Ⅳ　企業における認証制度の現状、課題と展望
～パスワードからバイオメトリクスへの転換～

王　　耀　鐘

序　章

本人認証とは、ある事柄を意図した人が本人であるかどうかを確認することで、成りすましを防ぐことであり、セキュリティを実現する上で必要不可欠な情報処理技術である。情報処理の分野において本人認証の必要性は、今から遡って60年代におけるTSS（タイム・シェアリング・システム）の登場から始まった。TSSの登場によって、通信回線を通じて遠隔地からもコンピュータが利用可能となった。旧国鉄のみどりの窓口、銀行のATM、LANやVANなどは、すべてTSSの登場によって可能となったコンピュータの新しい利用法である。

遠隔地からコンピュータを利用する際に、接続しようとするユーザーがそのコンピュータを利用する権限をもつ本人であるかどうかを確認しなければならない。そのため本人認証が必要とされたのである。それをうけて登場したのが、パスワードやIDカードによる認証制度である。コンピュータに接続して利用するたびに、パスワードを入力するだけで認証できるシステムやATMのようにキャッシュカードとパスワードを同時に提示しなければ確認できないシステムなど、色々な認証制度が考案されたのである。

TSSの登場をきっかけとした、パスワードとIDカードによる個人認証制度が考案されてから40数年の時が過ぎた。この認証制度もコンピュータ技術の進歩や社会環境の変化とともに精緻化されてきた。さらに、暗号化技術が導入さ

れた。そしてICカードも登場した。これはコンピュータ技術の進歩と認証に対する社会的環境の変化の要請に応えたものである。しかし、パスワードやIDカードによる認証制度の精緻化、暗号システムの導入やICカードの登場にもかかわらず、認証に関わる犯罪が後をたたない。その問題は情報処理技術の進歩と普及により、益々規模が大きくなり、情報ネットワーク社会の根幹を脅かすほどになってきている。

この、パスワードやIDカードによる認証制度を、バイオメトリクス認証制度へと転換させるきっかけになった出来事が、2001年アメリカで発生した同時多発テロである。この事件は、それまで、細々と研究・適用されてきたバイオメトリクス認証制度の有用性と必要性を再認識させ、普及させるきっかけを作ったのである。事件後、アメリカはテロに対処するため、素早く反応して、「国土防衛計画」を作成した。その目玉が、指紋、虹彩や顔などのバイオメトリクス情報による認証制度の導入である。その国土防衛計画は、世界各国に対してバイオメトリクス認証付きパスポートを発行するように要請したことと共に、全てのアメリカへの入国者に対して、バイオメトリクス情報の提供を義務づけたことで具現化した。

アメリカのこの動きと要請に応えるために、日本をはじめ世界各国が競ってこの1970年代に登場したバイオメトリクス認証制度に対する研究を進めることとなった。そして、従来のパスワードやIDカードによる認証制度から、生じた様々な弊害をなくすために、社会の各分野において、このバイオメトリクス認証制度の導入と普及を加速させた。

バイオメトリクスは、指紋、掌紋、虹彩、声紋、顔、静脈など「その人にしか存在しない固有の特徴」を用いるので、従来から用いられていたパスワードやIDカードに比べて、偽造や盗難、紛失、不正譲渡などの危険性が低く、より確度の高い個人認証制度となり得るのではないかと期待されている[1)]。

1）例えば、全国銀行協会が2006 年11月15日発表した偽造・盗難キャッシュカードによる預金の不正引き出しに関する調査結果によると、平成18年度上半期（４－９月）の偽造カー

本稿は、バイオメトリクス認証制度が、われわれの期待に応えて、次世代の認証制度として普及させるために、この制度を考察し、この制度の特徴、現状、抱える課題および今後、この認証制度を普及させるためにどうすればよいか考察し、この制度の特徴、現状、抱える課題および今後の展望を明らかにしていきたい。

そのために、まず第１章ではいまなぜ、バイオメトリクス認証でなければならないのかについての社会的・技術的環境と発展の歴史を考察したい。第２章では、この認証技術の機能を最大限に引き出すために、システムの特徴を考察したい。この章では、現在利用・研究されている様々な技術の現状、これらのシステムで使用されている生体情報の特徴を考察したい。第３章において、バイオメトリクス認証システムの運用方式と導入基準を考察したい。第４章においては、バイオメトリクス認証制度が現在適用している主な分野を検討し、実際導入されているいつかの分野の応用例を考察し、このシステムの有効性を考察したい。最後に、このシステムを更に普及させるために克服しなければならないいくつかの課題を考察して本稿を終えたい。

第１章　バイオメトリクス認証の登場

１．いまなぜバイオメトリクス認証か

情報ネットワーク化社会の進展とともに増大するさまざまな犯罪を抑制するための解決策として、「生体認証の導入」、つまりバイオメトリクス認証制度の導入が注目されている。バイオメトリクス認証が必要とされる、技術的、社会

ドによる被害額は、前年同期比55.3％減の１億3000万円と大幅に減少した。被害件数も35.2％減の149件にとどまった。指先や手のひらを使って本人識別する「生体認証」など、偽造対策の普及が功を奏しているとみられる。調査対象は大手銀行、地方銀行、第二地方銀行、国内で営業する外国銀行の計184行。
資料出所：http://www.sankei.co.jp/keizai/kseisaku/061204/ksk061204005.htm（2006年12月現在）

環境の背景として、表Ⅳ-1にも示しているように、下記の4つが挙げられる。

1）現行の認証システムにおける制度的疲労

TSSの登場をきかっけとして、パスワードとIDカードによる個人認証というセキュリティシステムが考案されてから、40数年の時が過ぎた。この認証システムもコンピュータ技術の進歩や社会環境の変化とともに精緻化してきた。暗号化技術の導入、ICカードの登場などは社会的要請に応じて導入された。しかし、この認証制度も情報処理技術の進歩や社会環境の変化により、その限界を迎えようとしている。

たとえば、銀行のATMカードや電子メール、ネット取引などパスワードはなくてはならないが、利用場面が増加の一途をたどるにつれ必然的に忘れることも多くなる。また、定期的に変えなければならない場合、面倒な手続きとなる。また、暗号化しても暗号解読技術とコンピュータ技術の進歩の前に殆ど無力化している。いままで、数多くの暗号システムが開発され、何十年、何百年も解読できないと宣言しながら、その都度、暗号解読技術とコンピュータ技術の進歩により、あっけなく解読される苦い経験を散々味わってきた。

さらに、IDカードの紛失による成りすまし、盗難による被害、内部における情報紛失や漏洩による被害も後をたたない。また、外部の不正アクセスにおいて情報の窃盗による被害などの認証に関わる犯罪の増加によって、被害の規模が益々大きくなり、情報ネットワーク社会を危うくしている[2)]。

特に、情報の窃盗、騙し取りや不正アクセスの手法は情報技術の進歩とともに、巧妙化してきた[3)]。これらの手法の登場により、情報処理分野において、セキュリティと盗難のイタチごっこに陥って、パスワードやIDカードによる

2）警察庁の発表によると、2004年の偽造・盗難キャッシュカードによるATMからの不正引出し件数は、全国で3448件、金額で24億249万円に上っている。

3）情報を騙し取りの主な手法として、下記の3つをあげることができる。
（1）スキミング（skimming）、（2）フィッシング（phishing）、（3）スパイウェア（spyware）

認証というセキュリティシステムが限界を迎えようとしている。

2）個人情報保護法の実施や預金者保護法の登場

個人情報保護法は、だれもが安心してIT社会の便益を享受するための法制度で、平成17年４月に施行された法律である。この法律は、個人情報の有用性に配慮しながら、個人情報を保護することを目的として、民間事業者が、個人情報を取り扱う上でのルールを定めている。

また、平成18年に預金者保護法が制定・実施され、金融機関が預金者や消費者に対して、カード犯罪被害に対する補償責任が盛り込まれた。この法律の制定の目的は、近年、増え続ける偽造・盗難キャッシュカードを使った犯罪から預金者を保護することを目的としている。個人情報保護法の実施や預金者保護法の登場により、情報を取り扱う企業や金融機関に認証強化の必要性がせまられている。

カードがどんどん便利になれば、それだけ盗難や偽造のリスクも高まる。クレジットカードでは、ICチップ搭載、盗難保険付きや不正使用チェックなどの対策が早くから導入されてきた。しかし、現在でも、キャッシュカードやクレジットカードによる偽造の被害は、依然として大きな問題となっている。このような不正利用や犯罪を対処するために従来のパスワードによる認証制度にかわる新しい制度が必要になってきている。

3）情報ネットワーク社会の到来

（1）情報ネットワークへのアクセスと電子商取引の普及

IT革命は、インターネットを中心とした情報ネットワーク社会を登場させた。インターネットは全世界のネットワークが相互接続した巨大なコンピュータネットワークであり、全体を統括するコンピュータが存在しない分散型のネットワークである。そのため、悪意をもった第三者が管理者不在のネットワークを利用し、他人や企業のパソコンへ不正にアクセスして情報を盗んだり、情

報改ざんや破壊を行ったりする事件が多発している。この悪意の第三者の不正アクセスを排除するため、様々な情報技術が開発されて来ているが、このような犯罪が後を絶たないばかりでなく、犯罪の規模がますます大きくなっており、情報ネットワーク化社会を危うくするほどになってきている。

そのため、日本では、平成12年に「不正アクセス行為の禁止等に関する法律」が施行された。この法律は、不正アクセス行為の禁止・処罰という行為者に対する規制と、アクセス管理者による不正アクセス行為からの防御措置等による防御側の対策という二つの側面から、不正アクセス行為の防止を図り、高度情報通信社会の健全な発展に寄与することを目的としているが、こういった犯罪は依然として横行している。

一方、インターネット上の電子商取引やネットオークションも盛んになってきているが、相手が見えない分、情報の漏洩や巧妙な手法による詐欺が多発している。これも現在の認証制度が、パスワードによる認証のために起因するものである。そこで、行政による法制度の整備や電子商取引を行う企業や団体では様々なセキュリティ対策を考案しているが、情報の漏洩や詐欺が依然として横行している。

