IMES DISCUSSION PAPER SERIES

バイオメトリックスによる個人認証技術の現状と課題

―― 金融サービスへの適用の可能性 ――

なかやま やすし　こまつ なおひさ
中山靖司・小松尚久

Discussion Paper No. 99-J-43

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

IMES Discussion Paper Series 99-J-43
1999 年 11 月

バイオメトリックスによる個人認証技術の現状と課題

――金融サービスへの適用の可能性――

なかやま やすし　　こまつ なおひさ
中山 靖司[*1]　　小松尚久[*2]

要　旨

本稿は、バイオメトリックスによる個人認証（バイオメトリック認証）について、金融サービスへの適用を想定しつつ、その概要、研究開発動向、標準化動向、安全性評価、実用化事例等を紹介したものである。

近年、情報技術の進展によって、金融サービスのほとんどはコンピュータ・ネットワーク・システムによって提供されるようになってきており、利用者がインターネット等を通じて自宅のパソコンからサービスを受けることも可能になってきている。ネットワークを介してサービスを提供する場合には、サービスを受けようとしている相手の真正性を確認することが重要である。しかしながら、キャッシュカードと暗証番号の組合せなど、既存の金融サービスで用いられている一般的な本人確認方法は、安全性の面から必ずしも確実な手段とはいえず、多くの課題を抱えている。そこで、安全で確実に本人を確認する手段として、バイオメトリック認証が注目されている。

バイオメトリック認証とは、対象者の身体的特徴（指紋、網膜等）や身体的特性（筆跡、音声等）などの対象者個人に固有の情報を予め計測してシステムに登録しておき、取引の都度測定する本人の特徴・特性が登録データと合致するかどうかによって相手の真正性を確認する方法である。バイオメトリック認証は、本人であることを証明するために何かを携帯したり、暗証番号を記憶する必要がなくなる可能性もあり、利用者にとって利便性が高いほか、既存の個人認証方式よりも高度なセキュリティを実現することが期待できる。現在、多くの産業分野で実用化が進みつつあるが、金融取引の安全性を高める手段としても検討に値する認証技術と考えられる。

キーワード：　バイオメトリックス、バイオメトリック認証、個人認証、個人識別、
金融サービス、標準化、認証モデル
JEL Classification: L86, L96, Z00

*1 東京大学 先端経済工学研究センター（E-mail: nakayama@aee.u-tokyo.ac.jp）
*2 早稲田大学 理工学部 電子・情報通信学科 （E-mail: komatsu@kom.comm.waseda.ac.jp）

本論文は、1999 年 11 月 1 日に日本銀行で開催された「第 2 回情報セキュリティシンポジウム」への提出論文に加筆・修正を施したものである。

目　次

頁

1. 金融サービスと個人認証の関わり――ネットワークにおける個人認証

近年、情報技術の進展によって、金融サービスのほとんどはコンピュータ・ネットワーク・システムによって実現されるようになってきている。銀行の勘定系システムに専用のネットワークで繋がっている ATM（現金自動受払機）を用いて、現金の受払、振込／振替、残高確認等の銀行取引機能が提供されるようになって久しい。商店での買い物に使用されるクレジットカードやデビットカードの決済サービスも、専用のネットワークによってカード会社や金融機関に接続された端末を介して提供されている。また、最近では、公衆電話回線やインターネットを介して自宅のパソコンや携帯電話を銀行のシステムに接続することにより、現金の受け払いを除いた銀行の一般的なサービスを受けることができるようになってきている。クレジットカードやデビットカードの決済サービスについても、インターネットを通じて自宅のパソコンから決済の指示を行うことが可能になってきている[1]。

このように、ネットワークを介してサービスを提供する時に重要なことは、サービスを受けようとしている相手の真正性を確認することである。ここでいう真正性とは、サービスを受けるためにあらかじめ契約を結んでいる本人に間違いないということである。キャッシュカードやデビットカードでは、取引を行おうとしている相手がカードを保持し、かつあらかじめ登録してある 4 桁の暗証番号を知っているということを ATM 等の機械で確認することによって、本人であると判断している。また、クレジットカードでは、カードを保持していることと、目の前でカードにあらかじめ記入されているのと同じ署名を行うことができることを商店が確認することによって本人確認を行う仕組みとなっている。

しかしながら、キャッシュカードは盗まれたり、不正に入手した口座に関する個人情報をもとに偽造されたりする可能性がある上に、暗証番号も現実には安全性よりはむしろ覚えやすさが重視されることが多く、60%以上の利用者が誕生日もしくは電話番号を当てはめているのが実態との調査結果（表 1）もあるなど、個人情報から容易に類推される危険性がある[2]。クレジットカードにしても、キャッシュカード同様に盗まれたり、偽造されたりする可能性があることに加え、商店における署名のチェックも実際にはあまり厳格には行われていないケースがある。さらに、これらの決済サービスが自宅のパソコン等からインターネットを介して使用される場合には、カードや署名の物理的な提示ができないため、カードの確認や署名の検証が行われず、口座番号と暗証番号あるいはカード番号と有効期限を送信するだけの確認となり、他人のカード情報を入手すれば容易に不正使用できてしまうのが実情である。このように、既存の本人確認手段は、特にオープンなネットワークでの利用においては、安全性の面から必ずしも安全で確実な手段とはいえず、多くの課題を抱えている。

---

[1] SET や SSL といった暗号を利用したプロトコルにより、インターネット上での利用を実現している。

[2] さらに、現金自動預け払い機（ATM）や小売店のデビットカード端末に偽造機が組み込まれ、口座情報とともに暗証番号が盗み見られることによって不正な引出しが行われる危険性もある。

（表 1）暗証番号の設定状況のアンケート結果

分野	人数	うちわけ	分野	うちわけ
誕生日	89 人 (46%)	工夫のない誕生日　53 人 誕生日をアレンジ　14 人 家族の誕生日　10 人 他人の誕生日　12 人	その他	2001　映画のタイトル（1941 も） 1568　身長 156.8cm だから 4789　名前画数。木村拓也 4 画 7 画 8 画 9 画 1425　カードを作った時刻 14 時 25 分 3612　番地。3 丁目 6 番 12 号 1789　フランス革命 1467　人の世むなし応仁の乱 1134　文化放送 0101　丸井 0480　民法 480 条（受取証書持参人への弁済） 1326　タンピンツモドラ 1 でイチサンニンロク 4147　西武の渡辺久信 41 と工藤公康 47 1777　昔交際のあった友人が使っていた番号 7777　気分で 2222　意味なく 1234　母に薦められ
電話番号	34 人 (18%)	自宅　17 人 実家　11 人 彼／彼女　3 人 その他　3 人		
受験番号 出席番号	7 人(4%) 5 人(3%)	入試、模試の受験番号 3419　3 年 4 組 19 番		
語呂合わせ	13 人 (7%)	4126　ヨイフロ（4 人） 1168　ビビンバ 2180　ニイハオ 0909　ワクワク 0439　与作 3594　三国志 0168　イロハ 9602　苦労人　など		

出典：週刊文春 95 年 10 月 12 日号

2. バイオメトリック認証とは

(1) 端末＋ネットワークにおける個人認証

近年のコンピュータ・ネットワークの発展には目を見張るものがあり、特にインターネットにより、ネットワークの大規模化、オープン化に拍車がかかっている。例えば、1998 年度の我が国におけるインターネット人口は約 1,700 万人に達しており、前年度と比較して約 45%以上の伸びを示している。また、企業内のイントラネットの普及も急速な勢いで進んでおり、業務のネットワーク化、迅速化が進んでいる。こうしたネットワークの大規模化、高度化に伴い、情報提供あるいは商品の販売等さまざまなビジネスがネット上で展開されるようになってきており、コンピュータ・ネットワークは生活基盤のひとつとしてますます我々の社会生活に溶け込んでいくものと思われる。こうした状況の下で、情報の送受信者が本人であることを確認する個人認証の必要性は、以下の点からも高まってくるものと考えられる（表 2）。

（表2）個人認証のニーズ

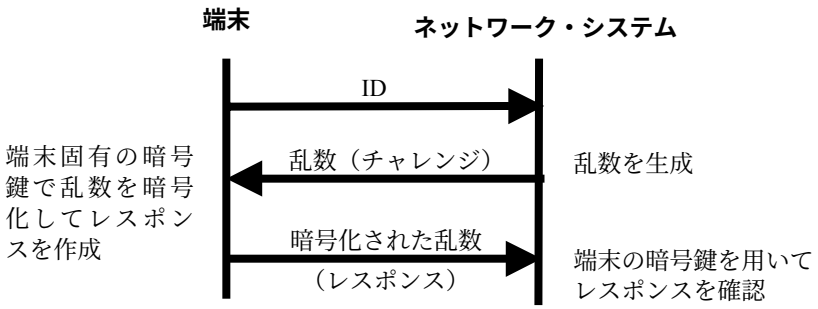
社会環境変化	社会環境変化に応じた社会・個人・企業の動向	システム化が期待できる分野	個人認証のニーズ
高齢化	•医療相談ニーズの拡大 •疾病者の在宅看護	•遠隔医療，遠隔健康管理 •疾病者監視（看護）	•医療情報の広域管理
国際化	•海外とのコミュニケーション増大（訪問・電話） •在日外国人の増加 •外国人雇用の増大（知識人・労働力） •海外事務所との遠隔会議 •国際分業化進展、物流、情報の拡大 •コンピュータシステム、オフィスの24時間利用	•テレビ会議 •海外情報提供 •自動翻訳 •グローバルネットワーク •エレクトリックコマース •24時間対応ビル入退管理	•課金（個人課金） •企業内データへのアクセス •リモートアクセス利用 者確認 •利用資格証明
キャッシュレス化	•電子マネー •カードの多様化・機能統合	•電子取引、電子決裁 •預金管理の統合	•カードの高機能化
コミュニティ化	•地域情報メディアの普及	•コミュニティ情報案内 •生涯教育	•個人情報のネットワーク管理 •サービス提供に関する決済
企業の組織構造の変化	•企業活動に関する情報管理の進展	•企業内情報伝達 •マルチメディア分散DB	•企業内データへのアクセス •利用資格証明
その他	•在宅選挙 •教育機関の連携、地域との結びつき •モバイルオフィスの普及	•電子投票 •遠隔教育 •テレワーク	•身分証明 •個人情報の管理

第 1 にネットワーク社会の進展が挙げられる。例えば、エレクトリック・コマースの普及とともにテレワークあるいは電子選挙が実現できる環境が整備される。ここでは、機密性、プライバシーの保護と課金の面からも端末とその利用者との対応を確認する必要性はさらに高まると考えられる。

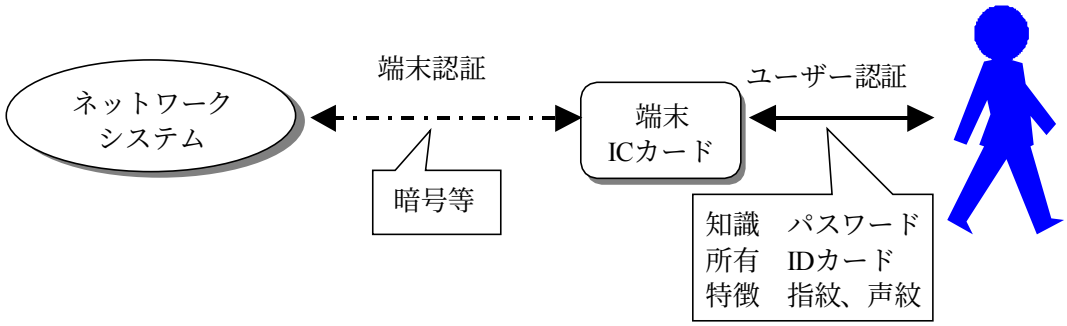
第 2 は高齢化社会の到来である。遠隔による医療診断および健康管理の必要性が高まるとともに、プライバシーに関する情報のアクセスおよび管理に対するシステムセキュリティは重要な課題となる。

普段我々が利用している端末＋ネットワーク・システムの身近な例としては携帯電話があるが、ここでもある種の個人認証が行われていると言える。現在、一般的に用いられているのは、チャレンジ／レスポンス型と呼ばれる認証方式である（図 1）。これはネットワーク側で乱数（チャレンジ）を生成して端末に送った後、端末は受け取った乱数にその端末しかできない処理（端末固有の暗号鍵による暗号化等）を施して返答する（レスポンス）ものである。ネットワーク側では、レスポンスの内容を確認することにより端末を認証する。なお、チャレンジとしては、乱数のほか、時間によって異なる値を取る情報（時刻情報等）が用いられる。

