バイオメトリクス

第１章　バイオメトリクス技術と本人認証

(1-1)　バイオメトリクスとは

Biometrics は、そのままバイオメトリクスと表記できるほど、一般的な言葉になっている。技術的な定義は、「Biometrics deals with identification of individuals based on their biological and /or behavioral characteristics（行動的あるいは身体的な特徴を用いて個人を自動的に同定する技術)」である。

名詞として用いる場合はバイオメトリクス（biometrics)、形容詞として用いる場合はバイオメトリック（biometric）と表記するのが一般的である。

認証に利用されるバイオメトリクスは次の 3 つの性質を持っている。

① 普遍性(universality)：　誰もがもっている特徴。
② 唯一性(uniqueness)：　万人不要。本人以外は同じ特徴を持たない。
③ 永続性(permanence)：　終生不変。時間の経過とともに変化しない。

(1-2)　バイオメトリック技術の歴史

バイオメトリクスを個人の識別に利用した歴史は古い。例えば、指紋を例に述べると以下のような歴史がある。

指先の表皮模様である指紋（fingerprint）は「万人不同」、「終生不変」という特徴をもつと経験的に理解されていた。このため指紋は、古くから個人同定の手段として用いられてきた。世の中に同一指紋を持つ人間が存在する可能性は 870 億分の 1 という。例えば、紀元前 6000 年頃から中国や古代アッシリアでは古くから指紋を使って個人認証を実施していた。また、わが国でも昔から拇印の習慣がある。

イギリスのゴールトンは、指紋を弓状(arch)、渦状(loop)、蹄状(whorl)の 3 分類とし、指紋が終生不変であり、同一個体がないことを指摘した。1897 年、インド政府は指紋法を採用し、1901 年、イギリス本土でも犯罪者の登録方法として採用された。

わが国における個人識別は、明治 41 年（1908 年）施行の刑法で再犯罪者を重く罰するために犯罪者の個人識別に指紋法を採用したことに始まる。警察庁でその活用が試みられ 1971 年にはコンピュータによる指紋鑑定の研究開発を開始し、実用的な犯罪者管理システム AFIS（Automated Fingerprint Identification Systems）として稼動している。

(1-3)　本人認証とは

認証とは、相手が意図した人であることを確認すること、なりすましを防ぐことであり、セキュリティを実現するうえで、必要不可欠な技術である。

厳密に定義すると、認証には認証すべき対象により 3 つのカテゴリーに分けられる。

① **本人認証**：コンピュータに接続しようとするユーザが、本人であることを証明する。文書の作成者だといわれる人物が本人であることを証明する。
② **権限認証**：ある行為をしようとしているユーザが、その権限を有することを証明する。
③ **同一性認証**：受け取った情報が、確かに送信者（あるいは作成者）が送信した（あるいは作成した）ものと同一であることを証明する。

本人認証については以下の 3 種類ある。

① **本人の所有物による認証**：磁気カードや IC カードを用いた認証である。携帯性や操作が容易などの長所がある反面、盗難、偽造の危険性がある。
② **本人が持つ知識による認証**：パスワードなどを用いた認証である。直接盗まれることは少ない。簡易な手段で実現できるという長所がある反面、本人が忘れる、パスワードが盗まれるなどの危険性がある。
③ **本人の身体的・行動的特徴による認証**：個体のもつ特徴を用いた認証である。記憶、所持などが不要であり利便性が高いが、認証のための特別な装置、高度な処理ソフトウェアが必要である。どの認証方式が優れているかは一概にはいえないが、個人を同定できる究極の方式としてバイオメトリック認証技術が注目されている。

また、バイオメトリクスの応用において、認証には識別(identification)と検証(verification)の 2 つの意味がある。例えば、検証とは提示された本人の特徴を示す情報と、利用者の PIN(Personal Identification Number)に対応したシステム内の登録情報との 1 対 1 の対応関係を確認することである。確認の方法は、一般的に類似度（登録データと入力データの似ている度合い）が用いられる。

両者の情報の差があらかじめ設定したしきい値以上であれば本人であると特定（検証）する。この検証機能を狭義の認証という場合が多い。

一方、識別とは、システムに提示された本人の特徴を示す情報と、あらかじめシステムの中に登録された情報を比較し、あらかじめ設定したしきい値以上のもっとも近いものを探すことをいう。

(1-4) 市場の推移

バイオメトリック技術の市場の変遷は、3 つのフェーズに分けられる。

1890 年代初期の犯罪検査においてコンピュータによる指紋照合アルゴリズムがはじめて開発された。これはミニコンピュータを利用したシステムとして開発された。デジタル画像処理技術が一般的になったのもこの時期であり、バイオメトリック認証の第 1 期に相当する。

第 2 期に相当するのは 1985 年頃である。ワークステーションが市場に現われ、システム構築コストが第 1 期に比べ 1 桁から 2 桁低減した。このため、バイオメトリクスが原子力発電施設などの重要施設関連の入退室管理システムに利用されるようになった。

第 3 期に相当するのは、ネットワーク技術などの発達によりテレホンバンキングやインターネットショッピングに代表される非対面の商取引のニーズが具体的になった 1996 年以降である。システムはネットワークに接続されたパソコンや IC カードで構築され、装置コストはさらに廉価になってきている。

第 1 期、第 2 期は、アクセス制御におけるパスワードの代替機能として、また、第 3 期はネットワーク環境下での本人認証機能の位置付けで技術の開発が行われた。

(1-5) いろいろなバイオメトリクス

バイオメトリクスは大きく身体的な特徴と行動的な特徴の 2 種類に分類できる。前者は、指紋、掌形、顔、虹彩などが相当し、後者は、声紋、署名が相当する。発声や筆記は随意的な要素があるために、声紋、署名は上記の身体計測的なバイオメトリクスと異なり行動計測的な特徴と呼ばれる。

(a) 身体計測的なバイオメトリクス

① **指紋**：人間の指紋には隆線とその間に形成された谷の紋様がその個人を特徴づける。指先の皮膚紋様は、弓状紋(Arch)、蹄状紋(Whorl)、渦状紋(Loop)に大別できる。紋様の山の部分を隆線(Ridge)、隆線の間を谷 (Valley) と呼ぶ。精度良く判別しようとすると、その紋様の詳細に着目し特徴を抽出する必要がある。特徴とは、隆線の端点 (Ridge ending) や分岐点 (Bifurcation) がある。これらを特徴点（マニューシャ: Minutia）と呼ぶ。

② **顔**：人間は顔によって相手を認識しており、バイオメトリクスの中では顔が人間にとって最もなじみやすい技術といえる。顔認証技術の特徴としては、登録情報としての顔画像と、認証時に撮影される提示情報としての顔画像を抽出して照合する必要があり、画像処理で人間が行うのと同じレベルの認証精度を実現するのはむずかしい。また、一卵性双生児などの認識可能性、めがね、髪型などの認証精度への影響検証が不十分であり、なりすましなどに弱い問題がある。また、顔認証システムにおいては、カメラの特性というより撮影条件、例えば、照明条件、顔の角度など、撮影条件による認証精度の劣化が著しい。

③ **虹彩**：虹彩と網膜は混合されることが多い。黒目の内側で瞳孔より外側のドーナツ状の筋肉質部分を虹彩という。網膜はレンズに相当する水晶体の奥にある視神経の集まった部分である。　人の目は、おおよそ妊娠 6 ヶ月ころまでに形成され、その時点で瞳の部分に孔があき、その開口部、すなわち、瞳孔から外側に向かってカオス上の皺（しわ）が発生される。この皺の成長は生後 2 年ほどで止まり、それ以降は変化しない。同一人の左右の目でも異なり、一卵性双生児でも異なる。疾病への影響に関しては、虹彩が角膜の下に存在することから眼球内部の疾病の影響を受けない長所がある。また、眼の充血や、眼の不自由な方の多くは視神経の障害であり、ほとんどの場合、虹彩認証精度の劣化にはならない。

④ **網膜血管**：直接観察できる血管パターンである。この網膜上の血管が形成するパターンは各人各様で個人識別に使える。網膜上の血管パターンを見るには、眼底撮影と同様に専用の装置が必要であり、微弱な赤外線を網膜の円周上を走査することにより、血管部分は温かく赤外線を吸収する性質を利用し血管パターンを撮影する。この血管パターンを一次元信号データとして処理し特徴量とする。しかし、網膜の血管パターンは糖尿病などにより変化するなど利用における問題がある。

⑤ **手の甲（ひら）静脈**：手の甲あるいは手のひらに浮き出した血管の模様（静脈パターン）に着眼するものである。静脈分布のパターンは人および左右の手によって異なるといわれている。静脈のパターンにおける血管分岐点における分岐角度や分岐点間の血管長を特徴量としている。血管

パターンは赤外線CCD(Charge Coupled Device)カメラによって撮影される。照合アルゴリズムは、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。

⑥ **指静脈**：指静脈パターン認証技術は近赤外光を指に照射し、その透過光から得られる指の静脈画像を撮影し、指静脈画像から指静脈パターンを抽出して、あらかじめ登録された指静脈パターンデータと照合して個人を識別する技術である。近赤外線には、身体組織に対して透過性が高い一方、血液中のヘモグロビンには吸収されるという特徴があるため、近赤外光を指に照射すると、指の静脈が影となって画像に現われる。この影が静脈パターンとなる。指静脈画像はカメラにより撮影され、指静脈画像に対して画像処理を施すことにより指静脈パターンが得られる。基本的には手の甲などと同じ原理で計測される。

　指は10本あること、指紋などと連携した認証装置構成を実現できること、装置を小型にできることが、他の類似の方式に対するメリットといえる。

⑦ **耳介**：人間の耳介は集音と増幅機能をもつように複雑に入り組んだ軟骨の凹凸によって、形づくられている。この凹凸形状は個人差があり、形態学的にも解剖学的にも万人不同であることが示されている。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、終生不変とみなしえる範囲といえる。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。

⑧ **汗腺**：指にある汗腺の分布は、各個人によって異なっている。指紋におけるマニューシャと同様、汗腺の位置を登録し、これにより認証を行う。ちなみに、犯罪捜査においては、マニューシャのほか汗腺分布なども個人同定に用いられている。

⑨ **匂い**：ボライタル（volatiles）と呼ばれる化学製品が人物の匂いを区別できることを利用し、多くのセンサが開発され現在検証実験が行われている。

⑩ **DNA**：人間のDNA(デオキシリボ核酸: deoxyribonucleic acid)は、約30億個の塩基配列からなり、人体の設計図ともいわれている。人間一人ひとりが少しずつ違うようにDNAの塩基配列も人により異なり、終生不要である。犯罪捜査にはおける個人識別を中心に利用されている。DNAパターンによる本人認証は、検証するための処理時間がかかり、また、処理(試薬や装置)が高価であることが問題である。

(b)　行動計測的なバイオメトリクス

① **声紋**：音声信号の周波数成分から声紋データを抽出し、事前に登録した同じ言葉の声紋データと照合することで話者認証する方式である。音声の個人差を用いて、誰の声であるかを自動的に判定することを声紋認証あるいは話者認識(Speaker Recognitionあるいは Voice Verification)という。

②**署名**：筆順、筆圧、運筆速度、ペンを上げたときの運動など、動的な筆跡を用いて識別する動的署名が一般的な技術である。手書き文字に対して、筆者が誰であるかを客観的に判断する試みは、筆跡計測として国内外でかなり古くから存在している。署名認証には静的署名認証と動的署名認証の2つがある。静的署名認証はオフライン認証ともいい、すでに書かれた純正書名（本物の署名）データと新しく提出された署名データを比較判定するもので、一般的には2次元座標値の類似性で個人認証を行う方式である。一方、オンライン署名認証は、タブレットなどの座標入力装置上に筆記された署名を利用する個人認証方式である。ペン先の座標、筆圧などを一定時間間隔でサンプリングして得られる時系列情報を署名の運筆情報としてとらえ、あらかじめ登録した基準となる書名データと入力署名の運筆情報を照合することにより本人の書いた署名であるかを判断する。

③ **キーストローク**：キーを打つパターンやリズムも各個人ごとに異なっている。キーストローク（ keystroke）認証技術は、キーストロークの持続時間、キーストローク中の回数、タイピングエラーの頻度、強制キーストロークなどの個人のタイピングの特徴に基づいている。キーストロークを登録するために、キーを打つリズムのテンプレートができあがるまで、繰り返しキーを打つ必要がある。

④ **手指動作**：手指動作を用いた個人認証の方法である。手指の形状および動作はカメラにより撮影する。「じゃんけん」のように手指の動作にそれぞれ個人固有の特徴が含まれていることに着目して、この手指動作情報を特徴量として用いている。動作であるから、静止物と違い能動的であり、行動パターンの変更も可能な特徴をもつ。

(1-6) これからのバイオメトリック技術のポイント

(a) セキュリティ装置としてのバイオメトリクス

バイオメトリック認証はパスワードやカードなどの本人認証技術と異なり、画像処理などにより特徴量空間における類似度でもって本人性を統計的に判別するため、その精度は 100%ではない。このため、誤認識の発生を前提にシステム構築する必要がある。したがって、画像（信号）処理装置として本人認証制度を追求するだけでなく、トータルシステムとしての構築コストと安全性を考慮したセキュリティ技術の観点からバイオメトリクス認証技術を展開する必要がある。

(b) 暗号との連携

ユビキタスネットワーキングにおいては、バイオメトリック技術は、人をサイバ空間とリアル空間に結びつけるインターフェース技術の位置づけで非常に重要となり、個人情報の扱いに配慮する必要があり、単に精度だけで論じるのは意味を持たないと考える。

PKI (Public Key Infrastructure)とは、公開鍵暗号技術をベースに構築する社会的な認証基盤をいう。バイオメトリック認証と PKI の関係は非常に密接な関係にあり、次の利用が考えられる。

（ｉ） 実印に相当する秘密鍵や証明書の管理媒体の所有者認証。

（ii） 管理されたバイオメトリクス自身の真生性の証明。

（iii） バイオメトリクス自身を電子認証の基盤とする PKI の構築。

以上のように、バイオメトリクスを電子認証基盤に展開する場合、バイオメトリクスが究極の個人情報であるため、個人情報の管理にプライバシー保護に関する運用基準が必要である。

(c) マルチモーダルバイオメトリック認証技術

マルチモーダブルバイオメトリック認証技術とは、指紋、署名、顔、声紋などのバイオメトリクスを 2 つ以上に用い､各バイオメトリクスの照合結果を用いて､融合判定により総合的に個人の識別を行う。複数のバイオメトリクスを用いるため、単体のバイオメトリクスに比較して本人拒否率や他人受け入れ率などの精度の改善が可能である。そのため、従来単体では精度が不足し、実用が困難であったバイオメトリクスを組み合わせて本人認証システムを構築できる。

