「マルチメディア，分散，協調とモバイル
(DICOMO2019)シンポジウム」 令和元年7月

インラインルール通知を用いたワンタイム図形認証

石井 健太郎[1]

概要：本研究では，のぞき見によりパスワード/パスコードが盗まれてしまう問題の低減を目指して，ワンタイム図形生成に基づく認証手法を提案している．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，のぞき見が行われても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，正規ユーザがあらかじめ設定し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正規ユーザであれば，ルールに基づき正解図形を選ぶことができる．これまでの研究により，単一の認証図形群生成ルールを連続して適用した場合であっても，のぞき見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両立する一定の効果が示されている．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が示されている．本論文では，この課題に対するさらなる改善のため，適用する認証図形群生成ルールを毎回ランダムで決定し，提示されている画像により正規のユーザに通知される仕組みである，インラインルール通知を導入する．インラインルール通知を適用した提案手法について評価実験を行ったところ，すべての認証図形群生成ルールについて説明を受けた実験参加者でも，インラインルール通知の設定を明かさなければ，不正に認証を受けることができないことが示された．

One-Time Shape-Pattern Authentication with Inline Rule Notification

KENTARO ISHII[1]

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，認証場面ののぞき見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画像認証手法を提案している [1], [2]．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，のぞき見が行われても，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，正規ユーザがあらかじめ設定し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正規ユーザであれば，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．

3 節で述べるとおり，単一の認証図形群生成ルールを適用する基本手法について，1 名の実験参加者が認証を受けている場面をもう 1 名の実験参加者がのぞき見を行う評価実験を行ったところ，認証成功率は正規ユーザで 92.8%・非正規ユーザで 17.1%と，のぞき見に対する一定の効果を示した [2]．しかし，実験参加者が同じカテゴリの認証図形群生成ルールを体験したあとにのぞき見を行う条件においては認証成功率は 25.7%と，同じカテゴリの認証図形群生成ルールを未体験の条件と比較して，有意に高い結果となった．これは，ルールを知る者が行うのぞき見においては認証に用いているルールを知られやすいという課題が残されていることを示している．

そこで本論文では，ルールを知る者が行う場合であってものぞき見に耐えることを追求する発展的手法として，インラインルール通知を導入する．インラインルール通知と

[1] 専修大学
Senshu University

は，認証図形群生成ルールを毎回固定するのではなくランダムで決定し，解答のための図形群にルールを通知するための図形を埋め込む手法である．このことにより，非正規ユーザには都度切り替わる認証図形群生成ルールを推測しづらくなる・正規ユーザには提示された図形群がどのルールで生成されたものであるかが通知されるために正解図形を選ぶことができるという 2 つの性質を両立することが可能となる．インラインルール通知を用いた発展的手法に対する評価実験を示し，結果に基づき議論する．

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 [3]．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 [4], [5] 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 [6]．

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，のぞき見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のぞき見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，のぞき見の影響を低減する手法が提案されている [7]．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 [8]．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 [8], [9]．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．

