平成16年度経済産業省委託事業成果

平成16年度基準認証研究開発委託事業 －2
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

（バイオメトリクス運用の法的解釈の調査分析）

研究委託先：　東京工科大学　専任講師　村上康二郎

平成17年３月

社団法人日本自動認識システム協会

目 次

バイオメトリクス・セキュリティ・コンソーシアム（BSC）リーガルWG

バイオメトリクス運用の法的解釈の調査分析の実施については、バイオメトリクス・セキュリティ・コンソーシアム（BSC）の基盤技術部会にリーガルWGを設置し、そこでの調査・研究成果を活用することとした。平成16年度のリーガルWGの基本的な組織体制は、以下のようになっているが、特に、本報告書の作成に当たっては、新保史生助教授、池野修一氏、藤村明子氏に御協力をいただいた。

	氏　名	所　属
主査	村上　康二郎	東京工科大学メディア学部
コアメンバー	新保　史生	筑波大学大学院図書館情報メディア研究科
コアメンバー	池野　修一	セコムIS研究所
コアメンバー	藤村　明子	NTT情報流通プラットフォーム研究所
メンバー	六川　浩明	弁護士
メンバー	平野　芳行	日本電気
メンバー	鈴木　康史	富士通
メンバー	山田　良子	富士通
メンバー	道坂　修	NTTデータ
メンバー	春山　智	NTTデータ
メンバー	森尻　智昭	東芝ソリューション
メンバー	石橋　雄一郎	東芝
メンバー	渡並　智	セコムIS研究所
メンバー	加藤　宣彰	日立エンジニアリング
メンバー	中嶋　晴久	日本自動認識システム協会

３．１　バイオメトリクス運用の法的解釈の調査分析

３．１．１　背景・目的

これまで、本人認証手段としてはID・パスワードなどが用いられてきたが、これらは成りすまし、偽造などの問題を増加させ、社会的混乱を招いている。そこで、究極の本人認証という観点から、バイオメトリクスが様々な用途に広がっていくことが予想されている。しかし、将来、バイオメトリクス技術が普及・発展し、便利な社会になる一方で、それがプライバシー問題など様々な法的問題を生じさせる可能性があることも否定できないものと考えられる。また、国際化が進み文化の違いが前面に出る社会において、各国の法律やルールの違いから、バイオメトリクスの運用について混乱を生じさせる恐れも存するところである。このように、バイオメトリクスシステムが新しい社会に定着したとき、既成社会では想定されていなかった新しい法的問題が生じることが予測される。

以上のような問題に対応するためには、先進的な海外における議論状況を参考にしながら、バイオメトリクスによって生じる法的諸問題について我が国においても整理、検討をしておく必要がある。

その際、バイオメトリクスが用いられる様々なモデルによって異なる法的問題が生じる可能性があることに配慮する必要がある。現在、パスポートの電子化に伴いバイオメトリクスの実証実験が始まる段階であるが、このようなシステムに潜む法的問題を想定するなど、主要なバイオメトリクス導入モデルを念頭に置いておくことは有益である。

今後、バイオメトリクスの運用に関する国際的なガイドラインの制定を検討していく必要があるものと考えられる。その前提として、バイオメトリクスに関する国内法の整理、検討が必要であると考えられる。これらの内容をＳＣ３７に向けたWDに盛り込むことを目標とする。

３．１．２　バイオメトリクスとプライバシー・個人情報保護

バイオメトリクスについては、それが人間の生体情報を用いるものであるところから、プライバシーないし個人情報の保護に関わる問題を生じさせるものと認識されている。個人情報には様々な種類のものがあるが、その中でも生体識別情報は、特に重要な情報であり、そのため慎重な取扱が要請される。

バイオメトリクスデータが特に重要であると考えられる理由は、それが以下のような特徴を有しているからである[1)]。第一に、取り替えが不能な情報であるということである。ＩＤやパスワードなどは、それが漏洩してしまった場合には変更するということが可能である。しかし、顔や指紋などの生体情報は、漏洩してしまったとしても、容易に変更することはできない。この点は、後に３．２において見るように、はじめから変更可能なように変形したデータを用いる技術（Cancelable Biometrics）なども開発されているが、今の技術によって完全に問題を解決することは困難であると考えられる。第二に、本人認証と関係のない副次的な情報が抽出される恐れがあるということである。例えば、顔画像からは、人種、健康状態、精神状態など本人認証とは関係のない情報が抽出され、利用される恐れがある。第三に、無意識のうちに情報が取得されやすいという側面を有しているということである。特に、顔画像は、本人の気がつかないうちに、遠隔システムによって取得されてしまう恐れがある。

そして、このようなバイオメトリクスデータは、一般的に指摘されているように、プライバシーや個人情報保護に関わる問題を生じさせる。この点については、認証システムごとの検討が必要である。

バイオメトリクスの認証モデルは、バイオメトリクスデータをユーザーが所持するＩＣカードなどのトークンに保管するトークン型（ローカルシステム）と、サーバーにデータベースとして保管する中央データベース型（センターシステム）の二つが存在する。前者のトークン型の場合にもプライバシー問題は発生するが、ここでは、より深刻な問題を発生させる中央データベース型を例に見ていくことにする。

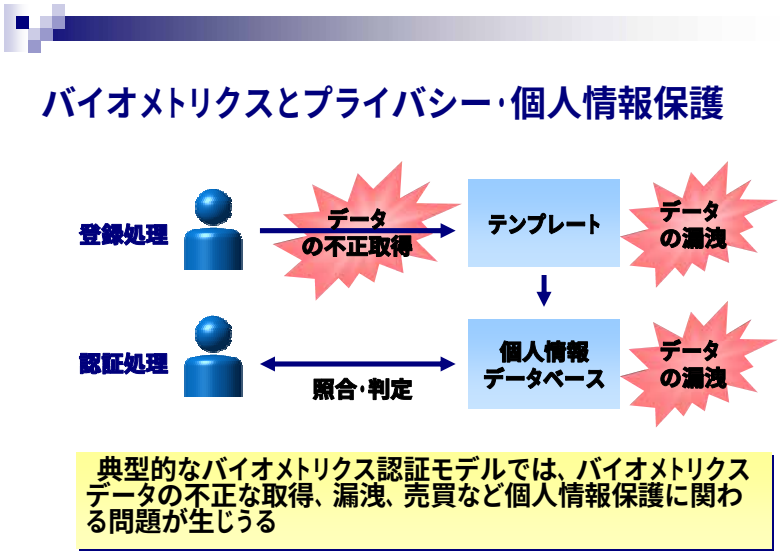

図　３－１　バイオメトリクスとプライバシー・個人情報保護

中央データベース型の場合、まず登録処理が行われる。すなわち、本人から生体情報を取得し、これから特徴抽出を行い、テンプレート化を行う。そして、これを蓄積していくことによってデータベースを作成する。また、認証処理の際には、データベースの情報と本人の生体情報を照合することによって、本人か否かの判定を行うということになる。これらの全ての段階において、プライバシーに対する脅威が存在する。まず、本人から生体情報を取得する時点で、不正な取得がなされる恐れがあり、テンプレートやデータベースの情報が、不正に漏洩したり、売買されたりする恐れがある。また、照合・判定の際にも、データが不正に取得される恐れがある。このようにして、バイオメトリクスにおいては、プライバシー・個人情報保護に関わる問題が生じることになる。

３．１．３　バイオメトリクスの個人情報保護に関する海外の議論状況

（１）諸外国における個人情報保護制度の状況

バイオメトリクスの個人情報保護の問題については、海外における議論の方が先行しているとい

うことができるが、まずは、前提として諸外国における個人情報保護制度を整理しておく必要がある[2)]。

1）ＯＥＣＤガイドライン

個人データ保護に関するガイドラインとしては、国際的に強い影響力を持つものとして、1980年にＯＥＣＤから出された「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」がある[3)]。現在、ほとんどの先進諸国において個人情報保護法制が整備されるようになっているが、いずれも多かれ少なかれ、このＯＥＣＤガイドラインから影響を受けているということができる。ＯＥＣＤガイドラインには、以下の８つの原則が定められている[4)]。

① 収集制限の原則

個人データの収集には制限を設けなければならず、データの収集は、適法かつ公正な手段によって、かつ適当な場合には、データ主体に通知または同意を得て行わなければならない。

② データ内容の原則

個人データは、その利用目的に沿ったものでなければならず、かつ利用目的に必要な範囲内で正確、完全であり、最新の状態に保たなければならない。

③ 目的明確化の原則

収集目的は収集時より遅くない時期において明確化されなければならず、その後における利用は当初の収集目的と矛盾することなく、かつ明確化されたものに制限すべきである。

④ 利用制限の原則

個人データは、目的明確化の原則に従って明確化された目的以外の目的のために、開示され、利用可能な状態に置かれ、またはその他の形での使用に供されてはならない。但し、（a）本人の同意がある場合または（b）法律によって認められる場合はこの限りでない。

⑤ 安全保護の原則

個人データは、紛失または無権限アクセス、破壊、使用、修正もしくは開示その他のリスクに対し、合理的な安全保護措置により保護されなければならない。

⑥ 公開の原則

個人データに係る開発、実施、方針は一般に公開しなければならない。また個人データの存在、種類およびその主要な利用目的とともにデータ管理者のアイデンティティおよび住所を明らかにするための手段が容易に利用できなければならない。

⑦ 個人参加の原則

個人は以下の権利を有する。（a）データ管理者が本人に関するデータを保有しているか否かに

ついて、データの管理者からまたはその他の方法により確認を得ること。（b）本人に関するデータについて、（i）合理的期間内に、（ii）仮に必要とする場合でも過度にならない手数料で、（iii）合理的な方法により、かつ、（iv）本人が容易に理解できる様式で、本人が通報を受けること。（c）上記（a）および（b）の権利に基づく要求が拒否されたときは、その理由がしめされることおよびそのような拒否に対して異議申立ができること。（d）本人に関するデータに対して異議を申立てること、および、その異議が認められた場合には、そのデータを削除、訂正、完全化または補正すること。

