# 使い捨て可能な生体認証の提案：爪の模様を用いたマイクロ生体認証

一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
BioX2017-57,PRMU2017-193(2018-03)

# 使い捨て可能な生体認証の提案
# 爪の模様を用いたマイクロ生体認証

杉本 元輝† 藤田 真浩† 眞野 勇人† 大木 哲史† 西垣 正勝†
†静岡大学 〒432-8011 静岡県浜松市中区城北 3-5-1
E-mail: nisigaki@inf.shizuoka.ac.jp

**あらまし** 生体認証は，忘却・紛失・盗難の恐れがないという利点があるため，さまざまな場面で用いられている．近年，ATM などの重要なサービスに加え，遊園地の入退場やコインロッカーなどの短期間のカジュアルなサービスでも生体認証が用いられるようになってきている．しかし重要なサービスとカジュアルなサービスでは生体認証に求められる要件が異なるため，それぞれに適した生体認証が必要である．本稿ではカジュアルなサービスの要求を満たす生体認証として，爪の模様を用いたマイクロ生体認証を提案する．

**キーワード** 生体認証，プライバシ保護，使い捨て，微細パターン，爪

# Disposable Biometric Authentication
## －Micro Biometric Authentication Using Fingernail Textures－

Genki Sugimoto†, Masahiro Fujita†, Yuto Mano†, Tetsushi Ohki† and Masakatsu Nishigaki†
† Shizuoka University, Japan
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp

**Abstract** Recently, biometric authentication has been applied to not only important services such as in emigration/immigration inspection systems and ATMs but also casual services such as entry/exit management systems or theme park lockers. However, biometric authentication requirements for important and casual services differ; therefore, each service requires suitable biometric authentications. In this paper, micro biometric authentication using fingernail texture for casual biometric authentication is proposed.

**Keywords** Biometric authentication, Privacy preservation, Disposability, Minute pattern, Nail texture

## 1. はじめに

生体認証とは，人間の身体的特徴や行動的特徴から個人を認証する技術である．生体認証は，忘却・紛失・盗難の恐れがないという利点があるため，さまざまな場面で用いられている．近年では，入出国審査や ATM などの重要なサービスに加え[1]，遊園地の入場やコインロッカーなどのカジュアルなサービスでも生体認証が用いられるようになってきている[2]．しかし重要なサービスとカジュアルなサービスでは生体認証に求められる要件が異なるため，それぞれに適した生体認証が必要である．本稿ではカジュアルなサービスに適した生体認証を提案する．

利用者の本人性の確認を必要とするサービスを，「重要なサービス」と位置付ける．典型的には，比較的高価なサービスやある程度長期に渡って利用されるサービスが，これに該当する．重要なサービスでは，認証は実名で行われることになる．ここで重要となるのは，生体情報の偽造などによるなりすましへの対策である．なりすましとは攻撃者が正規ユーザの生体情報を盗み，偽造することで認証を突破する攻撃である．実際に，攻撃者が盗んだ生体情報から顔写真や人工指を複製し，なりすましに成功した例が報告されている[3][4]．近年では，カメラの高性能化により，遠距離から虹彩や指紋の高精細な画像を盗撮することも困難ではなくなっている．また，重要なサービスでは比較的長期間に渡って本人性が確認できることが求められるため，生体情報の経時変化に対する対策（経時変化の少ない生体情報の採用）も必要となる．これらを満たす生体認証は幅広く研究が行なわれている．

一方で，利用者の属性（既に代金を支払った利用者であるかどうかなど）が確認できれば十分であるサービスを，「カジュアルなサービス」と位置付ける．典型的には，比較的廉価なサービスや一時的に利用するサービスが，これに該当する．廉価なサービスであっても安全性が不要というわけではなく，コストバランスを考慮して適度ななりすまし対策が講じられるべきである．コインロッカーなどの一時的なサービスにおいては，個人の所有物（思い入れの深い物品）や貴重品を預かることになるため，重要なサービスと同様になりすましに対する耐性が求められる（要求 1：なりすまし困難性）．

