バイオメトリクス技術とプライバシー

── その法的側面についての一考察 ──

Biometric Technologies and Privacy Issues

松前恵環*　Satowa MATSUMAE

1．はじめに

トム・クルーズ主演のミッション・インポッシブルに代表されるように、近年のハリウッド映画にはバイオメトリクス認証のシーンが頻繁に登場する。虹彩認証や指紋認証、そしてそれらの認証システムを欺くなりすまし等・・・こうしたハリウッド映画で描かれる世界はしかし、もはやSFの世界に止まるものではない。今や日本でも、静脈認証システムを用いた銀行ATMはごく一般的に見られるようになり、顔画像を搭載したIC旅券も2006年3月から発行される[1]など、バイオメトリクス技術は日に日に我々の日常生活に密着したものとなりつつある。

こうしたバイオメトリクス技術が世間の注目を集めている要因は、個人の身体的特徴を用いることで確実に本人認証を行い得るという、認証技術としての有用性にある。特に「9. 11」テロの衝撃以来、テロリズムへの対抗や国防、公共の安全への要請が世界的に強まる中で、テロリスト等を識別・特定する必要性が急激に高まっていることが、バイオメトリクス技術の利用を後押しする一大要因となっていると言えよう。

他方、こうした有用性と共に、様々な法的問題が生じ得ることも指摘されている。こうした法的問題の例としては、例えば電子署名、知的財産権に関わる問題等が挙げられている[2]が、特に強く懸念されているのは、プライバシーに関わる問題である。バイオメトリクス技術は「パスワードとしての身体」(Davis, 1997) を現実化する技術であるために、その利用に際しては個人の身体に関わる様々な情報が処理され、プライバシーについて看過できない影響を及ぼす虞が生じるのである。

我が国では、バイオメトリクス技術に関する一定の技術的検討は既になされているものの、プライバシー保護の文脈における法的な検討は未だ多くはない[3]。そこで本稿では、こうしたバイオメトリクス技術によって生じ得るプライバシーの問題について、バイオメトリクス技術という新しい技術がプライバシーに対してどのような影響を生ぜしめるのか、またそれらに対

*東京大学大学院学際情報学府
キーワード：バイオメトリクス技術、プライバシー、個人情報、法制度、身体

して現在如何なる措置が講じられ、今後どのような対応がとられるべきなのか、問題情況の分析、現在の我が国及び外国の法的対応の比較検討、そして対応のあり方についての考察を行いたい。これによりまず、バイオメトリクス技術が情報技術の進展とプライバシーの連関の歴史上にもたらす、一つの新たな局面を浮き彫りにすることができるものと考える。また本考察を行うにあたっては、「身体に関する個人情報」を生むというバイオメトリクス技術の本質に遡った検討を試みたい。そうすることで、近い将来現実化するであろうユビキタスネットワーク社会におけるプライバシーを考える上での、一つの手がかりを得ることができると考える。すなわち、ユビキタスネットワーク社会の象徴として「モノのインターネット（Internet of Things）」[4]という現象が頻繁に取り上げられるが、このネットワーク化は既にモノのみならずヒトにも及びつつあり、いずれは我々人間もネットワーク化された世界の一部となり（Rodota, 2005: 44）、従来を遥かに超える量の身体に関する個人情報がネットワークを流通する可能性も否定できない。バイオメトリクス技術はこうした現象の一端に位置付けられるものであり、かかる意味において、バイオメトリクス技術に関するプライバシーの問題を検討することは、今後のユビキタスネットワーク社会においてプライバシーをどう考えていくのかという未来の考察につながる、一つのステップとなり得るのである。

2．バイオメトリクス技術とプライバシー

2.1　バイオメトリクス技術の仕組みと利用[5]

バイオメトリクス技術とは、人の生体的な特徴・特性を用いて行う本人認証方式であり、生体的な特徴・特性を総称してバイオメトリクス情報と呼ぶ。バイオメトリクス情報には、指紋、掌形、虹彩、網膜、顔、血管等の身体的外観に基づくもの（身体的特徴）と、音声や署名等の行動特性に基づくもの（行動的特徴）とがある。

そもそも本人認証の方式としては、パスワード、暗証番号等の個人の記憶に基づくもの、トークン、ICカード等の個人の所持に基づくもの、そして、バイオメトリクス情報のように個人の存在・状態に基づくものの3つの方法が考え得る。こうした認証方式の中でもバイオメトリクス認証は、個人の記憶に基づく認証に付随して生じる漏洩や忘却といった問題、更には個人の所持に基づく認証に付随して生じる紛失、偽造、盗難といった問題を回避できる確実な認証方式として、注目を集めている。何故ならば、バイオメトリクス認証において用いられる身体的特徴は、まさにそれが本人の証であって常に個人の肉体に付随しているものであり、行動的特徴は言わば本人の癖であって、本人でありさえすればいつでもどこでも再現が可能になるものだからである。

バイオメトリクス認証に用いられる生体特徴の性格としては、特に次の3つを挙げることができる。第一は普遍性であり、当該生体要素が全ての人間に存在していること、第二は固有性・

独自性であり、当該生体要素が各個人に固有のものであること、第三は不変性であり、当該生体要素の特質が各個人について長期にわたって不変なままであるということである。これらの性格はまさにバイオメトリクス認証の確実性を可能にするものであり、バイオメトリクス認証に用いる生体特徴（モダリティ）の要件ともなっている。もっとも、こうした生涯にわたる固有性・不変性にも例外があり、老化や手術、事故等によって変化する可能性や、指紋認証においては、指の乾燥や酷使によって皮膚が擦り減ったり傷ついたりすることで認証が困難になる可能性等も指摘されている。このように、各モダリティ単独では要件を完全に満たすことはできない場合もあるため、幾つかのモダリティを組み合わせたマルチバイオメトリクス方式を用いたシステムや、他の認証方式と併用するシステムも検討されている。

