経済産業省「基準認証研究開発事業」

生体情報による個人識別技術を利用した社会基盤構築に関する標準化

「バイオメトリクスセキュリティ評価基準の開発」

2003 年度 報告書（抜粋）

（株）日立製作所

システム開発研究所

目次

要旨

近年，情報システムの安全性に対する要求の高まりから，本人確認手段としてバイオメトリクス技術の適用が進みつつある．バイオメトリクスを情報セキュリティ技術のひとつとして利用するには，他の情報システムと同様に ISO/IEC 15408（以下 CC：Common Criteria と称する）に基づいたバイオメトリクス製品の評価が必要になると考えられる．

バイオメトリクスは利用者の身体的あるいは行動的特徴（生体情報）を「鍵」として本人確認を行う技術である．そのため，生体情報の性質に起因するバイオメトリクス特有の脆弱性や，これにつけこむ脅威が存在する．CC に準拠したバイオメトリクス製品のセキュリティ評価を実施するには，これらのバイオメトリクス特有の脅威や脆弱性を考慮して CC を適切に解釈あるいは詳細化したバイオメトリクスのセキュリティ評価基準を開発し，国際的に標準化を進めていくこと重要である．

CC に基づいてバイオメトリクス製品の PP（Protection Profile）あるいは ST（Security Target）を作成する場合，開発者は，まず考えうるすべてのバイオメトリクスの脅威を抽出し，各脅威に対してリスク評価を行って，評価対象で識別すべき脅威を明らかにする．さらに脅威への対策を CC から選択したセキュリティ機能要件として記載する．また，評価者は各セキュリティ保証要件について，共通評価方法論（以下 CEM：Common Evaluation Methodology と称す）に従い，バイオメトリクス製品の評価を行う．

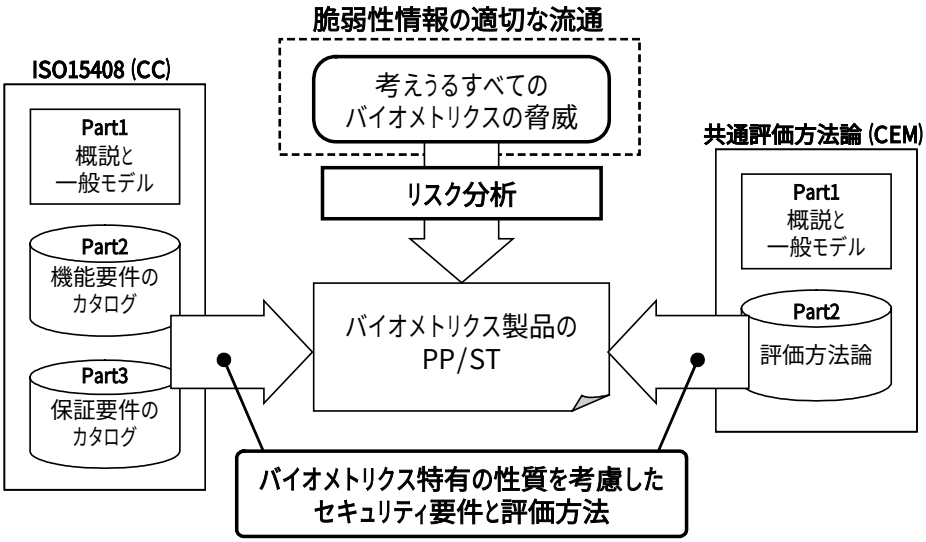


図 CC に基づくバイオメトリクス製品の評価

バイオメトリクス製品のセキュリティ評価を行うには，次の課題がある．リスク分析を行うには，バイオメトリクス特有の脅威および脆弱性がすべて洗い出され，それらの程度を評価する必要があるが，現在，バイオメトリクスの特性を考慮したリスク評価の方法は存在しない．また，バイオメトリクスの脆弱性に関する情報を適切に流通させることで，バイオメトリクス技術の安全性を向上させることが可能であるが，現在は脆弱性情報の流通に関する基準がないため，発見された脆弱性情報を共有化できない問題がある．PP や ST の作成においては，バイオメトリクスの特性を考慮して CC のセ

キュリティ機能要件や CEM の評価方法論を，適切に解釈あるいは詳細化する必要がある．現在，参考になるバイオメトリクス向けの PP や CEM への補足資料（Biometrics Evaluation Methodology：BEM）が公開されているが，国際標準化には至っていない．

そこで本研究では，以下の三つを三ヵ年の作業内容とし，最終的には，本研究の成果を ISO などの国際標準化機関で標準化することを目的とする．

1） バイオメトリクスのリスク評価基準の開発
2） バイオメトリクスのセキュリティ要件および評価方法の開発
3） バイオメトリクスの脅威・脆弱性公開のガイドライン開発

今年度は，上記 1）から 3）の各項目に関する現状の技術，制度，標準に関する調査および課題の明確化を行い，平成 16 年度以降の重点化すべき作業項目を示した．具体的な本年度の作業成果は以下の通りである．

1）バイオメトリクスのリスク評価基準の調査検討に関して，本年度はリスク評価基準を策定するにあたって必要となるバイオメトリクス特有の脅威と脆弱性の明確化を行った．検討に当たっては，現状の関連する研究を調査し，バイオメトリクス特有の脅威と脆弱性を抽出した．さらにバイオメトリクス技術（モダリティ）ごとの検討を加えた．今後はバイオメトリクス特有の脅威に関するリスク評価の方法を策定する必要がある．特に，リスク評価の基礎となるバイオメトリクス特有の脆弱性の程度を示す評価尺度と評価方法の策定が重要である．また，重要度の高い脆弱性について実際に評価実験を行い，実験結果をリスク評価のための基礎情報として共有する必要がある．

2）バイオメトリクスのセキュリティ要件と評価方法の調査検討に関して，本年度は，CC へのバイオメトリクス製品の適用可能性を調査する目的で，既存のバイオメトリクス向け PP と CEM について調査した．その結果，CC および CEM は基本的にバイオメトリクスに適用可能であるが，セキュリティ機能要件の解釈の統一およびバイオメトリクス特有の脆弱性に関する評価方法に課題があることを示した．

3）バイオメトリクスの脅威・脆弱性公開のガイドライン開発に関して，今年度は，バイオメトリクスの脆弱性情報を適切に流通させるための制度上の課題について検討した．今後は，バイオメトリクスシステムの適切な利用のためのインフラストラクチャの整備およびバイオメトリクス認証に関わる脆弱性の発見と活用が課題である．

現在，ISO/IEC JTC1 SC27 では，バイオメトリクスのセキュリティ評価のためのフレームワークを策定中である（NP 19792）．しかし，バイオメトリクス特有の脆弱性に関する知見が不足しており，標準に足る質に達してないのが現状である．今年度の成果の一部であるバイオメトリクス特有の脅威と脆弱性に関する分析結果は，標準を策定するにあたり重要な基礎情報になりうると考える．今後，SC27 への貢献を検討する方針である．

今後の作業方針に関して，上記 1）と 2）に共通する課題である，バイオメトリクス特有の脆弱性に関する評価尺度と評価方法の策定が重要である．これにより，リスク評価基準の基礎を提供するだけでなく，バイオメトリクス製品の具体的なセキュリティ評価方法を示すことが可能になる．本研究では，現状の BEM でカバーされてない脆弱性も対象としているため，BEM の拡充にも貢献可能と考え

る．

バイオメトリクス製品は，内部に利用者の生体情報を有するため，耐タンパ性が要求される場合がある．暗号モジュールのセキュリティ要件を定めた FIPS140 は，耐タンパ性に関する要件もカバーしており，今後バイオメトリクス製品との関係を検討する余地があると思われる．

1　委託業務実施計画

＜省略＞

2　バイオメトリクスのリスク評価基準の開発

2.1　背景と目的

IT システムの安全性を保証するためのセキュリティ評価基準として，ISO/IEC 15408［2-5］が標準化されている．ISO/IEC 15408 は，情報セキュリティの観点から，セキュリティ製品の適切な設計および実装などを評価・保証するための国際標準規格であり，本規格に沿って認証を受けた製品は，国際間でも相互に認証が得られるよう国際的な制度の整備が進められている．セキュリティ製品の例として，データベース，ファイアーウォール，オペレーティングシステム，IC カードなどが認証を受けている．

バイオメトリクスを情報セキュリティ分野に適用するには，上記のセキュリティ製品と同様に，ISO/IEC 15408 などに対応したバイオメトリクス装置のセキュリティ評価が重要になると考えられる．しかし現状では，情報セキュリティの観点に基づいたバイオメトリクスの安全性に関する検討が十分になされていない．バイオメトリクス技術は，本人確認のための識別情報として生体情報を用いているため，生体情報の性質に起因するバイオメトリクス特有の脆弱性を持つ．そのため，一般的な IT システムにおける情報セキュリティの考え方を直接適用することができないことが，安全性評価に関する検討が十分でない一因と考えられる．

バイオメトリクスの安全性評価を行うためには，以下の課題がある．

1）バイオメトリクス特有の脅威と脆弱性の明確化
2）バイオメトリクスのリスク評価方法の明確化

バイオメトリクス装置の安全性評価を行うためには，まずすべての考えうる脅威を洗い出す必要がある．バイオメトリクスの脅威には，一般的な IT システムに共通するものの他に，生体情報の性質に起因するものがある．現状では，生体情報の性質に起因する脅威が網羅的に分析されていないため，個々の開発者が相当のコストをかけて分析を行わなければならない問題がある．

さらに，洗い出した脅威に対してリスクの大きさを評価し，対策すべき脅威を識別しなければならないが，現状では適当なリスク評価の方法がなく，また，バイオメトリクス特有の脆弱性の程度に関する基礎情報がないため，開発者が個々の脆弱性に関して評価を行わなければならない問題がある．

本節では，バイオメトリクス特有の脅威と脆弱性を明確化する目的で，以下に示す分析と検討を行った．検討に当たっては，バイオメトリクスの脅威や脆弱性に関する従来の研究［49］，およびこれらの情報を含むプロテクションプロファイル［29,30］や共通評価方法論［17］などから，脅威や脆弱性を抽出し，さらに詳細に検討を行っている．

・バイオメトリクスシステムのセキュリティ要件
・バイオメトリクスシステムモデルの定義
・バイオメトリクス特有の脆弱性分析
・バイオメトリクス特有の脅威分析

2.2　セキュリティ要件

本節では，バイオメトリクスシステムが満たすべきセキュリティ上の要件について，情報セキュリティの観点から検討する．

情報システムはその内部に保護すべき資産（情報資産）を有しており，情報セキュリティとは，事故や不正などの脅威から情報資産を守ることを意味する．一般的な情報システムが満たすべき情報セキュリティ上の要件として，OECD 情報セキュリティガイドライン［12,13］では，次の三つを挙げている．

・機密性（Confidentiality）
　情報資産を権限のない第三者に秘匿できること．
・完全性（Integrity）
　情報資産を改ざん・破壊されないこと
・可用性（Availability）
　情報資産を必要なときに利用できること

さらに GMITS［14,15］における IT セキュリティマネジメントでは，これらに加えて次の 3 つを確保・維持することを目的としている．

・真正性（Authenticity）
　利用者，プロセス，システム及び情報又は資源の身元が主張どおりであること
　を保証すること．
・責任追跡性性（Accountability）
　主体の行為からその主体にだけ至る形跡をたどれることを保証すること．
・信頼性（Reliability）
　意図した動作と結果に整合性があること．

バイオメトリクス技術は，これらの情報セキュリティ上の要件を守るためのセキュリティ技術の一つに位置づけられ，特に情報資産の機密性および完全性を確保するためのアクセスコントロールを目的に利用者の確認に用いられる．したがってバイオメトリクス技術は，利用者の真正性を確保するための情報セキュリティ技術の一つであり，利用者の真正性はバイオメトリクスにおける情報セキュリティ上の要件といえる．

また，バイオメトリクスシステムは情報資産へのアクセスコントロールに用いられているため，情報資産の可用性を確保するには，バイオメトリクスシステムの可用性が必要となる．したがって，バイオメトリクスシステムのセキュリティ上の要件として，必要なときに利用書の認証あるいは識別を行える可用性の要件が必要となる．

バイオメトリクスは，情報システムの責任追跡性を確保するために用いられる例もある［1］が，これらはバイオメトリクス装置を利用したアプリケーションシステムの一種であり，バイオメトリクス

装置そのもののセキュリティ要件に責任追跡性は該当しないと考える．

バイオメトリクスシステムでは，認証のよりどころ（個人認証情報）として生体情報を用いる．生体情報はそれ自身が個人を特定しうる個人情報の一つであり，さらに生体情報から利用者の健康状態などの副次的な情報が取得できる可能性がある．そのため生体情報は今後特に保護の必要な個人情報として扱われる可能性がある［16］．したがって，生体情報から得られたデータおよび生体情報に関係する情報は，プライバシ情報として保護される必要があり，バイオメトリクスシステムにおけるプライバシ保護をセキュリティ要件の一つに挙げる必要がある．

以上から，本報告書におけるバイオメトリクスシステムのセキュリティ要件を次表の通り定義する．本報告書では，下記に示すセキュリティ要件を阻害する脅威と，それにつながる脆弱性を検討対象とする．

表 2-1 バイオメトリクスのセキュリティ要件

セキュリティ要件	説明
利用者の真正性	生体情報を利用して，利用者がすでにバイオメトリクス装置に登録された正しい利用者であることを確認することができること． 生体情報の偶然の一致あるいは偽造などにより，なりすましが成功し，利用者の真正性が阻害される場合がある．
可用性	必要なときに利用者の認証あるいは識別が行えること． バイオメトリクス装置の置かれた環境，あるいは装置に対して利用者が操作を習熟していない場合などに，照合未対応を多発し，可用性が阻害される場合がある．
プライバシ保護	利用者が他人に知られることを望まない情報（プライバシ情報）が保護されること． 生体情報あるいは生体情報に関係する情報が漏洩することで，プライバシが守られない場合がある．

2.3　システムモデルの定義

本節では，バイオメトリクスシステムの脅威と脆弱性を検討するにあたり，まず対象とするバイオメトリクスシステムの範囲を検討する．

一般的にバイオメトリクスシステムとは，バイオメトリクスを利用した本人確認機能を含んだ IT システムを指す［1］．しかしながら，バイオメトリクスの脅威と脆弱性を検討するうえで，IT システムのみを検討対象とするのは不十分である．

バイオメトリクスの安全性を示す指標は，主にその精度，特に他人受け入れ率（False Accept Rate：FAR）に関係する［1,17］が，FAR は，センサ，特徴抽出機能，照合機能などからなるバイオメトリクス装置の性能だけでなく，指紋や顔などの生体情報（Biometric Characteristics）自体の状態や，生体情報を取り込む時の周囲の物理的な環境，あるいは利用者の振る舞いに影響を受けることが知られている［20,21］．

また，生体情報は利用者を確認するための「鍵」として使用されるが，パスワードや秘密鍵のような他の本人確認手段には存在しない特性を持つ場合がある［11］．例えば，パスワードや秘密鍵は利用者（あるいはシステム）が任意に設定し，必要があれば変更することが可能であるが，生体情報は利用者自身の身体的あるいは行動的特徴であり，任意に設定あるいは変更することができない場合がある．そのため，いったん生体情報が再現可能なほどのデータが暴露されてしまうと，安全上，生体情報を鍵として使用できなくなる脅威がある．したがって，攻撃者の生体情報の入手のしやすさは，FAR には直接関係しないバイオメトリクスの安全性を示す指標となりうる．

さらに，常に必要なときに，必要な時間内で利用者の認証・識別が可能であることも安全性の指標のひとつに含まれると考える．利用者の認証・識別が適切に行えなかったり，適切な時間内で行えなければ，利用者のスループットが著しく下がり，システム全体が破綻する場合も考えられるからである．この場合，本人拒否率（False Reject Rate：FRR）や照合未対応（Failure to Acquire：FTA）率および認証に要する時間などが安全性の指標となるだろう．

以上の例から，バイオメトリクスの脅威や脆弱性を検討する上では，バイオメトリクス装置の性能だけではなく，安全性に影響すると考えられるすべての要素を検討対象に含むべきであるといえる．

表 2-2 にバイオメトリクスの安全性に影響すると考えられる要素と，安全性への影響の例を示す．

表 2-2 バイオメトリクスの安全性に影響する要素

要素	説明	安全性への影響例
利用者	バイオメトリクス装置に既に生体情報を登録されている者	生体情報の入力方法を習熟していない場合，著しく高い頻度で本人拒否や照合未対応を引き起こす.
環境条件	バイオメトリクス装置が利用される物理的な環境の条件. 特に生体情報の取得時の環境を指す.	生体情報の登録時の環境条件と著しく異なる環境条件化で認証・識別を行うことにより，しく高い頻度で本人拒否や照合未対応を引き起こす.
運用条件	生体情報の登録や認証･識別時の運用上の条件. 例えば登録時のオペレータによる監視など.	登録時の本人確認が十分でない場合，攻撃者が利用者になりすまして登録することができる.
生体情報	指紋や顔などの利用者の身体的あるいは行動的特徴そのもの	指紋の場合，センサ面に残留した指紋の跡を利用して，簡単になりすましを行える可能性がある.
バイオメトリクス装置	生体情報を登録する装置, また新たな生体情報を取得して, 既に登録した利用者との一致/不一致を判定する装置	登録されたテンプレートが適切に保護されていない場合，漏洩したテンプレートから人工的に生体情報を複製し，なりすましが行える可能性がある.

以上に述べたように，バイオメトリクスの安全性は，FAR や FRR，FTA，あるいはこれらの統計的な性能とは直接関係しない要因に関連する. FAR は, 利用者の振る舞い, 運用環境, 生体情報の性質, バイオメトリクス装置の性能に依存する.

以上の議論から，バイオメトリクスの安全性を脅かす脅威，および脅威がつけこむバイオメトリクスの脆弱性を検討する上では，表 2-2 に示す要素をすべて考慮する必要がある．そこで，本報告書では，検討対象とするバイオメトリクスシステムを図 2-1 に示すようにバイオメトリクス装置だけでなく，個人を認証あるいは識別するために生体情報を用いるスキーム全体とする.

