バイオメトリクス・セキュリティ評価に関する研究会

平成 18 年度　研究会中間報告書

平成１８年１２月

独立行政法人　情報処理推進機構

セキュリティセンター

研究会名簿

（2006 年 10 月末現在）

＜座長＞

小松　尚久	早稲田大学

＜委員＞（五十音順）

青木　芳人	松下電器産業株式会社
池野　修一	セコム株式会社
岩下　直行	日本銀行金融研究所
笹川　耕一	三菱電機株式会社
新崎　卓	株式会社富士通研究所
鷲見　和彦	京都大学
瀬戸　洋一	産業技術大学院大学
道坂　修	株式会社 NTT データ
保黒　政大	株式会社ディー・ディー・エス
星　佳典	沖電気工業株式会社
松本　勉	横浜国立大学
溝口　正典	日本電気株式会社
三村　昌弘	株式会社日立製作所

＜事務局＞（順不同）

三角　育生	独立行政法人情報処理推進機構
小林　偉昭	独立行政法人情報処理推進機構
中野　学	独立行政法人情報処理推進機構

目次

研究会名簿

1. 検討の背景と課題 4
1.1. **検討の背景** 4
1.2. **本中間報告書の目的** 8
2. バイオメトリクス・セキュリティ 9
2.1. **バイオメトリクス・セキュリティとは** 9
2.2. **バイオメトリック認証方式の特性** 9
2.3. **バイオメトリック認証システムのモデル** 10
2.4. **バイオメトリクス・セキュリティの脆弱性となる可能性** 13
2.5. **バイオメトリック認証システムに対する攻撃への対策** 16
2.6. **まとめ** 19
3. 認証精度評価 21
3.1. **精度評価の背景** 21
3.2. **各国の動向** 22
3.3. **認証精度評価に向けた生体情報 DB に対する分析** 23
3.4. **認証精度評価および生体情報 DB 構築における留意事項** 27
3.5. **まとめ** 29
4. 製品データベースに関する検討 30
4.1. **背景** 30
4.2. **収集情報** 30
4.3. **アンケート項目** 31
4.4. **収集方法** 33
4.5. **収集情報の確認** 34
4.6. **収集結果** 34
4.7. **公開検討** 34
4.8. **まとめ** 35
5. バイオメトリクス・セキュリティの今後の課題 36
5.1. **ユーザへのバイオメトリック認証の普及に向けた取組み** 36
5.2. **バイオメトリクス製品データベースの構築・公開** 36
5.3. **ガイダンスや注意事項集などによる，バイオメトリクス・セキュリティに関する情報提供** 37
5.4. **脆弱性情報の取り扱い** 37
5.5. **精度評価の手法について** 37

1. 検討の背景と課題

1.1. 検討の背景

近年，我が国では生体情報を用いたバイオメトリック認証技術を用いた製品やシステムが普及してきている。例えば，2004 年から銀行の現金自動預け払い機（ATM）などにおいてバイオメトリック認証の導入が始まっている。暗証番号などは，類推されたり忘却してしまう可能性があり，カードなどは盗難などにあう可能性がある。バイオメトリック認証は，こうした欠点を補える本人認証手段として期待されており，今後，さまざまな分野で利用されることが予想される。

一方，バイオメトリック認証には，脆弱性となる可能性等の検討すべきセキュリティ上の課題も存在する。本研究会では，これらの課題に対する必要な取り組みを提言すべく，2006 年 3 月から検討を進めてきた。

（1）本人認証技術

本人認証の方式は，大きく 3 つに分類できる（表 1 -1 参照）。一つには，パスワードなど本人の記憶に基づき認証を行う方式であり，次には，身分証明カードなど本人の所持物に基づき認証を行う方式であり，そして三つ目には，本人の身体的または行動的特徴などの生体情報に基づくバイオメトリック認証と呼ばれる方式である。

これらの認証方式には，それぞれ利点と留意点が異なり，また，利用環境や運用方法による影響も考えられるため，利用目的などにあわせて，いずれかの方式を選択または組み合わせて利用することが多い。

表 1-1　認証技術の特徴

方式	具体例	主たる特徴	
		利点	留意点
記憶 (知識)	暗証番号，パスワード 質問応答 等	利用･変更が容易 広く普及 等	忘却の可能性 推測による攻撃が可能 ソーシャルエンジニアリングによる盗難　等
所持物	IC カード，身分証明書 磁気カード，USB トークン 携帯電話，パスポート 等	暗号技術が併用可能 操作が容易である 偽造対策技術が存在 等	暗号方式の強度に依存 紛失･盗難の可能性 スキミングへの警戒 製造･設置コストが必要　等
生体情報	指紋，掌形，虹彩 血管パターン，顔 声紋，筆跡 等	万人不同･生涯不変とされる(医学的な証明は未完) 忘却･盗難がない 偽造困難なものが多い 等	無効化が困難 偽造の可能性 心理的抵抗感　等

このうち第三のバイオメトリック認証は，近年，注目が高まりつつある。これは，身体的特徴や行動的特徴が本人以外持ち得ない情報であり，また，記憶や所持物と異なって忘却や盗難・紛失などの心配がないため，高いセキュリティレベルを実現するとユーザから期待されてからではないかと推測できる。一方，バイオメトリック認証が用いる生体情報のうち身体的特徴は生涯不変という特長も合わせ持つ。異なる見方をすれば，これは変更不可ということを意味しており，身体的特徴が何らかの手段により盗まれたり偽造されたりした場合のために，運用システム上の技術として，偽造物の検知や，登録情報の無効化などの対策が望まれる。

（2）バイオメトリック認証の普及と安全な運用

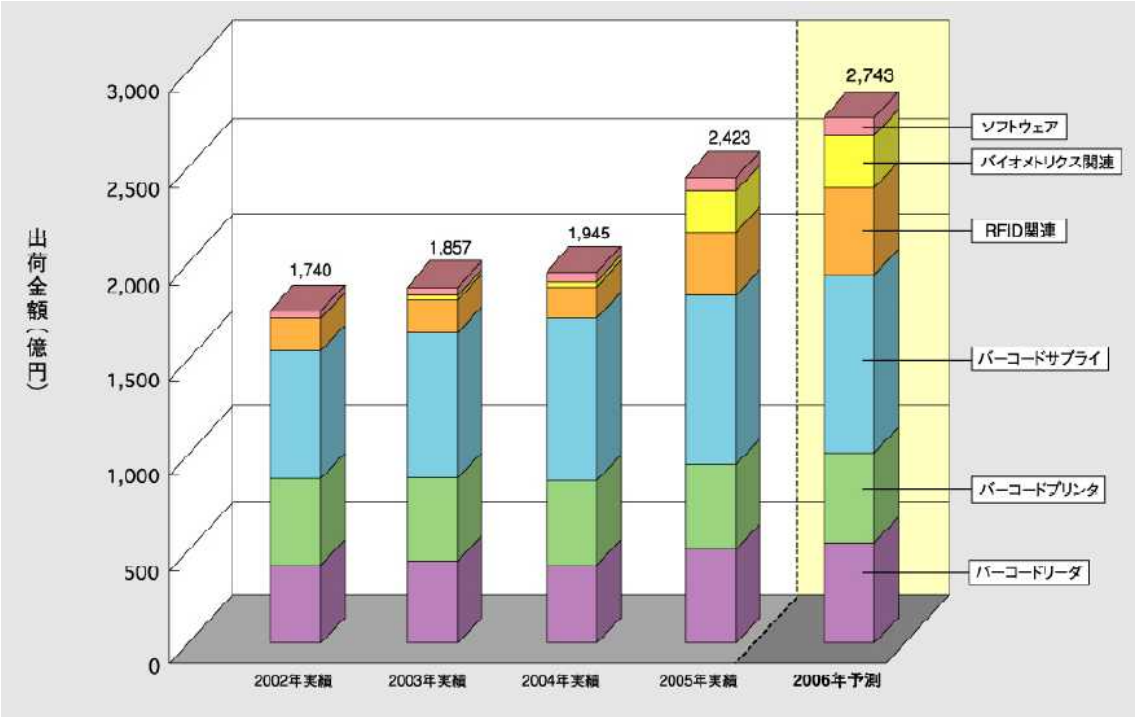
バイオメトリック認証技術は，物理的なセキュリティ管理を目的とした入退室管理などでの利用から，電子的なセキュリティ管理を目的とした情報システムや PC へのログイン時の本人認証などへ，その適用範囲が広がってきている。

我が国の市場規模を出荷金額の推移でみると，社団法人 日本自動認識システム協会（JAISA）[1]によれば 2002 年には指紋認証を中心として 7 億 6 千万円

[1] JAISA (Japan Automatic Identification System Association)

規模であったのが，2005 年には指紋認証のみならず静脈認証なども伸びて 210 億円規模と 26 倍以上に成長している。また，JAISA による資料では 2006 年は 274 億円規模とさらに拡大することが予想されており，市場規模が拡大していくと推測されている。（図 1 -1 参照）。