カジュアルなサービスでは，本人性の確認は不要あ

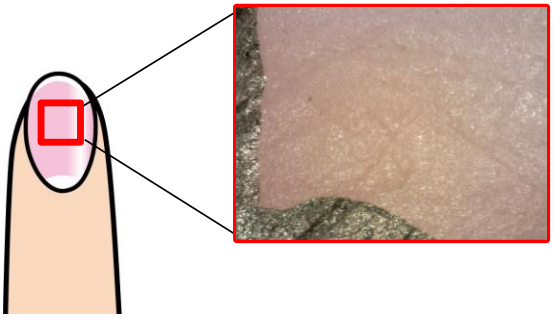


**図 1：爪の表面の模様（黒い領域はマーク）**

るため，認証は匿名あるいは仮名を用いて行えば良い．しかし，生体認証においては，匿名ユーザ群または仮名ユーザ群の中から生体情報を用いて同一ユーザの名寄せが可能である．生体情報は，パスワードやトークンのように変更や交換によって本人との間の紐づきをリセットできないため，複数のサービスのアカウントで同じ生体情報を認証情報として利用していた場合，生体情報からそれらのアカウントが同一ユーザに利用されていることが判明してしまう．すなわち，カジュアルなサービスにおいては，利用者のプライバシ保護も重要なニーズであり，生体情報の追跡を防ぐ必要がある（要求 2：追跡困難性）．

生体認証が普及した結果，様々なサービスの利用シーンにおいて生体情報の提示が求められるようになる．生体情報は，露出の機会が増えれば増えるほど，漏洩のリスクが増加する．特に廉価なサービスにおいては，安全対策のためにコストを多く割けないため，カジュアルなサービスでの生体認証は，重要なサービスに比べ生体情報の漏洩リスクが各段に高まることは必至である．そのため，カジュアルなサービスでは，使用した生体情報を廃棄可能な仕組みが必要である（要求 3：廃棄可能性）．特に一時的なサービス（登録から比較的短期間の内に認証のイベントが完遂するサービス）においては，むしろ，経時変化の大きな生体情報を積極的に採用することによって，過去の生体情報と現在の生体情報の紐づけを完全に断ち切るような方法も有用であろう．

以上より，カジュアルな生体認証では，生体情報の偽造等に対する「なりすまし困難性（要求 1）」，生体情報の名寄せに対する「追跡困難性（要求 2）」，生体情報の取り消しに関する「廃棄可能性（要求 3）」が求められる．

本稿では要求 1～3 を満たすカジュアルな生体認証として，爪表面の模様を用いたマイクロ生体認証を提案する．2 章で既存研究を紹介し，3 章でマイクロ生体認証と提案方式について説明する．次に 4 章で今回使用したシステムを紹介する，5 章で提案方式の可能性を示すための基礎実験を行ない，6 章でその実験を評価する．その後 7 章で考察を述べ，8 章で本稿をまとめる．

## 2. 既存研究

爪を用いた生体認証にはいくつか既存研究が存在する．

Garg らは爪表面全体に確認される縦の筋溝（longitudinal striations）を特徴として利用した認証を提案し，その有用性を示している[5]．しかし，縦の筋溝は指紋同様不変の特徴量であると示されているため，要求 2 や要求 3 を満たしていない．更に，模造物によるなりすましに対する耐性も低いと思われるため，要求 1 も有していない．

Barros Barbosa らは爪表面を利用した生体認証を提案している[6]．爪の生え変わりを利用することにより，要求 3 を満たした認証方式となっているものの，通常のカメラで撮影した爪画像をそのまま認証に利用しているため，模造物の偽造はそれほど難しくなく，また，同じ爪を用いて複数のアカウントを登録した場合は，登録情報（爪画像）によるアカウントの名寄せの可能性が残る．このため，要求 1 と要求 2 を満たしていない．

著者らの知る限り，要求 1～3 を全て満たす生体認証は，著者らの先行研究[8]以外には存在しない．

## 3. 使い捨てマイクロ生体認証

### 3.1. 肌理を利用したマイクロ生体認証

要求 1，2 を満たす生体認証として，著者らは「マイクロ生体認証」と呼ばれる方式を提案している[7]．マイクロ生体認証は，微細生体部位の静的な特徴量を認証情報として利用する．