(d) 脆弱性の明確化

ゼラチンなどを用いて人口指を作成し、指紋認証装置に対し偽造指紋がかなりすましできるか否かが実験室で検証された。ある種の偽造指紋に対し、見分ける能力が低いという結果になった。

指紋に限らずバイオメトリクスは非接触獲得が可能なものが多く、センサで生体か偽造かを低コストで実現することはむずかしく、脆弱性（vulnerability）の問題、つまり偽造（forgery, counterfeit）の問題がある。脆弱性の情報は信頼できる機関での管理が重要であり、脆弱性のガイドラインの策定も重要である。

(e) プライバシーとしてのバイオメトリクス

バイオメトリックデータに関するプライバシー問題は、バイオメトリクスが身体的な情報であるがゆえに生じる。

つまり、

① 取替えのきかない情報である：身体的な情報であり、例えば指を切り落としてしまった場合、代わりの指をつけるわけにはいかない。また、指紋を盗まれた場合、代わりの指紋を生成することはできない。

② 本人の同意なく収拾が可能なものが多い：一般にバイオメトリクスが身体の表面に露出しているため、カメラで本人の同意なく顔のデータをとるなどが可能である。

③ データから本人を特定できる：バイオメトリクスは個人と直接リンクした情報であるため、生体情報から逆に本人を特定することができる。

④ 本人の副次的な情報が抽出できる： バイオメトリクスによっては、例えば、網膜の血管パターンなどから糖尿病などの病歴を知ることができる。また、皮膚の色から人種が把握できる。

(f) キャンセラブルなバイオメトリクス

システムに保管されたバイオメトリックデータが盗難にあったり、また、Ａというシステムで登録されたバイオメトリックデータがＢというしステムで登録者の許可なく流用されたりする。つまりクロスリファレンス（cross-reference）を許さないシステムの構築が必要である。

このための研究開発としては、キャンセラブルなバイオメトリクスと呼ばれえる技術が開発されている。例えば、データ入力時にシステム内では、一方向性関数で変換されたデータを用いるという技術である。つまり、そのシステム固有のデータを作るということである。データは他のシステムでは正常に動かないし、もし盗難にあった場合は、別の一方向性関数でデータを生成すればよい。

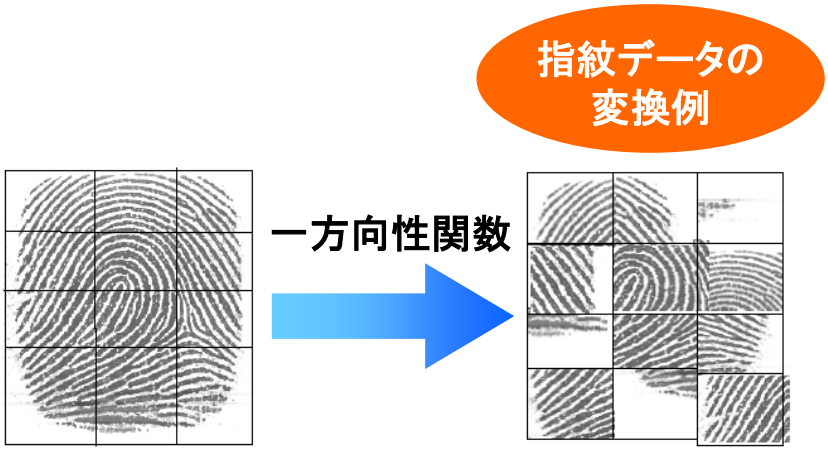


図１　取り消し可能なバイオメトリクス

第２章　バイオメトリック技術

(2-1)　指紋

バイオメトリック認証技術の中で、指紋認証技術は一番歴史が古く、簡単に使用することができるものの１つである。指紋は「万人不同、終生不変」といわれ、身体情報の中で、比較的簡単に個人を特定できるものとして活用されてきた。他人と同じ指紋は存在せず、自分の 10 本の指の指紋でさえ同じものがないため、個人を特定することができる。この特性のため、当初は犯罪者捜査に指紋が使用されていた。多数の指紋データから合致すると思われる指紋を効率よく見つけ出すために照合技術の進歩が加速された。特に自動照合の技術が確立され、大規模な指紋データを使用した評価が行われたことにより、今日の個人認証の基礎ができあがった。

当初、指紋認証は、指紋の照合という行為が、犯罪者捜査に使われたこともあり、指紋を取るというマイナスイメージが強かったのだが、最近では携帯電話や PC(Personal Computer)に搭載され、気軽な個人認証技術のひとつになってきている。指紋は人間の指先にあるため、手をよく使う仕事をしている人とか、皮膚に荒れがある人は指紋登録や指紋照合がしにくいことも事実である。しかし、照合技術の進歩やセンサ技術の進歩により、指紋自体を登録できない人や、指紋照合ができない人が減ってきている。それでも依然指紋登録や指紋照合ができない人がいることも事実である。

(a)　指紋の構造

指紋は皮膚の盛り上がった部分が織り成す模様として見ることができる。この盛り上がった部分を隆線（Ridge）と呼ぶ。この隆線には始まりと終わりがあるものがあり、この始まりあるいは終わりの部分を端点（Ridge ending）と呼ぶ。また、隆線の中には２つに分岐して別の隆線になるものもある。この分岐しているところを分岐点(Ridge bifurcation)と呼ぶ。

端点や、分岐点を総称して特徴点（Minutia）と呼んでいる。指紋を照合するときに、隆線のパターンを直接比較して行う方法と特徴点の位置関係に着目して照合を行う方法とがある。いずれにしても、自動的に指紋を照合する技術は、指紋の隆線のパターンを検出して行われる。

(b)　指紋の種類

隆線が織り成す模様には、いくつかの特徴的なパターンがあることがわかっている。これらの特徴的なパターンを分類してみると、おおまかに次に挙げるような３種類に分類することができるが、すべての指紋がこれらの３種類に分類されるわけでなく、これらの分類に入らないような指紋も存在している。

①　**蹄状紋**：指先の真ん中あたりに、馬蹄形をした隆線が形作られている指紋である。半分ぐらいの人がこの形状の指紋をもっているといわれている。

② **渦状紋**：指先の腹の部分が渦巻き、あるいは円形、楕円形をした隆線で構成されている指紋である。蹄状紋についでこの指紋を持っている人が多いといわれている。
③ **弓状紋**：指の腹の部分が左右へのびた弓の形状をした隆線で形作られている指紋である。数パーセントの人がこの紋様を持っているといわれている。

指紋認証に使用される指紋データは、人間の目で見たような指紋の形がそのまま使われるわけではない。特に、特徴点を使用して指紋認証を行う方式だと、抽出された指紋データから元の指紋画像を作り出すことはできない。このことは指紋を採取されるという心理的な抵抗感を緩和することに寄与しているといってよい。

図 2　指紋の構造

(c) センサの種類

センサは指紋の隆線と谷を電気的、あるいは光学的に検出、分離することにより紋様を読み出す。センサは方式で大別すると、光学方式と半導体方式に分けることができる。また、形状で分けると、面センサとスイープセンサに分けることができる。最近ではモバイル機器におけるセキュリティ機能を実現するために、指紋による個人認証が実装されてきており、これらのモバイル機器にスイープセンサが使用されてきている。

①面型静電容量センサの構造

指紋を形作っている隆線構造を検出するために、微小な検出器を面上に並べて、指先全部の指紋を一度に取れるようにした指紋センサである。指先をこの面型センサ上におくと、隆線と谷でセンサ面に触れる部分と触れない部分がでてくる。このときに、微小検出器は指の皮膚との間、あるいは空気層との間でコンデンサを形成することになり、隆線と谷の部分で蓄積される電荷容量に差が出てくる。この容量の差を検出して、隆線と谷の形状を読み込む方式である。半導体の生産方法でセンサを生産できるので、比較的安価なセンサといわれているが、指先すべてをセンサ面に入れるだけの大きさが必要であるため、一般の半導体と比較して高価になる。

②スイープセンサの構造

スイープ型センサは、指先全部を一度に検出するセンサを備えてはおらず、人間がセンサ面上に指をあて、滑らせることによって指紋形状を検出する方式のセンサである。センサの大きさとしては、横方向が指の幅で、縦方向が数ラインあれば指紋検出が行えるので、小さなものを作ることができる。このため、モバイル機器のようにセンサを実装するのにあまり場所がないところに使用することができる。検出方式としては、前述の静電容量方式、感熱方式、光学方式などがある。一般的に、数ラインで構成されたセンサ素子のデータを一度に取り込むので、帯状の画像が取得できる。この帯状の画像を連続的に取得して、合成することにより指紋画像を再構成することができる。

③プリズム型センサの構造

プリズムの原理を応用して指紋を検出するセンサである。プリズム面におかれた指先にプリズムを通して光を当て、反対側で反射光を検出する。この反射光の光量に違いが現われるため、隆線の紋

様を読み取ることができる。プリズム面におかれた指先は、隆線部分がガラス面に密着する。これに対して谷の部分はガラス面に密着できず、空気層ができる。このため、入力されて光は、密着された隆線部分では乱反射し、光検センサさに光量が少ない光でしか届かない。 これに対して、密着していない谷の部分ではほぼ全反射となり、光検出線さに光量の多い光が届く。この光の量の違いにより、隆線構造を検出することができる。構造的にある程度の大きさが必要なため、極端な小型化はむずかしい。

④指内散乱光方式センサの構造

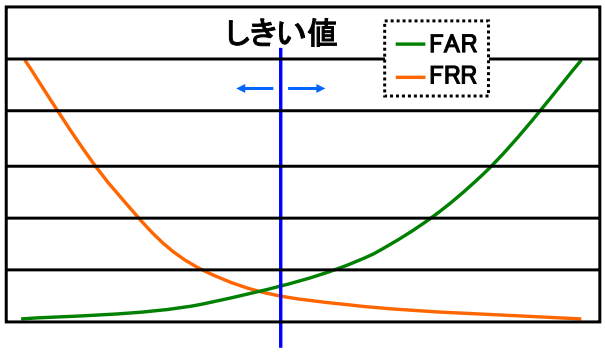
光を使用した検出方法であるが、プリズム型のように光を指に向けて照射するのではなく、指の横あるいは、斜め下から指先に光を当て、指の中を通って出てくる光の強弱によって指紋構造を検出する方式である。センサ面に触れている隆線の部分では、指内を通った光量の多い光がセンサまで届く。これに対して、谷の部分では空気層が谷とセンサ面にあるので、そこで光が散乱され、センサには光量の少ない光しか届かない。この光の強弱によって指紋の模様を検出する。指内を光が通るので、静電型のセンサに比べ乾燥した指や、汗の多い指でも紋様を読み取ることができる。

(c) 認証精度

バイオメトリック認証の動作は、事前に登録してあるデータと、認証したいときにとるデータとを比較することによって行われる。認証しようとして取得する指紋は、登録したときとまったく同じ状態にはならない。登録したときと認証するときの、温度、湿度、体調、指の押し付け方あるいは滑らせ方、精神状態などが違うことによって差が生じてしまい、経年による微妙な変化もでてくる。このため登録してあるデータと、認証用に取ったデータとの一致度をある閾値をきめて照合の成功、不成功をきめている。このため認証精度という概念が発生する。

指紋は「万人不同」といわれているが、ある部分だけを見れば同じような紋様が多数存在する。指紋認証を行うにあたり、どの程度の情報を使用して認証を行うかによって認証精度が変わってくる。確実な認証を行うために、情報量を多くすると、他人と間違えることはなくなる。しかし、自分自身の指紋でも指の当て方や体調によって少しでも登録してある指紋データと異なってしまうと、認証できなくなってしまう。

逆に少しでも認証しやすくしようとすると、他人の指紋と一致する可能性が出てきてしまう。これらの値を統計的に算出してひとつの指標としているのが、他人受け入れ率と本人拒否率になる。



他人受け入れ率(FAR)が上がると
本人拒否率(FRR)が下がるトレードオフの関係

図 3　認証精度

① **他人受け入れ率（FAR； False Acceptance Rate）** ：登録してある指紋データに対し、登録者以外の指紋を一致していると判断してしまう割合である。認証時に取得した指紋データを登録してある指紋データと比較したときに、あるしきい値以上の一致度があった場合である。

② **本人拒否率（FRR: False Rejection Rate）**： 登録してある指紋データに対し、登録者本人の指紋データを一致していないと判断してしまう割合である。認証時に取得した指紋データが登録時と違う状態で入力されることにより、あるしきい値以下になってしまった場合である。

指紋の場合は、指紋の紋様を検出できない場合があることが知られている。つまり、指が非常に乾燥している人や、反対に汗を非常にかいている人、指先をよく使う仕事をして指紋がすり減っている人、またはアトピーなどで皮膚が荒れている人などである。セキュリティシステムなどで指紋認証を使用する場合は、必ずこのように指紋登録ができない人がいることを考慮してシステム設計をする必要がある。

(d) 認証アルゴリズム

① **指紋認証システム**： 指紋認証を行う場合には、まず指紋登録が必要となる。登録に際しては、指紋データの他にその人の個人情報を同時に登録する場合もある。システムにより、指紋だけで認証するのか、個人コードを入力してそのコードの指紋と認証するのかによって、登録するデータは変わってくる。指紋データは怪我などがある場合を考慮して、一般的に左右１指ずつを登録する。それぞれにつき、何回か指紋を読み取らせ、相互認証して間違いのない指紋データを登録する。この登録指紋データがあまりよくないと、運用時に認証エラーが起こりやすくなる。登録指紋データをどこに保持しておくかにより、システム構成が変わってくる。サーバや PC 上にデータを保存し、認証もそこで行う場合と、指紋認証装置内部に指紋データを保持し、そこで行う場合とがある。指紋認証を行う場合には、指紋センサに１回だけ指紋を入力する。このとき、登録時と同じように指を置くことで認証動作が行われ、あるしきい値以上の一致度がある場合、認証成功となる。

② **アルゴリズム**： 一般的に、紋様の形状を比較する方式と、特徴点を利用して比較する方式がある。

・マニューシャマッチング方式： 隆線の端線や分岐点といった特徴点を利用した方式である。特徴点の個数、相対的な位置関係などの情報を指紋データとして使用する。指の表面は柔らかく、指をセンサに乗せると、指の押し付け方によって指紋が変形する。相対的な位置関係を使用することにより、この変形が起こっても、認証精度を確保できる。

・マニューシャリレーション方式： やはり、特徴点を使用した方式であるが、特徴点のほかに特徴点間を通る隆線の本数を合わせて指紋データとする方式である。特徴点間を通る隆線の数を使用することにより、特徴点の相対位置の類似や変形による誤認証を防ぐことができる。

・パターンマッチング方式： 隆線が作る紋様の一部を指紋データとして使用する方式である。各部分の隆線パターンを使用し、登録データと照合用に入力されたデータと照らし合わせて確認することにより、一致不一致を判定する方式である。特徴点を利用する方式に比べ、指紋データの容量は大きくなる。