（図 1） チャレンジ／レスポンス型の認証方式



（図2）ネットワークにおいて端末を利用する場合の個人認証



一般にネットワークで端末を利用する場合の個人認証は図 2 に示すとおり、①ユーザーと端末（あるいはネットワーク）間（以下、ユーザー認証とする）、②ネットワークと端末間（以下、端末認証とする）の 2 段階に分けられる。先に例として挙げた携帯電話の認証は、使用している端末を確認するだけであり必ずしもユーザーを確認している訳ではない。したがって、端末の貸し借りはもちろん他人の端末を不正に入手して使用することも可能である。実際に端末を利用しているユーザーを特定するためには、ユーザー認証を組み入れる必要がある。なお、いわゆる CA (Certification Authority) による電子認証の仕組みは、ここでいう端末認証に相当し、ユーザーが秘密鍵を持ち運びできる IC カード等の媒体に格納して保持しているとか、他人がアクセスできないパーソナル端末のハードディスクに格納してあることを前提にすることによって始めてユーザー認証の機能を持つと考えることができる。

ユーザー認証の方法は、①本人所有によるもの、②本人知識によるもの、③本人固有の特徴によるもの、の大きく 3 つに分類することができる。「本人所有によるもの」は、鍵や ID カード等正当な本人しか持ち得ないはずの物を所有していることにより認証する方法である。鍵や ID カードが盗まれたり、複製が作られたりすると、第三者による成りすましを行うことが可能であるほか、本人が紛失する危険性もある。「本人知識によるもの」は、暗証番号やパスワード等正当な本人しか知らないはずの情報を示すことにより認証する方法であり、コンピュータ・システムのアクセス・コントロール等で使われている。ただし、他人が容易に想像できるようなパスワードを使用したり、うっかり他人に漏れたりすることによって、第三者に容易に成りすまされる危険性があるほか、本人が忘れてしまう危険性もある。「本人固有の特徴によるもの」は、指紋や声紋、筆跡等を計測し、正当な本人固有の特徴と合致するかどうかを確認することによって認証する方法で、本人固有の情報をどう捉えるかが成りすましに対する耐性に影響する。キャッシュカードの場合は、「本人所有によるもの」であるカードと「本人の知識によるもの」である暗証番号の 2 つのパラメータを組み合わせたユーザー認証を行っていると考えられる。

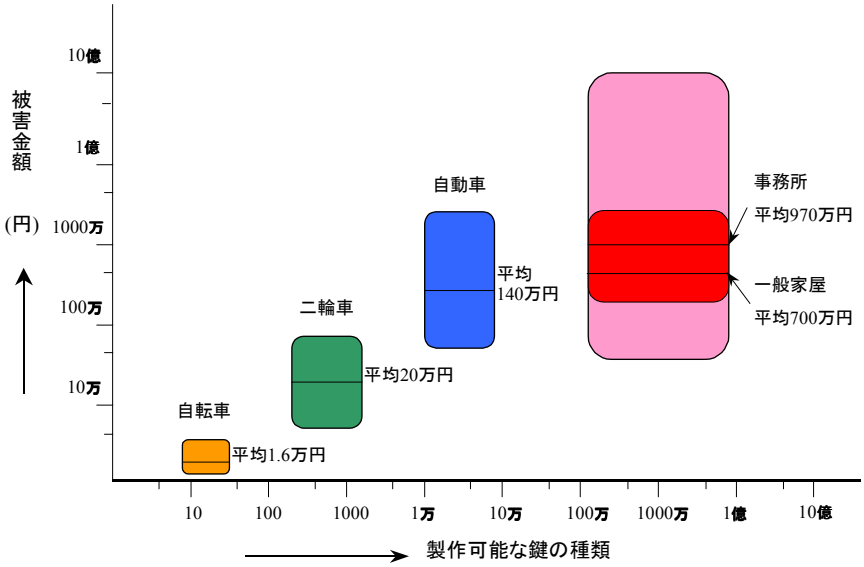
これらの様々な認証の方法は、システムで要求されるセキュリティのレベル、システムの処理量およびユーザーの許容度を考慮して、利用するパラメータの種類や形態を考えることが必要である。また、守るべき財産の額に応じてセキュリティ・レベルが高まることが考えられる。例えば、Miller [1994]は、コンピューター・センターにおけるアクセス領域に応じた個人認証技術の選択の例を示している（表 3）。この表は、センター内のアクセス領域のセキュリティ要請を財産価値に換算した上で、各々に適切と思われる個人認証手段を示したものである。この考え方は、我々が普段使用している鍵の種類（セキュリティ・レベル）と守るべき財産規模との関係と同じである。例えば、自転車、自動二輪車、自動車、家屋、といった財産について、そのセキュリティが侵害された場合に考えうる被害金額と、作成可能な鍵の値段とをプロットしてみると図 3 のようになるが、これは一般の人々が鍵を選択する際に、想定される被害金額の多寡に応じてセキュリティ対策のコストを増減させていることを示している。

（表 3）コンピューター・センターにおける個人認証手段の選択方法の例

アクセス領域	適切な個人認証手段	個人認証機能付きのゲート１個当りの設置コスト	守るべき財産の価値
一般エリア	IC カード	$400	$1000
コンピューター・ルーム	IC カード + パスワード	$600	$1,000,000
ネットワーク制御エリア	IC カード＋指紋	$5,000	$1,000,000,000

出典：Miller [1994]

（図3） 被害金額と製作できる鍵の種類（セキュリティ･レベル）



資料：機械統計年報等

(2) **本人固有の特徴を用いたユーザー認証**

本人所有および本人知識といった従来のパラメータを代替、あるいは補完するものとして、バイオメトリックス（biometrics）と呼ばれる本人固有の特徴を利用することが提案されている。バイオメトリックスは、身体的特徴（physiological characteristics）と身体的特性（behavioral characteristics）の 2 つに分類できる。身体的特徴の代表例としては指紋、網膜あるいは顔等が挙げられ、身体的特性の代表例としては筆跡、音声が挙げられる（表 4）。

（表 4）ユーザー認証の方法とパラメータ

<table>
<tr><td rowspan="2">認証タイプ</td><td rowspan="2">知識</td><td rowspan="2">所有</td><td colspan="2">個人の特徴（バイオメトリックス）</td></tr>
<tr><td>身体的特徴</td><td>身体的特性</td></tr>
<tr><td>パラメータ</td><td>暗証番号、パスワード</td><td>ID カード、鍵</td><td>顔、掌形、網膜、虹彩、指紋</td><td>筆跡、声紋、
キーストローク</td></tr>
<tr><td rowspan="2">ユーザー認証用データの比較処理方法</td><td colspan="3" rowspan="2">登録データ ⇔ 入力データ</td><td>（テキスト依存型の場合）
登録データ ⇔ 入力データ</td></tr>
<tr><td>（テキスト独立／提示型の場合）
登録時のデータ　　入力データ
↓　　↓
個人の特性 ⇔ 個人の特性</td></tr>
<tr><td>留意事項</td><td>忘れる危険性</td><td>遺失する可能性</td><td colspan="2">時間経過等により特徴が変わる可能性</td></tr>
</table>

さらに、筆跡、音声等の身体的特性には、何を書いても、あるいは何を言っても本人が特定できるという特徴が加わる。普段我々は、家族あるいは友人の筆跡や声だけで、誰であるかを判断できる場合が多い。すなわち、我々は無意識のうちに筆跡、音声から個人が特定できるパラメータを抽出し、その結果を利用して本人を特定しているのであろうと考えられる。このように、身体的特性を利用したユーザー

認証は、あらかじめ登録したテキストの内容にとらわれることのない柔軟性に富むマン・マシン・インタフェースを実現できる可能性がある。なお、この身体的特性の分類を拡張したものとして、本人の行動様式をパラメータとして認証を行う考え方も提案されており（安田[1999]）、さらなる技術と適用の拡大が期待できる。

Jain, Boille and Pankanti [1999]は、こうした身体的特徴、身体的特性が、①普遍性（universality：誰もが持っている特徴であること）、②唯一性（uniqueness：本人以外は同じ特徴を持たないこと）、③永続性（permanence：時間の経過とともに変化しないこと）の 3 つの条件を備えていることが理想的であるとしている。本稿では、こうした特徴を有する生体的な測定結果を用いた認証をバイオメトリック認証（小松[1998b]、小松[1998c]）と呼ぶことにする[3, 4]。

広い意味でのバイオメトリック技術を用いたユーザー認証は、研究とともに実用化が進められており[5]、金融の分野でも安全性をより高める手段として期待できるものである。ただし、身体的特徴を利用した認証も身体的特性を利用した認証も、あらかじめ登録した情報と入力した情報が等しいという結果をもって本人であることを確認する点が共通している。つまり、あくまでも登録した本人と同じであることを認証しているのであって、登録時に他人を騙って登録する不正があると以後の成りすましを防ぐことは不可能である。これは、本人所有および本人知識によるユーザー認証にも当てはまる特徴である。

(3) バイオメトリック認証の分類

バイオメトリック認証は、その認証プロセスの違い等の観点からも、いくつかの分類が可能である。

(a) 照合(verification)と識別(identification)

「照合」(verification)とは、指紋あるいは音声などのパラメータの種類には拠らず、入力された本人の特徴を示す情報と、ユーザーの ID 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。両者の情報の差があらかじめ設定した閾値以下であれば本人であると特定する。ユーザーは認証時に、自分の ID をシステムに入力する必要がある。一方、システムに入力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閾値以下の最も近いものを探す方法が「識別」（identification）である。ユーザーは認証時に、自分の ID をシステムに入力する必要はない。犯罪捜査における「指紋を登録した前科者リストからの容疑者の割り出し」が代表例として挙げられる。

---

[3] 海外の文献では biometrics, biometrics-based identification, biometric identification, biometric method 等の用語が使われている。国内でも特に決まった呼び方はないが、本稿では小松[1998b]で使用されている呼称を用いる。なお、最近の文献では、バイオメトリック本人確認、バイオメトリック個人認証といった用語も使用されている。

[4] バイオメトリック認証の定義については、The Biometric Consortium (http://www.biometrics.org/)に、"Automatically recognizing a person using distinguishing traits (a narrow definition)"とある。

[5] 研究の動向は Davis and Price [1989]、林[1986]を参照。

これらを一般論としてまとめたものとしては、Plamondon and Lorette [1989]（表 5）がある。同論文によれば、認証を行うシステムには、①あらかじめ本人に関する知識がない状態と、②既に知識を持っている状態の 2 種類の状態がある。またその分類法には、①特異性による分類（singular part）と、②意味論における分類（semantic part）の 2 通りが考えられる。特異性による分類によれば、本人に関する知識があらかじめない状態で本人の特定を目的とする場合が「識別」であり、あらかじめ知識がある場合が「照合」である。意味論における分類によれば、あらかじめ知識がない場合が「学習」、あらかじめ知識がある場合が「認識」ということになる。当然のことながら、認識するためには先に学習を行っておくことが必要である。

（表 5）識別と照合（学習と認識）

対象 ＼ 知識の形態	事前知識なし	事前知識あり
特異性による分類（singular part）	識別(identification)	照合(verification)
意味論における分類（semantic part）	学習(cognition or learning)	認識(recognition)

出典：Plamondon and Lorette[1989]

(b) **テキスト依存、テキスト独立とテキスト提示**

この分類は、身体的特性である音声あるいは筆跡を使った認証において使われるものである。

「テキスト依存型」とは、音声を例にすると、登録されたテキスト（音声の内容）と入力されたテキストが一致していることによって本人を特定する技術である。この技術は、テキストの内容を積極的に利用するものであり、登録と入力のテキストが異なる場合は本人の特定が不可能となるのが一般的である。例えば（手書きの）署名照合は、典型的なテキスト依存型の筆跡による個人認証方式である。これに対して「テキスト独立型」は、テキストの内容に依存せず、何を話しても、あるいは何を書いても本人であることを特定することが可能な技術である。例えば、裁判や犯罪捜査で利用される筆跡鑑定、声紋鑑定等は「テキスト独立型」の個人認証方式である。また、「テキスト提示型」はチャレンジ／レスポンス型の個人認証方式である。すなわち、システムの方から、テキストの発声あるいは筆記に関する指示（チャレンジ）を出し、その指示に対してユーザーがレスポンスを返すという方法である。前述のテキスト独立型の個人認証方式では、音声を録音すること等により第三者が特定の人物に成りすます危険性があるが、テキスト提示型の個人認証方式では、こうした成りすましを困難にするとともに、本人の特徴が現れ易いテキストをシステムが選択して提示することにより、信頼性の高い個人認証が実現できる可能性がある。

ところで、筆跡を例に、より安全性の高い個人認証を行うことを考えると、

F = 筆者間変動 / 筆者内変動

で定義される F-ratio と呼ばれるパラメータが大きいことが必要となる（保原[1989]）。筆者間変動（inter-writer variation）とは、個人ごとの筆記方法の相違、あるいは学習の過程で生じる習慣上の相違に依存する変動であり、本人と他人との特徴の違いに比例する値であることから、大きければ大きい程望ましい。一方、筆者内変動（intra-writer variation）は、疲労、情緒等に起因する変動であり、本人を正当でないとする過まった判断を行わないためにも、できる限り小さいことが望ましいといえる。

