

1 バイオメトリックセキュリティ 認証技術の動向と展望

瀬戸 洋一

首都大学東京 産業技術大学院大学
seto.yoichi@aait.ac.jp

バイオメトリックセキュリティ認証技術とその活用状況について、現在の動向および今後の展望を概説する。特に金融機関のATMや入出国管理の電子パスポートにおける本人認証など、社会インフラに広く利用され始めた現在の状況と今後の展望について解説する。

バイオメトリクスで本人を認証する

■ バイオメトリクスとは

Biometricsは、行動的あるいは身体的な特徴を用い個人を自動的に同定する技術であり、そのままバイオメトリック（生体）認証技術と表記できるほど、一般的な言葉になっている。表-1に示すように、バイオメトリクスには身体的な特徴と行動的な特徴の2種類ある。前者は、指紋、掌形、顔、虹彩、静脈などが相当し、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、署名は上記の身体的特徴（Physical Characteristics）の生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（Behavioral Characteristics）と呼ばれる¹⁾。

本人を確認するには、たとえば、指紋の場合、終生不変、万人不同の性質を持つ特徴点が個人個人に特有に存在することを利用している。

特に最近、日本では静脈認証技術が注目されている。たとえば、指静脈パターンは千差万別であり、個人差が大きく生体内部の情報であるため外観からは識別されに

	情報	特徴量	普遍性	唯一性	永続性	コスト	拒否率 (%)	受入率 (%)	データ量 (Byte)
* 1	 指紋	手指の指紋特徴量	◎	◎	◎	◎	1.0	0.01	250
	 掌形	手の大きさ・長さ・比率	◎	○	○	△	0.1	0.1	10
	 顔	顔輪郭、目・鼻の形・配置	◎	△	△	○	5	5	2,000
	 虹彩	虹彩の放射状紋様	◎	◎	◎	△	10	10 ⁻⁶	200
	 静脈	手指の静脈特徴点	◎	○	○	△	1.0	0.01	500
* 2	 声紋	話者の音声特徴	◎	△	△	◎	10	10	1,500
	 署名	字体、書き順、筆圧	◎	△	△	○	5	5	1,000
	その他、網膜、耳形状、匂い、DNAなど								

