卒業論文

# ユビキタス社会におけるバイオメトリクスの可能性

## ～究極の個人認証がもたらす衝撃と普及へ課題について～

日本大学法学部　政治経済学科　４年

学籍番号：0330397

小林　功幸

## ＜論文構成＞

## 序章　はじめに

これからは、誰もが「いつでもどこでも」コンピュータを通じて情報を利用できるユビキタス（ubiquitous）社会になるといわれている。その中で、バイオメトリクス（biometrics）という個人認証技術がユビキタス社会の実現に大きな役割を果たすと考えている。

ユビキタスとは何かというと、1988 年にマーク・ワイザーが提唱した概念であり、「偏在する」「至る所に存在する」という意味のラテン語から由来している。

アルビン・トフラーがこれから迎える情報化社会のことを「第三の波」に例えたことにちなみ、マーク・ワイザーはコンピュータの進化を波に例えて説明した。第一の波は、「メインフレーム」の時代と呼んだ。この時代は多くの人が 1 台のコンピュータを共有していた。この時代の IT の主役は、人ではなくコンピュータであった。次に第二の波は「パソコンの時代」呼んだ。この頃になると、1 人が 1 台のコンピュータを使えるようになる。この時代になり、人はようやくコンピュータと対等な関係になったといえる。そして第三の波が「ユビキタス・コンピューティング」の時代である。この時代には、多くのコンピュータが 1 人の人に仕えるようになると提唱した。

ユビキタス社会は、あらゆる人があまり意識せずにコンピュータを利用でき、あらゆるサービスを受けることができる。今までのライフスタイルを一遍させ、社会、経済にも大きな影響を与えると考えられ、今問題となっているデジタルデバイドの解消にも役立つのではないかともいわれている。

ユビキタス社会を実現するにあたり、いくつかの課題が挙げられている。①認証、セキュリティなどの基本技術の向上、②デバイス（機器）同士をつなぎ、素早く使えるようにするアクセス技術、③誰でもコンピュータを自分のものとして使える、ヒューマンインターフェイスを持ったハードウェアの実現、④実際に人間に提供されるサービスを実現するアプリケーション技術、この４つが主な課題である。バイオメトリクスは、①の「どこでも自分のものとしてコンピュータが使える」というユビキタスの本質の部分の実現を可能とすることができる。バイオメトリクスとは、身体的特徴や行動的特徴等、各個人に固有の特徴を用いて個人を自動的に認証する技術であり、「各個人に固有の特徴」として、指紋、虹彩、血管パターン、顔、声紋、動的署名等が挙げられる。

さて、バイオメトリクスは、携帯電話やパソコンの起動時における本人確認や、高度なセキュリティを求められる空港における入国者の審査にいたるまで、様々な場面で急速に利用されつつある。金融分野においては、大手銀行を中心に、窓口や ATM における顧客の本人確認の手段としてバイオメトリクスを採用する動きも 2004 年半ば以降目立っている。スルガ銀行と東京三菱銀行は、手のひら静脈パターンを利用したバイオメトリクスを 2004 年 6 月、同年 10 月にそれぞれ導入している。また、みずほ銀行、三井住友銀行、日本郵政公社等は、指の静脈パターンを利用したバイオメトリクスを今後導入する方針を明らかにしている。背景には、偽造キャッシュカードによる被害の多発があり（被害総額は 2004 年

9 月末時点で８億円)、預金を守るセキュリティとしての面で注目されている。

このように、現在、バイオメトリクスは非常に高度な次世代のセキュリティとして注目を浴びている。しかし、私は、ユビキタス社会を実現するための、人間と機械とをつなぐインターフェイスとしての側面にこそ、バイオメトリクスの真価があるのではないかと考えている。キーボードを代表する現在のユーザインターフェイスは、必ずしも人間にとって使いやすいとはいえない。人間同士が自然にコミュニケーションを取るように、人間にとってもっと自然な形でコンピュータとインタラクションできないか。人間が人間を認識するように、コンピュータももっと自然な形で人間のことを認識、理解してくれないか。こう考えたとき、ユビキタス社会に求められている、「人にやさしいコンピュータ」（単に操作性が簡単というだけでなく、人の意思をくみ取ってくれるという意味を含む）を可能とする唯一の技術がバイオメトリクスであることに間違いないと考える。

本論分の構成は以下のとおりである。一章において、バイオメトリクスの基本的な概念を説明するとともに、利用されているバイオメトリクスの種類について説明する。バイオメトリクスがもたらす生活の変化を社会ＩＤ・セキュリティの 2 つの視点より紹介する。三章においては、バイオメトリクスの脅威や脆弱性としてどのようなものが想定されるかを紹介する。四章においては、三章の内容をふまえた上でどのような対策をすべきかを考察する。第五章においては、実際に使われるようになるには、どのようなことが課題となっているのかを挙げる。最後に、終章において、本論文の考察結果とそのポイントを再度強調し本論文を締めくくる。

# １．　バイオメトリクスとは

本章では、バイオメトリクスの定義を明らかにし、バイオメトリクスの中でも、現在最も一般的な指紋認証、利用頻度の比較的多い虹彩認証、これから最も普及が見込まれる静脈認証などの身体的特徴や、音声認証、署名認証などの行動的特徴の概要を説明する。

## 1.1　バイオメトリクスの定義

バイオメトリクス（biometrics）とは、「biology(生物学)」と「metrics（測定）」の合成語で、身体的特徴や行動的特徴等、各個人に固有の特徴を用いて個人を認証する技術である。生体認証あるいは、生体認証技術とも呼ばれる。バイオメトリクスは、指紋や声紋などの生体情報そのものを意味する場合と、生体情報を用いた本人認証システムまでを意味する場合がある。曖昧さをなくすために、指紋や声紋などの特徴を「生体情報」、生体情報を用いた本人認証を「バイオメトリクス」、バイオメトリクスを導入した認証システムを「バイオメトリクス認証システム」と呼ぶ。バイオメトリクスにおいて利用される身体的および行動的特徴に求められる特性として、次の項目が挙げられる。

① 普遍性（universality：その特徴を誰もが有していること）
② 唯一性（uniqueness：本人以外は同一の特徴を有していないこと）
③ 永続性（permanence：時間の経過とともに変化しにくい特徴であること）
④ 収集可能性（collectability：その特徴をセンサ等によって容易に読取可能であること）
⑤ 受容性（acceptability：その特徴を認証に利用することが一般に抵抗なく受け入れられるものであること）

