解　説　論　文

バイオメトリック認証技術の研究開発と製品化への期待

Expectations for Products and Research & Development of Biometric Authentication Technology

瀬戸洋一 Yoichi SETO

アブストラクト　日本におけるバイオメトリック技術は，2004年に金融機関のATM（Automated Teller Machine）への静脈認証装置の採用，2006年にはIC旅券，2007年にはIC運転免許証への顔データの実装というように，社会基盤システムに着実に展開された．2010年を境に米国においてバイオメトリック市場のパラダイムシフトを目指す「Post 9.11」という動きがでてきた．次のステージに向けた市場の拡大の可能性はあるが，民生利用や行政サービスなどに利用されるには，バイオメトリクス特有の問題への対策が以前にも増して重要となっている．つまり，識別，認証のほか，ビッグデータ分野への応用として追跡という新しい利用分野が立ち上がり，これらの市場拡大には，プライバシーへの対策技術が重要である．本解説では，今後必要な技術開発および製品化のポイントについて述べる．

キーワード　セキュリティ，プライバシー，バイオメトリクス，認証，識別，追跡，国際標準

Abstract　Biometric technologies in Japan, which are the adoption of vein authentication device to ATM (Automated Teller Machine) of financial application in 2004, and e-passport in 2006, the implementation of face data to the IC driver's license card in 2007 and so on, have been expanded steadily in social infrastructure system. Movement to paradigm shift of biometric market in the United States as a boundary in 2010 called “Post 9.11” came out. There is a possibility of expansion of the market towards the next stage, but to be used, for example, administrative services and civilian use, it is important countermeasure to the problem of biometrics specific than ever before. One example is a protection of privacy issue. This paper describes the point of commercialization and technology development needed in the future.

Key words　Biometrics, security, privacy, verification, identification, tracking, International Standardization

1．はじめに

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．国際標準の用語定義では，「個人の行動的および生物学的特性に基づいた個人を自動認識する技術」としている[(1)，(2)]．

バイオメトリクスの重要性が認知されたのは2001年である．同年9月11日に起った米国同時多発テロを境に，バイオメトリクスへの評価が大きく変化した．それ以前は，バイオメトリクスは使えるか使えないのかといった導入賛否の議論が行われていた．利用も，重要施設の入退出管理などの市場に限定されていた．しかし，9月11日を境に，なぜ使わないのか，本人確認における主流の技術であるという導入を前提とした意見が大勢となった．

バイオメトリック認証技術は，従来，入退出管理への利用が主であった．現在は，PCなどのモバイル端末のアクセス管理や金融機関における本人認証など，非対面の状況でサービスに対する本人を同定するための手段として利用が拡大している．今後のデジタル社会のさまざまな分野での応用が期待されている．

図1に示すように日本におけるバイオメトリック技術は，2004年10月に金融機関のATM（Automated Teller Machine）への静脈認証装置の採用，2006年にはIC旅券（顔認証），入国管理システム（指紋），2007年にはIC運転免許証への顔データの実装というように，社会基盤システムに着実に展開され

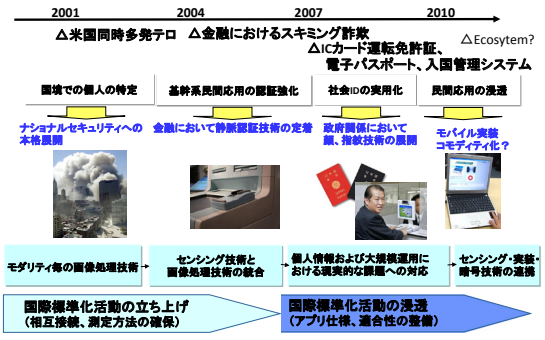

図1　9.11からpost9.11へ

瀬戸洋一　　正員　産業技術大学院大学　産業技術研究科　情報アーキテクチャ専攻
E-mail　seto.yoichi@aiit.ac.jp
Yoichi SETO, Member, (Advanced Institute of Industrial Technology, Master Program of Information Systems Architecture, Tokyo, 140-0011 Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.8 No.2 pp.〇–〇 2014年10月

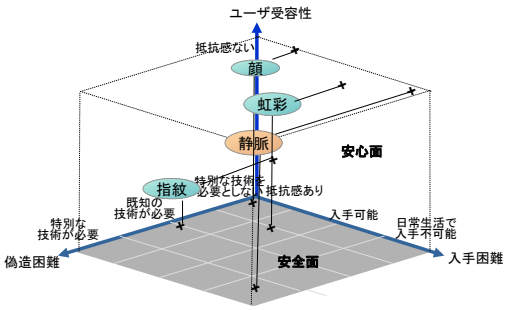

図2　安全安心を実現する静脈認証技術

た[3].