* 1: 身体的特徴, * 2: 行動的特徴

表-1 バイオメトリック認証技術の比較



- ・本人の意思がないと入手が困難（盗難耐性）
- ・表皮の汚れなどに依存しない（高信頼性）

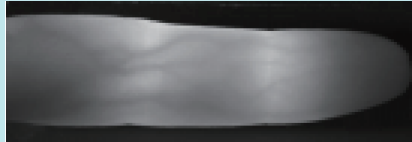
■指の静脈による個人認証の概要



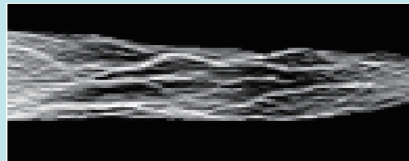
光源：近赤外線LED
カメラ：近赤外高感度
モノクロCCDカメラ

入力画像

近赤外光による透過画像



照合用画像



認識方法 指の静脈パターンのマッチング

図-1 指静脈認証技術

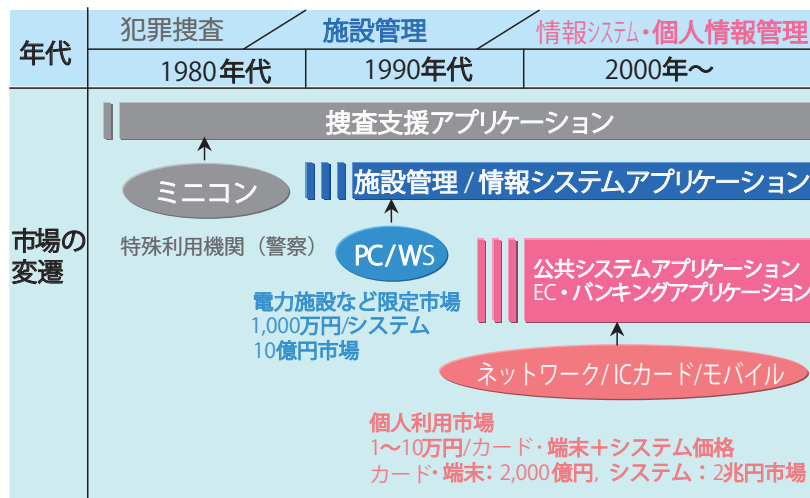


図-2 バイオメトリック認証技術・製品の推移

く、また、表皮の状況、たとえば汚れなどに認証精度が影響されない、本人の同意がないと取得が難しいことから、信頼性および安全性の高い個人認証技術といわれている²⁾。

指静脈認証技術は、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、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、生体組織に対して透過性が高い一方、血液中の酸素を失った還元ヘモグロビンには吸収されるといった特徴があるため、近赤外光を指に照射すると、図-1

に示すような指の静脈が影となって画像に現れる。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^{3), 4)}。

■バイオメトリックセキュリティ

バイオメトリック技術および製品開発の動向を図-2に示す。コンピュータで指紋などの認識技術が開発されたのが第1期、高性能な低価格のコンピュータが出て施設管理用途、たとえば、入退室に利用されたのが第2期、現在は第3期に相当し、IC管理カードなどとの連携により、ネットワーク応用や社会基盤系における応用が展開



図-3 日本の市場の立ち上がり

されている。

2000年代になりバイオメトリック認証技術が、画像処理製品からセキュリティ製品に様相を変えている。つまり、セキュリティに関する以下の脅威を防ぐことを考慮した製品が開発されている。

- ①機密性の喪失 (Confidentiality)：情報を不当に覗かれる、あるいは盗まれる
- ②正確性・妥当性の喪失(Integrity)：情報を不当に改ざん、破壊される
- ③可用性の喪失(Availability)：保存されている情報が外部からの不当な利用で使えなくなる

以上を考慮し対策した技術をバイオメトリックセキュリティ (Biometric Security) 技術あるいはバイオメトリックシステムセキュリティ (Biometric System Security)技術と呼ぶ^{2), 6)}。

具体的には、

- ①生体か非生体 (偽造) かを判別する能力 (正確性・妥当性)
- ②バイオメトリックデータのプライバシーの保護を考慮した技術 (機密性)
- ③盗聴盗難や改ざんを防御できる機能を有する能力 (機密性、可用性)

を所持した技術・製品を指す。技術の事例は後述する。

日本の市場動向

日本の市場では、社会ID (証明書) システム、個人情報保護、金融システムの3つの分野の製品が展開されている (図-3参照)。

■入出国審査システムへの展開

2001年9月11日以降、米国は国の安全保障のためにバイオメトリクスが重要な技術であることを認識した。このために米国国土安全保障省 (DHS: Department of

Homeland Security) を2002年11月に設置した。DHSは、入出国管理の強化を目的に、外国人にバイオメトリックデータの提示を義務付けるUS-VISITプログラムを実施した。US-VISITは、2002年5月14日に成立した米国内閣警備強化・ビザ入国改正法に基づき発表されたプログラムである。2004年1月5日から実運用され、米国入国の際、外国人の顔、指紋のデータを取得している。

日本でも同様のテロ対策システムを導入するため、バイオメトリック技術の位置付けを明確にする入出国管理法案の改定が2006年度国会で検討されている。

電子パスポートに関しては、ICAO (国際民間航空機関 International Civil Aviation Organization) で仕様の検討が行われ、2004年電子パスポート基本仕様書を公開した。本仕様はLDS (論理データ構造) を決め、保管するバイオメトリクスは顔を必須とし、指紋、虹彩はオプションとするものである。なお、ICAOで策定された仕様はISO/IEC JTC1/SC17 WG3およびSC37 WG3で国際標準化作業を行い、国際標準となっている。

