平成 26 年度工業標準化推進事業委託費
（戦略的国際標準化加速事業
（国際標準共同研究開発・普及基盤構築事業：
クラウドセキュリティに資するバイオメトリクス認証の
セキュリティ評価基盤整備に必要な国際標準化・普及基盤構築））

成 果 報 告 書

平成 27 年 3 月

一般社団法人日本自動認識システム協会
独立行政法人産業技術総合研究所
株式会社 OKI ソフトウェア

はじめに

バイオメトリクス認証技術は、市場に投入されて久しく、本人でなければ認証されない特性から、出入国管理時におけるブラックリスト照合や ATM など金融分野での本人確認などで使われている。また、利便性が高い特性から、入退室管理・勤怠管理・携帯電話・PC/アプリケーション等のログインなどでも使われている。また、国内外における近年の行政及び民間での電子サービスの充実あるいはクラウドコンピューティングの発展を考えると、サービスを安全で安心な形で提供するために、システムを利用するユーザの本人認証を安全また簡便に行う重要性が増していると考えられる。

一方、2020 年には東京オリンピック・パラリンピックが開催されるが、ここでは使用者の利便性を損なうことなく安全を確保するためのシステムが必要となると考えられ、その実現のために多様な活用技術や活用事例が登場してくることが想定される。これらを考えると、利便性の高いバイオメトリクス認証技術が注目すべき技術の一つとして、今後その重要性をますます増すことが予想される。

しかしながら、バイオメトリクス認証技術は、セキュリティが限界に達していると言われながら未だに広く利用されている ID/PW（PassWord）のようには普及していない。このひとつの要因は、バイオメトリクス認証製品のセキュリティは、各製品ベンダーが自己評価した結果に基づいてカタログ表示あるいは顧客に対して個別に説明しているのが現状であり、バイオメトリクス認証製品のセキュリティが客観性を持つ形で表現されている状況になっているとは言い難く、社会的に認知されたセキュリティ評価基準を基にして安全・安心できる技術あるいは製品であるとの説明ができないことにあると考えられる。

一方、列車、自動車、医療機器や制御システムの安全を確保するための考え方の一つの機能安全における安全性実現のための検討の中で、機能安全性を規定する IEC 61508 シリーズの認証を受けることが調達条件となる動きがあり、これら制御システムにバイオメトリクス認証技術が組み込まれる場合、IEC 61508 シリーズと対の関係にある CC（Common Criteria）認証を得ていることが調達上優位になる可能性も出て来た。

このような状況を考えると、バイオメトリクス認証技術が客観的に見て安全・安心に利用できる本人認証技術として社会的に認知されれば、その利用が促進されるだけでなく、適用市場も広がり、その市場が拡大することが予想される。つまり、利便性の言及と共に、国際標準に則った客観的なセキュリティ評価が行われる環境を整え、その環境を利用してバイオメトリクス認証製品の CC 認証を取得してゆくことが、今後の普及にとって極めて重要と考え、本研究開発に取り組んでいる。

最後に、本研究開発の実施にあたり、ご指導を賜った検討委員会の松本 勉 委員長（横浜国立大学 大学院）ならびに委員各位をはじめとして関係者各位に心より深く感謝を申し上げます。

注）CC 認証　CC は Common Criteria(ISO/IEC 15408 の別称)の略称であり、CC 認証とは CC に沿ったセキュリティ評価及び認証を得ること

平成 27 年 3 月

一般社団法人日本自動認識システム協会
独立行政法人産業技術総合研究所
株式会社 OKI ソフトウェア

目　　次

1. 事業の目的

本事業は、バイオメトリクス認証技術に対する社会的に認知されたセキュリティ評価基準がないことで、各製品のセキュリティ性を客観的に評価できない状況を改善するため、バイオメトリクス製品の CC（Common Criteria）認証に向け、国内に、①産業界が無理なく参加可能、②十分に有効性があり、③継続性のある、バイオメトリクス製品のセキュリティ評価基盤を 3 年間で整備することを目的としている。

精度及び安全性の観点での客観的な評価を可能にするために、精度については評価ツール、また安全性については既にあるセキュリティ評価基準に則って PP（Protection Profile）及び PP に付随する評価手法を作成し、更に評価機関及び認証機関が PP 及び評価手法に基づく評価及び認証を実施可能にすることによって、バイオメトリクス製品のセキュリティ評価・認証基盤を整備する。PP 及び PP に付随する評価手法は、国際標準案とするために作成することとした。

そして、これら成果を国際標準化原案として適当な標準化機関（PP については ISO/IEC JTC 1/SC 37、評価手法については ISO/IEC JTC 1/SC 27 を予定）へ提案することに取り組む。

また、本事業の範囲内で、本事業に参加するベンダー各社の協力を得て、各社のバイオメトリクス製品に対して、作成する精度評価ツールを適用して精度評価を実施し、開発した PP を基に各社製品の ST（Security Target、セキュリティ機能仕様書）を作成して、各社のバイオメトリクス製品に対するパイロット評価・認証の実施に取り組む。

なお、本事業で作成する PP は、バイオメトリクスに関するセキュリティ評価を推進しているドイツなどと意見交換、協力し、国際標準化に向けた活動に取り組む。

また、本事業の過程で、本事業に関係する評価機関・認証機関が確立するバイオメトリクス製品特有の評価及び認証に必要な手法・手順は、体系化して文書化することによって、本事業終了後も継続的に実施可能とすることに取り組む。

これらによってセキュリティ評価・認証基盤を整備して、バイオメトリクス製品のセキュリティの作り込みの正当性を確認し、日本のバイオメトリクス製品を他国に先駆けて CC 認証取得可能とし、国際競争力の向上に資すことにもに取り組む。

2. 事業の実施計画

バイオメトリクス製品の CC（Common Criteria）認証に沿ったセキュリティ評価・認証基盤を整備するために、平成 26 年度は以下の手順で研究を実施することを計画した。

(1)海外動向調査及び方針検討

バイオメトリクス製品のセキュリティ評価について、海外各国の動向調査を行った上で、本プロジェクトを推進するにあたっての方針を検討する。

(a) 海外動向調査

バイオメトリクス製品のセキュリティ評価を構成する 3 つの要素である精度評価・脆弱性評価・プライバシーの CC 認証への組み込みに関する海外動向を調査する。調査にあたっては、バイオメトリクスの CC 認証を国家として推進しているドイツをはじめとする主要国の行政・学会・産業界などから情報を収集する。

(b) 方針検討

調査結果から、日本における精度評価・脆弱性評価・プライバシーの CC 認証への組み込み方法に関する方針検討を行う。本検討において PP が対象とするバイオメトリクス製品の機能や対象範囲を決定する。あわせて、CC 認証において PP に付随し評価手法などを含むサポート文書（Supporting Document）や、セキュリティ評価の際に使用する評価ツールの開発方針を決定する。

(2)PP 開発及び PP 認証取得

「(1)海外動向調査及び方針検討」結果に基づいて PP について研究し、開発する。開発した PP について国内認証機関である IPA による認証を取得する。

(a) PP 開発

精度評価・脆弱性評価・プライバシーを組み込んだ PP について研究し、開発する。PP の開発においては、バイオメトリクスの専門知識を持つベンダーや学会の有識者、及び、CC 認証の専門知識を持つ 一般財団法人日本品質保証機構(JQA)の有識者などからのレビューを受けて完成させる。

(a) PP 認証取得

完成した PP は、評価機関での評価の後、CC 認証における国内認証機関である独立行政法人情報処理推進機構(IPA)で PP 認証を取得する。

(3)セキュリティ評価手法の研究

「(2) PP 開発及び PP 認証取得」で開発した PP に従ったセキュリティ評価を実施するための評価手法について研究する。特にバイオメトリクスに関する高い専門性が要求される精度評価と脆弱性評価について、評価手法を整理し、サポート文書の作成や評価ツール開発を推進する。

(a) 精度評価のためのサポート文書とツール開発

評価の効率化及び信頼性向上を考慮してサポート文書の原案を作成する。あわせて、効率化の実現や信頼性向上を目指した精度評価ツールのプロトタイプ開発を行う。

- 効率化：バイオメトリクスの精度評価手法に関する国際規格である ISO/IEC 19795 に準拠した精度評価ツールを開発することにより、ベンダーや評価機関が精度評価を実施する際の作業の効率化を実現する。開発にあたっては、国内ベンダー及び評価機関との間で意見交換を行うことで、機能の充実を図る。
- 信頼性向上：インターネット経由で評価機関のサーバとベンダーの端末を接続し、ベンダーによる精度評価の履歴がエビデンスとして評価機関側に記録される新しい精度評価スキームについて研究し、CC 認証における適用可能性を明確化する。

(b) 脆弱性評価手法の研究

生体を模倣する偽造物、生体を模倣しないが高い確率で誤判定を発生させるウルフ（なりすましの入力情報）などを使った脆弱性評価手法を研究する。生体を模倣する偽造物の作成にあたっては、既に保有する３次元スキャナや本事業でリース予定の OCT（Optical Coherence Tomography）を使って生体を精密に計測して偽造生体を作成する。ウルフについては、バイオメトリクス製品の開示された照合アルゴリズム毎に、ウルフによる脆弱性解析方法を検討する。偽造物の作成や、作成した偽造物を使った脆弱性評価の知見及び手順については、補助研究員によって実験して、再委託先の JQA に開示する。また、研究成果を基に、サポート文書を作成する。

また、脆弱性評価には精度評価に依存する項目が複数存在する。これらの項目については、上記「(a)精度評価のためのサポート文書とツール開発」で述べた精度評価ツールを活用することで、脆弱性評価の効率化や信頼性向上に貢献するための方法を検討し、必要に応じて来年度以降の事業における作業項目とする。

なお、前述のサポート文書の作成にあたっては、脆弱性評価機関(JQA)とともに検討し、JQA が独立して評価を実施できるよう育成する。

3. 事業の実施体制

3.1 管理体制及び研究体制

(1)管理体制及び開発体制

本事業の統括者は[研究機関 A]一般社団法人日本自動認識システム協会が行う。

共同開発者として、[研究機関 B] 独立行政法人産業技術総合研究所及び[研究機関 C] 株式会社 OKI ソフトウェアが活動した。

前期で立案した計画に従い、下記の各活動を研究機関毎に実施し、各々の開発の進捗管理及び予算管理も研究機関毎で行った。

なお、全体プロジェクト管理は、[研究機関 A]一般社団法人日本自動認識システム協会に一本化した。

また、PP 開発及び PP 認証取得のために、バイオメトリック認証に携わる機器ベンダー（富士通、ＮＥＣ、日立ほか）及び学識経験者により検討委員会を構成して精度評価ツールまたは PP（Protection Profile）を作成し、バイオメトリクス製品のセキュリティ評価・認証基盤に整備に取り組んだ。

1)共同研究体制

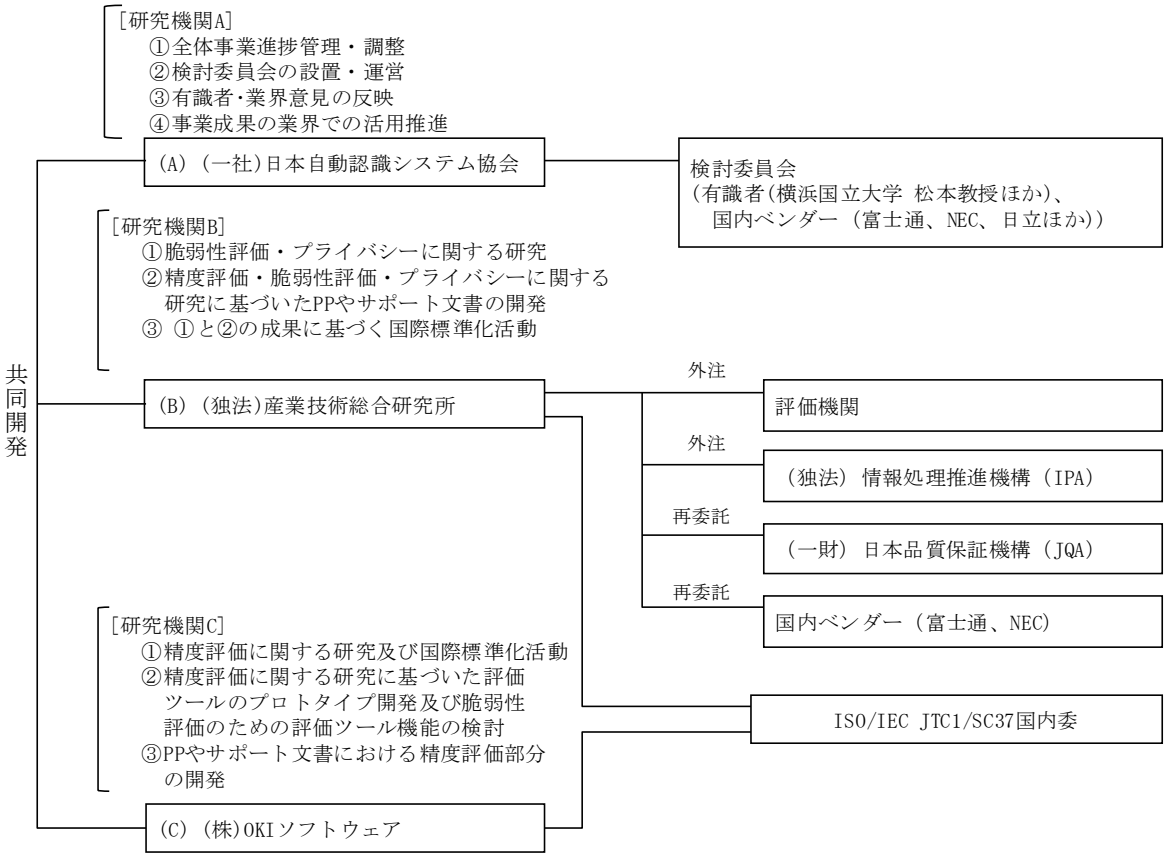


図 3.1-1　共同研究体制

2)個別の管理体制及び研究体制

【一般社団法人 日本自動認識システム協会（JAISA)】

(1) 管理体制

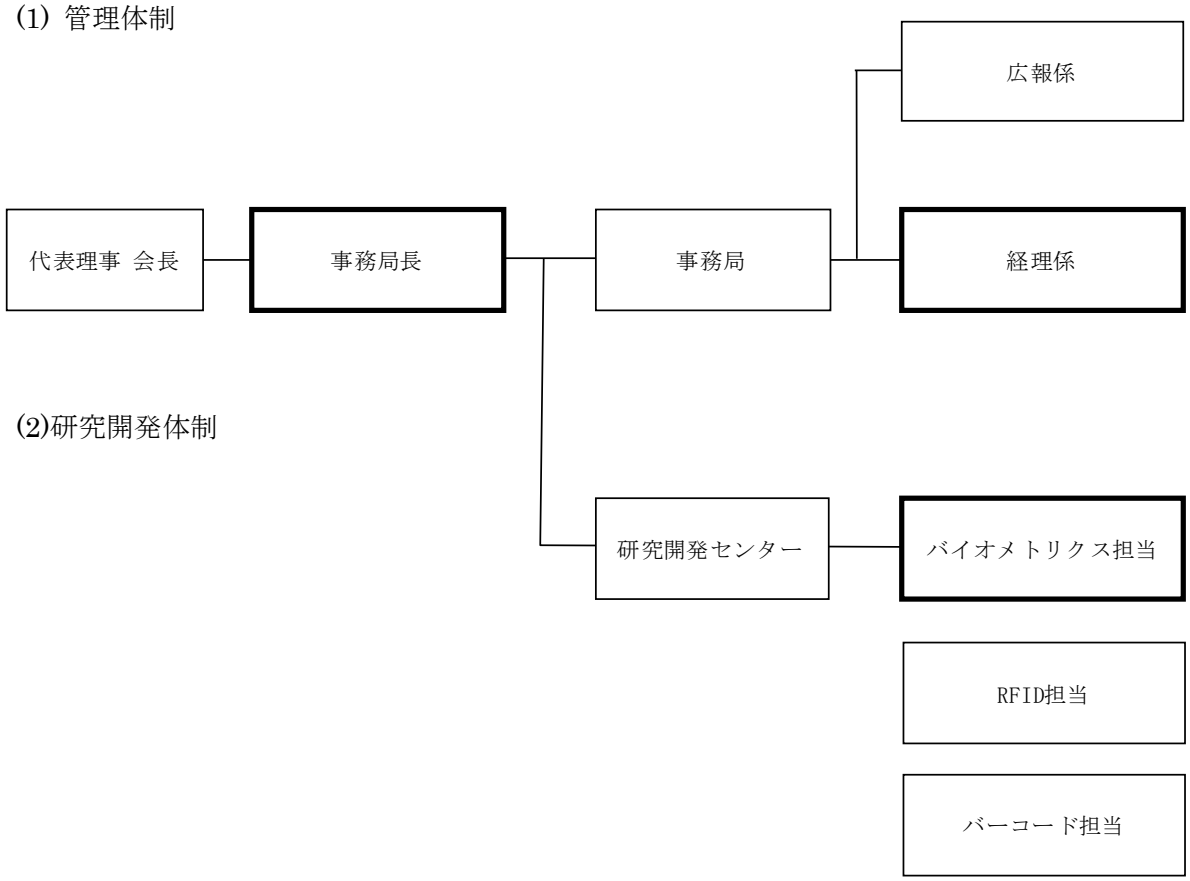


図 3.1-2　日本自動認識システム協会　管理体制・研究開発体制

【独立行政法人 産業技術総合研究所】

(1)管理体制

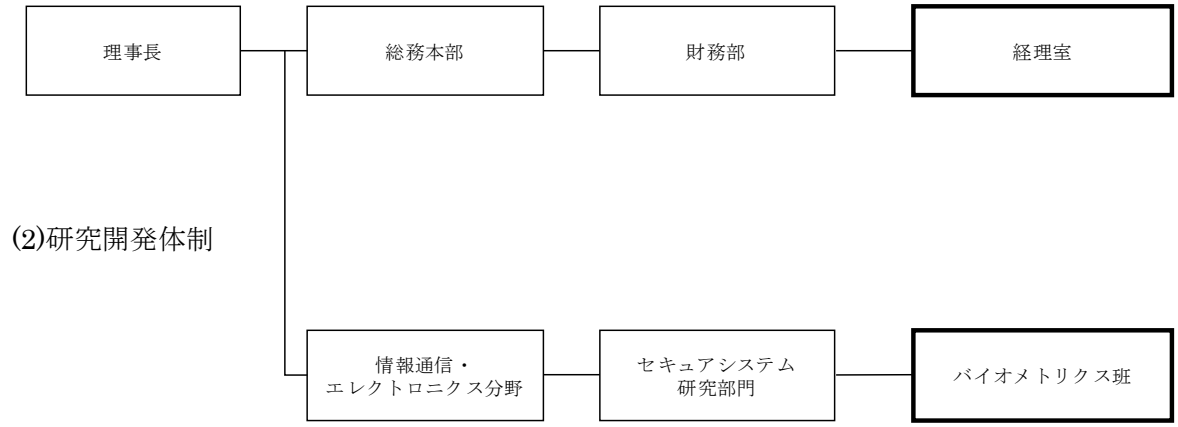
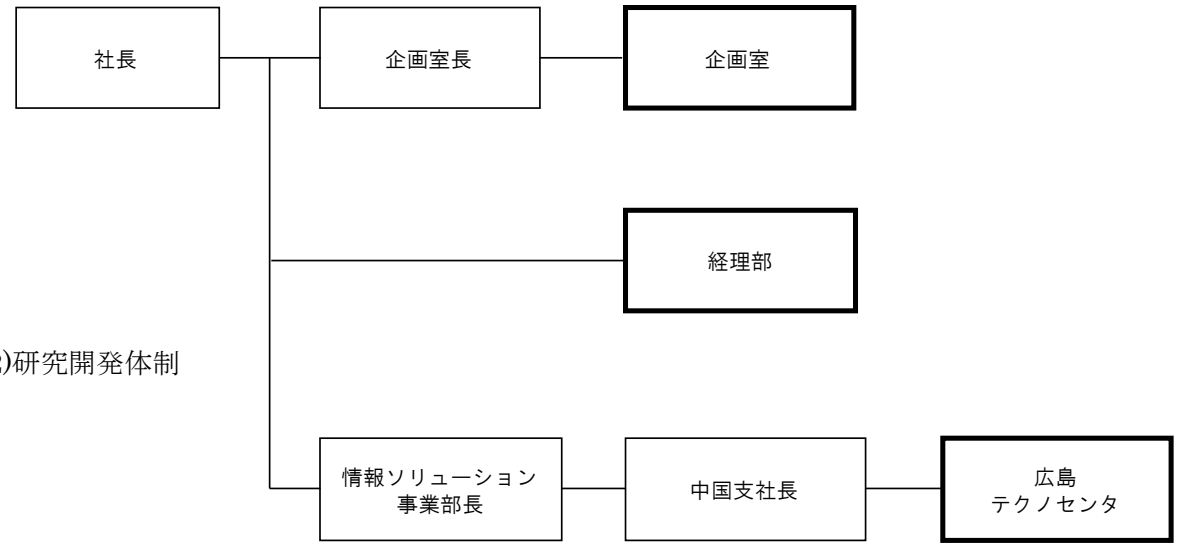


図 3.1-3　産業技術総合研究所　管理体制・研究開発体制

【株式会社 OKI ソフトウェア】

(1)管理体制



(2)研究開発体制

図 3.1-4　OKI ソフトウェア　管理体制・研究開発体制

3.2 検討委員会

表 3.2-1 検討委員会委員名簿 [順不同、敬称略]

	役割	氏名	所属	備考
1	委員長	松本 勉	横浜国立大学 大学院 環境情報研究院	
2	委員	鷲見 和彦	青山学院大学 理工学部	SC37WG5 委員
3	委員	石原 修	株式会社日立製作所	
4	委員	岩田英三郎	ユニバーサルロボット株式会社	
5	委員	須下 幸三	バイオニクス株式会社	
6	委員	出口 豊	株式会社モフィリア	
7	委員	齊藤 廣大	株式会社東芝	
8	委員	平野 誠治	凸版印刷株式会社	SC37WG3 ｴｷｽﾊﾟｰﾄ
9	協賛委員	新崎 卓	株式会社富士通研究所	SC37WG3 主査
10	協賛委員	溝口 正典	日本電気株式会社	SC37WG5 主査
11	協賛委員	近藤 潤一	独立行政法人情報処理推進機構	
12	協賛委員	口井 英人	一般財団法人日本品質保証機構	
13	推進委員	中村 敏男	株式会社 OKI ソフトウェア	SC37WG2 ｴｷｽﾊﾟｰﾄ
14	推進委員	寳木 和夫	独立行政法人産業技術総合研究所	
15	推進委員	山田 朝彦	独立行政法人産業技術総合研究所	SC37 委員長 SC37WG5 委員
16	推進委員	大塚 玲	独立行政法人産業技術総合研究所	
17	推進委員	大木 哲史	独立行政法人産業技術総合研究所	
18	ｵﾌｻﾞｰﾊﾞ	江口 真一	富士通フロンテック株式会社	
19	ｵﾌｻﾞｰﾊﾞ	杉澤 正俊	日本電気株式会社	
20	ｵﾌｻﾞｰﾊﾞ	佐藤 眞司	独立行政法人情報処理推進機構	
21	ｵﾌｻﾞｰﾊﾞ	神賀 誠	一般財団法人日本品質保証機構	
22	ｵﾌｻﾞｰﾊﾞ	岩永 敏明	経済産業省 産業技術環境局	SC37 専門委員
23	ｵﾌｻﾞｰﾊﾞ	中山 和泉	経済産業省 製造産業局	
24	事務局	酒井 康夫	一般社団法人日本自動認識システム協会	SC37 ﾘｴｿﾞﾝ
25	事務局	森本 恭弘	一般社団法人日本自動認識システム協会	

3.3 実施スケジュール

平成 26 年度の活動は下記日程で実施した。

表 3.3-2 実施スケジュール

(A:JAISA, B:産総研, C:OKI ソフトウェア)

項目	平成 26 年									平成 27 年		
	4	5	6	7	8	9	10	11	12	1	2	3
１．有識者･業界意見反映及び事業成果の活用推進活動												
(1) 委員会の開催･運営(A)					→	→	→	→	→	→	→	
(2) 事業成果の活用推進(A+B+C)					→	→	→	→	→	→	→	
２．海外動向調査及び方針検討												
(1)海外動向調査（文献及びﾋｱﾘﾝｸﾞ）(B+C+A)					→	→	→	→	→	→		
(2)方針検討 1:精度評価(C)					→	→						
(3)方針検討 2:脆弱性評価(B+C)					→	→						
(4)方針検討 3:プライバシー(B)					→	→						
３．PP 開発及び PP 認証取得												
(1)PP 開発 1：全体構成(B)					→	→						
(2)PP 開発 2：精度評価(C)					→	→	→					
(3)PP 開発 3：脆弱性評価(B+C)					→	→	→					
(4)PP 開発 4：プライバシー(B)					→	→	→					
(5)PP 認証取得(B)								→	→	→	→	
４．セキュリティ評価手法の研究												
(1)脆弱性評価手法の研究(B)					→	→	→	→	→	→	→	
(2)ｻﾎﾟｰﾄ文書開発 1：全体構成原案(B)					→	→	→	→	→			
(3)ｻﾎﾟｰﾄ文書開発 2：精度評価原案(C)					→	→	→	→	→	→	→	
(4)ｻﾎﾟｰﾄ文書開発 3：脆弱性評価原案(B+C)					→	→	→	→	→	→	→	
(5)脆弱性評価組織の育成(B)					→	→	→	→	→	→	→	
(6)精度評価ﾂｰﾙ開発：精度評価機能ﾌﾟﾛﾄ(C)								→	→	→	→	
(7)精度評価ﾂｰﾙ検討：脆弱性評価機能(B+C)								→	→	→	→	
５．成果報告書作成(A+B+C)									→	→	→	

3.4　検討委員会と検討内容

(1)第 1 回検討委員会

平成 26 年 7 月 24 日　15:00～17:00 （一社)日本自動認識システム協会（JAISA）にて開催

①本年度の計画概要について

「クラウドセキュリティに資するバイオメトリクス認証のセキュリティ評価基盤整備に必要な国際標準化・普及基盤構築」事業の概要の説明をし、質疑を経て、国際標準化組織への提案アクションを追加することとなった。

また、CC そのものの枠組みでは認証対象の内容を少し変えるだけでも再認証がいるため、小変更時の認証取得時のベンダー負担を軽減することに配慮した認証の枠組みの検討も含めて今後検討してゆくこととなった。

②セキュリティ評価の考え方と進め方

セキュリティ評価の進め方について検討状況と方針の説明をし、次を明確化した。

(1)このプロジェクトの取り組みの一つとして、バイオメトリクス製品に CC 認証を与え競争力を高めることを目標とし、バイオメトリクス製品に認証を与えるための、使い勝手の良い PP 作成に取り組む。

(2)PP 作成に向けて、バイオメトリクス脆弱性に対する脅威分析を行い、それについて委員間で合意をとる活動を行う。また、その中で、SW 評価や HW 評価という言葉の定義や、TOE のコンセンサスを作る。

(3)今回のプロジェクトの中では、cPP（Collaborative PP）を目指した活動を行うが、その国際標準化に向けた活動について、はやめに国際的な協力関係構築や提案などを含めて、アクション項目を具体化する。

③精度評価及び推進方針について

精度評価及び精度評価の推進方針について、検討状況と方針の説明をし、次を明確化した。

(1)海外、特に米国の PP の状況について確認する。スペイン関係で指紋に特定した PP があるか確認する。

(2)脆弱性評価については、これからコンセンサスを得る活動を行う。

(3)評価対象製品をどうするかについての提案内容は今後検討を進める。

(4)精度評価ツールの開発方針等は、ベンダー等関係者に説明し詳細検討を進める。

(2)第 2 回検討委員会

平成 26 年 9 月 29 日　14:00～17:00　JAISA にて開催

①PP 案検討状況報告（セキュリティ対策方針まで）

バイオメトリクス製品プロテクションプロファイル検討状況を報告し、質疑を経て、次のことも含めて今後検討してゆくこととなった。

(1)物理的攻撃を具体的にリスト化する。
(2) Capture Device の間のパスや境界について再検討する。
(3)前提条件の「A.PHYSICAL」について検討する。
(4)製品のイメージを具体的にするため、ある程度限定して整理する。また、通信経路についても検討する。

②PP 案検討状況報告（脆弱性評価の方針から）

脆弱性評価の方針の説明を行い、次回まで継続検討することとなった。

③精度評価検討状況及び今後の検討方針について

精度評価の検討状況及び今後の検討方針について説明し、質疑応答を経て、次のことも含めて今後検討してゆくこととなった。

(1)ROC カーブの必要性は、現状では、PP や今後のセキュリティ評価の検討の中でどうなるか分からないため、今後、要否を検討する。
(2)ウルフ攻撃を対象とするロジックについて検討する。
(3) AR だけでなく、FRR についても検討する。

(3)第 3 回検討委員会

平成 26 年 12 月 5 日　15:00～18:30　JAISA にて開催

①欧州出張報告

11 月 10 日から 16 日にかけてドイツの TUViT と BSI、スペインのマドリッド自治大学を訪問した内容について報告した。

②PP 作成状況報告

PP 作成状況について報告し、質疑応答を経て、次の訂正・追加を行うこととなった。

(1) FIA_BUA.1 の注釈は、この PP の中では最終的に使われないが、実際製品認証する場合には使われる場合もあると考え定義したという但し書きを追加する。
(2) TOE の図に、PAD Feature Extraction から Extraction に信号が入るケースもあるので、

Extraction に対しても点線を入れる。

(3) コミュニケーションの具体例として Capture 機能とストレイジ機能と TOE の間の通信が書かれているが、TOE の図では、GetID や Administrator や Policy Management/Access Control と TOE の間の通信があるので、それについても具体的に記載する。

また、審議事項の結論は下記となった。

(1) Capture について

8 ページのバイオメトリック製品の構成の統合型では、一塊のハードウェアの中に Capture デバイスも入っているが、そこは TOE とせず、TOE の範囲外であるとする。さらに TOE の Capture デバイスがどのようなものかが曖昧なので、Capture デバイス自体の中も Capture の機能と PAD Feature Extraction との機能が有ると考え、Capture の機能は TOE 内とは考えないと理解することとする。

Capture という機能から二つ矢印が出ているが、それは区別し、上側が純粋な Capture なので、一本を枝分かれさせる。そこに偽のものが来ると PAD Feature Extraction で検出するが通信は守られているとしているので、ここに攻撃のための信号が入力されることはないという前提で成り立っていると考える。

Capture 機能が Capture をどこまで捉えるかによるが、Capture 機能の一部が TOE の中に入っているという解釈をする。Capture 機能には TOE の外側の機能と内側の機能があり合体して Capture 機能ということにして、内側の機能から PAD Feature Extraction に内部でつながっていると解釈する。

(2) TOE とバイオメトリクス製品について

製品として売られているものや、世の中に流通するものは、TOE 単独ではありえないというケースもある。TOE というのが、目に見える製品そのものを表してないケースもあるので、TOE を含み製品となっているという理解をする。製品と TOE が一致しない場合には、ＳＴで明確に定義し、PP と同じものであることを論証することとなる。

さらに以下が検討事項となった。

(1) Capture について

たとえば、ある指紋ベンダーの製品で指紋センサーの取り込みのところで PAD 判定しており、置かれたものが人のものではないと何も反応しないものがあるが、そういう場合に、この TOE の中ではどういう扱いになるのかということについての検討すること。

③精度評価検討状況報告

精度評価検討状況について、被験者やオペレーターの人的要因ミスを一通りの評価をした後でエラーを除去する運用上の工夫やルールについても今後の予定として加えるとの補足と共に

報告があり、質疑応答を経て、以下を修正することとなった。

(1)シナリオのダウンロードは、評価組織の中に含むよう評価組織の枠を修正する。

また、以下が検討事項となった。

(1)ベンダーにセンサーという装置と SDK に相当する製品を持ち込んでもらい、端末自体は第三者機関が持っているものを使う前提の精度評価を考えているが、SDK を提供しないベンダーはどうするかなどについても検討が必要である。

(2)ベンダー社内の DB を使用した精度評価の取り扱いについて、社内 DB を使うことをどう解釈するか、どう取り込んで総合的な評価につなげるか。これを含めた評価方法について検討する必要がある。

(3)ベンダー社内の DB を使用する場合は、その取得時に公的評価にも用いられるということを、最初のデータ取得時点で納得してもらうということを今後していかなくてはいけない点を考慮する必要がある。

(4)ソフトウェアをどうするかという話と、バイオメトリクスの認証の具体的な方法を開拓するというのが完全に分離されていない。

後者については精度の部分についてまだ検討が足りてないという状況にある。今後どう進めていくかを、もう一回、事業実施者側で練ること。

④静脈認証装置の安全性評価について

CC 評価・認証のエビデンスの事例として、なりすましに対する調査結果と指紋と静脈を例とした安全性評価の例について説明した。

検討の結果、静脈のなりすまし攻撃に関して、ベンダーの方に意見をもらい、どういう攻撃をするかおおよそ決めて、その次のステップとしてそのような攻撃だったら攻撃能力はどうなるかを決めるように進めることとなった。

また、登録時のフェイクによるなりすましの問題の取り扱いについては、別途作成を計画している PP で対応することが確認された。

(4)第 4 回検討委員会

平成 27 年 2 月 20 日　14:00～17:00　JAISA にて開催

①PP 検討結果及び今後の方針について

PP 検討結果について報告した。この中で、今の PP は脆弱性評価の部分は AVA_VAN.2 を要求するとして作成しているが、来年度の偽造物を作った評価で攻撃能力が想定している基本よりも低くなった場合、現在の PP で評価をすることができなくなるので、その場合は、攻撃能力を最小に落とした PP を作り、それに基づいて CC の評価、認証していくという可能性もあると考えていることが説明された。

その後の質疑応答を経て、作成した PP を委員に配布することとなった。

作成した PP は付録 2 に示す。

②脆弱性評価の検討状況と今後の方針について

脆弱性評価の検討状況と今後の方針について報告し、質疑応答を経て、今後次の検討することとなった。

(1)「生体検知機能を無効化する」説明で、生体検知機能あることを前提とした表現になっているが、生体検知機能がない場合は無効化の対象ではないし、また生体検知機能とわざわざいっていない場合には無効化の対象にならないのではないかと思う。また、無効化という言葉がなじまない。説明と内容が一致するように整理すること。

(2) 攻撃の方法、攻撃の手順、その時の攻撃能力値について関係者で合意した文書である攻撃方法の規定文書の作成が必要である。その作成と取扱い、また他国との情報交換について整理すること。

(3) 脆弱性テストの方法に関して、偽造の方法あるいは装置によっては生体に付けることによって初めて使えるものがある可能性があり、その場合にはロボットアーム方式でテストができない場合があると思われる。そのような場合も含めてテスト方法について整理すること。

③精度評価検討結果及び今後の方針について

(1)ブートストラップ法について検討を進めること。

(2)ベンダーカスタマイズの内容の整理と、実際の運用開始後にその作業を誰がどうおこなって行くかについて今後整理すること。

(3)ツールの取り扱いについて、例えば評価機関に限定するのか、評価を受ける側にも提供するのかなど、今後の取り扱いについても今後整理すること。

(4)ツールの中のヒューマンインターフェイスについては評価機関になる JQA と連携して固めてゆくことが良いと思うので、その進め方等について検討すること。

(5)19795 に準拠する前提で、脆弱性評価に本ツールを適用する場合に、どのような評価指標が必要なのかについて、脆弱性評価の検討と連携して、整理しツールの仕様に反映することが必要と思うので、その計画について検討すること。

4. 実施内容概要

4.1 海外動向調査及び方針検討

本事業は、ISO/IEC 19792 の主張に基づいて、精度評価・脆弱性評価・プライバシーを組み込んだバイオメトリクス製品の CC（Common Criteria）評価・認証を可能にすることを目的としている。今までの活動を通じて、セキュリティ要件定義書に相当する PP（Protection Profile）を作成することを本事業で実施することとした。また、ISO/IEC 19792 に基づいたバイオメトリクス製品の CC 評価・認証のためには、そのための評価技術の確立も必要である。よって、海外動向調査では、バイオメトリクス製品に対する既存 PP と評価技術に関して文献及び海外出張による調査を実施し、その調査結果を参考にして、PP 作成及び評価技術確立の方針を作成した。

4.1.1 海外動向調査

PP については、インターネット上で入手可能な PP を調査した。評価技術については、インターネット上で入手可能な文献に加え、ISO/IEC JTC 1/SC 27/WG 3 への寄書、更に既に指紋のなりすまし攻撃検知の製品に対する CC 評価・認証を開始しているドイツの状況を海外出張して関係者から情報入手した。

(1)PP 調査

製品ベンダーの ST（Security Target。CC 評価・認証におけるセキュリティ設計仕様書）作成を容易化するための PP（Protection Profile）を作成するために、ドイツ 3 件、米国 2 件、英国 1 件の PP 及び PP 案の調査を実施した。このうち、英国の PP 案と米国の PP 2 件は、内容が妥当性を欠き、現在有効ではない。ドイツの 3 件は、指紋向けに限定されているが、これまでの PP と比べると、内容が良く整理されている。本事業で作成する PP では、CC パート 2 のセキュリティ機能要件及び CC パート 3 のセキュリティ保証要件だけでは作成できないと考えたため、上記 6 件の PP の拡張コンポーネント定義に特に注意した。この点においても、ドイツの PP、特に FSDPP[24]の拡張コンポーネント定義が最も参考になった。

本事業では ISO/IEC 19792 に基づいたバイオメトリクス製品固有の CC 評価・認証を可能にすることを目的としているが、ISO/IEC 19792 が主張する脆弱性評価のうち、どれがバイオメトリクス製品固有であるかが明確ではなかったので、ISO/IEC 19792 を詳細に分析して、バイオメトリクス製品固有の脆弱性評価の内容を絞り込んだ。

上記の調査結果は、第 4 回バイオメトリクスと認証・認識シンポジウム(SBRA2014)で論文発表した。内容は本書の付録のとおりである。

(2)ドイツの指紋に対するなりすまし検知機能の評価ガイダンス調査

脆弱性評価のための評価技術のために、文献 FSDEG[26]及び海外出張による調査を実施した。

FSDEG[26]には、FSDPP[24]に記述されているセキュリティ機能要件及びセキュリティ保証要件に対する拡張コンポーネントに加えて、セキュリティ保証要件に対する拡張コンポーネントの評価方法の概要が記述されている。FSDEG[26]からは、ドイツの認証機関である BSI と評価機関だけに開示されている別文書が参照されている。この別文書が定める偽造物タイプ及び偽造物の数に対する基準を満たし、それぞれの偽造物タイプについてエラー率の基準を満たせば合格とする、とされているが、それ以上の具体的な記述はない。

上記別文書に関する情報を入手できなかったため、その時点で案が固まっていた PP の紹介と併せて、平成 26 年(2014 年)11 月にドイツの評価機関 TUViT を訪問し、TUViT 技術者及び CC 認証機関である BSI 認証官と情報交換を実施した。この海外出張調査で、偽造物検知評価の標準体系の概要と合格基準を確認できた。

(3)欧州における精度評価及び脆弱性評価に対する取り組み調査

欧州におけるバイオメトリクス技術または製品の評価及び試験のための組織である BEAT（Biometrics Evaluation And Testing）において、精度評価及び脆弱性評価を推進しているマドリッド自治大学（Universidad Autonoma de Madrid）（以下 UAM と略す。）及び Idiap 研究所（Idiap research institute）（以下 Idiap と略す。）のメンバと面会し、欧州における精度評価及び脆弱性評価に対する取り組みを調査した。

BEAT における精度評価は Idiap が開発した BEAT プラットフォームを使用するとのことで、FAR、FRR 及び ROC カーブはともに重要は指標と考えており、精度評価では 3 のルールや 30 のルールは使用しておらず、ブートストラップ法と呼ばれる統計手法を採用している。

脆弱性評価では確率論的なアプローチを採用しようとしている。これは複数の被験者に対して複数の偽造物を用いてアタックを行い、成功率や効率といった性能指標を集計する統計的な評価を行うもので、本事業の脆弱性評価において、どのような方法論を採用するか早急に確立する必要があると考える。

また、Idiap の BEAT プラットフォームはテクノロジ評価を主目的とし、研究者向きツールであり、キャプチャを含めたシナリオ評価や運用評価の機能は含まれていないとの印象である。

ハードウェアを含んだ評価はできず、生体認証システムの一種のシミュレーションソフトであり、実際の製品の動作環境とは異なる評価のため、CC 認証には向いていないとの印象である。

これに対して本事業では、キャプチャ装置を含んだシナリオ評価を考えており、両ツールが実現すべき機能にも必然的に違いが生じると考えるに至った。

(4)韓国における精度評価に対する取り組み調査

平成 26 年(2014 年)12 月末に韓国 KISA で検討中の適合性評価、精度評価の検討状況調査を行い、韓国が開発を進めている Web ベースの試験システムを拡張して、精度評価化試験にも適用し

たいとの意向を持っているとの情報を得た。

(5)バイオメトリクス関係の標準化状況調査

平成 27 年(2015 年)1 月にスペインにて開催された SC37 国際会議に出席し、「脆弱性評価」「精度評価」等に関する標準化状況に関して調査するため、SC37 国際会議の WG 2 と WG 5 に参加した。

バイオメトリクスの精度評価に関する国際規格 ISO/IEC 29197 - Evaluation methodology for environmental influence in biometric system performance の FDIS 投票が可決した。本規格書は、バイオメトリック製品のシナリオ評価を含んだ規格であり、評価実施時の環境条件による性能への影響を測定する方法について示したものである。

特に Annex A: Values for environmental parameters (Informative Annex) には、基準となる性能を測定するための標準環境として気温[°C]、湿度[%]、照度[lx]、雑音[dB]、気圧[kPa]の値の範囲が示されている。

本事業において独立評価機関による独立試験を実施する際にも、何らかの環境条件を定義する必要があり、平成 27 年度における事業推進において、本規格の環境条件が検討候補のひとつになると考えられる。

4.1.2 方針検討

これらの調査結果を基に、PP 作成及び脆弱性評価の方針を作成した。これらの方針作成に当たっては、国内のバイオメトリクス製品ベンダー各社にインタビューして、その結果を参考にした。

(1)PP 作成

先ず、1.事業の目的にあるように、PP 及び PP に付随する評価手法は、国際標準案とするために作成することを目的としている。よって、作成する PP は、英語で作成することとし、広く活用されるように、バイオメトリクス製品のモダリティや身体部位に依存しないこと、ユーザ認証やユーザ識別に基礎的な機能を提供するバイオメトリクス製品の PP を作成することを方針とした。ユーザ認証とユーザ識別のいずれを対象にするかにについては、ベンダー各社へのインタビュー結果で決定することにした。

ISO/IEC 19792 が示すバイオメトリクス製品固有の評価内容、エラー率（精度）・脆弱性評価・プライバシーについては、個別に PP を作成することとし、製品に必要な PP を選択して、ST 作成、CC 評価認証できるようにすることを方針とした。ただし、平成 27 年度中に PP 評価・認証の完了を目標とするため、上記 3 つ全てを要件にすべきとのベンダーの合意があるなら、全てをまとめた PP を作成することも許容することとした。

脆弱性評価における想定する攻撃者の攻撃能力、製品の評価対象範囲である TOE（Target Of Evaluation）については、ベンダーへの意見聴取を通じて、決定することにした。

⑵脆弱性評価

5.1.1　海外動向調査 及び 5.3.3　脆弱性評価手法の研究 の結果を踏まえて、脆弱性評価の方針を検討した。

論文などの公開情報を基に、PP の定める攻撃能力を前提とした、攻撃方法及び偽造物のセット（レシピ）の案を作成する。試行用 TOE をベンダーに提供していただき、案に従って偽造物を作成して攻撃を試行する。この試行で攻撃方法及び偽造物のセットが妥当であるなら、認証機関の IPA も含めて、攻撃能力のレーティングを実施し、攻撃能力が基本であるかを確認する。そして、評価方法を決定するとともに、合否基準などの評定方法も決定する。この結果を適用して、再来年度からの製品の CC 評価・認証を実施する。静脈の偽造物を特徴付ける要素は素材、次元、波長であると考えられるので、これらの要素を組み合わせて、種々の偽造物を作成する。

偽造物作成のためのデータ収集は、装置（光源＋カメラ）を自製して、その装置を使用して行なう。3 次元の偽造物を作成する場合には、複数の 2 次元画像から 3 次元画像へ変換するソフトウェアの活用も検討する。

4.2　PP 開発及び PP 認証取得

4.2.1　PP 開発

ISO/IEC 19792 に基づいたバイオメトリクス製品固有の PP 作成に当たっては、産総研と JQA（日本品質保証機構）で協力し、素案を作成し、国内のバイオメトリクス製品ベンダー各社にインタビューし、委員会で意見聴取して、素案に反映されるという作業を 3 回繰り返し、PP 最終案をまとめた。作成した PP におけるバイオメトリクス製品の機能はユーザ認証だけを対象とし、CC 評価の対象となる TOE については各社の意見の共通部分とした。また、バイオメトリクス製品固有の CC 評価は精度評価と偽造物検知であると結論し、PP 最終案はこの結論に基づいた内容になっている。PP 最終案は、海外での活用も視野に入れて、英語で作成した。

バイオメトリクスによる利用者認証機能と CC パート 2 で定義された利用者認証（FIA_UAU（User Authentication））の機能との間に差異があるため、CC パート 2 のクラス FIA（識別と認証）を拡張して FIA_BUA（Biometric User Authentication）を定義した。セキュリティ保証要件は、EAL2 を基本とし、ALC_FLR.1 を追加の要件とした。

CC 評価・認証を受ける製品の TOE が、PP 最終案よりも多くの機能を含む場合の対応方法を記述したサポート文書案も作成した。

4.2.2　PP 認証取得

PP 最終案は、平成 26 年(2014)年 12 月 19 日からみずほ情報総研が評価を開始し、平成 27 年(2015 年)2 月 12 日に評価が完了し、評価合格した。本報告の時点では、IPA（情報処理推進機構）の認証作業中であり、認証の終了は 4 月 20 日の予定である。

4.3 セキュリティ評価手法の研究

本節では、バイオメトリック製品の CC 認証に基づくセキュリティ評価を行うにあたり実施する評価手法として、精度評価および脆弱性評価に関する研究結果の概要を示す。

4.3.1 精度評価のためのツール開発

精度評価の推進にあたっては、OKI ソフトウェアにて ISO/IEC 19795 規格の記載内容調査、他国が発行したバイオメトリック製品のためのプロテクションプロファイルの記載内容調査などを行った上で精度評価ツールの素案を作成し、今年度 4 回開催された検討委員会での審議に加え、本事業の委員として参加しているバイオメトリック・ベンダー6 社との個別会議を数回にわたり繰り返し意見交換を続けることで、素案へのフィードバックを加えていった。

精度評価ツールに関する今年度の主な検討結果を以下に示す。

①基本方針の決定

- コモンクライテリアにおける独立試験（ATE_IND）の作業を効率化することを目的とした精度評価ツールを開発する。
- 精度評価の国際規格である ISO/IEC 19795 に準拠したツールとする。
- 複数のバイオメトリック・ベンダーが使用できる共通ツールとするために BioAPI と呼ばれるバイオメトリクスの標準インタフェースを採用する。
- バイオメトリック装置とバイオメトリック・アルゴリズムの両方を評価できる、シナリオ評価を対象とする。
- バイオメトリック認証は 1:1 照合（Verification）を対象とし、精度評価項目として、FTE（登録失敗率)、FRR（本人拒否率)、FAR（他人受け入れ率）を算出する。ROC カーブは CC 認証において不要と判断される場合は、精度評価ツールの機能からは削除する。

② シナリオの検討

- 精度評価ツールが実行する処理フローをシナリオという言葉で表現し、バイオメトリック登録シナリオ（FTE 評価用)、バイオメトリック照合シナリオ（FRR 評価用)、クロスマッチシナリオ（FAR 評価用）を作成する。
- バイオメトリック登録シナリオは、キャプチャリトライを含むトランザクションを単位とし、FTE は 3 回の登録トランザクションをひとつのセットとして算出する（登録トランザクションを 3 回すべて失敗したら、バイオメトリック登録失敗として FTE を算出する)。
- バイオメトリック照合シナリオは、キャプチャリトライを含むトランザクションを単位とし、FRR は 3 回の照合トランザクションをひとつのセットとして算出する（照合トランザクションを 3 回すべて失敗したら、バイオメトリック照合失敗として FRR を算出する)。
- クロスマッチシナリオは、上記⑦と⑧で集められた被験者のバイオメトリック登録テンプレートおよびバイオメトリック照合データを用いた他人同士および同一人物の他の部位同士の全

件マッチングを行うことで FAR を算出する。

以上の精度評価ツールに関する検討を基にして、今年度は精度評価ツールの基本機能を開発した。開発機能の概要は以下のとおりである。

① 被験者用機能

・新規登録機能

・登録トレーニング機能

・照合トレーニング機能

・登録機能

・照合機能

② 管理者用機能

・総合進捗状況表示機能

・被験者毎の進捗状況表示機能

・クロスマッチ機能

・FTE・FRR・FTE 算出機能

4.3.2 精度評価のためのサポート文書開発

コモンクライテリアの評価・認証において、ベンダーによる社内試験や独立評価機関による独立試験における精度評価方法のガイドラインを、サポート文書案として作成した。本サポート文書案は、前述の精度評価ツールの開発における検討委員会および個別会議で得られた意見をまとめる形で、精度評価実施時の方針や、評価結果レポートの項目をまとめたものである。

精度評価サポート文書案は下記の内容を含んでいる。

①精度評価の分類

②取り扱う範囲

③精度評価実施時の基本方針

④精度評価レポートの全体構成

⑤レポート詳細

(1)本サポート文書案で取り扱う範囲

本サポート文書案において取り扱うバイオメトリック精度評価の範囲は以下のとおりとする。

①評価方法：シナリオ評価（テクノロジ評価、運用評価は対象外とする）

②バイオメトリック照合方法：1:1 照合（1:N 照合は対象外とする）

③評価単位：トランザクション単位（アテンプト単位、マッチング単位は対象外とする）

④評価尺度：FAR、FRR、FTE（FMR, FNMR,FTA などは対象外とする）

(2)精度評価実施時の基本方針

①製品が扱う生体の部位ごとに一つの ID を割当ててよい。（例えば左右の手が生体の部位であれば、ひとりの被験者あたり最大 2 つの ID を割当てられる。指であればひとりの被験者あたり最大 10 の ID を割り当てられる。）

②上記①で述べたそれぞれの部位におけるサンプル数は、登録テンプレート、1:1 照合バイオメトリック・データともに最大 1 枚とする。

③FTE の算出は、評価対象製品を用いた登録トランザクションを実行することで算出する。被験者ひとりの各評価対象生体部位あたりのトランザクション実行回数をあらかじめ設定し、規定回数分登録トランザクションを実行する。そのうち一度でもバイオメトリック登録に成功した場合、その部位については登録が成功したこととする。規定回数すべてに失敗した場合、その部位の登録は失敗とする。トランザクションの規定回数の推奨値は 3 とする。

④FRR の算出は、評価対象製品を用いた本人の同一部位同士の 1:1 照合トランザクションを実行することで算出する。被験者ひとりの各評価対象生体部位あたりのトランザクション実行回数をあらかじめ設定し、規定回数分 1:1 照合トランザクションを実行する。そのうち一度でもバイオメトリック照合に成功した場合はその部位については照合が成功したこととする。規定回数すべてに失敗した場合、その部位の照合は失敗とする。トランザクションの規定回数の推奨値は 3 とする。

⑤FAR の算出は、前述の FTE 評価で収集した登録テンプレートを各被験者の各部位からひとつ選択し、FRR 評価で収集した照合用バイオメトリック・データを各被験者の各部位からひとつ選択する。このように選択した、被験者の各部位ごとにひとつずつの登録テンプレートと 1:1 照合バイオメトリック・データを被験者全員分集めたデータを全件照合することにより求める。

⑥FTE、FRR、FAR を算出する際の信頼度は、原則として 3 のルール及び 30 のルールを用いる。これ以外の方法を用いる場合、その内容の詳細をレポートに含めなければならない。

⑦FTE、FRR、FAR の評価においては、ベンダーが定めるアルゴリズムの閾値を固定する。特に、FRR 評価と FAR 評価で異なる閾値を用いてはならない。

(3)精度評価レポートの全体構成

①基本情報：対象製品及び精度評価に関する概要情報である。製品情報（製品名、機能要約、想定用途、想定されるシステム構成)、評価者情報（精度評価実施者あるいは評価機関名）などを記述する。

②評価データ：評価に用いるバイオメトリック・データに関する記述である。見込み精度と必要な被験者数、データ収集条件、実際の被験者数及び被験者の構成（性別、年齢など）などを記述する。

③評価結果：精度評価を行った評価結果を記述する。FAR・FRR・FTE、未対応情報、限界精度などを記述する。必要に応じて ROC カーブも記述する。

④その他の報告事項：評価実施組織への連絡先に関する情報や認証書の送付先などを記述する。精度評価に関して特段の報告事項があれば自由記述形式で記述する。

(4)レポート詳細

①基本情報：実施したバイオメトリック精度評価に関する概要情報であり、評価対象製品を特定する情報、及び、精度評価の概要に関する情報が含まれる。

②評価対象製品：ベンダー名、アルゴリズム名、バージョン番号、モダリティ（指紋、顔、虹彩、静脈、署名、声紋、DNA など）、人体の部位名称（手、指、顔、目など）、部位の数（精度評価の対象となる指の本数、目の数など）、照合方式（1:1 照合のみ）、しきい値（推奨値、最小値、最大値）、評価者：精度評価実施組織名、評価条件：実施期間、被験者数

③評価データ情報：見込み精度（対象製品が見込んでいる精度値）、被験者募集方法及び募集条件（募集方法、募集条件など）、バイオメトリック・データ数（一人当たりのバイオメトリック・データ数、必要なバイオメトリック・データ数、実際に集めたバイオメトリック・データ数）、実際の被験者の分布（性別分布、年齢分布、職業分布など）、バイオメトリック装置情報（ベンダ名、製品情報）、データ収集環境（温度、湿度、環境光、ノイズなど）、シナリオ実行条件（被験者への事前説明状況、被験者の習熟度、被験者へのガイダンス）

④評価結果：FRR 及びその算出根拠を示す情報、FTE 及びその算出根拠を示す情報、FAR 及びその算出根拠を示す情報）

⑤その他報告事項：担当者連絡先、認証書の送付先など

4.3.3 脆弱性評価手法の研究

海外における研究動向調査として生体認証分野における最大規模の国際会議である IJCB2014 (International Joint Conference on Biometrics)へ出席し、調査を行った。

生体を模倣しないが高い確率で誤判定を発生させるウルフ(なりすましの入力情報)などを使った脆弱性評価手法の研究を行った。また、複数のバイオメトリクス照合アルゴリズムについて調査を行い、それらに共通して適用可能なウルフによる脆弱性解析方法を検討するとともに、ウルフ攻撃実験を行い、その有効性を確認した。

また、静脈認証装置に対する既存のなりすまし攻撃手段について調査を行った。本調査結果に加え、指紋認証機器における脆弱性評価手法の調査結果を基にして、静脈認証装置の脆弱性評価手法について対する基本的な考え方について検討した。

脆弱性評価の要件を 3 つに整理し、これらの要件を満たす脆弱性評価環境の構築を目的として、産業用ロボットを導入し、これによる実験環境を構築した。

また、非侵襲で生体等の内部を観察する測定装置である Santec 社製の OCT（IVS-2000）を用いて生体静脈及び偽静脈の測定を行い、偽静脈のように立体構造を有する偽造生体の内部構造の精密測定が必要な場合に OCT が極めて有効であり、他の測定方法に比べても優れていることを確認し

た。

4.4 国際標準化活動

ISO/IEC JTC 1/SC 37 においては ISO/IEC 30107 シリーズ：Biometric presentation attack detection へ評価式変更の提案、ISO/IEC JTC 1/SC 27 においては ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics の編集者に就任して第 1 作業原案の作成を実施した。