（2）e-Japan戦略による電子政府の到来

日本では、IT革命の進展に伴い、1994年に高度情報通信社会推進本部の設立、行政の情報化推進計画の策定から始まり、2000年12月に「高度情報通信ネットワーク社会形成基本法」が制定された。これに基づいて作成された「IT基本戦略」（後のe-Japan戦略）によって電子自治体や電子政府の実現を目指している。このe-Japan戦略の実施により、電子自治体と電子政府は、本格的に稼働し始めている。

電子自治体や電子政府が本格的に稼動する際は、基本的には人を介して申請などを行う必要がなくなるため、本人確認機能が今までより重要になってくる。ただ、いままでのような人が覚える必要のあるパスワードを利用する本人確認システムでは、悪意のある第三者に利用され、利用者の増加に合わせて虚

偽の申請を行う心配が以前にもまして大きくなってしまう。そのため、バイオメトリクス情報を用いた本人確認認証システムを構築すべく研究が進められている。

（3）経済のグローバル化による人的往来の増大

経済のグローバル化により、世界における人的往来が増大している。それに伴ってパスポートの偽造による不正入国も多発している。従来は、パスポートの顔写真と本人とを見比べるという方法が用いられてきたが、近年では組織的な密入国が増加しており、顔写真の張替えなどによる偽造パスポートを用いた、なりすまし技術にともなう密入国が増加している。そのために、偽造グループがパスポートの偽造を目的として、世界各地で、旅行者のパスポートを盗んだり、強奪したりする事件が頻発している。世界各国の旅行者が旅行先で再三にわたってパスポートを紛失・盗難する事件は、経済のグローバル化に伴う世界の共通問題となった。そこで、現在、張替えなどによる偽造や変造を防ぐために、IC化が進められている。IC化はパスポートの偽造や変造などの犯罪を防ぐのに役立ってはいるが、現在の情報技術の前ではまだ完璧ではない。

（4）アメリカの同時多発テロ

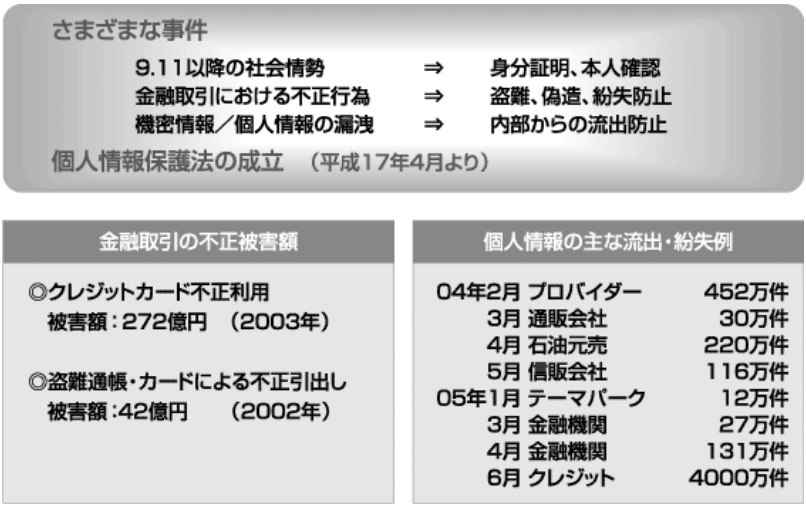
2001年に同時多発テロが起こったあと、アメリカは「本土防衛計画」の対策を打ち出した。この対策に基づき、アメリカ政府が世界各国に対して、電子パスポートの発行を要請した。また、アメリカに入国するすべての外国人に対して、指紋、虹彩や顔などバイオメトリクス情報を提供するよう義務づけた。そして、アメリカの主要国際空港に指紋、顔、虹彩などのバイオメトリクス情報を採集するデバイスを設置した。

電子パスポートは、パスポートに埋め込んだICチップに、顔や指紋などのバイオメトリクス情報を保存したものである。航空機への搭乗や入国審査の際、これをカメラやセンサーでとらえたバイオメトリクス情報と照合し、パスポートの偽造による違法な出入国を防ぐものである。日本やEUなど世界各国政府や関連機構でもアメリカのこの動きに対応するために、バイオメトリクス

認証に対する研究が盛んになってきた。ヨーロッパやアジア等ではバイオメトリクス情報を記憶しているパスポートの発行を始めた。

世界的レベルでパスポートの安全性が高まれば、不正入国という犯罪を未然に防ぐ可能性も高まると考えられるからである。

このように、従来、細々と研究・導入されてきたバイオメトリクス認証制度がアメリカの同時多発テロをきっかけとして、21世紀の新しい時代の要請に応えて、一気に情報処理分野の表舞台に躍り出てきたのである。



表Ⅳ－１　バイオメトリクス認証の必要性の背景
資料出所：富士通ジャーナル2005年７月・８月合併号より

２．バイオメトリクス（Biometric Identification; 生体認証）とは

バイオメトリクスとは、人体のさまざまな器官の特徴から個人を識別する方法で、これらの特徴は本人の証であり、常に本人に付随しているものである。本人に付いているので、いつでもどこでも再現可能であるという特徴を持っている。また、バイオメトリクス認証において、利用している人体の器官の特徴

は、一般には、次の４つの性質を持つ必要がある[4)]。すなわち、

１）普遍性、人間なら誰もが持っているものであること。

２）唯一性、自分以外に同じ特徴を持つ人がいないこと。

３）永続性、時間の経過で変化しないこと。

４）測定性、量的に測定可能であること。

例えば、指紋や静脈は誰でも持っているし、世界中、同じ指紋や静脈のパターンを持つ人はない。また、時間の経過でも変化しない。これらの特徴を根拠として、バイオメトリクス認証が、従来から用いられていたパスワードやIDカードによる認証と比べて、優れているとされている。

生体の特徴を利用したコンピュータによる本人認証を可能にしたのは、下記の技術の発展や照合アルゴリズムの進歩によるものである。

１）コンピュータ技術の発展

２）センサーテクノロジの発展

３）デジタル画像処理技術の発展

４）照合アルゴリズムの進歩

パスワードなどの記憶による認証の場合は、忘れや漏洩などの可能性があるが、IDカードなどの所持による場合は、破損、偽造、紛失、盗難などといった問題が発生する可能性がある。一方、バイオメトリクス認証は指紋、虹彩、静脈、掌型、声紋、顔、DNAなど「その人にしかない固有の特徴」を用いるので、前述した様々な問題が起こる可能性をパスワードやIDのように、偽造、盗難、紛失、不正譲渡などの危険が少なく、より確度の高い個人認証手段として、近年急速に認知されるようになった。

しかし、人間の身体の特徴におけるバイオメトリクスの情報は声紋や顔のように年とともに、変化することもある。これらの器官を使うと認証対象となる人物の特徴を正確に計測しても、その人物の特徴自体が変化することで、その

４）Anil K. Jain, etc., Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999 , P.4.

認証システムにとっては別人となってしまう可能性もあるので、認証システムの設計において、これらの点を特に注意しなければならない。

従って、バイオメトリクス認証はパスワードやID方式よりも、優れているとはいえ、バイオメトリクス認証システムの設計において万全ではないことを認識しなければならない。

3．バイオメトリクスの歴史とその発展

バイオメトリクスによる個人確認の手段として、指紋などが古くから利用されてきた。中国や日本でも古くから拇印を使う習慣があった。本格的に使われ始めたのは、19世紀に入ってからであった。それは、イギリスにおける犯罪容疑者の特定への利用であった。20世紀の初頭に日本でも犯罪捜査や犯人特定への利用が始まった。

現代の指紋認証システムが本格的に研究され始めたのは、60年代からであった。60年代から、コンピュータ技術の進歩によって情報の大量保存、検索が可能になった。また、70年代にはいると、コンピュータによるパターン認識技術が急速に進むようになり、コンピュータにおける指紋のパターン処理技術が確立された。日本では、指紋を自動的に照合するシステムの研究・開発が進められ、その活用の試みが始まった。

80年代に入り、デジタル画像処理技術が実用化され、日本では82年、FBIが83年から、指紋認識技術を採用して犯罪捜査に使い始めた。しかし、当時の製品は高価で、扱いづらく特殊な用途以外に利用されなかった。

90年代に入ると、コンピュータ処理能力の向上、センサーテクノロジやデジタル画像処理技術の進歩、識別に必要なソフトの改良により、認識技術も進歩した。これらの技術革新とコストの低減、センサーデバイスの高性能化と小型化の実現によって、認識技術は、オフィスや企業など身近なところに導入されるようになった。

しかし、身体の一部分を情報データとして登録・利用されることは、社会全

般としてプライバシーの侵害など根強い抵抗があった。特に、指紋は古くから犯罪捜査や犯罪者の特定など使われてきたので、たとえ善意的な利用のためであっても、指紋の登録や利用にはマイナスイメージが先行し、一般に普及することはなかった。

しかし、21世紀に入り、まず、2001年のアメリカで発生した同時テロ事件をきかっけとして、アメリカに入国する外国人に対して、バイオメトリクス情報を提供するよう義務付ける法律が成立・実施された。世界各国もこの動きに追随して、このバイオメトリクスと呼ばれる最新技術に対してにわかに注目するようになり、その研究や利用を加速させた。また、情報ネットワーク社会の到来による高度な情報セキュリティの要請により、金融などの民生分野にも導入され始めている。

第２章　バイオメトリクス認証の特徴

１．バイオメトリクス認証技術の現状

バイオメトリクスの認証技術としては現在研究され実用化されているものとして、主に以下の２つのタイプに分けることができる。

１）生体的特徴

生体的特徴としては、指紋、虹彩、網膜、指や手のひらの静脈パターン、顔、掌型、DNAなどがある[5)]。

２）習慣的特徴

習慣的特徴としては、サインと声紋がある。以下この２つのタイプについて考察していきたい。

５）ただし、DNA 認証の利用はいまのところ法医学分野に偏っているので、一般の情報処理分野においては、認証技法として馴染まない。また、掌型認証も次第にその優越性がなくなるので、この２つの認証技術はここでは取り上げない。

