「マルチメディア，分散，協調とモバイル
(DICOMO2017)シンポジウム」 平成29年6月

肌理を利用したマイクロ生体認証：プロトタイプシステムの構築

藤田 真浩[1] 眞野 勇人[1] 村松 弘明[1]
高橋 健太[2] 大木 哲史[1] 西垣 正勝[1]

概要：マイクロ生体認証は，人間の微細生体情報を利用した生体認証メカニズムである．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．静的な生体部位を利用することで，実用レベルの認証精度も達成可能である．筆者らは文献[8]にて，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肌理画像を利用した「肌理を利用したマイクロ生体認証」を提案した．本稿は，肌理を利用したマイクロ生体認証に関して，プロトタイプシステムを構築するものである．本稿の内容は次の三つの内容から構成される．はじめに，肌理を利用したマイクロ生体認証について，その内容を説明する．次に，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し，その動作を詳細に説明する．最後に，構築したプロトタイプシステムに関して考察を行い，実用化に向けた課題を議論する．

Micro Biometric Authentication using Skin Texture: Development of Prototype System

MASAHIRO FUJITA[1] YUTO MANO[1] HIROAKI MURAMATSU[1]
KENTA TAKAHASHI[2] TETSUSHI OHKI[1] MASAKATSU NISHIGAKI[1]

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．「生涯不変の情報であり，取り替えが効かない」ことに起因する「なりすまし」および「追跡可能性」の問題である．

「なりすまし」は，攻撃者が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][5]．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たりして生体情報をフィッシング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高い耐性）．

「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，ある生体情報を秘密情報として用いて「アカウント A」のユーザ名でシステムに登録していた正規ユーザが，アカウント A の登録を削除し，同じ生体情報を用いて「アカウント B」として再登録したとする．このとき，システム管理者はアカウント A とアカウント B の秘密情報が同一の情報であることを確認することによって，アカウント A と B が同一ユーザのものであ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）．

1 静岡大学
Shizuoka University
2 日立製作所
Hitachi, Ltd.

要求 1,2 を部分的に達成する方法として，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[6]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，生体情報そのもの（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．

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[7]，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）．

これら要求 1〜 3 を満たすため，筆者らは，新たな生体認証メカニズム「マイクロ生体認証」を提案した[8]．マイクロ生体認証は，人間の微細部位の生体情報を利用した生体認証である．文献[12]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肌理画像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，3 日間にわたるユーザ実験を実施した．その結果，肌理を利用したマイクロ生体認証の短期期間（3 日間）における有用性（要求 1〜 3 を満たすこと）を示した．

ただし，文献[12]で構築したプロトタイプシステムは，位置合わせを手動で行う等，Proof of Concept レベルの実装であった．そこで本稿では，文献[12]で構築したプロトタイプシステムを改良し，Proof of Implementation プロトタイプシステムを構築する．

以降，2 章でマイクロ生体認証および肌理を利用したマイクロ生体認証について紹介する．3 章では提案方式のプロトシステムを構築し，その動作について詳細に説明をする．4 章では，構築したプロトタイプシステムに関して考察する．最後に 5 章でまとめと今後の課題を述べる．

2. マイクロ生体認証とその一事例（肌理を利用したマイクロ生体認証

筆者らは，文献[8][12]でマイクロ生体認証とその一事例（肌理を利用したマイクロ生体認証）の提案を行った．本章では，文献[8][12]の内容を概説する．

2.1. コンセプト

1 章に示したとおり，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，本論文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（なりすましに対する耐性）：

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（追跡可能性に対する考慮）：

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（静的な生体情報の利用による認証精度の確保）：

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

文献[8]では，マイクロ生体認証の一事例として，マイクロスコープで拡大した肌理画像を生体認証へと応用した．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．

肌理の特徴量としては，表層状態（凹凸パターン）を利用することが可能である．肌の凹凸パターンに個人認証可能な十分な多様性が認められることは，文献[12]の実験によって確認されている．