日本の市場で特記すべき点は，複数の大手ベンダーが静脈認証技術を開発し市場投入していること，および大手SI企業が，社会ID（個人識別子）関係で利用される指紋認証，顔認証で世界トップクラスの技術をもちグローバル展開していることである[3].

市場規模は，世界で7,000億円，北米30 %，アジア25 %，中近東アフリカ20 %，ヨーロッパ15 %である．応用分野は，社会IDと犯罪捜査関係70 %，入退出10 %，民間利用ID10 %である．モダリティ利用割合は指紋が60 %，顔20 %，虹彩10 %，静脈3 %である[4]．フォレンジック用途（犯罪捜査用途）で市場形成されていたが，今後は，非フォレンジック用途である民間ID分野，モダリティは静脈の成長が期待できる．

静脈認証は，図2に示すように

① 犯罪捜査には使われず抵抗感がない．
② 露出や遺留がなく，本人の同意と専用装置がないと採取が困難であり，偽造に対して安全である．
③ 表皮の汚れに影響されにくく高信頼である．

などの優れた特徴が普及の要因となっている．また，国内における企業間競争により製品性能が著しく向上した．

現在，バイオメトリック市場のパラダイムシフトを目指す「Post 9.11」という動きがでてきた．つまり，フォレンジック用途から，民生応用という次のステージに向けた市場の拡大に期待が大きい．

民生利用や行政サービスなどに利用されるには，バイオメトリクス特有の問題への対策が，以前にも増して重要となっている．

その一つはセキュリティとプライバシーへの対策である．バイオメトリクスは矛盾する性質をもつ技術だと言える．例えば，バイオメトリクスは究極の個人情報であり，体ひとつで認証できる反面，保管されたデータが漏えい・盗難された場合，プライバシーの問題が生じる[1].

次に国際標準への準拠である．相互接続や性能に関するルールが明確ならば，ユーザーの製品選択において透明性が増す．一方，ベンダーにとってもビジネスチャンスが増えるメリットがある[5].

本解説では，バイオメトリック認証技術の最新状況について，技術，市場，国際標準の観点から俯瞰する．

2. 安全安心なバイオメトリック認証技術の実現

2.1　バイオメトリクスの脆弱性

システムのセキュリティ上の弱点（脆弱性）に対する考えは，バイオメトリック認証装置が，画像処理装置として扱われていた時には問題なかった．しかし，ネットワークに接続され本人認証に使われるようになり，セキュリティ上の問題（例えば，他人に成りすます．特徴量を盗難される．）を検討する必要がでてきた[1], [6].

画像処理装置の場合，カタログにはパターン認識の精度と処理時間の2つを記載すれば，製品性能を把握できたが，セキュリティ製品になり，脆弱性への対策機能などについても言及する必要がでてきた．つまり，システムのセキュリティ強度および，偽の身体情報を提示された場合，それを検知する生体検知技術などの実装の有無が製品仕様上，重要となる．

また，脆弱性への対策技術は，脅威の洗い出し（攻撃）とその対策のペアで開発するべきである．脆弱情報の公開のフレームワークがないことが，現在問題である．紙幣やコンピュータウイルスに関しては，法的に罰則規定が明確であり，その公開の方法もルール化されている．なんらかの公開フレームワークを作らないと，バイオメトリクスの技術は社会に根付かないと考える[6], [7].

2.2　特徴量の漏えい

システム内で管理する個人データ（特徴量）漏えいに関する問題は，2つの観点で考慮する必要がある．プライバシー情報の流出とデータの不正利用の問題である．顔，指紋，DNAはプライバシー度が高いとされている．静脈や虹彩はデータが氏名などの属性情報と一緒に漏洩された場合は，プライバシー流出になるが，それ以外は問題にならないというのが定説であり，データベースを適切に構築すればよいと考える．

一方，データの不正利用に関しては，偽造の生体特徴を作成し，成りすまし利用の問題があるが，センサー部分の生体検知技術の開発が有効である．一般的には，データは撮影データそのものではなく特徴量で保存されるため，偽造は困難である[6].

