4. 個人情報の取り扱い

4.1. 本章の対象

本章では、下記のテーマを調査の対象としている。
詳細について次節以降で報告する。

1） 収集されたデータの個人情報保護方法に関する調査

4.2. 収集されたデータの個人情報保護方法に関する調査

4.2.1. 指紋認証システムの制度評価方法（JIS-TR）の調査

「指紋認証システムの精度評価方法(JIS-TR)」において、個人情報の取り扱いについて「付属書2(参考) 生体データベースの取り扱い」記述がある。概要を以下に示す。

1. 適用範囲
   OECD 勧告における八原則を基本として, 生体認証データベースの取り扱いに関する指針を定める。

2. OECD 勧告
   OECD は,「国際データ障害とプライバシー保護専門家グループ」を 1978 年に設置し, このグループでの成果物をもとに 1980 年 9 月 23 日「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 Governing the Protection of Privacy and Transporder Flows of Personal Data) を採択した。このガイドラインは基本8原則から構成されていて, 個人情報保護に関する最小限の基準 (ミニマム・スタンダード) となっている。

   この基本八原則をもとに, わが国では 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の保護に関する法律」が制定された。いわゆる「個人情報保護法」である。内容は, 以下の通り。

   a) 個人情報ファイルの利用目的の限界 (4 条)
   b) 個人情報の安全確保 (5 条)
   c) 個人情報ファイルの保有に関する事前通知 (6 条)
   d) 個人情報ファイル簿の作成・閲覧 (7 条)
   e) 個人情報ファイルの公示(8 条)
   f) 個人情報ファイルの開示請求 (13 条)
   g) 個人情報ファイルの訂正の申出(17 条)

ただし，この法律は行政を対象としたものであって，民間は対象外とされている。

なおOECDでは，1998年10月にオタワで開催された閣僚会議で，インターネット上などのオンラインでもOECD8原則が基本となること，加盟国間の異なる保護手段を認め合って様々なアプローチで橋渡し作業をすること，などを盛り込んだ「プライバシー保護に関する宣言」を採択した。

3. 生体認証データベースの取り扱いに関するガイドライン

生体認証データベースを取り扱うすべての者は，以下に掲げる条項を遵守する必要がある。

a) 利用目的による制限

“生体認証データは，採集時あるいはそれに先立ってその利用目的を明確にしなければならない。また，明確化された利用目的以外のために利用してはならない。”

b) 適正な方法による取得

“生体認証データは，生体認証データ提供者の同意を得た上で，適法かつ適正な方法によって取得されること。”

c) 内容の正確性の確保

“生体認証データは，その利用目的の達成に必要な範囲内において正確（accurate）かつ完全（integrity）であり，最新なものに保たれること。”

d) 安全保護措置の実施

“生体認証データは，適切な安全保護措置を講じた上で取り扱われること。”

e) 透明性の確保・提供者の権利保証

“生体認証データベースに関わる開発，運用，および方針については，一般に公開されなければならない。また，生体認証データの提供者に対する権利を保証しなければならない。”

f) 生体認証データベース管理者の責任

“生体認証データベース管理者は，上記a)からe)の各項を実施するための措置に従うこと。”

4.2.2. 顔認証システムの精度評価方法（JIS-TR）の調査

「顔認証システムの精度評価方法(JIS-TR)」において、個人情報の取り扱いについて「付属書2(参考) 生体データベースの取り扱い」記述がある。
内容的には、「指紋認証システムの精度評価方法(JIS-TR)」における個人情報の取り扱いと同じため、ここでは詳細を割愛する。