⑧　責任の原則

データ管理者は上記諸原則を実施するための措置に従う責任を有する。

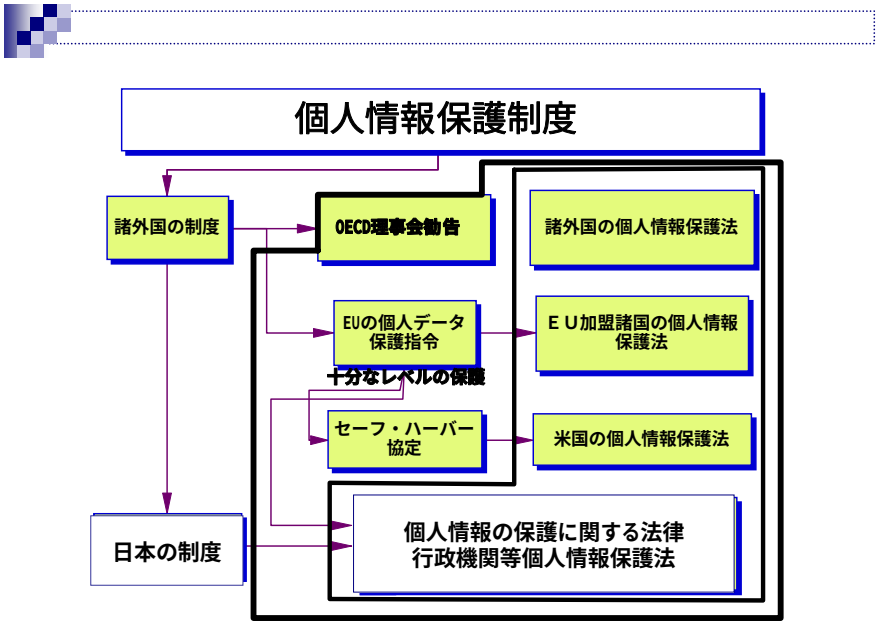

図　3－2　各国個人情報保護制度の相関図

2）EU個人データ保護指令

諸外国の個人情報保護法制は、ＯＥＣＤガイドラインから影響を受けているが、その中でも、ＥＵ諸国は高いレベルで個人データを保護している。ＥＵでは、「個人データの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」（ＥＵデータ保護指令）[5)] が重要な意味を持っている。このＥＵデータ保護指令は、公的部門と民間部門を特に区別しておらず、いわゆるオムニバス方式を採用している。特徴としては、個人データの収集、記録、蓄積、利用、頒布、削除などの処理を行うことについて、原則としてデータ主体の同意を要求していること（7条）、センシティブデータについては、特に厳格な保護を与えており、原則として処理を禁止していること（8条）、管理者は自動処理作業または一連の作業を実施する場合には、事前に監督機関に通知しなければならないとしていること（1

８条）、などをあげることができる。つまり、ＥＵデータ保護指令は、オムニバス方式、事前規制型を採用し、厳格に個人データを保護するものということができる。

また、ＥＵ域外の諸外国にとって問題となるが、ＥＵデータ保護指令２５条である。同条は、次のように規定している。すなわち、「加盟国は、処理過程にある個人データ又は移転後処理することを目的とする個人データの第三国への移転は、この指令の他の規定に従って採択されたその国の規定の遵守を損なうことなく、当該第三国が十分なレベルの保護を確保している場合に限って行うことができるということを規定しなければならない」というものである。つまり、個人情報について十分なレベルの保護を行っていない第三国に対しては、ＥＵ加盟国からは個人データを出してはいけないということである。そのため、ＥＵ域外の多くの国が、十分なレベルの保護に達しているという認定を受けるために、個人情報保護法制を整備せざるを得ないという状況になっている。

３）米国の個人情報保護制度

米国には、公的部門と民間部門の両方を包括的に規制している個人情報保護法は存在しない。公的部門については、１９７４年にプライバシー法が成立しているが、民間部門については、包括法は存在せず、基本的には自主規制に委ねられている。もっとも、民間部門については、特定の分野ごとに個別法が制定されており、いわゆるセクトラル方式が採用されている。代表的なものとしては、金融プライバシー権法（１９７８年）、電子通信プライバシー法（１９８６年）、ビデオ・プライバシー保護法（１９８８年）、児童オンラインプライバシー保護法（１９９８年）などがある。

このように、米国の個人情報保護制度は、ＥＵほど個人情報を厳格に保護しておらず、むしろ、情報の自由な流通や経済の発展を重視している。基本的には、プライバシー権の侵害があった場合に事後的に民事法上の救済を与えればよいという発想があり、緩やかな事後規制型ということができる。

問題となるのは、ＥＵ指令２５条との関係である。米国では民間部門を包括的に規制する法律が存在していないため、指令２５条の十分なレベルの保護に達していないということになり、ＥＵ加盟国からの個人データの移転について障害が生じてしまうことになる。そこで、米国は、ＥＵと協議を行い、セーフハーバー協定を締結するにいたった。これは、一定の要件を満たしている企業、組織については、セーフハーバーという安全な港の中にあるものとしてＥＵ加盟国から個人データの移転を受けられることにしたものである。

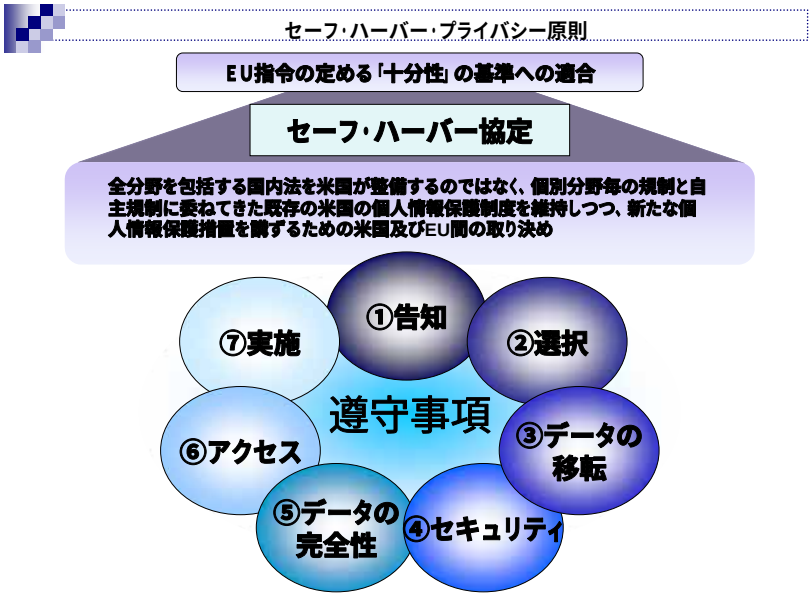

図　3-3　セーフハーバー協定

（2）海外におけるバイオメトリクスのプライバシー・個人情報保護に関する議論状況

現在のところ、バイオメトリクスのプライバシー・個人情報保護の問題に関する検討は、海外の方が進んでいるという状況にある。欧州では、ＥＵデータ保護指令とバイオメトリクスの関係が検討されており、また米国でもバイオメトリクスのプライバシー問題について注目すべき動きが見られる[6)]。そこで、バイオメトリクスに関する法的課題について、先行している海外における議論状況を見ていくことにする。

海外議論状況の概要

国際	北米	欧州	その他
1980: OECDプライバシガイドライン	1997: IPC(カナダオンタリオ州) 社会福祉改正法への関与	1997: TeleTrust/WG6(独)	
1999: IBIAプライバシー原則	2000- IBG: BioPrivacy	1998-2002: BioTrust(独)	
	2001: フロリダ州スーパーボウル 顔認証試行に対する議論	バイオメトリックデータの悪用／御用防止に関する勧告	
	2001: テキサス州法	2002-2003: BIOVISION(EC/FP5)	
	2001-: DoD/BMO (米) 2001-: DHS (米)	Privacy BestPractice	2003- Biometric Institute (豪)
2003- ISO/IEC JTC1 SC37/WG6	2002: ニュージャージー州法	2003/8: EUデータ保護指令のバイオメトリック情報への適用方法に関する提言書	Privacy Code for Biometric Industry
ISO/IEC TR24714(策定中)		英国: 国民IDカード	
2004: OECD WP on Information Security and Privacy Biometric-based Technologies			
2004: ICAOパスポート			

表　3－1　バイオメトリクスのプライバシー・個人情報保護に関する海外議論状況

1）国際的な取り組み

バイオメトリクスのプライバシー・個人情報保護問題に比較的早くから取り組んできたのは、ＩＢＩＡ(International Biometric Industry Association)である。ＩＢＩＡは、ワシントンDCに本拠地を置く業界団体であるが、米国の組織ではなく、国際的な団体である[7)]。

ＩＢＩＡは、１９９８年に設立されたが、１９９９に以下のようなプライバシー指針を公開している[8)]。

① バイオメトリクスデータに関する指針

バイオメトリクスデータは個人情報から分離・区別された電子コードであり、不正アクセスに対するバリアとなる。データの誤用や、本人・司法当局の同意なきデータ公開の防止の確保が必要である。

② 民間部門に関する指針

バイオメトリクスデータの収集、保存、アクセス、使用および目的外利用に対する個人の権利に関する明示的なポリシーの策定が推奨される。

③ 公的部門に関する指針

データ収集、アクセス、保存、利用に関する要件を定める明確な法的基準の規定が必要である。

④ 官民両部門に関する指針

バイオメトリクスデータベースの秘密性および完全性保持のための、適切な運用および技術的管理手法が適用されるべきである。

2）EUにおける議論状況

（a）EUにおいては、前述したようにEUデータ保護指令が重要な意味を持っている。そのため、バイオメトリクスについても、EUデータ保護指令をバイオメトリクスに適用していく際の解釈論という形で議論されることが多い。EUの中では、ドイツにおける取り組みが先行した。１９９７年には、TeleTrust/WG６が設立され、また、１９９８年から２００２年にかけては、BioTrustというプロジェクトが行われた。このプロジェクトは、「バイオメトリックデータの悪用・誤用防止に関する勧告」を出している。これらを受けて、さらにEU諸国を巻き込んで大規模に行われたのが、次のＢＩＯＶＩＳＩＯＮプロジェクトである。

（b）ＢＩＯＶＩＳＩＯＮプロジェクト

EUにおける取り組みにおいて注目されるのは、２００２年から２００３年にかけて行われたＢＩＯＩＳＩＯＮのプロジェクトである。このプロジェクトは、欧州委員会（ＥＣ）が統括する第５期研究開発プロジェクトの一環として行われたものであり、かなり大規模なプロジェクトである。

欧州における取組
BIOVISION

- BIOVISION:
  - 欧州委員会(EC)が統括する第5期研究開発プログラムの一環として、2002　2003に実施されたプロジェクト
  - 複数チームで多方面の課題を検討
  - 「プライバシ／法的課題」に対する検討チーム
    - プライバシベストプラクティスの策定
      - EUデータ保護指令(95/46/EC)のバイオメトリクス情報への適用方法に関する提言書(2003/8採択)策定に活用。
    - 2003年7年設立されたEUバイオメトリクス業界団体EBF内にプライバシー問題検討グループを設立
    - 国際標準化団体への関連WG設立(SC37/WG6)に関与