データの不正利用や，情報漏えいに対し，しきい値秘密分散法によるVisual Cryptography技術の研究開発も行われている[8].

ただし，脆弱性に関しては，安全性を客観的に測定できる評価尺度が重要である．これに関しては，2つの研究が実施されている．

(1) ウルフ攻撃確率：

バイオメトリック認証システムへの「なりすまし」に対するセキュリティ評価尺度として，他人受入率が使用される．ただし，他人受入率は，複数のテンプレートに対し

表1　海外におけるバイオメトリックシステムに関するPIA実施状況

ケース スタディ	概要	評価	効果
カナダ 運転免許証	カナダからUSへ容易に入国が可能とするため、USDHSにより発行された運転免許証 EDLは、RFIDチップにバイオメトリクスを実装したカードである。EDLのデータはUSの役所でシェアされる。	C+ 十分なPIA報告書がウエッブに公開されていない。 PIA報告書は、どのように利用されるか、助言をどのように利用するのか、明確にターゲットとなる関係者を識別できない。	PIAの結果、例えば、カナダのデータベースを検索するとき、US政府機関へ特定のアクションをとることができる。
ニュージランド 労働省におけるバイオメトリクスの収集	ニュージーランドの労働省は、入国し就労を希望する人々を識別するためバイオメトリック情報を収集し利用している。 バイオメトリック情報は、パートナーであるオーストラリア、カナダ、ニュージーランド、英国、米国で共有化している。	A- 報告書は、ウエッブサイトで公開されているが、見つけるのは容易ではない。 報告書は、PIAの実施時期、期間についての詳細が欠けている。	PIA報告は、きまった手順で統一されたドキュメントとして開発されている。2012年2月以来、PIAはアップデートされ、プライバシー評価は一つのプロジェクトととして完結している。
米国 USVISIT	US-VISITプログラムは、バイオメトリクスとRFIDなど異なる技術を組み合わせたソリューションとしての開発が増加する。米国を出入国する人を記録するシステムを構築する。 個人毎に入国に必要な個人識別を含む。	B PIA報告書はどのようにプログラムは改善したかを明確にしていない。しかし、簡単な表記に終わっている。 リスク分析に関しては、簡単なディスカッションしか行われていない。 プライバシーに関しレベルの低い設計の可能性がある。	USVISITの初期の高レベルな設計選定は法令で事前に決まっている。更なる設計選定はプライバシーリスクが回避か軽減かが検討されている
ニュージランド Google Street View	グーグルストリートビューは、公的な空間から360度撮影可能なカメラで撮影した画像を利用するアプリをもっている。2008年にグーグルは、ニュージランドでストリートビューをはじめた。	D+ PIAはプロジェクトの開始前に実施されていない。設計着手への反映ができていない。ステークホルダーへの助言の詳細がない。	Google street view のPIA報告は多くの助言をおこなっている。自動的に顔や車番をぼやかす技術において継続的な改善が必要 ユーザへのフィードバックに基づいた問題のレポートツールを継続的に調整必要。

て一致と誤判定される入力情報（ウルフと呼ばれる）を用いてなりすましを行う攻撃への耐性を評価する尺度ではない．そこで，一致と誤判定されるテンプレート数が最大となるウルフを用いる攻撃への耐性を評価する尺度であるウルフ攻撃確率が開発された[9]．

(2) Fault Tree Analysisによるリスク分析：

バイオメトリック認証システムの安全性を確保するためには，データの漏えいによるプライバシー問題や漏えいデータの再利用によるなりすましの問題がある．これらの問題への対策として，データ暗号化，生体検知，キャンセラブルバイオメトリクスが開発されている．これらの技術は別々にその効果が論じられているが，システム全体の安全性の確保の観点から，対策技術の適用効果や効果的な組合せについての検討がなされていない．このため信頼性解析手法であるフォールトツリー分析を用いて，バイオメトリック認証システムの安全性に対するリスク分析を行う．これにより，各対策技術の有効性を定量的に評価できることを示した[10]．

