Computer Security Symposium 2020
26 - 29 October 2020

画像合成技術を用いた個人認証における好まれる認証ルールの調査

石井 健太郎[1,a)]

概要：本研究では，認証場面ののぞき見への対策としてとりくんでいる画像合成に基づくワンタイム画像を用いた個人認証について，ユーザがどのような認証ルールを見出すのか，そして，その認証ルールを満たす画像をシステムは合成することができるのかを調査する．調査対象の個人認証手法では，Generative Adversarial Networks (GAN) の 1 種の画像生成技術である StyleGAN の style mixing と呼ばれる 2 つの画像の特徴を合成して新たな画像を生成する技術を利用して，正規のユーザがあらかじめ決めておいた特徴を持つ画像と持たない画像を複数生成して画面に提示する．認証を受けようとするユーザは，提示された複数の画像の中から，画像の特徴を手がかりにして，正解画像を選ぶことによって認証を受ける．この個人認証手法を利用する際には，StyleGAN で生成された画像をユーザに提示し，正解画像が持つ特徴を決定したうえで，その特徴を持つ画像をいくつか例示してもらう必要がある．本論文では，この正解画像が持つ特徴を認証ルールと呼ぶこととし，認証ルールの決定プロセスを，ユーザスタディにより調査した結果を報告する．

Study on User Preference of Authentication Rule in Image-Generation-based Authentication

Kentaro Ishii[1,a)]

Abstract: This paper studies an image-generation-based authentication method on what kind of authentication rules the users of the method prefer and whether the system of the method can generate the preferred rule-based images. The targeted method aims at shoulder-surfing resident utilizing many images generated by using the style mixing of StyleGAN, which is an implementation of Generative Adversarial Networks (GAN). The genuine user of the method can distinguish the correct image from the dummy images by a predefined generation rule. In the process of the rule definition, the genuine user needs to pick up both which images should be correct images and which images should be dummy images. In this paper, we investigate the process of the rule definition and discuss user preference.

1. はじめに

スマートフォンのようなタッチ操作をともなう端末では，入力の位置からパスワード/パスコードやパターンロックの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 [1], [2]．この課題に対して，本研究ではこれまでに，都度表示される画像を切り替えることでのぞき見のリスクを低減するワンタイム画像を利用した個人認証手法を扱ってきた [3], [4], [5]．

個人認証に画像を利用することの背景には，認証情報の入力を求める再生記憶よりも，提示された情報が目的のものであるかを求める再認記憶のほうが記憶負荷が低いとされることが挙げられる [6]．画像認証は，Cognometric 方式・Locimetric 方式・Drawmetric 方式の 3 つに大きく分類されるが，画像そのものを選択する Cognometric 方式が最もシンプルに再認記憶を用いる方式であり，さまざまな提案がなされている [6], [7], [8], [9], [10]．しかし，これら

[1] 専修大学
Senshu University
[a)] kenta@pc.fm.senshu-u.ac.jp

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，のぞき見によって画像を記憶されてしまうと，認証を受けるために必要な情報が完全に盗まれてしまうこととなる．これは，通常の Cognometric 方式画像認証の原理的な短所と言える．

Cognometric 方式画像認証におけるのぞき見のリスクの低減手法として，Locimetric 方式と組み合わせる手法 [11], [12], [13] や，正解画像そのものを提示するのではなく加工した画像を提示する手法 [14], [15] が提案されている．これらは，高いのぞき見耐性性能を示している一方で，画像の再認にかかるユーザへの負荷は高く，シンプルな再認が原理である Cognometric 方式の長所を妥協するものと考えられる．一方，画像の再認にかかる負荷はほとんど通常の Cognometric 方式と変わらないと考えられるが，画像の選択操作に加えてスマートフォン端末を振る操作を行う，2 種類の入力操作を組み合わせることによる手法 [16] も提案されている．以上の手法は，すなわち，再認タスクまたは入力操作を複雑にすることによって，対策を行うものであると分類することができる．