バイオメトリクス認証の利用は、これまで主に指紋やDNA[6]による本人認証を中心に行われてきた。特に指紋は、犯罪捜査等に代表されるように警察目的でその大規模収集が行われてきたという経緯を持つ。1980年代後半からは民間利用も始まり、現在ではモバイル機器、住宅、金融、医療、勤怠管理、アミューズメント等の幅広い分野で利用が進められている。もっとも、特に2001年の米国同時多発テロ以降は、公共の安全のための厳格な本人認証技術としてバイオメトリクスへの期待が高まっており、国防、航空等の分野での利用が増大している。こうした利用の例としては、外国人の出入国時にバイオメトリクス情報の提示を義務付ける、米国のUS-VISITプログラムが重要であろう。US-VISITプログラムについては、原則全ての外国人渡航者が指紋の読み取り及び顔画像の撮影を受けることになるという点で、プライバシーへの危険性が指摘されている[7]。

2.2　プライバシーの概念検討

そもそもプライバシーとは、「人間のプライバシーへの欲求は、その動物的起源に根ざす」（Westin, 1967: 8）と言われるように人間の本質に密接に関わる概念であって、古くより生物学、生態学、人類学等といった様々な分野において研究が行われてきた[8]。しかし、法学領域においてプライバシーの権利が法的権利として明確に主張されたのは比較的新しい。Cooly（1888）の「ひとりで居させてもらいたい」という権利の発想を受け、WarrenとBrandeisによる論稿において煽情的なイエロージャーナリズムへの対抗という文脈で、「一人で放っておいてもらう権利」（Warren & Brandeis, 1890）として主張されたのが最初であると言えよう。1960年代に入るとデータバンク社会の到来によるプライバシーへの影響が懸念されるようになり、Westin（1967: 7）の「プライバシーとは、自己に関する情報がいつ、どのように、そしてどの程度他者に伝達されるかについて自ら決定できる、個人、集団、或いは組織の要求」という定義に代表される、プライバシーの権利を自己に関する情報をコントロールする権利として理解する説が提唱された。もっとも、プライバシーの定義・価値等については今日に至るまで

多種多様な学説が展開されており、プライバシーそのものの何たるかについては、未だ一義的な理解は確立されていない。こうした多様な定義についてSolove（2002: 1095-1124）は、①一人で放っておいてもらう権利、②自己へのアクセスの制限、③秘密、④個人情報のコントロール、⑤人格、⑥親密性の6つに分類できるとしている。

日本では、アメリカの影響を強く受けてプライバシーの概念が発展してきており、現在では日本においても、消極的な「一人で放っておいてもらう権利」よりもむしろ、佐藤幸治（1970: 12-18）の主張する「自己情報コントロール権」としてプライバシー権を把握するのが通説的理解となっている。もっとも、かかる見解に異議を唱える説もある[9]ことに加え、憲法13条の幸福追求権の一環として認められると解されるプライバシー権に、所謂自己決定権としてのプライバシー権を含むかどうかについても争いがある[10]など、プライバシーについての統一的な理解は我が国でもやはり確立されていない。本稿では、基本的に自己決定的プライバシーは考察の対象から外し、所謂自己情報コントロール権としてのプライバシー権に関連する領域を中心に考察する[11]。

こうした自己情報コントロール権としてのプライバシーの権利を保護するための法的対応の一つとして近年その重要性が高まっているのが、個人情報の保護に関する法制度である。すなわち、プライバシー権を自己情報コントロール権と解したとしても、その性格、内容、範囲が必ずしも明確ではないことや、回復困難なプライバシー侵害についての予防的措置の必要性から、プライバシーよりも外延のはっきりしたより広い集合としての「個人情報」を保護する、個人情報保護制度が構築されている（藤原, 2003: 1-2; 22-23）のである。

個人情報保護については、様々な国際的議論や取組みを経て、国際的な指針として重要な役割を担っているOECD 8原則（収集制限の原則、データ内容の原則、目的明確化の原則、利用制限の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則）[12]や、それを更に具体的かつ詳細にしたと言われるEU指令（データ内容に関する原則：6条、データ処理の正当性の基準：7条、データ主体に提供されなければならない情報: 10・11条、データへのアクセス権：12条、処理の機密性及び安全性：16・17条、等）[13]、また公正な情報慣行（Fair Information Practices: FIPs）（通知／認識、選択／同意、アクセス／参加、データの完全性／セキュリティ、施行／救済）[14]といった個人情報保護のための基本原則が定着してきている。近年多くの国において、これらを基礎とした個人情報保護のための制度―法規制に加え、行政ガイドラインや、民間における自主規制等も含めて―が整備されつつある。

3．バイオメトリクス技術のプライバシーへの影響

3.1　二つの側面

では、バイオメトリクス技術はプライバシーに対して、如何なる影響を及ぼすのであろうか。この点に関し、EUで実施されたBIOVISIONプロジェクト[15]の報告書（以下、「BIOVISION報告書」）（Albrecht, 2003: 10）は、プライバシーとバイオメトリクス技術の関係について、バイオメトリクス情報は他の個人情報と同様にそれ自体保護されなければならない「対象・目的」であるという側面と、他のプライバシーを保護するための新しい有効な「道具」であるという、二つの側面を有するという点を指摘している。後者の意味するところはすなわち、プライバシー保護への積極的な影響である。BIOVISION報告書（Albrecht, 2003: 10）は、バイオメトリクス技術が上に指摘したような普遍性・固有性・不変性故に個人を特定するという点において高い精度を持つ本人認証技術であるため、個人情報への情報主体のアクセス権がより行使し易くなり、また、ID窃盗や不正利用を防ぐことができ、個人情報・プライバシーを「保護」することができるという点を指摘している。これは欧州評議会（Council of Europe: CE）が公表している「ヨーロッパ条約第108号に定める原則のバイオメトリクスデータの収集・処理への適用に関する報告書」[16]（以下、「CE報告書」）（Council of Europe（以下、「CE」）, 2005: 13）においても、バイオメトリクス技術の、プライバシー強化技術（Privacy Enhancing Technologies: PET）としての機能として言及されている。