4.4.1 PP/脆弱性評価関連

ISO/IEC JTC 1/SC 37 では、生体認証機器へのなりすまし攻撃検知に関する標準化として ISO/IEC 30107 シリーズ: Biometric presentation attack detection の開発が進んでいる。ISO/IEC 30107 シリーズは下記の 3 つのパートから構成される。

Part1: Framework（フレームワーク）
Part2: Data formats（データ形式）
Part3: Testing and Reporting（性能評価と報告の方法）

本年度は、脆弱性評価と特に関連の深い ISO 30107 Part3 文書開発に対する寄与を目的として、1 月にスペイン・トレドで開催された SC37 会合に参加した。現地審議では、産総研からなりすまし攻撃性能の評価式である APCER に関する変更提案を行った。提案の内容は、既存の APCER が Attack Potential の異なる複数の偽造物を用いて攻撃を行った際の平均攻撃確率であるのに対して、これを最大の攻撃確率と変更するものである。セキュリティの観点から現行の平均値ではなく、最悪値（最大値）を考慮するのは妥当であるとされ、これらの変更は標準化文書に反映されることとなった。

ISO/IEC JTC 1/SC 27/WG 3 では、日本が提案した新規作業項目が、ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics として、平成 26 年(2014 年)10 月のメキシコシティー会議で成立した。編集者には産業技術総合研究所の山田朝彦が就任した。ISO/IEC 19989 の目的は、センサーへの偽造物提示などの攻撃に対する検知（Presentation Attack Detection（PAD））機能の CC 評価・認証を可能にすることである。そのために、必要な拡張コンポーネントを CC パート 2 及びパート 3 に対して定義し、それらに対応して CEM の補完をすることである。

平成 27 年(2015 年)1 月の SC 37 トレド会議の WG 3/WG 5 の合同セッションにおいて、産業技術総合研究所の山田が ISO/IEC 19989 の作成方針を説明した。

平成 27 年(2015 年)2 月には、ISO/IEC 19989 の第 1 作業原案を提出した。第 1 作業原案では、TOE をふたつに分類し、一方の TOE 分類では FSDPP[24]にあるセキュリティ機能要件の拡張コンポーネントを適用することが妥当であるが、他方の TOE 分類では別の拡張機能コンポーネントを適用するのが妥当であるとした。後者はまだ定義されておらず、寄書募集状態にあり、本事業の成果

であるユーザ認証の場合の拡張コンポーネント、今後予定しているユーザ識別の場合の拡張コンポーネントを日本 NB として提供の予定である。FSDPP[24]にあるセキュリティ保証要件の拡張コンポーネントも第 1 作業原案に採用した。

4.4.2 精度評価関連

バイオメトリック製品の精度評価について、ISO/IEC JTC1/SC37 WG5 への国際標準化提案の可能性を検討中である。特に、精度評価の結果として宣言する FTE、FRR、FAR などの精度値算出根拠となるエビデンス情報の項目や内容に関する新規提案の可能性があると考え、国際新規提案の実現性について平成 27 年度以降さらに検討を進める予定である。

5. 事業成果詳細

5.1 海外動向調査及び方針検討

本事業は、ISO/IEC 19792 の主張に基づいて、精度評価・脆弱性評価・プライバシーを組み込んだバイオメトリクス製品の CC（Common Criteria）評価･認証を可能にすることを目的としている。CC 評価・認証のためには、製品ベンダーはセキュリティ設計仕様書である ST（Security Target）を作成しなければならない。ST 作成は CC 独自のノウハウを必要とするため CC 専門家以外には難しく、そのために CC 評価・認証にコストがかかるという問題が存在していることが今までの活動を通じてわかっていた。CC には ST の他にセキュリティ要件定義書に相当する PP（Protection Profile）が存在するので、ST 作成を容易化するために、本事業では ISO/IEC 19792 に基づいた PP を作成することにした。また、ISO/IEC 19792 に基づいたバイオメトリクス製品の CC 評価・認証のためには、通常の IT 製品とは異なる精度評価・脆弱性評価・プライバシーに関する評価機関・認証機関での評価・認証の作業が必要となる。そのための評価技術の確立も必要である。よって、海外動向調査では､バイオメトリクス製品に対する既存 PP と評価技術に関して文献及び海外出張による調査を実施し、その調査結果を参考にして、PP 作成及び評価技術確立の方針を作成した。

5.1.1 海外動向調査

PP については、インターネット上で入手可能な PP を調査した。評価技術については、インターネット上で入手可能な文献に加え、ISO/IEC JTC 1/SC 27/WG 3 への寄書、更に既に指紋のなりすまし攻撃検知の製品に対する CC 評価・認証を開始しているドイツの状況を海外出張して関係者から情報入手した。

(1)PP 調査

PP については、ドイツの BSI（Bundesamt für Sicherheit in der Informationstechnik）が 3 件（BVMPP [23]、FSDPP [24]、FSDPP_OSP [25]）、米国 Information Assurance Directorate が 2 件（PPBVMBR [30]、PPBVMMR [31]）、英国 UK Government Biometrics Working Group 1 件（BDPP [38]）、それぞれ作成して来た。

英国では、バイオメトリック機器の PP を 2001 年に作成していたようだが、CC の旧版に基づいたもので、草稿しかない。ISO/IEC 19792 が主張するようなバイオメトリクス固有の評価の観点は考慮されず、バイオメトリック機器のセキュリティが考慮されている。幅広い保証レベルに対応するために EAL1 から EAL4 のセキュリティ保証要件を定義しているが、セキュリティ機能要件については、FAR・FRR に関するセキュリティ対策方針に対応するセキュリティ機能要件がバイオメトリクス以外のパスワード認証や PKI 認証に適用される FIA_UAU.2 が適用されていて、バイオメトリクス固有の特性が考慮されていない。そのような意味で、草稿に終わっただけでなく、内容が妥当性を欠いている。

米国では、2 件の PP が認証されたが、ともに 2008 年に失効している。PPBVMMR [31] には通信データの秘匿性と完全性が要求されているのに対して、 PPBVMBR [30] にはそうした要求はない。PPBVMMR [31] では PPBVMBR [30] よりも、高い攻撃能力を想定した脅威を挙げ、セキュリティ対策方針も高度である。この 2 つの PP の最大の欠陥は、テンプレートが暗号の秘密情報と同様にランダムに生成でき、よって FAR や FRR が制御できるかのように考えられて、機能要件が設定されていることである。これだけでなく、BDPP [38]と同様に、バイオメトリクス固有の特性が考慮されていないという問題もある。

ドイツでは、2008 年から 2009 年に、3 件の指紋向けの PP が作られた。いずれも、バイオメトリクスの処理を、登録、認証、識別の 3 つがあるとしながら、登録だけを対象として作成されている。BVMPP [23]は、ユーザ認証自体を対象とした PP で、偽造物提示によるなりすましは想定されていない。FSDPP [24]と FSDPP_OSP [25]はなりすまし検知機能に特化した PP で、FSDPP [24] はなりすましなどの脅威を想定している。これに対し、FSDPP_OSP [25] は、脅威を想定せずに、バイオメトリクス製品がなりすまし検知することを組織のセキュリティ方針として、求めている。その結果、FSDPP [24] では脆弱性評定が保証要件になっているのに対して、FSDPP_OSP [25] では保証要件になっていない。これらの PP は、これまでの PP と比べると、内容が良く整理されている。しかし、BVMPP [23]は種々の脅威への対策が監査データのチェックによって成されることになっており、実装に大きく依存するので、一般性を欠く。FSDPP [24] と FSDPP_OSP [25] の差異は脆弱性評定の有無で、FSDPP_OSP [25] に基づいた評価では実際の攻撃による評価は実施されない。FSDPP [24] の特徴は、CC パート 3 にない最低レベルの攻撃能力（Minimal attack potential）を定義し、その攻撃能力での脆弱性評定を実施することを求めていることである。これは、バイオメトリクス製品の CC 評価を段階的に進めて行くための BSI の配慮とも考えられる。

本事業が目標とする ISO/IEC 19792 が示すバイオメトリクス固有の CC 評価・認証を可能にするための PP には、本事業開始前から、拡張コンポーネントの定義が必要であると考えて来た。その観点から上記の PP を見ると、英国の BDPP [4]には拡張コンポーネントはない。米国の PPBVMBR [30]と PPBVMMR [31]には、それぞれ 2 個と 11 個の拡張コンポーネントが定義されている。これらの差は、通信データの秘匿性と完全性に対する要求に基づく差異である。

PPBVMBR [30]における拡張コンポーネントは、登録における FIA_ENROLL_(EXT).1 と物理的攻撃に対する FPT_PHP_(EXT).1 である。前者は PP が登録を含む場合に参考になり、後者は PP が物理的攻撃を含む場合に参考になる。ドイツ作成の 3 つの PP では、FSDPP [24]と SDPP_OSP [25]がそれぞれ 2 個と 1 個の拡張コンポーネントを定義している。SDPP_OSP [25]で定義されている拡張コンポーネントは、FSDPP [24]でも定義されており、セキュリティ機能要件の拡張コンポーネント FPT_SPOD である。これは、バイオメトリクスのなりすまし攻撃検知のセキュリティ機能要件を定義するものである。FSDPP [24]で定義されているもうひとつの拡張コンポーネントは、セキュリティ保証要件 AVA_VAN.E であり、CC パート 3 にない最低レベルの攻撃能力

（Minimal attack potential）を導入した結果、CC パート 3 にある AVA_VAN.2 とは前提とする攻撃能力に違いがあるが、CEM が要求する評価方法論としてはほぼ同等のセキュリティ保証要件を定めている。FPT_SPOD については、FSDPP [24]と SDPP_OSP [25]がバイオメトリクスの処理全体を含まず、なりすまし検知の機能だけを TOE（Target Of Evaluation、CC 評価・認証の対象）としたことによって必要となった拡張コンポーネントなので、本事業で同様の拡張コンポーネントの要否は、本事業で作成する PP の TOE に依存すると判断した。AVA_VAN.E については、本事業で作成する PP が想定する攻撃能力に依存する。

調査した PP では、資産を 1 次資産と 2 次資産に分類している。PP の構造としては、脅威、セキュリティ対策方針、セキュリティ機能要件のいずれについても平坦な構造を持っているが、調査の結果、実際は 1 次資産と 2 次資産に応じて、CC の評価・認証は構造化されていることがわかった。ここで、1 次資産とはバイオメトリック製品が守る資産、すなわち、バイオメトリクスによるユーザ認証の結果として守る資産であり、2 次資産とはバイオメトリクス製品の中のセキュリティに関わるデータである。

図 5.1-1 に 1 次資産・2 次資産に基づいたセキュリティ評価の構造を図示する。

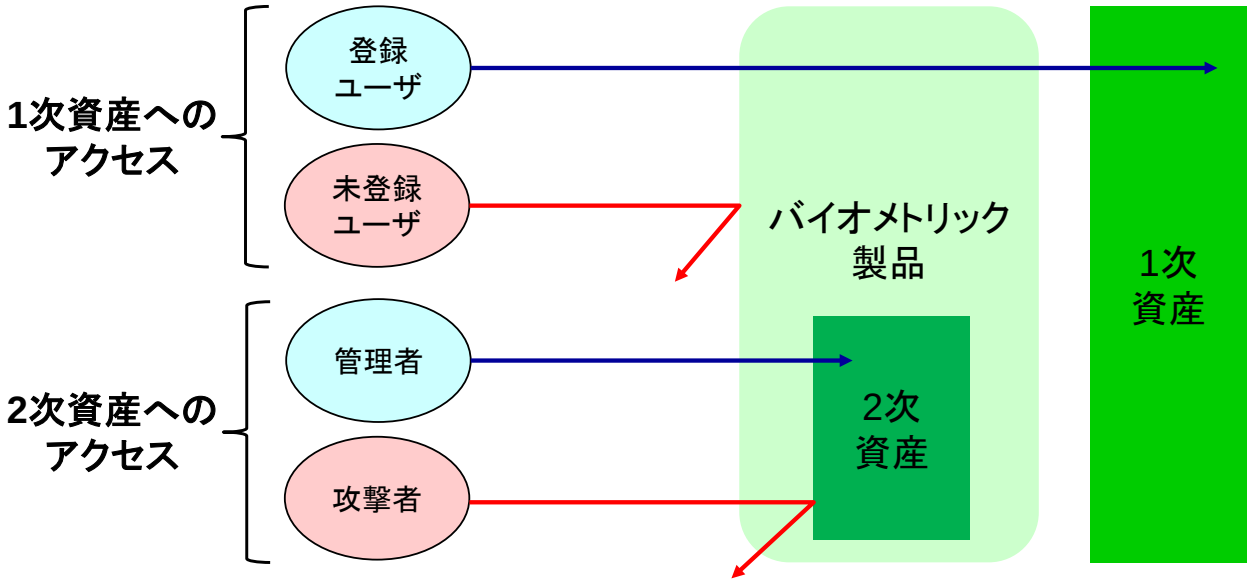


図 5.1-1　1 次資産・2 次資産に基づくセキュリティ構造の関係

図 5.1-1 に基づき、改めて CC 評価・認証におけるセキュリティ機能要件及びセキュリティ保証要件を整理すると、表 5.1.1 のようになる。1 次資産を守るという観点で必要となるセキュリティ機能要件は、CC パート 2 では FIA（識別と認証）だけである。このセキュリティ機能要件に対するセキュリティ保証要件として必要になるものは、表にあるように、ADV、AGD、ACL、ATE、AVA である。AVA は、表の注が示すように、PAD（Presentation Attack Detection）に対する脆弱性評定である。2 次資産を守るという観点で必要となるセキュリティ機能要件は、CC パート 2

のセキュリティ機能要件全てと CC パート 3 のセキュリティ保証要件全てが候補となる。作成する PP が対象とする範囲によって、これらは絞り込まれることなる。また、表の注に示したとおり、ここでの AVA は、2 次資産を守るバイオメトリック製品全体の機能に対する脆弱性評定となる。

表 5.1-1　1 次資産・2 次資産に基づく CC 機能要件・保証要件と ISO/IEC 19792 との関係

	対象機能要件	対象保証要件	ISO/IEC 19792観点
第1資産を守る	FIA（ユーザ対象）	ADV AGD ALC ATE AVA*1	精度評価 脆弱性評価
第2資産を守る	FAU FCO FCS FDP FIA（管理者対象） FMT FPR FPT FRU FTA FTP	ADV AGD ALC ATE AVA*2	プライバシー

注）＊1： PAD の意味での脆弱性評価、＊2： システムとしての脆弱性評価

また、PP 作成の過程で、ISO/IEC 19792 が示す脆弱性評価の構造を再調査した。ISO/IEC 19792 が示している脆弱性評価の観点は、以下の A から I までである。

A. 精度の限界

B. 偽造物提示

C. 自分でなく見せたり（認証や識別を失敗させる）他人をまねる（なりすまし）

D. 露出（顔など）または残存（指紋など）する生体データ（偽造物作成の元データにする）

E. 近親者のデータ類似（なりすまし）

F. 人間のラムやウルフ

G. 人工ウルフ

H. ノイズの入ったデータによる照合成功（特にノイズの入ったテンプレートと）

I. 不正な登録（異なる ID での登録，偽造物での登録，ノイズの入ったテンプレート）

J. バイオメトリック・データの漏えい・置換

これらの間の関係を図示したのが、以下の 5.1.2 である。

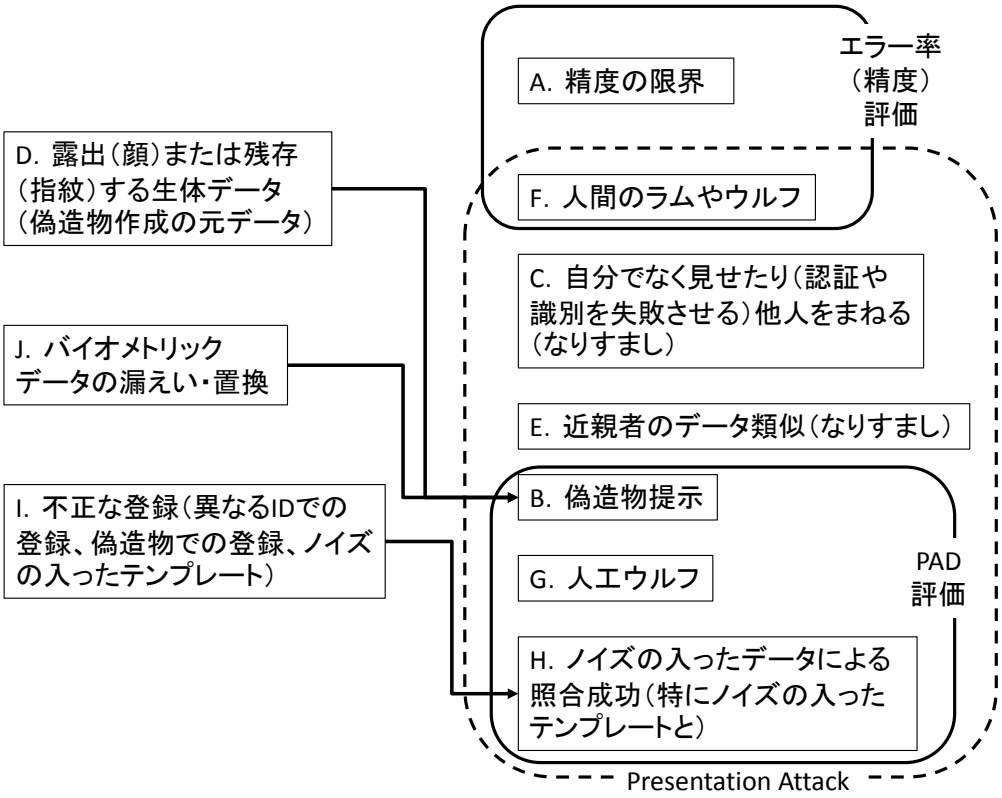


図 5.1-2　ISO/IEC 19792 における脆弱性評価の構造

この図において、D、I、J は、それ自体がバイオメトリクスによるユーザ認証の脆弱性となるのではなく、他の脆弱性の誘因となるものである。

A は精度評価自体で評価され、F の人間のラムやウルフも精度評価の結果として評価される。

C は評価者自身による実行は難しく、E はデータ取得が難しいので、評価に適用するのは難しい。

B、G、H は、PAD が扱う脆弱性であり、PAD 評価によって評価されるべきものである。

他の脆弱性の誘因となるものを併せると、本人の生体に由来するバイオメトリック・データか否かを評価するためには、D、I、J、B、G、H の評価が必要である。ただし、I は登録における脆弱性なので、ユーザ認証だけの評価であれば除外される。

PP 作成の過程での ISO/IEC 19792 の再調査において、ISO/IEC 19792 で問題とされているプライバシーは、匿名性、偽名性、リンク不能性、観察不能性などを対象とする CC パート 2 のセキュリティ機能要件クラス FPR(プライバシー)の内容ではなく、セキュリティ機能要件クラス FDP(利用者データ保護)の内容であることがわかった。また、バイオメトリクスに要求されるプライバシーが CC パート 2 のクラス FPR 以外のものを含まないと判断した。当初は、バイオメトリクス固有の要求を考慮して、必要があればクラス FPR の拡張コンポーネント定義をすることを考えたが、その必要はないとの結論に至った。

(2)ドイツの指紋に対するなりすまし検知機能の評価ガイダンス調査

FSDPP[24]に対する評価方法論を含む文書 FSDEG[26]が、ISO/IEC JTC 1/SC 27 の Study period on Security evaluation of anti-spoofing techniques for biometrics に対して、2012 年 10 月にドイツから寄書提出された。この文書は、SC 27 の委員だけが閲覧可能な文書である。

FSDEG[26]には、FSDPP[24]の TOE、セキュリティ機能要件及びセキュリティ保証要件に対する拡張コンポーネント、セキュリティ保証要件に対する拡張コンポーネント AVA_VAN.E の評価方法の概要が記述されている。しかし、詳細の記載はない。評価方法の詳細は、FSDEG[26]から参照の非公開文書である Toolbox に記載されている。FSDEG[26]が公開を想定した文書であるのに対して、実際の CC 評価・認証におけるより詳細な情報はバイオメトリック製品に対する攻撃を助長する結果になりかねないため、Toolbox の公開を CC の評価機関及び認証機関に限定している。

PAD の機能を ATE_FUN（ベンダーテスト）及び ATE_IND（評価機関による独立テスト）、更に AVA_VAN（評価機関による脆弱性評定）のペネトレーションテストで保証する。ATE_FUN に基づき ATE_IND を実施し、ATE_IND に基づき AVA_VAN を実施することが記載されている。

FSDEG[26]では、精度評価におけるエラー率である FAR・FRR と類似の PAD におけるエラー率を定義している。FSDEG[26]におけるエラー率の考え方を表 5.1.2 に示す。なお、ISO/IEC WD 30107-3[37]では、FSNDR は APCER（Attack Presentation Classification Error Rate）、FSDR は NPCER（Normal Presentation Classification Error Rate）、とそれぞれ定義されているが、呼称が異なるだけで本質的な差異はない。

表 5.1-2　FSDEG[26]におけるエラー率

		偽造物の提示	
		Yes	No
偽造物の判定	Yes		**このエラー率を FSDR**（False Spoof Detect Rate)
	No	**このエラー率を FSNDR**（False Spoof Not Detect Rate）	

FSDEG[26]では、ATE_FUN（ベンダーテスト）、ATE_IND（評価機関による独立テスト）、及び AVA_VAN（評価機関による脆弱性評定）に対して、次のような基準を設けている。

ATE_FUN では、Toolbox が定める偽造物タイプ及び偽造物の数に対する基準を満たし、それぞれの偽造物タイプについてエラー率の基準を満たせば合格とする。

ATE_IND では、ATE_FUN の偽造物の提供を受けて ATE_FUN の部分テストを実施し、併せて、独自に作成した偽造物を使った追加テストを要求している。そして、Toolbox の基準を満たせば合格としている。

AVA_VAN では、ST、AGD、ADV、及び ATE_FUN の結果を基に TOE の弱点を考察し、想定する攻撃能力に基づいて、偽造物を使ったテストを実施することを要求している。そして、合格基準は、FSNDR 及び FSDR を定義しているにも関わらず、誤判定が再現されないこととしている。

これらは、CC 評価・認証の実施を目標とする本事業にとって、脆弱性評定の基準作成において、重要な参考情報になる。

FSDEG[26]で参照されている Toolbox は、上述のとおり、開示されていない。ドイツ BSI と緊密な連携関係にある IPA を経由して情報入手を試みたが、情報を入手することはできなかった。部分的な入手であっても来年度以降の CC 評価・認証にとって重要な参考情報になると考え、その時点で案が固まっていた PP の紹介と併せて、平成 26 年(2014 年)11 月にドイツの TUViT を訪問し、CC 評価機関である TUViT 技術者及び CC 認証機関である BSI 認証官と情報交換を実施した。

ツールボックスの基本ツールは、25 素材で各素材 5 個の偽造指紋を作って評価する。それが通ってから、評価機関・認証機関とも評価対象個別の解析をして攻撃する。基本ツールの型取りにおいては歯型を取る素材は速乾性があって良く、偽造指作成においてはゼラチンが優れている、とのことであった。

また、FSDEG[26]にも提示されているとおり、PAD を検出エラー率で評価することには否定的であり、複数回誤判定で失格という基準であることも、改めて確認した。

(3)欧州における精度評価及び脆弱性評価に対する取り組み調査

欧州におけるバイオメトリクス技術または製品の評価及び試験のための組織である BEAT（Biometrics Evaluation And Testing）において、精度評価及び脆弱性評価を推進しているマドリッド自治大学（Universidad Autonoma de Madrid）（以下 UAM と略す。）及び Idiap 研究所（Idiap research institute）（以下 Idiap と略す。）のメンバと面会し、欧州における精度評価及び脆弱性評価に対する取り組みを調査した。

UAM のメンバのヒアリングより次の状況がわかった。

(a)BEAT 活動概要

・BEAT は大学及び企業を中心に構成されている。

・BEAT を主導する組織は Idiap であり、UAM は 2 番目のポジションとして精度評価と脆弱

性評価に関する学会としての活動を行っている。

・BEAT は 3 ヵ年の活動で今年が最終年である。

(b)精度評価について

・精度評価は Idiap が開発した BEAT プラットフォームを使用する。

・精度評価において必要となる被験者数は求められる FAR や FRR で変化する。UAM ではテクノロジ評価におけるデータベースの構築方法についてノウハウがあるので、契約を取り交わすことによりコスト効率良く精度評価用のデータベースの構築をサポートできる。

・FAR、FRR 及び ROC カーブはともに重要な指標である。ROC は細かい性能のチューニングが必要な場合に利用される。

・精度評価では 3 のルールや 30 のルールは使用しておらず、ブートストラップ法と呼ばれる統計手法を採用している。

(c)脆弱性評価について

・脆弱性評価では確率論的なアプローチを採用しようとしている。これは、複数人の被験者と複数の偽造物を用意し、アタックをかけて成功率（SR と呼ばれる）及び効率（Eff と呼ばれる）を評価するものである。

・成功率と効率を用いた評価方法については BEAT 内で議論が行われ過半数のメンバからの賛同を得ている。

・SR と Eff を算出する前に精度評価を行っておき、脆弱性評価を行う際にはアルゴリズム閾値の FAR と FRR の値を特定しておくことが重要である。（アルゴリズム閾値を変えることで SR と Eff が変化するため。）

(d)Idiap の BEAT プラットフォームについて

・BEAT プラットフォームはアルゴリズム評価のためのものでありハードウェアは含んでいない。シナリオ評価をしようとしたら、特定のシナリオを実行してその時に取得されたバイオメトリック・データを何らかの方法で収集し、BEAT プラットフォーム上に転送する必要がある。

・現在は精度評価機能しかサポートしていないが、年内に脆弱性評価機能もサポートする予定である。ここで言う脆弱性評価は spoof detection だけでなく、それ以外の脆弱性評価も含む予定である。

・BEAT テストプラットフォームが評価できるのはアルゴリズムの組み合わせの評価であり、アプリケーションのような製品の評価はできない。

・脆弱性評価機能を組み込んだ後は、さらに広いテーマとしてパターン認識系の技術の評価用プラットフォームに拡張していく予定である。

これらヒアリングにより、BEAT プラットフォームはテクノロジ評価を主目的としたツールであり、キャプチャを含めたシナリオ評価や運用評価の機能は含まれていないことがわかった。

これに対して本事業では、キャプチャ装置を含んだシナリオ評価を考えており、両ツールが実

現すべき機能にも必然的に違いが生じると考える。

また、精度評価値算出のための統計手法としてブートストラップ法を採用していることがわかった。これは、限定されたサンプル数で統計上の信頼度を向上する手法であり、結果的に被験者数の低減がもたらされると思われる。本事業においてもブートストラップ法を採用することで、独立試験の被験者数削減、すなわちコスト低減に寄与する可能性があると考える。

また、BEAT では複数の被験者に対して複数の偽造物を用いてアタックを行い、成功率や効率といった性能指標を集計する統計的な評価が考えられていることがわかった。本事業の脆弱性評価において、どのような方法論を採用するか早急に確立する必要があると考える。

また、精度評価機能に加えて、年内中に BEAT プラットフォームに脆弱性評価（セキュリティ評価）のための機能を開発が計画されていることがわかった。これに対して本事業におけるツールは、精度評価機能しか検討されていない。本事業の脆弱性評価において統計的な分析が必要な場合、脆弱性評価の統計情報収集機能を追加することで独立試験作業を効率化できる可能性があると考える。

次に Idiap のメンバのヒアリングより次の状況がわかった。

- BEAT プラットフォームの評価対象はアルゴリズム（ソフトウェア）である。ここで言うアルゴリズムとは、キャプチャデータの前処理（pre-processing）、コード化処理（processing）、比較（matching）など、バイオメトリック処理の構成要素となるロジック部分を意味する。
- BEAT プラットフォームは複数コアの CPU を持った PC が何台か並んだサーバシステムであり、フロントエンドとバックエンドの 2 つのサブシステムからなる。フロントエンドはブラウザを用いて画面操作を行うものであり、バックエンドは Web サーバ内でバイオメトリックデータベースやアルゴリズムを保持する。アルゴリズムはバックエンドで実行される。
- 事前に用意されたバイオメトリック DB と各種アルゴリズムのコンポーネントの出力部分と入力部分を GUI 操作で接続し、擬似的なシステムをプラットフォーム上で生成することができる。生成されたひとつの擬似的なシステムをツールチェイン（toolchain）と呼んでいる。
- 様々なアルゴリズムに対応できるようツールチェインは柔軟に構成できる。ツールチェインの最終端には精度計算用コンポーネントが接続され、ここで FAR や FRR などの精度値が算出される。この精度計算用コンポーネントも評価者が自分で開発し、ツールチェインに接続する。
- 各アルゴリズムは Python で記述することが前提となっている。今後は他の言語もサポートしていく予定。
- グループウェア的な機能を持っていて、自身が開発したアルゴリズムを BEAT プラットフォームに参加している他ユーザに公開することができる。公開の方法にはオブジェクトレベルとソースレベルの 2 通りが指定できる。
- Certification と呼ばれる機能がある。一度評価した結果を certification すると、ツールチェインの環境（アルゴリズム、データベースなど）がすべて変更できない状態（ロック状態）

になるため、BEAT プラットフォームにおいて再現性を持った証拠情報となる。このエビデンス情報は BEAT 外の他者にも示すことができる。

・ツールチェイン上の複数のコンポーネントの動作環境がそれぞれ異なっている場合でも（例えば Linux と Windows など）、利用者は意識せずに動作させることができる。

・BEAT プラットフォームはハードウェアの評価を含んでいない。CC 認証のための評価に適用することを考慮したものではない。

・BEAT プラットフォームには年内中に脆弱性評価を追加する予定である。実際の作業は UAM がこのツールを使って実現する予定。開発したアルゴリズムをツールチェインとして構成する BEAT プラットフォームの機能を脆弱性評価に適用する。脆弱性評価にはゴールデンフェイクと呼ばれる代表的な偽造物を使ってアタックを行いマッチングできなければ合格、マッチングできれば失格という二者択一の評価方法と、確率論的なアプローチを用いる方法の 2 つの考え方がある。BEAT プラットフォームはこのどちらも対応できる設計になっているため、それぞれの考え方に沿った評価環境の構築ができる。

・現在 BEAT プラットフォームは精度評価機能の開発を完了しスポンサーメンバーに公開中だが、平成 27 年(2015 年)12 月にオープンソース化する予定。EU 外にも公開することになると思う。

これらヒアリングにより、BEAT プラットフォームは研究者向きツールであり、以下のような状況において最も力を発揮するツールだと感じた。

・大学の研究者（及び企業の研究者）が特定の機能のアルゴリズムを開発した場合、擬似的なシステムをプラットフォーム上で構築することにより性能評価のシミュレーションができる。

・ツールチェインの構成要素を入れ替えることにより、自身が開発したアルゴリズムと相性の良いアルゴリズムの組み合わせを知ることができる。

また、ツールとしての完成度が高く、ビジュアルな表示、操作性、マルチプラットフォーム対応、グループウェア機能など、凝った作りこみがされている。

しかしながら､ハードウェアを含んだ評価はできず､また生体認証システムの一種のシミュレーションソフトであり、実際の製品の動作環境とは異なる（ただし、アルゴリズム製品の評価には適用できそう）評価のため、CC 認証には向いていないとの印象を持った。

(4)韓国における精度評価に対する取り組み調査

平成 26 年(2014 年)12 月 26 日に、韓国 KISA で検討中の適合性評価、精度評価の検討状況調査を行い、韓国の Web ベースでの BioAPI の適合性試験のプロジェクトは、平成 26 年度も INHA Univ.で開発が進められ、最終テストフェーズある。また、適合性試験は平成 27 年度に設立予定の KBID(Korea Biometrics Identity Security Association)で実施を予定しているとのことであった。

また、将来的には、この Web ベースの試験システムを拡張して、精度評価化試験にも適用した

いとの意向を持っているとのことであった。

韓国も精度評価化試験事業に取り組む予定なので、今後日本として韓国との連携について検討をしていく必要がある。

注) KBID は、KBA(Korea Biometrics Association)下の組織とする予定。KBA は、Dr. Jason Kim や Dr. Hale Kim などの韓国バイオメトリクス関係者で設立した韓国の民間組織。

(5)バイオメトリクス関係の標準化状況調査

平成 27 年(2015 年)1 月 12 日(月)～13 日(火)の期間、スペインにて開催された SC37 国際会議に出席し、「脆弱性評価」「精度評価」等に関する標準化状況に関して調査するため、SC37 国際会議の WG 2 と WG 5 に参加した。

WG 2 では、インターフェィス・適合性評価に関わる標準化プロジェクトが審議されていたが、進行中の BioAPI (2.0)や BioAPI (3.0)に関係するプロジェクトが、エディタ不在等で開発・審議が進んでいない状況であることが分かった。

WG 5 では、セキュリティに関わる事項として、次の審議状況を調査した。

①認証性能に対する環境（温度、照明、騒音など）の影響度の評価方法

・FDIS 29197 Evaluation methodology for environmental influence in biometric system performance として開発されている。国際審議の最終段階の投票が賛成多数で終了し、今後出版されることとなった。

本規格書は、バイオメトリック製品のシナリオ評価を含んだ規格であり、評価実施時の環境条件による性能への影響を測定する方法について示したものである。

特に Annex A: Values for environmental parameters (Informative Annex) には、基準となる性能を測定するための標準環境として気温[°C]、湿度[%]、照度[lx]、雑音[dB]、気圧[kPa]の値の範囲が示されている。

本事業において独立評価機関による独立試験を実施する際にも、何らかの環境条件を定義する必要があり、平成 27 年度における事業推進において、本規格の環境条件が検討候補のひとつになると考えられる。

②テンプレート防護に対する性能評価

・WD3 30136　Performance testing of template protection schemes として開発されている。章構成の変更やマルチ・システムとシングル・システムでの SAR(攻撃成功率(successful attack rate))の記述方法や irreversibility の定義などについて審議されている。

インターフェィス・適合性評価については、関係する審議プロジェクトが複数あるが、残念ながらエディタが不在となるなどで活動が停滞し、プロジェクトが中止されるものも出始めている。したがって、現在制定されている標準規格をベースに検討をすすめ、新たな国際標準化検討内容

については、動向を注視し、必要に応じで対応を検討することで進めていくのが良いとの印象を得た。

ただし、セキュリティに関わる事項については、プレゼンテーションアタックディテクションのテストと報告に関わる 30107 の動向を注視してゆく必要があると考える。

5.1.2 方針検討

(1)PP 作成

先ず、１．事業の目的にあるように、PP 及び PP に付随する評価手法は、国際標準案とするために作成することを目的としている。よって、作成する PP は、英語で作成することとし、広く活用されるように、バイオメトリクス製品のモダリティや身体部位に依存しないことを方針にした。

PP は、通常、用途を想定した製品のセキュリティ要件定義書である。この考えに基づいて、本事業の開始以前に、入退室向けのバイオメトリクス製品の PP 作成について、各社に意見聴取した。結果は、用途があまりに限定的であり、そのような PP を作成しても、それに基づいた ST 作成及び製品の CC 評価・認証も極めて限定されるという理由で、否定的された。この経験から得られた方針としては、バイオメトリクスには多様なアプリケーションがあるので、アプリケーション毎に CC 評価・認証を受けるのは現実的ではない、ということである。また、調査した 5 つの PP のいずれもが、アプリケーションを含まず、バイオメトリクスの機能だけを対象としたものであった。結果として、ユーザ認証やユーザ識別のように基礎的な機能を提供するバイオメトリクス製品の PP を作成することを方針とした。このような方針を取ったとしても、アプリケーションも含めた CC 評価・認証を受ける場合にも、バイオメトリクス製品だけの PP は活用可能である。よって、この方針に基づいた PP の適用範囲は広いと考えた。ユーザ認証やユーザ識別のいずれを対象にするかについては、ベンダー各社へのインタビュー結果で決定することにした。

ISO/IEC 19792 に基づいた PP 作成が基本方針であるが、製品によっては、エラー率（精度）・脆弱性評価・プライバシーの全てを要件にしない可能性がある。そのため、エラー率（精度）・脆弱性・プライバシーについて、個別に PP を作成することを方針とした。製品に必要な PP を選択して、ST 作成、CC 評価認証できるようにする。ただし、平成 26 年度中に PP 評価・認証の完了を目標とするため、上記 3 つ全てを要件にすべきとのベンダーの合意があるなら、全てをまとめた PP を作成することも許容する方針とした。エラー率（精度）・脆弱性評価・プライバシーを要件とする PP を作成するためには、拡張コンポーネント定義が必要と考えられた。エラー率（精度）については保証要件のテストの拡張コンポーネント、脆弱性評価については保証要件の脆弱性評定の拡張コンポーネント、プライバシーについては機能要件のプライバシーの拡張コンポーネントとすることを基本的な考え方として、進めることにした。この考え方を図 5.1-3 に示す。

図 5.1-3　想定した拡張コンポーネントの位置付け

PP が想定する攻撃者の攻撃能力に、認証までの全体コストが大きく依存する。脅威を適切なレベルに設定して、妥当な脆弱性評価のレベルを決定することが重要である。コスト負担はベンダーになるので、ベンダーへの意見聴取で PP が想定する攻撃能力を決定することにした。

PP 作成の出発点は、評価対象範囲である TOE を決定することである。製品によって含む処理が異なるので、これについても、ベンダーへの意見聴取を通じて、決定することにした。想定した TOE としては、図 5.1-4 に示す 3 つの形態を考えた。統合タイプは、全てのバイオメトリクスの処理を含む製品タイプである。センサータイプは、データ採取と特徴抽出だけの機能を持つ製品タイプであり、名前のとおりセンサーの製品タイプである。MOC (Match On Card) タイプは、銀行の生体認証機能付き ATM の IC カードのように、登録生体情報を格納する機能と実行時に採取され特徴抽出して得られたデータを登録生体情報と照合して判定結果を出す機能とを含む製品タイプである。STOC（Store On Card）タイプは、登録生体情報の格納機能だけを持つ製品タイプである。

CwC（Comparison with Capture）タイプは、STOC タイプ製品と組み合わせて使われ、STOC タイプの製品が持つ機能以外の機能を持ち、バイオメトリクスの処理を実行する製品タイプである。

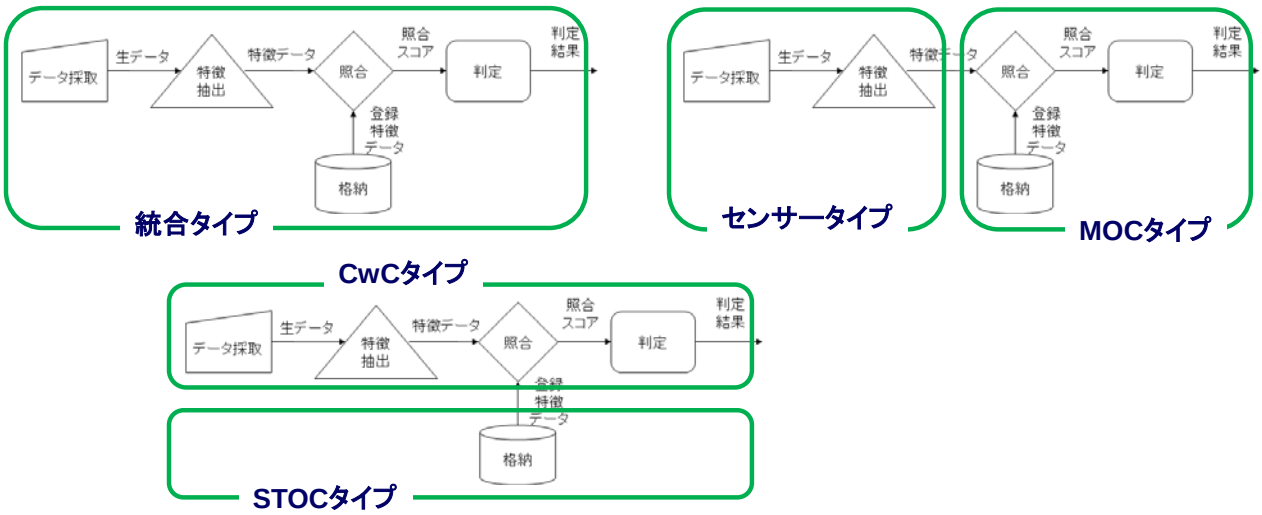


図 5.1-4　想定した製品タイプ

付録 1 は、PP 作成の過程の方針再検討の段階でまとめた論文である。平成 26 年(2014 年)11 月 25 日・26 日に開催された SBRA2014 で第 1 日目に発表した。

(2)脆弱性評価

5.1.1　海外動向調査 及び 5.3.3　脆弱性評価手法の研究 の結果を踏まえて、脆弱性評価の方針を検討した。脆弱性評価の進め方は、図 5.1-5 のようになる。

論文などの公開情報を基に、攻撃方法及び偽造物のセット（レシピ）の案を作成する。後述のように、本事業で作成した PP の保証要件では AVA_VAN.2、すなわち攻撃能力は基本を要求している。よって、攻撃能力基本を前提に、上記の攻撃方法及び偽造物の案を作成する。ベンダーの協力の下に試行用 TOE を提供していただき、上記の案に従って偽造物を作成して攻撃を試行する。この試行で攻撃方法及び偽造物のセットが妥当であるなら、認証機関の IPA も含めて、攻撃能力のレーティングを実施し、攻撃能力が基本であるかを確認する。そして、評価方法を決定するとともに、合否基準などの評定方法も決定する。この結果を適用して、再来年度からの製品の CC 評価・認証を実施する。

脆弱性情報は機微なものであるため、情報の管理が必要である。来年度事業の中で、公開と制限の範囲、脆弱性情報をどのような場で議論するか等を決定する。

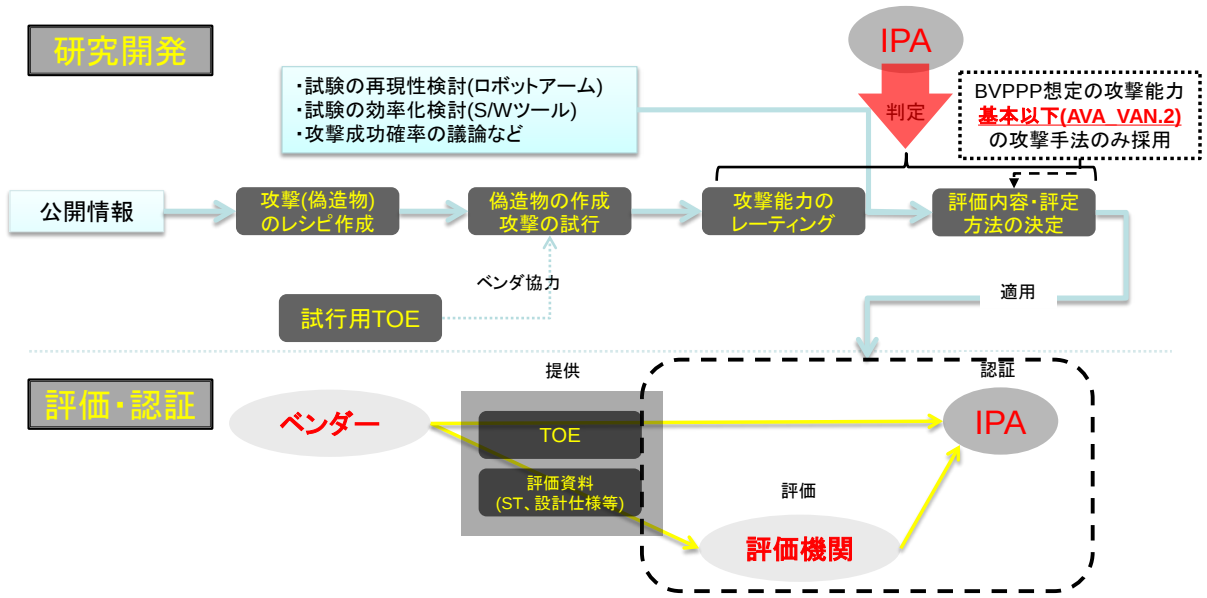


図 5.1-5　脆弱性評価の進め方

図 5.1-6 は、本事業成果の PP を前提にした静脈認証の攻撃ツリーを示している。既に図 5.1-2 で見たように、右の 2 つの枝は、客観的な CC 評価・認証の範囲を超えるものである。また、センサーに残留する静脈データの悪用は、静脈の場合は指紋と異なりセンサー面からのデータ採取はできず、本事業成果の PP ではメモリ上の残存データを脅威としていないため、評価の対象外になっている。よって、評価対象は左の赤枠で囲んだ部分だけになる。攻撃は、攻撃対象者の静脈を取得できたという前提（結託）で実施する。

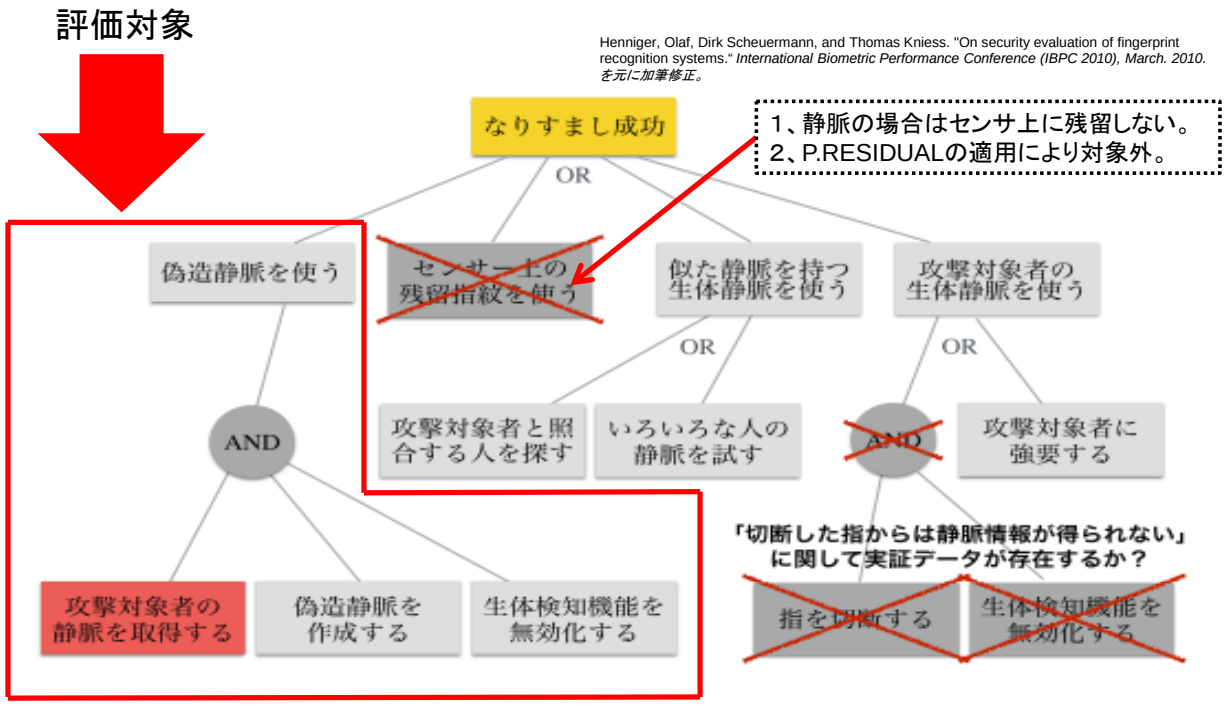


図 5.1-6　静脈認証の攻撃ツリー

静脈の偽造物を特徴付ける要素は、素材、次元、波長であると考えられる。素材については、紙、ゴム手袋、フィルム、液晶が考えられる。容易に入手できる素材から試行する。次元は、2 次元（写真など）と 3 次元（2 次元の貼合せ（四角柱、多角柱）、3D プリンタを使った造形物）がある。写真などの 2 次元を中心に作成して、段階的に 3 次元の偽造物も試行する。波長（偽造物作成に使用する光の波長）については、指を透過する波長を中心としつつ、製品ごとに使用する波長が異なる可能性があるので、他のさまざまな波長の使用も試行する。上記の要素を組み合わせて、種々の偽造物を作成する。それぞれの偽造物の作成に要する費用・時間を算出して、攻撃能力を計算する。

偽造物作成のためのデータ収集は、装置（光源＋カメラ）を自製して、その装置を使用して行なう。図 5.1-7 に示すように、全波長を出す光源を用意し、目的とする偽造物の部位（指やてのひら）に照射して、偽造物作成に使用する波長に応じたフィルタを使って、撮像用カメラでデータ収集する。または、フィルタを用いずに、必要とする波長の光源を使用して、データを収集する。いずれにしても、要求する波長に応じたデータを収集する。

図 5.1-7　データ収集方法

カメラの位置については、2 次元の偽造物を作成する場合は一点に固定して撮影するが、3 次元の偽造物を作成する場合は複数の点（角度）での撮影が必要になる。

収集したデータからの偽造物作成に当たっては、ひとつの素材の場合でもいろいろな質のものを試行する必要がある。また、ひとつの素材だけではなく複数の素材の組合せも検討する。3 次元の偽造物を作成する場合には、複数の 2 次元画像から 3 次元画像へ変換するソフトウェアの活用も検討する。TOE のセンサーの形状に合わせて偽造物の形状を変えることが必要な場合もある。順次、高価／高度な機器／素材を使用して作成することも検討する。

5.2 PP 開発及び PP 認証取得

5.1.2　方針検討にある方針に基づいて、ベンダー各社へのインタビューに基づく PP 素案作成と委員会での PP 素案への意見聴取をひとつのサイクルとし、このサイクルを 3 回繰り返して、PP を開発した。PP は 11 月末に完成し、12 月 19 日から評価開始、平成 27 年(2015 年)2 月 12 日に評価が完了し評価報告書が発行された。本活動報告書作成の時点では、IPA による認証作業中である。認証作業完了は 4 月 20 日に予定されている。

5.2.1 PP 開発

(1)ベンダー各社インタビューと委員会での意見聴取

5.1.2.にある方針を出発点として、ベンダー各社へのインタビューに基づく PP 素案作成と委員会での PP 素案への意見聴取をひとつのサイクルとし、このサイクルを 3 回繰り返した。

第 1 回のサイクルは、PP 作成の基本方針を決定することを目的とした。PP 作成の基本方針とは、以下の 4 つを決定することである。

1. 製品のどの機能（登録・ユーザ認証・ユーザ識別）を評価対象とすべきか。
2. エラー率（精度）・脆弱性・プライバシーのうち、どの評価を望むか。
3. どの程度の脅威を想定した評価にするか。HW 評価（物理的攻撃を想定）を含むか、SW 評価（物理的攻撃を除外）に限定するか。
4. 想定する TOE をどうすべきか。

上記 4 点について、ベンダー各社インタビューを、6 月 9 日、6 月 17 日、6 月 18 日（2 社)、6 月 23 日、6 月 26 日、6 月 27 日に、それぞれ実施した。この結果に基づき PP 作成基本方針案を作成し、7 月 24 日に第 1 回委員会で PP 作成基本方針案に対する意見を聴取した。

第 2 回のサイクルは、PP の構成の前半部分に当たるセキュリティ課題定義及びセキュリティ対策方針を決定することを目的とした。予め産総研と JQA で素案を作成し、8 月 26 日、8 月 27 日（2 社)、8 月 28 日（2 社)、8 月 29 日、9 月 5 日にそれぞれベンダー各社インタビューを実施して、9 月 29 日の第 2 回委員会でインタビュー結果を反映した素案に対する意見を聴取して、セキュリティ課題定義及びセキュリティ対策方針を決定した。

第 3 回のサイクルは、PP の構成の後半部分に当たる拡張コンポーネント定義及びセキュリティ要件を決定することを目的とした。予め産総研と JQA で素案を作成し、11 月 25 日、12 月 2 日、12 月 4 日にベンダー3 社にインタビューを実施して、12 月 5 日の第 3 回委員会で素案に対する意見を聴取して、拡張コンポーネント定義及びセキュリティ要件を決定した。

以下では、PP の構成に合わせて、PP 開発について報告する。5.1.2　方針検討で述べたように、PP は最終的には英語で作成したが、以下の報告では PP の構成も含めて日本語表記とする。ただし、英語版との対応がわかりづらい部分については、対応する英語を付記する。

(2)PP 概説（PP introduction）

CEM[35][42]では、PP 概説には PP 参照と TOE 概要を求めている。PP 参照は形式的な内容なので、ここでは報告しない。CEM では PP 概要（PP overview）を要求していないが、本 PP では 1.2 として PP 概要を設けて、本 PP の内容を簡潔に規定した。PP 概要は、ベンダー各社インタビューと委員会での意見聴取の第1回のサイクルで決定したPP基本方針にほぼ対応している。

ベンダーへのインタビュー内容は、以下のとおりだった。

1.製品のどの機能（登録・ユーザ認証・ユーザ識別）を評価対象とすべきか。

2.エラー率（精度）・脆弱性・プライバシーのうち、どの評価を望むか。

3.どの程度の脅威を想定した評価にするか。HW 評価（物理的攻撃を想定）を含むか、SW 評価（物理的攻撃を除外）に限定するか。

4.想定する TOE をどうすべきか。

1 から 3 に対するインタビュー結果は、以下のとおりである。4 については、PP 概要の後の TOE 概要の内容なので、後述する。

表 5.2-1　インタビュー結果概要

	どの機能を対象とするか	3つのいずれを評価するか	HW評価/SW評価
A社	ユーザ識別の重要性高いがユーザ認証からで良い。	3つの独立したPPが望ましいが、簡易なものからで良い。	先ずはSW評価。HW評価はバイオと独立した部分であるかも知れない。
B社	ユーザ認証	3点セット	先ずはSW評価を 実施する。
C社	ユーザ認証	エラー率（精度）、プライバシー、脆弱性の重要性の順だが、PPは 3点セットで良い。	先ずはSW評価で、HW評価は状況を見ながら検討する。
D社	ユーザ認証	エラー率（精度）と脆弱性のセットのPPが良い。	SW評価
E社	ユーザ認証とユーザ識別の重要性は同等であるが、ユーザ認証のPPで良い。	エラー率（精度）とプライバシーの次に脆弱性評価が重要であるが、PPは3点セットで良い。	先ずはSW評価
F社	ユーザ認証	エラー率（精度）	SW評価
G社	ユーザ認証	3点セット	SW評価

製品のどの機能（登録・ユーザ認証・ユーザ識別）を評価対象とすべきかについては、ユーザ認証からで良いとの了解が各社から得られたので、ユーザ認証だけを評価対象とする PP とした。ただし、表 5.2-1 にはないが、登録・ユーザ識別についても必要との意見があったため、ユーザ認証の PP が完成した後に作成に着手することにした。

エラー率（精度）・脆弱性・プライバシーのどの評価を望むかについては、独立に評価できることが望ましいが 3 点セットでも良いとの意見が多かったことから、独立に評価できることを目指しつつ、時間の制約などから難しいと判断した場合には 3 点セットとすることにした。

HW 評価（物理的攻撃を想定）か SW 評価（物理的攻撃を除外）かについては、SW 評価とす

ることにして進めようとしたが、後の委員会で SW 評価及び HW 評価の定義をめぐって議論があり、なかなか結論が出なかった。

このため、改めて ISO/IEC 19792 が主張するように、従来の CC では評価できないバイオメトリクスのセキュリティ評価とは何かを再考した。その結果、5.1.1　海外動向調査　(1) で述べたように、プライバシーについてはバイオメトリクス固有のセキュリティ要件はないと判断して、対象から外した。また、脆弱性評価についても、5.1.1　海外動向調査　(1) で述べたように、バイオメトリクス製品に固有の内容は、PAD 検知の評価であると結論した。その結果、PP 概要は、以下の内容とした。

本 PP は、CC の観点から、ユーザ認証用のバイオメトリクス製品に固有のセキュリティ機能要件及び保証要件を定める。バイオメトリクス製品に固有のセキュリティ機能要件とは、パスワードや PKI などによるユーザ認証製品にはない、他人受入れ及び本人拒否のエラーに対する要件、偽造物検出に対する要件である。従って、本 PP においては、セキュリティ課題としてエラー率及び偽造物検知だけに対抗し、その他の脅威は取り扱わない。また、TOE 及び運用環境の機器の自然故障は考慮しない。

本 PP は、TOE が使用する生体的特徴（顔、指紋、虹彩、静脈など）及び部位（手の場合は、指、てのひら、手の甲など）を特定しない。

本 PP は、バイオメトリクス製品のユーザ認証だけを対象とし、ユーザ登録やユーザ識別を対象としない。

次に、1.3 の TOE 概要について報告する。1.3.1.から 1.3.4.までは、それぞれ、TOE の種別、TOE が利用できる TOE 以外のハードウェア/ソフトウェア/ファームウェア、TOE の使用法、TOE の主要なセキュリティ機能を記述している。CEM ではこれらの記述が要求されているため必要な記述だが、これらはバイオメトリクスの製品に関する一般的な内容であるため、ベンダー各社インタビューと委員会での意見聴取を実施しなかった。内容については、英語版の PP のとおりである。

1.3.5.TOE の構成と運用環境 においては、統合型バイオメトリック製品（TOE の構成要素が物理的に分離していない。すなわち、TOE の構成要素が USB ケーブルやネットワークで接続されていることはない）と分離型バイオメトリック製品（TOE の構成要素が物理的に分離している。すなわち、TOE の構成要素が USB ケーブルやネットワークで接続されている）のいずれにも適用できることを述べた。

1.3.6. TOE の機能 が、第 1 回のベンダー各社インタビューと委員会での意見聴取で決定した内容である。ベンダー各社インタビューでは、以下の図 5.2-1（[23]に基づき、PAD Feature Extraction を追加して作成）を提示して TOE の範囲を回答してもらった。

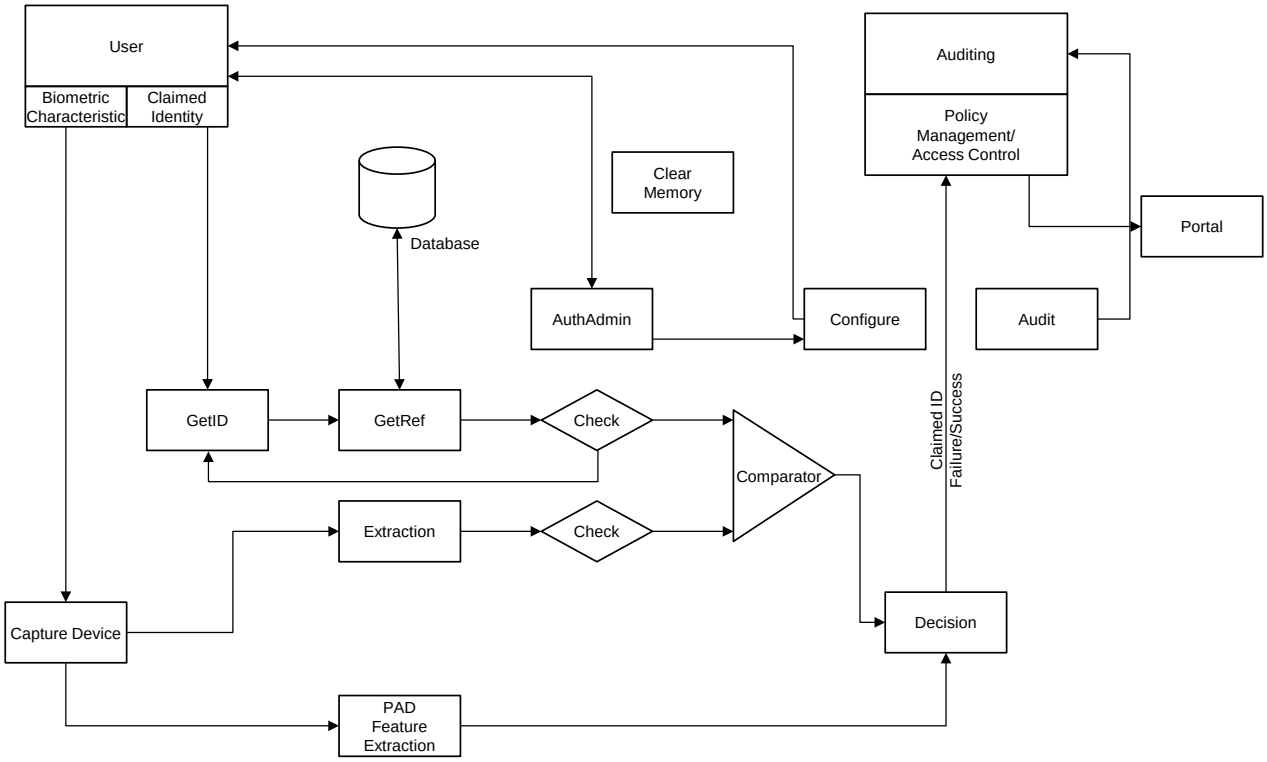


図 5.2-1　TOE 検討のための図

なお、各機能の説明は、以下のとおりである。

・Get ID: This component is responsible for getting the user's claimed identity. Its functionality is security relevant because the system uses the claimed ID to determine, which biometric reference has to be used for comparison. Furthermore, this component provides a mandatory user visible interface.

