

# [招待講演] バイオメトリック認証の技術と市場の動向

-過去から未来へ-

瀬戸 洋一

産業技術大学院大学

## 1.はじめに

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。

一方、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た[1]。

ンジック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。

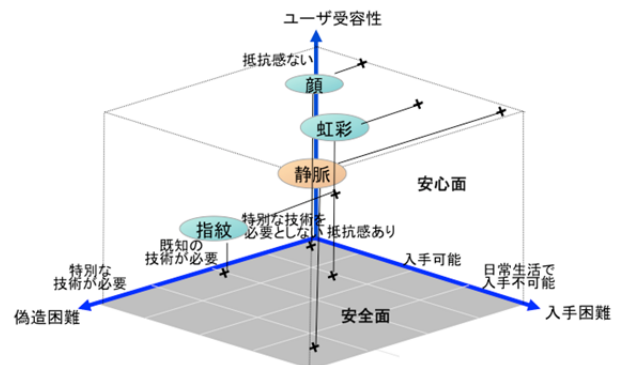


図2 安全安心を実現する静脈認証技術

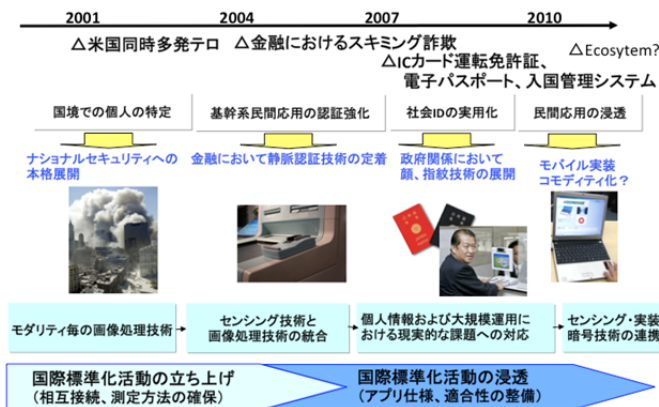


図1 9.11 から post9.11 へ

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 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[2]。

市場規模は、世界で7000億円、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 (RNCON2011年調査報告書)。フォレ

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。

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[1]。

その一つは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。

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。

本講演では、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の実現

### 2.1 脆弱性の扱いの問題

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。)を検討する必要があるがでてきた[5] [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[5]。

### 2.2 特徴量などの漏えいの問題

システム内で管理する個人データ(特徴量)が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。一方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]。

以上のように、システムの安全性強化のためには、運用を考慮したシステムの観点での議論が必要である。

### 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に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[7] [8]。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。2012年の早い時期に導入する予定である。

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。

韓国は昨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。両者とも筆者が担当した。

## 3. 国際標準のトピックス

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。最近ではユーザーの視点での開発が重要となっている。

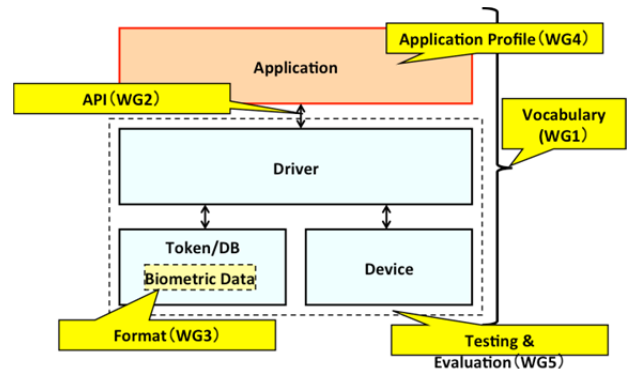


図3 SC37委員会の構成

バイオメトリックシステムは社会(国民)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である。このため、効率的なデータの相互接続や、遠隔地からの安全安心な認証方法の規格の開発が重要になっている。

今後重要となる開発中の規格を3点詳述する。

#### (1) XML化

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ェアが必要であるが、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) はテキスト形式のデータを扱う代表的なものである。

XMLはデータを記述するための言語であり、タグで囲みデータを表現する「拡張可能なマークアップ言語」と呼ばれる。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[6]。

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。

表1 海外におけるバイオメトリクスに関するPIAの事例

| ケーススタディ                            | 概要   | 評価   | 効果   |
|------------------------------------|--|--|--|
| カナダ<br>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+<br>十分なPIA報告書がウェブに公開されていない。<br>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。   |
| ニュージーランド<br>労働省における<br>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のバイオメトリック情報を収集し利用している。<br>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-<br>報告書は、ウェ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。<br>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報告書は、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して完結している。                 |
| 米国<br>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<br>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。<br>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。<br>プライバシーに関しレベルの低い設計の可能性はある。 | 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                                       |
| ニュージーランド<br>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、ニュージーランドでストリートビューをはじめた。                         | D+<br>PIAはプロジェクトの開始前に実施されていない。設計者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。自動的に顔や番号をぼやかせ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。 |

## (2) BIAS

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、遠隔利用に適したオープンなマルチプラットフォームである。

BIASは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。BIASはWebサービスなどSOAに基づくバイオメトリック用の各種サービスを定義した規格であり、IdM(Identity Management)システムへの高い接続性を持つことが予想される重要な規格である。