(2-2) 顔

われわれは人と出会ったとき、視覚により相手の顔を見ることによって誰であるかを識別している。誰であるかだけでなく、「どこ」「欧米系」「20 代」「女性」「美人」「笑顔」「眠そう」「好み」など、顔から視覚的に得られる情報は、人と人の円滑なコミュニケーションに大いに役立っている。これと同じように機械が視覚により人の顔を識別し、さらに顔から得られる情報を理解できるようになれば、より人と機械の円滑なコミュニケーションができるであろう。近年、急速な画像識別技術の進展とコンピュータの高性能化に伴い、セキュリティやデジタル画像機器、エンタテイメントなどの市場において顔認証技術の実環境下での利用が広がってきた。顔認証の最大の特徴は、非接触性・非拘束性にある。これを応用することにより、手軽で人に優しいセキュリティを実現することができる。

(a) 長所

(i) 顔を見て判断することは、ふだんから人間が自然に行っている方法であり、もっとも人間に近い認証方法であるといえる。

(ii) 距離が離れていても、歩きながらでも認識可能（非接触・非拘束）なので、心理的抵抗が少ない。

(iii) (何も身につけずに)本人が意識することなく認証することができる(出入口を通っただけで、通路を通っただけで、端末の前に立っただけで、席に座っただけで、……)。

(iv) 顔で認証されることは、「顔パス」という言葉に代表されるように、一種のステータスがある。

(v) 顔画像や映像が記録できる、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。また、不正時の早期解決に役立つ。

(vi) 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、人数カウントなど)。

(b) 短所

(i) 虹彩などに比べると認識率は低い。認識率は環境により大きく異なるが、一般的な環境でも 1%近いエラー率がある。

(ii) 双子などの厳密な識別は難しい。

(iii) カメラから入力した画像の画像処理を行うため、大きな照明変化・大きな顔の向き・大きな表情変化・サングラスやマスク、撮像機器や撮像条件の変化などに弱い。

(iv) 顔は少しずつ変化する。特に幼児は成長につれて変化が大きい。こういう経年変化につれて、登録時と認証時の年月差の拡大に伴い認識率が少しずつ低下する。

(v) 公共の場所では、プライバシーの保護が問題になる可能性がある。

(c) 顔認証技術の流れ

① 顔検出

まず画像の中から顔領域を高速に検索し、その顔領域の位置を検出する。

② 顔特徴点検出

次に顔領域内の目や口の端点など、基準となる特徴点を検出する。それにより、正確に顔の特徴を取り出せるよう画像位置補正が可能になる。

③ 前処理

顔の位置や回転・向き、照明変化や眼鏡の影響などさまざまな変動要因をできる限り除外する。

④ 特徴量抽出

顔を見分けるための特徴を顔の中から複数抽出する。大きくは 4 つに分類できる。

(i) **顔全体の見え方に基づく方法**： 顔の領域内の濃淡情報全体を用いてその顔の特徴とする方法。少しの位置ずれに対して敏感であるという欠点があるが、細かい表情の変化や眼鏡の変化、髪型の変化など、細かい変化に対して強いという特徴がある。この方法の中で最も有名なのは、主成分分析（PCA: Principle Component Analysis）を応用した固有顔法である。

(ii) **局所的な特徴を用いる方法**： 顔画像の局所的な濃淡変化の間隔と方向成分を特徴量として、顔期間の形を捉える方法。局所的な領域の特徴を用いるため、顔の向きの変化などにおいては、顔全体の見え方は顔の向きにより大きく変化するが、小領域に注目すればあまり大きな変化をしていない領域が多くあるので、ある程度までの向きの変化に強いという特徴がある。この方法の中で最も有名なのは、Elastic Bunch Graph Matching である。

(iii) **顔全体の見え方と局所的な特徴の両方に基づく方法**： 顔の全体的な見え方と、局所的な特徴の両方をバランスよく重み付けして融合することにより、両者の長所を生かした特徴抽出が可能になり、効果的である。最近は多くの企業・研究機関がこの方法に取り組んでいる。

(iv) **3 次元モデルによる方法**： あらかじめ 3 次元形状と顔全体の見え方の 2 つに対して標準的なモデルを持っておき、認識時にはその両方を任意の入力顔に適合させるという方法。3 次元情報を考慮しているにもかかわらず、入力の際には 3 次元情報は必要ではない。この方法では顔の向きや照明変化に強いという特徴があるが、欠点は非常に計算時間がかかること、モデルを記述するためのデータサイズが大きい点である。

⑤ マッチング

特徴群より、入力された顔が登録者であるか、または登録者の中にいないかを識別する。代表的な方法として、最近傍法、線形判別分析、SVM（サポートベクタマシン）などがある。顔認証では少ない登録画像（1～数枚）から識別しなければならないという課題がある。そのために、少ない登録画像から照明変化や顔向き変化などを人工的に生成して登録データに加えるという手法が提案されている。

また、顔の向きや照明の変化に対応するために、顔画像を小領域に分割し、その識別スコアが高かった小領域同志のみで識別を行う手法が提案されている。

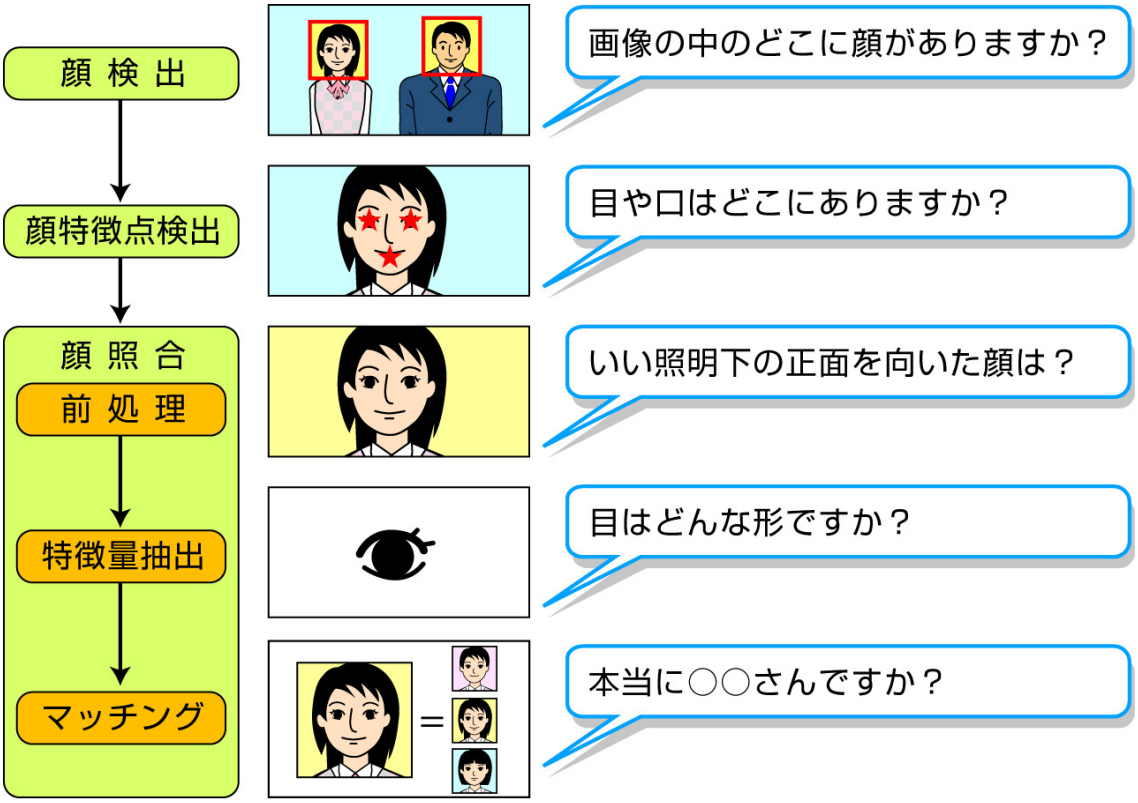


図 4　顔認証技術の流れ

(2-3)　虹彩

(a)　虹彩とは

虹彩とは、眼球内にある保護された内部器官で瞳孔の周りにある、瞳孔を取り巻く円盤状の薄い膜のことである。瞳孔を通して目の中に入る光を調整する筋肉から構成される。カメラにたとえると絞りの機能を行っている部分がこの虹彩である。虹彩は妊娠後 6 ヶ月ぐらいで生成され、その後生後 2 才ぐらいまで成長を続け、その後は、生涯変わらないといわれている。

虹彩の模様は、遺伝子の影響を受けず生成されるため、同一人物でも、左右別々の模様をもち、家族、一卵性双生児でも全く別の模様を持っている。虹彩は周囲の光に合わせて瞳孔を開いたり、閉じたりするため環境によって虹彩の面積が変わったり、年齢によって瞳孔の開き具合が変わってくるため、常に同じパターンではないのではないか？という疑問があるが、虹彩の模様は相似的変化をするため基の模様は変わることがなく、年齢、周囲の影響に左右されず同じ模様になる。疾病による虹彩認識への影響については、虹彩は目の表面（角膜の下）に位置することから影響を受けにくく、目の充血などでも影響を受けない。また、高齢者の発生が高い白内障は水晶体が曇る疾病で虹彩への影響はない。

(b)　虹彩認識の歴史

虹彩の模様については、古くから注目されていたが、1987 年眼科医 Leonard Flom と Aran Safir が虹彩パターンは人によって違うという概念の特許を取得した（フロム特許）。また、この特許を元に 1994 年、ケンブリッジ大学の John Daugman 博士が、虹彩のパターンを数学的な根拠に基づきコード化を行う特許を取得（ドーグマン特許）した。この 2 つの特許によって虹彩を使って認識を行う、本人を特定するという行為を行うこと、商品化を行うことはこの特許を使用しなければ実現できず、アメリカ Iridian Technology 社のライセンスを取得して商品化を行う必要がある。

現在、虹彩認証機器を製造販売するメーカは世界に 3 社あるが、すべて Iridian Technology 社の技術を使用している。虹彩の基本特許、フロム特許が近く失効するため、今後虹彩認識機器が各社から発売されるのではないかと考えられているが、身体情報をコード化するドーグマン特許は有効であることや、虹彩認識の精度の良さはドーグマン特許のアルゴリズムに寄与する部分もあり、各社か虹彩機器が発売されても一様な結果がでるとは限らない。

(c) 虹彩認識の特徴

虹彩認識とは前記で述べた虹彩という身体情報をビデオカメラで撮影し、登録されているデータと比較し、本人を判定する方法である。主な特徴としては、

(i) 認識精度が非常に高い。

(ii)完全に非接触で認識を行うことができる。

(iii)虹彩は生涯変わることがなく、外部の影響を受けにくいことから一度登録したデータを長年使用することができる。

(iv)虹彩の模様が複雑で、本人と他人の分布がはっきりしているため1：nの認識に適した方法である。

(d) 虹彩認識の概要

① 目画像の取得

人間の目は約24㎜の大きさで、この小さな組織に虹彩は位置しており、虹彩画像をいかにきれいに、簡単に取得するかが虹彩認識の重要な技術となっている。また、完全非接触なため、人間の動きやぶれ、身長差による撮像範囲の調整など虹彩認識特有の技術が必要となる。

虹彩認識の機器には大きく分けて2つの方式があり、自動取得型と誘導型で、自動取得型はある範囲内に入りカメラを見ていればカメラが自動的に虹彩を撮影する方法で、誘導型は鏡に映った自分の目を見ながら音声誘導に合わせて自分で距離を調整する方法で、なれが必要となる場合がある。それぞれ機器のコストや、サイズに違いがあるため、アプリケーションに応じて選定される。両方式とも撮像の基本原理は同じである。虹彩認識は、近赤外の光を当てて、赤外感度の高い白黒カメラを使って目画像を取得する。この際に認識に適した画像が得られるよう、フォーカス、センタリングなどを考慮して画像を取得する。

② 目画像から虹彩コードの生成

得られた画像から虹彩の位置を検出し、虹彩エリアの特定を行う。これは虹彩と白目の境の検出および虹彩と瞳孔の境を検出し、虹彩エリアを特定する。虹彩エリアには、上瞼（まぶた）、下瞼、睫（まつげ）などで虹彩部分が隠れてしまう場合があるが、コード生成前に除去を行い（睫と考えられる部分はコード化領域から除外する）虹彩コード（アイリスコード）を生成する。虹彩コードは8つの帯状に虹彩エリアを分割し、瞳孔の中心を原点とした極座標を設定し、特殊なフィルタを用いて各帯状のエリア内の濃淡を抽出する。この抽出された特徴点から256バイトの虹彩データが生成される。

③ 本人照合

取得された虹彩コードと登録された虹彩コードを用いて本人を照合する。本人を照合する際、2つのデータのハミングディスタンスを算出し、そのハミングディスタンスからしきい値に基づいて本人、他人という判断を行う。ハミングディスタンスは排他的論理和であるため、他人同士が全く違う虹彩を持っているため、0.5を中心に分布する。本人データの分布は理論的には0を中心に分布するが、取得条件の違いなどにより、0.1を中心に分布する。これらの分布は2項分布に一致することが確認されており、他人受け入れは、計算上120万分の1となっている。

④ 照合の特徴

虹彩は非常に複雑な模様があり、本人と他人の分布が交わらないことからしきい値を設定する必要がなく、ROC(Receiver Operating Characteristics)曲線を描く必要がない。そのため大規模のデータベースから1人を特定するのに適した認識方法であり、1：n認識に適した認識方法あるということができる。大規模になった場合でも虹彩だけで認識を行うことが可能で、カードや10keyとの連動が不要となる。本人拒否率は、虹彩カメラの誘導（うまく目を合わせ方法）により結果が異なる。虹彩の場合、完全な非接触であるため、体の動きや身長差による画像の取得、カメラとの立ち位置などによって変わってしまう場合がある。

(2-4) 静脈

静脈による本人認証技術は、執務室の入退管理システムやPCのログイン管理、マンション入り口での本人確認などさまざまな用途で利用されているが、最近では銀行など金融機関への適用が報じられ、

指紋や虹彩、顔など、他のバイオメトリック認識技術と比べて、現在最も注目を浴びている認証技術となっている。

一口に静脈認証技術とはいっても、指の静脈、手のひらの静脈、手の甲の静脈といろいろな部位を利用した技術および製品が存在する。また、静脈画像の取得方法も、光の透過による方法や反射による方法、また静脈の認証アルゴリズムも、血管パターンの分岐点の位置や方向などの特徴を利用する方法や血管パターンそのものをマッチングする方法がある。また、網膜による本人認証技術も血管のパターンを利用するという点で類似の技術といえる。

(a)　静脈認証の概要

近赤外線には、身体組織に対して透過性が高い一方、血液中のヘモグロビンには吸収されるという特徴（還元ヘモグロビン）があるため、近赤外光を指、手のひらや手の甲に照射すると、それぞれの静脈が影となって画像に現れる。この影が静脈パターンである。