4.2.3. Biometric Security Concerns の調査

(1) BWG 発行"Biometric Security Concerns V1.0 September 2003"の概要

本資料は英国バイオメトリクス・ワーキング・グループが、バイオメトリクス・データを取り扱うときのセキュリティに関する留意事項についてまとめたものである。

本文の記述形式は、個々の問題の詳細を述べ、回答の必要なものに対しては解決策を示す形式となっている。取り上げられている項目は、以下のとおりである。

1 性能の制限
2 登録の完全性
3 登録の品質
4 なりすまし（生理学のバイオメトリクス）
5 模倣（行動面からのバイオメトリクス）
6 潜在する／残余のイメージ
7 テンプレートの完全性／機密性
8 キャプチャー／リプライ攻撃
9 バイオメトリクスは、絶対的な識別を提供しない
10 生体認証は、秘密でありません
11 バイオメトリクスは、十分にランダムではありません
12 バイオメトリクス･アルゴリズムはプロプラエタリで検証されていません
13 危険にさらされた時バイオメトリクスは変更することができません
14 バイオメトリクスはスマート・カード上のみに格納されるべきです
15 バイオメトリクスは、否認を否定する
16 どのようにしてシステムの安全性が低下していることを知ることができますか
17 対抗策の公表はシステムをそれほど安全でなくしますか
18 偶然にバイオメトリクスの「署名」を与えることがありますか
19 バイオメトリクスは密かに集められることがありますか
20 私のバイオメトリクスを盗むことはできますか
21 いつ、そしてどのように、私のバイオメトリクスが使用されかわかるしょうか
22 バイオメトリクスの使用は、キャプチャー、強制、傷害の可能性を増加させますか

２３　単一の強い識別子がある場合、ID 不正行為はより悪くなります
２４　識別を備えたバイオメトリクス・システムはストーカーを助けますか
２５　登録データベースを犯罪の容疑者を捜すために使用することができますか
２６　管理者あるいはオペレーターによる誤用
２７　機能の変形

本書の目的は概要にまとめられている。以下に「概要」の一部を引用する。

概要

バイオメトリクスの使用に関する多くの問題があります。特に認証に関する問題の多くは、バイオメトリクスの認証プロセス自体に対する信頼性、あるいはシステムで使用され、ユーザにとってはプライベートで個人に関するバイオメトリクス・データの保護に関するものです。それは、従来のパスワード、PIN およびトークンに基づいた認証技術と異なるものとしてバイオメトリクス・システムとして表される概念であり、これから議論します。

このドキュメントの目的は、いわゆるセキュリティに関する配慮に焦点を当て、それが脅かす可能性のある脅威について議論し、それを除去するか、少なくとも緩和するためにできることについて、より詳細に調査することです。

このドキュメントにはバイオメトリクスの技術的なセキュリティ機能および詳細な対抗策を盛込んでいないことをご了承ください。

重要性

バイオメトリクス技術およびシステムの成功は、政府によって使用されるバイオメトリクスの適応性を決定する際に直面する重大、かつ困難なセキュリティへの挑戦にかかっています。多くの政府向けアプリケーションが、認証プロセスに対してハイ・レベルな信頼性を要求しています。また、市民との双方向システム「英国オンライン」の普及した時代には、プライバシーとデータ保護は非常に重要な問題となります。例えば、電子投票時、個人認証の目的で指紋を利用するユーザは、詐欺者が擬装することができないことを保証してほしいと思うでしょう。そして、そのデータは犯罪防止等の目的で第三者(例えば警察)に提供されないことを保証してほしいと思うでしょう。

警告

セキュリティが議論されるときは、一般に特定の問題が注目される傾向があります。特にバイオメトリクスがテーマになる時はこの傾向があります。「なりすましについてはどうですか? 」という質問が真っ先に飛び出します。しかし、このアプローチは、アプリケーションで有効なセキュリティを決定する要因の中でも、はるかに複雑な相互作用を見落とす危険があります。

システム・インプリメンターおよび管理者は、危険要因およびレベルを決定するためにアプリケーションを取り巻くすべてのセキュリティ問題について完全に理解していることが必要とされます。

