情報処理学会論文誌 Vol.60 No.12 2095–2105 (Dec. 2019)

忘れられる権利に配慮した生体認証：爪を用いたマイクロ生体認証

杉本 元輝[1,a)] 藤田 真浩[1] 眞野 勇人[1] 大木 哲史[1] 西垣 正勝[1]

受付日 2019年3月12日, 採録日 2019年9月11日

概要：近年，プライバシ保護の観点から「忘れられる権利」の必要性が度々議論されている．本権利はEUの一般データ保護規則に「消去権」として記載されたこともあり，世界的に注目を集めており，生体認証の分野においてもこの「消去権」への配慮が求められる．その一実現形態としてテンプレートを乱数でマスクするキャンセラブル生体認証（テンプレート保護技術）が存在する．しかしこの方式では，登録された電子的な生体情報を保護することは可能であるが，登録時や認証時に提示される物理的な生体情報の漏洩まで保護することは不可能である．本論文では，物理的な生体情報に対して「消去権」に配慮した生体認証を実現するため，人間の微細生体部位を用いたマイクロ生体認証システムを爪へと応用した生体認証システムを構築した．ユーザ実験を通じて有用性を検証した結果，本システムが物理的な生体情報に対してテンプレート保護技術に準じた安全性を提供できる可能性が示された．

キーワード：生体認証，微細生体部位，爪，忘れられる権利，プライバシ保護

Biometrics for the Right to be Forgotten: Micro Biometric Authentication Using Fingernail Surface

Genki Sugimoto[1,a)] Masahiro Fujita[1] Yuto Mano[1] Tetsushi Ohki[1] Masakatsu Nishigaki[1]

Received: March 12, 2019, Accepted: September 11, 2019

Abstract: In recent years, the necessity of “right to be forgotten” is frequently discussed from the viewpoint of privacy protection. Furthermore, since this right was described as “right to erasure” in the general data protection rule of the EU, it attracted worldwide attention and it is required to have this “right to be forgotten” even in the field of biometric authentication. As one of such implementations, there is a cancelable biometric authentication which gives a random number to a template. Although it is possible to protect registered biometric information by this technique, it is impossible to protect up to the leak of physical biometric information before registration. In this paper, we applied a micro biometric authentication system, which uses a human micro body part, to the nail to construct a biometric authentication system that is according to the “right to be forgotten” against physical biometric information. The effectiveness of our system was verified through user experiments, and we confirmed the possibility that it makes physical biometric information as secure as the template protection technique for registered biometric information.

Keywords: biometric authentication, minute biometric part, nail, a right to be forgotten, privacy preservation

1. はじめに

近年，インターネットの普及にともない，様々な情報を手軽に利用できるようになった一方で，個人にとって好ましくない情報がインターネット上に残り続け，誰もが検索エンジンなどによってアクセス可能な状態になっているといった問題が存在する．そのため個人にとって好ましくない情報は，本人の意志で他人の目に触れないように削除され，忘れてもらうことのできる権利を設けるべきであるということが主張されている．EUにおいて，このような権利を認める議論が活発に行われ，2016年4月に欧州議会が可

[1] 静岡大学
Shizuoka University
[a)] sugimoto.genki.17@shizuoka.ac.jp

決したEU一般データ保護規則（General Data Protection Regulation：GDPR）の17条には「消去権（忘れられる権利）」（Right to erasure（right to be forgotten））として明記されている [3]．これは個人データ主体が一定の条件を満たす場合に個人データの抹消を請求することのできる権利を認めたものである．ここで，「個人データ」とは，識別された人または識別可能な人（「データ主体」）に関する情報を意味する．日本でもその必要性について種々議論がなされている [1], [2]．

一方で，現在，忘却・紛失の恐れがないといった利点から生体認証が様々な場面で用いられている．近年では普及が進み，ATM [4] や入出国審査 [5] のようなオフィシャルなサービス（典型的には，利用者の本人性の確認を必要とするサービスであり，実名による利用が原則となるある程度長期にわたって利用されるサービス）だけではなく，ロッカの施解錠 [6] やアミューズメントパークの入退場管理 [7] などのカジュアルなサービス（典型的には，すでに代金を支払った利用者であるかどうかが確認できれば十分であるサービスであり，匿名あるいは仮名で利用することが可能な短期的なサービス）にも生体認証が利用されており，今後のさらなる普及が予想される．しかし，生体情報は基本的に生涯不変で変更することのできないことから，1度生体情報が漏洩してしまうと，永遠に攻撃の危険に晒され続けるという課題も存在する．そのため生体認証システムにも，個人データである生体情報を抹消できる権利，つまり「消去権（忘れられる権利）」に配慮することが求められる．

その一実現形態としてキャンセラブル生体認証（テンプレート保護技術）が存在する [8]．キャンセラブル生体認証では，乱数情報を用いて生体情報をマスクし，その情報をテンプレートとしてサーバに登録する．この乱数情報を変更することにより，テンプレートの廃棄，更新が可能となる．しかし，キャンセラブル生体認証が実現するのはあくまでも電子的なテンプレート（生体認証システムによって読み取られコード化された生体情報）に関する消去権のみであり，登録時あるいは認証時に提示された虹彩や指紋そのものといった物理的な生体情報まで保護することはできない．

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．また最近は，カメラの高性能化により，遠距離から虹彩や指紋などの高繊細な画像を盗撮することも困難ではなくなっており [9]，実際に「ピース写真」から指紋を復元し偽造に成功したという事例も報告されている [10]．さらに攻撃者は，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．そのため，物理的な生体情報に対しても忘れられる権利を満たす生体認証が必要である．

そこで本論文では，物理的な生体情報そのものに対する消去権に配慮した生体認証を「忘れられる生体認証」と命名し，カジュアルサービス（匿名あるいは仮名で利用することが可能な短期的なサービス）において忘れられる生体認証を実現する具体的なインスタンスとして，爪表面の微細部位を用いたマイクロ生体認証を提案する．以降，2章では忘れられる生体認証の要件を示す．3章で既存研究，関連研究を紹介し，4章で提案方式について説明する．5章では実装したシステムを説明し，6章で基礎実験を行い，その結果を評価する．その後7章で考察を述べ，8章で本論文をまとめる．なお本論文は，文献 [11], [12], [13] を基に，研究内容の精緻化を行ったものである．

