調査対象技術の技術概要

「バイオメトリック照合の入力と認識」

１　バイオメトリック照合の基本

エレクトロニック・コマースの発達や電子政府の構築など、これからの社会においてはネットワークを介した公的・私的サービスの需要が大きな比率を占めるようになる。その一方で、なりすましなどの不正が与える影響は計り知れぬものがあり、ネットワークにおける個人識別が非常に重要な課題として認識されてきている。

またアメリカで発生した同時多発テロ以降、安全を確保するためにも個人認証は重要性を高めてきており、広い応用範囲に対応でき、しかも精度が高いと言われているバイオメトリクスを利用した個人識別の技術開発が盛んになっている。

１．１　バイオメトリック照合の基本的特徴

現在、広く使われている個人識別の方法として、ID カードや暗証番号などがある。ID カードによるシステムは、例えば入退室管理などではそれ以前の鍵と錠からなるシステムに比べてシステム運用の自由度が高い。しかし ID カードを携帯しなければならないことや、紛失事故にあった場合、ID カードの保持者であれば本人でなくともアクセス可能であること（暗証番号の併用方式ではその番号を不正に知っていた場合）など、従来システムと本質的には同様の不都合がつきまとう。

これに対して、人間の生体情報を利用するバイオメトリック照合では、当該人間のバイオメトリック情報をオンサイトで照合するので、紛失事故の危険性が低減し、ID カードに比較してなりすましは困難になるという利点がある。

個々人を区別する個人情報としてはいろいろなものが手がかりとなる。しかしながら個人識別を人間が行うにせよ機械が自動的に行うにせよ、個人に固有のどのような特徴を見つけ出すかは大きな問題である。

バイオメトリック照合に用いる情報のひとつの目安としては、

（１）個人固有の特徴であること
（２）長期間にわたって不変な特徴であること
（３）観察あるいは計測しやすいこと

などがあげられる。人間を個体として識別する手がかりには、（１）形態学的特徴（指紋や虹彩、血管パターンなど）、（２）機能的特徴（署名や声紋など）、（３）生化学的特徴（血液型など）などがある。

１．２　バイオメトリック照合で使われる生体情報

上記のような特性を持つ生体情報としては次のようなものがある。

表　バイオメトリック照合で使われる生体情報

生体情報	特徴	照合の精度
指紋	手指の指紋のパターンや特徴点（マニューシャ）を利用。	○
虹彩	目の虹彩（アイリス）の放射状の模様を利用。	◎
血管パターン	網膜や手の甲、手のひら、指などの静脈のパターンやその特徴量を利用	○ 網膜は◎
顔	顔の輪郭、目や鼻の形および配置、顔画像の濃淡情報などを利用	△
声紋	話者の音声特徴を利用	×
署名	署名の字体や署名時の書き順、筆圧などを利用	×
その他	掌形（手の大きさや長さなど)、耳介、DNA などを利用	掌形△、耳介、DNA◎

注：「精度」の欄はアルゴリズムの精度を表す。10 点満点の評価をした場合、◎は 10-4 以上、○は 10-2 以上、△は１桁、×は１以上。

１．３　各生体情報に共通する処理の流れ

生体情報を使った認証（バイオメトリック認証）の処理の流れを図式化すると下図のようになる。この処理の流れは指紋や虹彩、網膜、静脈血管パターン、サインなど取り扱う生体情報が異なっても概ね同じである。

（１）データ収集

生体情報を認証システムに取り込む部分の処理であり、様々な生体特性（指紋のパターンや静脈血液の波長吸収特性など）ごとに、各種のセンサーが開発されている。この処理段階における中核的な技術はセンサー技術である。

（２）伝送

生体認証システムがネットワークを使ったものである場合、センサーで読み取った生体情報を伝送するという処理が必要となる。生体情報は極めて個人的な情報であり、またセキュリティシステムのキーとなる情報であるため、この処理段階では暗号化技術などの符号化技術が必要となる。

（３）信号処理

センサーから送られてきた生体情報を加工して、そこから個人の特徴に関する情報を抽出し、さらに、登録してあるバイオメトリックス情報（テンプレート）と比較照合（パターンマッチング技術）するといった生体情報による認証の中核的な処理段階である。この段階では、特徴抽出技術、比較・照合技術がバイオメトリックス特有の技術として極めて重要である。

（４）蓄積

センサーから送られてきた生体情報または、それから抽出された個人に固有の特徴情報をデータベースに蓄積し、認証の際の基準とする処理段階である。この段階では、認証処理の内容に合わせ

たデータ圧縮技術やセキュリティ技術、あるいは登録情報を固定せず常に変化させながら保持する方式など、バイオメトリックスと関連の強い技術もあり、今回の調査ではこうした関連の強い技術も標準技術の対象とする。

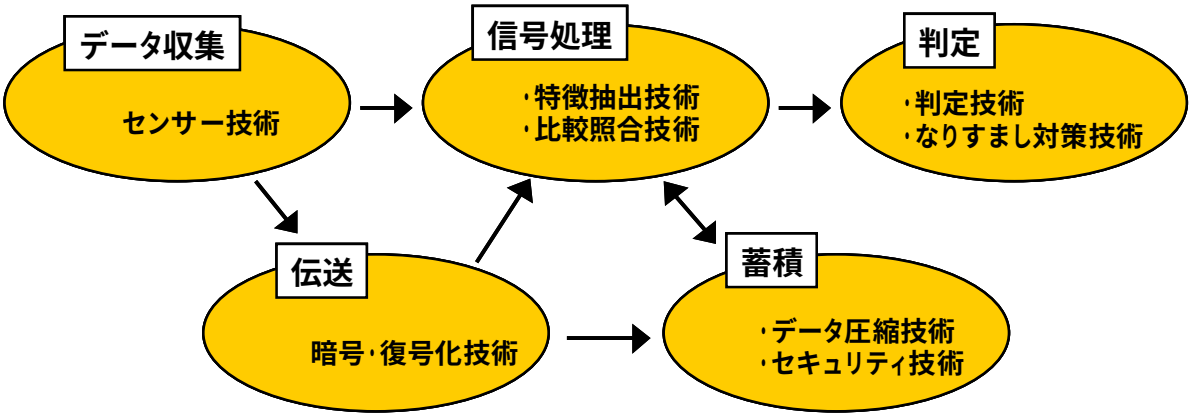


図　バイオメトリックス認証の処理の流れ
出典：本標準技術集のために作成

（５）判定

これは、入力された生体情報（特徴抽出などの信号処理を行った情報）とデータベースに蓄積された登録情報とのマッチング処理を行った結果に対して判定を行う段階である。判定のアルゴリズムもさることながら、なりすまし対策技術や認証失敗時の救済技術などこの段階の技術もバイオメトリック認証システムにおいては重要な技術である。

１．４　一般的な応用分野

バイオメトリクスの応用分野としては次のようなものがある。
（１）入退室管理
（２）パソコンやコンピュータシステムへのログイン
（３）特定のサービスへのアクセスコントロール
（４）出退勤管理
（５）身分証明書
（６）金融関連カード
（７）特定個人の探索
（８）犯罪者、身元不明者の本人確認

（参考文献）
・「これでわかったバイオメトリクス」、2001 年 9 月 10 日、日本自動認識システム協会編、株式会社オーム社発行
・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行
・「セキュリティにおける個人識別技術」、「システム／制御／情報　35 巻 7 号」、1991 年 7 月 15 日、増田功著、システム制御情報学会発行、431-439 頁

２．　指紋照合

手指の末端に存在する模様（指紋）は、「万人不同」「終生不変」の特徴を持つと経験的に理解されていて、中国やインドなどでは古代から個人を同定する手段として用いられ、日本でも昔から拇印の風習があった。今日、人の身体的特徴を用いて個人を認証するために様々なバイオメトリクス技術が研究されているが、この中で指紋は最も古くから研究され実用化が進んできた認証技術であり、最近ではネットワーク社会における本人認証方式として、様々な研究開発が行われている。

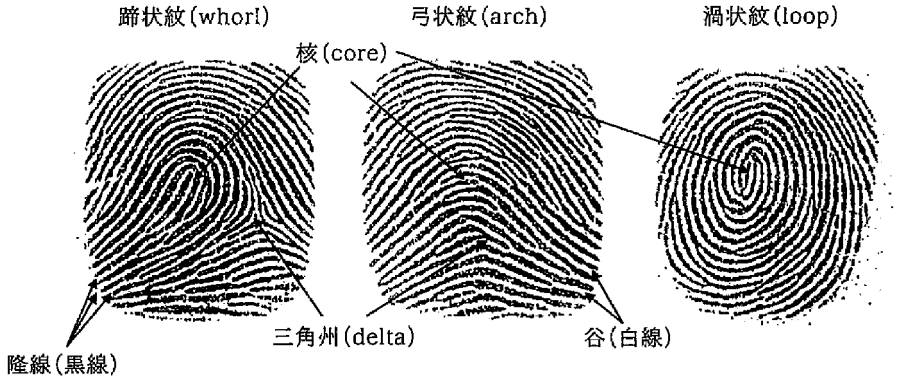
２．１　生体情報の特徴・特性

指紋は、隆線とその間に形成された谷の紋様が個人を特徴づけている。この紋様は、同一人の 10 本の指を比較しても、また一卵性双生児間でも異なっており、世の中に同一の指紋を持つ人の確率は 870 億分の１と言われている。指紋は、以下のような特徴・特性を持つ。

（１）　指紋の紋様の種類

指紋の紋様は、図 2.1 に示すように、大別して 3 種類（蹄状紋、弓状紋、渦状紋）に分類できる。蹄状紋は、隆線が一端から始まり 360 度回転して同じ側に戻るもので、流れの反対側に三角州と呼ばれる特徴点がある。弓状紋は、隆線が一端から他端に流れるもの。渦状紋は、隆線の少なくとも 1 本が渦状あるいは環状を呈するもので、左右一つづつの三角州がある。

図 2.1　指紋パターンの分類

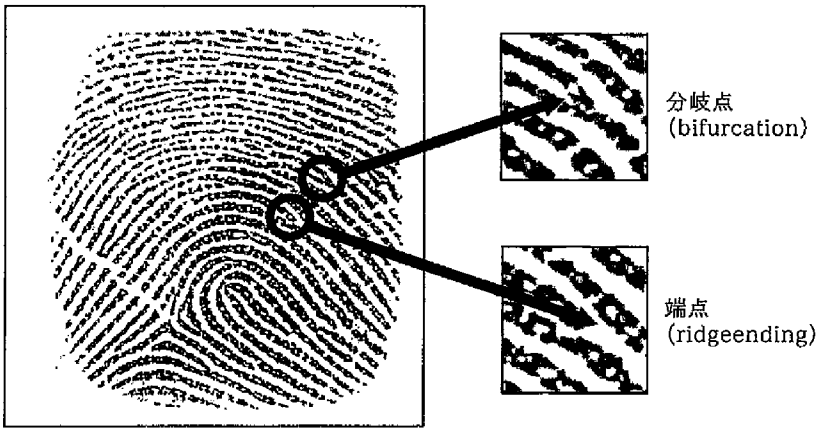


出典：「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、第 38 頁　図 2.5　指紋パターンの分類

（２）　紋様の特徴点

紋様に着目してその形状を詳細に分析すると、特徴点と呼ばれる紋様の特徴を表す場所が見つかる。この特徴点としては、図 2.2 に示すような隆線の分岐点や端点、他に三角州、湧出、ドットなどがある。これらを総称してマニューシャと呼び、一つの指に 150 程度あるといわれている。

図 2.2　指紋の特徴点



出典：「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、第 39 頁　図 2.6　指紋の特徴点

（3） 入力センサの小型化

入力センサの小型化および個人で照合技術の使用が可能なことから、利用形態としてパソコンや携帯端末に搭載しての使用が可能である。

（4） 指紋を採ることの抵抗感（受容性の問題）

個人認証の用途に一般の人が使用する場合、犯罪捜査における指紋採取を連想することから、指紋を採ることに抵抗を感じる人がいる。

（5） 指紋画像を得られない場合がある（可用性の問題）

労働作業による指紋の磨耗や体質による指の乾燥・発汗などの理由により、必要な品質で指紋画像を得られない場合がある。

２．２　技術開発の歴史

歴史的には、先史時代から中国やインドなどで個人を示すのに使われていたのが知られているが、指紋を用いた個人同定（認識）の科学的な研究は、1864 年にイギリス王室医科大学の N.Grew によって本格的に始められたとされている。