認証情報の物理サイズが微細になるほど，偽造生体を精密に作成するためのコストが高まり，認証情報として利用可能な生体部位の数が増加する．これにより不正者の偽造コストが高まり「なりすまし困難性」が満たされる．また，正規ユーザに登録生体部位を次々と変更させることによって「追跡困難性」が満たされる．更に，静的な特徴量を使用するため高い認証精度も期待される．

### 3.2. 爪の模様を利用したマイクロ生体認証

要求 3 を満たすマイクロ生体認証を実現するために，時間の経過によって生え変わる生体部位を利用する．本稿では，その一実現形態として，爪の微細部位を利用したマイクロ生体認証を検討する[8]．

爪は，爪先，爪床，爪郭，爪母基，遊離縁などから構成される皮膚の一部である[9]．爪の表面を大きく拡大すると，爪の表面上に不規則な模様の存在を確認で

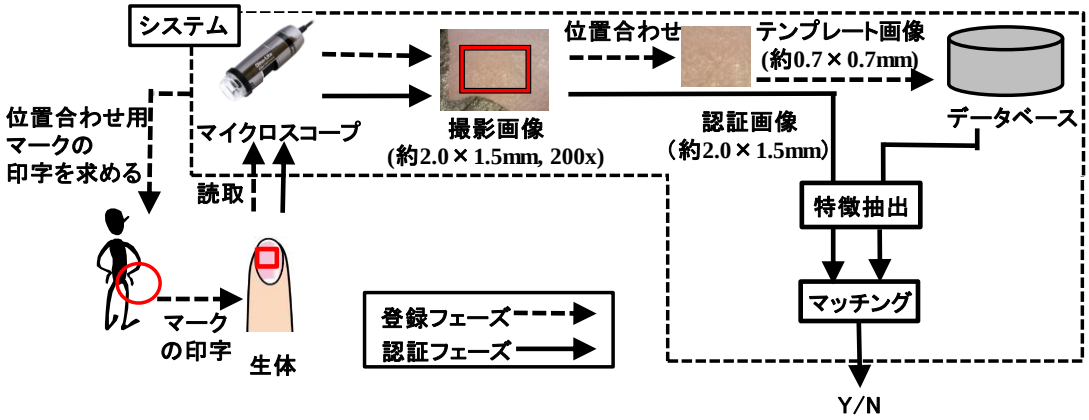



図 2：システム概要図

きる（図 1）．この模様を認証情報として利用することで，爪画像を利用したマイクロ生体認証が実現可能であると期待される．

一般的な若い成人男性の爪の伸びるスピードは，約 0.1 [mm/day]である[10]．爪が伸びて登録部位が遊離縁まで達し，爪を切ることで，それまでの生体情報が廃棄される．生え変わる微細生体部位を利用することによって，要求 1～3 のすべてを満たす「使い捨てマイクロ生体認証」が実現する．

### 3.3. 認証手順

使い捨てマイクロ生体認証の手順を以下に示す（図 2 も参照）．ここでは 1:1 認証の手順を示すが，1:N の認証への適用も可能である．

登録フェーズ：

1. ユーザは自分の ID をシステムへ登録する
2. システムはユーザに，爪表面へマークを印字するよう要求する
3. ユーザは爪表面へマークを印字する
4. システムはマークに従い，マイクロスコープでユーザの微細生体情報 X を読み取る
5. システムはそのユーザのテンプレートとして X をデータベースへ保存する

認証フェーズ：

1. ユーザは自分の ID をシステムへ提示する
2. システムはマークに従い，マイクロスコープでユーザの微細生体情報 X’を読み取る
3. システムはデータベースよりそのユーザのテンプレート T（＝X）を参照する
4. X’が十分 T と近い場合，そのユーザは正規ユーザと判断される

## 4. システム

今回構築したシステムについて詳細に説明する．本システムは，文献[7]で実装したマイクロ生体認証システムがベースに，爪画像から特徴量を抽出するプログラムモジュールを追加することによって作成している．なお，爪画像のテンプレートと認証画像を比較するにあたっては，著者らによる先行研究[8]では，テンプレートマッチングによって爪表面の模様の類似度を求めていた．しかし，爪表面の鏡面反射による撮影時の照明変動によって，本人の画像であっても類似度が低下してしまう問題が明らかになった．このため，本稿においては，Local Binary Pattern 変換の適用を試みる．

