マイクロ生体認証：人間の微細生体領域を利用した生体認証

藤田 真浩* 眞野 勇人* 村松 弘明* 高橋 健太† 西垣 正勝*

概要. 本稿では,「マイクロ生体認証」と呼ばれる新たな生体認証メカニズムを提案する．本メカニズムは，生体の微細部位を生体認証へ応用するものである．微細部位を利用することによって，なりすましに対する高い耐性を有し，かつ，プライバシ（追跡可能性）に対する配慮がなされた生体認証が実現される．生体部位の静的な生体情報を利用することで，実用レベルの認証精度も達成可能である．本稿では，マイクロ生体認証の一事例として，マイクロスコープによって撮像される人間の微細肌理画像を用いた生体認証システムを構築した．ユーザ実験を通じて，肌理を利用したマイクロ生体認証の有用性を検証した. その結果, 肌理を利用したマイクロ生体認証が, なりすましに対する高い耐性を有すること，追跡可能性に対する十分な配慮がなされていること，実用レベルの認証精度を有することを確認した.

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．通常，事前に採取した生体情報をテンプレートとして登録し，認証時に取得した情報とテンプレートを比較することで認証を行う．近年では実用化が進み，PC，ATM，パスポートの認証手段としても利用されてきている．最近では，オンライン認証の新業界標準の確立を狙う Fast Identity Online Alliance（FIDO）[1]が，ユーザ端末をアクティベートさせる認証手段として生体認証を有力視していることから，生体認証に益々注目が集まっている．また，公開鍵基盤（PKI）における秘密鍵を生体情報で置き換える「テンプレート公開型生体認証基盤（PBI）」が提案されている[2]. FIDO や PBI によって，今後さらなる生体認証の普及が予想される.

生体認証は，パスワードやトークンを用いた認証方式と異なり，忘却・紛失・盗難の恐れがないという利点がある．しかし一方で，生体認証には生体情報を用いるが故の課題がある．最も大きな課題が，生体情報の「基本的に生涯不変であり，任意に更新できない」という性質に起因する，なりすまし，および，追跡可能性に関する課題である.

「なりすまし」は，攻撃者が正規ユーザの生体情報を入手して偽造生体を作成する攻撃である．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．また攻撃者は，生体情報読取装置を正規ユーザの生活環境内に密かに仕込んで生体情報を収集したり，生体認証によってログインする正規の Web サービス提供サイトを装ったダミーサイトを設置して生体情報をフィッシングしたりすることも可能である．生体認証を実現するにあたっては，この「なりすまし」に対する耐性を有する必要がある（要求 1：なりすましに対する耐性）.

「追跡可能性」に関して，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，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を名寄せすることが可能である．たとえば，複数の Web サイト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．追跡可能性の観点から，生体情報の漏えいを防ぐ必要がある（要求 2：追跡可能性に対する考慮）.

課題 1,2 を部分的に解決する方法として，テンプレート保護型生体認証方式が提案されている．その代表例が，生体情報と乱数情報を組み合わせることにより，テンプレートを保護するキャンセラブル生体認証[5]である．乱数情報によって生体情報が秘匿されるため，テンプレートからの生体情報の漏えいが防がれ，要求 1 を満たす．また，乱数情報を変更することによってテンプレートの更新が可能となるため，要求 2 も満たしている．しかし，テンプレート以外の経路での生体情報の漏えいに対する対策にはなり得ていない.

テンプレート以外の経路で生体情報が漏えいしてしまった場合に対する対策としては，提示された生体情報が偽造物でない（生きている人間の生体情報である）ことを検査する生体検知技術[6]や，生体情報読取装置の真正性を検査するデバイス認証[7]が

* 静岡大学, † 株式会社日立製作所

存在する．しかし，これらはいずれも要求 1 に対処するものであり，要求 2 に対する対策とはなり得ていない．

ある時点での生体情報そのものが漏えいしてしまったとしても要求 1,2 を達成する方式が，生体情報のワンタイム化である．テキスト独立（text independent）型あるいはテキスト指定（text prompted）型の手書き署名認証や音声認証がその実例である．しかし，生体情報のワンタイム化が可能なのは基本的に動的な生体情報に限られる．一般に動的な生体情報を利用した場合の認証精度は低いことが知られており[8]，静的な生体を利用することで高い認証精度を確保することが望ましい（要求 3：静的な生体情報の利用による認証精度の確保）．