・GetRef:　This component is responsible for getting the stored (already enrolled) biometric reference related to a claimed user's identity.

・　Extraction: In preparation of the verification process a feature vector has to be extracted from the captured data. This is the objective of this component. Optionally, the biometric data may be compressed.

・Check: This component ensures the minimum quality requirements regarding the biometric references. It can be differentiated into integrity and authenticity check during the process of getting the biometric reference as well as the quality check of the biometric information during the processing of the live biometric characteristics.

・AuthAdmin: This component is responsible for identification and authentication of the dministrator　with other means than the biometric verification mechanism itself. This mechanism is a classical identification and authentication component that could for example be realized via a artCard/PIN　based mechanism. It is necessary to authenticate an administrator before he is allowed to figure security relevant settings of the TOE.

- Configure: This component provides an interface for the administrator to set security relevant TOE parameters. This component is especially used to configure the threshold setting for the comparator component and to determine audit events.
- Comparator (also called Matcher): This is an important component regarding the scope of this Protection Profile. It compares the enrolled biometric reference with the Biometric Live Record (BLR) and includes the determination whether these records match or not. A comparator oduces a value that shows how well the biometric reference and BLR match. To get a successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the biometric reference and the BLR are more similar than demanded by the threshold, the return value is success, otherwise it is fail. An "Exact match" comparison should not result in a positive verification as it may be a replay attempt and should be recorded in the audit log.
- Clear memory: In order to protect against attacks, this component clears the content of memory after use. The information that has to be cleared is not limited to the verification result but especially includes the biometric reference, BLR or any biometric raw data as well as authentication data for the administrator authentication. Because the memory that has to be cleared could belong to every other component no lines are drawn into the figure for this component.
- Audit: This component of the TOE records security relevant events to ensure that information exists to support effective security management (e.g. verification protocol, retry counter, etc.).

Some security related components, functions and interfaces of the TOE environment should be considered here:

- Capture Device: This component that is also called sensor is responsible for capturing the biometric characteristic from the user and forwards it into the biometric system. Depending on the used sensor technology also additional processes as a liveness detection or an image enhancement could be performed by this device.
- Policy manager: The result of the biometric verification process is passed on to the policy manager of the environment. This component is responsible for checking the user's rights and opening the portal if the user has sufficient privileges and was successfully verified by the TOE and is therewith realizing an access control mechanism for the portal.
- Storage: The environment has to provide a database to be used by the TOE. This is used to store the biometric reference of a user but it can be used to store additional information too.
- Portal: The physical or logical point beyond which information or assets are protected by a biometric system is controlled by the TOE environment policy management, which gets the verification results (verification "failed" or "successful") related to the user identity from the TOE.
- Auditing: The environment may provide additional audit functionalities and has to provide

a mechanism for audit review of the TOE audit logs.

・Transmission / Storage: The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE.

・PAD Feature Extraction: PAD (Presentation Attack Detection) features are extracted from the raw data captured at the capture device and is sent to Decision where Failure or Success is decided with the result sent from Comparator and PAD Feature.

TOE の範囲については、各社からの要望は、図 5.2-2 からのとおりであった。

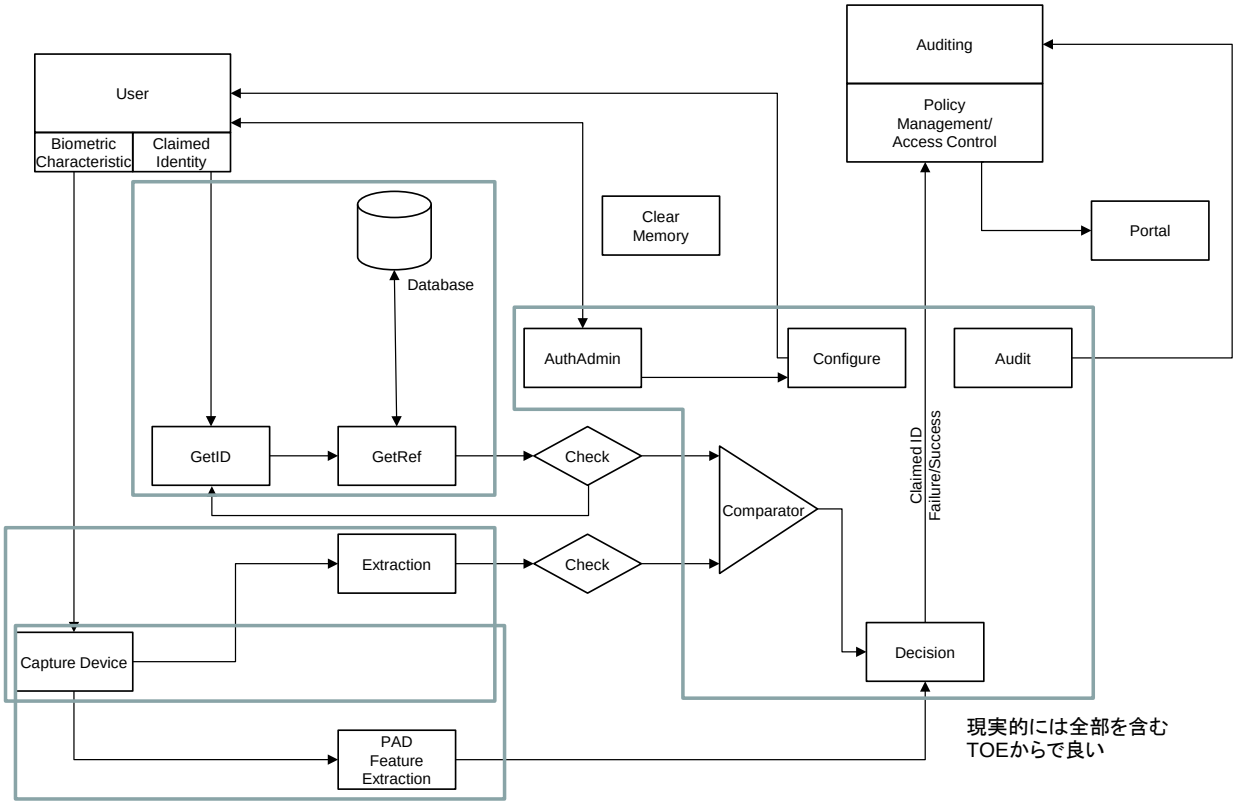


図 5.2-2 A 社 TOE 案

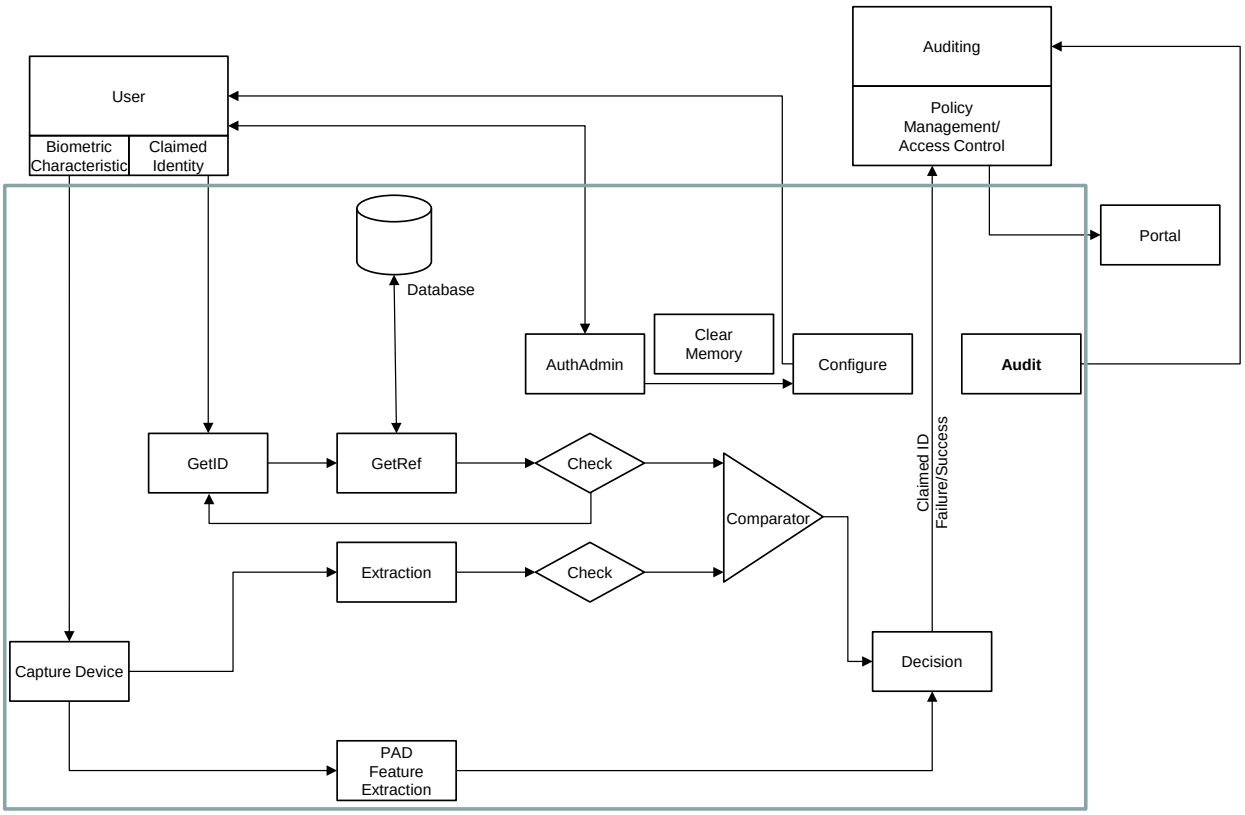


図 5.2-3　B 社 TOE 案

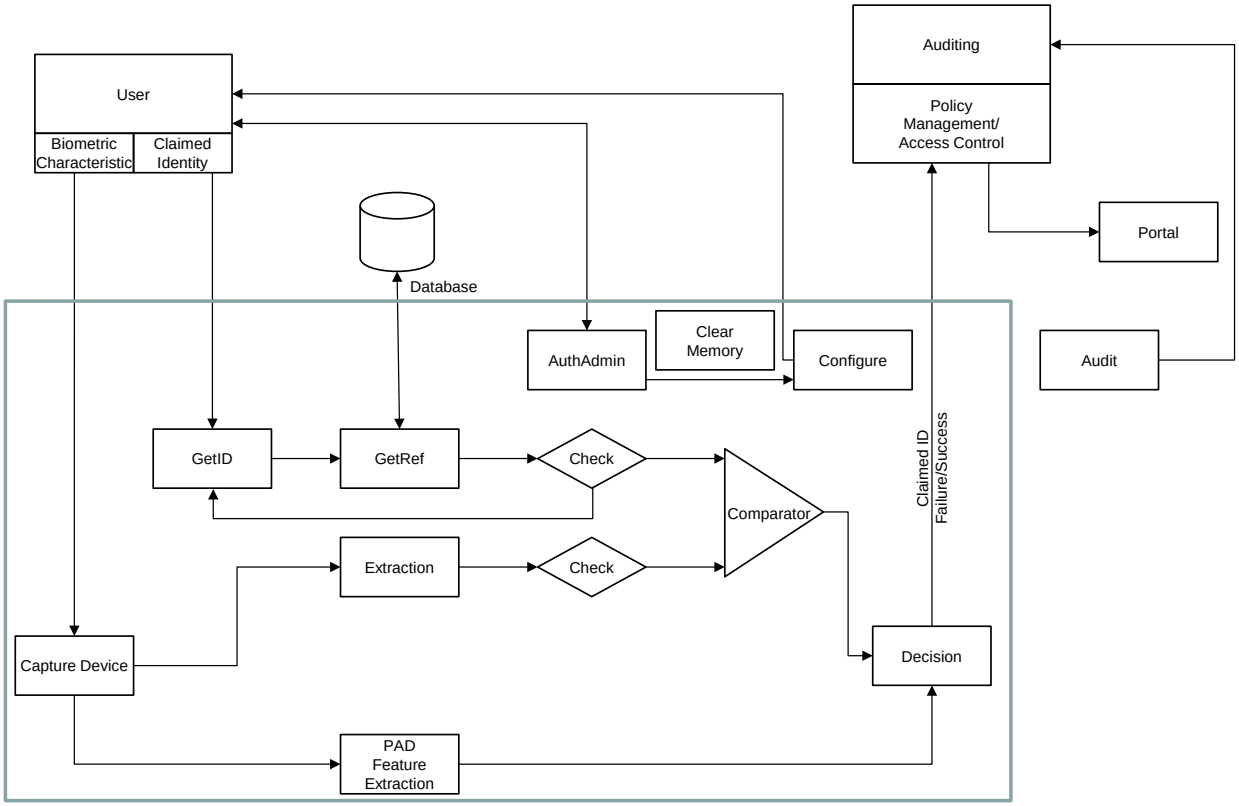


図 5.2-4　C 社 TOE 案

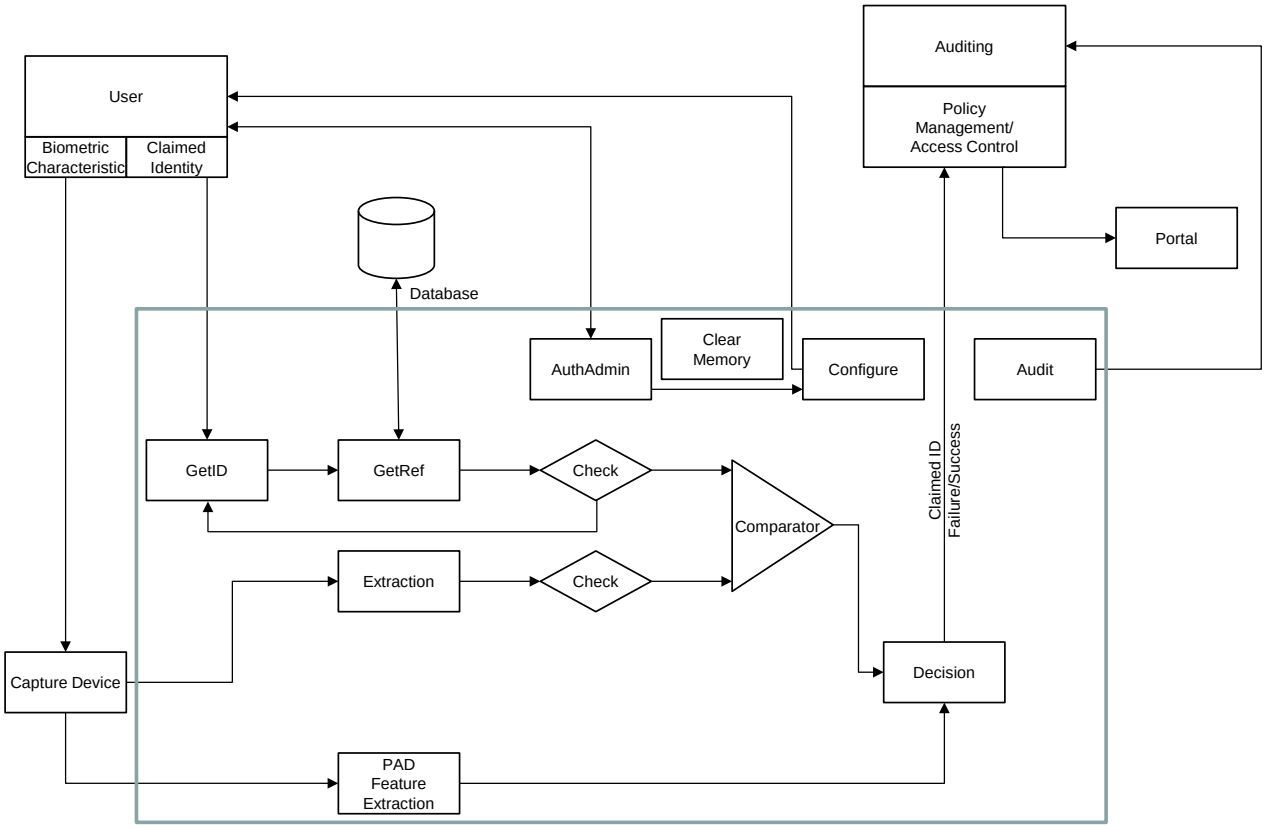


図 5.2-5　D 社 TOE 案

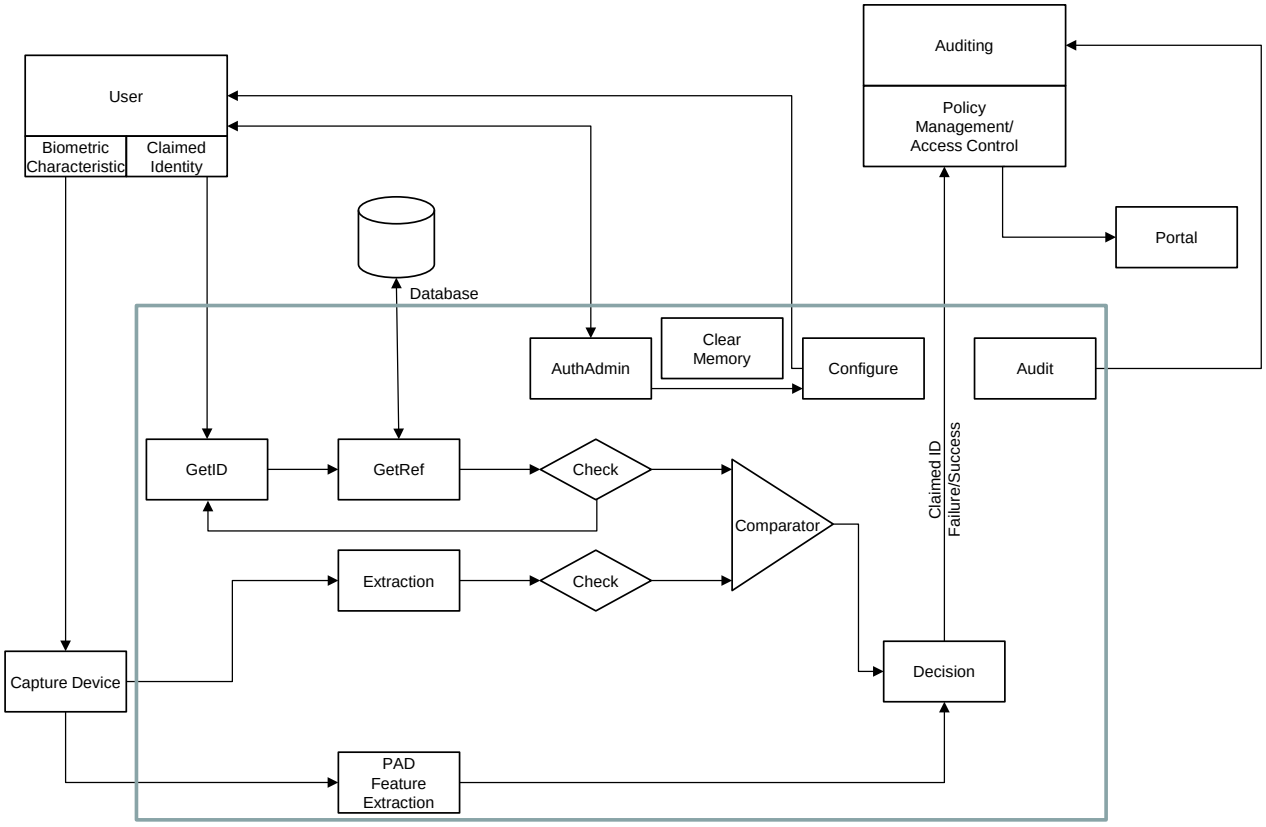


図 5.2-6　E 社 TOE 案

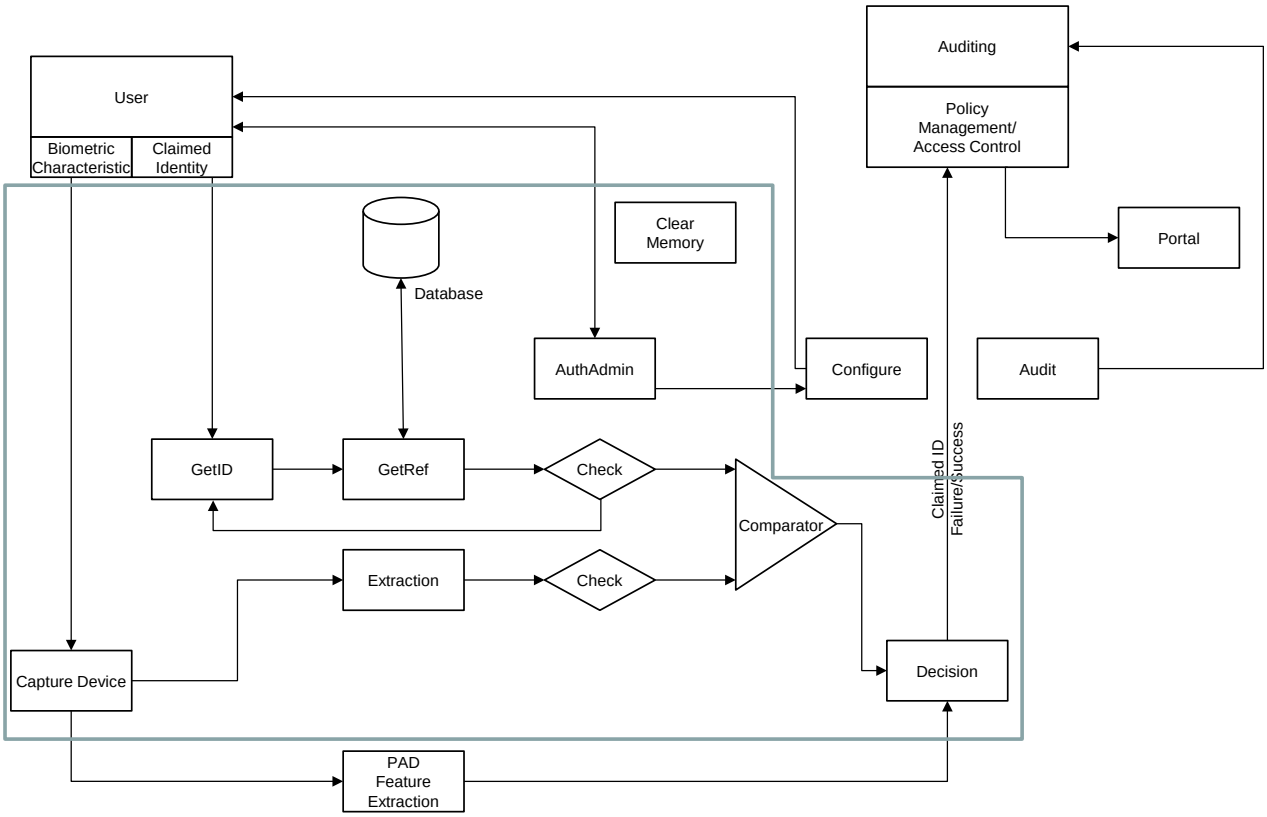


図 5.2-7　F 社 TOE 案

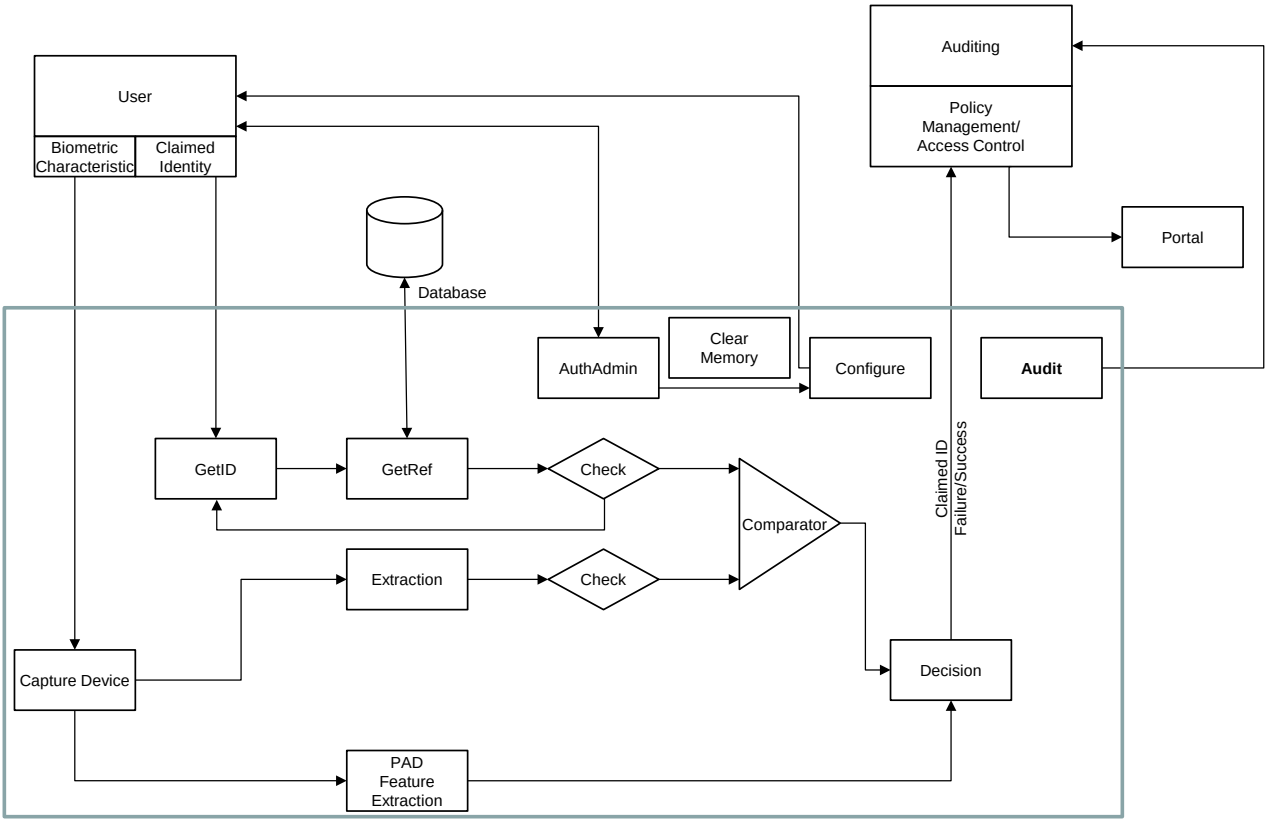


図 5.2-8　G 社 TOE 案

TOE に対する各社の意見をまとめると、以下のとおりである。

A 社の意見は、データ採取だけからなる製品、テンプレートだけを含む製品など、バイオメトリクスのシステムは、種々の製品から構成されることもあるので、できるだけ一般的な構成を許容するようにすることが汎用的に使える PP になるという考えに基づく意見である。

B 社の意見は、バイオメトリクスの処理を全て含む TOE 案である。

C 社の意見は、データベースは他社製品を使う場合もあるので、TOE から除外するという意見である。

D 社の意見は、データベースだけでなくデータ採取も他社製品を使う場合があることを想定した TOE 案である。

E 社の意見は、D 社と同様である。

F 社の意見は、PAD 検知を評価対象とせず、精度評価だけを評価対象としたいとの理由で、PAD Feature Extaction 機能を TOE から外す、Audit 機能も TOE に含めないという案である。

G 社の意見は、C 社と同様である。

各社の製品を評価可能にするためには、作成する PP の TOE は各社の共通部分にせざるを得ない。ある製品が含まない機能を PP の TOE が含めば、その製品に PP は適用できないからである。その結果、また更に機能を簡素化して、図 5.2-9 に示す機能を PP の TOE の範囲とした。図 5.2-8 までとの大きな差異は、Audit とそれに関連する機能を外したこと、Capture Device を Capture にしたことである。Audit については、製品によって機能有無に差があるので、TOE の図から外した。PP は構成する機能を記述する文書であることから、Capture Device をより機能に焦点を当てた Capture に変更した。また、Capture Device は PAD の機能を一部担う場合も多いが、そのような機能は PAD Feature Extraction の一部であるとして、Capture は生データ採取の機能に限定すると再定義した。

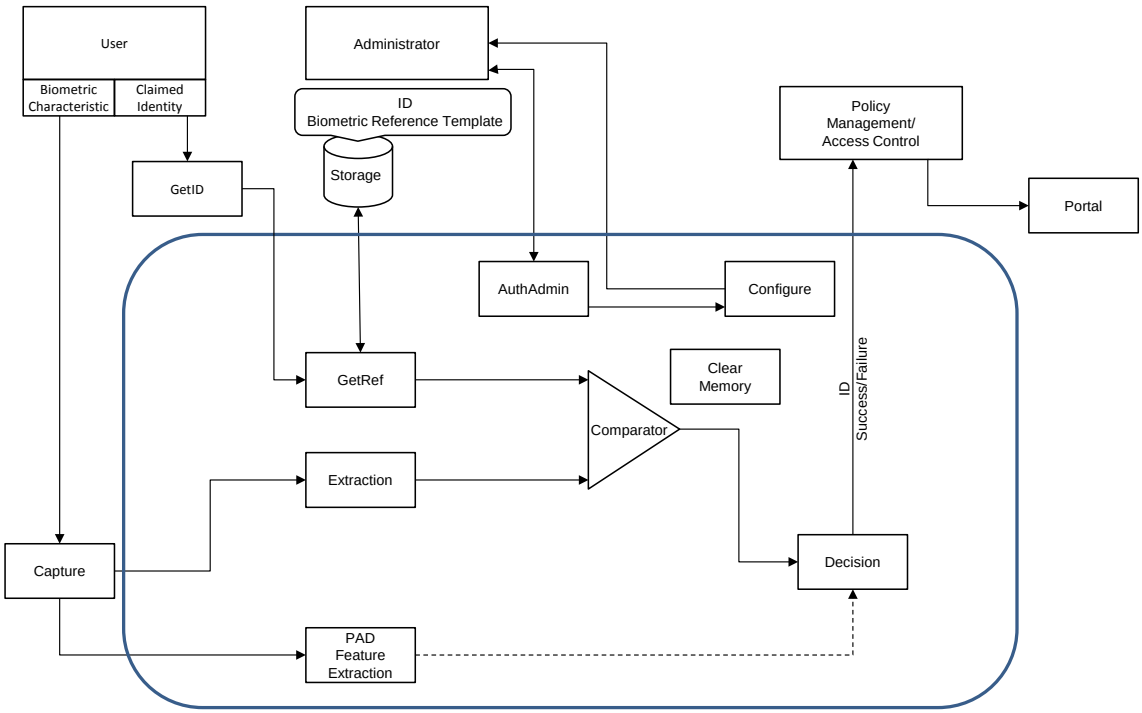


図 5.2-9　PP の TOE

(3)適合主張

2.適合主張では、本 PP が適合する CC が CC Version 3.1 Release 4 であること、CC Part 2 に後述の拡張コンポーネント FIA_BUA を使用して拡張適合していること、CC Part 3 に適合していること、保証要件パッケージ EAL2 に保証コンポーネント ALC_FLR.1 を追加していること、本 PP は他の PP/ST が本 PP に論証適合することを許容することを、述べている。論証適合を許容しているので、本 PP に要件を追加した ST を作成しても、本 PP への適合を主張することが可能である。

(4)セキュリティ課題定義

3.セキュリティ課題定義では、TOE に関連するエンティティ及び資産を定義し、TOE が機能するための、TOE の運用環境に対する前提条件を決めた上で、脅威、組織のセキュリティ方針を定めた。

3.1.TOE に関連するエンティティは、バイオメトリック・システム管理者（BS 管理者）、登録ユーザ、攻撃者の 3 者を定めた。

バイオメトリック・システム管理者（BS 管理者）：

TOE を含むバイオメトリックシステム（BS）の管理的操作の実行権限があり、TOE を含む BS の管理的機能を使用することができる。

TOE のインストール（HW がある場合はその設置を含む）、設定、及び保守の責任を持つ。

登録ユーザ：

TOE を含む BS に生体情報を登録し、TOE にユーザ認証されることによって、ポータルへア

クセスする。

攻撃者：

権限なくポータルへアクセスすることを目的に、TOE に不正にユーザ認証されることを試みる。

BS 管理者については、当初、BS ではなく TOE だけを対象として TOE 管理者として定義した。しかし、委員会での意見聴取で、管理者は登録なども管理すると考えられるため、BS を対象とする BS 管理者とすることになった。

3.2.資産については、素案のまま変更なく、以下のようになった。

1 次資産：

TOE 外のポータルに存在する資産であって、登録ユーザが TOE でユーザ認証されることによってアクセスできる資産。この資産は、物理的資産の場合も、論理的資産の場合もある。

2 次資産：

TOE が生成するデータ及び管理者が作成する TOE 内のデータ。

TOE 内で処理され使用される生体情報、閾値などのバイオメトリック処理のためのパラメータ、管理者権限を得るための情報など。

3.3.前提条件については、以下のように最終案をまとめた。

A.ADMINISTRATION

BS 管理者は、悪意を持たない。すなわち、攻撃者になったり、攻撃者に情報提供したりすることはない。BS 管理者は、TOE のガイダンス文書を注意深く読んで、正しく理解し、ガイダンス文書の内容を TOE に適用する。BS 管理者は、TOE のインストール（HW がある場合はその設置を含む)、設定、運用の責任を持つ。

A.ENROLMENT

登録ユーザの登録生体情報は、運用環境の Storage に格納され、TOE のユーザ認証機能を使用できる状態になっている。

A.CAPTURE

Capture 機能を実現する Capture Device は、ガイダンス文書が指定する製品が選択され、ガイダンス文書が定める運用環境で使われるものとする。

注：自然故障は考慮しない。

A.STORAGE

登録ユーザの登録生体情報を登録する Storage 機能を持つ。Storage 機能においては authenticity と integrity は保たれている。登録ユーザの登録生体情報へのアクセスは、TOE に許可されている他は、BS 管理者による管理的操作だけが許可される。

注：自然故障は考慮しない。

A.COMMUNICATION

TOE と Capture 機能との間及び TOE と Storage 機能との間の通信、TOE の構成要素が物

理的に分離している場合は TOE の構成要素間の通信は、例えば暗号化されて、保護されている。

注：自然故障は考慮しない。

A.ENVIRONMENT

ガイダンス文書が指定する、TOE が動作可能になるためのセキュアな運用環境が提供されている。少なくとも、ウィルスなどマルウェアから保護されている。

注 : TOE がモバイルデバイス上で動作する場合には、盗難時や紛失時に機能を停止できる運用環境が提供されている。そうでない場合には、TOE は持ち帰って解析したり、設置場所で解析できないような運用環境で使用される。いずれの場合も、攻撃者が TOE を解析できないような運用環境で TOE は使用される。自然故障は考慮しない。

上記最終案における素案からの変更は、A.COMMUNICATION と A.ENVIRONMENT への変更である。前者については、保護されている通信を具体的な記述に改めた。後者については、素案にあった A.PHYSICAL と統合したことである。

A.PHYSICAL

TOE を含む製品は物理的に保護された運用環境で使用される。

A.PHYSICAL にあった「物理的に保護」の意味が不明確であったのを、A.ENVIRONMENT の注として明確にしたこと、その結果として、攻撃者による攻撃内容を限定した。

なお、英語版 PP では、A.CAPTURE 及び A.ENVIRONMENT におけるガイダンス文書の参照が削除されている。これは、5.2.2　PP 認証取得に記載されているように、A.CAPTURE 及び A.ENVIRONMENT におけるガイダンス文書の参照が ST における循環参照の原因になるという指摘が認証キックオフミーティングであったためである。

3.4.脅威については、最終案は以下のとおりである。以下の内容については、素案との差異はほとんどない。

T.UNAUTHORIZED_USE

攻撃者がポータルの 1 次資産にアクセスしようとするかも知れない。

T.CASUAL_ATTACK

攻撃者が、自分自身の生体を使って登録ユーザになりすまし、1 次資産にアクセスしようとするかも知れない。

T.PRESENTATION_ATTACK

攻撃者が、偽造生体を使って登録ユーザになりすまし、1 次資産にアクセスしようとするかも知れない。

T.MODIFY__ASSETS

攻撃者が、管理的機能を使って、TOE 内の 2 次資産を改変、破壊、または収集して、TOE

を正常動作させないようにするかも知れない。

英語版 PP では、T.UNAUTHORIZED_USE は削除されている。これも、5.2.2　PP 認証取得に記載されているように、認証キックオフミーティングにおける脅威の記述がわかり辛いとの指摘の反映である。

3.5.組織のセキュリティ方針 については、最終案は以下のとおりである。

P.PORTAL_ACCESSIBLE
TOE 及び運用環境は、ガイダンス文書が指定したとおりに生体の提示をした場合の登録ユーザによるユーザ認証の失敗を、一定の割合以下にしなければならない。
P.RESIDUAL
ユーザ認証処理の後に残存するバイオメトリック・データ及び登録ユーザのその他の情報はパーソナルデータ保護の対象なので、これらの残存データを TOE 及び運用環境は削除しなければならない。

P.RESIDUAL は、素案では T.RESIDUAL と脅威として扱っていた。しかし、セキュリティ要件を検討する段階で、残存データへのアクセスインタフェースが TOE にはないため、高い攻撃能力がないと脅威にはならないと結論して、P.RESIDUAL に変更した。

(5)セキュリティ対策方針

4.セキュリティ対策方針では、TOE のセキュリティ対策方針と運用環境のセキュリティ対策方針を定めた。

4.1.TOE のセキュリティ対策方針の最終案は、以下のとおりである。素案では、OE.LIMIT_NUM_TRIAL を O.LIMIT_NUM_TRIAL として、TOE のセキュリティ対策方針に位置付けていた。しかし、OE.LIMIT_NUM_TRIAL の注にあるように、国際標準 ISO/IEC 19784-1（BioAPI）に基づく API 仕様を持つバイオメトリクス製品ではユーザ認証の試行回数を把握できないため、運用環境のセキュリティ対策方針へ移動した。これは、第 2 回のベンダー各社へのインタビューにおいての指摘事項の反映である。

O.BIOMETRIC_VERIFICATION
TOE は、バイオメトリクス技術で、ポータルへのアクセスのユーザ認証機能を提供しなければならない。
O.CONTROL_FALSE_ACCEPT
TOE は、運用に支障のない他人受入率(FAR)を持たなければならない。
O.PAD
TOE は、Capture 機能を実現する Capture Device に偽造生体が提示された場合、それが偽造生体であることを一定の割合で検知しなければならない。

O.AUTH_ADMIN

TOE は、BS 管理者をユーザ認証する手段を提供しなければならない。

O.PROTECT_TSFDATA

TOE は、BS 管理者だけが閾値などの TOE 内の処理に関わるセキュリティ関連データにアクセスできるようにしなければならない。

O.CONTROL_FALSE_REJECT

TOE は、運用に支障のない本人拒否率(FRR)を持たなければならない。

O.CLEAR_RESIDUAL

TOE は、TOE 内の処理に使用したバイオメトリック・データ（登録生体情報を含む)、及び登録ユーザのその他の情報を、ユーザ認証終了後に、削除しなければならない。

英語版 PP では、O.BIOMETRIC_VERIFICATION は削除されている。これは、前述の T.UNAUTHORIZED_USE の削除に対応するもので、O.BIOMETRIC_VERIFICATION が T.UNAUTHORIZED_USE のセキュリティ対策方針として設定されていたためである。

4.2.運用環境のセキュリティ対策方針の最終案は、以下のとおりである。

OE.LIMIT_NUM_TRIAL

運用環境は、バイオメトリクスを使ったユーザ認証の試行回数が一定回数以上に達した場合、攻撃と判断して、当該ユーザのアカウントをロックしなければならない。

注：国際標準 ISO/IEC 19784-1（BioAPI）に基づく API 仕様を持つバイオメトリクス製品の場合、バイオメトリクス製品はユーザ認証の試行回数を把握できない。よって、試行回数の把握は、TOE の運用環境であるアプリケーションでしかできない。

OE.ADMINISTRATION

BS 管理者は、悪意を持たない者（攻撃者になったり、攻撃者に情報提供することのない者）でなければならない。BS 管理者は、TOE のガイダンス文書を注意深く読み、正しく理解し、ガイダンス文書の内容を TOE に適用しなければならない。BS 管理者は、TOE のインストール（HW がある場合はその設置を含む)、設定、運用の責任を持ち、実行しなければならない。

OE.ENROLMENT

登録ユーザの登録生体情報は、運用環境の Storage に格納され、TOE のユーザ認証機能を使用できる状態になっていなければならない。

OE.CAPTURE

Capture 機能を実現する Capture Device は、ガイダンス文書が指定する製品が選択され、ガイダンス文書が定める運用環境で使われなければならない。

OE.CLEAR_RESIDUAL_CAPTURE

Capture 機能を実現する Capture Device は、採取した生体情報を TOE に送信した後に、採取した生体情報を削除しなければならない。

OE.STORAGE

登録ユーザの登録生体情報を登録した Storage を持たなければならない。Storage においては authenticity と integrity は保たれていなければならない。登録ユーザの登録生体情報へのアクセスは、TOE に許可されている他は、BS 管理者による管理的操作だけが許可されていなければならない。

OE.COMMUNICATION

TOE と Capture 機能との間及び TOE と Storage 機能との間の通信、TOE の構成要素が物理的に分離している場合は TOE の構成要素間の通信は、保護されていなければならない。

OE.ENVIRONMENT

ガイダンス文書が指定する、TOE が動作可能になるためのセキュアな運用環境が提供されていなければならない。例えば、ウィルスなどマルウェアから保護されていなければならない。

なお、英語版 PP では、OE.CAPTURE 及び OE.ENVIRONMENT におけるガイダンス文書の参照が削除されている。これは、上述の A.CAPTURE 及び A.ENVIRONMENT におけるガイダンス文書の参照の削除と同様に、認証キックオフミーティングにおける指摘の反映結果である。更に、英語版 PP では、以下の運用環境のセキュリティ対策方針が追加された。

OE.ACCESS_CONTROL

The operational environment shall permit a user to access to the portal if and only if the user is biometrically verified by the TOE.

これは、後出の所見報告書(136601-01-R008-01)発行以前のみずほ情報総研からの指摘に対応したものである。指摘事項の内容は、以下のとおりである。

T.UNAUTHORIZED_USE と O.BIOMETRIC_VERIFICATION は、以下のようになっている。

T.UNAUTHORIZED_USE

攻撃者がポータルの 1 次資産にアクセスしようとするかも知れない。

O.BIOMETRIC_VERIFICATION

TOE は、バイオメトリクス技術で、ポータルへのアクセスのユーザ認証機能を提供しなければならない。

ポータルの 1 次資産にアクセスを制御するのは TOE 外の Policy Management/Access Control の部分であり、T.UNAUTHORIZED_USE は TOE が対抗する脅威ではない。よって、ポータルへのアクセス制御は、TOE のセキュリティ対策方針では対策できず、運用環境のセキュリティ対策方針での対策が必要である。

4.3.セキュリティ対策方針根拠 では、4.2.セキュリティ対策方針に挙げたセキュリティ対策方針によって、4.1.セキュリティ課題定義に挙げた全てのセキュリティ課題が対策されていることを論述する。英語版 PP にあるので、詳細はここでは述べない。全体をまとめるセキュリティ対策方針根拠の表を挙げるにとどめる。ただし、以下の表は、日本語最終版のものではなく、英語版のものである。

表 5.2-2　セキュリティ対策方針根拠

	O.CONTROL_FALSE_ACCEPT	O.PAD	O.AUTH_ADMIN	O.PROTECT_TSFDATA	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.ADMINISTRATION	OE.ENROLMENT	OE.CAPTURE	OE.CLEAR_RESIDUAL_CAPTURE	OE.STORAGE	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK	×						×	×							
T.PRESENTATION_ATTACK		×					×	×							
T.MODIFY__ASSETS			×	×											
P.PORTAL_ACCESSIBLE					×										
P.RESIDUAL						×						×			
A.ADMINISTRATION									×						
A.ENROLMENT										×					
A.CAPTURE											×				
A.STORAGE													×		
A.COMMUNICATION														×	
A.ENVIRONMENT															×

(6)拡張コンポーネント定義

5.拡張コンポーネント定義では、この PP の対象となる TOE のバイオメトリクスによる利用者認証機能を記述するためにファミリ FIA_BUA （Biometric User Authentication）を定義した。CC パート 2 のクラス FIA（識別と認証）で定義された利用者認証（FIA_UAU（User Authentication））とバイオメトリクスによる利用者認証（ユーザ認証）には差異があるため、クラス FIA を拡張した。上記の差異とは、FIA_UAU が定義する利用者認証では認証データが正しければ認証は必ず成功しなければならないのに対して、バイオメトリクスによる利用者認証では利用者の生体情報が提示された場合でも、FAR の存在が示すように、失敗する可能性がある。また、FIA_UAU では認証データの偽造とコピーが別に扱われているが、バイオメトリクスによる利用者認証では両者は明確に区別できない。クラス FIA にバイオメトリクスによる利用者認証を適切に表現するファミリがなかったので、新しいファミリ FIA_BUA を定義した。

5.1.バイオメトリクスによる利用者認証 FIA_BUA の内容は、以下のとおりである。以下では、管理、監査、依存性に関する記述は省略する。それらについては、英語版 PP を参照されたい。なお、以下において、TSF とは TOE Security Function（TOE のセキュリティ機能）である。

ファミリのふるまい

このファミリは、TSF がサポートするバイオメトリクスによる利用者認証メカニズムを定義する。このファミリは、バイオメトリクスによる利用者認証メカニズムが基づかねばならない、要求された属性も定義する。

コンポーネントのラベル付け

FIA_BUA.1 バイオメトリクスによる認証のタイミングは、利用者の識別情報のバイオメトリクスによる認証の前に、利用者があるアクションを実行することを認める。

FIA_BUA.2 アクション前のバイオメトリクスによる利用者認証は、TSF がその他のアクションを許可する前に、バイオメトリクスによる利用者の認証を要求する。

FIA_BUA.3 偽造されないバイオメトリクスによる認証は、生体を模した偽造物の使用を、バイオメトリクスによる認証メカニズムが検出または防止できることを要求する。

FIA_BUA.1 バイオメトリクスによる認証のタイミング

FIA_BUA.1.1 TSF は、利用者がバイオメトリクスにより認証される前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。

FIA_BUA.1.2 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者にバイオメトリクスによる利用者認証メカニズムが、エラー率 FAR[割付 : *X*]以下、FRR[割付 : *Y*]以下で、動作することを要求しなければならない。

FIA_BUA.2 アクション前のバイオメトリクスによる利用者認証

FIA_BUA.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者にバイオメトリクスによる利用者認証メカニズムが、エラー率 FAR[割付 : *X*]以下、FRR[割付 : *Y*]以下で、動作することを要求しなければならない。

FIA_BUA.3 偽造されないバイオメトリクスによる認証

FIA_BUA.3.1 TSF は、TSF の利用者による生体を模して偽造された認証データの使用を[選択: *検出*、*防止*]しなければならない。

5.拡張コンポーネント定義の内容は、第 3 回のベンダー各社インタビュー及び委員会での意見聴取で、ほぼ素案のとおり合意された。この中で、FIA_BUA.1 は、本 PP のセキュリティ機能要件としては使われないが、バイオメトリクス製品を含むシステムの ST 作成で使われる可能性を考えて、本 PP で拡張コンポーネントとして定義した。

(7)セキュリティ要件

6.セキュリティ要件は、6.1. セキュリティ機能要件、6.2. セキュリティ保証要件、6.3. セキュリティ要件根拠 から成る。

セキュリティ機能要件は、TOE セキュリティ対策方針を実現するセキュリティ機能要件を、基本的には CC パート 2 のカタログから抽出して作成する。6.1. セキュリティ機能要件は結果としてのセキュリティ機能要件の羅列であり、セキュリティ対策方針とセキュリティ機能要件との論理的なつながりは、6.3.1. セキュリティ機能要件根拠の 6.3.1.2. セキュリティ対策方針とセキュリティ機能要件の対応関係根拠 に記述されている。

セキュリティ対策方針 O.CONTROL_FALSE_ACCEPT は、認証に適切な他人受入率(FAR)を規定する。本 PP では拡張コンポーネント FIA_BUA.2 で対応する。FIA_BUA.2 が要求される以前に登録ユーザは識別されていなければならない。よって、FIA_UID.2 も要求される。

セキュリティ対策方針 O.PAD は、偽造物による認証成功を防止するための要件である。これに対応するのは、拡張コンポーネント FIA_BUA.3 である。

セキュリティ対策方針 O.AUTH_ADMIN では、TOE 管理機能に BS 管理者だけがアクセス可能とするために、BS 管理者の識別・認証の要件が発生する。これに対応するのは FIA_UAU.2、FIA_UID.2 である。これにより、許可された BS 管理者がすべての TSF 実施の前に、TOE に認証されることが規定される。

セキュリティ対策方針 O.PROTECT_TSFDATA は、TSF を適切に管理するための機能を要求している。この管理は TSF データの操作を意図している。CC パート 2 によれば、FMT クラスがセキュリティ管理の要件を規定しており、管理を実現するためには管理を行う役割を規定する必要がある。本 PP では、FMT_SMR.1 を選択することにより、BS 管理者という役割を TSF の管理に関連付けている。またどのような管理機能が TSF によって提供されるべきか、という内容については FMT_SMF.1 で規定しており、その管理機能がどのような TSF データに、どのような操作を行うかを FMT_MTD.1 で規定している。この一連の FMT ファミリの規定により、O.PROTECT_TSFDATA が適切に満たされる。

セキュリティ対策方針 O.CONTROL_FALSE_REJECT は、認証に適切な本人拒否率(FRR)を規定する。これに対するセキュリティ機能要件は、O.CONTROL_FALSE_ACCEPT と同様に、

拡張コンポーネント FIA_BUA.2 及び FIA_UID.2 である。

セキュリティ対策方針 O.CLEAR_RESIDUAL は、生体認証を実施した際に使用された認証データが、TOE 内に残存することを防止し、許可されていない利用者(攻撃者)の認証に許可されている利用者の認証データが利用されることを防止する。本 PP では、FDP_RIP.1 が対応する。

6.1.セキュリティ機能要件では、上記のような考察の結果、セキュリティ機能要件がまとめられている。ただし、CC の作法に基づき、以下の記法が採用されている。

・割付及び選択は　[割付：*XXX(斜体)*]、[選択：*XXX(斜体)*]の形式で示す。

・選択操作は、選択対象外の項目を抹消線(~~抹消線~~)で示す。

・詳細化は、詳細化を施した部分を下線で示す。

・繰返し操作は、SFR 名称の後ろにカッコ付きで区別のための情報を示し、さらに短縮名に(1)、(2)のように番号を付けて示す。

・本 PP では、一部操作が未了であり、その個所をマーカーで示す。ST 作者は、未了部分の操作を完了させなければならない。

6.1.セキュリティ機能要件の内容は、以下のとおりである。ただし、以下では、階層と依存性に関する記述は省略する。

FDP_RIP.1サブセット残存情報保護

FDP_RIP.1.1 TSF は、[割付: *オブジェクトのリスト*]のオブジェクト[*からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

注：　消去するオブジェクトを全て割り付けよ。

FIA_BUA.2 アクション前のバイオメトリクスによる利用者認証

FIA_BUA.2.1 許可された利用者に対するバイオメトリクスによる利用者認証　TSFは、その利用者を代行する他のTSF 仲介アクションを許可する前に、各利用者にバイオメトリクスによる利用者認証メカニズムが、エラー率FAR[割付：*X*]以下、FRR[割付：*Y*]以下で、動作することを要求しなければならない。

FIA_UAU.2 アクション前の利用者認証 - BS管理者に対する認証

FIA_UAU.2.1 BS管理者に対する利用者認証　TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

