講　義

バイオメトリック認証技術の基礎

指紋や静脈など，生体的特徴により個人を認証する技術をバイオメトリック認証技術とよぶ。犯罪捜査や入出国管理から利用が始まったバイオメトリック認証は，今や施設の入退室管理，モバイル機器の利用者認証，金融端末における本人認証など，日常生活の様々な分野に応用されている。そして，これを支えるセンサー技術などは，化学計測と共通するものも多い。本稿では，バイオメトリック認証技術の基礎について述べる。

小　木　　修

1　はじめに

バイオメトリクス（biometrics）とは，“biology”と“−metrics（測定学）”という2語から成る合成語であり，本人だけが持つ生体的特徴の計測に関する研究分野を指す。そして，バイオメトリクスを利用した個人認証技術を，バイオメトリック認証技術とよぶ。この技術の実用化は，まず犯罪捜査における指紋データベースの利用や入出国管理に始まった。その後，世界的なセキュリティ意識の高まりや，インターネットにおける本人識別の必要性の高まりが大きな原動力となり，技術の発展および普及が進んできた。バイオメトリック認証技術は生体的特徴の計測に基づくものであり，これを支えるセンサー技術や画像撮影技術，データ解析技術などは，化学計測と共通するものも多い。

本稿では，バイオメトリック認証技術の基礎的な内容を解説する。なお，バイオメトリクスについてさらに知りたい読者には，入門書として文献1が，また，専門書として文献2および3が好適である。

2　バイオメトリック認証の本人認証プロセス

バイオメトリック認証システムによる本人認証プロセスを図1に示す[4]。まず，利用者の生体的特徴を計測し，その計測データを数値化する。この数値をテンプレートとして，システムのデータベースに登録する。認証の際には，新たに利用者の生体的特徴を計測し，この計測データを数値化する。この数値（サンプル）をシステムに提示し，データベース内のテンプレートと照合する。その照合結果に基づいて本人か否かを判定し，システムにその判定結果を報告する。

3　バイオメトリック認証で利用する生体的特徴

一般的な本人認証システムでは，磁気カードなどの所有物や，パスワードなどの知識を利用して認証を行う。これに対し，バイオメトリック認証システムでは，本人の生体的特徴を利用して認証を行う。バイオメトリック認証で利用する生体的特徴には，普遍性（誰でも持っている特徴であること），唯一性（人により異なる特徴であること）および永続性（生涯変わらない特徴であること）という三つの性質が必要である。

表1は，バイオメトリック認証で利用する生体的特徴の種類（モダリティ，modality）ごとに，それらの概

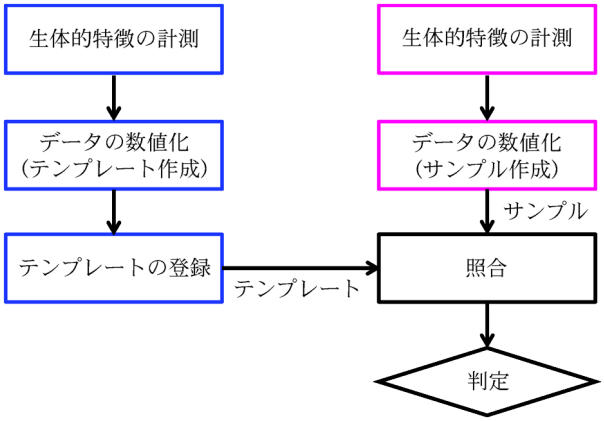

図1　バイオメトリック認証システムによる本人認証プロセス

表1　主な生体的特徴の種類（モダリティ）とその概要

分類	モダリティ	センサーの例	認証精度	受容性	導入経費
身体的特徴	指紋	光学方式センサー，静電容量方式センサー，電界強度方式センサーなど	高	中	安
	静脈	近赤外光を利用するCCDカメラ	高	中	中
	虹彩	CCDカメラ	高	中	高
	顔	CCDカメラ	中	高	中
行動的特徴	音声	マイクロホン	中	高	安
	署名	タブレット	中	高	安

Fundamentals of Biometric Authentication Technology.