しかし、かかる意義は否定できないにしても、バイオメトリクス情報が毀損・漏洩した場合にもこれを復元或いは撤回することは困難であること、更にバイオメトリクスが強力な認証手段であるが故に、無権限者の不正利用を証明することが極めて困難になること等に鑑みれば、プライバシーへの「脅威」という消極的側面もが同時に含まれていることを看過すべきではない[17]。プライバシーに対する脅威への対処なくしてバイオメトリクス技術の利用・普及は進展せず、そのプライバシー保護の側面も十分に機能し得ないのである。

3.2　プライバシーへの脅威

バイオメトリクス技術がプライバシーに及ぼす脅威については多くの問題点が指摘されているが、特に本稿の考察対象である自己情報コントロール権としてのプライバシー権に直接に関わる問題としては、バイオメトリクス情報の通知及び同意なき取得、目的を超えた利用、センシティブ情報の抽出に関する問題等が挙げられる。

通知及び同意なき取得については、経済協力開発機構情報コンピュータ通信政策委員会の情報セキュリティとプライバシーに関する作業部会（OECD/ICCP/WPISP）により公表された報告書「バイオメトリクス技術」（以下、「OECD報告書」）（OECD, 2004: 12-13）が、幾

つかのバイオメトリクス情報は、個人の同意なくして、またバイオメトリクス認証への現実の関与なくして、本人の知らないうちに収集され得る危険性があることを指摘している。こうした問題は、人間が特に意識しないうちに自らの行動に伴ってあらゆる場所に何らかの生体的痕跡を残しており、そこから何らかのバイオメトリクス情報が収集され得ることから生じる。例えば、我々は日常生活において手で触れるものに指紋を残しそれを特には意識しないが、そうしてグラス等に残された指紋は個人の気付かないうちに収集され利用される可能性がある。また、DNA情報[18]についても、個人が残した毛髪や、唾液の付着した煙草の吸殻やグラス等から情報収集を行うことが可能だと言われている(Rodota, 2005: 49)。虹彩に関しても、認証対象との間に相当の距離があっても本人認証を行い得るようになってきており、OECD報告書(OECD, 2004: 13)は、今後技術が一層発展すれば更に離れた距離から、かつ本人が全く関知しないままに、虹彩情報を取得できるようになるという可能性を指摘している。2005年の国際プライバシーコミッショナー会議で採択された「パスポート・IDカード及び渡航書類へのバイオメトリクスの利用に関する決議」(以下、「国際PC決議」)(International Conference of Data Protection & Privacy Commissioners(以下、「PC」), 2005)も、人が無意識のうちに生体的痕跡を残すことにより、本人が気付かないうちにバイオメトリクス情報が収集されるという点について、特に留意が必要だとしている。

次に指摘すべきは、バイオメトリクス情報の目的を超えた利用に関する問題である。OECD報告書(OECD, 2004: 12)は、目的を超えた利用('function creep')とは、ある特定の目的のために収集された情報が他の意図されていない、或いは不正な目的のために利用されるという、情報処理プロセスやシステムの不正な拡張を意味すると述べる。そして、こうした利用の具体例として例えば、生活保護システムにおいて登録に指紋のスキャンが要求されており、その指紋は扶助金の二重取りを防ぐという目的のためにのみ利用されるということが利用者に約束されているような場合に、収集した指紋を登録時に明らかにされていないそれ以外の目的のために利用するようなこと等を挙げている(OECD, 2004: 12)。BIOVISION報告書(Albrecht, 2003: 11-12)もバイオメトリクス情報の本来の目的を超えた利用に関して、バイオメトリクス認証がユビキタス認証スキームの基礎として利用されることにより、例えば個人の行動の追跡、個人に関する様々な情報からのプロファイリングが行われる危険性や、公的・民間部門双方における集中データベースの構築等が行われる危険性について述べている。Woodward(2001: 30-31)は、バイオメトリクス技術は、暗証番号やパスワードといった他の認証技術には不可能な「追跡」を可能にする点で、こうした目的を超えた利用が起こり得る可能性があることを指摘している。

更に、こうした問題に加え、バイオメトリクス情報からセンシティブな個人情報が抽出される危険性があることも指摘されている。Woodward(2001: 30)は、バイオメトリクス技術に固有な新しい問題として、医療情報等のセンシティブ情報が抽出される問題について言

及している。例えば、網膜や虹彩からは糖尿病、動脈硬化、高血圧等の疾患が明らかになり得ることや、指紋と染色体異常や、白血病、肺癌等との関連性等が指摘されている（Woodward, 1997: 115-116）。また、医療情報の他に、特に顔認証システムでは、不可避的に人種等のセンシティブ情報が明らかになることも指摘されている（Rejman-Greene, 2005: 345）。

こうした自己情報コントロール権としてのプライバシー権に関する問題に加え、更に、物理的・身体的プライバシーや自己決定権との関係でも問題が指摘されている[19]他、OECD報告書（OECD, 2004: 12）では、バイオメトリクス技術が監視社会のインフラとなり得る危険性－バイオメトリクス技術が大量の個人情報の体系的な収集・利用を可能にし、情報化社会の非人間的側面を助長させる危険性－も指摘されている。同報告書（OECD, 2004: 12）は、今後バイオメトリクス認証が人間の識別あるいは確認のための既定方法として定着すれば、バイオメトリクス情報に比してよりプライバシー侵害の危険性の少ない方法で十分な場合にも、単に人間が皆バイオメトリクス情報を有しておりそれを常に使っているという理由だけで、当該認証が利用されるようになるという懸念を示し、こうした場合、個人を特定するバイオメトリクス情報を利用した監視の容易性は非常に高まることを指摘する。小倉利丸（2003: 21-25）もまた、バイオメトリクス認証が監視社会のツールとして用いられる危険性を指摘している。