以上のように，バイオメトリック認証システムや技術の安全性強化のためには，セキュリティ評価方法の確立，運用を考慮したシステム的観点での研究開発が必要である．

2.3　プライバシーへの配慮

バイオメトリクスは究極の個人情報でもある．したがって，バイオメトリック認証システムの開発や運用においてプライバシーの観点からの評価が必要である．バイオメトリクスは，本人の許可なく，収集できるものが多い，また，データから個人を特定できる，あるいは，認証に必要ない性別，人種，病状などの情報も把握できてしまう．

日本では，個人情報を扱うシステムを構築，運営する際，プライバシーへの配慮が適切か評価する仕組みが整備されていないことも問題である．米国，カナダなどでは，プライバシー影響評価（Privacy Impact Assessment）という事前評価フレームワークがある．EUでは，個人情報を扱うシステムでは，PIAを実施することを義務付けている[11]～[13]．例えば，EC委員会の文書（EU（COM）2010/609/EC，4 Nov. 2010）では，PIAを個人データ保護における包括的なアプローチとしており，新しいデータ保護法にPIAを含める予定と伝えている．

米国は，電子政府法第208条および国土安全保障法第222条で，「各行政機関が個人情報を直接的または間接的に推定可能な方法で収集する場合，または配信するための情報技術を開発または調達する場合，事前にプライバシー影響評価を実施することを義務付けている．各行政機関は予算を要求するシステムに対するPIA報告書の写しを行政管理予算局OMB（Office of Management and Budget）長官に提出しなければならない.」としている．また政府省内にチーフプライバシーオフィサーCPO（Chief Privacy Officer）を任命することを義務付けている．

韓国は2011年秋個人情報保護法を改正したが，その中でPIA実施とCPOの設置を明記した．

表1にバイオメトリクスに関するPIAの実施状況例を示す．日本では，2006年法務省入国管理システムにおいてPIAが試行された．また，民間企業における認証システムに関しPIAが実施された．

3．国際標準活動のトピックス

バイオメトリクスの国際標準を開発するのはISO/IEC JTC1/SC37である．SC37における最近のトピックスを紹介する．図3に示すようにSC37は6つのワーキンググループから構成されている．WG2，3はベンダーが開発において強く関与する．一方，WG4，6はユーザーがシステム導入に際し考慮すべき仕様などが規定されている．WG1，5はベンダー，ユーザー両者に重要な用語や性能要件を規定している．最近はユーザーの視点での開発が重要となっている[5]．

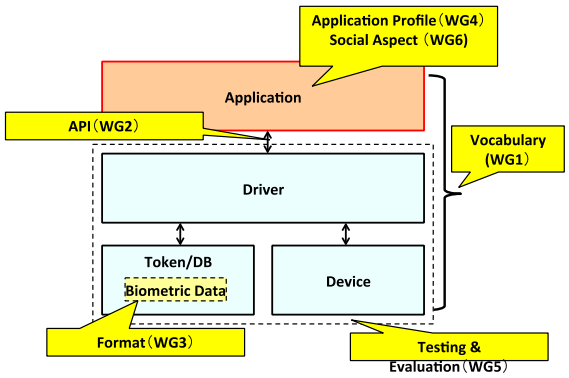

図3　SC37委員会の標準化対応

バイオメトリックシステムは社会IDにおける利用など大規模化している．また，複数のアプリケーションが関わるなど複雑化している．利用者も一般市民などが利用するため，社会的弱者対応やプライバシーの確保などのユーザビリティ，アクセスビリティなどの配慮が必要となっている．

今後重要となる規格を3点紹介する．

(1) Extensible Markup Language

図4に示すように，データの記述の方法には，テキスト形式とバイナリ形式がある．バイナリ形式で記述した場合，利用にあたって特定のソフトウエアが必要であるが，テキスト形式の場合は不要である．XML (Extensible Markup Language，拡張可能なマークアップ言語) である．

文字列で機能を記述していくため，データは基本的にテキストファイルである．項目ごとにタグで囲まれるため，データが何を示しているかが明確であり，不特定多数がデータを処理する場合に有効である[14]．

従って，国民IDやe-passportへの利用のように大規模化するバイオメトリックシステムにおいて，XMLの利用は，システムを効率よく構築するために重要な技術となる．