指紋による個人識別の実用化に貢献したのは、イギリスの植民地時代のインドでイギリス政府の役人であった W.Hershel(1833-1917)である。彼は、現地人に公式文書には指紋や手形を押させて悪事を犯させないようにしたが、その後、指紋は個人個人で異なり（後述する F.Galton が証明した）、自分の指紋を見て一生変わらないことに気付き大規模に導入した。同じ頃、イギリス人の F.Galton(1822-1911)は、マニューシャについて研究し、指紋の紋様を蹄状紋、弓状紋、渦状紋の三つに分類し、指紋が終生不変で、同一固体がないことを指摘した。個人同定に本格的に利用されるようになったのは 19 世紀の終わりごろで、イギリス人 E.R.Henry が勤務地インドにおいて、インド人を個人識別するのに容貌のみでは難しいことから指紋を用いた個人識別を提唱したことに始まり、1897 年にインド政府は指紋法を発布した。そして 1901 年にはイギリスで犯罪者の登録方法として指紋を採用した。日本における個人識別は、1908 年施行の刑法で再犯罪者を重罰にするために犯罪者の個人識別として指紋を採用したことに始まる。

自動化への取り組みも 1960 年代と比較的長い歴史を持つ。警察庁は 1971 年にコンピュータによる

指紋鑑定の研究を開始し、1981 年に犯罪者管理システム (Automated Fingerprint Identification Systems：AFIS)として稼動している。現在では、高い精度で個人を自動認証する方式・システムが実用化されており、最近ではネットワーク社会における本人認証方式として様々な研究開発が行われている。

２．３　照合技術の基本的な仕組み・原理

（１）指紋画像撮影の原理

指紋は、指先の皮膚紋様の盛り上がった部分で形作った線である「隆線」とその間の「谷線」で形成された紋様で、この凹凸の高さの違いをコントラスト良く 2 次元画像化するのが入力指紋センサの役割である。入力画像の標準的な解像度は、500dpi で、得られる画像サイズは 1.5cm から 2.5cm 角程度のものが多い。

このコントラストを得る手段としては大別して、指に光を照射する方法（光学式）と光以外の方法、の 2 通りの方式があるが、原則として、センサ面に触れるか否か（隆線と谷線）でコントラストを得ている。

（光学式）

この方式の原理は、基本的にはセンサに接して置いた指に光を照射した時、センサに触れる隆線とセンサに触れない谷線とでは光の反射の仕方が異なることを利用してコントラストを得るもので、隆線が明になる方式と隆線が暗になる方式の二通りがある。

例えば、代表的な方式である全反射法は、隆線がセンサに触れると指の水分により全反射条件が失われて黒く撮影され、谷線はセンサ面との間に空気が存在するために全反射し明るく撮影される。逆に光路分離法では隆線が明るく谷線が黒く撮影される。

なお、指の表面ではなく真皮部分における隆線と谷線を使用する方式もある。

（非光学式）

この方式の原理は、センサに接して指を置いたとき、センサに触れる隆線とセンサに触れない谷線とを光以外の方法（半導体技術など）で検知する方式である。

例えば、静電容量や温度の差を検知してコントラストを得ている。

（２）特徴抽出と照合

上記の原理に基づいて入力センサで得られた画像に対して、画像処理を施して隆線パターンを 2 値化画像として抽出し、必要があればそれを細線化する。指紋照合のアルゴリズムは、大別して、指紋の大局的なパターンを比較するパターンマッチング方式と、指紋の局所的な特徴を比較するマニューシャ方式、の 2 種類に分かれる。

（パターンマッチング方式）

パターンマッチング方式は、テンプレートに登録してある 2 値化画像もしくは細線化した指紋画像と、照合時に入力した 2 値化画像を直接比較して、その類似度を算出する方式である。しかし、入力時に指の変形などの影響を強く受けるため、画像同士の照合についても工夫がなされている。例えば、指紋画像の濃淡変化を時系列信号とみなして抽出したスペクトルを用い、HMM（隠れマルコフモデル）マッチングを行うなどの方法がある。

（マニューシャ方式）

マニューシャ方式は、最も古典的かつ実績のある方式で、テンプレートのサイズも小さく、多くの商用指紋照合システムで実用化されている。これらのアルゴリズムは、全て細線化画像からマニューシャを特徴として抽出し、マニューシャに付随する局所的な情報を比較することで照合

を行う。このマニューシャを用いた代表的な照合方式としては、次の三つある。

（ア） マニューシャ方式

マニューシャの位置、種類（端点、分岐点など）、方向を利用して照合する方式

（イ）マニューシャリレーション方式

マニューシャ方式に加え、隣接するマニューシャ間の隆線の数（リレーション）も特徴として抽出し、照合する方式

（ウ）チップマッチング方式

マニューシャの位置とマニューシャを中心とする 2 値化した小画像を特徴として抽出し、照合する方式

この三つの方式を比較すると、照合の精度はマニューシャリレーション方式が最も良い。しかし、処理が最も複雑である。照合時の処理が最も軽いのはチップマッチング方式で、単純なビット演算で照合処理を行うことができる。

２．４　応用分野・応用事例

（１） パソコンのアクセス管理

パソコンの起動時やファイルへのアクセスに対し、パスワードの変わりに指紋を使用することで、セキュリティ向上を図る。

（２） 入退室管理

部屋の入退室に指紋を使用することで、入退室用の IC カード紛失等による部外者を排除できる。また、タイムカードの使用では、他人による不正打刻を防ぐことが可能となる。

（３） 電子決済・電子商取引の本人認証

PKI の使用において秘密鍵の管理に IC カードなどが利用されるが、この IC カードの持ち主が本当の持ち主かを確認する手段として、指紋を用いる。指紋情報も IC カードに入れ、使用者の指紋が一致して初めて IC カードの中の秘密鍵がアクセス可能となり、電子決済や電子商取引などのアプリケーションに連携される。

２．５　技術、システム上の課題（原理的な問題、直面する課題）

（１） 原理的な課題

指紋照合は、最も歴史が古く分析が進んでいるが、指先の皮膚の状態（乾燥、濡れ、汚れなど）により指紋の紋様が取得できない場合があること、センサへの指の押し付けによる変形が大きいことなどの技術的な課題があり、現在も研究が盛んに行われている。今日まで改善されてきた例を、標準技術集から幾つか挙げると次のようになる。

（ア）皮膚の状態による低品質の指紋画像について

低品質の指紋画像の精度向上に向けて、センサの改良、画質の補正、アルゴリズムの改良などを行ってきた。

具体的には、センサでは指の表面の指紋画像を取得するのではなく、指内部の真皮の指紋画像を取得する「指内拡散光検出型」や「指内部特性検出型」の方式により乾燥・濡れに強くし、画質の補正では、特徴を抽出する前処理として「隆線のコントラスト強調」や「並行

隆線フィルタ」などを行って隆線を明確に復元することで、特徴を正しく抽出できるようにした。また、アルゴリズムでは、指紋画像全体を比べることから面積的に微小な“かすれ”や“汚れ”に強い「位相限定相関法」などがある。

（イ）センサへの指の押し付けによる変形について

指の押し付けによる変形については、試作レベルの段階ではあるがセンサに触れない「非接触型」の入力形態ができている。また、アルゴリズムではパターンマッチング方式が指の変形の影響を強く受けるので、指紋を波形とみなす「周波数解析法」などの工夫が行われている。

（２） 直面する課題

指紋照合アルゴリズムは適用する画像の品質や母集団によって評価結果が左右されやすいため、各種ベンダ製品の品質比較が困難であることから、共通の評価基準が求められている。現在、標準化作業が進められているが、アルゴリズム単体評価での実際の運用時の結果が異なるなど、まだ問題がある。

（参考文献）

・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、37―49 頁

・「指紋認証システム」、「映像情報メディア学会誌　Vol.58　No.6」、2004 年 6 月 1 日、鷲見和彦著、社団法人　映像情報メディア学会発行、759―762 頁

３． 虹彩

虹彩の模様は、妊娠 7、8 ヶ月頃から形成され、生後 1 年程度で安定した後には、経時的に変化しないなど、バイオメトリクス照合に適した多くの特性を有している。また、虹彩認証は、指紋、顔、サインといった他の認証方式のように複数の認証方式が存在する状況とは異なり、Daugman による虹彩認証アルゴリズム以上に実用性があるアルゴリズムは公知となっていない。そのため、現時点では、虹彩認証システム＝Daugman による虹彩認証アルゴリズムを実装したシステムという図式となっている。

３．１　生体情報の特徴・特性

虹彩認証が個人認証に利用されるようになってきたのは以下のような虹彩が持つ特性によっている。
（１）医学的に万人不同といわれ、右目と左目でも異なる。一卵性双生児間、クローンでも異なる。
（２）生後、約 1 年で虹彩パターンが定まると、その後は経年変化がなく、生涯不変である。
（３）体の中にある情報なので、偽造が困難である。
（４）外部から虹彩模様が観測できるため、無侵襲かつ非接触で撮影できるようになった。

（１）の個体差が明確であることや（２）経年的に安定である、（３）内部器官なので偽造が困難といった特性は、虹彩がバイオメトリクス照合のモーダルとして適している特性であるが、（４）の外部からの可視性は、体の外からの攻撃（盗み見）を受け易く、偽造や成りすましの可能性が指摘されている。また、同じく（４）無侵襲非接触性といった特性は、広い適用分野を可能にすると同時に、他人の触った機器に自分の体を触れさせずに済むといった利用者の忌避感を低減させている。

これらにより、虹彩認証は、高精度認証、偽造困難、高速応答、衛生的、抵抗感小など、バイオメトリクス認証の要件を数多く満たす利点が得られている。特に FAR（Fales Acceptance Rate：他人受入れ率）に関しては、各種バイオメトリクス照合技術のなかでも、比較的高い精度を実現している。

３．２　技術開発の歴史

虹彩の特性は以前から認識されてきたが、今日の虹彩認証技術の歴史は、1987 年に Leonard Flom と Aran Safir の２人のアメリカ人眼科医によって、ユニークかつ不変であり個人認証に使用できるという基本特許が成立したところから始まる。そして、1993 年に J.G.Daugman によって、虹彩画像から特徴を抽出した虹彩コードを比較照合する今日の虹彩認証アルゴリズムの嚆矢となる技術が開発された（特許は Iridian Technologies 社が保有）。また、Daugman はアルゴリズムを開発しただけではなく、個人の虹彩画像のユニーク性についても数学的な証明も実施し、虹彩認証技術の基礎体系を整備したと言える。

そして、このアルゴリズムの登場以降については、全自動認証やメガネ・コンタクトをつけたままで認証可能といった、製品化に伴うユーザニーズ関連の開発が主となっている。

３．３　照合技術の基本的な仕組み・原理

虹彩認証の基本的な仕組みは、まず虹彩画像の撮影、そして得られた虹彩画像から特徴量の抽出とコード化、事前に登録された虹彩コードとの照合という一連のプロセスを経て本人かどうかが決定される。

（1）虹彩画像の撮影

虹彩画像の取得に際しては、CCD や CMOS といった一般的な撮像素子によるデジタルカメラが用いられている。比較的低コストな製品については、虹彩（この時点では虹彩を含む目の画像）の撮影は手動で行われるため認証時の手間や所要時間がかかるが、高級機種では広角カメラとズーム機能付きの狭角カメラ、自動照明制御によりノイズ等が低減された最適な虹彩画像の自動撮影が可能となっている。なお、全自動型では広角カメラによって顔の画像を取得し、その顔画像から目の位置を判断して狭角カメラによって虹彩周辺部を含めた目の画像を撮影する。

また、手動型よりも撮影時の煩雑さが軽減され、全自動型よりも小型化・低コスト化された中間的な位置づけとして半自動型の製品も存在している。

（2）特徴抽出（コード化）と照合・判定

上記で得られた目の画像に対して、画像のコントラストを計測することで虹彩部分の境界を特定して、虹彩部分の画像を抽出する。なお、この時、反射光などのノイズの除去やサイズ補正等の画像処理も実施される。そして最終的に最適化された虹彩画像を 8 つの同心環状の解析領域に分けて極座標変換し、各領域の座標と輝度を特徴としてコード化する。