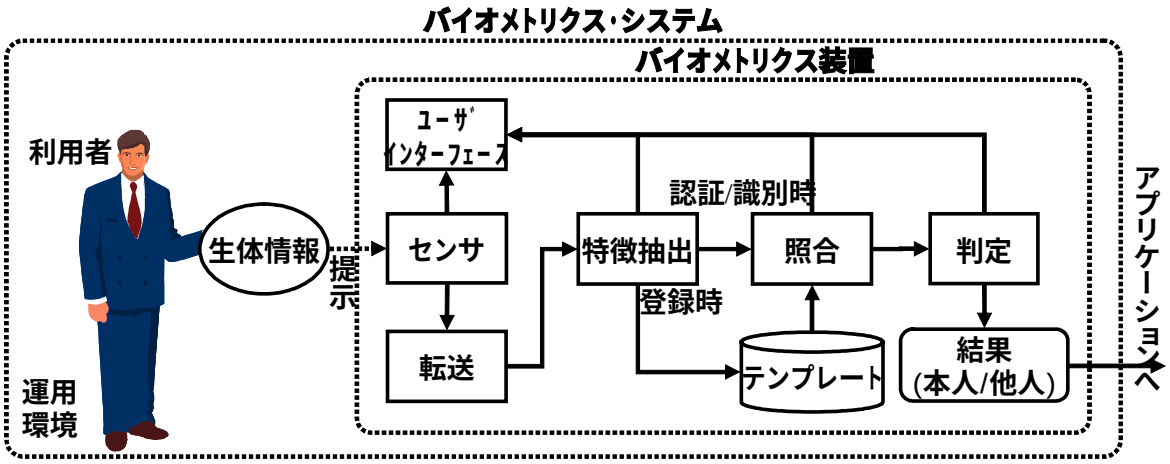


図 2-1 バイオメトリクスシステム

本報告書におけるバイオメトリクス装置は，生体情報を取得して電子的な生体情報（バイオメトリクスデータ）を出力するセンサ，バイオメトリクスデータの転送，特徴抽出，テンプレートとの照合，利用者本人か否かを判定する機能などからなる．これらの機能により，生体情報を提示した利用者の認証あるいは識別を行う．

バイオメトリクス装置の機能構成は必ずしも図 2-1 と同じである必要はなく，生体情報をもって利用者の認証あるいは識別を行うシステムを指している．バイオメトリクス装置は，パスワードや IC カードなど生体情報以外の本人確認手段を利用した本人認証・識別システムと同時に，あるいは補完的に用いられる場合がある．すなわち，装置，あるいはシステムとして実装したり，サーバ，クライアント，IC カードなどに機能を分割してもよい．また，バイオメトリクス装置として独立している必要はなく，アプリケーションの一部として実装されていてもよい．例えば，テンプレートを IC カードに保存して利用者が所有するモデルや，クライアントマシンで得られたサンプルをサーバに転送し，サーバーで照合を行うモデルなども，図 2-1 に示すバイオメトリクス装置として扱う．

本報告書におけるバイオメトリクスシステムは利用者の認証もしくは識別を目的に使用される．認証・識別結果は，入退室管理，コンピュータへのログイン，情報資産へのアクセス権限の付与など利用者の物理的および電子的なアクセスコントロールで利用される．これらの利用先をアプリケーションと呼ぶ．本報告書ではアプリケーションは特に限定されない．

生体情報は利用者の身体的あるいは行動的な特徴を指し，特定のバイオメトリクス技術に限定しない．

2.4 脆弱性分析

2.4.1 分析方針

本報告書における脆弱性分析の目的は，バイオメトリクスにおける既知の脆弱性を洗い出し，系統的に整理・分類することにある．これにより，バイオメトリクスの脆弱性に関する理解を深め，新たな脆弱性を発見するための基礎情報となす．

また，リスク評価においては，脆弱性の程度，すなわちある脆弱性につけこむ攻撃がどれ程の難易度（時間，設備，技術，コスト）で実現可能かを明らかにする必要がある．そのためには，脆弱性の性質をバイオメトリクス技術ごとに詳細化し，脆弱性の程度をあらわす指標，および脆弱性の程度を評価する方法が必要となる．

以上より，本報告書では以下の 2 点を脆弱性分析の目的とする．脆弱性の洗い出しに関しては，従来のバイオメトリクスの脆弱性に関係する研究などに基づくが，現在，確立された脆弱性の程度を測る指標および評価方法は存在しないため，本研究において検討したものである．

脆弱性分析の目的：

１）バイオメトリクスにおける既知の脆弱性の洗い出し，および系統的な整理・分類

２）バイオメトリクス技術ごとの脆弱性の詳細化

脆弱性分析は，従来の研究からの脆弱性の抽出，脆弱性の分類，バイオメトリクスごとの脆弱性の詳細化，の順で進める方針とした．

従来研究からの脆弱性の抽出では，バイオメトリクスの脆弱性に関する研究［11,27,28,49］や，バイオメトリクス向けのプロテクションプロファイル［29,30］あるいは共通評価方法論［17］から，バイオメトリクスの脆弱性を抽出した．プロテクションプロファイルや共通評価方法論では，脆弱性が直接的に記述されていないため，記述されている脅威がつけこむ脆弱性を検討により明確化した．

脆弱性の分類に関して, 現状, 確立されたバイオメトリクスの脆弱性の分類方法は存在しないため，本研究おいて脆弱性の分類方法を検討し，脆弱性が存在するバイオメトリクスシステムの要素および脆弱性の性質の二軸による分類を採用した．脆弱性の分類方法については，2.4.2 節で詳述する．

バイオメトリクス技術ごとの脆弱性の詳細化に関して，抽出，分類した脆弱性ごとに，具体的なバイオメトリクス技術を想定した場合の，その性質，脆弱性の程度を測る指標，評価の方法などについて検討した．詳細化の具体的な方針に関しては，2.4.3 節で詳述する．

以上の脆弱性の分析作業は, Biometric Security Consortium［51］の基盤技術部会 WG1 にレビューし，バイオメトリクス専門家の立場からの意見を集約した．

2.4.2　脆弱性の分類方法

本節では，バイオメトリクスの脆弱性を分析するにあたっての，分類の方法について検討する．また，次節以降で述べる脆弱性項目を分類した結果を示す．

2.3 節で述べたように，バイオメトリクスシステムは，利用者，環境条件，運用条件，生体情報，バイオメトリクス装置から構成される（図 2-1）．脆弱性はこれらの要素にそれぞれ存在するため，バイオメトリクスの脆弱性を理解するうえでは，脆弱性が存在する要素ごとに分類するのが妥当と考える．

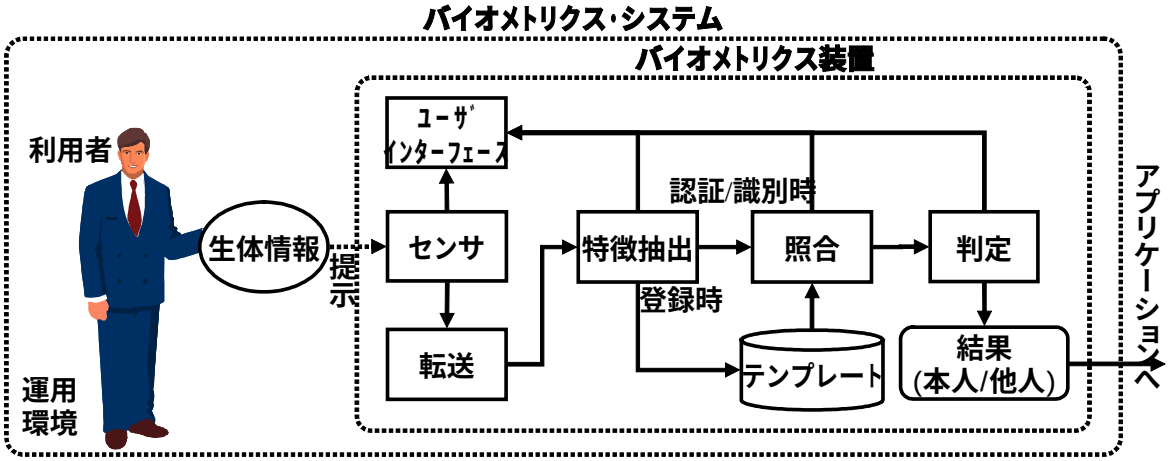


図 2-1 バイオメトリクスシステム（再掲）

脆弱性の存在する要素によるバイオメトリクスの脆弱性分類：

- バイオメトリクス装置
- 生体情報
- 利用者
- 運用条件・環境条件

さらに，バイオメトリクスシステムにはバイオメトリクス特有の脆弱性と，他の一般的な IT システムに共通する脆弱性を有していると考えられる．

脆弱性の性質に基づくバイオメトリクスの脆弱性分類：

- バイオメトリクス特有の脆弱性
- 一般的な脆弱性

以下，バイオメトリクス特有の脆弱性と一般的な IT システムの脆弱性の相違について検討する．

個人認証あるいは個人識別は，あらかじめ登録した個人認証情報と，認証時に新たに提示する個人認証情報を照合することで行われる．個人認証情報としては，パスワードに代表される秘密情報，IC カードなどの所有物（あるいは所有物内の秘密情報），生体情報の 3 つがある．

秘密情報や所有物を用いた本人確認については，既に CC などで十分に検討されており，脆弱性としては一般的な IT システムに共通するものと理解できる. 逆に, バイオメトリクス特有の脆弱性とは, 生体情報を個人認証情報に用いたことに起因する脆弱性と考える．すなわち，秘密情報や所有物を用いた本人確認システムには存在しないが，生体情報を用いた場合に問題となる弱点が，バイオメトリクス特有の脆弱性である．例えば，以下のような例がある．

顔を用いたバイオメトリクス装置の場合，利用者（あるいはシステム）は個人認証情報である顔を任意に変更することはできない．これをパスワードや所有物と比較すると，パスワードは利用者が任意に変更することが可能であるし，所有物の場合も，問題が生じれば交換することができる．この性質によって，パスワードや所有物が攻撃者の手に渡った場合でも，パスワードを変更したり，所有物を無効化してなりすましを防ぐことができる．一方，顔を用いた認証の場合，人工的に再現可能なほど詳細な利用者の顔の情報が攻撃者の手に渡った場合，顔を任意に変更することはできないため，なりすましの脅威につながる可能性がある．

このように，生体情報を個人認証情報として捉えたときに，他の本人確認手段にはない性質に基づく弱点は，代表的なバイオメトリクス特有の脆弱性といえる．また，他の本人確認手段と同じ性質の脆弱性であっても，生体情報を用いた場合に脆弱性の程度が大きく異なるものも，バイオメトリクス特有の脆弱性と考える．ここで，脆弱性の程度とは，脆弱性を攻撃し，実際に被害を発生させるために必要な，攻撃者の知識，技術，設備，時間，費用，あるいは成功の確率などを指す．例えば，以下の例がある．

パスワード，所有物，生体情報とも，複製が可能であり，かつ複製した個人認証情報を使用してなりすましを行う可能性があることから, 個人認証情報の複製は, 一般的な脆弱性ということができる．しかし，個人認証情報を複製するため技術，設備，時間，費用，成功確率は，個々の個人認証情報によって異なると予想される．例えばパスワードの場合，複製はほとんど何の労力も要さないし，成功確率は常に 100%である．物理的な鍵（例えばドアの鍵）もある程度の設備と技術があれば，15 分ほどで複製することができるだろう. 電子キーや IC カードのように複製を非常に難しくする技術もある. 生体情報の複製の難易度に関しては不明確な点が多いが，主に生体情報の性質と，バイオメトリクス装置の持つ生体検知機能に依存すると考えられる．したがって，生体情報の複製の難易度は他の個人認証情報とは大きく異なる可能性がある．

以上の議論から，バイオメトリクス特有の脆弱性を次の二つと定義する．

バイオメトリクス特有の脆弱性：

- 生体情報特有の性質に基づく脆弱性
- 脆弱性の程度が生体情報特有の性質に依存する脆弱性

バイオメトリクスシステムの脆弱性には，前述したバイオメトリクス特有の脆弱性のほかに，一般的な IT システムに共通する脆弱性も存在する. 例えば, バイオメトリクス装置内部のデータが十分に保護されていない場合，バイオメトリックデータやテンプレート，照合結果の漏洩や改ざんが生じ，なりすましの脅威につながる可能性がある．これらの脆弱性は，他の個人認証・識別にも共通する．主な対策は本人認証・識別システム内のデータの暗号化や電子署名の付与であり，生体情報の性質と

は無関係である．

本報告書では，バイオメトリクス特有の脆弱性を中心に詳細な検討を行った．一般的な脆弱性に関しては，後述する脅威に関連するものを項目として挙げる．秘密情報や所有物を用いた個人認証・個人識別における脆弱性はすでに十分に検討されており，その対策が ISO/IEC 15408（CC）のセキュリティ機能要件としてまとめられている．

以上の観点から分類した脆弱性の項目を次図に示す．脆弱性の各項目は，それが存在するバイオメトリクスシステムの要素，運用・環境条件，利用者，生体情報，バイオメトリクス装置の 4 つに分類される．また同時に，バイオメトリクス特有の脆弱性と，一般的な IT システムに共通する脆弱性に分類される．図では，網掛けで示した脆弱性がバイオメトリクス特有の脆弱性である．

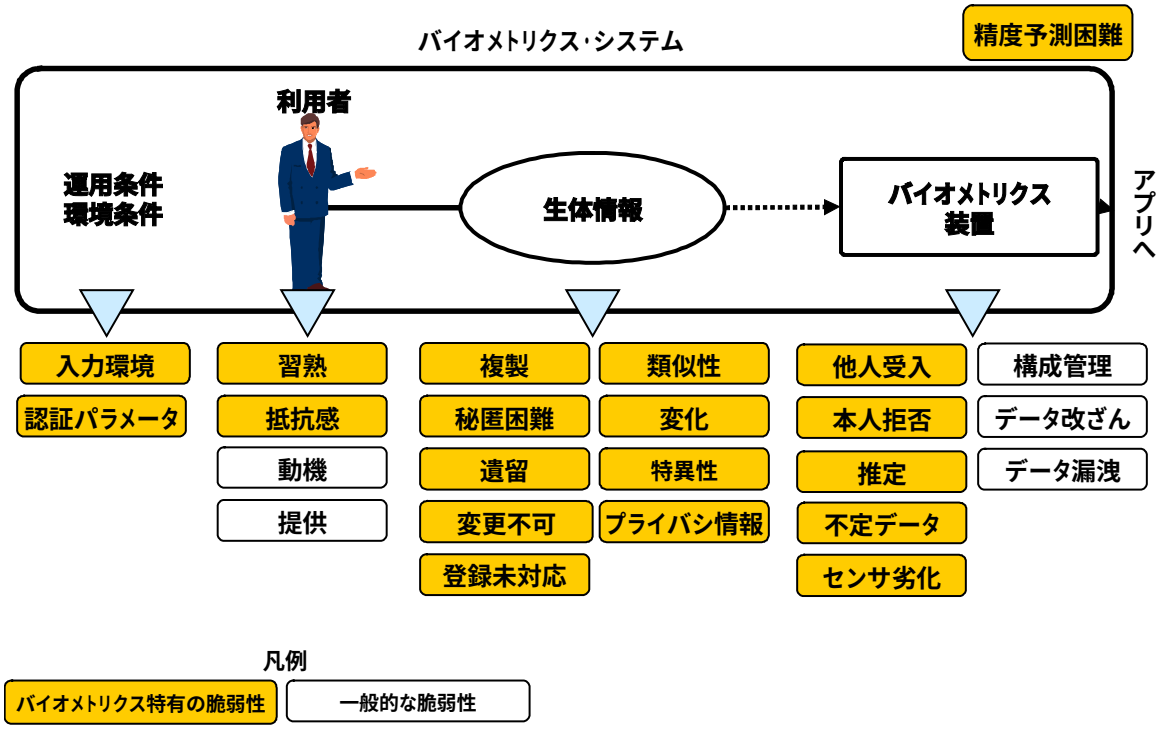


図 2-2 バイオメトリクスの脆弱性の分類

2.4.3 脆弱性の詳細化方法

本節では，バイオメトリクスごとの脆弱性の性質を詳細化する上での考え方について述べる．

リスク評価を行うためには，脆弱性の程度，すなわち，ある攻撃において損害を引き起こすために要する技術，時間，設備，コスト，あるいは攻撃の成功可能性などを明らかにする必要がある．現在，脆弱性の程度を測る尺度や評価の方法自体が確立されていないため，本報告書では，脆弱性の程度を決める要因，程度を測る評価尺度，評価方法の観点から脆弱性の詳細化を行う．

脆弱性の程度を決める要因は，バイオメトリクス技術（生体情報の種類）に依存する場合とバイオメトリクス製品に依存する場合の二つがあると考えられる．バイオメトリクス特有の脆弱性の場合，バイオメトリクス技術の特性に基づいているため，個々のバイオメトリクス技術によって脆弱性の程度は異なる．さらに，バイオメトリクス特有の脆弱性の一部には，脆弱性が製品のスペックに強く依存しているために，バイオメトリクス製品ごとに脆弱性の程度が異なるものもある．

生体情報を複製できる脆弱性を例に取ると，生体情報の複製のしやすさは生体情報の種類に依存するが，さらにバイオメトリクス装置が複製した人工的な生体情報を受け入れるか否かは，センサのデータ取得原理や生体検知機能の有無に関係する．したがって，生体情報を複製できる脆弱性の程度は，生体情報の種類だけでなく，バイオメトリクス製品にも依存している．

脆弱性の程度を決める要因は，脆弱性の評価対象に関係する．脆弱性の程度がバイオメトリクス技術に依存する脆弱性では，脆弱性の評価は生体情報の種類ごとに行われればよく，特に製品ごとの評価を必要としない．一方，脆弱性の程度が製品の仕様に依存する場合，同じ生体情報の種類を対象とした場合でも，製品ごとに評価する必要が生じる．また，脆弱性の程度を決める要因は，新たな脆弱性が発見された場合の対応にも関係する．程度がバイオメトリクス技術に依存する脆弱性が発見された場合，その生体情報を用いたバイオメトリクス製品すべてがなんらかの対策を要求される．バイオメトリクス製品に依存した脆弱性の場合は，関係する製品のみに対策が要求される．

以上のように，脆弱性の程度を決める要因は，脆弱性評価の対象と，対策が必要とされる範囲に関係する．そこで本報告書では，脆弱性評価の対象を明らかにする目的で，各脆弱性に関して脆弱性の程度を決める要因を検討する．

■脆弱性の程度を決める要因

・個々のバイオメトリクス技術に依存

　　・脆弱性程度の評価対象は生体情報の種類ごと

・個々のバイオメトリクス製品に依存

　　・脆弱性程度の評価対象はバイオメトリクス製品ごと

本報告書では，将来，脆弱性の程度をリスク評価の基礎データとして用いることを考えている．そのため，脆弱性の程度の評価尺度は，攻撃を成功させるのに要する技術，時間，設備，コスト，あるいは攻撃の成功可能性などを含む形で定義し，リスク評価に利用しやすいよう配慮される必要があると考える．本報告書では，評価尺度として，SOF 強度［2,3］の考え方により，技術，時間，設備，コストを表現し，バイオメトリクスの統計的な性能（精度や FTA，FTE など）により攻撃の成功可能性

を表現することとした.

評価方法に関しては，標準的な評価方法があれば，それに準ずるのが望ましいと考える．例えば標準的な精度評価方法［9,10,20-26］など．そこで本報告書では，標準あるいはそれに準ずる評価方法がある場合はこれを示した．また，標準的な評価方法がない場合は，条件などを追加して評価に流用が可能か否かを検討した．全く評価方法が存在しない場合，妥当な評価方法の案を検討した.

2.4.4 生体情報に存在する脆弱性

本節では，生体情報に存在する脆弱性に関して述べる．ここで挙げるすべての脆弱性は，他の本人確認手段における個人認証情報にはない生体情報の性質に起因するものであるため，バイオメトリクス特有の脆弱性に分類される．

次表に生体情報に存在する脆弱性の一覧を示す．

表 2-3 生体情報に存在する脆弱性

分類	項目	定義
特有	複製	物理的に生体情報を複製できる脆弱性
	秘匿困難	生体情報の秘匿が困難である脆弱性
	センサ残留	生体情報の痕跡がセンサ面に残留する脆弱性
	変更不可	生体情報を利用者が意識的に変更できない脆弱性
	登録未対応	生体情報をバイオメトリクス装置に登録できない脆弱性
	類似性	類似した生体情報をもつ他の利用者が存在する脆弱性
	変化	生体情報の状態が変化する脆弱性
	特異性	Wolf，Lamb，Goat などにより，高確率で FA や FR が発生する脆弱性
	プライバシ情報	生体情報は個人情報の一種でありプライバシ情報を含む脆弱性

＜以下省略＞

2.4.5　バイオメトリクス装置に存在する脆弱性

本節では，バイオメトリクス装置に存在する脆弱性について述べる．次表にバイオメトリクス装置に存在する脆弱性の一覧を示す．これらの脆弱性は，バイオメトリクスに特有のものと，一般的な IT システムにも共通するものに分類される．

バイオメトリクス特有の脆弱性は, パスワードや IC カードなどを利用した本人確認装置には存在しない性質に起因する．また一般的な IT システムにも共通する脆弱性に分類した「センサ劣化」および「構成管理」は，特にバイオメトリクス装置を対象とした場合に考慮すべき点を含んでいる．「データ改ざん」および「データ漏洩」に関しては，一般的な IT システムに共通する脆弱性であり，特にバイオメトリクス特有の問題を含まないが，後述する脅威を説明する都合上，ここに挙げた．

表 2-4 バイオメトリクス装置に存在する脆弱性

分類	項目	定義
特有	他人受入	他人受入が偶発的に発生する脆弱性
	本人拒否	本人拒否が偶発的に発生する脆弱性
	推定	テンプレートや照合結果から生体情報が推定できる脆弱性
	不定データ	生体情報でないノイズ画像などにより他人受入が発生する脆弱性
一般	センサ劣化	センサが劣化する脆弱性
	構成管理	バイオメトリクス装置の構成の変化により，精度が変化する脆弱性
	データ改ざん	バイオメトリクス装置内のデータを改ざんできる脆弱性
	データ漏洩	バイオメトリクス装置内のデータが漏洩する脆弱性

＜以下省略＞．

2.4.6　利用者に存在する脆弱性

本節では, 利用者に存在する脆弱性について述べる. 次表に利用者に存在する脆弱性の一覧を示す. これらの脆弱性は, バイオメトリクスに特有のものと, 一般的な IT システムにも共通するものに分類される.

バイオメトリクス特有の脆弱性は, パスワードや IC カードなどを利用した本人確認手段には存在しない性質に起因する. また一般的な IT システムにも共通する脆弱性は, 特にバイオメトリクス特有の問題を含まないが, 後述する脅威を説明する都合上, ここに挙げた.