セキュリティの適切なレベルを提供するために、技術的、手続的および環境上の手段が相互にかつ有効に成立している必要があります。

⑵ 個々の問題に対する検討内容

１　性能の制限

バイオメトリクスは完全な(固有の)個人識別を保証していない。そして、統計的なエラーの問題を内包している。

他人受入れと本人拒否が次のものを含む多数の要因に影響を受ける。

- バイオメトリクス特性のユニークさ
- 認証装置
- アルゴリズム
- 環境条件（光線、ノイズ、等）
- 人口（人口動性、職業、等）
- 行動（態度、協力、等）

本人拒否は、過度の場合、システムを使用不可能にするかもしれないが、直接のセキュリティの脅威にはならない。

間違って、個人が複数回登録されるとすると、他人受入れはセキュリティの問題となる。

２　登録の完全性

登録の完全性の保証は、バイオメトリクスを使用するか否かにかかわらず、すべての認証システムの重大な根本的要求となる。

登録プロセスそれ自身が安全であることを保証しなくてはならない。ほとんどの場合、これは信頼され、訓練されたスタッフによって実施することを意味する。

３　登録の品質

低い登録品質は、ほとんど必然的に貧弱なシステム性能を招く。性能が貧弱な場合、セキュリティは危機にさらされる。

登録の品質を保証するためには、よい登録手続きと訓練された管理者が必要である。バイオメトリクス・システムは登録品質をチェックし、品質の悪い登録を拒絶できなければならない。

４　なりすまし（生理学のバイオメトリクス）

注意深く抑制された条件の下ではなりすまし攻撃を成功裏に実施することが可能な場合

がある。

なりすまし攻撃は、技術的・手続き的な対抗策によりかわすことができる可能性がある。そのためには、生体に代わるコピーの使用を検知し、拒絶することができなければならない。バイオメトリクスの特徴と生体であることの把握を同じ場所と時間で取得することを保証しなければならない。

マルチモード・バイオメトリクス(例えば顔や音声)、バイオメトリクスと PIN のように複数の要素による認証、そして、行動特性を利用するチャレンジ/レスポンス機能の使用を通じて障壁をより高くすることができる。

偽造物の使用に対抗するのに必要と思われる唯一の運用上の手段は監視である。登録およびシステム運用が監視される場合、ほとんどの偽造物を詐欺者が使用することは困難となる。

５　模倣（行動面からのバイオメトリクス）

行動面での特徴を使用するバイオメトリクス･システムは、広範囲の攻撃者からの攻撃をより受けやすいかもしれない。

模倣に偽造品の機能が含まれていないとすると、生体検知は適用できない。本物の人体と模倣物を識別するべき能力に注目すべきである。これは改善された技術的な性能(FAR/FRR)、監視されたオペレーションおよびチャレンジ/レスポンス機能を含まなければならない。

６　潜在する／残余のイメージ

正しいシステムソフトウェア設計およびシステム・メンテナンス(掃除)は潜在あるいは残余のイメージ問題を処理できる。

７　テンプレートの完全性／機密性

認証プロセスの完全性は、テンプレートの完全性に依存する。

バイオメトリクス・アプリケーションは、法的な必要条件に応じるために適切な保護を含む必要がある。

テンプレートへの無許可のアクセスを防ぐために暗号化技術の使用によるアクセス・コントロールが必要である。テンプレート・データのデジタル署名の使用が完全な保護に十分かもしれない。しかし、デジタル署名は機密性を保護しない。

暗号の保護は他の技術(タイムスタンプのような)と併用する必要があるかもしれない。

８　キャプチャー／リプライ攻撃

次のものを含めて、多くの技術的・手続き的な解決策が利用可能である。

- 物理的なセキュリティ(タンパー抵抗および検知、ガード、検査など)
- コミュニケーション・パスのためのユニークなセッション・キー/タイムスタンプを備えたデータ暗号化
- 格納された参照テンプレートへのアクセス・コントロール
- マークされ署名された参照テンプレート