1）生体的特徴

（1）指紋認証（Finger Print）

バイオメトリクス認証の中でも特に注目されているのは指紋認証である。指紋というのは各人固有のもので、全く同じ指紋をもつ人間は世界中に存在しない。指紋による個人の識別は古くから使われてきたが、コンピュータによる指紋鑑定を開始し、本格的な研究へと展開しはじめたのは1960年代における現代的な情報処理技術の登場からである。

それ以降、指紋認証技術は、情報処理技術の進歩と犯罪捜査の精度を高める必要性とともに研究が進んできた。従って、指紋認証装置の開発も他方式に比べ歴史が長く、技術的に成熟しており、装置のコストが最も低くなっている。また、指の一部分しか使わないので小型化が可能であり、パソコンや携帯電話などのモバイル機器にも採用されだした。認識率などの性能もあがっている完成度の高い方式である。つまり、高精度と低コストを両立しているのが指紋認証システムの特徴と言える。

（2）虹彩認証（Iris Recognition）

虹彩とは眼球内部へ射入する光の量を調整する機能をもつ部分であり、カメラの絞りに相当するものである。虹彩の模様は指紋と同様にその人固有のパターンであり、同一人物の左右の目でも異なり、一卵性双生児でもそのパターンが異なる。虹彩は眼球内部の疾病などの影響を受けることはほとんどない。また、目の不自由な方の多くは、視神経の障害であり、ほとんどの場合、虹彩は正常に存在している。

虹彩認証はデジタルカメラ技術と、それにより取得された画像を処理するプロセッサ技術で実現される高精度の認証技術である。そのデジタルカメラやプロセッサは、すさまじい勢いで進歩しているので、虹彩認証装置の高機能化、小型化、低価格化にそのまま反映させている。また、デジタルカメラは、パソコンや携帯電話等様々な機器に標準的に組込まれるようになったので、将来的にはそのカメラを利用して虹彩認証を行うことにより、本人確認をセキュリテ

ィレベルの高い分野での利用が期待できる。

（3）網膜認証（Retinal Recognition）

虹彩と並んで目を利用したバイオメトリクス認証の一つとして網膜がある。網膜はカメラのフィルムのように目に入った映像を捉える部分である。網膜の血管パターンは、人間の一生のなかで変化することがない。また、同じ人物でも左右の目で異なる特徴を持っている。更に、目は光りをよく反射するので、赤外線を照射することによって、簡単に測定することができる。

網膜パターンは、指紋のような外面的な特徴ではなく、目の中に保持されているので、虹彩と同じように不安定要素が少なく、外部にも晒されないという特徴を持っている。つまり、データが正確で、安定性がある。認証時の誤認率は極めて低く、非常に精度が高い認証技術ということができる。

（4）静脈パターン認証（Vascular Image）

静脈パターン認証は比較的新しい認証技術である。指や手の甲の静脈パターンが、個人によって特徴があることに着眼したものである。静脈パターンは人により異なり、大きさ以外は成長や老化などによらず生涯変わらないという特徴がある。静脈認証では、赤外線などを使って撮影を行なう指のサイズや手のひらサイズの読み取り装置を用い、利用者はこれに手をかざすだけでよい。装置に手を触れずに済むので衛生的である。

指紋のような体表の情報は「型」を取って樹脂などで同じパターンを偽造される危険性があるが、静脈は体内の器官であるため偽造がより困難である。実際、血流があるかどうかまで判定する技術も開発されている。

（5）顔認証（Face Recognition）

人の顔は、双子などの場合を除いて、それぞれ違うことが古くからしられていた。従って、顔による認証は、従来から、運転免許証やパスポートのように人間の目による確認の方法が利用されてきた。しかし、顔の情報を利用して科学的に個人を識別する技術は、コンピュータ技術の発展とデジタル画像処理技術の進歩とともに、認証技術も急速に発展してきたことで、顔による自動認証

も可能となった。

顔認証の場合、確かに、顔をみて誰であるかを判断することは、人間にとって最も自然であり、カメラの前にそのままいるだけで認証できる利点をもっている。

2）習慣的特徴

（1）声紋認証（Voice Print）

指紋は古くから犯罪捜査に使われてきた歴史的経緯があるので、指紋認証には心理的に抵抗を感じる人が多いが、声紋認証には、このような心理的な抵抗が少ない。また、声紋認証において電話を使う場合、遠隔地でも認証ができるという特長がある。さらに、声紋認識を行うための標準的なパソコンのハードウェアがあれば処理が可能で、声紋認証のために特別のハードウェアを用意する必要はない。これらの特徴から声紋認識技術もにわかに研究されるようになった。

しかし、音声認証は虹彩や静脈などによる認証に比べると、認証精度が劣る点は否定できない。そのため、音声の使いやすさを活かしながら、他の手段と組み合わせることで、認証システム全体の認証精度を高めるというシステム設計が重要となる。

従来は、声紋を専門家が見て判断するものであったが、コンピュータによる音声処理技術の目覚しい発展に伴って、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。1990年代には米国や日本で実用化が始まった。
電話やインターネットを使った電子商取引の本格化が予想される21世紀に入って、声紋認証はますます注目される技術となっている。

（2）署名認証（Signature Recognition）

サインは、クレジットカードやチェックなど使用時の本人確認手段として日常的に使用されている。また、欧米では公的書類の「承認印」としても利用されている。従来から、利用者が本人であるかどうか、そのサインの筆跡を人間

の目による判断でしていたが、コンピュータを利用した自動認証においても、このような社会的認知性の高いサインをそのまま利用したい、と考えるのはごく自然な発想である。

署名認証は、サイン時の筆跡情報を利用することで本人の認証を実現することができる。また、サインの書き方を工夫することで、安全性の高い認証システムを構築することができる。

クレジットカードを日常の小額支払い手段としても使っているアメリカでは、現在、暗証番号の入力の代わりに、サインによる筆跡認証に移行している。将来、現在の利用の仕方が署名認証と結びつけば、かなり有望な認証技術の一つとなるであろう。

2．バイオメトリクス認証における各認証方式の比較

1）比較の基準

バイオメトリクス認証方式の優劣は下記の５つの基準から判定される[6)]。それぞれの認証方式の大まかな性能をまとめて表Ⅳ－２に示すことができる。

（1）扱いやすさ

扱いやすさとは、利用者が認証を受ける際のプロセスの簡潔さである。認証するプロセスにおいてほとんど何もしなければ扱いやすいシステムとなるが、認証するときに体の一部や顔を装置に正しく向けなければならないとか、または、何度もやりなおさなければならないとなると、扱いにくいシステムとなる。利用者にとって扱いやすさが最も重要である。

（2）経年変化耐性

経年変化耐性とは、利用者が年を取るごとに認証で使われている身体的特徴が変わりやすいかどうかを意味している。たとえば虹彩や指紋は年齢による変化がない。逆に顔や声紋などは大きく変化する。変化が大きいと、短期利用を

6）比較基準は下記のWebページを参照
http://www.atmarkit.co.jp/fsecurity/special/11biomet/biomet02a.htm（2006年12月現在）

除き、バイオメトリクス情報の定期的な更新が必要である。

（3）偽造のしにくさ

偽造のしにくさは、別人がなりすまして認証を受けることが難しいかどうかを意味している。声紋は録音テープを使うなどすることで偽造できてしまうかもしれない。サインもある程度まねることができる。いまのところ虹彩や網膜などの偽造は難しいが、指紋がシリコンを使って、指の型をとって偽造できるという報告があるが[7]、野菜の大根を使って、静脈パターンの偽造ができるとの報告も発表されているので[8]、こういった技術を使うときに脆弱性の確認は特に必要である。

（4）本人拒否率（FRR, False Rejection Rate）の少なさ

本人拒否率の少なさとは、利用者本人を正しく認識できずに拒否してしまう度合いの低さのことである。声紋、顔やサインなどは、本人であるにもかかわらず拒否される可能性が高い。指紋、虹彩、網膜、静脈などは、本人拒否率が低い。従って認証システムの設計において、本人拒否率の設定が重要になってくる。

（5）他人受け入れ率（FAR, False Acceptance Rate）のなさ

他人受け入れ率とは、登録されていない人物を受け入れる度合いのことである。偽造しなくても認識エラーで他人を本人と認証してしまうことがある。顔はもともと識別が難しいので、他人許容率が高い。コンピュータによる認識方法が人間の認識方法とは違うので、人間が見るとまったく似ていなくてもコンピュータ認証システムでは似ていると判断されることがある。同様に、声紋も人間が聴いた感覚とは違う判断をされることがある。

他人受け入れ率の設定も本人拒否率の設定と同様、認証システムの設計において重要な課題となる。

7）人工指偽造の研究につき、下記のWebページを参照
http://www.mackport.co.jp/WEEKLY-BIO/bio033/bio033.htm（2006年12月現在）

8）大根指の偽造の報告につき下記のWebページを参照
http://itpro.nikkeibp.co.jp/free/NC/NEWS/20050701/163801/（2006年12月現在）

2）バイオメトリクス認証方式の比較

以下、上記の基準で現在開発・運用されている様々なバイオメトリクス認証方式の比較を進めたい。

（1）指紋認証

指紋認証は、技術が成熟しているし、認証精度も高い。操作性も良いし、図Ⅳ－2Aのように装置の小型化が可能なので、価格が安いというメリットをもっている。しかし、今までは、犯罪捜査や犯人の特定に使ってきたので、指紋採集されることは、犯罪者扱いというイメージが強くて抵抗感がある。また、指紋状態が悪い場合、認識できないことがある。

従って、指紋認証は、大規模な利用としては公権力の及ぼす分野、例えば、IC旅券、出入国管理への利用、小規模な利用としては戸建住宅、集合住宅、オフィスや特別な施設などの入退室への利用、および携帯電話、パソコンなどのモバイルへの個人的な利用に集中している。他人受け入れ率は1000分の1程度で、精度は中ぐらいである。