日本の外務省は2006年3月より電子パスポートを正式に発行している。また、今後は、社会IDとして社員証など広い分野での展開が期待できる。

■金融システムへの展開

日本では印鑑を中心とした本人確認の社会的基盤ができていたが、昨今、コンピュータやカラーコピー機の出現により、通帳、印鑑などの偽造が簡単に行われ、問題となっている。このため、これに代わる本人確認としてバイオメトリック技術が注目されている。

インターネットバンキング、ATMなど人が介在しない認証には盗難耐性とユーザ利便性の高い指静脈技術などの導入が発表されている。

一方、口座の新規開設や、解約には、社会基盤における認証手段として整備される、ICカード運転免許証や電子パスポートに導入されている顔認証、指紋認証の適用が検討されている。基本的には電子パスポートなどで構築されるシステム技術が転用できるが、金融特有の技術課題も多々ある。

■個人情報保護応用への展開

2005年4月1日に個人情報保護法が完全施行された。これに伴い、個人情報の漏えいには罰則規定が実施される。このため、情報管理強化に指紋認証が実装されたモバイルPCの市場が立ち上がっている。ただし、現時点では、パスワードとの併用であり、セキュリティ対策が十分な製品は出ていない。

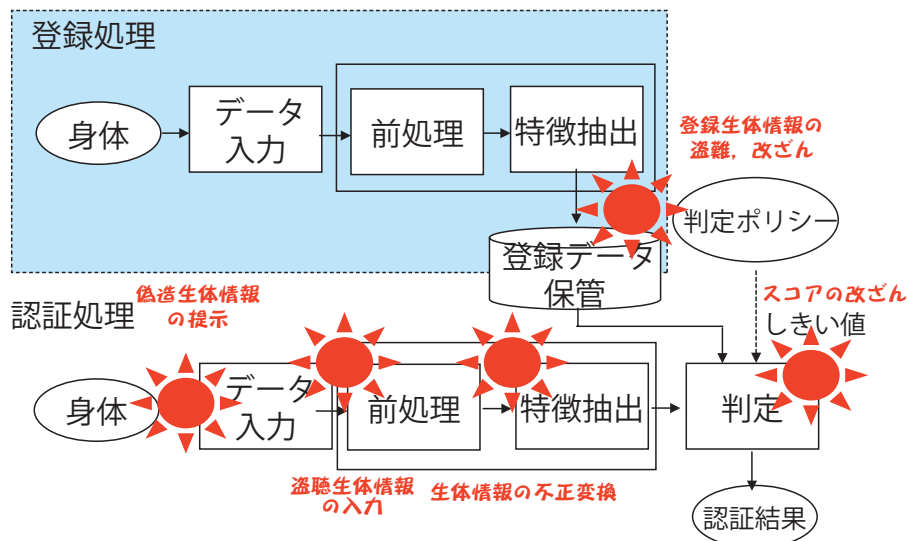


図4 バイオメトリック認証システムにおける脅威

バイオメトリックスの技術的・社会的課題

■ プライバシーの問題

バイオメトリックデータに関するプライバシー問題は、バイオメトリックスが身体的な情報を利用しているがゆえに生じる。つまり、

- ① 取り替えのきかない情報である：身体的な情報であり、たと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できない。
- ② 本人の同意なく収集可能なものが多い：一般にバイオメトリッ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：バイオメトリックスは個人と直接リンクした情報であるため、バイオメトリック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：バイオメトリックスによっては、たと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。