次に、同様の方法でコード化・登録されていた虹彩コードと比較することで照合判定を行う。2 つのコードの比較は、正規化されたハミング距離（HD: Hamming Distance）で判断される。HD は完全に一致している場合は 0、不一致の場合は 1 となり、統計的に本人であればほぼ 0.1 で完全他人はほぼ 0.5 となることから、要件によって閾値となる HD を設定してその値を越えていれば他人、越えていなければ本人と判定される。

３．４　応用分野・応用事例

（1）ゲート管理システム

固定型の虹彩照合機を用いた虹彩認証システムの利用事例として、コンピュータ室、ネットワーク管理室、空港の出入国管理、学校夜間入口、貴重品倉庫、薬品庫等への入退室時の管理など、比較的高度なセキュリティ確保を要求される場所へのゲート管理システムの利用があげられる。

具体的には、マシン室及びサーバ室への入室管理を行うシステムの具体例を下図に示す。この例では、管理室において事前に登録作業等を実施し、入室管理の対象となるマシン室は入退室（ゲートの入と出）の管理、サーバ室は入室のみの管理で運用している。また、これらの機器は、LAN でネットワーク接続され、管理装置内の登録情報の参照や各照合機でのログ情報の収集等が行われている。

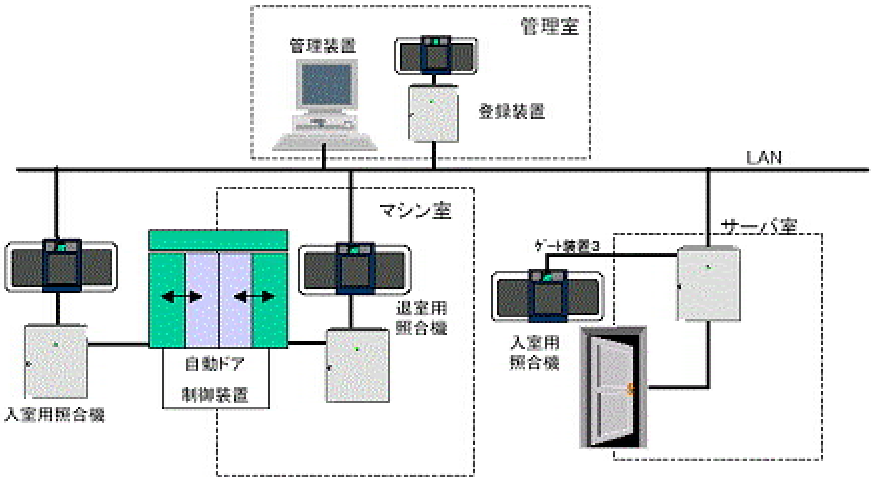


図 3.1 ゲート管理におけるシステム構成

・著者名：沖電気工業株式会社 羽鹿 健 著
・表題：バイオメトリクス認証技術と導入事例
・関連箇所：pp.38「3.2 国内導入事例国内導入事例　－ｺﾝﾋﾟｭｰﾀﾙｰﾑ入室管理－」
・掲載年月日 2004 年 7 月、江崎 浩 掲載、東京大学 電子情報学特論 I －2004 年夏学期－
・検索日：2005 年 1 月 16 日
・アドレス：http://hiroshi1.hongo.wide.ad.jp/hiroshi/files/toku1/Oki_Hajika.pdf

（2）情報セキュリティシステム

比較的安価な虹彩照合機を用いた虹彩認証システムの利用事例として、PC 等の端末のログイン認証、イントラネット内の Web アクセス認証、アプリケーション起動時認証といった情報セキュリティシステムへの適用があげられる。

例えば、特定 Web ページのログイン制御を行うシステムの場合、一般公開前の閲覧に使用するために、イントラネット内 Web サーバの特定ページアクセス時にアイリス認証を行い、登録者のみがその対象 Web ページを閲覧できるようになっている。

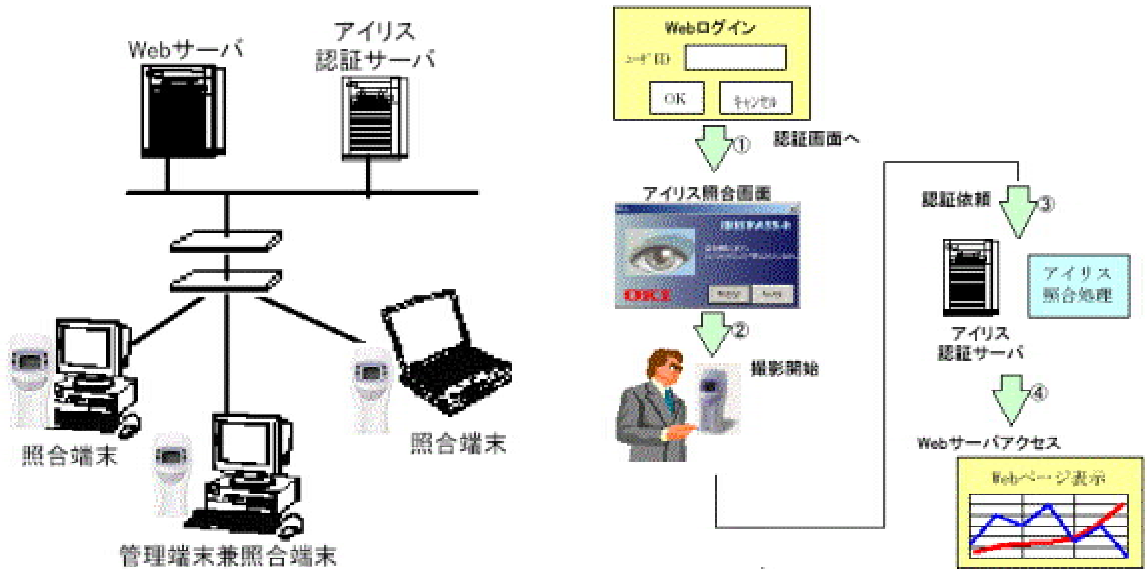


図 3.2 Web ページのログイン管理におけるシステム構成

・著者名：沖電気工業株式会社 羽鹿 健 著
・表　題：バイオメトリクス認証技術と導入事例
・関連箇所：pp.39「3.2 国内導入事例国内導入事例　－Webﾍﾟｰｼﾞﾛｸﾞｲﾝ管理－」
・掲載年月日 2004 年 7 月、江崎 浩 掲載、東京大学 電子情報学特論 I －2004 年夏学期－
・検索日：2005 年 1 月 16 日
・アドレス：http://hiroshi1.hongo.wide.ad.jp/hiroshi/files/toku1/Oki_Hajika.pdf

３．５　技術・システム上の課題

（1）原理的な課題

原理的な課題としては、高精度化や高速化といった普遍的な要求への技術対応が挙げられる。最近では、撮影処理の高度化やノイズ除去等の画像処理などの技術向上によって、高精度な画像を取得す

ることができるようになったため、ハード・コンタクレンズや眼鏡を装着したまま照合することは可能となっている。しかし、現状でも登録時には外すことが求められている。利便性の向上のためには、ハード・コンタクレンズや眼鏡を装着したまま登録可能とすることが望まれている。

この他にも比較的細い眼の利用者の場合、必要な虹彩画像が得られないといった問題も指摘されている。この対応として、従来よりも大幅に少ない虹彩画像情報量でも十分な精度をもった画像照合を実現する技術の実現が求められている。

また、認証失敗時の救済技術の開発なども原理的な課題と言える。現状では、沖電気工業（株）の「アイリスパス-WG」や松下電器産業（株）の「BM-ET500」といった比較的高機能な虹彩認証システムにおいては、本人ではないと判定された場合、自動的に未判定である側の眼の虹彩データによる認証を実施することで、本人拒否率の抑制を実現しているが、低い価格帯の製品などにおいてもその種の利便性を高める技術などが低コストで実装されていくことになると思われる。

（２）直面する課題

直面する課題に関してはモバイル環境への対応やセキュリティ対応などが特筆される。近年、高解像度対応のデジタルカメラ付き携帯電話の普及に伴って、将来的には専用の虹彩照合装置あるいはPC との組み合わせではなく、一般の携帯電話機を虹彩画像の照合並びに必要な通信・情報処理端末として活用する可能性がでてきている。これまでのように専用装置が不要で且つモバイル環境で利用可能となるため、従来では考えられなかった利用シーンが創出されるものと期待されている。しかしながら、携帯機器特有の問題である省電力化や限定された演算能力への対応、操作インタフェースの工夫、虹彩画像撮影時間や煩雑さの改善、屋外等での利用など、取り組むべき技術的な課題は、非常に大きいものと思われる。

特に虹彩画像の取得に関しては、従来のような据え付け型の入退室管理とは比較にならない虹彩画像しか入手できない場合も想定される。比較的精度に問題がある虹彩画像であっても、虹彩認証を可能とする技術の検討が進められており、その一つとして虹彩画像の補完があげられる。これは、取得される虹彩画像に精度的な問題があっても、複数の画像データから良好な画像部分を抽出・合成することで、認証に耐えうる精度を持った虹彩画像データとするものである。

また、セキュリティについては、なりすまし対策などへの対応が求められる。比較的に単純ななりすまし手法としては、任意の対象から撮影した虹彩画像を市販のプリンタで印刷して切り取った偽造虹彩（実際には瞼を含む眼全体）を利用するものがある。これらを用いた登録や照合・判定時に、対象となる虹彩が生体なのかどうかを判定するための方法の一つとして、上下の瞼の動きを観測する手法が利用されている。この他にも、コンタクレンズなどを用いた人工虹彩の場合の対応として、瞳孔の径の変化を観測する手法が利用されている。一般的に瞳孔は照明の変化が起きなくても径が変化するといった「瞳孔動揺」を生じさせている。虹彩照合においては、虹彩画像の撮影・切り出し処理のために、瞳孔の動きを計測する処理が実装されていることから、瞳孔動揺を検知することは可能であり、なりすまし対策の一つとして知られている。

（参考文献）

・「3.アイリス認証システム」、「映像情報メディア学会誌 Vol. 58 No. 6 pp.756～758」、2004 年 6 月 1 日、中村敏男著、映像情報メディア学会発行

・「3.虹彩による本人認証」、「情報処理学会誌 40 巻 11 号 pp.1～4」、1999 年 11 月、塚田光芳著、情報処理学会発行

・「極座標センサーによる虹彩個人認証の提案－新しい虹彩認証センサーの開発とその応用－」、「電子情報通信学会 ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会 第３回研

究報告会予稿集」、2004 年 9 月 13 日発行、伊藤春雄、齋藤邦男、長野雅彦、板倉征男著、電子情報通信学会 ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会発行

・著者名：沖電気工業株式会社 羽鹿 健 著
・表　題：バイオメトリクス認証技術と導入事例
・関連箇所：pp.34～39「3．導入事例」
・掲載年月日 2004 年 7 月、江崎 浩 掲載、東京大学 電子情報学特論 Ⅰ －2004 年夏学期－
・検索日：2005 年 1 月 16 日
・アドレス：http://hiroshi1.hongo.wide.ad.jp/hiroshi/files/toku1/Oki_Hajika.pdf

４．血管パターン照合

血管の模様（血管パターン）は万人不同で、胎児期に形が出来上がると経時的に変化しないなど、多くのバイオメトリクス照合に適した特性を有している。現在、網膜の血管、手の甲やひらの血管、指の血管などのパターンを使った照合技術が開発されている。

４．１　生体情報の特徴・特性

血管パターン（静脈パターン）が個人認証に利用されるようになってきたのは以下のような血管パターンが持つ特性によっている。

（１）右手と左手でも異なる。一卵性双生児間でも異なる。
（２）胎児期に胎内でパターンが定まると、大きさ以外は比較的経年変化がない。
（３）体の中にある情報なので、他の人に知られにくい。
（４）皮下の血管が近赤外光を用いて、無侵襲かつ非接触で撮影できるようになったこと。
（５）血管の特徴が大きくて安定であり、低分解能のイメージセンサーとシンプルな画像処理で認証システムが構築できること。