注： BS 管理者に対する利用者認証には、バイオメトリクス以外の利用者認証メカニズムを使用すること。

FIA_BUA.3 偽造されないバイオメトリクスによる認証

FIA_BUA.3.1 TSF は、TSF の利用者による生体を模して偽造された認証データの使用を[選択: *検出*、*防止*]しなければならない。

注 : 偽造物が提示された場合のアクションはこの PP では特定しない。ST 作者が実装に合わせて選択すること。どのようなアクションであっても、結果的に TOE は偽造物を受け入れなければよい。

FIA_UID.2(1) アクション前の利用者識別

FIA_UID.2.1(1) 許可された利用者に対する生体認証　TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

注 : 個人が使用するバイオメトリクス製品（例 : モバイルフォンやスマートフォンなどのポータブルデバイス）の場合は、当該個人の識別が成功しているものとみなして良い。

FIA_UID.2(2) アクション前の利用者識別

FIA_UID.2.1(2)BS管理者に対する認証　TSF は、その利用者を代行する他のTSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FMT_MTD.1 TSF データの管理

FMT_MTD.1.1 TSFは、[割付: *TSFデータのリスト*]を[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、*消去*、*[割付: その他の操作]*]する能力を[BS管理者]に制限しなければならない。

FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 TSFは、以下の管理機能を実行することができなければならない。: [割付: *TSFによって提供される管理機能のリスト*]

注 : バイオメトリック・システムの典型的な TOE 管理機能は、閾値の設定などがある。この機能の特定は ST 作者が実施する。

FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSFは、役割[BS管理者]を維持しなければならない。

FMT_SMR.1.2 TSFは、利用者を役割に関連付けなければならない。

6.2.セキュリティ保証要件では、セキュリティ機能要件の実装に対するセキュリティ保証要件をCC パート３のカタログから抽出する。本 PP では、保証コンポーネントは EAL2 を基本とし、ALC_FLR.1 を追加の要件とした。表 5.2-3 に保証要件の一覧を示す。

表 5.2-3　セキュリティ保証要件

保証クラス	保証コンポーネント
開発	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.1
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
テスト	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.2

6.3.1.セキュリティ機能要件根拠 の 6.3.1.1.セキュリティ対策方針とセキュリティ機能要件の対応 では、以下の表 5.2-4 で両者の関係を示している。

表 5.2-4 セキュリティ対策方針とセキュリティ機能要件の対応

	O.CONTROL_FALSE_ACCEPT	O.PAD	O.AUTH_ADMIN	O.PROTECT_TSFDATA	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL
FDP_RIP.1						x
FIA_BUA.2	x				x	
FIA_UAU.2			x			
FIA_BUA.3		x				
FIA_UID.2(1)	x	x				
FIA_UID.2(2)			x			
FMT_MTD.1				x		
FMT_SMF.1				x		
FMT_SMR.1				x		

6.3.1.2.セキュリティ対策方針とセキュリティ機能要件の対応関係根拠では、上述のセキュリティ機能要件の説明で述べたような内容が記述されている。

6.3.1.3.セキュリティ機能要件の依存性、6.3.2.セキュリティ保証要件根拠、6.3.2.1.セキュリティ保証要件の依存性 については、ここでは省略する。英語版 PP を参照されたい。

6.セキュリティ要件の内容は、第 3 回のベンダー各社インタビュー及び委員会での意見聴取で、ほぼ素案のとおり合意された。

(8)サポート文書の開発

本 PP のサポート文書は来年度の完成を予定している。今年度は、案としてその一部を作成した。今年度作成分の内容は、TOE 変更への対応方法である。ベンダー各社へのインタビュー結果でもわかるように、想定される TOE は各社各様である。本 PP では、既に述べたとおり、各社の共通部分を TOE にした。本 PP は論証適合を許容しているので、本 PP に適合しつつ、TOE からはみ出した機能も含めて CC 認証取得を希望するベンダーもあり得る。今年度作成のサポート文書案では、Capture を含んだ場合、Storage を含んだ場合のそれぞれに対して、セキュリティ課題定義、セキュリティ対策方針、セキュリティ要件をどのように変更すべきかをまとめた。

5.2.2 PP 認証取得

PP 認証取得は、日本の認証機関である IPA で取得することは予め決めていた。PP 認証取得のためには、その前段階として、評価機関による評価が必要である。日本で認定されている評価機関は 4 社あるため、産総研規程で競争入札によって評価機関を決定する必要があり、平成 26 年(2014 年)11 月 28 日に入札公告し、12 月 19 日に開札の結果、みずほ情報総研株式会社が落札した。評価終了は平成 27 年(2015 年)2 月 20 日に設定された。

PP 認証取得のためには、IPA への認証申請手続きが必要である。また、評価機関の評価のうち、一部の公式な作業は認証申請完了後のキックオフミーティング以後に実施されなければならない。そのため、平成 27 年(2015 年)1 月 7 日に IPA に認証申請手続きを実施し、最終的に 1 月 26 日に「認証申請（IT 認証 5529)」として認証申請が受理され、1 月 29 日に認証機関 IPA、評価機関みずほ情報総研、申請者産総研でキックオフミーティングを実施した。評価完了が 2 月 20 日、認証完了が 4 月 20 日であることが確認された。キックオフミーティングでの IPA による主な確認事項は、以下のとおりである。

1)調達者が理解しやすい脅威の表現であることが重要になる。現状の脅威では、詳細度で不足している内容や、内容が重複している脅威がみられるので、見直しが必要と思われる。

2) 前提条件の中で「ガイダンスが定める内容に従うこと」という趣旨の部分が複数あるが、CC 評価の中では前提条件（運用環境のセキュリティ対策方針）を達成するための方法が、ガイダンスに適切に記されているかが評価される。現状の内容では、評価の中で矛盾が生じ、評価が不合格になることが懸念される。また、ガイダンスについては、合理的な内容であること（利用者に過剰な要求を課していないこと）も、確認されるので、その観点も含めて前提条件の見直しが必要であると考えられる。

評価機関みずほ情報総研からは、2 月 3 日に所見報告書が発行され、8 件の指摘事項が提示された。

この指摘事項を反映した PP 改訂版を 2 月 9 日に提出の結果、2 月 12 日に評価合格の評価報告書を、評価機関みずほ情報総研から受領した。評価報告書は認証機関 IPA にも送付され、2 月 13 日に受領通知が認証機関 IPA から発行された。本活動報告書の作成時点では、認証機関 IPA による認証作業が実施されている。

評価機関みずほ情報総研からの指摘事項を、所見報告書(136601-01-R008-01)より以下に引用する。

所見報告番号/バージョン	APE-001-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	threshold value の設定機能について
評価サブアクティビティ名	APE_INT.1-3（APE_INT.1.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	threshold value を設定する機能の必要性が不明。
含意	「1.3.3. Usage of a TOE」に 「The threshold value is usually configured by the administrator of the BS.」 と記載されている。 「1.3.4.3. Security management functions」に「The setting of security relevant data of the TOE, including the threshold value, is done with the security management functions of the TOE.」と記載されている。 「1.3.6. Functions of the TOE」の「Configure」に「This function is especially used to configure the threshold setting for the decision function.」と記載されている。 これらの記述からはTOE が threshold value を設定する機能を持ち、threshold value は TSF データであることから設定機能に関する SFR が存在することが期待されるが、該当する SFR の記述が確認できない。
推奨処置	threshold value を設定する機能の必要性を確認し、必要であるならば SFR 等と一貫するよう PP の記述を見直す。

所見報告番号/バージョン	APE-002-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	Countering the threats T.MODIFY_ASSETS について
評価サブアクティビティ名	APE_OBJ.2-4（APE_OBJ.2.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	根拠の記述に不明確な部分が存在する。
含意	「4.3.1. Countering the threats」に T.MODIFY_ASSETST.MODIFY_ASSETS is a threat that an attacker may try to modify, destroy, or collect and exploit the secondary assets in the TOE.と記載されているが、 T.MODIFY__ASSETS の定義では The attacker may try to make the TOE work abnormally and give unauthorized access to the portal, by modifying, destroying, or collecting and exploiting the secondary assets in the TOE.と記載されている。 前者は TOE の 2 次資産の modify, destroy, or collect and exploit を脅威としているが、後者は unauthorized access to the portal を脅威とし TOE の 2 次資産については攻撃の手段という位置づけになっており、似て非なるものになっている。
推奨処置	脅威の内容について誤解を招くおそれがあることから、記述を見直し、内容を統一する。

所見報告番号/バージョン	APE-003-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	FIA_BUA.2 の定義について
評価サブアクティビティ名	APE_ECD.1-3（APE_ECD.1.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	FIA_BUA.2 の定義に不明確な部分が存在する。
含意	FIA_BUA.2 の定義において Hierarchical to: No other components. と記載されているが、その内容ならびに既存のコンポーネントとの関係から Hierarchical to: FIA_BUA.1 Timing of biometric user authentication. であると思われる。
推奨処置	FIA_BUA.2 の定義を確認する。

所見報告番号/バージョン	APE-004-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	FIA_BUA.2 の依存性の根拠について
評価サブアクティビティ名	APE_REQ.2-9（APE_REQ.2.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	FIA_BUA.2 の依存性の根拠に不明確な部分が存在する。
含意	Table 5 Fulfillment of the dependencies において FIA_BUA.2 の Fulfilled by の項に FIA_UID.1 と記述されているが、FIA_UID.2(1) であると思われる。
推奨処置	Table 5 の記述を見直す。

所見報告番号/バージョン	APE-005-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	FIA_BUA.3 の依存性の根拠について
評価サブアクティビティ名	APE_REQ.2-9（APE_REQ.2.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	FIA_BUA.3 の依存性の根拠に不明確な部分が存在する。
含意	Table 5 Fulfillment of the dependencies において FIA_BUA.3 の要求される依存性が「なし」になっており、「5.1. Biometric User Authentication FIA_BUA」における FIA_BUA.3 の定義と一貫していない。 定義においては Dependencies: FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of Management Functions となっている。
推奨処置	Table 5 の記述を見直す。

所見報告番号/バージョン	APE-006-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	セキュリティ要件の根拠について
評価サブアクティビティ名	APE_REQ.2-11（APE_REQ.2.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	セキュリティ要件の根拠の記述に不明確な部分が存在する。
含意	「6.3. Security requirements rationale」の O.BIOMETRIC_VERIFICATION に This security objective provides a function of biometric verification for access to the portal and prevents users expect Enroled Users from accessing to the portal. と記述されているが、下線の部分は「4. Security objectives」の O.BIOMETRIC_VERIFICATION の定義には記述されていない。 TOE に要求される機能は限定的であり、portal へのアクセスの制御は IT 環境である Policy Management/AccessControl によって行われることから、このような記述は TOE の機能と IT 環境の機能の関係について誤解を招くおそれがある。
推奨処置	セキュリティ要件の根拠の記述を見直す。

所見報告番号/バージョン	APE-007-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	前提条件 A.CAPTURE について
評価サブアクティビティ名	APE_SPD.1-4（APE_SPD.1.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	前提条件の記述に不明確な部分が存在する。
含意	前提条件は消費者が各自の運用環境が前提条件と一致していることを決定できる詳細度で記述されなければならない。 現状の記述の場合、消費者は Capture Device や運用環境を特定できず、各自の運用環境が前提条件と一致していることを決定できない。 PP は TOE の種別に対するセキュリティニーズについての実装に依存しないステートメントであることから、実装に依存する部分については ST で明確にすることを要請することもできるが、その場合は、ST author に対する要請として ST で明確にすべきことを記述しておく必要があると思われる。

推奨処置	前提条件 A.CAPTURE の記述を見直す。
所見報告番号/バージョン	APE-008-01
評価用提供物件	Protection Profile for Biometric Verification Products(BVPPP) Version：1.0 2015/01/05
タイトル（所見内容の要約）	拡張コンポーネントについて
評価サブアクティビティ名	APE_ECD.1-12（APE_ECD.1.1E）
問題の重大度（大/小/確認）	小
問題点（所見内容）	拡張コンポーネントの定義に不明確な部分が存在する。
含意	拡張コンポーネントは評価可能な客観的なエレメントで構成されていなければならない。 PP で定義されている拡張コンポーネントは error rates、rate to reject を満たすことを要求しているが、これらについては評価方法を示す必要がある。
推奨処置	拡張コンポーネントの評価方法（規格、基準等）を明記する。

付録に、指摘事項を反映して評価合格した PP を掲載する。

5.3　セキュリティ評価手法の研究

本節では、バイオメトリック製品の CC 認証に基づくセキュリティ評価を行うにあたり実施する評価手法として、精度評価及び
脆弱性評価に関する研究結果を示す。

5.3.1　精度評価

本節では、本事業におけるセキュリティ評価項目のひとつである精度評価について、評価の必要性、基本方針、使用する評価尺度、評価方法などを示したのち、評価効率化のための精度評価ツールの今年度の開発機能について述べる。

5.3.1.1　必要性

本事業は、CC 認証におけるセキュリティ評価・認証の仕組みをバイオメトリック製品に適用し、バイオメトリック製品の評価・認証基盤構築を推進することを目的としている。バイオメトリック製品のためのセキュリティ評価項目とその内容については、ISO/IEC 19792（Security evaluation of biometrics）で規定されている。主な規定内容を図 5.3-1 に示す。

本図に示すとおり、バイオメトリック製品のためのセキュリティ評価は、精度評価、脆弱性評価、及びプライバシー評価の 3 つで構成される。このうち本人拒否率や他人受け入れ率などといった尺度で示される精度評価は、バイオメトリック製品の基本性能を示すものとして重要な位置づけを持つ。あわせて、精度評価は脆弱性評価と密接な関係を持つことが同規格に示されている。脆弱性評価における最も基本的なアタックは、ゼロエフォートアタックと呼ばれる、たくさんの利用者を集めてバイオメトリック照合を試行する攻撃であるが、バイオメトリック製品の認証精度（他人受け入れ率）が低いと、比較的少人数の人を集めただけで、他人への成りすましが比較的容易に起こせてしまう。このことから、精度評価は脆弱性評価との関係においても重要である。

以上より本事業では、精度評価をバイオメトリック製品のためのセキュリティ評価の重要な項目と位置づけ、評価手法を研究することとした。

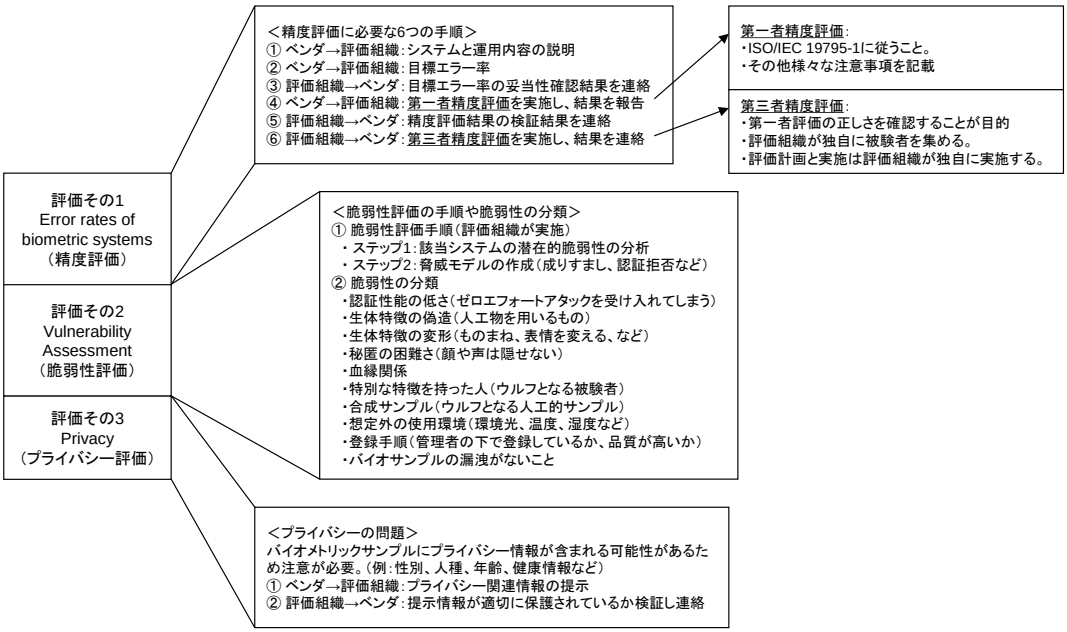


図 5.3-1 ISO/IEC 19792 における評価項目

5.3.1.2 精度評価の基本方針

本節では、本事業における精度評価の基本方針をまとめる。基本方針を定めるにあたり、プロテクションプロファイル（PP）、評価の目標、評価方法、脆弱性評価との関係、プロジェクトとしてのその他の重要条件の 5 つに分けて検討した。その内容を以下に示す。

(1) 独立試験

コモンクライテリアにおける精度評価は、機能試験を意味する ATE_FUN と独立評価機関が実施する独立試験を意味する ATE_IND の 2 つのケースが考えられる。本事業においては、国内の独立評価機関において実績のない独立試験における精度評価に、意義がより大きいと考え、独立試験（ATE_IND）に重点をあてて研究することとする。

(2) ISO/IEC 19795 準拠(1) 独立試験

精度評価を独立評価機関が実施するにあたっては、国際規格に準拠した方法で実施することがコモンクライテリアにおける評価として重要である。バイオメトリック製品の精度評価は、ISO/IEC 19795 規格により規定されている。したがって、本事業における精度評価は、ISO/IEC 19795 に準拠することを方針とする。

(3) 共通ツールの開発

独立評価機関が精度評価を行う場合、最も効率よく実現するには複数のバイオメトリック・ベンダー製品に対して共通的に使用できるツールを開発することが重要である。このような共通的なツールがなければ、異なるベンダー製品を評価するたびに、ツールを開発しなおさなければならなくなり、結果的に期間とコストの増大につながるためである。本事業では、共通ツールの実現のため に、バイオメトリック・ベンダー製品が提供する機能として、バイオメトリクスのため

の国際標準インタフェースである BioAPI を採用することにより、共通化を実現する。

(4) 脆弱性評価との関係の検討

精度評価を検討するにあたり、脆弱性評価との関係についてもあわせて検討していく必要がある。こうすることで、精度評価ツールの中に脆弱性評価のための機能を盛り込むことが可能となり、本事業の成果をより高くすることができると考えられるためである。(脆弱性評価機能の精度評価ツールへの適用は、平成 27 年度以降の検討テーマとし、平成 26 年度の検討対象外とすることとした。)

(5) コストと期間

本事業においては、コモンクライテリアとしてのセキュリティ評価のコストと期間が、ベンダー及び独立評価機関ともに適切で受容可能、かつ、継続可能でなければならない。精度評価ツールによって、独立評価の期間とコストはある程度の低減が可能と考えられるが、求められる精度に応じて募集する被験者の数が多くなりすぎると、コストと期間の増大を招くことになり、結果的に実現性や継続性に問題が生じる。本事業では、コストと期間に問題のない、コモンクライテリアにおけるセキュリティ評価として必要な被験者数について検討する。(本内容は平成 27 年度の検討項目とする。)

5.3.1.3 独立試験(ATE_IND)の手順

本節では、前節で述べた基本方針において研究対象として取り上げたバイオメトリック製品の精度評価を独立試験として実施する際の作業内容について述べる。

一般的にバイオメトリック製品の精度評価を独立試験として実施する際には、表 5.3-1 に示すような作業手順が必要になると考えられる。本表で示される各手順のうち、2、3、及び 4 で示される手順は実際の精度評価を実施するための評価前作業である。手順 5 で実際の評価作業を行った後に実施される手順 6 及び 7 は、評価後作業である。

表 5.3-1 バイオメトリック製品の独立試験に必要な手順

手順	評価組織の作業	説明
1	(ベンダー製品入手)	評価対象となるベンダー製品を入手する。
2	仕様・ソースチェック	精度評価実施に向けて、ベンダー製品の仕様書やソースコードを解析する。
3	評価方法検討	ベンダーから提供された製品に対して、19795-2 のシナリオ評価に準拠した精度評価方法を適用するための評価方法を検討する。
4	評価手順書作成 (評価方法の決定)	検討結果に基づいた精度評価手順書を作成する。
5	評価実施	手順書に基づいて精度評価を実施する。
6	評価結果分析	精度評価によって得られた評価結果を分析する。
7	評価レポート作成	分析結果から評価レポートを作成する。

独立評価機関が前述の評価前作業、評価実施、評価後作業を行うにあたっては、それぞれの作業において ISO/IEC 19795 への準拠が求められる。場合により独立評価機関は、ISO/IEC 19795 への準拠性の検証において、製品ごとに評価方法を検討したり、場合によってはベンダー製品のソースコードを解析したりしなければならなくなることが考えられる。

図 5.3-2 は、この評価前作業、評価実施、評価後作業の各種項目を、ISO/IEC 19795-1 に記述されている詳細な規定項目と対応付けたものである。本図に示すとおり、規格準拠性の検証のためにはベンダー製品のバイオメトリック登録や照合に関わる各機能について、提示されるドキュメントの調査やソースコード解析を通じて、ひとつひとつ確認する必要がある。これらの作業は一般的に、バイオメトリック製品や、ISO/IEC 19795 規格に精通した専門家の知識が求められる場合が多く、求められる専門性の観点より、必ずしも CC 認証における独立評価機関の評価者が行なう方法として適しているとは言えない。

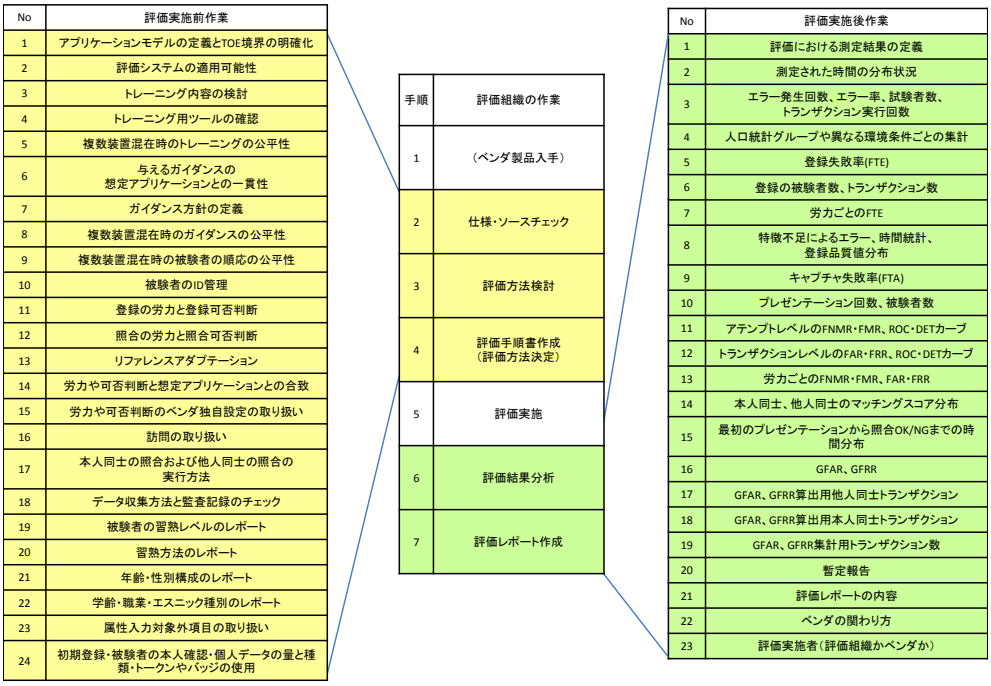


図 5.3-2 ISO/IEC 19795-2 で規定される項目との対応付け

表 5.3-2 は、ISO/IEC 19795 に準拠することを前提として独立評価機関がベンダーのバイオメトリック製品の独立精度評価を行う場合に必要となる作業量の目安を示したものである。本表における共通ツールとは、異なるベンダーによる複数のバイオメトリック製品に対して共通的に使える精度評価ツールを意味する。独自ツールとは、バイオメトリック・ベンダーが精度評価に利用可能なツールを独自に開発したものである。ツールなしとは、評価対象となるバイオメトリック製品に特にツールが存在しない状態である。例えば、アプリケーション・システム等、完結したシステムを評価対象とするような場合が相当する。本表に示すとおり、共通ツール、独自ツール、ツールなしの 3 つの場合において、精度評価のための各作業の作業要否に違いがでると考えられる。

表 5.3-2　ISO/IEC 19795 準拠の独立精度評価を評価組織が実施する際の予想作業量

手順	評価組織の作業	共通ツール	独自ツール	ツールなし
1	(ベンダー製品入手)	要	要	要
2	仕様・ソースチェック	不要	要	要
3	評価方法検討	不要	要	要
4	評価手順書作成（評価方法の決定）	不要	要	要
5	評価実施	要	要	要
6	評価結果分析	不要	要	要
7	評価レポート作成	不要	要	要
予想作業量		少ない	多い	多い

独自ツールやツールなしで独立評価機関が精度評価を行う場合、評価前作業や評価後作業が共通ツールを用いた場合に比べて大きなものとなることが予想される。独自ツールはベンダー毎に仕様が異なっているはずで、精度評価のための独自ツールを用いる場合は、ツールのソース解析を独立評価機関が行い、プログラムとしての適切さとともに ISO/IEC 19795 への準拠性について検証する必要がでる。ツールなしの場合は、アプリケーション・システムのソース解析を行い、ISO/IEC 19795 に準拠した精度評価の可否、精度評価の実施計画、評価実施時のエビデンス生成方法の確立、精度値の算出方法の検討から、最終的なレポートの生成まで、多種多様な作業の実施が必要となる。独立評価機関に求められるこれらの作業量は、ベンダーのバイオメトリック製品の仕様と、ベンダーが開発した精度評価環境の構築状況に大きく左右されることが予想される。

本事業は、3 ヵ年をプロジェクトの期間として推進する事業であり、最終年度での評価実施が計画されている。これを踏まえ本事業においては、評価に要する期間やコストの確定が困難な独自ツールやツールなしでの評価ではなく、評価前作業、評価実施、評価後作業の作業量を低減でき、かつ、作業計画が立てやすい共通ツールを用いた方法が望ましいと考え、このようなツールの開発を実施することとした。

5.3.1.4　精度評価の進め方

本節では、前節まで述べた精度評価の方針に従って、本事業における精度評価の進め方に関する方針について述べる。

(1)共通インタフェースの採用

第三者機関による独立試験で使用する共通ツールの開発においては、ベンダーのバイオメトリック製品が提供するインタフェースを共通化する必要がある。本事業においては、評価対象製品がサポートするインタフェースとして、国際標準規格 ISO/IEC 19784-1 BioAPI 準拠製品、あるいは、米国 ANSI 規格である BioAPI 1.1 を採用することとする。なお、本事業で開発する共通ツールは、国内ベンダーの社内試験の改善に寄与することを目的として、精度評価のリファレン

スツールとして国内ベンダーを中心に公開する予定である（公開時期は未定）。

また、独自ツールを用いた精度評価やツールなしでの精度評価は、本事業によって開発した共通ツールを用いた精度評価の実施により独立評価機関によるノウハウの蓄積とあわせて検討する。

（独自ツールやツールなしでの精度評価は検討までとし、独立評価機関による実施の精度評価は本プロジェクトのスコープ外とする）

(2)脆弱性評価へのツールの適用

独立評価機関による脆弱性評価(AVA_VAN 関係）に関わる精度評価も、共通ツールを用いることを検討する（具体的な検討は平成 27 年度以降とする）。

5.3.1.5 精度評価ツールの評価項目

本節では、本事業にて開発する精度評価ツールが対象とする評価項目について述べる。

(1)FTE（登録失敗率）

本事業で扱う登録のための精度評価はバイオメトリック装置とアルゴリズムを含んだシナリオ評価であり、登録のためのトランザクションを評価単位とする。

①評価方法：シナリオ評価

(a)精度評価ツールによる登録シナリオの実行

(b)バイオデータ収集は被験者募集で実現（独立評価組織が募集）

② ベンダー・アルゴリズムの登録用推奨閾値に設定

③成功・失敗のカウント

(a)登録トランザクションを 3 回実行する

(b)1 度でも成功したら FTE としない（すべて失敗したら FTE とする）

④トランザクションは BioAPI 関数で実現

（1 回のトランザクションは BioAPI_Enroll 関数呼び出し、あるいは、BioAPI_Capture / BioAPI_CreateTemplate 関数呼び出しで実現する）

(2)FRR（本人拒否率）

本事業で扱う 1:1 照合のための精度評価はバイオメトリック装置とアルゴリズムを含んだシナリオ評価であり、1:1 照合のためのトランザクションを評価単位とする。

①評価方法：シナリオ評価

(a)精度評価ツールによる 1:1 照合シナリオの実行

(b)バイオデータ収集は被験者募集で実現（独立評価組織が募集）

②ベンダー・アルゴリズムの照合用推奨閾値に設定　（後述の FAR 評価(3)と同じ値を用いる）

③成功・失敗のカウント

(a) 1:1 照合トランザクションを 3 回実行する

(b) 1 度でも成功したら FRR としない（すべて失敗したら FRR とする）

④トランザクションは BioAPI 関数で実現

（1 回のトランザクションは BioAPI_Capture / BioAPI_Process /BioAPI_VerifyMatch 関数呼び出しで実現する）

(3)FAR（他人受け入れ率）

FAR 評価は前述(1)及び(2)において収集された被験者の登録テンプレート及び 1:1 照合用バイオメトリック・データを用いたクロスマッチによって算出する。

①評価方法： 擬似的なシナリオ評価（クロスマッチ）

(a) 精度評価ツールによるクロスマッチシナリオの実行

(b) バイオデータ収集： 以下の 2 通りの方法がある

・前述の FTE 評価(1)及び FRR 評価(2)で収集（必須）

・ベンダーの既存社内データベースを使用（オプション）

②ベンダー・アルゴリズムの照合用推奨閾値に設定（前述の FRR 評価(2)と同じ値を用いる）

③成功・失敗はマッチング単位

④マッチングは BioAPI 関数で実現（1 回の比較は BioAPI_VerifyMatch 関数で実現する。）

(4)ROC カーブ（CC 認証として不要であれば削除予定）

ROC カーブは前述(3)のクロスマッチを異なるアルゴリズム閾値を設定することにより集計する。ただし、CC 認証の認証において不要と判断される場合は、精度評価ツールの機能からは削除する予定である。

①評価方法：擬似的なシナリオ評価（クロスマッチ）

(a)精度評価ツールによるクロスマッチシナリオの実行

(b)バイオデータ収集は以下の 2 通りの方法がある

・前述の FTE 評価(1)及び FRR 評価(2)で収集（必須）

・ベンダーの既存社内データベースを使用（オプション）

②ベンダー・アルゴリズムの照合用閾値を複数回変化させながら繰り返し実行

③成功・失敗はマッチング単位

④マッチングは BioAPI 関数で実現（1 回の比較は BioAPI_VerifyMatch 関数で実現する。）

表 5.3-3 に精度評価ツールの評価項目をまとめる。FTE 及び FRR は、被験者によるバイオメトリック装置を用いたキャプチャを伴う評価である。これらの評価はトランザクション単位に実行する。FAR 及び ROC カーブは、登録トランザクション及び照合トランザクションから集められた代表的なデータを 1 つずつ選ぶことにより、擬似的にトランザクション単位のクロスマッチを行うことで実現する。

表 5.3-3　精度評価ツールの評価項目

No	項目	評価方法	使用する生体情報	アルゴリズム閾値	成功・失敗の単位	トランザクション内で使われるBioAPI関数	算出方法
1	FTE	シナリオ評価	募集した被験者	登録用推奨値	トランザクション	BioAPI_Enroll or BioAPI_Capture + BioAPI_CreateTemplate	失敗した登録トランザクション数 / 総登録トランザクション数
2	FRR	シナリオ評価	募集した被験者	照合用推奨値	トランザクション	BioAPI_Capture + BioAPI_Process + BioAPI_VerifyMatch	失敗した照合トランザクション数 / 総照合トランザクション数
3	FAR	テクノロジー評価	募集した被験者＋ベンダの社内データベース	照合用推奨値	マッチング	BioAPI_VerifyMatch	他人受け入れマッチ数 / 総マッチ数
4	ROCカーブ	テクノロジー評価	募集した被験者＋ベンダの社内データベース	照合用閾値（最小値から最大値まで複数個）	マッチング	BioAPI_VerifyMatch	項番2および項番3参照

5.3.1.6　精度評価ツールの機能構成

精度評価ツールを実現するシステムの機器構成図を図 5.3-3 に示す。本図に示すとおり、精度評価ツールは試験の運用全般を管理する試験管理サーバ、被験者のバイオメトリック情報を管理するバイオメトリック DB サーバ、第三者評価機関の管理者が操作する管理者端末、被験者がバイオメトリック認証装置を用いてバイオメトリック登録やバイオメトリック照合を行う被験者端末の 4 種類から構成される。

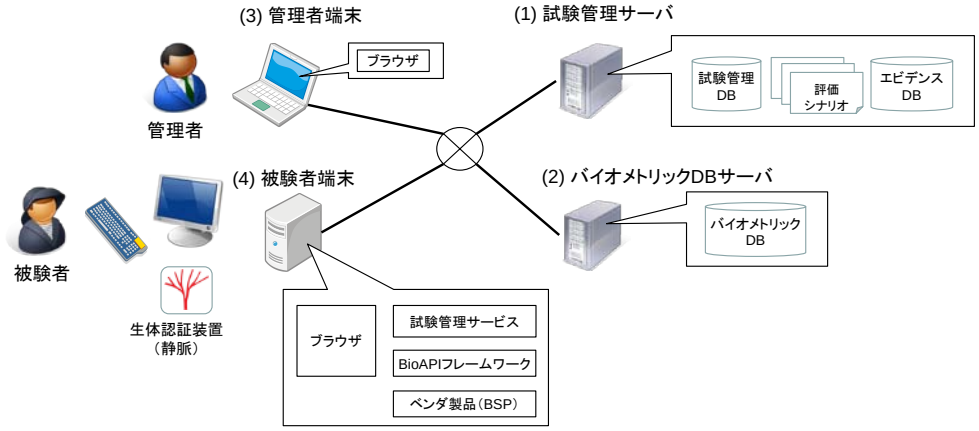


図 5.3-3 機器構成図

以下に各構成要素の詳細について説明する。

(1)試験管理サーバ

精度評価試験の運用全般を管理するサーバである。管理者や被験者は、管理者端末や被験者端末からこのサーバの URL にアクセスすることで精度評価の各種作業を行う。本サーバ内に格納される主な情報は以下のとおりである。

①試験管理 DB： アカウント管理（管理者・被験者)、バイオメトリック製品情報などを保存したもの

②評価シナリオ：バイオメトリック登録、バイオメトリック照合、クロスマッチ、トレーニングなどのシナリオファイル

③エビデンス DB： シナリオ実行時の履歴情報を保存したもの

(2)バイオメトリック DB サーバ

被験者ごとに割り当てられた ID、バイオメトリック装置を用いてキャプチャや特徴抽出を行うことにより生成された登録テンプレートや照合バイオメトリック・データなどを保存、管理する。

(3)管理者端末

管理者による精度評価の運用操作、アカウント管理をするための端末である。管理者は本端末上でブラウザを起動し､試験管理サーバの所定の URL にアクセスすることにより､精度評価ツールの管理者用機能を使用する。

(4)被験者端末

管理者によるバイオメトリック装置を用いた登録や 1:1 照合を行うための端末である。被験者は本端末上でブラウザを起動し、試験管理サーバの所定の URL にアクセスすることにより、精度評価ツールの被験者用機能を使用する。

5.3.1.7 精度評価の流れ

本節では、精度評価ツールを用いた精度評価の具体的な流れについて順を追って説明する。

(1)概要

図 5.3-4 に精度評価ツールを用いた評価の流れを概要として示す。本図は精度評価ツールを用いたシナリオ精度評価において中心的な評価実施部分を細分化したものである。本図の最下段に示すとおり、精度評価実施とは被験者への説明、被験者 ID・属性入力・トレーニング、登録シナリオ実行、照合シナリオ実行、FAR 算出シナリオ実行の 5 つから構成される。このうち、被験者への説明は、管理者が被験者に口頭ないしは資料などを用いて行う操作説明であり、精度評

価ツールとは直接関係しない。したがって、被験者への説明を除く 4 つが精度評価ツールに関係する。

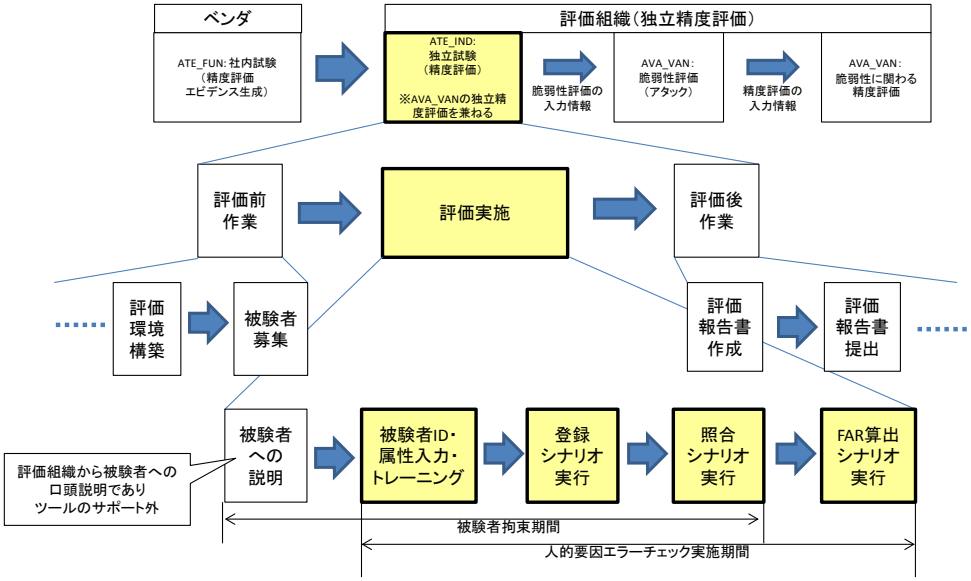


図 5.3-4 精度評価の流れ

(2)各ステップの内容

図 5.3-5 に上記(1)において精度評価ツールが関わる 4 つのステップの詳細を説明する。

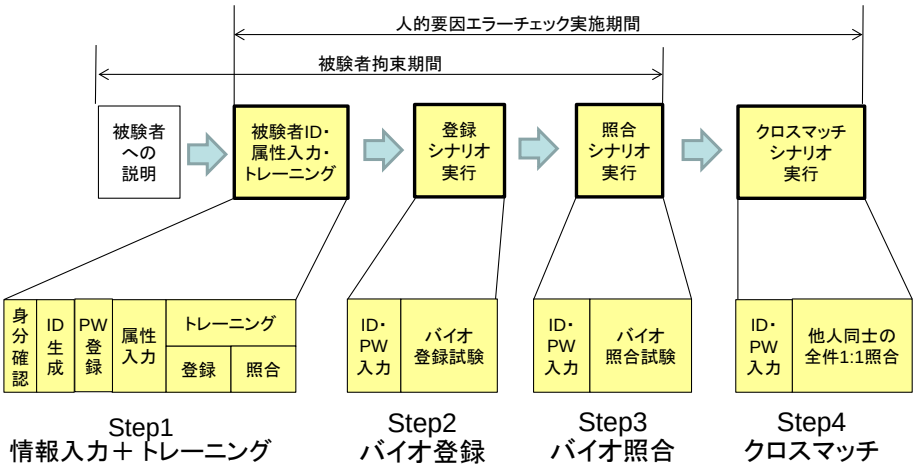


図 5.3-5 各ステップの詳細

①情報入力＋トレーニング

被験者の基本情報を登録し、評価対象となるバイオメトリック装置を、トレーニングを通して学習するステップである。それぞれの作業について以下に示す。

・身分確認：被験者の身分を何らかの情報を用いて管理者が確認する。確認方法は管理者が決定する。

・ID 生成：被験者が自分自身を一意に示す ID 番号を入力する。この ID は、あらかじめ第三者機関が定めた ID とすることもできるし、被験者が自分で決めた ID を入力することもできる。

・PW 登録：被験者が精度評価ツールにログオンする際のパスワードを入力する。ID とパスワードを登録しておくことにより、その後のバイオメトリック登録やバイオメトリック照

合の試験において、被験者の入れ替わりといった人的要因ミスを防ぐことができる。

・属性入力：被験者の年齢、性別などの属性情報を入力する。（ここで入力された情報は、将来的に、精度評価の人口統計的な分析に利用することができる。）

・トレーニング：ISO/IEC 19795-2 のシナリオ評価に記述されている、被験者の習熟を実現するための作業である。被験者はキャプチャ対象となっている部位に対して、バイオメトリック装置を用いた登録や 1:1 照合を行う。トレーニングにおいては、試験管理サーバ内に格納されているバイオメトリック登録トレーニングシナリオ、及び、バイオメトリック照合トレーニングシナリオが端末上に転送され、これらのシナリオが実行される。シナリオ実行を通じて被験者はバイオメトリック装置の取り扱い方を学ぶとともに、画面上に表示される GUI やガイダンス表示を通して操作方法に習熟する。バイオメトリック登録の成功や 1:1 照合の成功が習熟の目安となるが、習熟したかどうかの最終的な判断は管理者が行う。

②バイオメトリック登録

被験者がバイオメトリック装置を用いてバイオメトリック登録を行うステップである。それぞれの作業について以下に示す。

・ID・PW 入力：バイオメトリック登録をはじめるにあたり、被験者は精度評価ツールにログオンする。 ステップ①の ID 生成と PW 入力において登録した情報を被験者が入力することによりログオンする。

・バイオメトリック登録試験：被験者はキャプチャ対象となっている部位に対して、バイオメトリック装置を用いた登録試験を行う。登録試験においては、試験管理サーバ内に格納されているバイオメトリック登録試験シナリオが被験者端末上に転送され、実行される。シナリオにより示される手順に従い、被験者は評価対象となっているすべての部位に対して、あらかじめ定められた回数のバイオメトリック登録トランザクションを実行する。

③バイオメトリック照合（1:1 照合）

被験者がバイオメトリック装置を用いてバイオメトリック照合（1:1 照合）を行うステップである。それぞれの作業について以下に示す。

・ID・PW 入力：バイオメトリック照合をはじめるにあたり、被験者は精度評価ツールにログオンする。 ステップ①の ID 生成と PW 入力において登録した情報を被験者が入力することによりログオンする。

・バイオメトリック照合試験：被験者はキャプチャ対象となっている部位に対して、バイオメトリック装置を用いた本人同士の 1:1 照合試験を行う。1:1 照合試験においては、試験管理サーバ内に格納されているバイオメトリック照合試験シナリオが被験者端末上に転送され、実行される。シナリオにより示される手順に従い、被験者は評価対象となっているすべての部位に対して、あらかじめ定められた回数のバイオメトリック照合トランザクションを実行する。

④クロスマッチ

すべての被験者がバイオメトリック登録（ステップ②）及びバイオメトリック照合（ステップ③）を終えた後で、管理者が行う他人同士の全件照合（クロスマッチ）である。それぞれの作業について以下に示す。

・ID・PW 入力：クロスマッチをはじめるにあたり、管理者は精度評価ツールにログオンする。精度評価ツールにあらかじめ用意されている管理者アカウントの ID 及びパスワードを管理者が入力することによりログオンする。

・他人同士の 1:1 全件照合：管理者がクロスマッチ試験を実行すると、試験管理サーバ内に格納されているクロスマッチ試験シナリオが管理者端末上に転送され、実行される。シナリオにより示される手順に従い、バイオメトリック DB 内の全被験者の登録テンプレート及び 1:1 照合時に取得されたバイオメトリック・データが読み込まれ、他人同士の全件 1:1 照合が実行される。

(3)トランザクション回数について

図 5.3-6 に上記(2)で述べたトレーニング、バイオメトリック登録試験、バイオメトリック照合試験のトランザクションについて説明する。本図に示すとおり、トレーニングや登録・照合試験はトランザクションを単位とする。トランザクションとは、その処理内に一定時間あるいは一定回数のキャプチャリトライ、特徴抽出リトライ、マッチングリトライを含んだ一連の処理を表す。1 回のトランザクションを終了した時点で、被験者に対して、バイオメトリック登録やバイオメトリック照合の最終結果（成功あるいは失敗）が示される。

トレーニングで行われるバイオメトリック登録トランザクションあるいはバイオメトリック照合トランザクションは、精度評価ツールとして最大回数実行回数を規定する。被験者が十分に習熟したと判断した場合、すべての回数を終える前にトレーニングを終了する場合がある。

これに対してバイオメトリック登録試験及びバイオメトリック照合試験におけるトランザクション回数は、精度評価ツールが定めた所定回数を必ず実行する。

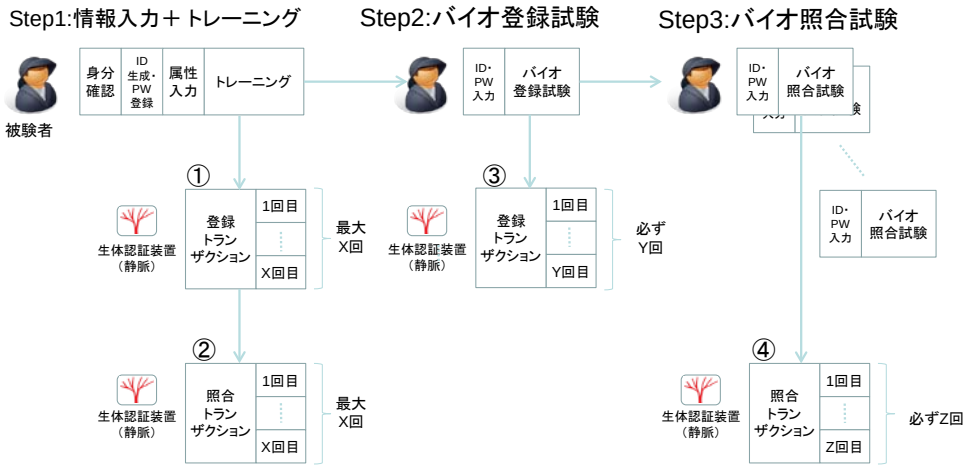


図 5.3-6 トランザクション回数

(4)複数被験者を考慮した評価の流れ

図 5.3-7 に前述までで示した精度評価を、複数の被験者が実施する際の流れを例として示す。本図では、すべての被験者が決められた順序でトレーニングを実行し、その後、すべての被験者が決められた順序でバイオメトリック登録試験を実行し、さらにその後、すべての被験者が決められた順序でバイオメトリック照合試験を実行した場合を示している。しかしながら、被験者を伴う実際の精度評価においては、被験者自身の個人的な都合を含む様々な理由により、決められた順序どおりの評価にならない場合が生じ得る。

本精度評価ツールは、バイオメトリック登録シナリオ実行前、及び、バイオメトリック照合シナリオ前に、必ず自分自身の ID とパスワードの入力を求めている。この操作を行うことにより、精度評価ツールは被験者を確実に特定した上で評価を実施できるため、被験者の試験順序の変更や、抜けなどの事象に正しく対応することができる。

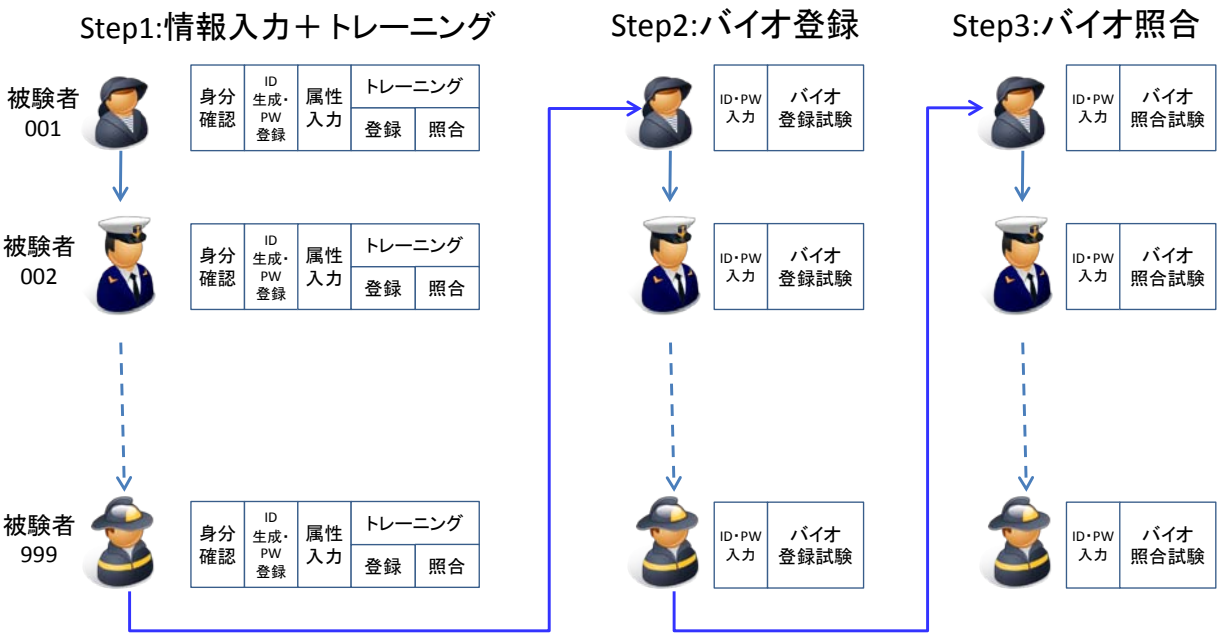


図 5.3-7 複数被験者の評価の流れ

(5)管理者の役割

本精度評価ツールでは、被験者によるトレーニング、バイオメトリック登録、及び、バイオメトリック照合など一連の評価シナリオを実行している間、管理者が被験者の状態を観察し、正しい評価が行われていることを確認することを前提とする。

バイオメトリック製品の精度評価においては、様々な形での人的要因ミスが発生しうる。装置の使い方に不慣れな被験者は、キャプチャ対象部位をバイオメトリック装置の定められた位置に移動されることができない場合があり、このような操作誤りによって精度評価尺度のひとつである FRR 値が悪化する。バイオメトリック登録試験で用いた部位と違う部位をバイオメトリック照合試験で用いてしまった場合も FRR 値が悪化する。また、本人の異なる部位間でクロスマッ

チを行う場合、バイオメトリック登録試験やバイオメトリック照合試験において、使用すべき部位を間違えると

FAR 値が悪化してしまう。このような人的要因エラーを防ぐため、管理者は被験者の振る舞いを観察し、操作誤りを発見した場合は評価作業を一時中断し、被験者の操作を正しくしなければならない。精度評価ツールとして、人的要因エラーの発生を考慮して、管理者によるトランザクションの取り消し機能が必要となることが考えられる。

図 5.3-8 に、精度評価ツールにおける管理者の役割を示す。

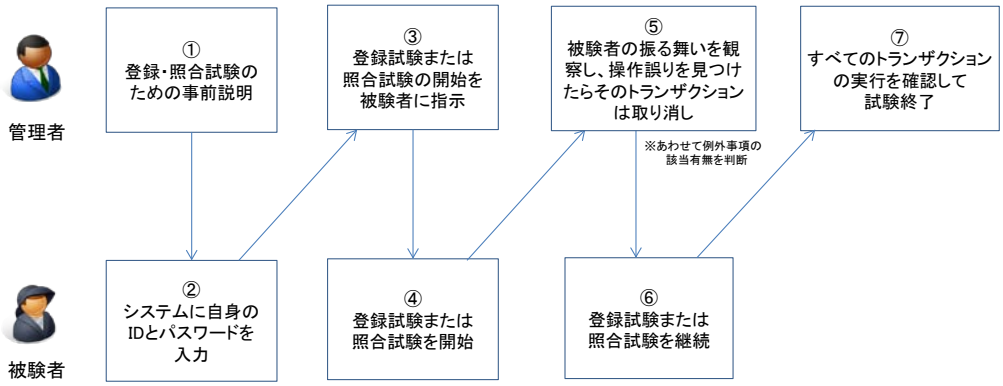


図 5.3-8 管理者の役割

(6)複数台同時接続

精度評価に必要となる被験者数は一般的に求める性能尺度（FAR あるは FRR）の値によって変化する。求める性能が高くなればなるほど、すなわち、FAR や FRR が数値として小さくなればなるほど、必要な被験者数が増加する。CC 認証における第三者機関による独立精度評価において、集めた被験者の拘束時間を短くし効率化を図ることは、試験コストの低減という意味においても重要である。

本精度評価ツールでは、多数の被験者でのバイオメトリック登録試験やバイオメトリック照合試験を効率よく進めるための対策として、複数台同時接続の機能をサポートする予定である。

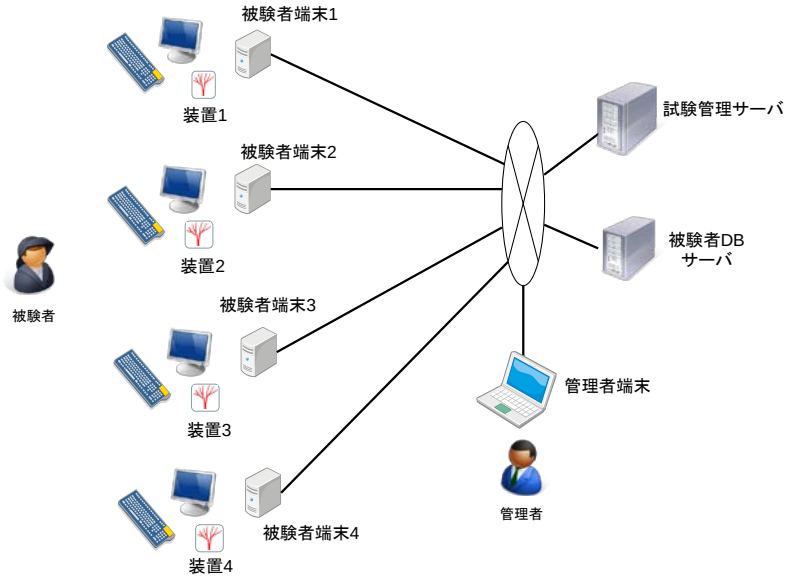


図 5.3-9 複数台同時接続

本精度評価ツールでは、多数の被験者でのバイオメトリック登録試験やバイオメトリック照合試験を効率よく進めるための対策として、複数台同時接続の機能をサポートする予定である。図 5.3-9 に複数台同時接続時のシステム構成を示す。本図に示すとおり、試験管理サーバに複数台の被験者端末を接続し、各端末に 1 台ずつバイオメトリック装置を接続することにより、1 つの精度評価システム上に複数のバイオメトリック装置を利用できるようになる。(被験者端末の上限は 4 台とする予定である。)

5.3.1.8 バイオメトリック DB とクロスマッチ

本精度評価ツールで実行するクロスマッチは、バイオメトリック登録試験、及び、バイオメトリック照合試験を実行したことによりバイオメトリック DB に保存されたバイオメトリック・データを用いて行う。本節では、バイオメトリック DB とクロスマッチについて説明する。

(1)概要

クロスマッチの方法は一般的に以下の 2 つの方式が考えられる。

① 登録テンプレートと 1:1 照合バイオメトリック・データ間の他人同士照合

② 登録テンプレート間の他人同士照合

本精度評価ツールでは、ISO/IEC 19795 が推奨する、上記①の方法に基づきバイオメトリック DB にバイオメトリック・データを収集する。図 5.3-10 に、バイオメトリック DB 内に収集される被験者の登録テンプレートと照合バイオメトリック・データ、及び、クロスマッチ照合時の組合せを示す。

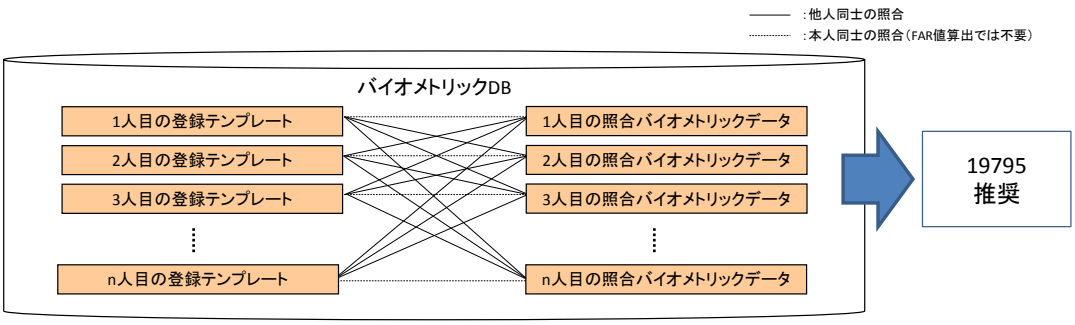


図 5.3-10 バイオメトリック DB の登録テンプレートと照合バイオメトリック・データ

(2)詳細

バイオメトリック DB の登録テンプレートや照合バイオメトリック・データは、1 つのトランザクションに対して原則 1 つのデータとして生成され、保存される。バイオメトリック登録試験やバイオメトリック照合試験では、精度評価ツールにより所定の回数のトランザクションが繰り返されることから、バイオメトリック DB に保存される生体情報も、ひとりの被験者のひとつの部位ごとに複数存在することになる。