代表的な身体的特徴として、指紋、掌形、顔、虹彩、網膜、血管パターン、耳形、ＤＮＡ等が挙げられるほか、代表的な行動的特徴としては、声紋、動的署名、キー・ストローク、歩行パターン等が挙げられる。複数の特徴を組み合わせて認証に利用するケースもあり、マルチモーダル（multi-modal）と呼ばれる。

## 1.2　様々なバイオメトリクス

### 1.2.1　主な身体的特徴（指紋、静脈、虹彩）

#### 1.2.1.1　指紋認証

指紋は、バイオメトリクスにおいて用いられる身体的特徴の中で最もよく知られている。指先の皮膚表面の隆線(盛り上がった部分)と谷(隆線に挟まれた部分)、三角州によって形成されおり、分岐点や端点などの特徴がある。これらの特徴をマニューシャ（minutia）と呼んでおり、1 つの指には一般に 150 ほどのマニューシャがあるとされている。指紋認証では、これらのマニューシャを用いて認証を行うマニューシャ方式と、指紋画像を比較して認証

を行うパターンマッチング方式がある。

#### 1.2.1.3　虹彩認証

虹彩（アイリス＜iris＞と呼ばれることもある）は、黒目の内側で瞳孔よりも外側に位置するドーナツ状の部分のことであり、瞳孔を開閉する機能をもつ。虹彩には筋肉によって形成される皺が存在し、その皺のパターンは各個人によって異なる。生後 2 年頃までに形成されるとその後ほとんど不変であるといわれている。この皺の形状は遺伝的影響が少なく、一卵性双生児でも異なり、同一人物でも左右が異なる。

虹彩認証の精度は非常に高く、120 万分の 1 にも達する。

#### 1.2.1.2　静脈認証

身体的特徴として静脈パターンを利用する場合、手のひら、手の甲、指に現れるものを利用する技術が提案されている。そうした技術の１つとして、静脈を流れる血液中の還元ヘモグロビンが特定波長（約 760 ナノメートル）の光を吸収しやすいという性質を利用し、当該周波数の近赤外線を照射することによって静脈パターンを浮かび上がらせる手法がある。また、近赤外線を照射して得られる反射光を撮影する方式や透過光から静脈パターンを撮影して読み取る方法も提案されている。

照合方法に関しては、静脈の分岐点や屈折点の位置およびそれらの点間の距離等を固有パターンとして照合・判定する方式（マニューシャ方式）がある。また、撮影した静脈パターンの画像において静脈部分とそうでない部分を画素値によって識別する方式（パターンマッチング方式）も提案されている。この場合、読み取った静脈パターンに対応する生体情報をテンプレートと比較して、異なる値となる画素値の全体に占める割合に基づいて判定を行う。

指紋認証と比較すると、読み取りセンサが非接触式であるため汚れに強く、指紋認証技術の欠点とされているセンサの汚れなどによる認識率の低下がほとんど無いというメリットがある。さらに、虹彩認証と同程度の認証精度を誇り、セキュリティに優れている。

以下では、静脈認証を活用している例の中でも、顧客向けサービスへの適用をスタートしているという意味で最近注目を集めているものとして、手のひら静脈認証を採用しているスルガ銀行と三菱東京ＵＦＪ銀行の事例を紹介する。

（１）スルガ銀行の事例

スルガ銀行が 2004 年 6 月にサービス提供を開始した「バイオセキュリティ預金」では、預金の払戻時における顧客の本人確認手段として手のひら静脈認証を利用している。顧客が窓口においてバイオセキュリティ預金の口座開設申込を行う際には、当該顧客の静脈パターンから固有のパターンを抽出し、口座番号等の顧客情報とともにスルガ銀行のサーバに登録される（サーバ認証方式）。このほか、顧客の印鑑の印影も登録されるほか、暗証番

号の設定も行われる。預金の払戻しに関しては、講座開設を行った店舗の窓口においてのみ行われる点が特徴であり、他の店舗や ATM において払戻しを受けることができない。顧客は、自分の名前や口座番号を提示するとともに、手のひらを読取装置にかざす。このとき採取される静脈の固有パターンは、顧客情報と紐付けされているサーバにおいて管理されている固有パターンと照合される仕組みになっている。ただし、固有パターンを生成する具体的なアルゴリズムやその照合方法については公開されていない。このほか、顧客は口座開設時に設定した暗証番号を提示する必要があるほか、登録した印鑑の印影も提示することになっており、これらの手段の組み合わせによって最終的に本人か否かの判定が行われる。

（2）三菱東京ＵＦＪ銀行の事例

三菱東京ＵＦＪ銀行では、キャッシュカード機能、クレジットカード機能等を備えた多目的 IC カード「スーパーIC カード」のサービスを 2004 年 10 月に開始しており、預金の払戻時における顧客の本人確認手段として、手のひらの静脈の静脈パターンによる認証方式を採用している。本サービスでは、静脈の固有パターンは顧客が保有する IC カードに保管され、銀行のサーバには保管されないという特徴（クライアント認証方式）があるほか、口座開設店舗の窓口だけでなく、他の店舗や IC カード対応 ATM においても静脈認証を利用して預金の払戻しを受けることが可能となっている。本サービスを利用するにあたっては、まず、利用申込を行い、銀行から IC カードと通帳の発行を受ける必要がある。顧客は、当該 IC カード、通帳、印鑑等を銀行窓口に持参し、静脈の固有パターンの抽出と IC チップへの封入を行う。預金の払戻時には、顧客は IC カードと暗証番号を提示するとともに、手のひら読取装置にかざし、静脈の固有パターンを提供する。顧客から提供された静脈の固有パターンは、IC カードに保管されている固有パターンと照合され、本人のものと判定されると、次に暗証番号の入力による本人確認も行われる。ただし、固有のパターンを生成する具体的なアルゴニズムや照合方法については公開されていない。

### 1.2.2　主な行動的特徴（音声、署名）

#### 1.2.2.1　音声認証

音声の個人差を用いて認証を行うことを、音声認証という。声を個人の認識に用いることは、犯罪捜査から始まったとされており、1660 年のイギリスに遡る。科学的な音声認証の研究は、1962 年にベル研究所のカースタが、声紋による話者認識の可能性を発表したことが始まりである。当初は声紋を人間が見て判断するものであったが、コンピュータの音声処理の発達にともない、自動的に音声認証を行う研究が活発に行われるようになった。

音声認証方式には以下の 3 つの方式がある。

①テキスト従属（キーワード、キーフレーズ）方式

発話内容（テキスト）があらかじめ決められている方式である。氏名や電話番号など比

較的短い音声で認証が可能になるが、テキストが詐称者に知られた場合には、話者の音声だけのチェックになるためセキュリティの強度が低下する。

②テキスト独立（フリーワード）方式

話者の声質だけでチェックされるため、十分な認証精度を得るためには比較的長い音読が必要となる。

③テキスト指定方式

システムが発話内容を指定しる方式。自由なテキストを指定する方式と、予め決められてたテキストの番号を指定する方式がある。テープレコーダなどに録音された音声による詐称を防ぐのに有効で、システムの信頼性をあげることができる。