（１）の個体差がかなりあることや（２）経年的に比較的安定であるといった特性は、血管パターンがバイオメトリクス照合のモーダルとして適している特性であるが、（３）の外部からの不可視性（網膜については難視性）は血管パターン特有の特性であり、体の外からの攻撃（盗み見、変形）を受けにくく、偽造や成りすましを困難にしている。また、（４）無侵襲非接触性といった特性は広い適用分野を実現するものであり、（５）システムをシンプルにしやすいことなどの特性は、個人照合システムを低価格にすることを可能にする。

これらにより、血管パターン照合は、高精度認証、偽造困難、高速応答、低コスト、衛生的、抵抗感小など、バイオメトリクス認証の要件を数多く満たす利点が得られている。

バイオメトリクス照合技術には従来技術として指紋認証技術があるが、血管パターン認証技術では読み取りセンサを非接触式にすることが可能であるために汚れに強く、指紋認証技術の欠点とされているセンサの汚れ等による認識率の低下はほとんどないが、センサへの指や手のひら、手の甲の置き方により認識率が多く低下する問題がある。

４．２　技術開発の歴史

血管パターンを使ったバイオメトリクス照合システムは、指紋照合技術などに比べると比較的新しい技術であり、まず網膜の血管パターン利用から始まった。

網膜の血管パターンを使った認証システムは、米国の Eydentify, Inc.（アイデンティファイ社）が 1985 年に開発し、刑務所の入退室管理などに使われてきた。

手や指の血管については網膜より 10 年ほど遅れて 90 年代半ば以降、研究が開始されている。

手の甲は英国 BTG で研究開発されたのが発端で、その後、韓国の明知大学電機情報制御工学部映像処理研究室の崔　煥洙教授が指揮する研究チームが、1995 年 8 月から産学協同研究の一環として、手の甲の静脈パターン認証に関するアルゴリズムの研究開発を実施し、人間の手の甲の静脈パターン認証技術の製品化に成功した。

日立製作所も医療用技術として開発した光トポグラフィー技術をベースに、1997 年より指の血管パターンを使った認証システムの開発に取り組み、2000 年に指静脈パターンによる個人認証技術を発表した。2004 年にはそれをさらに改良し、側面から光を照射する開放型の指静脈認証技術を開発している。

手のひらの血管パターンについては、2002 年に富士通が接触型の手のひら静脈認証技術を開発、2003 年には非接触型の手のひら静脈認証技術の開発に成功している。

４．３　照合技術の基本的な仕組み・原理

（１）血管画像撮影の原理

光は生体を透過しにくいとされていたが、人体に様々な波長の光を当ててその透過状況を調べてみると、波長 700～1200nm の近赤外領域は部分的に透過度が高く、「生体における光の窓」となっている。この波長域の光はヘモグロビン、メラニンなどの色素以外の生体組織を良く透過する特性がある。

血管パターン照合では、比較的人体を透過しやすい近赤外光を使い、それが血中のヘモグロビンに選択的に吸収される特性を利用して血管のパターン情報を入手する。

またヘモグロビンについては動脈中の酸化ヘモグロビンと静脈中の還元ヘモグロビンがあるが、特に還元ヘモグロビンは約 760nm の波長近辺の光を良く吸収するため、血管パターン照合では静脈のパターンを使っている。例えば、手のひらに約 760nm の波長の近赤外光をあてると、静脈が存在する部分だけ、光が吸収され反射が少なく、映像上、暗く映し出されることになる。
ます。

静脈認証システムで実用化されているイメージング方法には２つの方式があり、手の甲や手のひらの静脈パターンの撮影には反射光方式が、指の静脈パターン撮影には透過光方式が採用されている。

（２）特徴抽出と照合

上記の原理に基づいて CCD 等で得られた画像に対して、画像処理を施して血管パターンを抽出し、静脈パターンとして登録・照合するのであるが、本人かどうかを静脈パターンで識別する具体的な方法には、次の二つの方法がある。

ａ．認証する対象人物の静脈パターン登録画像と直接整合する画像照合方式

ｂ．静脈パターンの分岐特性などを利用する特徴量方式

ａ.の画像の直接比較方式を採用しているのは手のひらや指の血管パターン照合である。ここでは、入力画像を画像処理し血管部分を取り出した上で細線化し、この画像を既に登録してある画像（テンプレート情報）と直接照合している。

ｂ．の血管の分岐特性を利用してた特徴量方式を採用しているのは手の甲の血管パターン照合などである。血管の分岐特性を利用する方法では、手の甲の画像処理過程を通じて静脈部分を細線化した後、分岐点から次の分岐点、分岐点から最後点までの線をたどり、分岐点の座標、長さ、分岐点と分岐点の間の分岐角度などを分析・抽出して識別する。分岐点成分は個人的な差があるが、約 6～15 個分布している。線の長さは分岐点から分岐点まで、分岐点から最後点までの直線距離とし、分岐点あたり３つの線を持っているため、３つの分岐角を持っている。これらのデータを情報として取り込み、蓄積してある情報と比較する。分岐点における位置、方向などの特徴量を用いる点は指紋認証におけるマニューシャ方式に類似している。

網膜の血管パターンも、②の特徴量方式であり、網膜上に近赤外線で円を描き、その円周と血管の交差点の位置を情報として抽出し、蓄積している情報と比較する。

４．４　応用分野・応用事例

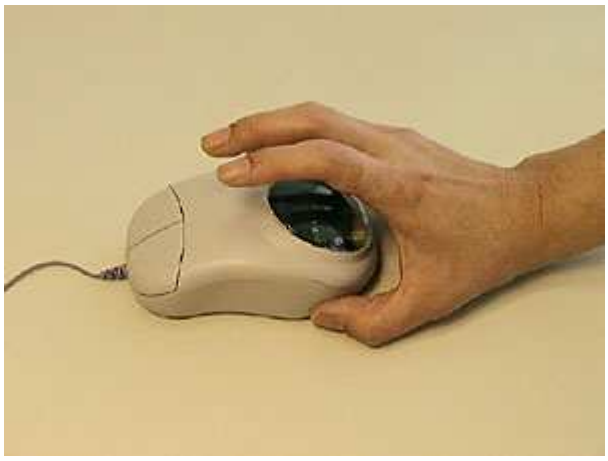
（１）入退室管理

建物やオフィスへの入退室管理に指紋や網膜と同じように血管パターンが使われている。ドアに取り付けられた認証装置のテンキーから ID 番号を入力し、装置に手や指を挿入して静脈パターンを撮影することで登録データとの照合を行っている。

（２）コンピュータの制御

コンピュータのログインや、データ処理を行う際のユーザ認証として血管パターンが利用されている。パソコンに接続された撮像装置に指を置いて血管パターンを撮影するものや、撮像部や認証システムを内蔵したマウスにより手のひらの静脈パターンで認証を行うものなどがある。また、認証にあたってはアクセス開始の際に１回のみ行うものや、データ処理を行っている間中、一定間隔で認証を繰り返すものなどがある。

図　マウス内蔵型血管パターン認証装置



＜引用情報＞

・著者の氏名：株式会社富士通研究所

・表題：PRESS RELEASE「手のひらで高精度に個人を識別するマウス型認証装置を開発」

・掲載年月日（2002 年 8 月 28 日)、掲載者（株式会社富士通研究所）

・検索日：2005 年 2 月 14 日

・情報源及びアドレス：(http://pr.fujitsu.com/jp/news/2002/08/28.html

（３）重要顧客の個人認証

重要顧客に対するサービスへのアクセスコントロールとして静脈パターンを利用している事例がある。東京三菱銀行では平成 16 年 10 月より、重要顧客に対するサービスとして ATM で手のひらの血管認証を行っている。

４．５　技術・システム上の課題

センサの位置決めが大変で、手や指の画像を撮影するたびに、手や指の位置や方向が微妙に変化する。こうした画像を、画像処理技術によって補正処理を行うと計算量が増え、一般的なプロセッサでは処理に時間がかかるといった課題が発生する。その他、近赤外線を使うために太陽光に弱い（ノイズとなる）ことや、医学的には血管パターンが個人個人異なるか、一生変わらないかという問題の証明がされていないことが課題としてあげられる。

（参考文献）

・「線追跡の反復試行に基づく指静脈パターンの抽出と個人認証への応用」、「電子情報通信学会論文誌 D－Ⅱ　J86-D-Ⅱ巻　5 号」、2003 年 5 月 1 日、三浦直人・長坂晃朗・宮武孝文著、社団法人電子情報通信学会発行、678-687 頁

・「静脈パターンを用いた個人認証」、「光学，33 巻 8 号」、2004 年 8 月、宮武孝文著、社団法人応用

物理学会　日本光学会発行、467-471 頁
・「バイオメトリクス認証技術」、「FUJITSU　54 巻 4 号」、2003 年.7 月 10 日、森雅博・新崎卓・佐々木繁著、富士通株式会社発行、272-279 頁
・「これでわかったバイオメトリクス」、2001 年 9 月 10 日、日本自動認識システム協会編、株式会社オーム社発行、54-58 頁

５．　サイン照合

筆記行為という、人間の行動特性を照合対象とするバイオメトリクス技術の 1 つである。筆跡には個人の特徴が多く含まれているため、目視による照合は、犯罪捜査や遺言書の鑑定などで古くから行なわれている。近年では小切手やクレジットカードなどの照合に機械による自動化が求められているため、行動特性を用いるバイオメトリクス技術の中では、最も研究が進んでいる。

５．１　生体情報の特徴・特性

筆記行為は指や腕などの多数の筋肉を用いる人間特有の活動であり、幼少時から訓練を開始して筋肉の活動パターンを定着させるため、その結果としての筆跡には、変動の少ない個人の行動特性という生体情報が多く含まれている。サイン(署名)は本人であることの証明として古くから用いられ、現在でも欧米では日常生活にありふれた行動であるため、バイオメトリクス技術の中では最も違和感が少ないといわれている。

指紋や虹彩といった生体に固着した生涯不変な特徴は、生涯不変であるがゆえに、一度パターンを盗まれると交換ができないという重大な問題がある。それに対して署名は、いくらでも交換(変更)できることが最大の特長である。

但し、本人の署名であっても、その時の体調や精神状態、筆記具の感触などにより変動が生じることや、長期的な変動が避け難いことが、本人と他人との識別を難しくしている。また、署名は本来紙に書いて他人に見せるためのものであること､電子機器の発達により複写が容易になったことに加え、日常的な行為であるが故に、署名行為自体を目撃され他人に真似されやすいという問題がある。

５．２　技術開発の歴史

署名の自動照合は、コンピュータの開発当初から試みられていた。当時は適当な入力装置がなかったため、文字パターンを手作業でコード化して入力していた。スキャナーが登場してからは、紙に書かれた文字はスキャナーで読み込むことが一般的となっている。このような、既に書かれた静的な文字を読み込む方式は、オフライン方式と呼ばれる。現在でも、小切手などの署名照合を目的として研究が行なわれている。

一方、署名を描いている動作をそのまま取り込むこともなされている。80 年代には、ペン内に圧力センサや加速度センサなどを組み込んだ電子ペンの研究が盛んになった。近年では電子手帳や PDA などの発達に伴いペンタブレットの利用が容易となり、これを入力装置とすることが一般的となっている。このように動的に筆記動作を取り込む方式は、オンライン方式と呼ばれる。

照合･判定技術としては､古典的にはパターン認識の一種として､クラスタ化やユークリッド距離、擬似マハラノビス距離などが用いられていた。署名と同様に人間の行動特性を比較する音声認識の影響を強く受けており、80 年代には DP マッチングが、90 年代には HMM が導入され、オンライン方式ではこの 2 つの技術を用いることが、現在の主流となっている。

５．３　照合技術の基本的な仕組み・原理

読み込んだ署名から個人性を表わす特徴量を測定し、登録された参照署名やモデルと比較した時の距離や尤度が、閾値より大きいか小さいかで真筆／偽筆を判定するのが基本である。個人性を表わす特徴は、全体的(global)特徴と局所的(local)特徴に大別できる。全体的特徴には、署名全体の長さや筆記時間、縦横比、スラント(斜め文字)角度、筆記速度の平均値や最大・最小値との差などがある。局所的特徴としては、ストロークごとの向きや曲率、局所的パターンなどがある。これら複数の特徴を