以上の議論から，「静的な生体情報のワンタイム化」が実現できれば，要求 1〜3 をすべて満たす生体認証となり得ると考えられるが，「静的」な生体情報は本質的にワンタイム化とは相容れない．

そこで，生体の微細部位を生体認証へ応用することで要求 1〜要求 3 を満たす生体認証を実現する．本稿では，この生体認証メカニズムを「マイクロ生体認証」と呼ぶ．マイクロ生体認証の一事例として，マイクロスコープによって撮像される人間の肌理画像を用いた認証システムを構築する．ユーザ実験を通じて，肌理を利用したマイクロ生体認証の 1 日間の認証精度を測り[1]，その応用について議論する．

以降，2 章ではマイクロ生体認証のコンセプトを述べるとともにその一事例（肌理を利用したマイクロ生体認証）について示す．3 章では肌理を利用したマイクロ生体認証のプロトタイプシステムを構築する．開発したシステムを用いて 4 章で実験を行ったのち，その結果について 5 章で議論をする．6 章でまとめと今後の課題を述べる．

なお，本研究のコンセプトはすでに文献[9]で発表している．本稿は，文献[9]で発表したコンセプトを再度論ずるとともに，プロトタイプシステムを改良してユーザ実験を行い，その有効性と適用先に関する議論を行うものである．

2　マイクロ生体認証の提案とその一事例

2.1　コンセプト

前述のように，要求 1〜3 を満たす生体認証が求められる．静的な生体情報を利用すれば，要件 3 を満たすことが可能である．しかし，（通常の）静的な生体情報は，なりすましが容易であり，ワンタイム化が困難であるため，要求 1 と 2 を満たさない．そこで，本稿では静的な生体情報の微細部位を生体認証へと応用することで，要求 1〜3 を満たすことを実現する．このメカニズムを「マイクロ生体認証」と呼ぶ．マイクロ生体認証は，下記のとおり，要求 1〜3 を満たす．

要求 1：

一般に，模倣品をより細部まで作り込むにつれて，その製造にかかる手間が非常に高くなるが，ズームレンズを使って対象物の細部を撮影することは，模造に比べはるかに容易である．この「撮影と偽造のコストの非対称性」を利用し，ある微細部位の生体情報をテンプレートとして登録することによって，たとえその部位の情報が盗まれたとしても偽造に大きなコストを要する生体認証が実現される．

要求 2：

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．

要求 3：

生体部位の静的な情報を利用するため，認証精度も（動的な生体情報を利用する認証と比較して）高い．

2.2　肌理を利用したマイクロ生体認証

本稿では，マイクロ生体認証の一事例として，拡大した肌理画像を生体認証へと応用する．

人の皮膚表面を細かく観測すると凹凸があることが認められる．これらは「皮溝」と呼ばれる種々の深さや長さの溝，「皮丘」と呼ばれる浅く細い皮溝で囲まれる細かい隆起，「皮野」と呼ばれるやや深い皮溝で囲まれる多角形の隆起により構成される．その他にも毛穴や汗腺などの要素もあり，毛穴は皮溝の交点に多く見られ，ほとんどの場合で開口部の面積と深さは比例していることや，汗腺は皮丘の頂上に開いていることが報告されている．肌理はこれらの要素により形作られる皮膚紋様であり，そのパターンは大きくとも数百 μm 程度で微細であり，一様ではないため，精密に模造することは困難であることが期待できる．