人の静脈パターンは千差万別であり、個人差が大きく、身体内部の情報であるため外観からは識別されにくいことから、個人の識別に利用できることが示唆されている。また、静脈は成長によってその大きさは変化してもパターン自体は変化しないといわれており、同じような容姿の双子でも静脈パターンは異なることが経験から得られている。静脈認証では、入力された静脈画像に対して画像処理を施し、静脈パターンを抽出して個人の識別に利用している。

(b)　指の静脈認証

①　指静脈認証技術の概要

指静脈画像は、光源となる近赤外光を指に照射し、その透過光から得られる画像をカメラで撮影することによって取得できる。撮影された指静脈画像の画質が良ければよいほど血管パターンが正しく抽出できるため、良質の指静脈画像を撮影する指静脈装置が必要となる。図左側の静脈画像処理部では、指の上側に設置された光源（LED: Light Emitting Diode、発光ダイオード）から近赤外光を指に照射し、指の下側に設置されたカメラで撮影する様子が描写されている。その結果、指の手のひら側の静脈が影となって指静脈画像として取得され、この画像から指静脈パターンが抽出される。

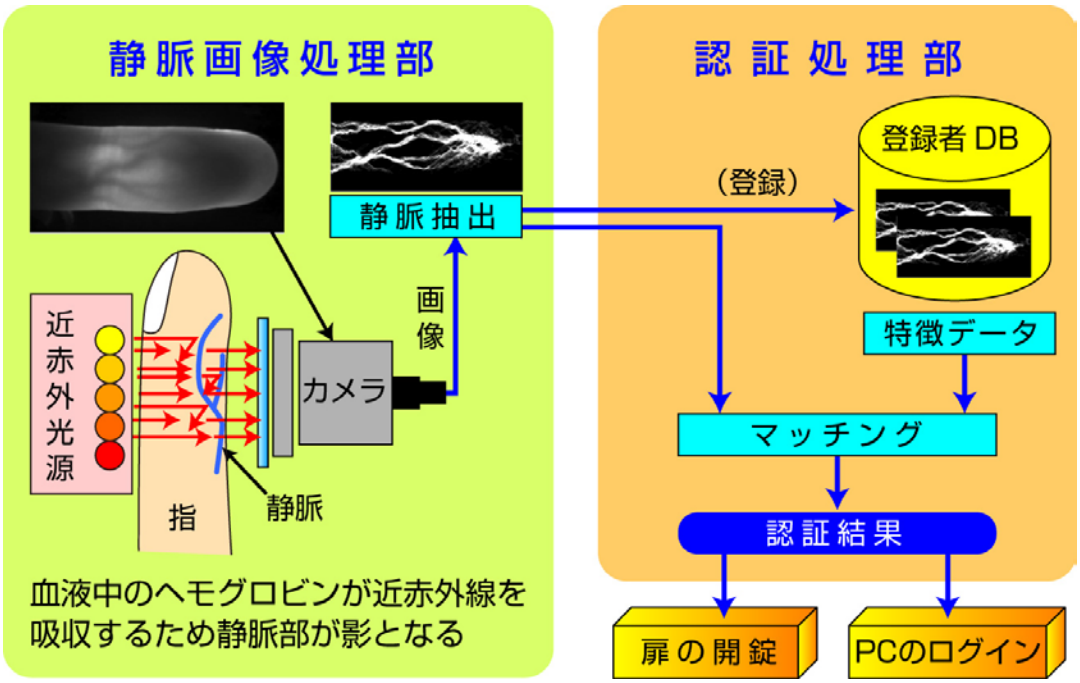


図 5　指静脈認証処理の概要

また、図右側の認証処理部では、データベースに登録済の指静脈パターン（特徴データ）と抽出した指静脈パターンとを照合（マッチング）して、その認証結果により扉の開錠や PC のログインが可能となることを示している。

② 指静脈認証の処理フロー

(i) 指静脈画像の入力処理を実施する。指静脈認証端末の開口部から指を挿入し、装置奥に設置されているボタンを押すことにより、指静脈画像が投影される。

(ii) 入力された指静脈画像から指の輪郭を検出する処理を実施し、入力画像のどの位置に指があるかを識別する。

(iii) 検出した輪郭を利用して指静脈画像の角度を補正する。本処理によりユーザの指挿入角度のバラツキを補正することができるため、仮にユーザがラフな指の挿入を行っても、認証することが可能となる。

(iv) 角度を補正された指静脈画像に対して、特殊な画像処理を実施することにより、高速に指の静脈パターンを抽出する。

(v) あらかじめデータベースや IC カードなどに登録してある指静脈パターンと、入力画像から抽出した指静脈パターンとの照合処理を実施する。照合処理では登録済の指静脈パターンと抽出した指静脈パターンのパターンマッチング処理を行い、どの程度類似しているかを示す類似度（照合値）を算出する。

(vi) 算出した類似度と本人判定しきい値を比較し、本人か他人かを判定する。本人判定しきい値は、多数の評価データを使った事前の精度評価テストから導出した最適な数値を設定する必要がある。

以上の処理を実施することにより、指の静脈を利用した本人認証処理が実現できる。

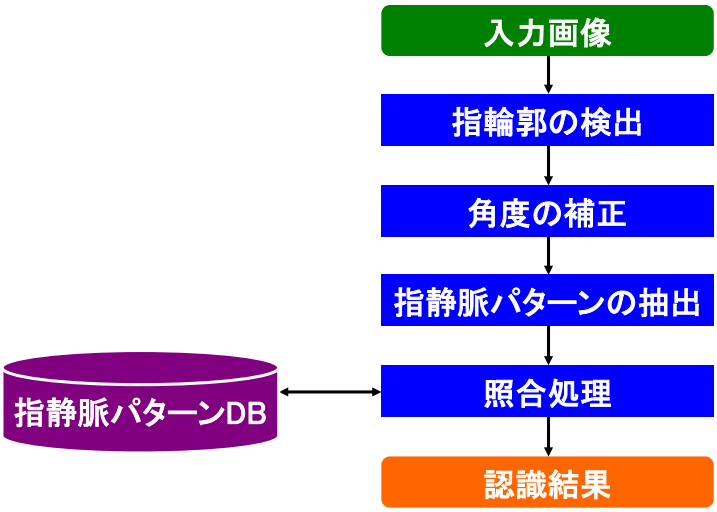


図 6　指静脈認証処理の流れ

③ 特徴

指静脈認証技術の特徴を次に示す。

(i) 外部から見えにくい身体内部情報を用いているため、他のバイオメトリック認証（指紋、顔、虹彩など）に比べて偽造することが困難で、信頼性が高い。

(ii) 透過光から得られる指の静脈画像を使用しているため、ほこり、汚れなどによる影響が少ない。

(iii) 指先の接触部分が少なく、利用者の心理的抵抗感が少ない。

(iv) 指の静脈パターンは、IC カードへも容易に記録できる。

(v) 認証速度が速い。

(vi) 認証精度が高い。

(vii) 他のバイオメトリック認証（例えば、指紋）では利用できないユーザがいるが、指静脈認証ではほとんどの人が利用できる。

(c) 手のひら静脈認証

衛生的かつ、心理的な抵抗感が低く、高い個人識別性能を持つバイオメトリック認証技術として、完全非接触型の手のひら静脈認証技術がある。非接触型の実現により、公共の場や医療業務など、衛生的に要求の高い場面への適用が可能となった。また、心理面でも、見ず知らずの人が触った後に、装置に

触れることへの抵抗感を持つ方にも十分配慮できるようになった。

①　特徴

手のひら静脈認証は、手の手首の境から指の付け根までの広い範囲の血管パターンを用いる。指や手の甲と比べて、認証する面積が広く、かつ静脈が複雑にからみ合っているため、人を識別する豊富な情報量がある。また、手のひらには、血管パターンを撮像するときに障害となる毛がなく、肌の色の影響も少ないため、世界中の多くの人に対応できる特長を持っている。さらに、手のひらは手の内側であるため、寒冷地などでも冷えにくく、冷えても指などの末端部に比べて先に温まるため、寒さによる血管の変化の影響が少ない部位といえる。

②　撮像方式

手のひらの静脈の撮像方式は、手のひらに相対して近赤外光を当て、手に入り込んで乱反射し、手のひら側に抜け出てきた光を結像する反射型方式である。手のひらに近赤外光を当てると、還元ヘモグロビンを含む静脈の血管パターンだけ光が吸収され、人間が見た場合の画像と異なり、静脈が存在する血管パターンだけ暗く映る。そこで、画像処理により暗く映った部分を静脈血管パターンとして抽出し、登録済みの静脈のパターンと照合する。反射型は照明と撮影を同一方向から行うので、照明部品と撮影部品を 1 箇所にまとめることができ、小型化にも適している。

完全非接触型の手のひら静脈認証では、手のひら静脈センサの上方に、手を開いてかざすだけでよい。手のひら静脈センサから手のひら全体に一様に近赤外光を照射し、ソフトウェアの処理により手のひらの多少の傾き、位置ずれ、高さの変動を補正する。

図 7　手のひら静脈認証

③　評価

手のひらの静脈認証の認証精度は、70,000 人 140,000 手のデータを用いた評価により本人受入率 99.99%のとき、他人受入率 0.000 08%以下（登録時に 3 回手をかざし、照合時には 1 回の再試行を含む場合。2005 年 2 月現在）が実証された。そのほかにも、総務省統計局センターが発表した人口分布に基づく 5 歳から 85 歳のさまざまな職業の方のデータ、国連が発表した世界の人口分布に基づく在日外国人によるデータ、日々の変化を数年にわたって追跡したデータ、飲酒、入浴、外出、起床などの各種生活場面などのデータにより、その性能が実証されている。

④　データ格納形態

手のひら静脈認証のシステムには、登録した手のひら静脈データを格納する形態として、現在、サーバ格納型と IC カード格納型の 2 つがある。サーバ格納型では、手のひら静脈センサをクライアントに連結し、クライアント側で手のひらを撮影して得た手のひら静脈パターンをサーバに転送して、サーバに格納する。照合時には、登録した手のひら静脈パターンをクライアントに転送し、ク

ライアント上で照合を行う。

ICカード格納型では､手のひらを撮影して得た手のひら静脈パターンをICカードの中に格納する。照合時には、一致を判定する手のひら静脈パターンをICカードの中に転送し、ICカード内で照合を行う。

サーバ格納型では、手のひら静脈パターンをサーバで集中管理できるという利点があり、ICカード型では、ユーザが自分の静脈パターンを自分で所持・管理できるという利点がある。

(2-5) 網膜

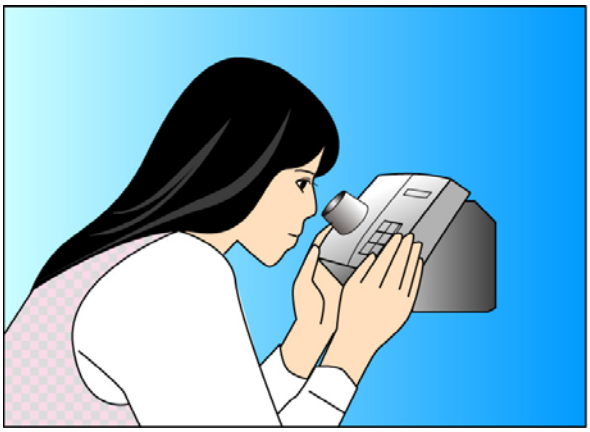
(a) 網膜認証の概要

網膜認証は、虹彩認証に先駆けて実用化された目のバイオメトリック認証であり、手のひらや指の静脈による認証と同様に血管パターンを利用した個人認証である。

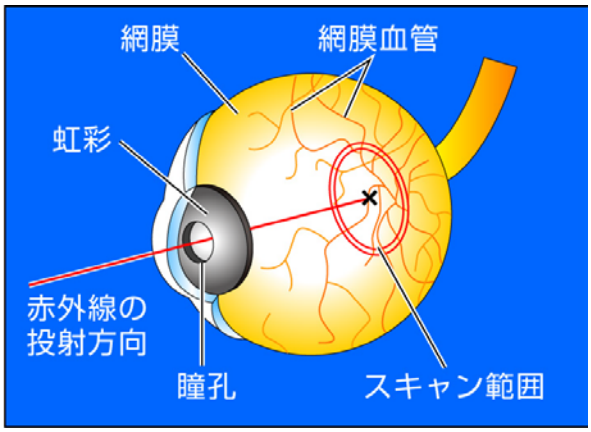
網膜は眼球の構成要素の1つで、眼球壁の最も内側に位置している。網膜はカメラのフィルムに例えられるように、目に入射した光を画像として取得する機能を持っている。網膜上には網膜血管が複雑なパターンを形成している。この血管パターンにより識別を行うのが網膜認証である。

網膜は、人間の一生のなかで変化することはなく、そのパターンは同一人物でも左右の目で異なり、個人性が強いといわれている。

目は高い反射的特徴を持っているため、網膜パターンを瞳孔から光学的に非接触で測定することができる。また、外表面的な特徴と異なり身体内部の情報であるため、スキャン時に安定的であるうえに、偽造や盗用に対して強固であるといえる。ただし、他のバイオメトリクスと同様、測定箇所の病害の影響を受ける。網膜認証においては、白内障などがそれにあたる。網膜の血管パターンによる個人識別の研究は1930年代から開始され、1984年にアメリカEyedentify Inc.（アイデンティファイ社）によって網膜照合個人識別機（網膜識別機）が開発、製品化された。



網膜パターンのスキャン方法



網膜パターンのスキャン範囲

図8 網膜パターンのスキャン

(b) 網膜による本人識別

被認証者は、網膜識別機のファインダをのぞきこみ、あらかじめ点灯している緑の光点を見つめながら、スキャンボタンを押す。すると、人体の健康に害を及ぼさない微弱な赤外線（890nm付近）が、網膜のスキャン範囲を走査する。血管部分は赤外線を強く吸収するので、その反射光は網膜のパターンを反映したものとなる。

反射光のアナログ画像信号をデジタル化し、これを個人データとして蓄積することによって個人識別システムとしての機能を持つことになる。

登録時にはより正確な再現性を期すために複数回の測定を行い、その平均値が登録データとなる。こうして登録されたデータと、実際の識別時の測定データがしきい値以上に一致していることで個人を認証する。

(2-6)　耳介

(a)　耳介認証の概要

耳介（じかい）とは、主に医学の分野で用いられる言葉で、側頭部両側から突き出した扇状の構造物であり、人体の耳の外側から見える部分を示す。耳介の形状から個人を認証する耳介認証の研究が進められている。人間の耳介は、その長さや幅の成長においては、耳長は 16～17 歳、耳幅は 10 歳前後で男女とも成長が止まり、40 歳前後まで少しずつ成長することが報告されている。この点で、身長の変化および加齢に対して、容貌の変化が少ないといえる。また、耳介は、その複雑に入り組んだ凹凸形状に個人差があるといわれている。この耳介の形状を用いて個人認証を行うのが耳介認証である。