要をまとめたものである[3]。これらのモダリティはいずれも，上記の三つの性質を有すると考えられている。このうち，指紋，静脈，虹彩，顔といったモダリティは，本人を直接特定できる物理的な特徴であり，身体的特徴とよばれる。これに対し，音声や署名といったモダリティは，何らかの行動に伴って現れる生成物から抽出される特徴であり，行動的特徴とよばれる。

本章では，既に実用化が進んでいる指紋および静脈を中心に，各モダリティの概要を述べる。

3･1　指紋

バイオメトリック認証技術において，指紋は代表的な生体的特徴として早くから利用され，現在も最も広く活用されている。指紋は，指表面の凹凸で成り立っており，凸部は隆線，凹部は谷線と呼ばれる。平均的な指紋の凹凸は高さ約 50 μm，隆線の間隔は約 400 μm である。この隆線が描く紋様は，弓状紋，渦状紋，蹄状紋などに分類される。これらの紋様に含まれる隆線の端点や分岐点の位置と方向などを特徴点として認証を行う。

現在，指紋認証はモバイル機器の使用開始時の認証，情報機器内の情報にアクセスするときの認証，重要施設への入退室管理など，幅広い分野で利用されている。また，医療分野では，電子カルテのセキュリティ強化のために指紋認証が利用されている例もある。

指紋画像は，指紋スキャナにより比較的容易に取得できる。具体的には，スキャナの平坦部分に指先を置いて静止状態で読み取る面型センサーや，直線的なセンサー上で指をスライドさせて読み取るスイープ型センサー（またはライン型センサー）がある。前者は据置型の指紋認証システムで用いられ，後者は携帯電話やノート PC などに搭載されている。特にスイープ型センサーは，指紋の読み取り後に，センサー上に指紋が残留しにくいという特長を有する。指紋スキャナの主な読み取り方式は以下の 5 種類である[3]。

(1)　光学方式

指紋への光照射の仕方によって，図 2 のように指表面反射光センサーと，指内散乱光センサーに分類される。両者とも，指紋の隆線と谷線の凹凸において光の反射および散乱特性が異なることを利用して，指紋を読み取る。

指表面反射光センサー｛図 2(a)｝は，赤外光や可視光を指表面に照射し，その反射光を CCD（charge coupled device）や CMOS（complementary metal oxide semiconductor）の撮像素子で読み取る。プリズムやレンズを用いる構造のため，センサーのサイズが大きくなる傾向がある。

一方，指内散乱光センサー｛図 2(b)｝は，指の側部から光を照射し，指内部を透過して指表面の指紋部分から漏れ出す光を撮像することで指紋を読み取る。光源と撮像素子を平面に配置できるため，センサーを薄く小型にすることができる。また，指表面反射光センサーで読み取りにくい乾燥指や湿潤指にも対応できるという特長を有する。

(2)　静電容量方式

この方式では，指紋の隆線や谷線の凹凸に応じて指とセンサーの距離が変化し，静電容量も変化するという特性を利用する。そして図 3 のように，指表面とセンサー内の電極間の静電容量を検出して，指紋を画像化する。この方式は，乾燥指の影響は受けにくいものの，指が濡れると静電容量が変化するために，湿潤指の影響を大きく受ける。この方式は，多くのスイープ型センサーで採用されている。

(3)　電界強度方式

指とセンサー内の電極間に印加した交流信号により発生する電界の強度は，指紋の凹凸で変化する。これを利用して，図 4 のようにセンサー内のアンテナで電界強度の大小を測定することにより，指紋を検出する。この方式も乾燥指の影響は受けにくいが，湿潤指の影響を大