(2) Biometric Identity Assurance Services

BIAS (Biometric Identity Assurance Services) はWebサービスを想定したバイオメトリック認証のための規格案であり，クライアントからの依頼を受け付けて動作するサービスプロバイダの内部で動作するサービスである．

システム構築で注目されているSOA (Service Oriented Architecture) に基づくインタフェースを採用する．特定のバイオメトリック技術，装置，ベンダーに依存しない，IdM (Identity Management) システムなど遠隔認証に適したオープンなマルチプラットフォームである．

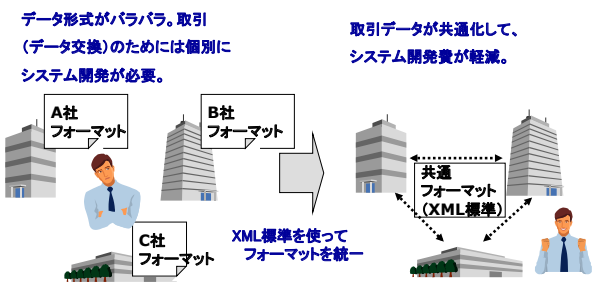

図4　XML (拡張可能なマークアップ言語)

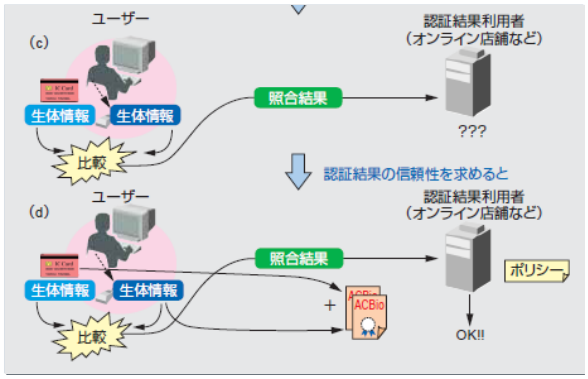

図5　ACBioの信頼モデル

(3) ACBio (バイオメトリクスのための認証コンテキスト)

ACBioは日本発の国際規格である．ISO/IEC 24761 Authentication Context for Biometricsとして2009年5月に国際規格として発行された[15]．

オープンネットワーク環境におけるバイオメトリクスによるユーザー認証 (以下，生体認証) をセキュリティ的に補完することがACBioの目的である．

文献 (15) では，オンラインショッピングの際のパスワード認証の図を利用して説明している．図5にACBioの信頼モデルを示す．

ICカードなどの媒体にあらかじめ生体情報を登録し，ローカルなバイオメトリック認証結果だけをオンライン店舗に送る方式が考えられる．この場合，オンライン店舗は結果だけを受け取ってもその結果を信じてよいか判断することができない．

しかし，このバイオメトリック認証結果の真正性を保証する何らかの仕組みがあれば，つまり，ACBioの信頼モデルがあれば，オープンネットワークを介した安全なバイオメトリック認証が実現することができると考えられる．

4. 新しい展開

バイオメトリック装置・システムの市場拡大には新しい利用分野の開拓が必要である．以下にその事例を紹介する．

4.1 米国で進む新しいアイデンティティ管理

2010年6月にオバマ政権は「Identity Ecosystem」の導入を促すとする発表を行った．アイデンティティエコシステムとは，信頼できる組織が発行し認証するデジタルID (個人識別子) を介し，個人や組織，サービス，デバイスが面倒な手続きなく情報をやりとりできる仕組みである[16]．

例えば，国や銀行や携帯電話会社などが信頼できるID証明を発行している．我々は複数のIDを利用して行政サービス，金融サービス，医療サービスなどを受けているが，これらのIDを統合して安全に利用するというものである．利用者名やパスワードを入力せずに自動的に，安全に必要なサービスに

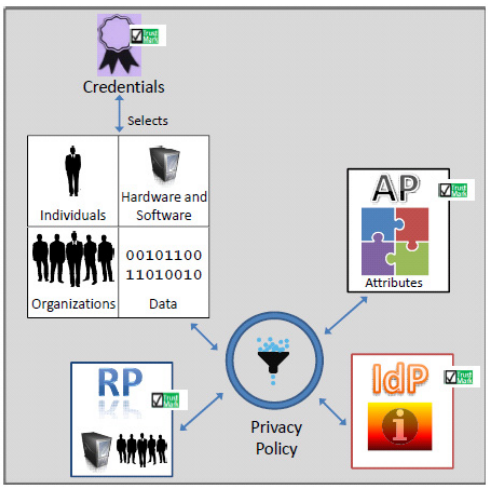

図6　アイデンティティエコシステム

ログインできるようになる．

アイデンティティエコシステムは，ICカード，携帯電話など信頼できるコンピューティングモジュール（モバイル端末）などを利用して個人識別する．バイオメトリクスはこれらのモバイル端末の所有者を認証するために利用される．