セキュリティ評価は有効で、性格に実施された解決策の保証をするために必要である。

９　バイオメトリクスは、絶対的な識別を提供しない

バイオメトリクス認証は、単に全面的な認証フレームワークの一部にすぎない。非バイオメトリクスの要素(登録前)は受理可能な信任状(例えば出生証明書、仲間の支持)を利用して、アプリケーションのために必要とされる保証基準を備える絶対的な同一性を確立するために必要である。

１０　生体認証は、秘密ではない

バイオメトリクスの特徴は、しばしば容易に観察され、等価な秘密を保有しない。実際、バイオメトリクスのセキュリティは、基礎的なバイオメトリクスの特徴に依存しない。バイオメトリクスのセキュリティは、認証メカニズムに完全に依存する。

１１　バイオメトリクスは、十分にランダムではない

ランダム性の欠如は、その特性によって個人を分離することがより困難であることを意味し、個人を混同しやすくなる。バイオメトリクスのアルゴリズムの振る舞いおよび人間の特徴のランダム性と差異についての現在の知識は、バイオメトリクス・システム性能の論理的な分析が可能なレベルにはない。

バイオメトリクス･システムの使用を計画する管理者は、エラー割合の必要条件を評価し、バイオメトリクス・システムが要求に合うかどうかを決定する必要がある。識別(1:n)システムについては、少数のユーザならば処理可能なエラー率も、登録されたユーザ数が上昇するとともに急激に耐えられなくなる。

１２　バイオメトリクス･アルゴリズムはプロプラエタリで検証されていない

バイオメトリクスのアルゴリズムの目的はセキュリティではなく機能である。

明かされていないアルゴリズムは不明瞭によるセキュリティの強化をもたらすかもしれないが、アルゴリズムのリバースエンジニアリングを含んでいるかもしれない攻撃には恐らく抵抗できない。

セキュリティ評価は、バイオメトリクスのアルゴリズムの効能を決定し、個人を分離、識別/認証し、そして、攻撃者によって開発可能かもしれないすべての弱点を決定するために使用することができる。

１３　危険にさらされた時バイオメトリクスは変更することができない

テンプレートが被害にあうと、無許可のユーザのテンプレートを代用するために登録されたバイオメトリクスのテンプレートの置換か修正、あるいは無許可のユーザ･テンプレートが追加されているかもしれない。

新しいテンプレートを加えることは、システム上に不正なユーザを登録する危険がある。これにより、テンプレート・データベースの整合性がひどく弱められるかもしれない。

なりすまし被害の解決策は、バイオメトリクス･システムに組み込まれた、監視されたオペレーションおよび生体検知にある。

解読可能なバイオメトリクスに対し、バイオメトリクスのイメージからテンプレートを生

成する場合、繰り返し使用可能であるが、不可逆的な方法で変形することが提案されている。

１４　バイオメトリクスはスマート・カード上のみに格納されるべき

これは中央のデータベース上に格納されたバイオメトリクス･データの潜在的な誤用に対して心配される表現である。

バイオメトリクス･データは通常、単独では保持されない。それは、一般に識別および認証プロセスの一部を形成する他の個人データ、あるいは、それに続くアクセス･コントロール許可に関連付けられている。

可能性のある解決策は、ユーザ自身によって保持される安全なトークンあるいはスマート･カード上に個人データを格納することにある。トークンあるいはスマート･カード上に個人データを格納することによるプライバシー保護の利点は、大部分が錯覚となる。

機能変化の危機を緩和するために、バイオメトリクス･データを暗号化による署名技術の使用を通じてアプリケーションに結びつけることができる。

１５　バイオメトリクスは、否認を否定する

識別/認証のための法的な波及がある場合、拒否はアプリケーションの問題である(例えば金融取引)。多くの金融機関とその他の契約上の処理がバイオメトリクス認証によって保証されるとき、これは潜在的な将来の問題となる。