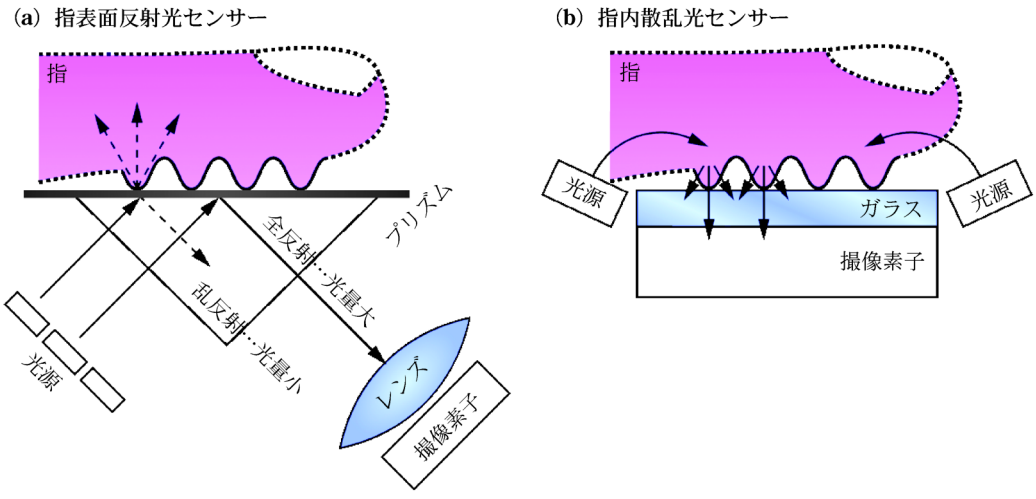

図 2　光学方式指紋センサーの模式図[3]

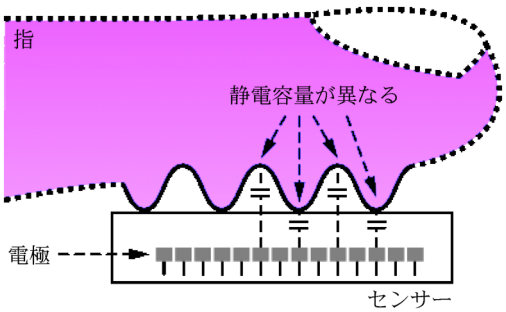

図 3　静電容量方式指紋センサーの模式図[3)]

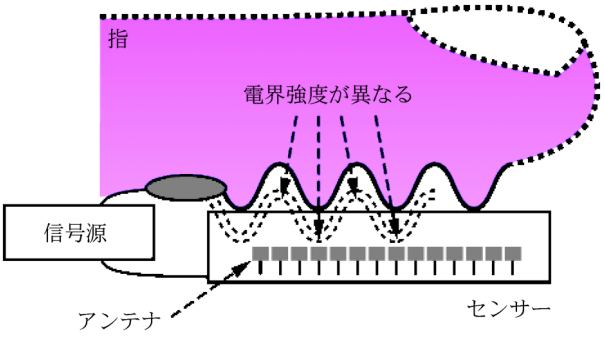

図 4　電界強度方式指紋センサーの模式図[3)]

きく受ける。本方式も静電容量方式と並んで，スイープ型センサーに採用されている。

⑷　感圧方式

指紋の凹凸によって変化する感圧センサーにかかる圧力を，圧力によるセンサーの変形具合で変化する静電容量により読み取る方式である。圧力を用いるため，指の乾燥・湿潤の影響を受けない利点がある一方，センサー表面が磨耗しやすい材質で製作されるため，耐久性が低い傾向がある。

⑸　感熱方式

感熱方式には，主に二つの方式がある。一つは，指先の凹凸で熱の伝導が異なり温度差が生じるという特性を利用し，指から伝わる熱の高低をセンサーで読み取る方式である。もう一つは，センサーの中に設けたヒーターからの熱が，接触した指紋の隆線部分で奪われることで生じる温度変化を利用するものであり，温度センサーでこれを読み取り，指紋画像を得る方式である。感熱センサーは耐久性が高く小型であるため，スイープ型センサーに採用されている。

3･2　静脈

波長 700～1200 nm の近赤外光は，生体を比較的よく透過する。例えば，手のひら側から近赤外光を照射すると，手の甲表面の血管網が明瞭に観察できる。一方，手の深部の血管や骨は観察できない。これは，手の深部の血管や骨により光が強く散乱され，血管や骨の構造が拡散光に埋もれてしまうことによる。従って，静脈認証で