耳介は、弾性軟骨と少量の脂肪および結合組織から構成されて、皮膚の皮下組織がほとんどなくすぐに耳介（弾性）軟骨となっている部分と、耳たぶ（耳垂）のように脂肪組織により作られまったく軟骨のない部分によって複雑な凹凸形状を形成している。耳介はその形状から、軟骨が隆起した扇状の耳翼部分と、陥没している耳甲介とに大別され、耳翼部分はさらに耳輪、耳垂、耳珠などから構成されている。耳介は、人間同士の会話に適した音の選別を有効にするためか、5kHz 程度の帯域に共振性を持つ。耳翼の部分で音を反射し、耳甲介腔で外耳道に音波を送り込み、この過程で人に固有な音色を付加していると考えられる。

耳介はその形状において、軟骨の隆起および陥没状態、軟骨の張り出し状態、軟骨の輪郭形状、軟骨間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、この非個人性の部分を明確にして、これを基準にすることによって、耳介比較（識別）を行うことができる。

(b)　耳介を構成する軟骨形状の個人性、非個人性

耳翼は、耳輪、上下対耳輪脚、対耳輪および対耳珠を支柱として、外耳輪および耳垂で張られた凹凸の著しい金管楽器の吹き出し口のように広く開いた部分のことで、耳介の耳甲介艇、耳甲介腔を含む窪み形状の部分を除いた部分である。耳翼を構成する軟骨の個々の形状およびそれらの接続状態が、強い個人性を形成していると考えられている。耳甲介の輪郭は、これらの軟骨の接続状態が反映されており、識別には重要である。耳輪は耳翼を構成し、対耳輪脚へのかぶさり方が耳輪を肥厚に見せたりして舟状窩の形を決める。上対耳輪脚は耳翼を支え、耳翼を頭部側に折りたたむように見せ、耳幅の大小にかかわる特徴がある。また、耳輪尾（耳輪下部の軟骨）は耳垂の張り出しを左右する特徴が見られる。交点 A は下対耳輪脚輪郭線と耳輪内縁との交点が作る部分で鋭角を形成する。この部分は比較的個人性が弱い。個人性が弱い部分を形状を比較する際の基準として、耳介要素の肥厚さ、屈曲の程度、屈曲の場所、張り出し、要素間の接続状態といった形状特徴を比較することによって、精度の高い耳介認証を行うことができると考えられている。

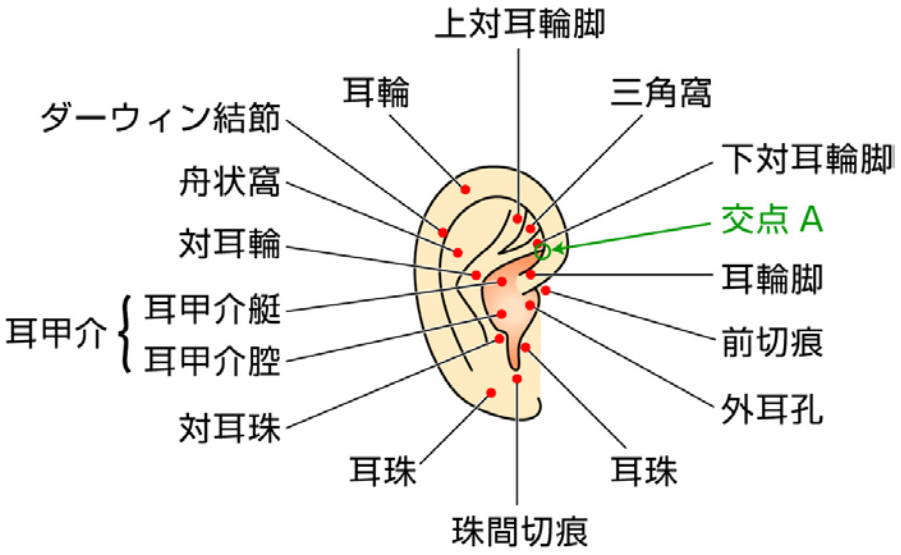
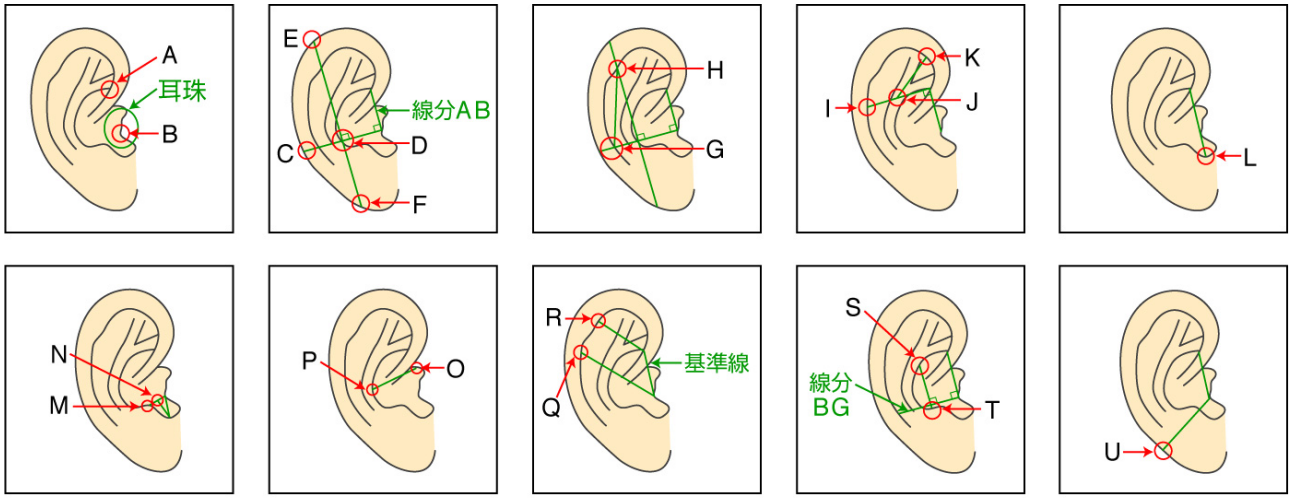


図 9　耳介要素の名称



名　称	線 分	名　称	線 分	名　称	線 分
耳輪脚長	AB	対耳輪脚幅	CG	対耳輪付け根太さ	AR
耳幅長	BC	三角窩長	JK	耳垂長	MF
耳　長	EF	耳甲介腔幅	OP	ダーウィン結節	BQ
上下対耳輪脚幅	AH	耳珠長	BL	耳甲介縦長	ST
耳輪太さ	EH	珠間切痕窪み	NL	耳介斜め長	BU
舟上窩長	GH	対耳珠—耳珠長	BM		

図 10　耳介要素長計測のための特徴点

(2-7)　声紋

(a)　声紋認証技術の概要

指紋認証や顔認証を行う場合、指紋や顔写真を取られるのは心理的に抵抗を感じるという人がいることは事実である。声紋認証には、このような心理的な抵抗が少ないという特徴がある。また、既存の電話設備を用いて遠隔地の認証ができるという特徴もある。一方、声紋認証は虹彩による認証などに比較して認証精度が劣る点は否定できない。そのため、音声の使いやすさを活かしながら、他の手段と組み合わせることでシステム全体の認証精度を高めるというシステム設計が重要となる。

声紋認証の研究は、1962 年にベル研究所の Kersta が、サウンドスペクトログラム（声紋）による話者認識の可能性を発表した時点にさかのぼる。当時は、声紋を研究者が見て判断するものだったが、その後のコンピュータによる音声処理技術の目覚しい発展に伴って、自動的に声紋認証を行う研究が活発に行われるようになってきた。1990 年代にはアメリカやわが国で実用化が始まった。電話やインターネットを使った電子商取引の本格化が予想される 21 世紀に入って、声紋認証はますます注目される技術となっている。

声紋認証には、サウンドスペクトログラムあるいはこれと等価な音声特徴を用いる。サウンドスペクトログラムの色の濃い部分は、そこに音声信号の成分が集中していることを示している。色が淡い部分は、音声信号の成分が存在しないことを示している。サウンドスペクトログラムのパターンは個人によって異なる。これは、サウンドスペクトログラムが個人ごとの発声器官（声道）の形や大きさの違い、さらには調音の違いを明確に表すためである。調音とは、母音や子音を発声する場合に、発声器官内での狭めの位置や、その狭めの位置の時間的な変化のパターンをいう。調音は、その個人の体格や、方言などのその個人が育った言語環境に大きく影響を受けている。声紋認証では、個人ごとの調音の違い、すなわち、サウンドスペクトログラムの違いを利用している。

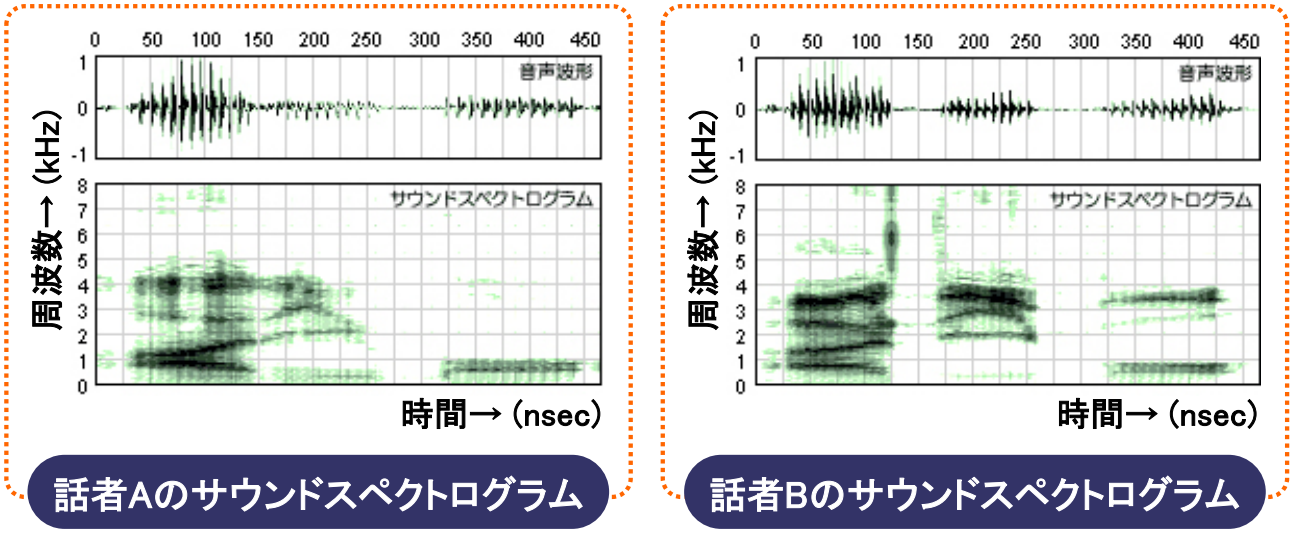


図 11　サウンドスペクトログラムの例

(b)　**声紋認証システムの構成**

マイクロホンから入力された音声は、音声分析部で周波数分析され、サウンドスペクトログラムあるいはそれと等価の情報に変換される。分析手法としては、高速フーリエ変換（FFT: Fast Fourier Transform）、ケプストラム分析（Cepstrum）などが用いられる。また、音声分析部では、音声や声紋収録系に含まれる種々の変動を正規化する処理が行われる。

登録時には、音声分析部の出力は話者モデル作成部に送られる。話者モデル作成部では、照合時に必要となる話者モデルを作成する。照合に DP 法（Dynamic Programming: 動的計画法）を用いる場合は、テンプレートと呼ばれる話者モデル、VQ 法（Vector Quantization: ベクトル量子化）を用いる場合は、コードブックと呼ばれる話者モデル、また、HMM 法(Hidden Marcov Model: 隠れマルコフモデル)や GMM 法（Gausian Mixture Model: 混合ガウス分布モデル）などの統計的手法を用いる場合は、複数の多次元正規分布のパラメータが話者モデルとして作成される。作成された話者モデルは話者モデル DB（データベース）に格納される。また、話者モデル作成時に、照合結果の判定時に必要となるしきい値を算出する。話者モデル作成時にしきい値を算出できない場合は、あらかじめ決められたしきい値を用いることもある。

一方、照合時には、音声分析部の出力は尤度/距離計算部に送られる。尤度/距離計算部では、入力音声の分析結果を話者モデル DB から読み出された話者モデルと照合し、入力音声と話者モデルの尤度（あるいは距離）を計算する。

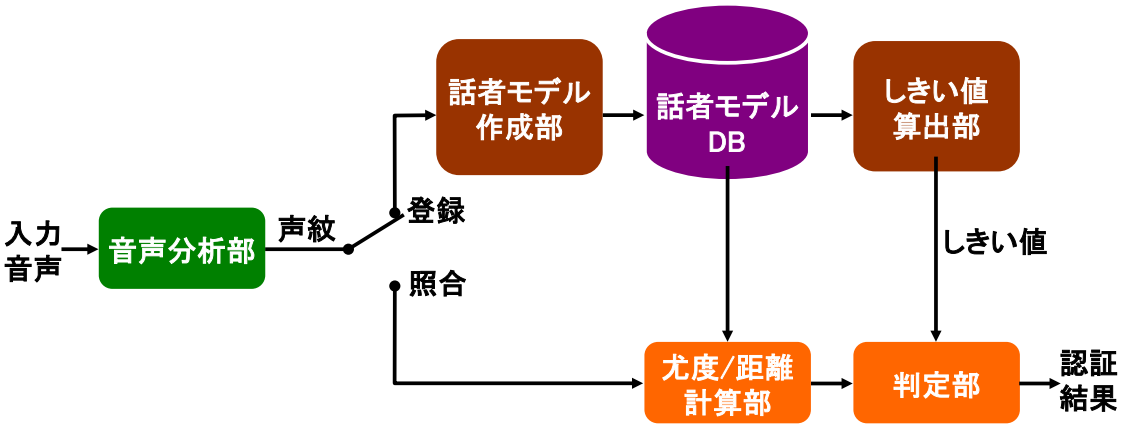


図 12　声紋認証のシステム構成

尤度（ゆうど）とは「もっともらしさ」という意味で、類似度と同じ意味合いを持つ尺度である。

ここでは、不特定話者の話者モデルあるいは入力音声に類似する他話者の話者モデルとの尤度（あるいは距離）を用いて本人モデルと入力音声の尤度（あるいは距離）を正規化することがある。これにより求める尤度（あるいは距離）の値の入力音声ごとのバラツキを抑えることができ、認証精度を高めることができる。判定部では、計算された尤度（あるいは距離）とあらかじめ設定されているしきい値を比較し、尤度がしきい値よりも大きい場合（あるいは距離がしきい値よりも小さい場合）に、入力音声が本人のものであるとして受理し、そうでない場合は、他人のものであるとして棄却する。

