平成２７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２８年３月

一般社団法人日本自動認識システム協会
国立研究開発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。さらに、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や、金融業界での FinTech が注目されはじめていることを考えると、使用者の利便性を損なうことなく安全を確保しているシステムの必要性がますます増大し、その中で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ために、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、セキュリティ性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いないことにあると考えられる。

また、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ている。

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 認証を取得していくことが、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る。

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 28 年 3 月

一般社団法人日本自動認識システム協会
国立研究開発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

本事業では、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整備することを目的とする。これによって、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、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ことを狙う。

セキュリティの観点から見た客観的な評価を可能にするために、セキュリティ評価基準に則って PP（Protection Profile）及び PP に付随する精度評価手法および脆弱性評価手法を作成し確立する。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。そして、PP 及び PP に付随する評価手法の成果は、国際標準化原案として、標準化機関である ISO/IEC JTC 1/SC 27 に提案する（精度評価や脆弱性評価については ISO/IEC JTC 1/SC 27 あるいは SC 37 へ新規国際提案に向けた国際合意形成活動や寄書などの国際標準化活動を行う）。国際標準化の活動に当たっては、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、協力して、活動する。

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の下、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・認証を実施する。

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・手順を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評価及び認証を実施可能となるようにする。

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ることを狙うものである。

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 年度より 3 年間で、それぞれ下記に取り組むことを計画した。

1）平成 26 年度（2014 年度）

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、以下の研究を実施した。

・認証機関・評価機関・ベンダー及び有識者からなる検討委員会の組織
・海外動向調査及び方針検討
・セキュリティ評価手法の研究
  - PP 開発及び PP 認証取得
  - 精度評価のためのサポート文書とツール開発
  - 脆弱性評価手法の研究
  - 国際標準化活動

2）平成 27 年度（2015 年度）

・認証機関・評価機関・ベンダー及び有識者からなる検討委員会の組織
・国際連携活動
・セキュリティ評価手法の研究
  - 追加 PP 開発とサポート文書全体構成案の作成
  - 精度評価手法の研究
  - 脆弱性評価手法の研究
  - パイロット評価・認証に向けた準備
  - 国際標準化活動

3）平成 28 年度（2016 年度）

・認証機関・評価機関・ベンダー及び有識者からなる検討委員会の組織
・国際連携活動
・セキュリティ評価手法の研究
  - サポート文書の検証
  - 精度評価手法の検証
  - 脆弱性評価手法の検証
  - 代表的なベンダー製品のセキュリティ評価の実施（パイロット評価と認定、認証）
  - 国際標準化活動

平成 27 年度は上記の取り組み計画内容に対して、以下の手順で研究を実施することを計画した。

(1) 委員会活動

認証機関・評価機関・ベンダー・有識者 ・官公庁および事務局から成る検討委員会を組織し、委員会にて、事業の実施に関係する事項について、検討方針、検討内容や今後の方向性について、専門的、具体的な検討を行う。

(2) 国際連携活動

（a）PP 及び CC 評価・認証

本事業の成果であるバイオメトリクス製品の PP 及び CC 評価・認証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、作成する。連携方針に従い、バイオメトリクス製品 PP を既に開発し CC 評価・認証を実施しているドイツを候補として、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

EU が出資して結成されたバイオメトリクス評価検討組織である BEAT（Biometric Evaluation and Testing）における精度評価手法の最新動向調査、および、欧米の海外研究機関による精度評価の最新動向調査を行い、本事業で開発する精度評価手法の妥当性を検証する。

(3) セキュリティ評価手法の研究

（a）追加 PP 開発とサポート文書全体構成案の作成

登録処理の PP を作成し、PP の評価・認証を試行する。また、平成 26 年度に開発した認証処理の PP の内容も含めて、本事業で開発する CC における評価方法をまとめた文書（サポート文書）の全体構成案を作成する。認証機関である IPA と協力して作成し、国内評価機関とも情報共有して、CC 評価・認証がスムーズに進められるようにする。

（b）精度評価手法の研究

精度評価ツールでの開発機能として、精度評価報告書生成機能のプロトタイプを開発する。加えて、追加機能としてベンダー製品へのカスタマイズ機能を開発する。あわせて、精度評価のためのサポート文書案を、前記（a）で示したサポート文書全体構成案、および、平成 26 年度作成の原案に基づいて作成する。

（c）脆弱性評価手法の研究

パイロット評価・認証に向けて、平成 26 年度に作成した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・攻撃方法を研究し、認証機関である IPA と連携して、サポート文書案を、前記（a）で示したサポート文書全体構成案に基づいて作成する。立体的な偽造物も評価における攻撃に必要なので、3D プリンターを使用した偽造物作成も研究する。また、

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評価を試行する。

他に、偽造物が適切に作成されていることを OCT（Optical Coherence Tomography）測定装置で測定するとともに、ロボットアーム試験装置を活用して試験再現性の高く測定誤差の少ない偽造物検知評価技術の研究を行なう。

更に、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。

（d）パイロット評価・認証に向けた準備

平成 28 年度のパイロット評価・認証に協力するベンダーを募り、対象製品選定と評価用資料を作成する。（c）に基づいて、IPA の協力を得ながら、国内評価機関の評価体制を準備する。

（d）国際標準化活動

作成した PP の内容を SC 27 の ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics のプロジェクトに寄書して本文書に盛り込むための活動を行う。脆弱性評価手法で得た成果は、SC 37 の ISO/IEC 30107-3 Biometric presentation attack detection -Part 3：Testing and reporting に寄書して本文書に盛り込むための活動を行う。 また、評価ツールの開発を通じて得た知見を基に、新しい精度評価手法を見出し、その内容について国際標準化に向けての国際合意形成を SC 27 あるいは SC 37 で得る。

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] 国立研究開発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。

前述の計画に従い、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

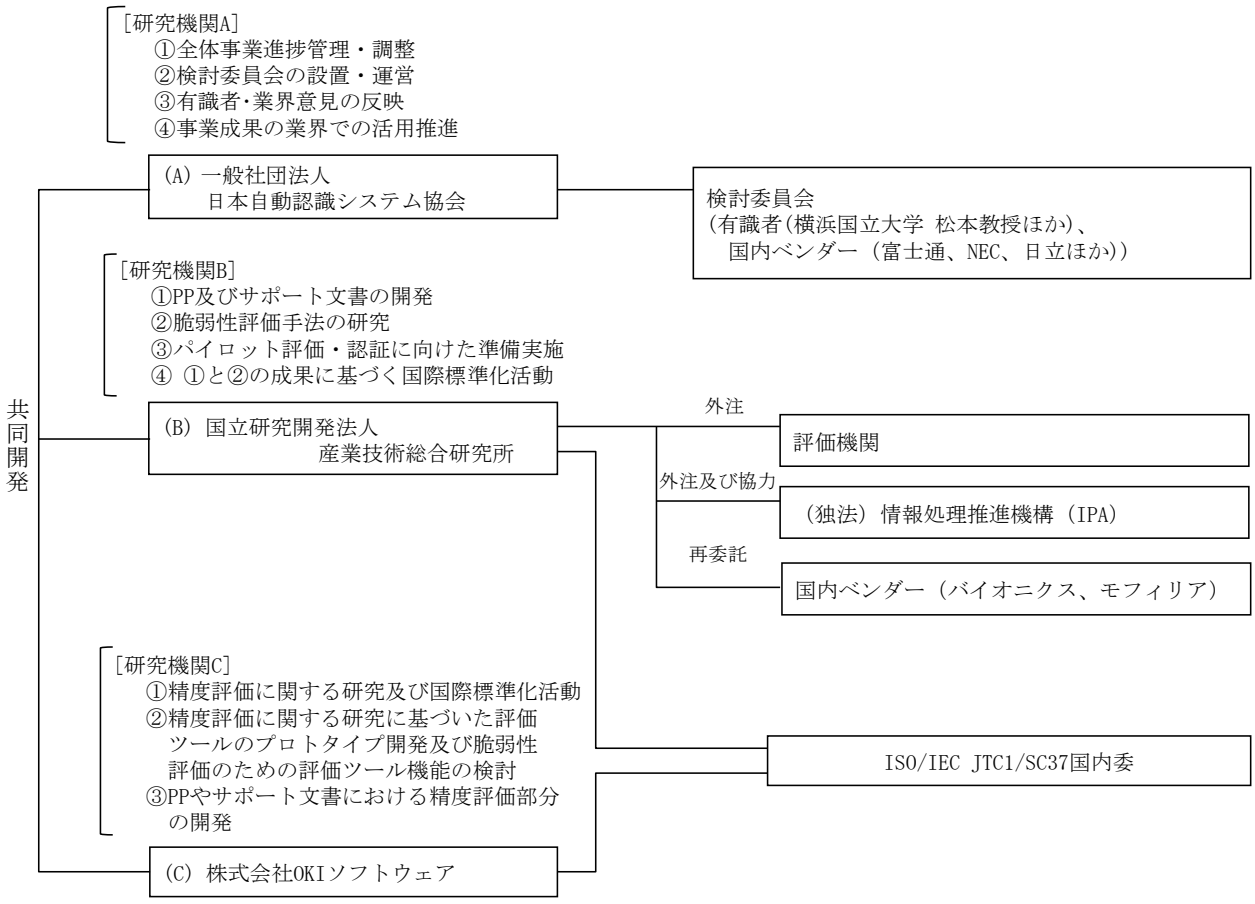


図 3.1-1　共同研究体制

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

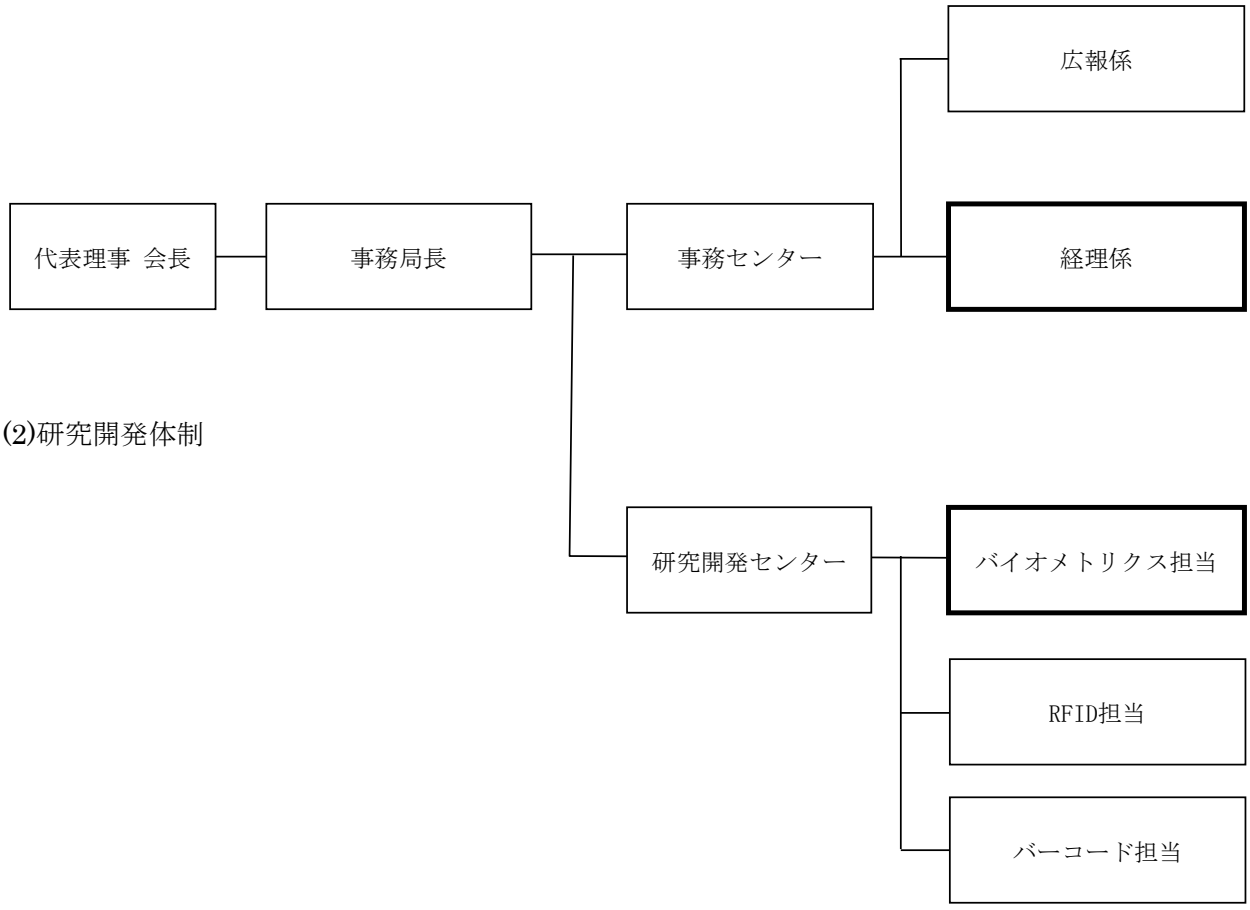


図 3.1-2　日本自動認識システム協会　管理体制・研究開発体制

【国立研究開発法人産業技術総合研究所】

(1)管理体制

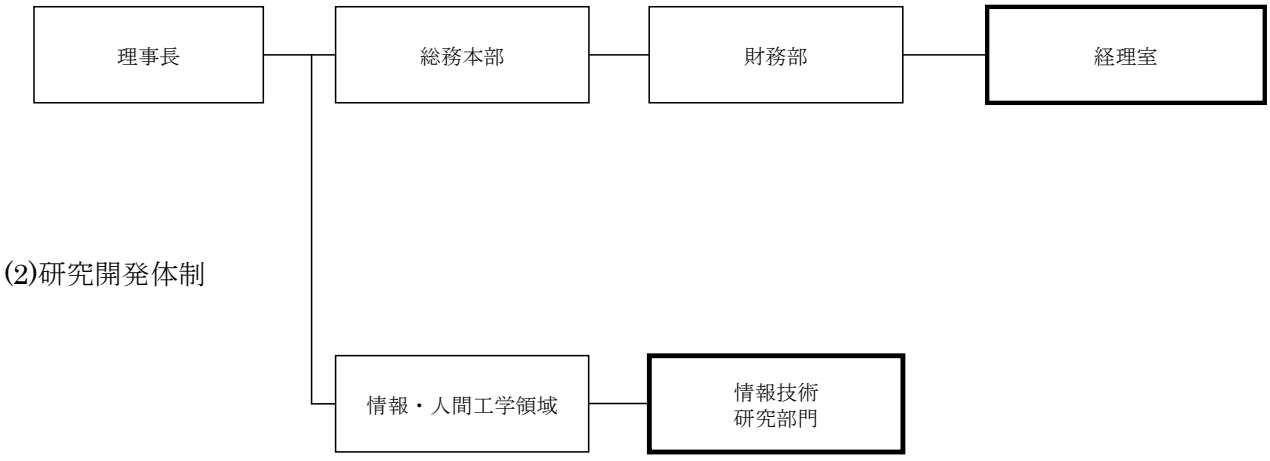
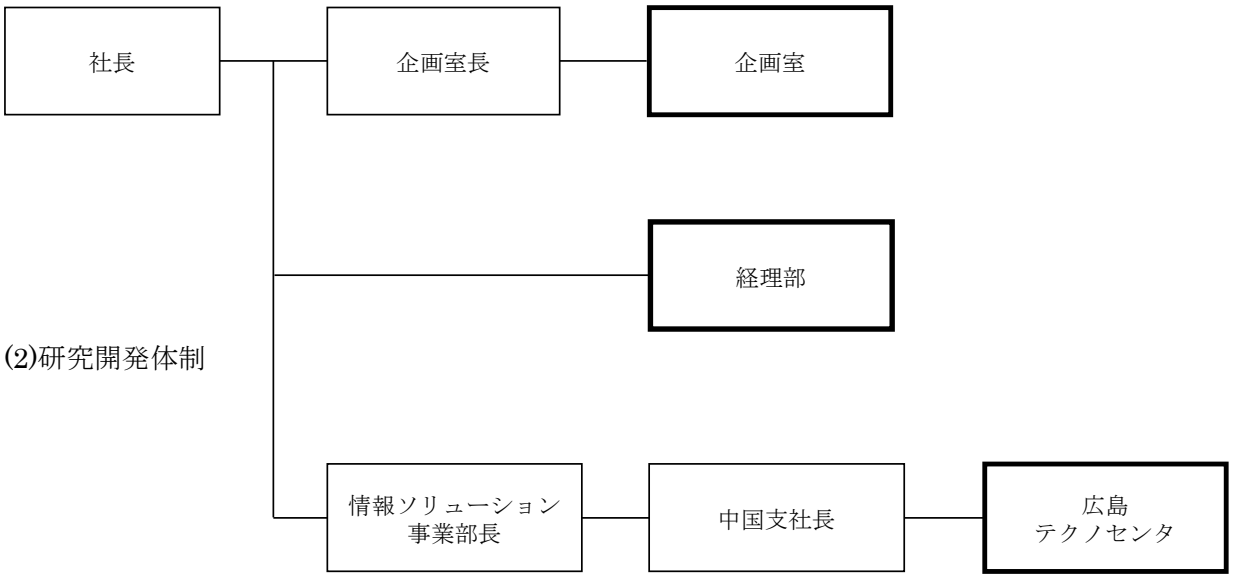