脆弱性について、シリコンを材質とした材料を用いて実験室で人工指の偽造に成功したという報告があるので、今後、安全性につき、更なる研究と検証が必要となる。

図Ⅳ－2A　小型化した指紋認証装置
左：NECの「Secure Finger」 中：富士通株式会社のFS-210U　右：ソニーの指紋認証付きのUSBメモリ

（2）虹彩と網膜認証

虹彩と網膜は､近年開発された新しい認証技術で、非接触型認証であるので、衛生的であり、現在の認証技術のうち、精度が最も高く、他人受け入れ率が120万分の１以下で、その精度はDNA認証に次ぐ認証技術である。しかも、両方とも眼内にあるもので、偽造が困難で経年変化も、病気による影響も殆どないという特徴を持っている。

しかし、認証装置が他の認証技術と比べて、大型になり、装置の価格も高い。また、操作性が他の技術と比べれば、複雑で認証するのに、網膜の場合、赤外線を照射するので、利用者の抵抗感が強く、頻繁に照射すると健康を害するおそれがあるのが大きな欠点である。従って、現在、利用されているのは、空港の通関のような特に高いレベルのセキュリティが求められる場所だけで、あまり普及されていない。

（3）静脈パターン認証

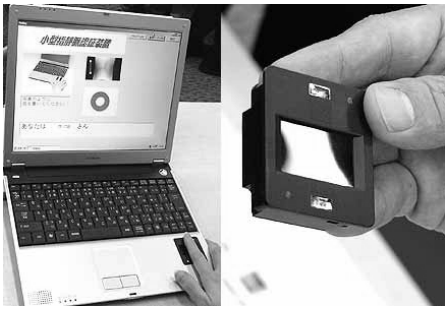
静脈パターン認証は、虹彩や網膜と同じように近年開発された認証技術で、指や手のひらの静脈パターンを利用した認証技術である。(図Ⅳ－２Ｂと２Ｃを参照)非接触型で衛生的である。しかも、精度は虹彩と網膜認証に次ぐもので、精度は高く、他人受け入れ率は100万分の１以下である。装置もかなり小型化されており、指認証の装置だと、図Ⅳ－２Ｃのように指紋認証装置と同じ大きさのものも登場している。

静脈パターンは指や手のひらの表皮の下にあるもので、偽造は難しく、利用者の抵抗感も少ない。現在我が国では、金融関係が全面的に導入して使っている。しかし、平成18年６月に、東京で開催された「情報セキュリティEXPO」において、野菜の大根で人工指の静脈パターンの偽造に成功したとの報告があったので、その脆弱性について更に検証と研究する必要がある。

（4）顔認証

顔はもともと外に晒されている器官で、認証として使われても何の抵抗感もない。また、カメラの前で顔認証システムを騙そうと思っても、心理的には

図Ⅳ－２B　富士通の手のひらタイプの静脈認証機器



図Ⅳ－２C　日立の小型指静脈認証装置

「顔が見られたらやばい」という危機意識があるので、なかなかできない。また、いままで、顔写真をIDとして使ってきた社会的慣習があるので、精度が低いにもかかわらずかなり普及している。

現在、世界各国がバイオメトリクス認証の旅券を発行しているが、顔についてのバイオメトリクス情報は必ず記憶・利用されている。これは、パスポートがいままで、顔写真による本人識別を用いてきた慣習上からであるが、今後、これをきかっけとして、顔による認証精度を高める研究が進められ、その成果を各分野に広げていくことが期待されている。

しかし、現段階では本人拒否率が高いことと、表情の変化、着用物、化粧や双子などのような状況では厳密に識別できないことが問題点である。また、顔の経年変化、周囲の光の変化、体調など、認証に影響を与えるという欠点も持っている。

（5）声紋認証

声紋認証はいまのところ、その精度は、まだかなり低いが、ユビキタス社会が進展するにつれ、携帯電話は重要な情報機器端末となってくるので、音声による認証のニーズも高まってくるため、精度を高める研究が必要となる。これからは、経年変化耐性が弱い問題、さらに体調に影響される問題などを克服しなければならない。

（6）署名認証

署名認証の精度はまだ低いが、古くから社会的慣習として使われてきたの

方式	データ化する部分	他人受入率（ＦＡＲ）	精度
指紋	指の模様	１０００分の１	○○（中）（３）
虹彩	虹彩の模様	１２０万分の１	◎◎（最高）（１）
網膜	網膜の血管の模様	１２０万分の１	◎◎（最高）（１）
静脈	指や手のひらや手の甲の静脈パターン	虹彩と指紋の間	◎（高）（２）
顔	顔の輪郭、目、鼻の形・配置	署名とほぼ同じ	○（やや低）（４）
声紋	音声の特性	３０分の１	△（低）（５）
署名	サインの筆跡と筆圧	声紋よりは低い	○（やや低）（４）

表Ⅳ－２　バイオメトリクス認証技術の比較

Anil K. Jain, etc., Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, P.16を参照して作成した。

で、受け入れやすい。これから、コンピュータ技術の進歩につれ、判別のアルゴリズムも進歩するので、認証制度も高まってくる。更に、欧米では、署名は東洋の印鑑代わりとして使われてきたので、精度を高めれば有望な認証システムとなる。

クレジットカードを小額決済としても使用しているアメリカでは、殆どの百貨店やスーパーなどのレジーの横に、サイン用のタブレットをおいている。将来、コンピュータによる認証システムを導入すれば、一気に署名による認証システムが広まっていくことが予想される。

しかし、署名認証は利き腕を使うので、怪我した場合に認証できないという大きな欠点を持っている。

第３章　バイオメトリクス認証の導入基準と運用方式

１．バイオメトリクス認証の導入基準

従来、バイオメトリクス認証技術を導入する場合、経済性、操作性、安定性安全性及び社会的受容性が検討の重点となっていたが、バイオメトリクス認証技術の進歩と普及によって、経済性や操作性などのようにその重要性が下がってきている項目もある。以下これらの項目を検討したい。

１）経済性

バイオメトリクス認証システムの経済性とは、認証するのに必要なデバイスが低価格であることと、運用コストが低いことである。従来、バイオメトリクス認証システムには、必要とするハードウェアとソフトウェアが高価でしかも運用コストが高いことが問題であった。このことはその導入の妨げとなる。しかし、近年、情報処理技術の進歩により、コンピュータのハードウェア自身のみならず認証用のデバイスと照合用のソフトの価格も急速に低下してきた。

この２年の間に数万や数十万円程度の小型指紋読取機や静脈パターン読取機

が殆ど数千や数万円程度まで下がってきている。また、顔認証用のデジタルカメラの価格も急速に下がってきている。そのため、十万円程度のノート型パソコン、携帯電話や一万円前後のUSBフラッシュメモリまでバイオメトリクス認証機能が付くようになった。これらの事実をみても分かるように、バイオメトリクス認証における経済性の問題はもはや問題ではない。

2）操作性

操作性とは、認証するために必要なデバイスの操作が簡単でかつ便利であることを意味している。また、認証プロセスが簡単であることと認証にかかる時間が短いことである。この操作性についても、経済性と同じように、バイオメトリクス認証技術のハードウェアとソフトウェアの進歩により、80年代や90年代と比べれば、その操作性もかなりよくなってきた。従来のように専門のオペレーターをも殆ど必要としないようになってきた。

また、バイオメトリクス認証の普及によって一般大衆もその使用に慣れてきているので、以前と比べれば、操作性はもはや問題ではなくなったのである。さらに、認証におけるハードウェアとソフトェアの進歩により、認証プロセスと認証する時間も以前と比べれば、かなり短くなったので、操作性の問題も経済性の問題と同様に問題ではなくなってきた。

3）安定性

バイオメトリクス認証は事前に登録するためのバイオメトリクス情報を採集する必要がある。また、認証時に事前に登録したバイオメトリクス情報と照合するための生のバイオメトリクス情報をも採集する必要がある。この両方のプロセスにおいて、バイオメトリクス情報を100％取り込むことは難しい。また、認証時に取り込まれるバイオメトリクス情報が、様々な外部条件の影響で不安定になることもしばしば起こる。従って、認証時に取り込んだ情報が予め登録した情報と完全に一致することはかなり難しい。

バイオメトリクス認証は参照情報と認証時の情報の一致と不一致は両者の類似度と予め設定された閾値との大小関係によって判定される。類似度が閾値より大きい場合には一致、小さい場合には不一致と判断される。バイオメトリクス認証にはこのような統計的特徴と基準が用いられる。

バイオメトリクス認証において、このような特徴と基準が用いられている以上、本人であっても不一致と判定される場合もあるし、他人であるにもかかわらず一致と判定される場合もある。これは、バイオメトリクス認証の弱点である。また、前者は本人拒否率（FRR）といい、後者は他人受入率（FAR）という。この両方の率とも低ければ低いほど、優れた認証システムとなるのである。バイオメトリクス認証システムの導入において、この認証の弱点を十分に認識してより安定したシステムを如何に構築するか大きな課題となる。

4）安全性

安全性とは、認証するためのデータの紛失、偽造、漏洩や盗難などに関する問題である。従来のパスワードやIDカードによる認証方式では、データの紛失、偽造、漏洩や盗難などは付きものであったが、バイオメトリクス認証においても、従来の方式と同様にデータの紛失、偽造、漏洩や盗難などは付きものである。

しかし、バイオメトリクス認証の場合、登録した参照情報がたとえ紛失、漏洩や盗難に遭っても、認証時に入力しなければならないバイオメトリクス情報の複製が難しいので、従来の認証方式と比べれば、安全性の高い認証方式といえる。また、指紋や静脈パターンのように実験室での複製ケースが報告される以外、虹彩、網膜や顔などの報告例は皆無である。

しかも、現在、バイオメトリクス認証において、複製されても、認証時における指紋や静脈パターンなど、採集のさいに、体温や血流など生きた生体であるかどうか、判断できる技術までも登場しているのであまり問題がない。

5）社会的受容性

従来、バイオメトリクス認証の導入において、むしろ一番問題になっているのは、社会的受容性である。従来、産業社会における新しい技術の導入において、何時も問題になるのは社会の抵抗である。バイオメトリクス認証の場合、典型的な受容性の問題は指紋による認証である。