署名で個人認証を行う場合は、筆跡の内容（自分の名前もしくは記号）は一般的には異なっているため前述式の分子は大きく、また通常書き慣れているため筆者内変動は少なく分母が小さくなる傾向が出る。これは、テキスト依存型の手法の特徴とも言える。一方、テキスト独立型の手法では、何を書いても良いというヒューマン・インタフェースの向上は図れるものの、テキスト依存な手法ほど筆者内変動が小さくなることを期待することは困難と考えられる。したがって、テキスト依存型の手法と同様の安全性を確保するためには、さらなる技術的な課題を解決することが必要である。

(c) オフライン情報の利用とオンライン情報の利用

例えば、筆跡を用いた個人認証の場合、あらかじめ紙等に書かれた筆跡をもとに認証を行う方法が「オフライン型」であり、タブレット等から筆跡情報をリアルタイムに入力して認証を行うものが「オンライン型」である。オンライン型は、表 6 に示すとおり、オフライン型に比べて個人識別に利用できる情報をより多く含んでいる。また、全く同じ筆記データを再入力することができないなど、安全性を高めることが可能である。リアルタイム性を有するネットワーク・システムにおいては、オンライン型を使用することがコスト・安全性の両面から有利と考えられる。

（表 6）筆跡による個人認証におけるオンライン／オフライン情報

	オンライン情報	オフライン情報
入力装置	特殊な装置（タブレット等）	多種多様（スキャナ等）
筆記の安定性	かなり不安定	かなり安定
データの型[6]	3 次元の時系列	2 次元濃度値
筆速	情報あり	情報なし
筆圧	情報あり	情報なし
筆順	情報あり	情報なし
筆記時間	情報あり	情報なし
文字の幅	情報なし	情報あり
平面上の接続	情報なし	情報あり
同一データの再入力	不可能	可能

出典：吉村・吉村 [1996]

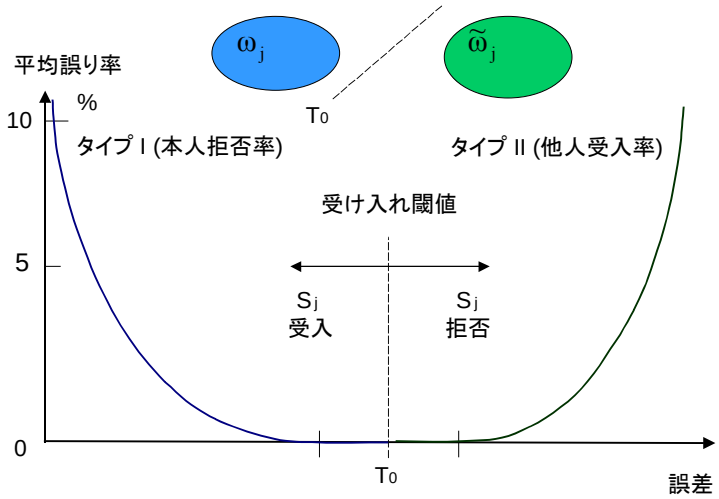
[6] オンライン型の筆跡認証では、タブレットから入力したペンの動きを 2 次元の座標データ＋筆圧の要素に分解して時系列情報として認識することにより、筆速、筆圧、筆順、時間等を利用する。一方、オフライン型では、紙に書かれた筆跡を 2 次元の画像データとして認識する。

(4) 認証時における誤りのタイプ

身体的な特徴あるいは特性を用いて本人を特定する場合、誤りの有無や程度をどう捉えるかは非常に重要なポイントの一つである。例えば、パスワードを用いた個人認証の場合は 1 ビットの誤りも許されるべきではない。この場合は、登録された情報と入力された情報との距離がゼロであることをもって本人であることを特定している。しかしながら、個人の特徴を用いたバイオメトリック認証の場合は、通常、登録情報と入力情報の距離がゼロとなることはあり得ず、入力時の条件に応じて距離が発生する。逆に距離がゼロの場合は、登録情報が不正に読み出されて使われている可能性を疑ってみる必要がある。したがって、入力された個人の特徴を示す情報と登録されている情報がどの程度似ているか、という観点から本人を特定せざるを得ず、統計的な取扱いが必要となる。そこで問題となるのが、タイプⅠ、タイプⅡという 2 種類の誤りである。タイプⅠの誤りとは、システムにアクセスしているのが本人であるにもかかわらずシステムがリジェクトする誤りである。一方、タイプⅡの誤りとは、他人に対して正しい本人であると判定してしまう誤りである。タイプⅠの誤りを犯す確率を本人拒否率（FRR: False Rejection Rate）、タイプⅡの誤りを犯す確率を他人受入率（FAR: False Acceptance Rate）という。

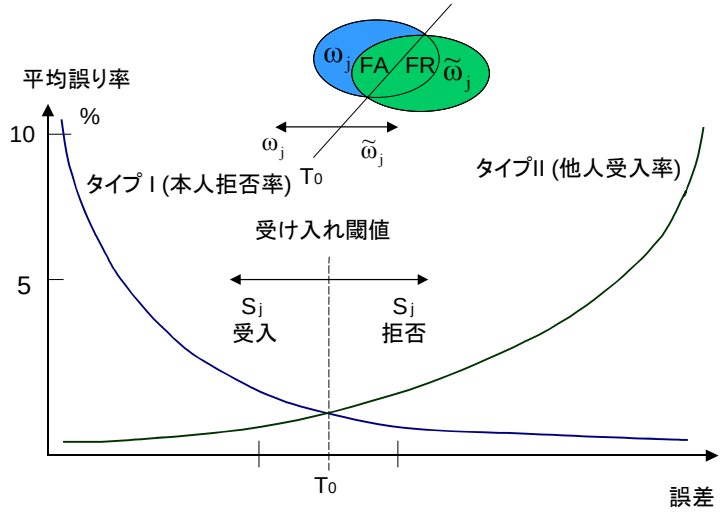
バイオメトリックス認証において理想的なのは、図 4 に示すように、本人の特徴の集合（ω）と、本人以外の他人の特徴の集合（ω̃）が全く独立に類似性なく存在しているような場合である。この場合、本人と他人との間に判定の閾値を設定すると、判定の結果が閾値以下であればシステムにアクセスしているのは本人であることが確認でき、また閾値より大きければ他人であることが確認できる。理想的な場合は、特定の個人に対してタイプⅠの誤りとタイプⅡの誤りは別々に発生し、それぞれが相互に関連性を持つことはない。

（図4）個人認証時における誤りのタイプ（理想的な場合）



一方、通常の場合（図 5）では、本人の特徴と他人の特徴には多かれ少なかれ類似性があり、部分的にオーバーラップしていると考えられる。この場合、タイプⅠの誤りとタイプⅡの誤りがクロスするポイントが存在する。すなわち、ある閾値を決めるとタイプⅠの誤りとともにタイプⅡの誤りが同時に発生することになる。タイプⅡの誤りは他人をアクセプトしてしまう誤りであり、システムの安全性に関わる重大な誤りである。それに対し、タイプⅠの誤りは本人がリジェクトされてしまう誤りであり、システムの安全性というより利便性に関わる誤りといえる。

（図5）個人認証時における誤りのタイプ（通常の場合）



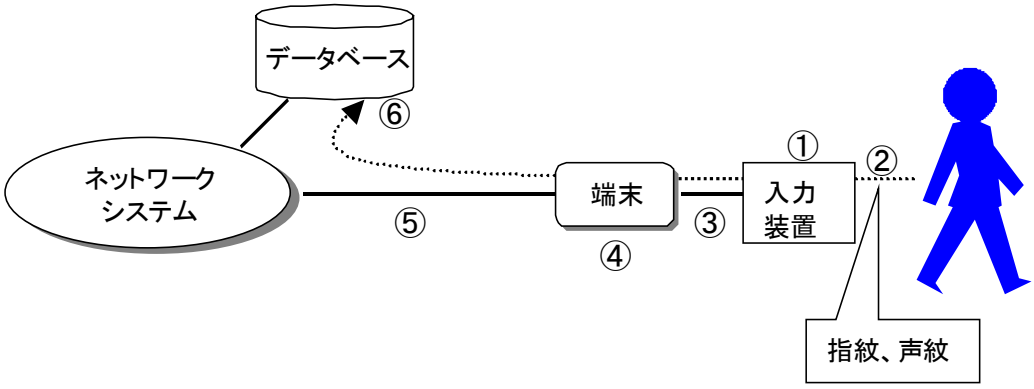
一般的に安全性を重視するシステムであればある程、タイプⅡの誤りを小さく設定する必要がある。逆に、利便性を重視すべきシステムでは、あまりタイプⅡの条件を厳しく設定すると本人が何度アクセスしてもリジェクトされてしまうことになりかねないため、まず、タイプⅠの誤りの程度を定め、このときのタイプⅡの誤りが安全性の設計の観点から許容できる値であることを確認するといったアプローチが考えられる。

なお、タイプⅡの誤りは、暗証番号等の他の安全性を確保する手段の併用により減少させることが可能であるが、タイプⅠの誤りは、他の手段を併用してもこれを減少させることはできない。このため、特にユーザーの利便性が重視されるようなシステムに使用されるバイオメトリック認証技術においては、タイプⅠの誤りを低減させる方向で研究開発を進めることが重要と考えられている。

3. バイオメトリック認証と安全性

本人を認証するプロセスは、事前登録処理と認証処理に分けることができる。以下は、一般的な認証＜照合＞モデルを例にした、それぞれの処理手順である。

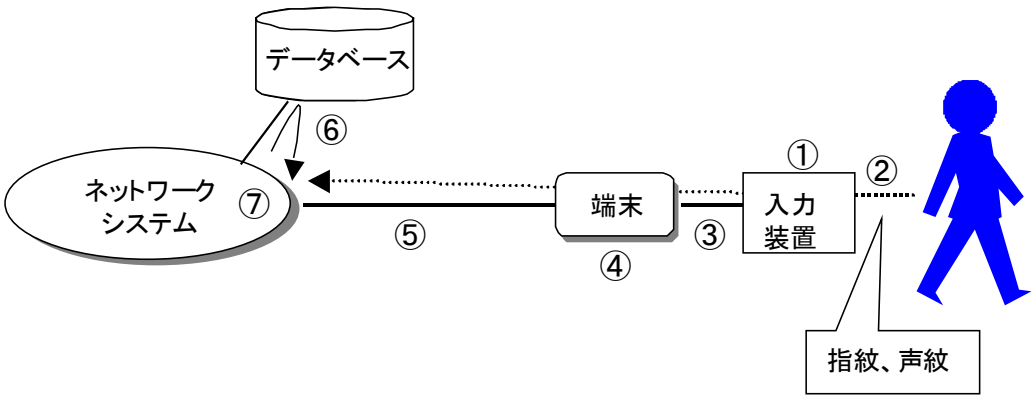
（図6）事前登録処理の流れ



（事前登録処理）
① ユーザーの ID 情報を端末に入力。
② ユーザーのバイオメトリック情報を入力装置から入力。
③ 入力装置から入力されたバイオメトリック情報を端末に伝送。
④ 端末は入力されたバイオメトリック情報から本人固有の特徴情報を抽出。
⑤ 本人固有の特徴情報と ID 情報をネットワークでセンターへ伝送。
⑥ 本人固有の特徴情報と ID 情報をセンターのデータベースに登録。

事前登録処理は、本人の特徴を抽出し、システムのデータベースに登録する処理であり、ユーザーはシステムを利用する前に 1 回だけ行っておく必要がある。バイオメトリック認証では、後にアクセスしてきたユーザーがこの登録時のユーザーに等しいかどうかを判断している。したがって、いくら認証の精度をあげたところで、登録のプロセスで不正が行われ、他人を騙って登録する等が行われると、以後の成りすましを防ぐことは不可能となる。つまり、登録処理が従来の社会における存在と、ネットワークシステムにおける存在をリンクする重要な役目を果たしているのであり、登録処理時に、登録者が正しい本人であることを確認する運用上の仕組みが整備されていることが重要である。

（図7）認証＜照合＞処理



（認証＜照合＞処理）
① ユーザーの ID 情報を端末に入力（照合の場合は ID 情報は不要）。
② ユーザーのバイオメトリック情報を入力装置から入力。
③ 入力装置から入力されたバイオメトリック情報を端末に伝送。
④ 端末は入力されたバイオメトリック情報から本人固有の特徴情報を抽出。
⑤ 本人固有の特徴情報と ID 情報をネットワークでセンターへ伝送。
⑥ センターはユーザーの ID 情報をもとにデータベースに登録されている情報を照会。
⑦ センターは伝送された特徴情報とデータベースに登録されていた情報を比較し、
一定の閾値以下かどうかを判断。