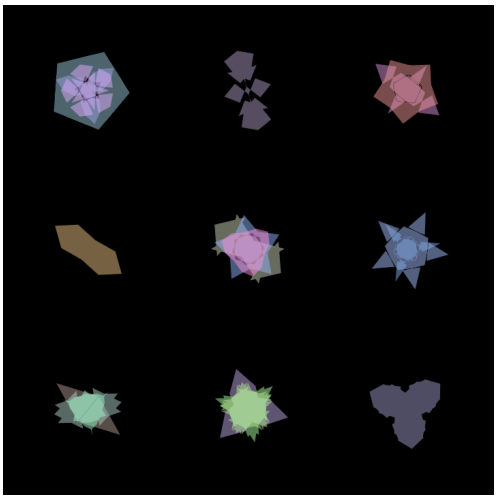


図 1 図形生成基本アルゴリズムによって生成された図形

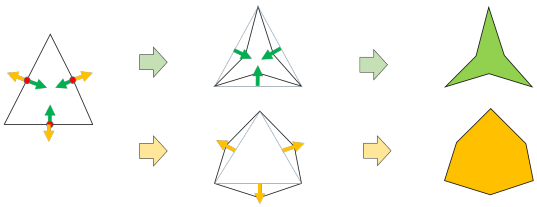


図 2 中点の移動による変形

3. ワンタイム図形認証の基本手法とその評価

本節では，提案手法であるワンタイム図形生成に基づく図形認証手法のうち，単一の認証図形群生性ルールを適用する基本手法の概要と評価実験の結果を述べる [2]．

3.1 図形生成基本アルゴリズムと認証図形群生成ルール

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 [10] を参考にしてアレンジしたものである．

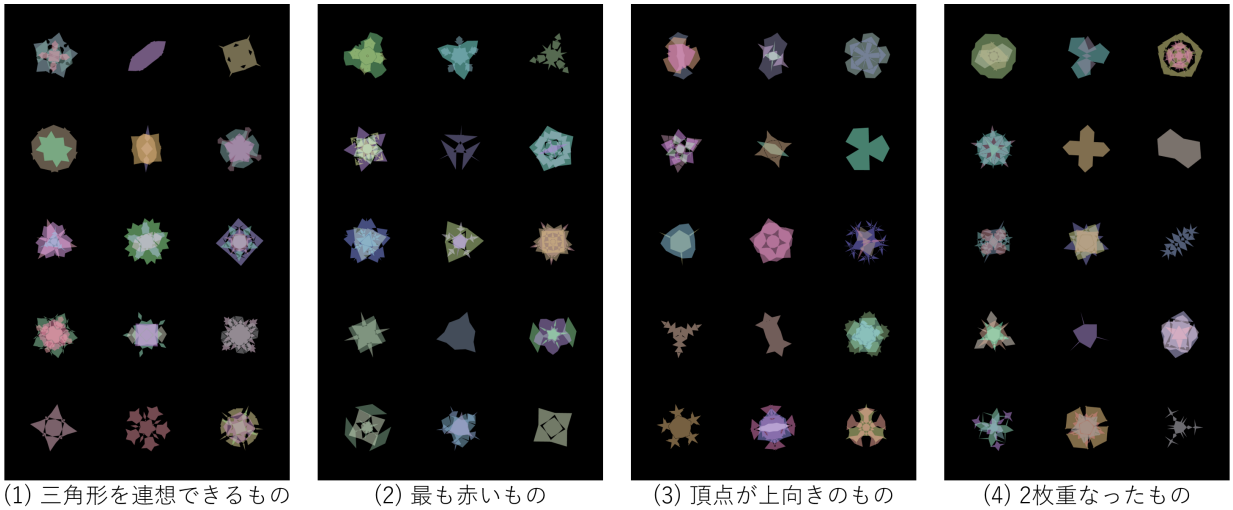
図形生成基本アルゴリズムの手続きを以下に示す．いずれの操作もランダムに選ばれるパラメータがあり，それにより毎回異なる図形が生成される．

(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) 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．

(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．

次に，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．認証図形群生成ルールは，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．

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

3.2　評価実験の目的と方法

3.1 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った [2]．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　事前知識条件ごとの認証成功率 (%)

	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

実験は 2 名 1 組の実験参加者を招いて行った．1 名の実験参加者が正規ユーザ役となり，もう 1 名の実験参加者はのぞき見を行う非正規ユーザ役となる．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 の順で正規ユーザ役を行い，もう一方が非正規ユーザ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，非正規ユーザの役割である B は，認証システムを利用したことがない状態でのぞき見を行う．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，非正規ユーザの役割である 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のぞき見を行う．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，非正規ユーザの役割である 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，自分が正規ユーザ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のぞき見を行う．したがって，似たようなルールを体験済みの状態でのぞき見を行うこととなる．

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．

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) 実験者は正規ユーザ役の実験参加者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，3.1 節で述べた直感的な説明のみを行う．

(2) 正規ユーザ役の実験参加者は認証アプリケーション利用の練習を 6 回行う．

(3) 正規ユーザ役の実験参加者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，非正規ユーザ役の実験参加者は正規ユーザ役の実験参加者のそばでのぞき見を行う．

(4) 正規ユーザ役の実験参加者の 3 回のテストの終了後，非正規ユーザ役の実験参加者は認証アプリケーション利用のテストを 3 回行う．

3.3 評価実験の結果

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，正規ユーザ役を 3 セッション・非正規ユーザ役を 3 セッション行っているため，全体としては正規ユーザ役のデータを 144 セッション分・非正規ユーザ役のデータを 144 セッション分取得した．正規ユーザ役の実験参加者も非正規ユーザ役の実験参加者も，1 セッションあたり 3 回の認証試行を行うため，全体としては，正規・非正規の両方について 432 認証試行のデータを取得したこととなる．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 認証試行のデータを取得した．

表 1 に，事前知識条件ごとの認証成功率を示す．全体としては，3 度連続でのぞき見が行われることは，通常利用よりも正規ユーザに厳しい条件であると考えられ，その条件下で正規ユーザ役の実験参加者と非正規ユーザ役の実験参加者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．非正規ユーザ役の実験参加者に関しては，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者は，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 2 に，事前知識条件ごとの平均解答時間を示す．全体としては，正規ユーザ役の実験参加者のほうが非正規ユー

表 2　事前知識条件ごとの平均解答時間 (msec.)