指紋は古くから犯罪捜査に用いられてきた。犯罪容疑者の特定や犯罪者に対して指紋を採集するので、認証のためであっても指紋の採集には抵抗を感じる人が多い。従って、個人のノート型パソコンのようなもので指紋の認証が利用されることはあっても、銀行などのように大規模な利用は皆無である。

しかし、静脈パターン、虹彩、網膜などの認証は最近発展してきた技術であるので、抵抗感は少ないといえる。従って、銀行などの金融業界への大規模な利用には、人々の抵抗感が少なくて適している。我が国の金融業界のバイオメトリクス認証には静脈パターン認証が主流となっているのもこの理由からである。

また、署名認証について、日本では従来から印鑑が主流であるので、署名認証への社会的な受容が小さく大規模な利用は難しいが、アメリカでは署名が主流であるので、署名による認証への受容が大きく導入しやすいのである。

2．バイオメトリクス認証における運用の方式

バイオメトリクス認証の運用において、バイオメトリクス情報の抽出、保存と認証の３つに分けられている。

指紋、静脈パターン、虹彩、網膜などのバイオメトリクス情報の抽出と認証については、それぞれの認証システムのハードウェアとソフトウェアの技術的限界に依存しているので、さほど議論する余地はないが、一番大きな問題はバイオメトリクス情報の保存場所と認証場所である。保存場所と認証場所の違いが、認証システムの負荷と情報漏洩のリスクに大きな影響を与えている。現在、バイオメトリクス情報の保存方法は下記の３つに分けられる[9)]。

1）保管場所と認証場所が共に、サーバーに集中している方式

この方式では、バイオメトリクス情報の保存と認証はともにサーバーで行う。この場合、認証時にクライアントから入力された利用者本人のバイオメトリクス情報がサーバーに転送・照合される。この方式だと、サーバーの負荷が大きいが、相対的にクライアントの負荷が小さい。低いコストで実現できるメリットがある。

しかし、この運用方式だと、サーバーにおける情報漏洩、盗難などの問題が従来と同様に存在している。ただ、盗まれた情報は利用者の指紋、顔、虹彩や静脈パターンなどのバイオメトリクス情報であるので、入手したバイオメトリクス情報の偽造は難しいため、被害の可能性が以前より低くなるのである。また、たとえ盗まれたとしても、使用は困難であるため、盗難にあう可能性も以前と比べれば少なくなる。

2）保管場所がクライアント、認証場所がサーバー方式

この方式は、採集したバイオメトリクス情報と認証情報との両方がクライアントからサーバーに送られて、サーバーで認証するというものである。この場合、クライアント側にバイオメトリクス情報を保管するICカードなどが必要となる。バイオメトリクス情報がクライアント側で保管されるため、サーバーから情報が漏れるリスクは軽減されるが、認証時に情報を転送する際、ネットワークやサーバーから情報が漏れるリスクは残る。

バイオメトリクス情報はICカードに保存されている場合、カードが紛失・盗難にあったとしても、本人しか持っていないバイオメトリクス情報を入手しない限り、なりすますことはできない。しかし、パスワード方式の場合、再発行のさい、新しいパスワードを決めればすむことではあるが、バイオメトリクス認証の場合、また同じバイオメトリクス情報を使うしかないので、紛失・盗難

9）瀬戸洋一編著『ユビキタス時代のバイオメトリクスセキュリティ』日本工業出版、2003年、ページ20-22。

にあったカードの扱いの問題は残る。

3）情報の保管も認証もクライアント側、認証事実のみ、サーバーに転送方式

この方式だとクライアント側の負荷が大きいが、ネットワークとサーバーの負荷が小さい。クライアント内で認証作業が完結するため、サーバーには認証されたという事実だけが送られる。ネットワークやサーバーから情報漏れのリスクが小さい。プライバシー保護の観点からこの方式が最も望ましい。

しかし、この方式だと、クライアント側で認証されたという事実を、ネットワークを通じてサーバーに転送するときに、傍受されるおそれがあるので、暗号化する方が望ましい。しかし、暗号が解読されるリスクのレベルは従来と同じである。

3．バイオメトリクス認証における脅威と脆弱性

1）バイオメトリクス認証と脅威[10)]

バイオメトリクス認証とは利用者は本人であることを確認する技術である。従って、バイオメトリクス認証に対する脅威は、一般的な情報システムにおける脅威と同様に、情報の機密性、安全性や可用性などの情報セキュリティを損なう攻撃や事故といえる。

情報の機密性と安全性に対する攻撃について、具体的には、偽造指や顔写真、録音した音声などの生体情報の偽造によるなりすまし、他人受け入れ率（FAR）に影響する認証パラメータの不正な変更などによるなりすましなどがある。

また、バイオメトリクス認証は正当な利用者がいつでもこれを利用できなければならない可用性をもつ必要がある。バイオメトリクス認証システムの可用性を損なう脅威としては、指紋センサー、カメラ、マイクなどバイオメトリク

10）ibid., ページ159-160。

ス情報を入力する装置の破壊や、指の怪我、顔の変化、風邪による音質の変化などバイオメトリクス情報の変化による本人拒否の頻繁な発生などがある。

2）バイオメトリクス認証と脆弱性[11)]

バイオメトリクス認証の脆弱性には、バイオメトリクス認証システム特有の性質に起因する脆弱性とパスワードやIDカードなど従来の個人認証方法にも共通する脆弱性の二つがある。前者は個人を認証するための認証情報としての生体情報の脆弱質を意味し、後者はバイオメトリクス認証システムのハードウェアとソフトウェアの脆弱性を意味する。

しかし、バイオメトリクス認証の脆弱性を検討する場合には、認証情報の特質がバイオメトリクス認証システムに起因する脆弱性より重要であると考えられる。バイオメトリクス認証における生体情報に特有の性質として、次の３つをあげることができる[12)]。

（1）バイオメトリクス情報は他人に晒されること

パスワードやIDカードは認証のよりどころなので、他人に知られたり渡ることのないように運用される。しかし、バイオメトリクス認証の場合、顔や音声などは常に他人に晒されるし、指紋は常に生活の物理的空間に遺留しているために、完全に秘密にするのは難しい。

従って、バイオメトリクス認証の場合、個人の生体認証情報は常に他人に晒されている性質がある。この性質に関連する脆弱性としては、バイオメトリクス情報が他人に取得されるということが考えられる。この脆弱性は取得されたバイオメトリクス情報をもとにバイオメトリクス情報を偽造して成りすまされる脅威につながる。

実際には、指紋のように取得が容易な場合や静脈パターンのように特殊なセンサーがないと取得できない場合などがあるため、脆弱性の程度は個々のバイ

11）ibid., ページ160-161。
12）ibid., ページ161-163。

オメトリクス認証技術で異なる。しかし、バイオメトリクス認証技術に共通して生体情報が他人に晒される性質があることは知るべきである。

（2）バイオメトリクス情報の数には限りがあること

指紋や顔などのように利用者の身体的特徴を用いるバイオメトリクス認証の場合、利用者の身体情報の数には限りがある。例えば、指紋、指の静脈パターンなら、一人あたり、両手で20種類、手のひらの静脈は両手で２種類、顔なら一つだけである。パスワードやIDカードは他人に知られたりした場合、新しいものに変更することができるが、バイオメトリクス認証の場合、バイオメトリクス情報の数が知られているため、新しいもので更新できるとは限らない。この性質に関係する脆弱性として、バイオメトリクス情報の更新回数の制限が挙げられる。これは、利用者のバイオメトリクス情報を公開することで、バイオメトリクス認証を利用できなくなる脅威につながる。人々がもつバイオメトリクス情報の数はバイオメトリクス認証技術によって異なるので、脆弱性の程度はバイオメトリクス認証技術によって異なることを知る必要がある。

（3）バイオメトリクス情報は変化すること

一般には、バイオメトリクス情報は終身不変と言われているが、実際にセンサーに入力されるバイオメトリクス情報は身体の状態によって変化する。パスワードやIDカードは常に同じなので、完全に一致していることが認証の条件になるが、バイオメトリクス認証で入力されるバイオメトリクス情報が常にある幅で変動しているため、一致の条件にはある程度の幅をもつ必要がある。これがバイオメトリクス認証における認証精度の問題が存在する理由である。

この特徴に関係する脆弱性として、他人受け入れる誤差の発生が挙げられる。関連する脅威としては、利便性を優先するために、他人受け入れ率を上げるようになるシステムをねらった、なりすましや認証の閾値を不正に操作するなりすましなどがある。また、他の脆弱性として本人拒否誤差からくる本人の拒否により、可用性が損なわれる場合がある。

4．バイオメトリクスの運営とその問題点

バイオメトリクス認証が従来のパスワード認証と違うところは、認証率は100%ではないことである。人体は時間のずれによって状態が違ってくる特徴がある。また、温度の変化や光の強弱、角度など環境の変化に影響されやすいのである。また、バイオメトリクス認証システムに対する攻撃、認証の代替手段やプライバシー問題などが、運営、サービスの支障になることも少なくない。

これらの問題点を克服するために、いくつかの対策を挙げて論じたい。

1）ICカードの併用

バイオメトリクス認証において、ICカードの併用によって安全性を向上させることができる。ICカードはその携帯性とともに、カードに内蔵したICチップにより、自身内部データの改ざんに対する防御が可能であるという特徴から、情報システムのセキュリティを保証する技術としての役割が期待されている。

しかし、ICカード自身は安全な保管媒体であるが、窃盗や紛失による不正使用の危険性がある。この場合、ICカードを正しい持ち主が利用しているか否かの確認が必要となる。

2）マルチモーダルバイオメトリクス認証技術の導入

バイオメトリクス認証システムの利用者、使用環境、目的はさらに多様化しているので、単独のバイオメトリクス認証で多様化する状況に対応していくのは困難である。これに対し、複数のバイオメトリクス技術の組み合わせによるマルチモーダルバイオメトリクス認証技術が有効といわれている[13)]。

マルチモーダルバイオメトリクス認証技術は、指紋、署名、顔、声紋などのバイオメトリクスを2つ以上用いて、各バイオメトリクスの照合結果から、総合的に個人の識別を行うものである。複数のバイオメトリクスを用いるため、