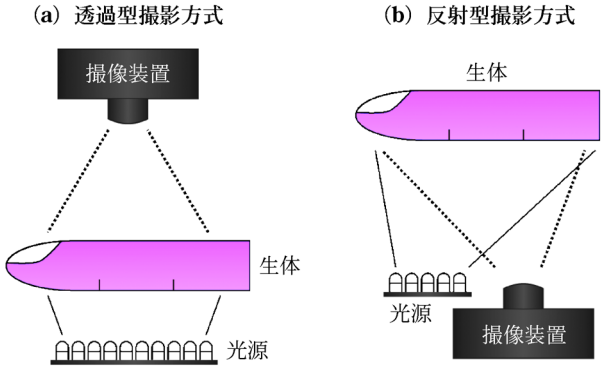

図 5　静脈像の撮影方式の模式図[3)]

対象とする血管パターンは通常，生体の表層付近のものであり，その代表例は網膜静脈，手部静脈および指静脈である。

近赤外光を利用した静脈像の撮影方式を図 5 に示す[3)]。透過型撮影方式(図 5a)では，光源と撮像素子を，生体の対象部位を挟んで反対側に対向させて配置する。一方，反射型撮影方式（図 5b）では，光源と撮像素子を生体の同じ側に配置する。いずれの場合も，生体の表層付近の静脈像を取得できる。

取得した静脈像は，静脈像自体のマッチング処理，または分岐点位置や血管セグメント方向などの特徴点処理により照合が行われる。静脈認証は ATM（automatic teller machine）利用時の本人認証，工場やデータセンターなど重要施設の入退室管理システムでの本人認証などに利用されている。

以下，生体の部位ごとに，静脈像の特徴を説明する。

⑴　網膜静脈

網膜静脈パターンは眼の中に保持されており，生体表面の特徴と比較して外部環境の影響を受けにくく安定である。また，外部から容易に観察できず，盗用や偽造に強いという特長を有する。網膜静脈認証はその像が複雑であるために認証精度が高く，早くから実用化されてきた。しかし，認証の際には微弱な近赤外光を目に照射しなければならず，撮影装置に目を近付ける必要があることなどから，利用者に心理的抵抗感を抱かせる。また，白内障，糖尿病，眼底出血などにより網膜静脈像が変化してしまうという問題もある。

⑵　手部静脈

手部静脈像は透過型撮影方式でも反射型撮影方式でも撮影することができる。いずれの方式も完全非接触型であり，衛生面の問題もなく，利用者が抱く心理的抵抗感も少ない。また，指先のように寒さによる血流変化の影響を受けることも少ない。一方，手部表面の傷や汚れの影響を強く受けるため，これらが原因となって認証精度が劣化するという問題がある。

⑶　指静脈

指静脈像の特徴は以下のとおりである。

- 個人間の差および同一人でも指間の差が大きく，認証精度が高い
- 指の内部にあり，長期にわたり安定している
- 両手で十指あることから，一指の情報が盗まれた場合でも，他の指の情報に変更できる
- 利用者によって静脈が深い位置にある場合や細い場合には，有効な指静脈像が撮影できない場合がある
- 寒さで指の血流が悪い場合には，指静脈像の撮影が困難な場合がある

指の表面付近の静脈像は，透過型撮影方式により撮影される。撮影対象である指が小さいことから照射光量が少なくてすみ，撮影装置を小型化できる。また，指表面の傷や汚れの影響も受けにくい。一方，撮影装置に指を挿入すると指先が見えなくなるため，慣れない利用者に不安を抱かせるおそれがある。

3･3　虹彩

虹彩（こうさい）とは，瞳の周りにある環状の領域である。この領域には筋肉の凹凸があり，そこに脂肪が沈着してランダムなパターンが形成される[1)]。赤外光により，このパターンを計測することができる。虹彩は人により異なり，瞳孔のサイズが変化しても相似的に変化する。また，虹彩のパターンは複雑で経年変化が少なく，偽造も容易ではない。このような特長を有することから，虹彩は早くから本人認証システムに利用されてきた。虹彩による認証は認証精度が高いことから，高いセキュリティを必要とする重要施設の入退室管理に利用されているほか，空港における入出国管理や搭乗手続きへの利用が試みられている。