本研究では，目的の画像を選択する操作のみの Cognometric 方式のシンプルさを維持しながら，のぞき見耐性を持つ手法を追求する．特に本論文では，Generative Adversarial Networks (GAN) [17] の 1 種の画像生成技術である StyleGAN [18], [19] により生成した顔画像を用いる手法 [5] を対象として，先行研究では未検証であった，ユーザがどのような認証ルールを見出すのか・その認証ルールを満たす画像をシステムは合成することができるのかの 2 点を調査する．

調査対象の個人認証手法では，StyleGAN の style mixing と呼ばれる 2 つの画像の特徴を合成して新たな画像を生成する技術を利用して，正規のユーザがあらかじめ決めておいた特徴を持つ画像と持たない画像を複数生成して画面に提示する．認証を受けようとするユーザは，提示された複数の画像の中から，画像の特徴を手がかりにして，正解画像を選ぶことによって認証を受ける（**図 1**）．この手法は，一定ののぞき見への対策性能を示したが，正解画像が持つ特徴を認証ルールと呼ぶこととすると，認証ルールとして利用する style mixing の入力画像にどのようなものが利用できるのかは未検証の課題であった [5]．設定できるルールに限りがある図形生成アルゴリズムを用いた手法 [3] と比較すると，調査対象の手法は原理的にはより多様で柔軟な認証ルールを確保できる可能性があるが，そのことを検証することが本論文の目的である．

本論文では，まず先行研究である調査対象の手法 [5] について，認証の原理と評価実験の結果を抜粋して簡潔にまとめる．その後，ユーザがどのような認証ルールを見出すのか・その認証ルールを満たす画像をシステムは合成することができるのかを，ユーザスタディにより調査した結果を報告する．

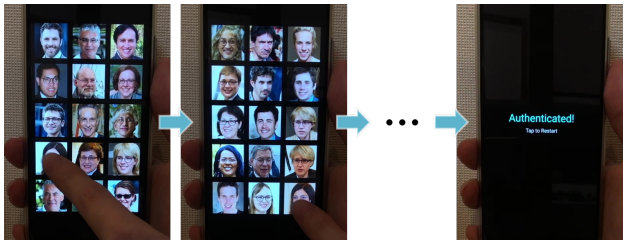

図 1 画像合成技術により生成した顔画像を用いた個人認証．ユーザは認証ルールに沿った正解画像をあらかじめ決められた回数正しく選択できれば認証されるが，画像合成技術を用いて生成された都度異なる画像が提示されることが特徴である．

図 2 style mixing によって生成された顔画像．1 行目と 1 列目を入力画像として，同じ列の入力画像と同じ行の入力画像を混ぜ合わせて生成された画像を並べている．概ね，入力画像の人物の顔の特徴は残したまま別の人物に見える顔画像が生成されている．

2. ワンタイム顔画像生成による個人認証

2.1 StyleGAN による顔画像合成

本研究で利用する StyleGAN [18], [19] には，style mixing と呼ばれる 2 つの画像を合成して新しく 1 枚の画像を生成する利用法がある [18]．**図 2** は，style mixing における入力画像を 1 行目と 1 列目に配置し，それらを合成して新しく生成された画像をその他の位置に配置することによって構成されている．合成した画像の粗い特徴から細かい特徴までを，2 つの入力画像のどちらの特徴を反映したものとするかは，合成時のパラメータによって制御できる．このため，パラメータを調整のうえ固定とすると，2 つの入力画像を入れ替えた合成結果は異なるものとなる．図 2 は，その事実を反映させたものであり，同じ 2 枚の入力画像で

(1) 眼鏡なし女性　(2) 金色の髪　(3) 帽子をかぶっている　(4) 口を開けている

図 3　認証ルールによって生成された認証問題の例．各認証問題は 1 つの正解画像と 8 つのダミー画像を含む．

も，互いを入れ替えると別の顔が生成される．この結果，入力画像の人物の顔の特徴を残しているが別の人物に見える顔画像を新しく生成することができる．このことを利用して，認証システムに応用する．

StyleGAN は顔画像に限らず任意の画像に適用できるものであるが，調査対象の個人認証には人間の顔画像を題材として応用したもののみを採用する．人間の顔画像を採用した理由は，公開されていてすぐに利用可能であった学習済み画像生成モデル[*1]のうち，正規ユーザにとって最も正解画像の特徴が識別しやすい画像であろうと考えたことによる．