図6に示すように，地域連携医療を例にエコシステムを紹介している．病気で意識不明になった夫の医療情報を妻がかかりつけ医療機関からネットワークを介して入手する例である．基本的な構成は，信頼性高く個人を認証するIdP（Identity Provider），実際の治療を行う医療機関RP（Relying Party），患者の医療データを保管するかかりつけ医療機関AP（Attribute Provider）から構成される．

患者の妻は，モバイル端末を用い検査データにアクセスできる権利を持つ正しい利用者であることを，バイオメトリック認証を用いモバイル端末（携帯電話）の認証を行い，次に，例えば携帯電話会社の発行するPKI証明書（暗号ベースの個人認証基盤）を用いてIdPにて端末認証を厳密に行う．認証が正しく行われると，患者の医療情報を保管するかかりつけ医療機関APのデータベースより，治療を行う医療機関RPにてデータを検索できる仕掛けである．医療サービスの例を示したが，ネットバンキングや行政サービスでも同様に利用できる．

4.2　発展途上国の医療福祉への応用

長崎大学がケニアにおいて実施しているHDSS（Health and Demographic Surveillance System；人口登録・動態追跡調査システム）では，モバイル端末などのIT機器を利用して，広域エリアにおいて，効率よく大規模な人口（約9万人）の静態動態調査をしている[17]．

このような調査研究のためには個人を同定する必要があるが，発展途上国では戸籍管理が十分でないため，バイオメトリック認証を用いることがコスト的にも有効と言われている[17]，[18]．

現在，個人を特定しHDSSのデータ収集をより効率的に行うため，また将来，病院の患者データ等とのリンクをするために，静脈認証装置の導入を目的に実証実験を実施している．

指静脈装置による被験者の登録

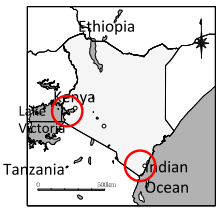

図7　指静脈を用いたケニア医療プロジェクト

図7に示すようにケニアの首都ナイロビなど3ケ所にて被験者の協力を得て実証している．指紋などは表皮の状態が悪いため指紋を正しくキャプチャできない問題がある．静脈認証は表皮の状態によらないために有効な手段であるという結論が得られた．

今後は，静脈認証技術を取り入れたアイデンティティ管理システムを開発し，住民情報のみならず，地域における情報を精度良く収集，管理できる仕組みを再構築し，電子カルテなどと連携した社会IDに発展させるための基礎技術を確立する計画である．

オランダの企業は，ガーナの社会保険システムNHIS（National Health Insurance System）において，不正や成りすましを防止するためにバイオメトリックメンバーIDを利用したMedical Claim Systemを構築している[19]．

4.3　ビッグデータとバイオメトリック技術の融合

顔認証技術の新しい市場が立ち上がりつつある．顔認証は個人を特定する技術であるが，個人の特定ではなく，人々の属性を識別することにポイントを置いている．例えば，デパートなどのサービス業において，多数の群衆の性別，年代，サービスへのリピート数などを正確に効率よく数値化することにより，実際の来場者にあった店舗展開や商品の品揃え，展示方法に関する戦略を立案できる．立案した店舗戦略を試行し，来場者層の変化を定量的なデータとして，素早く正確に把握することで，店舗戦略継続の判断ができる．更に，購買情報・会員情報などの従来情報と，気象・交通・位置などのビッグデータと組み合わせて分析を行うことで，顧客向け新サービスの立ち上げや売り上げ拡大につながるマーケティングが可能となる．