2. 忘れられる権利を満たす生体認証の要件

電子的なテンプレートに対する消去権に配慮した生体認証技術である「テンプレート保護型生体認証」の要件をベースに，物理的な生体情報に対する消去権に配慮した「忘れられる生体認証」の要件を精査する．

2.1 テンプレート保護型生体認証

テンプレート保護型生体認証技術の代表例として，キャンセラブル生体認証 [5] について説明する．キャンセラブル生体認証では，乱数コードを用いて生体コード（コード化された生体情報）をマスクし，その情報をテンプレートとしてサーバに登録する．

登録フェーズは以下の手順で行われる．

1. 登録者の生体情報を読み取り，生体コード X を得る．
2. 登録者に対して乱数コード R を生成し発行する．
3. 乱数コード R を用いて生体コード X を変換し，識別コード $T = F_R(X)$ を生成する．ここで，$F_R(\cdot)$ は乱数 R による変換処理を表す．
4. 識別コード T をテンプレートとしてサーバに登録する．

乱数コード R は，ユーザのICカードなどのトークンまたは第三者機関のサーバに保管され，認証の際に補助情報として使用される．

認証フェーズは以下の手順で行われる．

1. 認証要求者の生体情報を読み取り，生体コード X' を得る．
2. 認証要求者の乱数コード R を取得する．
3. 乱数コード R を用いて生体コード X' を変換し，識別コード $T' = F_R(X')$ を生成する．
4. T と T' が十分類似していれば認証成功とする．

乱数コード R や変換関数 $F_R(\cdot)$ を変更することで，識別コード（テンプレート）の更新が可能である．

2.2 テンプレート保護型生体認証の要件

テンプレート保護型生体認証においては，以下の 4 つの要件が定義されている [14], [15], [16].

① Irreversibility：生体情報から生成された識別コード（テンプレート）から，元の生体情報の類推ができないこと．
② Un-linkability：生体認証システムで用いられている識別コードを利用して，意図しない他のシステムで用いられる識別コードとの照合ができないこと．
③ Diversity：同じ生体情報から異なる識別コードを生成可能であること．漏洩した識別コードを利用不可にし，新しい識別コードを生成して安心安全に生体認証システムで利用できること．
④ Performance：上記の条件を満たすにあたり，本人拒否率，他人受入率を劣化させないこと．

2.3 忘れられる生体認証の要件

テンプレート保護型生体認証の目的が認証コードに対する消去権の達成であるのに対し，忘れられる生体認証の目的は「ユーザが生体認証システムに提示した生体情報そのもの」に対する消去権の達成である．そこで，テンプレート保護型生体認証の 4 つの要件をベースとし，要件中の「識別コード」の記載を「生体情報」と読み替えて各項目を再整理することによって，忘れられる生体認証の要件を策定する．ただし，テンプレート保護型生体認証の要件①については，単純に読み替えを行ってしまうと，「生体情報から生体情報が推測できないこと」という意味のなさない要件となってしまう．そのため，要件①については，その視点を「識別コードから生体情報が推測されるという事象」から「識別コードから生体情報が推測された結果，発生するリスク」へと変更し，なりすまし耐性に関する要件として再定義する．

著者らがとりまとめた 4 つの「物理的な生体情報そのものに対する消去権に関する要件」を以下に示す．ここで，③ Diversity の要件には，Disposability の要件が含意されることに注意されたい．以降では，この 4 要件を満足する忘れられる生体認証システムの実現について議論していく．

① Unforgeability：認証システムに提示した登録生体情報が漏洩したとしても，その情報を用いた他人がシステムに認証されないこと．
② Un-linkability：認証システムに提示した登録生体情報を利用して，意図しない他のシステムに登録されている生体情報との照合ができないこと．
③ Diversity：同じ生体部位から異なる生体情報を生成可能であること．漏洩した生体情報を利用不可にし（Disposability），新しい生体情報を登録して安心安全にシステムを利用できること．
④ Performance：上記の条件を満たすにあたり，本人拒否率，他人受入率を劣化させないこと．

3. 既存研究・関連研究

生涯不変の生体情報は，根本的には，物理的な生体情報に対する消去権とは相容れない関係にある．忘れられる生体認証を実現するにあたっては，新陳代謝によって日々生え変わる生体部位を利用するというアプローチをとることが基本となる．著者らが調査した限りでは，爪を利用した生体認証が唯一の先行事例であった．また，微細生体部位を利用して登録生体部位のつど更新を可能とすることで，忘れられる生体認証に準じた効果を狙ったマイクロ生体認証が提案されている．ここでは，これらの既存研究を紹介する．

3.1 Garg らの爪認証

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 [18]．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おり，忘れられる生体認証の要件②を満たさない．同じ理由で，1 つの爪に対して異なる生体情報を登録することができないため，要件③を満たさない（登録する指（爪）を変更すれば要件②および③を満たすが，変更可能回数はたかだか 10 回である）．

3.2 Barbosa らの爪認証

Barbosa らは爪表面の画像を利用した生体認証を提案している [19]．爪の生え変わりによって爪表面が変化するため，長期的（爪が生え変わるまでの数カ月）な観点では，忘れられる生体認証の要件②および③を満たした認証方式となっている．しかし，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，爪の概形を主な特徴量とした認証方式となっていると想定される．したがって，偽造物を作成してのなりすましはそれほど難しくないと考えられ，要件①を満たさない．また，爪が生え変わっても爪の概形については変化が僅かである場合もままあるため，要件②と③に対する効果も限定的である可能性が残る．

3.3 肌理を利用したマイクロ生体認証

微細生体部位を利用したマイクロ生体認証と呼ばれる方式が提案されており，文献 [20] では上腕部表面上の約 1 mm 四方の肌理画像を用いた際の有用性が示されている．一般に，小さいものであればあるほど，偽造することは難しい．微細生体部位を利用することにより，偽造物によるなりすましが困難となり，忘れられる生体認証の要件①が満たされる．ユーザはつねに認証システムに上腕部を提示するが，そのつど異なる微細部位を選んで登録生体情報を変更することができるため，要件②および③が満たされる．ただし，人間の肌理模様そのものは中短期的には大きく変化しないため，攻撃者にユーザの上腕部全体の肌理情報を

表 1 既存研究と要件
Table 1 Related works and the requirements.