表　3－2　ＢＩＯＶＩＳＩＯＮプロジェクト

ＢＩＯＶＩＳＩＯＮは、２００３年に“Privacy Best Practice in Deployment of Biometric Systems”[9]（以下「ベストプラクティス」と称する）という報告書を公開している。このベストプラクティスは、注目すべき報告書であるので、以下、詳細に見ていくことにする。

ベストプラクティスは、ＥＵデータ保護指令に従って法的に要求される事項と実務運用上配慮されるべき事項の双方について、両者の区別に配慮しながらまとめている。ベストプラクティスには、その意義や目標について次のように書かれている[10]。

「このバイオメトリクスにおけるプライバシー・ベストプラクティスは、ＥＵデータ保護指令に直接に従ったものである。ＥＵデータ保護指令とは、以下のものをいう。『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』。このレポートは、バイオメトリクスシステム・ユーザーのプライバシーの権利について、バイオメトリクスに対する一般常識への第一歩となるべく意図されたものである。これは、欧州委員会、特にバイオメトリクスに対し活動を始めたばかりの第２９条WGに対し、議論と更なる審議を提供することになるものであるとともに、２００３年のＢＩＯＶＩＳＩＯＮのプロジェクトの終了後初めて報告されたバイオメトリクスに関する評価および提言である」。

ベストプラクティスは、ＥＵデータ保護指令の条文ごとに検討を行っているが、以下では、そのうち重要な部分のみを取り上げる。

① どのような場合にバイオメトリクスデータは「個人データ」となるか

ＥＵデータ保護指令２条は、個人データを特定された、または特定しうる自然人に関する全ての情報と定義している。バイオメトリクスデータが、指令２条に定める個人データにあたるかどうかは、当該バイオメトリクスデータに指令が適用されるかどうかを左右するものであるため、重要な分水嶺となるものである。この点について、ベストプラクティスには、以下のように書かれている[11)]。

「ＥＵデータ保護指令は、自然人に関係しうる全ての情報を包含することができるように、個人データを非常に包括的な意味を有するものとして、定義している。このように、ＥＵデータ保護指令は、写真、声、指紋、遺伝的特徴のようなバイオメトリクスデータをも包含しうるように、開かれたものになっている。あるアプリケーションにおいて、正確にどのようなデータが記録されているのかということに厳重に依拠する場合には、バイオメトリクスデータは、この広範な個人データの定義に当てはまらない場合がありうる」。

つまり、ＥＵデータ保護指令の定義は、包括的になされているため、バイオメトリクスデータも包含される可能性がある。しかし、個別的に厳密に検討していった場合には、特定しうる自然人に関する情報にあたらない場合があるため、データの種類に応じた検討が必要である、ということが示唆されている。続けて、ベストプラクティスは、生データとテンプレートデータの違いについて検討している。

「一般的には、バイオメトリクスデータは、生データおよびテンプレートとして生じうる。生データは、ほとんどの場合、指紋、顔、虹彩など選択された特徴のオリジナルイメージであるが、それに対して、テンプレートは、オリジナルおよび数学的な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。バイオメトリクスのテンプレートからは、技術の状況は、オリジナルはほとんど復元されえないという状況にある」

「しかし、このことは、システムのアーキテクチャーに依存している。例えば、テンプレートが作り出されるために処理される情報量の範囲内において。復元が不可能な場合には、テンプレートは、匿名のデータとしてみなされうる。これは、もはや個人データにあたらないということを意味しないが、データの背後にある個人を特定することが技術的により困難になる。テンプレートが、個人との照合がもはや不可能であり、排除されるような方法によって記録されている場合には、テンプレートは個人データではなくなる。しかしながら、ほとんどの場合には、システムが適切に機能していること、および誤った排除や誤った受け入れがなされる場合を最終的にチェックするために、少なくともデータ管理者にとっては、特定されたものと想定される個人との照合が可能になっている。従って、ほとんどの場合には、取得され、処理され、記録されたデータは、データ保護指令の意味における個人データとして扱われることになるであろう」。

テンプレートからオリジナルを復元することが技術的に困難であるとされている点は、後に

３．２において見るように、必ずしもあてはまらなくなってきている。仮にその点をおいたとしても、少なくともデータ主体から生データを取得し、テンプレート化を行ったデータ管理者は、テンプレートを生データに復元することができるはずであるから、当該管理者にとっては原則として、テンプレートも個人データにあたるということになるであろう。それを超えて、当該管理者以外の者にとってもそれが個人データたり得るのかについては、テンプレートの復元可能性に関する最新の技術的な議論を踏まえながら、慎重な検討をする必要があるものと考えられる。いずれにせよ、バイオメトリクスデータの個人データ該当性は、国際的に見ても、また国内法の解釈論としても重要な点であり、今後、さらに議論していくことが必要である。

さらに、ベストプラクティスは、実務運用上推奨される事項について、以下のように記載している。

「この点に関しては、全てのアプリケーション、全ての場合において真実とはいえないかもしれないが、ベストプラクティスの意味において、我々は、バイオメトリクスデータを常に個人データとして取り扱うことを推奨する。我々はまた、認証手続の要請のために必要となるバイオメトリクスデータのみを保存することを推奨する。ＰＥＴの場合には、これは、特定がアプリケーションの目的のために必要ない場合であっても、認証を用いるということも意味しうる。特定性それ自体が意味するところから離れた記録が、アプリケーションの要請から必要となる場合には、不要な追加的な情報を伴うバイオメトリクスデータは、記録されないようにすることが望ましい。」

② バイオメトリクスデータとセンシティブデータ

ＥＵデータ保護指令の特徴として、センシティブデータを特に厳格に保護しているという点をあげることができる。指令８条１項は、センシティブデータに関する定義を置いており、人種、民族、政治的思想、信教または信条、労働組合への加入事実、および健康および性生活に関するデータの処理と定義している。そして、指令８条２項によれば、センシティブデータは、本人の明示的同意がある場合など一定の例外的な場合を除いて、原則としてその処理が禁止されている。

そこで、バイオメトリクスデータがどのような場合にセンシティブデータに該当するのかが問題となる。この点について、ベストプラクティスには、次のように書かれている[12)]。

「バイオメトリクスを用いることによって、一般的にバイオメトリクスで用いるデータ以外の情報も明らかになってしまうことがある。しかし、これは本人確認目的で用いられる特定のバイオメトリクスの性質によるところが大きい（例えば、自動顔画像認識システムで顔を利用する場合、虹彩認証または掌紋認証を用いる場合よりも、民族や人種に関する情報が明らかになってしまう傾向がある）。また、そのように本人確認目的で使用する情報以外の情報が明らかになる可能性については、生のデータを用いているのか、それともテンプレートが処理されているのかによっても異なる。」

「バイオメトリクスとの関係におけるセンシティブデータとしては、医療（虹彩学、ただし、学問的には必ずしも確立はしていない）、民族または人種、特定の行動に関する情報（例えば、労働組合への加入事実）、または性生活に関する情報などがあげられる。」

③ 処理の安全性

ＥＵデータ保護指令１７条は、偶発的なまたは違法な破壊、偶発的な損失、変更、無権限の開示またはアクセスから個人データを保護するために、管理者が適切な技術的および組織的措置を実施しなければならないと規定している。バイオメトリクスについて、どのような安全措置が要求されるのかについて、ベストプラクティスには、次のように書かれている[13)]。

「ベストプラクティスの意義やプライバシー意識高揚の観点の範疇においては、バイオメトリクスデータのエンコーディング（符号化）は可及的速やかに行われることが望ましい。可能な限り生データではなくテンプレートのみを利用して可及的速やかに生データは無効化処理しなければならない。もし生のイメージファイルがシステム操作に必須である場合は、それらは適切に保護されなければならない。」

基本的な姿勢として、バイオメトリクスデータを符号化、暗号化することが望ましいことはいうまでもないであろう。また、生データを可及的に無効化または破棄すべきであるとしている点についても、基本的には、個人データ保護の観点からは望ましいといえる。しかし、この点については、フォレンジックスの観点からむしろ生データを保存しておく要請もあるものと考えられ、両者のバランスをいかにしてはかるのかが問題になるものと考えられる。さらに、ベストプラクティスは、システム設計についても、処理の安全性の観点から以下のことを推奨している。

「アプリケーションに適している時は常に集中データベースよりも、分散ストレージを使用することが望ましい。なぜならば、集中データベース内の適切な保護手段には、他者の下で厳しいアクセス権に基づく徹底したコントロールや、暗号化される場合における適切な暗号鍵の管理が常に要求されるからである。多くの場合、これを実際に実現することは困難である。なぜならば、その結果、誤用という潜在的なリスクや、機能脆弱性が、データ主体の直コントロール下にあるストレージよりも、さらに容易に発生し得るからである。さらにいうと、ユーザーに対し、本人のバイオメトリクスデータのコントロール権を提供することがより高い透明性の提供を実現可能とするのである。ただし、このことは集中データベース利用を絶対的に回避せよという意味ではなく、プライバシーに関する法制でも一般的に禁止されてはいない。」

ここでは、バイオメトリクスデータを中央のデータベースに集中して蓄積させる集中データベース型よりも、ユーザーが所持しているストレージに保管する分散ストレージ型が望ましいものとされている。確かに、個人データ保護のためには、分散ストレージ型が望ましいものといえるであろうが、両システムにはそれぞれ長所と短所が存在するので、常に集中データベ

ース型でなければならないと強要することは適切ではないものと考えられる。

（c）EUデータ保護指令29条に基づいて設置された作業部会

さらに、EUでは、ＢＩＯＶＩＳＩＯＮのベストプラクティスを受けて、EUデータ保護指令２９条に基づいて設置された作業部会が、２００３年に“Working Document on Biometrics”[14]を公開している。これは、EU指令の作業部会が策定したものであり、ベストプラクティスよりも重要度が高いということができる。この報告書では、概ね以下のようなことが書かれている。