本論文では，肌理の表層状態（凹凸パターン）に注目する．肌理の凹凸パターンが安定して取得可能

[1] 長期的な実験およびその応用に関しては，文献[10]で報告予定である．

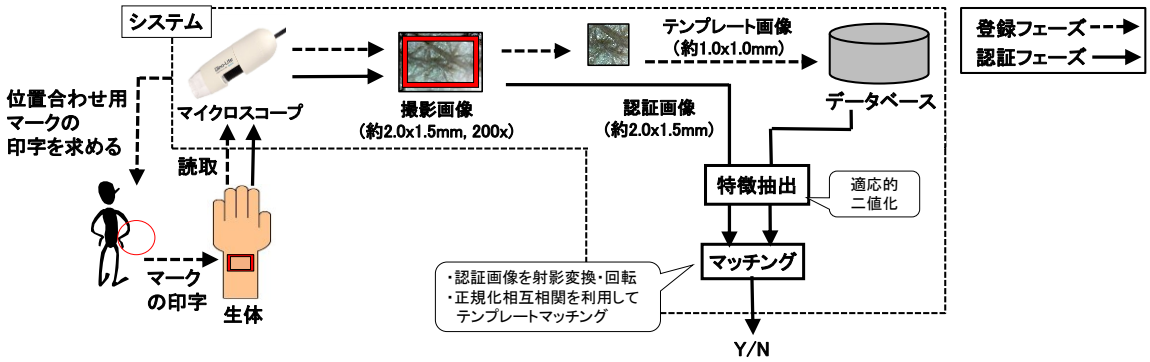

図 1. プロトタイプシステムの構成

であり，かつ，十分な多様性が認められるならば，指紋や掌紋の様に個人認証に利用することが可能となる．なお，肌分析のための手法は化粧品開発の分野などで活発に研究されている．これらの分析はあくまで医療目的などに限定されており，著者らが調べた範囲では拡大した肌理を用いた認証に関する既存研究は報告されていない．

2.3 肌理を利用したマイクロ生体認証の認証手順

拡大した肌理画像を利用したマイクロ生体認証の認証手順を説明する．ここでは，1 対 1 認証を例として説明するが，1 対 N 認証へも適用可能である．

【登録フェーズ】

1. ユーザは，ユーザ ID を決定しシステムへ登録する．
2. システムは，登録部位を示す位置合わせ用のマークの印字をユーザに要求する．
3. ユーザは，自分の身体の任意の位置にマークをつける．
4. システムは，マークの近くの部位の生体情報を読み取り，その特徴量を X とする．X はデータベースに登録される．

【認証フェーズ】

1. ユーザは，ユーザ ID をシステムに入力する．
2. システムは，マークで示された部位の生体情報を読み取り，その特徴量を X'とする．
3. システムは，データベースからユーザ ID と紐付いている登録情報 X を取り出す．
4. システムは，X と X' が十分類似していれば認証成功とする．

なお, 提案方式における認証フェーズにおいては，ユーザが身体にマークを保持し続けていることが前提となることに注意されたい．また，ユーザがマークを消してしまえば，システムは登録部位を発見することが難しくなるため，本人でさえも認証成功が困難となる．

3 プロトタイプシステムの実装

肌理を利用したマイクロ生体認証のプロトタイプシステムを実装した. その構成を図 1 に示す. なお，本システムは文献[9]で実装したシステムの一部を改良したものである．

3.1 登録部位の発見

マイクロ生体認証においては，システムが登録部位（肌理）を発見するために，ユーザが肌の表面にマークを印字する必要がある．このマークの位置を変更するたびに，ユーザは認証で利用する生体情報を変更することが可能となる．本稿では，プロトタイプであるため，最も単純な方法である「油性インクによってマークを印字する方法」を採用した．

3.2 生体部位の撮影

皮膚表面の形態情報を取得するには主に 3 種類の手法があげられる．レプリカを用いて表面形態を転写し共焦点顕微鏡などで取得する方法，三次元スキャナを用いて非接触で表面形態情報を取得する方法，マイクロスコープを用いて表面形態の拡大画像を撮像する方法，の三つである[11]．本稿は，プロトタイプであるため，最も安価で容易に利用可能な，マイクロスコープを利用する方法を採用した．使用したマイクロスコープは AM2001-Dino Lite Basic（サンコー株式会社製）である．

本システムにおいては，200 倍に拡大したマイクロスコープで撮影した肌理画像（640×480 pixel，約 2.0×1.5mm）の中央 256×256 pixel（約 1.0×1.0mm）を切り出し，それをテンプレート画像として利用する．

3.3 特徴抽出

本稿では，肌理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，テンプレート画像，および，認証画像は，マッチング前に適応的 2 値化を施して 2 値化画像に変換している．適応的 2 値化は，Open CV Ver. 2.4.9 に実装されている関数 cvAdaptiveThreshold()によって行った．関数