2.2　認証ルールの定義

本研究の認証の原理は，都度異なる画像群から，特定の特徴を持つ正解画像を言い当てることである．正解画像の手がかりとなる画像の特徴とは，例えば，「眼鏡をかけていない女性」といったものであり，これを認証ルールと呼ぶこととする．正解画像でない画像をダミー画像と呼ぶこととすると，認証ルールが「眼鏡をかけていない女性」である場合は，眼鏡をかけている人物の顔画像はダミー画像であり，男性の顔画像はダミー画像であり，このようにして正解画像とダミー画像を見分ける．

提案手法は都度異なる画像を提示することがのぞき見対策の原理であることから，正解画像とダミー画像をともに大量に生成する必要があり，このことに 2.1 節で述べた style mixing を利用する．手順は以下のとおりである．

(1) style mixing の材料となる入力画像候補を，StyleGAN の同じ学習済みモデルからランダムで繰り返し生成する．このときに，ランダム生成された画像の中には，提示する顔画像としては不適切である画像も比較的高い頻度で生成される．これは，StyleGAN あるいは GAN 一般の制約である．本論文の実装では，ランダム生成した最初の 1000 枚の画像のうち 434 枚は，著者により不適切であると判断され，以後の処理から除外された．

(2) 例えば，「眼鏡をかけていない女性」（以降「眼鏡なし女性」と呼ぶ）の場合は，前述のランダム生成画像の中から「眼鏡なし女性」である顔画像と「眼鏡なし女性」でない顔画像をそれぞれ選び出し，ルールに合致する画像同士・ルールに合致しない画像同士を style mixing で合成し，それぞれを正解画像・ダミー画像として認証問題作成の材料とする[*2]．

したがって，認証ルールの定義は，style mixing の入力画像としてルールに合致するか合致しないかを明確に分類できる顔画像を用意する用例ベースの方法によってなされると言うことができる．

この手順のうち，手作業が必要な部分とその主体をまとめる．まず，ランダム生成された画像のうち，不適切である画像を除外する作業は，機械が自動的に判断するのが難しく，人間の手作業によって行われる必要がある．これはシステムを運用する者が行うべき作業である．ただし，運用する段階では，システムのユーザが不適切な画像を発見した場合に報告できる仕組みを備えておくことが望ましい．次に，認証ルールに合致する画像と合致しない画像を選定する作業も，手作業で行われる必要がある．これはシステムのユーザがそれぞれに行うべき作業である．残りの手続きは，機械による自動処理が可能である．

3 章のユーザスタディに先立ち，著者は上記の方法で 12 種類の認証ルールを定義した．12 種類は，図形生成アルゴリズムを用いた手法 [3] の認証ルールの種類の数であるため，それと同等かより多様な認証ルールを定義できること

[*1] 実装を開始した時点で，人間の顔のほかに猫の全身・車・ベッドのあわせて 4 つの画像生成モデルが利用可能であった．

[*2] 検討を経て，先行研究 [5] から変更した箇所もある．

図 4　認証アプリケーション

が期待できる．3 章のユーザスタディでは，著者以外の参加者によって，認証ルールを定義することを試みる．

著者が定義した認証ルールのうち，「金色の髪」・「白色の髪」・「黒色の髪」など，似通った認証ルールは省略して，代表的な 4 つの認証ルール（「眼鏡なし女性」・「金色の髪」・「帽子をかぶっている」・「口を開けている」）の例を，**図 3** に示す．それぞれ異なる抽象度や部位の認証ルールで画像合成を行っているが，どの画面にも認証ルールに合致する正解画像が 1 枚だけ表示されていることがわかる．

2.3　認証アプリケーション

認証アプリケーションは，各認証ルールを用いて生成した画像を組み込み，認証のユーザインタフェースを追加したものである[*3]．Processing 言語を用いて Android スマートフォンのスマートフォンアプリとして用意したバージョンと，JavaScript 言語を用いてブラウザアプリケーションとして用意したバージョンの，2 つのバージョンを実装した（**図 4**）．