(2-8)　DNA

人間の DNA（デオキシリボ核酸）は、約 30 億個の塩基配列からなり、人体の設計図ともいわれている。人間の一人ひとりが少しずつ違うように、この DNA の塩基配列も人によって異なる部分がある。その部分の情報を利用することで個人認証を行うことができるというのが DNA 認証の考え方である。

人間の体は約 50～60 兆の細胞でできており、各細胞の核には複雑に畳み込まれた 23 対 46 本の DNA が含まれている。各 DNA は二重らせん構造の塩基配列と糖、リン酸によって構成されている。塩基配列の要素となる塩基には、A（アミン）、G（グアニン）、C（シトシン）、および T（チミン）の 4 種類があり、これらの塩基は、らせん型の列構造で連なっている。塩基配列とは、この塩基の並び順のことを指す。DNA の塩基配列は、同一人物であれば、どの細胞から取り出しても同じ並び順であり、終生不変とされている。また、その他の DNA の特性として、「無機質で安定である」、「水溶性なので容易にインクなどに溶かし込むことができる」などがあげられる。

(a)　DNA 個人認証の特徴

DNA の塩基配列は 4 種の塩基からなるデジタル情報であり、しかも情報量が豊富であることから、他のバイオメトリック認証と比較していくつかの特徴を持っている。

①　認識精度が高い

指紋のように DNA 以外のアナログ情報に基づくバイオメトリック認証方式では、10^{-3}～10^{-7} の認証精度（他人受入率）となっているが、DNA 情報を ID とした場合、現状の抽出技術で同値確立 10^{-18} 程度にすることができ、識別精度が高いといえる。

②　照合アルゴリズムが不要

DNA の塩基配列はデジタル情報なので、照合はデジタル情報同士の直接的な比較となる。他のバイオメトリック認証のようにアナログ情報からの特徴点抽出やパターンマッチングなどの処理を必要としない。

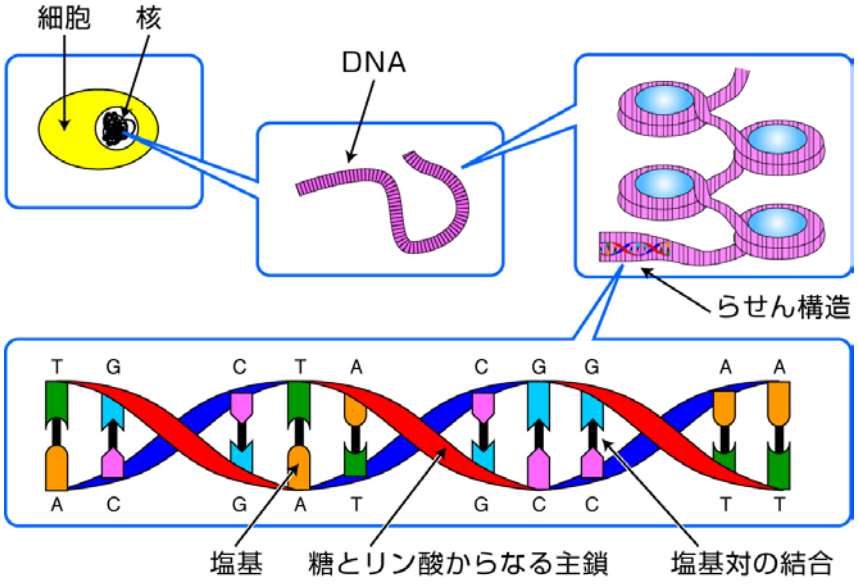


図 13　DNA の構造

③　親子関係を推定することができる

DNA の塩基配列には、親から子へと引き継がれる部位があり、ある程度の親子関係を推定すること

ができる。これは、あらかじめ本人の DNA 情報を取得していない場合にも本人認証（もしくは本人でないことの証明）を行える可能性もあることも示している。

④ 塩基配列情報の抽出・分析に時間と費用を要する

一般的な DNA-ID 生成方法（口腔を綿棒で軽くこすり、粘膜の細胞から DNA を抽出し、DNA-ID を生成する）は、最新の設備でも 3 時間以上かかるといわれている。また、DNA-ID を生成するには高価な試薬を必要とする。このため、DNA を利用した認証は、特別な用途に限られているのが現状であるが、今後技術開発が進展することでさまざまな分野への適用が期待されている。

(b) DNA 認証マーク

ブランド商品やプレミアムグッズの真贋識別に実用化されているのが DNA 認証マークである。この認証マークの印刷インクには、当人の ID となる DNA の一部が溶解されており、いわゆる DNA 入りインクを使った特殊印刷が行われている。当人の DNA はユニークなものであり、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 が再生できるか否かで行われる。なお、補助的確認手段として、インクに特別な波長に対して発光する蛍光剤を混入し、手持ちの赤外線レーザスキャナを使って正規の認証マークであることを見分ける。このインクの製法を秘密にすることにより、事前にある程度のチェックはできることになる。また、インクそのものをインビジブルとして、商品のどこにマークが刷り込んであるかを秘密にしておく方法もとられている。これによってなお真贋判定の安全性を高めている。

(c) 法医学分野における DNA 鑑定

① 犯罪捜査への適用

法医学部門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きている。犯罪捜査では現場に残した本人の血液（白血球のように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。これも DNA によるバイオメトリック本人認証といえる。最近の法廷の判例では、DNA 鑑定が証拠として採用されている。

② 身元不明人の DNA 鑑定

近年、犯罪捜査においても、より正確な本人鑑定のために DNA を用いた方法が盛んに行われている。オーストラリアの山岳ケーブルの火災事故では、焼死体の骨から DNA を抽出し、本人鑑定が行われた。照合する相手は両親や兄弟で、1～2 親等における DNA の関係は、親子関係のアルゴリズムである程度推定できるからである。津久井湖で発見された顔面の原形ととどめない遺体が、7 ヶ月前に丹沢の道志川で濁流に流された青年と同一人物であることは、母親と兄から採取した DNA の照合により判定された。また、2004 年末のスマトラ沖地震の際には、被害者の身元確認のため、わが国からも DNA 鑑定の専門家チームが被災地に派遣された。

わが国では、警察庁が、事件現場に犯人が残した血液や体液などの DNA 型情報のデータベースの運用を 2004 年 12 月 17 日より開始し、2005 年 4 月には「裁判所の令状を得て容疑者から採取した DNA について、指紋と同じようにデータベース化に踏み切る方針を明らかにした」と報じられている。

第 3 章　認証モデル

(3-1)　バイオメトリック認証モデルの基本的な性質

(a)　認証と識別

1 章でも述べたが、認証とは、相手が意図した人であることを確認すること（なりすましを防ぐこと）であり、セキュリティを実現するうえで、必要不可欠な技術である。

① 本人の所有物による認証

磁気カードや IC カードを用いた認証である。携帯性や操作が容易などの長所がある反面、盗難、偽造の危険性がある。

② 本人が持つ知識による認証

パスワードなどを用いた認証である。直接盗まれることがない、簡易な手段で実現できるという長所がある反面、本人が忘れる、パスワードが盗まれるなどの危険性がある。

③ 本人の身体的、行動的特徴による認証

個体の持つ特徴を用いた認証である。記憶、所持などが不要であり利便性が高いが、認証のための

特別な装置、高度な処理ソフトウェアが必要である。

どの認証方式が優れているかは一概にはいえないが、個人を同定できる究極の方式としてバイオメトリック認証技術が注目されている。認証技術において類似した言葉として、認証、識別やウォッチリストがある。以下に言葉の定義を簡単に述べる。

(i) **認証(verification)**： 提示されたユーザ名が本当にその人のものであるかどうかを確認すること。検証という場合もある。

(ii) **識別(identification)**： 主に法執行機関が使う利用方法である。つまり、提示されたバイオメトリックサンプルが含まれている可能性の高い包括的なサンプルデータベースが必要となる。このサンプルデータベースの登録件数が多ければ多いほど、効果的な識別システムとなる。例えば、警察関係の AFIS(Automated Fingerprint Identification System)が相当する。識別においては、他人受入れ誤差よりも本人拒否率を優先する。AFIS における識別機能を Positive Identification とも呼ぶ。

(iii) **ウォッチリスト(watch list)**： 識別の一種であり、提示されたバイオメトリックサンプルの所有者がこのデータベースに登録されているか判別する。例えば、政府の福祉サービスにおいて、受給対象者の重複防止確認などがある。このような福祉サービスシステムにおける識別機能を Negative Identification とも呼ぶ。

方法 / 要件		本人の所有物	本人の知識	本人の身体的特徴
		磁気カード、ICカード、証明書など	パスワード、電子署名	身体的(指紋、虹彩)、行動的(署名、声紋)特徴
安全性	●照合制度が高く、認証が確実 ●偽造、盗難などによる悪用が困難 ●無害 ●経年変化しない	●紛失、盗難、偽造のおそれあり	●忘失のおそれあり ●パスワードの管理方法によっては、第三者に盗難	●精度の比較的高いものがある
経済性	●費用が保護すべき利益に見合う	●ICカードは将来低価格化	●記憶によるので無償	●現時点では他の方法に比べ高価 ●適用対象に合わせ選択
簡便性	●操作が簡単 ●認証時間が早い ●携帯性がある	●ICカードなどを読み取り装置への挿入	●キーボードなどにより文字、数字を入力	●登録に時間を要する
社会的受容性	●違和感、抵抗感を感じさせない	●通常の社会生活で行われている行為	●通常の社会生活で行われている行為	●指紋は抵抗感があるなどの問題あり

図 14　本人認証の方法と生体認証製品の導入基準

(3-2)　基本的な性質

本人認証に利用されるバイオメトリクスは、以下の性質を持つ必要がある。

① **普遍性(universality)**： 誰もがもっている特徴である。

② **唯一性(uniqueness)**： 万人不同。本人以外は同じ特徴をもたないこと。

③ **永続性(permanence)**： 終生不変。時間の経過とともに変化しないこと。

現状のバイオメトリック認証技術では、上記の性質が経験的に実証されているものもあれば、かなりあいまいに使われているものもある。装置で処理されるバイオメトリクスは、一般に短期および長期に身体の状況が変化している。また、身体情報を取得する場合の環境条件の変動があり、数々の変動要因がある。例えば、声紋における、成長する上での声変わりや老化による声質の変化、センサの性能、伝送系の帯域、周辺ノイズなどにより、認証精度はかなり異なるといえる。

声紋認証の精度には、話者による大きな偏りがあり、誤認識の分散がきわめて大きい、一部の話者によって全体の認証性能が決まってしまうことがよく知られている。このような現象は、”Sheep and Goats 現象”と呼ばれる。話者による誤認識率の違いがカタログ値の 10 倍にもなることがある実際のシステムでは、全話者の平均値だけでなく、認識が特に難しい話者の誤認識がどの程度おさえられるかが重要である。

特殊な話者を次のように呼び、これらの話者を統計的に検出する方法が研究されている。

(i) **Sheep(羊)**： 誤認識の少ない大多数の話者。

(ii) **Goats(山羊)**： 誤認識のきわめて大きい一部の話者。

(iii) **Lambs(子羊)**： 他人が真似しやすい声の話者。

(iv) **Wolves(狼)**： 他人の声の真似が得意な話者。

Sheep(羊)は最も問題のない話者で、通常、話者集団の大部分を占める。実験に用いた話者数が少なくて、たまたまこのような話者だけから構成されていると、思いのほかよい認識率が得られることになる。ところが実験の規模を拡大していくと Goats(山羊)が含まれるようになり、話者数としてはわずかな割合であっても、平均認識率を大きく下げる。同じ日の声の比較では大きく変動しない、静かな理想的な環境では大きな変動がない、あるいは、変動が顕著に現れないので、実用を目指した実験では注意が必要である。さらに、本人の音声を拒否しないように、しきい値をゆるく設定すると、他人の音声を拒否しないように、他人の音声を受け入れやすくなってしまうので、なんらかの対策が必要になる。

Lambs(子羊)は Goats(山羊)に対するしきい値をゆるめることによって生じるのが一般的であり、Goats(山羊)と同じ話者になることが多い。Wolves(狼)に対する認証精度への影響はさらに研究が必要である。声帯模写者でも声の質をそっくりに真似することは難しい。主として話し方のくせを真似しており、声の質に関する特徴を用いている声紋認識システムには影響が少ない。このため、プロの声帯模写者がコンピュータによる声紋認識を容易に破れることはないと考えられる。声紋認証だけでなく、同様の行動的特徴を用いる動的署名認証などに関しても上記の考えを適用できる。

(3-3) パスワードモデルとバイオメトリック認証モデルの比較

本人認証の代表的な方法であるパスワードとの比較でバイオメトリック認証技術の問題点について述べる。

パスワードモデルにおける認証は、キーボードからのデータ入力と事前に登録したパスワードの文字（数）列との比較により行う。パスワードモデルにおける誤差要因としては、入力時における勘違いやタイプミスがある。判定は入力されたデータと蓄積パスワードとの文字列判定で行われる。したがって、誤差はいくつかの文字が一致しない場合に生じる確定的なものである。

一方、バイオメトリック認証モデルにおける認証は、センサからのデータ入力、特徴抽出などの前処理の後、事前に登録しておいた身体情報（テンプレートデータという）との照合処理により類似度を算出する。類似度とは入力データがテンプレートデータにどれだけ似ているかを表す。特徴空間での尺度である類似度が、事前に設定したしきい値以上の場合は一致、以下の場合は不一致と判定する。

バイオメメトリクスによる認証は、1 次元（例えば、声紋）あるいは 2 次元データ（例えば、指紋）の入力データに対するパターンマッチング処理が基本であり、これに起因する統計的な誤差が生じる。例えば、入力装置において、入力における環境条件、つまり、人間の身体的（例えば、指の湿気具合）もしくは行動的な変化（例えば、かぜをひいたときの声質の変化)、特徴抽出においては、入力データに対するアルゴリズム対応性（例えば、声紋において、どの程度の周辺ノイズが対応可能か）に起因する誤差、照合判定においては、設定するしきい値により、たとえ同一人物が入力した場合でも、結果が同じになることは保証できない問題がある。

① データ入力機能

ユーザが提示した身体情報をシステムに取り込む入力センサ機能。

② 特徴抽出機能

特徴抽出機能は、前処理機能と特徴抽出機能に分ける場合もある。

(i) **前処理**： システムに取り込んだ身体データから、判定処理に不要な環境要因の除去処理や保管したテンプレートとの比較判定を効率よく行うために、空間的位置や大きさ、時間的な変化などを正規化する処理。