① EUデータ保護指令のバイオメトリクスへの適用

バイオメトリクスデータは、ほとんどの場合、EUデータ保護指令２条の個人データにあたる。

② 目的原則

バイオメトリクスデータがアクセスコントロールのために取得された場合、それを精神状態の評価や仕事場の監視に用いてはならない。

③ 適正な収集

データを取得する際に、目的および管理者に関する情報を与えなければならない。遠隔でバイオメトリクスデータを取得する場合には、特に注意が必要である。

④ 処理の適法性

バイオメトリクスデータを処理する場合、原則として本人の同意が必要である。

⑤ 事前検査

データの処理が、データ主体の権利に特別な危険をもたらす恐れがある場合には、監督機関による事前の検査がなされるべきである。

⑥ セキュリティ対策

データ管理者は、技術的および組織的なセキュリティ対策を講じなければならない。テンプレートの暗号化、暗号鍵の保護、アクセスコントロールなど。

⑦ センシティブデータ

バイオメトリクスデータが、人種、民族、健康状態などのセンシティブデータに当たるものとみなされる場合、特別な保護が必要である。

以上見てきたように、EUにおいては、もともと個人データについてかなり高いレベルでの保護を与えており、センシティブデータに関する規律も明確であるため、それをバイオメトリクス

にそのまま適用すれば、バイオメトリクスデータについても十分な保護を与えることができる。

それに対して、個人データ保護のレベルがＥＵのレベルに達していない国々においては、バイオメトリクスデータについては特別に高いレベルの保護を与えるべきなのかどうかということが問題になるものと考えられる。

3）米国における議論状況

米国では、もともとプライバシー、個人データ保護がＥＵほど厳格ではないこともあり、バイオメトリクスについても、ＥＵにおけるような組織的な動きはない。しかし、個別的には、ガイドラインの策定や、いくつかの州における立法など注目すべき動きが見られるところである。以下ではこれらについて簡単に概要を紹介する。

（ａ）ＩＢＧ（International Biometric Group）

ＩＢＧは、バイオメトリクス・セキュリティに関する米国企業であり、コンサルティングや技術サービスの提供を行っているものである[15]。ＩＢＧは、バイオメトリクスのプライバシーないし個人データ保護の問題に関して、下記のような“BioPrivacy Initiative”と呼ばれるフレームワークを提供している[16]。特に、プライバシー・個人データ保護の観点からは、③の“BioPrivacy Best Practices”が注目されるところである。

① BioPrivacy Impact Framework

運用の潜在リスクを評価するツールである。データの所持者、認証方式、運用の形態に応じてリスク評価を行うことが可能になる。

② BioPrivacy Risk Ratings

各モダリティが有する潜在リスクを評価するツールである。モダリティごとにデータ入力の方法や特性などに応じてリスク評価を行っている。結論的には、指紋、顔、虹彩などがプライバシー侵害のリスクが高いという評価をしている。

③ BioPrivacy Best Practice

プライバシー保護を目的としたBest Practiceである。かなり詳細なものになっており、以下の２５項目が規定されている。

1 範囲の限定
2 普遍的な固有識別子の作成について
3 バイオメトリクス情報の保持の限定
4 潜在的なシステム性能の評価
5 無関係な情報の収集または保存について
6 オリジナルのバイオメトリクスデータの保持について
7 バイオメトリクス情報の保護

8　照合・判定結果の保護
9　システムへのアクセス制限
10　バイオメトリクス情報の分離
11　システムの終了
12　「不登録」の自由
13　バイオメトリクスに関係する情報の収集およびアクセス
14　匿名による登録
15　第三者による責任、監査および監督
16　監査データの完全な公開
17　システムの目的の公開
18　登録の公開
19　マッチングの公開
20　バイオメトリクス情報の利用についての公開
21　選択的・義務的登録の公開
22　システムの管理・監督責任者の公開
23　登録および認証プロセスの公開
24　バイオメトリクス情報保護およびシステム保護の公開
25　消去手続の公開

（b）米国防総省　BMO(Biometrics Management Office)

米国連邦議会の指導により、米国防総省にバイオメトリクス技術を導入する目的で２０００年に設立されたのが、BMOである[17)]。ここでは、バイオメトリクス技術の開発や制度化を先導する役割が期待されている。そして、２００３年9月に行われたバイオメトリックコンソーシアム会議では、「バイオメトリクスプライバシーに関する国防総省ガイダンス」を公開している[18)]。これは、国防総省内におけるプライバシー保護のためのプログラムやフレームワークの提供を目的としており、下記の３つを内容とするものである。

①　プライバシー権の保護に関するガイダンス
②　バイオメトリクス情報の収集権限に関するガイダンス
③　バイオメトリクス情報保護のための国防総省の責任

（c）州法制定の動向

上述したように、米国の連邦レベルの法律については、公的部門についてプライバシー法があるものの、民間部門は個別法によるほかは、基本的に自主規制に委ねられている。もっとも、米国は連邦制をとっており、州の立法権限が強いため、州ごとに特色のある法整備がなされている。とりわけ、注目されるのは、州法の中には、バイオメトリクスに直接言及した法律が存在しているということである。その例として、テキサス州法とニュージャージー州法をあげることができる。

① テキサス州　行政法560章

(CHAPTER 560. BIOMETRIC IDETIFIER) (2001年)[19]

560.001定義

バイオメトリクス識別子としては、眼底パターン、虹彩パターン、指紋、音声、掌形、顔型を対象とする。

560.002バイオメトリクス識別子の公開

個人のバイオメトリクス識別子を保有する政府機関は、本人の同意無しに、バイオメトリクス識別子を売り貸しし、又は第三者に開示してはならない。また、バイオメトリクス識別子が漏洩しないよう相当な注意を払って、保管・伝送しなければならない。

② ニュージャージー州法

バイオメトリクス識別子プライバシー法 (Biometric Identifier Privacy Act)

(2002年)[20]

バイオメトリクス識別子の定義、保護内容はテキサス州法と同様であるが、テキサス州法が政府機関のみを対象としているのに対し、バイオメトリクス識別子を保有する全ての者を対象としている点が異なる。違反者に対しては罰則があり、２万５千ドル以下の罰金が科されることになっている。

このように米国では、民間部門については自主規制に委ねるという伝統があるところから、自主規制を前提としつつ、バイオメトリクスに関するガイドラインを策定するという傾向がみられるところである。もっとも、連邦制をとっているところから、州によっては、バイオメトリクスデータの保護について、法律によって厳格な規律を設けているところも存在しているという状況にある。

３．１．４　バイオメトリクスの個人情報保護に関する国内法の検討

（1）日本の個人情報保護制度の概要

1）バイオメトリクスの個人情報保護問題について検討する前提として、日本の個人情報保護制度の概要を見ていくことにする[21]。

諸外国におけるのと同様に、我が国でも上述した１９８０年のＯＥＣＤイドラインを受けて、個人情報保護法制の必要性が強調されたが、公的部門の扱うデータについては、特に量的ウェイトが高いとのことから、まずは公的部門を対象とする法制度の整備が進められた。その結果、１９８８年に「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律」が制定された。それに対して、民間部門を構成する法律は、制定されず、基本的には自主規制に委ねられたままになった。しかし、その後、主として以下の４つの理由から、民間部門についても、個人情報を保護するための法整備が必要であると認識されるようになった[22]。

① １９８０年ＯＥＣＤガイドラインへの対応

② １９９５年ＥＵデータ保護指令への対応。同指令２５条は、加盟国から第三国への個人データ

の移転は、当該第三国が適切なレベルの保護を提供している場合に限定しているため、日本もこれへの対応が必要になった。

③　情報化社会の進展により個人情報の大量漏洩事件が頻発するようになった。

④　住民基本台帳ネットワークシステムの導入によって、個人情報漏洩の危機が生じる恐れがあることなどの理由から、民間部門についても、個人情報を保護するための法整備が必要であると認識されるようになった。

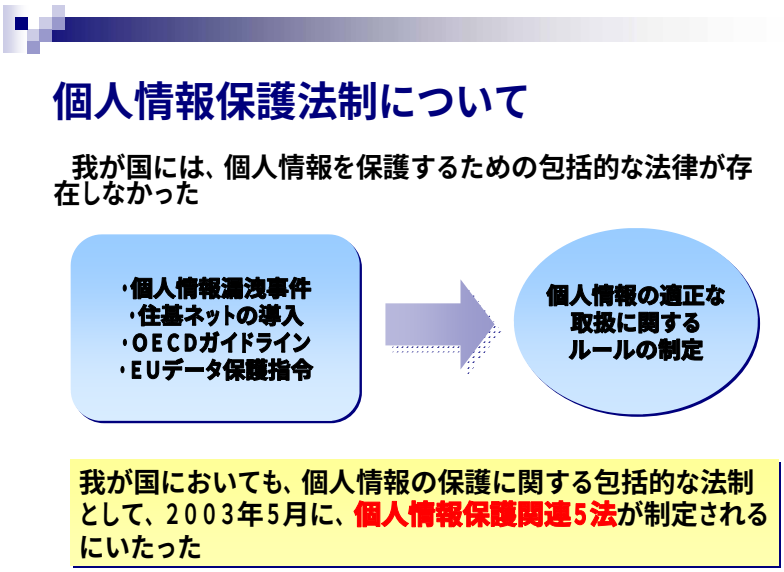

図　3－4　個人情報保護関連５法制定の経緯

2）このような認識を背景として、２００３年５月に、個人情報保護関連５法が制定された。これは以下の５つの法律からなる。

①　「個人情報の保護に関する法律」（個人情報保護法）
②　「行政機関の保有する個人情報の保護に関する法律」（行政機関個人情報保護法）
③　「独立行政法人等の保有する個人情報の保護に関する法律」（独立行政法人等個人情報保護法）
④　「情報公開・個人情報保護審査会設置法」（設置法）
⑤　「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律」（整備法）

これらのうち、①の個人情報保護法は、基本理念などを定めた基本法部分と、民間部門に関する一般法部分とから構成される[23)]。

すなわち、基本法部分では、基本理念、政府による個人情報の保護に関する施策の基本となる事項、国および地方公共団体の責務が定められている。

民間部門に関する一般法部分においては、個人情報取扱事業者の義務が定められている。すなわ

ち、この法律は、個人情報取扱事業者を「個人情報データベース等を事業の用に供している者」（２条３号）と定義し、この個人情報取扱事業者は、その取り扱う情報の種類により、以下のような義務を負うとしている。

・　利用目的の特定（１５条）
・　利用目的による制限（１６条）
・　適正な取得（１７条）
・　取得に際しての利用目的の通知（１８条）
・　データ内容の適切性の確保（１９条）
・　安全管理措置（２０条）
・　従業者の監督（２１条）、委託先の監督（２２条）
・　第三者提供の制限（２３条）
・　保有個人データに関する事項の公表（２４条）
・　開示（２５条）、訂正（２６条）、利用停止（２７条）
・　理由の説明（２８条）
・　開示の求めに応じる手続（２９条）