	要件①	要件②	要件③	要件④
Garg方式	×	×	×	○
Barbosa方式	×	△	△	○
マイクロ生体認証	○	△	○	○

すべて盗取されてしまった場合には，全体情報とのパターンマッチングによって認証システムに登録されている異部位情報が名寄せされてしまう．すなわち，微細肌理情報を利用したマイクロ生体認証は要件②および③を完全には満たさない．

これらの既存研究が忘れられる生体認証の各要件を満たしているか否かを示したものが**表 1** である．表 1 から読み取れるように，マイクロ生体認証が要件を最も多く満たしている．そのため，本研究では，マイクロ生体認証を改良することで，忘れられる生体認証の 4 つの要件をすべて満たす生体認証システムの実現を目指す．

4. 忘れられる生体認証の実現

4.1 マイクロ爪生体認証

物理的な生体情報そのものに対する消去権に関する 4 つの要件①～④を満たす忘れられる生体認証の実現に向けて，本論文では，生え変わる生体部位である爪を利用したマイクロ生体認証（マイクロ爪認証）について検討する．マイクロ爪認証の目的は，カジュアルサービス（匿名あるいは仮名で利用することが可能な短期的なサービス）に対する忘れられる生体認証の達成である．今回は，その第 1 実現形態として，文献 [20] の同様の拡大率を設定し，約 1 mm 四方の爪表面画像を 200 倍のマイクロスコープ用いて撮影する．

爪は，爪先，遊離縁，爪床，爪郭，爪母基，爪根などから構成される皮膚の一部である [21]．**図 1** に示すとおり，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きる．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 であるといわれている [22]．爪が成長すると登録部位が遊離縁まで達し，その爪を切ることでそれまでの生体情報が抹消される．それと同時に，新しい特徴を持つ爪が生え変わるため，同じ爪の同じ位置であっても一定期間が経過することで生体情報が一新される．また，紙やすりなどで爪表面を軽く擦ることによって，爪の成長を待たずに能動的に爪表面の特徴を変更することも可能である．

マイクロ生体認証の仕組みに上記の爪の性質が加わることにより，爪表面の微細部位の模様を用いたマイクロ生体認証は下記のように要件①～③を満たしうることが示唆される．要件④については，6.2 節のユーザ実験によって評価する．

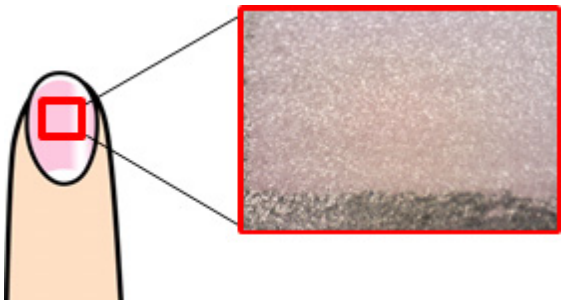


図 1 爪の表面の模様（黒い領域はマーク）
Fig. 1 Texture pattern on the fingernail plate (the black area is a part of mark).

要件①：一般的に，物理サイズが微細になるほど偽造物を精密に作成するためのコストは高まる [17]．一方，拡大鏡などで対象物の微細部分を撮影することは偽造物を作成するよりはるかに容易であると推測される．この撮影コストと偽造コストの非対称性により，認証システムに登録されている生体情報が漏洩したとしても，攻撃者が偽造生体を（単刀直入な方法で）作成してなりすましに成功するまでの障壁を高めることが可能であると期待される．この結果，要件①が満たされうることが示唆される．なお，マイクロ爪認証が実際にどの程度のなりすまし耐性を有しているのかについては，7 章で検証を行う．

要件②：爪は 1 指につき 1 つしかないが，登録情報が 1 mm 四方の微細部位であれば，1 つの爪の表面（表面積を 1 cm^2 と想定）中に異なる 100 部位が存在することになる．したがって，ユーザは異なる認証システムごとに別の部位を登録することが可能であり，異なる認証システムに登録されているユーザの生体情報間の名寄せを攻撃者が行うことは困難であると期待される．これにより，認証システムに登録されている生体情報のみを盗取した攻撃者に対し，要件②が満たされうることが示唆される．なお，同一ユーザの 1 枚の爪であっても部位によって微細生体情報（爪表面の模様）が異なるか否かについては，6.3 節の実験によってこれを確かめる．

攻撃者が（認証システムに登録されている生体情報に加え）ある時点におけるユーザの爪表面の全体画像をも盗取した場合には，登録生体情報と全体情報とのパターンマッチングを行うという攻撃が可能である．このような攻撃に対しては，異なる認証システムで別の微細生体部位を登録していたとしても，全体画像の情報を媒介として異部位の生体情報が名寄せされてしまう．しかし，短期的にはユーザが故意に紙やすりなどで爪を擦ることにより，長期的には爪の生え変わりにより，攻撃者が盗取した爪表面の全体画像は不能となる．この結果，ユーザの爪表面の全体画像

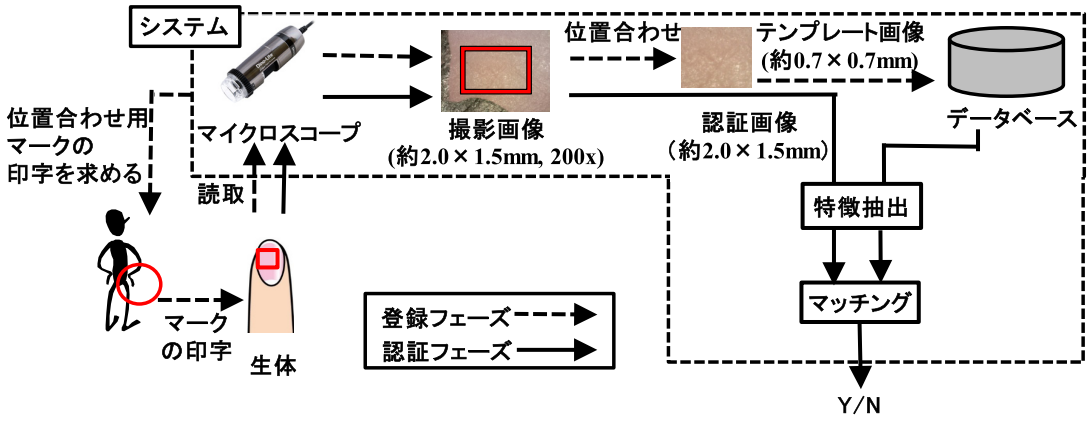


図 2 システム概要図
Fig. 2 System overview.