本精度評価におけるクロスマッチでは、ひとりの被験者のひとつの部位において、ひとつの登録テンプレートとひとつの照合バイオメトリック・データを取り出し、これらを用いて全件照合を行うこととする。ここで取り出した登録テンプレートや照合バイオメトリック・データは、ひとりの被験者のひとりの部位のために行われた登録トランザクションや照合トランザクションを代表するものとして取り扱う。

図 5.3-11 にバイオメトリック DB の詳細内容を示す。本図の左側（登録テンプレートの部分）においては、ひとりひとりの被験者のそれぞれの部位ごとに実行された複数の登録トランザクションに対応して、複数の登録テンプレートが保存されている。また、本図の右側（照合バイオメトリック・データの分部）においては、ひとりひとりの被験者のそれぞれの部位ごとに実行された複数の 1:1 照合トランザクションに対応して、複数の照合バイオメトリック・データが保存されている。実際には、1:1 照合トランザクションは、内部で複数の照合アテンプトを繰り返す処理が考えられており、各アテンプトで取得された照合バイオメトリック・データのうち、最初に照合に成功した照合バイオメトリック・データが保存される。

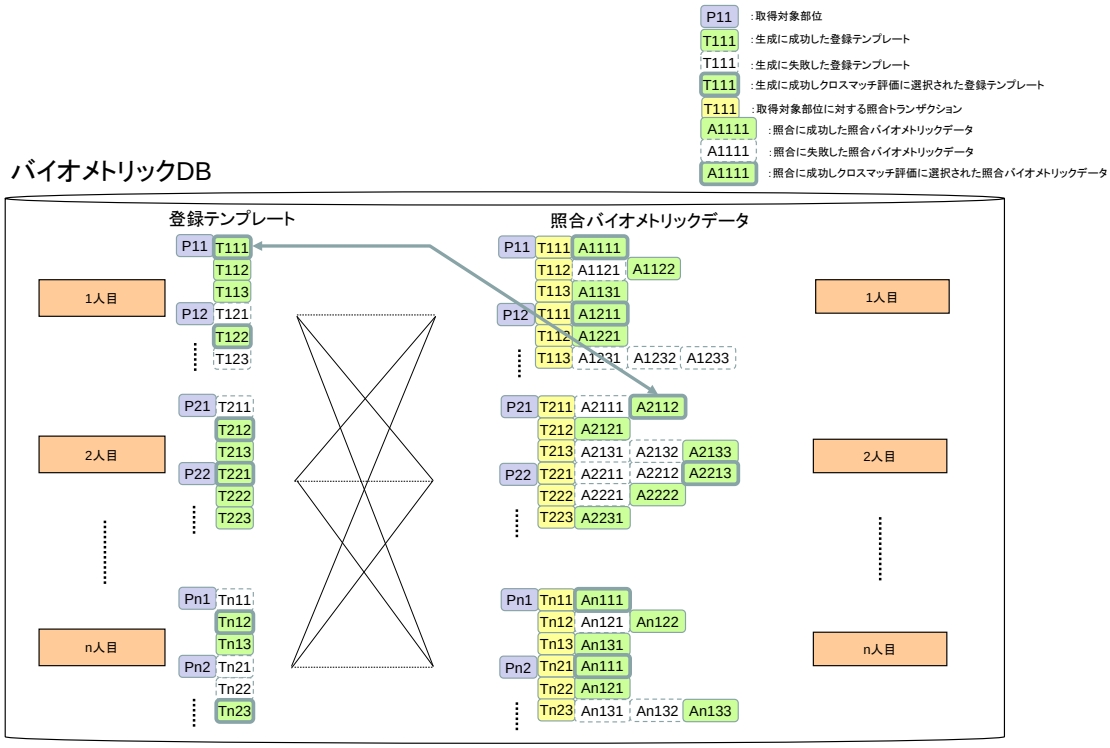


図 5.3-11 バイオメトリック DB の詳細

本精度評価ツールにおいては、このように保存されたバイオメトリック・データから、各被験者の各部位の最初の登録テンプレートを、登録トランザクションの代表データとして取り出す。また、各被験者の各部位の最初の照合バイオメトリック・データを、照合トランザクションの代表データとして取り出す。このような方法で取り出した登録テンプレートと照合バイオメトリック・データを用いてクロスマッチを実行する。

5.3.1.9 精度評価ツールの動作条件

今まで述べてきた精度評価ツールの平成 26 年度事業における動作条件を表 5.3-4 にまとめる。平成 26 年度の開発範囲において、サポート OS は Windows 7、ベンダーがサポートする BioAPI のバージョンは V2.0 とする。（平成 27 年度以降、動作条件をを変更する予定である。）

表 5.3-4　精度評価ツールの動作条件

No	項目	動作条件
1	サポート OS	Windows 7 （32 ビット ）
2	ベンダー製品の BioAPI サポート条件	① バージョン： V2.0（ISO 版） ② サポート関数 ・初期化・終了関数：BioSPI_Load / BioSPI_Unload / BioSPI_Attach / BioSPI_Detach ・ハンドル関数：BioSPI_FreeBIRHandle / BioSPI_GetBIRFromHandle ・バイオメトリック関数：BioSPI_Capture / BioSPI_CreateTemplate / BioSPI_Process / BioSPI_VerifyMatch ・その他：BioSPI_Cancel / BioSPI_Free

5.3.1.10　シナリオ詳細

本節では、精度評価ツールが実行するバイオメトリック登録トレーニング、バイオメトリック照合トレーニング、バイオメトリック登録、バイオメトリック照合の 4 つのシナリオの詳細について述べる。

(1)バイオメトリック登録トレーニングシナリオ

バイオメトリック登録トレーニングシナリオは、評価対象バイオメトリック装置を用いた登録作業を被験者が習熟することを目的としたシナリオである。登録トレーニングシナリオは、メイン部分と登録トランザクション部分で構成される。

本シナリオにおいては、評価対象部位すべてに対して最低 1 回分、登録トランザクションを実行する。ひとつの部位において登録トランザクションに失敗した場合は、成功するか規定回数に到達するまで登録トランザクションを繰り返す。ひとつの部位において登録トランザクションに成功した場合、その部位のトレーニングは完了したこととして次の部位に移動する。

図 5.3-12 にバイオメトリック登録トレーニングシナリオのフローチャートを示す。本シナリオでは BioAPI_Init、BioAPI_BSPLoad、BioAPI_BSPAttach、BioAPI_BSPDetach、BioAPI__BSPUnload、BioAPI_Terminate、BioAPI_Capture、BioAPI_CreateTemplate、BioAPI_GetBIRFromHandle の 9 種類の BioAPI 関数が呼び出される。

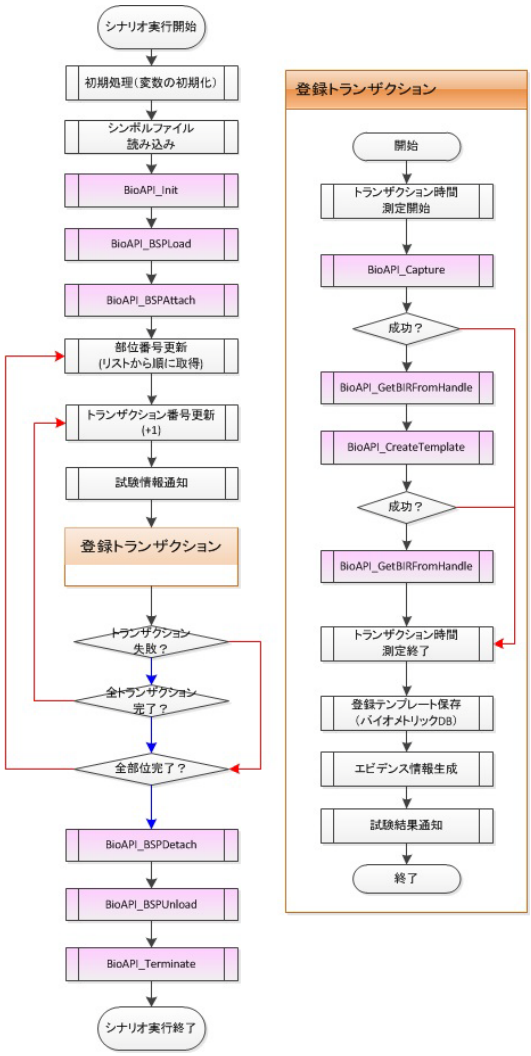


図 5.3-12 バイオメトリック登録トレーニングシナリオ

(2)バイオメトリック登録試験シナリオ

バイオメトリック登録試験シナリオは、評価対象バイオメトリック装置を用いた登録のための本試験を実行することを目的としたシナリオである。バイオメトリック登録試験シナリオは、バイオメトリック登録トレーニングシナリオと同様、メイン部分と登録トランザクション部分で構成される。

バイオメトリック登録トレーニングシナリオとの違いは、本シナリオにおいては、評価対象部位すべてに対して規定回数分、登録トランザクションを実行することである。ひとつの部位において規定回数分の登録トランザクションが完了したら、次の部位のバイオメトリック登録トランザクションを実行する。

図 5.3-13 にバイオメトリック登録試験シナリオのフローチャートを示す。本シナリオでは登録トレーニングシナリオと同様、BioAPI_Init、BioAPI_BSPLoad、BioAPI_BSPAttach、BioAPI_BSPDetach、BioAPI_BSPUnload、BioAPI_Terminate、BioAPI_Capture、

BioAPI_CreateTemplate、BioAPI_GetBIRFromHandle の 9 種類の BioAPI 関数が呼び出される。

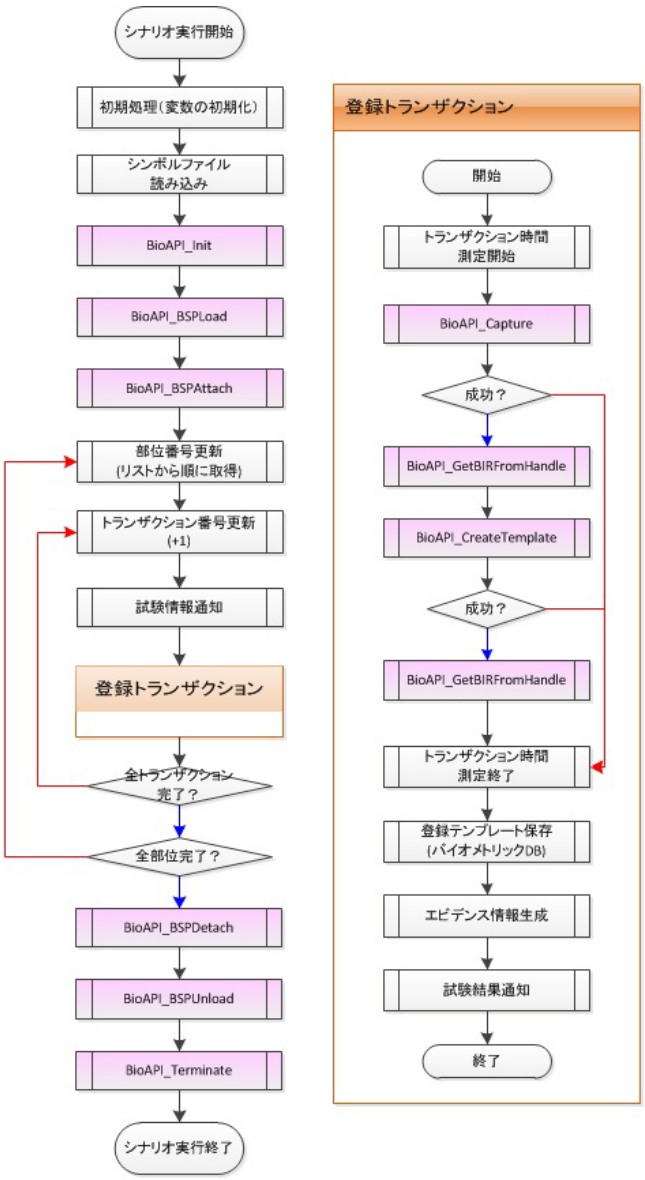


図 5.3-13 バイオメトリック登録試験シナリオ

(3)バイオメトリック照合トレーニングシナリオ

バイオメトリック照合トレーニングシナリオは、評価対象バイオメトリック装置を用いた 1:1 照合作業を被験者が習熟することを目的としたシナリオである。本シナリオは、メイン部分と照合トランザクション部分、及び、照合アテンプト部分で構成される。

本シナリオにおいては、評価対象部位すべてに対して最低 1 回分、1:1 照合トランザクションを実行する。ひとつの部位において 1:1 照合トランザクションに失敗した場合は、成功するか規定回数に到達するまで 1:1 照合トランザクションを繰り返す。ひとつの部位において 1:1 照合ト

ランザクションに成功した場合、その部位のトレーニングは完了したこととして次の部位に移動する。

図 5.3-14 にバイオメトリック登録トレーニングシナリオのフローチャートを示す。本シナリオでは BioAPI_Init、BioAPI_BSPLoad、BioAPI_BSPAttach、BioAPI_BSPDetach、BioAPI__BSPUnload、BioAPI_Terminate、BioAPI_Capture、BioAPI_Process、BioAPI_VerifyMatch、BioAPI_GetBIRFromHandle の 10 種類の BioAPI 関数が呼び出される。

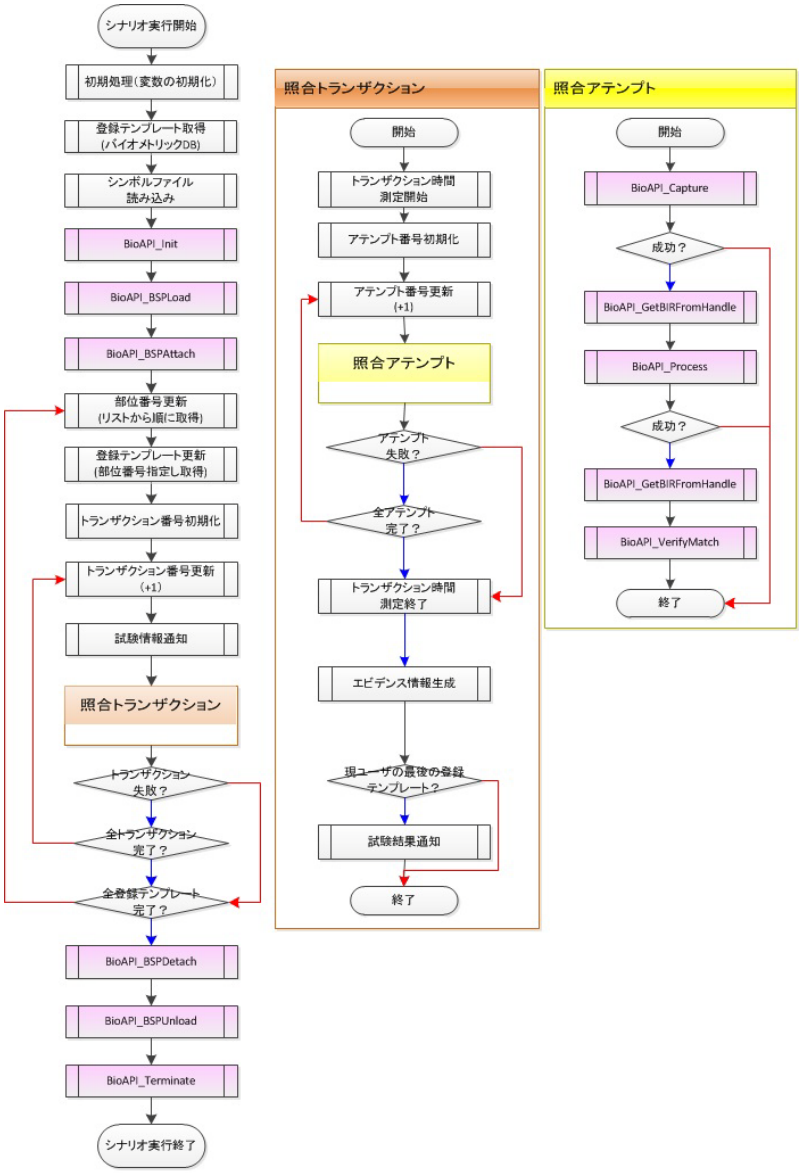


図 5.3-14 バイオメトリック照合トレーニングシナリオ

(4)バイオメトリック照合試験シナリオ

バイオメトリック照合試験シナリオは、評価対象バイオメトリック装置を用いた 1:1 照合のための本試験を実行することを目的としたシナリオである。本シナリオは、バイオメトリック登録

試験シナリオと同様、メイン部分と照合トランザクション部分、及び照合アテンプト部分で構成される。バイオメトリック照合トレーニングシナリオとの違いは、本シナリオにおいては、評価対象部位すべてに対して規定回数分、照合トランザクションを実行することである。ひとつの部位において規定回数分の照合トランザクションが完了したら、次の部位のバイオメトリック照合トランザクションを実行する。

図 5.3-15 にバイオメトリック照合試験シナリオのフローチャートを示す。本シナリオでは照合トレーニングシナリオと同様、BioAPI_Init、BioAPI_BSPLoad、BioAPI_BSPAttach、BioAPI_BSPDetach、BioAPI_BSPUnload、BioAPI_Terminate、BioAPI_Capture、BioAPI_Process、BioAPI_VerifyMatch、BioAPI_GetBIRFromHandle の 10 種類の BioAPI 関数が呼び出される。

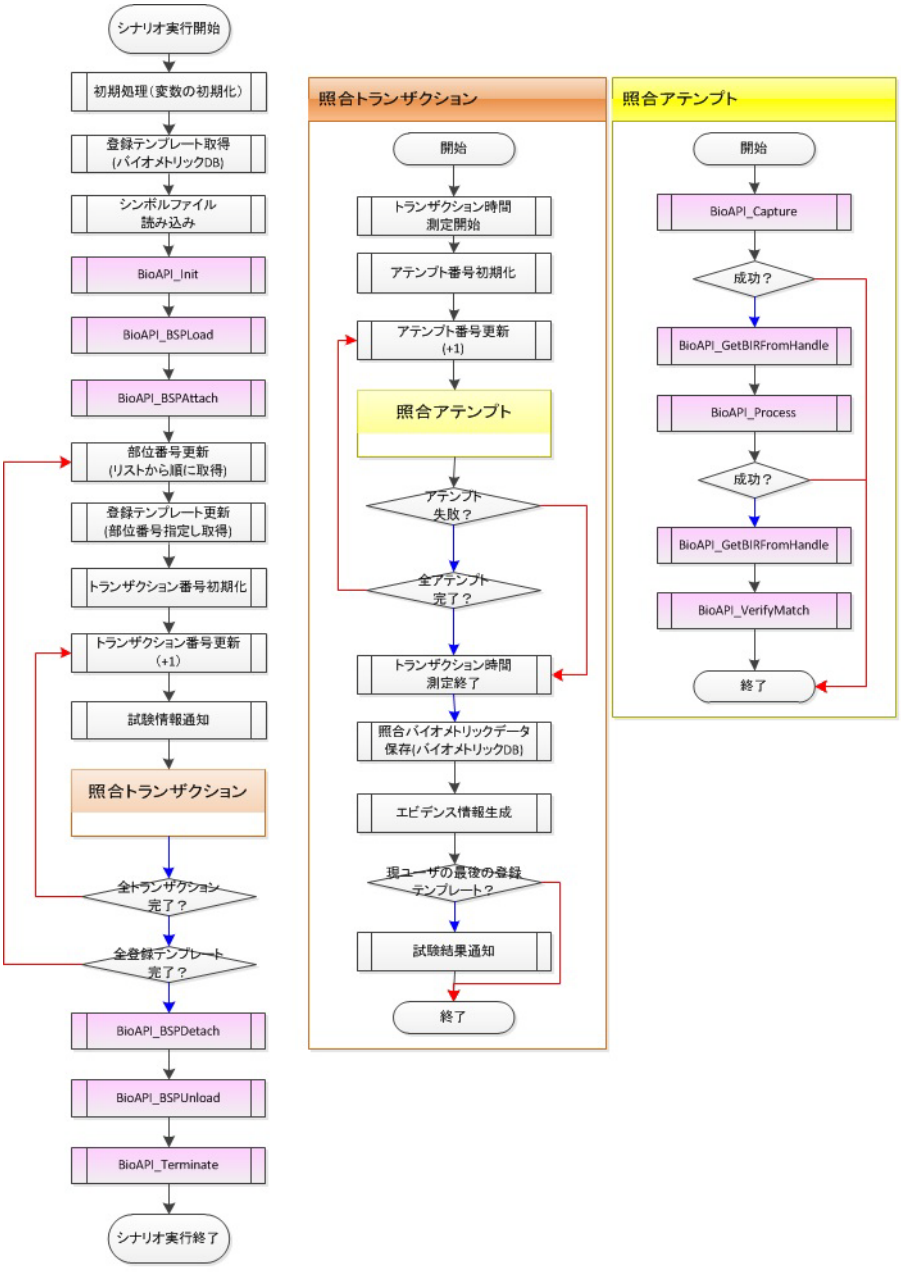


図 5.3-15 バイオメトリック照合試験シナリオ

(5)クロスマッチシナリオ

クロスマッチシナリオは、評価対象バイオメトリック装置を用いたすべての被験者に対する登録試験及び照合試験が終了した後で、評価対象バイオメトリック製品が提供する 1:1 照合機能を用いることにより、他人同士の全件照合（本人の他の部位同士の照合も含む）を実行することを目的としたシナリオである。本シナリオは、バイオメトリック登録試験シナリオと同様、メイン部分と照合トランザクション部分で構成される。

図 5.3-16 にクロスマッチシナリオのフローチャートを示す。本シナリオでは照合トレーニングシナリオと同様、BioAPI_Init、BioAPI_BSPLoad、BioAPI_BSPAttach、BioAPI_BSPDetach、BioAPI_BSPUnload、BioAPI_Terminate、BioAPI_ VerifyMatch の 7 種類の BioAPI 関数が呼び出される。

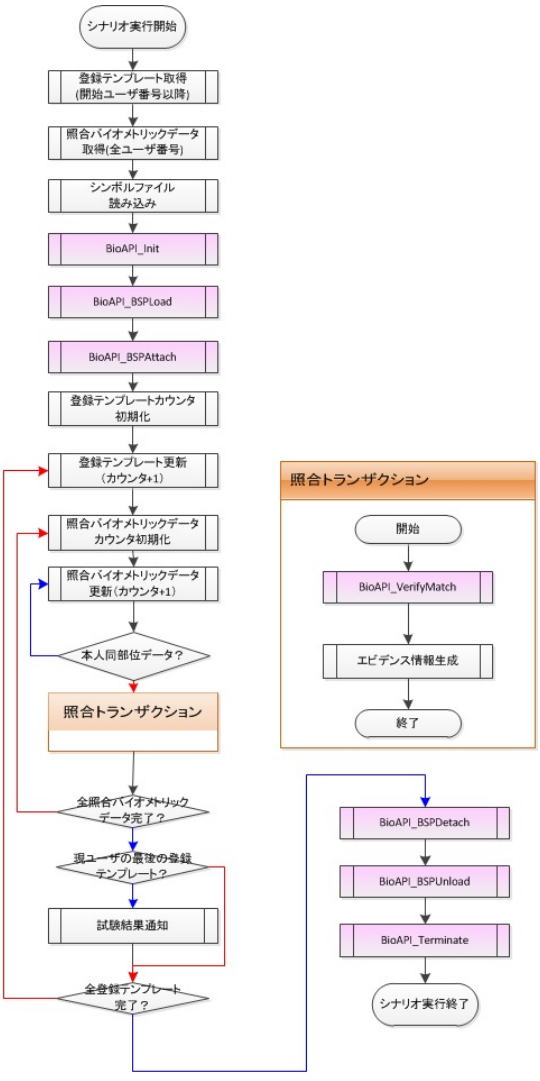


図 5.3-16 クロスマッチシナリオ

5.3.1.11　運用画面

本節では、平成 26 年度に開発した精度評価ツールのプロトタイプにおける運用画面に基づいて、精度評価ツールの操作手順を説明する。

(1)被験者の登録（被験者操作）

被験者は精度評価ツールを使用するにあたり、被験者は精度評価システムの URL にアクセスし、被験者の登録を行う。被験者は、初期画面で表示される[新規登録]ボタンを押下し、表示されるユーザ登録画面でユーザ ID とパスワードを入力する。

なお属性入力の機能は、平成 26 年度開発機能に含まれていない。図 5.3-17 に被験者登録画面の操作例を示す。

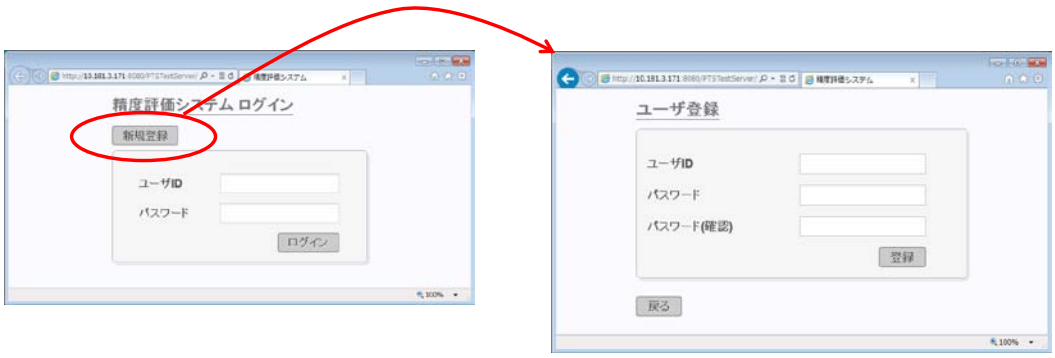


図 5.3-17 被験者登録画面

(2)被験者のログオンと初期画面（被験者操作）

新規登録が完了し評価を開始する際には、被験者は精度評価システムの URL にアクセスし、ログオン操作を行う。ログオンを行うと、その端末に接続されているバイオメトリック装置のための評価用画面が表示される。

画面の上部に精度評価において被験者のバイオメトリック情報のキャプチャが含まれる 4 つのシナリオ（バイオメトリック登録トレーニングシナリオ、バイオメトリック照合トレーニングシナリオ、バイオメトリック登録試験シナリオ、バイオメトリック照合シナリオ）の進行状況が表示される。

あわせて評価対象となる生体部位（指、手のひらなど）がグラフィック機能を用いて表示される。指を扱うバイオメトリック装置であれば、評価対象バイオメトリック装置において評価対象となっている指の部分が赤い色で示される。平成 27 年度以降、手のひらを扱うバイオメトリック装置に対応することにより、手のひら部分が赤い色で示されるようになる。

画面の最下部には、被験者が実行すべきシナリオの名前が付けられたボタンが表示される。被験者が最初に実行するシナリオは、バイオメトリック登録トレーニングシナリオである。

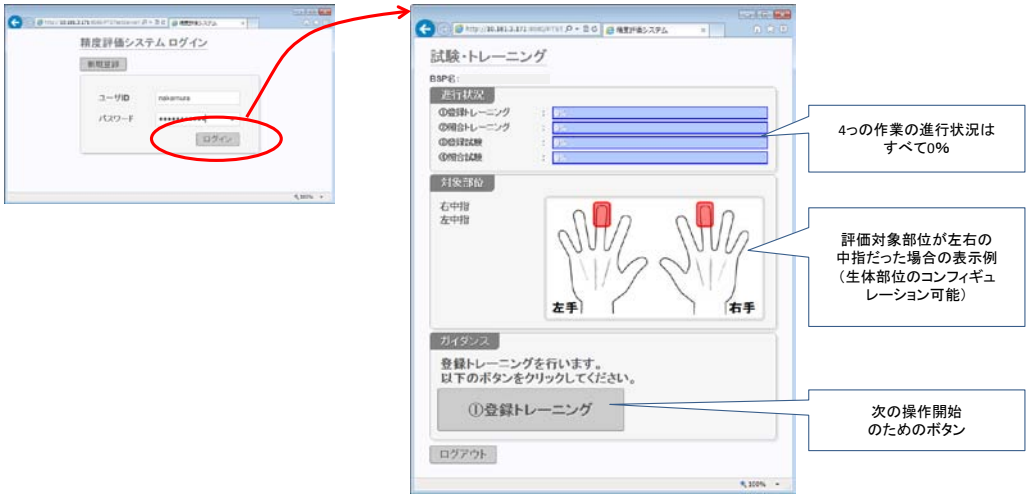


図 5.3-18 被験者登録画面

(3)管理者のログオン（管理者操作）

管理者が精度評価システムを使用する場合、管理者はブラウザから精度評価システムの管理者用 URL にアクセスする。精度評価システムにあらかじめ確保されている管理者用アカウントを使用してログオンを行う。

すると管理者用初期画面が表示される。管理者は本画面を用いることにより以下の操作を実行することができる。

① 試験全体の進捗状況の把握

② 被験者ごとの進捗状況の把握

③ クロスマッチの実行

④ 精度評価値（FTE、FRR、FAR）の算出

図 5.3-19 に管理者ログオン及び初期画面例を示す。

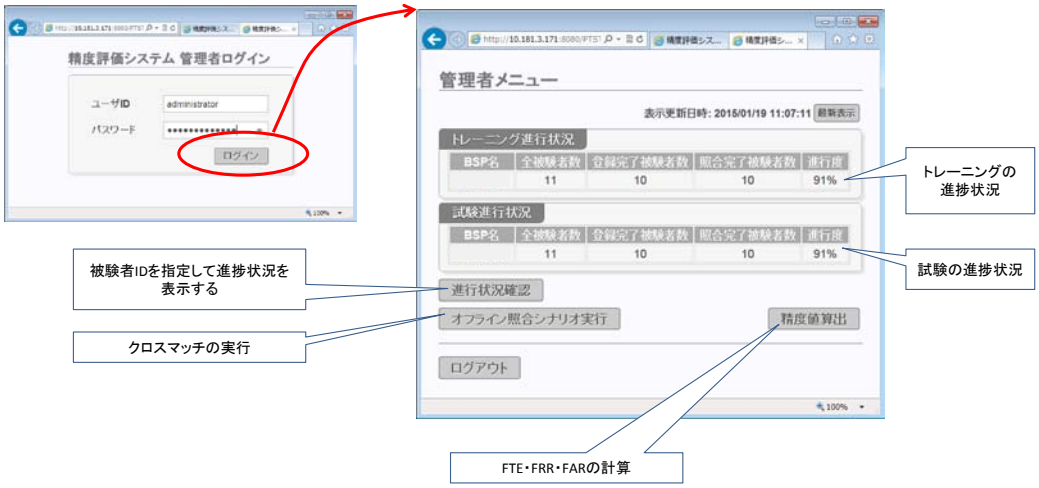


図 5.3-19 管理者ログオン及び初期画面

(4)バイオメトリック登録試験の実行（被験者操作）

被験者が行うバイオメトリック登録試験実行時の手順を説明する。（バイオメトリック登録トレーニング手順は、バイオメトリック登録試験手順に類似するため省略する。）

被験者はログオン後の初期画面において画面下部に表示される[登録試験]ボタンを押下する。すると登録試験シナリオが実行され、結果的にバイオメトリック登録トランザクションを開始するための画面が表示される。この画面では、バイオメトリック登録対象となる生体部位があらかじめ精度評価ツールにより選択されており、グラフィック画面において赤い色に着色されて表示される。管理者の指示のもと、被験者は示された部位を用いたバイオメトリック登録を、画面上の[開始]ボタンを押下することにより開始する。ボタンを押下するとただちに登録トランザクションが実行され、評価対象バイオメトリック製品が提供するキャプチャのための関数が呼び出される。あわせて、何らかの画面表示（あるいは音声ガイドなど）が行われるため、被験者はそのガイドの指示及び管理者の指示にしたがって、評価対象バイオメトリック装置を用いて指定された部位のキャプチャを行う。キャプチャが完了すると、登録トランザクション処理が先に進み、最終的にバイオメトリック登録の成功、あるいは、失敗の結果が画面上に表示される。この画面を見て、被験者は管理者のガイダンスに従って次のアクションを実施する。バイオメトリック登録試験においては、このような登録トランザクションが決められた回数繰り返される。なお精度評価ツールは、バイオメトリック照合トレーニングシナリオの実行と、バイオメトリック登録試験シナリオの実行の間に一定の時間が経過したかどうかをチェックする。両者の時間間隔が一定時間以内だった場合、被験者に対して、規定時間以上待つことを求める。

図 5.3-20 にバイオメトリック登録試験の画面及び操作手順の例を示す。

図 5.3-20 バイオメトリック登録試験の画面及び手順例

(5)バイオメトリック照合試験の実行（被験者操作）

被験者が行うバイオメトリック照合試験実行時の手順を説明する。（バイオメトリック照合トレーニング手順は、バイオメトリック照合試験手順に類似するため省略する。）

被験者は登録試験後の初期画面において画面下部に表示される[照合試験]ボタンを押下する。すると照合試験シナリオが実行され、結果的にバイオメトリック照合トランザクションを開始するための画面が表示される。この画面では、バイオメトリック照合対象となる生体部位があらかじめ精度評価ツールにより選択されており、グラフィック画面において赤い色に着色されて表示される。管理者の指示のもと、被験者は示された部位を用いたバイオメトリック照合を、画面上の[開始]ボタンを押下することにより開始する。ボタンを押下するとただちに照合トランザクションが実行され、評価対象バイオメトリック製品が提供するキャプチャのための関数が照合アテンプト内から呼び出される。あわせて、何らかの画面表示（あるいは音声ガイドなど）が行われるため、被験者はそのガイドの指示及び管理者の指示にしたがって、評価対象バイオメトリック装置を用いて指定された部位のキャプチャを行う。キャプチャが完了すると、照合トランザクション処理が先に進み、最終的にバイオメトリック照合の成功、あるいは、失敗の結果が画面上に表示される。この画面を見て、被験者は管理者のガイダンスに従って次のアクションを実施する。バイオメトリック照合試験においては、このような照合トランザクションが決められた回数繰り返される。なお精度評価ツールは、バイオメトリック登録試験シナリオの実行と、バイオメトリック照合試験シナリオの実効の間に一定の時間が経過したかどうかをチェックする機能を実現する予定である。

これは、両者の時間間隔が一定時間以内だった場合、被験者に対して、規定時間以上待つことを求めるものである。

図 5.3-21 にバイオメトリック照合試験の画面及び操作手順の例を示す。

図 5.3-21 バイオメトリック照合試験の画面及び手順例

(6)クロスマッチの実行（管理者操作）

精度評価に参加するすべての被験者のバイオメトリック登録試験及びバイオメトリック照合試験が終了したら、管理者は他人受け入れ率を評価するためにクロスマッチを実行する。これは、管理者でログオン後に表示される管理者用初期画面において、[オフライン照合シナリオ]ボタンを押下することで開始する。

図 5.3-22 に示す画面例の手順に従うことにより、クロスマッチの進行状況を示すステータスバーが画面上に表示され、クロスマッチ処理がすべて終了すると、完了画面が表示される。

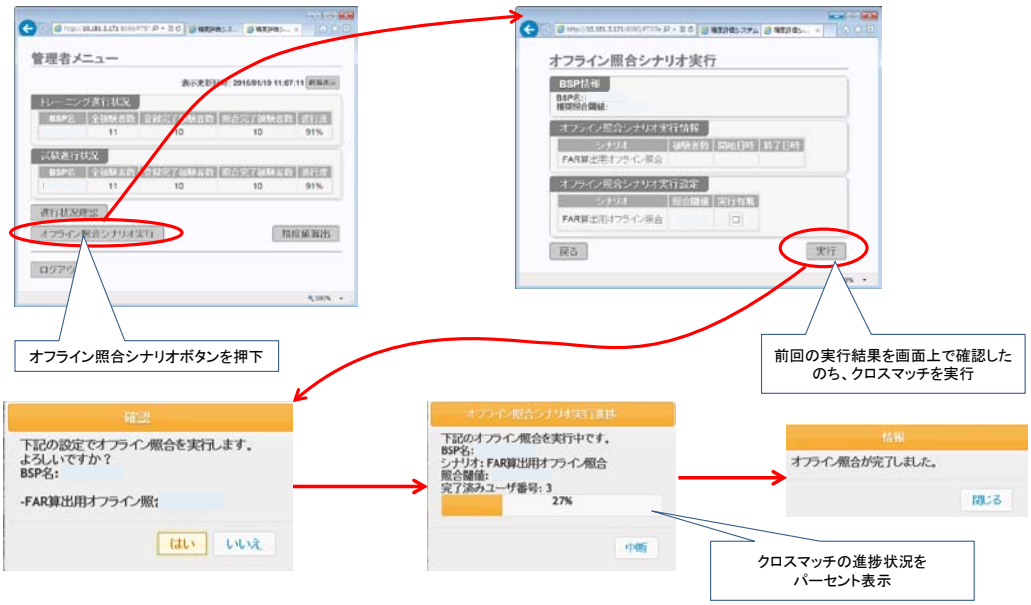


図 5.3-22 クロスマッチ画面例

(7)精度評価値の計算（管理者操作）

精度評価に参加するすべての被験者のバイオメトリック登録試験及びバイオメトリック照合試験、及び、クロスマッチが終了したら、管理者は評価対象バイオメトリック製品の精度値を計算するための機能を実行する。

図 5.3-23 に示す画面例の手順に従うことにより、登録失敗率を表す FTE（Failure To Enroll）、本人拒否率を表す FRR（False Rejection Rate）、他人受け入れ率を表す FAR（False Acceptance Rate）が画面上に表示される。

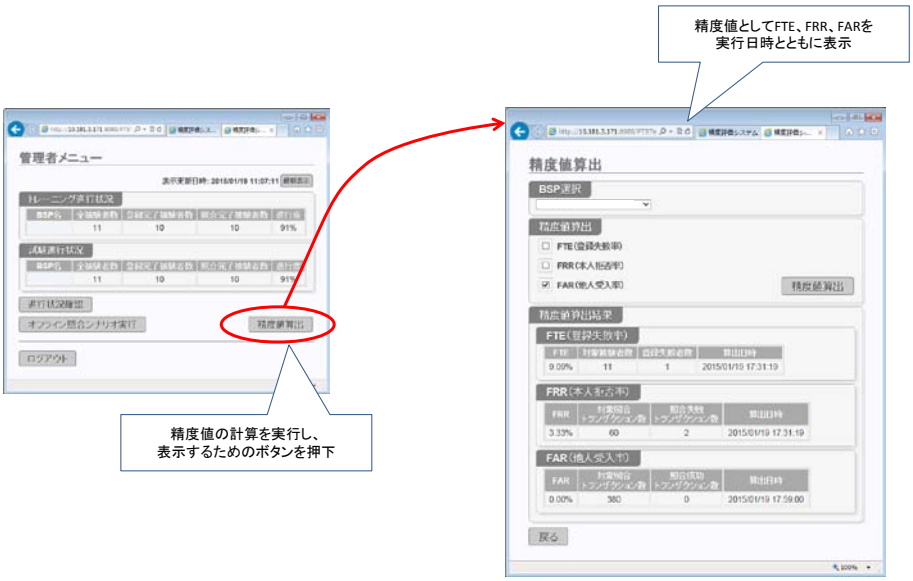


図 5.3-23 クロスマッチ画面例

5.3.2 精度評価のためのサポート文書開発

本節は、CC 認証におけるバイオメトリック製品の精度評価を、バイオメトリック・ベンダーあるいは独立評価機関が実施するにあたり、評価のガイドラインとなるべきサポート文書案としてまとめたものである。

5.3.2.1 精度評価の分類

本節では、バイオメトリクスにおける精度評価の分類を説明するとともに、本ガイドラインで取り扱う精度評価について述べる。

(1) 精度評価方法

バイオメトリック製品の精度評価には、テクノロジ評価・シナリオ評価・運用評価の 3 種類の方法が存在する。3 つの方法の概要を以下に説明する。(3 つの評価方法の詳細については、ISO/IEC 19795-1: Information Technology – Biometric performance testing and reporting – Part 1: Principles and framework を参照のこと。)

1)テクノロジ評価

バイオメトリック・アルゴリズムの認証精度を評価することを目的とした評価方法であり、事前にバイオメトリック装置でキャプチャ済みのバイオメトリック・データをデータベース上に保持しておき、これをバイオメトリック・アルゴリズムで照合する際の認証精度を評価するものである。

2)シナリオ評価

バイオメトリック装置及びバイオメトリック・アルゴリズムを含んだバイオメトリック・システ

ムのための評価方法であり、被験者を集めてバイオメトリック・テンプレートの登録を行った上で、同一あるいは異なる被験者がバイオメトリック照合を実行することによって精度評価を行うものである。シナリオ評価では、想定シナリオを設定し、これにあわせてアプリケーションや被験者、運用環境を準備して評価を行う。

3)運用評価

運用アプリケーションを含んだバイオメトリック・システムにおける精度評価である。実際に使用する運用アプリケーションを用い、実際に用いられる環境にバイオメトリック・システムを設置し、実際の被験者を集めて評価を行う。

5.3.2.2 本サポート文書案で取り扱う範囲

本サポート文書案において取り扱うバイオメトリック精度評価の範囲は以下のとおりとする。

(1)評価方法：シナリオ評価（テクノロジ評価、運用評価は対象外とする）

(2)認証方法：1:1 照合（1:N 照合は対象外とする）

(3)評価単位：トランザクション単位（アテンプト単位、マッチング単位は対象外とする）

(4)評価尺度：FAR、FRR、FTE（FMR, FNMR,FTA などは対象外とする）

5.3.2.3 精度評価実施時の基本方針

本サポート文書案では、精度評価実施における基本方針を以下のとおり定める。

(1)製品が扱う生体の部位ごとに一つの ID を割当ててよい。(例えば左右の手が生体の部位であれば、ひとりの被験者あたり最大 2 つの ID を割当てられる。指であればひとりの被験者あたり最大 10 の ID を割り当てられる。)

(2)上記(1)で述べたそれぞれの部位におけるサンプル数は、登録テンプレート、1:1 照合バイオメトリック・データともに最大 1 枚とする。

(3)FTE の算出は、評価対象製品を用いた登録トランザクションを実行することで算出する。被験者ひとりの各評価対象生体部位あたりのトランザクション実行回数をあらかじめ設定し、規定回数分登録トランザクションを実行する。そのうち一度でもバイオメトリック登録に成功した場合、その部位については登録が成功したこととする。規定回数すべてに失敗した場合、その部位の登録は失敗とする。トランザクションの規定回数の推奨値は 3 とする。

(4)FRR の算出は、評価対象製品を用いた本人の同一部位同士の 1:1 照合トランザクションを実行することで算出する。被験者ひとりの各評価対象生体部位あたりのトランザクション実行回数をあらかじめ設定し、規定回数分 1:1 照合トランザクションを実行する。そのうち一度でもバイオメトリック照合に成功した場合はその部位については照合が成功したこととする。規定回数すべてに失敗した場合、その部位の照合は失敗とする。トランザクションの規定回数の推奨値は 3 とする。

(5)FAR の算出は、前述の FTE 評価で収集した登録テンプレートを各被験者の各部位からひとつ選択し、FRR 評価で収集した照合用バイオメトリック・データを各被験者の各部位からひとつ選択する。このように選択した、被験者の各部位ごとにひとつずつの登録テンプレートと 1:1 照合バイオメトリック・データを被験者全員分集めたデータを全件照合することにより求める。

(6)FTE、FRR、FAR を算出する際の信頼度は、原則として 3 のルール及び 30 のルールを用いる。これ以外の方法を用いる場合、その内容の詳細をレポートに含めなければならない。

(7)FTE、FRR、FAR の評価においては、ベンダーが定めるアルゴリズムの閾値を固定する。特に、FRR 評価と FAR 評価で異なる閾値を用いてはならない。

5.3.2.4 精度評価レポートの全体構成

本章では、精度評価実施後に作成する評価レポートの全体構成を示す。精度評価レポートは原則として以下の 5 つの項目により構成されることとする。

(1)基本情報

対象製品及び精度評価に関する概要情報である。製品情報（製品名、機能要約、想定用途、想定されるシステム構成)、評価者情報（精度評価実施者あるいは評価機関名）などを記述する。

(2)評価データ

評価に用いるバイオメトリック・データに関する記述である。見込み精度と必要な被験者数、データ収集条件、実際の被験者数及び被験者の構成（性別、年齢など）などを記述する。

(3)評価結果

精度評価を行った評価結果を記述する。FAR・FRR・FTE、未対応情報、限界精度などを記述する。必要に応じて ROC カーブも記述する。

(4)その他の報告事項

評価実施組織への連絡先に関する情報や認証書の送付先などを記述する。精度評価に関して特段の報告事項があれば自由記述形式で記述する。

5.3.2.5 レポート詳細

本章では、前節で示した精度評価レポートの概要に基づき、各項目の詳細を示す。

(1)基本情報

実施したバイオメトリック精度評価に関する概要情報であり、評価対象製品を特定する情報、及び、精度評価の概要に関する情報が含まれる。

①評価対象製品

・ベンダー名

・アルゴリズム名

・バージョン番号

・モダリティ（指紋、顔、虹彩、静脈、署名、声紋、DNA など）
・人体の部位名称（手、指、顔、目など）
・部位の数（精度評価の対象となる指の本数、目の数など）
・照合方式（1:1 照合のみ）
・しきい値（推奨値、最小値、最大値）
②評価者
・精度評価実施組織名
③評価条件
・実施期間
・被験者数

(2)評価データ情報

精度評価に使用したバイオメトリック登録テンプレートの数やフォーマットなど評価データに関する情報について記述する。

①見込み精度

FAR・FRR・FTE の 3 つの性能指標において、推奨しきい値において対象製品が見込んでいる精度値を記載する。

②被験者募集方法及び募集条件
・被験者の募集方法を記載する。
例）募集先：社内従業員による募集、あるいは、被験者募集機能を持つ独立した企業のサービスを使用した募集、など。
・募集条件：性別、年齢、職業、人種などの募集条件。

③バイオメトリック・データ数

評価対象のバイオメトリック製品が取り扱う被験者一人当たりのバイオメトリック・データ数、見込み精度を満足するために必要なバイオメトリック・データ数、及び、実際に評価を行った際に集めたバイオメトリック・データ数を記載する。

記載例を以下に示す。

・一人当たりのバイオメトリック・データ数：該当製品において被験者一人あたりに取得可能な最小バイオメトリック・データ数及び最大バイオメトリック・データ数。
・必要なバイオメトリック・データ数：上述の見込み精度に対して、3 のルール及び 30 のルールを適用した場合に必要となるバイオメトリック・データ数。
・実際のバイオメトリック・データ数：精度評価に参加した被験者から取得したバイオメトリック・データ数。

④実際の被験者の分布

精度評価に参加した実際の被験者の分布情報を記載する。詳細評価、簡易評価ともに記載義務はないが、詳細評価では記載することが推奨される。

性別分布：被験者の男女分布である。

年齢分布：被験者の年齢分布を 20 歳かそれより細かい刻みで記載したものである。

職業分布:被験者を職業別に分類し､分布を集計したものである｡職業の分類方法はモダリティへの依存性を考慮することが推奨されるが、具体的な分類方法はベンダーの判断に任せることとする。

人種分布：被験者を人種別に分類し、分布状況を集計したものである。人種の分類方法はモダリティへの依存性を考慮することが推奨されるが、具体的な分類方法はベンダーの判断に任せることとする。

⑤バイオメトリック装置情報

バイオメトリック・データの収集を行ったバイオメトリック装置に関する情報を記載する。

・ベンダー名：センサーを製造したベンダー名を記載する。

・製品情報：センサーの製品情報として製品名やモデル名など製品を識別可能な情報を記載する。

⑥データ収集環境

データ収集環境として対象となるモダリティにおいてデータ取得に影響すると考えられるデータ収集環境を記述する。

・温度：データ取得が行われた場所の温度環境として最低温度、最高温度、平均温度を記載する。（室内で実施した場合、室内温度を記載する。）

・湿度：データ取得が行われた場所の湿度環境として最低湿度、最高湿度、平均湿度を記載する。（室内で実施した場合、室内湿度を記載する。）

・環境光：データ取得が行われた場所の光環境として、製品が関係する波長帯近傍の照度に着目し最低照度、最高照度、平均照度を記載する。

・ノイズ（音）：データ取得が行われた場所のノイズ環境として、製品が関係する波長帯近傍のノイズに着目し最低ノイズレベル、最高ノイズレベル、平均ノイズレベルを記載する。

⑦シナリオ実行条件

シナリオ実行時の被験者への事前説明やガイダンスの有無などを記載する。

・被験者への事前説明状況：バイオメトリック・データを取得する際に、被験者に対する事前説明が行われたかどうかを記載する。説明が行われた場合、その内容を記載する。

・被験者の習熟度：バイオメトリック・データを取得する際の、被験者全体の平均的な習熟度である。バイオメトリック・データを取得した経験がない被験者は習熟度が低いこととし、生体情報の登録と照合の事前練習をしたうえで取得した被験者は習熟度が高いこととする。この中間状態も考慮した上で、被験者全体の平均的な習熟度を記載する。

・被験者へのガイダンス：バイオメトリック・データを取得する際に被験者が何らかの取得エラーを発生した場合、エラーを解決するために行う何らかの指示をガイダンスと呼ぶ。このガイダンスの実施有無、及び実施したガイダンス内容を記載する。

(3)評価結果

実施した精度評価の結果の記載内容について説明する。

(a)照合性能

①精度算出用データ

精度評価値を算出するにあたり、算出の根拠となるデータである。詳細評価、簡易評価ともに記載義務がある。

・被験者総数：評価に参加した被験者の総数を記載する。

・登録テンプレート数：データベースに格納されている登録テンプレート数を記載する。被験者一人当たり、各部位について最大 1 つ存在する。

・照合バイオメトリック・データ数：データベースに格納されている照合バイオメトリック・データ数を記載する。被験者一人当たり、各部位について最大 1 つ存在する。

・FAR 算出用 1:1 マッチング件数：異なる被験者間の、あるいは、同一の被験者の異なる部位間の、登録テンプレートと照合バイオメトリック・データの 1:1 マッチングを行った件数を記載する。あわせて、マッチング件数を算出した根拠となる計算式などの情報を記載する。

・FAR 算出用 1:1 マッチングでの誤認識発生件数：推奨しきい値において、FAR 算出用 1:1 マッチングにおける誤認識発生件数（誤ってアクセプトした件数）を記載する。

・FRR 算出用 1:1 照合トランザクションセット件数：同一被験者の同一部位間の 1:1 照合トランザクションの規定回数分の実行を 1 回のセットと数えた場合の、総 1:1 照合トランザクションセット件数を記載する。

・FRR 算出 1:1 マッチングでのリジェクト発生件数：推奨しきい値において、FRR 算出用 1:1 照合トランザクションセットにおいて、すべてのトランザクションで照合に失敗した場合の件数を記載する。

・アルゴリズムしきい値：精度を算出した際のアルゴリズムのしきい値を記載する（推奨しきい値であることが望ましい）。

②認証精度値

精度算出用データに基づいて算出された精度値である。詳細評価、簡易評価ともに記載義務がある。

・FAR 値（他人受け入れ率）：評価に用いたアルゴリズムしきい値において、FAR 算出用 1:1 マッチング件数と FAR 算出用 1:1 マッチングでの誤認識発生件数から算出される FAR 値を算出式とともに記載する。

・FAR 限界精度：誤認識発生件数からリジェクト発生件数から 3 のルールあるいは 30 のルールを適用した場合の限界精度を記載する。3 のルール、30 のルール以外の計算方法を使用する場合は、計算方法の詳細を根拠とともに記述する。

・FRR 値（本人拒否率）：評価に用いたアルゴリズムしきい値において、FRR 算出用 1:1 トランザクションセット件数と FRR 算出用 1:1 照合トランクションセットでのリジェクト発生

件数から算出される FRR 値を算出式とともに記載する。

・FRR 限界精度 : リジェクト発生件数から 3 のルールあるいは 30 のルールを適用した場合の限界精度を記載する。3 のルール、30 のルール以外の計算方法を使用する場合は、計算方法の詳細を根拠とともに記述する。

・ROC カーブあるいは DET カーブ：必要に応じて、上記の FAR 及び FRR 値を最小しきい値、最大しきい値、最小しきい値と推奨しきい値の中間、最大しきい値と推奨しきい値の中間などで算出することにより、ROC カーブあるいは DET カーブを生成し、グラフ化する。

(b)登録性能

認証精度値とあわせてベンダーは登録に関する精度値として、バイオメトリック・データ取得時に算出する登録失敗率を報告する。

・登録を試みた被験者数：登録テンプレート生成のためのバイオメトリック･データ取得に参加した被験者の総数を記載する。

・総登録トランザクションセット数 : 被験者が実行した登録トランザクションセット（規定回数分の登録トランザクション）の総数を記載する。一般的に、被験者の数に登録対象部位の数を掛けた数が総登録トランザクションセット数となる。

・総登録失敗数 : 登録作業において実行された登録トランザクションセットにおいて、バイオメトリック登録ができなかった場合の総数を記載する。

・FTE 値（登録失敗率）: 総登録トランザクションセット数と総登録失敗数から算出される FTE 値を記載する。あわせて、FTE 値を算出した根拠となる計算式などの情報を記載する。

・FTE 限界精度： 登録失敗件数から 3 のルールあるいは 30 のルールを適用した場合の限界精度を記載する。3 のルール、30 のルール以外の計算方法を使用する場合は、計算方法の詳細を根拠とともに記述する。

(c)その他報告事項

その他報告事項として、ベンダーの連絡先情報や、精度評価に関する自由記述を記載する。

・担当者連絡先 : 本報告書の担当者の所属、住所、電話番号、メールアドレスなどを記載する。

・認証書の送付先：認証書の発行先住所、宛名、電話番号などを記載する。

・自由記述：評価実施時の特記事項や、認証機関への連絡事項を記載する。

5.3.3　脆弱性評価手法の研究

5.3.3.1 研究動向調査（IJCB2014）

海外における関連分野の研究動向調査として、IJCB2014 (International Joint Conference of Biometrics 2014) に参加した。ここではその調査結果について報告する。

(a)IJCB2014 開催概要

IJCB2014 は IEEE 及び IAPR が共催する国際会議であり、生体認証分野のトップカンファレンスである ICB(International Conference on Biometrics、IAPR 主催)と BTAS(Biometrics, Theory, Applications and Systems、IEEE 主催)が 3 年に 1 度合同で開催する国際会議である。今年度は平成 26 年(2014 年)9 月 29 日～10 月 1 日の日程で、米国フロリダ州クリアウォーター、Sheraton Sand Key Resort にて開催された。大学・企業・研究機関・政府組織から計 200 名を超える参加者があり、4 日間に渡り生体認証に関して、研究成果から社会展開に渡り様々な観点から最新の成果が報告された。

(b)IJCB2015 投稿論文から見る生体認証分野の研究動向

今年度は米国、ヨーロッパ、日本、中国、韓国をはじめとした 261 件の投稿があり、21 人の領域チェア、150 人の査読者による査読により 80 件が採択された（うち口頭発表 25 件、ポスター発表 55 件)。5.3.3-1 は分野別の採択論文数、また図 5.3.3-2 は IJCB2011(2011 年開催)からの分野別投稿論文数の推移を示したものである。2011 年と比較すると、依然として顔認証が多くの割合を占めていることがわかるが、それ以外の顕著な傾向として、本事業に関連が深いなりすまし対策に関する研究成果の増加が見て取れる。関連分野への国際的な注目の高さが伺える。この要因としては、ISO/IEC 30107 の開発をはじめとして、国際的に高度ななりすまし攻撃対策技術への需要が高まっている点に加え、ここ数年で、伊カリアリ大、米クラークソン大を中心とした LivDet（指紋なりすまし評価コンテスト）[7]や、Idiap Research を中心とした欧州 FP7 プロジェクト Tabura Rasa[8]のなりすまし攻撃対策への取り組み等において多くのなりすまし攻撃対策技術評価用データベースが開発され、アルゴリズムの評価環境が整いつつあることなどが挙げられる。本会議においても携帯端末を用いた虹彩認証におけるなりすまし攻撃対策技術の評価コンテスト MobILive2014[9]が開催された。