## (3) 実践規範

バイオメトリックシステムの実装における実践のための規範が国際標準として開発に着手した。これは、「バイオメトリックシステムの導入について、バイオメトリクスの必要性評価から構築、運用における留意事項(モダリティの選択基準、利便性、プライバシーなど)まで考慮した規格である。小・中規模のシステムをターゲットにし、詳細な規格を規定するものでなく、考慮すべき事項を網羅的にカバーした実践規範である」というスコープになっている。バイオメトリクスを専門としない調達者などが、要求仕様の確定、インテグレータとの打ち合わせに利用することを想定している。

最初にどのような認証技術が必要か、どのようなシステムにするか企画する。次にどのようなバイオメトリックシステムを構築するのか詳細検討を行い、テストを実施後、運用を行う。

このライフサイクルにおいて、導入、開発、運用各フェーズにおいてどのようなことを留意すればいいのか網羅的にまとめたガイドラインが、本規格となる。

ベンダーではなく、利用者の立場で適正なシステム構築が行われることを配慮した規格である。現在、日本では、金融や特定のシステム(入国管理システムや自動化ゲートなど)に大

規模に適用されたのみであり、市場の拡大には、裾野の広い適用先の拡大が必要であり、このためには利用者視点での構築が必要である。このために重要な規格と言える。

## 3.新しい展開

バイオメトリクスの市場拡大には新しい利用分野の開拓が必要である。医療分野に関する2つの事例を紹介する。一つは、米国で進むアイデンティティ管理、他は長崎大学の医学部が進める熱帯医療における事例である。

### 3.1 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[8]。

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4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。

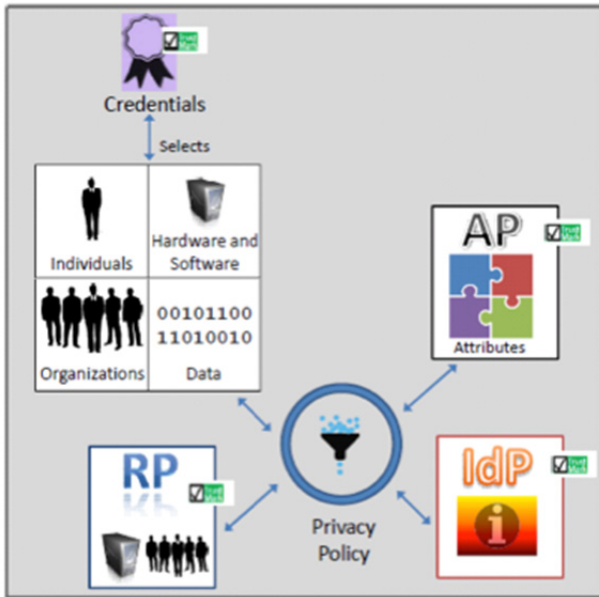


図4 アイデンティティエコシステム

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 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。

### 3.2 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)の静態動態調査している[9]。

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、生体認証を用いることがコスト的にも有効と言われている。

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。

図5に示すようにケニアの首都ナイロビなど3ヶ所にて被験者の協力を得て実証している。被験者の感想としては、登録時の手を置く回数の多さから、煩わしいと感じる被験者もいたが、「単に手を置くだけで難しくない」という意見が多く、静脈認証技術は、年齢や罹患状態にはあまり影響を受けないため、個人の識別に有効であることが実証できた。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認する計画である。



指静脈装置による被験者の登録



図5 指静脈を用いたケニア医療プロジェクト  
(提供 長崎大学医学部 金子教授)

## 5. おわりに

日本では、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という認識である。病院など医療機関での利用においては、非接触であること、利用者の個人情報の漏えいにつながらないことなどから静脈認証の利用が適している。院内における統合的な個人認証システムの構築も視野にいれた開発が必要な時期にきていると考える。

また、先端的な研究テーマは日本が先行するが、研究開発が進まなかったのが問題である。これは産学連携が進まなかったことが原因と考える。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、技術的に先端に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。

## 参考文献

- [1]瀬戸洋一ほか: 特集 自動認識技術の最新動向 バイオメトリクス、日本の最新自動認識技術増刊、pp.27 - 42、日本工業出版、2011年9月
  - [2]瀬戸洋一: サイバーセキュリティにおける生体認証技術、共立出版、2002年5月
  - [3]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、2004年8月
  - [4]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、2004年9月
  - [5]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
  - [6]Satoshi Kaneko: Application of biometric technology to Health and Demographic Surveillance System (HDSS) in Africa and Asia, ABC2011 in Beijing, 2011年12月5日
  - [7]Kush Wadhwa: SAPIENT project Supporting fundamental rights, privacy and ethics in smart surveillance technologies, Biometrics 2011, 18/Oct 2011
  - [8]瀬戸洋一: バイオメトリクスとプライバシー影響評価、JAISA/BSC セミナー2012年7月31日
- 補注) 大学 HP ([http://aiit.ac.jp/graduate\\_course/architecture/teacher/teacher\\_6.html](http://aiit.ac.jp/graduate_course/architecture/teacher/teacher_6.html)) にてバイオメトリクスに関する最新情報をダウンロードできます。