

6. 個人情報保護に対する提言

6.1 法的側面

日本においては、住民基本台帳の整備と合わせて「個人情報保護法」が国会で成立し2005年の5月からは施行される予定である。

バイオメトリクスに関しては、諸外国の動向を調べると現行法の範囲で個人情報として扱い特別な法律制定への動きは少ない。直接には法整備がされなくても別の法律で周辺が固められておりしっかりとした知識の元に運用される素地が出来上がっている。日本においては残念ながらこれからであり、社会的な啓蒙活動を続けバイオメトリクス技術の社会的認知度を高めていきたい。

個人情報保護法をその規制の強度で比較すると、EUとUSが両極端に位置し日本はほぼ中間に位置するといえる。個人情報を扱う事業者は、EUでは事前届出義務があるが日本では義務はない。しかし不具合発生時点で是正勧告をしそれに従わない場合罰則がある。一方USは、一般的に自主性にまかせる気運が強く民間事業者に対する規制は特にない。

米国発信ではあるが、入国審査においてバイオメトリクス情報（顔、指紋）の提示による本人認証を求められ、日本においてもいやおうなしにバイオメトリクス情報を一般人が使用せざるを得ない状況が作られる。新しい技術が世の中に導入されるときは、その実態をよく知って使用することが重要であり、知らないで使用する恐ろしさは筆舌に尽くしがたい。

6.2 文化的側面

バイオメトリクス技術に関する日本国内における文化的側面と考えると、外国人登録法による指紋押捺問題が挙げられる。第二次世界大戦後、外国人登録法が制定され指紋押捺の義務が付けられた。これは強制的な措置であり、根強い反対運動があった。

平成12年に、指紋押捺の義務が廃止されたが、日本人の中に指紋に対する拒否反応は、いまだ残っている。

欧米諸国で研究されている身体障害者に対する考慮に関しては、日本では法整備が遅れている。たとえば、車椅子に乗った人にとっては、日本の中を移動することは非常に骨が折れる状況は変わっていない。

駅の階段にさしかかり、駅員に申し入れをすれば特別の装置または人手によって気持ちよく運び上げてもらえるが、周りからの目や迷惑だという視線に耐えながらの移動となる。身体障害者の社会的地位は、まだまだ低いといわざるを得ない。

6.2.1 外国人登録法

1993年に外国人登録法が改正され指紋登録の義務化がなくなりました。しかしながらいまだに指紋に対する拒否反応が残っています。

6.2.2 身体障害者対応

日本規格協会では「高齢者・障害者等配慮設計指針—情報通信機器・サービス」に関し

て JIS 化を推進中。2003 年 7 月に公開レビューが実施された。

http://www.jsa.or.jp/domestic/instac/review/2003/itbf_review.htm

(1) 目的

情報通信機器に対して「障害者でも十分容易かつ安全に操作可能な I/F を考慮すべき」

(2) バイオメトリクスに関係した条項

障害者向けにバイオメトリクスを利用する場合には、身体の特徴に頼らない代替方式を準備する。

6.3 医学的側面

バイオメトリクス技術に関する医学的側面とは、次の項目が考えられる

- (1) 前の人が同じ装置を使用した場合、その人が持っている細菌等が伝染しないか
- (2) 医学的に病気と判断される人がバイオメトリクス機器を使用した場合、その病気の進行に影響を与えないか
- (3) 本来の使用目的である本人認証とは異なる、個人のプライバシーに関わる情報が簡単に入手できないか

これらについて検討すべきと考える。

しかしながら、バイオメトリクスといっても認証方法にはいろいろあり装置もいろいろあるので、それらをひとつずつ調査する必要がある。

NO	手法	接触機器	非接触機器
1	指紋	(1)(3)	-
2	虹彩	-	(2)(3)
3	顔	-	(3)
4	声	-	(1)
5	サイン	-	
6	静脈	-	(3)
7	DNA	-	(3)

医学的側面の課題については、使用するバイオメトリクス機器が上記(1)(2)(3)において問題点を指摘された場合、誰がそれを回避する方法を編み出し、誰がそれを保障できるかという新しい課題にぶつかる。