虹彩像は，目の画像を撮影するだけで取得できるため，完全非接触で衛生的な認証が可能である。ただし，目の画像撮影時にはカメラに正対静止する必要があり，利用者の体の動きや身長差，立ち位置などによって認証成功率が低下する可能性がある。また，まつ毛が映るなど虹彩像が低品質である場合も認証成功率が低下するため，その影響を回避する方法も研究されている。

3･4　顔

我々が他人を識別するとき，最も自然に利用するのが顔の概観である。デジタル画像処理技術の進歩により，顔画像中に多くの特徴点をとらえて解析することが可能となっている。顔によるバイオメトリック認証は，パスポートや運転免許証など従来からの本人認証の自然な発展形として受容されやすい。また，顔画像は非接触で撮影可能であり，利用者の行動を制約することが少なく，利用者が意識することのない認証も可能である。さらに必ず顔画像を取得することから，他のバイオメトリック認証技術と比較して不正防止効果が高い。このような特長から，重要施設の入退室管理に加え，空港などの防犯カメラからの画像を用いた監視や，入国時のパスポートの顔画像データとの自動照合などに利用されている。

顔認証には，唯一性に対する脅威（一卵性双生児や，うりふたつの人間の存在）や，永続性に対する脅威（加齢や病気による顔の変化）が存在する。また，顔画像の取得時には化粧，眼鏡や帽子などの装着物，照明条件，顔の向きや動きなどの影響を受けやすい。これらの問題を解決するため，近赤外光を使った顔画像撮影などにより，認証精度を向上させる試みが行われている。

3･5　その他の身体的特徴

その他の身体的特徴として，掌形（手の形状），耳介（耳殻）の形状，指にある汗腺の分布，およびにおいがある。また，心電図や唇紋，DNA を利用する試みもある。これらの身体的特徴はそれぞれ優れた特長を有するが，指紋や静脈のように実用化および普及が進むためには，さらなる研究および技術開発と，適切な応用分野の開拓が必要である[5)～7)]。

3･6　行動的特徴

音声による個人認証は，声道の物理的な形状によって決まる共振周波数に着目した認証方式であり，テレホンバンキングにおける本人認証などに利用されている。声道の共振周波数は本人の間でも変動が大きいため，用途は限定される。一方，音声は自然にかつ非接触で採取できることから，利用者が抱く心理的負担は少ない。

署名による本人認証は，紙に書かれた署名どうしを比較するオフライン署名認証と，署名時の時系列を採取する装置（タブレット）で得たデータを利用するオンライン署名認証とに分類される。音声同様，毎回の署名から抽出される特徴量は本人であっても変動が大きいことから用途が限定され，企業内の電子決済などで実用化されている。

音声や署名などの行動的特徴は，模倣やなりすましが困難であるという特長を有することから，今後の研究・開発の進展に伴い，利用の拡大が期待される。

4　バイオメトリック認証技術に関するトピックス

4･1　バイオメトリック認証システムの性能

バイオメトリック認証システムの基本性能のうち，本節では，本人拒否率と他人受入率について説明する。

2 章で述べたとおり，バイオメトリック認証では，生体的特徴を計測した後，取得したデータを数値化する。例えば，指紋認証や静脈認証では，画像上のパターン特徴点間の距離や配置などを数値化する。そして，認証システムに予め登録してある生体的特徴の数値（テンプ