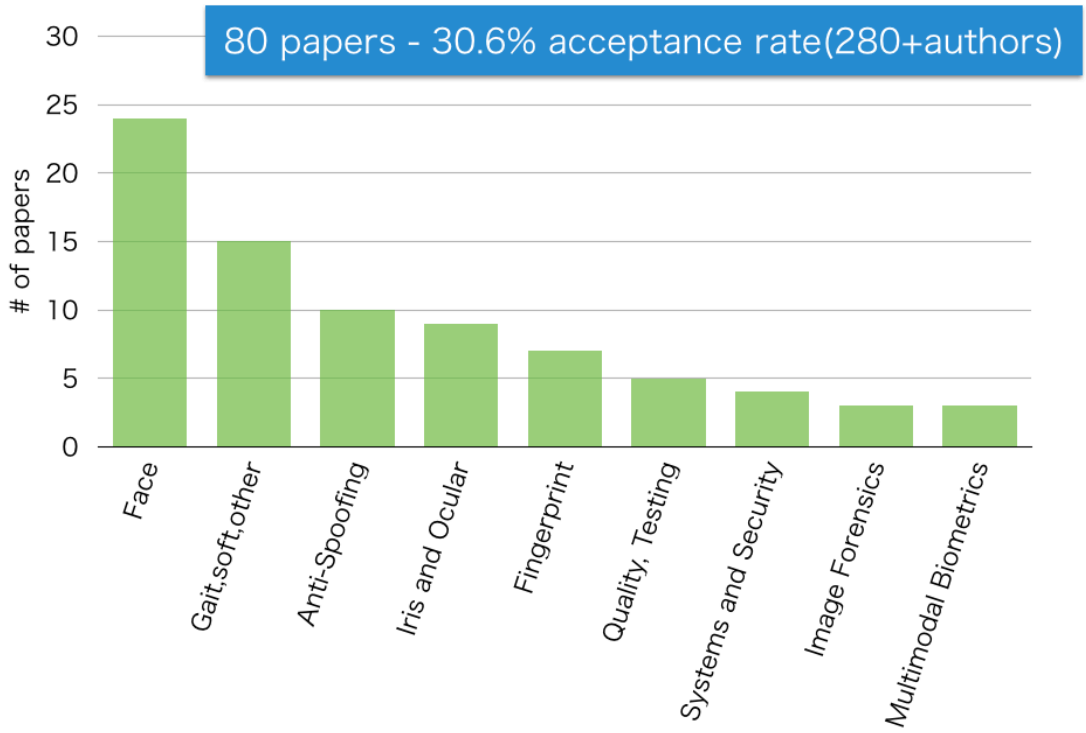


図 5.3.3-1　IJCB2014 分野別の採択論文数

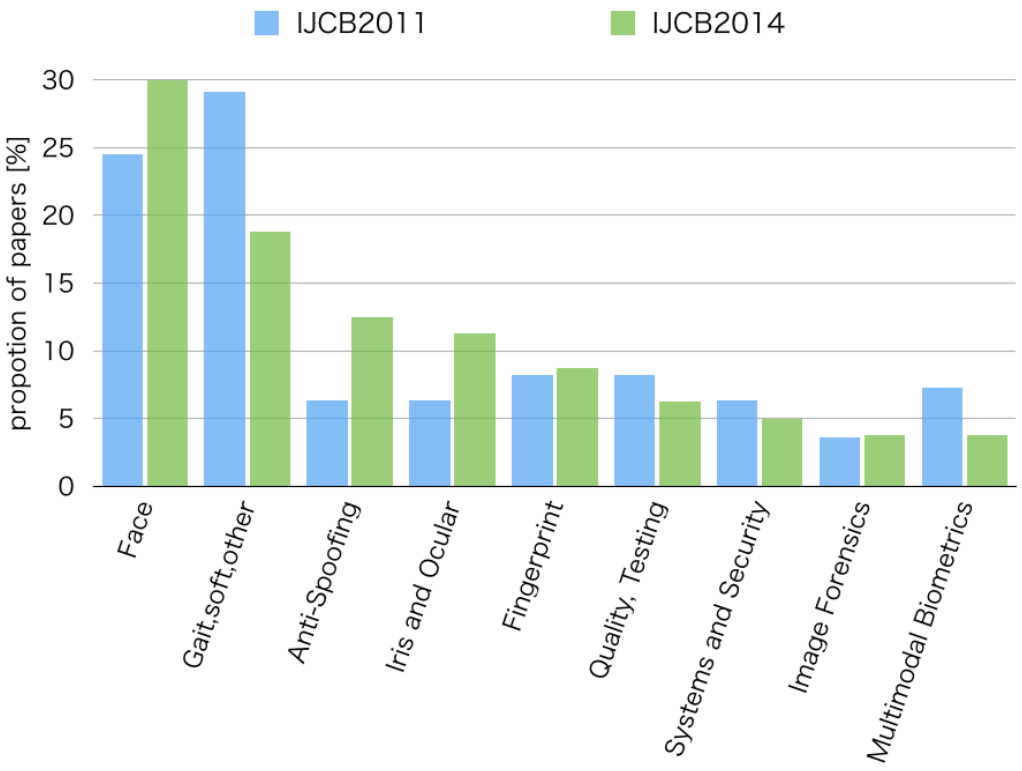
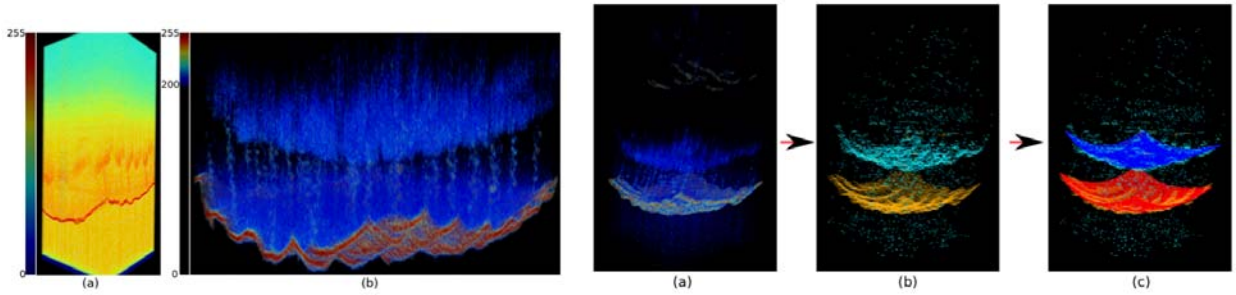


図 5.3.3-2　IJCB2011 と IJCB2014 での分野別発表数の推移

(c)関連研究(1)：Ctirad Sousedik, Christoph Busch “Quality of Fingerprint Scans captured using Optical Coherence Tomography (NISlab, Gjøvik University College) [6]

Gjøvik 大学のグループによる本発表は、指紋認証システムに対するなりすまし攻撃対策として、OCT(Optical Coherence Tomography) を用いて指紋表面のレイヤ構造を解析する方式を提案している（図 5.3.3-3(1),(2)）。OCT による指紋の 3 次元画像取得においては、撮影に数秒の時間がかかることから被験者の動きによる取得画像への影響が大きな問題となる。このため、本提案では取得画像の品質評価手法を提案することで、手ぶれ等の影響の大きい画像と比較的影響の少ない画像を弁別することを可能としている（図 5.3.3-3(3)）。



(1) OCT 画像による偽造指紋の判定

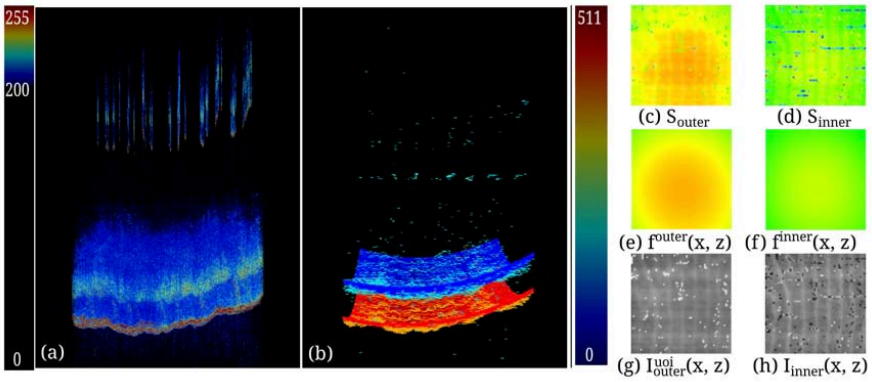
(a) ヒートマップによる可視化

(b) OCT スキャン画像

(2) 指紋と偽造物のレイヤ構造のロバストな検出

(a) OCT スキャン画像 (b) 二層レイヤ候補点の検出

(c) 候補点に基づくレイヤの平滑化



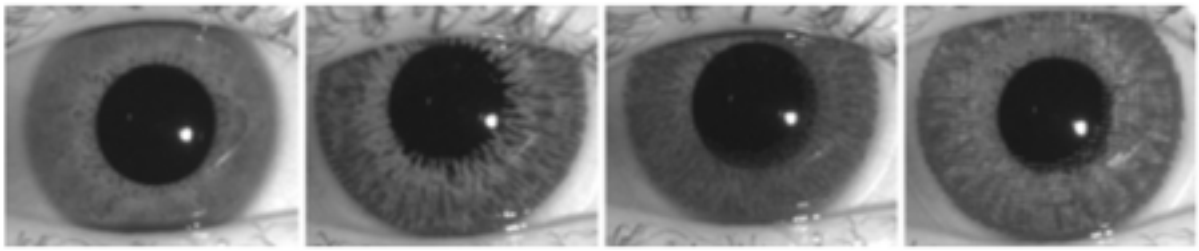
(3) OCT スキャン品質推定（手ぶれが少ない場合）

図 5.3.3-3 (1)～(3) OCT 画像による高精度な偽造物判定技術[6]

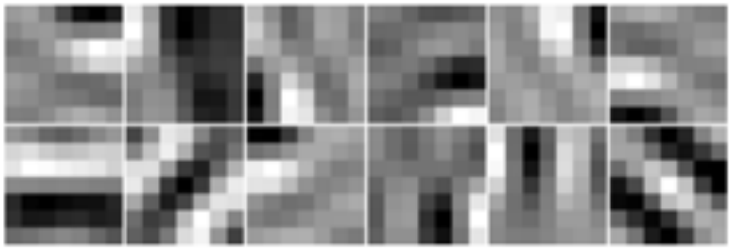
(d)関連研究(2)：Generalized textured contact lens detection by extracting BSIF description from Cartesian iris images (Jukka Komulainen, Abdenour Hadid, Matti Pietikainen, University of Oulu)[10]

虹彩認証システムへのなりすまし攻撃手段として、加工したコンタクトレンズを用いる手法が多く提案されている。これらへの対策としてレンズ表面のテクスチャパターンを判別することで偽造を検知する手法が提案されているが、従来の提案はいずれも特定のテクスチャパターンを判定するものであり、未知のテクスチャパターンへの対応が困難であった。そこで、本提案では生体から得た虹彩情報に基づき作成した 7x7 BSIF フィルタ（図 5.3.3-4 参照）を用いることで、テ

クスチャの種類に依らず、生体から得た虹彩情報と加工したコンタクトレンズから得られた虹彩情報とを判別可能とする手法を提案している。なお、本発表は全体から 4 件選出された Best Reviewed Paper Award のうち 1 件であった。



(a) Live　(b) Cooper Vision　(c) Johnson&Johnson　(d) Ciba Vision



(e) BSIF filter size of 7 x 7 learned from natural images

図 5.3.3-4　偽造虹彩の例(a)～(d) と偽造物検知フィルタ(e)
(a)は生体画像，(b)～(d)はそれぞれ Cooper Vision, Johnson&Johnson, Ciba Vision のコンタクトレンズに偽造虹彩パターンを印刷したもの，(e)は偽造物検知用 BSIF フィルタのパターン

5.3.3.2 生体認証システムのウルフ安全性評価手法に関する研究[13]

生体認証の安全性評価基準として古くから利用される FAR(他人受入率)は、なりすましを行う攻撃者が、攻撃者自身の生体情報を利用することを前提とした場合の、認証システムの平均的な誤受入率を評価することができる。しかし現実には、攻撃者は自身の生体情報のみならず、環境条件や認証アルゴリズム等を考慮して、より攻撃に適した生体情報を偽造物等により作成・入力することが可能である。このような仮定の下での安全性評価基準として、宇根らはウルフ攻撃確率(WAP)を提案している[11]。ウルフ攻撃は多数の登録ユーザに対して誤一致を引き起こすような入力情報（偽造物を含む）であるウルフを用いたなりすまし攻撃である。図 5.3.3-5 にウルフ攻撃の概念を示す。ウルフを含んだ認証システムの安全性評価を行うためには、平均的な誤受入率である FAR の評価に加えて、攻撃者の生体情報だけでなく、偽造物までも入力情報として考慮した際のなりすまし成功確率を WAP として評価するべきである。

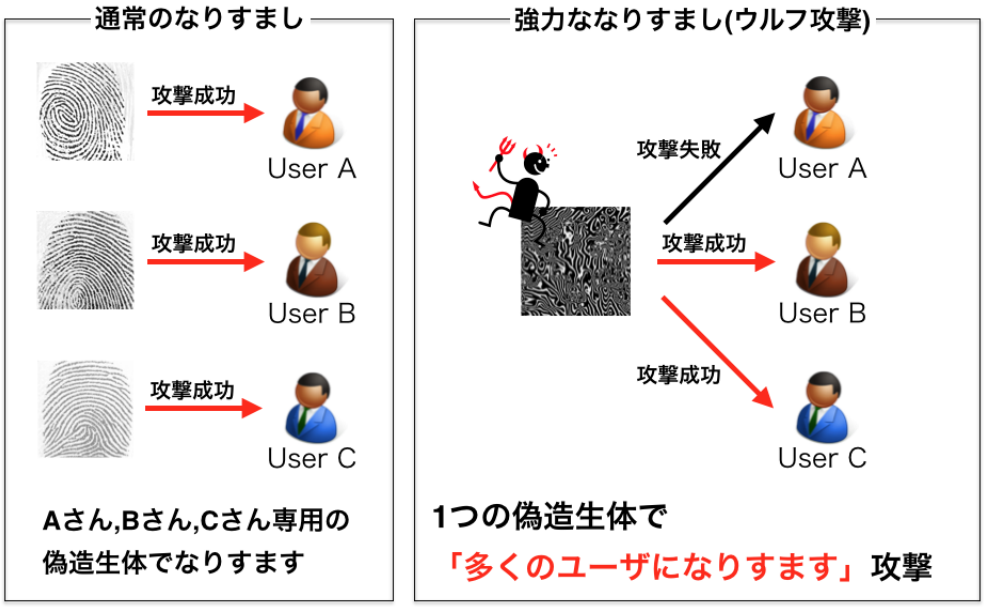


図 5.3.3-5　ウルフ攻撃の概要（指紋の例）

これまで行われてきた生体認証アルゴリズムに対するウルフ安全性評価としては、虹彩や指静脈[12]、また話者照合方式[13]に関する評価がある。これらのウルフ攻撃はいずれも特定のモダリティ・アルゴリズムの脆弱性を利用したものであった。本年度の事業では、特定のモダリティを想定せず、類似度に基づく本人判定手法として尤度比判定方式を用いる生体認証システムを対象とし、その脆弱性とウルフ安全性について評価を行った。さらに、尤度比に基づく生体認証方式の一例である GMM-UBM 話者照合方式に対して、ATR 多数話者音声データベースを用いたウルフ安全性評価を行い、これにより EER(等誤り率)が 0.9%の照合システムに対して WAP が 60%以上の確率で攻撃が可能なウルフが存在することを示した。本研究で提案したウルフ攻撃手法は、尤度比を類似度判定方式として利用する生体認証方式であれば、どのようなモダリティにも適用が可能であり、今後、本成果を用いることでさらに一般的な生体認証システムのウルフ安全性評価が可能となることが期待できる。

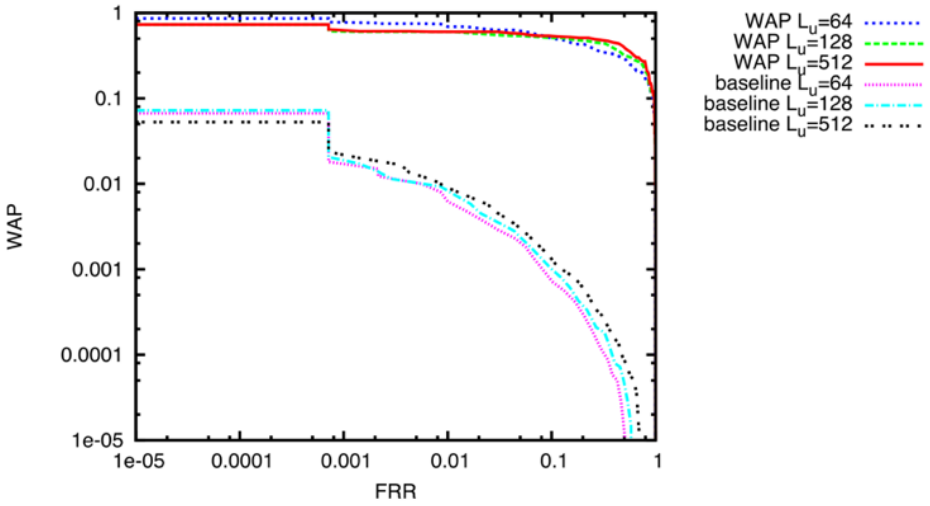


図 5.3.3-6　GMM-UBM 話者照合方式に対するウルフ攻撃実験結果

5.3.3.3　静脈認証装置の脆弱性評価手法

(a)静脈認証装置の脆弱性に関する研究事例

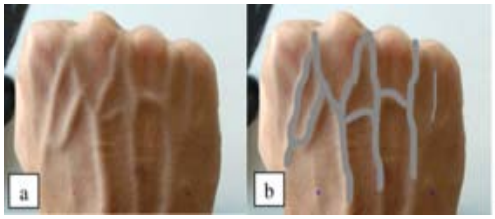
静脈認証装置の脆弱性評価に関する研究は指紋や顔認証と比較して少ないが、近年は徐々に研究例も増えつつある。代表的な研究例には FIDIS(Future Identity in the Information Society)、北方工業大学、横浜国立大学、産業技術総合研究所が含まれる。また、同分野の研究の活性化を図る目的で Idiap 研究所が偽静脈データベースを公開している他、ICB2015 では偽指静脈の検知技術に関するコンペティションが予定されている。以下、それぞれについて述べる。

1) FIDIS(Future Identity in the Information Society)

適切なアイデンティティとアイデンティティ管理がどのように（より）公平なヨーロッパの情報社会を発展させることができるかへの理解を深めることを目的とする EU の共同研究組織である。2006 年 12 月に発行された文書 D.6.1: “Forensic Implications of Identity Management Systems” において、フォレンジックの観点からの ID 管理について述べるとともに、生体認証デバイスの例や、それらの脆弱性の例としてなりすましの実例などをレポート[15]している。同じ結果は、2008 年に FBI 主導で作成された MITRE TECHNICAL REPORT[16]内にも掲載されている。

レポートでは TechSphere 社の Identica Vascular VP-II Scanner に対して、被験者の手の甲の写真を撮影し、画像処理ソフトウェアを用いて静脈パターンを抽出し、被験者の手のサイズに合わせて画像を画像の大きさを調整したのち印刷する。通常のカメラでは区別しにくい静脈についてはカメラの夜間モード（ナイトショット）で撮像する。このようにして取得された静脈像の様子を図 5.3.3-7 に示す。作成された偽静脈は図 5.3.3-8 に示すように(a,b)ペットボトルに貼り付けて提示する、もしくは(c,d) 手に貼り付けて提示するの 2 通りで実験が行われている。同認証装置は生体検知機能を登録時と照合時に独立に設定できるので、すべての設定について 2 通りの実験が行われている。FIDIS のレポートではこの方法によりなりすましは可能であったと結論付けており、生体検知機能を外した場合には、同装置は偽静脈と生体を区別できず、ペットボトルにゴム手袋をかぶせたもの（図 5.3.3-8）も受け入れたと報告している。さらに、生体検知機能をセットした場合でも紙に印刷した偽静脈で登録したものに対して生体で照合に成功した他、ゴム手袋も受け入れたとしている。（表 5.3.3-1）

(a) Identica Vascular VP-II Scanner



(b) 偽静脈の作成

(c) 生体情報の取得

図 5.3.3-7　FIDIS レポート[15]における生体情報（静脈）の取得と偽静脈の作成

(a,b)印刷した画像をボトルに装着して提示、(c,d) 印刷した画像を手に貼り付けて提示

図 5.3.3-8　偽静脈の提示

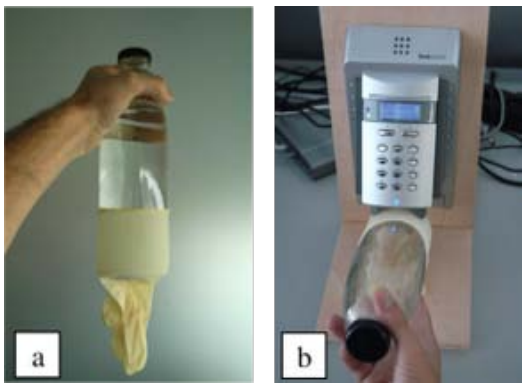


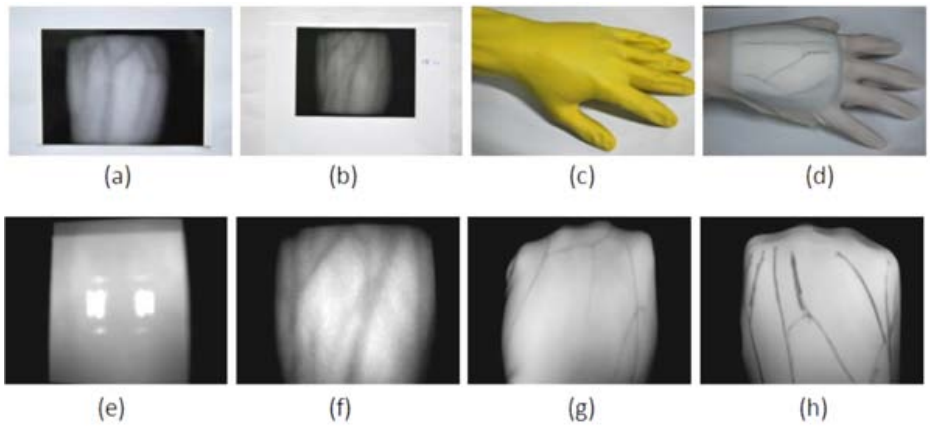
図 5.3.3-9　薄手のゴムをボトルに装着して提示

表 5.3.3-1 実験結果

登録時の 生体検知機能	照合時の 生体検知機能	偽静脈による 登録・照合	偽静脈による登録、生体による照合	生体による登録、偽静脈による照合	ゴム手袋の登録・照合
Off	Off	successful	successful	successful	successful
On	Off				successful
Off	On		successful		successful
On	On				successful

2) 北方工業大学

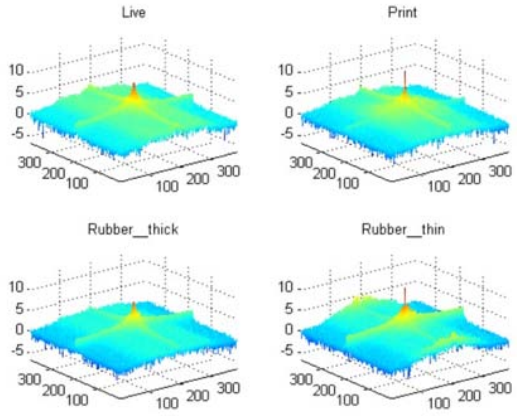
北方工業大学の Wang と Zhao[17]は、手の甲の静脈認証における生体検知手法としてフーリエ変換と SVM（Support Vector Machine）を用いる手法を提案しており、彼らの生体検知手法の評価のために偽静脈を用いた脆弱性評価を行っている。実験では手の甲静脈の近赤外画像 10 枚を写真用紙にプリントし、別の 10 枚を普通紙にプリントした上で、普通紙に印刷した静脈画像、偽静脈画像 10 枚に厚手のゴム手袋をかぶせたものと薄手のゴム手袋をかぶせたものを、それぞれ 10 サンプルずつの近赤外画像を取得し、合計 300 枚の偽静脈画像を作成して、200 個の生体静脈の近赤外画像と比較する実験を行った。ここで、写真用紙にプリントしたものは図 5.3.3.10(e)に示すように反射して静脈を撮影できないため除外している。



偽造物の例(a)～(d)とそれらをセンサーで取得した画像(e)～(h). (a) 写真用紙 (b) 普通紙 (c) 厚手のゴム手袋 (d) 薄手のゴム手袋 (e), (f), (g),(h) はそれぞれ上段の素材に対応するセンサー取得画像

図 5.3.3-10　北方工業大学における静脈認証装置の脆弱性評価例

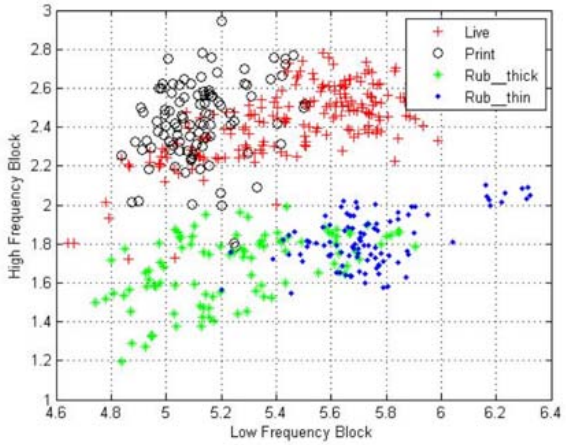
Wang と Zhao[17]は図 5.3.3-11 に示すように、これらの偽静脈の画像と生体静脈画像にそれぞれフーリエ変換を掛けることにより、低周波領域と高周波領域で反応の違いがあることに注目し、生体検知を行うことを提案している。特に、低周波領域では素材による赤外線の吸収率の違いが、高周波領域では偽静脈の筆跡と生体静脈の模様の違いが現れているためと分析している。



生体と偽造物の低周波領域や高周波領域における違いのフーリエ解析による比較。低周波領域では素材による赤外線の吸収率の違いが、高周波領域では偽静脈の筆跡と生体静脈の模様の違いが現れていると見られる。

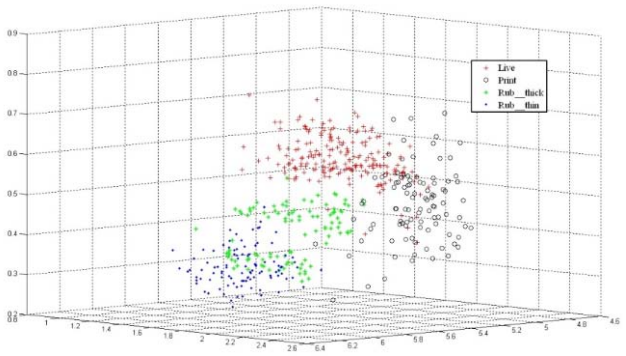
図 5.3.3-11　静脈像（生体）・偽静脈像（普通紙、厚ゴム手袋、薄ゴム手袋）のフーリエ解析

図 5.3.3-12 に示すように、(a)のフーリエ変換後の静脈画像と偽静脈画像の低周波領域、高周波領域のそれぞれを信号強度により 2 次元にプロットした分布を見ると、高周波領域の信号強度によりゴム手袋による偽静脈は識別可能だが、普通紙に印刷した偽静脈と静脈の分布は重なりが大きく識別は困難であることが示されている。一方、(b) 周波数領域を低周波領域、中周波領域、高周波領域に分け、それぞれの信号強度で 3 次元にプロットしたものを見ると、静脈と偽静脈（普通紙、厚ゴム手袋、薄ゴム手袋）の分布が比較的よく分離している。Wang と Zhao[17]は、この 3 次元の信号分布を特徴ベクトルとして SVM(Support Vector Machine)で識別器を構成することを提案している。



フーリエ変換後の静脈画像と偽静脈画像の低周波領域、高周波領域のそれぞれの信号強度によりプロットしたもの。ゴム手袋による偽静脈の分布は分離しているが、普通紙に印刷した偽静脈と静脈の分布は重なり大きい。

(a) 2 種類の周波数領域の信号強度による分布



周波数領域を低周波領域、中周波領域、高周波領域に分け、それぞれの信号強度で 3 次元にプロットしたもの。静脈と偽静脈の分布が比較的よく分離している。

(b) 3 種類の周波数領域の信号強度による分布

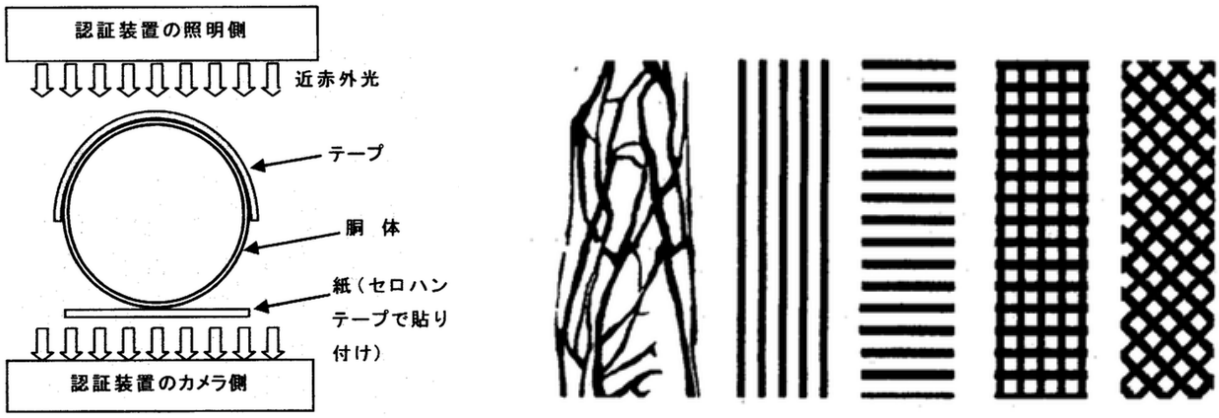
図 5.3.3-12 周波数領域毎の信号強度の分布

3) 横浜国立大学[18][19]

横浜国立大学の研究グループは、指静脈認証システムへのなりすまし攻撃に対する安全性を評価することを目的として、指静脈認証システムに提示した指でない偽静脈が登録されるかどうか、及び登録された場合、同じ対象物あるいは類似の対象物を提示して照合できるかどうかを実験的に評価している。偽静脈として大根、エポキシ樹脂＋人工雪剤等[18]に加え、ガラス製試験管やビニールチューブ等により作成した胴体部分に、光透過/拡散調整用のビニールテープによりレーザープリンタで印刷した紙を挟み込んだ偽静脈[19]を用いて実験を行っている。

(a) 大根スティック　　(b) エポキシ樹脂＋人工雪剤

図 5.3.3-13　偽静脈の例[18]



(a) 偽静脈の構成（断面図）　　(b)偽静脈の印刷パターン

図 5.3.3-14　偽静脈の構成と紙への印刷パターン[19]

研究グループでは、偽静脈の提示によるセキュリティ評価方法を次のような２つのステップ構成に分類し、評価を行うことを提案している。

第１段階：生体認証システムに偽静脈を提示し、

（A）　登録できるかどうか

（A－A）登録できた場合、再度提示して照合できるかどうか

について調べる

第２段階： 生体認証システムに偽静脈を提示し、

（A・L） 身体部分で照合できるかどうか

（L・A） 身体部分を登録し、テスト物体で照合できるかどうか

について調べる

横浜国立大学の研究グループによる検討は、第１段階の評価を対象とし、偽静脈での登録と偽静脈の再度提示による照合が可能であることを示し、また多少のバリエーションを加えた別の偽静脈であっても照合が可能である点を示している。

4) 産業技術総合研究所、中央大学

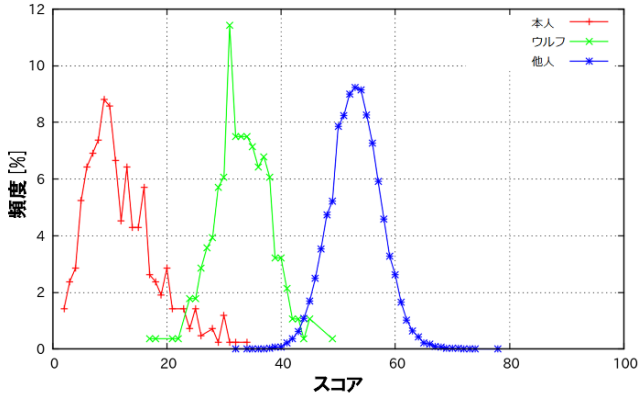
産業技術総合研究所及び中央大学の研究グループは、指静脈認証システムのウルフ攻撃に対する安全性を評価することを目的として、ウルフ偽静脈を提示することにより安全性評価を行う実験[20]を行っている。

静脈撮影装置　　ウルフ偽静脈

図 5.3.3-15　ウルフ偽静脈の撮影装置と偽静脈サンプル

実験では生体指静脈の近赤外画像に対してウルフ偽静脈による照合精度の測定を行っている。ウルフ偽静脈は、光量を調整するためのゴム板の上に薄い白色プラスチック板を重ねて光を拡散し、ウルフ偽静脈パターンを印刷した OHP シートをその上に重ねて構成されている。これは、普通紙では繊維の濃淡がノイズを増加するため、白色プラスチック板と印刷した OHP シートの組み合わせが良いとしている。また、白色プラスチック板は均一に光を拡散するため、ゴム板に含まれる濃淡や気泡によるノイズも吸収できるとしている。さらに、実験では静脈認証装置の画像分解能を 130dpi と想定している。

生体静脈 70 人分 280 サンプルとウルフ偽静脈１サンプルの照合によるスコア分布を図 5.3.3-16 に示す。ウルフのスコア分布（緑）が本人分布（赤）と他人分布（青）の中間に位置し、高い確率で誤受入が生じることを示している。EER 近辺でウルフ偽静脈によるなりすまし成功確率は 60%程度と確認されている。



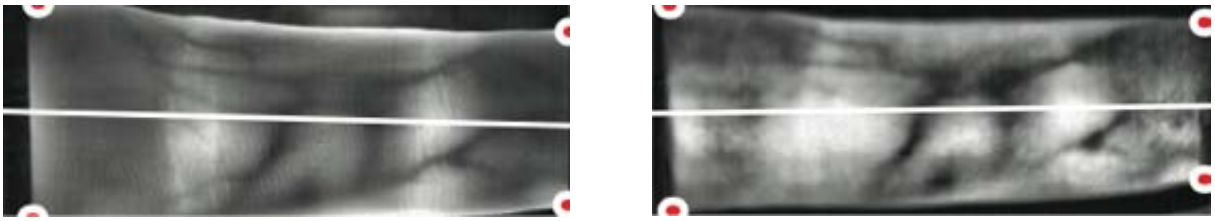
生体静脈 70 人分 280 サンプルとウルフ偽静脈 1 サンプルの照合によるスコア分布。ウルフのスコア分布（緑）が本人分布（赤）と他人分布（青）の中間に位置し、高い確率で誤受入が生じることを示している。

図 5.3.3-16　生体静脈とウルフ偽静脈のスコア分布

5) Idiap Research Institute

Idiap Research Institute は EPFL(École polytechnique fédérale de Lausanne)とジュネーブ大学に属するスイスの研究機関であり、FP7 の BEAT(Biometrics Evaluation and Testing)プロジェクトを主宰するなど生体認証の安全性評価に関する研究を積極的に進めている。

静脈の安全性評価の研究を促進する目的でIdiapはVERA FingerVein Dataset[1]という名称で 110 人の両手人差し指から 2 枚ずつ採取した 440 枚の指静脈画像のデータベースを公開している他、VERA Spoofing FingerVein Datasetという名称でVERA FingerVein Dataset から偽静脈を作成し、再度近赤外センサーで取得した偽指静脈画像を公開している。偽静脈は、VERA FingerVein Datasetに含まれる 50 名分の静脈画像にヒストグラム平坦化、ノイズ除去などの処理を施した後、(1)白紙(80g), (2)OHPシート, (3) 高品質紙(200g)、(4)ボール紙に印刷することで作成され、これを再度近赤外センサーで取得することで合計 200 枚の画像を偽静脈画像として作成している。



生体の静脈画像　　**偽静脈画像**

図 5.3.3-17　Idiap の指静脈及び偽指静脈データベースの画像

6) ICB2015 – 1st Competition on Counter Measures to Finger Vein Spoofing Attacks[2]

平成 27 年(2015 年)3 月に開催されるバイオメトリクスに関する国際会議 ICB2015 (International Conference on Biometrics)に併催で、BEAT と Idiap が偽指静脈によるなりす

1 https://www.idiap.ch/dataset/vera-fingervein

2 http://www.biometrics-center.ch/testing/icb-2015-fingervein-anti-spoofing

まし攻撃検知のコンペティションを開催する予定になっている。コンペティションは、30 人分の左右人差し指 から各 2 枚ずつ採取した 120 枚の生体静脈と、それらの偽静脈画像 120 枚の 240 枚を開発用とトレーニング用の 2 セット公開し、これを元に希望者がアルゴリズムを提出し、提出されたアルゴリズムに対して別途用意した 50 人分のテスト用データセット 200 枚を入力することで、生体静脈と偽静脈の識別性能を競う形で行われる。アルゴリズムの性能は、開発用データセットで偽静脈の誤受入率と生体静脈の誤拒否率が一致する閾値を固定し、テスト用データセットでの偽静脈の誤受入率と生体静脈の誤拒否率の平均値（HTER: Half Total Error Rate）で競われる。

図 5.3.3-18　1st Competition on Counter Measures to Finger Vein Spoofing Attacks

(b) 指紋における安全性評価の例

独では既に指紋認証装置の Presentation Attack を含めた安全性評価に関する PP（FSDPP : Fingerprint Spoof Detection Protection Profile）を発行し、2013 年に世界に先駆けて Common Criteria (ISO/IEC 15408)に基づく認証を与えている。独 Fraunhofer 研究所の Olaf, Scheuermann, Kniess らは、認証制度の立ち上げに先立って米 NIST が主催する IBPC2012（International Biometric Perforamance Conference）に指紋認証装置のなりすましの困難性を Common Criteria における攻撃ポテンシャル評価に関する論文[22]を提出しており、これが静脈認証装置の攻撃ポテンシャル評価を考える際の助けになると思われるので、以下に紹介する。

これは、論文[22]に記載されている攻撃ツリーであり、指紋認証装置で「なりすまし成功」を達成するためには、「偽造指紋を使う」、「センサー上の残留指紋を使う」、「似た指紋を持つ生体指紋を使う」、「攻撃対象者の生体指紋を使う」のいずれかを行う必要があり、さらに「偽造指紋を使う」で「なりすまし成功」を達成するためには「残留指紋から指紋を得る」、「偽造指紋を作成する」、「生体検知機能を無効化する」の 3 つを全て達成する必要があることを示している。論文[22]ではこの中から有効性の高い 4 つの攻撃を選び、それぞれの攻撃ポテンシャルを評価している。

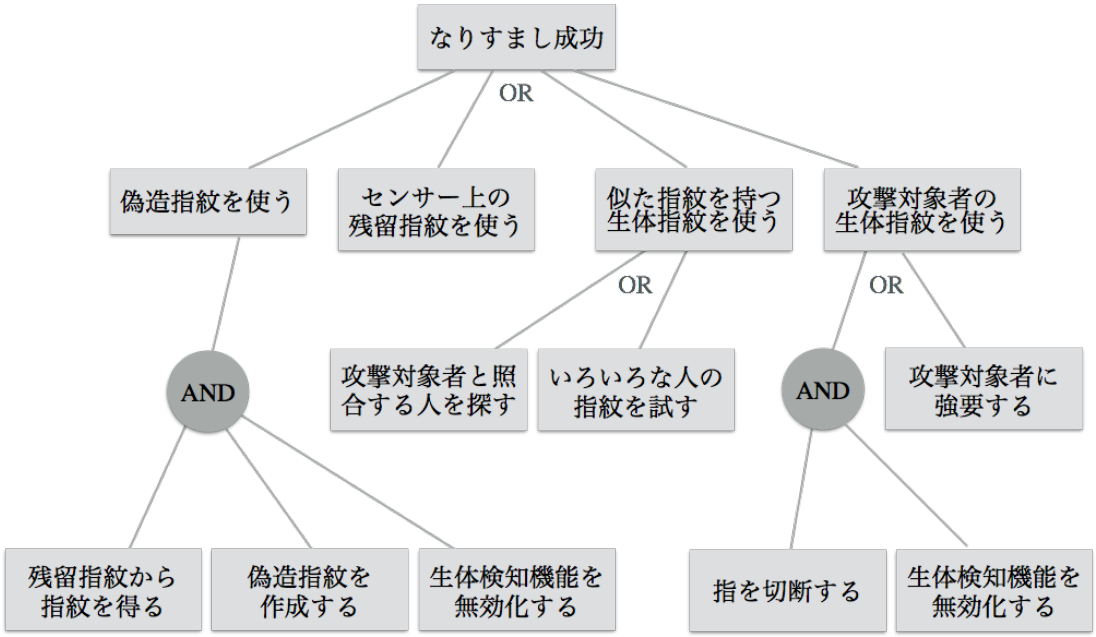
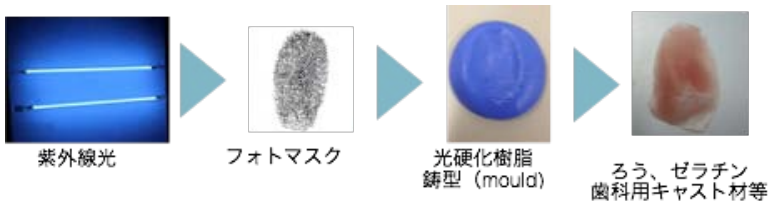


図 5.3.3-19　指紋認証の攻撃ツリー

1)「偽造指紋を作成する」の攻撃ポテンシャル

偽造指紋を作成する際に攻撃者に求められる能力を具体的に考えるために、論文[22]ではデジタル保存された指紋画像から光硬化樹脂で偽造指紋の型を作り、ろうやゼラチン、歯科用キャスト材等を用いて偽造指紋を作成するプロセスを実行するのに必要な攻撃ポテンシャルを考えている。さらに分解すると、(1) レーザープリンタで印刷したフォトマスクを作成し、(2) フォトマスクを光硬化樹脂に付着させて紫外線光を照射する。(3) 硬化していない部分を水で洗い流し、(4) 光硬化樹脂の型に各種素材を流し込むことで偽造指紋が作成される。論文[22]では、Common Criteria の評価

方法に従い、攻撃ポテンシャルを所要時間（Elapsed Time）、熟練度（Expertise）、知識（Knowledge of TOE: Target of Evaluation）、攻撃機会（Window of opportunity）、装置（Equipment）の 5 項目の合計得点で評価している。光硬化樹脂で型を作成してゼラチン等を流し込む作業について、論文では 1 週間以内に完了し(1 点)、偽造には熟練が必要（3 点）であり、公開情報で十分に達成可能（0 点）であり、いつでも実施可能（0 点）であり、光硬化樹脂などの種々の素材を揃える必要があるため特殊装置が必要（4 点）と評価しており、合計 8 点で攻撃ポテンシャルは基本（Basic）と評価している。



Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
Fabricate a dummy from a given fingerprint image	1	3	0	0	4	8	Basic

図 5.3.3-20　偽造指紋の作成プロセス例と攻撃ポテンシャル

2)「生体検知機能を無効化する」の攻撃ポテンシャル

生体検知機能の詳細や無効化の方法は、セキュリティや知財保護の目的で通常は秘密にされており、攻撃者の熟練度と TOE に関する知識の有無が生体検知機能の無効化の攻撃可能性に大きく影響する。TOE に関する知識が少ないと生体検知機能を無効化する方法を探すのに多大な時間を要するであろうし、開発に関わったベンダー内部の関係者は容易に生体検知機能を無効化できると考えられる。攻撃には、生体を模倣した偽指紋の作成に成功するか、装置を操作して生体検知機能を外すかのいずれかが必要である。論文[22]では生体検知機能を無効するためには、特殊な装置が必要になると考えるのが妥当であり、装置が監視下でなければ攻撃機会は多いと考えられる。通常、生体検知機能は攻撃に耐えるように設計されていると考えられるので、相当な高い攻撃ポテンシャルが求められると考えるのが妥当であるとして、合計 22 点で攻撃ポテンシャルは High と評価している。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
Circumvent liveli-ness detection	4	6	7	1	4	22	High

図 5.3.3-21　偽造指紋の作成プロセス例と攻撃ポテンシャル

3)「残留指紋から指紋を得る」の攻撃ポテンシャル

パスワード等と異なり指紋は秘匿されておらず、通常の生活の中で触った物の表面から採取することが可能である。しかし、攻撃対象者が協力的でない場合には、残留指紋から十分に高い品質の指紋を得ることは簡単ではない。残留指紋から指紋を取得する技術が求められることに加えて、特に良い指紋を得られる攻撃機会は限られており、これが攻撃ポテンシャルの評価に重要なポイントになることから、論文[22]ではこれらを加味し、14 点で攻撃ポテンシャルは Modearate と比較的高く評価している。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
Lift a latent finger-print from a touched surface	0	3	0	10	1	14	Moderate

図 5.3.3-22　「残留指紋から指紋を得る」の攻撃ポテンシャル

4)「似た指紋を持つ生体指紋を使う」の攻撃ポテンシャル

無作為に人を選んで指紋を提示する攻撃（ゼロエフォート攻撃）を考える場合、「なりすまし成功」には、TOE に関する知識や熟練は必要ないが、装置の他人受入率（FAR）に関連したコストが掛かる。無作為抽出した人の指紋が指紋認証装置に受け入れられる確率がそれぞれ独立であり、FAR で一定であると仮定すると、確率 95%以上でなりすましに成功するには、$N=log_{(1-FAR)}{}^{(1-0.95)}$人以上を動員する必要がある。

仮に FAR を 5×10^{-4} とすると、必要な人数は 5990 人となり、1 日 50 人を動員しても 4 ヶ月以上の時間を要する。このような考察から、論文[22]ではゼロエフォート攻撃の攻撃ポテンシャルを Moderate から High と評価している。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
Use a real finger of a biometric look-alike	13–19	0	0	1	0	14–20	Moderate – High

図 5.3.3-23　「似た指紋を持つ生体指紋を使う」の攻撃ポテンシャル

(c)静脈認証における安全性評価の考え方

静脈認証装置に対するなりすまし攻撃でも、指紋認証装置に対するなりすまし攻撃と同様に、静脈認証の攻撃ツリーを考えることができる。静脈認証は体内の血管を流れる還元ヘモグロビンが近赤外光を吸収することを利用した生体認証方式であることから、指紋のように日常生活の中で容易に採取されることはなく、切断して時間を経ると認証に必要な静脈構造が得られなくなるといったセキュリティ上の特長が自然に備わっている。いくつかの項目は指紋の攻撃ツリーから除外される。

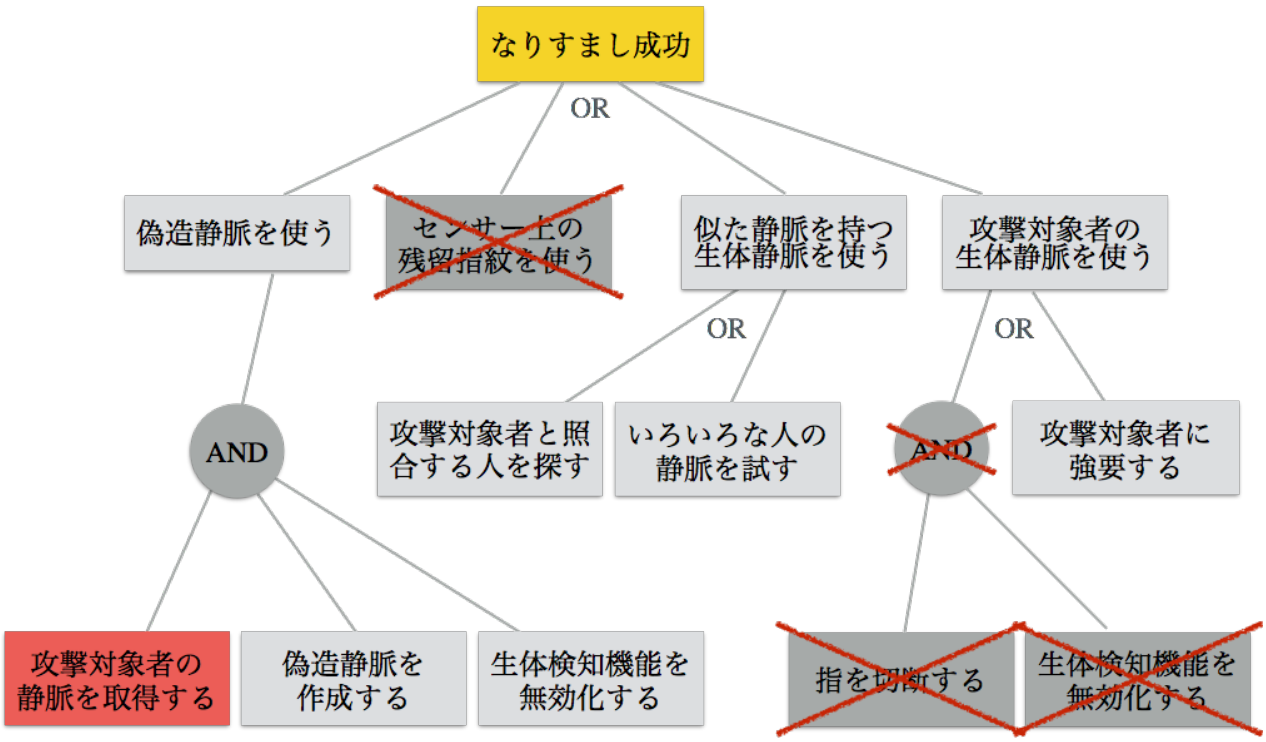


図 5.3.3-24　静脈認証の攻撃ツリー

静脈認証の利点は「攻撃対象者の静脈を取得する」攻撃が指紋認証に比べて著しく困難になることにあるため、本来は「攻撃対象者の静脈を取得する」ことの攻撃ポテンシャルを考察すべきであるが、これまでに紹介した研究例はほとんどが「偽静脈を作成する」に関するものであり、かつ独 BSI が開始した偽指紋の対策技術に関するプロテクションプロファイル（FSDPP: Fingerprint Spoof Detection Protection Profile）も「偽指紋を作成する」の困難さに焦点を絞ったものであることから、欧州の既存の制度的枠組みとの整合性を考慮して、本委託事業報告書では既に攻撃対象者の静脈が取得されていると仮定した上で、「偽静脈を作成する」攻撃に焦点を絞り、先に述べた既存研究の攻撃ポテンシャルを評価することにした。

1)FIDIS の研究例に対する攻撃ポテンシャル試算

静脈認証装置に受け入れられる偽静脈を作成できるためには、静脈認証装置が静脈を取得する原理を理解し、センサーが生体静脈と区別できない偽静脈を作成する必要がある。これには装置が静脈によく吸収される波長帯の近赤外線カメラで撮影しているなどの医工学的な知識が必要となる。また、装置は人体を通して光学的に拡散された静脈の像を観測しているため、装置の光源から出た光に対して人体に似た光学的拡散を模倣する必要がある。これらから偽静脈の作成には一定の熟練度と TOE に関する知識が求められると考えられる。

FIDIS のレポートにおける研究例[15]では、レーザープリンタで静脈パターンを紙に印刷し、手、ペットボトル、ペットボトル＋ゴム手袋（1 種類）にかぶせて提示する攻撃例が報告されており、比較的短い時間で偽静脈を作成できることから以下のように試算した。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
紙＋手など	0	3	3	1	0	7	Basic

図 5.3.3-25　FIDIS の研究例[15]に対する攻撃ポテンシャル試算

2) 北方工業大学の研究例に対する攻撃ポテンシャル試算

北方工業大学の Wang と Zhao の研究例[17]では、レーザープリンタで静脈パターンを写真紙、普通紙に印刷して、これを生体の手に貼り付け、ゴム手袋（厚、薄）にかぶせて装置に提示するといった攻撃を試みている。これもゴム手袋は皮膚の光学的拡散を模倣したものであり、生体の手にはりつけることで装置の光源から発せられた光を自然に拡散しているものと考えらえる。これらから偽静脈の作成には一定の熟練度と TOE に関する知識が求められると考えられる。同様に日常的な装置を利用して、比較的短い時間で偽静脈を作成できることから以下のように試算した。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
紙＋ゴム手袋	1	3	3	1	0	8	Basic

図 5.3.3-26　北方工業大学 Wang と Zhao の研究例[17]に対する攻撃ポテンシャル試算

3) 横浜国立大学の研究例に対する攻撃ポテンシャル試算

横浜国立大学の研究グループでは、作成した偽静脈の指静脈認証システムへの登録・照合に成功する確率を評価している。偽静脈として大根、エポキシ樹脂と人工雪剤の混合物に加え、外径の異なるガラス製試験管、透明ビニールチューブを胴体とし、ビニールテープで光量と拡散を調整し、レーザープリンタで静脈パターンを印刷した紙を胴体の前面にセロハンテープでカメラに対して水平に貼り付けて提示している。装置光源から発せられる近赤外光の指による拡散を考慮した偽静脈を構成しており、一定の熟練度と TOE に関する知識が求められると考えられる。人工雪剤やエポキシ樹脂の混合物を利用するなど、やや特殊な素材が用いられていることから、以下のように試算した。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
大根、人工雪剤、試験管 厚さの異なる普通紙等	2	3	3	1	4	13	Enhanced Basic

図 5.3.3-27　横浜国立大学に対する攻撃ポテンシャル試算

4) 産業技術総合研究所、中央大学の研究例に対する攻撃ポテンシャル試算

産業技術総合研究所と中央大学の研究グループ[20]は、先に述べたようにウルフ攻撃の成功確率を主眼とした偽静脈の作成を試みている。ウルフ攻撃は攻撃対象者の静脈情報を取得せずになりすましに成功することを目的とした攻撃であるから、「攻撃対象者の静脈情報を取得する」部分に対する一つの攻撃アプローチに分類され、ウルフ静脈パターンを発見する攻撃の主要な部分は本報告書の攻撃ポテンシャル評価から除外する。しかし、一旦発見されたウルフ静脈パターンがインターネット等で公開された際に、それを見た一般の攻撃者が偽静脈（ウルフ静脈）のサンプルを作成するプロセスは「偽指紋を作成する」に該当するため、攻撃ポテンシャルを評価しておく必要がある。論文[20]では、レーザープリンタで静脈ウルフパターンを OHP 用紙に印刷し、ゴム及び白プラスチック板に貼付して提示している。これは装置光源からの光の拡散や皮膚による静脈パターンの光学的拡散を模倣しており、偽静脈の作成には同様に TOE に対する一定の知識と熟練がもとめられると考えられる。ただし、一般的な装置と比較的短い時間で作成できることから、攻撃ポテンシャルは以下のように評価した。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
OHP、ゴム、白プラスチック板	1	3	3	1	0	8	Basic

図 5.3.3-28　産業技術総合研究所と中央大学の研究例[20]に対する攻撃ポテンシャル試算

5)Idiap Research Institute の研究例に対する攻撃ポテンシャル

Idiap では静脈撮影装置を自作して取得した 50 名分の静脈画像にヒストグラム平坦化、ノイズ除去などの処理を施した後、 (1)白紙(80g), (2)OHP シート, (3) 高品質紙(200g)、(4)ボール紙にそれぞれ印刷し、これを再度近赤外センサーで取得することで合計 200 枚の画像を偽静脈画像として作成して公開している。ここでは攻撃対象者の静脈画像を取得した攻撃者がヒストグラム平坦化、ノイズ除去などの処理を施して白紙、OHP シート等に印刷し、実際に偽静脈を作成するための攻撃ポテンシャルを考える。ヒストグラム平坦化やノイズ除去には TOE に対する一定の知識と熟練が求められるが、一般的な装置と比較的短い時間で作成できると考えられる。このことから、攻撃ポテンシャルは以下のように評価した。