具体的な個別の課題に対しての詳細分析は、次年度の調査項目として引続き研究開発する項目とする。

6.4 技術的側面

バイオメトリクス個人情報の保護は、バイオメトリクス個人情報が目的外のために不正に閲覧・複製・改竄・持ち出しされないよう運用基準を定め、それを遵守し、また、必ず遵守されているかを監査する運用面と、運用基準に正当性を与え、また、運用基準に違反する行為を罰する法的側面が重要であることは言うまでもない。しかし、万一、運用面で基準が満たされないような場合にも安易に情報が閲覧・複製・改竄・持ち出しされないような技術面での保護が効果的である。本節では、技術面からの保護策について提言を行う。

まず、第一に、保護すべき対象を定義する。保護すべき対象は二種類あり、それぞれ、運用要件が異なっている。

(ア) バイオメトリクス個人認証システムの開発や性能評価のために用いる標準データベース

(イ) 個人がバイオメトリクス個人認証を受けるために登録した個人情報(バイオメトリクステンプレート)

標準データベースは数百人から何万人ものデータを同時に用いることが必要である反面、一つ一つのデータと個人とを明確に結びつける必要はない。登録時には、同一人物が未登録であることさえ保証されれば問題ないので運用時には個人との関連を示す情報を取り去って用いることが望ましい。ここでの問題は、標準データベースは組織間を超えて流通させる必要があるため、データベースの提供元はいったんデータを外部の機関に提供した後で、その管理が適正に行われているかを監査したり、不正なアクセスから保護したりすることが極めて困難であるという点である。(すべてではデータを保有している機関の運用に依存する)

一方、バイオメトリクステンプレートは、1:1 照合においては同時には一名分のデータしか参照されないが、個人を特定する情報を含むためその取り扱いには慎重を期さねばならない。また、システム開発と異なり、閲覧・詐称・改竄・持ち出しにより具体的に利益をもたらす可能性が高く、不正なアクセスの動機付けが十分存在する。

以下、標準データベースと個人テンプレートとの場合に分けて、個人情報を保護すべき対象とその技術的可能性について検討し、今後行うべき技術開発を提言する。

A. 標準データベースにおける個人情報保護

(i) 標準データベースに対する攻撃の可能性

標準データベースに対して攻撃する動機となる要因は以下のとおりである。

(ア) データベースの不正取得

標準データベースはその構築に高い費用と労力を要するため、データベースを不正な手段で入手すれば利益が得られる。

(イ) データベースの改竄

性能評価用データベースに不都合なデータが含まれていた場合、被評価者に都合の良いデータに置き換えると利益が得られる

(ウ) 偽候補の検索

大規模なデータベースであれば、ある個人に極めて似たサンプルを探し出して利用することができる。

(エ) 興味本位

大規模データベースから好みや興味本位で個人のデータを読み出したり、それを不正に公開して身元を暴いたりする可能性がある。

(ii) 標準データベースの保護方法

これらの攻撃に対して、標準データベースは以下のように保護されるべきである

1. 不正な閲覧の防止
認証されたものだけがデータにアクセス可能とする。データベースの暗号化。アクセス制限。
2. データベースの正当性保証
構築されたデータベースが改変されていないことを保証する。電子署名など。
3. データベース利用履歴監査
外部の機関に配布されたあともデータベースがいつ・だれによって参照されたかを常に監査可能にする。
4. 実在する実体への探索の無効化
データベースがシステム開発・システム性能評価に影響がない程度に、データ自身が実在するデータから変形されており、実在する実体の個人を推定することを困難にする。