これらのうち、１５条から１８条は「個人情報」（生存する個人に関する情報で特定の個人を識別することができるもの）について適用される義務であり、１９条から２３条は「個人データ」（個人情報データベースなどを構成する個人情報）にのみ適用される義務であり、２４条から２７条は「保有個人データ」（個人情報取扱事業者が開示、訂正、削除などの権限を有する個人データ）にのみ適用される義務である。

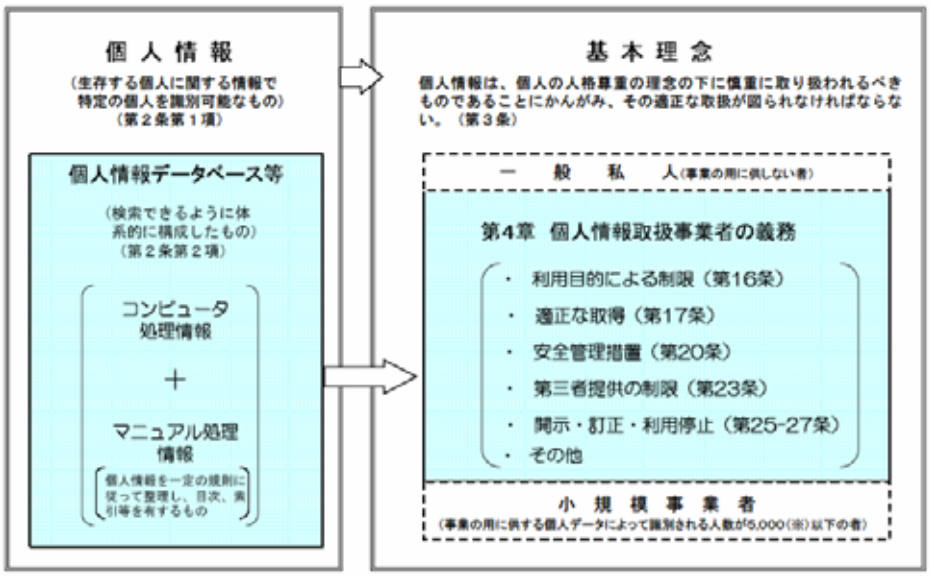

図　３－５　個人情報保護法の対象となる個人情報、事業者の範囲など
（出典：首相官邸・個人情報保護法の解説）

3）欧米と比較した場合の日本の個人情報保護法の特徴

上述したように、ＥＵ諸国では、一般に、公的部門と民間部門の双方を一つの法律で規制する法制がとられている。そして、第三者的な監督機関が置かれ、個人データの処理を行う際には、監督機関に事前に届け出をしなければならないとされることが多い。一般的にいって、ヨーロッパ諸国では個人データの保護について、かなり厳格な規制がなされている。

これに対して、米国では、ＥＵ諸国と大きく異なった法制がとられている。公的部門については、１９７４年にプライバシー法が制定されている。これに対して、民間部門については、包括法は存在せず、基本的に自主規制に委ねられており、特定の分野ごとに個別法が制定されているにすぎない。

以上の欧米諸国の法制と比較した場合、日本の個人情報保護法制は、以下のような特徴がある。

① 公的部門と民間部門を別々の法律で規律し、規制の内容に差異を設けている。

② 公的部門については、行政機関は、個人情報ファイルの保有を事前に総務省に通知しなければならないとされており事前規制の側面があるが、民間部門については、基本的に事業者の自主的な取り組みを尊重し、事後的に主務大臣が関与するという事後規制がとられている。

つまり、個人情報取扱事業者は、種々の義務を負うが、欧州諸国のような事前の届け出、通知は要求されず、事業者の自主的な取り組みを尊重しつつ、主務大臣が事後的に報告徴収、助言、勧告、命令を行うことよって規制するという枠組みがとられている。

このように、日本の個人情報保護法は、民間部門も包括的に法律で規制している点は、欧州型に近いが、事業者の自主性を尊重しつつ、事後的にゆるやかな規制を行っている点では、米国型に近いところがあるといえる[24)]。

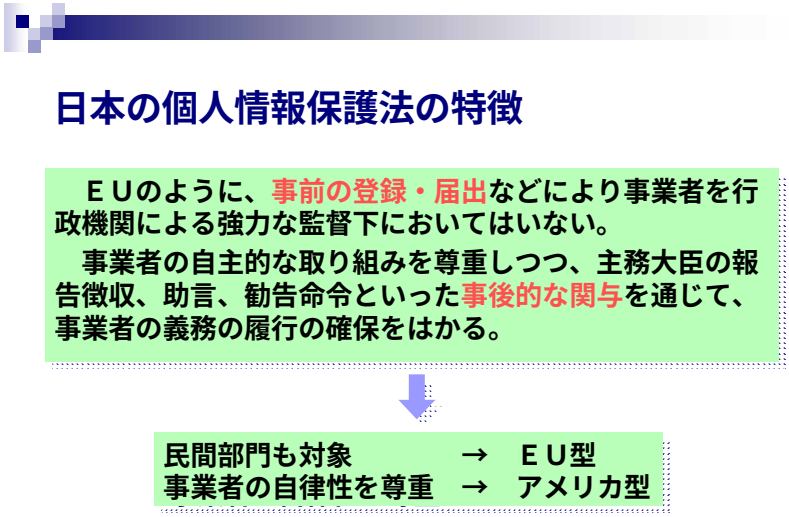

図 3－6 日本の個人情報保護法の特徴

（2）バイオメトリクスの個人情報保護問題に関する国内法の検討

ＥＵにおいて、ＥＵデータ保護指令におけるバイオメトリクスの取り扱いが検討されているように、我が国においても個人情報保護法制をバイオメトリクスに適用していく際の解釈論を行っていくことによって、法律上のバイオメトリクスの取り扱いを明確化していくことが重要である[25]。以下では、中心的に問題になると考えられる個人情報保護法との関係を見ていくことにする。バイオメトリック認証システムが一定規模以上の民間事業者、正確には個人情報保護法２条３項にいう個人情報取扱事業者によって運用される場合は、個人情報保護法が関係してくることになる。

1）バイオメトリクスデータの個人情報該当性

対象となるバイオメトリクスデータに個人情報保護法が適用されるためには、当該バイオメトリクスデータが、個人情報保護法2条1項の個人情報に該当することが必要である。そこで、バイオメトリクスデータがいかなる場合に個人情報にあたるのかが問題となる。

２条１項は、個人情報を「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、その他の記述により特定個人を識別できるもの（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）」と定義している。

バイオメトリクスデータの個人情報該当性については、ＥＵにおいても必ずしも十分な検討がなされていない。先に紹介したＥＵ指令２９条作業部会の“Working Document on Biometrics”においても、ほとんど場合に、個人データに該当するというような抽象的な記述しかなされていない。

確かに、バイオメトリクスデータは、本人認証のために用いられるものであるため、多くの場合には特定個人を識別することができるものとして、個人情報に該当することになる場合が多いであろう。しかし、厳密には、認証モデルの相違や生体情報の種別に応じて、慎重に検討する必要があるものと考えられる。例えば、中央データベース型かトークン型か、１対１認証か１対N認証か、また顔画像か、それともそれ以外の指紋、虹彩、静脈などの情報か、生データかそれともテンプレートデータかによって異なってこないか、今後の検討が必要とされるところである。また、バイオメトリクスデータが暗号化されている場合にも問題が生じるが、これは暗号化されたデータの個人情報該当性の問題であり[26]、この点をどう解するかによって結論が左右されることになるものと考えられる。

2）バイオメトリクスデータの取得

ＥＵデータ保護指令７条は、個人データの取得などの処理をするには原則として本人の同意が必要だとしている。これに対して、我が国の個人情報保護法１７条は、「偽りその他不正な手段により個人情報を取得してはならない」としているだけで、必ずしも明確には本人同意を要求していない。

この点については、実務運用上は、バイオメトリクスデータの重要性からいって、原則として本人の同意を得るようにすることを推奨するということも考えられるところである。

3）利用目的の明示について

個人情報保護法１８条は、利用目的の明示について、直接書面取得の場合と間接取得の場合とで

異なった規律を定めている。すなわち、本人から直接書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られている記録を含む）に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し利用目的を明示しなければならないが（２項）、それ以外の場合は、事後的な通知または公表でよいとしている（１項）。

バイオメトリクスデータを取得する場合に、どのような場合が２項の直接書面取得になり、どのような場合が１項の間接取得になるのかが問題となる。例えば、本人から顔画像を撮影して取得する場合、書面が電子的、磁気的記録を含むとしても、なんらかのものに「記載」（記録）されたものを本人から取得したとは厳密には言えないものと考えられる。従って、このような場合は１項の間接取得になり、事後的な通知または公表で足りるということになる。これに対して、本人から顔画像を記録した何らかの記録媒体を受け取る場合には、直接書面取得にあたるものと考えられるので、あらかじめ利用目的を明示することが必要になるであろう。

４）センシティブデータの取扱について

ＥＵとの比較法的観点から問題となるのは、センシティブデータの取り扱いである。前述したように、ＥＵデータ保護指令８条１項は、「加盟国は、人種又は民族、政治的意見、宗教又は思想信条、労働組合への加入を明らかにする個人データの処理、及び健康又は性生活に関するデータの処理を禁止しなければならない」として、センシティブデータの処理を原則として禁止している。

バイオメトリクスデータの場合、例えば、顔画像からは、人種、民族、健康状態などのセンシティブデータが抽出される恐れがある。また、静脈、掌形、虹彩などからもその人の健康状態を明らかにすることができるという指摘もなされてところである。

このような場合、ＥＵ指令ではセンシティブデータの取扱について規定があるためその規律が明確であるが、我が国の個人情報保護法では、センシティブデータに関する規定が存在しないため問題になる。もともと、我が国においてセンシティブデータの規定が設けられなかった理由は以下のところにある[27)]。

> 「本法では多種多様な個人情報の性質、取扱主体、利用方法等を区別せずにその取扱いを規律している一方、センシティブであるかどうかの程度はこれらの要素によって大きく左右されることから、本法にはセンシティブ情報に関する規定は設けられていない。しかし、個人情報の範囲が一定の範囲に限定される個別の法制度においては、こうした個人情報の取扱いについてきめ細かく措置することも可能と考えられる。」