さらに、前記の 3 方式を組み合わせることにより認証精度を向上させることができる。

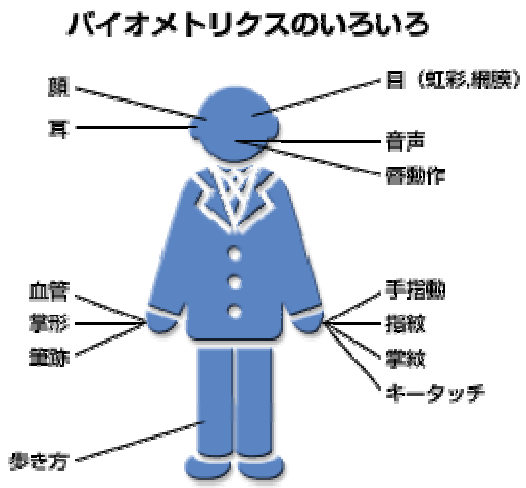
#### 1.2.2.2　署名認証

署名（サイン）は、古くから本人確認の有力な手段のひとつであった。印鑑社会である日本でも、クレジットカード使用時の本人確認の手段として日常的に使用されている。欧米ではさらに署名の役割は広く、公的書類の承認印としても利用されている。

署名認証には大きく分けて、①静的署名（カードや小切手へのサイン）、②動的署名(タブレットなどを用いて、ペン先の座標や筆圧などの運動情報を抽出して個人情報とする)の 2 つに分類されるが、バイオメトリクスで主に用いられるのは、動的署名認証である。

署名を信号処理によって自動的に認識する技術は 1960 年代半ばより試みられており、今日に至るまで研究が続けられている。具体的には、タブレットなどの座標入力装置に署名を筆記し、その署名の筆跡、ペンの運び方や筆圧などの運筆情報をあらかじめ登録している情報と照合することにより、本人の書いたものであるかどうかを判定する。何を基準に本人のものかどうかを判断するかというと、音声認識の分野で有効性の確認されているＤＰ（動的計画法）マッチングという手法を用いる。これは照合結果を相違度という尺度で評価する。基準署名と入力署名の相違度が、あらかじめ定めだ「しきい値（本人判定の基準値)」よりも小さい場合には本人の署名、大きい場合には他人の署名であると判定する。

**【図１－１】**



出展：『NTT データ』

**【図１－２】　様々なバイオメトリクス**

| バイオメトリクス認証技術 | 長所 | 短所 | コスト | 認証精度 |
|---|---|---|---|---|
| 指紋 | 最も普及している<br>社会的成熟度が高い<br>社会的信頼性が高い | 心理的抵抗がある<br>傷や汚れに弱い | 低 | ○ |
| 顔 | センサから離れて利用可能<br>なじみやすい<br>不正防止効果が高い | サングラスやマスクに弱い<br>歳をとると顔は変わる<br>長期間の使用に弱い | 中 | △ |
| 虹彩 | 他人受入率が非常に低い<br>偽造が困難<br>眼球内部の疾病の影響なし | 装置が大型で高価<br>操作に慣れが必要 | 高 | ◎ |
| 静脈 | 精度が高い<br>偽造が難しい<br>使用不可の人が少ない | なじみが薄い<br>装置がやや大型 | 中 | ○ |
| 掌形 | 精度が高い<br>操作が容易 | 装置が大型 | 中 | ○ |
| ＤＮＡ | 識別精度が圧倒的に高い | 抽出・分析するのにコストと手間がかかる | 高 | ◎ |
| 音声 | 心理的抵抗が少ない<br>音声ネットワークに適する | 体調や雑音などの影響を受けやすい | 低 | △ |
| 署名 | 他人受入率が低い<br>誰にでもできる容易さ | 本人拒否率が高い<br>手や腕を怪我しているときは認証できない | 低 | △ |

## 1.3　認証システム

### 1.3.1　クライアント認証モデル

認証の形態には、クライアント認証モデルとサーバ認証モデルの２種類がある。クライアント認証モデルは、利用者側が生体情報を管理し、端末（クライアント側）で利用者の認証を行うものである。この場合、自分の身体的あるいは行動的特徴を反映したバイオメトリクス情報を、氏名などの利用者を識別するための情報（以下、個人識別 ID と呼ぶ）とともに当該システムにあらかじめ登録しておくことになる。生体情報や個人識別 ID 等は利用者ごとに１つのデータとして保管されることが多く、テンプレートと呼ばれる。認証時に利用者は、自分の生体情報とともに個人識別 ID 等を機械に提示。端末に入力された認証情報はクライアント側に保管されている情報に基づいて認証処理され、結果に問題が無ければアプリケーションが駆動する。

メリット：①認証処理をクライアントで行うため、サーバ側のコストが低減できる。
②認証情報の管理が個人で行われるため、システム側のデータ管理負荷が軽減される。

デメリット：①利用者が IC カードなどを携帯しなければならない。
②端末のコストがかかる。

### 1.3.2　サーバ認証モデル

サーバ認証モデルは、生体情報をサーバで集中管理し、検索・照合エンジンを用いて高速に認証するものである。利用者は、生体情報や個人識別 ID をあらかじめ機械に登録しておく。個人情報はデータベースに登録される。認証時には端末から送られてきた生体情報は認証サーバで順次照合され、認証結果に問題が無ければサービスが提供される。

認証者がブラック・リスト等に登録されている個人でないことを同様の手続きで確認するものをネガティブ識別と呼ぶが、これもサーバ認証モデルの一種であると位置づけることができる。

### 1.3.3　生体を特定するレベル

バイオメトリクスを行う際に生体情報をどの程度まで特定して認証するかという観点からは、個人を特定するケースと、その個人が属するグループを特定して認証するケースに分けられる。

個人まで特定して認証するケースとして例を挙げると、銀行の ATM において利用者から静脈パターンと預金口座情報が提示され、その利用者が当該預金口座に持ち主であるか否かを確認する場合が考えられる。また、どのグループに属するかまで特定して認証するケースとしては、犯罪捜査において現場に残された血痕から容疑者等の関係者の血液型を特定する場合が例として挙げられる。