図 1 -1　バイオメトリクス関連他各技術における市場規模推移



注：2006 年度は JAISA による予測

出所：JAISA「統計調査委員会 活動報告 平成 17 年 1 月－平成 17 年 12 月 出荷数量・出荷金額」

バイオメトリック認証の適用が一般的な様々な用途に拡大していくと，ユーザもより広い層へと普及・増加することとなる。しかし，その際，前述の身体的特徴の盗難や偽造に対する対策を始めとするセキュリティ上の留意点が，新しい層のユーザに充分に理解されつつ広まるかという点については心配が残る。ここで，ユーザとは，認証をする本人（以下「利用者」という）のほか，バイオメトリック認証技術を導入したシステムを運用する者（以下「運用者」という）を含む。バイオメトリック認証の利点・留意点を十分理解せず，誤ったまたは不足した知識によって運用した場合，セキュリティ対策の観点から不十分なものとなりかねない。

人工物による生体情報の偽造のほか，登録された生体情報の改ざんなど，バイオメトリック認証における課題はこれまで指摘されてきている。バイオ

メトリック認証の普及とともに，セキュリティの観点からの研究も重要性が一層高まると予想できる。

（3）バイオメトリック認証の国際標準化に向けた取り組み

バイオメトリック認証に関連する技術の標準化については，国際標準化機関の様々な委員会で議論が行われている。

1）ISO[1]/IEC[2] JTC[3]1/SC37 での取り組みについて

ISO/IEC JTC1/SC37 はバイオメトリクスの基本技術について，ファイルフォーマットなどの電子的な規格から社会的，法的な観点に立った運用の問題までのさまざまなレベルの標準化を推進している。SC37 の活動の中でも，ISO/IEC 19794「バイオメトリックデータ互換フォーマット」，ISO/IEC 19785「汎用バイオメトリクス互換フォーマットフレームワーク」の規格は，ICAO[4]による電子パスポートの規格の中に取り込まれている。

日本では SC37 の議題を国内で検討する専門委員会を情報処理学会情報規格調査会内に設けている。専門委員会では，SC37 の議題を検討するほか，日本から新しい規格の提案を行うなど，積極的な活動を行っている。

2）ISO/IEC JTC1/SC27 での取り組みについて

ISO/IEC JTC1/SC27 では情報セキュリティ技術に係る案件として，セキュリティ要求条件，セキュリティサービスとそのガイドライン，セキュリティ評価基準に関する標準化活動を行っている。SC27 の成果には，一般的なセキュリティ技術に関する規格である，ISO/IEC 15408「セキュリティ評価基準」，ISO/IEC 15292「プロテクションプロファイルの登録手続き」，ISO/IEC 18045「セキュリティ評価方法論」，ISO/IEC 27001「情報セキュリティマネジメントシステム－要求事項」がある。

さらにバイオメトリック認証については，ISO/IEC 19792「バイオメトリクスの評価とテスト」として，セキュリティ関連項目の取扱いに対する基本方針が整備されつつある。そのセキュリティ評価を実施するための，SC27 とは別に 7 ヶ国からなるワーキンググループが ISO/IEC 15408 をバイオメトリックシステムに対して拡張した捕捉文書である BEM(Biometric Evaluation Methodology supplement)があるが，国際標準化に向けては SC27 内に Study period を設置し慎重に進める予定である。

---

[1] ISO(International Organization for Standardization)：国際標準化機構
[2] IEC(International Electrotechnical Commission)：国際電気標準会議
[3] JTC(Joint Technical Committee)：合同技術委員会
[4] ICAO(International Civil Aviation Organization)：国際民間航空機関

３）ISO/IEC JTC1/SC17 における取り組み

ISO/IEC JTC/SC17 ではカード及び個人識別に関する国際標準化を進めている。IC カードでのバイオメトリック認証技術の利用については，基本的な標準規格として 2004 年に ISO/IEC 7816 -11「バイオメトリック認証技術による個人認証」が発行された。機械読取渡航文書の標準である Doc 9303「入国審査･パスポートに関する規定」の制定は国連の専門機関である ICAO が行っているが，SC 17 は ICAO の唯一の公式リエゾンとして技術面で支援している。

４）ISO/TC[1] 68/SC 2/WG 10 での取り組みについて

金融サービスへのバイオメトリック認証技術適用の標準化は銀行業務を始めとした金融サービスを対象とする ISO/TC 68 の SC 2/WG 10 で進めている。金融サービスにおけるバイオメトリック認証技術のセキュリティに関する規格は，米国 ANSI X9.84 に基づいて ISO 19092 -1「セキュリティの枠組み」，ISO19092 -2 「メッセージシンタックスと暗号化機能の要求事項」が策定中である。

1.2. 本中間報告書の目的

バイオメトリック認証技術には，認証精度や本人認証のためのアルゴリズムなど，パスワード，暗号等を用いた他の認証技術と異なる独自の課題があり，国際標準化も進んでいる。一方，バイオメトリック認証技術が適用された製品やシステムは，既に我が国で普及しつつあり，広く利用され始めている。このため，本中間報告書では，多くの利用者が安心してバイオメトリック認証技術を利用できるように，バイオメトリック認証技術を安全に活用するときに必要となる知識を，国際標準化を踏まえた上で整理し，セキュリティ対策の観点から今後取り組むべき方向性と課題について検討する。

先ず，利用者にとっての安全なバイオメトリック認証技術の利用に向けた研究を行うための基礎知識的な事項として，２章でバイオメトリクス・セキュリティに関して，３章で認証精度評価に関して整理する。また，４章では本研究と並行して進めたバイオメトリクス製品の調査について，作成方法・コンテンツ内容などに関して記述する。最後の５章では，今後取り組むべきと考える課題をまとめる。

[1] Technical Committee

2. バイオメトリクス・セキュリティ

2.1. バイオメトリクス・セキュリティとは

本報告書ではバイオメトリクス・セキュリティ技術を，生体情報に基づく本人認証の実行を阻害する要因から保護する技術と定義する。阻害する要因とは，本人認証の実行環境に対する攻撃や，本人確認の判定を困難にする生体や物体の入力や実行環境である，バイオメトリクス・セキュリティ技術には，生体情報の漏洩を防ぐためのスキミング対策や耐タンパー技術，他人なりすましを防ぐための生体検知や他人受入エラー低減などの方式改善を含む。

従来我が国では，一般にバイオメトリック認証技術の議論は，主としてパターンマッチング技術に基づくバイオメトリック認証技術の面から捉えられてきた。これに対して，本研究会では，セキュリティの観点を考慮した技術および関連分野を捉え，これをバイオメトリクス・セキュリティという議論の枠組みとして検討を進めた。

2.2. バイオメトリック認証方式の特性

バイオメトリック認証では事前に登録した生体情報（テンプレート）と認証時にセンサによって取得した生体情報を比較することで，個人の特定を行う。異なる種類の生体情報を用いるバイオメトリック認証方式は，それぞれ異なった特徴を持っており，バイオメトリクス・セキュリティの確保の観点からバイオメトリック認証を利用する際はその特徴や課題に関して正しい知識を持っていることが望まれる。

バイオメトリック認証では，身体的特徴として，顔，指紋，静脈，虹彩など，行動的特徴として，署名，声紋，キーストロークなどが用いられている。バイオメトリック認証方式にはそれぞれのメリット･デメリットが存在する（表 2-1 参照）。このため，バイオメトリクス・セキュリティに対する攻撃への対策を実施する際には，こうしたメリット・デメリットを勘案しつつ，利用用途，利用環境などに適したシステムを選択する必要がある。

表 2-1　各バイオメトリック認証方式の特徴

モダリティ	メリット	デメリット
指紋	万人不同，終生不変 低コスト	指紋画像の品質 人工物による攻撃の可能性
網膜	認証精度が高い コピーが困難，非接触	専用装置が高コスト 疾病による変化
虹彩	認証精度が高い 眼球内部の疾病等の影響が無い	睫毛の影響を受ける 人工物による攻撃の可能性
静脈	非接触で認証可能 体内の情報のため盗まれにくい	太陽の直射光下では認証しにくい 怪我の際は認証できない
掌形	操作が容易 環境耐性が高い	信頼性の確保が必要 装置の小型化が困難
顔	心理的抵抗が少ない 不正抑止効果が高い	環境耐性が低い 時間･服飾等による変化
音声	非接触で認証可能 心理的抵抗が少ない	体調の影響 時間的な変化
筆跡	テキスト依存型 操作が容易	偽筆･模倣への対策が必要 認証者の状態により変化

バイオメトリック認証方式の特性による課題は，バイオメトリクス製品の設定・運用によって解決できる可能性がある。そのため，バイオメトリクス製品の利用者は，各バイオメトリック認証方式の特徴について，正しい知識を持つことが重要である。このためには利用者が正しい知識を持てるよう要点を整理することが望まれる。以下，バイオメトリック認証システムの一つのモデルを取り上げ，それに基づきバイオメトリクス・セキュリティに対する攻撃と対策を整理する。