すなわち、民間部門における個人情報の取り扱いの規制に関する一般法である個人情報保護法においては、センシティブデータに関する規定を置かないが、これはおよそセンシティブデータについて特別の保護を与えることを否定する趣旨ではなく、むしろ特定の分野ごとに制定される個別法において、センシティブデータに関する規定を設けることを予定しているということができる。

もっとも、現在のところ、特定の分野ごとにおける個別法の整備は必ずしも進んでおらず、各省庁から出される個人情報保護法に関するガイドラインにおいて、センシティブデータの取り扱いが定められるようになっている。例えば、金融庁から２００４年１２月６日に出された「金融分野に

おける個人情報保護に関するガイドライン」[28] の６条は、次のように定めている。この中で、バイオメトリクスとの関係で重要になるのは、１項８号である。

第６条　機微（センシティブ）情報について

１　金融分野における個人情報取扱事業者は、政治的意見、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下「機微（センシティブ）情報」という。）については、次に掲げる場合を除くほか、取得、利用又は第三者提供を行わないこととする。

①　法令等に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合

③　公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合

④　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合

⑤　源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等の機微（センシティブ）情報を取得、利用又は第三者提供する場合

⑥　相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微（センシティブ）情報を取得、利用又は第三者提供する場合

⑦　保険業その他金融分野の事業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合

⑧　機微（センシティブ）情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合

２　金融分野における個人情報取扱事業者は、機微（センシティブ）情報を、前項各号に定める事由により取得、利用又は第三者提供する場合には、各号の事由を逸脱した取得、利用又は第三者提供を行うことのないよう、特に慎重に取扱うこととする。

また、上記と同じ内容の規定は、経済産業省から出されている「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案」[29]の中にも見られるところである。

さらに、金融庁は、２００５年１月６日に、上記の「金融分野における個人情報保護に関するガイドライン」における安全管理措置の実効性を担保するものとして、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」[30]を出している。この実務指針は、７－１以下において、機微（センシティブ）情報の安全管理措置について定めているが、特に機微（センシティブ）情報に該当する生体認証情報（機械による自動認証に用いられる身体的特徴のうち、非公知の情報。以下同じ）の取り扱いについては、以下の措置を定めている。

７－１－１－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、取得、入力段階における取扱規程において、７－１－１に規定する事項に加えて、次に掲げる事項を含まなければならない。

① なりすましによる登録の防止策
② 本人確認に必要な最小限の生体認証情報のみの取得
③ 生体認証情報の取得後、基となった生体情報の速やかな消去

７－１－２－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、利用段階における取扱規程において、７－１－２に規定する事項に加えて、次に掲げる事項を含まなければならない。
① 偽造された生体認証情報による不正認証の防止措置
② 登録された生体認証情報の不正利用の防止措置
③ 残存する生体認証情報の消去
④ 認証精度設定等の適切性の確認

７－１－３－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、保存段階における取扱規程において、７－１－３に規定する事項に加えて、保存時における生体認証情報の暗号化を含まなければならないほか、サーバー等における氏名等の個人情報との分別管理を含むこととする。

７－１－５－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、消去段階における取扱規程において、７－１－５に規定する事項に加えて、生体認証情報を本人確認に用いる必要性がなくなった場合は、速やかに保有する生体認証情報を消去することを含まなければならない。

７－２　金融分野における個人情報取扱事業者は、２－５－２に規定する監査の実施に当たっては、機微（センシティブ）情報に該当する生体認証情報の取り扱いに関し、外部監査を行うとともに、必要に応じて、その他の機微（センシティブ）情報の取り扱いについても外部監査を行うこととする。

この金融庁の安全管理措置に関する実務指針については、機微（センシティブ）情報に該当する生体認証情報に対して特別な配慮を要求するものであり、基本的な方向性としては妥当なものであるということができるであろう。今後は、これらの要請を具体化していく技術、制度を検討していく必要があるものと考えられる。

このように、我が国においても各省庁ガイドラインの中において、センシティブ情報に関する規定が定められており、バイオメトリクスに関しても言及がなされている。もっとも、ガイドラインによる対応だけで十分なのかどうかは検討を要するところであり、今後、個別法の整備についても検討を行っていく必要があるものと考えられる。

３．１．５　バイオメトリクスの国際的な運用ガイドラインに関する検討

将来的には、バイオメトリクスデータが、国境を越えて国際的に流通することになるものと予測されるため、各国ごとの対応だけでは不十分であり、バイオメトリクスに関する国際的なプライバシー・ガイドラインが必要になるものと考えられる。実際に、ＩＳＯ/ＩＥＣ　ＪＴＣ１ ＳＣ３７ＷＧ６では、ＴＲ２４７１４の中で、このようなガイドラインについて検討を行っている。以下では、国際的なプライバシー・ガイドラインの制定に向けた議論状況を紹介し、さらに今後の課題について検討する。

（1）ＳＣ３７WG６における議論状況

ＩＳＯ/ＩＥＣ ＪＴＣ１ ＳＣ３７WG６は、Cross-Jurisdictional and Societal Aspects（相互裁判権および社会的事象）というタイトルが示すように、バイオメトリクスに関する技術以外の諸問題、すなわち法的課題、社会的課題などを広く検討の対象とするものである。ＳＣ３７WG６では、ＩＳＯ/ＩＥＣ ＴＲ２４７１４の作成を当面の目標としている。そのタイトルは、Multi-part Technical Report on Cross Jurisdictional and Societal Aspects of Implementations of Biometric Technologiesである。

国際的な取組
ISO/IEC JTC1 SC37WG6

- ISO/IEC TR24714
  (Multi-part Technical Report on Cross Jurisdictional and Societal Aspects of Implementations of Biometric Technologies)
  - **運用者/エンドユーザがバイオメトリクス認証システムを適切に設計運用するための、プライバシー、法的側面、アクセシビリティ、安全性などに関するガイドライン**
  - **欧州Biovisionプロジェクトでの検討中心者が実質リーダ**
  - **プライバシーに関しては、Biovision検討結果が色濃く反映されたドラフトを審議中**

表　２－１　ISO/IEC JTC1 SC37/WG6における議論状況

ＴＲ２４７１４の１stWDの目次は以下のようになっている。

- Part1: High Level Framework
  - Privacy

- Accessibility
- Health and Safety
- Best Practice in Use
- Jurisdictional
- Societal, Cultural and Ethical Aspects of Biometrics

- **Part2: Specific Issues in contexts of applications and technologies**
  - Considerations for Specific Biometric Techniques
  - Summary of recommendations
- **Appendix**
  - Relationships between stakeholders in the deployment of biometric systems
  - Case Studies in respect of personal data protection
  - Information to the individual using biometrics
  - Factors influencing the usability of biometrics

この中でも、特にPart 1のPrivacyの部分に重点が置かれており、２００４年４月に行われたRapporteur Group Meeting、２００４年６月に行われたソウル会議においても、最も多くの時間を割いて議論がなされたところである。1stWDにおいて提案されたプライバシー・ガイドラインの内容は、概ね以下のようなものである。

【Privacy章に記載されている１２のプライバシー原則】（初版）

１　バイオメトリックデータの使用について、公開制を定めた一般的なポリシーが存在しなければならない。そのポリシーは、そのデータが使用される目的、およびそのデータの使用に関する責任者の連絡先を含むべきである。

２　バイオメトリックデータは、当該地域の法律および行為規範に従って取得されるべきである。監視作業の場合を除いて、バイオメトリックデータは、データ主体への通知および同意を伴って、取得されるべきである。

３　バイオメトリックデータの取得および処理は、定められた目的を達成するのに必要な最小限の範囲に制限されるべきである。いくつかのバイオメトリクスのアプリケーションは、個人が特定されることを必要としない。

４　バイオメトリックデータは、特定された目的にとって必要な期間のみ保持されるべきである。

５　実現可能でありかつ実際的である場合には、オプト・インおよびオプト・アウトの手続をデータ主体が利用しうるようにしなければならない。これらは、バイオメトリクスの使用に代わる代替手段の提供を含みうる。

６　バイオメトリックデータは、本質的に変化しやすいものであるので、必要とされる正確性のレベルまでデータを維持するように配慮されなければならない。

７　たとえ、当該組織が事業を行っている法域において法律上要求されていなくても、ベストプラクティスとして、異なる法域（国）間におけるバイオメトリックデータの移転は、欧州委員会２９条データ保護作業部会によって提示される個人データの移転のためのモデル契約に従うべきである。

８　バイオメトリックデータは、無権限による利用または不法な処理に対して、適切な技術的および組織的手段によって保護されるべきである。

９　データ主体には、バイオメトリックデータの正確性を確認するために、合理的なアクセスが与えられるべきである。不正確なデータは、訂正されるべきである。

１０　バイオメトリックシステムは、データ移転の安全性監査を許容するように設計されるべきである。

１１　バイオメトリックシステムが、個人について重要かつ完全に自動的な判断を行うために利用される場合には、当該個人が機械ではなく人に対して判断を求められるようにすべきである。個人に対して、そのような自動的な判断についての通知がなされるべきである。

１２　当該組織内の者が、これらの原則の履行について責任を負うべきである。

その後、1stWDに対しては、２００４年９月に各国からのコメント、寄書が提出されたが、１２のプライバシー・ガイドラインに対しても、多くのコメントが寄せられた。これらを受けて、２００４年１１月に行われたパリ会合においてプライバシー・ガイドラインの修正が行われた。

修正後のガイドラインの概要は、以下のようなものである。

【Privacy章に記載されている１２のプライバシー原則】（修正版）

１　バイオメトリックデータの使用について、公開制を定めた一般的なポリシーが存在するべきである。そのポリシーは、そのデータが使用される目的、およびそのデータの使用に関する責任者の連絡先を含むべきである。

２　バイオメトリックデータは、データ主体への通知および同意を伴って、取得されるべきである。ただし、当該地域の法律が例外を定めている場合はこの限りではない。

３　実現可能でありかつ実際的である場合には、オプト・インおよびオプト・アウトの手続をデータ主体が利用しうるようにしなければならない。

４　バイオメトリックデータの取得および処理は、定められた目的を達成するのに必要な最小限の範囲に制限されるべきである。バイオメトリクス・アプリケーションの目的は、バイオメトリクスシステムが実行される前に、特定され、そして文章化され、個人が取得しうるようにするべきである。

５　バイオメトリックデータは、特定された目的にとって必要な期間のみ保持されるべきである。

６　運用者は、当該システムが正確に機能し、データ主体に不要な負担を生じさせないようにするために、バイオメトリクス・アプリケーションの正確な機能と安定性を保持しなければならない。