組み合わせて判定することが一般的であるが、近年では全体的特徴のみが比較されることはほとんどなく、局所的特徴の方が重視されている。

オンライン方式では、筆跡をサンプリングしたときのペン先の座標や筆圧、ペン傾度などを時間の関数として読み込み、それらの時間変化パターンを参照署名と比較することが多い。最近では音声認識で成功した手法が取り入れられ、DP マッチングによって入力署名と参照署名との時間的なずれを補正することや、参照署名を隠れマルコフモデル(Hidden Markov Model：HMM)によって状態間の遷移確率分布にモデル化し、入力署名を尤度検定することが主流となっている。

５．４　応用分野・応用事例

オフライン方式は、小切手などの有価証券類への応用が期待されている。但し現状では信頼に足る認識率が得られていないため、目視による判断の補助としての位置づけに止まっている。

オンライン方式では、パソコンや PDA などのログイン認証用に導入が始まっている。PDA やタブレット PC には元々文字入力用のペンタブレットがついており、親和性が高い。またノート PC に搭載されていることの多い、静電容量式ポインティングデバイス(タッチパッド)を指でなぞってサインを入力する方式も考案されている。

機密管理が必要な部屋などの入退場管理の他、工事現場での本人確認にも使用されている。工事現場では本人が入場したか否かの精度の高い労務管理が実現でき、血液型や資格などのデータベースと連携して、不測の事態に備えることもできる。更にカードやバーコードなどを用意する必要がないため、短期間の現場入場者にも柔軟に対応できる。

社内ビジネス文書の認証手段として、グループウェアへの組み込みソフトが、複数のシステムインテグレータから出荷されている。これを用いると、例えば電子ドキュメントの認証に、従来の紙書類と同様の感覚で署名を書き込むことができる。

５．５　技術・システム上の課題

サイン照合は、指紋や虹彩といった他のモーダルに比べて、認識誤り率が数桁高い。この原因は、行動特性という動的な特徴は、指紋などの静的な特徴に比べて個人内の変動が大きいためであるが、変動をもたらす要因として、次のようなものがあると思われる。

署名は弾道的(ballistic)、つまりやりっ放しの行為だといわれているが、同じ形の署名を描こうとすると、フィードバックをかけざるをえない。そのため入力に違和感があると、通常通りに描けないばかりか、毎回違う形になりかねない。ペン入力タブレットは通常厚みがあり、電子ペンには配線という余計なものがついているものもあり、どうしても違和感が生じる。また視覚からのフィードバックも重要であり、フィードバックがなければ署名ごとの変動が大きくなる。フィードバックが遅れれば形が崩れる。従って、できるだけ自然な状態で署名を入力できるインターフェースが望まれる。

また、今後はネットワーク上での応用が期待されるが、サイン入力デバイスが異なればサンプリング周波数やデータの形式などが異なり、同一のテンプレートが使用できない恐れがある。インターフェース間の仕様の統一が望まれる。

(参考文献)

・「書字による個人識別の技術」、「システム/制御/情報　Vol. 35　No.7　pp.398-407」、1991 年 7 月発行、田口英郎著、システム制御情報学会発行

・「導入の進む動的署名照合システム」、「情報処理　第 40 巻　11 号　pp.1-4」、1999 年 11 月発行、田吹隆明著、情報処理学会発行

・「筆者認識技術の現状」、「札幌学院大学社会情報学部紀要　Vol.9　No.1　pp.43-81」、1999 年 12 月発行、吉村ミツ著、札幌学院大学社会情報学部発行

６．顔照合

人が他人を識別する基本的な方法は相手の顔を見ることである。顔情報を使ったバイオメトリクス照合は人間にとって非常に親しみのある技術であるが、コンピュータを使ってこれを自動的に行おうとすると、顔の向きや、眼鏡や化粧、経年変化など難しい課題に直面する。

６．１　生体情報の特徴・特性

（１）長所

ａ．顔を見て誰であるかを判断することは、普段から人と人の間で自然に行われている認証方法である。指紋などと比べても心理的抵抗が少なく、親しみやすい個人認証といえる。

ｂ．撮影条件により認識率が落ちるという課題もあるが、センサに接触するのではなく、カメラによって撮影された画像を使うことから距離が離れていても認識することができる。

ｃ．ユーザーが何も身につけることなく、かつ能動的に意識して認識されるように行動しなくても認証できる。

ｄ．顔照合のため、顔画像や映像が記録される、または記録されるかもしれないということから、不正に対する心理的抑止効果がある。

ｅ．同じカメラを使って、顔認証以外の認識を兼用して行うことができる。（視線認識など）

（２）短所

ａ．双子などの厳密な識別は困難

ｂ．カメラから入力した画像の画像処理を行うため、照明変化・顔の向き・表情変化・サングラスやマスク・経年変化に弱いという短所がある

ｃ．公共の場では、プライバシーの保護が問題になる可能性がある。

６．２　技術開発の歴史

顔認証技術の歴史は、1973 年に金出武雄教授が京大で行った研究 “Picture processing by computer complex and recognition of human faces”から始まった。デジタル画像処理技術の進歩とともに進展し、93 年には米国陸軍研究所が中心となって行った FERET（FacE Recognition Technology）と呼ばれる顔認証アルゴリズム・コンテストによって共通の評価データベース基盤を持ったことにより、急速にアルゴリズムが発達した。97 年頃から、Visionics、Miros、Viisage などのメーカーが商品を市場に投入してきている。

６．３　照合技術の基本的な仕組み・原理

（１）処理の流れ

ａ．顔画像の入力

カメラ位置、証明条件などを最適にした上で正面顔画像を撮影する。

ｂ．顔領域の抽出

入力画像の中から顔領域を抽出する。一般的には入力画像のどの部分に顔が存在するかは未知であり、画面内に一人しか写っていない場合と、背景あるいは複数の人物が写っている場合とがあり。この場合、認証対象の顔を検出することが重要である。また、動画像をあつかう場合には、テレビカメラと人物との相対的な位置関係の変化に対応して、人物の顔部分の追跡を行う必要がある。

ｃ．顔領域の切り出しと正規化処理

顔領域の検出結果に基づき、入力画像から顔領域の切り出しを行う。切り出された顔画像においては、一般に顔領域の大きさ、傾き、輝度にばらつきが存在する。ばらつきを補正するために正規化処理を行う。カメラと人物との相対的な位置関係などの撮影条件が既知でない場合には、入力画像から取り出した顔特徴（瞳の位置など）を用いて正規化処理を行う。

d．顔特徴の抽出

切り出された顔領域に対して、その顔の特徴を表現するような特徴量を抽出する。抽出した特徴量を用いて切り出した顔領域が適切であるか否かを判定する。適切でない場合は再度切り出し処理を行う。

また、顔特徴量としては、目、鼻などの形状、それらの相対的位置関係などの「幾何学的特徴」と、顔表面の色や濃淡分布などの「パターン分布特徴」の２種類がある。特徴量に応じて複数の認証アルゴリズムがある。

e．照合処理

抽出した顔特徴をデータベースに蓄えられた顔特徴と照合する。入力顔画像の顔特徴とあらかじめデータベースに蓄えられている顔特徴との一致を調べることを認証という。一方、入力画像の顔特徴と最も類似した顔特徴を有する顔画像をデータベースの中から探索することを識別という。

（２）顔照合アルゴリズム

顔特徴としては、顔の幾何学的構造を表現する幾何学的特徴（構造特徴）と、色や濃淡の分布特徴（パターン特徴）が代表的である。前者では、顔の形状や構造を表現する特徴的な点（目尻、口の両端、あごの先の位置など）や輪郭線を抽出し、特徴点間の距離や角度、輪郭線の曲率などを取り出す。一方、後者では色や濃淡の分布パターンを用いる。ただし、色や濃淡の分布そのものではなく、固有空間に変換した特徴を用いる方法が主流である。

６．４　応用分野・応用事例

（１）入退室管理システム

アクセスコントロールの基本として、ビルやオフィスなどへの入退室管理に顔照合技術が使われている。入り口のドアホンなどに顔を見せてドアの解錠を行うというもので、ドアホンの撮像ボタンを押すだけで、登録している人であればドアが開く Identify 型と、ID カードまたはテンキーによる番号入力で、特定の人だけの入室を認める Verify 型がある。

（２）特定個人の抽出システム

街中や建物内に設置されたカメラが捉えた画像の中から、特定の人物を抽出するもので、多くの人が写る画像の中から人の顔を切りだし、探している人物の顔データと照合を行う。施設の出口にカメラを設置して、徘徊老人が施設から出ようとするのを検出したり、ロンドンのニューハム地区の防犯システムの事例のように、300 台のカメラを使って通行人の中から顔照合で登録してある犯罪者を抽出するシステムなどがある。

６．５　技術・システム上の課題

現状では高い認識率を保つためには、一定の良好な照明環境下と、ほぼ正面を向いた顔という制約がある。今後、さまざまな実環境下で様々なアプリケーションに対して実用化していくためには、次のような課題がある。

（１）耐照明環境性：屋内外など多様な照明環境への対応や照明の方向性への対応。

（２）顔の向きへの対応：上下、左右、傾きなどさまざまな顔の向きへの対応。

（３）眼鏡等への対応：眼鏡の有無・種類の変化やレンズの反射への対応
（４）表情変化への対応：少々の表情変化や口・目の開閉等への対応。
（５）化粧、髭、眉・頬にかかる髪等の変化への対応。
（６）なりすまし防止：写真やディスプレイなど偽造へのより高度な対応（現在、顔器官の動き検出やステレオ画像による立体視などにより対応）

（参考文献）

・「これでわかったバイオメトリクス」、2001 年 9 月 10 日、日本自動認識システム協会編、株式会社オーム社発行、59-71 頁
・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、49-58 頁

７．　音声照合

音声による個人照合は、特殊なセンサなどを必要とせず、ありふれたマイクの使用が可能であるため、ユーザの負担は心理的にも経済的にも小さく導入できる。そのため、あまり高セキュリティを必要としない情況での手軽な個人認証手段として、またセキュリティを少しでも高めたい場合の補助手段として、その需要はますます高まると考えられる。

７．１　生体情報の特徴・特性

音声は次のようにして生成される。肺から押し出された空気が気管を通り、喉頭にある声帯の間を通るとき、声帯との相互作用により空気流に振動が生じ、これが音声の音源となる。この音源の周波数を基本周波数といい、声の高さ(ピッチ)に対応する。声帯の緊張が大きく肺からの空気圧が高いと基本周波数が高くなり、声が高くなる。逆のときは低くなる。この音源に対して、顎、舌、口唇といった調音器官を動かすと音の伝達特性が変わり、共鳴作用によって周波数的にエネルギーの強弱が生じて、音色が付与される。

こうした、肺から口唇に至る声道の大きさや形、弾性特性、更にこれらの動かし方は人により様々であるため、音声には多くの個人的特徴が含まれる。具体的には、次のような特性に個人性がよく表れていると考えられている。

・声帯音源の特性および基本周波数(ピッチ)の平均的特性
・調音器官の形状に依存する短時間スペクトルの包絡形状
・調音器官の運動制御に依存するスペクトルの動的特性

この中でピッチパターンは、電話など伝送系の影響がある場合は有力な特徴量であるが、他人に真似されやすいため、音声照合には向いていない。スペクトル包絡は声道の共振特性を表わし、他人には真似できないため、個人の識別に最も適している。現在では、このスペクトル包絡の時系列を基に、個人の照合が行なわれている。

７．２　技術開発の歴史

音声を個人の特定に用いることは犯罪捜査においてモチベーションが高く、古くは 1660 年の裁判で、初めて音声が手掛かりにされたといわれている。音声の個人性が初めて科学的に検討されたのは、1937 年のことである。1945 年に「声紋」(サウンドスペクトログラム)を描く技術が発明され、1962 年に、これによる話者認識の可能性が発表された。このときは人が声紋を見て判断していたが、客観性に乏しいため、その後自動的な話者認識方法が盛んに研究されるようになった。