１６　どのようにしてシステムの安全性が低下していることを知ることができるか

いくつかのバイオメトリクス･システムはセルフアダプティブである。登録者と共謀して働く詐欺者は、最後には登録者のテンプレートを詐欺者のテンプレートに替えるようにシステムを「訓練」することがある。

この危険は、システムの監査とテストによって知ることができる。

１７　対抗策の公表はシステムの安全を脅かすか

一般に、不明瞭によってセキュリティを達成することはありえない。セキュリティを達成することは将来の災いとなりかねないと想定する事柄の分析の困難さに依存する実行可能な政策である。不明瞭が保護を提供できないというのではなく、不明瞭による保護はやや予測不能で短命かもしれないということである。

バイオメトリクス装置およびアプリケーションを安全にしたければ、脅威を理解し、適所に技術的･手続き的である有効な対抗策を置く事が必要である。

１８　偶然にバイオメトリクスの「署名」を与えることがあるか

バイオメトリクスでないシステムは、一般に明示的なユーザ行為を必要とする。

認証アプリケーションにおいては、プロセスは、カードの挿入や暗証番号をタイプインするといった明示的な同意を意味する行為を含むべきである。

１９　バイオメトリクスは密かに集められることがあるか

いくつかのバイオメトリクスは容易に「密かに」使用することができる。バイオメトリクス以外の情報は、ほとんどの場合、それほど容易に密かに集めることができない。

密かな収集の脅威に対する技術的な対抗策は無い。しかし、バイオメトリクスの秘密使用の可能性は認識されており、バイオメトリクス・アプリケーションは、適切な法的・手続き的な制約を課すべきである。

２０　バイオメトリクスを盗むことはできるか

格納されたイメージあるいはテンプレートは暗号化により保護することができる。

盗んだイメージデータが偽造品を作成するために使用される場合、バイオメトリクスが実際に人から提供されていることを保証するために生体検査を使用することができるかもしれない。

盗んだテンプレートおよびテンプレート･データは、暗号に基づいた完全チェックあるいは暗号化の使用を通じて無害にできる。一方で、テンプレート変換技術は、そっくりに変形された特徴ベクトルを使用してマッチング用に変形されたテンプレートによる代用が成功することにより信用をなくすことを回避するように討論された。

２１　いつ、どのように、バイオメトリクスが使用されるかわかるか

異なる技術を使用するバイオメトリクス･アプリケーションがそれ自身、各々制限的要因となるアプリケーション間でバイオメトリクス･データを共有することはありそうにない。将来、バイオメトリクス･システムの統合および相互運用に関する要求は拡大し、標準化が推進されるかもしれない。

データ保護行為は、個人のデータを格納および処理するアプリケーションが原理原則を厳守し、情報管理者だけでなく、ユーザにもシステムの目的およびオペレーションが説明されることを必要とする。

相互参照監査は、ユーザに生じたかもしれないシステム･プライバシー政策および任意の妨害の適切な印譜裏面テー所ンを示す証拠を供給することができる。

一般的に、バイオメトリクス･システムが照合プロセスの実行を可能とするため、バイオメトリクス･データが明瞭な形式で(一時的に)存在するであろうことは注意が必要である。

２２　バイオメトリクスは、キャプチャー強制あるいは傷害の可能性を増加させるか

ユーザの物理的な存在が要求されるバイオメトリクスが使用される場合、ユーザをより多くの危険にさらすかもしれない。

犯罪の内容によっては、バイオメトリクス認証が抑制物の役割をすることがあるようにも思える。バイオメトリクスの使用が、強制や暴力の頻度あるいは程度に重要な違いを生じさせるか否かは明らかでない。