Attack	Elapsed time	Exper-tise	Knowl-edge of TOE	Window of oppor-tunity	Equip-ment	Required attack potential	
						Sum	Rating
紙, OHP等	1	3	3	1	0	8	Basic

図 5.3.3-29　Idiap Research Institute の研究例に対する攻撃ポテンシャル試算

(d)静脈認証装置の安全性評価の進め方

独で開始された Common Criteria に基づく指紋認証装置の安全性評価(FSDPP)では、「残留指紋から指紋を得る」困難さを評価しない Cooperative（攻撃対象者が協力的な）条件下で、攻撃対象者の指紋を既に攻撃者が得ていることを前提にして「偽造指紋を作成する」攻撃に対する指紋認証装置の Persentation 攻撃に対する耐性のみを評価している。この方針に従って、静脈認証装置に対する Presentation 攻撃に関する既発表研究例の攻撃ポテンシャルは、静脈認証装置の静脈取得方法や静脈パターンの光学的拡散等に関して一定の知識と熟練があれば、全ての研究例で比較的容易に偽静脈を作成できることから、攻撃ポテンシャルは 7～8 の Basic であると評価した。このことから、既存の研究例には比較的簡単な Presentation 攻撃しかなく、AVA_VAN.2 への耐性を評価には攻撃ポテンシャルが 5 から 6 程度高い、やや高度な攻撃方法を列挙・充実する必要がある。これには例えば、3D プリンタ、電子ペーパー、反射型液晶などの特殊装置(Specialized, +4)を利用した攻撃が含まれると考えられる。

さらに、静脈認証は、攻撃対象者の静脈を得るのが難しいことが他の認証方式に優る重要な特長の一つであり、Cooperative 条件下での評価だけは安全性の高さを十分に主張できない問題がある。フラウンホーファー研究所の Olaf らによる論文[22]では、「残留指紋から指紋を得る」ことの攻撃ポテンシャルを比較的高い Moderate と評価しており、攻撃対象者の静脈を得ることの攻撃ポテンシャルは更に高いと推定されるため、必ずしも静脈認証装置の本来の安全性を評価できていないと言わざるを得ない。当面は独等との互換性を優先すべきだが、将来は、独等と連携して AVA_VAN.2 よりも高い基準で生体認証装置の安全性を評価できる仕組みの検討も必要である。

5.3.3.4 脆弱性評価環境構築に関する検討

(a)産業用ロボットを用いた評価環境の構築

脆弱性評価環境の構築にあたり、センサーとアルゴリズムを含めた生体認証機器の脆弱性評価における評価要件について整理する必要がある。本年度は、まずこの評価要件について検討し、次の3つとしてまとめた。

1)統計的信頼性

ISO/IEC 19795 Part1 Annex.B[1] では統計学上の 3 の法則(突合数 n に対して 95%信頼区間が 3/n で求められる)に基づくテストサンプル数の決定法が記載されており、0~0.1 %の信頼区間を設定したければ、3000 回の突合が必要となる。脆弱性評価においても同様に、統計的信頼性が高い結果を得るためには多くの評価を行う必要がある。

2)評価結果の再現性

脆弱性評価を行う際には評価者に依存しない、再現性のある方法で評価を行う必要がある。

3)評価結果の網羅性

脆弱性評価対象となる攻撃技術は年々増大しており、これらを網羅した評価を行う必要がある。

これらの 3 つの要件を満たす技術として、高速かつ正確な動作が可能な産業用ロボット（仕様は表 5.3.3-2 を参照）に着目し、脆弱性評価用環境の構築を行った。

表 5.3.3-2EPSON C4 ロボット仕様

機種名	C4
アーム長	600mm
サイクルタイム*2	0.37 秒
繰り返し位置決め精度	±0.02mm
可搬重量	最大 4kg(下向き
環境仕様	標準 / クリーン
取付方法	架台*3
適合コントローラ	RC700

図 5.3.3-30　ロボットによる脆弱性評価環境

（左）全体図　（右）偽静脈のセンサーへの提示例

図 5.3.3-30 に構築した脆弱性評価環境を示す。脆弱性評価環境は、6 軸ロボット（中央)、カメラ（右上)、評価用センサー（左)、及び制御用 PC の 4 つの部分から構成される。カメラにより撮影した映像をリアルタイムに解析し、カメラ撮影範囲内に存在する偽造物を検出する。検出された偽造物は順次ロボットによりピックアップされ、評価対象のセンサーに対して、あらかじめ設定された位置、角度、強さで正確に提示される。この際、評価対象のセンサーは様々な形状を持つことを想定しているが、6 軸ロボットを用いることで複雑な形状のセンサーに対しても高速かつ正確な偽造物の提示が可能となった。今後は本評価環境を用いた脆弱性評価を進めていく予定である。

(b)OCT（Optical Coherence Tomography）

非侵襲で生体等の内部を観察する測定装置である Santec 社製の OCT（IVS-2000）を用いて生体静脈及び偽静脈の測定を行った。指の背面を近赤外光で照らした近赤外フィルタを通じてデジタルカメラで撮影した生体の静脈像にヒストグラム平坦化処理後、静脈抽出アルゴリズムで静脈を強調している。この画像を普通紙に印刷したもの（図 5.3.3-31）を薄手のゴム手袋に挟んだ偽静脈を作成し、OCT で観察した。

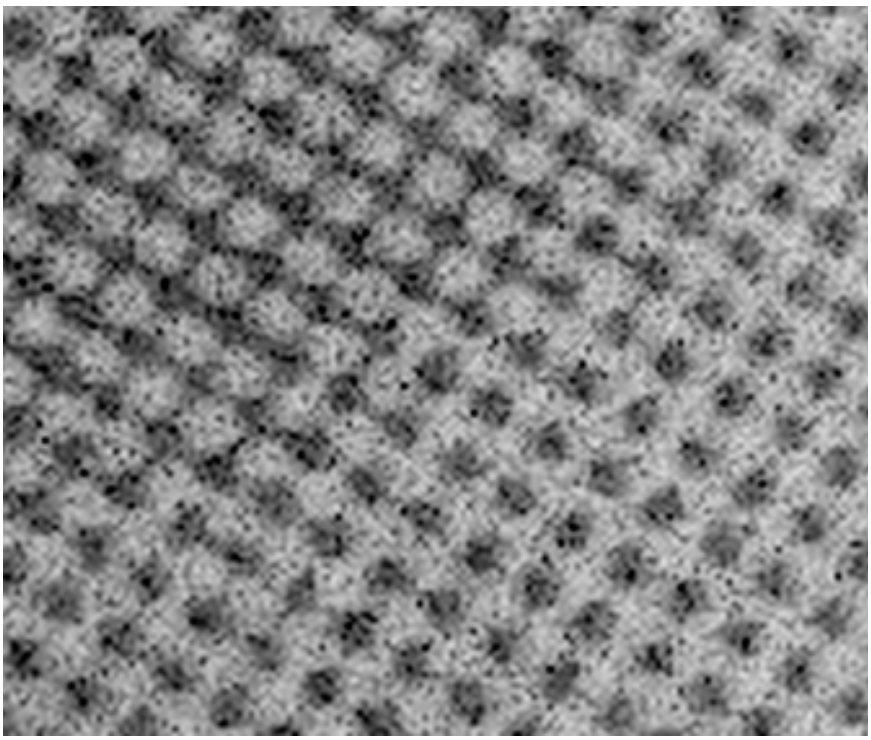
普通紙に印刷した偽静脈像は、図 5.3.3-31(b)に示すようにレーザープリンタの特性によりカーボントナーが周期的に分布している。OCT の近赤外レーザー光はカーボントナーに吸収されるため明らかに生体とは異なるパターンが観測される。さらに、図 5.3.3-32 に示すように薄手のゴム手袋に偽静脈を印刷した普通紙を挟み込むようにして作成した偽静脈を OCT で観察したものを図 5.3.3-33 に示す。

図 5.3.3-34 に示した生体の OCT 像とは明らかに異なる起伏のパターンがゴム手袋表面に見られる他、OCT の内部観察能により、ゴム手袋と普通紙の隙間、ゴム手袋の厚さ、普通紙上のカーボントナー分布に起因する柵状構造がそれぞれ観察された。

他に非侵襲の内部観察が可能な測定装置に X 線 CT や MRI（磁気共鳴イメージング）装置が知られているが、X 線 CT は今回のように人体を偽造生体の一部に使う偽造物の解析への適用が難しいこと、MRI はより生体の深い構造の観察が可能だが測定精度は OCT と比べて劣ることなどから、今回の結果より、偽静脈のように立体構造を有する偽造生体の内部構造の精密測定が必要な場合に OCT が極めて有効であり、他の測定方法に比べても優れていることが確認された。

(a) 普通紙に印刷した偽静脈

近赤外で撮影した生体の静脈像をヒストグラム平坦化処理後、静脈抽出アルゴリズムで静脈を強調している。

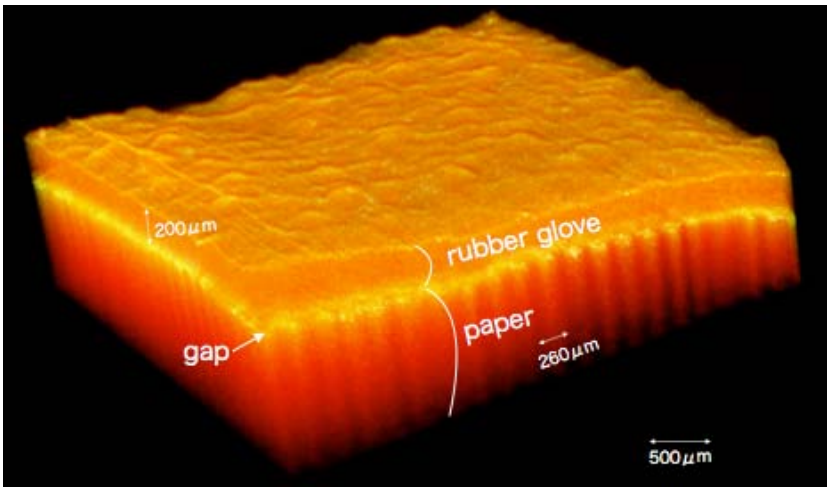


(b) 印刷した偽静脈の OCT による 2D 観察像

レーザープリンタのドットが普通紙の表面に確認できる。

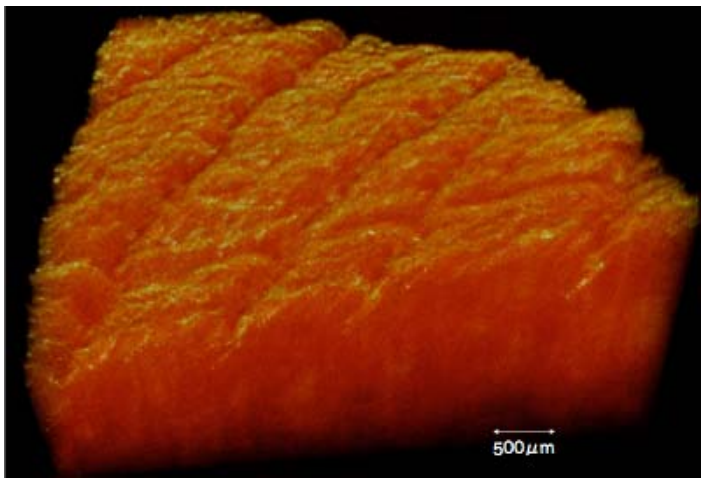
図 5.3.3-31　OCT 観察実験に用いた偽静脈（普通紙に処理済み偽静脈画像を印刷）

図 5.3.3-32　OCT 観察実験に用いた偽静脈（普通紙と薄手のゴム手袋）



ゴム手袋表面の起伏に特徴が見られる他、ゴム手袋と普通紙の隙間や、非侵襲内部観察によりゴム手袋の厚さや普通紙に印刷された偽静脈画像のものと見られるカーボントナーの周期的な分布により OCT の近赤外レーザー光が吸収され、普通紙の内部構造が柵状に観察される。

図 5.3.3-33　偽静脈の OCT 観察像



皮膚の OCT 観察像、皮膚表面の起伏や皮膚内部の構造が観察される。

図 5.3.3-34　生体指の OCT 観察像

5.4 国際標準化活動

5.4.1 PP/脆弱性評価関連

PP と脆弱性評価の国際標準化活動は、ふたつの活動が現在進んでいる。

(1)ISO/IEC 30107 Biometric presentation attack detection

ISO/IEC JTC 1/SC 37 では、生体認証機器へのなりすまし攻撃検知に関する標準化として ISO/IEC 30107 シリーズ：Biometric presentation attack detection の開発が進んでいる。ISO/IEC 30107 シリーズは下記の 3 つのパートから構成される。

Part1: Framework（フレームワーク）
Part2: Data formats（データ形式）
Part3: Testing and Reporting（性能評価と報告の方法）

本年度は、脆弱性評価と特に関連の深い ISO 30107 Part3 文書開発に対する寄与を目的として、1 月にスペイン・トレドで開催された SC37 会合に参加した。現地審議では、産総研からなりすまし攻撃性能の評価式である APCER（Attack Presentation Classification Error Rate）に関する変更提案を行った。新しく提案した評価式を式 5.4.1-1 に示す。

$$\mathrm{APCER} = \max_{AS \in \mathcal{A}^{AP}} \frac{1}{N_{AS}} \sum_{i=1}^{N_{AS}} RES_i$$

where $\mathcal{A}^{AP}$ is a set of artifact species with the same attack potential AP. $\mathcal{A}^{AP}$ is a subset of all artifact species $\mathcal{A}$. Namely, $\mathcal{A} = \mathcal{A}^{minimal} \cup \mathcal{A}^{basic} \cup \mathcal{A}^{enhanced-basic} \cup \mathcal{A}^{moderate} \cup \mathcal{A}^{high}$

式 5.4.1-1　APCER の評価式

ここで、attack potential AP は 5.3.3 節で述べた攻撃ポテンシャルに対応しており、たとえば、$\mathcal{A}^{minimal}$ は、攻撃ポテンシャルが minimal となる Artefact species (同じ偽造物作成手法を用いて、異なる生体特徴から作成された偽造物) の集合を表す。従来の提案では、APCER は攻撃ポテンシャルの異なる複数の偽造物を用いて攻撃を行った際の平均的な攻撃確率を評価するものであったが、平均的な攻撃確率では特定の偽造物を用いた際に高い攻撃成功確率を示すような認証機器を正しく評価できない可能性があった。そこで式 5.4.1-1 では、攻撃ポテンシャルごとに評価した攻撃確率のうち、最大の攻撃確率を APCER としている。

セキュリティの観点から従来の平均値ではなく、最悪値（最大値）を考慮するのは妥当であるとされ、これらの変更は標準化文書に反映されることとなった。今後も、本評価式を含めた文書の品質向上に対して貢献していく。

(2)ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics

ISO/IEC JTC 1/SC 27/WG 3 と WG 5 では、SC 37 で ISO/IEC 30107 のプロジェクトが発足した当時から、ISO/IEC 30107 への貢献を目的として、スタディピリオド Study period on Security evaluation of anti-spoofing techniques for biometrics を継続して来た。スタディピリオドにおいては、ドイツが 2012 年 10 月に BSI が作成した Fingerprint Spoof Detection Evaluation Guidance 2.1 を寄書提出し、英国も平成 26 年(2014 年)3 月にバイオメトリクスの脆弱性の評定方法論に関する寄書提出した。平成 26 年(2014 年)4 月の SC 27 香港会議では、スタディピリオドは終了する予定だったが、ドイツから上記寄書に基づく新規作業項目を提案予定であることが報告された。平成 26 年(2014 年)4 月時点で開始準備を進めていた本事業と上記新規作業項目との関連性、本事業成果の新規作業項目への反映の可能性について、WG 3 国内委員会が勘案し、産業技術総合研究所に参加要請があった。最終的には、新規作業項目は、産業技術総合研究所が作成して提案した。新規作業項目は、ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics として、10 月のメキシコシティー会議で成立した。編集者には産業技術総合研究所の山田朝彦が、共同編集者にはフランスの Ludovic Merrien が、それぞれ就任した。

SC 37 でも、ISO/IEC 19989 は、ISO/IEC 30107 との関係において関心が持たれている。平成 27 年(2015 年)1 月の SC 37 トレド会議の WG 3/WG 5 の合同セッションにおいて、産業技術総合研究所の山田朝彦が ISO/IEC 19989 の作成方針を説明した。質疑応答では、ISO/IEC 30107 との連携の重要性を確認した以外は、特記すべきものはない。

平成 27 年(2015 年)2 月には、ISO/IEC 19989 の第 1 作業原案を提出した。第 1 作業原案に対する各国コメントは、平成 27 年(2015 年)5 月に開催される SC 27 クチン会議で審議される。作業原案は SC 内文書なので、本報告書では、全体を引用せず、概要の報告と目次の引用だけに留める。

ISO/IEC 19989 の目的は、センサーへの偽造物提示などの攻撃に対する検知（Presentation Attack Detection（PAD））機能の CC 評価・認証を可能にすることである。そのために、必要な拡張コンポーネントを CC パート 2 及びパート 3 に対して定義し、それらに対応して CEM の補完をすることである。

引用規格（Normative reference）では、バイオメトリクスの用語として ISO/IEC 2382-37:2012、CC については対応する国際標準規格である ISO/IEC 15408 シリーズ、CEM については同様に ISO/IEC 18045、バイオメトリクス固有のセキュリティ評価についてまとめた ISO/IEC 19792、更に ISO/IEC 30107 シリーズを参照している。

用語等は、ISO/IEC 19989 自体では定義せず、上記引用規格から必要なものを参照している。

5 Biometric product and presentation attack detection では、バイオメトリクス製品における PAD 機能を含む機能構成を ISO/IEC 30107-1 に基づいて定め、TOE が Capture 機能と PAD 機能だけを含む場合と TOE がそれ以外の機能を含む場合に TOE を分類した。TOE がこの分類のいずれかによって、セキュリティ機能要件の拡張コンポーネントが異なって来ると考えられる。

6 Common vulnerabilities of biometric systems listed in ISO/IEC 19792 and PAD では、5.1.1 海外動向調査で述べた ISO/IEC 19792 が示す脆弱性評価の構造分析に基づき、PAD 評価の範囲を

明確にした。

7 Extended security functional components to Class FPT: Protection of the TSF は、ドイツで作成された FSDPP[24]にある拡張コンポーネント FPT_SPOD の名称を FPT_PAD に、対象を指紋から一般のバイオメトリクスに、変更したものである。この拡張コンポーネントは、5 の TOE 分類のいずれにも適用できる。しかし、TOE が Capture 機能と PAD 機能以外を含む場合は、以下の 8 を適用することが望ましいと考えている。

8 Extended security functional components to Class FIA: Identification and authentication は、記載はまだなく、寄書募集状態にある。本事業の成果であるユーザ認証の場合の拡張コンポーネント、今後予定しているユーザ識別の場合の拡張コンポーネントを日本 NB として提供の予定である。

10 Extended assurance component to Class AVA_VAN: Vulnerability assessment では、FSDPP[24]にある拡張コンポーネント AVA_VAN.E を AVA_VAN.2m として定義した。AVA_VAN.2 が攻撃能力基本に対応するものであるのに対し、AVA_VAN.E は攻撃能力最小（Minimal）に対応するものとして FSDPP[24]では定義されている。しかし、両者は想定する攻撃能力の相違を除けば、要件としての差異は少ない。SC 27 のスタディピリオドへのドイツ寄書 FSDEG では、AVA_VAN.E の評価方法の詳細が定義されているが、これも AVA_VAN.2 との差異は少ない。よって、AVA_VAN.E を AVA_VAN.2-（2 マイナス）と位置付けて、定義していると言って良い。そのため、ISO/IEC 19989 の作業原案では、AVA_VAN.E を AVA_VAN.2m（m は minus の意）と定義した。

11 Complement to ISO/IEC 18045 on Class APE: Protection Profile evaluation 以下においては、附属書（Annex）も含めて、ドイツ寄書 FSDEG に記述されている評価方法を CEM の記述順序に再配置したものである。

以下は、ISO/IEC 19989 の第 1 作業原案の目次である。

5.4.2 精度評価関連

バイオメトリック製品の精度評価について、ISO/IEC JTC1/SC37 WG5 への国際標準化提案の可能性を検討中である。特に、精度評価の結果として宣言する FTE、FRR、FAR などの精度値算出根拠となるエビデンス情報の項目や内容に関する新規提案の可能性があると考え、国際新規提案の実現性について平成 27 年度以降さらに検討を進める予定である。

6. 平成26年度活動まとめ

本事業は、バイオメトリクス認証技術に対する社会的に認知されたセキュリティ評価基準がないことで、各製品のセキュリティ性を客観的に評価できない状況を改善するため、バイオメトリクス製品の CC（Common Criteria）認証に向け、国内に、①産業界が無理なく参加可能、②十分に有効性があり、③継続性のある、バイオメトリクス製品のセキュリティ評価基盤を 3 年間で整備することを目的として活動をはじめた。

事業実施者は海外動向調査で得た知見をもとに方針を立て、PP 開発及び PP 認証取得と、セキュリティ評価手法の研究、脆弱性評価組織の育成、また精度評価ツールの開発に取り組んだ。

並行して日本のバイオメトリクス産業界から 6 社、また評価関係者から 2 団体の委員やオブザーバに参加いただいた検討委員会を設け、実施者の検討内容に対して、4 回の委員会の場で、あるいは委員の方への個別のヒアリングで種々のご意見をいただき、そのご意見を考慮しつつ取組内容の質を高めた。

その結果、当初掲げていた①産業界が無理なく参加可能、②十分に有効性があり、③継続性のある、バイオメトリクス製品のセキュリティ評価基盤の整備という目標に向け、第一年度目としてほぼ満足できる成果を得たと考えている。

(1)海外動向調査と方針検討

(a)海外調査

PP に関する情報を得るため、インターネット上で入手可能な PP を調査した。

評価技術については、インターネット上で入手可能な文献に加え、ISO/IEC JTC 1/SC 27/WG 3 への寄書、更に既に指紋のなりすまし攻撃検知の製品に対する CC 評価・認証を開始しているドイツの状況を海外出張して関係者から情報入手した。

この中で、ISO/IEC 19792 を詳細に分析することで、バイオメトリクス製品固有の脆弱性評価の内容を絞り込むことができた。脆弱性評価のための評価技術については、ドイツの評価機関 TUViT を訪問し、偽造物検知評価の標準体系の概要と合格基準を確認することができた。

また、欧州におけるバイオメトリクス技術または製品の評価及び試験のための組織である BEAT（Biometrics Evaluation And Testing）において、精度評価及び脆弱性評価を推進しているマドリッド自治大学（Universidad Autonoma de Madrid）及び Idiap 研究所（Idiap research institute）のメンバと面会し、欧州における精度評価及び脆弱性評価に対する取り組みを調査し、BEAT における精度評価は Idiap が開発した BEAT プラットフォームを使用し、脆弱性評価では確率論的なアプローチを採用しようとしているとの情報を得ることができた。

しかしながら、BEAT プラットフォームはテクノロジ評価を主目的とし、キャプチャを含めたシナリオ評価や運用評価の機能は含まれていないためハードウェアを含んだ評価はできず、CC 認証には向いていないとの印象を得た。一方、本事業の検討では、CC 認証を念頭に置いた

ツール開発をしているため、本事業の有効性を改めて確認できた。

上記と並行して、韓国における精度評価に対する取り組みを調査し、韓国が開発を進めている Web ベースの試験システムを拡張して、精度評価化試験にも適用したいとの意向を持っているとの情報を得ることもできた。

また、バイオメトリクスの関わる「脆弱性評価」「精度評価」等に関する標準化状況に関して調査し、バイオメトリック製品のシナリオ評価を含んだ規格であり、評価実施時の環境条件による性能への影響を測定する方法について示す国際規格 ISO/IEC 29197 の FDIS 投票が可決したことを確認した。本規格の Annex A には、基準となる性能を測定するための標準環境として気温[°C]、湿度[%]、照度[lx]、雑音[dB]、気圧[kPa]の値の範囲が示されているため、本事業において独立評価機関による独立試験を実施する際にも、何らかの環境条件を定義する必要があるため、留意する必要があると考えている。

(b)方針検討

調査結果を基に、PP 作成及び脆弱性評価の方針を作成した。これらの方針作成にあたっては、国内のバイオメトリクス製品ベンダー各社にインタビューして、その結果を参考にした。

PP 作成の作成方針として、PP 及び PP に付随する評価手法は、国際標準案とするために作成することを目的としていため、英語で PP を作成することとし、広く活用されるように、バイオメトリクス製品のモダリティや身体部位に依存しないこと、ユーザ認証やユーザ識別に基礎的な機能を提供するバイオメトリクス製品の PP を作成することを方針とした。

ISO/IEC 19792 が示すバイオメトリクス製品固有の評価内容、エラー率（精度）・脆弱性評価・プライバシーについては、個別に PP を作成することとし、製品に必要な PP を選択して、ST 作成、CC 評価認証できるようにすることを方針とした。

また、脆弱性評価における想定する攻撃者の攻撃能力、製品の評価対象範囲である TOE（Target Of Evaluation）については、ベンダーへの意見聴取を通じて、決定することにした。

まず、脆弱性評価の海外動向調査や脆弱性評価手法の研究の結果を踏まえて、脆弱性評価の方針を検討することとした。また、論文などの公開情報を基に、PP の定める攻撃能力を前提とした、攻撃方法及び偽造物のセット（レシピ）の案を作成し、試行用 TOE に対して案に従って偽造物を作成して攻撃を試行し、認証機関の IPA も含めて、攻撃能力のレーティングを実施し、攻撃能力が基本であるかを確認することとした。合わせて、評価方法を決定するとともに、合否基準などの評定方法も決定することとした。これらの検討結果を適用して、再来年度からの製品の CC 評価・認証を実施する方針とした。

また、偽造物作成のためのデータ収集は、装置（光源＋カメラ）を自製して、その装置を使用して行い、3 次元の偽造物を作成する場合には、複数の 2 次元画像から 3 次元画像へ変換するソフトウェアの活用も検討することとした。

(2)PP 開発及び PP 認証取得

PP 及び PP に付随する評価手法は、ユーザ認証あるいはユーザ識別に基礎的な機能を提供す

るバイオメトリクス製品の PP を作成することを方針として取り組んだ。その取組の中で、CC の評価・認証として構造化されている 1 次資産と 2 次資産という考え方に則してセキュリティ機能要件及びセキュリティ保証要件を整理した。

バイオメトリクス製品ベンダー各社へのインタビューや委員会で意見聴取を経て、本年度開発する PP におけるバイオメトリクス製品の機能はユーザ認証だけを対象とし、CC 評価の対象となる TOE については各社の意見の共通部分とすることとし、PP を開発した。

また、CC 評価・認証を受ける製品の TOE が、PP 最終案よりも多くの機能を含む場合の対応方法を記述したサポート文書案も作成した。

作成した PP は認証取得に向けて、評価機関による評価が完了し、4 月半ばに認証機関である IPA より認証をいただく予定で作業を進めている。

なお、この PP の開発で得た知見を活用して、ISO/IEC JTC 1/SC 27 に対して、新規作業項目として ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics を産業技術総合研究所より提案し、10 月のメキシコシティー会議で成立することができた。なお、編集者には産業技術総合研究所の山田朝彦が、共同編集者にはフランスの Ludovic Merrien が、それぞれ就任した。

(3)セキュリティ評価手法の研究

(a)精度評価のためのサポート文書とツール開発

セキュリティ評価項目のひとつである精度評価を実施するための精度評価のためのツール開発は、ツール開発の基本方針を検討し、CC における独立試験（ATE_IND）のためのツールと位置づけ、国際標準に準拠した複数のバイオメトリック・ベンダー製品に対して共通的に使用できるよう設計する方針を定め、精度評価ツールの評価項目として必要なものを検討し、①FTE（登録失敗率)、②FRR（本人拒否率)、③FAR（他人受け入れ率）また必要により④ROC カーブ（CC 認証として不要であれば削除予定）とするとの結論を得ることができた。

また、評価時の機器構成、精度評価の流れ、評価条件、評価のシナリオなどを検討し、評価の作業効率を高めるためのツールとして精度評価ツールのプロトタイプの一部を開発した。

さらに、CC 認証におけるバイオメトリック製品の精度評価を、バイオメトリック・ベンダーあるいは独立評価機関が実施する際の評価ガイドラインをサポート文書案としてまとめた。

(b)脆弱性評価手法の研究

セキュリティ評価手法の研究における脆弱性評価手法の研究については、海外における研究動向調査を行い、生体を模倣しないが高い確率で誤判定を発生させるウルフ(なりすましの入力情報)などを使った脆弱性評価手法の研究とウルフによる脆弱性解析方法を検討し、またウルフ攻撃実験を行いその有効性を確認した。

静脈認証装置に対する既存のなりすまし攻撃手段についても調査を実施し、静脈認証装置の脆弱性評価手法について基本的な考え方を整理した。脆弱性評価の要件については、3 つに整理

し、これらの要件を満たす脆弱性評価環境の構築するため、産業用ロボットを導入し、これによる実験環境を構築することができた。

また、これらで得た知見をもとに、認証機関の IPA も含めて脆弱性評価の方針を検討し、論文などの公開情報を基に攻撃方法及び偽造物のセット（レシピ）の案を作成し、TOE に対して攻撃を試行するという案をまとめた。脆弱性情報は機微なものであるため、情報の管理が必要であり、来年度事業の中で、公開と制限の範囲、脆弱性情報をどのような場で議論するか等を決定する予定である。

7. 平成27年度活動に向けて

平成 27 年度も、バイオメトリクス製品の CC（Common Criteria）認証に向け、国内に、①産業界が無理なく参加可能、②十分に有効性があり、③継続性のある、バイオメトリクス製品のセキュリティ評価基盤を 3 年間で整備することを目的として活動を継続したいと考えている。

活動が継続できる場合は、平成 28 年度のパイロット評価に向けて、平成 26 年度の活動で得た知見と成果を基にして、国際連携活動、PP の開発・評価・認証とサポート文書開発、脆弱性評価手法の開発と脆弱性評価組織の育成、精度評価ツールの開発、協力ベンダーによる準備実施及びに国際標準化活動に取り組んで行きたいと考えている。

(1)国際連携活動

(a) PP に関して

本事業の成果であるバイオメトリクス製品 PP の普及のための国際連携方針を、国内関係者の意見を参考に、検討する。この連携方針に従い、バイオメトリクス製品 PP を既に開発しているドイツやアメリカを候補として、活動する。バイオメトリクス製品 PP のシリーズ化、本事業成果の拡張コンポーネント、評価方法に関して、考え方の紹介と意見交換を実施する。

(b) 精度評価ツールに関して

精度評価ツールを活用した国際連携について検討する。連携先は BEAT（前述）を推進する欧州を想定する。連携方法として、以下の 3 段階を想定し、連携活動を実施する。(連携の深さは① < ② < ③ である。)

①精度評価ツールの欧州機関による評価やレビューによる連携

②精度評価ツールが生成するエビデンス情報や精度評価報告書の日本と BEAT での共通化（標準化）

③精度評価ツールの機能の日本と BEAT 間の共通化（動作仕様レベルの共通化）

※ なお、脆弱性評価についても、精度評価と同様の連携可能性について検討する。

連携対象国：BEAT において精度評価活動のリーダを擁するスペインを主要連携国候補とし、脆弱性評価のリーダ国であるドイツも連携候補とする。

(2) PP の開発・評価・認証とサポート文書開発

平成 26 年度に開発した登録処理の PP の評価・認証を取得する。また、平成 26 年度に開発した PP 及び PP のサポート文書の開発を完了する。評価機関に内容を理解していただき、認証機関である IPA にできた部分から順に意見をいただくことによって、評価・認証がスムーズに無事に終了するように取り組む。

また、今年度作成したユーザ認証を対象とした PP に加え、登録及びユーザ識別の PP を完成させる。必要があれば、攻撃能力の異なるユーザ認証用 PP を作成する。これらのうちの 2 件に対して、

CC 認証を受ける。

更に、今年度作成したサポート文書案を拡充し、PP を基に製品の CC 評価・認証を受ける製品ベンダーが利用するためのサポート文書を作成する。ここでは、PP の TOE に含まれない機能も含めて製品の CC 評価・認証を受けようとする時への対応方法などを記述する。

(3)脆弱性評価手法の開発と脆弱性評価組織の育成

平成 28 年度に評価・認証が可能になるように、平成 26 年度に検討した静脈の偽造物検知の評価方針案(偽造物作成のためのデータ採取方法や偽造物の種類など)に基づき、評価機関で実際の評価作業を実施するために必要な偽造物作成方法・攻撃方法を、産総研で研究し、認証機関である IPA と連携して、再委託先であり評価機関候補 JQA と産総研共同で評価手順書案としてまとめる。平成 28 年度からの評価・認証に備え、再委託先を含む国内企業の製品を使って、再委託先である JQA で評価を試行し、これを通して脆弱性評価組織を育成する。

OCT 測定装置とロボットアーム試験装置を活用した測定誤差の少ない偽造物検知評価技術の研究を産総研で行なう。

また、CC 評価の内容は製品の機微な情報を含むので、評価結果の開示範囲などの扱いについては、認証機関である IPA・各企業と調整して決定する。

(4)精度評価ツールの開発

平成 26 年度に開発した精度評価ツールの開発を継続すると共に、検討の中で判明したベンダー毎のツールカスタマイズの実現に取り組む。また、脆弱性評価手法の開発の中で明確になる脆弱性評価に必要なツールの機能の基本設計に取り組む。

① 当初予定機能の開発

平成 26 年度計画時点で予定されていた、精度評価報告書生成機能のプロトタイプを当初計画どおり開発する。

② 追加機能（平成 26 年度計画時点で予定になかった機能）の開発

(a) ベンダー毎のツールカスタマイズ

・ベンダーヒアリングにより明らかになった、BioAPI の実装に関するベンダー毎の差異を吸収するための実現方式を検討し、ツールの変更作業を実施する

・大規模評価を可能とするためのベンダー社内バイオメトリックデータベース（多人数のバイオメトリック・データが格納されている）を用いた精度評価方法について検討する

※ツールカスタマイズは、各ベンダーから実装の詳細情報を入手し、個別にツールを修正することで実現する。(例 : BioAPI V1.1 対応、ベンダー社内データベースを用いた他人受入率評価のための各種対応など)

(b) 脆弱性評価に関わる機能追加（基本設計のみ）

精度評価ツールの価値向上のため、脆弱性評価に関わる機能の基本設計を行う。

(5)平成 28 年度のパイロット評価に向けた協力ベンダーによる準備実施

本事業に参加していただいているベンダーに協力をいただき、平成 28 年度に予定するパイロット評価に向けた準備として、製品選定と ST 開発と評価トライアルの準備を行う。

(a) 製品選定と ST 開発

対象製品選定と協力ベンダーにより評価用資料を作成する。

(b) 評価トライアルの準備

協力ベンダーによる評価エビデンスの作成と 評価機関による評価体制を準備する。

(6)国際標準化活動

本事業の成果を基にして、次の標準化活動を進める。

(a) SC 37 ISO/IEC 30107-3 Biometric presentation attack detection

脆弱性評価手法で得た成果をコメントして反映させる。

(b) SC 27　ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics

作成した PP の内容をのプロジェクトへ反映させる。

(c) 評価ツールの開発を通じて得た知見をもとに、SC 37 への新規国際提案の可能性を検討する。

参考文献

[1] ISO/IEC 19795-1:2006 Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework

[2] ISO/IEC 19795-2:2007 Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation

[3] ISO/IEC 2382-37:2012 Information technology -- Vocabulary -- Part 37: Biometrics

[4] JIS X 8101-1:2010 情報技術–バイオメトリック性能試験及び報告–第１部：原則及び枠組み

[5] JIS X 8101-2:2010 情報技術–バイオメトリック性能試験及び報告–第２部：テクノロジ評価及びシナリオ評価の試験方法

[6] Ctirad Sousedik, Christoph Busch. “Quality of Fingerprint Scans captured using Optical Coherence Tomography,” Proceedings of International Joint Conference of Biometrics 2014, September 2014.

[7] “LivDet - Liveness Detection Competitions,” http://livdet.org.

[8] “Tabura Rasa,” https://www.tabularasa-euproject.org.

[9] A. Sequeira, H. Oliveira1, J. C, Monteiro, J. P. Monteiro and J. Cardoso “MobILive 2014 - Mobile Iris Liveness Detection Competition, ” Proceedings of International Joint Conference of Biometrics 2014, September 2014.

[10] Jukka Komulainen, Abdenour Hadid, Matti Pietikainen, “Generalized textured contact lens detection by extracting BSIF description from Cartesian iris images,” Proceedings of International Joint Conference of Biometrics 2014, September 2014.

[11] M. Une and A. Otsuka. “Wolf attack probability: a new security measure in biometric authentication systems. “ Lee, S.-W., Li, S.Z.(eds.) ICB 2007, LNCS, Vol. 4642, pp. 396–406, 2007.

[12] Y. Tanabe and H. Yoshizoe, K. Imai. “A study on security evaluation methodology for image-based biometrics authentication systems.” In 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, pp. 1–6. IEEE, September 2009.

[13] Tetsushi Ohki, Seira Hidano, and Tatsuya Takehisa. “Evaluation of wolf attack for classified target on speaker verification systems. “ In International Conference on Control, Automation, Robotics and Vision, pp. 182–187, 2012.

[14] 大木 哲史, 大塚 玲. “尤度比に基づく生体認証方式の脆弱性とウルフ安全性評価,” 暗号と情報セキュリティシンポジウム 2015(SCIS2015), 3B2-5, January 2015.

[15] FIDIS (Future of Identity in the Information Society). D6.1 Forensic Implications of Identity Management Systems. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf

[16] D.Davis, P.Higgins, P.Kormarinski , J.Marques,N.Orlans, J.Wayman. State of the Art Biometrics Excellence Roadmap, MITRE TECHNICAL REPORT was produced for the U. S. Government under contract J-FBI-07-164 , October 2008; v1.2

[17] WANG, Yiding; ZHAO, Zhanyong. Liveness Detection of Dorsal Hand Vein Based on the Analysis of Fourier Spectral. In Biometric Recognition. Springer International Publishing, 2013. p. 322-329.

[18] 松本 勉, 鉢嶺 拓二, 田辺 壮宏, 森下 朋樹, 佐藤 健二, “バイオメトリクスにおける生体検知と登録失敗（２）－静脈認証システムに関する研究（その１）－,” 電子情報通信学会技術研究報告, ISEC2005-5, pp.29-33, May 2006.

[19] 松本 勉, 森下 朋樹, 李 文, “バイオメトリクスにおける生体検知と登録失敗（３）－静脈認証システムに関する研究（その２）－,” 電子情報通信学会技術研究報告, ISEC2006-5, pp.53-60, May 2006.

[20] 森田, 井沼, 大塚, 今井, 静脈認証模擬システムへのウルフ攻撃に対する安全性評価, 暗号と情報セキュリティシンポジウム (SCIS 2014), 電子情報通信学会、2014.

[21] Tome, Pedro, Matthias Vanoni, and Sébastien Marcel. "On the Vulnerability of Finger Vein Recognition to Spoofing." IEEE International Conference of the Biometrics Special Interest Group (BIOSIG). No. EPFL-CONF-200310. 2014.

[22] Henniger, Olaf, Dirk Scheuermann, and Thomas Kniess. "On security evaluation of fingerprint recognition systems." International Biometric Performance Conference (IBPC 2010), March. 2010.

[23] Bundesamt für Sicherheit in der Informationstechnik, Biometric Verification Mechanisms Protection Profile BVMPP v1.3, August 2008.

[24] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile FSDPP v1.8, November 2009.

[25] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies FSDPP_OSP v1.7, November 2009.

[26] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Evaluation Guidance v2.1, December 2009.

[27] Common Criteria Recognition Arrangement. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1 Revision 4, CCMB-2012-09-001, September 2012.

[28] Common Criteria Recognition Arrangement. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-002, September 2012.

[29] Common Criteria Recognition Arrangement. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003, September 2012.

[30] Information Assurance Directorate, U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.1, July 2007.

[31] Information Assurance Directorate, U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.1, November 2003.

[32] ISO/IEC 15408-1:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, August 2008.
[33] ISO/IEC 15408-2:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components, August 2008.
[34] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components, August 2008.
[35] ISO/IEC 18045:2008, Information technology — Security techniques — Methodology for IT security evaluation, August 2008.
[36] ISO/IEC 19792:2009, Information technology — Security techniques — Security evaluation of biometrics, August 2009.
[37] ISO/IEC WD 30107-3　Information Technology — Presentation Attack Detection — Part 3: Testing and reporting and classification of attacks
[38] UK Government Biometrics Working Group, Biometric Device Protection Profile (BDPP), Draft Issue 0.82, September 2001.
[39] 独立行政法人情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリアパート 1: 概説と一般モデル, バージョン 3.1 改訂第 4 版, 2012 年 9 月
[40] 独立行政法人情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリアパート 2: セキュリティ機能コンポーネント, バージョン 3.1 改訂第 4 版, 2012 年 9 月
[41] 独立行政法人情報処理推進機構, 情報技術セキュリティ評価のためのコモンクライテリアパート 3: セキュリティ保証コンポーネント, バージョン 3.1 改訂第 4 版, 2012 年 9 月
[42] 独立行政法人情報処理推進機構, 情報技術セキュリティ評価のための共通方法 評価方法, バージョン 3.1 改訂第 4 版, 2012 年 9 月

付録１

バイオメトリクスにおける評価技術の国際標準化とその周辺

International Standardization and Related Activities on Evaluation Technology for Biometrics

山田　朝彦† 大木　哲史† 大塚　玲† 口井　英人‡ 神賀　誠‡

†産業技術総合研究所

‡日本品質保証機構

YAMADA Asahiko† OHKI Tetsushi† OTSUKA Akira† KUCHII Hideto‡ KAMIGA Makoto‡

†National Institute of Advanced Industrial Science and Technology

‡Japan Quality Assurance Organization

アブストラクト

バイオメトリクスにおける評価は、API などの準拠性評価、他人受入れ・本人拒否などの精度評価、偽造物検知をはじめとするセキュリティ評価に大別される。これらのそれぞれに対して、ISO/IEC JTC 1/SC 37 を中心に、評価基準の国際標準化が進められている。バイオメトリクス製品を実際に評価するには、評価基準の国際標準化だけでは不十分であり、国内外でさまざまな取組みが進められている。精度と偽造物提示攻撃検知に対する評価、特にそのための共通に使える要件定義は、バイオメトリクス製品に固有のセキュリティ評価として重要になるであろう。その結果として、調達者にも製品ベンダーにも共通の客観的なセキュリティ評価基準を与えることができる。

はじめに

バイオメトリクスにおける評価は、API などの適合性評価、他人受入れ・本人拒否などの精度評価、偽造物提示に対する耐性をはじめとするセキュリティ評価に大別される。これらのそれぞれに対して、情報技術を標準化対象とする ISO/IEC JTC 1(ISO (International Organization for Standardization (国際標準化機構)) と IEC (International Electrotechnical Commission (国際電気標準会議)) の第一合同技術委員会(Joint Technical Committee 1 (JTC 1)))の下のバイオメトリクスを対象とする第 37 専門委員会(SubCommittee 37 (SC 37))を中心に、国際標準化活動が進められている。SC 37 における評価基準の国際標準化活動に基づいて、実際の評価を実現するための取組みが国内外で進んでいる。

適合性評価

バイオメトリクスにおける相互運用のための国際標準規格には､データ構造と API に関するものがある。

データ構造の標準化と適合性試験

データ構造については、バイオメトリック・データ自体とバイオメトリック・データの属性情報などを含むメタデータの国際標準規格がある。前者については､SC 37 の下のデータ交換フォーマットを扱う WG 3 で、ISO/IEC 19794 シリーズ［11］［12］として、モダリティ毎に国際標準化活動が実施されている。

後者については、SC 37 の下のバイオメトリックテクニカルインタフェースを扱う WG 2 が担当しており、ISO/IEC 19785 シリーズ［9］として国際標準規格になっている。

いずれも、バイオメトリクス製品の開発者は知るべき仕様であるが、製品を使用するシステム構築者・調達者・管理者にとっては隠ぺいされた仕様なので、以下では簡単に紹介するにとどめる。以下では、マルチパートの規格については、特別な場合を除き、参考文献ではパート 1 だけを参照する。

ISO/IEC 19794 シリーズ

ISO/IEC 19794 シリーズについては、第 1 世代のデータ構造の国際標準規格が 2005 年から 2007 年にかけて作成され［11］、第 2 世代の国際標準化がその後開始されて 2011 年から規格化されて来ている［12］。適合性試験仕様については、第 1 世代では ISO/IEC 19794 の各パートに対応して ISO/IEC 29109 シリーズ［15］で 2009 年から 2013 年にかけて規格化がほぼ完了している。第 2 世代では ISO/IEC 19794 の各パートに対して追補 1(Amendment 1)で適合性試験仕様が標準化されている［13］。適合性試験には、論理的データの適合性確認（レベル 1）、データ内部の整合性確認（レベル 2）、生体情報内容の確認（レベル 3）の 3 つのレベルが設定されている。米国 NIST(National Institute of Standards and Technology)は、CTS(Conformance Test Suite)を開発者向けの自己評価のための適合性試験ツールとして提供している［19］。対象となっているフォーマットは、第 1 世代については、パート 2 指紋特徴点、パート 4 指紋画像、パート 5 顔画像の 3 つであり、第 2 世代については、上記の 3 パートとパート 6 虹彩画像である。評価の結果、上述のレベル 1 からレベル 3 のどのレベルまで適合しているかが判定される。しかし、これは自己評価に留まり、適合性を認証するスキームは存在していない。

ISO/IEC 19785 シリーズ

ISO/IEC 19785 は、現在 4 つのパートからなっている。パート 1 は、バイオメトリック・データの属性情報の項目を抽象的に定義している。パート 1 の抽象的な定義は、適用分野や使用する団体がパトロンフォーマットと呼ばれる具体的仕様を定義して使用する。パート 3 はいくつかのパトロンフォーマットを定義している。ISO/IEC 19785 シリーズに対する適合性評価の仕様は存在しないが、米国 NIST が、ISO/IEC 19785 の基になった米国 ANSI 仕様のパトロンフォーマット A に対する CTS を開発している［18］。

API の標準化と適合性試験

ISO/IEC 19784 シリーズ 0 は、BioAPI と呼ばれるバイオメトリクス製品の標準 API 仕様を定めている。ISO/IEC 19784 シリーズは、標準 API だけでなく、バイオメトリクスのソフトウェア構造も規定し、BioAPI フレームワークと BSP（Biometric Service Provider）に大きくは分類している。BSP はバイオメトリクスの装置に対応するソフトウェアである。一般のアプリケーションに対する API を提供するのは BioAPI フレームワークであり、BSP は BioAPI フレームワークに対する API である SPI（Service Provider Interface）を提供する。BSP はベンダー各社が実装しているのに対し、BioAPI フレームワークはかつて米国のベンチャー企業が実装し製品化したが既に供給が停止されている。よって、現実には、アプリケーションは SPI を介して BSP に直接アクセスするような構造にならざるを得ない。これは、BioAPI フレームワークの API の仕様と SPI の仕様にあまり差がないため、BioAPI フレームワークを実装しても製品としての付加価値がないことが原因となっている。

ISO/IEC 19784 シリーズに対する適合性試験仕様は、ISO/IE 24709 シリーズ［16］として規格化されている。パート 1 はこのシリーズでの XML を使った試験仕様の記述方法などを規定し、パート 2 はパート 1 に基づいて BSP の SPI の適合性試験仕様を規定している。パート 1 とパート 2 は、ともに 2007 年に規格化され、2012 年に改訂が開始された。パート 1 は改訂作業が継続されているが、パート 2 は編集者が不在となり改訂は停止された。パート 3 は、BioAPI フレームワークの API の適合性試験仕様であり、2011 年に規格化された。パート 3 では、パート 1 に定められた記述方法を使用しつつも、BioAPI 仕様に定められた各 API 関数に対する入力や返却値を表形式で表現し、よりわかり易い試験仕様の記述方法も併せて提案した。この結果は、現在改訂が進むパート 1 にも採用されることになった。パート 3 の内容作成は、実質的には、副編集者を担当した中村敏男（ＯＫＩソフトウェア）によるものである。

パート 3 の作成過程で、各 API 関数に対する期待される入力や返却値の組合せを網羅すると巨大な試験仕様になることから、組合せの妥当なサブセットも抽出できた。その結果、パート 2 における SPI 関数の試験仕様に基準がなく、極めて限定的であることがわかった。これは、上述のとおり、多くの API 関数と SPI 関数に対応関係があるため、わかったことである。BSP は多数の企業によって実装されているので、パート 2 は改訂されることが望ましいが、上記のとおり、改訂は停止されている。

製品が BioAPI 仕様に適合しているか否かがわかることは、相互運用性確認のために、製品調達者・開発者にとっては、重要なことである。多数の企業による BSP の実装があるという状況を反映して、パート 2 の試験仕様が不十分ではあるものの、パート 2 に準拠した適合性試験を韓国インターネット振興院(Korea Internet & Security Agency(KISA))の K-NBTC(Korea National Biometrics Test Center)が実装しており、これに基づいた韓国独自の認証制度も立ち上げている［17］［19］。米国 NIST も BSP の CTS を実装しているが、対象となる BSP 仕様が、ISO/IEC 19784-1 の基になった米国 ANSI 仕様であり、ISO/IEC 19784-1 準拠の BSP を対象としたものには移行していない。なお、韓国 KISA は、K-NBTC による第三者評価には時間がかかるので、それに先立って BSP の実装者が事前に自己評価するための Web ベースの適合性試験ツールを開発していることが報告されている［22］。

日本では、経済産業省アジア基準認証推進事業として、日本自動認識システム協会とＯＫＩソフトウェアが、ベンダーが第三者組織に製品を持ち込まなくても評価を可能にするリモート適合性評価のための CTS プロトタイプを、限定的な仕様であるが、開発・実装した［21］［22］。この CTS プロトタイプの特徴は、この活動で開発した BioAPI フレームワークが CTS プロトタイプの一部として動作して、評価対象である BSP を呼び出して試験することである。従来の BSP の適合性評価は ISO/IEC 24709-2 準拠でなされて来たが、この CTS プロトタイプでは内包される BioAPI フレームワークが ISO/IEC 24709-3 仕様に基づいて試験される結果として BSP を試験する構造になっている。よって、この CTS プロトタイプの構造は、ISO/IEC 24709-2 の試験仕様としての不備を補って、ISO/IEC 24709-3 と同等の精度の試験仕様に引き上げて BSP を試験できるようになっている。ISO/IEC 24709-2 の改訂が停止されている状況においては、この CTS プロトタイプは、リモート適合性評価を可能にしたことよりも、BSP の新しい CTS 構造を提示したことの意味が大きい。しかし、この CTS プロトタイプは、まだ実用化されていない。

精度評価

精度評価に関する国際標準規格は、ISO/IEC 19795 シリーズである。2006 年に規格化されたパート 1 では、精度評価を実施するに当たっての種々の指針が提示されている。提示されている指針は、計画作成、データ収集、分析のための指標（FTE (Fail ure-To-Enrol rate、生体情報登録失敗率)、FAR (False Accept

Rate、 他人受入れ率)、FRR (False Reject Rate、本人拒否率)など)、記録、報告に関するものである。2007年に規格化されたパート 2 では、特徴抽出及び照合のアルゴリズムを評価する技術評価とデータ採取から始まるシステム全体での評価を対象とするシナリオ評価に対して、より詳細な指針が示されている。

精度評価には、データとなる生体情報の提供者（被験者）が必要であり、高い精度での精度評価にはより多くの被験者が必要である。被験者を N 人とすると、FAR は 1/N(N-1)の桁数を超えることはなく、FRR は 1/N の桁数を超えることはないからである。

評価の実施者は、一般に、製品ベンダー自身、製品調達者、第三者のいずれかである。高い精度での精度評価は、いずれにとっても意味がある。製品ベンダーにとっては製品力訴求になり、製品調達者・第三者にとっては製品比較に寄与するからである。しかし、より多くの被験者を集めるには、被験者の協力、最終的には費用が必要になる。規模の大きい製品ベンダーの場合は、製品ベンダーの従業員を使って相対的に低コストで被験者を集めることができる。製品調達者・第三者による評価の場合には、被験者を低コストで集められるかが問題になる。

第三者による精度評価で良く知られているのは、米国 NIST によるものである。NIST の精度評価は、指紋・顔・虹彩を対象とするものであり、これらはいずれもボーダーコントロールで使用するモダリティである。NIST の精度評価結果は、国家の製品調達にフィードバック可能であり、製品調達者による評価という側面も持っている。

製品ベンダーによる精度評価は、製品訴求力と関係するので、一般的には客観性に乏しいとみなされる。得られた結果の信頼性は、製品ベンダーに依存することになる。製品調達者・第三者による評価の客観性は高いが、多くの製品ベンダーが自己評価をしていることを考えると、全世界的な規模では多重のコストを発生させることになる。特に、製品調達者による評価は、製品調達者毎に行なわれるので、製品調達者の分だけコストも重複することになる。第三者による評価を活用できれば、このコストは低減できる。米国 NIST の精度評価はモダリティが限定されているので、より多くのモダリティに対する第三者による精度評価が期待される。

しかし、第三者による精度評価には、被験者収集のコストがかかる。これを回避するため、製品ベンダーによる精度評価結果を第三者が認証するという考えが、［22］に示されている。製品ベンダーが精度評価を実施するに当たり、その評価結果の信頼性を主張できるエビデンスを同時に収集し、そのエビデンスを第三者が確認することによって、製品ベンダーによる精度評価を追認できるようにする考えである。ここで提示されているエビデンスの妥当性は十分とは言えないが、製品ベンダーによる精度評価結果を第三者が活用するという考え方には意味があると考えられる。

セキュリティ評価

バイオメトリクスを使ったユーザ認証は、その後に実行されるアプリケーションのセキュリティの基礎になるという意味で、その重要性は大きい。よって、バイオメトリクス製品のセキュリティ評価の重要性は大きい。セキュリティ評価においては、評価が客観的であることが特に要求される。客観的なセキュリティ評価の枠組みとしては、SC 27（セキュリティ技術）でも ISO/IEC 15408[28]として国際標準化されているよる CC(Common Criteria)[26]がある。しかし、CC は一般の IT 製品を対象としており、バイオメトリクス製品のセキュリティ評価としては不十分であることを、SC 27 で国際標準化された ISO/IEC 197920 は主張している。この活動においては、日本から副編集者として、三村昌弘（日立）・大塚玲（産総研）が貢献した。

ISO/IEC 19792

ISO/IEC 19792 では、CC パート 2 のセキュリティ機能要件及びパート 3 のセキュリティ保証要件がバイオメトリクス製品に対して不十分な点として、エラー率（精度）、脆弱性評定、プライバシーを挙げている。ただし、ISO/IEC 19792 の「プライバシー」は、パーソナルデータであるバイオメトリック・データの保護であり、バイオメトリクス製品以外のパーソナルデータ保護より多くの内容を含んでいない。バイオメトリクスにおけるプライバシーの議論は十分なされておらず、また、プライバシー確保のための技術も確立されていないので、バイオメトリクス製品におけるプライバシーに関するセキュリティ評価を論ずることは時期尚早であろう。

よって、ISO/IEC 19792 の主張で考慮すべきバイオメトリクス製品のセキュリティ評価の内容は、精度と脆弱性評定である。精度と脆弱性評定には依存関係がある。FAR が十分でないことは、それ自体が脆弱性を示していることになるからである。

ISO/IEC 19792 ではバイオメトリクス製品のセキュリティ評価の考え方を示してはいるが、これを基にした評価スキームは存在していない。しかし、ISO/IEC 19792 自体が CC 評価におけるバイオメトリクス製品評価に不足するものを検討していることを考えれば、CC 評価を活用するのが妥当である。