2.3. バイオメトリック認証システムのモデル

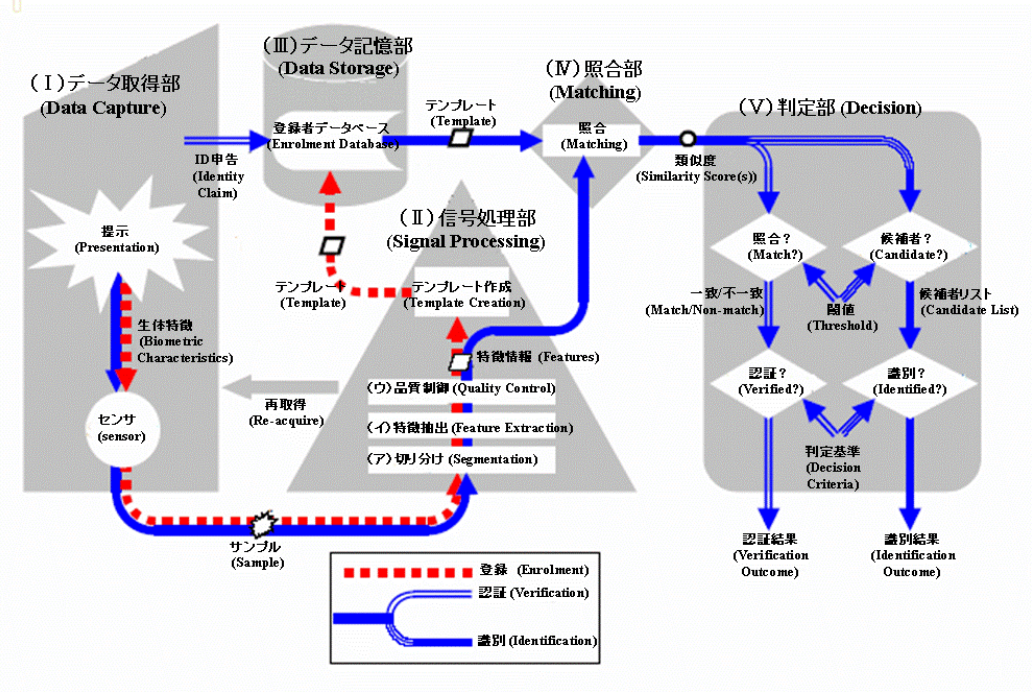
ISO/IEC DTR 24741[1]では，バイオメトリック認証システムのモデル化のために，バイオメトリック認証システムの機能を大きく五つに分類している。本節では ISO/IEC DTR 24741 を基とした，バイオメトリック認証の一連の流れ（図 2-1）を示し，各要素について説明する。

バイオメトリック認証では,登録時と照合時と処理の流れが異なり,さらに，照合時においても，正当な本人であると検証する「認証」の場合と，多数の登

[1] ISO/IEC DTR 24741 Information Technology – Biometrics Tutorial

録者の中から当該本人を抽出する「識別」の場合で流れが異なる。

図 2 -1　一般的なバイオメトリック認証システムの構成要素



(ISO/IEC DTR 24741 より。和訳は IPA)

（Ⅰ）データ取得

データ取得は生体特徴としてセンサに身体的・行動的特徴を提示することによって実現される。センサにより取得された生体情報は,サンプルとして,信号処理部に伝達される。なお,認証時は,生体特徴のセンサ提示に加えて,認証しようとする人の ID も入力し,あらかじめ登録し記憶された照合対象データを指定するためにデータ格納部に ID が伝達される

（Ⅱ）信号処理

信号処理では，人間から得た生体情報であるサンプルを特徴情報に変換する。信号処理で受け取ったサンプルは，特徴情報に変換するにあたり，大きく三つのステップを踏む。

（ア）　切り分け

一般にセンサが取得する情報は，人間の生体情報のみならず，周囲の雑音情報を含む。切り分けとは，照合に用いる顔や声などの生体情報を，背景や雑音などの環境情報と切り分ける処理のことを指す。

（イ） 特徴抽出

特徴抽出では，サンプルの中から生体特徴を抽出する。例えば指紋認証では指紋の映像から分岐点や端点を見つけ出し，その座標情報を求めるステップがこれに相当する。

（ウ） 品質制御

品質制御では，サンプルから抽出した生体特徴のデータの品質を確認する。品質制御では，サンプルや抽出した特徴に対し，照合を実行するのにふさわしい品質か否かをチェックする。

以上の三つのステップを踏んだ結果，照合を実行するために十分な特徴情報が得られなかった場合は，再度，生体情報を取得する。

（III）データ記憶

生体情報の登録時，登録者の生体情報はテンプレートに変換され，登録者のデータベースに記憶される。また，生体情報の照合時には，データ取得部から指定を受けた ID に基づいて，照合対象のテンプレートを取り出し，次の照合部に引き渡す。

（IV）照合

登録済みのテンプレートと，認証用に入力したサンプルの一致の程度を計算する。一致の程度は，類似度として数値として表現される。一般に，類似度は二つの生体情報が類似しているほど大きい値を持つ。

認証時は,指定された ID に対する生体情報と照合用に入力した生体情報の類似度が計算される。もし指定された ID に対して複数の生体情報が登録されていた場合や，照合用に生体情報が複数回入力された場合は，複数の類似度が計算される。

また，識別時は，照合用に入力した生体情報と登録者データベースに登録されたすべての生体情報との類似度が計算される。

何れの場合でも，照合部は，算出した全ての類似度を判定部に引き渡す。

（V）判定

照合部が出力した類似度をもとに判定を行う。

認証時は，先ず，照合部から引き渡された類似度が，あらかじめ設定された閾値を上回ったか否かを判定する。もし，引き渡された類似度が 1 つの場合はこの時点で本人と判定できるか否かが決定される。またもし引き渡された類似度が複数の場合は，複数の類似度の取り扱いについてあらかじめ定め

た判定基準に従って，本人と判定するか否かを決定する。判定基準には，例えば，閾値を上回った類似度が少なくとも 1 つあることや，閾値を上回った類似度が少なくとも 2 つあることなどが用いられる。そして，最終的に指定された ID に対する認証結果として OK もしくは NG を出力する。

識別時は，先ず，照合部から引き渡された複数の類似度のうち，あらかじめ設定された閾値を上回る類似度を抽出する。抽出した類似度を持つ登録者が識別の候補者となる。もし，候補者が 1 人の場合は，この時点で識別用に入力した生体情報に該当する本人の ID を特定でき，候補者が 0 人の場合は，本人を特定できなかったことが決定される。また,候補者が複数人の場合は，次に，あらかじめ定めた判定基準に従って本人に該当する ID を特定する。判定基準には，例えば，最も高い類似度が計算された生体情報の ID を本人と特定することや，最も高い類似度と 2 番目に高い類似度が僅差の場合は本人を特定しないことなどが用いられる。そして，最終的に識別結果として，本人と特定した ID もしくは本人を特定できなかったことを出力する。

2.4. バイオメトリクス・セキュリティの脆弱性となる可能性

バイオメトリック認証の実行における脆弱性となる可能性が，様々なメディアを通して言及されているが，その多くは脅威の大きさや対策と関係なく利用者の注意を促す範囲に留まっており，なかにはバイオメトリック認証の実行に対する不安や不信感を呼び起こすものもある。バイオメトリック認証技術の安全な利用を促進するためには，これらの脆弱性となる可能性を簡潔に整理し，利用者に必要な対策としてまとめ，理解が広がるようにする必要がある。

バイオメトリック認証の脆弱性となる可能性（Potential Vulnerability）は，SC27 を中心として整理が進んでおり，ISO/IEC 19792 バイオメトリック認証技術のセキュリティ評価(Security Evaluation of Biometrics)において，11 種類の脆弱性となる可能性が挙げられている。本節ではこれらの脆弱性となる可能性の紹介を行うと共に，前節で提示した一般的なバイオメトリック認証システムの簡単なモデル（図 2-1）に従って，脆弱性となる可能性とその原因となる処理部を示す。また，次節ではその対策についても言及する。

① 生体特徴の偽造

顔，指紋，虹彩など，身体的特徴に基づくバイオメトリック認証技術には，生体に似せた偽造物や，他人の生体情報をコピーした偽造物を作成し，それをセンサに感知させることで，他人になりすませる可能性がある。

原因となる処理部：データ取得（Ⅰ），特徴抽出（Ⅱ－イ）

② 生体特徴の模倣

声紋認証，署名認証，歩き方に基づく認証など，行動的特徴に基づくバイオメトリック認証技術には，他人の特徴を模倣することで，他人になりすませる可能性がある。

原因となる処理部：データ取得（Ⅰ），特徴抽出（Ⅱ－イ）

③ 生存判定の欠如

生存判定機能が弱いバイオメトリック認証技術では，生存中の生体と生存していない生体の区別をすることができないことがある。その場合，例えば指紋認証などでは，身体から切り離された他人の指を指紋センサに読み取らせることにより，第三者が他人になりすませる可能性がある。

原因となる処理部：データ取得（Ⅰ）

④ 生体特徴の秘匿不能性

顔，指紋，声など体の表面の生体情報は，一般の生活において他人に知られないようにすることが困難であり，第三者に盗まれる危険性がある。盗まれた生体情報は，①生体特徴の偽造や②生体特徴の模倣を通じて，他人なりすましに利用される可能性がある。

原因となる処理部：データ取得（Ⅰ）

⑤ 類似

生体情報の中には，親子，兄弟，双生児などの血縁者間で特徴が類似する場合がある。例えば，一卵性双生児は顔貌が似ていることが多く，顔認証で双生児を見分けることは原理的に不可能である。そのため，双生児間で互いになりすませる可能性がある。

原因となる処理部：データ取得（Ⅰ），特徴抽出（Ⅱ－イ），照合（Ⅳ）

⑥ 特殊な生体特徴

稀に通常に比べて多くの他人に照合してしまう人がいることがある。そのような人が見つかると他人なりすましやバックドアの生成に悪用される可能性がある。

原因となる処理部：データ取得（Ⅰ），特徴抽出（Ⅱ－イ），照合（Ⅳ）

⑦ 合成サンプル

ランダムに合成したサンプルが，信号処理部の入力データの仕様に合致すればシステムに受け入れられる場合がある。そのようなサンプルは登録者の何れかに偶然合致すると他人なりすましが起こる可能性がある。