図 3.1-3　産業技術総合研究所　管理体制・研究開発体制

【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	SC 37/WG 5 委員
3	委員	溝口 正典	日本電気株式会社	SC 37/WG 5 主査
4	委員	日間賀 充寿	株式会社日立製作所	
5	委員	新崎　卓	株式会社富士通研究所	SC 37/WG 3 主査
6	委員	岩田 英三郎	ユニバーサルロボット株式会社	
7	協賛委員	須下 幸三	バイオニクス株式会社	
8	協賛委員	出口　豊	株式会社モフィリア	
9	協賛委員	甲斐 成樹	独立行政法人情報処理推進機構	
10	協賛委員	大堀　雅勝	みずほ情報総研株式会社	
11	推進委員	中村 敏男	株式会社ＯＫＩソフトウェア　企画室	SC 37/WG 2 委員
12	推進委員	寶木 和夫	国立研究開発法人産業技術総合研究所	
13	推進委員	山田 朝彦	国立研究開発法人産業技術総合研究所	SC 37 委員長 SC 27 委員
14	推進委員	大塚　玲	国立研究開発法人産業技術総合研究所	
15	推進委員	大木 哲史	国立研究開発法人産業技術総合研究所	
16	ｵﾌｻﾞｰﾊﾞ	江口 真一	富士通フロンテック株式会社	SC 37/WG 2 委員
17	ｵﾌｻﾞｰﾊﾞ	平野 誠治	凸版印刷株式会社	SC 37/WG 3 アドバイザー
18	ｵﾌｻﾞｰﾊﾞ	中村 浩一郎	独立行政法人情報処理推進機構	
19	ｵﾌｻﾞｰﾊﾞ	金子　浩之	みずほ情報総研株式会社	
20	ｵﾌｻﾞｰﾊﾞ	加藤 誠司	経済産業省　産業技術環境局	SC 37 委員
21	ｵﾌｻﾞｰﾊﾞ	中山 和泉	経済産業省　製造産業局	
22	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	SC 37 委員

3.3 実施スケジュール

平成 27 年度の活動は下記日程で実施した。

図 3.3-1 実施スケジュール

(A：JAISA, B：産総研, C：OKI ソフト)

項目	平成２７年									平成２８年		
	4	5	6	7	8	9	10	11	12	1	2	3
１．全体事業推進・管理及び事業成果の活用推進活動												
(1) 事業の推進および調整(A)	→	→	→	→	→	→	→	→	→	→	→	→
(2) 委員会の開催･運営(A)		→	→	→	→	→	→	→	→	→	→	
２．国際連携活動												
(1)PP 及び CC 評価・認証(B)			→	→	→	→	→	→	→	→		
(2)精度評価 (C)			→	→	→	→	→					
３．セキュリティ評価手法の研究												
(1)追加 PP 開発(B)		→	→	→	→							
(2)サポート文書全体構成(B)			→	→	→	→	→	→	→	→	→	
(3)精度評価手法およびサポート文書開発(C)			→	→	→	→	→	→	→	→	→	
(4)脆弱性評価手法およびサポート文書開発(B+C)			→	→	→	→	→	→	→	→	→	
(5)パイロット評価・認証に向けた準備 (A+B+C)				→	→	→	→	→	→	→	→	
(6)国際標準化活動(B)		→	→	→	→	→	→	→	→	→	→	
５．成果報告書作成(A+B+C)										→	→	→

4. 実施内容概要

4.1 検討委員会と検討内容

認証機関(IPA 2 名)・評価機関(みずほ情報総研 2 名)・ベンダー(7 社 7 名)・有識者(3 団体 3 名)・官公庁(2 名)・実施者（2 団体 5 名）および事務局(１名)から成る検討委員会(22 名)を組織した。4 回の委員会を開催し、事業の実施検討方針、検討内容や今後の方向性について、専門的、具体的な検討を行い、事業の検討にフィードバックした。各委員会の検討内容は下記であった。

(1) 第 1 回検討委員会

平成 27 年 8 月 28 日(金) 9：00～12：00 に(一社)日本自動認識システム協会（JAISA）にて開催した。主な内容は、下記であった。

①本年度の計画概要について

JAISA 事務局より、「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」事業の概要が説明された。

説明後、山田委員より、平成２７年度取り組み内容の「パイロット評価・認証に向けた準備」には、記載の他に「活動協力ベンダー殿にエビデンス準備の活動」をお願いすることも含まれるとの追加説明があり、活動協力ベンダー殿の活動内容が参加者に提示された。

②精度評価の進め方

中村委員より、「精度評価の進め方」について説明と提案があった。

合否判定方法の検討についての考え方について意見交換され、現実性を勘案し、合否判定方法は、現在開発した PP の記述と合致し、ＰＰの変更まで必要ない案を第一として選定し、検討を継続することとなった。

次に国際提案の可能性の検討について意見交換がなされ、新提案の尺度であるＦＴＲやＦＴＶの意義について、既存の尺度との差や活用性などの観点から有効性と必要性などを踏まえた再検討が必要との意見をいただき、それらの点を踏まえた検討を継続することとなった。

また、国際提案活動の活動内容と日程について整理してほしいとの要望があり、検討することとなった。

③登録及び認証の PP について

山田委員より、「登録及び認証の PP」についての説明と提案があった。

登場人物における攻撃者の記載が「登録時に偽造生体や品質の低い生体情報を意図的に‥‥」となり、二つに限定されているが、その他にも在ることが考えられるので、「‥‥生体情報等‥‥」のように攻撃方法に触れる記述でカバーする範囲を広げておくことが必要との意見をいただき、修正することとなった。

FIA_EBT.1 に記載の「TOE の判断基準の TOE 設計への記載」について、公開範囲に関する質問があり、これは申請者と評価者、認証者間でのみ交換される情報であり、他へは秘匿さ

れるよう扱うとの回答があった。

FIA_BUA.1 に記載の FIA_EBT.2 の「失敗率・・・」の失敗率の定義があいまいであるとの指摘があり、「登録失敗率・・・」と訂正することとなった。

④cPP 提案に向けた活動

甲斐委員より、「cPP 提案に向けた活動について」および「バイオ製品のセキュリティ要件」の説明と提案があった。

本事業で開発する PP の cPP 化の活動主体は、IPA であることが確認された。

また、本事業で開発する PP の cPP 化を目指して良いかについて審議し、cPP 化を目指した活動をすることとなり、IPA の cPP 化活動に本委員会も協力することとなった。

また、今後の本事業の活動も cPP 化に留意しながら検討を進めることとなった。

(2) 第 2 回検討委員会

平成 27 年 10 月 23 日(金)　9 : 00～12 : 30 に JAISA にて開催した。主な内容は、下記であった。

①登録及び照合 PP について

山田委員より、「登録及び照合 PP について」今まで各社個別にヒアリングしてまとめた結果の報告があった。質疑応答を経て、次を行うこととなった。

(1)オプショナル SFR（4）の記述で Capture から PAD feature Extraction が保護されている場合の記述について触れていないとの指摘を受け、Capture から Extraction 機能へ送る生体情報の保護と書いてある部分を、実装に合わせて記述を変更する必要があることを明示するよう変更する。なお、この PP の記述明示化に際しては CC 側の確認を取ったうえで変更する。

(2)セキュリティ対策方針の中で、「必要でなくなった時点で保護する」という中には、消すことも含まれているのかとの質問を受け、そのような懸念があることを考慮し、保護の中に消去が含まれていることを記載するよう変更する。

(3)オプションが 4 つあり、組み合わせを考えると１６通りとなる。各ベンダーは、実際の ST を作成するときには、本体部分と必要なオプションを選択して合わせた PP を基にして ST を作成することとなる。この行為は開発者にとって分かりづらいので、全ての組み合わせに番号を振って、何番とすれば、どれとどれのオプショナル SFR を選択したのかが分かるように整理してはどうかとのご指摘を受け、CCRA の中でオプショナル SFR の書き方とか扱いを含めた議論している段階なので、まずその議論結果を待ち、それに合うようにオプショナル SFR の扱いについて考えていくこととなった。

②安全性評価について

大塚委員より、「安全性評価について」の説明があった。また、参考のために昨年度の安全性評価に関する資料が再配布された。質疑応答の中で次の指摘と確認があった。

(1)先ほど PP を基に考えると、ST を作成してそれに合うかたちで評価をするということになるので、PAD に関係するのは、登録は FIA の EBT. 1 になる。PP の資料には、生体を

模した偽造物を登録してはならないとある。FIA_EBT.1.2 というものに関して評価をするときには、PP ではともかく生体を模したものは登録してはならないということなので、誰に似ていなくても、生きていないものは登録しないことが評価できるようにしないといけないのではないか。

照合は FIA_BVR4.1 になる。PP の資料には、生体を模した偽造物の仕様を検出、防止しなくてはならないとある。FIA_BVR4.1 というものに関して評価をするときには、生体として偽造されたものというのをチェックしないといけないということとなるのではないか。

これらは、なんらかの方法によって評価するわけで、その評価結果を出す場合は、どのようなものを出すという大枠の議論を既になされているのか。ある方法で評価し、最終的にその結果をどのようなかたちでリポートをして、認証につなげるのかという部分はについて、教えてほしい。

例えば IC チップの場合は、何が Attack Potential 何点、これが何点とかいう評価をして、Attack Potential が合計 31 点以上になっていれば、その項目はオーケーとか、どの項目を取って評価するかというようなメニューがある。そのようなものをバイオメトリクスの PAD 関係について、どのぐらいしっかりやるのか、やらないのか、評価結果をどう使って認証評価に結びつけるのかというところを決めないと、細かいセキュリティ評価のやり方で何を求められているかというところが、決まらないと思う。

委員会は、アドバイザーの位置付けなので、受託者から案が出てくると認識している。

(2)今回考える EAL について質問があり、EAL2 で取り組むことを確認した。

それに伴い、EAL2 を前提として、公知の情報を基に攻撃が通らないということを、先ほどご説明いただいた「静脈認証機器の安全性評価」についても、その対象の TOE に関する情報を評価者がどれぐらい得られるかとか、そこから出力を見られるかとか、スコアが使えるとか、使えないとか、仕様が全部分かるとか、そういうことのどこをどう評価するのかという方法論の大枠を決めないと、細かい議論ができないと思う。

(3)PAD 評価は、人工物による攻撃についてご説明があったが、人工物を提示するという以外の PAD の評価というのもあると思う。たとえば指紋の場合は息を吹きかけるとかがある。静脈の場合は、本物の指とか手のひらプラス何かを加えることなど、たとえば手術するなどがあると思う。

要するに、攻撃は、既存の方法で、既存の知られている攻撃方法が一応一通りあって、どんどん追加されていくと思うが、それらについて、どれについてやってみるのかとか、そのやる方法についてもどのくらいしっかりと調べてみるのかなど、両側面があると思う。

今は、人工物で生体をまねしたものを作って、それを TOE に合わせて、なるべく厳しめに評価するためには、その人工物をどうやって作ればいいか、何が必要か、どのような方法で攻撃するかというような検討と議論になっていると思う。

まず、それ以外には評価方法はないのかという議論がいるのではないか。たとえば、

ABCDEFG というやり方があるが、ABCD まででとどめておいて、EFGH は今回はやらないというような整理が必要と思う。

その中には、適度な攻撃者の能力によって、それがどこまでできるかというは別途判断するとしても、ネットワーク等で入手した技術で作ってみた人工物が通るかどうかという形を TOE によらずに評価するというタイプと、TOE の特性を考慮してチューンアップして評価するという 2 段構えもあると思う

また、ごく一般的な方法で製品の知識がなくても対応できるようなタイプの評価と、それから、製品の内部情報等を評価者にはもちろん NDA を結んで開示してもらって、いろいろと創意工夫を評価者が行うことにより、初めてできる評価という二つもあると思う。

(4)偽造物による攻撃見地も、製品では、TOE にある PAD 検出部のような一か所で検出しているというわけではなく、実は信号処理サブシステムとかスキャナ部とかなどシステムの全部を含んで、混然一体となってやるということものもある。そのようなものもあることを考慮した、評価を考えることが必要と思う。

(5)具体的にやった事例みたいなのが、ドイツとかアメリカとかにないのか。そういう情報も集めて検討していくのが良いと思う。

(6)攻撃方法についても整理が必要と思う。

考えられる攻撃方法を列挙して、Attack Potential の各項目を評価し、EAL2 のレベルに含まれる攻撃がなんなのかという整理をして、評価使う攻撃方法を幾つか選択していくというアプローチが必要と思う。それを決めるときは、実効性に対する配慮もいると思う。

また、認証されたという製品が世の中で使われ脆弱性による事故が多数発生すると、制度自体が崩壊することになるので、点数の付け方で配慮して置くことが必要である。

以上を参考にして、次を行うこととなった。

(a)先の(1 から(3)で指摘を受けた安全性評価の方法論等については、IPA と評価機関殿のご協力を得て取り組む。

(b)安全性評価の整理に際して、いろいろな攻撃に対して Attack Potential 計算して、今回の評価に用いるのは、既存の攻撃については Attack Potential による範囲で選定し、今回の「静脈認証機器の安全性評価」にあったようなものを用いる攻撃については、EAL2 のレベルだと、どのくらいのレベルまでやるべきなのかというのを第 1 ステップとしてまとめる。そのあとに、それぞれの攻撃について準備をするということで考える。

③cPP 提案活動報告

甲斐委員より、cPP 提案活動について報告があった。

④精度評価の推進状況報告

中村委員より、「精度評価の推進状況」について報告と提案があった。

この中で、中村委員が計画しているアンケート内容について質疑応答があり、提案したアンケートの中で、疑問に思うことが多々あるようであることが分かり、アンケートを回答するに

あたり、わからないところは質問をして、文書で回答をしてもらうことで対応することとした。

また、精度評価試験法については、提案の「社内試験と独立試験のスコア分布形状の比較」と「社内試験エビデンスを用いた検証」について詳細検討を進めることとなった。これについては、社内試験だけでなく、独立試験も良い方法でできるように工夫をとのコメントを委員長よりいただいた。

(3) 第3回検討委員会

平成 27 年 12 月 16 日(水)　14:00～17:00 に IPA 殿 13 階会議室 A にて開催した。主な内容は、下記であった。

①登録及び照合 PP について

山田委員より、「登録及び照合 PP について」最終報告として、前回委員会から変更になった点の報告があり、内容が確認された。

②脆弱性評価について

山田委員より、「脆弱性評価について」の検討状況についてご報告があり、質疑応答の中で次の点が確認された。

1) 攻撃は、今回の PP では登録と照合ともに偽造物を受け入れないということを機能要件で要求しているので、両方が対象となること。
2) 攻撃者で素人とあるものは、公知の論文や情報を入手し理解できるがバイオメトリクスの専門知識を持たない人という意味。また、評価の際は、実際の素人がするのではなく、評価機関の中で「素人のレベルをシミュレーション」して実施する。
3) 説明の中の所要時間と攻撃識別は同じ意味であり、攻撃方法を開発に要する時間である。
4) 攻撃を仕掛けるために必要な時間は、攻撃を何回も繰り返して攻撃に成功するまでの時間である。
5) 説明の中の攻撃成功率は、攻撃の一個一個のトライアルの集まりに対する率なのか、それとも一個一個のトライアルの成功率なのかにより、意味と実施する内容が異なると思われるので、定義を記載すること。
6) 来年度パイロットで使う攻撃シナリオとして十分なもの、これだけをやればいいというものは、来年度パイロットの評価認証開始までに完成することに取り組む。また、そこまで、この委員会で継続して議論する。
7) 静脈製品攻撃シナリオ 1 と 2 と 3 の違いは次である。
   ①攻撃シナリオ 1：攻撃者が独自に開発した装置で静脈情報を入手し、それで偽造物を作る。
   ②攻撃シナリオ 2：攻撃者が評価対象の装置より何らかの手段で静脈情報を入手し、それで偽造物を作る。静脈情報は given である。
   ③攻撃シナリオ 3:攻撃シナリオ 1 に加えて、近赤外線カメラで 2 次元イメージを撮って、立体的な静脈のイメージを作成して、それを基に偽造し、攻撃する。

8) 攻撃識別時間の定義を明確にする。

特に、公知の論文やインターネット公開情報などを基にして攻撃する場合について、「偽造物の作成に必要な道具や材料を揃える時間」や「その偽造物が攻撃に使えるものと評価する時間」や「偽造物作成に使用する静脈情報の入手に要する時間」など攻撃識別時間に含むものが何かについて明確にしておく必要がある。

9) 攻撃者が評価対象の装置より何らかの手段で静脈情報を入手するのに要する技術や時間を攻撃評価の中でどのように評価するかについて明示する。

10) 攻撃シナリオに、装置からの得られる何らかの情報を基にして、偽造物や攻撃方法を洗練していく、いわゆるヒルクライミング法に関わるシナリオの追加について検討する。