表 2-5 利用者に存在する脆弱性

分類	項目	定義
特有	習熟	利用者はバイオメトリクス装置の使用方法を習熟していなければならない脆弱性
	抵抗感	バイオメトリクス装置の使用に抵抗感を感じる脆弱性
一般	動機	利用者は認証・識別される意思を持って生体情報の入力を行わなければならない脆弱性
	提供	利用者が第三者に生体情報を提供できる脆弱性

＜以下省略＞

2.4.7　運用条件, 環境条件に存在する脆弱性

本節では，運用条件および環境条件に存在する脆弱性について述べる．次表に運用条件および環境条件に存在する脆弱性の一覧を示す．これらの脆弱性はバイオメトリクスに特有の脆弱性に分類される．

表 2-6 運用条件および環境条件に存在する脆弱性

分類	項目	定義
特有	入力環境	入力環境が精度に影響する脆弱性
	認証パラメータ	認証パラメータの設定が精度に影響する脆弱性

＜以下省略＞

2.4.8　**その他の脆弱性**

本節では，これまでに述べた精度に影響するさまざまな脆弱性の複合的な影響に起因する脆弱性を示す．そのため，ここで述べる脆弱性は他の脆弱性と完全に切り分けられるものでなく，他の脆弱性と関連を持つ．

名称：精度予測困難

定義：運用時の精度を予測することが困難である脆弱性

＜以下省略＞．

2.5 脅威分析

2.5.1 分析方針

本節では，バイオメトリクスシステムにおける脅威の分析方針を述べる．本報告書における脅威分析の目標は次の 2 点である．

1）バイオメトリクスシステムにおける考えうるすべての脅威の洗い出し
2）脅威のつけこむ脆弱性および脅威を実現するための条件の明確化

バイオメトリクスシステムのリスク分析を行うためには，まずバイオメトリクスシステムにおけるすべての脅威を洗い出す必要がある．そのためにはバイオメトリクスシステムに対するセキュリティ上の前提条件を仮定せず，できる限り広く脅威を抽出する必要がある．例えば，既に策定されているバイオメトリクス装置のプロテクションプロファイル（PP）［29,30］では，PP 開発者は TOE であるバイオメトリクス装置の仕様，バイオメトリクス装置周辺の IT 製品，あるいはバイオメトリクス装置の運用に対してなんらかの前提条件を導入している．そのため，これらの前提条件で対策される脅威については，PP に明示的に記載されない．また，リスクの大きさに対して対策のコストが見合わないと PP 開発者が判断した脅威についても PP には記載されない．したがって，既存のバイオメトリクス装置の PP から脅威を抽出するだけでは，本報告書の目的には不十分である．

そこで，従来のバイオメトリクスの脅威に関する研究［11,49］からの脅威抽出，および，これまでに洗い出したそれぞれの脆弱性に関して，その脆弱性につけこむ脅威を抽出した．つまり，脆弱性から攻撃の方法や事故のプロセスを導出した．また，バイオメトリクス向けの共通評価方法論（BEM）［17］の第 3.5 節にもバイオメトリクスの一般的な脅威が記載されているので，これも参考にした．以上をまとめると，バイオメトリクスシステムにおける考えうるすべての脅威の洗い出しを目的に以下の作業を行った．

1）バイオメトリクスシステムにおける考えうるすべての脅威の洗い出し
- 従来のバイオメトリクスに関する脅威の研究の整理
- 既存のバイオメトリクス向け PP に記載された脅威の整理
- 既存のバイオメトリクス向け共通評価方法論（BEM）に記載の脅威の整理
- 本報告書における脆弱性からの脅威抽出

本報告書では，以上の作業により抽出した脅威を整理し，関連する脆弱性および，PP および BEM に記載された脅威との対応関係を明示した．

次に，抽出した脅威について，脅威の実現手段あるいは事故のプロセスを詳細化し，脅威がつけこむ脆弱性と，その脅威を実現するための条件を明らかにする作業を行った．これらを明らかにすることによって，ある脅威に対してどの脆弱性に対策を打つべきかが明らかになる．また，脆弱性への対策が技術やコスト面から困難であれば，実現の条件に対して対策する方法もある．さらに，ある脅威に関連する脆弱性の程度が今後明らかになることで，そのリスクを見積もることが可能になると考え

る．

2）脅威のつけこむ脆弱性および脅威を実現するための条件の明確化

・個々の脅威の具体的な実現手段の詳細化

・詳細化された脅威に関連する脆弱性と条件の明確化

本報告書では，脅威がつけこむ脆弱性との関係を示すのみで，具体的に個々のバイオ技術についての攻撃方法や事故のプロセスは明示しない．具体的なバイオメトリクス技術をターゲットに脅威を詳細化する場合には，脆弱性をバイオメトリクス技術ごとに詳細化した情報（2.4 節）が参考になる．

また，本報告書では，バイオメトリクス技術に特有の脅威に重点化している．すなわち，バイオメトリクス特有の脆弱性が関連する脅威の詳細化を行った．したがって，一般的な IT システムに共通する脆弱性のみに関連する脅威は簡単な記述にとどめた．

例えば，バイオメトリクス装置内部の転送機能からバイオメトリクスデータを盗聴し，攻撃者が盗聴したデータを転送機能に入力することでなりすましを行う攻撃（リプライアタック）などでは，バイオメトリクス装置におけるデータの漏洩や改ざんを利用しており，他の個人認証でも同様の攻撃が可能である．また，生体情報とテンプレートを照合した結果を改ざんすることでなりすましを行う攻撃では，バイオメトリクス装置の照合結果が改ざん可能である脆弱性を利用しており，他の個人認証でも同様の攻撃が可能である．この他にも，バイオメトリクス装置の電源断による可用性の阻害など一般的な脅威があるが，このように一般的な個人認証にも共通する脆弱性のみを利用した脅威については 2）の詳細化を行っていない．

2.5.2 脅威の分類

本報告書では，前節で述べた方法で洗い出し詳細化した脅威を，次のように分類した．
まず，脅威の発生するフェーズにより分類を行った．フェーズとは，バイオメトリクス装置に利用者を登録する「登録フェーズ」，登録された利用者を認証あるいは識別する「認証・識別フェーズ」，バイオメトリクス装置の導入あるいはその他における「導入・その他のフェーズ」の 3 つである．

さらに，各フェーズにおいて，脅威が引き起こす被害の内容で分類を行っている．被害の内容は次表の通りである．

表 2-7 フェーズと被害内容による脅威の分類

フェーズ	被害の内容	説明
登録	バックドアの生成	第三者が容易になりすましを行うことのできるバックドアの生成につながる脅威
	可用性阻害	認証・識別時に可用性を阻害する脅威
	プライバシ漏洩	プライバシ漏洩につながる脅威
認証・識別	なりすまし	第三者のなりすましにつながる脅威
	可用性阻害	正当な利用者の可用性阻害につながる脅威
	プライバシ漏洩	利用者のプライバシ漏洩につながる脅威
導入・その他	その他	フェーズや被害内容で分類できないその他の脅威

バックドアの生成につながる脅威とは，第三者が認証・識別時に容易になりすましを行えるような生体情報の登録を行うことを意味する．したがって，登録フェーズ実際には第三者が認証・登録時になりすましを行わなければ被害は発生しないが，本報告書では，第三者は意図的あるいは偶発的になりすましを行うと仮定し，脅威として識別した．

可用性の阻害は，必要なときに利用者の認証・識別が行えなくなる被害である．認証・識別フェーズに実際に被害が生じる脅威である. さらに本報告書では, 登録フェーズにおける攻撃や事故により，結果的に認証･識別フェーズにおいて可用性阻害を引き起こす可能性のある脅威についても記述した．可用性の阻害は，認証・識別時の利用者のスループット（単位時間当たりに認証・識別できる利用者の数）や，利用者への対応，あるいは保守にかかるコストを増大させるなどの二次的な損害を発生する．さらに，バイオメトリクスメ以外の代替手段をもつ本人確認システムの場合，代替手段の安全性がバイオメトリクスに比較して低い場合，代替手段をねらったなりすましなどの攻撃につながる場合があることに注意が必要である．本報告書では，ここに例示したような二次的損害については記述していない．

生体情報は個人を識別しうることから個人情報の一種であると考えられる．さらに生体情報自体から人種，性別，健康状態などの情報を取得しうる可能性があることから，機微な情報（Sensitive Information）［19］として，特に厳重に保護されるべきとの考え方もある［16］．したがって，生体情

報およびそれに関係するあらゆる電子データは，プライバシ情報になりうると考えるべきである．本報告書では，登録フェーズおよび認証・識別フェーズにおいてプライバシ漏洩につながる脅威を記述した．

以上のように，脅威は，発生するフェーズ，および脅威によって生じる一次的な被害の内容によって分類した．フェーズによる分類を大分類，被害内容を中分類とする．さらに，各脅威を，主に関連する脆弱性で細分類する．細分類された脅威には，関連する脆弱性，および PP あるいは BEM への対応を示した．脅威の細分化の程度は PP などで記述されている脅威に相当するよう調整した．

細分化された脅威のうち，バイオメトリクス特有の脆弱性につけこむものは，さらに脅威の実現方法を具体的に記述し詳細化している．詳細化された脅威には，脅威の実現に必要となる脆弱性と条件を詳細に記述した．

次図に脅威の分類と詳細化の関係を示す．

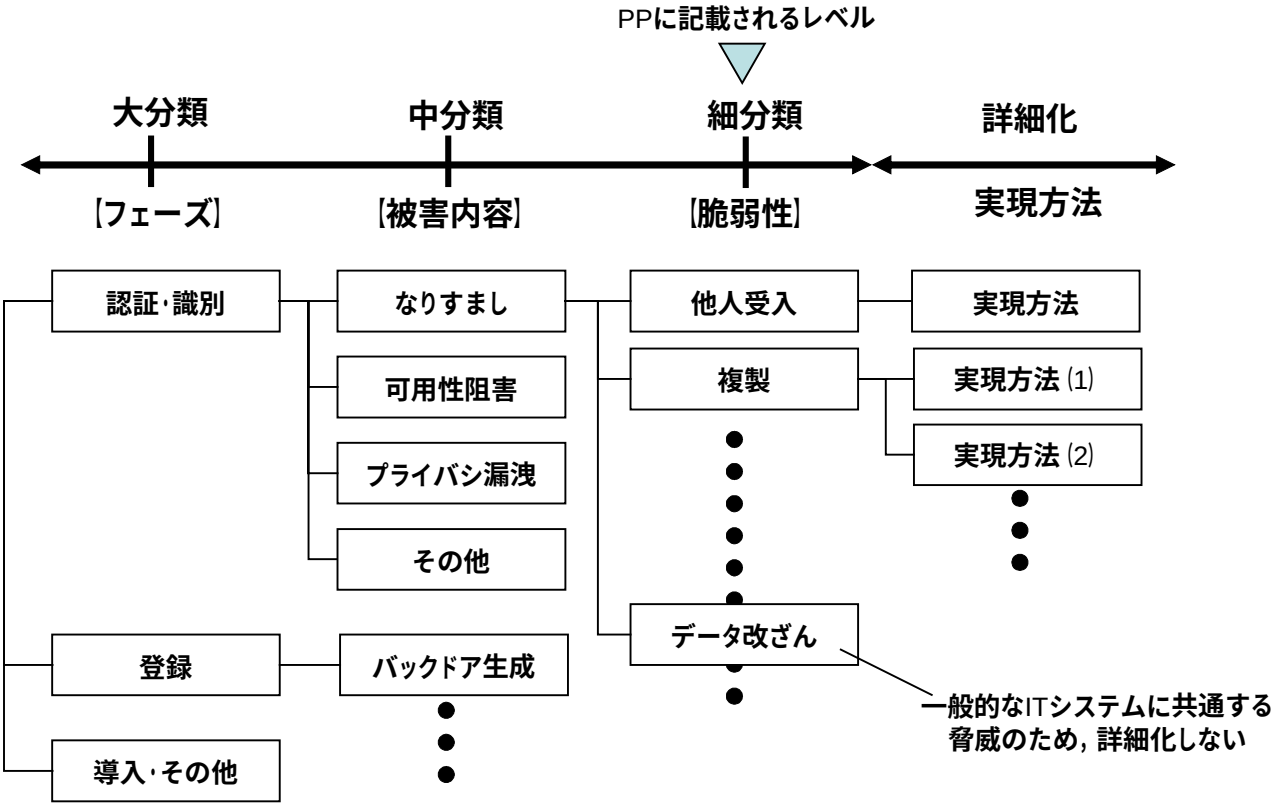


図 2-3 脅威の分類と詳細化の関係

2.5.3　利用者の登録における脅威

本節では，利用者の登録における脅威を示す．利用者の登録における脅威は，次の 4 つである．

・バックドアの生成につながる脅威
・可用性の阻害につながる脅威
・プライバシの漏洩につながる脅威

バックドアの生成につながる脅威とは，第三者が認証・識別時に容易になりすましを行えるような生体情報の登録を行うことを意味する．実際には第三者が認証・登録時になりすましを行わなければ被害は発生しないが，本報告書では，第三者は意図的あるいは偶発的になりすましを行うと仮定し，脅威として識別した．

可用性の阻害につながる脅威とは，正当な利用者が認証・識別を受けられなくなるような生体情報の登録を行うことを意味する．実際には利用者が認証・識別を受けなければ被害は発生しないが，本報告書では，登録した利用者は認証・識別を受けると仮定して，脅威として識別した．

プライバシの漏洩につながる脅威とは，バイオメトリクスデータを含め，利用者のプライバシにかかわる情報が漏洩する可能性のある登録作業を意味する．特に登録フェーズは生体情報に関連するデータを扱うことが多い. 例えば, 利用者の生体情報を取得できなかった理由を記録するかもしれない. 生体情報が利用者の身体の欠損や疾病によるものであった場合，記録された情報ばプライバシ情報に相当する可能性がある．したがって，登録時に得たすべての生体情報に関わる情報はプライバシ情報に相当する可能性があることを考慮すべきである．

次表に利用者の登録における脅威の細分類と, 既存の PP あるいは BEM に記載の脅威との対応を示す．

表 2-8 登録フェーズにおける脅威の細分類

中分類（被害）	細分類（脆弱性）	PP・BEM との対応
バックドア生成	特異性	－
	複製	－
	変化	－
	認証パラメータ	－
	不定データ	BDPP：T.POORING BVMPP：T.POOR_ENROLLMENT
	データ改ざん	－
	その他（なりすまし）	BDPP：T.ILLENROLL BEM：5.2(a)
可用性阻害	認証パラメータ	－
	データ改ざん	－
	その他（不一致）	－
プライバシ漏洩	プライバシ情報	－

＜以下省略＞

2.5.4　利用者の認証･識別における脅威

本節では，利用者の認証・識別における脅威を示す．利用者の認証・識別における脅威は，次の３つである．

・なりすましにつながる脅威
・可用性の阻害につながる脅威
・プライバシの漏洩につながる脅威

なりすましにつながる脅威とは，第三者が利用者になりすまして認証を受ける攻撃や，第三者が利用者として認証されてしまう事故などを指し，利用者の真正性をそこなう脅威である．

可用性の阻害は，必要なときに利用者の認証・識別が行えなくなる被害である．可用性の阻害は，認証・識別時の利用者のスループット（単位時間当たりに認証・識別できる利用者の数）や，利用者への対応，あるいは保守にかかるコストを増大させるなどの二次的な損害を発生する．さらに，バイオメトリクスメ以外の代替手段をもつ本人確認システムの場合，代替手段の安全性がバイオメトリクスに比較して低い場合，代替手段をねらったなりすましなどの攻撃につながる場合があることに注意が必要である．本報告書では，ここに例示したような二次的損害については記述していない．

生体情報は個人を識別しうることから個人情報の一種であると考えられる．さらに生体情報自体から人種，性別，健康状態などの情報を取得しうる可能性があることから，機微な情報（Sensitive Information）として，特に厳重に保護されるべきとの考え方もある．したがって，生体情報およびそれに関係するあらゆる電子データは，プライバシ情報になりうると考えるべきである．

次表に利用者の登録における脅威の細分類と，既存の PP あるいは BEM に記載の脅威との対応を示す．

表 2-9 認証･識別フェーズにおける脅威の細分類

中分類（被害）	細分類（脆弱性）	PP・BEM との対応
なりすまし	他人受入	BDPP：T.CASUAL BEM：2.1（a）（b）
	複製	BDPP：T.ARTIFACT BVMPP：T.HIGH_QUALITY_ARTIFACT BEM：1.1, 1.2, 1.3, 1.4, 3.1, 4.1, 6.2，2.3
	変化	BDPP：T.MIMIC BVMPP：T.MIMIC BEM：1.1, 1.2, 1.3, 1.4, 3.1, 4.1, 6.2，2.2
	認証パラメータ	BDPP：T.WEAKID，T.BADUSR，T.BADADM BEM：2.1(c), 2.4
	類似性	BDPP：T.EVILTWIN BEM：2.1(d)
	センサ残留	BDPP：T.RESIDUAL BVMPP：T.REPLAY_RESIDUAL_IMAGE BEM：2.5
	不定データ	BDPP:T.POORING BVMPP：T.POOR_ENROLLMENT
	特異性	BDPP：T.WEAKID BEM：2.1(c), 2.4
	推定	－
	データ改ざん	BDPP：T. FAKETMPL BVMPP：T.REFERENCE_TEMPLATE BEM：2.6(a)(b)(c)，6.1, 6.3
	その他	BDPP：T.BADUSER，T.BADADM など BVMPP：T.BYPASS，T.TAMPER など BEM：11.1，13.1，14.1，2.6(d),3.1, 3.2 など
可用性阻害	本人拒否	－
	変化	－
	特異性	－
	入力環境	－
	認証パラメータ	－
	習熟	－
	抵抗感	－
	その他	－
プライバシ漏洩	プライバシ情報	－

＜以下省略＞

2.5.5　導入･その他のフェーズにおける脅威

本節では，導入やその他のフェーズにおける脅威を示す．ここで述べる脅威によって引き起こされる被害は，なりすまし，可用性阻害，プライバシ漏洩などには分類されないものを含む.