(ii) **特徴抽出**： 前処理により、環境要因の除去、正規化を行ったデータより、判定処理に必要な個人の特徴を抽出する処理。

③ 判定機能

登録テンプレートデータと入力データの特徴量の類似性を照合比較し、所定の判定水準を超えたが否かで、本人であるか他人とみなすかの同定を行う処理。判定水準の決定はアプリケーションにより異なり、ポリシーの元に決定するしきい値でコントロールされる。

③ 登録データ保管機能

本人認証を行う者の身体データの特徴量の形で事前に特徴抽出処理し、システムに保管しておく機能。認証機能として重要なのは項目②の特徴抽出機能であり、同一の身体情報を用いた認証技術であっても複数の方法（アルゴリズム）が存在する。また、項目③の判定基準（しきい値）の設定には、実際の運用ノウハウが必要であり、性能を決める重要な因子である。

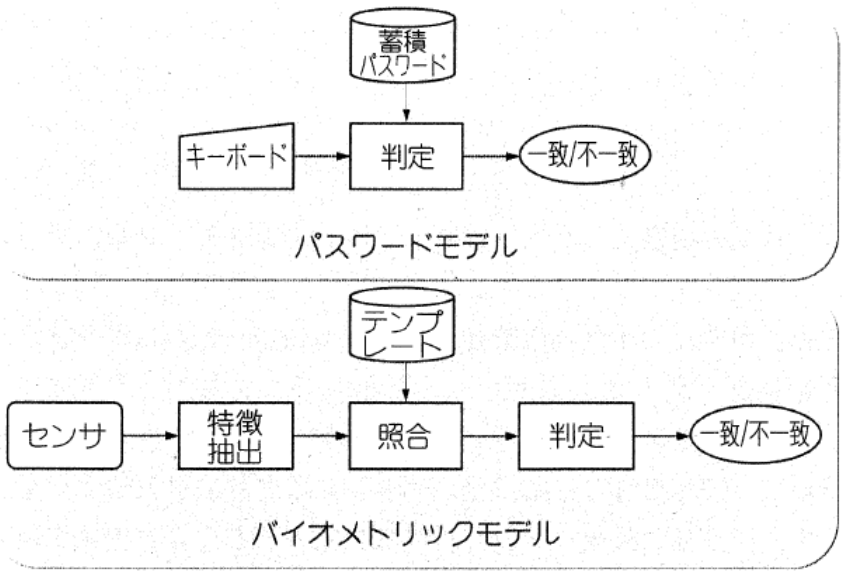


図 15　認証モデルの比較

(3-4)　サーバ認証モデルとクライアント認証モデル

(a)　サーバ認証モデル

バイオメトリクスは集中管理し、検索エンジンを用いて高速認証するモデルである。登録および認証のフローを簡単に述べる。

① 登録処理

(i)　センサで入力したバイオメトリクスと氏名などの個人情報を認証サーバに転送する。

(ii)　認証サーバで与信を行う。

(iii) 与信の結果、問題ない場合は、個人情報、ID 情報、特徴量を登録する。登録した特徴量をテンプレートとする。

② 認証処理

(i)　クライアント端末より ID 情報およびセンサで入力したバイオメトリクスを認証サーバに転送する。

(ii)　認証サーバで転送されたデータの認証処理を行う。

(iii) 認証結果が妥当ならばアプリケーションを駆動する。

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の間におけるデータ転送は、機密性および完全性の観点から暗号化およびデジタル署名処理を行う。本件はクライアント認証におけるデータ転送でも同様に必要である。サーバ認証方式のメリットは、クライアント端末の処理負荷の軽減およびコストの削減にある。一方、デメリットは、利用者が多くなった場合、ネットワーク負荷およびサーバ負荷が大きくなる。また、個人情報の一括管理を行うため、その管理体制が重要となる。

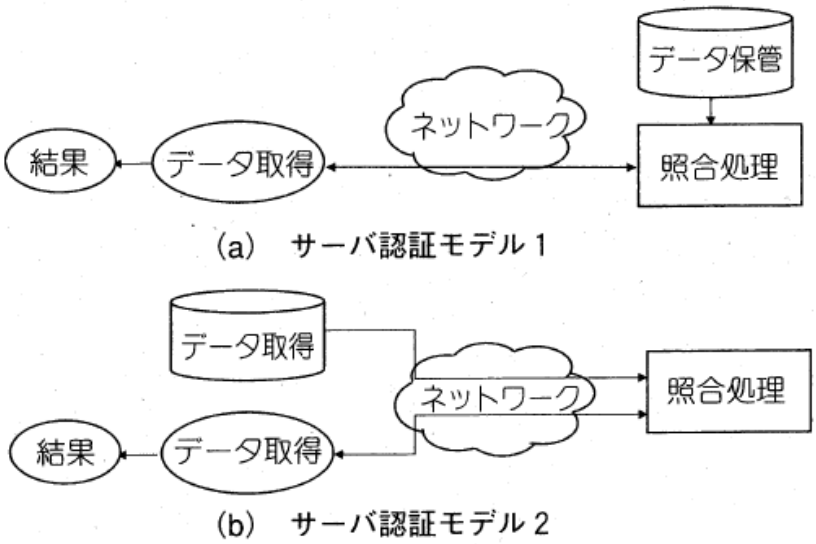


図 16　サーバ認証モデル

(b)　クライアント認証モデル

例えば、IC カード内にバイオメトリクスを管理し、端末側で IC カードの利用者認証を行うモデルである。登録および認証のフローを簡単に述べる。クライアント認証モデルは認証結果を端末側で管理するため、アプリケーションの駆動はクライアント端末から行うのが基本である。

①　登録処理

(i)　センサで入力したバイオメトリクスと氏名などの個人情報を認証サーバに転送する。

(ii)　管理サーバで与信を行う。ここまでは、サーバ認証モデルと同じであるが、以下の処理が異なる。

(iii) 問題ない場合は、テンプレートをクライアント端末に転送し、クライアント端末で保管する。個人情報、ID 情報、特徴量はシステムの安全性を確保するため、管理サーバで保管する。テンプレートデータには、認定された管理サーバで特徴抽出した旨の情報を埋め込む。また、テンプレートはクライアント端末の中、例えば、PC のハードディスクに保管する。より高セキュリティに管理する場合は、IC カードなどの耐タンパ性のある媒体に保管する。

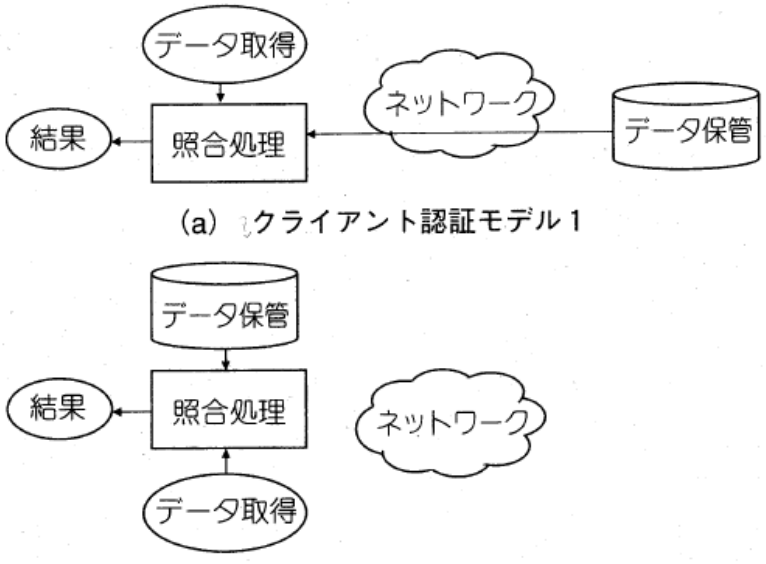


図 17　クライアント認証モデル

② 認証処理

(i) クライアント端末のセンサで入力したバイオメトリクスをクライアント端末で処理する。この場合、利用するテンプレートが正しい管理サーバで管理されたものであるか、管理サーバに問い合わせることも有効である。

(ii) 認証結果が妥当ならばアプリケーションを駆動する。

クライアント認証方式のメリットは、認証サーバを設ける必要がなくコスト低減と、個人情報は個人で管理するという利用者の受容性が高い点にある。また、バイオメトリクスが盗難にあっても、システム全体に波及しないメリットもある。一方、デメリットは、クライアント端末の処理負荷が高く、端末コストが高くなる点にある。

どちらのモデルが優れているかは、一概にはいえないが、利用者受容性、脅威対抗性、システム構築のしやすさなどを考慮し、アプリケーションごとに導入の際、評価する必要がある。

(3-5) IC カードと連携した認証モデル

アプリケーションから IC カードの正当性を認識するためには、暗号技術を用いた認証方式で行う。しかし、これは IC カードや端末の正当性を認証するもので、IC カードの所持者の正当性を確認していない。このため、IC カードの所持者の認証は身体情報を用いて行う。つまり端末から IC カードの正当性の認証、IC カードから持ち主の正当性の認証、2 段階の認証構成を採用している。身体情報を用いた IC カード持ち主認証技術の実現方法は国際標準の対象であり、ISO 7816-11 の標準規格が審議されている。

(a) Store On Card (SOC)

Stored Template 型とも呼ばれる。テンプレートを IC カードに保管しておき、テンプレートに新たに入力した指紋を IC カードの外部処理装置（例えば、PC）で照合する。電子パスポートなど社会 ID タイプのシステムに適用される。

(b) Match On Card (MOC)

Embedded Process 型とも呼ばれる。テンプレートの保管および照合処理を IC カード内で行う。このためテンプレートデータが外部に漏れないため、安全性の高いシステムを構築できる。

(c) All On Card (AOC)

MOC と同じくカード上で判定する。テンプレートデータが外部に漏れない安全な方式である。また、バイオメトリック入力センサもカード上に実装され端末の構築負荷が軽減されるが、IC カード自体のコストがかかるのと、センサ電源の供給などの問題があり、実用的とはいえない方式と考える。

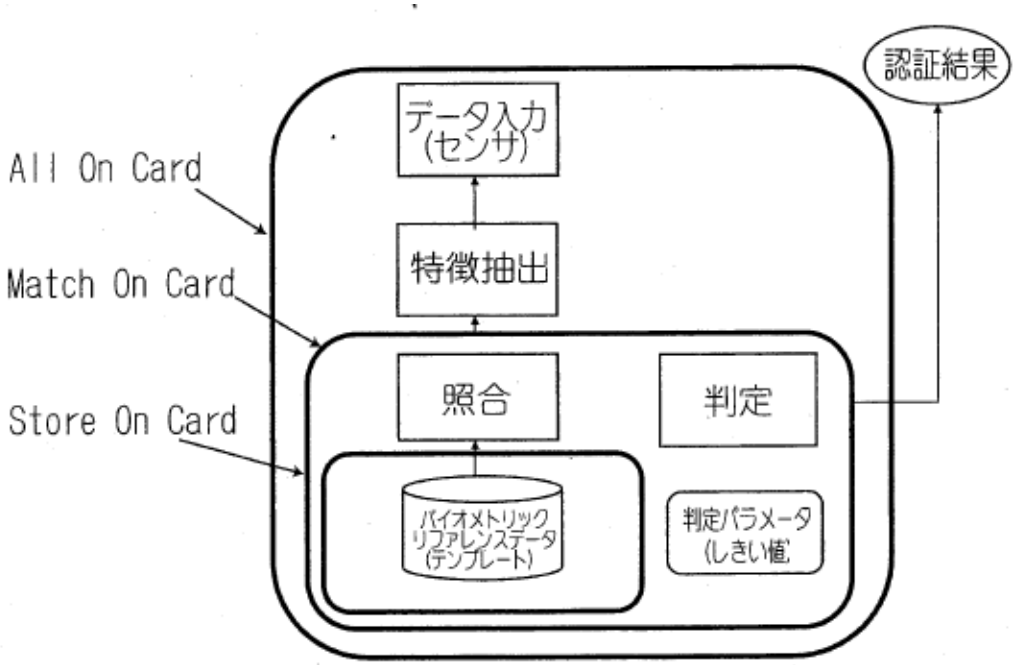


図 18 IC カードへの実装スキーム

(3-6)　バイオメトリック認証の誤差とは

バイオメトリック認証においては、有意性検定法における誤差(エラー)で定義される。

- タイプⅠエラー（本人拒否率）
- タイプII エラー（他人受入れ率）

タイプⅠエラー（本人拒否率）が高いと利用者はフラストレーションを引き起こし、タイプII エラー（他人受入れ率）が高くなると詐欺を引き起こす。タイプII エラーはタイプⅠのエラーに比べ1桁から2桁小さくするのが一般的である。

指紋による本人認証の誤差を例に述べる。ここでは指紋による本人認証の例を用いた2つの分布は、それぞれ同一のデータを照合した場合と、異なるデータを照合した場合の類似度分布を示す。類似度は右にいくほど大きくなる。これは、比較する2つのバイオメトリック認証における特徴量が一致している度合いが増えることを意味する。2つの類似度分布曲線が重ならず、しきい値を重なりのないところに設定すれば、原理的に誤差はゼロになるが、現実には重なり合うことが多い。このため認証誤差が生じる。同一指紋同士を照合した場合の類似度分布 hg が却下される場合、つまり、分布 hg,r に相当する値を本人拒否誤差（あるいは本人拒否率）FRR(False Reject Rate)、異なる指紋同士を照合した場合の類似度分布 hi が受理される場合、つまり、分布 hi,a に相当する値を他人受入れ誤差（あるいは他人受入れ率）FAR(False Acceptance Rate)と呼ぶ。本人拒否率 FRR は、有意性検定におけるタイプⅠエラー、他人受入れ率 FAR はタイプII エラーに相当する。

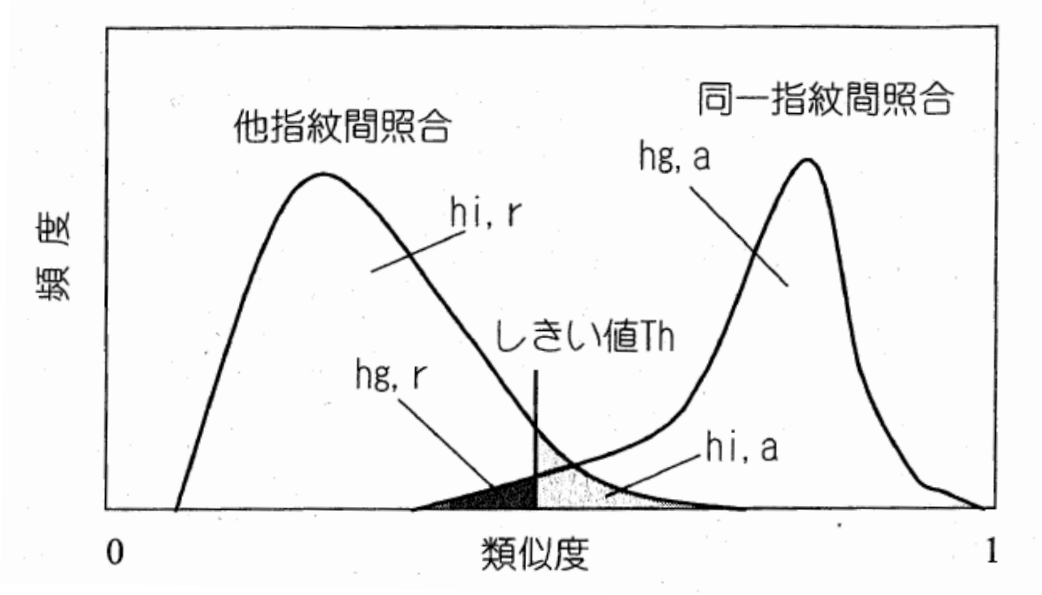


図19　認証における2つの誤差

バイオメトリック技術をセキュリティの分野に展開する場合、パターン認識における誤差だけでなく、セキュリティ的な強度を明確にする必要がある。バイオメトリクスに関するセキュリティ強度は暗号技術などで使われている総当り攻撃に対する情報空間で表すが、その方法としては次の2つがある。