計算機の能力が低かった時代には、音声のモデル化には長時間統計量や線形予測分析が用いられていた。比較・照合技術としては、1970年代には板倉の線形予測分析における距離尺度、および千葉・迫江のＤＰマッチングの両技術で、日本が世界をリードしていた。またスペクトル中の優勢な周波数成分(フォルマント)を抽出して比較することもなされていたが、その後スペクトル全体をケプストラムで表現することが主流となり、ケプストラム間のユークリッド距離や種々の重み付けした距離を測定する方法が研究された。現在ではケプストラム係数から隠れマルコフモデル(HMM)や混合ガウス分布モデル(GMM)を立て、入力音声のモデルに対する尤度で話者を判定することが主流である。

話者認識方式としては、発声内容が決められているテキスト依存方式と、発声内容に依存しないテキスト独立方式とがある。テキスト独立方式では、1988年にベクトル量子化(VQ)を用いて話者をモデル化する方式が発表され、1995年にGMMが発表されるまでは、テキスト独立方式の主流であった。また1996年に松井・古井により、システムの側から発声内容を指定するテキスト指定方式も発表されている。

７．３　照合技術の基本的な仕組み・原理

音声波は、先ず 10msec 程度の細かい時間ごとにスペクトルに変換される(音声分析)。スペクトルは、対数スペクトルを逆フーリエ変換して時系列化したケプストラムパラメータを用いて、滑らかに表現される。そのパラメータの時系列を話者ごとにそのまま登録するか、話者の特徴を表現するパラメータに変換し(特徴抽出)、それに基づいて各話者のモデルを作成して登録する(学習)。モデル作成の技術として、ベクトル量子化 (VQ)や隠れマルコフモデル(HMM)、混合ガウス分布モデル(GMM)などがある。HMM は統計理論に基づく方法であり、最近の音声認識で最も広く用いられている。音声は同じ人でも時期的な変動があるため、あらかじめ話者ごとの変動の幅を調べておき、その人の典型的なモデルを作成すると共に、許容限界の閾値を調べておく。入力音声も同様に特徴を抽出し、登録されたモデルに対する尤度で、話者を判定する。

７．４　応用分野・応用事例

現在までに最も成功しているのは、更生産業での利用である。T-NETIX 社は、米国の刑務所など 1400 以上の更生施設に電話監視システムを導入し､決められた相手以外と電話で会話をしていないか､話者照合技術を用いてチェックしている。また仮釈放中の人が、夜間に自宅など決められた場所にいることを確認するシステムも、T-NETIX 社、Persay 社、BI 社により開発・導入されている。

複数の調査によれば、ネットサービスのヘルプデスクで最も時間が費やされるのは、ユーザのパスワード忘れや盗難によるパスワード再発行であり、1 ユーザあたり年間 300 ドルもの費用が掛かっている。このパスワードリセット業務を、話者照合技術により自動的に実施するシステムが販売され、利用が進んでいる。多くのシステムではテキスト指定型の技術を用いており、ユーザのパスワード忘れに対応できる。また個々の機器に照合用の装置を追加する必要がないため、導入側のメリットも大きい。

今後期待されるサービスとして、第三者による内容確認サービスがある。これは、電話による契約変更のやり取りを第三者に確認させるもので、一部では本人確認に話者照合技術の導入が始まっている。最近はテレマーケティング全般で同サービスの利用が広まりつつある。

７．５　技術・システム上の課題

話者照合では、特徴量として 10～20 次のケプストラム係数が用いられることが多い。しかし話者情報は、スペクトルの微細構造に含まれる韻律情報や長時間の情報にも存在する。観測点や周期が必ずしも一致しない情報や、無声区間では観測できない情報の処理はチャレンジングな課題である。限られた量のデータからいかに頑健に韻律情報を取り出すかは、今後の課題である。

現在用いられている特徴量は、加齢など時間の経過により変化が生じるため、多くのシステムでは照合時の音声を用いて話者モデルを更新する。従来、閾値の頑健性が問題となっていたが、照合スコアの正規化により、他人受容率を一定以下に抑えることは容易となった。一方で、風邪をひいたり、酒を飲んだ後、朝と晩との声の質の違いなど、本人拒否率に関する閾値の頑健性の検討は不十分である。こうした変動に対していかに頑健にするかも、今後の課題である。

発声器官が似ている親子・兄弟、特に一卵性双生児については、これまで話者認識は難しいとされてきた。しかし、実際どの程度難しいかの検討例は少ない。話者認識技術の性能限界を明らかにするためにも、先ずは親子・兄弟の音声データベースを整備する必要があると考えられる。

(参考文献)

・「音声と筆跡による個人識別技術」、「情報処理　Vol.25　No.6　pp.592-598」、1984 年 6 月発行、

白井克彦著、情報処理学会発行
・「音声による本人認証のしくみと技術動向」、「情報処理　第 40 巻　11 号　pp.1-4」、1999 年 11 月発行、古井貞熙著、情報処理学会発行
・「音声情報処理」、「電子情報通信工学シリーズ」、1998 年 6 月 30 日発行、古井貞熙著、森北出版株式会社発行
・「音声による個人認証技術の現状と展望」、「電子情報通信学会誌　Vol.87　No.4　pp.314-321」、2004 年 4 月発行、松井知子　黒岩眞吾著、社団法人電子情報通信学会発行

８．その他の照合技術

８．１　ＤＮＡ

人間の DNA は人体の設計図ともいわれており、人がそれぞれ少しずつ違うように DNA の塩基配列も人によって異なっている部分がある。また、DNA は終生不変という性質を持っていることから、DNA の情報を使って個人照合を行うことができる。

DNA パターン認証は、1983 年に初めてイギリスにおいて使用された。指紋や虹彩のように人の体のある部分にしか存在しないものとは異なり、DNA は身体のすべての細胞もしくは組織について同じであり、採取可能な領域は多いという特長も持っている。

塩基配列とは、A（アミン）、G（グアニン）、C（シトシン）、および T（チミン）の 4 種類の塩基の列のことで、人間の DNA 場合約 30 億個の塩基配列からなっており、二重化されて細胞核に畳み込まれている。人体は 50～60 兆の細胞でできあがっているが、どの細胞を取り出しても DNA の塩基配列は同じである。

（１）DNA バイオメトリクス認証の特徴

１）識別精度が高い

指紋のようなバイオメトリック照合方式に比べて DNA 情報を ID とした場合、現状の抽出技術によっても桁違いに高い識別精度を達成できる。

２）照合アルゴリズムが不要

DNA 情報から ID を生成するアルゴリズムによって ID は一意に定まるので、照合は一意に決まったデジタル情報同士の直接的な比較により行えばよいことになる。ここで ID の生成アルゴリズムというのは、他のバイオメトリック技術のように、統計的もしくは画像処理のようなベンダー独自のノウハウを要するものではなく、DNA の塩基配列のどこを見るかという定義をするだけのシンプルなものである。他のバイオメトリクスのように特徴点抽出やパターンマッチングによる難しい照合アルゴリズムを特に必要としない。

（２）DNA 照合の仕組み

ヒトゲノム（DNA の全塩基配列）は、人体の構造や疾病等に関する情報を持つ「遺伝子領域」と、そうした情報を持たない「遺伝子外領域」から構成されている。DNA を使った照合では遺伝子外領域の塩基配列を利用する。

遺伝子外領域の情報の中にはサテライトといわれる塩基配列のあるセットが反復繰り返している部分がある。また、STR（Short Tandem Repeat）と呼ばれ、2～4 塩基文字が繰り返し反復したものが存在し、しかもその回数は個人によって違いが見られる。この情報をうまく組み合わせると、個人の識別が可能な DNA 個人 ID となる。

DNA 上にある STR の位置を座位またはローカスといい、ローカスは人間の場合 5000 ヶ所以上あると言われている。ひとつの STR ローカスでは、短い塩基配列の繰り返し回数（アレル数）が２つのペアになっている。一方は父方から、もう一方は母方から引き継いだものである。この二つの数値を小さい順に並べたものをひとつの数値コードとする（例えば 5 と 10 であれば、510 という数値コードとする）。しかし、これだけでは同じ値となる他人はいくらでも出てくるので、STR ローカスを複数定義して、それから得られたアレル数をそのままつなげて数値コードを大きく（長く）していく。STR ローカスを 16 カ所定義したとき、このようにして得られる DNA 個人 ID の同値確率は 10 のマイナス 18 乗程度となる。ローカス座位を追加すればさらに高い精度の識別能力を得ることができる。

（3）用途事例

1）犯罪捜査での利用

犯罪捜査における本人鑑定の作業に DNA が多く用いられるようになっている。犯罪の現場に残された犯人の血液（白血球のような細胞を有していること）、唾液（同）、精液、毛根のついた毛、細胞そのものなどから容易に DNA が抽出できるので、本人との結びつきを判定することができる。一般に本人の DNA の塩基配列は、綿棒で口の中を軽くこすり、綿棒に付着した口腔の粘膜細胞から収集するのが普通である。

2）身元不明人の DNA 鑑定

犯罪捜査以外でも、より正確な本人鑑定に DNA による方法が使われるようになっている。災害の被災者や犯罪被害者などの身元不明人で焼けたりあるいは腐乱したりして外見からの本人鑑定が難しい場合など、遺体から DNA を抽出し、本人鑑定が行われる。照合する相手は両親や兄弟で、1～2 親等における親族の関係は、DNA で確率的に推定できる。

3）DNA 認証マーク

DNA 個人 ID のほかの応用例として、ブランド商品やグッズの真贋識別に利用されている DNA 認証マークがある。この認証マークは、当事者 DNA の一部が溶解された、いわゆる DNA 入りインクを使った特殊印刷が行われており、細胞を盗まれない限り認証マークの複製は困難である。真贋の判定は、マークのインクに溶解されている DNA 断片を解析し、当初の ID が生成できるか否かで行われる。

（4）DNA バイオメトリクス認証の課題

1）生体情報の取得・分析コスト

細胞から DNA を抽出・解析し DNA 個人 ID を生成するための時間とコストが大きい。他のバイオメトリック認証のようにリアルタイム計測をリーズナブルなコストで可能とする端末装置の実用化にはいくつかの大きなブレークスルーが必要である。

2）プライバシー保護

DNA 個人 ID は本人の病因や人体の構造とは無関係な部分の DNA 情報であるが、親子関係が想定できるなどプライバシー情報であることは間違いないので、指紋以上に個人情報としての配慮が必要である。また、他の生体情報と同様に、DNA は毛根付きの毛髪などにより容易に他人の情報を盗むことができる。このため、実際の DNA 個人 ID は、生の ID 情報に個人が管理する秘密乱数を加えるなどして操作したものを使う。

3）一卵性双生児の識別

一卵性双生児のように全く DNA が同じ二人を識別することができない。

8．2　掌形

（1）掌形照合の特徴

古くから掌形（手の形）は個人を識別する手がかりのひとつとして知られてきた。掌形が人それぞれに特有であることが証明されたきっかけは、アメリカの航空宇宙局において、パイロットの用いるグラブ（革手袋）を作製する際に、各パイロットの手の型紙を作成したところ、ほとんど全員の形状がわずかであるが異なったことにある。

掌形照合とは、掌の幾何学的な特徴を測定して個人の照合をすることをいう。幾何学的な特徴の測定とは、掌の大きさと形を測定することで、指の長さ、幅、厚み、4 本の指の表面積が含まれる。この場合、親指は含まれない。

この掌の長さを識別する装置が、バイオメトリクス商品として初めて登場したのは 1976 年であっ

た（Identimat 社）。初期の装置は、大きなコピー機のような形状をしており、各指の影の長さを測定し、磁気カードに記憶させ、単純に比較し照合するだけの装置だった。現在製品化されている技術は掌形をカメラで３次元計測し、掌の幅や長さなど 96 に及ぶ項目測定の結果をもとに行われており、テンプレートサイズは 9 バイトと他の生体認証技術に比べて小さいのが特徴である。

応用分野としては、現在ではアクセスコントロールだけでなく、タイムレコーダーとしても使用されるようになった。

（２）今後の課題

掌形照合では、指紋照合で問題になっている偽造指紋のような偽造掌形を作成することは、本人の協力がなければ極めて困難である。なぜなら、照合時には点灯したガイド用 LED を、ガイドピンを指で挟む行為で消していき、すべての LED が消えなければ掌形照合装置は照合を始めないからである。この LED を消す行為が生体反応にもなっている。