11) 評価時の装置の設定値は、評価を受ける側が申告することとし、その値に設定して評価者は評価する。

コメントとして次の事項をいただいた。

1) IC カードなどでは、シナリオのレーティングと時系列的な見直しをしている。

今回の事例についても、シナリオを継続的に見ていくということに取り組んだほうが良い。

2) 装置そのものをなんらかの形で攻撃して、装置の動作を狂わせて偽物が提示されたにも関わらず通過するように、ＯＫだと出力がでるようにしてしまう、というような攻撃の取扱いをどうするか検討が必要ではないか。

③cPP 提案活動報告

甲斐委員より、「cPP 提案活動報告」があり、質疑の中で、QITC 参加者募集は、CC ユーザーフォーラムのウェブページで行われ、会議は Face to Face ではなく、ネットミーティングとなることや、CPP はモダリティに依存する形で作成することを計画しており、日本は静脈をメインに考えており、スペインは指紋の検討をするといっていることなどの情報が提供された。

④精度評価について

中村委員より、「精度評価について」の説明があった。質疑応答の中で次の点が確認された。

1) 年齢層の粒度は、ある程度指針を定めたほうが良い。被験者で詳細年齢をいうことに抵抗がある方がいるので、5 刻みや 10 刻みが適当である。

2) 「並べ替えて」試験するのは、同じことを評価機関が再度やっても全く意味がないので、なにかしら変えられるものを変えて実施するという意味である。

3) アテンプト回数など装置やベンダー毎に異なる場合は、ベンダー申告値で評価する。

4) テンプレートエージングなどの評価条件は、評価報告書の中に明示する。

5) 式の定義で使われている言葉「全ての部位が登録できなかった人・・・」の登録という言葉が二重に用いられており解釈が混乱するので、表現を変えること。

6) シミュレーテッド・トランザクションを適用することに意味はある。

コメントとして次の事項をいただいた。

1) サポート文書で使われている言葉を英訳した時に、SC 37 で使われている英文体系との間で混乱が起こらないように使用する言葉について再整理する。たとえば、FRR と FAR は、正確に言えば本人拒否率や他人受入れ率ではなく、クレームを拒否する、あるいは間違って受け入れる率のことなので配慮が必要。

⑤ISO/IEC 19989 進捗状況報告

山田委員より、「ISO/IEC 19989 進捗状況報告」があり、19989 の進捗へり影響を考えながら、対応を進めることとなった。

(4) 第 4 回検討委員会

平成 28 年 2 月 17 日(水) 9:00～12:00 に JAISA にてにて開催した。主な内容は、下記であった。

①登録及び照合 PP 状況報告

山田委員より、「登録及び照合 PP 状況報告」の説明があり、特に質疑なく終了した。

②脆弱性評価状況報告

山田委員より、「脆弱性評価状況報告」の説明があった。

質疑の中で、次のことが再度説明され、

①脆弱性評価の取り組みの考え方は、AVA_VAN.2 に妥当な偽造物を作って脆弱性を評価するために、(a-1)公開情報からセンサーを試作し静脈情報を入手する、あるいは(a-2)ベンダーから静脈情報を提供してもらう、(b)公開情報と前記の手段で入手した静脈情報から偽造物を作る、(c) 作った偽造物を公開されているアルゴリズムを使って評価し、それがある程度本物と似ている結果が得られるまで偽造物の品質を高める、ということをした上で、(d)その品質の確認された偽造物を使って評価対象に攻撃して脆弱性を評価する、というもの。

②上記(a-1)あるいは(a-2)と(b)(c)が攻撃識別にあたり、(d)が攻撃実施にあたる。

③上記の(a-1)あるいは(a-2)と(b)(c)や(d)の必要時間や難易度等を基にしてアタックポテンシャルを算出し評価する。

上記の考え方が、BEAT の考え方にあっているかを確認し、その上で、攻撃識別と攻撃実施の定義を明確にすることとなった。

また、続いて、次の説明と要望が出て、今後引き続き検討することとなった。

④センサーからの指紋情報と PAD 情報が同一の生体から得られていることを判断する部分の機能が十分かどうかの判断は、以下のようになされる。申請者（ベンダー）がセキュリティアーキテクチャに記載内容（センサーからの指紋情報と PAD 情報を同一の生体から得るための実現方法）をベースに、評価機関は攻撃手法を検討し、攻撃し、もし攻撃に成功すれば評価としては不合格になる。

⑤PAD に関して記述する情報については、評価機関において、セキュリティ要件が設計書に反映されていて、確かに要件が設計レベルに落ちていることを確認する作業があるので、

何かしらの情報は記載する必要がある。レベル感として、分解してすぐ分かるような情報は最低限書いてもらうという考え方で、その具体的指針をサポート文書の中に記載する必要がある。

また、アタックする側が、容易に PAD の仕組みをリバースエンジニアリングして、アタック法を考えることができるようなものは、評価機関で分解するという手間暇を省くためにも、最低限証拠資料に書いてもらうことが必要と考えている。

さらに、攻撃側が入手できる情報は、例えば、製品のライフサイクル管理が徹底されているものとそうではないものでは、入手の困難さなども異なる。その点も考慮し、記載の内容を検討する。

以上を含めて、サポート文書の中で認証取得する EAL のレベルも考慮して示す。

⑦「わかってしまう情報」という部分を客観的に記載する必要がある。一つの変更案は、「なお、評価対象製品を消費者が入手できる場合、製品を入手して製品を分解・測定すれば分かる情報は、評価エビデンスに記載する。」である。

⑧TOE 自体から入手する場合の改変の可否は TOE に依存するとしてあるが、この改変の可否の難易度がアタックポテンシャルのどこかの項目に反映されると思う。それが全体の考え方の中で、どこでどのように反映するのかを明確にする。

⑨シナリオ（案）(2)の TOE 自体から入手する場合とシナリオ（案）(1)では、攻撃のための情報入手の容易性が異なると思う。その点はアタックポテンシャルのどこかの項目に反映されると思うが、それについても全体の考え方の中で、どこでどのように反映するのかを明確にする。

⑩今回の報告は PAD についてだけだが、低品質データが実際に排除されていることの検証について、検討する。

③cPP 提案活動報告

甲斐委員より、「cPP 提案活動報告」があり、その中で来年度本事業が継続した場合を前提として、次の要請があった。

- この委員会で意見ヒアリングやドラフトに対してのコメントについて話し合ってほしいこと
- cPP 関連の会議の時期に合わせてこちらの委員会を設定することも検討しなくてはならないこと
- cPP 関連の会議メンバーに、本委員会に参加される方は基本的に参加してほしいこと

④精度評価について

中村委員より、「精度評価状況報告」があった。

質疑を通して、ほぼ提案していただいた考え方で進めてよいということとなったが、次のような意見をいただき、引き続き検討することとなった。

①社内試験エビデンスの独立評価機関の評価方法とその結果に対する評価機関が行う独立試験の関係。例えば、評価機関は必ず独立試験を行うのかどうか、独立試験を行う条件があるのかなど。あるいは、エビデンスから社内評価の信憑性が客観的に確認・納得できる方

法があるかなど。

②独立試験方法案における誤受入率（FAR）の考え方の数式による表現

③今後の性能の向上時に独立試験のコストが加速度的に増えないような仕組みと考え方の検討。

④ROC カーブやスコア値の活用なども考えてよいかとも思うこと。

⑤独立評価機関の評価の目的を明確にすることも必要。申請者の不正を見抜くための評価なのか、あるいは申請者が定められた手順にしたがってちゃんとやっているかどうかを確認するための評価なのか。まず、最初の大本があって、その目的を果たすために何をすればいいのかという風に考えることも大切。この時、EAL2 ということを前提として考えてもよいと思うこと。

⑥不正をしたものは、実際の市場で痛い目を見るということも考慮して良いかもしれないこと。

⑤ISO/IEC 19989 進捗状況報告

山田委員より、「ISO/IEC 19989 進捗状況報告」があり、参加意思表明をしているところにスペインがあるとの情報が提供された。

4.2 国際連携活動

本事業の成果を海外で広く認知させるための国際連携活動は、CCRA（CC Recognition Arrangement）における cPP（collaborative PP）活動に集約されることになった。

4.2.1 PP 及び CC 評価・認証

本事業成果については、検討委員会委員より本事業の成果は日本国内でのみ通用させるのではなく、国際的に広く認知させるべきという強い意見・要望があったため、本事業成果である PP を、CCRA で cPP（collaborative PP）化するという方針が検討委員会により承認された。cPP は、技術分野毎の CCRA 加盟国間の共通の PP であるが、生体認証分野での cPP は未だ存在していない。また cPP に対応した当該技術分野の評価手法を定めるサポート文書も併せて cPP とともに開発する必要がある。この cPP とサポート文書により、当該分野での評価すべきセキュリティ要件や CC 評価手法が統一され、国際的な認知度の向上も併せて図られる。cPP の開発は、CCRA に加盟する認証機関の提案を通して申請しなければならないため、本事業の検討委員会に委員として参加している IPA がその作業を受け持った。

2015 年 9 月に英国ウィンザーで開催された CCRA 会議でスペインと共同で cPP 開発を申請し、トルコとオーストラリアが cPP 及びサポート文書開発に参加する旨意思表明が為された。CCRA での審査を経て、CCRA 内で Biometric Working Group が設立され、第 1 回会議（WebEX 会議）が 2016 年 2 月 25 日に IPA 主催で開催された。今後 Working Group により cPP の基本方針が固まり次第、cPP 及びサポート文書開発のための iTC（international Technical Committee。認証機関だけでなくベンダー・評価機関の技術者も参加する）が設立される予定である。iTC には、本検討委員会参加のベンダー及び評価機関が参加予定であり、cPP 及びサポート文書のドラフトは、本事業成果である PP と精度評価と脆弱性評価に対応したサポート文書素案の英訳を基にして、作成される予定である。

4.2.2 精度評価

精度評価に関する国際連携のための調査活動として、欧州のバイオメトリクスの評価と試験に関する研究プロジェクトである BEAT（Biometrics Evaluation And Testing）が発行した、精度評価に関係する記述が含まれる公開文書である”D4.5: Description of metrics for the evaluation of vulnerabilities to direct attacks”に関する文献調査を実施した。前半部分（2 章 評価尺度）で精度評価と脆弱性評価を組み合わせた新概念である EPSC（Expected Performance and Spoofability Curve）が述べられ、後半部分（3 章 脆弱性評定）でセキュリティ評価に関わる考えが述べられている。調査結果の詳細を後述する（5.1.2 (2)参照）。

今後の欧州の精度評価に関するプロジェクトへの本概念の採用や、国際標準化活動において欧州から本概念に関する標準化提案が行われる可能性もあるため、国際連携活動の推進において本概念に関する欧州の動きがないか今後注視する必要がある。

また、4.2.1 で述べた PP の cPP 化に伴うサポート文書の開発のために、本事業で作成した精度評価サポート文書素案の英訳を提供予定である。なお、精度評価サポート文書は、バイオメトリクス技術の CC 評価認証を進める上で重要な役割を担うものなので、cPP 化活動との連携を継続する予定である。

4.3 追加ＰＰ開発とサポート文書全体構成案の作成

4.3.1 追加 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 作成は、産総研が担当し、昨年度開発の認証処理を対象とした PP に加えて、登録処理の PP を作成することを目標とした。しかし、検討の結果、登録処理単独ではセキュリティ機能要件を導出できないため、登録処理単独の PP を作成することはできないとの結論に達し、登録処理と認証処理の両方を含む PP を作成することにした。PP 作成に当たっては、素案を産総研が作成し、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繰り返し、PP 最終案をまとめた。CC 評価の対象となる TOE については、昨年と同様に、各社の製品の共通部分とした。その結果、ベンダーの製品の中には、ID を全く処理せず、登録生体情報が外部から与えられて、入力された身体的特徴から得られる特徴データと登録生体情報が同一ユーザのものであるかだけを判定するものがあることがわかった。このような処理は、認証とは呼ばれず、バイオメトリック照合（Biometric verification）と呼ばれる。TOE の処理内容をバイオメトリック照合にすることによって、PP のより広い適用が可能になった。昨年度は国際化を考慮して英語で PP を作成したが、来年度のパイロット評価認証を円滑に進めることを優先して、今年度の PP は日本語で作成することにした。以上の結果、PP の名称は、バイオメトリック照合製品プロテクションプロファイルとした。

バイオメトリック照合機能と 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_EBT（Enrolment of Biometric Template）及び FIA_BVR（Biometric VeRifacation）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。

PP 最終案は、2015 年 11 月 30 日からみずほ情報総研が評価を開始し、2016 年 1 月 26 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 3 月末の予定である。

4.3.2 精度評価サポート文書素案の開発

静脈認証バイオメトリック製品に対する CC 評価の適用に向けて、バイオメトリック製品のセキュリティに関わる性能指標である誤受入率（FAR）、誤拒否率（FRR）、及び、登録失敗率（FTE）を評価するための精度評価に関するサポート文書素案を作成した。本素案は、静脈認証バイオメトリック製品の精度評価を CC 評価に適用するにあたり、静脈認証バイオメトリック製品に特有な必要事項をガイダンス文書としてまとめたものである。本素案では、ベンダーが静脈認証製品の精度評価

を社内試験として実施した結果を評価機関に提示する際のエビデンス、及び、評価機関の社内試験エビデンスの適正さを確認するために実施する独立試験方法を記載した。精度評価サポート文書は2017年度に完成予定である。以下に社内試験のエビデンス、及び、独立試験方法それぞれの概要を示す。

(1) 精度評価サポート文書における社内試験エビデンス素案（ベンダー作業）

静脈認証バイオメトリック製品のCC評価を受けるベンダーが、評価機関に提示する精度評価に関する社内試験のエビデンス項目およびその内容を精度評価の国際標準規格であるISO/IEC 19795-1及びISO/IEC 19795-2において準拠項目であることを示すshall文や推奨項目であることを示すshould文に着目し、まとめたものである。shall文やshould文で示される内容をサポート文書にそのまま盛り込もうとすると、ベンダーの社内試験に沿いにくい場合があることが判明したため、試験の適正さを失わないことを考慮したうえで、社内試験に沿った表現への変更を行った。活動の詳細を5.2.2.2に、素案を付録-3に示す。

(2) 精度評価サポート文書における独立試験方法素案（評価機関作業）

上記(1)で示した社内試験エビデンス素案に従ってベンダーが社内試験結果のエビデンスを評価機関に提示したあと、評価機関が実施する精度評価の独立試験の方法についてまとめたものである。本素案では以下の2つの試験方法を示した。

・被験者試験：評価機関が独自に被験者を募集して行う精度評価である。被験者だけでなく、試験環境についても独立性を高めるため、評価機関内に社内試験と同等の試験環境を構築することが一般的である。（試験実施の際、試験の独立性を高めるために評価機関が用意したツールを用いる場合がある。）

・立ち入り試験：誤受入率を測定するためのテクノロジ評価を行うことを主な目的として、評価機関がベンダーの社内試験環境に立ち入って行う精度評価である。前述の被験者試験で生成された被験者のテンプレートや照合バイオメトリックデータをベンダーの社内試験環境に持ち込み、ベンダーが社内試験のために集めたテンプレートや照合バイオメトリックデータと混合させてテクノロジ評価を行う。

活動の詳細を5.2.2.3に、素案を付録-4に示す。

4.3.3 脆弱性評価サポート文書素案の開発

脆弱性評価サポート文書は、精度評価サポート文書とは異なり、前例として、ドイツで作成さされたものとEUのBEAT（Biometric Evaluation And Testing）プロジェクトで作成されたものが1件ずつある。これらはいずれも指紋を対象にしたものであるが、両方を調査し、それらの調査結果を考慮して素案を作成した。素案作成には、ベンダー各社に意見を求め、意見をまとめた結果を検討委員会で審議した。評価のための文書に対する要件及び攻撃シナリオについて、サポート文書の

骨格を作成した。攻撃シナリオ検討の結果、BEAT プロジェクトの成果と協調できる見通しである。脆弱性評価サポート文書はまだ素案の段階であり、来年度のパイロット評価認証開始までに原案を完成させ、パイロット評価認証で検証して完成させる。

4.4 精度評価手法の研究

本ツールはバイオメトリック製品の精度評価を行うための標準的なツールとして開発するものであり、前年度に引き続き活動を行った。ツールの主な特徴を以下に示す。

①用途：評価機関による独立試験
②評価の種類：
・FTE, FRR：シナリオ評価
・FAR：テクノロジ評価
③適用可能製品：SDK（ソフトウェア開発キット）
④対応インタフェース：BioAPI
⑤対応 OS：Windows

今年度は主に以下の 2 つの開発作業を実施した。活動の詳細を 5.3.2 に示す。

・BioAPI V1.1 対応：評価対象製品である静脈認証 SDK（ソフトウェア開発キット）がサポートするインタフェースの条件が前年度は BioAPI V2.0（ISO/IEC 規格）だったが、BioAPI V1.1（ANSI 規格）をサポートしている SDK 製品が存在することが判明したため、BioAPI V1.1 への対応を行った。
・ツールの柔軟性の向上：被験者の習熟度を上げるために試験官が被験者に対して行うトレーニングのタイミングの自由度を向上すること、複数の身体部分が存在する場合（左右の手、手のそれぞれの指など）の身体部分の順番の自由度を上げること、及び、ツールが生成する精度評価結果の実測値の出力内容を独立試験がしやすくなるよう柔軟性を向上させることの 3 つの対応を行った。