＜以下省略＞

2.6 今後の課題

2.6.1 リスク評価基準策定における課題

第 2 節では，リスク評価基準を策定するにあたってまず必要となる，バイオメトリクス特有の脅威と脆弱性の明確化を行った．検討に当たっては，バイオメトリクスの脅威や脆弱性に関する従来の研究，およびこれらの情報を含むプロテクションプロファイルや共通評価方法論などから，脅威や脆弱性を抽出・整理し，さらに各脅威や脆弱性項目にバイオメトリクス技術ごとの詳細な検討を加え，脆弱性の程度を示す評価尺度および評価方法に関して検討した．

具体的な検討項目は以下の通りである．

・バイオメトリクスシステムのセキュリティ要件
・バイオメトリクスシステムモデルの定義
・バイオメトリクス特有の脆弱性分析
・バイオメトリクス特有の脅威分析

バイオメトリクスシステムのセキュリティ要件では，バイオメトリクスシステムに要求されるセキュリティ要件を定義した．具体的には，利用者の真正性，認証・識別の可用性，プライバシの保護をセキュリティ要件として設定し，これらを阻害する攻撃や事故をバイオメトリクスシステムへの脅威とした．

バイオメトリクスシステムモデルの定義では，バイオメトリクス特有の脅威や脆弱性を検討する上での対象を定めた. バイオメトリクスシステムの安全性は, バイオメトリクス装置の性能だけでなく，生体情報の性質，利用者の振る舞い，バイオメトリクス装置の使用される環境条件や運用条件に依存するため，これらの要素を含めたシステムを検討対象とした．

バイオメトリクス特有の脆弱性分析では，従来のバイオメトリクスの脆弱性に関する研究やバイオメトリクス向けのプロテクションプロファイルおよび共通評価方法論から，バイオメトリクス特有と考えられる脆弱性を抽出し，整理した．さらに各脆弱性項目について，リスク評価の実現に向けて，脆弱性の程度を測るための評価尺度と評価方法について検討し，バイオメトリクス技術ごとの詳細化を行った．

バイオメトリクス特有の脅威分析に関しては，従来のバイオメトリクスの脆弱性に関する研究やバイオメトリクス向けのプロテクションプロファイルおよび共通評価方法論から，バイオメトリクス特有と考えられる脆弱性を抽出し，その関係を整理した．さらに脅威を実現するための前提条件に関して検討を加えた．また，脅威と脆弱性の関係を示した．

以上の分析では, 特定のバイオメトリクス装置を想定した装置の仕様や前提条件を導入していない．したがって，バイオメトリクスの安全性評価を行ううえでまず必要になる脅威の洗い出しを広く行えたと考える．また，脅威と脆弱性の関係を明確化することで，ある脅威についてどの脆弱性に対策すべきかも明確にした．バイオメトリクスにおけるセキュリティ要件およびバイオメトリクスシステムのモデルを定義し，バイオメトリクス特有の脅威と脆弱性および両者の関係を明確化した．これらの

分析では，特定のバイオメトリクス装置を想定した装置の仕様や前提条件を導入していない．したがって，バイオメトリクスの安全性評価を行ううえでまず必要になる脅威の洗い出しを広く行えたと考える．また，脅威と脆弱性の関係を明確化することで，ある脅威についてどの脆弱性に対策すべきかも明確にした．

しかし，ここで洗い出したすべての脅威に対策するのは技術やコストの面から現実的ではない．実際には，リスクマネージメントの考え方から，リスクの大きい脅威に対してコストの見合う対策を施していく必要がある．リスクの大きさを明らかにするリクス評価の方法として，一般的な IT システムを対象にしたものがいくつか提案されている［14,15］．しかし，通常のリスク評価方法は，バイオメトリクス特有の性質を考慮していないため，バイオメトリクスに直接適用するのは困難と予想される．

したがって，今後はバイオメトリクス特有の脅威に関するリスク評価が課題となる．具体的には，本報告で洗い出した脅威を，具体的なバイオメトリクス装置にあてはめた場合のリスクの評価方法について検討する必要がある．特に，バイオメトリクス特有の脆弱性の程度を示すなんらかの尺度とその測定方法が重要と考える．また，脆弱性の程度が主にバイオメトリクス技術に大きく依存し，かつ製品への依存が小さいものについては，実験により脆弱性の程度を明確化し，リスク評価のための基礎情報として共有すべきと考える．

リスクは，脅威とそれに対応する脆弱性の程度から定義される．例えば，脅威の程度とは攻撃によって発生する被害額と攻撃の発生頻度など，脆弱性は攻撃を受けたときの成功率と攻撃を成功させるための難易度などである．難易度とは，攻撃を成功させるために必要な情報，技術，設備，コスト，時間などを指している．リスク評価にあたっては，まずこれらの脅威と脆弱性の程度を明確化する必要があるが，現状では評価のための共通的な基準は存在しない．

脅威による被害額や発生頻度は，主にバイオメトリクスを利用したアプリケーションに依存し，バイオメトリクス特有の性質への依存は小さいと考えられる．例えば，複製の脆弱性によるなりすましを例にした場合，被害額はバイオメトリクス装置によって保護されている情報資産の価値できまるし，攻撃の頻度にも特にバイオメトリクスの特性には関連ないと考えられる．一方，脆弱性の程度である攻撃を受けたときの成功率や攻撃を成功させるための難易度は，バイオメトリクス特有の性質に強く依存する．例えば，人工的な生体情報を作成したときの成功率は，その人工的な生体情報による FAR で決まるし，難易度は人工的な生体情報を作成するための情報，技術，設備，コスト，時間などで決まる．また，これらの難易度や成功率は脆弱性だけでなく，生体情報の種類，製品によっても異なるため，脆弱性の評価は，生体情報の種類や製品のレベルに具体化して行う必要がある．

以上をまとめると，バイオメトリクスのリスク評価のための今後の課題は以下の通りである．

バイオメトリクスのリスク評価のための今後の課題

（a）バイオメトリクス特有の性質を考慮したリスク評価方法
（b） 脆弱性の程度に関する評価尺度および評価方法の策定
（c） 生体情報の脆弱性の程度を評価するのための実験

（a）に関して，脆弱性の程度を定量的に評価するのは難しいが，攻撃における成功率や難易度などの各評価項目についてレベル分けを行うことで，相対的なリスク評価の基礎とすることが可能と予想

する．相対的なリスク評価により，あるシステムにおいて優先的に対策すべき脅威と脆弱性を明らかにする効果がある．

（b）に関して，評価尺度と評価方法については，本報告書でも簡単な検討を行っている，今後はこれらを詳細化し，より具体的な評価方法を定める必要がある．

（c）に関して，現在まで生体情報の特性に依存した脆弱性の程度は明らかになっておらず，生体情報の種類毎に実験による評価が必要になる．例えば，生体情報には人工的な複製を作成可能な脆弱性がある．複製を作成するための難易度やコストは指紋や顔など生体情報の種類毎に異なると考えられるが，これらの差異を定量的に評価した例はない．理論的な評価は困難であるため，今後は実験的な評価により生体情報の種類毎の脆弱性の程度を明らかにしていくことが重要と考える．脆弱性評価実験を行うに際の方針については次節で述べる．

2.6.2　脆弱性評価実験の方針

本節では，前述のバイオメトリクスシステムの脆弱性評価に関して，今後検討すべき研究項目と関連する実験について述べる．

１）指紋・虹彩・静脈

指紋，虹彩，静脈などのバイオメトリクス (Biometrics) を用いた個人識別技術ないし個人認証技術を評価する際の評価項目としては，

・様々な状況下で安定して使用できるか
・誤受理率(False Acceptance Rate)と誤拒否(False Rejection Rate)の客観的算出が可能か
・誤受理率と誤拒否率を十分小さくできるか
・偽造や偽装の困難性を十分高くできるか

が少なくとも含まれると考えられる．本項においては，平成 16 年度に主として上記偽造の困難性に関する脆弱性実験を行うための方針につきまとめる．

指紋・虹彩・静脈についての脆弱性評価実験は，横浜国立大学の松本が，2000 年 7 月より指紋照合技術について，また，2003 年 7 月より虹彩認識技術について，脆弱性研究結果を報告してきた経験をベースとして担当する計画としている．

指紋照合装置・虹彩照合装置・静脈照合装置について公表されている知識は用いるが，装置自体をリバースエンジニアリングすることはしないでブラックボックスとして扱い，生体の指・手・虹彩（本稿ではこれらを総称して生体部分とよぶことにする）の形状をした人工物体（これをそれぞれ人工指・人工手・人工指とよび，総称として人工生体部分とよぶことにする）で照合装置に受け入れられるものを作製することが，どの程度困難か容易かを，

（A）　生体部分の情報の入手方法に関する評価
（B）　人工生体部分の作製方法に関する評価
（C）　人工生体部分の照合装置への提示方法に関する評価

の観点から実行する．なお，「生体部分」，「人工生体部分」という用語の妥当性の検討および見直しについても平成 16 年度にコンセンサスが得ることを望む．

平成 16 年度は，以下に示す平成 15 年度の準備状況を踏まえ，各種実験を行うこととするが，指紋照合装置は各種のものを比較的容易に入手することができるものの，虹彩照合装置や静脈照合装置については，個々の製品を脆弱性評価の目的で入手することが困難である場合が多いという共通の困難性がある．これがこれまでの準備において直面する最大の課題であり，関係各位のご協力を得て打開していきたい．

【指紋】

人工指の作製プロセスは，指の型を作る部分と，型と人工指の材料とから人工指を作る部分とに大別される．人工指の型の作製方法には，生体指から直に型を作る方法と，押捺指紋または残留指紋から型を作る方法とがあり，押捺指紋または残留指紋の撮影にディジタル顕微鏡，ディジタルカメラ，携帯電話のカメラを用いる場合について実験をしている．また，人工指の材料としては，シリコーンゴム，導電性シリコーンゴム，ゼラチンなどを用いている．

人工的に作られた指がどの程度受け入れられるのかは, 生体の指を直に押し当てて作った型［54-56］，およびガラス表面［57,58］や携帯電話本体や液晶部分［61］，CD やコップ［60］などに残った遺留指紋などから指紋画像を採取し，定められた作製方法により作製した型をもとに，ゼラチンや導電性シリコーンゴム［59］などを材料として作製した人工指が，光学式，静電容量式，電界式，指内散乱光直接読取り方式，感圧式の 17 機種の指紋照合装置に高い割合で受け入れられることを確認している．初期の結果は国際的にも公表している[27]．代表として，これまでに報告した評価結果の一例を図 2-4 に示す．

補足：図 2-4 に示す結果は，17 機種の装置のうち，

装置 A～N：ガラス板に残った遺留指紋をモデルとしたフラットタイプ人工指（20 代女性 1 名）［61］

装置 O～Q：プラスチック粘土に生体指を直接かたどった 3D タイプ人工指（20 代男性 1 名）［60］

をそれぞれ提示したときの受入回数を示したものである．L-L，L-A，A-L，A-A はそれぞれ，生体指で登録し生体指で照合した場合，生体指で登録し人工指で照合した場合，人工指で登録し生体指で照合した場合，および，人工指で登録し人工指で照合した場合を示している．

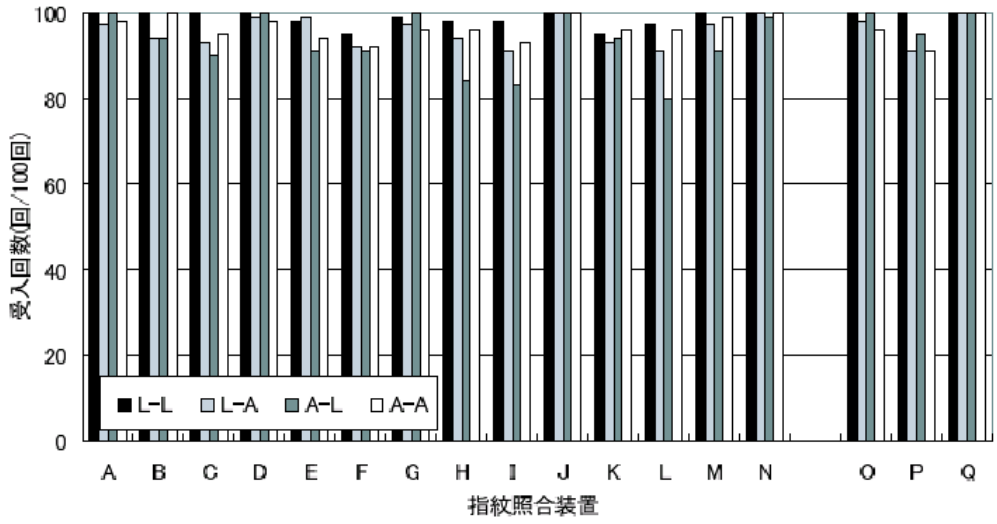


図 2-4 人工指予備的実験結果の例

この結果は被験者数が少なく予備的なものではあるが，指紋照合技術の脆弱性を示していることは間違いない．平成 16 年度は，評価方法そのものを吟味し，より信頼性のある形で脆弱性の評価を示すことに注力する計画である．

【虹彩】

虹彩照合技術についても指紋照合技術の脆弱性評価の経験を踏まえ，虹彩の赤外光により撮影した画像を紙にレーザプリンタで印刷して作成した人工虹彩が 3 機種の虹彩照合装置に受け入れられることを示した[18,62,63]．この結果は被験者数が少なく予備的なものではあるが，虹彩照合技術の脆弱性を示していることは間違いない．平成 16 年度は，評価方法そのものを吟味し，より信頼性のある形で脆弱性の評価を示すことに注力する計画である．

【静脈】

静脈照合技術については，静脈照合装置を入手することができないために，不本意ながら検討はあまり進んでいない．静脈照合技術としては，指先の静脈，手の甲の静脈，手のひらの静脈を用いるものが販売されているが，いずれもマスユーザ用の販売か，脆弱性実験を行わないことを前提とした販売に限定されているのが現状である．静脈照合技術は最近急速に注目を浴びている技術であるので，第三者による評価とその結果の公表が特に大事であることを考慮してこの課題を打破する必要性を強く主張したい．

2）音声・署名・顔

音声，書名，顔認証の実験方針については以下の通りである．

【音声】

音声に基づくバイオメトリクス認証では，秘匿困難性を利用した詐称，ならびに入力環境に関する脆弱性(生体情報の入力環境の変化により精度が変動する脆弱性)が大きな脅威であると考えられる．一方，今後のネットワーク環境において，ユーザが様々なネットワークサービスを利用する際の最も有力な情報端末の一つが携帯電話（端末）である点を考慮すると，携帯電話を使用した音声によるバイオメトリクス認証についても考慮する必要がある．

ディジタル音声通信における音声符号化方式との親和性を考慮した話者照合方式，中でも携帯電話をはじめとする移動通信システムや IP ネットワークで使用される CELP（Code Excited Linear Prediction：符号励振線形予測）符号化方式に基づく話者照合方式を対象とし，公開および入力環境に関する脆弱性について下記の項目を中心とした検討が重要と考える．なお，信頼性の評価には，PC 上でのシミュレーション実験に加え，市販の話者認識装置（システム）を使用した実験も考慮すべきと考える．具体的な検討項目として以下が考えられる．

・話者照合方式の詐称耐性ならびに詐称対抗手段に関する検討

従来提案されている代表的な話者照合アルゴリズムを対象とし，録音音声ならびに合成音声を用いた詐称に対する耐性を評価する．また，詐称に対抗する防御手段に関する検討を行い，その有効性を評価する．

・雑音環境下における話者照合方式の信頼性評価

話者の音声に混入する雑音が話者照合アルゴリズムに与える影響を評価するとともに，耐雑音性を有する話者照合アルゴリズムの検討を行い，その有効性を評価する．

・入力系の相異による話者照合方式の信頼性評価

登録時と認証時あるいは毎回の認証時にそれぞれ異なる端末を使用するなど，入力系の相異が話者照合アルゴリズムに与える影響を評価するとともに，入力系の相異による影響が少ない話者照合アルゴリズムの検討を行い，その有効性を評価する．

【署名】

署名に基づくバイオメトリクス認証では，秘匿困難性および変化を利用した偽筆による詐称が最も大きな脅威の一つであると考えられる．従来，筆者認識研究において，偽筆に対する耐性を評価する際，対象となる筆跡が署名の場合には，単純偽署名（simple forgery），模倣署名（simulated forgery），訓練偽署名（skilled forgery）等が使用されてきた．しかしながら，評価に使用される偽筆がどの程度忠実に対象となる署名を模倣しているか，またどのようにして偽筆データを作成したか，という点について報告されることは少なく，偽筆に対する共通認識および定量的な評価尺度の欠如が，偽筆を使用して筆者認識手法の信頼性評価を行う際の問題点の一つとなっている．

重要と考えられる項目は以下の通りである．

・偽筆の定義に関する検討

筆者認識に使用する筆記情報の相異（オンライン情報，オフライン情報）を考慮した偽筆の定義に

ついて検討する．

・偽筆の生成手法に関する検討
　従来使用されてきた単純偽署名，模倣署名，訓練偽署名の生成手法を整理し，より一般的な偽筆の生成手法を確立する．

・筆者認識手法の偽筆耐性に関する検討
　従来提案されている代表的な筆者認識アルゴリズムを対象とし，生成した偽筆に対する耐性を評価する．

・偽筆に対抗する防御手段に関する検討
　偽筆に対抗する防御手段に関する検討を行い，その有効性を評価する．

【顔】
　顔に基づくバイオメトリクス認証では，秘匿困難性に関する脆弱性（他人が利用者の生体情報を取得できる脆弱性），ならびに推定に関する脆弱性（他人が利用者の生体情報を推定できる脆弱性）を利用した詐称が大きな脅威と考えられる．そのため，これらの脆弱性を用いた詐称方法および顔認証装置の偽顔に対する耐性の調査が重要である．しかしながら詐称方法の検討には，まずどのような画像が偽顔に成り得るのかを調査し，偽顔の定義を固める必要がある．そこで，下記の項目を中心に検討に着手する必要があると考える．

・偽顔の定義に関する検討
　従来提案されている代表的な顔認証アルゴリズムを対象とし，顔認証アルゴリズムごとの偽顔の定義について検討する．

・生体情報を元にした偽顔の生成手法に関する検討
　最小限の生体情報を元に，実世界，もしくはソフトウェア上で偽顔を作成し，偽顔の生成手法を確立する．

・推定による偽顔の生成手法に関する検討
　類似度が出力されるような顔認証装置（システム）において，ヒルクライミングアタックを利用した偽顔生成手法を確立する．

・顔認証装置（システム）の偽顔耐性と防御手段に関する検討
　従来提案されている代表的な顔認証アルゴリズムを対象とし，生成した偽顔に対する耐性を評価する．またその結果を元に詐称に対抗する防御手段に関する検討を行い，その有効性を評価する．

3　バイオメトリクスのセキュリティ要件および評価方法の開発

3.1　背景と目的

バイオメトリクス認証装置を情報セキュリティ分野における本人認証機能として適用するには，他のセキュリティ製品と同等の安全性を持つことを保証する必要がある．このためには，ISO/IEC 15408［2-5］に準拠したバイオメトリクス製品の開発が重要である．

しかし，ISO/IEC 15408 は一般的な IT 製品を対象としており，バイオメトリクス特有の問題をカバーしていない．ISO/IEC 15408 に準拠したバイオメトリクス製品の開発を実現するには，バイオメトリクス特有の問題を考慮した TOE の設定やセキュリティ機能要件および保証要件の解釈が必要となる．

本節では，ISO/IEC 15408 へのバイオメトリクス製品の適用可能性を調査する目的で，既存のバイオメトリクス向けプロテクションプロファイルと共通評価方法論について調査する．具体的には，以下の 3 点を調査対象とした．

（1）Biometric Device Protection Profile （BDPP）
（2）Biometric Verification Mode Protection Profile（BVMPP）
（3）Biometric Evaluation Methodology（BEM）

これらの調査結果から，今後 ISO/IEC 15408 に準拠したバイオメトリクス製品の開発を実現するための課題について検討する．

また，調査の過程で得られたバイオメトリクス特有の脅威および脆弱性に関する知見は，2 節に含めて記述した．

3.2 バイオメトリクス対応 PP におけるセキュリティ機能要件の調査

3.2.1 Biometric Device Protection Profile (BDPP)

調査対象

ドキュメント名称： Biometric Device Protection Profile (Draft Issue 0.82)
発行元： Communications-Electronics Security Group, Biometric Working Group （英国）
発行日： 2001 年 9 月 5 日
入手元： http://www.cesg.gov.uk/site/ast/biometrics/media/bdpp082.pdf （2004 年 3 月 10 日現在）

策定経緯

BDPP は英国の Communications-Electronics Security Group, Biometric Working Group で策定されたものである．また，米国の産官学共同コンソーシアムである Biometric Consortium においても同様のセキュリティ要求仕様書の策定を目指しているが，そこでも本セキュリティ要求仕様書がたたき台として使用されている．現在，本セキュリティ要求仕様書はドラフトの位置付けである．

目的と適用範囲

本 PP の目的は，商用利用可能な生体認証装置に適用されるべき機能，および保証要件を定めることである．適用範囲はなんらかの手段で保護された資産へのアクセスを要求する者が，正当な権限をもつものか否かを判定する機能を有する商用の生体認証装置全般である．

ドキュメント構成

BDPP は ISO/IEC 15408 に準拠した以下の構成となっている．

第 1 章：用語説明を含む序文
第 2 章：評価対象（TOE）に関する記述
第 3 章：評価対象のセキュリティ環境
第 4 章：セキュリティ対策方針
第 5 章：IT セキュリティ要件
第 6 章：第 5 章までであげられた種々の要件についての根拠

本節では，第 2 章から第 5 章までの各内容について報告する．

要約

生体認証装置とは個々人に特有の身体的特徴や行動的特徴（指紋，掌形，虹彩や網膜の紋様，音声，動的署名など）を検査することで個人識別を行うものである．生体認証装置は認証を求めてきた人が誰かを判別するために，採取された個人の特徴と多数のイメージを登録したデータベースとを比較する．あるいは採取される個人の特徴と，データベースに登録されているその人に関する特徴とを比較する．

本 BDPP の目的は，保護の対象となる資産が格納されている（物理的あるいは論理的な）場所への

入口からの入場に際して，入場者が誰であるか，あるいは既に登録済みであるかを検査するために使用される商用の生体認証装置に適用できる機能，および保証要件を定めることである．

BDPP は個人と生体認証装置の関わり，および生体認証装置と入口の関わりに関する要件を含んでいる．しかし，本仕様書は資産に関わる要件を言及するものではない．言い換えるならば，ひとたびその人が入口から入ったならば，さらなる資産の保護についてはここで想定する生体認証装置以外の手段によって提供されなければならず，その場合の要件についてはここでは言及していない．特定の生体認証装置を前提とはせず，何を選ぶかは ST の著者にまかされる．

生体認証装置は個人の身元を確認する機能だけを持つ単純な装置である．本 BDPP は身元の確認，検証，監査，および完全性についての方針を支援するものである．

BDPP は EAL1 に追加を施したもの（EAL1+）から EAL4 までの 4 段階の保証レベルを明らかにするものである．PP への適合を主張する ST はどの保証レベルであるかを明確にすべきであり，例えば「本 ST は BDPP に保証レベル EAL1+で適合している．」といった宣言を含むべきである．