バイオメトリック認証はパターン認証の枠組みの中に位置付けられる。典型的なバイオメトリック認証システムの処理フローを図-4に示す。

第1ステップは利用者からの身体情報の取得である。指紋は電子的なスキャナ、顔はカメラ、声紋はマイクロフォンによって取得される。

入力された身体情報は、取得される条件が毎回異なるため変動したものであり。たとえば、身体の変動として、指先の汚れ、風邪による声のしゃがれなどである。また、

入力する装置側の変動として、顔を撮影する場合の照明光の条件、乾燥あるいは湿気などによる指紋センサの表面条件などである。これらの変動条件の補正も含め、入力された身体情報から個人特有の特徴を抽出する処理を次に行い、登録処理においては、個人特有の特徴量をテンプレートデータとしてデータベースに保管する。

認証処理においては、利用者を特定する利用者IDを入力し、相当するテンプレートデータベースから検索し2つの特徴量の類似度を求め、類似度がある決められた数値以上の場合には認証が成功したとして、アプリケーションの利用権限を得られる。テンプレートデータはデータベースで集中管理せず、個人がICカードなどで持つモデルもある。

次に、バイオメトリック認証システムをセキュリティ技術の観点から分析する。

バイオメトリック認証システムにおける攻撃つまり不正利用のアプローチを受ける場所はいくつかある。攻撃脅威の一例を表-2に示す。

- ① センサへの偽の身体情報の提示：この攻撃は、偽の身体情報がシステムへ入力されるなりすまし攻撃。たとえば、偽造の指、偽の署名、顔写真を貼った覆面などが使用される。
- ② 蓄積された身体情報の再入力：この攻撃は、センサを介さずに、以前に入力された身体情報が入力されるリプライアタック攻撃。たとえば、以前使われた指紋情報の再使用、または、音声の再生などによる攻撃である。

バイオメトリクスの問題		セキュリティ上の問題	対策
取り替えの きかない情報	身体的な情報であり、たと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。	・盗難 ・許可しない クロスリファレンス	・キャンセラブル バイオメトリクス ・チャレンジレスポンス ・電子透かし ・暗号化
本人の同意なく 収集が可能	一般に身体情報が身体の上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。	・盗難(スプーフィング) ・法的責任能力	・バイオメトリクスの 適正選択
データから 本人を特定	身体情報は個人と直接リンクした情報であるため、身体情報から逆に本人を特定することができる。	・プライバシーの侵害	・キャンセラブル バイオメトリクス ・暗号化
本人の副次的な 情報を抽出	身体情報によっては、たと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。	・プライバシーの侵害	・運用ガイドライン ・暗号化
生体が非生体かの 判定が困難	センサ入力された情報が身体から直接入力されたものか否かの判定が難しく、場合によっては模造品を入力許可することがある。	・偽造 ・なりすまし (スニファリング、 リブライアタック)	・生体検知機能 ・チャレンジレスポンス 耐タンパセンサ

表-2 バイオメトリクス特有の課題とその対策

■バイオメトリック認証システムへの不正防止技術

バイオメトリック認証システムにおける不正利用に関する対策技術は、まだ研究開発に着手されたばかりである。代表的な方法としては以下がある。本方式の詳細は文献2)を参照。

- (1)可変認証文字の電子透かし埋め込み方式
- (2)画像に対するチャレンジレスポンス方式
- (3)取り消し可能な(Cancelable)バイオメトリクス方式

特にキャンセラブルバイオメトリック技術は非常に注目されている技術である。バイオメトリクスは、それ自身で識別を確実に行えると同時に、身体の一部であり、変更ができないという事実がある。これは個人認証における長所であるが、運用においては避けることのできない欠点となる場合もある。この欠点を軽減するための方式が「取り消し可能な(キャンセラブルな)バイオメトリック認証技術」である。この方法は、意図的に反復可能なかたちで選択した変換方法によりバイオメトリックデータを歪ませる方法である。図-5によれば、バイオメトリック情報を登録の時、また、各々の認証の時に異なる歪みを生むようにする。バイオメトリック情報は登録のたびに異なる歪みを生じるので、バイオメトリック情報の信頼性が失われた場合、その時使用していた歪曲方式を変更し、新しい方式に基づく再登録を行って、バイオメトリック認証を行えばよい。