### 4.1. 登録部位の発見

マイクロ生体認証においては，システムが爪全体の中から登録微細部位を発見するために，爪の表面にマークを印字する必要がある．本稿では，水性インクを用いて爪の表面にマークを直接印字し，その上からトップコート（透明のマニキュア）を塗ってマークを保護する方法を採用する．油性インクを用いた場合，トップコートが油性のため互いに反発し，インクが滲んでしまうという問題が確認された．そのため本稿では油性インクではなく水性インクを用いている．

### 4.2. 生体部位の撮影

本稿では爪の撮影にマイクロスコープを使用する．使用するマイクロスコープは AM7915-Dino Lite Edge S（サンコー株式会社製）である．このマイクロスコープを用いて爪の表面の約 2.0×1.5mm の領域を 200 倍で撮影することによって，2592×1944 pixel の爪画像が得られる．登録時には，爪画像の中央 800×800 pixel をトリミングし，テンプレート画像として利用する．認証時は，同様に撮影された爪画像（2592×1944 pixel）の中にテンプレート画像（800×800 pixel）が含まれるか否かを探索し，テンプレートと最も類似する 800×800pixel をトリミングする．

### 4.3. 特徴抽出

本システムでは，爪の表面の凹凸パターンを特徴量として利用する．安定した特徴を得るために，テンプ

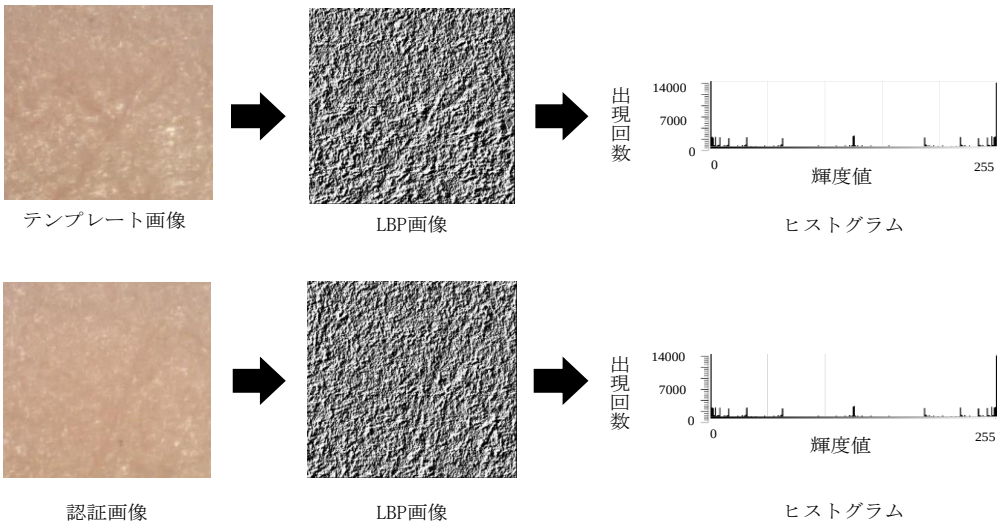



**図 4：特徴抽出とマッチング**

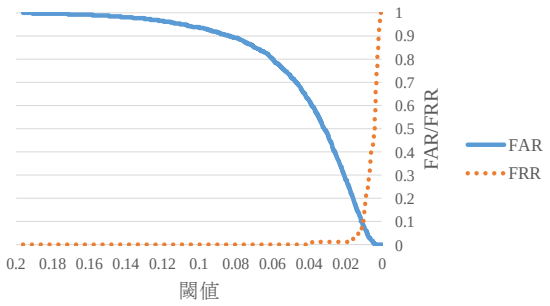



**図 3：総当りで比較した際の FAR，FRR**

レート画像および認証画像をグレースケール変換した後に Local Binary Pattern（以下 LBP）変換を行なう．LBP とは 1994 年に Ojala らによって提案された手法であり，画像の濃淡値の変化に頑健であるという性質を持つ[11][12]．なお，LBP 変換の実装は scikit-image Ver.0.14dev[13]を用いた．