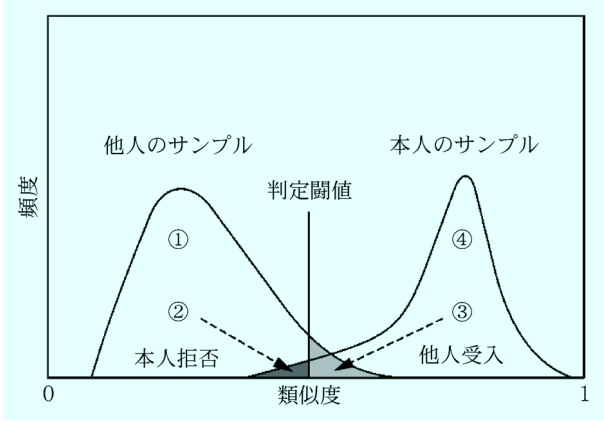

図 6　本人拒否率と他人受入率の概念を示す図

レート）と，認証時に得られた生体的特徴の数値（サンプル）が比較され，その類似度に基づき，サンプルを提示した者が本人であるか否かを判定する。

図 6 は，本人の登録テンプレートに対して，本人と他人が混在する多数のサンプルを比較した場合の，類似度のヒストグラムを模式的に示したものである[1)4)]。このとき，本人のサンプルと他人のサンプルに対応する二つの分布が形成される。この二つの分布が十分に離れていれば，その境界に判定閾値を設定することにより，理想的な判定が実現できる。しかし一般的には，図 6 のように二つの分布に重なりが生じるため，この図のように判定閾値（いきち）を設定した場合，その両側の②と③の領域は判定誤りとなる。つまり，領域②は本人のサンプルであるにもかかわらず他人であると判定されてしまう領域，また，領域③は他人のサンプルであるにもかかわらず本人であると判定されてしまう領域である。これらの割合を次のように定義する。

FRR（false rejection rate，本人拒否率）
＝②/(②＋④)
FAR（false acceptance rate，他人受入率）
＝③/(①＋③)

FRR および FAR は，バイオメトリック認証システムの基本性能を表す重要な指標である。理想的には，FRR も FAR もゼロであることが望ましいが，そのようなシステムを実現することは不可能であると考えられている。そこで，両者の値を可能な限り小さくすべく，生体的特徴の取得方法や数値化方法の改良が行われている。

なお，バイオメトリック認証システムでは，利用者から取得した生体的特徴のサンプルが登録テンプレートに一致した場合に，その利用者を拒否するという応用もある。例えば，ブラックリスト掲載者の入国を拒否する場合である。この場合は，上述の例と比較して，拒否と受入の意味が逆転する。このような混乱を避けるため，FRR および FAR の代わりに，それぞれ FNMR（false non-match rate）および FMR（false match rate）という呼称が使われる場合もある。

4･2　バイオメトリック認証技術の標準化

他の様々な技術と同様，バイオメトリック認証技術も，当初はそれぞれの技術を開発した企業などが独自の方法で，データフォーマットの設定や認証精度の評価を行ってきた。しかし，バイオメトリック認証技術の急速な発展および国際的な普及に伴い，個々の規格の不統一が問題となってきた。

そこで 2002 年に，ISO（International Organization for Standardization）と IEC（International Electrotechnical Commisson）の合同委員会である JTC1 (Joint Technical Committee 1)により，バイオメトリック認証技術の開発と標準化を担う SC（subcommittee）が設置され，グローバルなバイオメトリック認証技術の構築を目指した活動が行われている[3)4)]。

4･3　バイオメトリック認証技術とプライバシー

バイオメトリック認証で利用する生体的特徴は以下のような特性を有するため，個人のプライバシーとして保護されるべきものである。

- 身体的特徴はパスワードのように何度も変更することができず，一度盗まれると利用できなくなってしまう
- 指紋や顔など体外に露出した身体的特徴は，本人の同意なく盗み取ることが容易である。また，顔画像が取得された場合，本人を容易に特定できることから悪用されやすい
- バイオメトリクスで取得した生体的特徴から，人種や健康状態などの個人情報を引き出すことが可能である

バイオメトリック認証において個人のプライバシーを守る方策として，ハードウェア技術やソフトウェア技術により，テンプレートなどのデータの保護を強化することが挙げられる。また，法律などによりプライバシーを制度的に保護することも挙げられる。

このうち，プライバシーの制度的保護については，1980 年の OECD（Organization for Economic Co-operation and Development）の理事会勧告に基づき，世界各国で個人情報保護の法制化が行われた。わが国でも「個人情報の保護に関する法律」（個人情報保護法）が 2005 年 4 月から全面施行されている。バイオメトリック認証で取り扱う生体的特徴のほとんどは，本法律における個人情報に該当するため，バイオメトリック認証技術はこの法律に基づいて実施および運用していくべきである[4)]。