第 2 章 評価対象（TOE）の記述

BDPP の第 2 章では，BDPP で評価対象（TOE）となるバイオメトリクス認証装置の概要を定義している．次図に評価対象（TOE）を示す．

評価対象（TOE）は，保護された「資産」に通じる物理的・論理的な「入口」を通過しようとする人の身体的特徴を計測して入口の開閉を制御するものと定義している．具体的な装置の詳細については ST で定義するものとしている．

続いて，評価対象であるバイオメトリクス認証装置の装置構成についての概観を示している．バイオメトリクス認証装置は個人の生体的特徴を取り込む装置と，取り込んだ生体的特徴をデータベースと照合することにより比較を行う装置と，入口の開閉を制御する装置から構成されているものとして定義している．

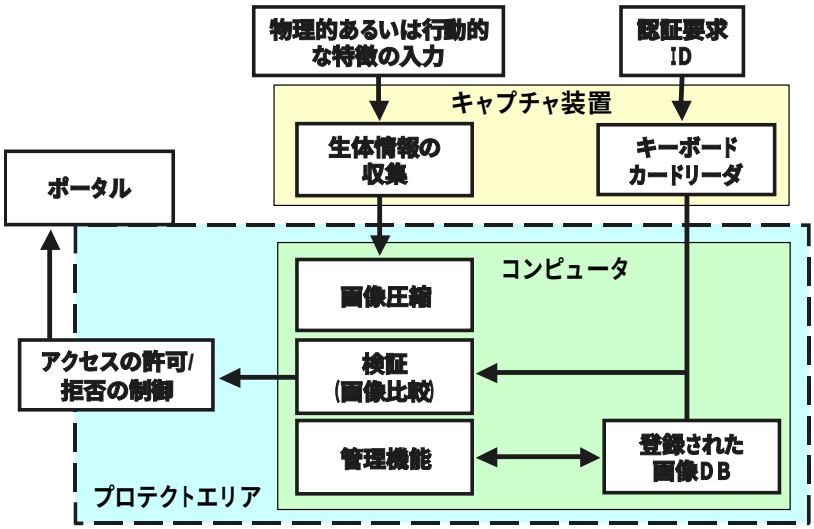


図 3-1 BDPP **の評価対象** (TOE)

第 3 章 評価対象(TOE)におけるセキュリティ環境

BDPP の第 3 章では，評価対象（TOE）に関する前提条件と脅威，運用ポリシーを列挙し，評価対象のセキュリティ環境を規定している．

BDPP の評価対象が安全と見なされるため，満たされるべき前提条件としては以下の五項目が挙げられている．

・A.PORTAL　本 PP が対象とするのは「入口（ポータル）」の防御に限られる．
・A.FALLBACK　バイオメトリクス認証装置が使用できない場合のセキュリティの確保はなされている．
・A.ROLES　本 PP が対象とするのは，管理者，操作者，正規利用者についてである．
・A.NO_EVIL　管理者は不正をしない．
・A.USERTMPL　利用者側に生体認証テンプレートを持たせる場合，検査することが可能である．

BDPP の評価対象に関連する脅威としては以下の 18 項目を列挙している．「ものまね」や「生体特徴の偽造」,「類似（双子など）」「残留」など，バイオメトリクス特有の問題も脅威として取り上げており，セキュリティの観点で漏れのない脅威抽出を行っている．

バイオメトリクス特有の脅威は以下の通りである．
・**T.CASUAL**　特に何もしなくても認証された利用者になりすまされる場合がある．
・**T.MIMIC**　ものまねによるなりすまし．
・**T.ARTIFACT**　人工の生体的特徴（手形など）によるなりすまし．
・**T.WEAKID**　脆弱な ID を狙ったなりすまし．
・**T.EVILTWIN**　類似あるいは瓜二つの生体テンプレートでのなりすまし．
・**T.RESIDUAL**　直前の利用者の残留生体イメージによるなりすまし．
・**T.POORIMG**　ノイズの載った画像，あるいは存在しない画像によるなりすまし．
・**T.ILLENROL**　生体認証システムへの不正な登録によるなりすまし．

その他の脅威は以下の通りである．
・T.FAKETMPL　生体テンプレートの偽造によるなりすまし．
・T.BADUSER　権限を越えた利用者による不正利用．
・T.BADADM　正当な管理者による意図しない誤用．
・T.BADOPER　正当なオペレータによる定期点検時の誤用．
・T.BYPASS　バイオメトリクス認証装置を迂回することによる不正利用．
・T.CORRUPT　FRR や FAR などの設定を改変されることによる誤動作．
・T.UNDETECT　検知不能な攻撃．
・T.POWER　電源断によるバイオメトリクス認証装置の誤動作．
・T.NOISE　大量のノイズによるバイオメトリクス認証装置の誤動作．
・T.TAMPER　バイオメトリクス認証装置の全部，あるいは一部の構成を改変されることによる

誤動作.

さらに，評価対象が適用される組織の運用時の規則（ポリシー）がどうあるべきかについての三つの指針を示している．BDPP は，適用分野やアプリケーションを特定していないプロテクションプロファイルであるため，認証精度に関しては,「国家が認めた標準書が定めた規格に適合させる」との記述に留まっており，具体的な指針を示していない.

・P.FARFRR　バイオメトリクス認証装置は国家が認めた標準書が定めた規格に適合させる.
・P.TRAIN　関係者は装置の使用法と，セキュリティ問題および危険性の訓練を受ける.
・P.USERLIMIT　同一 ID の多数回の試行は拒否することで不正を防止する.

第 4 章セキュリティ対策方針

BDPP の第 4 章では，評価対象（TOE）とそのセキュリティ環境についてのセキュリティ対策要件が列挙されている．前節で列挙した脅威などのセキュリティ環境に基づき，それぞれどのようにセキュリティ対策をとるかの方針を述べている.

・O.FARFRR　評価対象は FAR と FRR について国家が認めた標準書の基準を満たす.
・O.ADMIN　評価対象の管理者権限は限定された管理者にのみ付与される.
・O.BYPASS　評価対象の迂回を防止する構造とする.
・O.NOFORGE　評価対象は認証データの詐称を検知する機能を持つ.
・O.OPER　評価対象の操作者権限は限定された操作者にのみ付与される.
・O.PHYS.TOE　評価対象のセキュリティ的に重要な部分は物理的に保護される.
・O.RECORD　評価対象は発生した事象のうち管理に必要なものは適切に記録する.
・O.USERLIMIT　多数回の試行によるなりすましを防止する.
・O.ENROL　生体認証データの登録はセキュリティを確保できる，訓練された者だけによる.
・O.PHYS.ENV　評価対象の属する環境のセキュリティ的に重要な部分は物理的に保護される.
・O.SECOP　評価対象の運用は IT セキュリティを維持できる者だけが行う.
・O.TRAIN　全関係者に初期教育，継続教育を行う.
・O.USERTMPL　利用者側に生体情報テンプレートを持たせる場合，テンプレートを検査する.

ここで示したセキュリティ対策方針の根拠となる脅威などのセキュリティ環境については，BDPP の第 6 章で詳述している.

第 5 章 IT セキュリティ要件

BDPP の第 5 章では，評価対象（TOE）のセキュリティ機能要件およびセキュリティ保証要件を列挙している.

評価対象のセキュリティ対策方針を満たすために必要なセキュリティ機能要件について，ISO/IEC 15408 のパート 2 のセキュリティ機能要件集から抽出している．セキュリティ対策方針のうち，IT 技

術での対策が必要なものと，運用での対策が必要なものとに分けられる．IT 技術での対策が必要なものは，O.FARFRR，O.FEEDBACK，O.ADMIN，O.BYPASS，O.ENROL.TOE，O.NOFORGE，O.OPER，O.PHYS.TOE，O.RECORD，O.USERLIMIT の 10 のセキュリティ対策方針となる．このうち，バイオメトリクス特有の脅威に対応するセキュリティ対策方針に関連付けられた機能要件を表 3-1 に示す．特にバイオメトリクス特有の対策と考えられるものについては太字で示した．

ISO/IEC 15408 のセキュリティ機能要件集の規定に対し, BDPP の評価対象に合わせて, FIA_UAU.3,7 を生体情報データのみに適用するような改良や，FMT_MTD.3 や FAU_GEN.1 の用語を特定する改良を行っている．

表 3-1 セキュリティ機能要件

短縮名	説明	セキュリティ対策方針との関係
クラス FIA：識別および認証		
FIA_AFL.1	認証回数の制限機能	O.USERLIMIT,
FIA_ATD.1	利用者属性の定義機能	O.FARFRR O.ADMIN, O.OPER
FIA_UAU.2	実行前の利用者認証機能	O.FARFRR, O.ADMIN, O.BYPASS, O.OPER
FIA_UAU.3	**認証の偽装対策機能**	O.NOFORGE
FIA_UAU.7	**認証応答の保護機能**	O.FEEDBACK
FIA_UID.2	実行前の利用者識別機能	O.FARFRR O.ADMIN, O.BYPASS, O.OPER
クラス FMT：セキュリティ管理		
FMT_MOF.1	セキュリティ機能動作の管理機能	O.ADMIN, O.OPER, O.RECORD
FMT_MTD.1	**セキュリティ機能データの管理機能**	O.ADMIN, O.RECORD
FMT_MTD.3	**セキュリティ機能データの保護機能**	O.FARFRR, O.ENROL.TOE
クラス FPT：信頼できるセキュリティ機能の保護		
FPT_AMT.1	抽象マシン試験機能	O.ADMIN
FPT_RCV.1	手動回復機能	O.ADMIN, O.OPER
FPT_TST.1	セキュリティ機能の試験機能	O.ADMIN

以下，バイオメトリクス特有の対策と考えられる機能要件について詳述する．

FIA_UAU.3：認証の偽装対策機能

FIA_UAU.3.1（詳細化）

TSF は利用者から偽造されたバイオメトリクス認証データを検知および防止しなければならない．Application Note：ここでいうバイオメトリクス認証データには，テンプレートも含まれる．したがって，TOE は攻撃者によって作成されたテンプレートを識別する必要がある．本機能要件は，利用者の

「ものまね」を検知する意図はない．ものまねは偽造には相当しないと考えられている．ものまねによる対策は，O.FARFRR における FAR の要件を TOE が満たすことでなされる．評価者は特定のバイオメトリクス技術に影響する偽造の脆弱性に関する情報について検証する必要がある．

FIA_UAU.3.2 （詳細化）

TSF は利用者から複製されたバイオメトリクス認証データを検知および防止しなければならない．
Application Note：利用者からのバイオメトリクス認証データの偽造は複製を含むため，FIA_UAU.3.1 とはオーバーラップする場合がある．本機能要件は，リプライアタックの防止を意図したものではない．リプライアタックは，FPT_RPL.1 によって対策される．また，本機能要件はものまねの防止を意図したものでもない．

FIA_UAU.7：認証応答の保護機能

FIA_UAU.7.1 （詳細化）

TSF は［割付：攻撃者のなりすましを援助しないフィードバック］のみを提供しなければならない．
Application Note：バイオメトリクス装置は利用者にいかなる類似度やしきい値なども知らせてはならないことを意味する．また，提示した生体情報の画像などもこのフィードバックに相当する．

FMT_MTD.1：セキュリティ機能データの管理機能

FMT_MTD.1.1（1） （詳細化）

TSF は［割付：バイオメトリクスシステムの性能を制御するパラメータのリスト］の変更を管理者に対して制限しなければならない．
Application Notes：バイオメトリクス認証装置の性能はパラメータ（しきい値など）に依存する．パラメータの変更は信頼できるスタッフのみに制限されるべきであり，さもなければ安全性が低下する．

FMT_MTD.3：セキュリティ機能データの保護機能

FMT_MTD.3.1 （詳細化）

TSF は安全な値だけがテンプレートを登録するために受理されることを保証しなければならない．
Application Note：バイオメトリクスのセキュリティレベルはテンプレートの品質に関連する．一般的に人間が登録の品質を評価することは難しいため，TOE はテンプレートの品質を評価し，低品質の登録を排除する手段を提供できなければならない．TOE が自動的に低品質のテンプレートを排除するか，管理者に品質を示すことができる．

また，BDPP が対象にしている EAL1+～4 までのセキュリティ保証要件について，ISO/IEC 15408 のパート 3 のセキュリティ保証要件集から抽出している．バイオメトリクス特有の保証要件は追加されていない．

3.2.2 Biometric Verification Mode Protection Profile（BVMPP）

調査対象

ドキュメント名称： Biometric Verification Mode Protection Profile
for Medium Robustness Environments (version 1.0)

発行元： National Security Agency , Information Assurance Directorate（米国）

発行日： 2003 年 11 月 15 日

入手元： http://niap.nist.gov/cc-scheme/PP_VID1022.html （2004 年 3 月 10 日現在）

策定経緯

BVMPP は米国国防省の Biometrics Management Office（BMO）および National Security Agency（NSA）の支援により策定された．現在 National Information Assurance Partnership（NIAP）の Common Criteria Evaluation and Validation Scheme（CCEVS）にドラフトとして登録されている．これまでの経緯は以下の通り．

・2002 年 12 月 12 日 Version 0.5 発行

・2003 年 11 月 15 日 Version 1.0 発行

また，バイオメトリクス認証装置を対象とした Basic Robustness Environment 版，およびバイオメトリクス識別装置を対象とした PP も策定中である．

目的と適用範囲

本 PP の目的は, 生体認証装置に適用されるべき最低限の機能要件と保証要件を定めることである．適用範囲は Medium Robustness Environment における情報システムへの物理的あるいは論理的なアクセスコントロールに利用される生体認証装置である．Medium Robustness Environment とは，中程度のセキュリティを要求される環境を意味する．詳細は，BVMPP の第 3.0 節を参照のこと．

ドキュメント構成

BVMPP は ISO/IEC 15408 に準拠した以下の構成となっている．

第 1 章：用語説明を含む序文

第 2 章：評価対象（TOE）に関する記述

第 3 章：評価対象のセキュリティ環境

第 4 章：セキュリティ対策方針

第 5 章：IT セキュリティ要件

第 6 章：第 5 章までであげられた種々の要件についての根拠

本節では，第 2 章から第 5 章までの各内容について報告する．

要約

本 PP では，生体認証装置に適用されるべき最低限の機能要件と保証要件が定められている．バイオメトリクスの特性のため，CC の要件を大幅に改善する必要があった．本 PP の要件では，機密性と完全性を実現するために，テンプレート保護の必要性を明記している．利用者の ID やテンプレートは TOE の制御範囲外に保管されるため，TOE はこれらのデータを暗号化し，電子署名を付与する．

本 PP に従う TOE は特定の機能要件と，Medium Robustness な保証要件を満たす．保証要件は EAL4 を基準にしているが，Medium Robustness に必要な保証レベルを確保するため，明示的な要件が ADV ファミリに追加されている．

第 2 章 評価対象（TOE）の記述

BVMPP の第 2 章では，評価対象（TOE）となるバイオメトリクス認証装置の概要を定義している．本 PP における TOE は，センサから入力された生体情報とテンプレートを照合し，一致/不一致を結果として出力する．TOE は利用者のデータを保存せず，いかなるインターフェースも利用者には提供しない．したがって，TOE は TSF データのみを保存し，提供されるインターフェースは管理機能のためだけに存在する．利用者のテンプレートは TOE 外部に保管されるが，TOE によって暗号化および署名が付与される．また，TOE はバイオメトリクス以外の手段による本人確認機能を持つ．

図 3-1 は本 PP の TOE において必要とされる主なコンポーネントを示している．各機能の説明は下記の通り．

（1）Liveness Check & Capture

Liveness Check 機能は受け付けた生体情報が生体から得られたものかをチェックし，Capture 機能は生体情報からサンプルを取得する．

（2）Extraction

サンプルから特徴量を抽出する．

（3）Package Creation

登録時のみ機能し，暗号的な手段でユーザの ID とテンプレートを関連付け Biometrics Package を生成する．本 PP では，登録管理者のみが利用者を TOE に登録できる．

（4）Package Assurance

登録時のみ機能し，暗号を用いて Biometrics Package の機密性と完全性を保持する．

（5）Package Validation

認証時のみ機能し，Biometrics Package の完全性と署名の検証を行う．

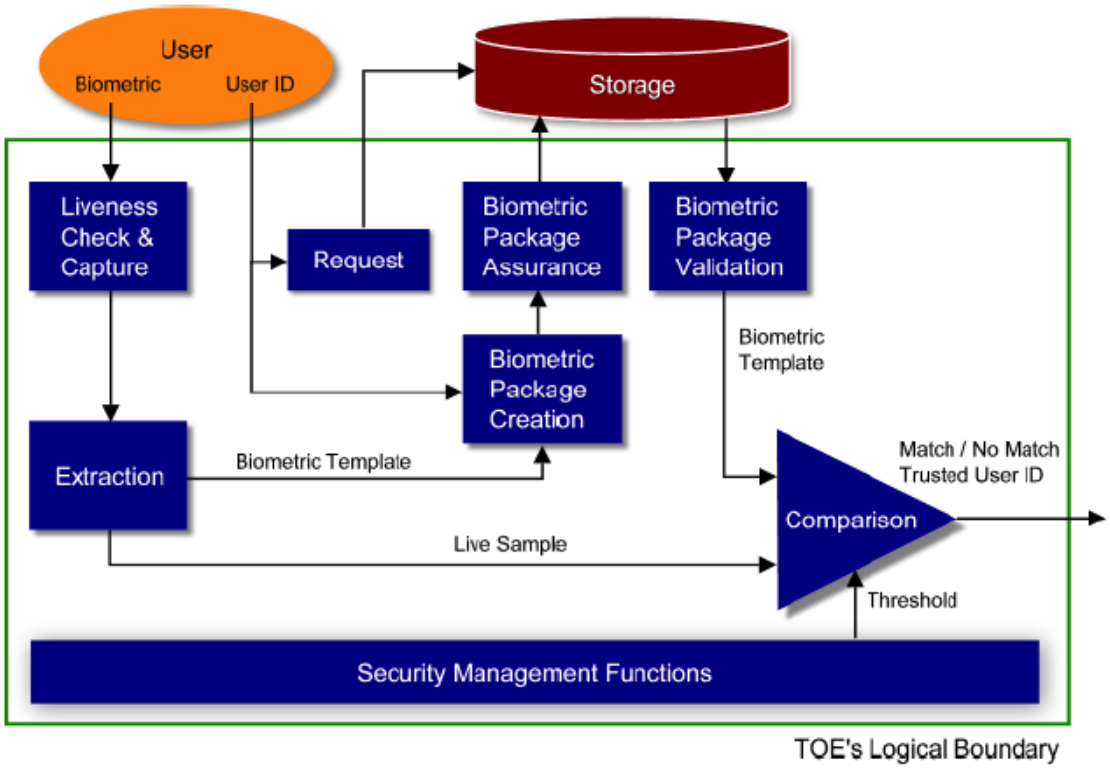
（6）Comparison

認証時のみ機能し，生体情報のサンプルとテンプレートを比較し，類似度を出力する．その後，類似度はしきい値と比較される．本 PP は類似度が最大値あるいは最小値の範囲をこえる場合，不一致の結果を生成することを要求している．

（7）Security Management Functions

TOE 管理者に対して提供される機能であり，しきい値の設定，監査イベントの決定，監査情報の閲覧，鍵管理などを行う．

本 PP における暗号および暗号モジュールは，公的な標準を満たし，かつ NIST の FIPS140-2 に準拠しなければならない（must）.



BDPP Figure.2 より

図 3-2 BVMPP の評価対象 (TOE)

第 3 章 評価対象(TOE)におけるセキュリティ環境

前提条件

満たされる前提条件としては以下の 3 項目が挙げられている.

・A.ENROLLMENT_APPROVAL
登録される利用者の身元を確認するため，適切な手順がとられる.

・A.NO_GENERAL_PURPOSE
TOE 上で一般目的の計算やデータ保管が行われることはない.

・A.OPERATING_RANGE
TOE はベンダがさだめた通常の環境（温度や湿度）を越えない環境におかれる.