例えば，NECは以下のような事例を紹介している[20]．

店舗に設置したカメラの情報から取得した来場者情報とPOSなどで取得した購買情報を元に，購買者の傾向分析がで

図9　ビッグデータとバイオメトリック技術

きる．更に，複数のカメラを活用することにより，店舗動線，店内滞留時間，非購買者情報の採取も可能となり，マーケティング分析に活用できる．取得した来場者情報と，ビッグデータ（気象，広告，交通，SNSなど）とを組み合わせることで，店舗内では取れなかった来場者の来場に至る背景を把握し，来場者の写像を推測できる．

5．技術および製品化への期待

最後に，バイオメトリクス市場と技術開発への期待をまとめる．

5.1　予想と現実

筆者は，2006年1月号の日経バイトで，今後のバイオメトリック市場と技術開発で重要なポイントとして，以下を論述した[21]，[22]．

（予想1）ビジネスモデル：　装置価格は下落し，装置ビジネスではなく実装・ソリューションビジネスが重要．海外では専業メーカが多いが，日本ではシステムインテグレータがバイオメトリックビジネスを展開している．このため，実装・ソリューション展開が容易である．

（実態）→医療健診システム，ビッグデータ対応システム，XML，BIAS

（予想2）認証形態：　サービス対象に認証装置（センサー）を実装しない個人管理が進む，ICカードやモバイル端末への実装利用が主体となる．この場合，信頼モデルの構築，セキュリティ，プライバシー対策が重要となる．

（実態）→モバイル端末への実装，ACBio，ウルフ攻撃確率，FTA分析

（予想3）多種多量センサー利用：　バイオメトリック装置コストは年々非常に安くなっている．このため，マルチバイオメトリクスやモバイル端末への実装が重要になる．

（実態）→指紋や静脈装置の小型化，モバイル端末への実装

8年経て，市場の創出という意味では，量的にはまだ不十分であるが，上記の3点の方向性は正しかったと言える．

更に，技術開発における期待を次節にまとめる．

5.2　新市場の創出

欧州，米国は社会IDなどの基盤系へバイオメトリック技術を展開してきた．一方，日本では民生分野への展開が主であった．自由な発想で技術開発が行われてきた．このため，新市場創出の期待は大きい．以下の2点が重要と考える．

5.2.1　追跡

バイオメトリクスの機能として，下記が重要である．

（1）識別（Identification）：1：N照合という．多くのデータが保管された中から候補となる生体情報を検索する．最終的には，誰の生体情報なのか特定する．

（2）認証（Verification）：1：1照合という．パスワードの代替利用に利用する．事前登録した生体情報と一致するか判定する．他人を誤って認証してはいけない．この利用は，基本的には，誰であるかという個人を特定するのではなく，登録した個人の情報と入力した個人情報が同じか否か判定する．

（3）追跡（Tracking）：基本は1：1照合であるが，年齢，性別などの特定できない個人情報を抽出する．また，位置情報などとの利用である．**4.3**で紹介した応用である．現在は顔認証を用いているが，その他の生体情報の利用も可能である．

以上のように，従来の応用は，識別と認証であったが，あらたに追跡利用に関する技術開発，製品開発が期待できる．この場合，バイオメトリクスに関する技術開発だけでなく，プライバシー保護など法律や社会制度の整備が重要となる．

5.2.2　IdM連携

バイオメトリック認証技術がデファクト的な認証フレームワークの中で利用されるべきであると考える．**4.1**で紹介したアイデンティティ管理は，様々なIDとの連携（フェデレーション）がはじまったが，まだ，バイオメトリック認証との連携は実現していない．モバイル端末実装，BIASやACBioを活用し，既存のOpenIDなどのフレームワークへのバイオメトリック認証技術の連携が，新しい認証市場を切り開くと考える．

6．おわりに

日本では，e-パスポート，金融ATM，モバイル端末認証などにバイオメトリック技術の適用が進んでいる．小型化，高性能化の観点で技術開発は進んでいるが，システムとしての安全・安心の検討が不十分である．

特に日本で技術開発が進む静脈認証技術は，体内にある情報を利用すること，非接触であることから，盗難耐性があり利用者の個人情報の漏えいにつながらないことから民生分野の市場展開で期待が大きい．