このアプリケーションでは，画面上に 9 つの画像が提示され，ユーザがそれらのうちの 1 つを選択するのを待ち受ける．画像の選択を行うと，画面が切り替わり別の 9 つの画像が提示される（図 4 左）．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，認証ルールに基づいて 1 つの正解画像と 8 つのダミー画像が含まれており，すべての画面で正解画像を選択できれば認証される．また，認証ルール選択のための設定画面も用意し，各認証ルールの代表画像を選択することにより，認証ルールを切り替えることができる実装である（図 4 右）．

2.4　評価実験の結果

評価実験は，実験者が正規ユーザ役となり，実験参加者はのぞき見を行う非正規ユーザ役となり行われた．正規ユーザ役の実験者が認証を受けている場面を 3 回連続で見たあとに，非正規ユーザ役の実験参加者が認証を受けられるかをテストする方法で行われた．認証ルールは正規ユーザが自由に定義できることを考慮して，また，先行研究 [3] のシステム未体験条件と条件を揃えることを目的として，非正規ユーザ役の実験参加者には，各認証画面に 1 つの正解画像があることのみが知らされ，認証システムが認証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状態で評価実験を設計した．

その結果，16 名の実験参加者のうち，2 名がのぞき見後に認証問題を解くことができ，残りの 14 名は認証問題を解くことができなかった．また，認証問題を解くことができた実験参加者 2 名はいずれも，認証ルールが存在することを見抜き，言い当てることができた．一方，当初認証問題を解くことができなかった 14 名全員が，認証ルールを言葉で与えられたあとに，認証問題を解くことができた．これらの結果は，のぞき見耐性を有していると同時に，既存の手法と同等程度の利用しやすさを有していることを示している．

3.　ユーザスタディ

3.1　目的と方法

本ユーザスタディでは，参加者を初めて本手法を利用する正規ユーザと見立てて，ユーザがどのような認証ルールを見出すのか・その認証ルールを満たす画像をシステムは合成することができるのかの 2 点を調査する．より具体的には，2.2 節の手順 (2) において，認証ルールに合致する画像と合致しない画像として，どのような画像が選ばれるのかを取得することが目的である．加えて，参加者には，認証ルールの解釈を言葉で記述してもらい，その記述を取得することで，認証ルールの多様性を検証することも目的である．

ユーザスタディは，オンライン形式にて，大きく以下の 3 つの段階に分けて実施する．

(1) 本個人認証手法の利用方法と原理を説明する．このときに，ユーザスタディの進行役が認証を受けている場面を見ることで，参加者はのぞき見を疑似体験しながら，段階的に説明を受ける．このことによって，本個人認証手法がのぞき見耐性を持つことを同時に理解することを意図している．また，オンライン形式であることを利用して，ブラウザアプリケーションバージョンの認証システムを自由に試してよいことを参加者に示し，納得するまで認証手法を理解してもらう．

(2) 不適切である画像を除外したあとのランダム生成された画像の最初の 100 枚を参加者に提示し，認証ルールを自由に決めることと，その認証ルールに沿った画像を 5 枚・沿わない画像を 5 枚選定することを指示する．認証ルールの解釈と選定した画像は，オンラインフォームにより入力・記録してもらい，進行役は，記録された画像をもとに，style mixing をその場で実行して，認証問題と画像の合成結果を参加者に示す．

[*3] 検討を経て，先行研究 [5] から変更した箇所もある．

(3) 進行役はまず認証問題を解いてみるように参加者に指示し，認証問題が解けるかどうかを試してもらう．参加者には，認証問題を解けたか解けなかったかを，進行役にフィードバックしてもらう．その後，進行役は画像の合成結果を確認するように参加者に指示する．参加者には，自分が意図したとおりに画像が合成されているか，そして，合成した画像に不適切が画像が含まれていないかを，進行役にフィードバックしてもらう．

以上が基本的な手続きであるが，最後まで終了した段階で，もう 1 度認証ルールを定義したいと参加者が希望する場合には，手続き (2) に戻り，繰り返す．

3.2 結果

12 名の参加者を招きユーザスタディを実施した．このうち 1 名の参加者は途中で参加を辞退したため，以下では残りの 11 名の参加者による結果を示す．11 名の参加者は全員大学生で，情報技術系の理工学を専攻している者が 9 名・情報技術以外の理工学を専攻している者が 2 名であり，女性 7 名・男性 4 名であった．11 名のうち 1 名は，2 回目の認証ルールの定義を希望したため，延べ 12 の認証ルールがこのユーザスタディにより定義された．