### 4.4. マッチング

マッチングは，LBP 変換後の画像のヒストグラムを比較することで行なう（図 4）．ヒストグラムの比較にはヒストグラム値のカイ二乗値を用いる方式を採用している．テンプレート画像のヒストグラムを $H_1$，認証画像のヒストグラムを $H_2$ とした時のマッチングスコア d（$H_1$,$H_2$）は以下の式で算出する．

$$d(H_1, H_2) = \sum_I \frac{(H_1(I) - H_2(I))^2}{H_1(I) + H_2(I)}$$

## 5. 基礎実験

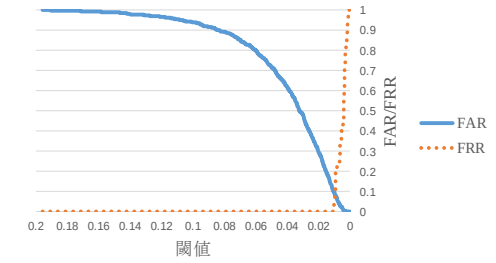
提案方式の有用性を確認するために微細爪画像を用いた基礎的な認証実験を 3 日間に渡って実施した．被験者は同大学の学生 5 名に協力してもらった．1 人あたり右手の人差し指，中指，薬指の 3 つの爪を使用し，各爪で縦に並ぶように任意の 2 箇所を設定し，1 日 1 回それらの画像（計 6 箇所）を撮影した．1 日目は午前中にテンプレート画像を撮影し，午後に 1 日目の認証画像を撮影，2 日目と 3 日目は日中の任意の時間帯に認証画像の撮影を行なった．テンプレートの撮影時，撮影する爪の任意の 2 箇所に水性インクでマークを印字し，その上からトップコートを塗布した．テンプレートはこのマーク付近をマイクロスコープで撮影した．認証画像の撮影は，爪に印字されたマークを基に登録部位を発見し，テンプレート画像と可能な限り見た目が一致するように行なった．

## 6. 評価

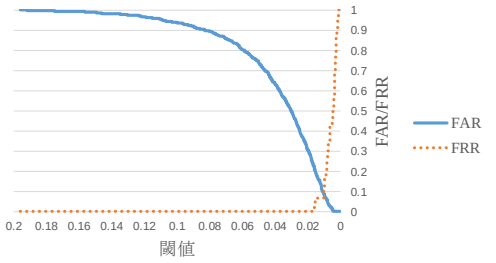
5 章で得られた微細爪画像のサンプルを元に提案方式の評価を行なう．以下，人差し指の根元側の箇所に 1，爪先側に 2 と番号を振り，中指と薬指にも同様に 4~6 の番号を振る．被験者 i（1≦i≦5）の j 番目の部位（1≦j≦6）のテンプレート画像を $t_{i,j}$ と表記し，被験者 k（1≦k≦5）の L 番の部位(1≦L≦6)の m 日目（1≦m≦3）の認証画像を $a_{k,L,m}$ と表記する．

### 6.1. 提案システムの可用性評価

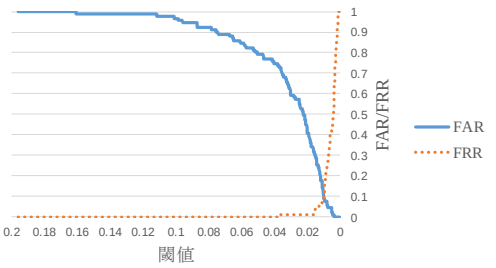
爪の微細部位を用いて認証が可能かを評価する．本人のマッチングスコアは $t_{i,j}$ と $a_{k,L,m}$(i=k, j=L)を比較することで算出し，他人のマッチングスコアは他人の部位，つまり $t_{i,j}$ と $a_{k,L,m}$($i \neq k$)を総当りで比較することで算出する．これらを基に認証閾値を変更した際の本人拒否率（FRR）と他人受入率（FAR）の変化を図 3 に示す．この時の等価エラー率（EER）を算出したところ，閾値≒0.0101 で EER≒0.086 であった．少し EER は高いものの，本システムは爪の微細部位を十分識別可能なシステムだといえる．