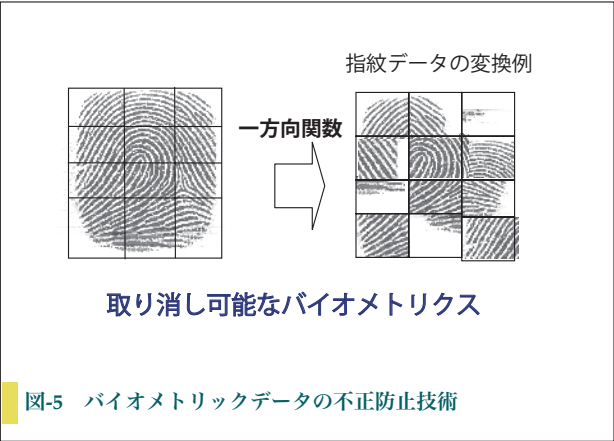


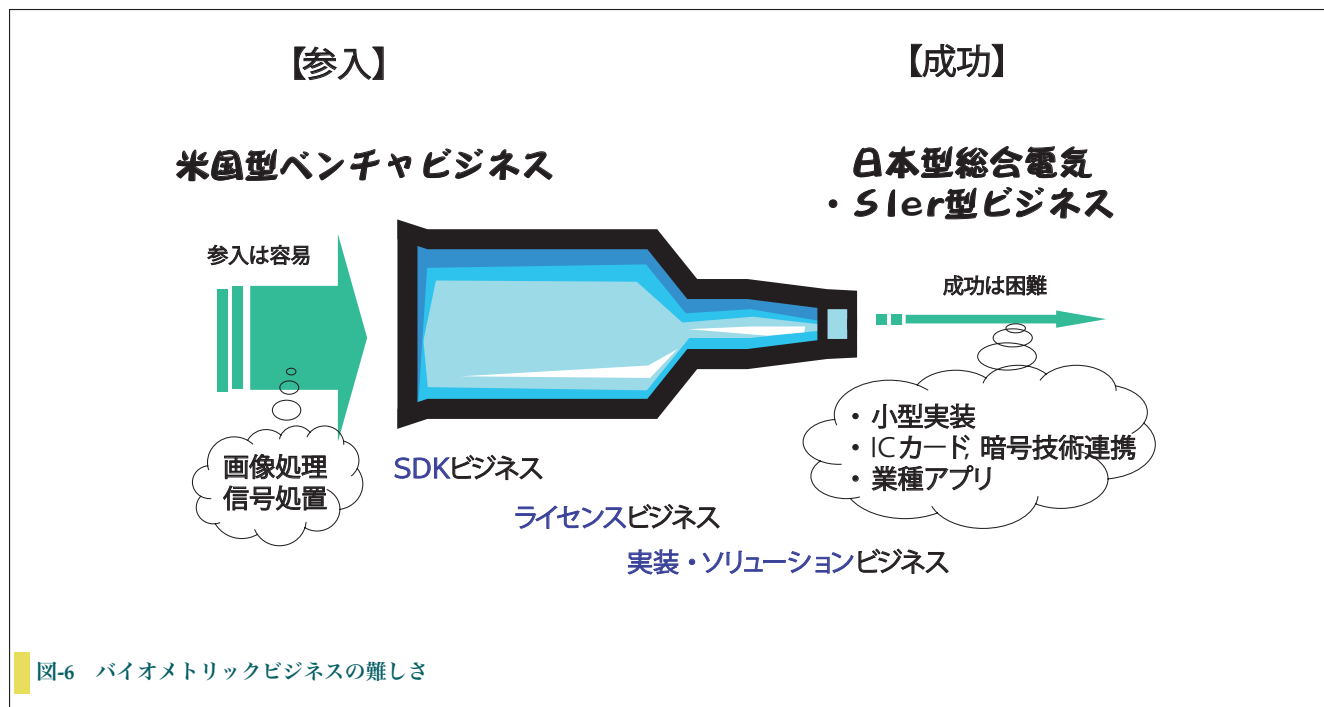
図-5 バイオメトリックデータの不正防止技術

■セキュリティ強度

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、セキュリティ的な強度を明確にする必要がある。他人受け入れ誤差や本人拒否誤差はパターン認識での精度であり、セキュリティ強度にそのまま読み替えることはできない。