を盗取する攻撃者に対しても，要件②が満たされうる．

要件③：前述のとおり，1 つの爪の中に 100 部位の登録情報が存在する．よって，ユーザは，使用する爪を変えることなく，パスワードの変更やトークンの交換と同様の感覚で登録部位を変更することが可能となる．紙やすりなどで爪表面を擦ることによって，それまでの登録情報を完全に廃棄することも可能である．これにより，短期的な観点での要件③が満たされうる．また，爪の生え変わりによって新たな登録可能部位が順次成長してくるため，長期的な観点においても要件③が満たされうることが示唆される．

4.2 認証手順

マイクロ爪認証の手順を以下に示す（**図 2** 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 を認証システムへ登録する．
2. 認証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. 認証システムはマークを目印にして，マイクロスコープでユーザが提示した爪表面の微細部位の画像 X を読み取る．
5. 認証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. 認証システムはマークを目印にして，マイクロスコープでユーザが提示した爪表面の微細部位の画像 X' を読み取る．
3. 認証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 X を参照する．
4. X' が十分 X と近い場合，そのユーザは正規ユーザと判断される．

5. 実装

文献 [20] のマイクロ生体認証システムをベースにマイクロ爪認証システム実装を行った．その構成を図 2 に示す．

5.1 登録部位の発見

マイクロ爪認証においては，認証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．本論文では，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した．

5.2 生体部位の撮影

本システム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表面の約 2.0 × 1.5 mm の領域を 200 倍で撮影することによって，2,592 × 1,944 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[*1]．

5.3 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，テンプレート画像および認証画像はグレースケール変換した後に Local Binary Pattern（以下 LBP）変換を行う．LBP は画像の濃淡値の変化に頑健であるという性質を持つ [23], [24]．各処理は，scikit-image Ver.0.14dev [25] に実装されている rgb2gray 関数，local_binary_pattern 関数を使用してそれぞれ実装した．local_binary_pattern のパラメータは，P を

[*1] 正確には，5.4 節の手順 3 においてテンプレート候補画像群を作成する際に必要となるため，800 × 800 pixel よりも一回り大きな領域を保存する．

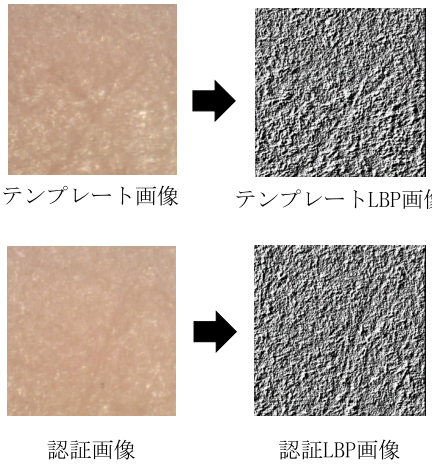


図 3 特徴抽出
Fig. 3 Feature extraction.

24，R を 3，method を default とした．テンプレート画像および認証画像に対して，これらの処理を施した画像の例を**図 3** に示す．

5.4 マッチング

マッチングはヒストグラムの比較による類似度検出で行う．具体的には，登録画像と認証画像を LBP 変換した後のヒストグラムの類似度をカイ二乗値で算出した値を使用する．ヒストグラムの類似度検出には OpenCV3 [26] に実装されている cv2.compareHist 関数を使用し，パラメータは method を cv2.HISTCMP_CHISQR とした．テンプレート画像のヒストグラムを $H_1(I)$，認証画像のヒストグラムを $H_2(I)$ としたときの類似度 $d(H_1, H_2)$ は以下の式で表される．ここで，I はヒストグラムのビンであり，$I = \{0, 1, 2, \cdots, 255\}$ である．

$$d(H_1, H_2) = \sum_I \frac{(H_1(I) - H_2(I))^2}{H_1(I)} \quad (1)$$

認証画像の撮影時，マイクロスコープの傾きや位置をテンプレート画像の撮影時とまったく同じにすることは非常に困難であり，これらの傾きや位置のズレはノイズとなり認証率の低下を引き起こす．そこでまず，テンプレート画像に射影変換を施し，歪ノイズを補正する．その後，認証画像に対してテンプレート画像を水平・垂直方向に走査させながらマッチングを行うことで，平行移動ノイズを補正する．これらの補正を施したうえでテンプレート画像と認証画像のマッチングスコアを求める．具体的な手順は下記のとおりである．

1. テンプレート画像の各頂点を左上から反時計回りに $\mathrm{P_{t0}}$，$\mathrm{P_{t1}}$，$\mathrm{P_{t2}}$，$\mathrm{P_{t3}}$ とする．
2. 認証画像撮影時のひずみや位置ずれの発生によって，認証画像の各頂点はテンプレート画像の各頂点 $\mathrm{P_{ti}}$ $(0 \leq i \leq 3)$ と完全には一致しない可能性が高い．そこで，テンプレート画像の頂点 $\mathrm{P_{t0}}$ を中心とした 5×5 画素の集合を $\mathrm{P_{t0}}$ に対する候補点群 $\{C_{0j} | 0 \leq j \leq 24\}$ とする．同様に，頂点 $\mathrm{P_{t1}}$, $\mathrm{P_{t2}}$, $\mathrm{P_{t3}}$ を中心とした 5×5 画素の集合を候補点群 $\{C_{1k} | 0 \leq k \leq 24\}$, $\{C_{2m} | 0 \leq m \leq 24\}$, $\{C_{3n} | 0 \leq n \leq 24\}$ とする．
3. 4 つの候補点群 $\{\mathrm{C_{0j}}\}$, $\{\mathrm{C_{1k}}\}$, $\{\mathrm{C_{2m}}\}$, $\{\mathrm{C_{3n}}\}$ の中からそれぞれ 1 点を総当たりで取り出し，それら 4 点によって囲まれる 390,625 $(= 25^4)$ 個の四辺形領域をテンプレート画像から切り出す．各四辺形領域が 800 × 800 pixel の矩形画像となるように射影変換を施した画像群を，テンプレート候補画像群とする．
4. テンプレート候補画像群からテンプレート画像を 1 枚取り出し，認証画像（2,492 × 1,944 pixel）に対してそのテンプレート画像（800 × 800 pixel）を水平方向ならびに垂直方向に 1 pixel ずつ平行移動させながらマッチングを行い，認証画像の中でテンプレート画像と最も類似度の高い領域におけるマッチングスコアを算出する．
5. 手順 3. で得たテンプレート画像群のすべてに対して手順 4. を行い，最も類似度の高いマッチングスコアがテンプレート画像と認証画像のマッチングスコアとなる．