掌形照合は指紋照合に比べて機器がどうしても大きくなる。今後は技術的な問題がクリアできれば、機器のサイズ縮小を目標とし、更に信頼性の高い製品が開発されると思われる。

８．３　耳介

（１）耳介照合の特徴

人間の耳介は集音と増幅機能を持つように複雑に入り組んだ軟骨の凹凸によって形づくられており、それらの複雑なつながり方に個人性および特徴がある。耳の大きさは、長さ、幅とも 16 歳以降は安定期に入り、40 歳前後まで少しずつ成長するが、終生不変とみなし得る範囲といえる。

耳介の形状は、軟骨の隆起および陥没状況、軟骨の張り出し状態、軟骨の輪郭形状、隆起、陥没の状態、軟骨の接続状態および頭部との接続状態などに強い個人性を持っている。また一方、個人性の弱い非個人性を持つ部分があり、この非個人性部分を明確にし、これを基準に、耳介比較（識別）を行うことができる。

（２）今後の課題

耳の形の個人差に関しては欧米および日本で研究報告されている。しかし、親子、兄弟、姉妹、双子などの遺伝的側面からの万人不同性の検証はなお研究が必要である。

（参考文献）

・「DNA バイオメトリックス本人認証方式の提案」、「情報処理学会論文誌　43 巻 8 号」、2002 年 8 月 15 日、板倉征男・長嶋登志夫・辻井重男著、社団法人情報処理学会発行、2394-2404 頁
・「これでわかったバイオメトリクス」、2001 年 9 月 10 日、日本自動認識システム協会編、株式会社オーム社発行、48-53 頁
・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、62-63 頁
・「セキュリティにおける個人識別技術」、「システム／制御／情報　35 巻 7 号」、1991 年 7 月 15 日、増田功著、システム制御情報学会発行、431-439 頁

９．マルチモーダルバイオメトリクス

マルチモーダルバイオメトリック認証技術は、指紋、署名、顔、声紋、虹彩などの複数の生体情報を用いて本人認証を行う技術である。マルチモーダル化の本質はセンサデータを統合することにより、個々のバイオメトリック技術の不完全さを補完し、性能を向上させることにある。

マルチモーダルバイオメトリック認証技術は、各バイオメトリック認証技術の認証照合結果を用いて、総合的に個人の認証あるいは識別を行うもので、一番重要な処理は融合判定処理である。

複数の生体情報を用いるため、単体のバイオメトリック認証に比べ次の効果がある。

（１） 本人拒否率や他人受入率などの精度改善
（２） 識別を目的とした場合の処理時間の改善
（３） 生体情報の偽造対策
（４） 最適な生体情報を選択することによる利便性改善

９．１　複数のバイオメトリックの融合による精度向上

バイオメトリック認証システムの精度を高める方法としては、既存のセンサや照合機能を組み合せることによって、より多くの情報を融合する方法が数多くの提案されている。

これらの方法は、融合する情報の種類により次の 3 つのモデルに分類される。

（１） アンサンブルモデル

同じバイオメトリクスを入力し、複数の異なる照合アルゴリズムを組み合せることで精度の向上を図る。取得された生体情報は複数の照合機能へ渡され、各照合機能が各々特徴量を抽出して照合・判定した結果は融合判定機能に送られ、そこで最終的に受理するか拒否するかを決定する。

同じサンプルから各照合機能はそれぞれ異なる特徴量を抽出して照合するため、より精度を高めると考えられている。

（２） マルチサンプルモデル

一つの生体情報を複数回繰返して取得・照合し、得られた複数の判定結果を総合的に判断して受理するか拒否するかを決定する。同一人の同じ生体情報であっても、サンプリング結果は毎回異なる。例えば指紋でいえばセンサ面の指の置き方や圧力の違いによりサンプリング結果に影響を与える。それ故、同一生体情報を複数回サンプリングし、それらの照合結果を利用することでこのような影響を軽減し、精度を高めると考えられている。

ただ、複数回繰返して生体情報を取得するので、利便性は低くなる。

（３） マルチモーダルモデル

一人の人間が持つ複数の異なる生体情報をそれぞれ独立に取得・照合して得られた複数の照合結果を総合的に判断して受理するか拒否するかを決定する。

一般に異なる生体情報は互いに高い独立性を持っている（顔は似ている人同士でも指紋は全く異なる）と考えられていることから、上記二つのモデルと比べて高い精度を得ることができる可能性がある。

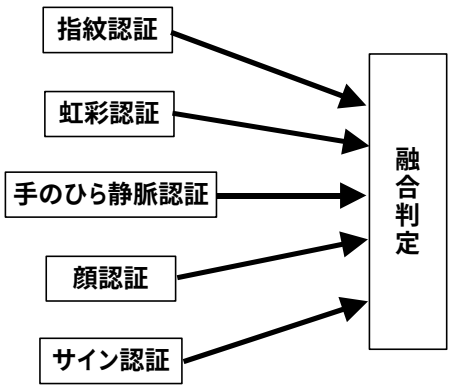
マルチモーダルバイオメトリック認証システムの精度は、個々の照合機能の性能と融合判定の方法に依存し、マルチモーダルバイオメトリック認証システムの研究は主として融合判定方式を対象に活発な研究が行われている。

バイオメトリック認証のマルチモーダル化は、認証に適用する場合と識別に適用する場合の 2 つがある。

９．２　認証のためのマルチモーダル化

マルチモーダルバイオメトリック認証システムは、図 9.1 に示すように一人の人間が持つ複数の異なる生体情報を、それぞれ独立に取得・照合し、得られた複数の照合結果を融合し総合的に判断して受理／拒否を判定するので、一般に複数のセンサと複数の照合機能、および融合判定機能から構成される。一般に異なる生体は高い独立性を有していると考えられることから、マルチモーダル認証の精度は単体のバイオメトリック認証に比べ高くなる。また、マルチモーダル認証は、可用性や受容性を高める可能性がある。つまり、一つの生体情報（例えば指紋）が使えない場合、声など他の最適な生体情報を用いて認証するような運用が考えられる。さらに、複数の生体情報が全て認められて初めて本人と認められるような運用を想定すると、複数のモダリティを同時に偽造することは困難なことから、生体の偽造対策としても使える。

図 9.1 マルチモーダルバイオメトリック認証のイメージ



出典：本標準技術集のために作成

マルチモーダルの融合判定技術は、次の 3 種類に分類される。

（１）　アブストラクトレベル

アブストラクトレベルは、サブシステムは特徴量と生体情報が一致したかを OK あるいは NG などで出力する。そして、複数のサブシステムを単純な AND（論理積）や OR（論理和）で結合して評価・判定する。本人拒否率あるいは他人受入率を選択的に向上する場合に適しており、この判定技術を用いた製品は、既に商品化されている。

（２）　ランクレベル

ランクレベルでは、複数の特徴量と一つの生体情報を照合したとき、生体情報と類似度の高い順番に特徴量を並べたリストを出力する。他の方法と組合せて個人識別に高速化を要するアプリケーションに用いられる。ただ、他の二つの融合判定技術と比べると中途半端な技術であることから、最近では余り研究がなされていない。

（３）　メジャメントレベル

メジャメントレベルでは、サブシステムは類似度の値を出力する。サブシステムが出力した本人分布（本人同士照合時の類似度分布）と他人分布(他人同士照合時の類似度分布)

から、多次元空間における類似度の分布を求め、これらの分布を最も効率よく分離する境界を決定することで、本人拒否率と他人受入率を同時に改善する。

このメジャメントレベルの問題点は 2 つあり、一つは類似度分布の計測に多量のデータが必要であること、もう一つは類似度分布の推定方法が未確立なことであり、研究者の数だけ推定方法があると言われている。現在はまだ研究段階であり、製品化にはいたっていない。

９．３　識別のためのマルチモーダル化

識別を目的としたマルチモーダル化は、識別処理の高速化が可能となる。識別処理では多人数の生態情報をデータベースに格納して入力したデータに対し検索する際、処理速度が速く精度は低いバイオメトリック認証技術と、反対に処理速度は遅いが精度は高いバイオメトリック認証技術とを組み合わせた場合に識別処理速度の改善が可能となる。つまり、最初に高速なバイオメトリック認証技術で候補を抽出し、次に精度の高いバイオメトリック認証技術で最終的に決定するシステムである。

９．４　マルチモーダルの応用例

マルチモーダルバイオメトリック認証技術は、利便性の向上により効果があるといえる。以下に応用例を示す。

（１） バリアフリー本人認証システム

高齢者などのバイオメトリック認証システムとして使い、アブストラクトレベルの OR で融合判定する。具体的な生体情報としては、顔や声紋などの非接触で認証できる生体情報が適当である。

（２） 運転者自動認証システム

ITS(Intelligent Transport System：高速道路交通システム)サービスにおけるドライバ認証に有効なシステムで、走行中に高付加価値サービスを受ける際、ハンドフリー状態で本人認証を行うことが考えられ、走行中のノイズなどの問題があることからマルチモーダルの利用が期待できる。融合判定では、メジャメントレベルやランクレベルが有効と考える。

（参考文献）

・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、80―93 頁

・「バイオメトオリックセキュリティ入門」、2004 年 8 月 25 日、瀬戸洋一著、株式会社ソフト・リサーチ・センター発行、121―129 頁

１０．バイオメトリック認証システム

一般的なパスワード方式による本人認証は、盗み見などによる盗用で安全性の面から必ずしも確実な手段とは言えなくなり、安全に確認できる本人認証の手段として、本人の生体情報を用いて認証するバイオメトリック認証システムが注目されている。このシステムは、生体情報の保管および照合処理をどこで行うかにより、大別してサーバ認証モデルとクライアント認証モデルの二つのモデルがある。また、最近では PKI（公開鍵基盤）を用いた電子認証が本格的に利用され始めたが、PKI による本人確認は本人が秘密鍵を所有していることが前提であることから、秘密鍵の盗用によるなりすましの脅威は否定できない。この問題を解決するために PKI と生体情報を連携した本人認証システムが期待されている。

１０．１　サーバ認証モデル

図 10.1 に示すサーバ認証モデルは、生体情報をサーバで集中管理し、検索エンジンを用いて高速認証するモデルである。登録および認証の概略を示す。

（１） 登録

（ア）センサで入力した生体情報を氏名などの個人情報を付加して認証サーバに転送する。

（イ）認証サーバで正しい者が登録しているかの確認をする与信照会を行う。

（ウ）与信に問題のない場合は、個人情報、ID 情報、特徴量を登録する。

（２） 認証処理

（ア）クライアント端末より ID 情報およびセンサで入力した生体情報を認証サーバに転送する。

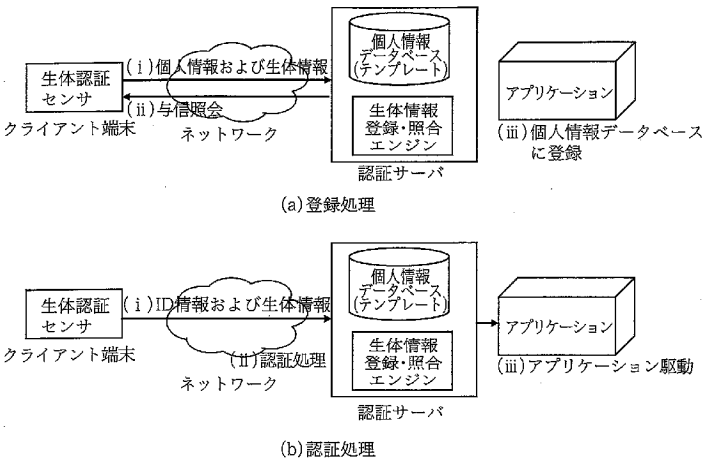
（イ）認証サーバで転送されたデータの認証処理を行う。

（ウ）認証結果が妥当ならアプリケーションを起動する。

このモデルでは、ユーザはセンサで生体情報を抽出するだけでよいためクライアント端末の負荷が少なく経費も安いが、サーバ側では利用数が多くなったときの負荷やネットワーク負荷に注意を払う必要がある。また、個人情報を一括管理するため、その管理体制も重要である。

情報の流れの観点では、クライアント端末と認証サーバ、認証サーバとアプリケーションとの間におけるデータ転送は、機密性や完全性を保つために暗号化やデジタル署名が必要である。特に登録時のなりすましを防ぐ上では、デジタル署名が必須である。このことは、クライアント認証モデルにおけるデータ転送でも同様である。