13）Anil K. Jain, etc., ibid., pp, 327-332

単体のバイオメトリクスに比較して本人拒否率や他人受入れ率などの精度の改善が可能である。そのため、従来、単体では精度が不足し、実用が困難であったバイオメトリクスを組み合わせて本人認証システムを構築できる。

3）暗号化技術との併用

PKI（Public Key Infrastructure、公開鍵基盤）ベースの暗号技術は、情報を秘匿するという暗号の本来の機能に加えてデジタル署名、相手認証など極めて有用な機能を情報処理の世界に提供することになっている。バイオメトリクス認証システムに暗号技術を導入することは、2つの技術を融合することを意味している。バイオメトリクス認証システムに暗号技術の導入は、バイオメトリクス認証システムの機能の高度化が図られる。

バイオメトリクス情報の情報源となる生体情報は、典型的な個人情報である。従来のローカルな範囲での利用ではあまり問題にはならないが、今後、IC旅券のように広域で汎用的な本人認証方式が普及するにつれて、プライバシー保護の観点からバイオメトリクス情報の適確な秘匿と厳密な管理のために、暗号技術は欠かせない手段になる。特に共用されるバイオメトリクス情報データベースの十分な暗号化と管理、運用の厳格さは、システムにとって重要である。

4）バイオメトリクス認証局制度の導入

パスワードによる認証の環境においては、PKI認証局制度を導入して認証の安全性を確保しょうとしているが、いまのところ、バイオメトリクス認証を基盤とした認証局は構築されていない。将来的には認証の安全性を高めるために、生体認証版の認証局の運用も考えられる。

5）代替認証手段

バイオメトリクスは、人間の生体情報を用いて本人認証を行うものであるため、認証に必要な身体部分が、欠如していたり、不自由があったりすると、バ

イオメトリクスの利用が困難になるという問題がある。

今後、バイオメトリクスは、利用場面を拡大していくことが予想されるが、身体の障害や不自由を理由に、重要なサービスが受けられなくなるという問題は残る。そこで、何らかの対応が必要になってくるものと考えられる。この点については、今後、慎重に議論を進めていく必要がある。

第４章　バイオメトリクスの利用分野

１．バイオメトリクスにおける有望な利用分野

我々の生活に身近なところでは、銀行のATMへのバイオメトリクス認証装置の取り付けが目立っている。ほかにも、パソコンの本人確認としての利用はもちろん，指紋認証を導入した携帯電話、さらに顔認証による本人確認が行える製品の登場など、バイオメトリクスの応用分野は急速に広がっている。現在バイオメトリクス認証は主には下記の分野に導入され利用されている。

１）入退室管理

個人住宅、集合住宅、オフィス、工場、施設の防犯や入退室状況の管理と確認により、従来の鍵、パスワードやカードによる入退室のように、忘れ、紛失や盗難の問題点を克服することができる。

２）パスポート、ビザなどの身分証明および入出国管理

IC旅券の発行など、本人確認は、指紋、両眼や顔などのバイオメトリクス情報を用いるので、本人認証の確実化、不法入国の防止、入出国手続きの迅速化などを向上させることができる。

３）労務管理

会社における労務管理、出勤状況の把握などを確実にし、従来のタイムカー

ドによる管理の弊害をなくすことができる。

4）金融サービス、電子商取引など

クレジットカードなど各種カードのIC化とバイオメトリクス認証の導入により、偽造などの問題を克服することができる。また、インターネットバンキング送金、振込、電子商取引などの本人認証、既存パスワードとの併用により、詐欺、マネローリングの問題を克服することができる。

5）医療、福祉や公共サービス

医療と福祉への導入により、病院患者の管理強化、介護や公共サービスなどを受ける本人の確認と福祉や公共サービスの向上などをはかることができる。

6）携帯やパソコンなどのモバイル機器への導入

近年、バイオメトリクス認証機能を搭載したモバイル製品の登場と普及により、モバイル端末のセキュリティを一層向上させることができる。また、個人認証を必要とするネットワーク上のアプリケーションへの利用の拡大を後押している。

7）自動車

バイオメトリクス認証システムの導入により、とくに指紋が自動車の鍵としての役割を果たすことができ、盗難されても動かないので、一層安全になる。

8）情報やデータの管理、インターネットへのアクセス

情報やデータにおける閲覧者の本人認証、アクセスのコントロールが可能になるので、現在のようにデータの紛失、盗難などの危険性を減らすことができる。

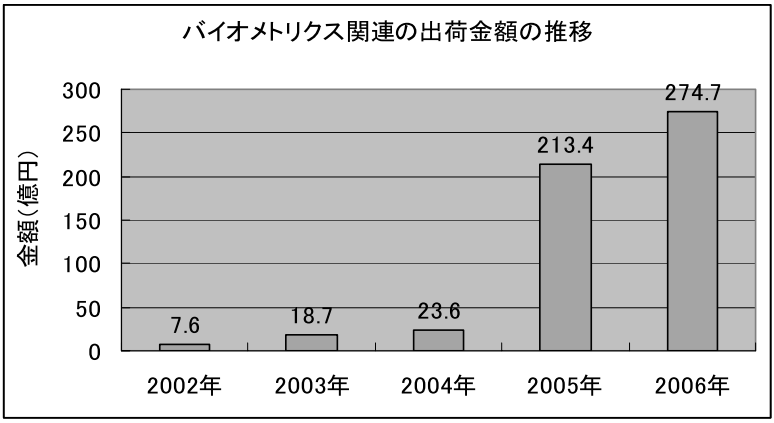
2．バイオメトリクス認証システムの市場

バイオメトリクス認証が本格的に利用され始めたのは、今から二十数年前の

1980年代から指紋を用いた犯罪捜査からである。まず、1982年に日本の警視庁、そして、その翌年には米国のサンフランシスコ市警が導入し、未解決事件の解決に貢献した。その成果を受けて、米国内の各州、各市はもとより、世界各国の警察に日本の技術が活用されていった。犯罪捜査以外では、原子力発電所などの一部の特殊な場所でも使われた。

1990年代になると集合住宅の出入りやオフィス，工場や特殊な施設の入退室管理などで徐々に導入が進んでいた。しかし、身体の一部を情報データとして管理されるため、プライバシーの侵害や犯罪者の登録といったマイナスのイメージが阻害して、一般に大きく普及することはなかった。

今日のように商用製品として一般な普及を見せ始めたのは、つい最近のことである。そのきっかけとしては、米国の2001年９月11日に起きた同時多発テロである。国内でも、個人情報保護法と預金者保護法の実施、生活の身近なところでは偽造キャッシュカードや偽造クレジットカードなど、金融関連の被害が続出したことなどが挙げられる。このような状況を受けて、国内外では、バイオメトリクス認証技術の開発が本格化し、ここ数年の間にバイオメトリクス製



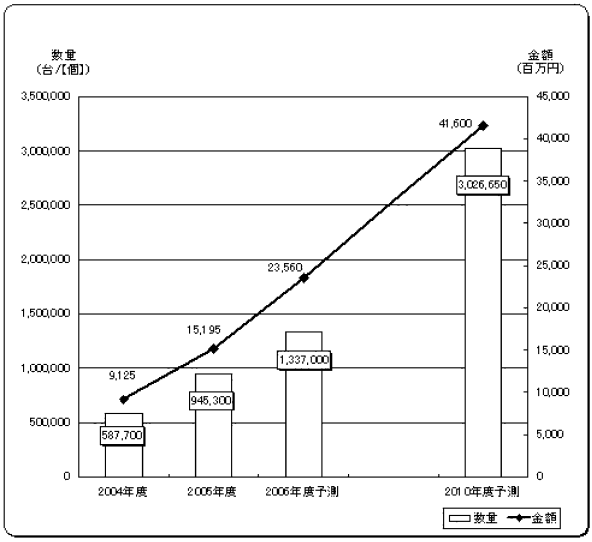
図Ⅳ－４Ａ　資料出所：社団法人日本自動認識システム協会統計調査委員会
http://itpro.nikkeibp.co.jp/as/bio2006/contents 01.html（2006年12月現在）（2006年の数字は予測）

品の普及が始まった。

この変化を受けて、バイオメトリクス認証関連製品の市場も急速に拡大してきた。その市場の変化を社団法人「日本自動認識システム協会」の調査データで見てみると、図Ⅳ－４Ａのように大幅な成長を見せている。

この図によれば、2005年の自動認識機器におけるバイオメトリクス関連の出荷金額は、前年比9.1倍の213.4億円である。今後も同様なセキュリティ需要の高まりが期待できることから、2006年の出荷金額は2005年比で28.7%増の274.7億円という大幅な伸びが予測されている。

これを認証方式で見てみると、指紋認証はパソコンや携帯電話などのログイン・キーまたは電子カルテでの採用などにより着実な伸びが予測される。一方、静脈認証では引き続き金融機関へのATM導入が拡大することから，出荷台数



図Ⅳ－４Ｂ　バイオメトリクス認証関連の市場推移と予測

資料出所：矢野経済研究所2006年バイオメトリクス白書
http://www.itmedia.co.jp/survey/articles/0410/19/news058.html（2006年12月現在）

も大幅な伸びが予測されている。

また、矢野経済研究所の2006年発行のバイオメトリクス白書によれば、国内のバイオメトリクス市場全体のマーケットサイズは、図Ⅳ－４Ｂを見れば、2005年から大幅な成長を見せている。この図によれば、金額ベースでは、2004年度が91.3億円、2005年度が152.0億円、2006年度予測が235.6億円である。また、需要予測については、2010年度予測が416.0億円であった。

このように、社団法人日本自動認識システム協会と矢野経済研究所の調査と予測の数字いずれからも、今後大幅な成長が見込まれている。[14)]