6. 基礎実験

マイクロ爪認証の有効性をユーザ実験によって評価する．

6.1 データセット

被験者は静岡大学生の男女 10 人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，各爪で縦方向（爪が成長する方向）に任意の 2 カ所を登録生体部位として設定し，それらの画像（計 6 カ所）を撮影した．実験は，テンプレートを撮影した日を 1 日目として 5 日間行った．1 日目の午前中にテンプレート画像を撮影し，午後に 1 回目の認証画像を撮影した．その後 3 日目と 5 日目に日中の任意の時間帯で認証画像の撮影を行った．

1 日目午前のテンプレート画像撮影時に，各爪の計 6 カ所の登録部位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てもらった．テンプレート画像については，このマーク付近をマイクロスコープで撮影した．認証画像については，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撮影を行った．日常生活の中でトップコートが剥がれ落ちそうになった被験者においては，その時点でトップコートを再度塗布してもらった．

今回の実験で収集した認証画像は 10 人 × 6 部位 × 3 日間 = 180 枚である．人差し指の根元側の部位に 1，爪先側に 2 と番号を振り，中指と薬指にも同様に 4〜6 の番号を振り，被験者 i $(1 \leq i \leq 10)$ の p 番目の部位 $(1 \leq p \leq 6)$ のテンプレート画像を $t_{i,p}$ と表記する．同様に被験者 j $(1 \leq j \leq 10)$ の q 番の部位 $(1 \leq q \leq 6)$ の d 日目 $(1 \leq d \leq 3)$ の認証画像を $a_{k,q,d}$ と表記する．

6.2 Performance 評価

マイクロ爪認証が忘れられる生体認証の要件④を満たしているかを，同じ被験者内の同部位間のマッチングスコア（本人スコア）と異なる被験者間のマッチングスコア（他人スコア）を比較することで評価する．

本人スコアは $t_{i,p}$ と $a_{j,q,d}$（$i = j$，$p = q$）を比較することで算出する．組合せのデータ数は 180 通りである．他人スコアは $t_{i,p}$ と $a_{j,q,d}$（$i \neq j$）を比較することで算出する．ただし，本論文では処理時間短縮のため，本人スコアと同数の 180 通りの組合せをランダムに抽出して他人スコアを求めた．その際，各被験者から同一数のデータが抽出されるように行った．このように求めた本人スコアと他人スコアを基に，本人と他人を切り分ける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 4 (a) に示す．このときの等価エラー率（EER）を求めたところ，認証閾値 = 182 で EER ≒ 7%であった．

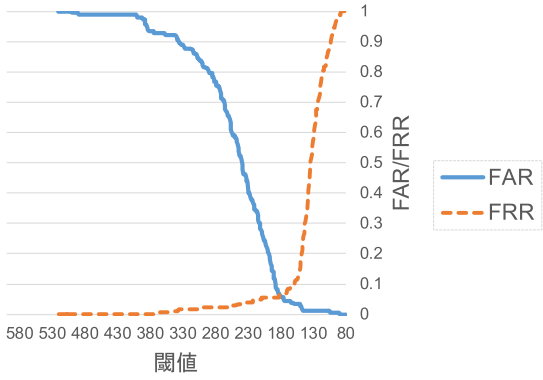
また，今回の実験（図 4 (a)）からは，認証閾値 = 150 を採用した場合には，FRR ≒ 15%，FAR ≒ 2%という認証精度となるという結果が得られている．このような特徴を有する生体情報の場合は，複数部位を利用した OR 型認証を構成することによって，その認証精度をさらに高めることが可能である．たとえば，爪の微細部位 2 カ所を利用した OR 型認証の認証精度は，単純な理論計算では，FRR ≒ 2%（2 カ所とも本人拒否される事象の確率のため，$0.15^2 \fallingdotseq 0.023$），FAR ≒ 4%（2 カ所とも他人受入が起こらない事象の余事象の確率のため，$1 - \{1 - (0.02)\}^2 \fallingdotseq 0.040$）となる．5.2 節では，提案システムにおいては 2,592 × 1,944 pixel の爪画像の中央 800 × 800 pixel をテンプレート画像として利用することを述べたが，2,592 × 1,944 pixel の爪画像の中から 2 カ所の「800 × 800 pixel の画像領域」を互いに重ならないように抽出することができる．これによって，撮影の手間を増加させずに 2 カ所の微細部位を用いた OR 型マイクロ生体爪認証を実行することは可能であると考えられる．

このように，被験者 10 人による基礎実験の結果ではあるが，本システムが，爪の微細部位 1 カ所で EER 約 7%の認証精度を達成し，また，2 カ所の OR 型認証で FAR 約 4%のときに FRR 約 2%の認証精度向上を達成することが確認できた．適用先によっては十分な認証精度とはいえないものの，マッチングアルゴリズムの改良などを通じて認証精度をさらに改善する余地は残されていると期待される．以上より，要件④を満たす可能性が示唆された．