金融分野をはじめとして活用の範囲が今後広がるとみられているバイオメトリクスは、

今後、どの個人かを特定して認証する形態が中心となっていくことが予想される。

### 1.4　バイオメトリクスの歴史

人が他人の顔や声により識別することは昔から行われてきた。指紋を例に挙げると、以下のような歴史的背景がある。

指先の表皮紋様である指紋(fingerprint)は、「万人同一」「終生不変」という特徴を持つと経験的に理解されてきた。世の中に同一の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、日本でも昔から拇印の習慣が根付いている。

指紋を用いた個人識別の科学的な研究は、1684 年、イギリスのグリュー(N.Grew)により行われたと言われている。諮問による個人識別の実用化に貢献したのは、インドに派遣された英国政府職員のハーシェル（W.J.Herschel）である。ハーシェルは契約書や年金受領書、犯罪者の登録に指紋を採用した。

また、英国医師フォールズ（H.Faulds）は 1874 年に来日し、日本人が証文に爪印を押すという習慣に着目して指紋による個人識別を研究し、初めて科学的な論文としてまとめた。

その後、イギリス人のガルトン(F.Galton)は指紋を弓状（arch）、渦状（loop）、蹄状(whorl)に 3 分類し、指紋が終生不変であり、同一固体がないことを指摘した。

日本では、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はじまる。警察庁でその活用が試みられ、1971 年には実際にコンピュータによる指紋鑑定の研究開発を採用し、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。

### 1.5　バイオメトリクス市場の変遷

コンピュータを用いた画像（信号）処理技術としての市場の変遷は、以下の 3 つの時期に分類できる。

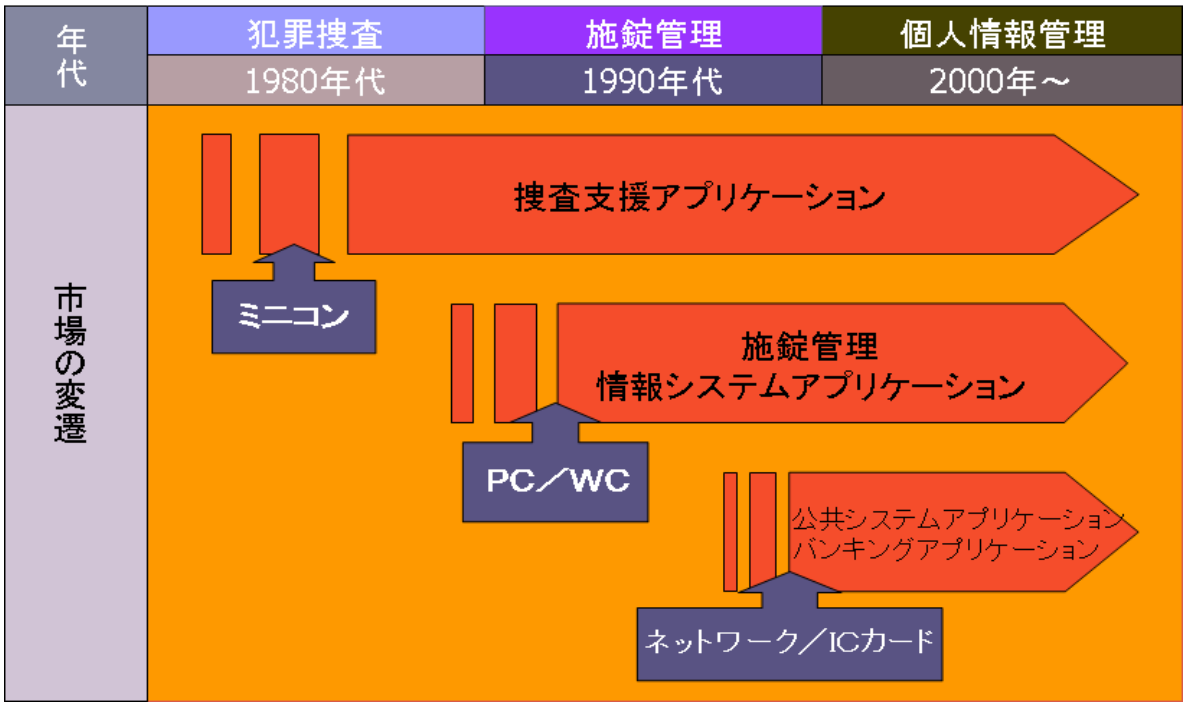
第一期に相当するのが 1980 年代初期である。犯罪捜査において、計算機による指紋照合アルゴニズムが始めて採用された。これは、ミニコンピュータベースのシステム上に開発されたものであり、デジタル画像処理技術が一般的になったのもこの時期になる。

第二期に相当するのは、1985 年頃である。ワークステーションが市場に現れ、システム構築コストが第一期に比べ 1 桁から 2 桁低減した。このため、原子力発電所などの重要施設関連の入退室管理システムとして利用されるようになった。

第三期に相当するのは、ネットワークやインターネットの発達により、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、1995 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安くなった。

第一期、第二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、第三期はネットワーク環境下での本人認証機能の位置づけでの技術の開発が行われている。

【図１－４】




出展：『ユビキタス時代のバイオメトリクスセキュリティ』をもとに筆者作成

# 2．　バイオメトリクスがもたらす生活の変化

## 2.1　セキュリティとしてのバイオメトリクス

「インターネット」と「コンピュータ」の発達により、個人が様々なトラブルに巻き込まれる可能性が高くなった。そこで、モノ自体を保護する施錠などの「物理的セキュリティ」だけでなく、ファイヤーウォール、アンチウィルスなどのネットワーク下で情報を保護する「論理的セキュリティ」の必要性が出てきた。現在、ネットワーク・セキィリティ手段として、データに暗号処理を施したり、本人確認のためのパスワードや磁気カード、IC カードによる認証等をおこなうのが一般的である。これらは比較的簡単に扱えて大変便利であるが、その半面パスワードは本人が忘れたり、他人に推測される場合がある。カード類は落としたり盗まれたりする場合がある。ところが、バイオメトリクスによるセキュリティは、ほかの手段と比べても、本人が忘れたり、盗まれたりする性質のものではないから、セキュリティレベルが非常に高く、その上、利便性も高い。

### 2.1.1　偽造カード対策

クレジットカードは便利であり、日々多くの人が利用している。しかし、磁気カードは作るのが簡単なので色々な場面で利用されているが、その反面、偽造されやすいという問題が生じている。現にクレジットカードが偽造されて、購入していない商品の請求書や借りていないお金の請求書が届いたという事件が全国で起こっている。