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する例を用いて，マイクロ生体

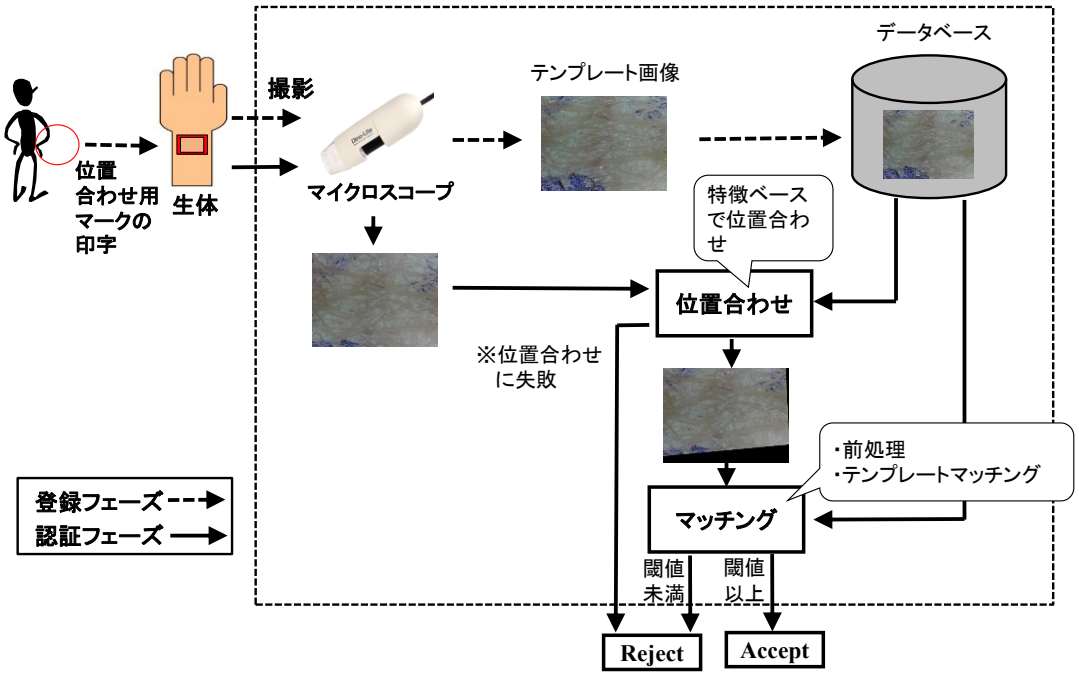

図 1. プロトタイプシステムの全体像

認証の手順を説明する．ここでは 1 対 1 認証を例として説明をする．提案方式は 1 対 N 認証の場合にも適用可能である．

【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．

3. プロトタイプシステムの構築

文献[12]で構築したプロトタイプシステムは，位置合わせを手動で行う等，Proof of Concept レベルの実装であった．そこで本稿では，文献[12]で構築したプロトタイプシステム改良し，Proof of Implementation レベルのプロトタイプシステムを構築した．構築したプロトタイプシステムの全体像を図 1 に示す．以下に詳細を説明する．なお，各パラメータは，プロトタイプシステムを開発する過程で複数の値を試し，最も適切な値を経験的に決定したものである．

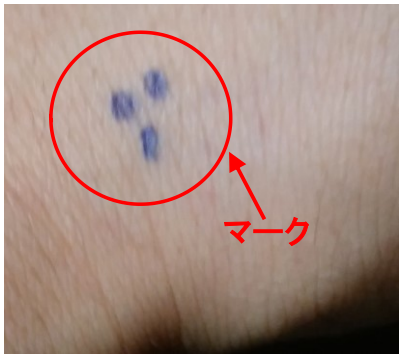

図 2. マーク

3.1. マーク

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．本論文では，最もシンプルな手法として「油性インクによってマークを印字する方法」を採用した．今回利用したマークを図 2 に示す．図 2 に示したとおり，四角形の左上，右上，左下の頂点 3 点に油性インクで印字することでマークを実現している．

3.2. テンプレートの撮影

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[9]．本システムでは，この三つの方法のうち，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．

テンプレートの撮影は，ユーザ自身が行うこととした．前節に示したマークに囲まれた四角形の微細肌理領域をユーザが撮影し，テンプレートとして利用する．テンプレートは，200 倍に拡大したマイクロスコープで撮影し，そのサイズは 640×480 pixel（約 2.0×1.5mm）である（ただし，後述のとおり，マッチングスコア算出にあたっては，テンプレート画像の中央 256×256pixel，約 1.0×1.0mm のみを使用する）．

3.3. 認証画像の撮影

認証時に，ユーザはマークに囲まれた四角形の微細肌理領域を撮影する．認証画像の撮影条件は，テンプレート画像の撮影条件と同様である．

3.4. 位置合わせ

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，テンプレート画像とユーザが撮影した認証画像間で，システムが位置合わせを行う．位置合わせの方法は，特徴ベースマッチングを採用した．具体的な手順は次のとおりである．