３．バイオメトリクス認証への応用例

１）パスポート、ビザと入国管理への応用

2001年９月11日の同時多発テロ事件を機に、米政府は「本土防衛計画」の対策を打ち出した。その目玉は、関係国に対して、電子パスポートの発行を要請したことである。電子パスポートとは、パスポートにICチップを埋め込み、そのチップに、顔や指紋などのバイオメトリクス情報を保存するものである。そして、航空機への搭乗や入国審査の際に、このチップに保存されているバイオメトリクス情報を空港に設置しているカメラや指紋読み取りセンサーでとらえた画像や指紋などのバイオメトリクス情報と照合し、パスポートの偽造による違法な出入国を水際で防ぐというものである。

また、アメリカ政府は、アメリカへの入国にビザが必要な渡航者に対してビザを申請する際、顔や指紋などのバイオメトリクス情報を提供するよう義務づけている。日本やEUなどを含むビザ免除の渡航者に対して、テロ対策への協力策として、空港で設置しているカメラや指紋採集センサーから顔や指紋の採集をして、入国者への管理に利用している。

アメリカのこの要請にこたえて、日本では平成18年に電子パスポートを発行

14）社団法人日本自動認識システム協会と矢野経済研究所の調査数字の違いは多分調査手法と項目の違いからである。

した。日本で導入された電子パスポートは「IC旅券」と略称され、表紙の下にICを模したシンボルマークが印刷されること以外に、現在のパスポートとあまり変わりがない。このパスポートに、1ページだけICを封入するための厚いページがあった。このパスポートのICには、国籍や名前，生年月日などのほか、本人の顔写真のデータが記録されている。そして、ページの中央にICチップと通信用のアンテナを格納したカードが組み込まれている。なお、将来に向けて指紋、虹彩などの情報を追加記録する方式も検討されている。

このIC旅券に記録されるデータは顔写真を含めて原則として暗号化しない形で記録される。これはパスポートが広く国際社会のIDとして長年用いられ、様々な場面で利用されている歴史的な背景を配慮したものである。ただし、セキュリティ対策として、偽造・変造対策、コピー防止対策、盗聴防止対策を施しているほかに、カードのインターフェースは無線であるため、データをそのまま通信路に流すと第3者による盗聴や傍聴の危険があるため、この対策として暗号通信手順が用いられ、伝送データが暗号化されている。

このように、IC旅券は2006年から、世界各国で導入が始まったが、多くの国では、当面は空港の審査端末がIC旅券を読み出せる装置に置き換えられることからスタートするが、将来はバイオメトリクス情報の機械認証、自動化ゲートなどに発展して行くものと思われる。テロの防止策は世界共通の緊急課題となっており、今後は出入国管理だけでなく、エアライン、旅行代理店などでもチェックを行うことができるほかに、将来は金融機関の口座開設や宿泊施設などにおける本人確認にも応用されると期待されている。

IC旅券の運用にはまだいくつかの克服しなければならない課題が残されている。例えばICチップの耐久性検証、バイオメトリクス認証の世界規模での互換性検証、バイオメトリクス認証における顔の精度、IC読取りからバイオメトリクス認証における操作性の検討、失効情報や暗号鍵の世界的規模への配布と管理の問題や、バイオメトリクス情報の取り扱いに関する仕様の標準化とその規格の統一など問題は山積されている。

しかし、顔認証の分野において、近年の性能向上は目覚しいものがある。将来はIC旅券で使われる顔認証技術がIC旅券以外の本人認証システムでも応用されていくと期待されている。

2）ビザと入国管理への応用

（1）アメリカの応用例

同時多発テロ後、外国人がアメリカのビザ取得時に指紋と顔のバイオメトリクス情報を提供するように義務付けられた。また、入国時に、各空港に設置している指紋採取装置とデジタルカメラで指紋と顔のバイオメトリクス情報を採集して、ビザ取得時に採取した情報と照合して本人であるかどうかを判別する。また、観光などビザの取得が免除されている場合でも、入国時に指紋と顔のバイオメトリクス情報を採取・保存して、入国者の管理に役立つようなバイオメトリクス認証システムを構築している。

また、アメリカは陸路や海路でカナダ、メキシコ、カリブ海地区、バミューダ諸島を往来する国民に対して、パスポートカードを発行するよう計画している[15)]。このカードはクレジットカードと同じサイズで、頻繁に陸路で近隣諸国を往来している人、外航航路の船員、観光船でカリブ海地区やバミューダ諸島を観光する人には便利である。

RFID[16)] を採用しているので、カードリーダーにかざすだけで、身分を確認することができる。また、抵抗感をなくすために、個人のバイオメトリクス情報はカードに保存しない。このカード式のパスポートの導入によって、国境の安全管理に役立ち、国境の出入りにも便利になる。手数料は大人で45ドル、子ともで35ドルで従来のパスポートの発行手数料の97ドルと比べればかなりやす

15）パスポートカードにつき
http://cryptome.org/dos101706.htm を参照（2006年12月現在）

16）RFID（Radio Frequency Identification の略）では、ID 情報を埋め込んだタグから、電磁界や電波などを用いた近距離の無線通信によって情報をやりとりするものおよび技術全般を指す。

くなる。

（2）イギリスの応用例

イギリスでは2006年の12月から、EUで最も忙しい空港、ロンドン近郊のヒースロー国際空港にバイオメトリクス認証による通関設備を導入して、部分的な路線でバイオメトリクス認証による通関手続を試験的にはじめた。選ばれたのは、アラビア首長航空（Emirate Airline）が運行しているドバイ（Dubai）路線およびキャセイ航空が運行しているホンコン路線の2路線である。対象はこの2路線で指紋情報を自発的に提供する乗客から運用を始めた。成果が認められれば、順次世界各国の路線に拡大していく方針である。

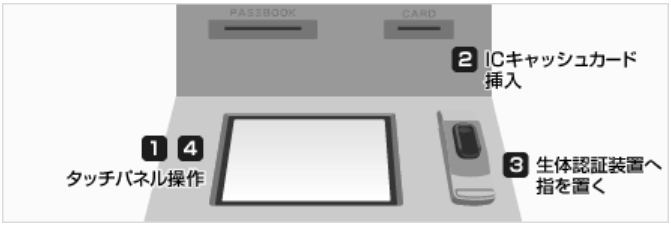
イギリスの移民局担当責任者によれば、このシステムの目的は通関スピードを上げるだけではなく、国の安全保障を更に向上することである。最終的には、移民の管理につながっていくことである。なぜならば、イギリスの2005年のロンドンテロ事件は移民やその関係者によって起こされた事件であるので、移民の動きの把握と管理は緊急の課題となるからである。

3）金融分野への応用：日本の応用例

我が国では、平成18年から預金者保護法が実施された。この法律では、金融機関が預金者や消費者に対して、カード犯罪被害に対する補償責任が盛り込まれた。これをきっかけとして、金融機関がなるべく被害を最小限に抑えるために、バイオメトリクス認証のATMカードの導入と普及を急いでいる。

現在、我が国の金融機関が利用しているバイオメトリクス認証は静脈パターンによる認証方式である。静脈認証は最近登場した新しい認証方式である。指紋認証のように犯罪捜査や犯人扱いのイメージがなく、また、指紋のように生活の現場にその痕跡を残さない特徴を持っているので、偽造の危険も少ない。そのために、社会的受容性が高いので、その導入において、抵抗はさほどないが、利用者の身体的な状況による認証ができないことがあるなど抵抗感が残る。

日本で導入されている静脈認証方式には、図Ⅳ－4Cの日立が開発した指静



図Ⅳ－４Ｃ　みずほ銀行の指静脈認証ATM
資料出所：http://www.mizuhobank.co.jp/start/seitai_ninsho/（2006年12月現在）

図Ⅳ－４Ｄ　東京三菱銀行の手のひら静脈認証ATM
資料出所：http://jp.fujitsu.com/about/journal/282/topstory2/03.html（2006年12月現在）

脈方式と図Ⅳ－４Ｄの富士通が開発した手のひら静脈方式の２方式にわかれている。指方式は三井住友銀行、みず方銀行、りそな銀行、日本郵政公社などに採用されている。みずほと三井住友は2006年の10月から郵貯のATMでバイオメトリクス認証カードが使えるサービスを始め、2007年の春には、みずほと三井住友も相互利用できるようになる。一方、三菱東京UFJ銀行は手のひら方式で、2006年７月現在でATMの２割の1700台に導入済みであった。

ただ、「バイオメトリクス認証ATMカードが一層普及するには、指方式と手のひら方式の規格の統一か相互乗り入れが必要となる」との声は強く、全銀協でもその方向で研究を進めている。そのような中、大日本印刷が、指と手のひ

17）大日本印刷が開発した技術の記事は下記のWebを参照
http://www.dnp.co.jp/jis/news/2006/060512.html（2006年12月現在）
http://www.rbbtoday.com/news/20060512/30781.html（2006年12月現在）

らのいずれの方式にも１枚のカードで対応可能な技術の開発に成功した[17]。さっそく関西地銀の泉州銀行など複数の銀行が導入する予定である。

これによって、これから両方式を一本化せずに両立できるならば、それに超したことはないが、両方式の互換性を保つために、両方式のカードとも読むことができるための端末が必要になるので、日本の金融機関の負担が大きくなる。また、金融機関のATMカードのバイオメトリクス認証化は世界に先駆けとなるので[18]、今後、世界中に広げていく際に大きな影響を与えると考えられ、規格の不統一したままでの導入は、今後世界に広げていくのに、世界に大きな負担をかけることになるので、検討を要するのである。

第５章　終章～今後の課題と展望～

本稿のこれまでの考察を通じて、我々はバイオメトリクス認証の特徴と有用性を明らかにしてきた。最後にこの認証技術を今後一層普及させていくために克服しなければならない幾つかの課題を考察したい。

１．標準化および規格統一

情報処理技術の急速な進歩、バイオメトリクス認証における認証精度の向上や装置の低価格化に伴い、バイオメトリクス製品の市場は急速に拡大している。現在数多くの入力装置や認証システムが製品化されているが、これらの入力装置や認証システムなどは各社が独自の規格を用いているため、製品間の互換性はなく、認証システム同士を接続して相互運用することができなかったり、可能であっても多大なコストが発生したりする。