この問題に対応するために、クレジット会社等では IC チップに認証情報を登録したカードの導入を進めてきた。ただ、IC カードもカード自体に認証システムが入っており、カード本体だけでなく IC チップの情報が偽造されるという問題もはらんでいる。そのため、現在導入が検討されているのが指紋認証機能をつけたクレジットカードである。この機能を導入することにより、カード自体の偽造では利用できなくなり、なりすましの危険性が小さくなる。他にも上記で挙げた、手のひら静脈認証の三菱東京 UFJ 銀行のような事例がある。

今までクレジットカードで用いられてきた筆跡鑑定も必要なくなり、様々な理由でサインが出来なかった人でもクレジットカードの利用が可能になってくる。ただ、指紋・手のひら静脈による認証では、理由で利用できない人もいるので、虹彩など他の認証機能を併用していく必要がある（マルチモーダル認証）。利用者が複数の認証システムの中からあらかじめ認証方式を選択するということになれば、どの認証方法を選択するかというポイントを本人認証のひとつとして利用できるようになる。

### 2.1.2　電子商取引

インターネット上で電子商取引やネットオークションが盛んになっている。ヤフーオー

クションなどのインターネット上の商品売買により、一般の店頭販売よりも簡単に商品を購入したり、個人と個人の間での商品の取引（C to C：Consumer to Consumer)が可能になった。しかし、ネットオークションは実際の店舗で行われるわけではなく、また商品の引渡しがその場で行われないので相手が見えない。そのため、クレジットカード情報やパスワードが盗まれ、入金しても商品を送ってこないという問題が起こっている。

このような事件が多発しているため電子商取引を行う際にセキュリティ対策を行う業者が増えてきている。セキュリティ対策のひとつとしてよく利用されているのは SSL（Secure Socket Layer）というセキュリティプロトコルで、ネットワーク上で送受信される情報を暗号化して、他人に情報が漏れないようにするものである。

また、現在は一般的な本人認証手段としてパスワードを利用するのが一般的だが、人が覚えることのできる文字数を利用したパスワードには限界があることや利用者が他人に悟られやすいパスワードを使っていたり、管理が適切でなかったりすることなどによるパスワード情報の流出が問題になっている。そこで、電子商取引を行う企業や団体では、パスワードの代わりにバイオメトリクスを用いたセキュリティ対策の検討が始まっている。アメリカでは指紋認証を使った検討が進められている。これはクレジットカードを利用する際、4 桁のパスワードを入力する代わりに指紋認証で本人確認を行うものである。

### 2.1.3　既存の認証システムとの違い

ここでは、セキュリティシステムの重要な機能のひとつに位置づけられる「認証」について説明していきたい。本人認証を行うには、大きく分けて 3 つの方法がある。

①知識：パスワードや暗証番号などを用いた認証
　　長所　記憶（知識）は盗難されない。変更可能。
　　短所　本人が忘れる。パスワード自体は盗難の可能性がある。
②所有物：カードや鍵、切符などを用いた認証
　　長所　携帯性、操作性が高い。
　　短所　偽造や盗難されやすい。
③バイオメトリクス
　　長所　記憶・所持しなくてよい。偽装・盗難されにくい。
　　短所　認証のための特別な装置が必要。変更できない。

本人認証には３つの方法があり、それぞれ一長一短あるが、安全性と利便性はトレードオフの関係になる。よって、セキュリティの重要度合いやコスト、利便性等、導入目的に応じて選択していく必要がある。

## 2.2　社会ＩＤとしてのバイオメトリクス

私たちは、自分が本人であると社会に証明することで、様々な恩恵をうけている。逆に、本人であることを証明できないと、とても満足な社会生活を送ることができなくなってしまうともいえる。自分自身を社会的に証明するものは、国に登録している「戸籍」が挙げられます。現行の戸籍は昭和 22 年(1947 年)に制定された戸籍法にのっとった公文書になる。一般的には「謄本」や「抄本」といった形で目にすることができる。もっと身近なものであれば、「運転免許証」、「健康保険証」、「パスポート」などが自分を本人だと証明可能だ。キャッシュカードやクレジットカードも限定的な機能としてではあるが、お金のやり取りに関しては、保有することで本人と証明しているといえる。

ところが、困ったことにこれが「モノ」として存在している限り、盗難や紛失の危険性をともなう。クレジットカードの不正使用、運転免許証や健康保険証を使った身分偽装による詐欺行為など、まったく身に憶えのない事件に巻き込まれる恐れもある。例えば、パスポートの偽造によって、自分がまったく知らない所で外国人と結婚していた、などというトンデモない話もある。自分を証明してくれるモノが、かえって災いの種になったりする。

最近では犯罪に巻き込まれないように、社会全体がセキュリティレベルを上げる傾向にあるが、そうすると便利さが限定されてしまい、社会活動に影響を及ぼしてしまう。できるだけ簡単なやり方で、自分本人だと証明できる方法はないのだろうか。こう考えたとき、人間の体に備わっている本人固有の情報を使えばよい。そこで現在、脚光を浴びているのが、指紋や虹彩などの固有の生体情報によって本人証明を可能とするのがバイオメトリクスなのである。

私たちが認証という行為を行うことにはそれなりの理由がある。それは、自分自身や自分が保有しているモノが第三者に認められ、本来持ち合わせている正当な権利を行使する際に、高い信頼性を持って利用できる。例えば、銀行で定期預金を急に解約したくなったとき、通帳・印鑑のほかに運転免許証や健康保険といった身分証明書を提示しなくてはならない仕組みになっている。この預金は確かに自分自身のものなのに銀行側のセキュリティが第三者の証明を求める。そのとき、他者やモノが介在することなくバイオメトリクスがその第三者の証明の代わりに本人であることを証明してくれれば、煩雑な証明手続きが簡略化され生活は便利になる。まさに、自分自身が自分を証明するカギになるといえる。

### 2.2.1　IC カードとのコラボレーション

普段私たちが利用しているカードの 1 つに IC カードがある。クレジットカードに似たプラスチック製のカードで、中に IC チップが埋め込まれている。従来の磁気カードに比べ、より大量のデータを扱うことができ、また複製が困難でデータの改ざんや盗聴が難しいなどセキュリティにも優れている。しかし、IC カード自体が安全なものであっても、セキュリティ上、問題がないとはいえない。「なりすまし」による不正使用の危険性がある。つまり、IC カードの利用者が正しい持ち主であるかどうかの確認が必要となる。

そこで、バイオメトリクスの高い認証精度と生体情報の偽造耐性のため、IC カードによる所有物認証との組み合わせることにより、安全性を高める効果も期待できる。バイオメトリクスと IC カードはセキュリティを補完する関係にあるといえる。