定義された 12 の認証ルールの解釈は，同一視できるものをまとめると，「前髪をおろしている」が 3 つ，「サングラスをかけている」が 2 つ，「眼鏡やサングラスをかけている」が 1 つ，「耳飾りをつけている」が 2 つ，「背景に青空」と「背景に植物」がそれぞれ 1 つ，「顔の右側から撮影されている」が 1 つ，「若い女性」が 1 つという結果であった．異なる参加者による認証ルールが一致している例があるが，概ね多様な認証ルールが定義されていると言える．事前に定義された認証ルールを合わせると，少なくとも 20 種類の認証ルールは定義できることがわかる．重複するルールは「前髪」・「サングラスまたは眼鏡」といった，顔の大きな部分を占めるものが多いが，「耳飾り」は小さいパーツであり，必ずしも目に留まりやすいというような理由に限らないことが示唆される．なお，すべての認証ルールの選定画像とその解釈は，文末の付録に掲載する．

興味深いことに，顔の特徴そのものではなく，「背景」や「顔の向き」のような副次的な特徴が認証ルールとして選ばれるケースが見られた．それらのケースでも，ルールを定義する手順と作業負荷は同様であり，柔軟な認証ルール定義が可能であることを示す 1 つの根拠であると言える．また，「若い女性」といった，主観的であり，ユーザによっては基準が一定ではない認証ルールも許容する点にも，本認証手法の柔軟性が示されていると考える．後述するとおり，この参加者は認証問題は解けたと報告しており，基準があいまいな認証ルールであっても，定義した本人には利用できる可能性を示している．

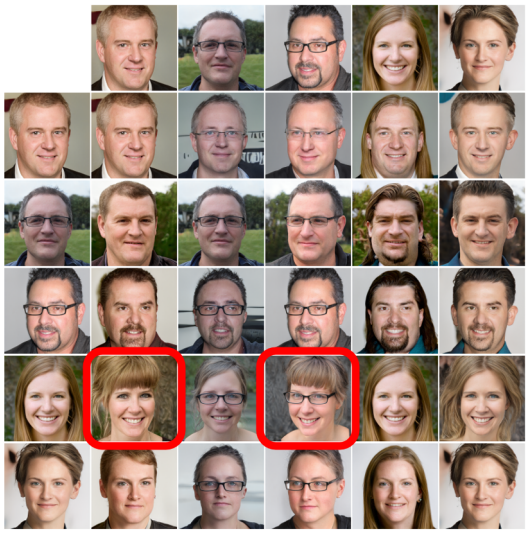

図 5 参加者 No.8（「前髪をおろしている」）のダミー画像．赤角丸は著者の注釈であり，意図しない合成画像を示す．

生成された認証問題が解けるかどうかに関しては，参加者 No.8 であり，「前髪をおろしている」という認証ルールを定義した参加者 1 名が，うまく解けなかったと報告した．この参加者によると，認証ルールに沿わない画像の合成画像の中に，認証ルールに沿っている画像が含まれてしまっているとのことであった．すなわち，「前髪をおろしていない」画像を合成した結果，「前髪をおろしている」画像が生成されたということである．**図 5** に，この参加者のダミー画像として生成された画像を示すが，たしかに，「前髪をおろしていない」と解釈できる 2 つの画像から，「前髪をおろしている」画像が合成されている．この点に関して，今後解決法を検討する必要があるが，少なくともルールを定義したあとに利用を始める段階の前に，合成画像が意図に沿ったものであるかユーザが確認する段階を設ける必要があると言える．

その他の 10 名 11 ルールについては，認証問題は解けたと報告された．また，これらの参加者から，合成された画像に意図しない画像があったり，不適切な画像があったりしたという報告はなかった．