バイオメトリック認証の安全性は、採用しているバイオメトリック技術の精度はもちろんであるが、どのようにバイオメトリック認証技術を実装・運用しているかといったことも考慮して判断することが大切である。ここで説明した認証モデルにおける認証処理では、認証の判断はセンターのネットワークシステムで行われており、入力されたバイオメトリック情報は、本人⇒入力装置、入力装置⇒端末、端末⇒ネットワークシステム、と伝送されていく。そのため、これらの過程においても不正防止対策が施されていることが大切である。

(a) 本人⇒入力装置

本人の固有の特徴として使われるパラメータを複製あるいは偽造して入力装置を欺き、成りすましを行う不正行為に対する安全対策が必要である。入力装置を欺く不正行為としては例えば、指紋を写し取ったゴム製の義指や録音された音声を用いたり、筆跡を真似たりすることが考えられる。多くのバイオメトリック技術は、こうしたアタックの可能性をある程度考慮した安全対策を講じているが、あくまでも一般的に利用可能な製品や技術を利用したアタックを前提にしているに過ぎない。しかしながら、現時点でも技術的には、汗腺までも再現した人工皮膚に指紋を写し取った義指や、人間に聞こえない周波数帯まで精巧にカバーした高音質の音声録音

装置、あるいは他人の筆の動きをカメラで正確に捉えこれを再現する装置などを開発し、アタックを成功させることは可能と考えられる。したがって、こうしたアタックがどれくらいのコストで実現可能となるのかについて把握しておくことは、守るべき資産の価値に応じてどのバイオメトリック技術を選択すべきか、あるいは、必要な安全性を確保するためには、さらに別のどのような安全対策を組み合わせる必要があるかといった検討を行うためにも必要なことである。

現在では、バイオメトリック技術が一定の認証精度を実現しつつあるが、安全性の観点からは一方で、成りすましのフィージビリティに関する研究が盛んに行われるようになることも必要であろう。例えば、人間は環境や状態によってコンディション等が微妙に変化するため、パラメータの入力値が毎回同じになるように再現することは不可能であり、ある統計的な分布に従う「振れ」が生じるという特徴がある。こうした「振れ」を利用することによって、入力装置を欺くことを困難にする研究等も行われており、成果が期待されているところである。

(b) 入力装置⇒端末

入力装置は、端末の周辺機器として接続されていることが普通である。しかしながら、この機器との間に流れる情報をタッピングして記録しておき、後に入力装置を偽って不正に入手した情報を端末に送ることにより、不正が行われる可能性もある。この間の伝送路の暗号化や、入力装置と端末の一体化によって、こうしたタッピングを困難にすることは一つの解決方法である。最近では、さらに安全性を高めるものとして、CPU チップと指紋読み取りセンサーを一体化して携帯性に優れた IC カード型の指紋照合ユニット[7]の製品発表（図 8）なども行われている。

（図 8）指紋照合機能付内蔵 IC カード[8]

出典：http://www.protectivetech.com

[7] IC カードの中に個人のバイオメトリック情報を保存しておき、IC カードのみで、「ユーザー認証」を行うことが可能である。なお、さらに、暗号文の復号やデジタル署名を行うために本人が所有する秘密鍵を保存することによって、「端末認証」を実施している。

[8] もともと、Safe Guard 社の技術であったが、1999 年 4 月、Protective Technology 社に吸収合併されたため、現在は Protective Technology 社の製品となっている（http://www.protectivetech.com）。

(c) 端末⇒ネットワークシステム

端末は暗号を利用して端末認証を行った上でネットワークシステムと接続され、その後は暗号通信が行われることが通常である。正しく暗号通信が行われている限りは、この間の伝送経路は安全であるが、適用する暗号の強度が不十分であったり、システムへの不適切な実装が行われたりしている場合には、盗聴等によって不正な成りすましが可能になる危険性がある。

4. バイオメトリック認証の研究事例

バイオメトリック認証技術に対する要求条件としては、以下の項目が挙げられる。

①安全性

利用する特徴パラメータおよび照合／識別アルゴリズムによって、個人認証の精度とともに適用できる環境が異なる。本人を正しく認証できることは当然であるが、特徴パラメータの偽造によるなりすまし、あるいはパラメータの時間的な変化に対応できることが望まれる。

②マン・マシン・インタフェース

子供や高齢者でも容易に操作が行えるとともに、個人情報を入力しているという心理的抵抗感が極力少ないことが望まれる。

③端末の小型化、低廉化

④社会的な認知

社会的にコンセンサスが得られる特徴パラメータの利用が必要である。

現在、表 7 のとおり、様々なパラメータを使ったバイオメトリック認証の研究が行われており、一部のものは既に実用化されつつある。

（表7） バイオメトリック認証の特徴

パラメータ		特　徴	課　題
指紋	•特徴点（マニューシャ）の位置 • リレーション	•万人不同，終生不変 •犯罪捜査での利用	•指紋画像の品質 •衛生面の確保 •社会的な受容（プライバシー）
網膜	•毛細血管パターン	•万人不同，終生不変 •コピーが困難	•システムの規模，価格 •赤外線照射に対する抵抗感
虹彩	•瞳孔の開きを調節する筋肉のパターン	•万人不同，終生不変 •眼球内部の疾病等の影響がない	
掌形	•掌の幅，厚さ •指の長さ等	•操作が容易	•信頼性の確保 •衛生面の確保
顔	•目，口，鼻の位置や形状等	•非接触で認証可能 •心理的抵抗が少ない	•時間的な変化 •メガネ，ひげ等の影響 •照明や撮像角度，背景等の制約
音声	•スペクトル包絡 •ピッチ，発音レベル，発声速度等	•非接触で認証可能 •心理的抵抗が少ない •テキスト依存型	•テキスト独立，テキスト提示型の実用化 •時間的な変化 •体調の影響
筆跡	•筆順，筆速，筆圧等	•心理的抵抗が少ない •操作が容易（小型タブレット） •テキスト依存型	•テキスト独立，テキスト提示型の実用化 •時間的な変化 •偽筆対策

指紋は同一人物の同一指以外には同じものが存在せず、また 6 ヶ月程度の胎児で完成し、その後は成長に伴い大きさに変化はあっても指紋模様自体に変化は生じないといわれている。すなわち、万人不同、終生不変の 2 大特徴を有するものであり、個人認証において絶対的な価値を持った、確実性の高いものとして広く認められている。最近は、指紋入力装置の低廉化に伴い、多くの実用システムが開発されている[9]。

指紋の照合技術は、大別して二つの方法がある。一つは、指紋の端点や分岐点等の特徴点（マニューシャ）を利用するマニューシャ法（瀬戸・星野 [1986]、浅井・星野・木地 [1989]）である。また他方は、指紋画像自体を用いる画像相関法（小林他 [1995]）である。後者については、空間的フーリエ変換を用いた手法が提案されている。

指紋による個人認証の具体的な適用事例としては、個人が保有する IC カードに指紋読み取りセンサーを付加して、カード使用者が本人である場合のみ、カードがアクティブになるハイセキュリティカードのコンセプト（木下・清水・小松 [1992]、郵政省郵政研究所 [1993]）が提案されている（模型は図 9 参照）。こうした製品の具体化には、センサ技術の向上が寄与しており、図 8（14 頁）に示した製品が実現しているほか、さらに携帯端末への直接組み込み（図 10）も提案されている。

（図 9）バイオメトリック認証の適用例

指紋認証を搭載した IC カード

携帯電話への適用

（図 10）携帯端末への組み込み例

[9] 「指紋ビジネス進化」、朝日新聞、1998 年 3 月 5 日

眼をバイオメトリック認証に応用する際の代表的なパラメータとしては、網膜と虹彩がある。**網膜**は、その表面に血管パターンは 3 歳程度で完成して外傷等がなければ一生変化しないと考えられている。このため、赤外線を円形にスキャンして血管のパターンを取り出し、この情報をもとに個人認証を行うシステムが実用化されている（川崎 [1998]）。

虹彩は、瞳孔の開閉を調節する筋肉から構成されている。瞳孔から外側に向かって発生するカオス状の皺は生後数年で完成し、一生涯変化しない。この皺のパターンを近赤外線でスキャンして個人認証を行うシステムが製品化されている（斎藤・松下 [1998]）。

掌形は、個人認証の手段としては最も古くから使用されているものである。かつて、我が国の鎌倉時代において、画指という指の長さや関節の位置を写し取った身分証明書が発見されたことが報道されている（小畑 [1991]）。現在実用化されている装置では、3 次元の画像により指の長さ、掌の幅と厚さ、および指の関節部分の幅と高さ等 100 程度の特徴を測定して、個人認証を行っている（高木 [1998]）。

顔は我々の日常生活において個人を確認するうえで最も自然に利用するパラメータの一つであり、100 年以上前に研究成果が発表されている（Galton [1888]）。非接触で心理的抵抗感が少なく、かつヒューマンインタフェースとして優れた特徴をもつことからも、実用化が多いに期待される。顔による個人認証は、目、鼻、口部分を抽出してマッチングを行う方法と、顔画像をそのまま用いる技術が提案されている（平山・中村 [1996]、土居他 [1996]、栗田・長谷川 [1997]）。

音声は、声帯の性質や声道系の形状などに起因する音響的特徴に着目して個人を特定するうえで有効な手段であり、これまでに多くの研究、開発がなされている。音声を用いた個人認証を実用化しているシステムとしては、米スプリント社による公衆電話用クレジットカード「Voice Phone Card」が代表例として挙げられる（古井 [1995]）。この実用例は、テキスト依存な個人照合であるが、隠れマルコフモデル[10]を用いたテキスト指定型話者照合方法（松井・古井[1996a]）も提案されている。もっとも、声の時間的な変動、疾病あるいは周囲の雑音の影響の排除等、今後一般的に利用されるためには解決すべき課題も幾つか残されている（古井 [1998]、松井・古井[1996b]）。

筆跡に関しては、手書き文字は、まず文字形態のイメージが意識空間で想起され、次に腕、手の動きを制御する運動指令の発生の過程を経て、2 次元空間信号の形で出力されることが分かっている（田口 [1991]）。最終的に空間図形として表現された文字は、筆記者の網膜を介して形状が認識され、意識空間にフィードバックされる。

[10] 隠れマルコフモデル（HMM: Hidden Markov Model）：不確定な時系列のデータをモデル化するための統計的手法のひとつ。状態遷移の確率が出力値のみによって一意に決まらず、状態に依存した確率関数で決定されるところに特徴がある。背後にある確率過程は直接には観測できず（隠れている）、観測系列を生成するもう１つの確率過程の集合を通してのみ観測できる。音声によるバイオメトリック認証においては、例えばテキストの音素の間の繋がりの学習等に応用される。

文字の形状を決定するパラメータは幾つか存在するが、運動指令の過程で与えられる筆点の動的特性が文字の形状を修飾する形で現れた特徴が個人性を示すものであり、個人認証では重要な情報となる。テキスト依存かつオンライン型については製品化の事例があり[11]（佐々木 [1996]）、パーソナルコンピュータに接続された電磁誘導式の小型タブレットを用いて、認証を行う過程のペンの動き、書き順、速度、筆圧をあらかじめ登録された情報と比較して、本人か否かを判定する仕組みとなっている。また、テキスト独立あるいは提示型の個人認証については多くの研究成果が発表されている（Plamondon and Lorette [1989]、Yamazaki and Komatsu [1997]、吉村他 [1996]、山崎・小松 [1996]）。

音声、筆跡は我々のコミュニケーションにおいて使用されている手段であり、表 5（8 頁）でも示したとおり特異性による分類（singular part）と意味論による分類（semantic part）が存在する。この両者の特徴を利用した、すなわち個人認証と音声認識／文字認識とが融合して、高度かつ安全性の高いヒューマンインタフェースが実現できると考えられる。

バイオメトリック認証については、一般的な解説（Miller [1994]、吉村他[1996]、Davis and Price [1998]、増田 [1991]、Jain, Boille and Pankanti [1999]、坂野 [1999]）とともに技術動向に関する報告[12]が数多くなされている。また、実社会への導入に関する検討結果も報告書としてまとめられている（社会安全研究財団 情報セキュリティ調査研究委員会[1997]、電子商取引実証推進協議会 本人認証技術検討 WG[1998]）。