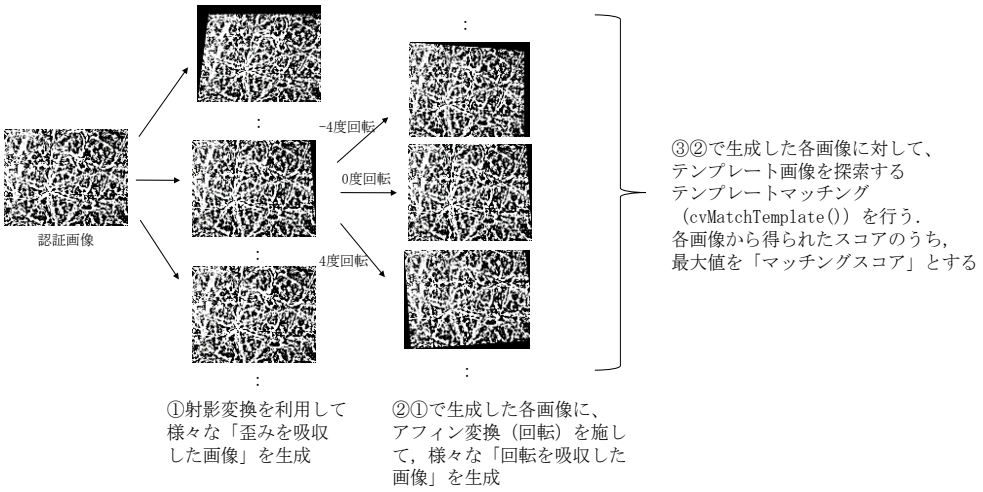

図 2. マッチングアルゴリズムの概要

のパラメータは，inThresholdType を THRESH_BINARY，inBlockSize を 25 とした．

3.4 マッチング

システムは，位置合わせ用のマークによって，テンプレート画像とほぼ同じ位置の肌理画像（認証画像）を得ることができる．しかし，マイクロスコープのわずかな傾きや位置ずれによって，この画像は（テンプレート画像と比較して）歪みや位置ずれを起こしている場合が多い．これらは，ノイズとなり，マッチングスコアの低下（認証率の低下）を引き起こす． そこで，撮影した画像に対して，射影変換とアフィン変換（回転）を施して，これらのノイズを吸収したのち，テンプレートマッチング（正規化相互相関）を利用してスコアを求めた．テンプレートマッチングは，Open CV Ver2.4.9 で実装されている cvMatchTemplate()で行い，引数 method（テンプレートマッチングの方法）の値は CV_TM_CCOEFF_NORMED を利用した．

以上をまとめたマッチングアルゴリズムの概要を図 2 に示す．本稿では，紙面の関係上，マッチングアルゴリズムやパラメータ設定に関する詳細な議論は割愛する．

4 基礎実験

肌理を利用したマイクロ生体認証の 1 日間の認証精度をユーザ実験によって求める．

4.1 肌理画像の収集

静岡大学の学生 8 名（全員男性）に協力してもらい，1 名当たり任意に 10 箇所の肌理を採取した．体毛が少ないことや，撮影が比較的容易な部位であることから，撮影範囲は前腕部内側に限定した．利用する腕は，左腕で統一した．実験実施期間は 1 日間である．

実験実施日の午前にテンプレート画像の撮影を行った．各被験者の左前腕部 10 箇所に油性インクでマークを印字し，それぞれのマークを基準にして，（マーク近くの）肌理をマイクロスコープで撮影した．3.2 節で示したとおり，この画像の中央 256×256 pixels をテンプレート画像として利用する．その結果，8 名×10 箇所=80 枚のテンプレート画像を収集した．

実験実施日の午後（テンプレート画像撮影から 6 時間以上経過した後)に,認証画像の撮影を行った．認証画像の撮影は，実験実施者（著者）が目視で調整することで行った．具体的には，肌に印字された各マークを参考にして，登録部位を発見したのち，撮影する肌理画像の見た目がテンプレート画像とできる限り一致するように撮影を行った．その結果，8 名×10 箇所=80 枚の認証画像を収集した．

4.2 評価方法

4.1 節で得た被験者 i（1≦i≦8）の j（1≦j≦10）箇所目のテンプレート画像を $t_{i,j}$ と定義する．同様に，被験者 k（1≦k≦8）の l（1≦l≦10）箇所目の認証画像を $a_{k,l}$ と定義する．これらを利用して，3.3 節，3.4 節の手順に沿って，以下の三つのマッチングスコアを計算する．

① 同じ被験者内の同箇所間のマッチングスコア．すなわち，$t_{i,j}$ と $a_{k,l}$（i＝k, j＝l）間のマッチングスコア．このとき，$t_{i,j}$ と $a_{k,l}$ の組み合わせは 80 通りであるため，得られるスコアの総数は 80 である．

② 同じ被験者内の違箇所間のマッチングスコア．すなわち，$t_{i,j}$ と $a_{k,l}$（i＝k, j≠l）間のマッチングスコア．このとき，$t_{i,j}$ と $a_{k,l}$ の組み合わせは 720 通りである．ただし，本稿では，実験時間