4.5 脆弱性評価手法の研究

偽造物作成のための装置を購入し、静脈の偽造物作成の研究を進めた。評価・認証に使用するための偽造物の品質について検討し、第２回委員会で議論した。今後、信頼できる安全性評価に向けた偽造物のバリエーションを検討すると共に、来年度の評価に使用する偽造物のセットを提案し、委員会の合意を得る予定である。

なお、脆弱性評価手法について本報告書に記述することは攻撃者に対して有益な情報を与えることになるため、詳細は関係者限りの別文書に記述する。

4.6 パイロット評価・認証に向けた準備

来年度のパイロット評価・認証を実施するためには、評価・認証される側とする側それぞれの準備が必要である。評価・認証される側のベンダーと評価・認証する側の評価機関及び認証機関で、それぞれの準備を進めた。

4.6.1 ベンダーにおける CC 評価のための文書の準備

来年度のパイロット評価・認証への参加意思を示したベンダーに、来年度の準備と本事業で作成した PP の検証のふたつを目的に、設計関連の文書である、機能仕様、TOE 設計、セキュリティアーキテクチャ、ST を作成してもらった。文書を作成する各社と産総研は NDA を締結した上で、各社が作成した文書を産総研に提供し、CEM に基づいて産総研が確認しフィードバックするという作業を繰り返した。最終的に 3 社が上記の 4 文書作成を完了した。

ベンダーの文書作成の過程で、いくつかの点で、作成した PP が各社製品へ適用できないことがわかり、PP 作成にフィードバックした。

4.6.2 評価機関・認証機関との評価方法の検討

精度評価を担当する OKI ソフトウェアと評価機関・認証機関の間で精度評価のためのサポート文書案開発に関する検討を行い、今年度の成果物として精度評価のサポート文書における社内試験エビデンス素案、および、独立試験方法素案の 2 つの文書の作成を完了した。

両文書の作成にあたり、評価機関・認証機関と OKI ソフトウェアとの間で 2015 年 7 月から 2016 年 3 月まで、7 回にわたって会議が開催され、サポート文書の全体構成、活動の推進方法、推進の途中段階における状況確認、両素案の各記述項目など、様々な意見交換が行った。詳細については 5.5.2 (1)を参照されたい。

4.7 国際標準化活動

本事業の対象とする CC 評価認証の国際標準化は SC 27 で ISO/IEC 15408 として実施しており、提示型攻撃検知の CC 評価認証は SC 27 の ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics で国際標準化が進められている。精度評価を CC 評価認証でどう扱うかについても、SC 27 でスタディピリオドが開始された。

また、バイオメトリクスの国際標準化は ISO/IEC JTC 1/SC 37 で実施している。偽造生体などの提示型攻撃（presentation attack）の検知に関する国際標準化も 3 パートから成る ISO/IEC 30107 Biometric presentation attack detection シリーズとして SC 37 での活動がある。

ISO/IEC 30107-3 と ISO/IEC 19989 との分担をどうするかの議論は今までなされて来なかったが、SC 37 の 1 月のマルティニー会議で、ISO/IEC 19989 エディタから ISO/IEC 19989 の状況を説明した結果、CC アプローチについては ISO/IEC 19989 が担当することが結論された。

4.7.1　SC 27 での国際標準化

今年度の SC 27 国際会議は、5 月にマレーシアのクチンで、10 月にインドのジャイプールで開催された。ISO/IEC 19989 については、クチン会議では WD 1 に対する審議、ジャイプール会議では WD 2 に対する審議が実施された。コメントはドイツ、フランス、英国、日本、米国から提出されており、国際会議審議へはドイツ、フランス、英国、インド、日本、韓国、米国のエキスパートが参加している。各国からのコメント・寄書がまだ多く、WD 段階に留まっている。本事業の活動で、エディタとして WD2 及び WD3 を作成し、国際会議での審議を取りまとめた。本成果報告書の作成時点では、WD 3 に対するコメント募集中である。

WD2 に対しては、EU の BEAT（Biometric Evaluation And Testing）プロジェクトの寄書がドイツ及びフランスから提出された。この寄書には精度評価に関する内容も含んでいたため、スタディピリオド Security evaluation of biometric performance based on ISO/IEC 15408 and 18045 を開始することが WG 3 で決議された。本スタディピリオドのラポータも本事業の活動として実施する。

4.7.2　SC 37 での国際標準化

SC 37 での本事業に関わる国際標準化プロジェクトは、WG 3（パート 3 は WG 5 と共同）で開発している ISO/IEC 30107 Biometric presentation attack detection と WG 5 で開発が完了している ISO/IEC 19795 シリーズがある。本事業における精度評価の成果を ISO/IEC 19795 シリーズに反映させることを検討していたが、SC 27 のスタディピリオドへ寄書提出することで国際標準に反映させる。ISO/IEC 30107 に対しては、レビューを継続する。

5. 事業成果詳細

5.1 国際連携活動

本事業の成果が、日本国内だけなく海外でも活用されることを目指し、PP、CC 評価認証、精度評価について、ぞれぞれ国際連携を念頭に活動している。PP と CC 評価認証については、CCRA（CC Recognition Arrangement）における cPP（collaborative PP)、及びサポート文書の開発活動を実施している。精度評価についても、CC 評価認証での精度評価のあり方を本事業では検討し、対応するサポート文書の開発活動を行っている。なお、精度評価に関する成果は CCRA 以外に ISO/SC27 にも提供される予定である。PP の cPP 化に関しては、認証機関であり検討委員会の委員でもある IPA の協力も得ながら活動を実施した。

5.1.1 ＰＰ及びＣＣ評価・認証

本事業では、今年度作成した PP、及び精度評価と脆弱性評価に対応したサポート文書に基づいたパイロット CC 評価認証を来年度予定している。パイロット CC 評価認証が合格し CC 認証書が発行された場合、CCRA の相互承認制度によって、その認証書は CCRA 加盟国間で有効となる。しかし、精度評価や生体認証の脆弱性評価の CC 評価手法は、現状 CCRA 内で統一化されたものはない。従って本事業の成果物であるサポート文書を、CCRA 加盟国共通の評価手法にし、広く使用されるようにすることが望ましい。また、本事業で作成した PP も、cPP 化することにより日本国内だけでなく CCRA 加盟国内でも利用されることが望ましい。

本事業成果の上記のような国際的活用のあり方は、検討委員会委員より本事業の成果は日本国内でのみ通用させるのではなく、国際的に広く認知させるべきという強い意見・要望に基づいている。本事業においては、日本の有識者やベンダーの意見を集約しながら生体認証における評価手法を開発している。しかし日本の意見が集約された評価手法が、結局日本国内のみで通用し海外では認知されず使用されないのでは、グローバルに活動する事業者から見ればメリットが少ない。また日本の事業者が関与せず意見が反映されない評価手法が海外で開発された場合、日本の事業者にそぐわない評価手法が普及する可能性もある。そのため本事業成果の PP を CCRA で cPP（collaborative PP）化するという方針が検討委員会により全員一致で承認された。

cPP は、技術分野毎の CCRA 加盟国間の共通の PP であるが、生体認証分野での cPP は未だ存在していない。また cPP に対応した当該技術分野の評価手法を定めるサポート文書も併せて cPP とともに開発する必要がある。

CCRA では一つの技術分野で一つの cPP と関連するサポート文書のみ開発可能であり、cPP や関連サポート文書が CCRA で承認された後は、その cPP に適合した CC 評価のみが CCRA での相互認証の対象となる。従って、本事業の成果物である PP とサポート文書を CCRA で認知させ cPP 化させることにより、本事業成果が CCRA 内で広く使用される可能性があり、国際的な認知度の向上も併せて図られることになる。cPP の開発は、CCRA に加盟する認証機関の提案を通して申請しな

ければならないため、本事業の検討委員会に委員として参加している IPA がその作業を受け持った。

2015 年 9 月に英国ウィンザーで開催された CCRA 会議において、IPA とスペイン認証機関共同で cPP 開発の申請を実施した。申請が CCRA で承認されるためには、CCRA 加盟国の 2 ヶ国以上がその申請を支持する必要があるため、スペインとの共同申請を実施している。CCRA 会議では、本事業受託者である産総研が、cPP 化の対象である本事業で作成する PP について説明した。この説明に対して、cPP とサポート文書の関係が議論された。産総研で開発中の PP はモダリティ（バイオメトリクスで処理する静脈や指紋などの身体的特徴）を特定していない。それは PP で定義される精度や偽造生体を用いた攻撃に関するセキュリティ要件は、全てのモダリティに共通したものであるからである。しかしながら本事業で開発中のサポート文書は、静脈のみを念頭に開発している。従って一部の国からは、サポート文書が存在せず、評価手法が明確になっていないモダリティに対応した製品の CC 評価認証が、cPP に基づき実施されてしまう懸念が示された。その懸念に対応するため、cPP 化の際には、cPP で評価可能となるのは対応したサポート文書が存在するモダリティのみであるということを明記する必要がある。なお CCRA 会議の場では、日本は静脈のサポート文書を作成予定である旨説明している。会議の席上、医療分野でバイオメトリクスを国家で推進しているトルコから、活動への参加表明があった。また、米国は、モバイルデバイスの PP を国内で開発しており、生体認証をセキュリティ機能要件として定義していることから、cPP 活動への関心を示していた。現在改訂中の米国のモバイルデバイス PP に関しては、産総研・IPA 共同でコメントを送付し、本事業での知見を共有するように求めている。

cPP 申請に対して、同様な cPP が存在しないこと及び cPP の必要性の確認が CCRA で審査された結果、認証機関にメンバーが限定される Biometric Working Group の設立が承認された。WG の第 1 回会議は、2016 年 2 月 25 日に、IPA 主催で WebEX を使って実施された。会議では、IPA より WG の TOR（Terms Of Reference）、活動計画、ディスカッションペーパー（cPP 開発で論点をまとめた文書）、ESR（Essential Security Requirement、PP のセキュリティ課題定義に相当。cPP は WG が開発したこの ESR をベースに実施される）案を紹介し、議論を実施した。

3 月末に向けて、各認証機関からのレビューを反映した ESR の完成を予定している。ESR が完成次第 iTC（international Technical Committee。認証機関だけでなくベンダー・評価機関の技術者も参加する）が設立される予定であり、この iTC により最終的に cPP やサポート文書が開発される。iTC には、本検討委員会参加のベンダー及び評価機関も参加予定である。iTC の議長やテクニカルエディタは今後 WG の中で議論し決定される予定であるが、日本はテクニカルエディタとして産総研を推薦している。cPP と精度評価及び脆弱性評価のサポート文書のドラフトは、本事業成果が英訳され iTC へ提出される。cPP と精度評価サポート文書のドラフト第一版の提出は、3 月末を予定している。脆弱性評価のサポート文書のドラフト第一版の提出は、6 月末の予定である。なお、各々のサポート文書は日本のベンダーや有識者へのヒアリングを重ね開発が実施されている。

利用者認証において、CC 認証された製品が使われているか否かを認証サーバが判別できることは、より信頼できる製品を使っているか否かを認証サーバが判別できることになるので、重要である。

PP はそれぞれ固有の識別番号を持つので、CC 認証された製品が PP 適合していれば、PP の識別番号を示すことで、当該製品がどのようなセキュリティ機能要件を満たすかを認証サーバは知ることができる。PP の cPP 化が進み、cPP に適合する製品が増えれば、上記の判別はより普及し易くなる。このような判別方法に関する報告を産総研から 2015 年 5 月にドイツハンブルクで開催された IFIP2015 で報告した。発表内容は、以下のとおり、出版された。

"A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant", Asahiko Yamada, ICT Systems Security and Privacy Protection Volume 455 of the series IFIP Advances in Information and Communication Technology pp 145-158, 2015

5.1.2 精度評価

精度評価については、国際連携を目指して BEAT プロジェクトの文献調査を実施した。本事業で作成した精度評価サポート文書素案を cPP 化活動の中で活用し、本事業成果の国際化を推進する。

(1)BEAT の文献調査

精度評価に関する国際連携のために、欧州のバイオメトリクスの評価と試験に関するプロジェクトである BEAT（Biometrics Evaluation And Testing）において、精度評価に関係する記述が含まれる公開文書である"D4.5: Description of metrics for the evaluation of vulnerabilities to direct attacks"に関する文献調査を実施した。以下に文献の概要を示す。

本文献は前半部分（2 章 評価尺度）で精度評価と脆弱性評価を組み合わせた新概念が説明され、後半部分（3 章 脆弱性評定）で生体認証製品を CC 評価に当てはめた場合の評価方法が述べられている。以下にそれぞれの概要を示す。

① 評価尺度（2 章）

性能評価尺度 EPSC (Expected Performance and Spoofability Curve) と呼ばれる新しい性能評価尺度を紹介している。まず、精度評価における性能尺度のひとつである FAR の代わりに FAR_ω という概念を導入する。これは誤受入率とスプーフィングアタックによる成りすましの受入率である SFAR を、ω という 0~1 の範囲の値を用いて重みづけを行ったものである。こうして得られた FAR_ω と精度評価におけるもうひとつの性能尺度である FRR を用いて、β という 0~1 の範囲の値を用いて重みづけを施したエラー率 WER を算出する。

$WER = \beta \cdot FAR_\omega + (1-\beta) \cdot FRR$　　（β は 0~1 の値）

$FAR_\omega = \omega \cdot SFAR + (1-\omega) \cdot FAR$　　（ω は 0~1 の値）

本文献では様々なデータベースとアルゴリズムを用いて、このような方法の正しさを検証することで、アルゴリズムの良し悪しは単一の閾値では表現できず、重みづけをしたうえで評価すべきという結論を導いている。

② 脆弱性評定（3 章）

ここではバイオメトリクスのアタックポテンシャルの分析を行っている。内容は同定

フェーズ（Identification Phase）と悪用フェーズ（Exploitation Phase）に分けることを示した上で、アタックポテンシャルの構成要素である時間、知識、機会、機器に関する分析を行ったものである。

上記①で示された概念は本報告書作成時点において世界的に広く浸透しておらず、本事業での採用は予定していない。しかしながら、今後の欧州の精度評価に関するプロジェクトへの本概念の採用や、国際標準化活動において欧州から本概念に関する標準化提案が行われる可能性もあるため、国際連携活動の推進において本概念に関する欧州の動きがないか今後注視する必要がある。

(2) cPP サポート文書のドラフト提出

後述のとおり、精度評価のサポート文書素案を今年度の活動で作成した。これは、英訳の後、cPP サポート文書のドラフトとして活用され iTC で議論されることになる。脆弱性評価については、今までに指紋を対象としたサポート文書がドイツやスペインで開発されて来た。しかし、精度評価を CC 評価認証の中でどのように扱うかは十分に議論されて来なかった。精度評価サポート文書は BEAT プロジェクトによるものがあるだけで、本事業で作成しているサポート文書素案は BEAT プロジェクトのものより詳細な内容になっている。精度評価サポート文書のドラフトは、バイオメトリクス技術の CC 評価認証を進める上で重要な役割を果たすので、来年度の活動の成果も継続的に反映させていく。

5.2 追加ＰＰ開発とサポート文書全体構成案の作成

本事業では昨年度認証 PP を開発した。今年度は加えて、昨年度ベンダーから開発要求が出ていた登録処理を対象とする PP の追加開発を計画した。しかし、検討を進めると登録処理単独の PP を作ることはできないとの結論に達し、登録処理と認証処理の両方を対象とする PP を開発することになった。最終的には、各ベンダーの製品に適用することを考慮して、登録処理を含むバイオメトリック照合製品向けの PP を開発した。PP は 1 月 26 日に評価合格し、3 月末に認証予定である。

来年度は、この PP に適合する製品のパイロット CC 評価認証を予定している。実際に CC 評価認証するためには、CEM に不足する評価手法を決定する必要がある。PP に付随する評価方法で CEM に不足する内容は、一般的に、サポート文書としてまとめられる。本 PP のサポート文書として含むべき内容は、精度評価及び偽造生体等の脆弱性評価に関する内容である。評価方法としては、これらの内容がひとつのまとまっていることが望ましい。しかし、これらのふたつの内容は別々のサポート文書とまとめることになった。理由は、精度評価については、CC 評価認証の観点とは異なるが、ISO/IEC 19795 シリーズに要求事項がまとめられおり、ISO/IEC 19795 シリーズとの関係がわかり易い内容になっていることが望ましいという意見が有識者からあったことによる。以下に述べるとおり、本事業では、精度評価サポート文書及び脆弱性評価サポート文書のそれぞれ素案を今年度作成した。来年度のパイロット評価認証で、使用して検証して完成させる。

5.2.1 追加 PP 開発

昨年度開発した認証処理を対象とした PP（認証 PP と略記する）とは別に、新たに、登録処理を対象とした PP（登録 PP と略記する）を開発することを目標とした。この目標設定の理由は、昨年度の認証 PP 作成過程で、企業から登録 PP への要望があり、その必要性には妥当性があると考えたからである。