ただし，先端的な研究テーマの多くは，日本が先行するが，必ずしも市場は拡大していないのも事実である．

市場創出のポイントは，バイオメトリック装置単体を売るのではなく，バイオメトリック技術で応用製品を売る．つまりリューションを提供する観点での進める必要がある．

大学などの研究機関は，海外の学会の研究動向を精査しテーマ設定するのではなく，技術的に先端を行く産業界と連携し，補完関係で研究開発を進めることが重要である．セキュリティやプライバシーの研究は大学などの研究機関の期待が大きい．

文　献

(1) 瀬戸洋一,“バイオメトリックセキュリティ入門,”ソフトリサーチセンター, Aug. 2004.
(2) Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalinik K. Ratha, Andrew W. Senior: Guide to BIomerics, Springer 2004年
(3) 瀬戸洋一, 溝口正典, 赤羽雅之, 森原　隆, バイオメトリクス, 自動認識増刊号, 日本工業出版, Sept. 2013.
(4) Electronics Security Global Biometric Forecast to 2012, RNCOS, Sept. 2010.
(5) 情報規格調査会サイト https://www.itscj.ipsj.or.jp
(6) 経済産業省委託 平成18年度産業技術研究開発委託費 生体情報による個人識別技術(バイオメトリクス)を利用した社会基盤構築に関する標準化成果報告書3.1節平成19年3月
(7) 瀬戸洋一, バイオメトリクスの脅威及び脆弱性公開におけるガイドライン, バイオメトリックセキュリティ研究会, Sept. 2004.
(8) Arun Ross,“Visual Cryptography and Mixing Techniques for Biometric Privacy,”Biometric consortium conference 2013, 2013.
(9) 大塚玲ほか, バイオメトリクス認証システムのウルフ攻撃に対する安全性評価技術に関する研究, ICTイノベーションフォーラム2013戦略的情報通信研究開発推進事業(SCOPE), 2013年
(10) 清水將吾, 瀬戸洋一, バイオメトリック認証システムに対するFTAによるリスク分析情報科学技術フォーラム講演論文集 7 no.4, pp.95-96, Aug. 2008.
(11) Kush Wadhwa: SAPIENT project Supporting fundamental rights, privacy and ethics in smart surveillance technologies, Biometrics 2011, 18/Oct. 2011.
(12) 瀬戸洋一, バイオメトリクスとプライバシー影響評価, AISA/BSCセミナー 2012年7月31日
(13) 瀬戸洋一, 実践的プライバシーリスク評価技法, 近代科学社, 2014年
(14) 熊谷　隆, XMLとバイオメトリクスについて, JAISA/BSC委員会　バイオメトリクス部会 合同セミナー, 2011年11月19日
(15) R & D最前線, バイオメトリクスのための認証コンテキスト(ACBio)東芝レビュー, 東芝レビュー vol.61, no.9, 2006.
(16) Jean Camp：Identity Management's Misaligned Incentives, IEEE security & privacy, PP.90-95, vol8, no6, 2010.
(17) Satoshi Kaneko: Application of biometric technology to Health and Demographic Surveillance System (HDSS) in Africa and Asia, ABC2011 in Beijing, Dec. 2011.
(18) 瀬戸洋一, バイオメトリック認証技術の最新動向, 特集　病院のセキュリティ, 病院, vol.71, no.7, pp.552-557, 2012.
(19) Biometrics2013, UK London, Oct. 2013.
(20) 高屋正裕ほか, 生体認証技術の俯瞰, 第2回先進国における事例, 顔認証技術を応用したビッグデータマーケティング, 自動認識, pp. 54-57, 日本工業出版, May 2014.
(21) 瀬戸洋一, 瀬戸洋一の生体認証論, 日経バイト, pp.109-116, Jan. 2006
(22) 瀬戸洋一：バイオメトリック認証の技術と市場の動向 ～過去から未来～, 第1回バイオメトリクス研究会資料, Aug. 2012.

（BioX 研究会提案，平成26年6月9日受付　7月25日最終受付）

瀬戸洋一（正員）

1979年慶応義塾大学大学院修士課程修了(電気工学専攻)，同年日立製作所入社，以来システム開発研究所にて，画像処理，情報セキュリティの研究に従事．現在，公立大学法人首都大学東京産業技術大学院大学教授．情報セキュリティ，プライバシー保護技術の教育研究に従事．工学博士(慶大)，技術士(情報工学)，2010年経済産業省産業技術環境局長賞を受賞，著書「バイオメトリックセキュリティ」等