こうしたプライバシーへの脅威の背景には、バイオメトリクス技術が「パスワードとしての身体」を実現する技術であり、身体そのものに関する情報が処理されるという点において、他の認証技術とは異なる特徴を有しているということが存すると考えられる。CE報告書（CE, 2005: 9）が指摘する、バイオメトリクス情報は「人間の身体」から収集され、「人間の身体」に由来するという本質的な特徴こそが、こうしたプライバシーへの新たな脅威をもたらしていると言えよう。

4．バイオメトリクス技術についての法的対応の現状

4.1　国際的動向

では、こうしたバイオメトリクス技術がプライバシーにもたらす脅威について、法的には如何なる対応がなされているのか。本稿では、主に個人情報保護法制を中心として検討を進める。

まず我が国では如何なる対応を採っているのかについて検討するに、バイオメトリクス情報が「個人情報の保護に関する法律」（平成15年法律第57号）（以下、「個人情報保護法」）に言う「個人情報：生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。（第２条１項）」に該当すれば同法が適用されるため、基本的には個人情報保護法の問題となり[20]、一

定の法的対応がとられているとも考えられる。もっとも、個人情報保護法のバイオメトリクス技術への適用については、バイオメトリクス技術特有の問題への対応のために付加的な考慮が必要となるが、現在我が国では特にバイオメトリクスに関する包括的な指針やガイドライン等は策定されていない。金融・信用分野に関する「金融分野における個人情報保護に関するガイドライン」（金融庁, 2004）及び、「経済産業分野のうち信用分野における個人情報保護ガイドライン」（経済産業省, 2004）において、センシティブ情報に関する規定の中でバイオメトリクス情報（生体認証情報）についての規定があるに止まる[21]。

一方で国際的な動向に目を向けると、国際的指針として意義を有するものとして、前述国際PC決議（PC, 2005）が挙げられる。同決議では、「1.バイオメトリクス認証に固有のリスクを制限するために早期に安全対策を実施すること、 2.法律上の義務に基づいて公共目的のためにバイオメトリクス情報が収集・保存される場合と、同意に基づいて契約目的で行われる場合とを厳密に区別すること、 3.バイオメトリクス情報が記載されたパスポートやIDカードを、それらの記載情報と持ち主が提供したバイオメトリクス情報とを照合して、確認目的で利用することについて技術的制限を設けること」の3つの指針が示されている。

米国においては、公的部門を規制するプライバシー法は存在するもののそもそもプライバシー保護のための包括的な民間規制法が存在せず、分野毎の個別法と自主規制を組み合わせるというセクトラル方式での対応が行われている。バイオメトリクス技術についても、米国防総省（Department of Defense: DoD）のバイオメトリクス・マネジメント・オフィス（Biometrics Management Office: BMO）において、プライバシー保護のために指針作成等の取組みが行われている[22]ものの、その他は自主規制を中心に対応がなされており、業界団体や企業等によってプライバシー保護のための幾つかの指針が提唱されているに留まる。特に業界団体の策定した指針として意義を有するのが国際バイオメトリック産業部会（International Biometric Industry Association: IBIA）（IBIA, 2000）の指針であり、公的部門、民間部門双方に配慮した4つの原則が定められていることが特徴的である。

こうした米国と対照的に、EUではプライバシー保護について特に積極的な取組みが行われている。EUは1995年に前述のEU指令を公表し、公的部門及び民間部門を包括する、特に厳格な個人情報保護法制を基本としてプライバシー保護の問題に取り組んでいる。そして、新しい技術の登場によって生じる新たな個人情報の問題についても、基本的にかかるEU指令を適用することを前提に、個々の問題について指令を適用する際のガイドラインを策定して指針を示すという形で対応してきている[23]。バイオメトリクス技術についても同様の姿勢を採っており、バイオメトリクス技術を利用した個人情報の処理にEU指令を適用するにあたっての指針としては、EU指令29条に基づく作業部会（Article 29 Data Protection Working Party）が「バイオメトリクスに関する作業文書」（以下、「EU作業文書」）を公表している（European

Commission（以下、「EC」), 2003)。また、EUでは2002年から、欧州委員会（European Commission: EC）が統括する第5期研究開発プログラムの情報社会技術（Information Society Technologies: IST）プロジェクトの一環として実施されたBIOVISIONプロジェクト[24]で、欧州におけるバイオメトリクス普及のためのロードマップが検討されており、当プロジェクトで公表されたBIOVISION報告書（Albrecht, 2003）において、プライバシーベストプラクティス（以下、「ベストプラクティス」）が策定されている。これはバイオメトリクス技術を用いた個人情報の処理へのEU指令の適用について、EU指令を補完するものとしてその要求事項の説明や解釈に関する提言を行うものであり、データ管理者及びサプライヤ、そしてエンドユーザに対するガイダンスを提供することを目的として、極めて詳細なガイドラインを提示している。

4.2　個別の問題についての対応－EU指令を中心に－

本稿では、EU指令を基礎としつつバイオメトリクス技術特有の問題にも配慮してプライバシー保護に積極的な対応を行っているEUの状況を中心に、先に指摘した個別の問題－バイオメトリクス情報の通知及び同意なき取得、目的を超えた利用、センシティブ情報の抽出に関する問題－に対し、どのような法的対応がとられているのか、検討を行うこととする。