バイオメトリクスの使用は、ユーザを危険にさらす可能性を縮小する役目をするかもしれない。なぜなら、多くの場合、犯人逮捕の機会を増加させるからである。

有効な生体チェックは、死骸あるいは切断された四肢の使用などへの試みに対する動機に対する対抗策となる。

２３　単一の強い識別子がある場合、ID 不正行為はより悪くなるか

バイオメトリクス登録自体の質が、それに続く識別か認証の試みの性能および信頼度を制限する。

操作および管理スタッフは、登録の重要性に気づかなければならない。そして、適切な登録品質が維持されることを保証するために適切なトレーニングを行わなければならない。

２４　識別を備えたバイオメトリクスはストーカーを助けるか

技術的に、分配されたバイオメトリクス･システムを横断したトラッキング能力を提供する機能の除去は、有効な制限を提供する。

技術面以外の解決策は、システム使用の適切な監査によりバックアップされた手続き的なセキュリティ対策(安全な操作の手続き、スタッフ･トレーニング)に依存する。

２５　登録データベースを犯罪の容疑者を捜すために使用することができるか

解決策の大部分はバイオメトリクス･データの使用および共有中の強制の領域にある。技術的解決策としては、バイオメトリクス･データの暗号化によりプライバシーを保護することがある。

センタにデータを保持しない場合、つまり、ユーザの管理化の下でユーザのバイオメトリクスがスマート・カード上で単独に保持されるアプリケーションでは問題にならない。

２６　管理者あるいはオペレーターによる誤用

全国規模のアプリケーションに必要である。部分的解決策には以下のものがある。

- 管理者／オペレーターを注意深く選択する。
- 役割の分割を行い、単独でデータ検索できないようにする。
- バイオメトリクス･データベースへの管理者／オペレーターによるアクセスの監査を行う。
- バイオメトリクス･データを中央で一括管理しない。
- マルチモード･バイオメトリクスを使用する。
- データベースを暗号化する。

２７　機能の変形

バイオメトリクス(個人)データの共有は、データ保護行為の法的必要条件を超えないようユーザに対して明示的な同意を要求する。

機能の変形に対する技術的な解決策は、暗号を使用するアプリケーションへのバイオメトリクス･テンプレートの結合を含んでいる。しかし、ユーザ(あるいは信頼されたサードパーティー)の手にコントロールを委ねることが必要である。PKI 基盤は技術的な解決策を提示するかもしれないが、実用的ではないだろう。これは将来の課題である。

4.3. まとめ

4.3.1. 生体認証データベースの取り扱いに関するガイドライン

わが国では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の保護に関する法律」いわゆる「個人情報保護法」が制定された。これは１９８０年9月２３日に採択された「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」(Recommendation of the Council concerning Governing the Protection of Privacy and Transporter Flows of Personal Data)をもとにしている。

ただし、上記「個人情報保護法」は行政を対象にしたものであって、民間は対象外とされている。

「指紋認証システムの精度評価方法(JIS-TR)」および「顔認証システムの精度評価方法(JIS-TR)」では、上記「個人情報保護法」をもとに「生体認証データベースの取り扱いに関するガイドライン」を定めている。

ここでは、生体認証データベースを取り扱うすべての者は、以下に掲げる条項を遵守する必要があるとしている。

a) 利用目的による制限
b) 適正な方法による取得
c) 内容の正確な確保
d) 安全保護措置の実施
e) 透明性の確保・提供者の権利保証
f) 生体認証データベース管理者の責任