脅威

BVMPP で識別している脅威は，以下の通りである．暗号に関係する脅威が多く，バイオメトリク

ス特有の脅威は BDPP に比べて少ない．特に FAR につけこんだ脅威，BDPP では T.CASUAL として識別されている，が識別されていない．

バイオメトリクス特有の脅威は以下の通り．

・**T.HIGH_QUALITY_ARTIFACT**

攻撃者が精巧に作られた人工的な生体情報でなりすます．

・**T.MIMIC**

攻撃者が利用者と似たような生体情報を提示しなりすます．

・**T.REPLAY_RESIDUAL_IMAGE**

攻撃者が利用者の生体情報の痕跡を再利用し，なりすます．

・**T.POOR_ENROLLMENT**

攻撃者は低品質のテンプレートを攻撃しなりすます．

・**T.RESIDUAL_DATA**

攻撃者がメモリ内の利用者の生体情報の痕跡を利用しなりすます．

・**T. REFERENCE_TEMPLATE**

攻撃者はテンプレートを改ざんしなりすます．

また，本 PP の TOE に要求される組織のセキュリティポリシーとして下記が挙げられている．

・P.ACCESS_BANNER

TOE は使用の制限，法的同意，あるいは他の適切な情報を利用者に表示しなければならない．

・P.ACCOUNTABILITY

TOE に認証された利用者は TOE 内における行動に責任を持たなければならない．

・P.CRYPTOGRAPHIC_FUNCTIONS

TOE は，TSF データの機密性の確保と改ざん検知のために暗号機能を提供しなければならない．

第４章 セキュリティ対策方針

BVMPP の第 4 章では，セキュリティ対策方針を記述している．ここでは，第 3 章に挙げたバイオメトリクス特有の脅威に関係するセキュリティ対策方針を記述する．

・O.AUTHENTICATION

TOE はバイオメトリクス認証機構を IT 環境および非 IT 環境の利用者に提供する．

対応する脅威：T.HIGH_QUALITY_ARTIFACT，T.MIMIC，T.REPLAY_RESIDUAL_IMAGE，T.POOR_ENROLLMENT，T．REFERENCE_TEMPLATE

・O.ROBUST_TOE_ACCESS

TOE は利用者の TOE への論理アクセスを制御し，明示的に特定の利用者のアクセスを拒否する機構を提供する．

対応する脅威：T.MIMIC

・O.RESIDUAL_INFORMATION
TOE 内部に残されたバイオメトリクスデータの再利用を防ぐため，保護すべき情報は開示されない．
対応する脅威：T.RESIDUAL_DATA

第 5 章 IT セキュリティ要件

BVMPP の第 5 章では，評価対象（TOE）のセキュリティ機能要件およびセキュリティ保証要件を列挙している．セキュリティ機能要件は，TOE が暗号機能を含むため広範囲にわたる．ここでは，バイオメトリクス特有の脅威に関連付けられるセキュリティ機能要件とセキュリティ保証要件について詳述する．

表 3-1 にバイオメトリクス特有の脅威に関連付けられるセキュリティ対策方針の一覧を示す．特にバイオメトリクス特有の対策に相当するセキュリティ機能要件を太字で示した．

表 3-2 セキュリティ機能要件

短縮名	説明	セキュリティ対策方針との関係
クラス FDP：利用者データ保護		
FDP_RIP.2	**残存情報保護**	O.RESIDUAL_INFORMATION
クラス FIA：識別および認証		
FIA_AFL.1	認証回数の制限機能	O.ROBUST_TOE_ACCESS
FIA_ATD.1	利用者属性の定義機能	O.ROBUST_TOE_ACCESS
FIA_ENROLL_EXP.1	**登録機能**	O.AUTHENTICATION
FIA_SOS.1	秘密の検証	O.ROBUST_TOE_ACCESS
FIA_SOS.2	**TSF 秘密生成**	O.ROBUST_TOE_ACCESS
FIA_UAU.2	実行前の利用者認証機能	O.ROBUST_TOE_ACCESS
FIA_UAU.5	**複数の認証メカニズム**	O.AUTHENTICATION O.ROBUST_TOE_ACCESS
FIA_UAU.7	**認証応答の保護機能**	O.ROBUST_TOE_ACCESS
FIA_UID.2	実行前の利用者識別機能	O.AUTHENTICATION O.ROBUST_TOE_ACCESS
クラス FPT：信頼できるセキュリティ機能の保護		
FPT_ITC_EXP.1		O.AUTHENTICATION
FPT_ITI_EXP.1		O.AUTHENTICATION
クラス FTA：TOE アクセス		
FTA_TSE.1	TOE セッション確立	O.ROBUST_TOE_ACCESS
FTA_SSL.3	TSF 起動による終了	O.ROBUST_TOE_ACCESS

以下，上表に示した，バイオメトリクス特有の対策に相当するセキュリティ機能要件について述べる．

FDP_RIP.2：残存情報保護

FDP_RIP.2.1 詳細化

TSF はすべてのリソースからなる古い情報を，すべてのオブジェクトの［選択：リソース配置，リソース削除］に際して，あるいは TSF の終了に際して，使用不能としなければならない．

Application Note:このセキュリティ機能要件は，認証終了後に TOE に残留したバイオメトリクスデータを使用不能にする．例えば，キャプチャデバイスのメモリや照合機能，判定機能のメモリをクリアすることを意味する．

FIA_ENROLL_EXP.1：登録機能

本セキュリティ機能要件は，CC の機能要件セットに追加されたものであり，利用者の登録における要件を規定している．規定されている要件は以下の通り．

a） 信用できる利用者の ID およびテンプレートなどを含んだバイオメトリクスパッケージは，登録処理のみで生成される．

b）テンプレートは改ざんされない

c）登録（初期登録およびテンプレートの更新や追加）は登録管理者によって実施される．

d）FTE は［割付：ST 開発者によって設定された 5%を超えない値］とする．

e）登録管理者は新規に生成されるテンプレートの品質測定基準を提供される．

Application Note：バイオメトリクスのセキュリティレベルはテンプレートの品質に関連する．本 ST 開発者は明示的な品質基準を登録管理者に与え，十分な品質に達しないテンプレートを排除すべきである．また，ST 開発者は，既存のテンプレート間で照合を行う機能を設計することもできる．これにより登録管理者は簡単に区別できない利用者の組み合わせを知ることができる．ただしこの種の情報は，攻撃者に悪用される可能性があるため，秘匿されるべきである．

f）登録が成功した場合，バイオメトリクスパッケージは TOE によって電子署名され，保管される前に暗号化がなされる．

g）［選択：［割付：ST 開発者によって決められる他の規定］,なし］.

FIA_SOS.2：TSF 秘密生成

FIA_SOS.2.1-TSFは，以下に合致する秘密を生成するメカニズムを提供しなければならない．

a）FAR はセキュリティ管理者が定めた最小［割付：ST 開発者が割り付けた値］から最大 1/100,000 の範囲になければならない．

b) FRR はセキュリティ管理者が定めた最小［割付：ST 開発者が割り付けた値］から最大 5/100 の範囲になければならない．

（注）上記 FAR および FRR は T.MIMC に対しても実現されなければならない．

FIA_UAU.5：複数の認証メカニズム

FIA_UAU.5.2 詳細化：

TSF は以下に相当するどんな利用者の身元も認証しなければならない.

非管理者に対して，TSF は利用者を認証し，信頼しうる ID に IT 環境を提供し，以下の規定に従って一致もしくは不一致の決定をしなければならない.

a）セキュリティ管理者の選択により，［割付：TOE が生体検知で実施する内容の記載］からなる［選択：無意識の，意識した，協力的な，生命活動に関する，realness］生体検知を実施する．生体検知に失敗した場合は，TOE はテンプレートとの比較を行わない.

b）バイオメトリクスパッケージの完全性をチェックし，TOE あるいは信頼できる機関が署名していることを確認する.

c）一致判定を提供するために，類似度はある最大値と最小値の間に存在し，そうでなければ不一致の決定を生成する.

d）セキュリティ管理者の選択によって，TOE は一定期間内に連続する同一の ID からの認証要求を受け付けない.

管理者に対しては, バイオメトリクス認証あるいは非バイオメトリクス認証を選択することができる. あるいは両方を用いてもよい．バイオメトリクス認証を用いる場合の要件は，上記 a）～d）と同じである. 両方の認証方式を用いる場合, 両者の結果がそろうまで, 利用者に結果を通知してはならない.

FIA_UAU.7：認証応答の保護機能

FIA_UAU.7.1 詳細化

TSF は利用者が TOE に生体情報を提示するための説明だけを提供しなければならない．これは，バイオメトリクス装置は利用者にいかなる類似度やしきい値なども知らせてはならないことを意味する．明示的には記述がないが，生体情報のモニタなども含まれると考える.

BDMPP の保証要件は，CC の保証要件セットに準拠しておらず，独自の保証要件セットを記述している．これはおおむね EAL4+に相当すると考える．ただし，ADV_FSP は存在しない.

バイオメトリクス特有の追加・拡張はなされていないため，本報告書では詳細を説明しない.

3.3 バイオメトリクス対応 CEM におけるセキュリティ保証要件の調査

本節では，ISO/IEC 15408（Common Criteria：CC）の評価における標準評価方法（Common Evaluation Methodology：CEM［6-8］）をバイオメトリクスに適用する際に考慮すべき追加要件をまとめた Biometrics Evaluation Methodology（BEM）［17］の概要を述べる．

調査対象

- ドキュメント名称：Biometrics Evaluation Methodology Version 1.0
- 発行元：The Common Criteria Biometric Evaluation Methodology Working Group
- 発行日：2002 年 8 月
- 入手元：http://www.cesg.gov.uk/technology/biometrics/media/BEM_10.pdf

策定経緯

BEM は Common Criteria（CC）の評価における Common Evaluation Methodology（CEM）をバイオメトリクスに適用する際に考慮すべき追加要件をまとめる目的で作成された．作成元は，非公式の国際グループ Biometric Evaluation Methodology Working Group （BEM WG）であり，オーストラリア，ニュージーランド，アメリカ，カナダ，ドイツ，イギリス，イタリア，フィンランドの評価機関，認証組織, バイオメトリクスベンダなどの代表からなる. 現在 BEM は, ISO/IEC JTC1 SC27 で検討中の ISO 19792 " A framework for security evaluation and testing of biometric technology"の 1st Working Draft の Annex として提案されている．今後の対応については検討中であり，19792 として採用されるか否かは現在のところ不明である．これまでの主な策定の経緯は以下の通り．

・2002 年 8 月：バージョン 1.0 を発行．公的機関からは未承認.
・2003 年 4 月：SC27 NP19792 への寄書（N3522）としてカナダより提出.
・2003 年 10 月：BEM は NP19792 の WD の Annex に含める決定
・2003 年 11 月：NP19792 の 1st WD（SC27N3806）発行

目的と適用範囲

バイオメトリクスシステムは，他の IT システムと同様に CC に基づいた評価が可能であるが，現状の CC はバイオメトリクス製品の適切な評価方法を提供していない．バイオメトリクス製品実装は，アプリケーションの性質，使用環境，ユーザなどに依存するが，現状の CC や CEM ではこれらの特性が十分にカバーされないためである．そのため，CC に基づくバイオメトリクス製品の評価方法を明確化する必要がある．そこで，ITSEF で実施される予備的な評価での使用，および CCIMB により，CC の補足文書としての可能性を検討するため， BEM ver1.0 を発行する．

BEM の目的は，バイオメトリクス製品評価の保証要件に適用可能な CC の評価方法論を明確にすることである．また，ST 評価に関する追加的なガイドラインを示す．具体的には，適当なセキュリティ機能の選択，脆弱性と脅威，統計的試験などである．

ドキュメント構成

BEM の構成は以下の通り．本報告書では 2 章および 3 章について報告する．

1. Introduction
   背景，目的，文書構成，典型的なバイオメトリクスシステムのモデル
2. Assurance Requirements and Evaluation Methodology
   バイオメトリクスの評価に関する CC の保証要件
   CEM を補足するための追加的なガイダンスの概要
3. Testing and Analysis
   評価において特有の問題を生ずるバイオメトリクスの性質の詳細
4. Conclusion

要約

BEM の目的は，CC におけるバイオメトリクス製品およびシステムの保証要件に適した評価方法論を明確化することにある．BEM はさらに ST 評価の定義に関連した追加的なガイドラインを含む．たとえば，適切なセキュリティ機能の選択，脆弱性と脅威，統計的な試験などである．

バイオメトリクスシステムは，他の IT システムと同様に CC に基づいた評価が可能であると結論している．CC のセキュリティ機能要件は，CEM における評価プロセス，評価保証レベル（Evaluation Assurance Level：EAL）はバイオメトリクスシステム評価の ST で使用可能である．さらに本文書で示した助言により適切に解釈が可能である．ただし，EAL1 にセキュリティ機能強度（Strength of Function：SOF）として精度評価を追加すべきである．

バイオメトリクスシステムの評価において特に注意すべき点を以下にまとめる．

a) バイオメトリクス特有の脅威と脆弱性
   例えば，生体情報の偽造など．評価において，これらの脅威を検討し，TOE の Penetration Testing で明確化する必要がある．

b) 統計的な性能試験
   例えば，他人受入率（False Accept Rate：FAR）とその解釈などが重要である．

c) 物理的な環境要因を考慮した性能試験の実施
   物理的な環境はシステム構成の定義の一部として制御される必要がある

第 2 章 Assurance Requirements and Evaluation Methodology

本章では，CC におけるセキュリティ保証要件のバイオメトリクスシステムの設計，開発，運用に対する適合性を検討している．

CC におけるセキュリティ保証要件は，一般的な IT セキュリティシステムやコンポーネントと同様に，バイオメトリクスにも適用可能と考えられる．つまり，すべての保証要件のクラス，ファミリ，

コンポーネントはバイオメトリクスシステムに適用可能である．

ただし，バイオメトリクスのセキュリティ評価では，以下の三点を特に考慮しなければならない．

a） 脆弱性の分析（Analysis of Vulnerabilities）

評価者はバイオメトリクス特有の脆弱性に精通していなければならない．また，脆弱性試験のための専門技術と施設が必要となる．

b） 性能評価（Performance Testing）

評価者は，開発者が FAR（False Acceptance Rate）のような統計値を立証するために行った試験を慎重に検査しなければならない．また，自ら試験を実施することでこれらをチェックする必要がある．

CC 準拠の評価方法は標準評価方法論（Common Evaluation Methodology：CEM）にまとめられている．本章ではバイオメトリクスシステム特有の説明をこれに加える．以下，バイオメトリクス特有の考慮が必要となる保証要件についてのみ述べる．

ST 評価および PP 評価

バイオメトリクスの ST 評価および PP 評価においては，評価者は以下に注意する必要がある．

b) バイオメトリクスシステムの記述は，取り込み装置（capture device）の物理環境および運用環境を含まなければならない．また，環境の制御や試験（Environmental Test）に関する要件も記述しなければならない．

c) セキュリティ機能強度（Strength of Function：SOF）は FAR と関連付ける必要がある．

評価保証レベル

バイオメトリクスにおける評価保証レベル（EAL）を表 3-3 にまとめる．表において［+］は CEM の要件に付け加えるべきコンポーネントを，［*］は BEM で詳説するコンポーネントを表す．

CC パート 3 で定義されている EAL はバイオメトリクスシステムの評価に対しても適切である．ただし，SOF として測定される FAR をはじめとした統計値の重要性を考慮し，EAL1 においても AVA_SOF（TOE セキュリティ機能強度）を加えることを強く推奨する．

以下の節では，バイオメトリクスに必要となる評価アクション（evaluation action）を示し，各ワークユニット（work unit）ごとに CEM を補完する解説を付け加える．

表 3-3 評価保証レベルのまとめ

Assurance Class	Family	EAL1	EAL2	EAL3	EAL4
Configuration Management	ACM_AUT				1
	ACM_CAP	1	2	3	4
	ACM_SCP			1	2
Delivery and Operation	ADO_DEL		1	1	2
	ADO_IGS	1	1	1	1
Development	ADV_FSP	1	1	1	2
	ADV_HLD		**1 [*]**	**2 [*]**	**2 [*]**
	ADV_IMP				1
	ADV_INT				
	ADV_LLD				1
	ADV_RCR	1	1	1	1
	ADV_SPM				1
Guidance Documents	**AGD_ADM**	**1 [*]**	**1 [*]**	**1 [*]**	**1 [*]**
	AGD_USR	**1 [*]**	**1 [*]**	**1 [*]**	**1 [*]**
Life Cycle Support	ALC_DVS			1	1
	ALC_FLR				
	ALC_LCD				1
	ALC_TAT				1
Tests	ATE_COV		1	2	2
	ATE_DPT			1	1
	ATE_FUN		**1 [*]**	**1 [*]**	**1 [*]**
	ATE_IND	**1 [*]**	**2 [*]**	**2 [*]**	**2 [*]**
Vulnerability Assessment	AVA_CCA				
	AVA_MSU			**1 [*]**	**2 [*]**
	AVA_SOF	**1 [+] [*]**	**1 [*]**	**1 [*]**	**1 [*]**
	AVA_VLA		**1 [*]**	**1 [*]**	**2 [*]**

出典：BEM Table 1: Evaluation Assurance Level Summary

ADV（開発）

ADV クラスは上位レベル設計に関する要件を含む（ADV_HLD ファミリ）．バイオメトリクスシステムのロバスト性を評価する上で，評価者は策定中のバイオメトリクスに関する標準を考慮することができる．

より高い EAL において, 評価者は開発者がどのようにバイオメトリクスの標準に従ったかを検討することができる．また，システム設計の解析にこれらの標準を利用することができる．

バイオメトリクスの標準としては，現在，BioAPI，CBEFF，X9.84 などがある．

表 3-4 上位レベル設計 (ADV_HDL) アクションの追加要件

Applicable EAL(s)	Evaluator Action ADV_	Work Unit :ADV_	Comments
2, 3, 4	HLD.1.1E, HLD.2.1E	HLD.1-1, HLD.2-1	No additional comments.
		HLD.1-2, HLD.2-2	No additional comments.
		HLD.1-3, HLD.2-3	No additional comments.
		HLD.1-4, HLD.2-4	No additional comments.
		HLD.1-5, HLD.2-5	No additional comments.
		HLD.1-6, HLD.2-6	No additional comments.
		HLD.1-7, HLD.2-7	No additional comments.
		HLD.1-8, HLD.2-8	No additional comments.
3, 4	HLD.2.1E	HLD. 2-9	インターフェースの記述は BioAPI や CBEFF といった標準に従うかもしれない
		HLD.2-10	No additional comments.
2, 3, 4	HLD.1.2E, HLD.2.2E	HLD.1-9, HLD.2-11	インターフェースの記述は BioAPI や CBEFF といった標準に従うかもしれない
		HLD.1-10, HLD.2-12	No additional comments.

出典：BEM Table 2: High Level design (ADV_HLD)

AGD（ガイダンス文書）

AGD クラスはガイダンス文書の要件である．AGD クラスの要件はバイオメトリクスに対しても適切であるが，評価においてはさらに下記の助言がある．

a） 生体情報のプライバシ（Biometric Privacy）

生体情報（biometric data）の収集と保管に関する個人的あるいは法的な問題が記述されなければならない．詳細は Annex C, section C.8.を参照のこと．

b） 環境の影響（Environmental Influences）

バイオメトリクスシステムの運用は物理的な環境から強い影響を受ける. 例えば明るさや音の強さ，ほこり，湿気，取り込みデバイスの清潔さなどである．また，これらは登録や照合処理の正確さにも影響を与える．したがって，ガイダンス文書は環境の影響に関する情報と，これらの影響を最小限にする方法について記述しなければならない．環境試験（environmental testing）に関しては第 3.2.2 節を参照のこと．

c） しきい値の設定（Setting of Thresholds）

照合においてマッチングのしきい値が変更可能な場合，ガイダンス文書は，しきい値を変更した場合の影響，しきい値変更の意味，セキュリティの決定におけるしきい値変更の重要性，について記述しなければならない．

表 3-5 管理者ガイダンス (AGC_ADM) アクションの追加要件

Applicable EAL(s)	Evaluator Action AGD_	Work Unit :AGD_	Comments
1, 2, 3, 4	ADM.1.1E	ADM.1-1	No additional comments.
		ADM.1-2	環境管理および環境要因がセキュリティに与える影響について記述すべき
		ADM.1-3	閾値の変更には安全な制御が必要であることを記述すべき
		ADM.1-4	登録プロセスにおける利用者の監視・管理の必要性を含めることができる
		ADM.1-5	認証閾値はセキュリティパラメタとして認識される必要がある
		ADM.1-6	No additional comments.
		ADM.1-7	No additional comments.
		ADM.1-8	No additional comments.

出典：BEM Table 3: Administrator Guidance (AGD_ADM)

表 3-6 ユーザガイダンス (AGD_USR) アクションの追加要件

Applicable EAL(s)	Evaluator Action AGD_	Work Unit :AGD_	Comments
1, 2, 3, 4	USR.1.1E	USR.1-1	No additional comments.
		USR.1-2	No additional comments.
		USR.1-3	No additional comments.
		USR.1-4	生体情報取得プロセスの記載と考慮すべき環境条件を記載すべき．登録プロセスに対する専用の説明を記載することができる．プライバシーなどの問題を記載することができる
		USR.1-5	No additional comments.
		USR.1-6	No additional comments.