18）我々の調査では金融機関におけるバイオメトリクス認証の利用が初めてのケースで、台湾の場合は従来のパスワードによる認証方式にIC カード化に力を入れているが、アメリカでは個人チェックやクレジットカードが主流でATM におけるバイオメトリクス認証にはまだ至っていない。

また、一度導入したバイオメトリクス認証システムを他社のシステムへ移行させる際には、膨大な手間と再セッテイングのコストが発生するため、結果的にユーザーの囲い込みが進み、自由競争による業界の発展を妨げる要因となる。これらの理由から、バイオメトリクス認証システムにおけるハードウェアとソフトウェアの互換性に関する標準規格が必要となる。

バイオメトリクス技術は世界の国々で共通に応用されてはじめて意味を持つセキュリティ技術である。例えば、IC旅券はICカードなどの媒体を人が所持して、世界中を旅するので、その利用の際には世界での互換性が必要となる。そのために、バイオメトリクス認証の用語からシステムの仕様までの技術標準が必要となる。

日本のATMの例をとってみても分かるように、標準化および規格統一は非常に重要である。日本の金融業界においては、偽造や盗難キャッシュカードの被害を防ぐために加盟各行がATMなどへの静脈パターンによるバイオメトリクス認証の導入を進めている。

現在、日本ではこの静脈認証が指の静脈と手のひらの静脈認証に分かれている。２方式が乱立している影響で、別の銀行のATMが使えなかったり、利用者が銀行によって認証方式を使い分ける不便を強いられたりすることが問題になっている。このため、全銀協は大手銀行関係者らで構成されている作業部会で、バイオメトリクス認証の規格統一について検討してきたが、統一しないままそれぞれの規格で運用拡大している。このため、将来、規格統一に要するコストはますます大きくなる一方である。

このような規格の乱立は、預金者を混乱させ、バイオメトリクス認証の普及に大きな影響を与えるのである。現在、水面下では規格の統一が模索されてきたが、調整は難航している。従って、今後バイオメトリクス認証を更に普及させていくためには、標準化と規格の統一が必要である。

2．認証システムにおける脅威と脆弱性の明確化と克服

バイオメトリクス認証は、利用者が本人であることを確保するための情報セキュリティ技術である。この技術を情報システムに展開するには、情報セキュリティ上の要件を考慮した安全性の検討が重要である。しかし、システムに対する脅威はバイオメトリクス認証の脆弱性と結びついて、被害をもたらすので、脆弱性に対して対策を講じるべきである。

したがって、脅威と対策を明確化するには、まずバイオメトリクス認証の脆弱性を明らかにする必要がある。さらに、とるべき対策は脅威と脆弱性の程度から決まるので、脅威と脆弱性の程度についても明らかにする必要がある。

異なる認証システムには異なる脅威と脆弱性が存在するので、脅威と脆弱性を明らかにすることで、セキュリティ問題に対して予め予防の手立てを講ずることができ、また、問題が発生した際にパニックに陥らずに対処することも可能となるのである。したがって、導入しようとするバイオメトリクス認証システムの脅威と脆弱性を、事前にある程度明らかにすることが、システムに対する信頼性の確立とバイオメトリクス認証の普及のために必要である。

3．社会的受容性問題の克服

産業革命以来、産業社会が新しい科学技術を受容する際には、否定的な傾向が大きい。このバイオメトリクス認証という新しい技術に対しても同じことがいえる。指紋は、犯罪捜査、容疑者の確定などの暗いイメージで社会的受容性が悪いが、アメリカへ渡航するためには、ビザの取得や入国手続の際、法律で提供しなければならないと決まっている。そのようなものには従わざるをえない。集合住宅、オフィスや特殊な施設の出入り管理などは、社会環境の変化によって徐々に慣れて受け入れられていくこともあるだろう。しかし、銀行のATMのような場合では指紋技術に対する反発は確実である。

このように、このバイオメトリクス認証技術における受容性の問題は、バイオメトリクス認証技術の普及に対する影響が複雑多岐にわたるため、どのよう

に克服していくかを今後更に考察して対処していく必要がある。

例えば、アメリカでは近年、テロに対処するために、不法移民と不法入国者の問題を如何に対処するかにその重点を置いている。そのために着眼したのは、従来、全国民に与えている社会安全保障番号（Social Security Number）である。就職、銀行口座の開設、運転免許証の取得などあらゆる分野において、この番号の提示が義務付けられた。当然、偽の番号の横行、成りすまし、盗用などが社会的問題となる。2006年12月の初めごろ、全米で大がかりな摘発が行われたが、不法移民と不法入国者に寛大な国柄であることもあり、反響は大きかった。

アメリカのこの複雑な状況を有効に解決するには、社会安全保障番号にバイオメトリクス認証技術を導入することが必要であるが、プライバシーを重視するアメリカでは、今のところ、到底社会的に受容されないだろう。そこで、時を待つか立法で対処するしかない[19)]。この事実をみても分かるように、バイオメトリクス認証の有効性は認められていても、普及させるためには、社会的受容性の問題を如何に克服するかが重要な課題となる。

4．e-コマースにおける本人認証への導入と促進

e-コマースは、大きくＢ２Ｂ、Ｂ２ＣとＣ２Ｃに分けられる。Ｂ２Ｂは業者間の取引で、取引に参加している業者ははっきりしているので、認証の問題は殆どないが、Ｂ２Ｃは小売業者対消費者で、Ｃ２Ｃは消費者間の取引であるゆえに、誰もが参加でき、取引参加者の身分ははっきりしない。そのため騙しや詐欺の問題が横行している。

e-コマースは2000年のIT不況を経験しながら、定着・普及している重要な商取引ツールである。取引額も年々増えてきており、2005年１年間でヤフー１

19）例えば、アメリカは現在、出入国やビザの取得に指紋認証を導入しているが、同時多発テロ以前は、議会の反対で導入できなかった。テロという政治と社会環境の変化が、法案の議会での通過、導入を可能にしたのである。

社のＣ２Ｃの取引金額は5000億を軽々と超えて、これは百貨店一社の取引金額を超えている。しかし、年々騙しや詐欺などの手口も巧妙になり、金額も件数も大幅に増えて、大きな社会問題へと発展してきている。業者はこの問題を解決するために色々な対策を取ってきているが、何れも大きな成果がみられなかった。e-コマースにおける認証のニーズは、金融機関のATMに匹敵するほど大きくなっている。従って、今後、このバイオメトリクス認証のe-コマース分野への導入は重要である。そのための研究も重要な課題となるのである。

５．関連する法制度の整備

IC旅券、金融機関における本人認証など、集合住宅の出入り管理などバイオメトリクス認証技術に対する社会的なニーズが高まっている。このために、バイオメトリクス認証技術を導入するための法整備が行われる必要がある。また、バイオメトリクス情報は究極の個人情報であるので、その安全性を確保するための法律の整備も行われる必要がある。

現在、情報処理分野に関連する法律としては、平成12年に実施された不正アクセス行為の禁止に関する法律、平成16年１月に実施された電子署名･認証法、17年４月に個人情報保護基本法、平成18年２月には預金者保護法が成立し、実施されているが、どの法律もバイオメトリクス認証に直接関連する法律ではないので、今後、バイオメトリクス認証の実施を促進する関連法案の制定が必要となる。バイオメトリクス認証に関する法律としては、導入促進するための法制度および、その実施を妨げる行為の処罰に関するものが考えられる。

参考文献

1．和文資料

1）稲村雄監訳『認証技術～パスワードから公開鍵まで』オーム社、平成15年、Richare E. Smith, Authentication: From Passwords to Public Keys, Addision Wesly, 2002.

2）宇根正志、松本勉「生体認証システムにおける脆弱性について」『金融研究』日本銀行金融研究所、第24巻２号2005年７月

3）瀬戸洋一著『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

4）瀬戸洋一編著『ユビキタス時代のバイオメトリクスセキュリティ』日本工業出版、2003年

5）日本自動認証システム協会編『これでわかったバイオメトリクス』オーム社、2001年

6）日本自動認証システム協会編『自動認識システムの基礎知識』オーム社、2005年

7）日本自動認識システム協会編『バイオメトリクスの基礎』オーム社、平成17年

8）星野幸夫著『指紋認証技術～バイオメトリクス・セキュリティ』画像電子学会、2005年

2．英文資料

1）Anil K. Jain, etc., Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

2）Anil K. Jain, Biometric Technology for Human Identification, SPIE-International Society for Optical Engine, Aug. 2004.

3）Anil K. Jain, Biometric Technology for Human Identification II , SPIE-International Society for Optical Engine, Mar. 2005.

4）Borko Furht and Darko Kirovski, Multimedia Encryption and Authentication Techniques and Applications, AUERBACH, May. 2006.

5）Colin Boyd and Anish Mathuria, Protocols for Authentication and Key Establishment, Springer, Sep. 2003.

6）David D. Zhang, Biometric Solutions: For Authentication in an E-World, Springer, Jul. 2002.

7）Mark Burnett and Dave Kleiman, Perfect Passwords: Selection, Protection, Authentication Syngress Publishing, Jan. 2006.

8）Nalini Ratha and Ruud Bolle, Automatic Fingerprint Recognition Systems, Springer, Oct. 2003.

9）M. H. M. Schellekens, Electronic Signatures: Authentication Technology from a Legal Perspective, Asser Press, Sep. 2004.

10）Peter Komarinski, Automated Fingerprint Identification Systems, Academic Press, Dec.

2004.
11）S.Y. Kung, M.W. Mak, and S.H. Lin, Biometric Authentication: A Machine Learning Approach, Prentice Hall, Sep. 2004.

3．その他の参考資料

1）早稲田大学理工学総合研究センター
「応用例からみたバイオメトリクス認証のあり方～進むATM への普及とその将来像～」2005年７月
資料出所：
http://www.ubiteq.co.jp/ubiq/research/report/paper/biometrics-auth.pdf,（2006年12月現在）
2）新規産業レポート「バイオメトリクス認証の現状と今後の展望～研究開発段階から普及の段階へ」2006/冬
資料出所：大和総研、小坂大輔
http://www.dir.co.jp/research/report/hitech/06010901hitech.pdf,（2006年12月現在）