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たり攻撃（暗号の鍵をすべて生成し攻撃する）に対する情報空間で表すが、その方法としては、2つの研究例がある。まだ、どの方法が妥当かの結論は出ていない。本技術に興味がある方は文献2)、5)を参照。

- (1) FAR（他人受け入れ誤差）から算出する平均攻撃空間：エントロピーの概念を用いFARから攻撃空間を類推する



(2) 指紋特徴点への総当たり攻撃：たとえば偽の特徴点を生成しそれを用い攻撃する

標準の意義

バイオメトリックスの技術開発およびビジネス展開において、国際標準化は重要な意味を持つ。バイオメトリック技術の国際標準化は、2002年に発足したISO/IEC JTC1/SC37で行われている。SC37は、一般的なバイオメトリック技術に関する標準化を担当する。

標準化の意義としては、以下がある。

- ①世界中で利用される→相互運用ができないといけない
- ②システムが大規模になる→複数のベンダで開発できないといけない
- ③セキュリティ製品→第三者が評価しなければいけない

今後の展望

本稿では、バイオメトリック認証技術をセキュリティの観点から概観した。本稿では述べなかったが、ISO15408、ISO17799などのセキュリティを考慮したシステム構築、運営などのアプローチも重要である。応用事例、セキュリティ技術および国際標準化動向の詳細に関しては、個別の解説をご覧になっていただきたい。

バイオメトリック認証システムビジネスの状況を図示すると図-6のようになる⁶⁾。

バイオメトリック技術は基本的に画像処理あるいは信号処理技術からなる。このため、1990年初頭、米国の

大学の博士課程をでてそのままベンチャ企業を設立する企業家が多かった。参入のしやすいビジネスであった。そのビジネスは単一のバイオメトリック製品のツールキット商売であった。その後、ツールキット商売では儲けられず、ライセンスビジネスに展開した。しかし、単一のバイオメトリック製品、たとえば、指紋だけでは実システムへの適用はできず、ICカードとの連携、複数のバイオメトリックスを用いるマルチモーダル技術が重要となり、そのつど、米国では会社の合併が生じた。しかし、バイオメトリック技術は、アルゴリズム、精度評価、適用システムのノウハウが重要であり、ビジネスに成功するための狭いビン口から出るようなビジネスの形態といえる。出口を出すためには、小型実装の製品化力、適用先アプリケーションを熟知することが必要であり、情報家電メーカー、システムインテグレータが成功をリードするビジネスといえる。これは、日本の得意な分野といえる。

今後は、実装面の技術開発が必要なことと、脆弱性情報などの管理、また、精度評価情報を管理する評価センタの設置が重要と考える。

参考文献

- 1) Bolle, R. M., Connell, J. H. et al. : Guide to Biometrics, Springer (2004).
- 2) 瀬戸洋一：バイオメトリックセキュリティ入門, SRC (Aug. 2004).
- 3) 王 欣, 清水孝一ほか：指の透視光による個人同定法の基礎的検討, 信学技報, pp.43-49, MBE2003-135 (Mar. 2004).
- 4) (社)日本自動認識システム協会：すぐわかるバイオメトリックスの基礎, オーム社 (Sep. 2005).
- 5) R. Smith著, 稲村雄監訳：認証技術, オーム社 (Apr. 2003).
- 6) 瀬戸洋一：技術の真髄 生体認証論, pp.109-116, No.272 BP (Jan. 2006).

(平成18年4月28日受付)