EU指令をバイオメトリクス技術を用いた個人情報の処理に適用するにあたり、まず前提として検討すべきは、そもそも如何なるバイオメトリクス情報が法に規定される「個人データ: 特定又は特定し得る自然人（データ主体）に関する全ての情報を意味するものとする。特定し得る個人とは、特に身元確認番号や、その個人の肉体的、生理的、精神的、経済的、文化的、社会的アイデンティティーの一つ以上の要素の参照によって、直接又は間接に特定することができる者を意味する。(指令2条(a))」の定義に該当するのかという点であろう。バイオメトリクス情報については、オリジナルデータとそこから特徴量抽出を行って得たテンプレートデータが存在するため、これらをどう評価するのかが問題となるのである。ベストプラクティス（Albrecht, 2003: 16-17）はこの点について、オリジナルデータはほとんどの場合、指紋、顔、虹彩等選択された特徴のオリジナルイメージであり、テンプレートはオリジナルから抽出され数学的方法によって計算されたオリジナルデータのハッシュコードのみを含むものであると、両者の区別を述べる。そして現在の技術状況においては、バイオメトリクスのテンプレートからはオリジナルはほとんど復元され得ないことから、テンプレートが個人データに該当しない場合もあることを指摘するが、結論としては、ほとんどの場合は個人データに該当するとし、またベストプラクティスにおいてはそのように扱うことを推奨している。EU作業文書（EC, 2003: 5-6）も、オリジナルデータ及びテンプレートデータは、まさにその性質上自然人に関する情報であり、バイオメトリクス認証において当該人物は他の人間と区別されるという点では一

般的に識別可能であるという点を指摘して、ほとんどの場合「個人データ」に該当すると述べている。

4.2.1　通知及び同意なき取得

こうしたEU指令の適用を前提とし、EU作業文書（EC, 2003: 8）は、バイオメトリクス情報が本人の通知及び同意なくして、本人の知らないうちに収集され得るという問題につき、指令10条及び11条から「適正な収集及びデータ主体への情報提供」の原則が導かれることを指摘する。そして、データ管理者は指令10条及び11条に従って情報主体に情報提供をすべきであり、特に厳密に明確化した目的とデータ管理者の身元を通知すべきであるという指針を示している（EC, 2003: 8）。また、情報主体が知らないうちにバイオメトリクス情報を収集するシステムの利用は避けるべきであり、遠隔顔認識システムや指紋の収集等はこの観点から危険性が高いことを指摘している（EC, 2003: 8）。また、指令７条の「データ処理の正当性の基準」に従って、同意が情報処理の適法理由となる場合には[25]、指令２条の要件を満たす同意―データ主体の当該個人情報の処理についての合意を示す、任意の、明確な、十分な情報提供を受けた上での、意思の表示―が必要であることを示している（EC, 2003: 8）。

4.2.3　目的を超えた利用

当初定められていた個人情報の収集目的を逸脱した利用が行われるという目的を超えた利用の問題については、EU作業文書（EC, 2003: 6-8）が、指令６条より「目的明確化の原則」が導かれることを指摘し、個人データが明確かつ適法な目的のために収集されなくてはならず、それらの目的を超える態様で処理されてはならないという指針を示している。また、バイオメトリクス情報は集中的なデータベースに保存されるよりも利用者が有するICカードや携帯電話等に保存される方が望ましいことや、例えばアクセス管理のために処理された情報が情報主体の精神状態を評価するためや職場における監視のために用いられることは禁止すべきであること等を述べている（EC, 2003: 6-8）。ベストプラクティス（Albrecht, 2003: 22-23）は、EU指令前文28項によれば指令６条は特に、データはそれらが収集される目的との関係において適切で、関連性を有し、過度であってはならず、またそれらの目的は明確かつ適法で、データ収集時に決定されなければならないことを意味するとし、データ処理の目的は元々特定された目的に従わなくてはならないことを示している。

4.2.4　センシティブ情報の抽出

指紋や顔画像等から医療情報や、人種といったセンシティブな情報が抽出されるという問題に関しては、EU指令において、センシティブ情報の処理の制限規定が置かれている（指令８

条)。指令 8 条 1 項によれば、センシティブ情報とは、「人種又は民族的起源、政治的見解、宗教的・思想的信条、労働組合への加盟事実、健康状態及び性生活を明らかにする個人情報」であり、かかる情報については、情報主体の明示の同意がある場合等を除いては原則として処理が禁止されている（指令 8 条 1 ，2 (a)）。EU 作業文書（EC, 2003: 10）は、例えば顔認証システムにより人種や民族的起源が明らかになる場合等においては、指令 8 条が適用されるとしている。

もっとも、センシティブ情報の抽出については慎重な検討が必要であるという指摘もなされていることには、留意が必要であろう。例えば Rejman（2005: 345）は、そもそもオリジナルデータをテンプレートデータにする際にオリジナルデータが存在しなくなるのであれば、オリジナルデータ自体をセンシティブ情報と評価すべきではないことを指摘している。Woodward（1997: 115）も、センシティブ情報が抽出されるからと言って虹彩や網膜等のスキャン自体がプライバシーを侵害するとは言えず、テンプレートデータがこうしたセンシティブ情報を含むのかが検討されねばならないとする。そして、仮に含まれたとしても、そこからセンシティブ情報が抽出されるのは、テンプレートデータ自体がセンシティブ情報を明らかにするか、若しくはオリジナルデータが復元されることによりセンシティブ情報が明らかになるのかのいずれかであるとしている。この点についてテンプレートデータからオリジナルデータを復元することは不可能であるとして、テンプレートデータはセンシティブではないとする見解もある（de Hert, 2005: 16-17)。また、処理の目的がセンシティブ情報を抽出することにないのであれば、センシティブ情報とは評価されないという点も指摘されている（de Hert, 2005: 16-17)。

5．むすびにかえて－対応のあり方についての考察と今後の課題－

5.1　対応のあり方についての考察

本稿における検討からまず、バイオメトリクス技術という新たな技術により、プライバシーについて深刻な脅威が現実化する可能性、その脅威の態様、その脅威とプライバシーの接点が明らかになった。具体的には、通知及び同意なき取得、目的を超えた利用、センシティブ情報の抽出が自己情報コントロール権との関係で特に問題となり、これらの背景には、身体に関する個人情報を生み出すというバイオメトリクス技術の本質的特徴があることが指摘できる。情報技術とプライバシーの連関の歴史の上でも、こうした新たな特徴により新たな局面が生じていると言えよう。また、こうした問題情況に対し、我が国では未だ十分な法整備がなされていないのに対し、海外、特にEUにおいては積極的な法的対応がなされていることを示しておいた。