企業からの要望は、顧客から製品が偽造生体を登録しないことを要求されるためである。偽造生体の登録が可能であれば、登録したユーザと結託した別のユーザがなりすますことが可能になり、顧客に損害を与える可能性がある。よって、偽造生体が登録されないことは重要な要件である。昨年度は認証 PP を作成したが、バイオメトリクスを使った認証には登録処理が必須であることを考えれば、登録処理に関するセキュリティ機能要件が必要なことは当然のことである。

認証 PP とは独立の登録 PP を開発する方針としたのは、登録処理と認証処理の両方を実行する製品もあるが、登録処理だけの製品、認証処理だけの製品もあるとの指摘があったためである。いずれの製品も CC 認証を得ることを可能にするために、独立した認証 PP と登録 PP が必要になる。

しかし、独立した登録 PP は、作成過程で作成できないとの結論に達した。登録処理と認証処理を対象とする PP を作成することに方針変更した。以下に、登録 PP 作成の検討、登録処理と認証処理を対象とする PP 作成の検討について、報告する。

(1) 登録 PP 作成の検討

上記のとおり、登録 PP は最終的に作成できないという結論に達したが、以下にその検討経緯を報告する。

登録 PP は認証 PP の対になるものなので、バイオメトリクスに固有のセキュリティ機能要件及び保証要件を定めることを方針とした。すなわち、ISO/IEC 197972 が主張するエラー率、脆弱性評価に特化した PP を作成することにした。ISO/IEC 197972 ではプライバシーもバイオメトリクス固有の考慮が必要であると主張しているが、プライバシーについては、昨年度の認証 PP の検討過程で通常の IT セキュリティ製品と異ならないとの結論に達したので、登録 PP についても範囲外とした。

登録におけるエラー率は生体情報登録失敗率 FTE（Failure To Enrol）である。脆弱性評価は、偽造生体等に対する耐性評価である。ISO/IEC 197972 では、バイオメトリクス技術の脆弱性を以下の A から J のように分類している。このうち、登録に関係するものは、B・G・I 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）他人をまねたりする（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

登録 PP は、FTE 測定、上記の B・G・I に対する脆弱性評価をセキュリティ保証要件に含むようなセキュリティ機能要件を持つことが要求される。それらのセキュリティ機能要件に到達するようなセキュリティ課題定義、TOE のセキュリティ対策方針が必要である。

B・G・I に対する脆弱性評価を求めるための脅威は、偽造生体や品質の低い生体情報を意図的に登録することを試みる攻撃者がいて、次のようものが容易に考えられる。

・攻撃者が、偽造生体を登録したり、品質の低い生体情報を登録したりしようとするかも知れない。

この脅威に対抗する TOE のセキュリティ対策方針として、以下を考えることができる。

・TOE は、登録時に、データ採取機能に偽造生体が提示された場合または品質が低い登録生体情報となるように提示された場合等、それらを登録してはならない。

この TOE の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として、以下のような拡張セキュリティ機能要件を考えることができる。

・登録生体情報の検査は、登録されようとする情報を TSF が検査し、品質の低い生体情報または生体を模した偽造物を登録しないことを要求する。

これに対して、FTE 測定については、脅威を設定することはできない。生体情報登録が失敗することは、登録できないユーザは TOE を使えないだけで、何らの脅威も発生しないからである。セキュリティ課題定義の中の組織のセキュリティ方針として、以下を設定することを検討した。

・TOE は、登録ユーザの生体情報の登録の失敗を、一定の割合以下にしなければならない。

これに対して、形式的に以下のような TOE のセキュリティ対策方針を考えることはできる。

・TOE は、運用に支障のない生体情報登録失敗率(FTE)を持たなければならない。

しかし、上述の組織のセキュリティ方針自体がセキュリティに関する記述ではないので、最終的にセキュリティ機能要件を作成することはできない。

以上のような考察の結果、独立した登録 PP は作成できないと結論した。しかし、ベンダーは、FTE 測定は実施すべきと主張した。その根拠は、登録の際に、後の認証における FAR（False Accept Rate、誤受入率）や FRR（False Reject Rate、誤拒否率）が良くなるような生体情報だけの登録を許す可能性を排除できないからである。すなわち、FTE を悪くして FAR を見かけ上良くすることが可能である。もし、FTE 測定がなされず、FAR 測定及び FRR 測定だけがなされれば、上記の不正が可能である。よって、独立した登録 PP の作成はできないが、FTE 測定を要求する PP を検討することになった。すなわち、登録処理と認証処理を対象とする PP を作成し、その中で FTE 測定を要求することを新たな方針にした。

(2) 登録処理と認証処理を対象とする PP の検討及び作成

ベンダーの FTE 要求の根拠は、FAR 及び FRR が FTE に依存するということである。CC のセキュリティ機能要件の定義においては、依存性も定義されている。PP または ST において、あるセキュリティ機能要件 A を選択した場合、セキュリティ機能要件 A が依存するセキュリティ機能要件 B は選択されなければならない。セキュリティ機能要件 A を実現するために必要な機能要件は、それ自体がセキュリティに十分に関連してくても、セキュリティ機能要件 A に依存するセキュリティ機能要件として定義することができる。CC パート２のセキュリティ機能要件の中にもそのような例はある。FAR 及び FRR に関するセキュリティ機能要件は、昨年度作成した認証 PP で拡張コンポーネントとして定義されていた。よって、FTE に関する機能要件を FAR 及び FRR に関するセキュリティ機能要件が依存するセキュリティ機能要件として、PP の中で拡張定義することにした。

昨年度は国際化を考慮して英語で認証 PP を作成したが、来年度のパイロット評価認証で PP を基に ST 及び他の CC 評価のための文書を作成するので、今年度の PP は日本語で作成することにした。また、パイロット評価・認証に向けた準備として、ベンダーの CC 評価のための文書準備の過程で認証の用語が妥当でないことがわかり、認証を照合に変えた。認証は ID を主張するユーザが ID を対応する本人であることを確認する行為であるが、ベンダーの製品の中には、ID を全く処理せず、登録生体情報が外部から与えられて、入力された身体的特徴から得られる特徴データと登録生体情報が同一ユーザのものであるかだけを判定するものがあることがわかった。このような処理は、通常、バイオメトリック照合（Biometric verification）と呼ばれる。昨年度の認証 PP の内容をそのまま継承すると、一部のベンダーの製品は PP に適合しなくなるため、結果的に、認証処理ではなくバイオメトリック照合処理を対象とする PP に内容変更することになった。以下では、PP の構成に基づき、一部作成経緯に触れながら、登録処理と照

合処理を対象とする PP の内容について報告する。PP の名称は、処理の中心はバイオメトリック照合であることから、バイオメトリック照合製品プロテクションプロファイルとした。

［PP 概説］

CEM 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 の内容を簡潔に記述した。登録処理を含むことの記述以外は、昨年度作成した認証 PP と大きく変わらない。

本 PP は、CC の観点から、バイオメトリック照合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。バイオメトリック照合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 などによる利用者認証製品にはない、誤受入及び誤拒否のエラーに対する要件、偽造生体検知に対する要件等である。従って、本 PP においては、誤受入及び偽造生体検知に関係しない脅威は、取り扱わない。

本 PP は、TOE が使用する身体的特徴（顔、指紋、虹彩、静脈など）と対応する身体部分（静脈の場合は、指、てのひら、手の甲など）を特定しない。

本 PP は､バイオメトリック照合及びそのための利用者登録だけを対象とし､バイオメトリック識別を対象としない。

［TOE 概説］

次に、PP の 1.3 に記載のの TOE 概要について報告する。TOE 概要の構成は、以下のとおりであり、昨年度の認証 PP の構成から変更ない。

1.3.1. TOE の種別
1.3.2. 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
1.3.3. TOE の使用法
1.3.4. TOE の主要なセキュリティ機能
1.3.5. TOE の構成
1.3.6. TOE の使用が想定される環境
1.3.7. TOE の機能

既に述べたとおり、ベンダーの CC 評価のための文書準備の過程で TOE が含む機能の再検討が必要になった。また、登録処理において品質の悪い生体情報となるような身体的特徴の提示をした場合に生体情報登録がされないようにするための検査機能を追加した。これらはまとめて、1.3.7. TOE の機能に記述した。1.3.1.から 1.3.6.までについては、1.3.7.の内容変更に伴う変更及び表現の見直しを除くと、昨年度の認証 PP の記述と基本的に変わらない。

1.3.7. TOE の機能の概要は、以下の図 5.2-1 および図 5.2-2 のとおりである。図中の表記は、以下のとおりである。

・太枠は、TOE の範囲を表す。

・太枠内の実線四角（特徴抽出機能など）は、TOE が含む機能を表す。

・太枠内の破線四角（データ採取機能など）は、本 PP では提供されないとしているが、TOE が含んでよい機能を表す。

・太枠外の実線四角は、TOE の運用環境を表す。

・影の付いた実線四角は、ユーザを表す。

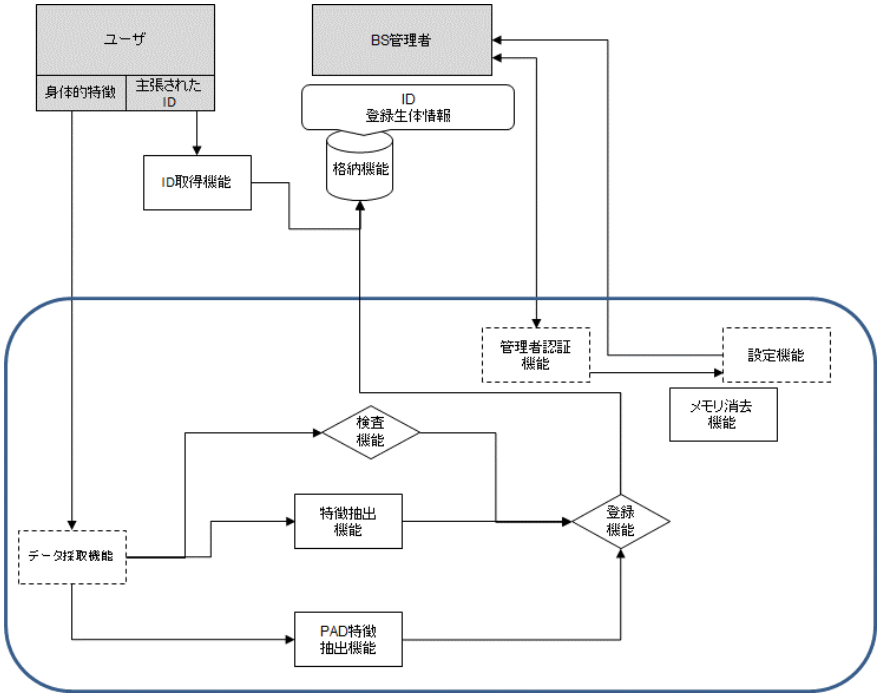


図 5.2-1　一般的な TOE の構成（登録の場合）

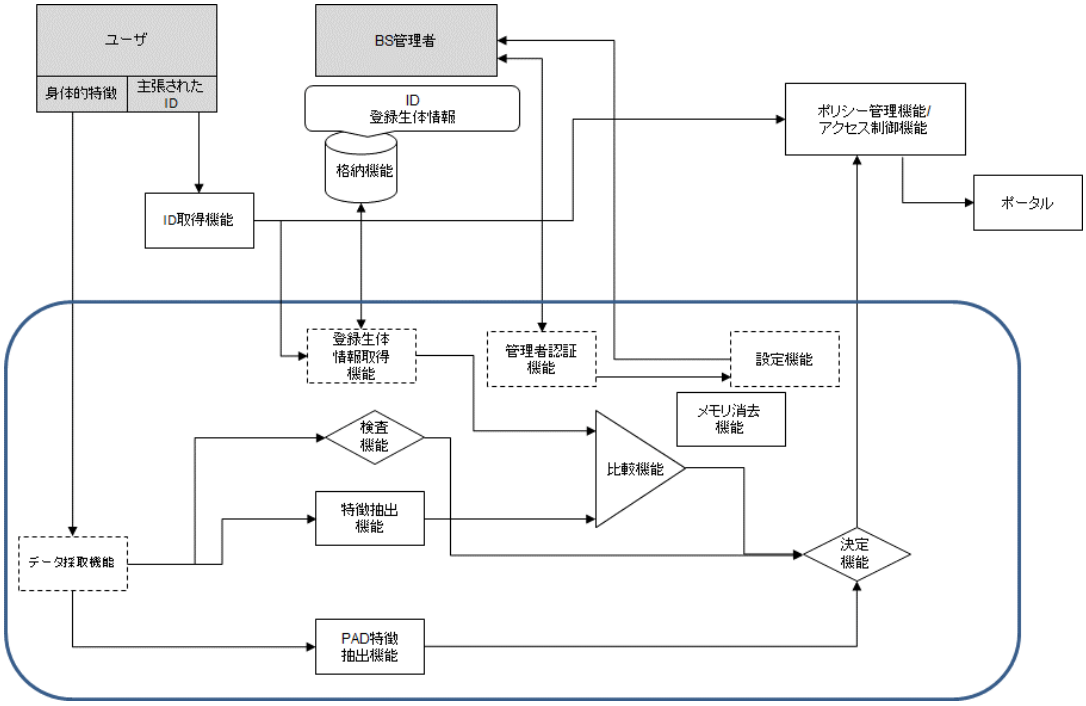


図 5.2-2　一般的な TOE の構成（照合の場合）

昨年度の認証 PP との違いは、登録の場合の図 5.2-1 の追加に加えて、以下のとおりである。

検査機能の追加は、既に述べたとおり、登録処理における要求からである。照合処理においても追加した。設定機能については、ベンダーによっては、公開していない場合もあるので、選択機能とした。よって、設定機能にアクセスするための BS 管理者に対する管理者認証機能についても、選択機能とした。データ採取機能は、昨年度の認証 PP では運用環境の機能としたが、TOE の選択的機能とした。登録生体情報取得機能については、ベンダーの CC 評価のための文書準備の過程で、製品によってはサポートしていないことがわかったため、選択機能にした。

選択機能は、cPP 化のための対策である。cPP では選択的セキュリティ機能要件を設定可能となる可能性が高いので、ベンダー各社が ST を作成し易いように、想定されるバリエーション毎にセキュリティ課題定義からセキュリティ機能要件までの組合せを PP の付録として記載した。しかし、cPP における選択的セキュリティ機能要件の記載方法が PP 認証の時点で決定しなかったため、付録として作成した選択的セキュリティ機能要件は、最終的には PP から削除した。

TOE が含む機能は以下のとおりである。

特徴抽出機能：

照合の前段階として、採取された生データから特徴が抽出される。これが、本機能の役割である。抽出されたデータは圧縮される場合もある。抽出されたデータを特徴データと呼ぶ。

検査機能：

この機能は、データ採取機能から得られた生データが以後の処理のために十分な品質を持っているかを検査する。

登録機能：

この機能は、検査機能によって登録に十分な品質を持つと判断され、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃でないと判断できる場合に、特徴抽出機能から得られた特徴データを登録生体情報として出力する。条件を満たさない場合は、登録生体情報となる特徴データを出力しない。

比較機能：

この機能は、特徴抽出機能で抽出された特徴データを格納機能に登録されて登録生体情報取得機能で取り出された登録生体情報と比較し、両者の類似度を算出する。

決定機能：

この機能は、検査機能、PAD 特徴抽出機能、及び比較機能の出力に基づき照合成功か照合失敗かを決定する。生データが十分な品質を持っていると検査機能が判断し、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃ではないと判断でき、特徴データと登録生体情報の類似度が要求される閾値を超える場合のみ、照合成功とする。いずれかの条件を満たさない場合は、照合失敗とする。また、完全一致は登録生体情報を特徴データとして再使用の可能性があるので失敗にすべきである。

PAD 特徴抽出機能：

PAD 特徴データは、データ採取機能が処理する生データから抽出される。PAD 特徴データは、データ採取機能への偽造生体などを使った攻撃の有無を決定するために使われ、登録時の登録機能における登録の成功/失敗の決定、照合時の決定機能における照合の成功/失敗の決定に使われる。

メモリ消去機能：

この機能は、攻撃からの保護のために、使用後のメモリの内容を消去する。消去されるべき情報は、登録生体情報、特徴データ、生データなどが含まれる。

TOE の選択機能は、以下のとおりである。

データ採取機能：

この機能は、ユーザから生データを採取し、特徴抽出機能や検査機能に生データを送る役割を担う。

登録生体情報取得機能：

この機能は、ユーザの ID に対応する既に登録された登録生体情報を取得する。

管理者認証機能：

この機能は、BS の管理者に対する識別・認証を担う。この手段の例としては、スマー

トカードと PIN が挙げられる。BS 管理者は、認証された後に、TOE のセキュリティ関連設定を許可される。

設定機能：

この機能は、BS 管理者に TOE のセキュリティに関連するパラメータの設定をするためのインタフェースを提供する。この機能は、TOE によっては、決定機能のための閾値設定に使われる。