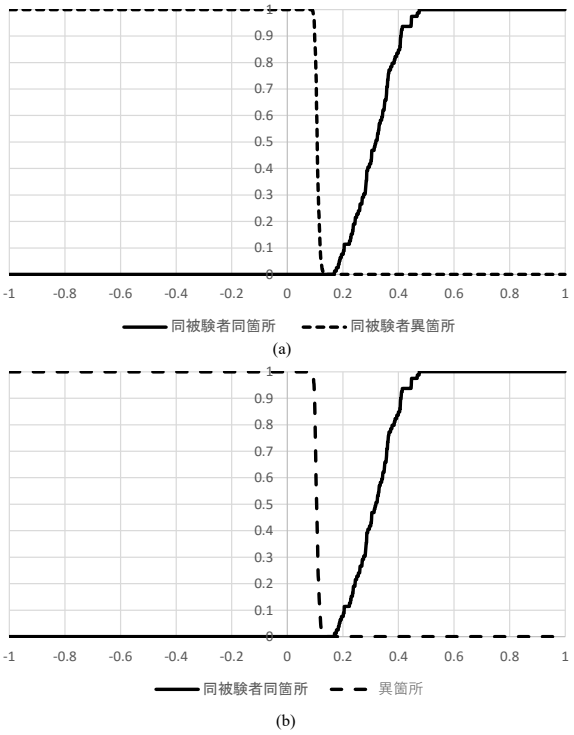

図 3. 実験システムにおける FRR,FAR

短縮のため，このうち 300 通りの組み合わせをランダムに抽出し，それらのスコアを求めた．すなわち，得られるスコアの総数は 300 である．

③ 異なる箇所間のマッチングスコア．すなわち，$t_{i,j}$ と $a_{k,l}$（$i \neq k$ または $j \neq l$）間のマッチングスコア．このとき，$t_{i,j}$ と $a_{k,l}$ の組み合わせは 6320 通りである．ただし，本稿では，実験時間短縮のため，このうち 300 通りの組み合わせをランダムに抽出し，それらのスコアを求めた．すなわち，得られるスコアの総数は 300 である．

4.3 結果

4.2 節に示した三つのスコアの計算を行った．スコア①（同被験者同箇所間）とスコア②（同被験者異箇所間）をもとに，本人と他人を切り分ける閾値を変更した場合の本人拒否率（FRR）と他人受け入れ率(FAR)の変化を記したグラフが図 3(a)である．スコア①とスコア③（異箇所間）をもとに，FRR と FAR の変化を記したグラフが図 3(b)である．

マッチングスコア①～③を，それぞれ，仮に正規分布と仮定して等誤理率 (EER) を計算したところ，図 3(a)においては認証閾値≒0.13 の際に EER≒0.5%であった．図 3(b)においては，認証閾値≒0.13 で EER≒0.6%であることが確認できた．

5 議論

5.1 要求 1 に対する考察

プロトタイプシステムでは約 1.0×1.0mm の範囲の肌理を倍率約 200 倍で拡大した画像をテンプレート画像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（単純計算で）約 1μm レベルの偽造物の生成が求められるため，偽造コストは非常に高い．したがって，プロトタイプシステムは，要求 1（なりすましに対する耐性）を満たしているといえる．

5.2 要求 2 に対する考察

4.3 節に示した結果（図 3(a)）より，同じ被験者の同じ箇所間の FRR と同じ被験者の異箇所間の FAR を求めた結果，それらの EER は約 0.5%であった．本結果は，同じ被験者であっても利用する肌理の部位が違えば，異なる生体情報としてみなせることを意味している．

人間の肌の総表面積は約 1.6m² であるといわれているため[12]，仮に 1.0×1.0mm を登録面積とすると，理論上約 2.6×10^6 通りの生体情報を利用可能となる．服を脱がないと採取できない部位を考慮したとしても，数千から数万パターンの生体情報が利用可能である．これらのパターンを利用することで，ユーザは自身の登録生体情報を更新し続けることが可能となる．

以上の議論より，プロトタイプシステムは，要求 2（追跡可能性に対する考慮）を満たしているといえる．

5.3 要求 3 に対する考察

4.3 節に示した結果（図 3(b)）より，今回の評価実験において，プロトタイプシステムが有する EER は 0.6%であった．筆者らが知る限り，提案方式と同等の認証精度を誇る動的生体認証は存在しない．したがって，プロトタイプシステムは，要求 3（静的な生体情報の利用による認証精度の確保）を満たしているといえる．