原因となる処理部：信号処理（Ⅱ）

⑧ 予期せぬ環境

バイオメトリック認証システムが保証しない動作環境で動作させた場合，生体情報を正確に読み取れず，認証結果が不定になる恐れがある。場合によっては，認証精度が著しく低下し，他人なりすましの可能性が高くなる。

原因となる処理部：データ取得（Ⅰ），品質制御（Ⅱ－ウ）

⑨ 設定

一般的にバイオメトリック認証システムでは，登録済みの生体情報と認証用に入力した生体情報の一致は，二つの生体情報の類似度があらかじめ設定した閾値を上回っているか否かで判定する。そのため，不正によりその閾値を変更すれば，認証精度が著しく低下し，他人なりすましの可能性が高くなる。

原因となる処理部：判定（Ⅴ）

⑩ 低品質のテンプレート

生体情報のデータが低品質の場合，認証精度が低下することがある。そのため，低品質の生体情報が登録されている ID は，他人なりすましの可能性が高くなる。

原因となる処理部：品質制御（Ⅱ－ウ）

⑪ 生体情報データの漏洩と差し替え

バイオメトリック認証システムの各処理部の連結箇所には盗聴の危険性がある。また，連結箇所で不正なデータに差し替えられると，他人なりすまし

が起こる可能性がある。

原因となる処理部：各処理部の連結箇所

2.5. バイオメトリック認証システムに対する攻撃への対策

金融サービスへのバイオメトリック適用の標準化を行う ISO/TC 68/SC 2/WG 10 では，ISO/IEC FDIS[1] 19092 バイオメトリック技術の金融サービスへの適用 (Biometric Information Management and Security for the. Financial Services Industry)に準じて，バイオメトリクス・セキュリティの脆弱性となる可能性への攻撃とその対策が検討されてきた。バイオメトリック認証を安全に利用するためには，運用者と利用者が共にバイオメトリック認証の脆弱性となる可能性を理解し，その運用・利用に関して適切な取扱いをすることが重要である。本節では，攻撃への可能性と対策方法を紹介すると共に，前節で説明した脆弱性となる可能性との関係について整理する。本節で挙げる対策方法はそれぞれ独立した対策であり，併用することによって，さらにバイオメトリック認証のセキュリティを高めることができる。

（1）人工模造物による攻撃への対策

バイオメトリック認証システムへの既登録者が認証に使用している身体的特徴の情報を攻撃者が入手した場合，それを模倣した人工模造物を利用する事によって，他人受入エラーを発生させる可能性がある。

このような攻撃に対しては，人工模造物を利用させない，人口模造物によって登録者の生体情報を偽造させないことが重要であり，以下のような対策が考えられる。

- 生体検知などの模造品検出機能を付与し，人工物による登録・認証を防止する。
- 登録時，認証時の環境を監視し，不正行為を防止する。
- 生体情報の流出を防ぐため，他人に盗まれることの少ない人間の体内の生体情報に基づくバイオメトリック認証方式を利用した製品を用いる。
- データ格納へのアクセスに対するセキュリティを高め，既登録者の登録データの漏えいを防止する。
- テンプレートから生体情報を復元できないようなデータ登録方式を採用し，既登録者の登録データを保護する。

[1] Final Draft International Standard

対応する脆弱性となる可能性：①，③，④，⑪

（2）模倣による攻撃への対策

行動的特徴を用いたバイオメトリック認証システムにおいて，システムが登録している行動を，攻撃者が学習した場合，それを模倣する事によって，他人受入エラーを発生させる可能性がある。

このような攻撃に対しては，模倣させないこと，登録者を模倣するための情報を入手させないことが重要であり，以下のような対策が考えられる。

- データ格納へのアクセスに対するセキュリティを高め，既登録者の登録データの漏えいを防止する。
- テンプレートから生体情報を復元できないようなデータ登録方式を採用し，既登録者の登録データを保護する。
- 登録時，認証時の環境を監視し，不正行為を防止する。

対応する脆弱性となる可能性：②，④，⑪

（3）類似した生体情報に基づく攻撃への対策

外見的な相似，あるいはデータ的な相似により，他人受入エラーを起こしてしまう二人の既登録者の生体情報を，登録データ中に見つけることが出来れば，類似した生体情報を持つ他人になりすます攻撃を行うことができる。

このような攻撃に対して，以下のような対策が考えられる。

- バイオメトリック認証システム内の通信や処理の覗き見に対するセキュリティを高め，似た登録データの存在を隠匿する。
- 照合アルゴリズムの認証精度を高めることで，外見的な相似に対して，明確な相違点を判定する。

対応する脆弱性となる可能性：⑤，⑥，⑪

（4）ヒルクライミングアタックへの対策

バイオメトリック認証システムに人工的なデータを入力し，照合部の出力する比較結果が一致に近くなるように電子的な変更を繰り返すことで，他人受入エラーを起こすデータを生成する攻撃が存在する。

このような攻撃に対して，以下のような対策が考えられる。

- 比較・判定の出力が漏えいしないように，個々の機能のセキュリティを高める
- 信号処理及び比較の入力が差し替えられないように，暗号化などによるセキュリティを高める。

対応する脆弱性となる可能性：①，②，⑪

（5）センサの不正な設定や操作による攻撃への対策

仕様と異なる状態・環境においてバイオメトリック認証システムのキャリブレーションを行った場合，認証精度を低下する可能性がある。このような不正なキャリブレーションによって，他人受入エラーの発生率を上昇させることができる。

このような攻撃に対して，以下のような対策が考えられる。

- センサのキャリブレーション処理に環境の異常を検知する機能を組み込むことで，適切なキャリブレーション作業を行わせる。
- 信号処理時において，実行環境の確認機能を埋め込むことで，仕様外の環境での使用を防止する。
- センサのキャリブレーションは正しい管理者によってのみ行われるようにする。又は，複数の作業者によりキャリブレーション作業を実行する。
- 認証処理の実行環境を監視することで，仕様環境外で利用されていないことを確認する。

対応する脆弱性となる可能性：⑧

（6）認証判定閾値の変更による攻撃への対策

認証を行う際に基準となるテンプレートとサンプルの類似度の閾値を変更することで，他人受入エラー率を大きく変化させることができる。閾値を異常に低く設定することで，他人受入エラー率を上昇させることができる。

このような攻撃に対して，以下のような対策が考えられる。

- 認証精度判定の閾値変更処理に，異常な閾値の設定を検知する機能を組み込む。
- 認証精度判定の閾値変更は正しい管理者によってのみ行われるよう

にする。

対応する脆弱性となる可能性：⑨

（7）生体情報データの差し替えによる攻撃への対策

バイオメトリック認証システムに対して電子的な介入を行い，認証作業中に他人の ID と生体情報を，既登録者のものと差し替えることによって，攻撃者によって都合の良いバイオメトリック認証結果を出力する攻撃が行える。また，認証結果を改ざんすることでも，同等の攻撃が可能となる。

このような攻撃に対して，以下のような対策が考えられる。

- データ取得と信号処理間，あるいは信号処理と照合間にあるデータを保護するために，各処理間でやり取りされる情報を暗号化する。
- 正しい管理者によってのみ電子的な介入が行える等の，正しいルールに基づいた管理方針で運用する。

対応する脆弱性となる可能性：⑪

（8）その他の留意点に関して

バイオメトリック認証システムに登録を行う際に，他人になりすまして登録作業を行うことで,偽の ID 申告の基にテンプレートが作成される可能性がある。登録作業を行う際は手順を明らかにし，登録時の本人確認を厳重に行う必要がある。

バイオメトリック認証システムによっては，本来の登録作業とは別に，生体情報の更新手段や，緩やかに変化した生体情報への順応機能を用意するものがある。この機能を悪用し,登録者とは異なる生体情報を登録することや，異なる生体情報を用いて認証処理が繰り返された結果，順応機能によって既登録者のテンプレートが変更される可能性がある。テンプレートの変更を行う際には，更新者や操作者の正当性を確認する必要がある。

バイオメトリック認証技術で用いる生体情報はそれ自体が個人情報であり，個人情報保護法などの社会的側面から見ても重要な情報である。従ってバイオメトリック認証システムや認証精度とは別に，データ記憶部に格納された生体情報の管理は安全に行う必要がある。

2.6. まとめ

本節ではバイオメトリック認証の典型となるモデルを想定し，モデルの各部

分におけるセキュリティ上の課題と,それに関する対策について整理を行った。

バイオメトリック認証技術の脆弱性となる可能性は，認証システムの実装・運用などが不適切なときに高まる。これは，推測が容易なパスワードを設定してしまえばパスワード認証が脆弱なものになってしまうのと同様である。逆に，実装・運用を適切に行うことによって，そのリスクを軽減することができる。このため，バイオメトリック認証システムの利用者や運用者が，セキュアにバイオメトリック認証を行うためには，バイオメトリック認証技術のセキュリティ課題と対策についての知識を有することが必須である。