	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

ザ役の実験参加者よりも短い時間で回答している傾向が見られる．正規ユーザ役の実験参加者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．非正規ユーザ役の実験参加者に関しては，事前知識条件によって解答時間はあまり変化していない．

4. インラインルール通知を用いた発展的手法

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者にどう対応するかという課題が明らかになった．本節では，この課題に対処するための発展的な手法としてインラインルール通知を提案する．

4.1 インラインルール通知とその制約

非正規ユーザの思考をそらすためには，1 つの認証試行において複数のルールを切り替えることが有効ではないかと考える．なぜならば，非正規ユーザがルールを推測するときには，ルールが何であるかを絞り込む作業をしていると考えられるため，そのルールが都度切り替わるものであれば推測が十分に進まないことが期待できるからである．

さらに，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を考える．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．すなわち，解答のために提示されている図形の中に，ルールを通知するための図形を埋め込むことが，インラインルール通知のアイディアである．

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．残りの図形は基本手法と同様に認証図形群生成ルールによって生成されており，1 つの正解図形と 13 のダミー図形が含まれる．どの場所にルールが通知されるかは正規ユーザのみが知るとすると，非正規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．

さて，インラインルール通知により通知されるルールの候補と通知場所は，正規ユーザが設定すべき事項であるが，

図 4　インラインルール通知

以下に示す 3 つの点に注意しなければならない．

第 1 に，原理上インラインルール通知がなされる位置には正解図形は配置されないため，常に同じ位置にルールが通知されるように設定すると，正解を選択しない位置としてルール通知の位置が推定できる可能性があることである．ルール通知は，複数の位置を切り替えて行うことが必要である．例えば，1 回の認証試行の中で，解答試行ごとに異なるルール通知の位置を設定することが対処法として考えられる．

第 2 に，カテゴリ内のすべてのルールを通知候補とするのは，原則 1 つのカテゴリまでに限られることである．2 つ以上のルールカテゴリにおいて，カテゴリ内のすべてのルールを通知候補としてしまうと，あるカテゴリのルールが通知された場合に，そのカテゴリ内では一意に定まるルールとなるが，ほかのカテゴリでの生成条件を満たすルールが存在することになる．例えば，カテゴリ 1 の初期多角形ルールすべてとカテゴリ 2 の色空間ルールすべてが通知候補だとすると，カテゴリ 1 の三角形ルールを通知するために生成した図形が，赤・緑・青のいずれかが最も大きい RGB 値を持つことになるため，カテゴリ 2 のいずれかのルールを通知するための図形と見分けがつかないことになる．

この点に対処するために，ユーザはカテゴリ間に優先順位をつけ，優先度上位のカテゴリは優先度下位のカテゴリに通知ルールを明け渡すための生成ルールを 1 つ以上は確保することを行わなければならない．例えば，カテゴリ 1 のが優先度上位でカテゴリ 2 が優先度下位の場合，五角形ルールが優先度下位に通知ルールを明け渡すためのルールだとすると，インラインルール通知で二角形・三角形・四

角形が現れた場合はそのまま通知ルールであり，五角形が現れた場合は色空間ルールカテゴリに通知ルールを明け渡すこととみなし，赤・緑・青のうち現れた図形により通知ルールが判明するといった具合である．最も優先順位の低いカテゴリのみは，ほかのカテゴリに通知ルールを明け渡す必要がないため，カテゴリ内のすべてのルールを通知候補とすることができる．

例外は，カテゴリ 3 の回転角度ルールであり，ダミー図形に用いられる回転角度はカテゴリ内のほかのルールの正解図形にも使用されていないため，ダミー図形であれば，優先度下位のカテゴリに通知ルールを明け渡すこととみなすことができるため，通知ルールを明け渡すための生成ルールを確保する必要はない．

第 3 に，インラインルール通知の図形と適用されているルールの図形が異なる設定も可能であることである．例えば，二角形が通知されれば三角形が適用ルールであり，三角形が通知されれば四角形が適用ルールであり，四角形が通知されれば二角形が適用ルールであるといったことが可能である．これは，二角形が通知されれば赤が適用ルールであるというように，カテゴリをまたいだ設定も可能である．

4.2 評価実験の目的と方法

4.1 節のインラインルール通知を導入し，1 度に提示する図形の数や 1 認証試行あたりの解答試行数といった値とともに，インラインルール通知の通知ルールと通知場所を設定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．本実験のために，実験者でも実験参加者でもない者に，設定を繰り返し変更しながらインラインルール通知の好みの設定を 2 種類決定してもらった．その結果，(1)1 度に 9 つの図形提示・1 認証試行あたり 3 回の解答試行・適用されているルールと同じ図形によるルール通知の設定と，(2)1 度に 4 つの図形提示・1 認証試行あたり 4 回の解答試行・適用されているルールと異なる図形によるルール通知の設定の 2 種類が選択された．正規ユーザにとっては，インラインルール通知の導入により認証を受けるための難易度が増すことになるが，この好みの設定の聞きとりによって，正規ユーザによる認証の実行可能性を確保することを意図している．