かかる検討結果を踏まえ、我々が現状において如何なる対応をとっていくべきかについて考察する。まず指摘すべきは、バイオメトリクス

認証の利用について、その無制限な利用に歯止めをかけることの重要性であろう。バイオメトリクス認証は一面においてプライバシーを「保護」する役割を担い得るものの、本稿で検討した通り、プライバシーを保護する役割を担い得るだけの個人特定の正確性こそが、逆にプライバシーを「侵害」するという危険性を孕んでおり、いずれの効果ももたらし得る両刃の剣である。とすれば、かかる技術の利用については何らかのルールないし一定の制限を設けて、これをプライバシーを侵害しない態様で用いることが必要になると考えられる。よりプライバシーを侵害する危険性の低い代替的手段がある場合には、バイオメトリクス技術を用いるべきではないという基本的姿勢[26]は、こういったルールにおいて特に尊重されるべきであろう。

日本においては、基本的に個人情報保護法の適用が肯定されると考えられ一定のルールは存在するとも言えることを指摘したが、EU指令を例に検討したようにバイオメトリクス技術特有の問題も存在するため、適用にあたっての何らかの指針を示すことが望ましいと考えられる。特にセンシティブ情報の処理制限については、日本の個人情報保護法に規定されていないため、金融分野のガイドラインも含め、今後検討を進めていく必要がある。指針の在り方については、バイオメトリクス技術が未だ発展段階にあることに鑑みれば、柔軟な対応を可能にするために、法的な規制よりはむしろ、行政或いは民間によるガイドラインによって一次的には対応し、今後法規制も視野に入れた検討を行っていくことが現実的かつ有効であろう[27]。

また、技術の利用について一定の歯止めをかけるという観点からは、こうした法的ルールに加え、バイオメトリクスシステム自体がプライバシーの保護に配慮した形で、社会的リスクを最小化し、バイオメトリクス情報の不正利用を防止するように、設計されることが重要である。バイオメトリクス技術のようにプライバシーへの深刻な影響を及ぼし得る技術が有用性という免罪符を得て一旦導入されてしまえば、プライバシー保護の要請はそのコスト等を理由に、隅に追いやられる危険性が大きい。よって、システムの設計段階でプライバシー保護のための措置を組み込んでいくことが極めて重要になると考えられる。こうした総合的措置の必要性に関連して、Cavoukian（1999: 11）は、バイオメトリクス技術がプライバシーへの脅威とならないためには、法的、手続的、技術的な措置を含む厳格な保護装置が不可欠であることを指摘している。

5.2　今後の課題－バイオメトリクス情報についての本質的考察－

本稿における考察では、「身体に関する個人情報」を生むというバイオメトリクス技術の本質的特徴故に、自己情報コントロール権としてのプライバシーに対する新たな脅威が生じていることを明らかにした。これにより、冒頭に示したような「身体に関する個人情報」が大量に処理される社会の到来に直面して、我々は従来とは異なる視点を視野に入れた考察を迫られていること、そして今後こうした新たな視点を手がかりにプライバシーの考察を行っていくべき

ことが指摘できよう。しかし最後に、「身体に関する個人情報」についてのより原理的課題が依然として残っていることを指摘しておかなければならない。

そもそも「身体に関する個人情報」については、こうした情報が処理され、流通することへの根深い抵抗感が我々の間に存在しているという指摘がある。例えば本稿で主に検討対象としてきたヨーロッパでは、CE報告書（CE, 2005: 9-10）が、自己の身体は最も個人的なものであってそういった情報を収集することは人間の尊厳の侵害になると主張する人もいれば、人間の身体を情報源として利用されることに心理的抵抗を感じる人もおり、また、指一本であっても自らの身体の一部を機械に読み取らせることに抵抗する人もいれば、人間の身体の無分別な平凡化に懸念を示す人もいることを指摘する。Rodota（2005: 41）も情報化時代における身体の変化について述べる中で、身体は情報化時代においてはデータの集合―情報システム―と見なされると指摘し、身体は新たな情報の源となり、絶えず情報を搾取されると述べている。こうした懸念の根底には、EU基本権憲章第3条では、身体の不可侵原則及び身体的精神的統合が規定されている（EGE, 2005）ということからも理解されるように、「人間の身体」というものが単なるモノとは異なるという考えが存在しているように思われる。

こうした懸念や抵抗感を踏まえて今後の課題として提起しなければならないのは、こうした「身体に関する個人情報」の本質をどう考えるべきか、すなわち、身体に関する情報であるが故に他の情報と異なる何らかの特別の性質を有するのか、有するとすればどのようにこれを法的に位置付けるべきか、といった、原理的な課題であろう。本稿では、「身体に関する個人情報」を、あくまで自己情報コントロール権を背景とした個人情報保護法制の枠組みの中で、主に「個人情報」という視点を軸に検討したが、今後は、「身体」という視点からより重点的に考察し、その理解を背景として「身体に関する個人情報」を検討していくことが必要なのではないだろうか。Rodota（2005: 41-44）は、データの集合となりつつある身体の現状を‘electronic body’と表現して、今まさに再び「身体」概念が重要になりつつあることを指摘している。また日本においても、主にDNAに関する検討においてではあるが、身体に関する情報を如何に扱うかという問題が提起されており[28]、こうした議論も参考になり得るであろう。

バイオメトリクス技術が人間の身体を機械で読み取ることを可能にし（PC, 2005）、また、センサー技術は人間の身体の状態や更には感情までも読み取ることを可能にするといった技術の進展により、近い将来、人間自体がデジタル情報の集合として扱われるようになり、人間の身体に関する情報はますます増加していくであろう。今後のプライバシーに関する法的考察においては、「身体」について、そして「身体に関する個人情報」について、原理的な考察を行っていくことが一つの大きな課題となっていくものと考えられる。

註

1 IC旅券については、外務省のホームページ参照。＜http://www.mofa.go.jp/mofaj/toko/passport/ic.html＞

2 *See* Albrecht & Walsh（2003）.