(iii) 利用・開発すべき技術

上記の(ii)を実現するため、次のように既存技術を応用したり、あるいは、新規に開発することが望ましい。

(ア) 電子署名や暗号化によるデータベースの保護

認証された人物・コンピュータ・プログラムだけがデータベースを参照し、また、データベースの不正な改竄を検出する機能を暗号技術を用いて実装する。

(イ) システム開発やシステム性能評価を実用上高い精度で行うことができる仮想標準データベースの開発

システム開発あるいはシステムの性能評価を行うには、個人データの密度・中心・分散・データ間最小距離が重要である。これらの統計的性質がまったく同じで、かつ、個別のデータ自身は実在しない仮想的な個人データであるデータベースを開発することが望ましい。このデータベースは個人情報を含んでいないため、自由に流通させて問題ない。たとえば、指紋に関しては Sfinge: 人工的指紋生成プログラム(参考資料 1)とそれを用いた指紋照合アルゴリズム評価 FVC2002(参考資料 2)が、試験的に用いられて実画像データベースとの対比も行われているが、その他のバイオメトリクスでは人工標準データベースはまだ実現していない。

B. 個人のバイオメトリクステンプレートの保護

(i) バイオメトリクステンプレートに対する攻撃の可能性

テンプレートに対して攻撃する動機となる要因は以下のとおりである。

(オ) データベースの不正取得

他人へのなりすましを行うために、まず他人のテンプレートを不正に取得することが行われる可能性が高い。

(カ) データベースの改竄

他人の認証を妨害したり、なりすましたりするために、登録済みのテンプレートを改竄しようとする可能性がある。

(キ) 偽候補の検索

大規模なテンプレートデータベースにアクセスできれば、なりすましやすい他人を検索してくることが可能である。

(ク) 興味本位

大規模テンプレートデータベースから好みや興味本位で個人のデータを読み出したり、それを不正に公開して身元を暴いたりする可能性がある。

(ii) バイオメトリクステンプレートの保護方法

この攻撃に対しテンプレートデータベースは以下のように保護されるべきである

5. 不正な閲覧の防止

認証されたものだけがデータにアクセス可能とする。データベースの暗号化。アクセスの制限または閲覧できてもテンプレートとして利用不可能。

6. データベースの正当性保証

構築されたデータベースが改変されていないことを保証する。電子署名など。

7. データベース利用履歴監査

テンプレート登録・閲覧の履歴が監査可能なこと。

8. 不要な一括管理の廃止

大量のテンプレートが一度に不正アクセスされる可能性があるので、絶対必要でない限り大量の個人テンプレートデータベースを一括管理すべきではない。

(iii) 利用・開発すべき技術

上記の(ii)を実現するため、次のように既存技術を応用したり、あるいは、新規に開発したりすることが望ましい。

1. 電子署名や暗号化によるテンプレートデータベースの保護

テンプレートに電子署名を付加したり、テンプレートを暗号化して特定のアプリケーションのみがテンプレートを複合化したりできる仕組み。たとえば、Bioscript 社 Template Protection 方式の発展実装（参考資料3）

2. 暗号化されたテンプレートを復号せずに照合する照合技術

テンプレートデータベースを暗号化しても、それを復号して照合に用いるならばシステム内に復号されたテンプレートが存在したり、あるいは、復号キーを盗まれたりすることで復号されたテンプレートを略取される可能性が残る。テンプレート暗号化に一方向関数などを用いて複合化不能にできるならば登録されたテンプレートが盗まれても再登録すればよい。

ただし、全一致の場合のみ照合が成功する文字ベースの暗号鍵システムとことなり、パターン認識に基づくバイオメトリクス照合では部分的一致の加算によって照合結果が決まるため、単純には暗号化されたテンプレートとの照合は実現できない。

3. バイオメトリクステンプレート格納媒体の工夫

現在、バイOMETリクステンプレートをセンターデータベースで管理すると、一度に多人数分のデータベースが閲覧・改竄・持ち出しされる可能性が否定できないため、テンプレートトークン（たとえば非接触 IC カード）に個人のテンプレートを保存し、トークンは認証を受ける個人が管理するというシステムが多く見られる。しかし、トークンの不携帯や紛失・盗難が少なからず発生するため、日常の運用において、登録テンプレートがない場合のバックアップ本人確認手段、トークン再交付などの運用負荷の増大が予見される。したがって、

- (a) 紛失・盗難耐性があり、かつ、個人管理可能なテンプレート格納手段
- (b) テンプレートの個人管理部分が得られない場合の個人識別手段の提供の実現が求められる。