私たちは数多くの ID を所持することを余儀なくされている。運転免許証、パスポート、住民基本台帳カード、保険証、診察カード、ハンコ、学生証（社員証）、ポイントカード、電子マネーなど挙げたらきりがない。持っていなければサービスが受けられないため、普段から所持していなければならず、非常に管理が大変である。この ID を IC カードに組み込むことにより、1 枚の IC カードで複数の ID が管理可能になる。これにより、利便性が向上し、バイオメトリクスの普及も進むのではないだろうか。

## 3．　バイオメトリクスの脆弱性

バイオメトリクスを採用する場合、当該アプリケーションにおける要件を満たすものを選択することが求められる。主な要件としては、一般にセキュリティ、利便性、コスト、社会的受容性を挙げることができる。これらの要件に優先順位をつけた上で、要件間のバランスをとりながらバイオメトリクスを導入することが求められる。

セキュリティの観点からバイオメトリクスが一定の要件を満足しているか否かを確認するためには、各システムのセキュリティ評価を実施する必要がある。その場合、アプリケーションの環境を考慮してバイオメトリクスに関する脆弱性や脅威を明確にし、必要に応じて脆弱性を回避するための対策が求められる。バイオメトリクスにおいてどのような脆弱性が想定されるかに関しては、日立製作所において検討されている。①攻撃者による第三者へのなりすましにつながる恐れのある脆弱性、②バイオメトリクス認証システムへのサービス妨害につながる恐れのある脆弱性である。なりすましにつながる恐れのある脆弱性に関しては 19 項目に分類されており、それらを整理すると次項表 1 の通りである。

なりすましにつながる恐れのある脆弱性のうち、指紋、虹彩、静脈パターンをいった身体的特徴に焦点を当てると、物理的に偽造された身体的特徴を生体認証システムが誤って受け入れてしまうという脆弱性にとりわけ留意する必要があるとの指摘がある。これは本脆弱性がいくつかの市販のバイオメトリクスに存在することが示されている反面、その対策に関する研究結果がほとんど公表されておらず、脆弱性の評価手法が確立していないという理由による。市販のいつくかのバイオメトリクスにおいて脆弱性の存在を示した代表的な研究結果としては、横浜国立大学の松本教授らによる一連の研究が挙げられる。松本教授らは、指紋および虹彩を用いたいくつかの照合装置が人口の指紋や虹彩を高い割合で誤って受け入れてしまっているのを実験によって確認しているほか、指の静脈パターンを用いた照合装置が生体でない物質(大根や人工雪材)の内部形状を高い確率で誤って静脈パターンとして読みとってしまうことも実験によって確認している。こうした脆弱性に伴って発生するリスクが当該アプリケーションのリスク許容度を超える可能性があると判断される場合には、脆弱性を軽減するための対策を検討することが必要となる。

【図３－１】　**日立製作所において列挙されている脆弱性**

| 脆弱性の名称 | 対象 | 概要 |
|---|---|---|
| 他人受入 | バイオメトリクスに特有と考えられるもの | 自分の生体特徴情報を提示すると、他人の個人として偶然に受け入れる。 |
| 狼 | | 複数のテンプレートに対して高確率で他人受入を可能にする生体特徴情報を有する利用者(「狼」と呼ぶ)が存在する。 |
| 子羊 | | 複数の生体特徴情報に対して、高確率で他人受入を可能にするテンプレートを有する利用者(「子羊」と呼ぶ)が存在する。 |
| 類似性 | | 双子等、類似の生体特徴情報を有する人が複数存在してしまう。 |
| 偽生体情報 | | 生体特徴情報を物理的に偽造し、それが受け入れられてしまう。 |
| 公開 | | 生体特徴情報が本人の同意なく容易に他人の手に渡ってしまう。 |
| 推定 | | テンプレートや照合結果が生体特徴情報推定の手がかりになる。 |
| 利用者状態 | | 生体特徴情報が自身の事情で変化し、システムに受入れられない。また、品質の劣る生体特徴情報を登録し、他人になりすまされる。 |
| 入力環境 | | 生体特徴情報の読取データが環境用で変化し、システムに受け入れられない。また、品質の劣る生体特徴情報を登録し、他者に成りすまされる。 |
| 認証パラメータ | | 不適切な認証パラメータの設定によって他人受入の可能性が高まる。 |
| 登録 | 個人認証を行う各種システムに共通するもの | 本人確認が不適切であり、他者の生体特徴情報が登録されてしまう。 |
| データ漏洩 | | システム内部で処理･保管されるデータが漏洩してしまう。 |
| データ改ざん | | システム内部で処理･保管されるデータが改ざんされてしまう。 |
| 単独 | | 生体特徴情報のみを提示する場合、ICカード等のトークンを利用する方式に比べて攻撃を相対的に容易に実行することができる。 |
| 代替手段 | | 代替手段による本人確認手段のセキュリティがバイオメトリクスの場合に比べて低くなっている場合がある。 |
| 提供 | | 利用者本人の意思で自分の生体特徴情報を他者に提供できてしまう。 |
| サイド･チャンル | | システムから各種情報(処理時間･消費電力量等)が漏洩する。 |
| センサ露出 | | 生体特徴情報を読み取るセンサは外部に露出しており、生体特徴情報の入手、破壊等の対象になりうる。 |
| 構成管理 | | システムを構成する要素間の整合性が取れていない場合がある。 |

出展：『日立製作所 2004』をもとに筆者作成

# ４．　なりすまし・偽造への対策

身体的特徴の偽造への対策に関しては、いくつかの文献において言及されている。これらの文献に取り上げられている対策は、①生体検知機能の組込み、②マルチモーダル認証の採用、③人間による登録・認証プロセスの監視、④1 種類の身体的特徴を複数利用するという手法の４つにまとめられる。

ただし、1 種類の身体的特徴を複数利用する手法に関しては、採用されている身体的特徴が容易に偽造可能になってしまう可能性がある。仮に、そうしたことが起きたという状況を想定すると、登録の対象となっている複数の特徴すべてが偽造される可能性があり、結果として本体策の有効性は大きく損なわれると考えられる。こうしたことから、以下では、対策の効果という点で相対的に有効と考えられる①、②、③に絞って考察する。

## 4.1　生体検知機能の組込み

生体検知機能の定義は、センサによって読み取られていた生体情報が人間から読み取られたものか否かを確認するという機能である。

セキュリティの観点からみると、生体検知機能をバイオメトリクス認証システムに適用した場合、当該システムにおいて第三者へのなりすましを試みる攻撃者は身体的特徴だけでなく生体検知情報もなんらかの形で提示することが必要になると考えられるため、なりすましが成功する可能性は生体検知機能を適用しない場合以下になると期待される。ただし、これまでに多種多様な生体検知機能の有効性について各種実現方式の提案者以外の第三者による評価結果が公表されているバイオメトリクス認証システムにおいて実際にどのような生体検知の手法が採用されているか（あるいは採用されていないのか）に関しても、公開されていないケースが多い。