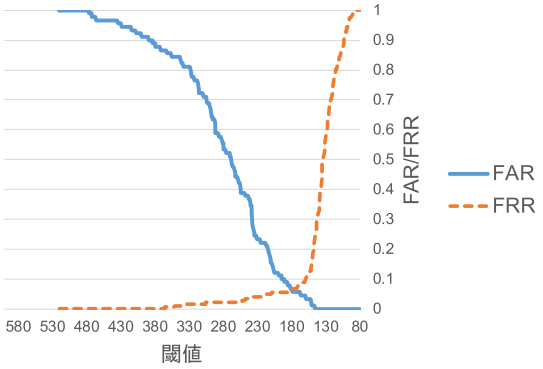
6.3 Unlinkability 評価，Diversity 評価

本節では，マイクロ爪認証が忘れられる生体認証の要件②および③を満たしているか否かを，同一被験者の同じ爪であっても部位が異なれば別の生体情報と見なせるか（爪母基でつど生成される爪の表面の凹凸模様に規則性はないか）という観点から評価する．同一被験者の異爪間の凹凸模様の不規則性については，同一被験者内の異部位間を比較したマッチングスコア（同人異部位間スコア）を算出することによって評価することができる．また，今回の基礎実験では，5.1 節で述べたとおり，爪ごとに爪の成長する方向に 2 カ所の異なる微細部位を登録している．そこで，同一被験者の同じ爪の異部位間の比較に特化したマッチングスコア（同爪異部位間スコア）についても算出し，同一爪内の微細部位間の凹凸模様の不規則性についても評価する．

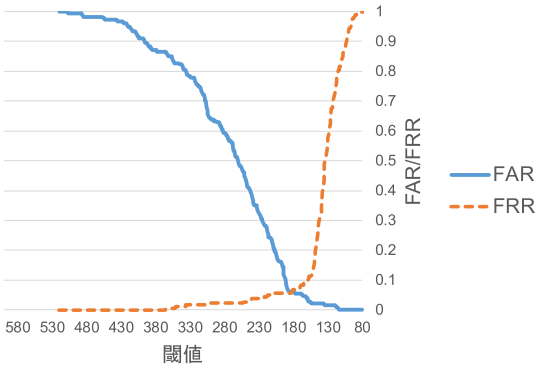
同人異部位間スコアは $t_{i,p}$ と $a_{j,q,d}$（$i = j$，$p \neq q$）の比較により，同爪異部位間スコアは $t_{i,p}$ と $a_{j,q,d}$（$i = j$，$p = q - 1$ もしくは $p = q + 1$）の比較により，それぞれ算出する．なお，5.2 節と同様，処理時間短縮のため，同人異



(a) 本人スコアと他人スコアの比較



(b)本人スコアと同人異部位間スコアの比較



(c)本人スコアと同爪異部位間スコアの比較

図 4 本実験における FAR，FRR
Fig. 4 FAR and FRR in this experiment.

部位間の比較は 180 通りの組合せをランダムに抽出してスコアを求めた．本人スコアは，5.2.1 項同様，$t_{i,p}$ と $a_{j,q,d}$（$i = j$，$p = q$）の比較により算出している．このように求めた本人スコアと同人異部位間スコアを基に，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 4 (b) に示す．そして，本人スコアと同爪異部位間スコアを基に，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 4 (c) に示す．

図 4 (b) ならびに図 4 (c) の等価エラー率（EER）をそれぞれ求めたところ，前者は認証閾値 ≒ 182 で EER ≒ 6%，後者は認証閾値 ≒ 180 で EER ≒ 7%であった．これは 5.2 節で評価した本人スコアと他人スコアを比較した際の閾値および EER とほぼ同等である．この結果より，提案システムにおいては，同一ユーザであっても爪が異なれば，また，同一の爪であっても微細部位の位置が異なれば，爪表面の凹凸模様は他人と同程度に異なるということが確かめられた．

ただし，今回の結果は，爪の表面の凹凸模様に基づいた攻撃に対し，要件②および③が満たされたことが確認されたにすぎない．今後は，それ以外の攻撃方法に対しても要件②や③が満たされうることを調査していく必要がある．

7. Unforgeability に関する考察

マイクロ爪認証のなりすまし耐性について考察する．

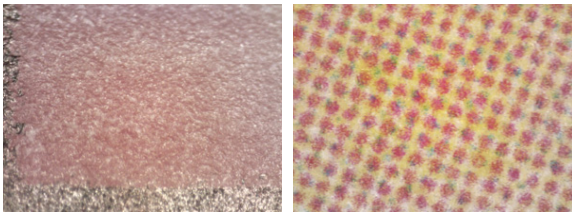
7.1 印刷物に対するなりすまし耐性

提案システムは画像ベースの類似度によって認証を行っているため，最も一般的な偽造手段である「印刷」に焦点を当てる．

本システムは，爪表面を約 200 倍に拡大した部位をマイクロスコープで撮影し，その撮影画像を認証に利用する．**図 5** (a) は「爪表面の約 2.0 × 1.5 mm の領域をマイクロスコープで撮影した画像」，図 5 (b) は「市販のプリンタ（Brother HL3170-CDW）を使用して，印刷サイズが約 2.0 × 1.5 mm の大きさとなるように，**図 6** (a) の画像を最高解像度（2,400 dpi）で印刷し，それをマイクロスコープで撮影した画像」である．市販のプリンタ程度の解像度であれば，撮影される画像が本物と比べて大きく異なることが確認できる．このように，本システムは，仮に生体情報が漏洩したとしても，攻撃者が印刷画像を使って本人になりすますことが困難となっている．