７　データ主体には、バイオメトリックデータの正確性を確認するために、合理的なアクセスが与えられるべきである。不正確なデータは、訂正されるべきである。

８　バイオメトリックデータは、無権限による利用または不法な処理に対して、適切な技術的および組織的手段によって保護されるべきである。

９　バイオメトリックシステムは、安全な監査を許容するように設計されるべきである。

１０　たとえ、当該組織が事業を行っている法域において法律上要求されていなくても、ベスト・プラクティスとして、異なる法域（国）間におけるバイオメトリックデータの移転は、欧州委員会２９条データ保護作業部会によって提示される個人データの移転のためのモデル契約に従うべきである。

１１　バイオメトリックシステムが、個人について重要かつ完全に自動的な判断を行うために利用される場合には、当該個人が機械ではない人による介入を要求する仕組みが提供されるべきである。

１２　当該組織内の者が、これらの原則の履行について責任を負うべきである。

修正後も基本的な内容は変わっておらず、各原則の順序の変更や、細かな表現の変更などが中心になっている。

いずれにせよ、このプライバシー・ガイドラインは、基本的にはＯＥＣＤの８原則をバイオメトリクスに当てはめていくことによって、具体化を図ったものということができ、その基本的な方向性は妥当なものであるといって良いであろう。

これらのガイドラインのうち、ＯＥＣＤ８原則から出てこないものとして、１０と１１をあげる

ことができる。１１については、プライバシーに関する問題なのかどうかにつき疑義がないわけではない。しかし、バイオメトリクスの場合、完全に自動的なシステムによって重要な判定がなされる場合には、誤った判定によって事後的に回復困難な損害が発生する恐れがあるため、そのような重要な判断を自動的に行う場合には、機械によらない人による判断を受けられる機会を保障するということは重要であると考えられる。

これに対して、１０については疑問がないわけではない。ＥＵ指令２９条の作業部会が定めているモデル契約は、本来、ＥＵデータ保護指令２５条との関係で、ＥＵ加盟諸国から、十分なレベルの保護に達していない国に対して、個人データを移転する場合に必要とされるものである。このようなＥＵ主導で作成された条項を、世界的に国境をまたいでバイオメトリクスデータが移転される場合に適用することが適切なのかどうかは、なお慎重な検討が必要であると考えられる。

（2）国際標準化活動に対する日本からの貢献

ＳＣ３７ＷＧ６において、国際的なプライバシー・ガイドラインの策定を議論していく際には、まず各国の個人情報保護法制の相違を十分に把握しておく必要がある。前述したように、EU諸国と米国では、個人情報保護法制が大きく異なってあり、さらに日本の個人情報保護法制は、両者のいずれとも異なったものとなっている。国際的なガイドラインの策定は、通常、欧米が主導になって行われることが多いが、アジアの存在も重要である。特に、日本では、ごく最近の２００３年5月に個人情報保護関連5法が制定されたため、その内容については、まだ海外ではほとんど知られていないというのが実情である。従って、日本の個人情報保護法制に関する近時の動向をＳＣ３７ＷＧ６の国際委員会に紹介することは、きわめて重要な作業であるといえる。そこで、日本からの寄書として、日本の個人情報保護法と関連動向に関する以下の文書を作成し、提出した（以下は個人情報保護法制の部分のみを抜粋したものである。）

PERSONAL INFORMATION PROTECTION ACT AND RELATED TRENDS IN JAPAN

SC37WG6 Japan Domestic Subcommittee

1. PERSONAL INFORMATION PROTECTION ACT IN JAPAN

1.1. History of Establishment of Related Acts and Schedule of Enforcement of Personal Information Protection Act

(1) The OECD adopted the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" as international guidelines relating to the protection of personal information in 1980. In Japan as well, upon influence of these guidelines, the need for regulations for protection of personal information became stressed. Due however to the particularly high weight of the volume of the data handled by the public sector, efforts focused on the establishment of a legal system directed at the public sector. As a result, in 1988, the "Act for Protection of Computer Processed Personal Information Held by Administrative Organs" was established. As opposed to this, no legal system regulating the private sector was established. Basically, the

private sector was allowed to continue to regulate itself.

Subsequently, however, due mainly to the following four reasons, the need for establishment of Acts for the protection of personal information in the private sector as well became recognized:

- Efforts to deal with the 1980 OECD guidelines
- The need for dealing with the 1995 EU Personal Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data". That is, Article 25 of that Directive limits the transfer of personal data from member states to third countries to cases where those third countries offer an adequate level of protection. Japan consequently also had to deal with this.
- The increased frequency of incidents of massive leakage of personal information due to the growth of the information society
- The danger of the leakage of personal information due to the introduction of the new "basic residential registers network system". Due to these and other reasons, the need for establishment of laws for the protection of personal information in the private sector as well became recognized.

(2) With this recognized, in May 2003, five Acts relating to the protection of personal information were established. There were the following five Acts:

[1] "Act for the Protection of Personal Information" (Personal Information Protection Act)
[2] "Act for the Protection of Personal Information Held by Administrative Organs" (Administrative Organ Personal Information Protection Act)
[3] "Act for the Protection of Personal Information Held by Independent Administrative Institutions" (Independent Administrative Institution Personal Information Protection Act)
[4] "Act Establishing Information Disclosure and Personal Information Protection Council" (Establishment Act)
[5] "Act Relating to the Improvement of Related Acts along with Enforcement of Act for the Protection of Personal Information Held by Administrative Organs" (Improvement Law)

Among these, the [1] Personal Information Protection Act is comprised of a basic law section setting down the basic principle and general law section relating to the private sector.

That is, in the basic law section, basic principle, matters forming the basis of measures relating to the protection of personal information by the government, and the duties of the central and local governments are set down.

In the general law section relating to the private sector, the duties of entities handling personal information are set down. That is, this law defines entities handling personal

information as "party providing personal information databases etc. for business use" (Article 2, Paragraph 3) and requires that these entities handling personal information assume the following obligations according to the type of information handled:

- Purpose specification (Article 15)
- Use limitation by specified purpose (Article 16)
- Proper Collection (Article 17)
- Purpose notice at the time of collection (Article 18)
- Security control measures (Article 20)
- Supervision to employees (Article 21) and supervision to contractors (Article 22)
- Limitation of offering third parties (Article 23)
- Disclosure of items of possession personal data (Article 24)
- Disclosure (Article 25), correction (Article 26), and suspension of use (Article 27)
- Explanation of reasons (Article 28)
- Procedures for responding to requests for disclosure (Article 29)

(3) The schedule for enforcement of the five Acts relating to the protection of personal information is as follows.

The basic law section of the Personal Information Protection Act is being immediately enforced, but the parts corresponding to the general law relating to the private sector will be enforced from the date specified by Cabinet Order within a range not more than two years from the date of promulgation (date specified: April 1, 2005). Normally, the dates of enforcement of a single legal code do not differ by section, but in this law, there is the interesting feature of the division of enforcement dates, that is, the immediate enforcement for the basic law section setting down the basic principle etc. and after two years for the general law section relating to the private sector setting down duties of entities handling personal information.

The other related laws are also supposed to be enforced from April 1, 2005.

1.2. Comparison of Japanese Laws and Western Laws

(1) At the present time, almost all industrialized countries are establishing laws for protection of personal information, but the legal systems differ greatly by country reflecting the differences in history, culture, national systems, etc.

In the European countries, generally legal systems regulating both the public sector and private sector by single law are being adopted. Further, in most cases third party like supervisory authority is being established and advance notification to the supervisory authority is being mandated for processing of personal information. Generally speaking, the European countries can be said to be establishing considerably tough regulations regarding the protection of personal information.

As opposed to this, in the U.S., a legal system very different from that of the European countries

is being adopted. Privacy Act was established for the public sector in 1974. As opposed to this, there is no comprehensive Act for the private sector. The private sector is basically allowed to regulate itself. Individual Acts are merely being established for specific sectors.

(2) Compared with the legal systems of the Western countries, the Japanese legal system for the protection of personal information has the following interesting features:

- Regulation of the public sector and private sector by different Acts and provision differences in content of regulations.
- For the public sector, requirement that administrative organs notify the Ministry of Public Management, Home Affairs, Posts and Telecommunications in advance of holdings of personal information files and therefore an aspect of "Regulation before the Fact", while for the private sector, basic respect for voluntary approaches by entities handling personal information and only later involvement of the competent minister, that is, "Regulation after the Fact".

  That is, entities handling personal information have various obligations, but are not required to make advance reports or notification like in the European countries. The framework is adopted of regulation by the competent minister after the fact by collection of reports and issuance of advice, recommendations, and orders while respecting the voluntary approaches by entities.

In this way, Japan's Personal Information Protection Act is close to the European model in terms of also regulating the private sector comprehensively by Acts, but can be said to have facets close to the American model in terms of respecting the autonomy of entities handling personal information and establishing moderate regulation after the fact (see Personal Information Protection Basic Legal System Study Group, *Q&A Personal Information Protection Law*, p. 11 (in Japanese)).

1.3. Acquisition of Biometrics in Personal Information Protection Act

While five Acts relating to the protection of personal information were established in Japan last year, these Acts do not include any provisions explicitly alluding to biometrics.

Whether biometrics corresponds to personal information under the Personal Information Protection Act will in the end have to be debated in terms of interpretation of the Act, but up to now there has been almost no debate regarding this point.

Article 2, Paragraph 1 of the Personal Information Protection Act defines personal information as "information relating to living individuals enabling identification of specific individuals by names, dates of birth, and other descriptions included in that information (including information which can be easily referenced with other information and thereby enable

identification of specific individuals)". The Administrative Organ Personal Information Protection Act and the Independent Administrative Institution Personal Information Protection Act also define it almost the same.