[11] 「筆跡などで本人確認」、日経産業新聞、1997 年 7 月 20 日

[12] 「特集 個人認証・識別はどこまで可能か？」、『エレクトロニクス』、オーム社、1998 年 2 月

5. バイオメトリック認証の金融サービスにおける実用化事例

バイオメトリック認証の実用化例としては、企業等の内部の入退出管理システム向けが多くみられる。これは、システムを利用するユーザーの数が比較的少なく、また、組織内部に閉じたシステムであるため、導入が容易であることが要因と考えられる。金融機関でも、スルガ銀行がコンピュータシステムの稼動するコンピュータセンターへのアクセス制御のために、沖電気工業㈱の虹彩を利用した認証システムを導入しているほか、様々なバイオメトリック認証を使用した入退出管理システムを実験ないし検討中の金融機関も複数みられるようである。

しかしながら、一般の顧客を対象とする金融サービスにおいて、バイオメトリック認証を使用する例はまだ数えるほどしかない。これは、①登録するユーザーの数が膨大になることから、性能要求が厳しくなること、②一般の顧客を相手にするため、安全性はもちろん利便性にも十分配慮する必要があること、等から様子を窺う先が多いものと思われる。以下は、各企業の発表資料をもとにした金融サービスにおける利用事例の概略である。

(1) 日本国内における事例

【泉州銀行＜大阪＞のテレフォンバンキング[13]】

泉州銀行は、テレフォンバンキング[14]において、声紋を活用した音声による本人確認を行うシステムを富士通㈱とともに開発し、1997 年 5 月よりサービスを開始している。利用者がサービスを受けるには、まず、銀行に電話をかけ、自動音声に従って 7 桁の会員番号と事前登録した 4 桁の暗証番号をダイヤルボタンで入力する。暗証番号が正しいことが確認されると、オペレータが応答し利用者の誕生日等事前に届出済みの顧客属性を尋ねること（可変暗証）によって本人であることを確認する。その後、口座振替等資金移動に関わる取引を行うには、さらに取引指示を行った後、事前に登録されている本人のデータとの間で声紋の照合を行うことによって本人確認を行っている。つまり、①暗証番号、②可変暗証、③声紋と複数の本人確認手段を併用することによって、安全性を確保している。なお、会話の最中に特殊な波長の音声を流すこと等によって、盗聴録音による不正行為などが行えないような対策もとられている。

【㈱武富士＜東京＞の ATM[15]】

㈱武富士は、人間の目の瞳孔を取り巻く筋肉の模様である虹彩（アイリス）から

[13] http://www.senshubank.co.jp/teleban.html

[14] テレフォンバンキングで扱えるサービスは、①照会サービス（普通預金、貯蓄預金、当座預金の残高照会、入出金明細照会、振込照会、金利照会）、②資金移動サービス（振込、振替）、③定期預金（預入・解約・継続・口座開設）、④外貨預金（預入・解約・継続）、⑤投資信託（口座開設申込受付、購入、解約）、ローンサービス（ローン事前審査、申込受付）、⑥ホームアドバイザーサービス（家計診断、資産運用相談、年金相談）、⑦各種届出受付（住所変更手続き、公共料金口座振替の受付）等であり、現金の出し入れを伴わないほとんどの取引が可能である。

[15] http://www.takefuji.co.jp/takefuji/html/721.html

本人かどうかの照合を行い、現金の入出金を可能とする ATM を沖電気工業㈱と共同で開発し、1999 年 2 月より実用化を開始している。顧客は、あらかじめ虹彩をカメラで撮影して登録しておき、取引の都度、ATM に組み込まれている識別装置で本人を確認する仕組みになっている。眼鏡やコンタクトレンズを付けていても識別は可能で、誤認確率は百億分の一と発表されている。なお、現在では顧客の電話番号等の個人情報とカードを確認のために併用することによって不正防止に備えており、表 5（8 頁）の分類では「照合」目的で利用しているが、将来的には、カードレス化、すなわち事前知識を入力せず虹彩情報だけで顧客を見分ける「識別」目的での利用を目指している。

(2) 海外における事例

【Bank of America（米）のオンラインバンキング[16]】

Bank of America は、1999 年 1 月、インターネット経由でのオンラインバンキングのセキュリティを確保するために指紋認証を使ったシステムの実験を開始した。同行のシステムでは、あらかじめ指紋情報を記録した IC カードを発行してもらい、利用者の PC に接続されたカードリーダーに IC カードを挿入するとともに、指紋読み取り用のスキャナーに指をあてがい指紋を読み取ることによって、認証を行う仕組みとなっている。

【Riverside Health System Employees Credit Union（米）の ATM [17]】

米バージニア州にある同信用組合は、1998 年、全米で初めて指紋スキャナーで本人確認を行う ATM をメディカルセンター内に設置した。この ATM は、リアルタイム・データ･マネージメント･サービス社の製品で、取引履歴出力、預金振込／振替（ただし、同信用組合内の口座間のみ）、ローンの申込／返済、小切手による預金引出等の銀行業務が可能である。

【Conavi 銀行（コロンビア）の顧客認証機器[18]】

コロンビアの Conavi 銀行は、1997 年 8 月、オーストラリアの生物測定関連企業である Fingerscan 社が開発した指のパターンで本人確認を行う装置を、支店 50 店に導入し、顧客の認証に使用することを発表している。Fingerscan 社の装置は、人の指を立体的にスキャンし、あらかじめ登録されている情報と比較することによって、誰であるかを判断するもので、指紋による識別とは異なるものである。なお、この Fingerscan 社の機器は、金融関連の内部のセキュリティシステムとしては、インドネシアの Bank of Central Asia が採用している事例がある。

---

[16] http://www.bankofamerica.com/newsroom/press/press.cfm?PressID =press.19990106.01.htm
[17] http://www.rhsecu.org/new.html
[18] http://www.conavi.com/ (http://www.fingerscan.com.au/news/press_26-8-97.htm)

【Nationwide Building Society（英）の ATM[19]】

貯蓄貸付組合である Nationwide Building Society は、1998 年 4 月、世界で初めて虹彩によって本人確認を行う ATM の公開実験を開始した。同 ATM は Sensar 社の虹彩識別技術を使って NCR 社が開発したもので、利用者は ATM にバンクカードを挿入し、PIN の代わりに虹彩によって本人照合を行う仕組みとなっている。なお、1999 年 6 月には、NCR 社が新開発した虹彩のみで本人を識別する ATM（バンクカードの提示も不要）を使って、Royal Bank of Canada がカナダで実験を開始している。

また、米国では 1999 年 5 月 Bank United が、やはり Sensar 社の虹彩識別技術を使って Diebold 社が開発した虹彩のみで本人を識別する ATM の導入を開始している。

【Mr. Payroll 社（米）の自動小切手清算機<check-cashing machine>[20]】

ATM や自動小切手清算機の大手サービス会社である Mr. Payroll 社は、Miros 社の顔認識技術によって本人確認を行う自動小切手清算機を 1997 年 6 月より導入した。同機はその後、BancOne 銀行などにも採用されている。

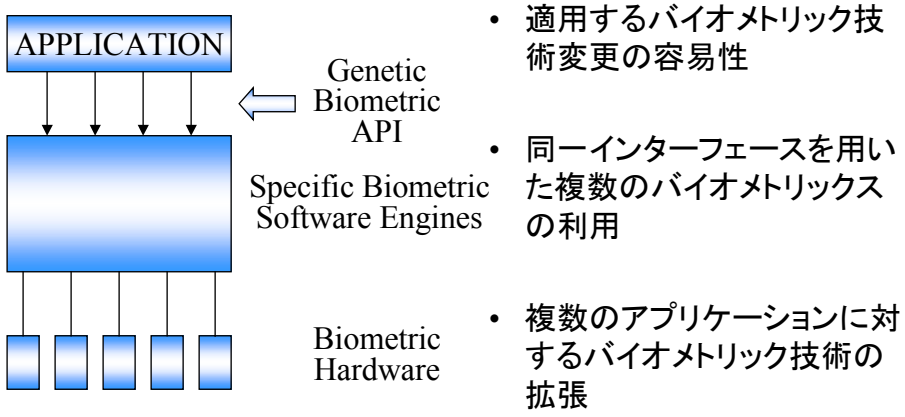
[19] http://www.nationwide.co.uk/whatsnew/whatsnewsetup.htm
[20] http://www.mrpayroll.com/ (http://www.miros.com/MrPayroll_PR.htm)

6. バイオメトリック認証の標準化動向

(1) バイオメトリック認証の主要な標準化活動

各研究機関、企業等で開発されたバイオメトリック認証のハードウェアやアルゴリズム（以下、バイオ認証機能とする）の仕様は必ずしも標準化される必要はないが、アプリケーション毎に独立のバイオ認証機能が実現され、かつこれらの機能に互換性がないとユーザーにとっての利便性は極めて悪いものとなる。例えば、IC カードにバイオ認証機能を組み込むことを例にとると、アプリケーション毎に異なるカードを使用しなければならない事態に追い込まれる可能性がある。したがって、バイオ認証機能が種々のアプリケーションに対して柔軟に適用できる技術的要件を検討することが重要な課題の一つとなる。また、バイオ認証機能個々についても、技術革新とともに高機能化、小型化が進むことが考えられ、こうした要求条件に対しても柔軟なシステム構成を実現しなければならない。API (Application Program Interface)（図 11）の標準仕様を定めることによって、こうした問題は解決されるとともに、複数のアプリケーションに対しても複数のバイオ認証機能を同一のインタフェースで利用することが可能となる。

（図11）API (Application Program Interface) の標準化の必要性



API の標準仕様として検討が進められている主要なものとしては、HA-API、BAPI、BioAPI 等[21]がある。各々推進主体が違い、標準化しようとしている適用領域も微妙に異なっているが、個々のバイオメトリック方式の処理方法やアルゴリズム自体は標準化の対象外とされ、特定のベンダーやバイオメトリック技術に依存しない API の仕様を標準化の対象としている点で共通している。なお、最近になって、これらをすべて統一し、国内標準、国際標準に仕立てようとする動きが盛んになってきている。

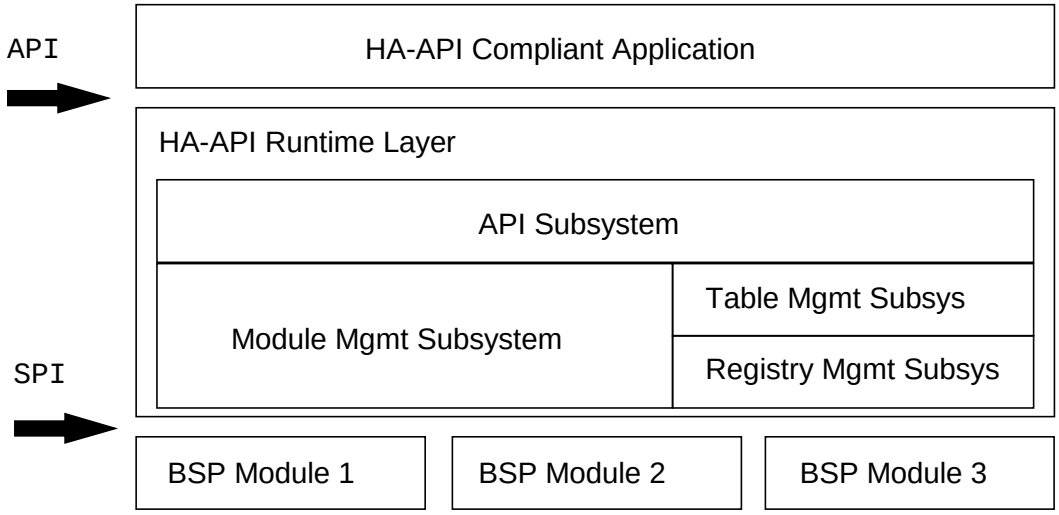
[21] 他にも、Novell Inc.が議長を務める SRAPI (Speech Recognition API) Committee が開発した、話者認識用 API の SVAPI (Speaker Verification API)などがある。

(a) HA-API (Human Authentication – Application Program Interface)[22]

HA-API は、個人の認証や識別のためのバイオメトリック技術を組み込むソフトウェア･アプリケーションのインターフェースを定めたものである。もともと National Registry 社が米国防総省の依頼により開発した仕様であるが、後に世間に幅広く普及させることによって、バイオメトリック技術の相互互換性が確保されるよう、一般に公開されている。1997 年 8 月 27 日に Rev.1.0 が作成されたあと、1998 年 4 月 22 日に Rev.2.0 までが発表されている。

HA-API は、プラットフォームや機器に依存しない仕様となっており、アプリケーションの開発や、装置の変更に容易に対応できるようになっているほか、複数のバイオメトリック技術を、単独のみならず組み合わせてサポートすることも可能である。

（図 12）HA-API のアーキテクチャ



出典：http://:www.saflink.com/haapi.html

(b) BAPI （Biometric Application Programming Interface）[23]

BAPI は、ソフトウェア・アプリケーションとバイオメトリックデバイスが通信する場合のアプリケーションインターフェースを定義しており、I/O Software 社がバイオメトリックスのハードウェア、ソフトウェアベンダーに声をかけて組織したワーキンググループ[24]によって提案されている。MS-Windows アプリケーションが印刷を