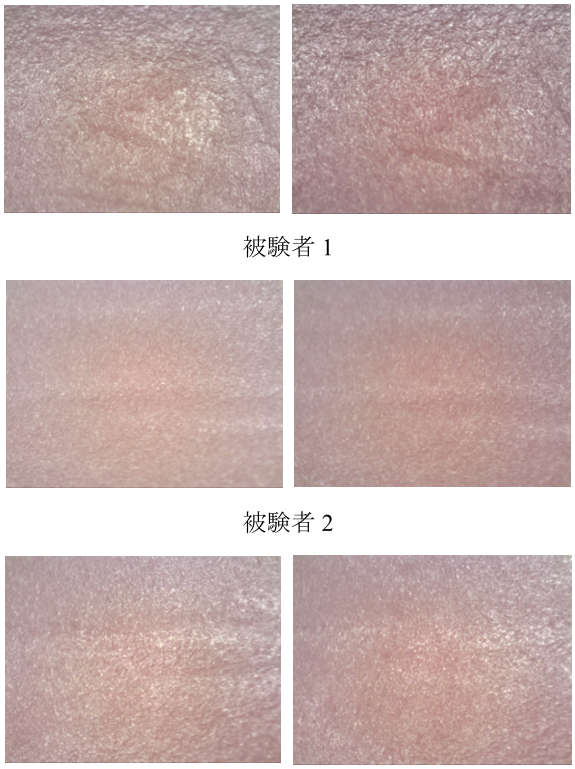
「プリンタの解像度よりもマイクロスコープの解像度のほうが高ければ，印刷画像を拡大して撮影することによって，印刷物であることが判別できる」という想定の下で，定量的な分析を行ってみよう．5.1 節で述べたように，今回のマイクロスコープを用いると，爪表面の約 2.0 × 1.5 mm の領域を 200 倍で撮影することによって，2,592 × 1,944 pixel の爪画像が得られる．ここでは，議論を簡単にするために，爪表面の 2.0 mm 四方の領域を 200 倍で撮影することによって，2,600 × 2,600 pixel の爪画像が得られるとする．すなわち，このマイクロスコープは，2.0 mm 四方の領域を 2,600 × 2,600 pixel の解像度で撮影する．この場合，上述の想定に従うと，攻撃者が「2.0 mm 四方の領域に 2,600 × 2,600 dot 以上の解像度で印刷ができるプリンタ」を利用して偽造画像を作成したならば，このマイクロスコープの撮影では偽造画像を判別することはできないということになる．したがって，単純な理論計算からは，攻撃者は 33,020 dpi（= 2,600 dot ÷ 2.0 mm = 2,600 dot ÷ 2.0 mm × 25.4 mm/inch）以上の解像度のプリンタを用いる必要があると算出できる．

現在の市販のプリンタの解像度は，上述のように 2,400 dpi



(a) 元画像　　(b) プリンタ画像

図 5 市販のプリンタによるなりすまし攻撃
Fig. 5 Impersonation by a commercially available printer.



被験者 1

被験者 2

被験者 3

図 6 圧迫前後の撮影画像，（左）圧迫前，（右）圧迫後
Fig. 6 Images before/after shot fingers are pressed left images are before pressed, right images are after pressed.

程度である．よって，プリンタによる印刷画像を使用したなりすまし攻撃に対しては，提案システムは要件①を満たすことが示された．しかし，攻撃者が市販製品を超える高解像度のプリンタを使用した場合は，拡大率 200 倍のマイクロ生体認証では十分なりすまし耐性が得られない可能性もある．そのような攻撃にも対抗するには，偽造物と生体を区別するための生体検知を組み込むなどの追加対策が必要となるだろう．

7.2 生体検知技術の併用

マイクロ爪認証に好適な生体検知の一例として，末梢血管における血流途絶や反応性充血 [27] の利用が考えられる．指先を机に強く押し付けるなどの方法によって，指の腹に圧力を加えた場合には，爪の下の皮膚に流れる抹消血流の血流が途絶えて，爪床下の皮膚の色が白くなる．そして，指の圧迫を解いた際には，一時的に血管の拡張が起こり，血流が増加して皮膚が赤くなる．これらの現象を利用し，撮影時に少し強く撮影部位の爪あるいは指腹を軽く圧迫して，撮影される画像の色度の変化を確認することで生体検知が可能であると考えられる．

実際に 3 人の被験者に対し，指腹を軽く圧迫する前後の爪表面の微細部位を撮影した画像が図 6 である．目視でも圧迫解放後の画像は少し赤みが増していることが確認できる．今回は，以下の方法で撮影された画像の色度を数値的に比較した．

1. 白飛びしている画素をマスクするために，画像内においてR，G，B の輝度値すべてが 200 以上の画素を間引く．
2. R，G，B それぞれで，輝度値が 150 以上の画素数をカウントし，その数をそれぞれ n_R，n_G，n_B とする．
3. 画像がどの程度赤色傾向にあるのかを $n_R/(n_R + n_G + n_B)$ を計算して求める．

実際に，図 6 の圧迫前と圧迫後の画像に対して上記の赤色度を求めたところ，圧迫前：圧迫後の値はそれぞれ，0.44 : 0.59（被験者 1），0.34 : 0.48（被験者 2），0.38 : 0.43（被験者 3）となった．これに対し，印刷物や偽造物は圧迫前後で色度は変化しない．この結果から，指腹の圧迫（と解放）という簡易的な方法によって，マイクロ爪認証に生体検知機能を付加することができる可能性が示された．

7.3 爪の加工容易性

本システムでは，認証のモダリティとして爪表面の凹凸を用いているが，爪という部位はマニキュアやネイルアート，爪磨きなど，加工が加えられやすい部位であるといえる．今回の実験ではすべて無加工の爪を使用したが，加工された爪を用いた場合，登録時と認証時で状態が異なる（例：登録時はマニキュアをしていたが，認証時はしていない）と認証精度へ影響が出ると考えられる．また，加工後の爪表面の凹凸が万人で似通ってしまう可能性も考えられる．その場合は故意か偶然かにかかわらずなりすましの可能性が発生してしまう．この課題については今後，実証実験を通じて検討を深めていく必要がある．

8. むすび

本論文では，物理的な生体情報に対する消去権（忘れられる権利）に配慮した生体認証を「忘れられる生体認証」と命名し，カジュアルなサービスで運用することを考慮した忘れられる生体認証として爪表面の微細部位を用いたマイクロ生体認証を提案した．忘れられる生体認証に必要な要件を定義した後，マイクロスコープを利用した生体認証システムを実装し，その有用性評価となりすまし耐性の考察を行った．その結果，小規模な実験ではあったものの，提案方式が要件を満たしうる可能性を有する生体認証（忘れられる生体認証）であることが確認された．

今後は，認証精度の向上や爪の加工への対応などシステムをさらに改良していくとともに，提案システムが忘れられる生体認証の要件を満足しているのか多角的な観点から検証を行っていく必要がある．それとともに生体検知や想定される攻撃方法についてもさらに検討を深めていく予定である．