4.3.2. バイオメトリクスのセキュリティに関する配慮

２００３年9月に英国政府バイオメトリクス作業部会(BWG : the UK Government Biometrics Working Group)により作成された「バイオメトリクスのセキュリティに関する配慮」(Biometric Security Concerns V1.0 September 2003)においては、より具体的な表現で生体認証データの保護に関する注意点を挙げている。

a) バイオメトリクスは完全な(固有の)個人識別を保証していない。
b) 生体情報の登録の完全性が保証されていなくてはならない。
c) 生体情報の登録の品質が生体認証システムの性能を左右する。
d) なりすましは、生体検知と生体認証の組み合わせにより排除することができる。
e) 偽造物の使用に対抗する唯一の運用上の手段は監視である。

f) テンプレートのデジタル署名は、テンプレートの機密性を保護しない。
g) バイオメトリクスのセキュリティは、認証メカニズムに依存する。
h) セキュリティ評価は、バイオメトリクスのアルゴリズムの効能を決定し、弱点を強化するために使用することができる。
i) バイオメトリクスのテンプレートは不可逆的な方法で変換し、格納すべきである。
j) ユーザが保持するトークンあるいはスマート・カードによるプライバシー保護の利点の大部分は錯覚である。
k) 機能(使用目的)変化の危険を緩和するために、バイオメトリクスデータを暗号化による署名技術を通じてアプリケーションに結び付けるべきである。
l) システム安全性低下の危機を取り除くためには、システム監査とテストが必要である。
m) 認証アプリケーションにおいては、プロセスはカードの挿入や暗証番号をタイプインするといった明示的な同意を意味する行為を含んでいるべきである。
n) バイオメトリクスの秘密使用の可能性は認識されており、バイオメトリクス・アプリケーションは、適切な法的・手続き的な制約を課さねばならない。
o) 格納されたイメージあるいはテンプレートは暗号化により保護できる。
p) バイオメトリクスが実際に人から提供されていることを保証するために生体検査を使用することができる。
q) 盗んだテンプレートおよびテンプレート・データは、暗号化技術に基づいた完全チェックあるいは暗号化の使用を通じて無害にできる。
r) データ保護行為は、個人のデータを格納および処理するアプリケーションが原理原則を遵守し、情報委員だけでなく、ユーザにもシステムの目的およびオペレーションが宣言されることを必要とする。
s) バイオメトリクスの使用は、多くの場合、犯人逮捕の機会を増加させる。そのため、バイオメトリクスの使用が、ユーザをより多くの危険にさらすことはない。
t) バイオメトリクスの登録自体の質が、それに続く識別か認証の性能および信頼性を制限する。
u) 技術的に分配されたバイオメトリクス・システムを横断してトラッキング能力を協調する能力の除去は、有効な制限を提供する。
v) 技術面以外では、システム使用時の適切な監査によりバックアップされた手続き的なセキュリティ対策(安全な操作の手続き、スタッフ・トレーニング等)に依存する。
w) 登録データベースを犯罪の容疑者を探すために利用する場合、生体情報の暗号化によってプライバシーの保護が可能である。
x) バイオメトリクス・データを保護するためには、管理者あるいはオペレーターを注意深く選び、権限を制限・分散させることが必要である。
y) バイオメトリクス・データの共有は、データ保護行為の法的な必要条件を超えないよう、ユーザに対して明示的な同意を求める必要がある。

4.3.3. 調査結果のまとめと今後の課題

今回の調査結果をまとめると以下のことが言える。

a) ユーザ自身によって保持される安全なトークンあるいはスマート・カード上に個人データを格納することによって個人情報を保護することには限界がある。
b) 認証あるいは識別には中央のデータベースが必須となる。
c) バイオメトリクス・データの使用時は、提供者に対して明示的な同意を必要とする。
d) バイオメトリクス・データの完全性が個人情報保護のレベルを規定する。
e) バイオメトリクス・データのテンプレートは不可逆的な方法で変換し格納すべきである。
f) バイオメトリクスにおける個人保護の最重要課題は、運用にある。
g) 特に、管理者あるいはオペレーターに対する考慮が必要である。

これら調査結果から、今後の課題として以下のものがあげられる。

a) 使用目的による個人情報の取得および使用方法に関する法的制限の明確化。
b) バイオメトリクス･データの中央での一括管理における運用上の制限事項の明確化。
c) バイオメトリクス･データの管理者およびオペレータの運用面での監査項目の明確化