（3）国際的なプライバシー・ガイドラインの検討

バイオメトリクスに関する国際的なプライバシー・ガイドラインを策定していく際には、まず、各国において、国民のプライバシー意識が異なっているということ、そのため、各国の個人情報保護法制に大きな差異が存在するということを十分に認識する必要がある。このように各国の個人情報保護法制が異なっている状況下において、バイオメトリクスに関するプライバシー保護のレベルをどの程度のところに設定するのかということは、微妙な調整を要する困難な課題であると考えられる。現在のところ、ＥＵ諸国が議論を主導し、ガイドラインの内容もややＥＵ寄りのものになっているところがあるが、国際的なガイドラインとして制定するものである以上、過度にＥＵ寄りのものにならないようにする必要があるであろう。

プライバシー保護に関する国際的なガイドラインとしては、前述したＯＥＣＤの８原則が存在する。もっとも、この８原則は、極めて抽象的な内容のものとなっているため、それをバイオメトリクスに対して適用していくにしても、相当な幅が生じうるところである。そこで、バイオメトリクスにおいて、ＯＥＣＤ８原則をどのように具体化していくのかということが問題になりうる。

バイオメトリクスデータについては、変更不可能な生体情報を用いるものであるところから、特に厳格な保護が必要であるという指摘がなされることがある。しかし、他方で、前述したようにＥＵは、個人データのうちセンシティブデータにあたるものだけを特に厳格に保護するという態度をとってきている。そのため、基本的な問題として、バイオメトリクスデータ一般が高いレベルの保護を必要とするものなのか、それとも、バイオメトリクスデータのうち、センシティブデータにあたるものだけが特に高いレベルの保護を必要とするものなのか、ということが問題になってくることになる。

ＥＵデータ保護指令を基準とするＢＩＯＶＩＳＩＯＮのベストプラクティスやＥＵ指令２９条作業部会のWorking Documentなどは、後者の方向性をとるものであるが、これではセンシティブデータに特別な保護を与えていない国々との関係が問題になる可能性がある。また、仮に前者のように、バイオメトリクスデータ一般について、高いレベルの保護を与えるとしても、次にそれをどの程度のレベルの保護にするのかということが問題となる。

今のところ、ＳＣ３７WG６における議論は、このような基本的な課題に関する認識に欠けているところがあるように思われるが、今後、このような基本的な課題を十分に認識し、慎重に検討を進めていく必要があるものと考えられる。

３．１．６　今後の日本からの国際貢献について

現在のところ、ＳＣ３７WG６では、バイオメトリクスに関するプライバシー・個人情報保護の問題が中心的に検討されており、それ以外の法的課題については、ほとんど検討がなされていない状況にある。しかし、バイオメトリクスはプライバシー・個人情報の問題以外にも様々な法的問題を生じさせるものと考えられる。例えば、偽造指紋・偽造虹彩を用いたなりすましに対する法的規制の問題、

本人拒否・他人受入によってユーザーに損害が発生した場合の法的責任の問題、電子署名法を含めた本人認証基盤に関する法整備の問題、障害者差別禁止法などの障害者のアクセシビリティに関する法的課題などである。これらの法的課題について、日本における議論状況などをＳＣ３７WG６に紹介するということが、今後の国際貢献活動の一つとして考えられるところである。

３．１．７　まとめ

今後、バイオメトリクスが本格的に普及していくと、様々な法的問題が発生するものと予測される。その中でも中心的に問題になるのは、やはりプライバシー・個人情報保護に関わる問題である。海外においては、特にＥＵを中心に、個人情報保護法制上のバイオメトリクスの取り扱いが議論されてきたが、我が国においても、２００５年４月１日から個人情報保護関連５法が施行されるところから、これらの法律上、どのようにバイオメトリクスが扱われることになるのかを明確化していく必要がある。

さらに、法律の一般性、抽象性という性格上、どうしても法律の規定は抽象的にならざるを得ないところがある。そのため、個人情報保護法を具体化した指針として、各省庁から個人情報保護法に関するガイドラインが出されるようになっている。特に、金融庁の金融分野ガイドライン、経済産業省の信用分野ガイドラインが、生体認証情報に言及しているところが注目されるところである。もっとも、バイオメトリクスは今後、金融・信用分野以外においても広範に活用されるようになるものと予測されるのであり、これらだけで十分なのかどうかという問題は残っている。また、各省庁から出されているガイドラインは、あくまで告示にすぎないところから、個別の分野ごとの法律（個別法）の整備についても今後、検討していく必要があるであろう。

また、各国において、バイオメトリクスの法律上の取り扱いを明確化し、実務運用上の指針を明らかにしていく作業はもちろん重要であるが、さらに国際的な運用ガイドラインについても、検討が必要である。世界には様々な国が存在し、各国の歴史、文化の違い、特にプライバシー意識の違いから、個人情報保護法制も各国において様々である。しかしながら、今後、旅券にバイオメトリクスが搭載されるように、バイオメトリクスデータは国境を越えて流通、利用されるようになることが予測される。そこで、バイオメトリクスデータのプライバシー・個人情報保護問題については、各国で個別に対応しているだけでは不十分であり、国際的なガイドラインが必要になるものと考えられるのである。そのようなガイドラインを策定していく際には、各国の個人情報保護法制の相違を十分に考慮しなければならない。国際標準の活動においては、得てして、ＥＵ諸国が指導権を握ることが多いが、過度にＥＵ寄りのものにならないよう、日本側からも積極的に関与していくことが重要であると考えられる。

これまでバイオメトリクス運用の法的側面についてみてきたが、バイオメトリクスのプライバシー・個人情報保護に関する問題は、法律やガイドラインだけで解決のできるものではない。法律によって必要以上に過度の規制を行うことは、情報の自由な流通や経済の発展を阻害するという側面もあるのであり、技術によって解決できるものについては、できるだけ技術的に解決することが望ましいということができる。バイオメトリクスのプライバシー問題については、法と技術の相乗効果によって解決をはかることが重要であると考えられる。

「参考文献」

（1）See, e.g. John D Woodward Jr., “Biometrics: Identifying Law and Policy concerns” BIOMETRICS Personal Identification in Networked Society, 1999, pp.385-405.

（2）諸外国の個人情報保護制度については、榎原猛『プライバシー権の総合的研究』（法律文化社、1991）233頁以下、堀部政男編『情報公開・プライバシーの比較法』（日本評論社、1996）71頁以下、岡村久道＝新保史生『電子ネットワークと個人情報保護―オンラインプライバシー法入門―』（経済産業調査会、2003）93頁以下、堀部政男ほか「個人情報保護法制の国際比較」比較法研究64号（2003）3頁以下、園部逸夫編『個人情報保護法の解説』（ぎょうせい、2003）273頁以下など参照。

なお、海外においては、保護の対象となる個人に関する情報を指す言葉として、「個人データ」（Personal Data）という言葉が使われることが多い。そこで、以下でも、海外の議論状況を紹介する際には、主として「個人データ」という言葉を用いることにする。後に見るように、我が国の個人情報保護法は、「個人情報」、「個人データ」、「保有個人データ」という三つの言葉を使い分けているが、これらのうち「個人情報」が、海外において用いられている「個人データ」に概ね対応するといってよいであろう。

（3）OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_119820_1_1_1,00.html

（4）訳文は、岡村久道『個人情報保護法』（商事法務、2004）20頁による。

（5）Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

翻訳としては、宇賀克也『解説 個人情報の保護に関する法律』（第一法規、2003）86頁以下、EU指令「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欧州議会及び理事会の指令」（ECOMプライバシー問題検討WG訳）（http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/Direct-1995-EU.htm）がある。

（6）バイオメトリクスのプライバシー問題に関する海外の議論状況については、ＩＰＡ『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）196頁以下が概要をまとめている。以下の記述は、これを参考にしつつ、さらに詳細な調査・検討を行った成果をまとめたものである。

（7） http://www.ibia.org/

（8） http://www.ibia.org/privacy.htm

（9） BIOVISION, Privacy Best Practice in Deployment of Biometric Systems, http://www.eubiometricsforum.com/dmdocuments/D7.4%20Best%20Practices1.pdf

(10) BIOVISION, supra note 9, pp. 5.

(11) BIOVISION, supra note 9, pp. 16.

(12) BIOVISION, supra note 9, pp. 20.

(13) BIOVISION, supra note 9, pp. 23.

(14) ARTICLE 29 - Data Protection Working Party, Working Document on Biometrics, http://europa.eu.

int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf.

(15) http://www.biometricgroup.com/index.html.

(16) http://www.bioprivacy.org/

(17) http://www.biometrics.dod.mil/

(18) The Biometric Consortium Conference, http://www.biometrics.org/bc2003/program.htm.

(19) GOVERNMENT CODE CHAPTER 560. BIOMETRIC IDENTIFIER, http://www.capitol.state.tx.us/cgi-bin/cqcgi?CQ_SESSION_KEY=SOEKKOSTWKFQ&CQ_QUERY_HANDLE=126172&CQ_CUR_DOCUMENT=2&CQ_TLO_DOC_TEXT=YES

(20) Biometric Identifier Privacy Act, http://www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM

(21) 我が国における個人情報保護法制定にいたる経緯については、園部編・前掲注（2）５頁以下、岡村・前掲注（4）10頁以下、宇賀克也『個人情報保護法の逐条解説』（有斐閣、2004）１頁以下、三宅弘＝小町谷育子『個人情報保護法』（青林書院、2003）54頁以下など参照。

(22) 岡村・前掲注（4）10頁以下参照。

(23) 個人情報保護法については多数の文献が存在するが、代表的なものとしては、園部編・前掲注（2）、個人情報保護基本法制研究会編・三上明輝＝清水幹治＝新田正樹著『Q&A個人情報保護法〔第２版〕』（有斐閣、2004）、宇賀・前掲注（21）、岡村・前掲注（4）、三宅＝小町谷・前掲注（21）、藤原静雄『逐条個人情報保護法』（弘文堂、2003）、堀部政男監修＝鈴木正朝著『個人情報保護法とコンプライアンス・プログラム』（商事法務、2004）などがある。

(24) 個人情報保護基本法制研究会・前掲注（23）10、11頁参照。

(25) 村上康二郎「バイオメトリクスに関する法的諸問題」情報ネットワーク法学会第４回研究大会予稿集（2004）57頁参照。

(26) 暗号化された情報の個人情報該当性については争いがあり、①鍵データを保有する者との関係においてのみ肯定する「鍵データ保有者肯定説」（宇賀・前掲注（21）34頁）と、②暗号化されているかどうかを問わず個人情報該当性を肯定する「全面肯定説」（経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（http://www.meti.go.jp/feedback/downloadfiles/i40615hj.pdf）２頁）と、③当該暗号を容易に解読しうる者にとって個人情報たりうるとする「容易解読可能者肯定説」（岡村・前掲注（4）66頁）が対立している。

(27) 園部編・前掲注（2）81頁。

(28) 金融庁「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/siryou/siryou/kj-hogo/01.pdf

(29) 経済産業省「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案」、http://www.meti.go.jp/feedback/downloadfiles/i41001bj.pdf.

(30) 金融庁「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、http://www.fsa.go.jp/siryou/siryou/kj-hogo/04.pdf.