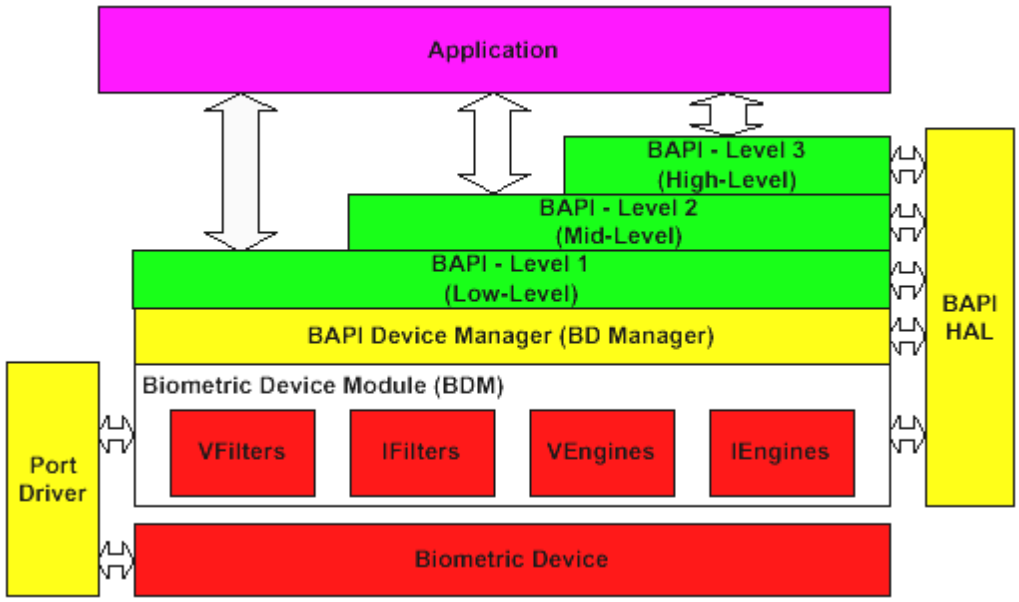
[22] http://:www.saflink.com/haapi.html

[23] http://www.iosoftware.com/bapi/

[24]現在のメンバーは、Amano Cincinnati, Inc., Association for Biometrics, AuthenTec, Bergdata AG, Biometric Identification, Inc. (BII) , Biometric Sciences Corporation, Center for Signal Processing, Cherry GMBH, DelSecur, Fujitsu, I/O Software Inc., International Biometric Group, IriScan, Kent Ridge Digital Labs, MAG Innovision, Miros Inc., Precise Biometrics, PrintScan, Prologex Inc., Quality System, Inc., Sagem-Morpho, Inc., Siemens AG, Singapore Centre for Signal Processing, Sony Corporation, StarTek Engineering, Inc., TechnoImagia, Toshiba/TEC, Thomson-CSF, Veridicom Inc., Viisage Technology, Inc., Who?Vision。

行う際、標準のドライバ・インターフェースを通して個々のプリンターと通信するのと同様に、アプリケーションがバイオメトリックスを利用した高度なセキュリティを実現する際の互換性、統一性を確保することによって、識別デバイスの仕様・性能等を意識することなく効率的な開発を行えるようにすることを目的としている[25]。なお、BAPI はデバイス固有の機能の使用有無によって使い分けられる 3 つの機能的に異なるレベルから構成されている。1998 年 9 月に Biometric API (BAPI) Device Module Interface Specification (BDMI) Version 1.3, Biometric API (BAPI) Software Developer's Kit (SDK) Version 1.2 が出ている。

（図 13）BAPI のアーキテクチャ



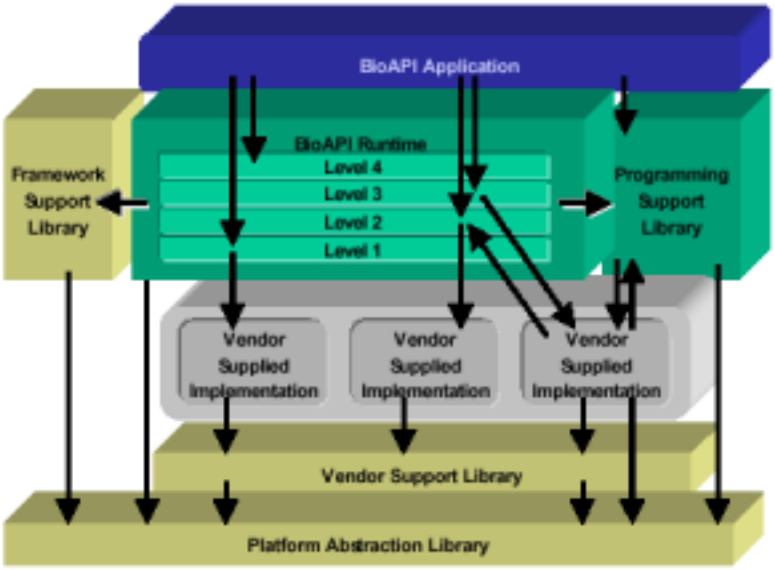
出典：http://www.iosoftware.com/bapi/

(c) BioAPI[26]

BioAPI は、1998 年 4 月に Compaq Computer 社, IBM 社, Identicator Technology 社, Microsoft 社, Miros 社, Novell 社が推進主体となって組織された BioAPI コンソーシアムで開発されたバイオメトリック技術のための標準 API 仕様である。コンソーシアムには、HA-API の National Registry 社、BAPI の I/O Software 社、NSA（National Security Agency）や NIST（National Institute of Standards and Technology）情報技術研究所の政府関係者のほか、様々な分野の組織が参加し、活動に貢献している[27]。BioAPI のドラフトは、プラットフォームやデバイスに依存しないマルチレベル API を実現する仕様として、1998 年 12 月にコンソーシアムのメンバーに対して公表されている。

[25] 当初は、MS-Windows をベースに開発されているが、BAPI では、OS に依存しない柔軟性を備えているため、ほとんどすべてのプラットフォームに容易に移植可能としている。
[26] http://www.bioapi.org
[27] これらの活動に貢献する組織は contributor と呼ばれ、I/O Software, IriScan, NIST, NSA, Printrak International, Recognition Systems, Saflink, Siemens, Unisys 等がある。

（図 14）BioAPI のアーキテクチャ



出典：http://www.bioapi.org

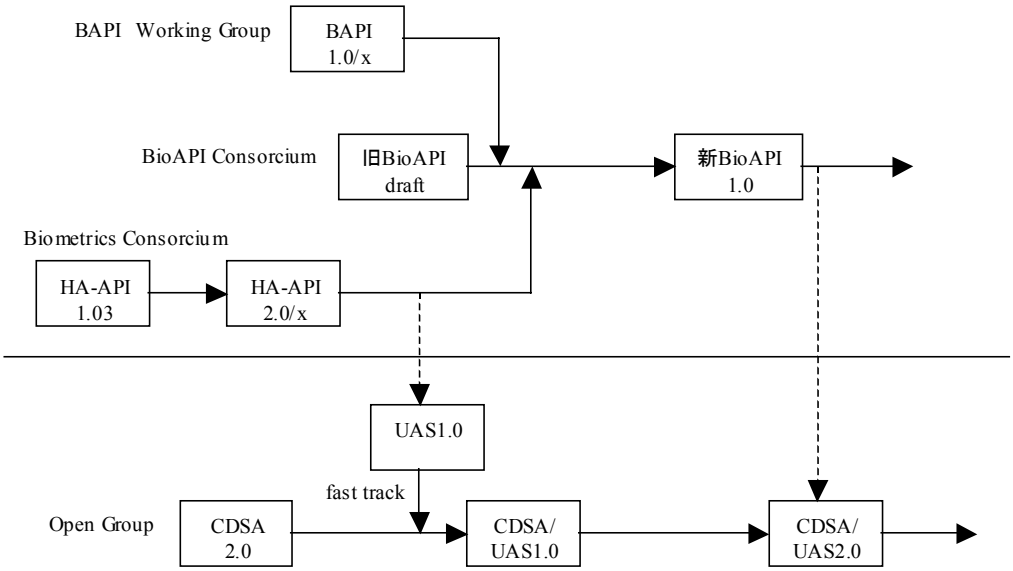
(2) API の標準仕様統一化の流れ

1998 年 12 月、BAPI の設立主体である I/O Software 社が BioAPI の推進主体の一員として加わることになり、BAPI は Version 1 の完成を持って作業を終了し、その仕様は BioAPI に引き継がれる形で統合されることになった。さらに、1999 年 2 月、NIST の仲立ちにより、BioAPI コンソーシアムと HA-API のワーキンググループとの間で仕様統一に向けた会合が持たれ、1999 年 3 月には両者の仕様を統合することが合意された。HA-API は Version2.0 で凍結され、その後の活動は BioAPI の策定に注がれることになっている。こうして、新 BioAPI[28]は、BAPI、旧 BioAPI、HA-API の 3 つの API を統合した仕様として、2000 年第 1 四半期末までに Version1.0 の完成を目指し、現在、作業が進行している。

また、これに合わせて BioAPI コンソーシアムは改組され、国内標準あるいは国際標準の策定プロセスにならい、すべての参加組織がフラットな投票権限をもつように変更された[29]。さらに、BioAPI コンソーシアムは外部の標準化団体ともリエゾン関係を設け、Open Group[30]の CDSA/UAS (Common Data Security Architecture / User Authentication System) 等、主要なコンピュータ・セキュリティの枠組にバイオメトリック認証サービスを付加する標準仕様の策定に対して影響力を持っている。

[28] http://www.bioapi.com
[29] 25 の組織がメンバー登録を済ませ、Compaq, Miros, IBM, NIST, Intel, SAFLINK, I/O Software の 7 社が steering member として選出されている。
[30] X/Open Company 社と Open Software Foundation とが合併して 1996 年 2 月に設立されたベンダーニュートラルの国際的なコンソーシアムで、200 以上のメンバーから構成される。世界中のコンピューターとインターネットを結合する情報インフラの創造を使命とする標準化組織で、本部は米国マサチューセッツ州ケンブリッジ市。

（図 15）バイオメトリック API の標準化の動向



なお、日本では 1999 年 5 月セキュリティベンダー8 社[31]が「本人認証規格統一協議会」を設立し、バイオメトリック認証の API や共通評価基準策定のほか、米国の BioAPI に対し、日本の意見・要望を提出する活動を行っている。

一方、ISO などの国際標準としては、個々にバイオメトリック認証に関する提案が行われているのが実態である。ISO/IEC JTC1/SC17/WG4（接触端子つき IC カード）では、NWI (New Work Item)として接触式 IC カードを使用したバイオメトリック認証の API 標準化の作業を行うことが決まっている。

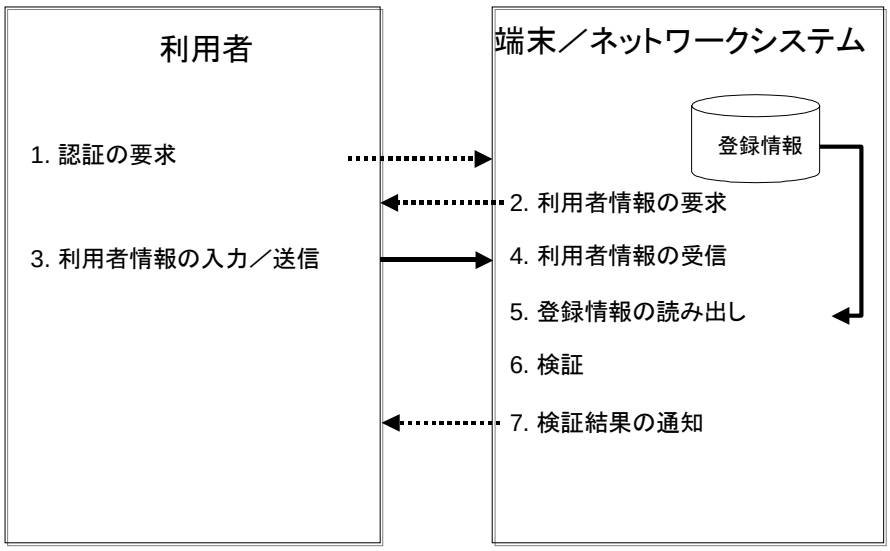
[31] オムロン、システムニーズ、シュルンベルジェ、ソニー、翼システム、東芝、日立製作所、三菱電機。