1 日目




2 日目




3 日目

**図 5：日毎の FAR，FRR の推移**

## 6.2. 撮影画像変動による影響の評価

3.2 節で述べた通り，先行研究では爪の経時変化や撮影環境の変化によって本人であっても類似度が著しく低下する問題が存在した．そこで本節では，日数が経過しても提案システムの可用性は保たれているかを評価する．具体的には 1 日目の本人スコアを $t_{i,j}$ と $a_{k,L,m}(i=k, j=L, m=1)$を比較することで算出し，他人のマッチングスコアは $t_{i,j}$ と $a_{k,L,m}(i\neq k, m=1)$を総当りで比較することで算出する．2 日目と 3 日目は，m の値を変化させて同様に算出する．これらを基に認証閾値を変更した際の本人拒否率（FRR）と他人受入率（FAR）の変化を図 5 に示す．1 日目の等価エラー率（EER）は，本人スコアの平均≒0.0048（閾値≒0.0094 で EER≒0.073）であった．2 日目は本人スコアの平均≒0.0056（閾値≒0.01 で EER≒0.091），3 日目は本人スコアの平均≒0.0065（閾値≒0.012 で EER≒0.099）だった．今回サンプル数が少ないため統計的な評価は不可能なものの，今回のシステムは先行研究の課題点であった経時による本人スコアの低下を抑えることに成功しているといえる．

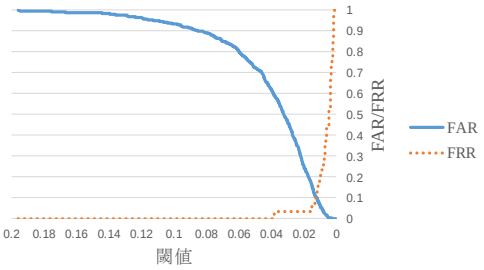



**図 6：同じ爪の異箇所を他人とした際の FAR，FRR**

## 6.3. 使い捨て可能性の評価

爪表面の模様が使い捨て可能な生体部位か否かを評価する．同じ爪の縦方向の別箇所が他人として識別されれば，同じ爪でも位置毎に特徴が異なる，つまり使い捨て可能な生体部位であるといえると考えられる．本人のマッチングスコアは $t_{i,j}$ と $a_{k,L,m}(i=k, j=L)$の比較で算出し，他人のマッチングスコアは同じ爪の異箇所，つまり $t_{i,j}$ と $a_{k,L,m}(i=k, j=L-1$ もしくは $j=L+1)$を比較して算出する．これらを基に認証閾値を変更した際の本人拒否率（FRR）と他人受入率（FAR）を図 6 に示す．この時の等価エラー率（EER）を算出したところ，閾値≒0.101 で EER≒0.093 であった．これは 6.1 節で評価した他人の部位との比較とほぼ同等の EER のため，同じ爪の異箇所は他人の部位と同様であるとみなすことが可能である．

# 7. 考察

## 7.1. 要求 1 に対する考察

本システムでは約 200 倍で拡大した約 0.7×0.7mm の範囲の爪画像をテンプレートとして利用している．不正者がなりすましを成功させるためにはマイクロレベルの偽造物の生成が求められるため，偽造コストは高いと期待される．したがって本システムは，要求 1（なりすまし困難性）を満たしている．

## 7.2. 要求 2 に対する考察

生体部位を微細にすることで，生体部位の更新可能回数（微小部位を 1 つずつ使っていった際に未使用部位が枯渇するまでの回数）が激増する．ユーザは，パスワードの変更やトークンの交換と同様の感覚で，その必要が生じた際に，ユーザ自身の意思で，今まで利用していた生体部位を別の生体部位に変更する．ユーザが生体部位を更新する度に，認証に用いる生体情報が変更され，追跡可能性が分断されることになる．したがって本システムは，要求 2（追跡困難性）を満たしている．