4. 議論

本論文のユーザスタディの結果は，調査対象の個人認証手法によりユーザが自由に定義した認証ルールを特別な熟練なく概ね利用できることを示したものであり，先行研究 [5] ののぞき見耐性の評価と合わせて，一定の安全性と利便性を同時に提供しうるものだと考える．4 カテゴリ 12 ルールと設定できるルールに限りがあった図形生成アルゴリズムを用いた手法 [3] と比べると，認証ルールの定義に関する多様性と柔軟性は飛躍的に上昇しており，図形生成アルゴリズムを用いた手法の欠点を克服していると言える．また，顔画像以外の画像生成モデルを利用することで，さ

らなる認証ルールの多様性を確保できる可能性がある．

一方で，ユーザが意図しない合成画像が生成された事例も明らかになり，改善の余地があることと，ユーザにとってのわかりやすさに配慮すべき点があることも明らかになった．この点については，さらなる調査で知見を積み上げていくことが重要であり，今後の計画として考えている．

5. まとめ

本論文では，先行研究 [5] で提案した画像合成技術を用いた個人認証手法について，定義される認証ルールを調査した．調査対象の個人認証手法は，StyleGAN [18], [19] の style mixing という画像合成技術を用いて，ユーザが自由に定義した認証ルールに合致する画像と合致しない画像を用意する用例ベースの方法であろ．特に，初めて利用するユーザがどのような認証ルールを見出すのか・その認証ルールを満たす画像をシステムは合成することができるのかに注目してユーザスタディを実施した．

ユーザスタディの結果，12 回の試行の中から 8 つの異なる認証ルールが定義され，概ね多様な認証ルールが定義されうることが確認された．また，顔の特徴そのものではなく，「背景」や「顔の向き」のような副次的な特徴が認証ルールとして選ばれるケースや，「若い女性」のような基準があいまいな認証ルールを許容することが示され，利用するユーザにより，柔軟な認証ルールを定義することができることも示唆された．先行研究 [5] ののぞき見耐性の評価と合わせて，調査対象の個人認証手法が一定の安全性と利便性を同時に提供しうるものだと考える．

参考文献

[1] Aviv, A.J., Davin, J.T., Wolf, F., Kuber, R.: Towards Baselines for Shoulder Surfing on Mobile Authentication, *Annual Computer Security Applications Conference*, pp.486–498 (2017).

[2] 石塚正也，高田哲司：CCC：携帯端末での暗証番号認証における振動機能を応用した覗き見攻撃対策手法，情報処理学会論文誌，Vol.56, No.9, pp.1877–1888 (2015).

[3] 石井健太郎，香川将樹，島谷和樹：ワンタイム図形生成に基づく個人認証の生成ルールとその評価，情報処理学会論文誌，Vol.60, No.12, pp.2127–2138 (2019).

[4] 石井健太郎：インラインルール通知を用いたワンタイム図形認証，マルチメディア，分散，協調とモバイルシンポジウム 2019 論文集，pp.1161–1167 (2019).

[5] 石井健太郎：ワンタイム顔画像生成に基づく画像認証手法，マルチメディア，分散，協調とモバイルシンポジウム 2020 論文集，pp.1594–1600 (2020).

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

[7] Tari, F., Ozok, A.A., Holden, S.H.: A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords, *Symposium on Usable Privacy and Security*, pp.56–66 (2006).

[8] 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).

[9] 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).

[10] 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).

[11] Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.C.: Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme, *International Working Conference on Advanced Visual Interfaces*, pp.177–184 (2006).

[12] Man, S., Hong, D., Matthews, M.: A Shoulder-Surfing Resistant Graphical Password Scheme - WIW, *Security and Management*, pp.105–111 (2003).

[13] Zhao, H., Li, X.: S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme, *International Conference on Advanced Information Networking and Applications Workshops*, pp.467–472 (2007).

[14] 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.8，pp.1997–2013 (2005).

[15] 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).

[16] 吉田光宏，高田哲司：Pict Place Shuffle: 情報配置と間接入力による再認式画像認証の改良，インタラクション 2020 論文集，pp.882–886 (2020).

[17] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative Adversarial Nets, *International Conference on Neural Information Processing Systems*, pp.2672–2680 (2014).

[18] Karras, T., Laine, S., Aila, T.: A Style-Based Generator Architecture for Generative Adversarial Networks, *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp.4401–4410 (2019).