7. バイオメトリック認証の参照モデル

バイオメトリック認証を実行するシステムの形態としては、様々なモデルやそのバリエーションが考えられる。ここでは、バイオメトリック認証を行ううえで必要とされる個人の特徴データをどこで管理するかといった側面から、①ユーザーが利用する端末もしくはサービス提供者といった相手方システムが個人性情報を保有（モデルⅠ）、②ユーザー自身が個人性情報を ID カード等に格納した形で保有し自ら管理（モデルⅡ）、③第三者である登録機関が個人性情報を保有（モデルⅢ）、という 3 つのモデルに分類[32]して、それぞれの特徴を整理して考察を行った。なお、安全性の拠り所となる技術の選択や、ユーザーとシステム間の認証の手順等については種々の方式が候補となりうるが、本章では大まかなモデルの一例を示すに留め、安全性等の観点からの類型化や考察は行わない。

(1) モデルⅠ（個人情報を相手方システムが保有）

（図16）認証モデルⅠ



本モデルにおける個人認証のプロセスは、例えば、キャッシュカードを使って銀行の ATM から現金を引き出す場合に対応する。端末側あるいはセンターにユーザーの個人性情報があらかじめ登録されており、その情報に基づき本人の認証を行うものである。本モデルでは、ユーザーが端末に直接アクセスすることを念頭においている。

現行のキャッシュカードの安全性を高める目的で暗証番号に加えてバイオメトリック認証を行う場合、従来の磁気カードをそのまま利用することは可能である。暗証番号のみによる本人確認方式は、個人の生活情報に関連したパラメータが用い

[32] モデルの分類にあたっては、電子商取引実証推進協議会が 1997 年 5 月に公表した「本人認証技術検討 WG 中間報告書」を参考にしている。

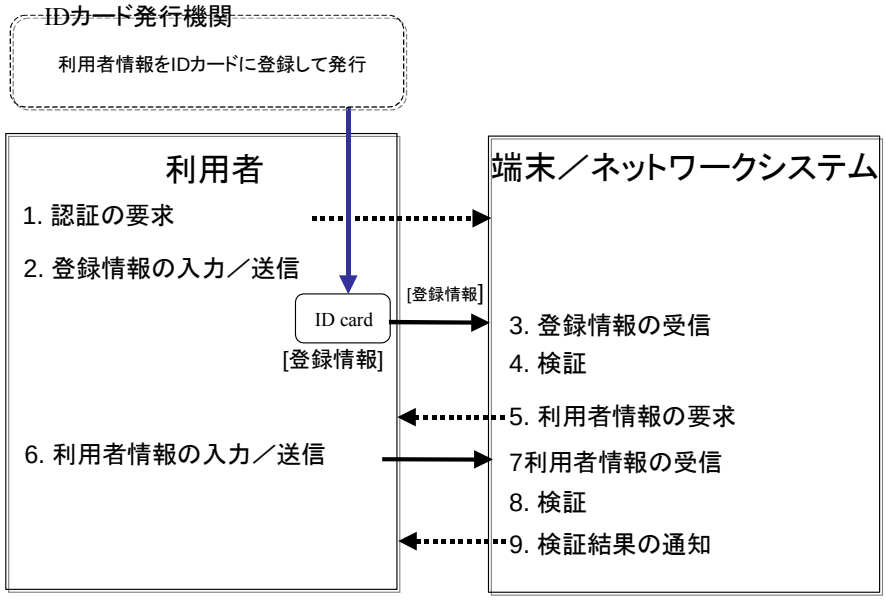
られていることが多く、安全性があまり高くないことは既に指摘した。この問題をバイオメトリック認証でカバーすることにより、カードの不正使用による被害が減少することが期待できる。

モデルⅠは、個人性情報をシステム側で保管する点に特徴があるが、この情報が外部に露呈しないように、情報管理については万全の対策が必要とされる。また、システム側での個人性情報の管理は、プライバシー保護の観点から利用を問題視するユーザーも存在することを念頭に置かねばならない。

以上のことから、バンキングシステムで本モデルを適用する場合は、金庫室への入退室管理等特別なエリアにおけるユーザーの認証に限定して適用することが現実的との見方もある。

(2) モデルⅡ（個人情報をユーザーが自ら管理）

（図17）認証モデルⅡ



モデルⅡは、クレジットカードにおける本人の認証プロセス等[33]にも対応している。図17における個人性情報を格納するIDカードは、例えばICカードで実現される。

IDカードの発行機関では、ユーザーの個人性情報をIDカードに記録[34]したうえでユーザーに発行する。本モデルでは、ユーザーはIDカードを端末に入力し、端末（もしくはネットワークシステム）はIDカード内の個人性情報と、入力された特徴パラメータとの類似性を確認することにより個人認証を実行するが、IDカード自体にパ

[33] 例えば、センターと回線で結ぶことが困難な場所にあるシステムのアクセスコントロールや、クレジットカードを使った支払いにおいて、センターによるオーソリを必要としない小額決済を行う場合等。

[34] 実際には、個人性情報に発行機関のデジタル署名を付したものを記録することが普通である。

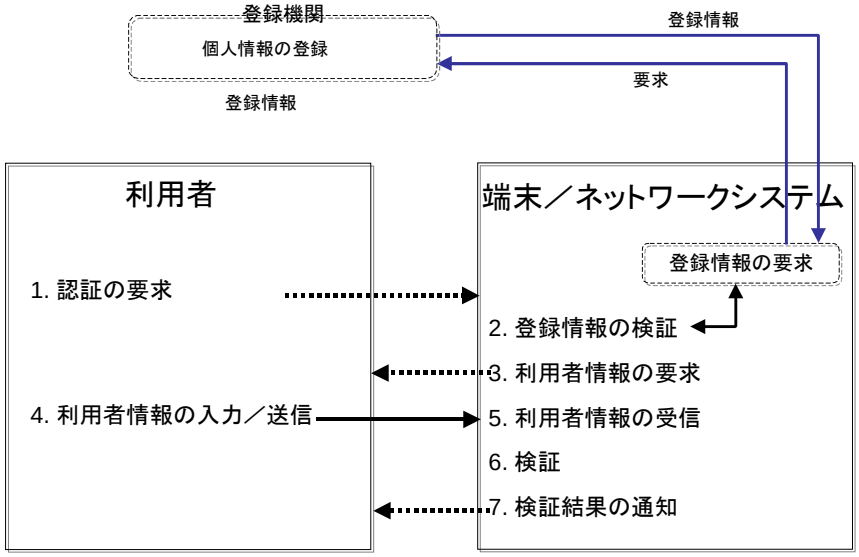
ラメータの類似性を確認する機能を持たせる方式も考えられる[35]。

本モデルの特徴は、認証処理の負荷がセンターに集中せず分散しているため、ユーザーの数が増えたときでも処理がスムーズに行えることや、個人情報を各ユーザーが自ら管理できる点にある。また、ID カードの発行機関がカード発行後に原個人性情報を保有することがなければ、プライバシーの問題はモデルⅠと比較して大幅に軽減できる。したがって、モデルⅡを適用することにより、バイオメトリック認証を普及させる上で主要な課題の一つである社会的なコンセンサスが得られる可能性がある。

このため、バンキングシステムにおいても、本モデルに基づいてバイオメトリック認証を適用することは有用であると考えられる。これには、キャッシュカードの IC カード化を進めることが必要になるが、IC カード化はカード内情報の機密性を確保するうえでも有効である。当面 ID カードの発行機関は各個別銀行となると考えられるが、一行に止まらない共通のインフラとして、バンキングシステム全体で適用するためには、共通の第三者機関が ID カードへの個人性情報の登録および発行を一手に引き受ける方式も考えられる。さらに、この共通インフラとしての第三者機関の実現により、バンキングシステムに限らず、個人認証が必要とされる多くのシステムに本モデルが容易に適用可能となることも考えられる。

(3) モデルIII（個人性情報を第三者である登録機関が保有）

（図18）認証モデルIII



モデルIIIでは、ユーザーはネットワークシステムを介して、第三者である登録機関にアクセスすることを念頭に置いており、個人性情報はすべてこの登録機関が管

[35] ただし、この場合，IC カードの偽造が困難なように、使用される IC カードが耐タンパー性を持つことが特に重要である。

理する点に特徴がある。この登録機関は、公開鍵インフラにおいて公開鍵にお墨付きを与える認証局の機能に類似したものと位置づけられる。

ネットワークシステムは、ユーザーからの認証要求があると、登録機関に登録情報を要求する。この登録情報は、主にユーザーの個人性情報から構成されている。登録情報を入手した後の認証プロセスは、モデルⅠもしくはモデルⅡと同様である。

本モデルは、バンキングシステムにかかわらず、多くの個人認証を必要とするシステムに適用可能である。ネットワークシステムは、登録機関に登録情報を要求する際にユーザーの無効リスト（revocation list）を参照することも可能となる（モデルⅡでは、端末もしくはネットワークシステムから ID カード発行機関へのアクセスは特に示していないが、無効リストの参照を行う際には必要となる）。

個人認証の目的のためには、ユーザーは何も所持する必要がないという意味においては理想的な形態である一方、ネットワーク上を個人性情報が流れるため、これが外に漏れないようなセキュリティ対策や、モデルⅠおよびモデルⅡと同様に、端末内での個人性情報の不正な入手対策を講じる必要がある。

8. バイオメトリック認証に求められる精度

(1) バイオメトリック認証の金融サービスへの適用

前章で説明したどのモデルが金融サービス等に適用されようとも、当面バイオメトリック認証は現状の暗証番号方式に対する補足的な手段として用いられるのが現実的であろう。その場合、バイオメトリック認証に対して極めて強力な安全性を要求する必要は必ずしもない。例えばモデルⅠあるいはモデルⅡにおいては、ユーザーがカードを紛失した場合に、金融サービスを提供する機関がカードの無効化処理を行うまでの間における安全性が、現状よりも向上するという程度でも十分な効果はある。また、安全レベルを幾つか設定して、それをユーザーが自ら選択する形態も考えられる。ここで重要なことは、カード、端末等の小型化、低廉化を十分念頭に置き、バイオメトリック認証の社会的コンセンサスを得る原動力となる実用化を考慮すべきということである。

(2) 複数のバイオメトリック認証の組み合わせの適用

バイオメトリック認証を実装に移す場合、通常は、必要なセキュリティレベルを確保するために、認証精度が一定のレベルに達している認証技術が適用される。しかしながら、個人認証においては、①利用者からバイオメトリック情報を得る際に、心理的、生理的な圧迫感や抵抗感がないか、②プライバシーに十分配慮しているか、③高齢者等にも問題なく扱えるのはもちろん、バイオメトリック情報の取得が不可能な身障者への配慮しているか、④利用者にとって使いやすいユーザーフレンドリーなものか、等の観点からも十分評価し、利用目的への適合性に十分配慮されたシステムとなっていることが大切である。その場合、単体では十分なセキュリティレベルに達していないバイオメトリック技術であっても、複数の認証技術[36]を組み合わせることによって、必要なセキュリティレベルを確保することができるほか、特定のバイオメトリック情報が取得できない身障者等でも、他の認証技術で補完することによって個人認証を行うことも可能である。

複数の身体的特徴、特性を利用したバイオメトリック認証（伊藤・小松他 [1996]）はマルチモーダル･バイオメトリックス（multimodal biometrics）とも呼ばれ（Jain, Boille and Pankanti [1999]）、特に最近関心が持たれている。複数の特徴利用は、単に個人認証の信頼性を高める可能性があるばかりでなく、利用環境あるいは個人の体調等に応じて特徴の選択が可能となり、バイオメトリック認証が広く利用される条件を整備するうえでも重要な技術として位置づけられる。

マルチモーダル・バイオメトリックスは識別と照合の両者に適用可能であり、識別で用いる場合は時間短縮の効果が挙げられる。例えば、第一段階で複数の候補を選択し、第二段階で候補から最終結果を導く手法がある。一方、照合で用いる場合は照合時間の短縮には結びつかず、むしろ照合精度の向上に効果がある点に注意す

[36] バイオメトリック認証に限定される必要はなく、カードや暗証番号との組み合わせなども考えられる。

る必要がある。各特徴パラメータに対する判定結果を総合的に評価する手法には、判定値（類似度）を考慮せずに例えば多数決の論理で決定する提案、また判定値に対して統計的手法を適用する提案等がある。

ここで、2 種類のバイオメトリック認証技術を組み合わせてシステムを構築した場合の本人拒否率、他人受入率について説明する。それぞれの認証技術の本人拒否率を FRR_1, FRR_2、他人受入率を FAR_1, FAR_2 とすると、(a)すべての認証方法をクリアした場合に本人と判断するシステムの本人拒否率は１－（１－FRR_1）×（１－FRR_2）、他人受入率は $FAR_1 \times FAR_2$ となる。すなわち、この場合、本人拒否率は増加し、他人受入率は低減する。さらに、n 種類の認証技術を組み合わせることも可能であり、その場合、本人拒否率は$1-\prod_{K=1}^{n}(1-FRR_K)$、他人受入率は$\prod_{K=1}^{n} FAR_K$ となる。