TOE の運用環境の提供機能は、以下のとおりである。

格納機能：

運用環境は TOE が使うデータベースを提供しなければならない。このデータベースは、ユーザの登録生体情報を格納する。登録生体情報以外の情報を含むこともある。

ID 取得機能：

この機能は、ユーザが入力する ID を獲得する。この機能は、入力された ID に基づき生体情報を登録し、入力された ID で照合に使う登録生体情報を決めるので、セキュリティに関連している。この機能は、ユーザに見えるインタフェースを提供する。運用環境がこの機能を含むかどうかは製品に依存する。個人利用の製品の場合は、ユーザは自動的に決まるため、この機能は必ずしも必要ではない。

ポリシー管理機能/アクセス制御機能：

バイオメトリック照合の結果は、運用環境のポリシー管理機能/アクセス制御機能に渡される。この機能は、ユーザの権利をチェックし、ユーザが十分な権限を持っていて TOE によるバイオメトリック照合が成功し、利用者認証された場合に、ユーザのポータルへのアクセスを許可する。すなわち、この機能は、ポータルへのアクセス制御を実現するものである。

セキュア通信機能：

運用環境は、セキュリティ関連データのセキュアな通信をサポートする。セキュアな通信は、TOE からの通信、TOE への通信、TOE の構成要素間の通信の場合がある。

ポータル：

物理的または論理的な点であって、そこから先にある物理的または論理的な資産が運用環境のポリシー管理機能/アクセス制御機能で守られているような点である。ポリシー管理機能/アクセス制御機能は、上述のとおり、TOE からユーザの ID に対するバイオメトリック照合結果を受け取り、アクセス制御を実施する。

［適合主張］

2.適合主張では、2.1. CC 適合主張における拡張コンポーネントの記載及び 2.4.適合ステートメントを除いて、昨年度の認証 PP と同じである。昨年度の認証 PP では論証適合を許容して

いたが、cPP では論証適合は許容されないため、正確適合要求に変更した。昨年度の論証適合許容は ST において要件追加した場合の適合主張を考慮したためだったが、CC の定める方法での要件追加は正確適合とされることが確認できた。正確適合になるようなセキュリティ課題定義からセキュリティ機能要件までの組合せを、PP の付録として作成した。

［セキュリティ課題定義］

3.セキュリティ課題定義では、登録処理が加わったことと TOE が含む機能に変更があったことによって、昨年度の認証 PP から以下のような変更が生じた。

3.1.TOE に関連するエンティティにおいては、それぞれのエンティティの記述を変更した。BS 管理者については設定機能が TOE の必須機能ではなくなったため、登録ユーザについては TOE の処理がユーザ認証せずバイオメトリック照合に限定されたため、攻撃者については照合処理が加わったための変更である。

BS 管理者：

TOE のインストール（ハードウェアがある場合はその設置を含む）、設定、及び運用の責任を持つ。

登録ユーザ：

TOE を含む BS に生体情報を登録し、TOE にバイオメトリック照合され利用者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、登録時に偽造生体や品質の低い生体情報を意図的に登録することを試みたり、照合時に TOE に不正にバイオメトリック照合されることを試たりする。

3.2.資産については、登録ユーザについては TOE の処理がユーザ認証せずバイオメトリック照合に限定されたことによる変更だけである。

1 次資産：

TOE 外に存在する資産であって、登録ユーザが TOE でバイオメトリック照合され利用者認証されることによってポータルを経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 BS 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照合のためのパラメータなど。

3.3. 前提条件については、登録処理が PP に含まれ、データ採取機能が選択機能となったため、昨年度の認証 PP にあった A.ENROLMENT 及び A.CAPTURE を削除した。格納機能に関する前提条件 A.STORAGE は、A.ENVIRONMENT に統合した。設定機能が必須でなくなったため、昨年度の認証 PP の脅威 T.MODIFY_ASSETS を削除し、新たに A.PROTECT_ASSETS を追加した。その他は、表現の変更である。

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 のインストール（ハードウェアがある場合はその設置を含む)、設定、運用の責任を持ち、これらを正しく実行する。

適用上の注釈：

BS 管理者は、TOE が正しく稼動することに対して責任を持つ。しかし、攻撃者は、BS 管理者の目を盗み、偽造生体または品質の低い生体情報を登録するなどの可能性があり、そのような攻撃は、後述する T.PRESENTATION_ATTACK として定義されている。

A.PROTECT_ASSETS

TOE の 2 次資産は、改変、破壊、または収集されないように保護されている。

適用上の注釈：

例えば、閾値等のパラメータを変更する管理機能が運用環境より提供されている場合、そのような機能は BS 管理者だけが実施できるように管理されていなければならない。

A.COMMUNICATION

運用環境のバイオメトリクスの処理に関わる機能と TOE 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、保護されている。

A.ENVIRONMENT

TOE が正しく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。

適用上の注釈：

例えば、登録ユーザの登録生体情報を登録する格納機能は、適切に管理され、真正性と完全性が保たれている。また、TOE はウィルスなどマルウェアから保護されている。

3.4. 脅威については、設定機能が必須でなくなったため、昨年度の認証 PP の脅威 T.MODIFY_ASSETS を削除した。登録処理を PP に追加したため、T.PRESENTATION_ATTACK の内容を変更した。T.CASUAL_ATTACK については、TOE の処理がユーザ認証せずバイオメトリック照合に限定されたことによる変更だけである。

T.CASUAL_ATTACK

攻撃者が、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、自分自身の身体的特徴を提示するかも知れない。

T.PRESENTATION_ATTACK

攻撃者が、別の攻撃者に 1 次資産にアクセスさせることを狙い、品質の低い登録生体情報になるように身体的特徴を提示したり、偽造生体を提示して、登録を試みたりするかも知れない。また、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、品質の低い生体情報になるように身体的特徴を提示したり、偽造生体を提示したりするかも知れない。

3.5. 組織のセキュリティ方針については、登録処理を PP に追加したため、P.ENROL_ADMINISTERED の追加が必要になった。まあ、P.PORTAL_ACCECIBLE は P.CONTROL_FALSE_REJECT に名称を変更し、TOE の処理がユーザ認証せずバイオメトリック照合に限定されたことによる適切な変更を施した。

P.ENROL_ADMINISTERED

登録ユーザの生体情報登録は、BS 管理者だけが実行できるようにしなければならない。

P.RESIDUAL

登録ユーザの生体情報及びその他の関連データは、バイオメトリック登録及び照合の処理が終了して必要がなくなった時点で、削除するなどして利用できないようにしなければならない。

P.CONTROL_FALSE_REJECT

登録ユーザが身体的特徴の提示をした場合のバイオメトリック照合の失敗は、一定の割合以下にしなければならない。

[セキュリティ対策方針]

4.セキュリティ対策方針では、登録処理が加わったことと TOE が含む機能に変更があったことによって、昨年度の認証 PP から以下のような変更が生じた。

4.1. TOE のセキュリティ対策方針では、登録処理における PAD の要求である O.PAD_ENROL を追加した。その結果、昨年度の認証 PP の O.PAD を O.PAD_VERIFY と名称変更し、品質が低い生体情報となるように生体が提示された場合の対策を追加した。設定機能及び管理者認証機能が選択機能になったことで、O.AUTH_ADMIN を削除し、O.PROTECT_TSFDATA を運用環境のセキュリティ対策方針 O.PROTECT_ASSETS に移動した。その他、TOE の処理がユーザ認証せずバイオメトリック照合に限定されたことによる適切な変更を施した。また、FAR 及び FRR に対応する日本語を ISO/IEC 19795-1 の翻訳 JIS である JIS X8101-1 の用語に変更した。TOE のセキュリティ対策方針は、以下のとおりである。

O.PAD_ENROL

TOE は、バイオメトリック登録において、入力されたデータが偽造生体から採取されたもの

であった場合または品質が低い登録生体情報となるように身体的特徴が提示された場合、それらの登録を防止しなければならない。

O.CLEAR_RESIDUAL

TOE は、バイオメトリック登録及び照合の処理が終了後に、TOE 内に残存する生体情報及びその他の関連データを、削除しなければならない。

O.CONTROL_FALSE_ACCEPT

TOE は、誤受入率(FAR)に対する基準を満たさなければならない。

O.PAD_VERIFY

TOE は、品質が低い生体情報となるように身体的特徴が提示された場合、及び偽造生体が提示された場合、バイオメトリック照合が成功することを防止しなければならない。

O.CONTROL_FALSE_REJECT：

TOE は、誤拒否率(FRR) に対する基準を満たさなければならない。

4.2. 運用環境のセキュリティ対策方針における昨年度の認証 PP からの変更は、基本的には、登録処理が加わったことと TOE が含む機能に変更があったことに起因する 3.3. 前提条件の変更に伴うものである。運用環境のセキュリティ対策方針は、以下のとおりである。

OE.ENROL_ADMINISTERED

BS 管理者は、BS 管理者だけが TOE の登録処理を実行できるようにしなければならない。

OE.PROTECT_RESIDUAL_ENVIRONMENT

BS 管理者は、一時的に使用した生体情報があれば、必要がなくなった時点で削除するなどして保護できる運用環境を登録ユーザに提供しなければならない。

OE.ACCESS_CONTROL

BS 管理者は、バイオメトリック照合が成功した場合に限って、ユーザのポータルへのアクセスを許可する運用環境を提供しなければならない。

OE.LIMIT_NUM_TRIAL

BS 管理者は、生体情報登録の試行失敗が一定回数以上に達した場合、登録を失敗とするアプリケーションを利用しなければならない。また、バイオメトリック照合の試行失敗が一定回数以上に達した場合、当該ユーザのアカウントをロックするアプリケーションを利用して、TOE に対する試行回数を制限しなければならない。

OE.ADMINISTRATION

BS 管理者は、悪意を持たない者でなければならない。すなわち、攻撃者になったり、攻撃者に情報提供したりしてはならない。BS 管理者は、TOE のインストール（ハードウェア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.PROTECT_ASSETS

BS 管理者は、 TOE の 2 次資産が改変、破壊、または収集されないように保護する運用環境を提供しなければならない。

OE.COMMUNICATION

BS 管理者は、運用環境のバイオメトリクスの処理に関わる機能と TOE 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がセキュアな通信となる運用環境を提供しなければならない。

OE.ENVIRONMENT

BS 管理者は、TOE が正しく動作可能になるためのセキュアな運用環境を提供しなければならない。

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。後出の 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 5.2-1 を挙げるにとどめる。

表 5.2-1　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	OE.ENROL_ADMINISTERED	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_ASSETS	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x					x	x				
T.PRESENTATION_ATTACK	x			x				x	x				
P.ENROL_ADMINISTERED						x							
P.RESIDUAL		x					x						
P.CONTROL_FALSE_REJECT					x								
A.ADMINISTRATION											x		
A.PROTECT__ASSETS										x			
A.COMMUNICATION												x	
A.ENVIRONMENT													x

［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、登録処理が加わったことで登録処理に関わる新たな拡張コンポーネントの定義が必要になった。また、昨年度の認証 PP では FIA_BUA バイオメトリクスによる利用者認証を拡張定義したが、TOE の処理がバイオメトリック照合となったため、FIA_BUA の内容を変更し、名称も FIA_BVR（Biometric VeRifacation）とした。

5.1. 生体情報の登録 FIA_EBT（Enrolment of Biometric Template）では、O.PAD_ENROL を満たすために定義した。O.PAD_ENROL は、偽造生体が提示された場合や品質が低い登録生体情報となるように身体的特徴が提示された場合の登録を防止することを求めている。よって、これらに対応するセキュリティ機能要件が必要になる。また、FTE は FAR・FRR との相互関係があるため測定が必要とのベンダー意見に基づき、FTE に関する要件の定義も必要である。偽造生体が提示された場合のセキュリティ機能要件は、昨年度の認証 PP で定義した偽造生体提示に対するセキュリティ機能要件と同様に考えることができる。しかし、品質の低い登録生体情報となるように身体的特徴が提示された場合のセキュリティ機能要件は新規に検討が必要になった。これについては、8 月からベンダー各社へのインタビューで得られた意見、検討委員会で得られた意見を反映して、作成した。

低い登録生体情報となるように身体的特徴が提示された場合のセキュリティ機能要件を検討

するに当たって注意したのは、セキュリティ機能要件はテストが可能になるレベルで明確にしなければならないことである。生体情報の品質については、生体情報が TOE 内部の情報であるから、生体情報の品質も TOE に依存したものになってしまう。よって、生体情報の品質を指標にすると、TOE 非依存のテスト要件を記述することはできない。TOE に与えるデータの品質は TOE に依存せずに定義できる可能性は残るが、それも定義は難しい。データの品質に影響を与える要因については、ISO/IEC 19795-1 に網羅的に記述されている。データの品質に影響を与える要因に対する定量的指標で、テストを規定できないかを検討した。

登録時のデータの品質自体に影響を与える要因ではないが、精度に影響を与える要因について、ISO/IEC 19795-1 の Annex C (informative)に Factors influencing performance がある。PP はモダリティ非依存としているので、静脈に限定しない考察も実施した。しかし、結果的に静脈に限定した場合と同様であることがわかった。

ISO/IEC 19795-1 の C.2.4 User behaviour には以下がある。

movement: some systems require the subject to remain still, while others work better with some movement;
pose and positioning, for example:
facing camera, profile, angled;
offsets and rotations: affect fingerprint and hand systems;
distance to camera;
too high, too low, too far left or too far right;
prior activity, for example;
swimming: shrivelling of fingers will affect fingerprint systems;

これら要因は、静止していないこと、データ採取機器との位置関係が妥当でないこと（距離と角度）のふたつにまとめることができる。

ISO/IEC 19795-1 の C.2.5 User appearance には、以下があり、データ採取される生体の一部を隠すものである。

cosmetics: will temporarily alter face appearance;
glasses, sunglasses: can partly obscure the face or iris;

ISO/IEC 19795-1 の C.2.7 Sensor and hardware には、以下があり、上記と同様に、データ採取される生体の一部を隠すことにつながる。

dirt smears residual prints:
camera lens;

以上をまとめると、(登録) 生体情報の品質に影響を与える要因は、静止していないこと、データ採取機器との位置関係が妥当でないこと（距離と角度)、生体の一部が隠されていること、の３つである。これら３つの要因について、TOE 非依存の要件を定義できないかと考え、ベンダー各社に意見を求めた。しかし、たとえ静止していなくても、または生体の一部が隠れていても、

生体情報登録ができて正しく照合できることは製品の優位性でもあり、製品にとって後の照合のための十分な情報量があれば問題ない。十分な情報量は TOE に依存するので、TOE 非依存の要件を作ることはできないとの結論になった。ただし、これら要因に対する TOE の判断基準を、TOE 設計に記載することを求めることになった。

FIA_EBT ファミリの内容は、以下のとおりである。管理、監査に関する記述は省略する。

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ック照合のための生体情報の登録のメカニズムを定義する。このファミリは、生体情報の登録の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_EBT.1

登録時の生体情報の検査は、偽造生体や品質の低い生体情報の使用を防止できることを要求する。

FIA_EBT.2

生体情報登録失敗率の低い生体情報の登録は、後のバイオメトリック照合における精度を良く見せるために、照合され易い生体情報だけ使用することを防止できることを要求する。

FIA_EBT.1 登録時の生体情報の検査

下位階層: なし

依存性: なし

FIA_EBT.1.1 TSF は、TSF の利用者による品質が低い登録のための生体情報の使用を防止しなければならない。

適用上の注釈：

品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.1.2 TSF は、TSF の利用者による登録のための偽造生体の使用を防止しなければならない。

適用上の注釈：

偽造生体とは、 TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.2　生体情報登録失敗率の低い生体情報登録

下位階層: なし

依存性: なし

FIA_EBT.2.1　TSF は、FTE[割付：X]以下で動作する登録のための生体情報の受け入れメカニズムを提供しなければならない。

適用上の注釈：

FTE の定義は、TOE の登録ポリシーに依存する。ST 作成者はそのポリシー概略を示さなければならない。

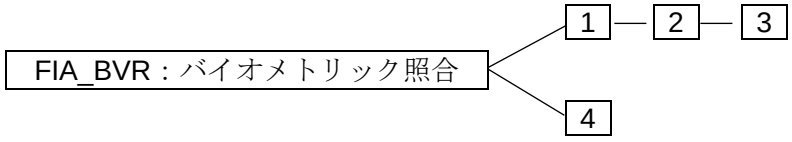
5.2. バイオメトリック照合 FIA_BVR は、昨年度の認証 PP で拡張定義した FIA_BUA をバイオメトリック照合に適応させたものである。ベンダーによっては、照合だけではなく認証をする製品もあるので、バイオメトリック照合のセキュリティ機能要件を FIA_BVR.1 として定義して、昨年度の FIA_BUA.1 から FIA_BUA.3 に対応するセキュリティ機能要件として FIA_BVR.2 から FIA_BVR.4 を定義した。FIA_BVR.4 は、FIA_EBT.1 に対応させて、品質の低い生体情報に対する照合の成功を防止するセキュリティ機能要件を加えた。FIA_BVR.1 から FIA_BVR.3 において、FIA_EBT.2 に依存性を持たせることによって、FIA_EBT.2 のセキュリティ機能要件としての存在理由としている。

FIA_BVR ファミリの内容は、以下のとおりである。管理、監査に関する記述は省略する。

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ック照合のメカニズムを定義する。このファミリは、バイオメトリック照合の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_BVR.1