バイオメトリック認証システムを利用する上での留意点等を利用者・運用者に広く知らしめると共に，バイオメトリック認証の運用者や利用者が，利用用途に適したバイオメトリック認証技術を選べる環境を整備するべく，現在市場で流通しているバイオメトリック認証技術の製品調査を行った。この調査に関しては，本研究会報告書の４章において記述する。

3. 認証精度評価

3.1. 精度評価の背景

バイオメトリック認証では，別人を登録者と認識してしまう他人受入エラーや，登録者が本人と認識されない本人拒否エラーが起こりうる。これら 2 種類のエラーが起こる確率を，それぞれ，他人受入エラー率，本人拒否エラー率と呼ぶ。他人受入エラー率が高いと,他人なりすましが起こる可能性が高くなり，本人拒否エラー率が高いと，利用者の利便性が低くなる。原理上，この 2 つの確率はトレードオフの関係にあり，照合時に本人の受入を判断する閾値を増減させることで，他人受入エラー率と本人拒否エラー率のバランスを調整することができる。

重要な情報を管理するシステムや建物等のセキュリティ確保を主目的としてバイオメトリック認証を導入する際は，特に他人受入エラー率が注目される。そのため，セキュリティを追及して，他人受入エラー率が小さくなるように照合時の閾値を調整した場合,本人拒否エラー率が高まり利便性は落ちる。一方，利便性を追求して，本人拒否エラー率が小さくなるように調整すれば，必然的に他人受入エラー率が高まりセキュリティは低下する。

さらに，これらの認証精度は，照合に関わる閾値以外にも，導入場所の物理的な環境（湿度や照明など）や利用者の属性（年齢・性別等）にも影響を受ける場合がある。したがって，セキュリティシステムの構築上，バイオメトリック認証の他人受入エラー率と本人拒否エラー率の関係，および，導入環境の影響は，正しく把握されていなければならない。

一般に,認証精度は,サンプルを用いた実験により統計的に推定するもので，他人受入エラー率は本人の生体サンプルと他人の生体サンプルを照合させた回数に対して本人と他人が一致すると判断した回数の比率として計算し，本人拒否エラー率は本人の生体サンプルと本人が再提示した生体サンプルを照合させた回数に対して本人と判断できなかった回数の比率として計算する。そのため，安定した結果を推定するためには，偏りのない環境で収集された，数多くの背生体サンプルが必要である。しかし，実際には，そのような条件の生体サンプルの収集には多くの労力とコストを必要とするため，小規模な研究機関や企業では現実的でない。

各国の認証精度評価の状況をみると，評価用の指紋等のサンプルを一般協力者から収集した生体情報 DB を構築しているケースが見られる。IPA が 2005 年度に実施した「バイオメトリクス評価に関する調査」では，アメリカ，イギリ

ス等，5 カ国の 12 件のプロジェクトについて調査した。このほか，ITIRT[1]，CBT[2]といったバイオメトリック認証技術の評価プロジェクトが進行しつつある。こうした事例を見ると，国際的には第三者検証機関があるようにも見られる。

このため，本章では，まず，各国のプロジェクトの動向を調査し，わが国として，ユーザにとって望ましい精度評価のあり方の方向性について整理することとする。

3.2. 各国の動向

バイオメトリクス製品の認証精度評価についての各国の動向について，IPA では従来，調査事業「バイオメトリクス評価に関する調査[3]」などにおいて，世界各国の実施例を調査・整理してきている。これらに加えて，本研究会では，米国の民間コンサルティング会社による事例，英国における実証実験の事例，日本におけるデータベース構築事例についても調査した。先の調査と合わせた調査の範囲を表 3 -1 に記す。表中*が付記された項目が，新規に調査した事例である。

表 3-1 調査の範囲

実施国	機関	実施プロジェクト
米国	国防総省	FERET[4]（顔）
	国立標準技術研究所（NIST）	FRGC[5]（顔），FRVT[6]（顔），FpVTE[7]（指紋），Speaker Recognition Evaluation（声）
	IBG[8]	ITIRT[9]*（虹彩），CBT[10]*（マルチモーダル）
米国+イタリア	ミシガン大（米），サンノゼ大（米），ボローニャ大（伊）	FVC[11]
英国	英国旅券発給課（UKPS）	顔，指紋，虹彩の実証実験*

1 Independent Testing of Iris Recognition Technology
2 Comparative Biometric Testing
3 バイオメトリクス評価に関する調査，独立行政法人 情報処理推進機構，2005 年 3 月
http://www.ipa.go.jp/security/fy16/reports/biometrics/documents/biometrics2004.pdf
4 Face Recognition Technology
5 Face Recognition Ground Challenge
6 Face Recognition Vendor Test
7 Fingerprint Vendor Technology Evaluation
8 International Biometric Group
9 Independent Testing of Iris Recognition Technology
10 Comparative Biometric Testing
11 Fingerprint verification Competition

実施国	機関	実施プロジェクト
韓国	韓国情報保護振興院（KISA）	指紋 DB， 顔 DB， 認証精度評価ツール
	バイオメトリックエンジニアリング研究センター（BERC）	マルチモーダル DB
中国	中国科学院（CAS）	虹彩 DB
日本	ソフトピアジャパン HOIP	顔 DB*

これらの事例からみられることはバイオメトリクス製品の精度評価を実施する場合，認証精度を測定するための多くの生体情報が必要となるということである。次節以降では，精度評価を行うための生体情報を収めた生体情報データベース（以下，生体情報 DB と略）の調査・分析を行い，我が国における認証精度評価の課題についての整理を行った。

3.3. 認証精度評価に向けた生体情報 DB に対する分析

表 3-1 に挙げるプロジェクトについて，認証精度評価に用いる生体情報 DB としての有効性の観点から分析を行った。これらには，予め用意された性能評価用の生体情報 DB を用いて実施されたプロジェクトの他,プロジェクトの目的に適う生体情報 DB がないか，あるいは，登録拒否に関する評価といった予め用意された生体情報 DB を用いては評価ができない目的のため,生体情報データを参加者から収集し,一時的に生体情報 DB を構築して活用したプロジェクトなどがあった。以下，利用目的，特殊性などに関して整理した。

（1）利用目的

認証精度を測定するために利用される生体情報 DB は,利用目的に合わせて，「研究開発用生体情報 DB」,「コンペティション用 DB」,「調達者検証用生体情報 DB」3 種類に大別されると考えられる。以下，3 種類の利用目的に相当する例を示す。

(a) 研究開発用生体情報 DB の例

研究開発用生体情報 DB とは，研究開発機関が研究・開発したバイオメトリック認証技術の有効性を評価するなどの認証精度評価を実施するために構築された生体情報 DB である。

韓国のバイオメトリクスエンジニアリング研究センター（BERC）において構築中のマルチモーダルデータベースは研究開発用の DB に相当する。BERC は Yonsei 大学内に 2002 年に設立されたバイオメトリック認

証技術に関する研究センターであり,韓国科学財団から毎年 100 万ドルの資金援助を受けている。BERC が構築中の生体情報 DB は韓国内の研究開発機関が利用する。

当該マルチモーダルデータベースは 2004 年から 2009 年までの 6 ヵ年計画として構築中のものであり，指紋，顔，虹彩，音声の 4 つの生体情報について，2000 人規模のデータベースの構築を目指している。経年変化を含むデータベースとするため,各被験者に対し 2 年毎にデータ収集を行なっているのも特長である。

他にも日本の財団法人ソフトピアジャパンが構築した顔画像 DB がこれにあたる。ソフトピアジャパンは人間とコンピュータの高度なインタラクションの研究の中で,画像センシング技術により人間の顔をセンシングし,従来に無い新しいヒューマンインタフェースの実現を目指した。そのために 15 歳から 64 歳まで計 300 人の様々な顔の向きの画像が計 306,000 枚撮影されたが，これは顔認証の研究開発にも十分転用可能である。

(b) コンペティション用生体情報 DB の例

コンペティション用生体情報 DB とは，バイオメトリック認証技術の完成度を競わせるため,認証精度ベンチマーク用に第三者が構築した生体情報 DB である。

米国ミシガン州立大学，米国サンノゼ州立大学，伊ボローニャ大学の 3 大学に属するバイオメトリック関連研究組織が主催する指紋認証技術コンテスト FVC で用いられた指紋 DB はコンペティション用の DB の代表的な例に相当する。FVC は,2000 年より 2 年毎に開催されている。2006 年にも開催予定となっている。

FVC で用いられる指紋 DB は，複数方式のセンサを用いて収集されている。DB 規模は大きくないが，低品質指紋も含まれており，ロバスト性評価（不鮮明な画像に対する生体特徴抽出率）も考慮されている。

コンペティションを目的としているため，指紋 DB そのものは公開されていないが，アルゴリズムを指紋 DB に適合させるためのチューニング用のサンプル DB が参加者に公開されている。

FVC の評価結果は，あくまでもコンペティションとしての結果であり，実運用時の性能の優劣を示すものではない点に注意が必要である。

(c) 調達者検証用生体情報 DB の例

調達者検証用生体情報 DB とは，自らバイオメトリック認証技術を利用するために,調達者もしくは調達者の代理者が認証精度評価を実施するために構築された生体情報 DB である。

米国において実施された顔認証ベンダテスト FRVT，指紋認証ベンダ技術評価 FpVTE で使用された DB は,調達者検証用の生体情報 DB に相当する。米国政府が調達者として主導し，認証精度評価を実施したものである。評価代行者は NIST である。米国のパトリオット法（反テロリズム法）により NIST を評価機関として指定した上で，資金およびデータそのものを提供している点が特徴といえる。