謝辞 本研究は一部，情報通信研究機構（NICT）の委託研究（契約番号 193）の助成を受けました．

参考文献

[1] 安藤 均：「忘れられる権利」は新しい人権か：「忘れられる権利」をめぐるプライバシの検討，旭川大学経済学部紀要，No.76, pp.71–100 (2017).
[2] 石井夏生利：「忘れられる権利」をめぐる論議の意義，情報管理，Vol.56, No.4, pp.271–285 (2015).
[3] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, available from ⟨https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN⟩ (accessed 2019-01-24).
[4] NEC，台湾・玉山銀行の ATM 向けに顔認証システムを提供，入手先 ⟨https://tech.nikkeibp.co.jp/it/atclact/activer/nkpr/RSP503461_25022019/⟩（参照 2019-03-12）.
[5] 成田，出国手続きも「顔認証」開始 待ち時間の短縮狙い，入手先 ⟨https://www.asahi.com/articles/ASLB33398LB3UDCB00C.html⟩（参照 2019-03-12）.
[6] ロッカーも指紋認証式に ····· 立命館大，導入後は盗難被害なし，入手先 ⟨https://www.rbbtoday.com/article/2015/11/30/137456.html⟩（参照 2019-03-12）.
[7] Privacy Information Center, available from ⟨https://www.universalorlando.com/web/en/us/privacy-info-center/index.html#subnav-e⟩ (accessed 2019-01-24).
[8] Rathgeb, C. and Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics, Journal on Information Security, pp.1–25 (2011).
[9] Politician's fingerprint 'cloned from photos' by hacker,

available from ⟨https://www.bbc.com/news/technology-30623611⟩ (accessed 2019-03-12).
[10] 「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，入手先 ⟨http://www.sankei.com/affairs/news/170109/afr1701090002-n1.html⟩ （参照 2019-01-24）.
[11] 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 (2017).
[12] 杉本元輝，藤田真浩，眞野勇人，大木哲史，西垣正勝：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，信学技報，Vol.117, No.520, BioX2017-57, pp.127–132 (2018).
[13] 眞野勇人，米山裕太，高橋健太，西垣正勝：忘れられる権利を有する生体認証と補助情報を付帯させた生体認証の提案，電子情報通信学会バイオメトリクス研究会予稿集，BioX2013-13, pp.46–51 (2013).
[14] ISO/IEC DIS 30136. Information technology – Performance testing of biometric template protection schemes (2017).
[15] Jain, A.K., Nandakuma, K. and Nagar, A.: Biometric Template Security, *EURASIP Journal on Advances in Signal Processing*, Vol.2008, Article ID 579416, p.17 (2017).
[16] 新崎　卓：生体認証と改正個人情報保護法をめぐる動き，電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review，Vol.11, No.2, pp.108–112 (2017).
[17] Matsumoto, T., Hoga, M., Ohyagi, Y., Ishikawa, M., Naruse, M., Hanaki, K., Suzuki, R., Sekiguchi, D., Tate, N. and Ohtsu, M.: Nano-artifact metrics based on random collapse of resist, *Scientific Reports*, Vol.4, No.6142, pp.1–5 (2014).
[18] Garg, S., Kumar, A. and Hanmandlu, M.: Finger Nail Plate: A New Biometric Identifier, International, *Journal of Computer Information Systems and Industrial Management Applications*, Vol.6, pp.126–138 (2014).
[19] Barbosa, I.B., Theoharis, T. and Abdallah, A.E.: On the use of fingernail images as transient biometric identifiers, *Machine Vision and Applications*, Vol.27, No.1, pp.65–76 (2016).
[20] 藤田真浩，眞野勇人，村松弘明，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，電子小情報通信学会論文誌 (A)，Vol.J100-A, No.12, pp.465–474 (2017).
[21] R. クルスティッチ，牛木辰男，金沢寛明：立体組織学アトラス（原題：Human Microscopic Anatomy An Atlas for Students of Medicine and Biology），pp.236–237, 西村書店 (2017).
[22] Yaemsiri, S., Hou, N., Slining, M.M. and He, K.: Growth rate of human fingernails and toenails in healthy American young adults, *Journal of the European Academy of Dermatology and Venereology*, Vol.24, No.4, pp.420–423 (2010).
[23] Ojala, T., Pietikainen, M. and Harwood, D.: Performance evaluation of texture measures with classification based on Kullback discrimination of distributions, *Proc. 12th International Conference on Pattern Recognition*, Vol.1, pp.582–585 (1994).
[24] 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, No.3, pp.1–6 (2012).
[25] scikit-image, available from ⟨https://scikit-image.org/⟩ (accessed 2019-01-24).
[26] OpenCV, available from ⟨https://opencv.org/⟩ (accessed 2019-01-24).
[27] 蔵本　築，矢崎義雄：冠血管の反応性充血，呼吸と循環，Vol.17, No.9, pp.793–799 (1969).

杉本 元輝

2017 年静岡大学情報学部情報科学科卒業．2019 年同大学院情報科学技術研究科情報学専攻修士課程修了．在学中は情報セキュリティ，特に生体認証に関する研究に従事．

藤田 真浩 （正会員）

2013 年静岡大学情報学部情報科学科卒業．2015 年同大学院修士課程修了．2018 年同創造科学技術大学院博士課程修了．現在，三菱電機株式会社情報技術総合研究所勤務．情報セキュリティ，特に認証システムに関する研究開発に従事．博士（情報学）．2016 年度情報処理学会山下記念研究賞受賞．

眞野 勇人

2012 年会津大学コンピュータ理工学部卒業．2015 年静岡大学大学院修士課程修了．在学中は情報セキュリティに関する研究に従事．

大木 哲史 （正会員）

2002 年早稲田大学理工学部電子情報通信学科卒業．2004 年同大学院理工学研究科電子・情報通信学専攻修士課程修了．2010 年早稲田大学理工学術院情報・ネットワーク専攻博士 (工学) 取得．2010 年早稲田大学理工学総合研究所次席研究員．2013 年産業技術総合研究所特別研究員を経て，2017 年より静岡大学大学院総合科学技術研究科講師．情報セキュリティ全般，特に個人認証を中心としたネットワークセキュリティに関する研究に従事．電子情報通信学会会員．

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械工学科卒業．1995 年同大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2010 年より同創造科学技術大学院教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013～2014 年情報処理学会コンピュータセキュリティ研究会主査．2015～2016 年電子情報通信学会バイオメトリクス研究専門委員会委員長．2016 年日本セキュリティマネジメント学会編集部会長．2019 年より情報処理学会情報環境領域委員長．本会フェロー．