4･4　マルチモーダル認証技術

バイオメトリック認証システムは，他の一般的な認証

システムとは異なる，以下のようなリスクを有する。

- 身体的負傷により認証不能となるリスクがある。例えば，指紋認証では指を怪我した場合である
- 不正に入手した生体的特徴から人工の複製物（クローン）が製作され，悪意の者により認証が突破されるリスクがある。例えば，指紋を写し取ったグミキャンディによる指紋認証の突破，野菜（大根）で製作した人工指による指静脈認証の突破，顔写真や仮面による顔認証の突破がある
- あらゆる登録テンプレートに対して高い類似度を得る生体的特徴を有する利用者が出現するリスクがある。このような利用者は“wolf（狼）”とよばれ，あらゆる他人になりすますことができる
- あらゆる利用者の生体的特徴サンプルから高い類似度を得られてしまう生体的特徴を有する利用者が出現するリスクがある。このような利用者は“lamb（子羊）”とよばれ，あらゆる他人に認証を突破されるおそれがある

このようなリスクを低減し，システムの認証精度を向上させるため，テンプレートとサンプルの照合プロセスを強化する方法がいくつか提案されている。例えば，複数のバイオメトリック認証技術の組み合わせにより，認証精度や利便性を向上させることができる。これを，マルチモーダル認証という。

この方法では，互いに独立した複数種の生体的特徴のテンプレートを，それぞれ異なるデータベースに登録する。認証の際には，複数種の生体的特徴を取得し，それに基づくサンプルを作成し，それぞれ対応するテンプレートと照合する。これらの照合結果を総合して判定結果を得る。これにより，個々のバイオメトリック認証技術の欠点が補完され，認証精度や利便性の向上につながる。マルチモーダル認証では，一つの生体的特徴が使用できない利用者でも認証が可能となり，対応可能な利用者の割合（対応率）も向上する。

ただし，この方式では一般に装置やシステムが複雑化・大型化する傾向がある。そこで，例えば指紋と指静脈，虹彩と網膜静脈など，同一部位の生体的特徴を組み合わせることにより，最小限の拡張で効果が期待できる。

5　おわりに

本稿では，バイオメトリック認証技術の基礎について解説した。本稿で述べたように，バイオメトリック認証システムはユビキタス社会およびネットワーク社会のインフラとして，既に不可欠なものとなりつつある。

本稿で紹介した生体的特徴のほかにも，普遍性・唯一性・永続性の三つの要求を満たす生体的特徴があると考えられており，今後も様々な生体的特徴を利用したバイオメトリック認証技術が新たに登場してくると予測される。そしてその際には，化学計測で用いられる様々な技術が応用される可能性も高い。簡易かつ安全に使用でき，低コストでかつ高い認証精度を持つバイオメトリック認証技術が実用化されることを期待する。

文　献

1）小松尚久，内田　薫，池野修一，坂野　鋭：“バイオメトリクスのおはなし”（2008），（日本規格協会）．
2）バイオメトリクスセキュリティコンソーシアム編：“バイオメトリックセキュリティ・ハンドブック”（2006），（オーム社）．
3）映像情報メディア学会編，半谷精一郎編著：“バイオメトリクス教科書”（2012），（コロナ社）．
4）清水孝一：生体医工学，**44**，3（2006）．
5）岡嶋裕史：“セキュリティはなぜ破られるのか”，p. 100（2006），（講談社）．
6）D. Bhattacharyya, R. Ranjan, F. Alisherov A., M. Choi : *International Journal of u- and e- Service, Science and Technology*, **2**, 13 (2009).
7）S. Chauhan, A. S. Arora, A. Kaul : *Procedia Computer Science*, **2**, 213 (2010).

小木　修（Osamu Kogi）
㈱日立製作所横浜研究所（〒244-0817 横浜市戸塚区吉田町 292）。北海道大学大学院理学研究科修了。博士（理学），情報セキュリティスペシャリスト。≪現在の研究テーマ≫生体試料分析技術の研究・開発。≪主な著書≫“Single Organic Nanoparticles”（分担執筆）（Springer）。
E-mail : osamu.kogi.mq@hitachi.com