（1） テンプレート画像・認証画像それぞれに対して，特徴量を算出する

（2） （1）で算出した特徴量を利用し，認証画像がテンプレート画像と可能な限り一致するように，認証画像に変換を施す．

以上の手順の実装にあたっては，Mathematica Ver.11[10]で実装されている，ImageCorrespoindingPoints（画像間の対応点の算出），FindGeometricTransform（幾何変換を求める），ImagePerspectiveTransformation（透視変換を実施する）をこの順で利用した．ImageCorrespoindgPoints の Method は KAZE を利用した．FindGeometricTransform では Method に RANSAC を採用した．位置合わせ実施前後の様子の一例を図 3 に示す．

なお，位置合わせに失敗する（テンプレート画像・認証画像間で対応する特徴点対が十分に存在しない）場合も存在する．この場合，システムはこの時点で，ユーザを正規ユーザでないと判定する．

3.5. マッチング

テンプレート画像と（3.4 節で位置合わせされた）認証画像間でマッチングを行い，マッチングスコアを求める．具体的な手順はつぎのとおりである．

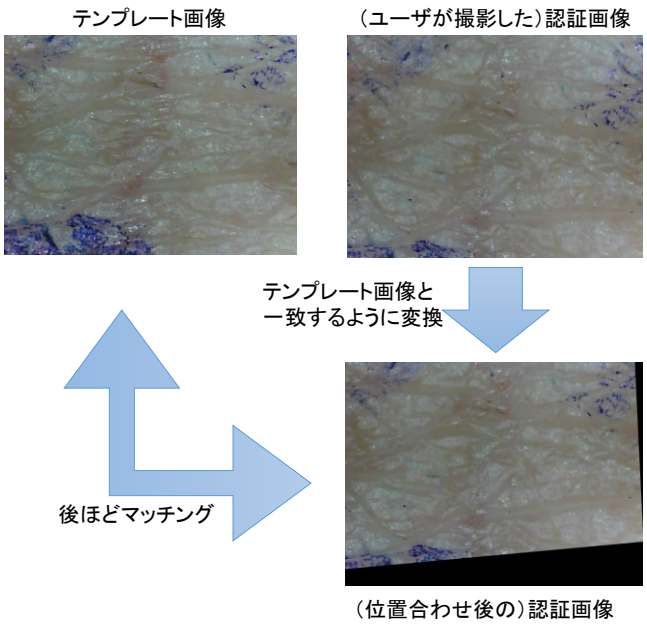

図 3. 位置合わせ後の認証画像

（1） テンプレート画像・認証画像に対してそれぞれ前処理を施す．今回は，「グレースケール化」「ヒストグラム均一化」「適応的 2 値化」をこの順で施して前処理を行った．

（2） テンプレート画像の中央 256×256pixcl を切り抜いた画像を用意する．位置ずれ部分（認証画像に移っていない領域）を考慮するため，テンプレート画像の一部をスコアの算出に利用していることに注意されたい．

（3） （2）で用意した画像をテンプレートとして，認証画像に対してテンプレートマッチングを施す．テンプレートマッチングによって求められたマッチングスコアが閾値以上であれば，システムはユーザを正規ユーザとして判定する．閾値未満であれば，正規ユーザでないと判定する．

以上の手順で，前処理の実装にあたっては，opencv Ver. 2.4.9[11]で実装されている関数 cv::cvtcolor()，cv::equalizeHist()，cv::adaptiveThreshold()を利用した．cvAdaptiveThreshold()のパラメータは，maxValue を 255，adaptiveThreshold を CV_ADAPTIVE_THRESH_MEAN_C，thresholdType を CV_THRESH_BINARY_INV，inBlockSize を 25 とした．これら前処理を施した画像の様子を図 4 に示す．テンプレートマッチングの実装にあたっては，Open CV Ver.2.4.9 で実装されている cv::matchTemplate()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．閾値は，文献[12]で求めた値（0.14）とした．

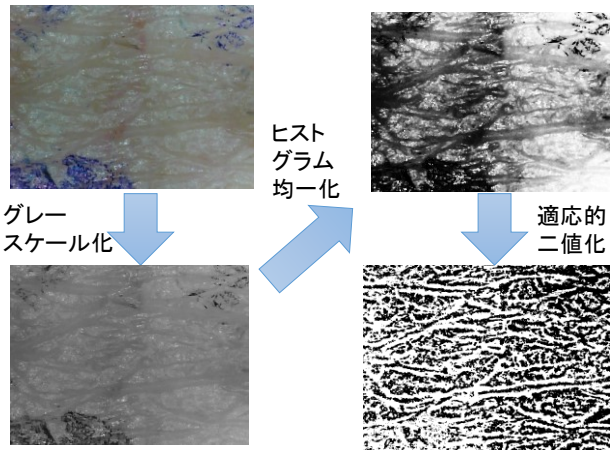

図 4. 前処理を施した画像の一例

4. 考察

4.1. 評価に関して

本稿執筆時点では，プロトタイプシステムを実装するにとどまっており，構築したシステムのユーザビリティ評価を行うことは今後の課題である．実用化にむけて，ユーザビリティ評価やさらなる考察を通じて，次のような事項を調査し，Proof of Implementation レベルのプロトタイプシステムを実用化レベルまで改良する必要がある．