FRVT は，2002 年と 2005 年に実施された顔認証ベンダテストであり，多量のデータが収集されている。FRVT2002 においては，37,437 人の被験者から，姿勢，照明といった変動要因を考慮したデータを 121,589 枚収集している。FRVT2005 においては，データベースサイズは 50,000 枚程度であるが，高精細画像や 3D データも含まれており，それらの認証精度への寄与率を確認したい調達者側の意図が確実に反映された DB となっている。

FpVTE は，指紋認証の技術評価を目的としたものであり，FRVT 同様 DB サイズは大きく，25,309 人の被験者から収集された 393,370 枚のデータが用いられている。これらのデータが調達者側から提供されているのも特長である。

他にもアメリカの ITIRT,英国の UKPS の行った実験もこれにあたる。

（2）認証精度評価用生体情報 DB の特殊性

今回の調査した範囲では，個々の取り組みで，それぞれの目的に合致した生体情報データベースの利用／生体情報データ収集が行われていた。そして，既存の生体情報データベースの流用や他目的で使用している生体情報データの利用などは行われていなかった。バイオメトリクス製品の認証精度は標準的な生体情報データベースを用意すれば測定可能と思われがちだが，多くの目的に対応する万能な生体情報データベースの構築が困難であること示していると考えられる。

バイオメトリクス製品は，生体情報を取得するセンサ／カメラと登録／照合ソフトとの組み合わせでの結びつきが強く，また，生体情報を取得する際の運用環境による影響や利用者（被験者）の人的要因による性能への影響が非常に大きい。そのため，個々のバイオメトリクス製品は，各々組み合わされるセンサ，運用環境，利用目的，ユーザの人口構成等に合わせ，最高性能が発揮できるよう，ハードウェアおよび登録／照合ソフトウェアの両面で最適チューニングが施されている。

この特殊性により，中立的な第三者が精度評価を行うといった利用のための「標準的な生体情報データ」を活用可能な状況は，その生体情報を取得し

た際の運用環境や，ソフトウェア，センサなどの組み合わせが一致または近似していることが条件となり，かなり限定的になってしまう。そのため，様々な用途で利用可能な「万能な標準的な生体情報データベース」のような形で整備することは相当難しいと考えられる。

（3）生体情報の品質について

バイオメトリック認証の認証精度は 3 節で述べたように環境等によって大きく影響を受ける。ISO/IEC 19795-1 において，具体的には影響を受ける因子として，①被験者構成の統計量，②アプリケーション，③ユーザの身体的状態，④ユーザの行動的状態，⑤ユーザの見かけの状態，⑥周囲の状態，⑦生体情報を取得するセンサやハードウェア，⑧ユーザインタフェースがあげられている。以上の異なる影響因子の下で収集された生体情報から成る生体情報 DB に対して同一のバイオメトリック技術を適用すると，異なった認証精度が測定される。したがって，測定された認証精度は，測定に用いられた生体情報 DB の品質と合わせて理解されるべきである。さらに，測定に用いられた生体情報 DB の品質を，多くの人が容易に理解できるようにするためには，生体情報 DB の品質が，定量的に測定され，数値として表されるべきである。

しかしながら，バイオメトリックサンプル（バイオメトリクス製品に登録された生体情報）の品質を定義するものは未だ標準化されていない。ISO/IEC 19785 Common Biometric Exchange Formats Framework， Part 1: Data Element Specification で記載されている生体情報データの共通フォーマット中では，バイオメトリックサンプルの品質を記述する欄は用意されているが，それを算出するためのアルゴリズムや方法については規定されていない。

バイオメトリックサンプルの品質を算出することにより，そのバイオメトリックサンプルを認証に用いた時の認証精度を推定することが出来る。また，バイオメトリックサンプル品質を用いて，認証精度評価に用いた認証精度評価用生体情報 DB の難易度を算出することも可能になる。

2006 年から ISO/IEC JTC1 SC37/WG3 において，バイオメトリックサンプル品質に関する標準化活動が ISO/IEC29794 シリーズとして正式に始まった。現在は，ISO/IEC29794-1　バイオメトリックサンプル品質 - フレームワーク，ISO/IEC29794-4　バイオメトリックサンプル品質 - 指紋画像，としてフレームワークと指紋画像の品質について規格化が進んでいる。顔画像の品質についても，今後，ISO/IEC29794-5 として規格化が進む予定である。

顔画像の撮影方法については，品質に関する標準化よりも先に，ISO/IEC 19794-5 Amd.[1]1 顔画像撮影ガイドラインとして標準化が進んでいる。この規

[1] Amendment（修正）

格では，フォトブース（証明写真ボックス）や写真スタジオで機械的な顔認証を行うのに適した顔画像を撮影するための条件が規定されている。

今後，バイオメトリックサンプル品質の算出方法が標準化されれば，認証精度評価に用いた認証精度評価用生体情報 DB の品質を算出することも可能になる。そこで初めて，各提供者が製品評価に用いている認証精度評価用生体情報 DB の比較を行うことも可能になる。早期の標準化が期待される。

3.4. 認証精度評価および生体情報 DB 構築における留意事項

バイオメトリック認証技術の認証精度評価に対しては，何のために認証精度評価を行うのかという目的を明確にして，目的ごとに認証精度評価用生体情報 DB や試験方法，試験環境を用意する必要がある。

認証精度評価用生体情報 DB の構築を検討する場合，先ず，構築する生体情報 DB の利用目的を明らかにすることが重要である。また，既に構築した生体情報 DB においては，その生体情報 DB の構築目的と測定できる質を明らかにすることが重要である。

以下,認証精度評価および認証精度評価用生体情報 DB 構築に向けた留意事項を列挙する。

（1）生体情報 DB 構築方針の明確化

認証精度評価は評価の目的に合ったデータを使用する必要があり，評価用の生体情報 DB も評価の目的に合った採取条件と品質で構築しなければならない。

このために，生体情報 DB を構築する際には，実施者，目的，測定する生体情報認証方式，使用するセンサ（一部のバイオメトリック認証方式ではカメラのこと），採取環境，生体情報データの品質，規模など，予め定義が必要となる項目はどの様なものかを明らかにする必要がある。また，認証精度評価を行う上で重要である項目について，個々の項目の条件を明確に定める必要がある。

（2）プライバシーへの配慮

生体情報 DB の利用／運用にあたっては,生体情報自体が備え持つ個人情報という性格を充分に理解し，その生体情報 DB の利用，第三者への提供，二次的利用などにあたっては，慎重な取り扱いが必要になる。このことは，生体情報 DB 構築の際にも非常に重要な点である。構築時に個人情報への充分な配慮をすることで，利用の際の生体情報の扱いへの制限が軽減される場合も考えられる。

（3）最新技術との整合性

構築当初に要求条件や環境条件の明確化が充分に行われた生体情報 DB を整備したとしても，その後の技術の進歩により，最新技術に即した形で生体情報の条件の見直しが必要になることが考えられる。同様の評価目的に利用する場合であったとしても，常に最新技術動向を確認し，必要に応じて保守をすることが必要になる。また，バイオメトリック認証技術の進歩により，認証精度が著しく向上した場合などには，バイオメトリック認証技術の認証精度評価において統計的な処理が必要となるという性格上，必要となる生体情報のデータ数自体が大幅に増大することも考えられる。このような点にも考慮し，必要に応じて，生体情報 DB のデータメンテナンスを行うことが重要である。

（4）技術開発をした当事国以外の人の生体情報

認証精度は被験者集団の人種等の構成にも影響を受ける。国内ベンダが国内で取得した評価サンプルを用いて開発した装置を，国外で利用する場合及び国内でも当事国以外の人が主に利用する場合などが考えられるので，認証精度を正確に測定するためには，製品を開発した当事国以外の人のデータを用いた評価も必要である。

（5）コスト

生体情報 DB の構築にはコストがかかる。認証精度を測定するためには精度に応じたデータ数が必要であり，高い認証精度を測定するためには甚大なコストが必要である。大規模な生体情報 DB を一つの機関で整備することはコスト上，負担が大きいことに留意する必要がある。

（6）評価できるバイオメトリック技術の範囲

生体情報 DB の生体情報は，生体情報を取得した時点で，生体情報を取得したセンサや取得時のインターフェースなどの取得条件が不動となる。すなわち，取得条件を後から変更することはできない。生体情報 DB を用いて評価できる認証精度は，生体情報を取得した条件に限った場合の認証精度であり，他の取得条件に対する評価はできない。逆に，当該取得条件内に限定すれば，取得後の処理を変更した再評価を行える。変更可能な項目は，生体情報の特徴データへの変換，特徴データ間の照合など，主に照合アルゴリズムに関わる処理である。したがって，生体情報 DB は，照合アルゴリズムの研究開発において再利用可能という意味で有用である。