精度の高いバイオメトリック照合は、TSF が利用者のバイオメトリック照合の誤受入及び誤拒否がそれぞれ一定の割合以下であることを要求する。

FIA_BVR.2

バイオメトリック照合による利用者認証のタイミングは、利用者の識別情報のバイオメトリック照合による利用者認証の前に、利用者があるアクションを実行することを認める。

FIA_BVR.3

アクション前のバイオメトリック照合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、バイオメトリック照合による利用者認証を要求する。

FIA_BVR.4

偽造生体等を受け入れないバイオメトリック照合は、品質が低い生体情報や偽造生体の使用を、バイオメトリック照合のメカニズムが防止することを要求する。

FIA_BVR.1 精度の高いバイオメトリック照合

下位階層: なし

依存性: FIA_EBT.1　登録時の生体情報の検査

FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.1.1 TSF は、各利用者に FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供しなければならない。

FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング

下位階層: FIA_BVR.1 精度の高いバイオメトリック照合

依存性: FIA_UID.1 識別のタイミング

FIA_EBT.1　登録時の生体情報の検査

FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.2.1 TSF は、利用者がバイオメトリック照合による利用者認証を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_BVR.2.2 TSF は、FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に当該メカニズムで認証が成功することを要求しなければならない。

FIA_BVR.3 アクション前のバイオメトリック照合による利用者認証

下位階層: FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_EBT.1　登録時の生体情報の検査

FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.3.1 TSF は、FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し､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、その利用者に当該メカニズムで認証が成功することを要求しなければならない。

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合

下位階層: なし

依存性: FIA_EBT.1　登録時の生体情報の検査

FIA_BVR.4.1 TSF は、TSF の利用者による品質が低い照合のための生体情報の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_BVR.4.2

TSF は、TSF の利用者による照合のための偽造生体の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

偽造生体とは、TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

5.3. 機能ファミリ FIA_EBT 及び FIA_BVR 定義の理由は、FIA_UAU ファミリに定義されているセキュリティ機能要件ではバイオメトリック照合に対するセキュリティ機能要件を正しく記述できないことを述べた。詳細は省略する。

［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。

6.1. セキュリティ機能要件 において定めるセキュリティ機能要件は､以下の表 5.2-2 のとおりである。TOE が含む機能が減ったため、昨年度の認証 PP と比べると機能要件は少なくなっている。

表 5.2-2　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	生体情報登録失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合

クラス FIA のセキュリティ機能要件については、拡張コンポーネント定義で述べたとおりである。もうひとつの FDP_RIP.1 は、以下のとおりである。

FDP_RIP.1サブセット残存情報保護

下位階層: なし

依存性: なし

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　[選択: ~~*への資源の割当て、*~~*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。

適用上の注釈：

ST 作者は、割当て解除するオブジェクトを全て割り付けよ。

6.2. セキュリティ保証要件 の内容は、昨年度の認証 PP から変更なく、以下の表 5.2-3 とおりである。

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. セキュリティ要件根拠 は、6.3.1. セキュリティ機能要件根拠 と 6.3.2.セキュリティ保証要件根拠 から成る。6.3.1. セキュリティ機能要件根拠 は、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 と 6.3.1.2. セキュリティ機能要件の依存性 とから成る。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 の詳細は省略するが、概要は以下の表 5.2-4 のとおりである。6.3.1.2. セキュリティ機能要件の依存性 については、各セキュリティ機能要件の定義で定義された依存性と PP の依存性に差異がないことを述べている。

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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X			
FIA_EBT.1	X				
FIA_EBT.2			X		X
FIA_BVR.1			X		X
FIA_BVR.4				X	

6.3.2.セキュリティ保証要件根拠 では、PP のセキュリティ保証要件の依存性が満たされていることを記述した。

［選択的なセキュリティ機能要件］

本事業で PP を作成する理由のひとつは、ST を作成することがベンダーにとっては難しいことである。最終的に作成した PP は TOE の機能が絞り込まれたため、国内ベンダーの製品でも PP の TOE が含む機能以外の機能を持つものが多い結果になった。これでは、本 PP に適合した ST を作成する場合に、ベンダーの負担が増大してしまう。本 PP に適合する ST 作成の負担軽減のために、国内ベンダー製品の事例を参考に TOE に機能が追加された 5 つの場合について、セキュリティ課題定義、セキュリティ対策方針、セキュリティ機能要件を、それぞれどのように変更したら良いかを示すガイダンスを PP の付録として作成した。最終的には、現行の CEM バージョン 3.1 改訂第 4 版においては付録の評価方法が定義されていないため、付録は評価認証の過程で削除することになった。しかし、本成果報告書では、その概要を示し、その内容を付録として掲載する。

第 1 の場合は、TOE が管理機能を持ち BS 管理者の利用者管理機能（利用者認証機能含む）を運用環境が持つ場合である。PP の本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定めた。これらは、昨年度の認証 PP にも含まれていなかった場合であり、今年度追加されたものである。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。ただし、BS 管理者

の利用者管理機能は運用環境が管理する。

第 2 の場合は、TOE が管理機能を持ち BS 管理者の利用者識別機能を持たず利用者認証機能を持つ場合である。PP の本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定めた。これらは、昨年度の認証 PP にも今年度の PP にも含まれていない場合であり、やや特殊な場合である。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。
TOE が、BS 管理者の利用者識別機能を持たないが、BS 管理者の利用者認証機能を持つ。

第 3 の場合は、TOE が管理機能も BS 管理者の利用者管理機能（利用者認証機能を含む）も持つ場合である。PP の本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定めた。これらは、昨年度の認証 PP には含まれていて、今年度の PP からは削除された内容を含む。BS 管理者に対する利用者認証機能がバイオメトリクスの場合が、昨年度の PP になく新規に追加した内容である。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。
BS 管理者の利用者管理機能も TOE が持つ。

第 4 の場合は、TOE が登録生体情報取得機能を持つ場合である。PP の本編に加えて、以下のような場合に対するセキュリティ機能要件を定めた。これは、昨年度の認証 PP には含まれていて、今年度の PP からは削除された内容である。

利用者が入力した ID を基に TOE が格納機能から登録生体情報を取得してバイオメトリック照合による利用者認証を実行する。

第 5 の場合は、TOE のコンポーネントが暗号化機能を持つ場合である。PP の本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定めた。これは、昨年度の認証 PP にはなく、今年度の PP で新規追加した内容である。

TOE 間のデータ授受に脅威が存在し、その対策として、TOE のコンポーネントが TOE の他のコンポーネントと授受するデータを暗号化する。

(3) PP の評価認証

今年度の PP 認証取得は、日本の認証機関である IPA で実施することにした。PP 認証取得の前段階としての評価機関による評価は、産総研規程により、競争入札で評価機関を決定した。2015 年 11 月 6 日に入札公告し、11 月 30 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 2016 年 1 月 29 日に設定された。IPA においては、今年度の PP 認証は、昨年度作成した認証 PP の内容変更として扱われることになった。PP の名称をバイオメトリック照合製品プロテクションプロファイルに変更することなどから成る申請書記載事項訂正願を 2015 年 12 月 1 日に IPA に提出した。

評価機関みずほ情報総研から 12 月 11 日と 1 月 14 日に確認シートが発行され、それぞれ 12 月 21 日と 1 月 16 日に回答と修正した PP を送付した。1 月 26 日に評価合格の評価報告書（案）を、評価機関みずほ情報総研から受領した。評価報告書（案）は認証機関 IPA に送付され、認証機関 IPA による認証作業が開始された。認証作業は 3 月末完了の予定である。本報告書作成時点で、IPA から 5 回の指摘があり、評価報告書（案）もそれに合わせて改訂されている。この過程で PP の付録は削除された。本報告書で参照した PP の内容は、IPA からの指摘を反映したものである。

5.2.2 精度評価サポート文書素案

静脈認証バイオメトリック製品に対する CC 評価の適用に向けて、バイオメトリック製品のセキュリティに関わる性能指標である誤受入率（FAR）、誤拒否率（FRR）、及び、登録失敗率（FTE）を評価するための精度評価に関するサポート文書素案を作成した。本素案は、静脈認証バイオメトリック製品の精度評価を CC 評価に適用するにあたり、静脈認証バイオメトリック製品に特有な必要事項をガイダンス文書としてまとめたものである。本素案では、ベンダーが静脈認証製品の精度評価を社内試験として実施した結果を評価機関に提示する際のエビデンス、及び、評価機関の社内試験エビデンスの適正さを確認するために実施する独立試験方法を記載した。精度評価サポート文書は 2017 年度に完成予定である。以降に、今年度の活動成果について説明する。

5.2.2.1 素案の構成

精度評価サポート文書素案は、作業効率上 2 つの文書として別々に作成した（2017 年度において 2 つの文書を合わせて 1 つの文書にまとめる予定である）。

① 精度評価サポート文書における社内試験エビデンス素案：静脈認証バイオメトリック製品の CC 評価を受けるベンダーが、評価機関に提示する精度評価に関する社内試験のエビデンス項目およびその内容をまとめたものである。

② 精度評価サポート文書における独立試験方法素案：上記①の社内試験エビデンスを受領した評価機関が、エビデンス内容の適正さを確認する目的で実施する精度評価のための独立試験の実施方法および判定方法をまとめたものである。

それぞれの素案作成にあたり実施した活動内容を 5.2.2.2 以降で説明する。

5.2.2.2 社内試験エビデンス素案作成活動

バイオメトリック製品の精度評価のためのサポート文書における社内試験のエビデンスの項目およびその内容に関する素案の作成活動の実施結果を以下に説明する。

(1) 作成方針決定

素案作成開始の際、以下の 2 つの作成方針を定めた。

① 精度評価の国際規格に基づくこととする

バイオメトリクスの精度評価に関する国際標準規格である ISO/IEC 19795-1 及び 19795-2 に記載されている、精度評価実施における準拠項目としての shall 表現及び推奨項目としての should 表現を抽出し、抽出した項目に基づいて素案を作成する[1]。両規格は、バイオメトリクスの精度評価の原則や方法を評価実施前の準備段階から評価実施後の報告内容までをまとめた内容となっており、社内試験のエビデンス項目を決定する際に、網羅性を高めることができると考えられたため、両規格を取り上げた。

② 社内試験への適用難易度を考慮する

各項目の記載にあたっては、ISO/IEC 19795-1 及び ISO/IEC 19795-2 の shall/should 表現を機械的に取り上げるのではなく、それぞれの項目の目的及びベンダーにとっての実施難易度を考慮したうえで、CC 評価に適用しやすい表現を採用する。両規格は研究機関や中立的な評価機関がバイオメトリクスの精度評価を実施する際に用いることを意図した記述が一部含まれており、すべての shall 表現や should 表現をそのままベンダーの社内試験に適用することが CC 評価の考えに必ずしも沿わない場合があることが判明した。例えば ISO/IEC 19795-1 では、誤合致率算出において、遺伝子的に同じ生体特徴の比較（同じ人の異なる指などの間の比較）は排除されなければならないと記述されている（ISO/IEC 19795-1 8.2.4.5 節）。これは、遺伝子的に近い身体部分同士の比較は誤合致を起こしやすく、結果的に誤受入率が悪化してしまうことを回避するためのものである。しかしながら、静脈認証製品のベンダーの多くは、同じ人の異なる身体部分でも自社アルゴリズムを使えば正しく判別することができ、誤受入することはないと考えていることがわかった。また CC 評価の観点においては、遺伝的に同じ生体特徴の比較を受け入れたとしても、誤受入率が悪化するだけであり CC 評価の健全性が損なわれることはない。また、同じ人の異なる身体部分を比較することは、偽者トランザクション数を増加できることを意味し、ベンダーにとっては誤受入率の評価の信頼性を高めることができる。このことから、同じ人の異なる身体部分同士の比較は、ISO/IEC 19795-1 では shall 表現を用いて禁止されていたとしても、精度評価の社内試験エビデンスのサポート文書素案としては許可することとした。このように、社内試験のエビデンスとしては許容した方が良いか否かをひとつひとつの shall 表現、should 表現で検討することとする。ただし、shall 表現を許容する場合は、試験の適正さを損なうことがないよう慎重に検討するとともに有識者からの意見を得た上で決定する。

(2) ベンダー・有識者調査の実施

前述(1)で示した作成方針に基づき、学会及びベンダーの有識者からヒアリング調査を実施した。調査内容は以下のとおりである。

① ベンダーアンケート調査

ISO/IEC 19795-1 及び ISO/IEC 19795-2 の shall 項目・should 項目をひとつひとつ表に整理し、各項目についてベンダーの社内試験エビデンス提示の難易度に関するアンケート調査を実施した。本アンケートでは難易度を 5 段階に分け（「容易」・「やや容易」・「普通」・「やや困難」・「困難」）、「やや困難」または「困難」と回答された項目について、その理由を記述してもらう形式とした。アンケート調査を実施したベンダーは国内の静脈認証ベンダー6 社で、半数以上から回答を得た。

② 有識者ヒアリング

ベンダーからの回答が「やや困難」あるいは「困難」だったものについて、それぞれの項目

の目的や意味を明確化するため、ISO/IEC 19795-1 及び ISO/IEC 19795-2 規格の有識者へのヒアリングを実施した。規格文書の各項目の意味や意図についての知見を得るとともに、素案作成に向けての助言を得た。

(3) 素案作成

ベンダーからのアンケート及び有識者ヒアリングの結果から、社内試験エビデンスの素案作成を行った。素案作成において考慮した点を以下に示す。また、素案そのものを付録-1 に示す。

① ベンダーアンケートにおいて実施難易度が「容易」、「やや容易」あるいは「普通」の回答だった項目については、原則素案に規格と同等の表現で記載することとする。

② ベンダーアンケートにおいて実施難易度が「やや困難」あるいは「困難」の回答だった項目については、各項目の意図を明確化するとともに、社内試験への適用の適切さを踏まえて表現方法を一部緩和する。

③ 本素案が対象とする性能尺度である FTE・FRR・FAR の社内試験における算出方法については、ISO/IEC 19795-1 及び ISO/IEC 19795-2 の記述だけではその意味の解釈がベンダー間で異なる余地があることが判明した。CC 評価に精度評価を適用するにあたり、ベンダー間で共通化が可能な算出方法を定める必要性があると考え、研究機関の有識者やベンダーの技術者との意見交換を実施し、共通化が可能な算出方法を検討した。

(4) 素案の主な内容

① 性能値の提示方法

バイオメトリック製品の性能を表す登録失敗率（FTE）、誤拒否率（FRR）、誤受入率（FAR）を CC 評価における社内試験エビデンスとして提示する場合、ベンダーは実測値と諸元値の 2 種類の値を提示しなければならないこととした。以下に、FTE、FRR、FAR それぞれについて、実測値と諸元値の記載方法を説明する。（これらの値を提示するとともに、その値の元となる各種エビデンスをベンダーは提示しなければならないが、エビデンスの詳細については本素案では触れておらず、来年度に追加する予定である。）

② 登録失敗率（FTE）

登録失敗率の実測値の記載方法を以下に示す。

$$\text{FTE 実測値} = \frac{\text{登録ポリシーを満足できなかった人の総数}}{\text{登録に参加した総人数}}$$

上記式の分子にある「登録ポリシー」とは、登録成功を満足するために必要な条件を意味

する。例えば、身体部位として指を用いるバイオメトリック製品の場合（指静脈)、少なくとも 2 本の指のテンプレート生成に成功することが登録ポリシーであったとすると、これを満足しなければ分子の数がカウントアップされる。表 5.2-5 に登録ポリシーと登録結果の具体例を示す。

表 5.2-5 登録ポリシーと登録結果の具体例

No	登録ポリシー（例）	テンプレート生成に 成功した身体部分の数	登録結果
1	最低限 1 つの身体部分の テンプレート生成が成功すること	1	成功
2	同上	0	失敗
3	最低限 2 つの身体部分の テンプレート生成が成功すること	2	成功
4	同上	1	失敗

次に登録失敗率の諸元値の記載方法を以下に示す。

FTE 諸元値	＝	実測値に基づきベンダーが定めた性能諸元値

ベンダー製品に二項検定が適用できる場合、諸元値は二項検定においてベンダーが定める信頼区間の上限値を超える値の中からベンダーが製品仕様として定めるひとつの値を選んだものである（統計手法において慣例的に 95%信頼区間が選ばれる場合ががあるが、本素案では特定の信頼区間を定めず、信頼区間の設定はベンダーの判断に委ねる)。二項検定が適用できない製品の場合、ベンダーはそれに代わる何らかの検定方法を根拠と共に提示し、その検定方法を用いてベンダーが定める信頼区間の上限値を超える値の中から選んだ諸元値を提示する。

登録失敗率算出におけるその他の留意事項を以下に示す。

- 人単位で集計する（身体部分単位ではない）
- ひとりが登録に参加できるのは 1 回とする（二重登録は許されない）
- ひとつの身体部分のテンプレート生成トランザクション数は 1 回とする（トランザクションの定義は概要をサポート文書で示し、詳細はベンダーが定義する）