(a) **すべての認証方法をクリアした場合に本人と判断**

		認証技術 2	
		本人	他人
認証技術 1	本人	本人と判断	他人と判断
	他人	他人と判断	他人と判断

(b) **いずれか一つの認証方法をクリアすれば本人と判断**

		認証技術 2	
		本人	他人
認証技術 1	本人	本人と判断	本人と判断
	他人	本人と判断	他人と判断

一方、(b)いずれか一つの認証方法をクリアすれば本人と判断するシステムでは、本人拒否率は、$FRR_1 \times FRR_2$、他人受入率は１－（１－FAR_1）×（１－FAR_2）となる。この場合、本人拒否率は低減し、他人受入率は増加する。さらに、n 種類の認証技術を組み合わせることも可能であり、その場合、本人拒否率は$\prod_{K=1}^{n} FRR_K$、他人受入率は$1-\prod_{K=1}^{n}(1-FAR_K)$ となる。

また、(a), (b)を組み合わせ、n 種類の認証方法のうち m 種類でクリアすれば本人と判断するという多数決論理を適用した方法や、重要視する認証方法にウェイトを付けて調整する方法も考えられ、本人拒否率と他人受入率の要求条件を同時に満たすように必要に応じて調整を図ることも可能である[37]。

[37] 人間は人が誰であるかを認識するとき、一つのパラメータだけで判断していることはまれであり、顔の形や体格、仕種、声、言葉使い等複数の「個人を特定する特徴」によって総合的に判断していると考えられる。その意味では、このような方式は、人間が実際に行っている判断方法に近いものと言える。

9. おわりに

バイオメトリック認証に関する研究は一部では実用段階へ入りつつある。しかしながら、この技術が実際に個人認証の手段として使われるようになるためには、安全性は当然のことながら、様々な側面について配慮が必要である。例えば、社会的な容認を得るためのコンセンサスづくりの必要性、操作の容易性、端末の小型化・低廉化等である。

特に、バイオメトリック認証においては、個人の身体的特徴等のプライバシーに関わる情報を扱うため、利用者に受け入れられるような社会的な配慮を行うことによって、バイオメトリック認証の導入に関するコンセンサスを得ておくことが必要不可欠である。誰もしくはどの機関がバイオメトリック情報を登録して管理するのか、という運用面の課題も解決されていなければならない。7 章のモデルⅡのように、個人が保有する ID カードで情報を管理し、オフラインで認証を行うのもひとつの方法である。

7 章で述べた参照モデルをもとに、認証システムを具体化するための技術、法規等の検討も必要とされる。さらに、ネットワークを介して広くバイオメトリック技術を利用していくためには、6 章で述べた API の標準化を進めるとともに浸透させ、①適用するバイオメトリック技術変更の容易性、②同一のインターフェースを用いた複数のバイオメトリック技術の利用、③複数のアプリケーションに対するバイオメトリック技術の拡張等を実現する必要がある。

1992 年、英国の金融機関によって組織された決済サービス協会(APACS: Association for Payment Clearing Services)が、バイオメトリック認証に対する基準を策定している。これによると、

- ●タイプⅠエラー：0.001%以下
- ●タイプⅡエラー：5.00%以下
- ●認証時間：3 秒以下
- ●価格：150 ポンド以下
- ●デザイン：単体もしくは組み込み

となっている（European Committee for Banking Standards [1996]）。現状の技術では、いかなるバイオメトリック認証についても単独では上記の基準を満足することは困難と考えられるが、複数のパラメータの組み合わせにより利便性を落とさずに一定の精度を実現できる可能性はあろう。また、こうした基準自体についても、利用環境、保護すべき財産の規模等を考慮した複数のレベルを検討する必要がある。

本稿では、本人確認のパラメータとしてバイオメトリックスを用いるものに着目してきたが、新たな利用の可能性も検討されている。すなわち、バイオメトリックスを公開鍵暗号方式における公開鍵、秘密鍵と本人との結びつきを保証するパラメータとして用いる提案（辻井 [1999]）であり、こうした技術が確立されれば、鍵情報の不正使用を防止したり、公開鍵の真正性を証明するための有効な手だての一つとなろう。

いずれにせよ、バイオメトリック認証は、ローカルで利用されている技術が改良を重ねながら広く世の中に浸透していくものと思われる。バイオメトリック認証は、本人であることを証明するために何かを携帯したり、暗証番号を記憶する必要がなくなる可能性もあり、利用者にとって利便性が高いほか、既存の個人認証方式よりも高度なセキュリティを実現することが期待できる。現在、多くの産業分野で実用化が進みつつあるが、金融取引の安全性を高める手段としても検討に値する認証技術と考えられる。

以　上

【参考文献】

浅井・星野・木地、「マニューシャネットワーク特徴による自動指紋照合」、『電子情報通信学会論文誌』D-II、J72-D-II、5、電子情報通信学会、1989 年、724-732 頁

伊藤・小松他、「ヒューマンステーションのインタフェース技術」、『画像電子学会誌』第 25 巻第 1 号、画像電子学会、1996 年 2 月、79-87 頁

稲田他、「高齢者に優しい技術」、『電子情報通信学会論文誌』第 80 巻第 8 号、1997 年 8 月、812-821 頁

小畑、「個人認証技術の現状と展望」、『システム/制御/情報』第 35 巻第 7 号、システム制御情報学会、1991 年、383-389 頁

川崎、「『網膜』の識別でセキュリティを守る」、『エレクトロニクス』2 月号、オーム社、1998 年、52-54 頁

木下・清水・小松、「個人認証の適用領域とセキュリティレベルに関する一考察」、『1992 年暗号と情報セキュリティシンポジウム』SCIS'92-8C、電子情報通信学会、1992 年 4 月

栗田・長谷川、「顔画像からの個人識別」、『映像メディア学会誌』第 51 巻第 8 号、映像メディア学会、1997 年 8 月、1132-1135 頁

児玉・茨木・小松、「医療通信のための基盤技術」、『画像電子学会誌』第 26 巻第 3 号、画像電子学会、1997 年 6 月、161-164 頁

小林他、「光学的相関演算を用いた指紋照合装置」、『第 1 回画像センシングシンポジウム予稿集』、画像センシング技術研究会、1995 年、25-28 頁

小松、「個人認証の技術動向」、『画像電子学会誌』第 27 巻第 3 号、画像電子学会、1998a 年、196-204 頁

――、「バイオメトリック認証（１）」、『郵政研究所月報』NO.117、郵政省郵政研究所、1998b 年 6 月、108-110 頁

――、「バイオメトリック認証（２）」、『郵政研究所月報』NO.118、郵政省郵政研究所、1998c 年 7 月、73-75 頁

斎藤・松下、「『虹彩』の識別でセキュリティを守る」、『エレクトロニクス』2 月号、オーム社、1998 年 2 月、48-51 頁

坂野、「バイオメトリック個人認証技術の動向と課題」、『電子情報通信学会技術研究報告』PRMU99-29、電子情報通信学会、1999 年 6 月、75-82 頁

佐々木、「ネットワーク署名認証システム Cyber-SIGN」、『インターネットアスキー』Vol.1、No.8、アスキー出版、1996 年

社会安全研究財団 情報セキュリティ調査研究委員会、『情報セキュリティ調査研究報告書』、1997 年 4 月

瀬戸・星野、「指紋照合の自動化技術」、『画像電子学会誌』第 15 巻第 3 号、画像電子学会、1986 年 6 月、184-191 頁

高木、「『掌形』の識別でセキュリティを守る」、『エレクトロニクス』2 月号、オーム社、1998、32-34 頁

田口、「書字による個人識別の技術」、『システム/制御/情報』Vol.35、No.7、システム制御情報学会、1991 年、398-407 頁

辻井、「文明構造・社会概念の変容と情報セキュリティ」、『電子情報通信学会論文誌』第 79 巻第 2 号、1996 年 2 月、98-106 頁

――、「生体情報が秘密鍵に埋め込まれた構造を有する公開鍵暗号方式」、『FAIT (Forum on Advanced Information Technology)講演資料(1999.8)』

電子商取引実証推進協議会 本人認証技術検討 WG、『本人認証技術検討 WG 中間報告書』、1997 年 5 月

――――――――――――――――――――――――――、『本人認証技術検討 WG 報告書 －本人認証の評価基準（第１版）－』、1998 年 3 月

土居・千原、「『顔』の識別でセキュリティを守る」、『エレクトロニクス』2 月号、1998 年、44-47 頁

――・他、「顔画像照合のセキュリティ応用」、『テレビジョン学会技報』MIP’96-55、第 20 巻第 41 号、テレビジョン学会、1996 年 7 月、13-18 頁

中尾・大橋、「移動通信におけるセキュリティ技術」、『画像電子学会誌』第 23 巻第 5 号、画像電子学会、1994 年 10 月、407-415 頁

林、「個人識別技術とそのニーズおよび期待」、『計測と制御』Vol.25、No.8、計測自動制御学会、1986 年、683-687 頁

平山・中村、「色情報と等濃線分布に基づいた顔画像による人物識別方式」、『テレビジョン学会技報』MIP’96-54、第 20 巻第 41 号、テレビジョン学会、1996 年 7 月、7-12 頁

古井、「声の個人性の話」、『日本音響学会誌』第 51 巻第 11 号、日本音響学会、1995 年、876-881 頁

――、「『音声』の識別でセキュリティを守る」、『エレクトロニクス』2 月号、オーム社、1998 年、38-40 頁

松井・古井、「テキスト指定型話者認識」、『電子情報通信学会論文誌』D-II、J79-D-II、電子情報通信学会、1996 年、647-656 頁

――・――、「話者認識研究の現状と展望」、『テレビジョン学会技報』MIP’96-56、第 20 巻第 41 号、テレビジョン学会、1996 年 7 月、19-24 頁

松下・重野、「モーバイル・コンピューティングとコミュニケーションのためのプラトフォーム」、『画像電子学会誌』第 26 巻第 6 号、画像電子学会、1997 年 6 月、639-647 頁

増田、「セキュリティにおける個人認証技術」、『システム/制御/情報』第 35 巻第 7 号、システム制御情報学会、1991 年、431-439 頁

村田、「人を場所・時間的制約から開放するモバイルコンピューティング」、『電子情報通信学会論文誌』第 80 巻第 8 号、電子情報通信学会、1997 年 8 月、844-849 頁

安田、「Things Thinking ―全てが情報発信―」、『画像電子学会第 27 回年次大会予稿集』、1999 年 6 月、63 頁

保原、「24.4 筆跡による識別」、『画像処理ハンドブック』、昭晃堂、1989 年、582-590 頁

吉村・吉村、「筆者認識研究の現段階と今後の動向」、『電子情報通信学会技術研究報告』Vol.PRMU96-48、電子情報通信学会、1996 年、81-90 頁

吉村他、「筆者認識研究の現段階と今後の動向」、『電子情報通信学会技術研究報告』PRMU96-48、電子情報通信学会、1996 年、81-90 頁

山崎・小松、「身体的特性に基づく個人認証システムにおける個人性の抽出手法」、『電子情報通信学会論文誌』Vol.J79-B-I、No.5、電子情報通信学会、1996 年、373-380 頁

郵政省郵政研究所、『個人認証技術と通信システムへの応用に関する研究調査報告書』、調-93-V-06、1993 年 3 月

「特集 個人認証・識別はどこまで可能か？」、『エレクトロニクス』2 月号、オーム社、1998 年

「分解能 500dpi の指紋検出器」、『日経エレクトロニクス』No.709、日経 BP 社、1998 年 2 月、149 頁

『週間文春』、文藝春秋、1995 年 10 月 12 日号

「『本人確認』の技術開発花ざかり」、朝日新聞、1996 年 7 月 21 日

「機械の目で本人確認」、読売新聞、1997 年 1 月 10 日

「筆跡などで本人確認」、日経産業新聞、1997 年 7 月 20 日

「指紋ビジネス進化」、朝日新聞、1998 年 3 月 5 日

D. W. Davis and W. L. Price, “Security for Computer Networks,” John Wiley & Sons, 1989, pp.169-208.

European Committee for Banking Standards, ”Biometrics: A Snapshot of Current Activity,” 1996. (http://www.ecbs.org/download.html)

F. Galton, “Personal Identification and Description,” Nature, 1888, pp.173-177.

A. Jain, R. Boille and S. Pankanti, "Biometrics -Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

B. Miller, “Vital Signs of identity,” IEEE Spectrum, Institute of Electrical and Electronic Engineers, New York, 1994.2, pp.22-30.

R. Plamondon and G. Lorette, “Automatic Signature Verification and Written Identification-The State of the Art,” Pattern Recognition, volume 22, number 2, 1989, p.109.

Y. Yamazaki and N. Komatsu, “A Proposal for a Text-Indicated Writer Verification Method,” IEICE Trans., Vol. E80-A, No.11, 1997, pp.2201-2208.