生体検知機能を実装する際に留意すべき事項を指摘する文献は非常に少ない。数少ない文献として英国政府傘下の Biometric Working Group（以下 BWG）が挙げられる。これにおいて、生体特徴情報の読取りと同一のタイミングで同一の部位から生体検知情報の読取りを行うことが必要であるといった指摘がなされている。こうした状況が満足されていない場合、攻撃者は生体特徴情報を人工物によって提示するとともに、自分の生体検知情報を提示するというタイプの攻撃が可能になると考えられる。

生体検知機能をバイオメトリクス認証システムに組み込む際のコストや利便性について考えると、採用する方式によっては生体検知用の線さを追加したり、照合アルゴニズムを変更したりする手間やコストがかかると予想される。また、通常の生体情報に加えて生体検知の処理も実行するために照合・判定に一定の時間が必要になり、認証処理時間が増加した結果、バイオメトリクス認証システムの利便性が低下する可能性がある。

### 4.2　マルチモーダル認証の採用

マルチモーダル認証は、複数の身体的特徴等を組み合わせ、それらの照合結果を総合して本人か否かを判定するという認証の手法である。マルチモーダル認証を採用した場合には、当該システムにおいてなりすましを試みる攻撃者は異なる複数の特徴を偽造しなければならない。このため、なりすましが成功する可能性は単一の特徴を用いる認証方式(ユニモーダル認証)以下になると期待される。ただし、マルチモーダル認証における誤受入率（false accept rate）や誤拒否率（false reject rate）等の認証精度がユニモーダル認証に比べてどの程度向上するかに関しては、既に数多くの研究結果が発表されているものの、なりすましへの耐性がどの程度向上するのかに関する検討結果は筆者等が知る限り発表されていないようである。

ユニモーダル認証からマルチモーダル認証へ移行する場合のコストや利便性への影響に関しては、生体検知機能の組込みと同様の状況が発生すると考えられる。まず、複数の特徴を読み取るためにセンサを追加的に設置する必要がある。さらに、認証処理も複数の特徴に関して実行することになり、認証処理時間が増加する可能性がある。

### 4.3　人間による登録・認証プロセスの監視

運用上の対策として挙げられている人間による登録・認証プロセスの監視は、身体的特徴がそれを有する人間によってバイオメトリクス認証システムに提示されているか否かを、別の人間が自分の目で確認するというものである。また、ビデオ等によって登録・認証プロセスを録画しておき、仲問題が発生した場合には後日人間が確認できるようにする仕組みも本体策に含まれる。

本手法を採用する場合、上質紙で作成した人工の虹彩やグミ製の人工指を用いた攻撃等、人間の目でみて明らかに不正行為であると判断できる攻撃については比較的容易に検知可能であり、高い効果を期待することができると考えられる。ただし、人間の目では不正行為を見つけることが困難なケースも想定される。例えば、指紋を利用した生体認証システムにおいて指紋付きの薄膜を指に装着してセンサに指を置くといった攻撃が実行された場合には、監視人が近距離から目視によって攻撃者の行動をチェックしていたとしても攻撃を検知できない場合も考えられる。

人間による監視を採用する場合のコストや利便性への影響については、センサの追加等の生体認証システムにおける技術使用の変更には直接結びつかないと考えられるものの、被認証者による認証プロセスの監視を行う人員を配置するためのコストを新たに負担することが必要になる。その結果、自動化された生体認証システムの導入に伴うコスト削減のメリットが監視のための人員配置によって損なわれてしまう可能性がある。ただし、認証プロセスは通常の生体認証のプロセスのみで実行可能であり、認証処理時間の増加にはつながりにくいケースが多いとみられる。

**考察のまとめ**

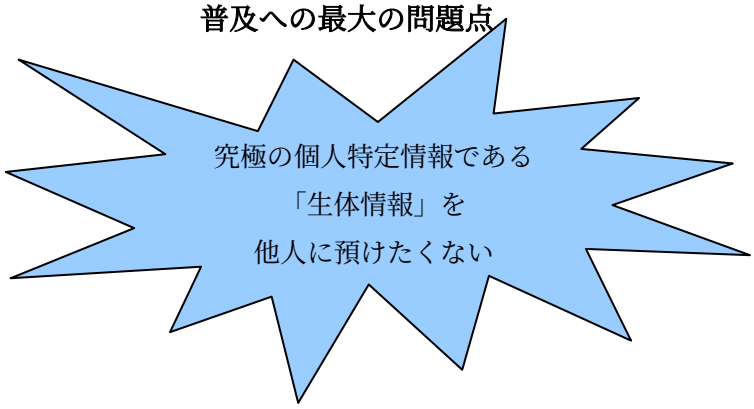
セキュリティの観点では、いずれの対策においても人体的特徴の偽造に対する耐性をどの程度向上させることができるかに関する分析結果がほとんど公表されていないのが実情である。このため、生体認証システムの運営者や利用者が、どのような対策を選択すればよいかについて客観的な情報に基づいて判断を下すことが事実上困難な状況にあると見られる。今後、セキュリティの観点から各対策がどのような効果を有しているかに関する研究を進めていくことが重要である。

コストや利便性の観点では、いずれの対策を適用しても生体認証システムにとっては別の処理を追加することになり、コストの増加や利便性の低下につながることとなる。ただし、こうした影響の度合いや形態は対策によっては変わってくると考えられる。生体検知機能やマルリモーダル認証に関しては、これらを実現するためのセンサやソフトウェア等を生体認証システムに適宜組込むことが必要であり、そうした組込みに伴ってコストや利便性にどのような影響が及ぶかについて評価する必要がある。一方、人間による監視に関しては生体認証システムにおける自動処理自体に及ぼす影響は少ないものの、監視のための人員配置に伴うコストや利便性の観点から望ましいかは個々のアプリケーションに依存することになるが、機会の自動処理によって効率的な個人認証を実現することが生体認証システムの主たる特徴であると考慮すると、生体検知機能やマルチモーダル認証を選択するケースが現実には多くなると考えられる。

# ５．　バイオメトリクス普及への課題

面倒なパスワードの記憶や鍵をジャラジャラ持ち歩く必要がなくなる可能性を秘めた便利なこのバイオメトリクスだが普及に際し、導入するコスト以外にもいくつかの問題があると考えている。その中でも最大の問題といえるのが心理的課題ではないか。