(i)　FAR から算出する平均攻撃空間

(ii)　指紋特徴点への総当り攻撃

第4章　プライバシーとバイオメトリクス

(4-1)　情報源としての身体

近年、治安悪化や犯罪手口の高度化に伴い、バイオメトリクスが社会基盤における本人確認手段として活用され始めている。具体的には、9.11 アメリカ同時多発テロに端を発したホームランドセキュリティ分野での応用、日本国内における預金不正引き出し事件多発をきっかけとした金融分野での応用をあげることができる。

社会基盤における適切なバイオメトリクス応用は、社会の安全確保に寄与する一方、身体そのものを情報源として扱うため、プライバシー侵害や監視社会化に対する懸念を生じる。これは程度の差こそあれ、特定の組織内におけるバイオメトリクス応用でも同様である。

(4-2)　プライバシーの概念

日常生活において、「プライバシー」という言葉は「他人に知られたくない自分の私生活や秘密に関する情報」という意味で使われることが多い。そもそも外来語であるプライバシー（Privacy）は、1890年代にアメリカのWarren Brandeisによって発表された論文「The Right to Privacy」において、プライバシー権＝“the right to be let alone”（一人にしておいてもらう権利）として定義されたのが初めてといわれている。この定義は、放っておかれることによって自分の私生活や秘密を公開されるのを防ぐという消極的な概念といえる。

プライバシーの概念も時代とともに変遷してきた。1967年にはWestinが著書「Privacy and Freedom」において、”individual’s right to control the circulation of information relating to oneself”（自己に関する情報の流れを管理する個人の権利）と定義している。情報化社会の進展とともに、多量の個人情報が電子データとして蓄積され、ネットワークを介して簡単にアクセスすることが可能となった現在、いわば放っておかれることは困難であり、「自己情報コントロール権」と呼ばれるWestinの定義が一般的となっている。

プライバシー権およびその概念に関する詳細について知りたい人は、例えば、参考文献を参照されたい。

(4-3)　バイオメトリクスとプライバシーの関係

バイオメトリクスとプライバシーの関係については、以下の2つの側面から論ずる必要がある。

(a)　プライバシー保護技術としてのバイオメトリクス認証利用への期待

個人情報にアクセスする際の認証手段として、アクセス履歴の証跡性、否認防止の観点で効果が期待できる。

(b)　データ主体に対するプライバシー保護の必要性

バイオメトリック情報そのものが下記に列挙する特性を有する、ある意味、究極の個人情報であるため、プライバシー保護技術などの技術面と、プライバシー原則や法規制による制度面という両面からの厳格な保護が必須となる。

①　取替不能

PINやカードの盗難紛失時には、何回でも再設定/再発行することが可能であるのに対し、バイオメトリクス情報は身体的な特徴ゆえに、そのようなことはできない。指紋は他の指で代用することができるもののその回数は有限である。

また、バイオメトリクス情報の漏洩により、そのデータ主体になりすまし可能な人工バイオメトリクスが作成される可能性が否定できない。

②　強力な個人識別能力

目的外利用により、データ主体が不利益を被る可能性がある。気づかずに漏洩したバイオメトリクス情報から人工バイオメトリクスが作成され、なりすましが行われた場合、否認が困難となる。

③　同意なき情報取得が可能

顔などのいくつかのモダリティは、本人の同意および本人への通知なく情報取得が可能であり、行きすぎた監視や行動追跡応用への懸念が生じる。

④　副次的情報抽出が可能

人種情報、病歴、健康状態といったセンシティブな個人情報に分類される副次情報が抽出される可能性がある。

(4-4)　バイオメトリクスのプライバシー侵害に対する潜在リスク

データ主体に対するプライバシー侵害のリスクは、データ主体が提供する情報の機微度合・受け手・利用法の影響を受ける。Adamsによるプライバシーモデルはマルチメディアコミュニケーションを対象に検討されたものであるが、バイオメトリクスの利用・運用形態による潜在リスク評価を検討するうえでも有用である。

(a)　OECD

OECD(Organization for Economic Cooperation and Development)が1980年に採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」は、8原則から構成されている。本勧告は、各国におけるプライバシー保護の法的根拠の拠り所となっているものであり、近年のバイオメトリクスに関する各種規約に対するベースになっている。

(b)　IBIA

IBIA(International Biometric Industry Association、本部：ワシントンDC)は、1999年に4項からなるバイオメトリクスに関するプライバシー指針を公開した。

① バイオメトリックデータに関する指針

バイオメトリックデータは個人情報から分離・区別された電子符号とし、データ誤用や本人または司法当局の同意なきデータ公開の防止確保が必須。

② 民間部門に対する指針

データの収集・保存・アクセス・利用・目的外利用に対する明示的なポリシー開発を推奨。

③ 公的部門に対する指針

データの収集・保存・アクセス・利用に対する要件を定める明確な法的基準の規定が必要。

④ 官民両部門に対する指針

バイオメトリクスDBの秘密性および完全性保持のための適切な運用および技術的管理的手法の適用。

原　則	ポイント
収集制限の原則	適法かつ公正な手段で収集。 妥当な場合には，データ主体の同意を得る。
データ内容の原則	利用目的に沿った内容で，利用目的に必要な範囲内で正確，完全，最新に維持。
目的明確化の原則	収集目的を，収集時以前に明確化。 収集後のデータ利用は，当該目的に限定。
利用制限の原則	前項で明確化された目的以外の開示・使用の制限。ただし，データ主体の同意/法律規定がある場合を除く。
安全保護の原則	不正アクセス・破壊・使用・修正・開示などの危険に対し，合理的な安全保護措置により保護。
公開の原則	開発・運用・方針の一般公開。 データの存在とデータ管理者連絡先へのアクセス手段。
個人参加の原則	データ主体(個人)に次の権利： 1）データ管理者が当該個人データを有しているかの確認。 2）自己に関するデータを遅滞なく明瞭に通知してもらう。 3）前2項が拒否された場合の理由確認および異議申立。 4）自己に関するデータへの異義申立およびその異議が認められた場合のデータ消去，修正，完全化，補正。
責任の原則	データ管理者には，上記諸原則実施のための措置に従う責任。

図20　OECD基本8原則

(b)　IBIA

IBIA(International Biometric Industry Association、本部：ワシントンDC)は、1999年に4項からなるバイオメトリクスに関するプライバシー指針を公開した。

① バイオメトリックデータに関する指針

バイオメトリックデータは個人情報から分離・区別された電子符号とし、データ誤用や本人または司法当局の同意なきデータ公開の防止確保が必須。

② 民間部門に対する指針

データの収集・保存・アクセス・利用・目的外利用に対する明示的なポリシー開発を推奨。

③ 公的部門に対する指針

データの収集・保存・アクセス・利用に対する要件を定める明確な法的基準の規定が必要。

④ 官民両部門に対する指針

バイオメトリクスDBの秘密性および完全性保持のための適切な運用および技術的管理的手法の適用。

(c) 欧州

① 先駆的取組み

プライバシー保護に関する関心の高いヨーロッパにおいては、データ主体の視点に立ち、プライバシーや法的課題に対する検討が早くから議論されてきた。1997 年にドイツ TeleTrust に組織されたバイオメトリクスに関する包括的な課題把握を目的とした WG のチェアマンは法律専門家であったとのことである。

また、1998～2002 年に同じくドイツで実施された BioTrust プロジェクトでは、TeleTrust、ベンダ、研究機関、ユーザ、消費者保護団体、プライバシーオフィサによる多面的な評価が実施され、プライバシーに関連しては、バイオメトリクスデータの誤用/悪用防止に関する勧告が策定された。

② BIOVISION

このような活動を背景に、2002～2003 年に欧州委員予算で実施されたバイオメトリクスに関する包括的な検討課題プロジェクト BIOVISION において、プライバシーベストプラクティスが策定された。このプライバシーベストプラクティスは、プライバシーを考慮し、強化するバイオメトリックシステムの使用法に関する最善策として、EU 各国の法制度のレビューや専門家へのヒアリング調査を経て策定されたものである。EU データ保護命令に基づく法的要件および提言として下記 9 項目が規定されている。

(i) データ提供者の同意のみに基づくデータ処理。
(ii) センシティブなデータ使用時の明示的同意。
(iii) 事前説明に基づく目的特化したデータ収集/使用。
(vi) データ提供者の同意の範囲内での第三者へのデータ提供。
(v) 司法判断による場合に限定した法執行機関へのデータ提供。
(vi) 取扱いデータに関するプライバシーポリシーの告知（セキュリティレベル、システムへのアクセス制限、バイオメトリックデータと他の個人情報との分離保存など）。
(vii) 精度維持のためのバイオメトリックデータの更新。
(viii) バイオメトリックデータ取扱いに関する監査当局への通知。
(ix) 監査当局による事前監査。

なお、プライバシーベストプラクティスはバイオメトリクス・セキュリティ・コンソーシアム(BSC)リーガル WG において和訳された。本和訳は、リーガル WG の 2004 年度報告書の付録として、BSC ウェブサイト上に公開されている。

③ ARTICLE 29-Data Protection Working Party

BIOVISION における検討を受け、EU データ保護指令に基づき設置された個人データ処理に関する個人保護に関する作業部会が、EU データ保護指令におけるバイオメトリック情報への適用方法の検討を実施した。この検討結果は 2003 年 8 月に公開されている。本文書において、ほとんどのバイオメトリックデータは個人データに該当するとされており、目的と均整性・適正収集とデータ主体への通知・合法的データ処理のための規範・事前検査・セキュリティ対策・センシティブデータ・唯一性・プライバシー強化技術の使用と行動規範といった観点からの検討結果が記載されている。

(d) アメリカ

アメリカの場合、ヨーロッパのような議論は存在せず、前述の IBG のような民間企業によるコンサルティングや、バイオメトリクスを導入する国防総省や国土安全省といった政府機関による検討が主となっている。なお、州法レベルではバイオメトリックデータの保護を規定している州が存在する。

① テキサス州

2001 年 9 月、バイオメトリックデータ保護に関する州法（559 章）が制定された。個人のバイオメトリック情報を保有する政府機関が、本人の同意なしに、その情報の売り貸しや開示を禁止しているほか、その漏洩防止に関わる義務が規定されている。

② ニュージャージー州

2002 年 6 月に制定された州法は、テキサス州法と同種の法律であるものの、対象が政府機関のみならずバイオメトリック情報を保有するすべてのものを対象とし、さらに違反者に罰則が規定されている点で、より厳格な法となっている。

(e) 日本の状況

わが国では 2004 年 4 月 1 日より個人情報保護法が施行された。本法 2 条 1 項において、個人情報を

「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述などにより特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることになるものを含む）」と定義している。法律専門家による解釈ではないものの、本定義のもとでは、多くのバイオメトリック情報は個人情報に該当すると考えるのが自然であろう。

個人情報保護法の施行に伴い、個人情報やプライバシーに関する関心が高まりつつある。「バイオメトリクスプライバシー」という 2 つの単語を google などの検索サイトに入力して検索してみると、バイオメトリクスとプライバシーに関して論じられたニュース、団体などの意見、プログ上での個人的な見解が多くヒットすることがわかる。このヒット数は 2 年前に検索したときとは格段の違いである。中には、取替え不能な情報であるがゆえにリスク、同意なき二次利用やファンクションクリープを懸念する意見など、ネガティブな意見が含まれているのも事実である。

引用文献:「よくわかるバイオメトリクスの基礎」（一社）日本自動認識システム協会編　オーム社
引用文献:「これでわかったバイオメトリクス」（一社）日本自動認識システム協会編　オーム社
引用文献:「バイオメトリクス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
参考文献:「自動認識システムの基礎知識」（一社）日本自動認識システム協会編　オーム社
参考文献:「生体認証技術」 瀬戸洋一著　共立出版
参考文献:「ユビキタス時代のバイオメトリクスセキュリティ」 瀬戸洋一著　日本工業出版
参考文献:「バイオメトリクスセキュリティ入門」 瀬戸洋一著　ソフトリサーチセンター（SRC）
参考文献:「バイオメトリクスの本」 明石正則監修　日刊工業新聞
参考文献:「人の生物的特徴を用いた免疫系ネットワークセキュリティ」 溝口文雄共著　日刊工業新聞
参考規格:ISO/IEC 19794-1 Biometrics Data Interchange Format – Part1 Framework
参考規格:ISO/IEC 19794-2 Biometrics Data Interchange Format – Part2 Finger Minutiae Data
参考規格:ISO/IEC 19794-3 Biometrics Data Interchange Format – Part3 Finger Pattern Spectral Data
参考規格:ISO/IEC 19794-4 Biometrics Data Interchange Format – Part4 Finger Image Data
参考規格:ISO/IEC 19794-5 Biometrics Data Interchange Format – Part5 Face Image Data
参考規格:ISO/IEC 19794-6 Biometrics Data Interchange Format – Part6 Iris Image Data
参考規格:ISO/IEC 19794-7 Biometrics Data Interchange Format – Part7 Signature/Sign Behavioral Data
参考規格:ISO/IEC 19794-8 Biometrics Data Interchange Format – Part8 Finger Pattern Skeletal Data
参考規格:ISO/IEC 19794-9 Biometrics Data Interchange Format – Part9 Vascular Image Data
参考規格:ISO/IEC 19794-10 Biometrics Data Interchange Format – Part10 Hand geometry silhouette Data
参考規格:ISO/IEC 19794-11 Biometrics Data Interchange Format – Part11 Signature/sign processed dynamic Data
参考規格:ISO/IEC 19794-13 Biometrics Data Interchange Format – Part13 Voice Data
参考規格:ISO/IEC 19794-14 Biometrics Data Interchange Format – Part14 DNA Data