- 認証精度
- 認証時間
- 位置合わせに成功する／失敗する際のノイズの程度（マイクロスコープがどの程度傾きや位置ずれがあった場合に認証失敗するか）
- 偽造困難性
- 閾値
- 適切なパラメータの理論的な分析（3.1 節に記した通り，現時点では，経験的に定めたものである）

ただし，文献[12]にて，微細肌理模様によって実用レベルの個人認証精度が確認されていることに鑑みるに，改良を重ねることで，実用レベルの個人認証システムを実現可能であることが十分に期待される．

4.2. マークとアプリケーションに関して

提案方式では，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．本稿で実装したプロトタイプシステムでは，油性インクのマークを利用している．油性インクのマークであるため，保持できる期間は比較的短い．したがって，現状のプロトタイプシステムの適用先は，遊園地の 1 日入場券やロッカーの開閉といった短期間の認証システム(ショートターム型認証)といった範囲に限定される．今後，より長期的に保持可能なマークを検討したい．

4.3. 非接触型撮影機器の利用

現状のシステムでは，撮影時に，ユーザ自身がマイクロスコープを用いて，マークを基準として登録部位を発見した後，その部位を撮影する仕様となっている．システムがこの仕様であることは，価格や実装コストの点でメリットはあるものの，ユーザの認証における手間を大きく増加させている．今後，非接触型撮影機器を利用することで，「マーク付近の肌をシステムへ提示するだけで認証可能なシステム」へとすることも検討したい．

5. まとめと今後の課題

本稿では筆者らが提案している，マイクロスコープによって撮像される微細肌理画像を用いた生体認証メカニズム（肌理を利用したマイクロ生体認証）について紹介した．次に，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の構築を行い，その動作の説明を詳細に行った．最後に，構築したプロトタイプシステムについて，今後の見通しと課題を議論した．今後は，構築したプロトタイプシステムを利用してユーザビリティ評価を実際に行う．さらに，その結果を利用して，プロトタイプシステムのさらなる改良を行う．並行して，非接触型撮影機器による撮影についても検討をしていきたい．

謝辞

情報セキュリティ大学院大学　大塚玲教授には認証精度の評価で有益なご助言を頂きました．静岡大学　中谷広正元教授，佐治斉教授には画像処理手法に関しての有益なご助言を頂きました．ここに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, Inc.: FIDO 1.0 Specifications are Published and Final Preparing for Broad Industry Adoption of Strong Authentication in 2015 (online), available from <https://fidoalliance.org/news/item/fido-1.0-specifications-published-and-final1> (accessed 2015/02/26).

[2] 高橋健太，村上隆夫，加賀陽介ほか：“テンプレート公開型生体認証基盤，2012 年暗号とセキュリティシンポジウム予稿集，論文 No.1F1-3（2012）.

[3] 星野哲，松本弘之，松本勉：指紋画像からの人工指作製，電子情報通信学会技術研究報告，ISEC2001-60，Vol.101，No.311，pp.53-60（2001）.

[4] Zoe Kleinman: Politician’s fingerprint ’cloned from photos’ by hacker (online), available from <http://www.bbc.com/news/technology-30623611> (accessed 2015/02/07).

[5] 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，available from <http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html> (accessed 2017/03/17).

[6] C. Rathgeb, and A. Uhl.,: A survey on biometric cryptosystems and cancelable biometrics,” Journal on Information Security, pp. 1-25（2011）.

[7] 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，バイオメトリクスセキュリティコンソーシアム，オーム社，東京（2006）

[8] 眞野勇人，兼子拓弥，高橋健太，西垣正勝：マイクロ生体認証の提案とその一事例報告，電子情報通信学会技術研究報告，Vol.114，No.520，BioX2014-64，pp.153-157（2015）.

[9] 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）.

[10] Wolfram Mathematica, available from <https://www.wolfram.com/mathematica/> (accessed 2017/05/05).

[11] OpenCV, available from <http://opencv.org/> (accessed 2017/05/05).

[12] M. Fujita, Y. Mano, T. Kaneko, K. Takahashi and M. Nishigaki: A Micro Biometric Authentication Mechanism Considering Minute Patterns of the Human Body, Proceedings of 19th International Conference on Network-Based Information Systems, pp. 159-164 (2016).