出典：BEM Table 4: User Guidance (AGD_USR)

ATE（テスト）

本保証クラスは，TSF（Target of Evaluation Security Function）がセキュリティ機能要件を満足していることを示すための試験の要件を定義する. 基本的に ATE クラスのファミリおよびコンポーネントはバイオメトリクスにも適用可能である.

バイオメトリクスシステムの振る舞いは取り込み装置（capture device），アルゴリズム，環境条件（environmental condition），本人同士と他人同士の特徴量の分布，に依存する．これらを理論的に解析するのは困難であるため，バイオメトリクスのセキュリティ機構（security mechanism）の効果を決定する上で，性能試験（performance testing）は必要不可欠である.

性能を示す主な特性としては，FMR，FNMR，あるいは FAR，FRR などがある．これらの値を得る

ための試験は，統計上典型的なデータを含まなければならない．試験は収集した生体情報のデータベースもしくは典型的な被験者グループの登録と照合によって行うことができる．データベースを用いる場合，サンプルの収集条件を慎重に検討しなければならない．また，装置の設定，機能の正当性確認，データ収集過程の一貫性などに注意を払わなければならない．詳細は" Best Practices in Testing and Reporting Performance of Biometric Devices,"［20］を参照のこと．

機能テスト（ATE_FUN）および独立テスト（ATE_IND）のアクションにおける追加要件は次表の通り．

表 3-7 機能テスト (ATE_FUN) アクションの追加要件

Applicable EAL(s)	Evaluator Action ATE_	Work Unit :ATE_	Comments
2, 3, 4	FUN.1.1E	FUN.1-1	No additional comments.
		FUN.1-2	FAR，FRR などの統計的性能試験および環境影響に関する試験を含む必要がある
		FUN.1-3	No additional comments.
		FUN.1-4	環境の制御設定を含むべきである
		FUN.1-5	No additional comments.
		FUN.1-6	No additional comments.
		FUN.1-7	No additional comments.
		FUN.1-8	No additional comments.
		FUN.1-9	No additional comments.
		FUN.1-10	必要な被験者数については“ Best Practice ”を参照する．
		FUN.1-11	No additional comments.
		FUN.1-12	No additional comments.

出典：BEM Table 5: Functional Tests (ATE_FUN)

表 3-8 独立テスト (ATE_IND) アクションの追加要件

Applicable EAL(s)	Evaluator Action ATE_	Work Unit :ATE_	Comments
1, 2, 3, 4	IND.1.1E, IND.2.1E	IND.1-1, IND.2-1	構成に関する解説には，環境上の制御について記述すべき
		IND.1-2, IND.2-2	環境条件の確認を含むべき
2, 3, 4	IND.2.1E	IND.2-3	No additional comments.
1, 2, 3, 4	IND.1.2E, IND.2.2E	IND.1-3, IND.2-4	FAR や FRR などに関する統計的性能試験を標準的に実施する
		IND.1-4, IND.2-5	No additional comments.
		IND.1-5, IND.2-6	No additional comments.
		IND.1-6, IND.2-7	No additional comments.
		IND.1-7, IND.2-8	No additional comments.
2, 3, 4	IND.2.3E	IND.2-9	No additional comments.
		IND.2-10	No additional comments.
1, 2, 3, 4	IND.1.2E, IND.2.3E	IND.1-8, IND.2-11	No additional comments.

出典：BEM Table 6: Independent Testing (ATE_IND)

AVA（脆弱性評定）

AVA_MSU（誤使用）に関して，精度に影響するすべての要因がガイダンスに記述されるべきである．具体的なワークユニットへのコメントは以下の通りである．

AVA_MSU.1-1, 2-1（ガイダンスと評価証拠の検査）

ガイダンスは，環境の制御，およびセキュリティへの環境要因の影響を含むべきである

AVA_MSU.1-4, 2-4（前提条件の適切な記述の検査）

ガイダンスは，IT 環境と同様に物理的な環境も含むべきである

AVA_MSU.2-10 （開発者の誤使用分析の検査）

ガイダンスは，閾値の設定方法を含むべきである

AVA_SOF（TOE セキュリティ機能強度）に関して，バイオメトリクスにおけるセキュリティ機能強度は，正しく利用者を識別する能力に依存する．これは，認証システムにおいては，運用環境における FAR として計測される．具体的なワークユニットへのコメントは次の通り．

AVA_SOF.1（ TOE セキュリティ機能強度評価）はすべての EAL に適用されるべき

AVA_SOF.1-4（SOF 分析の検査）

文献 [20]が認証精度に関して参考になる．また，マルチモーダルの場合，SOF 分析は必須．

AVA_SOF.1-5（SOF 分析の検査）

CEM Annex B.8，文献[31]，BEM3.3 節を参照のこと

AVA_VLA（脆弱性分析）に関して，バイオメトリクスの脆弱性分析には，通常の IT システムとは明らかにことなる特徴を有する．バイオメトリクス特有の脆弱性分析を考慮するには，BEM3.5 節を参照のこと．具体的なワークユニットへのコメントは以下の通り．

AVA_VLA.1-4，2-4（侵入テストの考案）
AVA_VLA.2-9（潜在的な脆弱性の仮定）
AVA_VLA.2-10（独立脆弱性分析による侵入テストの考案）
評価者はバイオメトリクスの脆弱性に関する適当な文献を参考にすべき．3.5 節など．

第 3 章 Testing and Analysis
本章では，バイオメトリクスの評価に関し，以下についての詳細な検討を行っている．

環境試験（Environmental Testing）
バイオメトリクスの安全性は環境に影響されるため，環境影響を含んだ試験を実施すべきである．バイオメトリクスシステムにおいて有意な環境的テストの範囲について検討する

機能強度（SOF）
バイオメトリクスシステムのセキュリティ性能は FAR などの値に関連する. FAR を含めた機能強度（SOF）の定義を検討する

統計的性能試験（Statistical Performance Testing）
バイオメトリクスシステムの SOF は，FAR や他の統計値により定義される．FAR のレベルを設定するために必要とされる被験者数を検討する

脆弱性試験（Vulnerability Testing）
バイオメトリクスに特有の脅威や脆弱性が存在しうる．例えば人工指による指紋システムへの攻撃などである．したがって，バイオメトリクス特有の脅威に関する検討が必要であり，評価機能はこれらの脅威に対する適当なテストを実施する必要がある．

以下各項目について説明する．

環境試験（Environmental Testing）
バイオメトリックスの性能は，他の情報システムで通常は扱わない物理的な環境条件に依存する．例えば，虹彩認識の照明レベル，音声認識の騒音，指紋認証の空気中のほこり，などである．様々な環境条件おいて，安全性にかかわる耐久性試験を実施する必要がある．耐久試験における
環境条件には，センサ，ハードウェア，ユーザへ影響する要因を考慮すべきである．また，バイオメトリクスシステムに対するあらゆる環境上の制限をガイダンスに記載しておく必要がある．さらに環境のテストは，センサの経年変化などを考慮し，定期的に実施すべきである．

次表にバイオメトリクスと精度に影響する環境要因の関連を示す.

表 3-9 バイオメトリクスと環境要因の関係

	虹彩	顔	指紋		手	音声
			光学センサ	半導体センサ		
照明条件	×	×	×		×	
騒音条件						×
温度			×	×	×	
電磁ノイズ	×	×	×	×	×	×
湿度			×	×		
埃, 汚染物質	×	×	×		×	
電源変動	×	×	×	×	×	×
衝撃と振動	×	×	×	×	×	×

機能強度（SOF）

機能強度（SOF）は他人受入率（FAR）に関係づけられるが，FAR と SOF との間の関係は単純に定義できない．バイオメトリクスの ST は，SOF の要件とその理論的根拠を含むべきであり，具体的な SOF の要件としては，FAR，FTA，FTE などの許容値が考えられる．したがって FAR を SOF レベルで定義する必要はないが，例えば下記のガイドラインが利用できる．

表 3-10 SOF レベルの設定例

SOFレベル	FARの最大値
SOF-Basic	0.01 (1 in 100)
SOF-Medium	0.0001 (1 in 10,000)
SOF-High	0.000001 (1 in 1,000,000)

上表はシングルモーダルのバイオメトリクスにおける FAR の許容値を示している. マルチモーダルバイオメトリクスや他の本人確認方式との併用時には，さらに複雑な統計上の論理的根拠が必要とされる.

統計的性能試験（Statistical Performance Testing）

SOF と FAR の関係を考慮すると，FAR の統計的な性能試験手法が重要となる．また，FRR，FTE（Failure to Enroll），FTA（Failure to Acquire）も統計的性能試験に含まれるべきである．統計的性能試験を実施する際には，ライブ/オフラインテストの選択，サンプルの母集団，環境条件，付加的な試験の要否などについて注意する必要がある.

評価試験の規模（被験者数）に関し，統計的信頼性を保証した被験者数の決定は困難であり，現実

には合理的に管理しうる最大数の被験者を用いることを推奨する．

統計的性能試験に関しては，以下を考慮する必要がある．

・性能試験は ST で定義されたものと同等のコントロールされた環境下で実施すべき
・性能試験は導入先のエンドユーザと同等の母集団に対して実施すべき
・統計的性能試験は，国家施策により認可された独立な施設で実施されてもよい
・国家施策に基づく認証機関に認められた過去の独立テストの結果を用いてもよい
・評価者にはバイオメトリクスの専門家に相談することを強く勧告する

脆弱性試験（Vulnerability Testing）

特定のバイオメトリック技術に関連する脆弱性を追加して考慮する必要がある．例えば，以下がある．数字は次図に記載の場所への攻撃を意味する．

①ユーザからの生体情報の取得/提供/共謀
②偽造，物まね
③④生体情報/特徴情報の盗聴，リプライアタック
⑤⑥⑦テンプレートの置き換え，不正テンプレート，盗聴
⑧しきい値の不適切な変更
⑨⑩⑪⑫⑬⑭⑮バイパス，無効化，監査の不十分

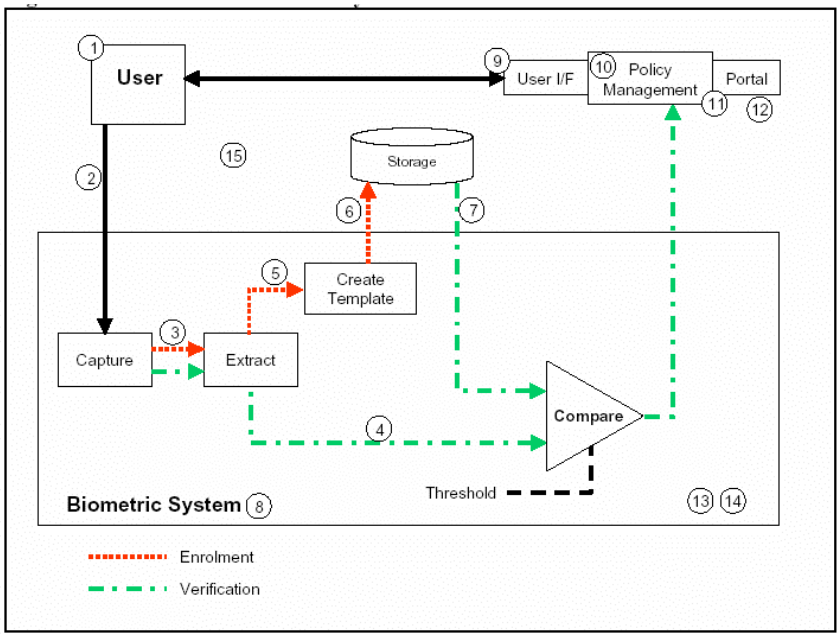


図 3-3 バイオメトリクスシステムの脆弱性

3.4 今後の課題

第 3 節では，ISO/IEC 15408 へのバイオメトリクス製品の適用可能性を調査する目的で，既存のバイオメトリクス向けプロテクションプロファイルと共通評価方法論について調査した．

具体的には，以下のドキュメントにおける，バイオメトリクス特有のセキュリティ機能要件と保証要件を抽出し，詳述した．

（1）Biometric Device Protection Profile（BDPP）
（2）Biometric Verification Mode Protection Profile（BVMPP）
（3）Biometric Evaluation Methodology（BEM）

BDPP および BVMPP はバイオメトリクス認証装置を対象とした PP であり，生体情報の偽造やものまねによるバイオメトリクス特有の脅威を識別している．これらの脅威に対して，CC の機能要件を詳細化あるいは追加することで，対策を実現している．しかし，実質的に同じ対策であっても，PP によって異なる機能要件に割り当てられていることがわかった．これは，ISO/IEC 15408 へバイオメトリクス製品を適用することは可能であるが，CC の機能要件をバイオメトリクス向けに解釈する方法が幾通りも存在することを示唆している．異なる解釈で記述された PP や ST が多数存在することは，これらの利用者あるいは評価者にとって大きな負担になると予想される．今後は，バイオメトリクス特有の脅威に対する対策をどの機能要件に割り当てるかを示す共通的なガイドラインが必要になると考える．これにより，PP や ST の利用者，開発者，評価者の負担を軽減し，ISO/IEC 15408 へのバイオメトリクス製品の適用を促進させることが可能である．

BDPP および BVMPP は，認証時のなりすましによる脅威に重点化しており，本報告書の 2 節で示した可用性の阻害やプライバシ侵害の脅威，あるいは登録時の脅威は含まれていない．これは，BDPP や BVMPP の TOE やその利用環境を考慮した場合に，開発者がリスクを小さいと判断し，識別されなかったものと思われる．これに対して本報告書で抽出した脅威は，特定の TOE や利用環境を考慮していないため，PP に比べ広範囲の脅威を抽出できている．今後作成される PP や ST においては，本報告書で抽出した脅威が識別される場合もありうるため，上記ガイドラインの策定においては，既存の PP に記載の脅威だけではなく，本報告書で抽出したような広範囲の脅威を対象とすべきである．

BEM は CC におけるバイオメトリクス製品の保証要件に適した評価方法論を明確化することにあり，CC の保証要件にバイオメトリクス特有の要件を追加している．BEM で主張されているように，バイオメトリクス特有の要件を追加することで，CC の保証要件をバイオメトリクスに適用することが可能と考える．

BEM では，バイオメトリクスシステムの評価において，特に TOE のおかれる物理環境や認証パラメータの設定が安全性に影響する点に重点化している．これらの影響を考慮した上で安全性を保証するため，ガイダンス文書（AGD），テスト（ATE），脆弱性評定（AVA）に評価時に考慮すべき点を追加している．特に環境の影響による精度評価は十分に記載されていると考える．

一方，脆弱性分析（AVA_VLA）では，バイオメトリクス特有の脆弱性の考慮が重要であることを指摘しているが，具体的に考慮すべき脆弱性やその評価方法は記載されておらず，バイオメトリクス専

門家の助言が必要との記述にとどめられている．今後は，バイオメトリクス特有の脆弱性の分析について，考慮すべき主要な脆弱性項目とその評価方法を具体化していく必要があると考える．

4　バイオメトリクスの脅威･脆弱性公開のガイドライン開発

平成１５年度は，バイオメトリクスに関する脆弱性情報の健全な流通の実現にむけて検討すべき課題の抽出を行った．具体的な検討課題は以下の通りである．

１）脆弱性への対応方針の明確化の必要性

脆弱性にはすでに知られているものと，今後新たに発見されるものがあり，それぞれ対応が異なると考えられる．既知の脆弱性に関しては，体系的・網羅的に収集しナレッジベースを作ることが有用であり，この知識の蓄積を活用してセキュリティ基準や評価／テストの方法を開拓していくことが考えられる．また，新たに発見される脆弱性に関しては，次の三種類があると考えられる．

・バイオメトリクス認証技術に共有の脆弱性
・指紋，顔，虹彩等のモードに固有な脆弱性
・個々のバイオメトリック・システムの脆弱性

バイオメトリクス認証技術に共有の脆弱性およびモードに固有な脆弱性については，セキュリティ基準の改定に反映させる必要がある．また，個々のバイオメトリック・システムの脆弱性については，場合によっては，その特定システムの利用停止や差し替え，等の対応をとらなければならない．

収集した脆弱性情報の扱い方についても慎重な検討が必要である．個々のバイオメトリクス・システムの脆弱性に関する指摘の場合と，バイオメトリクス認証技術に共有の脆弱性やモードに固有な脆弱性の場合とでは，情報の扱い方が異なることも考えられる．後者は，セキュリティ基準の改訂の際の貴重な知識として活用できる．

２）脆弱性情報の提供を促すための方策（ガイドライン策定）の必要性

現状では，脆弱性を発見したらどのようにすればよいかということに対するコンセンサスがないので，脆弱性情報が死蔵されたり，不適切な流通がおこなわれたり，発見者・公表者の身を守ること，名誉を保証すること，等が十分に行われるような仕組みが必ずしもできていない問題がある．

脆弱性の発見者が，脆弱性情報をうまく公表するために，何をしたらよいのか，どこにどのように報告すればよいか，その際に考慮すべきことは何か，といったことが，よくわかるようなガイドラインが作れないか，検討することが必要である．このために，人工指や人工虹彩に対する脆弱性の指摘で松本が得た経験が役立つと期待できる．

３）脆弱性情報を受け付ける組織の整備などの必要性

脆弱性情報のナレッジベースを維持する制度および組織体制に関して，

・バイオメトリクス認証技術に共有の脆弱性
・指紋，顔，虹彩等のモードに固有な脆弱性

のうち，既知のものは，十分に考慮した，バイオメトリック・システムのセキュリティ基準を確立する必要がある．セキュリティ基準に基づいて，バイオメトリック・システムを評価／テストし，ある

いは第三者による認証をする，といった，バイオメトリック・システムのセキュリティ面での品質を保証する仕組みが必要である．品質保証の仕組みを利用することで，利用者が必要なバイオメトリック・システムのセキュリティ上の質やレベルを，セキュリティ基準を利用して適切に記述し，それに見合ったバイオメトリック・システムを調達することができる．また，利用者の要求条件に応じて，セキュリティ基準によって評価／テストされ，必要に応じ認証をうけて，利用がなされているバイオメトリック・システムに対して，新たに脆弱性が発見された場合にどのような対応をとるべきかについて，検討しておく必要がある．

脆弱性情報を受け付ける組織を作るとすればその体制はどうあるべきかついても検討していく必要がある．また，特定の組織に脆弱性情報を直接報告するという情報提供の方法以外にも学会での発表など多様なルートでの情報提供がなされたとした場合でも，脆弱性情報のナレッジベースを充実させる努力を日々怠らずに行う必要がある．

5　結論

5.1　技術開発

5.1.1　成果

バイオメトリクスを情報セキュリティ分野に適用するには，バイオメトリクスの安全性評価が重要である．しかし現状では，情報セキュリティの観点に基づいたバイオメトリクスの安全性に関する検討が十分になされていない．そこで本研究では，以下三点を三ヵ年の作業内容とし，最終的には，本研究の成果を ISO などの国際標準化機関で標準化することを目的とする．

1）　バイオメトリクスのリスク評価基準の開発
2）　バイオメトリクスのセキュリティ要件および評価方法の開発
3）　バイオメトリクスの脅威・脆弱性公開のガイドライン開発

平成 15 年度は，上記 1）から 3）の各項目に関する現状の技術，制度，標準に関する調査および課題の明確化を行い，平成 16 年度以降の重点化すべき作業項目を示した．具体的な技術的成果は以下の通りである．

1）バイオメトリクスのリスク評価基準の調査検討

本年度は，リスク評価基準を策定するにあたってまず必要となる，バイオメトリクス特有の脅威と脆弱性の明確化を行った．検討に当たっては，バイオメトリクスの脅威や脆弱性に関する従来の研究，およびこれらの情報を含むプロテクションプロファイルや共通評価方法論などから，脅威や脆弱性を抽出・整理し，さらに各脅威や脆弱性項目にバイオメトリクス技術ごとの詳細な検討を加え，脆弱性の程度を示す評価尺度および評価方法に関して検討した．脅威に関しては，なりすましだけでなく，認証が必要なときにいつでも行える可用性や生体情報に由来するプライバシの阻害につながる脅威，および生体情報の登録時に問題となる脅威に関しても検討に含めた．

以上の分析は，特定のバイオメトリクス装置に限定することなく行った．つまり特定の仕様や前提条件を仮定することなく，脅威と脆弱性を抽出している．したがって，バイオメトリクスの安全性評価を行ううえでまず必要になる脅威の洗い出しを広く行えたと考える．また，脅威と脆弱性の関係を明確化することで，ある脅威についてどの脆弱性に対策すべきかも明確にした．