3.5. まとめ

認証精度評価について各国のプロジェクトの動向を調査した結果，多くのプロジェクトが生体情報 DB を用いて評価を行っており,それら生体情報 DB は「研究開発用生体情報 DB」,「コンペティション用 DB」,「調達者検証用生体情報 DB」に大別できることがわかった。一方，バイオメトリック認証技術の認証精度は測定環境が異なると，大きく変化する可能性がある。したがって,「研究開発用生体情報 DB」や「コンペティション用 DB」を用いて測定した認証精度は運用環境における認証精度を保証するものではなく,「調達者検証用生体情報 DB」も，異なる利用環境の，他の調達者が活用できるものではない。すなわち，生体情報 DB を構築して，第三者が運用環境における認証精度を測定し，中立の立場で保証する，または，認証するということは成立し難い。むしろ，生体情報 DB は，運用環境とは切り離し，バイオメトリック認証技術のパターンマッチング機能の研究開発・評価の観点で構築することが望ましい。

生体情報 DB の構築に必要とされるコストの大きさを考えると，生体情報 DB を頻繁に再構築することは現実的でない。将来的に再利用されることを踏まえて構築することが望まれる。その一つとして，収集したセンサや収集時のインターフェース，また，生体情報を提供した被験者の情報（性別，年齢，職種など）などを記録しておくことが重要である。また，生体情報 DB が数多く構築された場合，再利用可能な生体情報 DB を容易に探索できるように，生体情報 DB の所在などの概要に関する DB が存在すると有用である。他国の生体情報 DB をも参照できるように，生体情報 DB の概要に関する DB がグローバル規模で構築されることも望ましい。

近年，バイオメトリック認証製品が広く普及してきた。現在のところそのような製品の認証精度はベンダが独自に評価しているのが主流である。独自評価のため，具体的な装置の機能構成・試験方法・環境・被験者・運用など精度の値に影響する項目が統一されていないため，複数の製品を横並びに比較するのは事実上不可能である。

また，バイオメトリック認証の運用において，ユーザは，ユーザが求める認証精度（要求精度），認証時間（要求認証時間），操作性，利用環境などの機能要件と，本人拒否エラー率，対応率（装置あるいはアルゴリズムが生体情報を認識できない割合）などの利便性要件を規定する。一方，当然のことながら，ベンダが認証精度を評価する際の評価環境は，各ベンダが独自に設定しているため，ユーザの要件に合致することは稀である。長期的には，各ベンダの製品がユーザの要件に合致するか否かを評価する方法の検討を始めとして，ユーザの要件とバイオメトリック認証製品の認証精度のギャップを，ユーザとベンダが協力して理解し合うことも期待される。

4. 製品データベースに関する検討

4.1. 背景

バイオメトリクスのセンサや照合ソフトウェアなどの製品の現状を調査するため，アンケートによりバイオメトリクスの製品情報を収集した。本章ではこの調査の目的，方法及び結果について述べる。

生体情報を利用した個人の認証を可能とするバイオメトリック認証システムが普及し始めて来ているが，安心してバイオメトリック認証技術を使用するためには，導入にあたり，セキュリティ，認証精度の観点で充分に検討された製品を選択できることが必要である。しかしながら，セキュリティや認証精度は評価が確立しておらず，一般ユーザが容易に理解し，確認できる情報が提供されているとは限らないと考えられる。そのような状況をふまえると，まず利用者が仕様について共通な項目について確認することができるような形で，国内のバイオメトリック認証技術の情報を閲覧できるような仕組みを用意することが，バイオメトリック認証システムを適切に導入できるための第一歩と考えられる。そのためバイオメトリクスの製品情報を収集した。

本アンケート調査は照合ソフトウェアおよび照合ソフトウェアを組み込んだ装置を対象にしており，バイオメトリック認証技術を含んだアプリケーションは対象外である。アプリケーションを対象とした調査は，本調査の結果を参考として，別途検討していきたい。

4.2. 収集情報

製品情報の収集を対象とする製品は，生体情報の照合機能を実現するセンサやソフトウェアそのものが製品となっているものであり，国内で一般ユーザおよびシステムインテグレータが入手可能なものであることを条件とした。

収集した製品情報は一般ユーザへの公開を前提としている。収集にあたってはベンダから，以下の項目を前提として情報提供を求めた。

- 収集した製品情報は，例えばバイオメトリクス製品情報データベース（以下，６項まで製品情報 DB と略）の形で，IPA のウェブサイトを通して一般に公開する事が望まれる。閲覧者は，購入を検討するユーザを想定としている。
- 対象とする製品は，Software Development Kit(SDK)[1]レベル相当以上のバイオメトリック認証機能（生体情報の登録，照合）を有している製品であ

[1] SDK：ソフトウェアを開発する際に必要なツールのセット

る（PC の CPU で照合するタイプの周辺機も含む）。デバイスのみ，サービスコンサルタントのみ，認証精度評価用生体情報のデータベース構築のみなどの製品は対象としない。

・製品情報 DB には，ベンダから提供される情報をすべて記載する。また，各製品の評価など，ベンダから提供されない情報は，追記しない。

・製品情報は，カタログに記載されている注意事項，例外事項などもすべて提供してもらう。不明な点があった場合は，質問等をすることがある。また，他ベンダ製品の情報など，不適当と判断した情報は修正を要求することがある。

・ベンダが提供した製品情報は，随時，修正，削除，追加に応じる。

・製品情報 DB の公開にあたっては，上記の五つの条件に基づいて情報収集したものであることを明記する。

4.3. アンケート項目

製品情報はベンダにアンケートに記入する形で回答を求めた。アンケート項目は，国内の製品を踏まえ，認識方式，コスト，利用用途，バイオメトリック認証技術の他の機能との組合せを明らかにするために必要な項目として決定した。

アンケート中，製品名，モダリティなどの基本情報，アンケートを記載した情報提供の責任元となる連絡先は，回答必須とし，その他の項目は任意回答とした。また，連絡先は個人情報を含むため，製品情報の公開においても非公開とした。

以下，各項目を説明する。

（1）基本情報

製品を一覧するときに，各製品を識別するための項目，および，各製品の概略を知るための項目である。

＜回答項目＞

製品名・概要・モダリティ・代表型格・利用用途・利用目的

（2）概要

ユーザが製品の導入を検討する際に参考となる，一般的にカタログに記載される項目である。

＜回答項目＞

写真・サイズ・重量・電源条件・インターフェース条件・利用環境・適合した試験

（3）センサ

製品がセンサを持つ際，センサに使われている技術の概略をユーザが理解するために設けた，センサ技術の基本的な情報に関する項目である。

＜回答項目＞

方式名・方式概要・特長

（4）照合アルゴリズム

生体情報の照合を求めるアルゴリズムの概略をユーザが理解するために設けた，照合アルゴリズムの基本的な情報に関する項目である。

＜回答項目＞

方式名･方式概要・特長

（5）システム

ユーザが各製品をシステムとして導入する際に参考となる項目，および，運用の参考となる項目である。

＜回答項目＞

標準的な構成および付帯条件・一人当たりのデータサイズ・利用可能人数（標準・最大）・スループットの目安（標準・最大）・処理時間（登録時・照合時）・1:N への対応・認証精度調整の可否・ネットワーク構成・連携できる他のシステムの製品名・他の認証方式との連携・導入事例

（6）認証精度（ベンダ評価）

ベンダが評価した認証精度の回答を求める項目である。測定条件も合わせて回答を求めることで，回答された認証精度の確からしさを確認することができる。認証精度の測定と報告は 1:1 認証が対象となっているため，本アンケートの回答も 1:1 認証の認証精度のみについて回答を求めた。認証精度については，装置（ベンダ）が保証する保証精度と，利用者側の機能要件と利便性要件により分析されたリスクに基づき算出される要求精度がある。本項目に記載されている認証精度は保証精度である。

＜回答項目＞

本人拒否エラー率・他人受入エラー率・登録失敗率・生体情報取得失敗率・評価手法・テストの種別・登録条件・照合条件・試験回数・測定用データベース

（7）認証精度（第三者評価）

ベンダ以外の第三者がベンダの技術の認証精度を測定した結果を記載する項目である。

＜回答項目＞

評価者・評価レポートの入手方法・評価手法（概要）・評価結果（概要）

（8）特記事項

本アンケートに用意された項目以外でベンダが自由に製品の補足説明を行う項目である。

＜回答項目＞

カタログ記載事項・カタログ以外の補足事項・公開情報

（9）販売

ユーザが購入を検討する際に参考となる製品の販売に関する情報を記載する項目である。

＜回答項目＞

価格・販売実績・販売方法・最新情報（URL）・問合先

（１０）記載日

本アンケートの記載内容を時間軸の上で保証するための項目である。

＜回答項目＞

記載日

（１１）連絡先（情報責任元）

本アンケートの内容を確認する場合の問い合わせ先に関する情報である。本情報は調査の遂行上回答必須とした。また，個人情報を含むためユーザに対して非公開とした。

＜回答項目＞

企業名・部署名・担当者名・郵便番号・住所・電話番号・FAX 番号・メールアドレス

4.4. 収集方法

製品情報の収集にあたっては，①製品情報収集の告知，②製品情報アンケート用紙の配布，③製品情報アンケートの回収の手順を踏んだ。

（1）製品情報収集の告知

製品情報収集の告知は,案内文を IPA から ISO/IEC JCT1/SC37 国内委員会，

BSC（バイオメトリクス・セキュリティ・コンソーシアム），JAISA（社団法人日本自動認識システム協会）バイオメトリクス部会にメールにて依頼した。この方法により，SC37 国内委員会，BSC，JAISA バイオメトリクス部会に参加しているベンダには製品情報収集が依頼された。また，その他のベンダに対しては，SC37 国内委員会，BSC，JAISA バイオメトリクス部会の会員の協力により，製品情報収集を直接依頼した。