[19] Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J., Aila, T.: Analyzing and Improving the Image Quality of StyleGAN, *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp.8110–8119 (2020).

付　　録

A.1 参加者が選定した画像と合成画像

以下に，ユーザスタディにおいて，参加者が選定した画像とその画像から合成された画像を示す．また，キャプションには，参加者が記述した認証ルールの解釈をそのまま示す．なお，参加者 No.4 の参加者のみ，2 回目の認証ルール定義を希望したため，2 回分の選定画像と合成画像がある．

図 **A·1**　参加者 No.1：前髪がある女性と、ない女性（おでこが出ていない女性が正解）

図 **A·2**　参加者 No.2：サングラスをかけている人

図 **A·3**　参加者 No.3：背景に青空が写っている

図 **A·4**　参加者 No.4（1 回目）：顔の右側から撮影されている

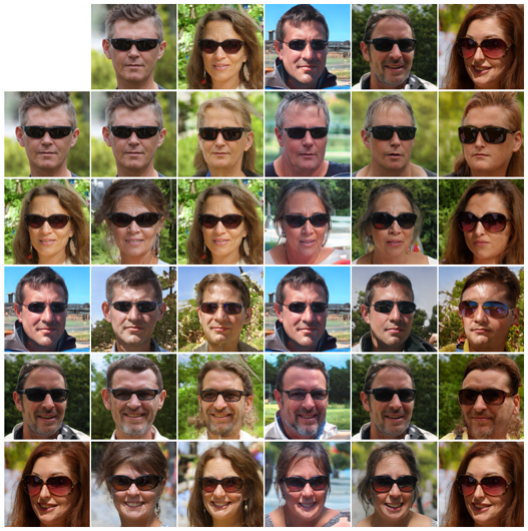

図 **A·5**　参加者 No.4（2 回目）：サングラスを掛けている

図 **A·6**　参加者 No.5：メガネやサングラスをかけている

図 **A·7**　参加者 No.6：耳に装飾品をつけている

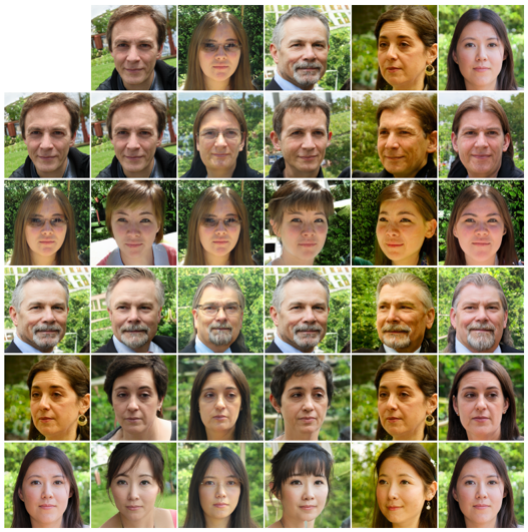

図 **A·10**　参加者 No.9：背景に植物がある

図 **A·8**　参加者 No.7：耳飾り（イヤリング　ピアス）をつけている

図 **A·11**　参加者 No.10：若い女性

図 **A·9**　参加者 No.8：前髪があるか (前髪をおろしているか)

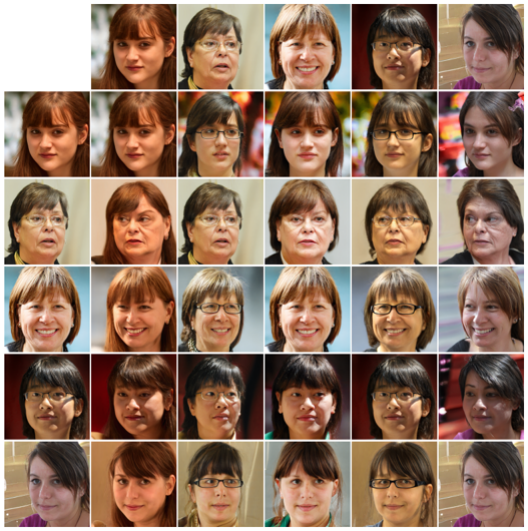

図 **A·12**　参加者 No.11：前髪がある女性