分けることは困難である．なお，図 4 の例では，ルール通知と適用されているルールの図形が同じであるが，適用されているルールとは異なるルールや異なるカテゴリの図形で通知することも可能である．

Vol.2019-GN-108 No.15
Vol.2019-SPT-33 No.15
2019/5/10

図 4　インラインルール通知

6. ユーザ設定に関する調査

正式な評価は未実施であるが，5 節で導入した発展的手法を採用すると，ルールを知るショルダーハッカーであっても，適用されているルールを絞り込むことができないことが観測されている．一方で，正規の被認証者が認証を受ける際も，発展的手法は基本手法よりも難しいことが観測されている．基本手法の場合であっても，正規の被認証者の 1 回の解答に平均 6.5 秒かかっていることから，すばやくあるいは繰り返し認証を行う場面には向いていないと言える．このことを考えると，正規の被認証者は正解できるが時間がかかる設定となっていると言うことができ，図形を並べる数をいくつにするかといったパラメータで難易度を調整する余地がある．ショルダーハッキングが行われても非正規に認証を受けることができないという性質を損なわない程度に，正規の被認証者にとって受けやすい認証の設定を探るべく，ユーザスタディを行った．

認証アプリケーションに，図形を並べる数・ルール切り替えの有無・ルール切り替えの方法・インラインルール通知の通知方法といった項目を設定できるカスタマイズ機能を追加し，ユーザに自由に設定変更を行ったうえで認証を試してもらう．ただし，必ず 1 度はすべての設定を試すことを指示する．ユーザスタディは，好みが固まるまで十分に設定変更と認証試行を繰り返したあと，質問紙調査によって，下記の設定のどれが好みであるかを回答してもらうという方法で行う．

質問 1　1 度に表示される図形は，{ 15 個, 9 個, 4 個, その他 } がよい

質問 2　ルールは，{ インラインルール通知, 単純ルール切り替え, ルール固定 } を利用したい

質問 3　インラインルール通知を利用するならば，{ 回答とは異なる, 回答と同じ } ルールで通知したい

なお，インラインルール通知を好まなかったユーザにも質問 3 を回答してもらう．

24 名の大学生を招きユーザスタディを実施した．質問 1 への回答は，15 個が 10 名・9 個が 11 名・4 個が 2 名・その他が 1 名であった．その他の回答者は毎回異なる数がよいと回答した．質問 2 への回答は，インラインルール通知が 11 名・単純ルール切り替えが 8 名・ルール固定が 5 名であった．質問 3 への回答は，回答とは異なるが 6 名・回答と同じが 18 名であった．質問 2 のインラインルール通知との回答者のみ集計すると，回答とは異なるが 3 名・回答と同じが 8 名であり，全体と同様の傾向であった．

これらの結果を考察すると，インラインルール通知にて回答と異なるルールで通知することは多くのユーザスタディ参加者が難しいと感じたようであるが，その他の設定は，どれか 1 つが決定的に好まれるというものはなく，ユーザによってばらつきがあることを示唆している．今回の調査だけでは，正規の被認証者が認証を受けやすい設定の結論を出すことはできないため，調査を精緻化して，引き続き取り組む予定である．

7. まとめ

本研究では，ショルダーハッキングによる他者の不正認証を低減するための手法であるワンタイム図形生成に基づく画像認証手法に関して，基本手法の評価実験によりショルダーハッキングを認めているにも関わらず高い本人パス率と他者拒否率を示すという提案手法の有効性を確認した．一方で，同じルールカテゴリのルールを体験したことがある実験参加者は，非正規に認証を受けやすいことも示され，このことへの対応として複数ルールを切り替えて用いる発展的に手法を導入した．さらに，解答にかかる時間は通常の認証方法よりも必要であり，ショルダーハッキングが行われても非正規に認証を受けることができないという性質を損なわない程度に，正規の被認証者にとって受けやすい認証の設定を探るべく，ユーザスタディを行った．

提案手法の利点を考えると，公共の場で周りに人が多い状況で個人認証が必要な場合に，通常の認証手法から切り替えて使用するというのが応用場面ではないかと考える．例えば，乗車率の高い電車やバスの中で，銀行口座の操作が必要なときに，本手法に切り替えて認証を行うというようなことである．現在の実装では，正規の被認証者は正解できるが時間がかかる設定となっていると言うことができ，今後も図形を並べる数や今回調査しなかった 1 認証試行あたりの解答試行数をいくつにするかといったパラメータを検討していく予定である．また，利用場面によって求められる難易度が異なることも考えられ，どのようなパラメータの値でどのような場面に適してくるかということも検討していく予定である．

参考文献

[1] 石井健太郎：ワンタイム図形生成に基づく画像認証手法，インタラクション 2019 論文集，pp.264–269（2019）．
[2] Dhamija, R., Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *USENIX Security Symposium* (2000).
[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*, pp.347–351 (2003).
[4] 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（2003）．
[5] 増井俊之：インターフェイスの街角 (49)—画像を使ったなぞなぞ認証，Unix Magazine, Vol.17, No.1（2002）．
[6] 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—手掛かりつき再認方式，情報処理学会研究報告，Vol.2006-CSEC-34，pp.411–418（2006）．
[7] 山本匠，漁田武雄，西垣正勝：不鮮明化画像を利用した暗示・応答型画像認証方式の提案，情報処理学会論文誌，Vol.50，No.9，pp.2062–2076（2009）．
[8] Yamamoto, T., Harada, A., Isarida, T., Nishigaki, M.: Advantages of User Authentication Using Unclear Images —Automatic Generation of Decoy Images—, *IEEE International Conference on Advanced Information Networking and Applications*, pp.668–674 (2009).
[9] Miyashita, Y., Higuchi, S., Sakai, K., Masui, N.: Generation of fractal patterns for probing the visual memory, *Neuroscience Research*, Vol.12, No.1, pp.307–311（1991）．