2）バイオメトリクスのセキュリティ要件と評価方法の調査検討

本年度は，ISO/IEC 15408 へのバイオメトリクス製品の適用可能性を調査する目的で，既存のバイオメトリクス向けプロテクションプロファイルと共通評価方法論について調査した．具体的には，以下のドキュメントにおけるバイオメトリクス特有のセキュリティ機能要件と保証要件を抽出し，詳述した．

・Biometric Device Protection Profile（BDPP）
・Biometric Verification Mode Protection Profile（BVMPP）
・Biometric Evaluation Methodology（BEM）

BDPP および BVMPP はバイオメトリクス認証装置を対象とした PP であり，生体情報の偽造やものまねによるバイオメトリクス特有の脅威を識別している．これらの脅威に対して，CC の機能要件を詳細化あるいは追加することで，対策を実現している．CC の機能要件への対策の割り当ては，各 PP で異なるため，統一的に理解するのは難しいが，PP で識別されたバイオメトリクス特有の脅威は，CC の機能要件を詳細化することですべて対策されており，CC へのバイオメトリクス製品の適用は可能と結論した．

ただし，BDPP および BVMPP は，認証時のなりすましによる脅威に重点化しており，上記 1）で示した可用性の阻害やプライバシ侵害の脅威，あるいは登録時の脅威は含まれていない．これは，BDPP や BVMPP の TOE やその利用環境を考慮した場合に，開発者がリスクを小さいと判断し，識別されなかったものと考えられる．これに対して本報告書で抽出した脅威は，特定の TOE や利用環境を考慮していないため，PP に比べ広範囲の脅威を抽出している．

BEM は CC におけるバイオメトリクス製品の保証要件に適した評価方法論を明確化することにあり，CC の保証要件にバイオメトリクス特有の要件を追加している．BEM で主張されているように，バイオメトリクス特有の要件を追加することで，CC の保証要件をバイオメトリクスに適用することが可能と結論した．BEM では，バイオメトリクスシステムの評価において，特に TOE のおかれる物理環境や認証パラメータの設定が安全性に影響する点に重点化している．これらの影響を考慮した上で安全性を保証するため，ガイダンス文書（AGD），テスト（ATE），脆弱性評定（AVA）に評価時に考慮すべき点を追加している．特に環境の影響による精度評価は十分に記載されていると考える．

3）バイオメトリクスの脅威・脆弱性公開におけるガイドラインの調査検討

今年度は，バイオメトリクスの脆弱性情報を適切に流通させるための制度に関する現状をまとめ，今後の課題を示した．

5.1.2 今後の課題

以下の各項目について今後の課題を述べる．

1） バイオメトリクスのリスク評価基準の開発
2） バイオメトリクスのセキュリティ要件および評価方法の開発
3） バイオメトリクスの脅威・脆弱性公開のガイドライン開発

1） バイオメトリクスのリスク評価基準の開発

バイオメトリクスのリスク評価基準の開発に関して，本年度は，考えうるすべてのバイオメトリクス特有の脅威と脆弱性を抽出・整理した．しかし，これらの脅威すべてに対策するのは技術やコスト

の面から現実的ではない．実際には，リスクマネージメントの考え方から，リスクの大きい脅威に対してコストの見合う対策を施していく必要がある．したがって，今後はバイオメトリクス特有の脅威に関するリスク評価が課題となる．具体的には，本報告で洗い出した脅威を，バイオメトリクス装置にあてはめた場合のリスクの評価方法について検討する必要がある．特に，バイオメトリクス特有の脆弱性の程度を示すなんらかの尺度とその測定方法が重要と考える．また，脆弱性の程度が主にバイオメトリクス技術に大きく依存し，かつ製品への依存が小さいものについては，実験により脆弱性の程度を明確化し，リスク評価のための基礎情報として共有すべきと考える．

以上をまとめると，バイオメトリクスのリスク評価のための今後の課題は以下の通りである．

バイオメトリクスのリスク評価のための今後の課題

（1-a）バイオメトリクス特有の性質を考慮したリスク評価方法

（1-b） 脆弱性の程度に関する評価尺度および評価方法の策定

（1-c） 生体情報の脆弱性の程度を評価するのための実験

2） バイオメトリクスのセキュリティ要件および評価方法の開発

本年度は，ISO/IEC 15408 へのバイオメトリクス製品の適用可能性を調査する目的で，既存のバイオメトリクス向けプロテクションプロファイルと共通評価方法論について調査した．その結果，現状の CC および CEM を適切に解釈あるいは詳細化することで，基本的に ISO/IEC 15408 のフレームワークをバイオメトリクスに適用可能であることを示した．

CC の機能要件に関しては，BDPP や BVMPP において，生体情報の偽造やものまねによるバイオメトリクス特有の脅威に対して，CC の機能要件を詳細化あるいは追加することで，対策を実現している．しかし，実質的に同じ対策であっても，PP によって異なる機能要件に割り当てられているため，ことがわかった．これは，CC の機能要件をバイオメトリクス向けに解釈する方法が幾通りも存在することを示唆している．異なる解釈で記述された PP や ST が多数存在することは，これらの利用者あるいは評価者にとって大きな負担になると予想される．今後は，バイオメトリクス特有の脅威に対する対策をどの機能要件に割り当てるかを示す共通的なガイドラインが必要になると考える．これにより，PP や ST の利用者，開発者，評価者の負担を軽減し，ISO/IEC 15408 へのバイオメトリクス製品の適用を促進させることが可能である．また，BDPP および BVMPP は，認証時のなりすましによる脅威に重点化しており，可用性の阻害やプライバシ侵害の脅威，あるいは登録時の脅威への対策が不足していると考える．今後作成される PP や ST においては，本報告書で抽出した広い範囲の脅威が識別される場合もありうるため，上記ガイドラインの策定においては，既存の PP に記載の脅威だけではなく，本報告書で抽出したような広範囲の脅威を対象とすべきと考える．

CC の保証要件および評価方法に関しては，BEM で主張されているように，バイオメトリクス特有の要件を追加することで，CC の保証要件をバイオメトリクスに適用することが可能である．しかし，BEM では，バイオメトリクスシステムの評価において，TOE のおかれる物理環境や認証パラメータの設定が安全性に影響する点に重点化しいるが，一方，脆弱性分析（AVA_VLA）では，バイオメトリクス特有の脆弱性の考慮が重要であることを指摘しているにもかかわらず，具体的に考慮すべき脆弱性やその評価方法は記載されていない．バイオメトリクス専門家の助言が必要との記述にとどめられ

ている．したがって，今後は，保証要件で考慮すべき主要な脆弱性項目とその評価方法を具体化していく必要があると考える．

以上をまとめると，バイオメトリクスのセキュリティ要件および評価方法の開発のための今後の課題は以下の通りである．

バイオメトリクスのセキュリティ要件および評価方法の開発のための今後の課題

（2-a）バイオメトリクス特有の広い脅威に対応した機能要件の詳細化に関するガイドライン

（2-b）脆弱性の程度に関する評価尺度および評価方法の策定

3） バイオメトリクスの脅威・脆弱性公開のガイドライン開発

今後は，バイオメトリクスシステムの適切な利用のためのインフラストラクチャの整備およびバイオメトリクス認証に関わる脆弱性の発見と活用が課題である．

5.1.3 当初の目標に照らした達成状況とその要因

本年度は，（1）節で述べた 1）～3）の各項目に関して，現状の調査を行い，今後の課題を明確化することが当初の目的であった．本研究では，（1）（2）節で示したように，バイオメトリクスのセキュリティ評価を実現するために必要とされる，バイオメトリクス特有の脅威や脆弱性分析，プロテクションプロファイル，共通評価方法論について現状の調査を行った．また，調査結果からバイオメトリクスのセキュリティ評価基準策定のための課題を明確にした．したがって本年度の当初の目的は十分に達成できたと考える．

5.2 国際標準化

5.2.1 成果

バイオメトリクスの脅威・脆弱性分析および脆弱性情報の公開ガイドライン策定に関して，本研究の活動内容紹介および標準化への打診を目的に，ISO/IEC JTC1 SC37 "Biometrics"（以下 SC37 と称する）のシドニー国際会議の WG6 小委員会にて発表した．また，WG5 に出席の英国代表に意見を伺った．バイオメトリクスの脅威・脆弱性分析および脆弱性情報の公開ガイドライン策定に関しては，両者とも非常に重要と認識されている．技術的には SC37 の協力が必要な分野であるが，提案先としては ISO/IEC JTC1 SC27（以下 SC27）が妥当とのコメントが多数を占めた．

本発表を通じ，バイオメトリクスのセキュリティ評価に関する日本の活動を国際標準化の場で認知させることができた．また，今後本研究を標準化提案する上で，提案方針を決定するにあたっての貴重な意見を得ることができたと考える．

今後は，5.1 節で述べたバイオメトリクス特有の脆弱性の評価尺度および評価方法を検討し，SC27 案件である NP 19792 "A framework for security evaluation and testing of biometric technology"への貢献を具体的な目標として，標準化を進める方針である．

5.2.2 当初の目標に照らした達成状況とその要因

本年度は，研究開発の初年度であり，標準化に関しては来年度以降の活動方針を明確にすることが目的であった．上記成果により，SC27 案件への貢献を具体的なターゲットに定めることができ，当初の目標は達成したと考える．

5.2.3 今後の課題

バイオメトリクスのセキュリティ評価基準は，情報セキュリティを扱う観点からは SC27 のスコープである．しかし，技術的には相当のバイオメトリクス技術に関する知見が必要であり，SC37 の援助なくして標準化の実現は難しいと考える．そのため，SC27 と SC37 のリエゾン関係は今後さらに強化されると予想する．したがって，今後本研究の標準化を進めるにあたっては，SC27 への貢献だけでなく，SC27 から SC37 に依頼されるであろう技術検討についても，十分に貢献し，標準化を推進する必要があると考える．

6　あとがき

近年，情報システム分野へのバイオメトリクス技術の適用が急速に進んでいる．今後は，入退室管理や端末内のデータ保護だけでなく，電子パスポートをはじめとした社会 ID 分野や，ユビキタスネットワーク環境における本人確認への適用が見込まれる．バイオメトリクス技術を本人確認の基盤技術として利用する際に問題になるのが，バイオメトリクス製品のセキュリティ評価・認証である．CC に準拠したバイオメトリクス製品の評価を行うには，生体情報の性質に起因するバイオメトリクス特有の脅威や脆弱性を考慮した評価方法が必要になることがその原因である．

本研究は，CC に基づくバイオメトリクス製品のセキュリティ評価を実現するための技術的課題を解決し，成果の国際標準化を推進することで，セキュリティに関する信頼性の高いバイオメトリクス製品の実現を目指している．本研究により，バイオメトリクスのセキュリティ評価の重要性が認識され，残る課題に対して活発な研究活動がなされることを期待する．

7　参考文献

［1］瀬戸編著「ユビキタス時代のバイオメトリクスセキュリティ」日本工業出版，2003

［2］ISO/IEC 15408 : Information technology - Security techniques - Evaluation criteria for IT security，1999

［3］JIS X 5070，セキュリティ技術-情報技術セキュリティの評価基準，2000

［4］永井ほか ” 情報システムに対するセキュリティ国際評価基準の動向と日立製作所の対応 ”,日立評論 Vol.81 No.6(1999/6)

［5］永井ほか ” セキュリティ対策目標の最適決定技法の提案 ”，情報処理学会論文誌，Vol.41，No.8，2264-2271（2000/8）

［6］"Common Evaluation Methodology for Information Technology Security Evaluation (CEM)," CEM-97/017,CEM-99/045

［7］IPA（情報処理振興事業協会）セキュリティセンター翻訳 「情報技術セキュリティのための共通評価方法論」

［8］瀬戸 ” サイバーセキュリティにおける生体認証技術 ”，共立出版（2002/5）

［9］磯部 “ バイオメトリクス技術最前線ーバイオメトリクス技術とセキュリティ標準 ” 月刊バーコード 2002 年 6 月号，日本工業出版（2002/6）

［10］Y.Seto，M.Mimura : Standardization of accuracy evaluation for biometrics authentication in Japan ，IEICE Trans. INF. & SYST., Vol.E84-D, No.7, pp.800-805 (July 2001)

［11］三村ほか「生体認証における脅威および脆弱性に関する分析」，電子情報通信学会 バイオメトリクスセキュリティ研究会，2003

［12］"OECD RECOMMENDATION CONCERNING AND GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA," O. E. C. D. Document C（80）58（Final）, October 1, 1980

［13］「平成 13 年度 OECD 情報セキュリティガイドラインに関する調査」，情報処理振興事業協会 セキュリティセンター，2002 年

［14］ISO/IEC TR 13335:1996　Information technology -- Guidelines for the management of IT Security --

［15］TR X 0036:2001「ＩＴセキュリティマネジメントのガイドライン」日本規格協会

［16］村上「バイオメトリクスに関する法的課題」バイオメトリクスセキュリティコンソーシアム 部会報告会 2004

［17］"Biometrics Evaluation Methodology," Biometric Evaluation Methodology Working Group, 2002

［18］松本「虹彩照合技術の脆弱性評価（その 1)」電子情報通信学会 バイオメトリクスセキュリティ研究会，2003

［19］EU Directive 95/46/EC "The Data Protection Directive," 1995

［20］Biometrics Working Group : Best Practice in Testing and Reporting Performance of Biometric Devices Version 1.0，2000 年 1 月

［21］JIS TR X 0053「指紋認証システムの精度評価方法」日本規格協会，2002

［22］JIS TR X 0072「虹彩認証システムの精度評価方法」日本規格協会，2002

［23］JIS TR X 0079「血管パターン認証システムの精度評価方法」日本規格協会，2003

［24］JIS TR X 0086「顔認証システムの精度評価方法」日本規格協会，2003
［25］JIS TR X 0098「音声認証システムの精度評価方法」日本規格協会，2004
［26］JIS TR X 0099「署名認証システムの精度評価方法」日本規格協会，2004
［27］松本,“ Impact of Artificial gummy fingers on fingerprint systems ”, proc.　SPIE Optical Security and Counterfeit Deterrence Techniques IV, 2002
［28］Ton van der Putte and Jeroen Keuning, ”Biometrical fingerprint recognition : Don't get your fingers burned ”, Smart card research and advanced applications IFIP TC8/WG8.8, pp.289-303, 2002
［29］"Biometric Device Protection Profile (Draft Issue 0.82)," Communications-Electronics Security Group, Biometric Working Group，2001
［30］"Biometric Verification Mode Protection Profile for Medium Robustness Environments (version 1.0)," National Security Agency,2003
［31］Joint Interpretation Library, Integrated Circuit Hardware Evaluation Methodology: Vulnerability Assessment, Version 1.3, April 1999.
［32］A.Jain, R.Bolle, and S.Pankanti, “BIOMETRICS --- Personal Identification in Networked Society,” Kluwer, 1999.
［33］S.Furui, “Recent Advances in Speaker Recognition, in Audio- and Video-based Biometric Person Authentication,” pp.237-252, Springer, 1997.
［34］松井ほか“ 話者認識の研究動向, ”2002 年電子情報通信学会総合大会パネルディスカッション：(PD-2) 音声による個人認証に向けて，PD-2-2，2002.
［35］吉村ほか“ 筆者識別技術の現状, ” 計測と制御，Vol.25，No.8，pp.12-18，1986.
［36］吉村ほか“ 筆者認識技術の最近の動向, ” 信学誌，Vol.72，No.7，pp.788-791，1989.
［37］R.Plamondon and G.Lorette, “Automatic signature verification and writer identification --- The state of the art,”　Pattern Recognition, Vol.22, No.2, pp.107-131, 1989.
［38］F.Leclerc and R.Plamondon, “Automatic signature verification : The state of the art --- 1989-1993,” Int. J. of Pattern Recognition and Artificial Intelligence (IJPRAI), Vol.8, No.3, pp.643-660, 1993.
［39］吉村ほか “ 筆者認識研究の現段階と今後の動向, ” 信学技報，PRMU96-48，pp.81-90，1996.
［40］R.Plamondon and S.N.Srihari, “On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey,” IEEE Trans. on PAMI, Vol.22, No.1, pp.63-84, 2000.
［41］J.P.Campbell, “Testing with The YOHO CD-ROM Voice Verification Corpus,” Proc. of ICASSP, pp.341-344, 1995.
［42］松井ほか“ テキスト指定型話者認識, ” 信学論 D-II，Vol.J79-D-II，No.5，pp.647-656，1996
［43］益子ほか“ 話者照合システムに対する合成音声による詐称, ”信学論 D-II，Vol.J83-D-II，No.11，pp.2283-2290，2000.
［44］海野ほか“ 話者照合に対する合成音声詐称を防止するための合成音声検出法, ”コンピュータセキュリティシンポジウム 2003，pp.73-78，2003.
［45］Y.Yamazaki and N.Komatsu, “A proposal for a text-indicated writer verification method,” IEICE Trans. Fundamentals, Vol.E80-A, No.11, pp.2201-2208, 1997.
［46］独立行政法人　情報処理推進機構（IPA）, “ 各国バイオメトリクスセキュリティ動向の調査, ”

電子政府行政情報化事業，2004 年 2 月
［47］P. Jonathon Phillips, Patrick Grother, Ross J. Micheals, Duane M. Blackburn, Elham Tabassi, Mike Bone, “FACE RECOGNITION VENDOR TEST 2002”.
［48］赤松, “ コンピュータによる顔の認識　－サーベイ－, ” 信学論 D-II Vol. J80-D-II, No.8, pp.2031-2046, 1997.
［49］日本バイオメトリクス認証協議会 活動成果「バイオメトリクスシステムの脆弱性に関する報告書 Ver. 0.6」 http://www.biometrics.gr.jp/JBAA/seika.html （2003/3 現在）
［50］C. Soutar, "Biometric System Security," http://www.bioscrypt.com/assets/security_soutar.pdf （2004/3 現在）
［51］"Biometrics Security Consortium" http://www.bsc-japan.com/ （2004/3 現在）
［52］Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, “Body Check,” c’t 11/2002, page 114 - Biometrie, http://heise.de/ct/english/02/11/114 （2004/3 現在）
［53］Colin Soutar, “Biometric system performance and security,” Mytec Technologies Inc., http://www.bioscrypt.com/assets/bio_paper.pdf （2004/3 現在）
［54］山田ほか “指紋照合装置は人工指を受け入れるか, ” 信学技報, ISEC2000-45, pp.159–166. 及び, 情報研報 Vol.2000, No.68, pp.159–166, July 2000.
［55］山田ほか “指紋照合装置は人工指を受け入れるか（その 2）, ” コンピュータセキュリティシンポジウム 2000, Vol.2000, No.12, pp.109–114, Oct. 2000.
［56］山田ほか “指紋照合装置は人工指を受け入れるか（その 3）, ”2001 年暗号と情報セキュリティシンポジウム（SCIS2001）, Vol.II, pp.719–724, Jan. 2001.
［57］星野ほか “指紋画像からの人工指作製, ” 信学技報, ISEC2001-60, pp.53–60, 2001.
［58］星野ほか“指紋画像からの人工指作製（その 2）, ”2002 年暗号と情報セキュリティシンポジウム（SCIS2002）, Vol.II, pp.821–826, 2002.
［59］遠藤ほか “指紋照合装置は人工指を受け入れるか（その 4）, ” コンピュータセキュリティシンポジウム 2002, Vol.2002, No.16, pp.245–250, Oct. 2002.
［60］遠藤ほか “指紋照合装置は人工指を受け入れるか（その 5）, ” 情処研報, Vol. 2003, No.18, ISSN0919-6072, 2003-CSEC-20-44, pp..251–256, 2003.
［61］青山ほか “指紋画像からの人工指作製（その 3）：ディジタルカメラを用いた場合, ”2003 年暗号と情報セキュリティシンポジウム（SCIS2003）, Vol.I, pp. 393–398, Jan. 2003.
［62］松本ほか“虹彩照合技術の脆弱性評価（その 2）, ” コンピュータセキュリティシンポジウム 2003, Vol.2003, No.15, pp.187–192, Oct. 2003.
［63］松本ほか“虹彩照合技術の脆弱性評価（その 3）, ” 2004 年暗号と情報セキュリティシンポジウム, SCIS2004, Vol.I, pp.701–706, Jan. 2004.
［64］松本, “セキュリティ技術の弱点をみつけたらどうしますか？, ” 電子情報通信学会誌, Vol.84, No.3, pp.202–204, March 2001.