## 7.3. 要求 3 に関する考察

6.3 節に示した通り，爪表面の模様は同一被験者の同一の爪であっても，異箇所ならばそれぞれ異なる．

つまり生え変わった爪は生え変わる前の爪とは別の特徴を持つと考えられるため，使用済みの生体情報を完全に廃棄することが可能となる．そのため，爪表面の模様は使い捨てが可能な生体部位である．したがって本システムは，要求 3（廃棄可能性）を満たしている．

### 7.4. 適用性

1 章で述べたとおり，カジュアルなサービスは廉価なサービスや一時的に使用するサービスが該当する．このうちの廉価なサービスでは，安全性自体は求められるものの，サービスの価値に見合ったコストの対策が求められるため，安全性よりも利便性が優先される場合もある．そのため提案方式の 200 倍率のマイクロスコープを用いた生体認証は廉価なサービスに適していない可能性がある．ただし，安価な低倍率のマイクロスコープや拡大鏡を用いて，利便性を損なわずに安全性が高まる場合は微細生体部位を用いること自体は有用だと考えられる．また，一時的に利用するサービスでは，物品を預かる貴重品ロッカーなど高い安全性が求められることも多いため，提案方式が適していると考えられる．

## 8. おわりに

本稿では，カジュアルなサービスに適した使い捨て可能な生体認証として爪の微細部位を用いた生体認証を提案し，基礎実験を通して評価を行なった．実験結果より，生体認証としての爪の使い捨て可能性や，先行研究で課題となっていた撮影環境の変化による本人認証スコアの大幅な低下が改善された．今回はサンプル数の少ない基礎実験であったため統計学的に評価出来なかったので，サンプル数を増やしての再評価に加え，精度の改善が今後の課題である．

## 文　献


[1] “Japanese bank using fingerprint authentication at its ATMs,” http://www.biometricupdate.com/201512/japanese-bank-using-fingerprint-authentication-at-its-atms, February 2018.

[2] “Privacy Information Center,” https://www.universalorlando.com/web/en/us/privacy-info-center/index.html#subnav-e, February 2018.

[3] Z. Kleinman, "Politician's fingerprint 'cloned from photos," http://www.bbc.com/news/technology-30623611, Feb. 2018.

[4] 産経新聞，“「ピースサインは危険！！」３メートル離れて撮影でも読み取り可能，” http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html, February 2018.

[5] Shruti Garg, Amioy Kumar, and M. Hanmandlu, “Finger Nail Plate: A New Biometric Identifier,” International Journal of Computer Information Systems and Industrial Management Applications, Vol.6, pp.126-138, October 2014.

[6] Igor Barros Barbosa, Theoharis Theoharis, and Ali E. Abdallah, “On the use of fingernail images as transient biometric identifiers,” Machine Vision and Applications, Vol.27, Issue 1, pp.65-76, January 2016.

[7] Masahiro Fujita, Yuto Mano, Takuya Kaneko, Kenta Takahashi, and Masakatsu Nishigaki, ”A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body,“ NBiS2016, pp.159-164, September 2016.

[8] 杉本元輝，藤田真浩，眞野勇人，村松弘明，西垣正勝，“爪の微細部位を利用したマイクロ生体認証，”信学技法，vol.116，no.527，pp.93-97，March 2017.

[9] David de Berker, “Nail anatomy,” Clinics in Dermatology, Vol.31, Issue5, pp.509-515, September–October 2013.

[10] S Yaemsiri, N Hou, MM Slining, and K He, ”Growth rate of human fingernails and toenails in healthy American young adults,” JEADV, vol.24, Issue 4, pp.420‑423, April 2010.

[11] T.Ojala, M. Pietikainen, and D. Harwood, “Performance evaluation of texture measures with classification based on Kullback discrimination of distributions,“ Proceedings of 12th International Conference on Pattern Recognition, vol.1, Jerusalem, Israel, October 1994.

[12] 長谷川修，“Local Binary Pattern とその周辺，“情報処理学会研究報告グラフィクスと CAD, Vol.202-CG-149(3)，pp.1-6，November 2012.

[13] “scikit-image,” http://scikit-image.org/, February 2018.