3 バイオメトリクス技術とプライバシーに関する法的検討を行った主な論稿としては、新保（2006）、飯田（2006）等がある。

4 「モノのインターネット」については、ITU（2005）参照。

5 バイオメトリクス技術の仕組みと利用については、日本自動認識システム協会（2005）、情報処理推進機構（2004）、瀬戸（2003）、バイオメトリクスセキュリティコンソーシアム（2006）、CE（2005）、EC（2003）等を参照。

6 OECD（2004: 11）によれば、DNAを用いた照合は、一般的なバイオメトリクス技術と異なり、実際の物理的なサンプルを必要とするという点、DNAの照合はリアルタイムで行うことができず、またほとんどの場合自動化されていないという点、更にDNA照合はテンプレートや特徴抽出を要せず、実際のサンプルの比較を意味するという点等において、厳密にはバイオメトリクス認証ではないとされる。

7 当プログラムによって、バイオメトリクス情報が搭載された国際民間航空機関（International Civil Aviation Organization: ICAO）標準準拠のｅパスポートの提示が必要となる。これを受けて我が国でも、国籍・氏名等の身分情報の他、顔画像を搭載したIC旅券が採用されている。

8 Westin（1967: 8-11）は、こうした研究を紹介し、プライバシーへの欲求における人間と動物の共通点を指摘している。

9 例えば、棟居（2002: 37）は、「多分に情報化社会に適合的なプライバシー保護の技法として提唱されている」として、自己情報コントロール権の限界を指摘する。

10 長谷部（2001: 155）によれば、自己情報コントロール権と自己決定権の二者を含むのが通説的理解とされるが、佐藤（1990: 282）は、自己決定権は自己情報コントロール権とは別個のものとして理解されるべきであるとする。

11 もっとも、自己決定権と自己情報コントロール権とは、密接に関連するものであることには留意が必要である。例えばRichards（2006, 1102-1121）は、情報プライバシーと自己決定権的プライバシーの密接な関連について述べている。

12 OECDの「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data」で定められている原則。

13 正式名称は「個人データ処理に係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95/46/EC指令: Directive 95/46/EC of the European Parliament on the Protection of individuals with regard to the processing of personal data and on the free movement of such data」である。

14 OECD 8 原則と基礎を同じくする個人情報保護の基本原則である。*See* US FTC (1998).

15 EUのBIOVISIONプロジェクトについて詳しくは、本稿4.1参照。

16 「ヨーロッパ条約第108号」とは、欧州評議会の閣僚委員会により1980年に採択された「個人データの自動処理に係る個人の保護に関する条約: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data」を指す。

17 BIOVISION報告書（Albrecht, 2003: 10）も、こうしたプライバシーへの消極的影響について論じている。

18 これが厳密にはバイオメトリクス情報と言えないことについては前掲注 6 参照。

19 Woodward（2001）は、情報プライバシー、自己決定的プライバシー、物理的・身体的プライバシーの 3 つの側面から、プライバシーとバイオメトリクス技術を巡る問題を検討している。

20 もっとも、バイオメトリクス情報が個人情報に該当するのかについては後述のEUの議論に見られるように慎重な検討が必要である。バイオメトリクス情報の個人情報該当性も含め、バイオメトリクス技術への個人情報保護法の適用について論じている論稿として、新保（2006）参照。

21 当ガイドラインについての論稿として、飯田（2006）がある。

22　米国防総省のホームページを参照。＜http://www.dod.mil/nii/biometrics/＞

23　例えば電子タグ等に利用されるRFID（Radio Frequency Identification）技術についても、基本的にEU指令に基づいた対応がなされている。RFID技術とプライバシーについて比較法的考察を行った論稿として詳しくは、松前（2006）参照。

24　プロジェクトの概要については、
＜http://cordis.europa.eu/fetch?ACTION=D&CALLER=PROJ_IST&QM_EP_RCN_A=63054＞参照。

25　指令７条によれば、契約の履行に必要な場合（７条(b)）、データ主体の重要な利益のために必要な場合（７条(d)）等、同意以外の適法理由によって同意なくして処理が適法とされる場合もある。

26　例えばEU作業文書（2003）は、個人情報処理について意図された目的が、他のより侵害度の低い方法によって達成できないかを考慮すべきであるとしている。

27　民間における取組みとしては、日本バイオメトリクス認証協議会や日本自動認識システム協会内のバイオメトリクス部会等を中心に、産業界主導の活動が行われてきており、2002年にISO/IEC JTC1にバイオメトリクスの国際標準を策定する分科会SC37が設立されてからは、SC37国内委員会、ユビキタスネットワーク社会におけるバイオメトリクスセキュリティ研究会、バイオメトリクス・セキュリティ・コンソーシアムが設立されている。プライバシーを含めた法的な問題についても検討が行われ、報告書『バイオメトリクスの法的課題に関する基礎的研究』も公表されている。＜http://www.bsc-japan.com/＞

28　シンポジウム「『人間の尊厳』と身体・生命の倫理的法的位置づけ－先端医療技術の提起する諸問題を中心として－」(1,2)『北大法学論集』55巻２号、54巻６号を参照。

参考文献

Albrecht, Astrid（2003）: *Privacy Best Practices in Deployment of Biometric Systems*.
＜http://www. eubiometricsforum.com/dmdocuments/D7.4%20Best%20Practices1.pdf ＞

Albrecht, Astrid & Walsh, Martin（2003）: *Report on legal and privacy issues*.
＜http://www.biteproject.org/documents/biovision-privacy-issues.pdf＞

バイオメトリクスセキュリティコンソーシアム（2006）:『バイオメトリックセキュリティ・ハンドブック』オーム社.