図 10.1　サーバ認証モデル



出典：「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、34 頁　図 2.3　サーバ認証モデル

１０．２　クライアント認証モデル

図 10.2 に示すクライアント認証モデルは、クライアント端末側で、例えば IC カード内に生体情報を管理し、センサを含むクライアント側のシステムで利用者認証を行うシステムである。登録および認証の概略を示す。このクライアント認証モデルでは認証結果を端末側で行うため、アプリケーションの起動はクライアント端末から行うのが基本である。

（1）登録

（ア）センサで入力した生体情報を氏名などの個人情報を付加して認証サーバに転送する。

（イ）　管理サーバで与信（登録者の正当性確認）の照会を行う。

（ウ）　与信に問題のない場合は、テンプレートに認定された旨の情報を埋め込んでクライアント端末に転送し、クライアント側で保管する。サーバ側では、個人情報、ID 情報、特徴量を登録管理サーバで安全に保管する。なお、クライアント側ではサーバから受信したテンプレートを IC カードなどの耐タンパ性のある媒体で保管する。

（2）認証処理

(ア)　クライアント端末側でセンサから入力した生体情報の認証処理を行う。この場合、利用するテンプレートが正しい管理サーバで受理されたものかを、管理サーバに問い合わせることも、セキュリティ確保の点で有効な方法である。

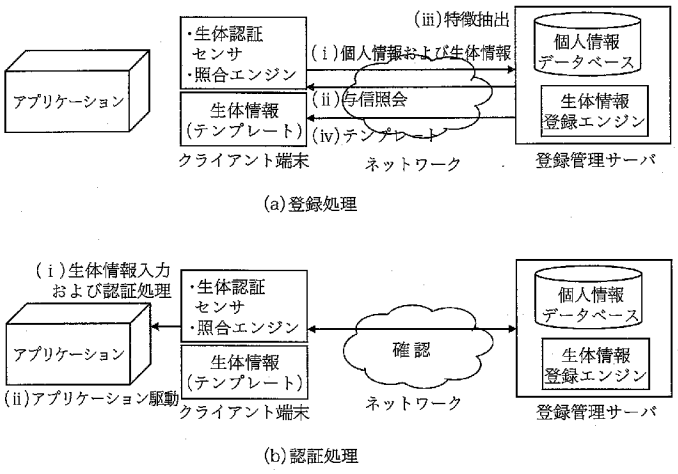
(イ)　認証結果が妥当ならアプリケーションを起動する。

このモデルでは、認証サーバが不用なため経費が安く、個人情報はユーザが管理するという受容性の面でメリットがある。またクライアント側の生体情報が盗難にあってもシステム全体に影響が及ばない。一方、クライアントの端末の処理負荷は高く端末コストも高くなる。

なお、低セキュリティシステムへの適用としてコストを削減したい場合は管理サーバを用いなくても良い。この場合は利用者が勝手に登録処理ができないような運用を行う必用がある。

どちらのモデルが優れているかは、利用者の受容性、脅威の対抗性、費用などを考慮し、システムごとに評価する必要がある。

図 10.2　クライアント認証モデル



出典：「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、共立出版株式会社発行、34 頁　図 2.4　クライアント認証モデル

１０．３　PKI とバイオメトリクスを連携した認証モデル

PKI による本人認証は本人の秘密鍵の所有が前提であるため、秘密鍵の盗用によるなりすましに対処する必要がある。したがって、セキュリティの確保としては、秘密鍵が秘匿されていること（他者に複製・詐取されないこと）、秘密鍵が正しい所有者以外に利用できないこと、この二つが重要な要件となり、現状では IC カード等の耐タンパ装置に秘密鍵を格納し、格納した持ち主を暗証番号で確認する対策が一般的である。しかし、暗証番号は本人の記憶を拠り所にしていることから盗用の危険がある。そこで予め PKI の本人認証フローに生体情報を組み込むことで、暗礁番号を用いなくとも良い PKI とバイオメトリクスを連携させた本人認証システムが期待されている。

（1） バイオメトリック認証への要件

大規模な利用者へ展開する PKI に生体情報を組み込んだ場合、安全性と利便性の効果を得るには、次のような 4 つの要件を満たす必用がある。

（ア） PKI との整合性

生体による本人認証の対象者と PKI による本人認証の対象者が一致していることを確認した上で認証処理を行う必用がある。そうしないと、データの組合せを変えることで、なりすましが可能となる。このため、テンプレートフォーマットとして、RFC3039 クオリファイド証明書が提案されているが、次の 2 つの問題がある。

- 証明書の有効期限と比較して経年変化のあるバイオメトリクスの寿命が短い場合には、テンプレートを更新する度に証明書を発行する必要があることから、証明書発行コストが増大するなどの問題がある。
- バイオメトリクスデータの格納先のアドレス情報が証明書に含まれていて、プライバシー情報であるバイオメトリクスデータをネットワーク上で公開する必要があることから、プライバシー保護の観点で問題がある。

このため、PKI 情報と生体情報の正当性を保持しながら生体情報と PKI 証明書と独立に運用でき、さらに利用者の責任の範囲でテンプレートを管理できるフォーマットが求められている。

（イ） クライアント処理の内容確認

クライアント側でバイオメトリック認証を行い、その結果で PKI の本人認証を行う場合には、クライアント側でどのような認証処理を行ったか判断できない。このため、どのようなバイオメトリック認証処理をどのような閾値によって本人と判定したのかを、認証側に通知する必要がある。

（ウ） テンプレート寿命への対応

テンプレートには時間経過による寿命があり、バイオメトリック認証技術や利用者ごとにその寿命は異なるので、テンプレートの寿命が切れる前に簡便に生体情報を更新できる仕組みが必要である。

（エ） 未対応問題への対応

利用者によっては、各バイオメトリック認証技術が適用できない未対応問題が存在するので、各利用者に適したバイオメトリック認証技術を選択できる仕組みが必要である。

（2） 認証モデル

バイオメトリック認証システムは、10.1 と 10.2 で記述したように大別してサーバ認証モデルとクライアント認証モデルに大別できる。

（ア） サーバ照合モデル

PKI と連携する場合は、クライアントでの署名結果と収集した生体情報をサーバで検証・照合することにより認証する。

（イ） クライアント照合モデル

PKI と連携する場合は、クライアント側で収集した生体情報と照合を行って所有する秘密鍵を活性化し、PKI で本人認証する 2 段階の認証となる。

（3） バイオメトリック PKI モデルの一例

上述したバイオメトリック認証への 4 つの要件と認証モデルを考慮した本人認証システムについて、次に示すモデルが提案されている。

（ア） テンプレートフォーマット

生体による本人認証の対象者と PKI による本人認証の対象者を一致させるには、予め登録する生体情報のテンプレートの対象者と PKI の証明書の指す対象者とが一致する必要があり、かつ、テンプレートの完全性を確保しなければならない。また、テンプレートは PKI 証明書とは独立に運用・保守ができることが求められる。

以上を考慮して、表 10.3 に示すように PKI の証明書とは分離したテンプレートが提案されている。

テンプレートには、バイオメトリクスの対象者の識別情報として PKI 証明書を一意に識別できる情報（例えば発行者命とそのシリアル番号）のフィールドを持つことで PKI との関係を保持する。そして、テンプレート発行者がこのフォーマットにデジタル署名する（PKI 証明書とは独立に添付する）ことでフォーマットの完全性を保証するとともに、PKI 証明書とテンプレートは独立に運用することが可能となる（図 10.3 参照）。

この運用の独立性と、テンプレートフォーマットのフィールドにテンプレートデ

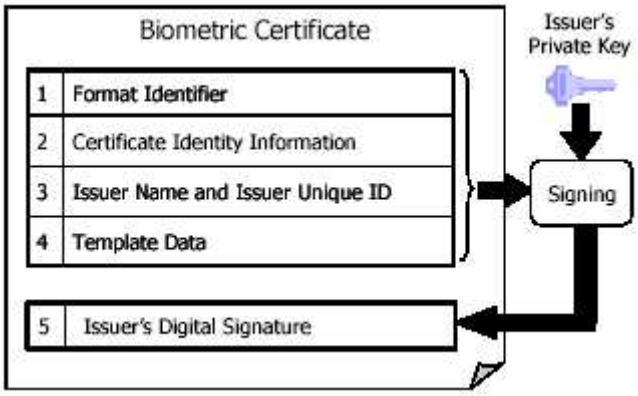
ータ（バイオメトリクスのタイプやアルゴリズム識別情報など）を持つことにより、バイオメトリクス技術ごとに個別に運用することができ、さらに必用なテンプレートを後から追加したり複数所持したりすることも可能となるので、柔軟に運用することができる。

表 10.3　テンプレートフォーマットの内容

#	項目	内容
1	Format Identifier	テンプレートフォーマットを識別する情報
2	Certificate Identity Information	PKI の証明書を一意に指定する情報．例えば，発行者名とそのシリアル番号．
3	Issuer Name & ID	このテンプレートを発行した発行者の名前および識別情報
4	Template Data	テンプレートデータ（バイオメトリクスのタイプやアルゴリズム識別情報などを含む）
5	Issuer's Digital Signature	このテンプレートの発行者によるディジタル署名（署名アルゴリズム情報を含む）

出典：「PKI とバイオメトリクスを連携した本人認証の課題と要件」、「2004 年暗号と情報セキュリティシンポジウム(SCIS2004) 予稿集」、2004 年 1 月 27 日、磯部義明、瀬戸洋一著、
社団法人 電子情報通信学会 情報セキュリティ研究専門委員会発行、
565 頁　表 3　提案するテンプレートフォーマットの内容

図 10.3　テンプレートフォーマットの完全性保証



出典：「PKI とバイオメトリクスを連携した本人認証の課題と要件」、「2004 年暗号と情報セキュリティシンポジウム(SCIS2004) 予稿集」、2004 年 1 月 27 日、磯部義明、瀬戸洋一著、
社団法人 電子情報通信学会 情報セキュリティ研究専門委員会発行、
565 頁　図 5　提案するテンプレートフォーマットの完全性保証

（イ） 本人認証の処理イメージ

アプリケーションサーバからのクライアントに対する利用者認証要求コマンド（チャレンジコード含む）を受けて、次の処理を行う。

(a) PKI 証明書が改ざんされていないかを認証局(CA) の公開鍵を使って検証した後、

PKI 証明書の ID 情報とテンプレートデータの ID 情報が一致しているか確認する。その後、テンプレートデータが改ざんされていないかをテンプレートの発行機関（BIA：Biometric Issuing Authority）の公開鍵を使って検証する。不一致があれば、サーバへ NG レスポンスを返す。

(b) 次に利用者から入力された生体情報とテンプレートデータとを生体照合し、不一致であれば証明書対象者以外の利用としてサーバへ NG レスポンスを返す。

(c) 安全に保管された利用者の秘密鍵を使って、チャレンジコードと生体照合の処理情報 P.C.（プログラムの識別情報、算出した類似度、本人判定の閾値など）に対しデジタル署名を施し、利用者の証明書と共にサーバへ OK レスポンスを返す。

(d) サーバでは受信した情報に基づき、利用者の証明書の公開鍵を使ってレスポンスコードを検証する。この時、クライアント側での照合処理情報 P.C.をサーバ側で独自に判断して、サービス提供の可否を決定できる。

秘密鍵が漏洩しても上記(b)で示すように、他者が秘密鍵に対応するテンプレートの生体情報と一致しないため、サービスの不正利用を防ぐことができる。また、クライアントの照合処理内容がサーバ側で分かるため、本人認定の閾値などが低すぎると判断した場合は、サービス提供を拒否することも可能である。

（参考文献）

・「サイバーセキュリティにおける生体認証技術」、2002 年 5 月 25 日、瀬戸洋一著、
共立出版株式会社発行、32―36 頁
・「PKI とバイオメトリクスを連携した本人認証の課題と要件」、「2004 年暗号と情報セキュリティシンポジウム(SCIS2004) 予稿集」、2004 年 1 月 27 日、磯部義明、瀬戸洋一著、
社団法人 電子情報通信学会 情報セキュリティ研究専門委員会発行、561―566 頁