**普及への最大の問題点**




## 5.1　心理的課題

（１）生体情報を他人に預けたくない

バイオメトリクスが一般化する前の個人認証システムは、国や会社などの「管理したい側」が国民や社員といった「管理される側」に対して、社員証や免許証、健康保険証やパスポートといった認証トークンを事前に配布していたため、一般的に、認証媒体（以下、「トークン」と呼ぶ）は管理したい側のものであるケースが多く、個人のものとする意識が小さかった。そのため、プライバシー問題が起きなかったと言われている（トップダウントークン認証)。しかし今後、バイオメトリクスに限っては、個人の生体の一部や行動癖の一部を管理したい側に預ける（サーバ認証）ため、バイオ認証方式に疑問を感じるのではないか。

この問題を解決するための方法として、唯一１つの方法しかないのではないだろうか。それは、管理したい側が IC カードや USB キーを配布し、この中に生体情報を格納してもらう。認証する際にはこの格納媒体を認証するが、この格納媒体の持ち主が本人であるかどうかは、格納媒体と利用者の間でバイオメトリクスを直前に行うというものである。
現在でも公的な個人認証の場合には、上記のトップダウントークン認証とボトムアップトークン認証の折衷案である「上下折衷トークン認証」システムが主流となっている。

上下折衷トークン認証はバイオ認証のために開発されたものではなく、意外と古くから実は存在する。例えば社員証や学生証、免許証やパスポートには、顔写真が貼り付けて ある。これはれっきとした特徴量データ化されていないアナログ生体情報を、顔を利用して上下折衷トークン認証をしたことに他ならない。しかし、このシステムにも更なる問題点がある。 IC カードや USB キーなどの『バイオデータ格納トークン』を紛失したら 認証できなくなるというところである。マイクロソフトも以下のような懸念を示している。

**マイクロソフト**

システム的な問題点は、生体データをどこに保存し、だれが管理するのかというポイントがある。例えばコマースサイトを利用するときに、指紋データを 登録しろといわれたらあまりいい気持ちはしないはずだ。

この問題を解決する 方法の 1 つとして IC カードなどに生体データを記憶させておき、そのデータ をローカルコンピュータなどで認証処理を行うことが考えられる。

一見いい解 決方法のように思えるが、カードがないといけないということは、生体認証の “なくさない”というメリットがなくなってしまうというジレンマを抱えることになる。

セキュリティも大事だがプライバシーはさらに大事だ。生体認証が普及することは間違いない。自分の生体データがどのように管理・保存されているかを、ユーザーID とパスワード以上に気をつけなければならない時代がもうすぐそこまで来ている。

（2）個人の特定目的以外に使われたくない

私たちは、国家権力や知らない団体・組織に、「あなたは確かにあなたですね」って言われたくない。「私は私」だと自分で言いたい。 また、DNA や虹彩などの「生体情報」を使い、個人の病歴や頭がいいなどの優生度合いを調べるために使われたくない。

これはバイオメトリクスが、①取り替えのきかない情報であり、②本人の同意なく収集可能なものが多く、③人種などの本人の副次的な情報が抽出できる、という性質を持つゆえに生じる。このように、バイオメトリクスにおけるプライバシー問題は最終的に、究極の個人特定情報である生体情報を他人に預けたくもないし、そのデータを利用して、自分を勝手に特定して欲しくないという１点にまとめられることができるのではないか。生体情報を他人に預けなければ、そもそも個人を特定することは不可能である。

しかし、何でもかんでも上下折衷トークン認証にしてしまうと、マイクロソフトが指摘したように、トークンをなくしてしまうと、再発行の手続きを取らないといけない。たとえば、自分の家の玄関ドアや車にまでプライバシーに考えて、上下折衷ドークン認証にしてしまうと、バイオメトリクスを導入するメリットが失われてしまう。なので、安全性を重視するか、利便性を重視するかの２つの観点から考察すると、

① 国家･社会的の安全対策としてバイオメトリクスを導入するならば「安全性」を重視し、上下折衷トークン認証にすべきである。
② 個人や会社と従業員が信頼関係で成り立っている会社であるならば、安全性と同時に利便性も要求したいところであり、サーバ認証方式でよいのではないか。

このように「公的」と「プライベート」に用途分けすることが、バイオメトリクスとプライバシー問題の解決策として有効であると考える。

## 終章　おわりに

トム・クルーズ主演の 2054 年の世界を描く映画「マイノリティ・レポート」のような、街中にあらゆるセンサが張り巡らされて、例えば虹彩認証を利用し街中が個人向けの広告媒体になってしまっているような、個人の領域にシステムが勝手に踏み込んでくるような世界を望んではいない。

しかし、バイオメトリクスの技術を利用なしには、ユビキタス社会の実現はない。マイクロソフトのビル･ゲイツ会長も予言している。2004 年サンフランシスコで行われた「RSA Conference」での講演で、「やがては、人々がパスワードに頼ることがますます少なくなっていくだろう。ユーザーはいま、さまざまなシステムで同じパスワードを使い回したり、パスワードを紙に書き留めたりしている。このような状況では、本当に保護したいものに対応できない」と述べている。まずは警察や官公庁などでの利用から徐々に普及しやがては社会インフラとしてなじんでいくようになるのだと思う。今以上にバイオメトリクスが身近になる社会が訪れるのは間違いない。

さて、映画「マイノリティ・レポート」では主人公が虹彩認証から逃れるために、他人の眼球を購入し眼球ごと交換するという荒業をやってのけてしまう。つまり新しい技術が確立されれば、その技術を突破するための技術というのも必ず現れる。バイメトリクス認証に次ぐ新しい技術（例えば脳波認証のようなものなど）を考え出さなければいけない時期も近い将来訪れるのだろう。

**《参考文献・URL》**

〈書籍〉

●「ユビキタス・コンピューティング革命」、坂村健著、角川書店、2002 年 6 月
●「ユビキタス社会が始まる」、坂村健×竹村健一著、太陽企画、2004 年 4 月
●「バイオメトリクスセキュリティ入門」、瀬戸洋一著、ＳＲＳ、2004 年 8 月
●「とことんやさしいバイオメトリクスの本」、明石正則監修、
日本工業新聞社、2004 年 3 月

〈URL〉

●「生体認証における検知機能について」、宇根正志×田村裕子著
http://www.imes.boj.or.jp/security/、2005 年 8 月
●「富士通フロンテック　手のひら静脈認証　期待される活動分野」
http://www.frontech.fujitsu.com/services/jomyaku/practical.html
●「週刊バイオ　第 61 号　NTT データ」
http://mackport.co.jp/OPEN-WEEKLY-BIO/bio61/