Cavoukian, Ann（1999）: *Privacy and Biometrics*.
＜http://www.europeanbiometrics.info/images/resources/104_120_file.pdf＞

CE（Council of Europe）Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data（2005）: *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data*.
＜http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/O-Biometrics_en.asp#TopOfPage＞

Cooly, Thomas M.（1988）: *A Treatise on The Law of Torts. 2d ed.*

Davis, Ann（1997）: *The body as password.*＜http://www.wired.com/wired/archive/5.07/biometrics_pr.html＞

de Hert, Paul（2005）: *Biometrics: legal issues and implications*.

EC（European Commission）Article 29 Data Protection *Working Party*（*2003*）*: Working Document on Biometrics*.
＜http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf＞

EGE（European Group on Ethics in Science and New Technologies）（2005）: *Ethical Aspects of ICT Implants in the Human Body*.
＜http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf＞

藤原静雄（2003）:『逐条　個人情報保護法』弘文堂.

長谷部恭男（2001）:『憲法　第２版』新世社.

IBIA（International Biometric Industry Association）(2000): *Privacy Principles*.
＜http://www.ibia.org/aboutibia/privacyprinciples.asp＞
飯田耕一郎（2006）:「金融取引における生体認証に関する法的諸問題（上）（下）」『旬刊金融法務事情』54巻15, 16号.
International Conference of Data Protection & Privacy Commissioners（2005）: *Resolution on the Use of Biometrics in Passports, Identity Cards and Travel Documents*.
＜http://www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf＞
ITU（International Telecommunication Union）（2005）: *The Internet of Things*.
＜http://www.itu/int/publ/S-POL-IR.IT-2005/e＞
情報処理推進機構（2004）:『電子政府行政情報化事業　各国バイオメトリクスセキュリティ動向の調査』
＜http://www.ipa.go.jp/security/fy15/reports/biometrics/documents/biometrics2003.pdf＞
経済産業省（2004）:『経済産業分野のうち信用分野における個人情報保護ガイドライン』
＜http://www.meti.go.jp/feedback/downloadfiles/i41202ij.pdf＞
金融庁（2004）:『金融分野における個人情報保護に関するガイドライン』
＜http://www.fsa.go.jp/singi/singi_kinyu/siryou/kinyu/tokubetu/f-20041207-1/01.pdf＞
松前恵環（2006）:「RFID技術とプライバシーに関する法的考察」『社会情報学研究』11巻１号.
棟居快行（2002）:「情報化社会と個人情報保護」『ジュリスト』1215号.
日本自動認識システム協会（2005）:『よくわかるバイオメトリクスの基礎』オーム社.
OECD（2004）: *Biometric-Based Technologies*. ＜http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00166988.PDF＞
小倉利丸「日本型監視社会に対抗するために」白石孝、小倉利丸、板垣竜太（2003）:『世界のプライバシー権運動と監視社会－住基ネット、IDカード、指紋押捺に対抗するために』明石書店.
Rejman-Greene, Marek（2005）: Privacy Issues in the Application of Biometrics: a European Perspective. James Wayman, et al., *Biometric Systems: Technology, Design and Performance Evaluation*. Springer.
Richards, Neil M.（2006）: Reviewing the digital person: privacy and technology in the information age. By Daniel J. Solove. New York University Press, 2004. 282 pages. *Georgetown Law* Journal, 94.
Rodota, Stefano（2005）: Transformations of the Body. EGE（The European Group on Ethics）, *General Report on the Activities of the European Group on Ethics in Science and New Technologies to the European Commission: 2000-2005*.
佐藤幸治（1970）:「プライヴァシーの権利（その公法的側面）の憲法論的考察(一)」『法学論叢』86巻５号.
佐藤幸治（1990）:『憲法[新版]』青林書院.
瀬戸洋一（2003）:『ユビキタス時代の情報セキュリティ技術』日本工業出版.
新保史生（2006）:「個人情報保護法に基づくバイオメトリクスの利用」『情報メディア研究』４巻１号.
Solove, Daniel J.（2002）: Conceptualizing privacy. *California Law Review*, 90.
US FTC（1998）: *Privacy Online: A Report to Congress*.
＜http://www.ftc.gov/reports/privacy3/priv-23a.pdf＞
Warren, Samuel D. & Brandeis, Louis D.（1890）: The Right to Privacy. *Harvard Law Review*, 4.
Westin, Alan F.（1967）: *Privacy and Freedom*. Bodley Head.
Woodward, John D., Jr.（1997）: Biometric Scanning, Law & Policy: Identifying the Concerns Drafting the Biometric Blueprint. *University of Pittsburgh Law Review*, 59.
Woodward, John D., Jr. (2001): Army Biometric Applications: Identifying and Addressing Sociocultural Concerns. *RAND*.
＜http://www.rand.org/pubs/monograph_reports/2007/MR1237.pdf＞

松前恵環（まつまえ　さとわ）

東京大学大学院学際情報学府修士課程修了
［**専攻領域**］情報法
［**著書・論文**］
『RFID技術とプライバシーに関する法的考察』「社会情報学研究」11巻１号、日本社会情報学会（JSIS）、2006年
［**所属**］東京大学大学院学際情報学府博士課程
［**所属学会**］日本社会情報学会（JSIS）

Biometric Technologies and Privacy Issues

Satowa MATSUMAE

This article discusses privacy issues and legal systems concerning biometric technologies. In part 2, I briefly look at biometric technologies, and the idea of privacy. In part 3, I explore possible concerns posed to privacy. I mainly point out three problems which arise from the use of biometric technologies: the problem of collection of personal data without notice and consent, the problem of processing data without the consent and inconsistent with the purpose specification given at the time of data collection, and the revelation of the sensitive information. Based on this exploration, in part 4, I examine current legal systems about biometric technologies and privacy. In particular, I examine the application of EU Directive to biometric technologies. Finally in part 5, I conclude that some legal measures for the protection of personal data and individual privacy should be taken in our country. Further, I point out the issue that remains to be seen: the importance and necessity of thinking about the idea of 'body' and 'information about body'.

The University of Tokyo, Graduate School of Interdisciplinary Information Studies
Key Words：biometric technologies, privacy, personal information, legal systems, body