その後，上記の 2 種類の設定それぞれについて，実験者が認証を受ける場面のビデオ撮影を行い，実験用の素材とする．このビデオから，無作為に選んだ連続 10 回の認証試行を，10 回中の何回目であるかを示すテロップとともに提示するビデオを用意する（**図 5**）．

実験は，以下の手順により行う．はじめに，実験参加者は基本手法についての説明を実験者から受ける．この際に，4 カテゴリ 12 種類の認証図形群生成ルールすべてについても説明を受ける．また，基本手法を組み込んだ実機の

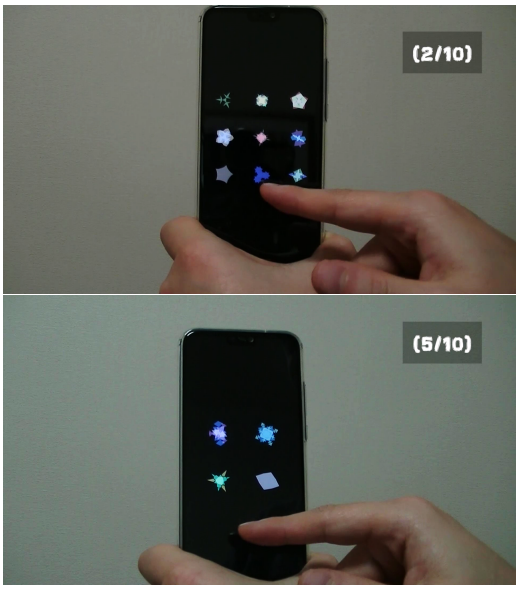


図 5 評価実験に用いたビデオのスクリーンショット

認証アプリケーションを何度でも解いてよいことを教示される．このことにより，認証図形群生成ルールについて十分な理解を得ることを意図している．

基本手法を十分に理解したら，次に，実験参加者はインラインルール通知についての説明を実験者から受ける．すなわち，いずれかの場所にルールを知らせる図形が提示されており，それにより正規ユーザはランダムに決定される適用ルールを知ることの説明を受ける．

インラインルール通知を十分に理解したら，最後に，あらかじめ用意した認証場面のビデオを繰り返し見てよいものとし，同時に，実験参加者はビデオと同じ設定の実機の認証アプリケーションを渡され，認証を受けることを目指して任意で認証試行を行うように指示される．実験者は，解きかたが理解できたか解けずにあきらめるかする場合はこのセッションを終了することを実験参加者に指示し，実験参加者からの申し出を待つ．最初のセッションが終了したら，設定をもう一方に変更したうえで，この手順をもう 1 度繰り返す．

4.3 評価実験の結果

16 名の実験参加者を招き実験を実施した．最初に行うセッションが 2 つの設定について同数になるように実験参加者を割り振り，8 名の実験参加者は 1 番目の設定・8 名の実験参加者は 2 番目の設定から開始することとした．

16 名の参加者から，1 番目の設定は 102 認証試行を取得し，2 番目の設定は 73 認証試行を取得した．そのうち認証に成功した試行は，いずれの設定においても 0 回であり，本評価実験において実験参加者は 1 度も認証に成功できなかった．特に第 2 セッションにおいては，ビデオを見ても解きかたがわからず，まったく認証を試行しないかわずかに認証を試行するのみであきらめる実験参加者が多くいた．

5. 議論とまとめ

本研究では，のぞき見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，新たにインラインルール通知と呼ぶ仕組みを導入し，ルールをすべて把握している者であっても設定を明かさなければ，認証に必要な情報を取得することを防ぐことができることを示した．インラインルール通知は，1つの認証試行において複数のルールをランダムに切り替えることによって，非正規ユーザの思考をそらす手法である．その際に，解答のために提示されている図形の中に，ルールを通知するための図形を埋め込むことで，正規ユーザが正解図形を知るための手段を提供している．

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，正規ユーザ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 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] 石井健太郎：Cognometric 方式画像認証のユーザ設定に関する調査，情報処理学会研究報告，Vol.2019-GN-108，No.15，pp.1–8（2019）．

[3] Dhamija, R., Perrig, A.: Déjà Vu: A User Study Using Images for Authentication, *USENIX Security Symposium* (2000).

[4] 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).

[5] 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）．

[6] 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）．

[7] 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）．

[8] 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）．

[9] 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).

[10] 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）．