（2）製品情報アンケート用紙の配布

製品情報アンケート用紙は，製品情報収集の調査依頼を受けて IPA に回答する旨の返答のあったベンダに配布した。製品情報の記入にあたっては BSC において， バイオメトリクス製品 DB 調査 TF(タスクフォース)を設立し，説明会を開催した。

（3）製品情報アンケートの回収

製品情報アンケート用紙を受け取ったベンダは，記入後，記入済みのアンケート回答および製品概観写真，カタログなどの補足資料を IPA に送信することで製品情報アンケートの回収を行った。

4.5. 収集情報の確認

回収した製品情報アンケートは，記載に不備がないか確認した。例えば，認証精度については，測定時に実施した試験回数で計測できる測定限界値を下回っていないか，試験回数と測定に用いたデータの数の間に不整合はないか，などを確認した。

4.6. 収集結果

収集した製品情報の数は 57 であった。国内の指紋，掌形，虹彩，顔，静脈，音声，署名のモダリティに関する製品の情報を収集した。2005 年版バイオメトリクス市場白書に記載されている製品数は 42 であり,主要製品はカバーできたと判断する。

4.7. 公開検討

バイオメトリック認証技術は，運用製品を利用する環境や利用者によって性能に大きく差が出る可能性がある。従って，各ベンダの認証技術の比較・検討を行う際は，各ベンダが提示する認証精度の数字の大小だけではなく，認証精度を測定したときの条件なども考慮する必要がある。そのため，公開時には，

一般ユーザが製品情報を誤解なく容易に理解できるように，アンケート項目の意味を始めとして，製品データの読み方などの情報提供が必要である。

4.8. まとめ

バイオメトリック認証技術の製品の現状を調査するために，アンケートの形式にて製品情報の収集を行った。その結果，指紋，掌形，虹彩，顔，静脈，音声，署名のモダリティに関する 57 製品の情報を収集することができた。

このたびのアンケートでは，基本情報と連絡先のみ回答必須とし，認証精度を含めて，その他すべての項目を回答任意とした。そのため，ベンダのポリシーによっては，回答の無い項目もあった。一方，バイオメトリック認証技術を利用するユーザにとっては，無回答の項目は少ない方が良い。今後は，より多くの情報を掲載できるように，本データベースの有用性についてベンダの理解を得ることも検討していきたい。その手段には，アンケート項目の適切な説明を増やして製品情報データベースの利用価値を高めることなども検討の対象として考えられる，

他方，アンケートの回答内容はベンダを信用し，内容の正確さを検証しなかった。検証には，特許，論文により示された方式や認証精度の回答結果が実際の製品と一致するかを確認することなどが含まれる。このような課題に対しては，製品情報の検証になるルールの設定・明確化に関して，引き続き議論をしていく必要がある。既に，国際標準化の場では，ISO/IEC 19795 で認証精度の測定と報告が，ISO/IEC 19792 でセキュリティの議論が進んでいる。同国際標準の策定にあわせて議論を進めることで，ユーザおよびベンダの双方にコンセンサスが得られた，より詳細な製品情報をまとめられることが期待できる。

5. バイオメトリクス・セキュリティの今後の課題

研究会で議論に上がった，今後，さらに検討を行うべき課題の中で特に継続して議論を進めるべき課題は以下のとおりである。

5.1. ユーザへのバイオメトリック認証の普及に向けた取組み

セキュリティ対策としてバイオメトリック認証を利用する場合，利用者のなりすましに対しては堅固な安全性が実現できる一方で，認証に利用する生体情報（身体的・行動的特徴）そのものが個人情報であることから，その管理や，認証精度を左右する本人判定閾値の作為的な調整といった新たなセキュリティ上の留意事項が生じる。バイオメトリクス製品を利用する上で，システム設計者，システム運用者及び利用者はこれらのセキュリティ上の留意事項に関して正確な知識を持ち，必要な対策を実施する必要がある。今回の研究会ではバイオメトリック認証の長短を整理し，ユーザ（運用者ならびに利用者）が知るべき技術知識をまとめた。

具体的にはバイオメトリック認証を扱う国際標準化団体や他の諸団体の活動を調査し，バイオメトリック認証をセキュリティ分野で利用する際の課題を整理した。特に，バイオメトリック認証の脆弱性となる可能性（Potential Vulnerability）に関して研究会で情報収集と分析を実施し，セキュアなバイオメトリック認証システムの構築にむけて必要な知識を整理した。

これらの成果については，ユーザにわかりやすい形で速やかに Web 等を通じて情報提供をすることが適当である。また，今後もバイオメトリック認証の最新動向について引き続き調査し，情報提供していくことが重要である。

5.2. バイオメトリクス製品データベースの構築・公開

現在，ユーザがバイオメトリクス製品を導入するにあたって，製品を検討する際には，各社が提供するカタログ等に頼らざるを得ない状況にある。そのため，本研究会ではユーザのバイオメトリクス製品の検討を容易にするために，各製品のベンダに対して共通の調査項目を設定したアンケート調査を実施し，バイオメトリクス製品情報の収集を行った。この製品情報を収集するために，JAISA/BSC や ISO/IEC JTC1/SC37 国内委員会を介して，製品提供者に呼びかけることで，一般に市販されている主要なバイオメトリクス製品の情報を収集した。

今回収集したバイオメトリクス製品情報は,例えば製品 DB のような形で公開できるように，今後可能な限り速やかに取り組むことが適当である。一方で，

バイオメトリック認証技術に対する充分な知識を持たないユーザが，バイオメトリクス製品情報において，ベンダが主張する数値のみでバイオメトリクス製品を判断することはかえってユーザの誤った判断をまねく可能性があるため，情報提供方法については今後も議論が必要である。

5.3. ガイダンスや注意事項集などによる，バイオメトリクス・セキュリティに関する情報提供

バイオメトリック認証技術の利用が一般に広まりつつある現在において，バイオメトリクス製品は様々な場所で簡単に利用できるようになりつつある。一方で，ユーザにおいてはバイオメトリック認証を利用することによって発生するリスクへの意識は必ずしも充分ではない状況にある。本研究会ではバイオメトリクス製品を利用する上での技術上の留意点の他にも，ソーシャルエンジニアリング等への注意が必要であることをまとめ，バイオメトリック認証技術に関する情報を精査し，バイオメトリクス製品の運用者と利用者を対象としてわかりやすい形での情報提供が必要であると考える。

今後バイオメトリック認証のセキュアな利用に向けての取り組みとして，対策のポイントなどのようなものを取りまとめることによってバイオメトリクス・セキュリティに関するユーザの啓発方法を研究会で検討していく必要がある。

5.4. 脆弱性情報の取り扱い

現在，IPA は JPCERT/CC[1]他とのパートナーシップの下，ソフトウェアと Web アプリケーションにおける脆弱性関連情報の取扱いを行っている。バイオメトリクス製品についてみると，その脆弱性情報に関しては組み込みソフトウェアとの類似点もある一方で，ハードウェア面などの独特の一面も持つ。バイオメトリクス製品の脆弱性情報の取り扱いを考えるにおいては，現行の制度との親和性などの視点をもって検討することが重要である。

本研究会としては IPA 等が今まで脆弱性情報を取扱ってきた実績を踏まえつつ，バイオメトリクス製品の脆弱性情報の取り扱いをどのように行うべきかなどについて，今後その詳細に関して調査することが適当であると考える。

5.5. 精度評価の手法について

今回の研究会では精度評価手法の調査を行った。海外では国がバイオメトリクス製品を調達する上で，認証精度評価を行っている国も存在する。このために精度評価 DB を構築している国などもあり，これを産業においても利用可能と

[1] JPCERT/CC：Japan Computer Emergency Response Team Coordination Center

している事例もある。

ただし，DB を利用した精度評価は認証アルゴリズムの性能比較に適しているものの，実運用で使用される認証装置の精度を測定することはできない問題がある。産業上は，生体情報のセンサまで含めた認証装置の精度を，より信頼しうる比較可能な形で測定することが重要となる。現在のところ精度評価はベンダ独自評価が主流であるが，具体的な装置の機能構成・試験方法・環境・被験者・運用など精度の値に影響する項目が統一されていないため，横並びに比較するのは事実上不可能である。また，独自評価のため，その信頼性も保証できないのが現状である。

信頼しうる比較可能な評価を実現する観点では，中立的な第三者機関による精度評価の実施，あるいは第三者機関によるベンダ評価の検証などを検討することも考えられる。しかし，精度評価を行う中立的な第三者機関の設立は理想的だが，多数の被験者からのデータ収集などが必要なため，評価には多大なコストがかかる。また評価技法を持った技術者の育成も課題になるだろう。

比較可能な精度評価を実施するためには，ISO/IEC や JIS TR などで示されている評価方法よりもさらに詳細なレベルでの規定が必要である。その考えに沿ったアプローチとして，ベンダの評価・報告に関する記述事項の仕様とその検証プロセスを定めることも考えられ，検証評価を行う中立的な第三者機関を設立することよりこれを実現するアプローチも有効と考えられる。

今後は，こうした規定や検証プロセスなどの研究を推進できる環境の整備や第三者機関による評価・検証の必要性および実現可能性を検討するため，認証精度評価に関わる国際標準化動向に注視しつつ，諸外国の取組み等の調査を続ける必要がある。