CC では、パート 2 のセキュリティ機能要件またはパート 3 のセキュリティ保証要件に不足する要件を、セキュリティ要件定義書である PP (Protection Profile)やセキュリティ設計仕様書である ST (Security Target)で、拡張コンポーネントとして定義して、使うことができる［1］［5］。精度や脆弱性評定に関する要件を、パート 2 の FIA（識別と認証）の拡張コンポーネントとして扱えれば、ISO/IEC 19792 が示すバイオメトリクス製品のセキュリティ評価の CC を使った実現が可能になる。

ISO/IEC 19792 を考慮した CC 評価

CC の制度では、評価機関による評価の後、最終的に認証機関（日本の場合は情報処理推進機構）によって認証されて、認証書が発行される。CC による評価・認証は、製品ベンダーに多くのコストを発生させると言われている。その原因は、CC が要求する ST 及びエビデンスの作成にあるとの指摘がある。ST 作成は評価のはじめに行なわれるが、製品ベンダーが作成した ST が評価機関や認証機関に認められず、多数の書直しが生じることが高コストとなる原因として指摘されている。エビデンス作成には一定のコストがかかることはやむを得ないが、CC 評価・認証のために新たにコストが発生するか否かは、製品ベンダーの既存開発過程におけるエビデンス作成方針に依存する。

一般に設計仕様書が要件定義書に基づいて作成されるように、もしセキュリティ要件定義書である PP があれば、ST は PP に基づいて作成できる。もし多くの用途に適用できる PP があれば、［1］［5］にあるように PP の記載内容と ST の記載内容が大きく類似しているため、上記の ST 作成のコストを低減できることになる。

CC で対応し切れないバイオメトリクス製品に固有の評価（再検討）

バイオメトリクス製品の PP のあるべき姿を検討する前に、ISO/IEC 19792 のエラー率（精度）と脆弱性以外にバイオメトリクス製品に固有の評価内容はあるかを再検討しておく。バイオメトリクス製品をユーザ認証機能に限定すれば、他のユーザ認証製品との差異に起因するセキュリティ評価を検討すれば良いことがわかる。

バイオメトリクス製品とそれ以外の大きな差異は、認証の成否が決定的に決まるか否かである。その差異は、バイオメトリクス製品のユーザ認証におけるバイオメトリック・データ採取の際のノイズやアナログデータからデジタルデータへの変換に起因する。ここからエラー率（精度）評価の必要が生じる。

いずれの認証においても本人が処理をしていることが前提になるが、バイオメトリクス製品の場合の前提は本人が生体を提示していることになる。最終的な判定はデジタルデータでの処理になるので、ユーザ認証時に本人の生体からデジタルデータ（バイオメトリックデータ）が生成されることが、正しい認証のために必要である。これについて、ISO/IEC 19792 の脆弱性に関する記述を基に検討する。

ISO/IEC 19792 が示す脆弱性は、以下のとおりである。

A。 精度の限界

B。 偽造物提示

C。 自分でなく見せたり（認証や識別を失敗さ　せる）他人をまねる（なりすまし）

D。 露出（顔など）または残存（指紋など）する生体データ（偽造物作成の元データにする）

E。 近親者のデータ類似（なりすまし）

F。 人間のラムやウルフ

G。人工ウルフ

H。 ノイズの入ったデータによる照合成功（特にノイズの入ったテンプレートと）

I。 不正な登録（異なる ID での登録、偽造物での登録、ノイズの入ったテンプレート）

J。 バイオメトリック・データの漏えい・置換

それぞれの関係は以下の図 1 のとおりである。

D、I、J は、それ自体がバイオメトリクスによるユーザ認証の脆弱性となるのではなく、他の脆弱性の誘因となるものである。

A は精度評価自体で評価され、F の人間のラムやウルフも精度評価の中で評価される。

C は評価者自身による実行は難しく、E はデータ取得が難しいので、評価に適用するのは難しい。

残る B、G、H は、PAD(Presentation Attack Detection)が扱う脆弱性であり、PAD 評価によって評価される。

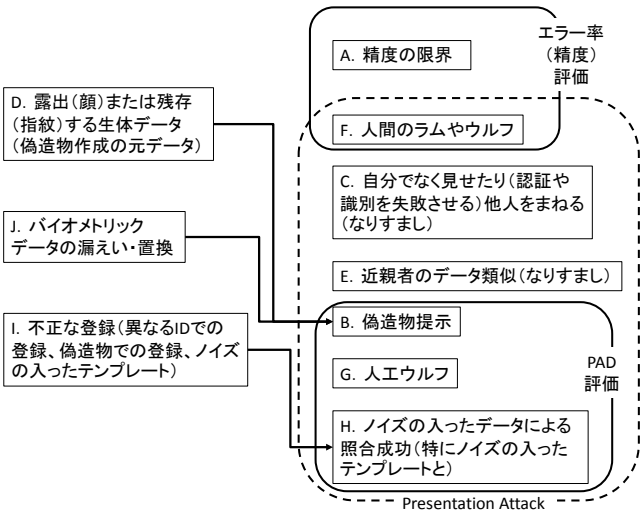


図 1　ISO/IEC 19792 が提示する脆弱性の関係図

他の脆弱性の誘因となるものを併せると、本人の生体に由来するバイオメトリック・データか否かを評価するためには、D、I、J、B、G、H の評価が必要である。ただし、I は登録における脆弱性なので、ユーザ認証だけの評価であれば除外される。

以上から、バイオメトリクス製品に固有の評価内容は、ISO/IEC 19792 のエラー率（精度）と PAD とその誘因だけである。

期待される PP のあり方

以下では、バイオメトリクス製品の PP のあるべき姿を検討したい。そのために、先ず諸外国における PP 作成の取組みを見てみる。

英国では、バイオメトリックデバイスの PP を 2001 年に作成していたようだが、ドラフトしかない［19］。CC の旧版に基づいたもので、FAR・FRR に関するセキュリティ対策方針に対応するセキュリティ機能要件に不備がある。

米国では、２つの PP が認証されたが[28][31]、ともに 2008 年に失効している。［6］には通信データの暗号化が要求されているのに対して、［5］にはそうした要求はない。［6］では［5］ よりも、高い攻撃能力を想定した脅威を挙げ、セキュリティ対策方針も高度である。この２つの PP の最大の欠陥は、テンプレートが暗号の秘密情報と同様にランダムに生成でき、よって FAR や FRR が制御できるかのように考えられて、機能要件が設定されていることである。

ドイツでは、2008 年から 2009 年に、３つの指紋向けの PP が作られた［1］［2］［3］。［1］は、ユーザ認証自体を対象とした PP で、偽造物提示によるなりすましは想定されていない。［2］と［3］はなりすまし検知機能に特化した PP で、［2］はなりすましなどの脅威を想定している。これに対し、［3］は、脅威を想定せずに、バイオメトリクス製品がなりすまし検知することを組織のセキュリティ方針として、求めている。その結果、［2］では脆弱性評定が保証要件になっているのに対して、［3］では保証要件になっていない。これらの PP は、これまでの PP と比べると、内容が良く整理されている。しかし、［1］は種々の脅威への対策が監査データのチェックによって成されることになっており、実装に大きく依存するので、一般性を欠く。［2］と［3］の差異は脆弱性評定の有無で、［3］に基づいた評価では実際の攻撃

による評価は実施されない。［2］の特徴は、CC パート 3 にない最低レベルの攻撃能力を定義し、その攻撃能力での脆弱性評定を実施することを求めていることである。

PP はセキュリティ要件定義書であり、本来は調達者が示すものである。しかし、最近は、世界で共通の PP である cPP（collaborative PP）を作る動きもある。バイオメトリクス製品にも cPP ができて、共通の基準で製品が比較できるのは、調達者には望ましいことであろう。バイオメトリクス製品に共通の評価項目は、以上で見て来たように、精度と PAD の評価になる。精度だけではセキュリティ評価とは言い難く、一定の精度が満たされてはじめて PAD の意味があることを考えれば、この 2 つの評価がセットになっていることが望ましい。

PP をバイオメトリクス製品の比較のための共通基準にするには、PP における評価対象（TOE (Target Of Evaluation)）がバイオメトリクス製品に共通しなければならない。データ採取機能とテンプレート保存機能を除いた部分が多くのバイオメトリクス製品に共通の機能と考えられるので、これを TOE とするのが適切であろう。

おわりに

適合性評価、精度評価、精度評価と PAD 評価を組みにした CC の枠組みを使ったセキュリティ評価、特に共通に使える PP を作成することの重要性について述べた。しかし、精度評価については、製品ベンダー評価と第三者評価の問題が残っている。製品ベンダーの評価結果を、評価機関が統計学的検証をすることで、CC 評価の枠組みの中で活用できるようにすれば、バイオメトリクス製品の CC 評価の意味はより増すであろう。また、このような PP は攻撃能力毎にシリーズ化されて行くことが、調達者にとっても製品ベンダーにとっても望ましいと考える。

PAD 評価については、SC 37 で ISO/IEC 30107 Presentation attack detection のプロジェクトが 3 パートで進行している。パート 3 は Testing、 reporting and classification of attacks で大木哲史（産総研）が副編集者を担当している。また、SC 27 では、2014 年 10 月の国際会議で ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics が新規作業項目として成立し、PAD の CC 評価を扱う。山田朝彦（産総研）が編集者に就任した。これらの活動は、本稿で述べたバイオメトリクス製品のセキュリティ評価を促進することになるであろう。

謝辞

たくさんのご教示をいただいた SC 37 及び SC 27 の専門家の方々、並びに戦略的国際標準化加速事業の委託をいただいた経済産業省に深謝します。

参考文献

[1] Bundesamt für Sicherheit in der Informationstechnik, Biometric Verification Mechanisms Protection Profile BVMPP v1.3, August 2008.

[2] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile FSDPP v1.8, November 2009.

[3] Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies FSDPP_OSP v1.7, November 2009.

[4] Common Criteria Recognition Arrangement. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1 Revision 4, CCMB-2012-09-001, September 2012.

[5] Information Assurance Directorate, U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 1.1, July 2007.

[6] Information Assurance Directorate, U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.1, November 2003.

[7] ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, December 2009.

[8] ISO/IEC 19784-1:2006, Information technology — Biometric application programming interface — Part 1: BioAPI specification, May 2006.

[9] ISO/IEC 19785-1:2006, Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification, May 2006.

[10] ISO/IEC 19792:2009, Information technology — Security techniques — Security evaluation of biometrics, August 2009.

[11] ISO/IEC 19794-1:2006, Information technology — Biometric data interchange formats — Part 1: Framework, April 2006.

[12] ISO/IEC 19794-1:2011, Information technology— Biometric data interchange formats — Part 1: Framework, June 2011.

[13] ISO/IEC 19794-1:2011/Amd 1:2013, Conformance testing methodology, February 2013.

[14] ISO/IEC 19795-1:2006, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework, February 2006.

[15] ISO/IEC 24709: 2007, Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures, February 2007.

[16] ISO/IEC 29109-1: 2009, Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 — Generalized conformance testing methodology, September 2009.

[17] Kwon, Y.B. and Kim, J, K-NBTC BIOMETRIC TEST SERVICES AND CERTIFICATION, Biometric Consortium Conference 2013, September 2013 http://www.biometrics.org/bc2013/presentations/int_kwon_wednesday_1040.pdf

[18] Lee, Y., Podio, F.L., Jerde, M., Conformance Test Suite for CBEFF Biometric Information Records, Proc. of First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007 (BTAS 2007), VA, September 2007, 1-4.

[19] UK Government Biometrics Working Group, Biometric Device Protection Profile (BDPP), Draft Issue 0.82, September 2001.

[20] Yaga, D., Podio, F.L., McGinnis, C.J., BioCTS for ISO/IEC Binary and XML Encoded Records User Guide, August 2014.
http://csrc.nist.gov/groups/ST/BiomResCenter/CTA_BETA/BioCTS_for_ISO_IEC_XML.pdf

[21] 一般社団法人日本自動認識システム協会 ＯＫＩソフトウェア株式会社, 平成２４年度アジア基準認証推進事業費補助金事業アジア生体認証技術評価基盤システムの構築活動報告書, March 2013

[22] 一般社団法人日本自動認識システム協会 ＯＫＩソフトウェア株式会社, 平成 25 年度アジア基準認証推進事業費補助金事業 アジア生体認証技術評価基盤システムの構築活動報告書, March 2014

付録 2

Protection Profile for Biometric Verification Products

Based on ISO/IEC 19792

I

2015/02/12

Contents

・1. PP introduction

・1.1. PP reference

Title:	Protection Profile for Biometric Verification Products (BVPPP)
Version	1.0
Date	
Author	YAMADA Asahiko, National Institute of Advanced Industrial Science and Technology
Registration	
Certification-ID	
CC-Version	3.1 Release 4
Keywords	authentication; biometric; face-recognition; fingerprint-recognition; iris-recognition; Protection Profile; vein-recognition

・1.2. P overview

This PP specifies security functional requirements and security assurance requirements specific to products for biometric verification in terms of CC. Security functional requirements specific to products for biometric verification, which are not found in password or PKI authentication products, are those of error rates, FAR and FRR, and of presentation attack detection. As a result, threats irrelevant to error rates or presentation attack are not dealt with in this PP. Spontaneous failures of the TOE and its operational environment are out of scope of this PP.

This PP is independent of modalities (fingerprint, face, iris, vein, etc.) and parts of the body used for biometric verification. This PP is only for biometric verification, not for enrolment or biometric identification. The PP for enrolment and biometric identification will be defined in other document.

Note: Biometric verification and biometric identification are explained in 0.

This PP is supposed to be used for procurement of biometric products when they are applied to systems for the purpose of user authentication. Vendors shall write STs based on this PP adding appropriate descriptions of their products.

・1.3. TOE overview

・1.3.1TOE type

The TOE is a product used for biometric verification. The functions for enrolment and biometric identification are not considered. The TOE provides user authentication function of high usability and special characteristic that only the enroled user is authenticated with the authentication data of his/her biometric characteristic such as face, fingerprint, iris, or vein. The TOE does not contain Capture function, which captures biometric characteristic of the user, and Storage function, which stores the biometric reference template of the user. The user is assumed to have his/her biometric reference template enroled beforehand in Storage, which is out of the TOE, and is to be ready to use the biometric verification function of the TOE.

・1.3.2. Non-TOE hardware/software/firmware available to the TOE

The operational environment shall be available to the TOE as instructed in the guidance document in order to run and use the TOE. From a biometric functional point of view, a Capture Device for Capture function and a product for Storage function such as a database software are available to the TOE.

The hardware available to the TOE is a dedicated hardware to the TOE, a general-purpose PC, or a mobile device such as a smartphone. One of the software available to the TOE is an OS. It may be a dedicated OS to the hardware, Windows OS or Mac OS for PCs, or iOS or Android OS for mobile devices, depending on the hardware on which the TOE runs. Antivirus software is also available if the TOE runs on a general OS on PCs or mobile devices.

For example, a TOE running on a PC is software on an OS for the PC. If the embedded camera on the PC is used as the Capture Device, the driver for the camera belongs to the operational environment of the TOE. ST authors shall specify the operational environment for the TOE to work with. Procurer shall prepare the operational environment required for the TOE.

・1.3.3. Usage of a TOE

Examples of the TOE are biometric products for user authentication used for PC login in offices, those for ATMs at banks, those for unlocking door, those for unlocking mobile devices such as smartphones. If the TOE is used for PC login in offices, the operation to the TOE is seen by particular or general people in office hours. But after and before office hours, no one may be in the office. In such a situation, the TOE is assumed to be stored to a safe place if it is portable as a general rule. If the TOE is used for ATM or unlocking door, it is generally set fixed to the facilities and watched by a video surveillance system or security guards. If the TOE runs on a mobile device, most of the operational environment can stop its functions when the mobile device is lost or stolen.

The minimal system of systems which contain biometric verification mechanism consisting of the TOE, Capture function, and Storage function is called a Biometric System (BS) in this PP.

To use a BS, enrolment process is necessary at first. During the enrolment process, the BS captures the biometric characteristic, of which the TOE specifies the modality (face, fingerprint, iris, vein, etc.) and the part of the body (finger, palm, or back of hand if the hand is used), of a user and extracts the features.. The quality of the biometric feature has to be checked. In the case of lower quality, the user has to repeat the process or is impossible to be enroled. If the quality is sufficient, then the set of features is stored as a biometric reference template in Storage (database) combined with the identity of the user.

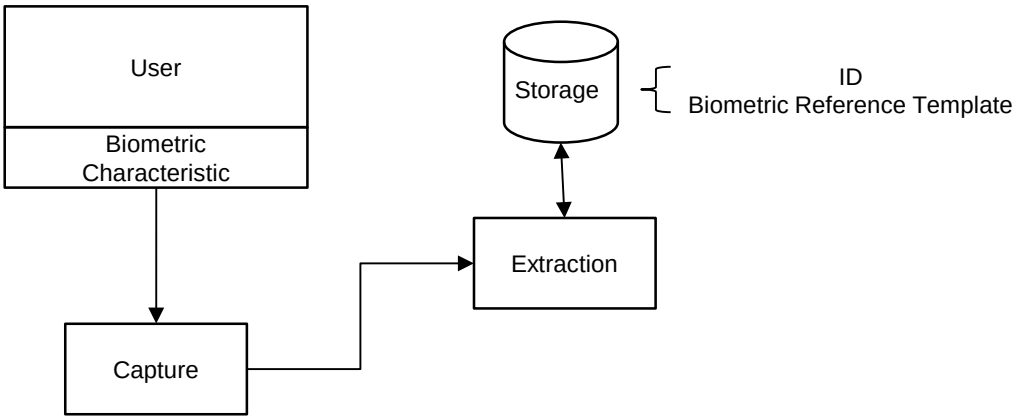


Figure 1 Enrolment process

For a BS, the verification process is the major functionality to verify or refuse a claimed identity of a user. The user has to claim an identity to the BS. The BS gets the biometric reference template associated with this identity from Storage and captures the biometric characteristic of the user using Capture. If the biometric feature extracted from the characteristic and the biometric reference template from Storage are similar enough, the claimed identity of the user is verified. Otherwise or if no biometric reference template was found for the user, the claimed identity is refused.

Decision function decides whether the biometric reference template and the extracted biometric feature are similar enough. Decision uses a threshold value for the decision. The threshold value may be configured by the administrator of the BS. If Decision finds that the similarity of the extracted biometric feature against the biometric reference template is more than the threshold value, it returns Success, otherwise Failure.

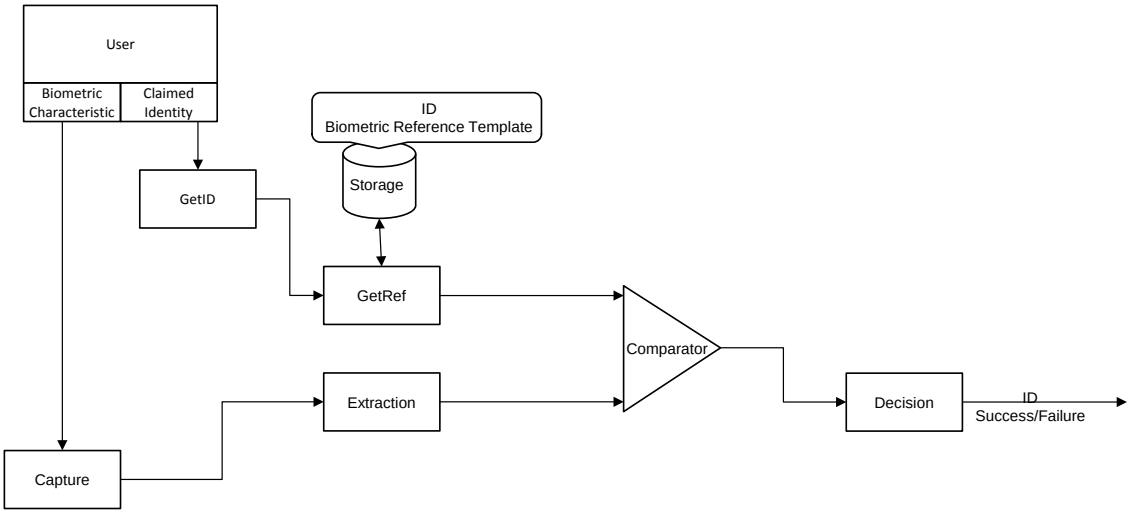


Figure 2 Biometric verification process

In this PP, an enroled user can access logical or physical assets after successful biometric verification.

Note 1: An example of a physical asset is a space available after successful biometric

verification at the door. That of a logical asset is digital data or applications available after successful biometric verification at a web system. The use cases of biometric verification is almost the same as those of password authentication.

Note 2: There is another application of biometrics, biometric Identification. In contrast to a biometric verification process, there is no claimed identity for the user. The system directly captures the biometric characteristic of a user and compares it to all biometric reference templates in Storage. If at least one biometric reference template is found to be similar enough, the system returns this as the found identity of the user.

・1.3.4. Major security features of TOE

The major security feature of the TOE is biometric verification used for user authentication. Comparing with other user authentication method such as password or IC card used, biometric verification has advantages as follows.

When password authentication is used, there are often the cases that a user has forgotten his/her password and is not authenticated. There are also the cases that inappropriate management of password results in impersonation. When an IC card is used for authentication, a user cannot be authenticated if he/she does not carry the IC card. When the IC card is lost or stolen, impersonation may be done. In either case of authentication methods, the security level decreases by inappropriate management and the usability is not sufficient.

When biometric verification is used, a user does not have to memorize or carry anything in order to be authenticated because his/her biometric characteristics are used as authentication data. Biometric verification is high in usability and difficult in impersonation.

・1.3.4.1 Characteristics of biometric verification

Biometric verification provides its own different characteristics from other authentication methods. These characteristics relate to the vulnerabilities and threats.

(1) Error rates: FAR (False Accept Rate) and FRR (False Reject Rate)

In biometric verification, a user is verified if the similarity of the extracted biometric feature against the biometric reference template exceeds the threshold value as stated in 0. Therefore an enroled user may be falsely rejected and an attacker may be falsely accepted. The rate of false reject is called FRR (False Reject Rate) and that of false acceptance is called FAR (False Accept Rate).

FAR and FRR are the shaded areas depicted in Figure 3. The curve Imposter represents the distribution of the frequency of successful comparison result between a biometric reference template and an extracted biometric feature of a different user. On the other hand, the curve Genuine represents the distribution of the frequency of successful comparison result between a biometric reference template and an extracted biometric feature of the same user.

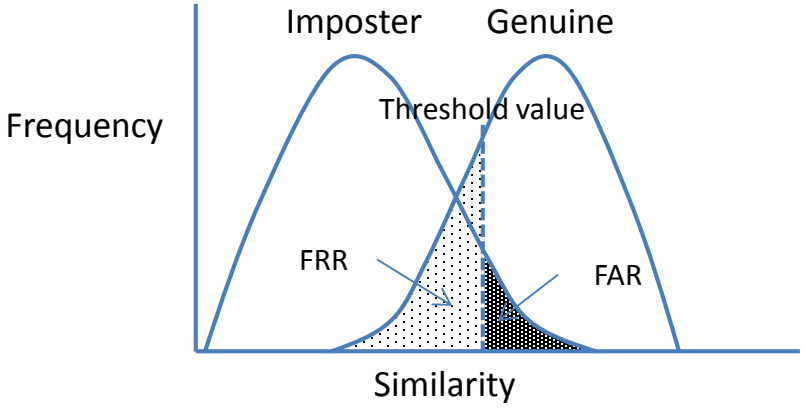


Figure 3 Distribution of similarity in biometric verification

If the threshold shifts to the right, the FAR decreases but the FRR increases. That results in a biometric system of less usability. If the threshold shifts to the left, the FRR decreases but the FAR increases. That results in a biometric system of less security.

To address the issues related to FAR and FRR, the TOE is to have a function to satisfy a sufficient FAR and FRR.

(2) Presentation attack

There is an attack method called presentation attack to biometric systems, presenting fake biometric to Capture Device for the sake of impersonation. To address this issue, the TOE is to detect or reject presentation attacks at a certain appropriate rate.

- **1.3.4.2 Attack methods against the TOE and attack potential**

Typical attacks to biometric systems are attacks exploiting the error rates and presentation attacks as explained in0. The concrete methods for these attacks and the necessary attack potentials depend on the modality and operational environment. As stated in 0, threats irrelevant to error rates and presentation attack are not dealt with in this PP. As written in 0, the TOE is used in an environment where it is seen by particular or general people as in office in the office hours and stored to a safe place when no one is around the TOE for a long time, if the TOE is portable. The TOE in a biometric system runs in an operational environment which prevents the TOE from being analyzed or taken away though the TOE may be bought and analyzed for a long time. For an attack to be successful, attack potential beyond a certain level is necessary. In this PP, protection against attackers possessing basic attack potential is considered.

- **1.3.4.3. Security management functions**

The setting of security relevant data of the TOE, possibly including the threshold value, is done with the security management functions of the TOE. Only the authorized administrator of the BS can access the security management function of the TOE.

Note: The details of the management functions cannot be specified in this PP and shall be specified in ST.

・1.3.5. TOE configuration and operational environment

The configuration of the TOE is categorized into the following two cases. This PP can be applied to both cases.

・Integrated Type: The components of the TOE are not physically separated, i.e., the components are not connected by USB cables or network.

・Separated Type: The components of the TOE are physically separated, i.e., the components are connected by USB cables or network.

Note: This PP can be applied to both cases because these two cases can be treated equally with the assumption A.COMMUNICATION and A.ENVIRONMENT defined in 0.

The performance of a biometric product depends on the physical environment where it is used. Physical environmental factors depend on the modality of the product and Capture Device. ST author shall describe the Capture Device appropriate to the TOE and the recommended operational environment of the TOE in detail.

・1.3.6. Functions of the TOE

The following Figure 4 depicts an example of functions in the TOE and its operational environment. The TOE does not have Capture function which captures biometric characteristic of the user or Storage function which stores biometric reference templates. The TOE does not contain none of audit logging, security audit, and security audit review functions.

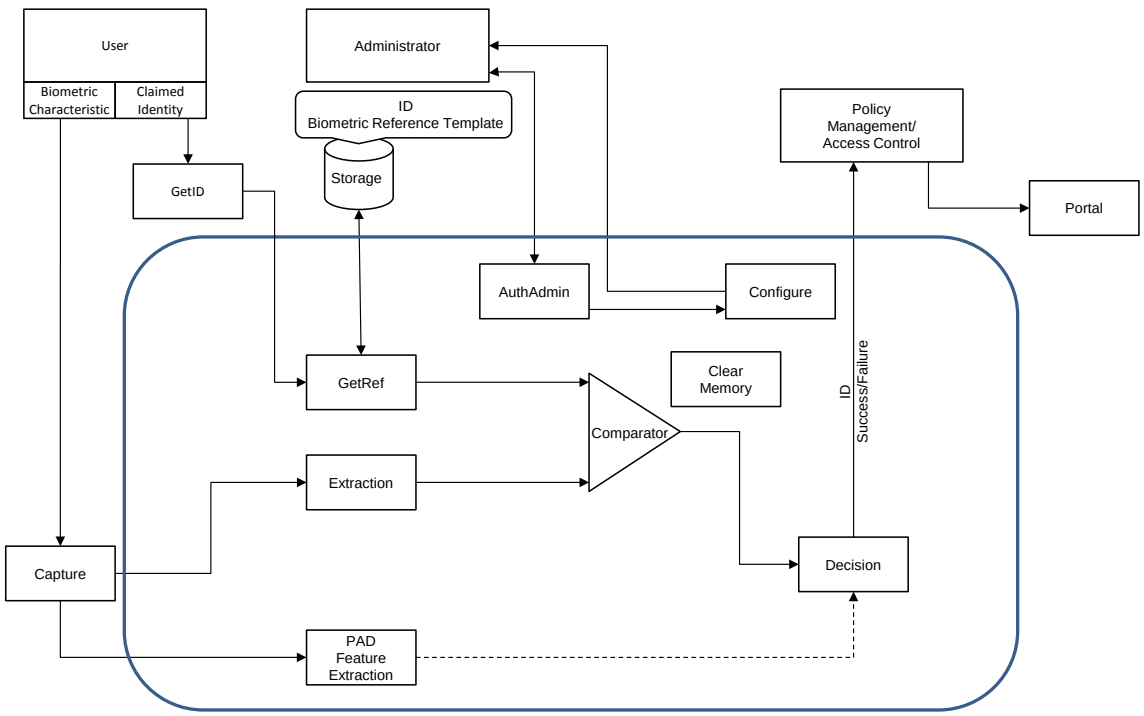


Figure 4 General functions in TOE and its operational environment (example)

The TOE provides the following functions.

・GetRef: This function is responsible for getting the stored (already enroled) biometric reference template related to a user's identity.

・Extraction: In preparation of the verification process, a set of features has to be extracted from a captured data. This is the objective of this function. Optionally, the biometric data may be compressed. The data extracted is called biometric feature.

・Comparator: This function compares the biometric feature from Extraction with the enroled biometric reference template stored in Storage and retrieved via GetRef, and produces a score that shows how well the biometric feature and the biometric reference template match.

・Decision: This function determines whether a score produced by Comparator is regarded as success or failure. To get a Success/Failure return value, this Decision considers a threshold. If the score shows that the biometric feature from Extraction and the biometric reference template are more similar than demanded by the threshold, the return value is Success, otherwise it is Failure. An “Exact match” comparison should not result in a positive verification as it may be a replay attempt.

・PAD Feature Extraction: PAD (Presentation Attack Detection) features are extracted from the raw data captured at Capture function and are used to determine whether there is a presentation attack or not, and are used directly or indirectly to decide Success or Failure at Decision later.

・AuthAdmin: This function is responsible for identification and authentication of the administrator of the BS with other means than the biometric verification mechanism itself. This mechanism may be a smartcard/PIN based mechanism, for example. It is necessary to authenticate an administrator of the BS before he or she is allowed to configure security relevant settings of the TOE.

・Configure: This function provides an interface for the administrator of the BS to set security relevant TOE parameters. This function may be used to configure the threshold setting for the decision function.

・Clear memory: In order to protect against attacks, this function clears the content of memory after use. The information that has to be cleared is not limited to the verification result but especially includes the biometric reference template, biometric feature from Extraction or any biometric raw data as well as authentication data for the authentication of the administrator of the BS.

Some security related functions and interfaces of the TOE operational environment should be considered here:

・Capture: This function is responsible for capturing the biometric characteristic from the user and forwards raw data into the TOE. Capture has no other functions.

・Storage: The environment has to provide a database to be used by the TOE to store the

biometric reference templates of users but it can be used to store additional information, including identity information, too.

- GetID (optional): This function is responsible for getting the user's claimed identity. Its functionality is security relevant because the TOE uses the claimed identity to determine which biometric reference template to be used for comparison. Furthermore, this component provides a mandatory user visible interface. It depends on the product whether the operational environment contains this function or not. For a product for personal use, for example, this function does not have to be necessary because the user is supposed to be unique.
- Policy manager: The result of the biometric verification process is passed on to the policy manager of the environment. This function is responsible for checking the user's rights and opening the portal if the user has sufficient privileges and was successfully verified by the TOE and is therewith realizing an access control mechanism for the portal.
- Portal: The physical or logical point beyond which assets are protected by the TOE operational environment policy management, which gets the verification results (verification "Success" or "Failure") related to the user identity from the TOE.
- Communication: The environment cares for a secure communication where security relevant data is transferred to/ from the TOE or between the components of TOE.

・2. Conformance claims

・2.1. CC conformance claims

This PP has been developed using Version 3.1 Release 4 of Common Criteria (CC).

The conformance of this Protection Profile is CC Part 2 extended (due to the use of FIA_BUA).

The conformance of this Protection Profile is CC Part 3.

・2.2. PP claim

This PP does not claim conformance to any other Protection Profile.

・2.3. Package claim

This PP claims conformance to EAL2 as defined in CC Part 3, augmented by ALC_FLR.1.

・2.4. Conformance statement

This PP allows demonstrable conformance of PPs/STs to this PP.

・3. Security problem definition

・3.1. External entities related the TOE

The following external entities interact with the TOE.

Biometric System Administrator (BS Administrator):

The BS Administrator is authorized to perform the administrative operations of the BS of which the TOE is a part, and able to use the administrative functions of the TOE.

The BS Administrator is also responsible for the installation, settings including HW if necessary, and maintenance of the TOE.

Enroled User:

An Enroled User is a user whose biometric reference template is enroled to the BS and accesses to the assets via the portal by biometrically verified by the TOE.

Attacker:

An Attacker is any individual who is attempting to subvert the operation of the TOE to gain unauthorized access to the assets protected by the portal.

・3.2. Assets

The following assets are defined in the context of this PP.

Primary assets:

Primary assets are either physical or logical systems not belonging to the TOE which the Enroled User can access via the portal after successful biometric verification of the TOE.

Secondary assets:

Secondary assets are the data generated by the TOE, such as biometric data processed in the TOE, and the data in the TOE which are set by the BS Administrator, such as the threshold value for the biometric verification if appropriate, the authentication data for the BS Administrator.

・3.3. Assumptions

A.ADMINISTRATION

The BS Administrator is not hostile. He/she does not become an attacker or give relevant information to attackers. The BS Administrator is well trained and reads the guidance documentation carefully, completely understands, and applies it to the TOE. The BS Administrator is responsible for the installation, settings including HW if necessary, and maintenance of the TOE.

A.ENROLMENT

The biometric reference templates of the Enroled Users are stored in Storage in the operational environment so that the Enroled Users are ready to be biometrically verified by the TOE.

A.CAPTURE

The Capture Device for Capture function operates inside its regular range and is suitable to be used with the TOE. It is assumed that all environmental factors are appropriate with respect to the used Capture Device and biometric modality.

Note: ST author shall add description on the specification of the Capture Device in ST. Spontaneous failures are out of scope.

A.STORAGE

The Storage function in the operational environment stores the biometric reference templates of Enroled Users. Authenticity and integrity are kept in Storage. Access to the biometric reference templates is permitted only to the TOE and administrative operations by the BS Administrator.

Note: Spontaneous failures are out of scope.

A.COMMUNICATION

The communication between the TOE and Capture, between the TOE and Storage, and between the components of the TOE if they are physically separated are protected, cryptographically for example.

Note: Spontaneous failures are out of scope.

A.ENVIRONMENT

Secure operational environment is provided to make the TOE operate. At least, the TOE is protected from malware such as viruses.

Note: For a TOE on a mobile device, the secure operational environment can stop all the functions of the mobile device when it is lost or stolen. If the TOE runs on other kind of hardware, the secure operational environment prevents the TOE from being analyzed or taken away. In either case, the TOE is assumed to work in a secure operational environment where it is not analyzed. Spontaneous failures are out of scope.

・3.4. Threats

T.CASUAL_ATTACK

The attacker may try to present his/her own biometric characteristics in order to get biometrically verified by the TOE using the identity of an enroled user and to access to the primary assets via the portal.

T.PRESENTATION_ATTACK

The attacker may try to present fake biometric characteristics in order to get biometrically

verified by the TOE using the identity of an enroled user and to access to the primary assets via the portal.

T.MODIFY__ASSETS

The attacker may try to make the TOE work abnormally in order to give unauthorized access to the portal, by modifying, destroying, or collecting and exploiting the secondary assets in the TOE.

・3.5. Organizational security policies

P.PORTAL_ACCESSIBLE

The TOE shall not reject Enroled Users beyond a certain rate when they try to get biometrically verified by the TOE.

P.RESIDUAL

After every execution of biometric verification, the TOE and operational environment shall clear the residual data such as biometric data and other relevant data to the Enroled User.

・4. Security objectives

・4.1. Security objectives for the TOE

O.CONTROL_FALSE_ACCEPT

The TOE shall satisfy a certain criteria for the FAR.

O.PAD

The TOE shall detect or reject fake biometric characteristics at a certain rate when they are presented to the Capture Device.

O.AUTH_ADMIN

The TOE shall provide a mechanism to identify and authenticate the BS Administrator.

O.PROTECT_TSFDATA

The TOE shall restrict the access to the security relevant data of the TOE to the BS Administrator. Other users are not allowed to access to them.

O.CONTROL_FALSE_REJECT

The TOE shall satisfy a certain criteria for the FRR.

O.CLEAR_RESIDUAL

After every execution of biometric verification, the TOE shall clear the residual data such as biometric data and other relevant data to the Enroled User.

・4.2. Security objectives for the operational environment

OE.ACCESS_CONTROL

The operational environment shall permit a user to access to the portal if and only if the user is biometrically verified by the TOE.

OE.LIMIT_NUM_TRIAL

The operational environment shall lock a user account if the number of trials of biometric verification to the user exceeds a certain number, recognizing the trials to be an attack.

Note: A biometric product which has a conformant API to ISO/IEC 19784-1 (BioAPI) cannot count the number of trials. Only the application which calls the biometric product conformant to BioAPI can count the number of trials.

OE.ADMINISTRATION

The BS Administrator shall not be hostile. He/she shall not become an attacker or give relevant information to attackers. The BS Administrator shall be well trained and read the guidance documentation carefully, completely understand and apply it to the TOE. The TOE administrator shall be responsible for the installation, settings including HW if necessary,

and maintenance of the TOE.

OE.ENROLMENT

The biometric reference templates of the Enroled Users shall be stored in Storage in the operational environment so that the Enroled Users are ready to be biometrically verified by the TOE.

OE.CAPTURE

The Capture Device for Capture function shall be selected and used in the environment as instructed in the guidance documents.

OE.CLEAR_RESIDUAL_CAPTURE

Having sent the captured biometric data to the TOE, the Capture Device shall clear the residual biometric data.

OE.STORAGE

The Storage function in the operational environment shall store the biometric reference templates of Enroled Users. Authenticity and integrity shall be kept in Storage. Access to the biometric reference templates shall be permitted only to the TOE and administrative operations by the BS Administrator.

OE.COMMUNICATION

The communication between the TOE and Capture, between the TOE and Storage, and between the components of the TOE if they are physically separated shall be protected, cryptographically for example.

OE.ENVIRONMENT

Secure operational environment shall be provided to make the TOE operate, as instructed in the guidance documents. At least, the TOE shall be protected from malware such as viruses.

・4.3. Security objectives rationale

The security objectives address the assumptions, threats, and organizational security policies defined in 0. Table 1 overviews the coverage of the threats, organizational security policies, and assumptions with the security objectives.

Table 1 Security objectives rationale

	O.CONTROL_FALSE_ACCEPT	O.PAD	O.AUTH_ADMIN	O.PROTECT_TSFDATA	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.ADMINISTRATION	OE.ENROLMENT	OE.CAPTURE	OE.CLEAR_RESIDUAL_CAPTURE	OE.STORAGE	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK	×						×	×							
T.PRESENTATION_ATTACK		×					×	×							
T.MODIFY__ASSETS			×	×											
P.PORTAL_ACCESSIBLE					×										
P.RESIDUAL						×						×			
A.ADMINISTRATION									×						
A.ENROLMENT										×					
A.CAPTURE											×				
A.STORAGE													×		
A.COMMUNICATION														×	
A.ENVIRONMENT															×

・4.3.1. Countering the threats

T.CASUAL_ATTACK

T.CASUAL_ATTACK is a threat that an attacker may try to present his/her own biometric characteristics in order to get verified by the TOE. It is countered by a security objective combination of O.CONTROL_FALSE_ACCEPT, OE_ACCESS_CONTROL, and OE.LIMIT_NUM_TRIAL because casual attacks are rejected by the TOE with an FAR which satisfies a certain criteria and the operational environment does not permit the rejected attacker to access to the portal. In addition, the account is locked by the operational environment when the number of the trials of casual attacks exceeds a certain number.

T.PRESENTATION_ATTACK

T.PRESENTATION_ATTACK is a threat that an attacker may try to present fake biometric characteristics in order to get verified by the TOE. It is countered by a security objective combination of O.PAD, OE_ACCESS_CONTROL, and OE.LIMIT_NUM_TRIAL because presentation attacks are detected or rejected by the TOE with a certain rate and the operational environment does not permit the rejected attacker to access to the portal. In addition, the account is locked by the operational environment when the number of the trials of presentation attacks exceeds a certain number.

T.MODIFY_ASSETS

T.MODIFY_ASSETS is a threat that an attacker may try to modify, destroy, or collect and exploit the secondary assets in the TOE in order to give unauthorized access to the portal. It is countered by a security objective combination of O.AUTH_ADMIN and O.PROTECT_TSFDATA because the access to the security relevant data of the TOE is restricted to the BS Administrator that is authenticated by the TOE.

・4.3.2. Coverage of organizational security policies

P.PORTAL_ACCESSIBLE

P.PORTAL_ACCESSIBLE is an organizational security policy that the TOE is required not to reject Enroled Users beyond a certain rate. It is met by O.CONTROL_FALSE_REJECT because this security objective requires an FRR for which the TOE satisfies a certain criteria.

P.RESIDUAL

P.RESIDUAL is an organizational security policy that the TOE and its operational environment are required to clear the residual data such as biometric data and other relevant data to the Enroled User. It is met by a security objective combination of O.CLEAR_RESIDUAL and OE.CLEAR_RESIDUAL_CAPTURE because the residual data in the TOE and that in the Capture Device are cleared after every execution of biometric verification.

・4.3.3. Coverage of the assumptions

A.ADMINISTRATION

The assumption A.ADMINISTRATION is covered by security objective OE.ADMINISTRATION as directly follows.

A.ENROLMENT

The assumption A.ENROLMENT is covered by security objective OE.ENROLMENT as directly follows.

A.CAPTURE

The assumption A.CAPTURE is covered by security objective OE.CAPTURE as directly follows.

A.STORAGE

The assumption A.STORAGE is covered by security objective OE.STORAGE as directly follows.

A.COMMUNICATION

The assumption A.COMMUNICATION is covered by security objective OE.COMMUNICATION as directly follows.

A.ENVIRONMENT

The assumption A.ENVIRONMENT is covered by security objective OE.ENVIRONMENT as directly follows.

For each assumption, the corresponding security objective is stated in a way, which directly corresponds to the description of the assumption. It is clear from the description of each security objective that the corresponding assumption is covered, if the security objective is valid.

・5. Extended component definition

The extended functional family FIA_BUA (Biometric User Authentication) of the Class FIA (Identification and Authentication) is defined here to describe the functionalities of biometric verification used for user authentication which is provided by the TOE of this PP: The TOE shall provide a function of biometric verification for access to the portal. The class FIA (Identification and Authentication) defined in CC Part 2 has been selected to resolve the differences between the requirements in FIA_UAU and those for biometric verification.

The family is named Biometric User Authentication to mean biometric verification used for user authentication.

・5.1. Biometric User Authentication FIA_BUA

Family Behaviour

This family defines the types of biometric user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the biometric user authentication mechanisms must be based.

Component levelling

FIA_BUA.1 Timing of biometric user authentication, allows a user to perform certain actions prior to the biometric user authentication of the user's identity.

FIA_BUA.2 Biometric user authentication before any action, requires that users are biometrically verified before any other action is allowed by the TSF.

FIA_BUA.3 Unforgeable biometric user authentication, requires the biometric user authentication mechanism to be able to detect and prevent the use of authentication data that has been forged.

Management of FIA_BUA.1

The following actions could be considered for the management functions in FMT:

a) management of the TSF data including the threshold value by an administrator;

b) managing the list of actions that can be taken before the user is authenticated.

Management of FIA_BUA.2

The following actions could be considered for the management functions in FMT:

a) management of the TSF data including the threshold value by an administrator.

Management of FIA_BUA.3

The following actions could be considered for the management functions in FMT:

a) management of the TSF data configured for the presentation attack detection or rejection by an administrator.

Audit of FIA_BUA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the biometric user authentication mechanism;

b) Basic: All use of the biometric user authentication mechanism;

c) Detailed: All TSF mediated actions performed before biometric user authentication of the user.

Audit of FIA_BUA.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the biometric user authentication mechanism;

b) Basic: All use of the biometric user authentication mechanism.

Audit of FIA_BUA.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Detection of fraudulent biometric user authentication data;

b) Basic: All immediate measures taken and results of checks on the fraudulent biometric user data.

FIA_BUA.1 Timing of biometric user authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_BUA.1.1

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is biometrically verified.

FIA_BUA.1.2

The TSF shall require each user to be successfully biometrically verified before allowing any

other TSF-mediated actions on behalf of that user with the error rates of FAR [assignment: *X*] and FRR [assignment: *Y*].

Note 1: The values for FAR and FRR shall be given in ST.

Note 2: The evaluation of FAR and FRR shall be done in alignment with ISO/IEC 19795-1

Note 3: FIA_BUA.1 is not used in this PP. This requirement is defined so that it may be referenced by STs for systems in which biometric verification is used.

FIA_BUA.2 Biometric user authentication before any action

Hierarchical to: FIA_BUA.1 Timing of biometric user authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_BUA.2.1

The TSF shall require each user to be successfully biometrically verified before allowing any other TSF-mediated actions on behalf of that user with the error rates of FAR [assignment: *X*] and FRR [assignment: *Y*].

Note 1: The values for FAR and FRR shall be given in ST.

Note 2: The evaluation of FAR and FRR shall be done in alignment with ISO/IEC 19795-1.

FIA_BUA.3 Unforgeable biometric user authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_BUA.3.1

The TSF shall [selection: *detect, prevent*] use of biometric user authentication data that has been forged by any user of the TSF.

Note: The rate to reject forged biometric user authentication data is defined separately by the certification body.

- **5.2. Justification for the definition of functional family FIA_BUA**

User authentication in FIA_UAU is deterministic that authentication with a genuine authentication data is to result in success while biometric verification is not free from the error rates FAR that the result of biometric verification may result in failure even if a genuine biometric characteristic is presented to the Capture Device.

Forgery and copy are considered separately in FIA_UAU while these two cannot be distinguished in biometric verification.

The new family FIA_BUA has been defined because there is not an appropriate family in Class FIA to describe biometric verification.

・6. Security requirements

・6.1. Security functional requirements for the TOE

The following Table 2 summarizes all TOE security functional requirements of this PP.

Table 2 Security Functional Requirements

Class FDP: User data protection	
FDP_RIP.1	Subset residual information protection
Class FIA: Identification and authentication	
FIA_BUA.2	Biometric user authentication before any action - Biometric user authentication for Enroled Users
FIA_UAU.2	User authentication before any action - User authentication for the BS Administrator
FIA_BUA.3	Unforgeable biometric user authentication
FIA_UID.2(1)	User identification before any action (1) - User identification for Enroled Users
FIA_UID.2(2)	User identification before any action (2) - User identification for the BS Administrator
Class FMT: Security management	
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

The following notations are used to mark operations that have been performed:

·Iteration operations are identified with a number inside parentheses (e.g. (1)) after an SFR.

·Assignment operations (used to assign a specific value to an unspecified parameter, such as the length of a password) are denoted by *italicized text*.

·Selection operations (used to select one or more options provided by the CC Part 2 in stating a requirement) are denoted also by *italicized text*. Unselected options are denoted by ~~strike-through text~~.

·Refinement operations (used to add details to a requirement, and thus further restricts a requirement) are denoted by underlined text.

In this PP, there are operations to be completed in ST. They are denoted by shaded text. ST author shall complete such operations.

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] the following objects: [assignment: *list of objects*].

Note: List all the objects to be deallocated.

FIA_BUA.2 Biometric user authentication before any action

Hierarchical to: FIA_BUA.1 Timing of biometric user authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_BUA.2.1 Biometric user authentication for Enroled Users

The TSF shall require each user to be successfully biometrically verified before allowing any other TSF-mediated actions on behalf of that user with the error rates of FAR [assignment: *X*] and FRR [assignment: *Y*].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 User authentication for the BS Administrator

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Note: Authentication mechanism other than biometrics is required for user authentication for the BS Administrator.

FIA_BUA.3 Unforgeable biometric user authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_BUA.3.1

The TSF shall [selection: *detect, prevent*] use of biometric user authentication data that has been forged by any user of the TSF.

Note: This PP does not specify the action against a forged authentication data presented. ST author shall select the option as in the implementation. Either action will do if a forged authentication data is not accepted by the TOE.

FIA_UID.2(1) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1(1) User identification for Enroled Users

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Note: For the case that the identity is used fixed as for personal use of mobile devices such as smartphones, identification may be regarded as successfully done.

FIA_UID.2(2) User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1(2) User identification for the BS Administrator

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [*the BS Administrator*].

Note: The typical TSF data is the threshold value. The assignment is to be specified by ST author.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*BS Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

・6.2. Security assurance requirements for the TOE

The following table summarizes security assurance requirements of this PP. EAL2 augmented by ALC_FLR.1 is applied to this PP.

Table 3 Security Assurance Requirements

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.1
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

・6.3. Security requirements rationale

・6.3.1. Security functional requirements rationale

This chapter proves that the set of security functional requirements is suited to fulfill the security objectives described in chapter 0 and that each SFR can be traced back to the security objectives in 0. At least one security objective exists for each SFR. In 0, the fulfillment of dependencies is shown.

・6.3.1.1. Fulfillment of the security objectives

The following Table 4 summarizes the fulfillment of the security objectives by the SFRs.

Table 4 Fulfilment of Security Objectives

	O.CONTROL_FALSE_ACCEPT	O.PAD	O.AUTH_ADMIN	O.PROTECT_TSFDATA	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL
FDP_RIP.1						X
FIA_BUA.2	X				X	
FIA_UAU.2			X			
FIA_BUA.3		X				
FIA_UID.2(1)	X	X				
FIA_UID.2(2)			X			
FMT_MTD.1				X		
FMT_SMF.1				X		
FMT_SMR.1				X		

The following paragraphs contain more details on this mapping.

O.CONTROL_FALSE_ACCEPT

This security objective intends that the TOE satisfies a certain criteria for the FAR. To fulfill this security objective, FIA_UID.2(1) requires that each user be successfully identified before performing any action and FIA_BUA.2 requires that each user be successfully biometrically verified with the error rates of FAR [assignment: *X*] where X is to be assigned in ST..

O.PAD

This security objective intends that the TOE detects or rejects fake biometric characteristics at a certain rate. To fulfill this security objective, FIA_UID.2(1) requires that each user be successfully identified before performing any action and FIA_BUA.3 requires that the TOE detect or prevent use of biometric user authentication data that has been forged.

O.AUTH_ADMIN

This security objective provides a mechanism to authenticate the BS Administrator. To fulfill this security objective, FIA_UAU.2 requires that the BS Administrator be successfully authenticated before performing any action and FIA_UID.2(2) requires that the BS Administrator be successfully identified before performing any action.

O.PROTECT_TSFDATA

This security objective intends that the TOE restricts the access to the security relevant data of the TOE only to the BS Administrator. To fulfill this security objective, FMT_SMF.1 requires that the TSF be capable of performing the management functions on which the operations, the TSF data to be dealt, and the authorized role to access, namely the BS Administrator which is maintained by FMT_SMR.1, are specified by FMT_MTD.1

O.CONTROL_FALSE_REJECT

This security objective intends that the TOE satisfies a certain criteria for the FRR. To fulfill this security objective, FIA_BUA.2 requires that each user be successfully biometrically verified with the error rates of FRR [assignment: *Y*] where Y is to be assigned in ST.

O.CLEAR_RESIDUAL

This security objective intends that the TOE clears the residual data such as biometric data and other relevant data to the Enroled User after every execution of biometric verification. To fulfill this security objective, FDP_RIP.1 requires that the TSF ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the relevant objects.

・6.3.1.2. Fulfillment of the dependencies

The following Table 5 summarizes all TOE security functional requirements dependencies of this PP and demonstrates that they are fulfilled.

Table 5 Fulfillment of the dependencies

SFR	Dependencies	Fulfilled by
FDP_RIP.2	-	-
FIA_BUA.2	FIA_UID.1	FIA_UID.2(1)
FIA_UAU.2	FIA_UID.1	FIA_UID.2(2)
FIA_BUA.3	-	-
FIA_UID.2(1)	-	-
FIA_UID.2(2)	-	-
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.2(2)

・6.3.2. Security assurance requirements rationale

This PP has selected EAL2 because it is appropriate for basic attack potential to the TOE and the cost for evaluation and certification. ALC_FLR.1 is necessary to maintain the security.

・6.3.2.1. Dependencies of assurance components

Security assurance requirements are as in EAL2 except ALC_FLR.1. Among SARs from EAL2, dependencies are fulfilled as defined in EAL2. As for ALC_FLR.1, there is no dependency. Therefore all the dependencies are fulfilled.

・7 Appendix

・7.1 Glossary

Term	Description
Attacker	An Attacker is any individual who is attempting to subvert the operation of the TOE to gain unauthorized access to the assets protected by the portal.
Authentication	Act of revalidating a claim to an identity before granting access to a system or resources.
Biometric	Pertaining to the field of biometrics.
Biometric feature	Digital representation of the information extracted from a biometric sample (by the extraction function) that is to be used to construct or compare against an enroled biometric reference template.
Biometric identification	Application in which a search of the enroled biometric reference templates in storage is performed, and a candidate list of 0, 1 or more identifiers is returned.
Biometric reference template	Biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison.
Biometric sample	Information obtained from a capture function.
Biometric system (BS)	The minimal system of systems which contain biometric verification mechanism.
Biometric System Administrator (BS Administrator)	The Administrator authorized to perform the administrative operations of the BS of which the TOE is a part, and able to use the administrative functions of the TOE, and also responsible for the installation, settings including HW if necessary, and maintenance of the TOE.
Biometric verification	Application in which the user makes a positive claim to an identity, features derived from the submitted sample biometric measure are compared to the enroled biometric reference template for the claimed identity, and an accept or reject decision regarding the identity claim is returned.
Biometrics	Automated recognition of individuals based on their behavioural and biological characteristics.
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation.
CEM	Common Evaluation Methodology.
Comparison	The process of comparing biometric data with a previously stored biometric reference.

Term	Description
EAL	Evaluation Assurance Level.
Enroled User	A user whose biometric reference template is enroled to the BS and accesses to the assets via the portal by biometrically verified by the TOE.
FAR	False Accept Rate (FAR) - proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed.
FRR	False Rejection Rate (FRR) - proportion of verification transactions with truthful claims of identity that are incorrectly denied.
OS	Operating system.
Portal	The physical or logical point beyond which information or assets are protected by a biometric system.
PP	Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Presentation attack	Presentation to the biometric capture function with the goal of interfering with the operation of the biometric system.
Presentation attack detection (PAD)	Automated determination of a presentation attack.
Score	Value indicating the degree of similarity or correlation between a biometric sample and a biometric reference template.
SFR	Security Functional Requirement.
SmartCard	Credit card sized chip card with embedded integrated circuits, often used to store keys for authentication.
ST	Security Target – A set of implementation-dependent security requirements for a specific TOE.
Threshold	Predefined value which establishes the degree of similarity or correlation (that is, a score) necessary for a biometric sample to be deemed a match with a biometric reference template.
TOE	Target of Evaluation.
TSF	TOE Security Functionality.

・7.2 References

[1] Common Criteria for Information Technology Security Evaluation –
Part 1: Introduction and general model, September 2012, Version 3.1 Revision 4,
Part 2: Security functional requirements, September 2012, Version 3.1 Revision 4,
Part 3: Security assurance requirements, September 2012, Version 3.1 Revision 4.

[2] ISO/IEC 19785-1:2006, Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification.

[3] ISO/IEC 19792:2009, Information technology — Security techniques — Security evaluation of biometrics, August 2009.

[4] ISO/IEC 19795-1:2006, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework.

[5] Biometric Verification Mechanisms Protection Profile BVMPP v1.3, August 2008.

[6] Fingerprint Spoof Detection Protection Profile FSDPP v1.8, November 2009.

平成 26 年度工業標準化推進事業委託費
（戦略的国際標準化加速事業
（国際標準共同研究開発・普及基盤構築事業：
クラウドセキュリティに資するバイオメトリクス認証の
セキュリティ評価基盤整備に必要な国際標準化・普及基盤構築））
成果報告書

平成 27 年 3 月

作　　成　　一般社団法人日本自動認識システム協会
東京都千代田区岩本町 1-9-5
FK ビル 7 階
TEL　03-5825-6651
独立行政法人産業技術総合研究所
東京都千代田区霞が関一丁目３番１号
TEL　029-861-5284
株式会社 OKI ソフトウェア
埼玉県蕨市中央 1-16-8
TEL　048-420-5286