5.4 アプリケーションに関する議論

実験結果より，提案方式は少なくとも 1 日の間，実用レベルの認証精度を有することが確認された．今回の実験から，少なくとも，駅のロッカーの開閉や遊園地の入退場管理といった，短期的に利用するシステム（ショートターム型認証システム）に対しては，提案方式の適用が可能であることが示された．提案方式においては，位置合わせのために「認証フェーズにおいてマークが保持されている」ことが前提となる．ショートターム型認証システムであれば，短期間の利用に限られるため，マークが消失する心配も少ない．

6 おわりに

生体認証が抱える課題を解決したマイクロ生体認

証を提案した．微細肌理画像を利用したプロトタイプシステムを開発し，1 日間の実験を行い，その結果を通じて,マイクロ生体認証の有用性を確認した．今後は，より微細な領域を利用した認証の実現可能性の評価など，提案システムをさらに改良するとともに，より長期的かつ大規模な実験，および，他のモダリティの利用についても模索していきたい．

謝辞

本研究をご支援してくださった産業技術総合研究所大塚玲様，大木哲史様，静岡大学中谷広正教授，佐治斉教授にここで深く謝意を表します．本研究は JSPS 科研費 JP15K12036 の助成を受けました．

参考文献

[1] FIDO Alliance. https://fidoalliance.org/. （2016/08/28 確認）

[2] Y. Kaga et al. Biometric Authentication Platform for a Safe, Secure, and Convenient Society—Public Biometrics Infrastructure. Hitachi Review, vol. 64, no. 8, pp. 472–479, 2015.

[3] T. Putte, and J. Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. Proc. IFIP TC8 / WG8.8 Fourth Working Conf. on Smart Card Research and Advanced Applications, pp. 289-303, 2000.

[4] Politician's fingerprint 'cloned from photos' by Zhacker. http://www.bbc.com/news/technology-30623611. （2016/08/28 確認）

[5] C. Rathgeb, and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. Journal on Information Security, pp. 1–25, 2011.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing Security and Privacy in Biometrics-based Authentication Systems. IBM Systems Journal, vol. 40, no.3, pp.614-634, 2001.

[7] 宇根正志，田村裕子．生体認証における生体検知機能について．金融研究，vol. 24, 別冊 2， pp.1-56, 2005.

[8] バイオメトリクスセキュリティコンソーシアム．バイオメトリックセキュリティ・ハンドブック．オーム社， 2006.

[9] M. Fujita et al. A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body: A proposal and the first attempt. Proc. of NBiS 2016, 2016. (to be appeared)

[10] 藤田真浩, ほか. 肌理画像を利用したマイクロ生体認証の長期実験に関する報告．電子情報通信学会バイオメトリクス研究会 10 月研究会予稿集（発表予定）

[11] 荒川尚美, 大西浩之, 舛田勇二．ビデオマイクロスコープを用いた皮膚の表面形態解析法の開発とキメ・毛穴の実態評価．日本化粧技術者会誌，vol. 41，no. 3, pp. 173-180, 2007.

[12] A. E. Bender, and D. A. Bender. Body Surface Area. A Dictionary Food and Nutrition, Oxford, England. Oxford University Press, 1995.

未来ビジョン

生体認証は,「生体情報の変更が効かない」という根本的な問題をはらんでいる．生体認証システムの中では，①生体部位の生体情報が読み取られた後，②その生体情報がビット列に符号化され，テンプレートとして登録される．ここで，②の生体情報（テンプレート）の更新に対しては，近年，暗号技術と生体認証技術を融合する研究が大きく飛躍し，「テンプレート保護」技術として結実した．テンプレート保護技術によって，同一の生体情報から異なるテンプレートを任意に生成させることが可能となるため，テンプレートを再生成する度にテンプレートが更新される．

その一方で，①の生体情報（人間の生体情報そのもの）を更新する方法に関しては，今まで誰もその解決の糸口を見つけることができていなかった．本研究は，この究極の最難関課題に対する果敢な挑戦である．筆者らは現在，肌理以外のモダリティとして,「爪」に着目している．爪の表面の拡大画像を利用したマイクロ生体認証システムが構築できれば,「一定期間後に生え変わる生体情報」を用いたショートターム生体認証が実現するため，生体認証においては不可避と思われていた「トレーサビリティに関するプライバシの懸念」が完全に解消する．