③ 誤拒否率（FRR）

誤拒否率の実測値の記載方法を以下に示す。

$$\text{FRR 実測値} = \frac{\text{誤拒否が発生した本人トランザクション総数}}{\text{本人トランザクション総数}}$$

上記式の分子にある拒否とは、一度も照合に成功しなかったトランザクションを示すものであり、提示失敗など、テンプレートと照合バイオメトリックデータ間のマッチング失敗以外の要因で起きた誤拒否も含まれる。

次に誤拒否率の諸元値の記載方法を以下に示す。

FRR 諸元値	＝	実測値に基づきベンダーが定めた性能諸元値

登録失敗率の諸元値と同様、ベンダー製品に二項検定が適用できる場合、諸元値は二項検定においてベンダーが定める信頼区間の上限値を超える値の中から、ベンダーが製品仕様として定めるひとつの値となる。二項検定が適用できない製品の場合、ベンダーはそれに代わる何らかの検定方法を根拠と共に提示し、その検定方法を用いてベンダーが定める信頼区間の上限値を超える値の中から選んだ諸元値を提示する。

誤拒否率算出におけるその他の留意事項を以下に示す。

・部位単位で算出する（人単位ではない）

・ひとつの部位の照合トランザクション数は１回とする（トランザクションの定義はサポート文書で概要を示し、詳細はベンダーが定義する）

④ 誤受入率（FAR）

誤拒否率の実測値の記載方法を以下に示す。

$$\text{FAR 実測値} = \frac{\text{受入が発生した偽者トランザクション総数}}{\text{偽者トランザクション総数}}$$

上記式の分子にある受入とは、その偽者トランザクション内で最低一度照合に成功した（すなわち誤受入が発生した）事象を表すものである。

次に誤受入率の諸元値の記載方法を以下に示す。

FAR 諸元値	＝	実測値に基づきベンダーが定めた性能諸元値

登録失敗率及び誤拒否率の諸元値と同様、ベンダー製品に二項検定が適用できる場合、諸元値は二項検定においてベンダーが定める信頼区間の上限値を超える値の中からベンダーが製品仕様として定めるひとつの値となる。二項検定が適用できない製品の場合、ベンダーはそれに代わる何らかの検定方法を根拠と共に提示し、その検定方法を用いてベンダーが定める信頼区間の上限値を超える値の中から選んだ諸元値を提示する。

誤受入率算出にあたってのその他の留意事項を以下に示す。

- 部位単位で算出する（人単位ではない）
- 登録テンプレートと照合バイオメトリックデータのひとつの組の照合トランザクション数は 1 回とする（トランザクションの定義はサポート文書で概要を示し、詳細はベンダーが定義する）
- 登録テンプレートと照合バイオメトリックデータの組は順列ではなく組み合わせとする（ひとつの組の登録テンプレートと照合バイオメトリックデータを逆にして照合トランザクション数に加えてはならない）

⑤ 誤合致率（FAR）算出における遺伝子的に同じ生体特徴の比較について

前述のとおり ISO/IEC 19795-1 では、誤合致率算出において遺伝子的に同じ生体特徴の比較（同じ人の異なる指などの間の比較）は排除されなければならないと記述されているが（8.2.4.5 節）、本素案においては、遺伝子的に同じ異なる身体部分を用いた誤合致率算出を認めることとした。理由は、遺伝的に近い部位同士を比較するということはベンダーにとって不利な性能評価になると思われる。このことから、個人内比較を行うことが性能評価結果を不当に良い結果に欺くことにならないと言えるためである。

⑥ テクノロジ評価のためのシミュレーテッド・トランザクションの導入

精度評価をテクノロジ評価で実施しているベンダーが FAR や FRR などトランザクション単位の精度を提示する場合、保存されている一連のテンプレートや照合用バイオメトリックデータのセットから、想定アプリケーションに従ってトランザクションをシミュレートすることで精度を算出して良いこととする。これは、トランザクションを実行する際に、被験者に生体認証装置を都度使ってもらいその場でシナリオ評価を実行するのではなく、収集済みの一連のデータのセットを用いてトランザクションを再現できることを意味する。シミュレーテッド・トランザクションを用いる場合、最小・最大アテンプト回数や最小・最大プレゼンテーション回数など、通常の本人トランザクションや偽者トランザクションと同様の情報を作成し、評価機関に提示しなければならない。

⑦ 制御要因に関する配慮

ISO/IEC 19795-1 及び ISO/IEC 19795-2 における精度評価の制御要因に関する項目について、社内試験におけるデータ収集の困難さなどについて考慮を加える。具体的内容を以下に示す。

・被験者の属性である民族的出身に明確な定義を与えることはプライバシーの問題などから必ずしも容易ではない。民族的出身のエビデンスは、ベンダーが民族的出身を定義し、定義に沿って各被験者の属性を表現できるようにした。

・年齢をすべての被験者から収集することはプライバシーの問題などから必ずしも容易ではない。このため、ベンダーが年齢層の幅を定義し、それぞれの幅における被験者数などの情報をエビデンス化できるようにした。

・性能に影響を与える要因のうち、被験者の習熟度は定量化が困難なため、本活動において習熟度の定義づけを行った

・試験の環境要因として一般的に挙げられる温度、湿度、騒音などのうち、静脈に関係するものとして、定量化が可能な要素として ISO/IEC 19795-3 で取り上げられている温度を採用することとした。

制御要因に関するエビデンスを表 5.2-6 に示す。

表 5.2-6 社内試験における制御要因に関するエビデンス

No	要因	優先度案
1	母集団の人口統計	年齢層、性別、民族的出身（ただし海外市場が対象の場合）
2	アプリケーション	利用者の習熟度、生体情報登録~照合間の経過時間（習熟度が低の場合は異なる日の測定を推奨）
3	利用者の生理状態	なし
4	利用者の振る舞い	（習熟度が低の場合のみ）姿勢と位置決め（カメラの正面や角度など・頭の傾き・ずれ及び回転・カメラまでの距離・高すぎる低すぎるなど）
5	利用者の外観	なし
6	環境の影響	温度

表 5.2-7 に、本素案における被験者の習熟度の定義を示す。

表 5.2-7 習熟度の定義

No	分類	定義
1	低	正しい部位の提示方法を理解していない。 試行に失敗しても部位の提示方法の誤りかどうか確実に判断できない。以降の試行で部位の提示方法をどのように修正すべきか確実に判断できない。
2	中	正しい部位の提示方法を理解している。 部位の提示方法の誤りにより試行に失敗することがあるが、後の試行では正しい部位の提示方法に修正することができる。
3	高	正しい部位の提示方法をよく理解している。 ほとんどの場合、正しい方法で部位を提示できる。 部位の提示方法の誤りにより試行に失敗することがあるが、後の試行では正しい部位の提示方法に修正することができる。

5.2.2.3 独立試験方法素案作成活動

上記 5.2.2.2 で示した社内試験エビデンス素案に従ってベンダーが社内試験結果のエビデンスを評価機関に提示したあと、評価機関はエビデンスの内容を確認し、必要に応じて精度評価の独立試験を実施する。ここでは、評価機関による独立試験方法についての素案作成活動について説明する。

バイオメトリック製品の精度評価のためのサポート文書における独立試験素案の作成は以下の流れに沿って実施した。

(1) 独立試験方法の洗い出し

精度評価のための独立試験として評価機関にとって実現性が高いと考えられる試験方法の洗い出しを行った。独立試験方法には以下の 2 種類が考えられる。

・被験者試験：評価機関が独自に被験者を募集して行う精度評価である。募集する被験者の人口統計的な属性、実行する登録や照合のためのトランザクション処理の内容（最小・最大アテンプト数など）や温度環境など、社内試験と同等の条件で評価者が独立して行う試験である。試験の独立性を高めるため、評価機関が用意した精度評価ツールを用いる場合がある。

・立ち入り試験：誤受入率を測定するためのテクノロジ評価を行うことを主な目的として、評価機関がベンダーの社内試験環境に立ち入って行う精度評価である。上記の被験者試験で生成された被験者のテンプレートや照合バイオメトリックデータ

をベンダーの社内試験環境に持ち込むことにより、評価機関が独自に生成したデータを含めたテクノロジ評価を行う。

(2) 有識者ヒアリング

上記(1)で示した独立試験の方法の進め方を検討するにあたり、バイオメトリック製品の精度評価および CC 評価の有識者に対して被験者試験および立ち入り試験の必要性や実施方法に関するヒアリング調査を実施した。主な意見を以下に示す。

① 被験者試験について

・近年のプライバシー意識の高まり等から国内で被験者を集めることは困難になりつつあり、今後この傾向はさらに強まると思われる。海外の CC 評価機関からも、評価機関による被験者集めは非常に難しく、そういった要件が課されると妥当なコストと期間で CC 評価を実施することが不可能になり、制度として成り立たなくなると危惧されている。

・海外で被験者を集めるのに数百万円かかったとしても RFP に書かれるのであれば費用は関係ない。信頼性の低い製品が書面だけで認定を受けられないよう、評価機関による被験者試験という選択肢を残すべきである。

・被験者試験で募集する被験者は、募集コストの問題があるのであれば少人数であったり、評価機関の職員が被験者であったりすることはやむを得ない。しかしながら、何も動かさずにベンダーが作成した書類や試験環境だけで判断するべきでない。評価機関は導入者の代理人という立場で試験をすべきである。被験者数がたとえ 30 人であったとしても、そのような小規模ユースの利用者もいるはずである。

② 立ち入り試験について

・立ち入り試験では、社内試験環境のデータベースに保存されているテンプレートや照合バイオメトリックデータの並びのままで再現させるだけでなく、何らかの方法でデータを並べ替えて実行し、それでも同じ結果が出るかどうかを試験した方が、確実性が向上する。

・社内試験環境のデータベースに保存されている項目の並べ替えの方法をどの程度まで詳細に行うか、評価機関として十分に検討した上で試験を実施すべきである。ID の並べ替えだけでなく、データの中身の入れ替えまで考えるべきである。また、並べ替えの操作を行う人も、ベンダーではなく評価機関の試験官であるべきである。

・社内環境の一部を別のテンプレートに置き換えてクロスマッチを行い、入れ替えた部分以外が一致するかどうかを評価するという方法も考えられる。

(3) 基本方針

有識者からのヒアリング結果を踏まえ、精度評価のための独立試験に関する選択肢を以下の 2 種類とし、これらの選択肢の内容を検討するとともに、これらの選択肢をどのように使い分けるかをまとめたものを、精度評価のサポート文書における独立試験方法の素案とする。本素案の中では、これらの選択肢のうち、今年度は特に重要性が高いと考えられる被験者試験についてまと

める。

① 被験者試験：ベンダーが示す FTE・FRR・FAR などの精度値の正しさを検証するためには、精度値に応じて非常に多数の被験者を募集しなければならなくなるが、試験コストの問題から制度として成立させることが困難となるため、できる限り少数の被験者で試験を実施する方針とする。

② 立ち入り試験：ベンダーの社内試験環境のデータベースの項目を並べ替えるとともに、被験者試験で収集したテンプレートや照合バイオメトリックデータをベンダーの社内試験環境に持ち込み、ベンダーのデータベースに追加（あるいは置換）した上で偽者トランザクションを実行し、ベンダーが示した性能が得られることを確認する方法について検討する。

(4) 解決すべき課題

近年のバイオメトリック製品、特に静脈認証の性能向上より、ベンダー製品の FRR や FAR の諸元値を少数の被験者数で検証することは非常に困難である。高性能の製品をより厳密に評価するために被験者を多数募集すると大幅な人件費の増加を招く。仮に FRR が 0.1%の製品があったとして、それだけの率を測定するために 1000 人の被験者が必要だとすると、被験者に支払う報酬を 1 万円／人とした場合これだけで試験コストは 1 千万円となる。このため被験者試験における被験者の募集人数は、コストが障壁にならない程度に十分に少ない数に抑え、かつ、できる限り信頼性の高い判定手段を考案しなければならない。

(5) 素案作成

有識者ヒアリングの結果、および、解決すべき課題を考慮し、独立試験方法に関する素案作成を行った。以下に、被験者試験と立ち入り試験の概要を示す。また、素案を付録-2 に示す。

① 被験者試験

少人数の被験者で FTE、FRR、FAR を測定した場合、測定されたエラー率とベンダーが ST に記載した FTE 諸元値、FRR 諸元値、FAR 諸元値とを単純に比較して合否判定しようとすると、エラーが 1 つで出たか出なかったかで合否が決まってしまう場合もある。少人数被験者による測定は統計的な信頼度が低くなるため、その測定結果で製品の性能を評価することができない場合がある。この問題を解決するため、以下の方法を採用することとする。

(a) 評価機関はベンダーの社内試験エビデンスを詳細にチェックし、FTE、FRR、および FAR が十分に信頼できる程度に適正に試験され、測定されていることを書面上で確認する。

(b) 評価機関はベンダーの社内試験エビデンスの充実度、および、ST に記載されている性能値（FTE 諸元値、FRR 諸元値、FAR 諸元値）から、被験者試験で募集する被験者数を決定する。

(c) 評価機関は被験者を募集し、被験者全員に対して登録試験及び本人トランザクション試験を実施し、FTE 実測値及び FRR 実測値それぞれを算出するための、分子に相当するエ

ラー数、および、分母に相当する人数（FTE の場合）やトランザクション数（FRR の場合）を集計する。

(d) 評価機関は社内試験エビデンスで提示されたエラー数に独立試験で集計されたエラー数を加算して総エラー数を算出する。次に、以下の方法で社内試験結果と独立試験結果を合算した FTE、FRR を算出する（これらをそれぞれ合算 FTE、合算 FRR と呼ぶこととする）。

・合算 FTE：社内試験エビデンスで提示された登録に参加した被験者の総数に、独立試験において登録に参加した被験者数を加算して、登録試験参加者の合算値を計算する。次に、社内試験エビデンスで提示された登録ポリシーを満足しなかった被験者の総数に、独立試験で登録ポリシーを満足しなかった被験者の総数を加算して、登録ポリシーを満足しなかった人の総数を計算する。このようにして得られた登録参加者の総数を分母とし、登録ポリシーを満足しなかった人の総数を分子として、合算 FTE を算出する。

・合算 FRR：社内試験エビデンスで提示された本人トランザクション数に、独立試験で実施した本人トランザクション数を加算して、本人トランザクションの合算値を計算する。次に、社内試験エビデンスで提示された誤拒否件数に、独立試験で発生した誤拒否件数を加算して、誤拒否件数の合算値を計算する。このようにして得られた本人トランザクションの総数を分母とし、誤拒否件数を分子として、合算 FRR を算出する。

(e) 評価機関は合算 FTE、合算 FRR がそれぞれベンダーの FTE 諸元値、FRR 諸元値以下であれば、性能を満足したと判断する。

② 立ち入り試験

上記①で実施した被験者試験により収集された被験者のテンプレートおよび照合バイオメトリックデータをベンダーの社内試験環境に持ち込み、試験環境のデータベースに書き込むとともに、データベースの項目の並べ替えを実施したのち、偽者トランザクションを実行する。この際評価機関は以下の作業を実施することとする。

(a) ベンダーの社内環境にて、偽者トランザクションを実行する何らかのツール（通常はベンダーが作成したツール）を用いてデータベースに保存されたテンプレートと照合バイオメトリックデータ間が総当たりで照合されるよう、偽者トランザクションを実行する。この試験で得られた偽者トランザクションの総数を分母とし、誤合致件数を分子として、FAR を得る（ここではこれを合算 FAR と呼ぶこととする）。

(b) 評価機関は合算 FAR がベンダーの FAR 諸元値以下であれば、性能を満足したと判断する。

(c) 独立試験で募集した被験者のテンプレートあるいは照合バイオメトリックデータを含まない偽者トランザクション、すなわち、ベンダーが社内試験で募集した被験者のテンプレートや照合バイオメトリックデータを用いた偽者トランザクションによる結果が、ベンダーの社内試験エビデンスの内容にすべて一致することで、社内試験の適正さを確認する。

③ 精度評価における総合判定

評価機関は、以下の 2 つの条件を共に満足すると判断できる場合、ベンダー製品が ST に記載する FTE 諸元値、FRR 諸元値、FAR 諸元値を認定する。

(a) ベンダーが提示した社内試験エビデンスの内容が十分に適正で矛盾がないことが、机上の検査で確認されること。

(b) 独立試験で得られた合算 FTE・合算 FRR・合算 FAR がすべてベンダーの諸元値以下であること。

(c) 立ち入り試験で実行したベンダーが募集した被験者のテンプレートと照合バイオメトリックデータによる偽者トランザクションの試験結果が社内試験エビデンスの結果と一致すること。

5.2.2.4 今後の予定

2017 年度に予定されているパイロット評価における評価対象ベンダーによる社内試験エビデンス作成、および、評価機関による独立試験で使用されることを想定し、ベンダーの作業や評価機関の作業が滞りなく推進できるようスケジュールに沿って改定作業を進める。

5.2.3 脆弱性評価サポート文書素案

脆弱性評価サポート文書は、精度評価サポート文書とは異なり、前例として、2009 年にドイツで作成された FSDEG（Fingerprint Spoof Detection Evaluation Guidance）と EU の BEAT（Biometric Evaluation And Testing）プロジェクトで作成された D6.5: Towards the Common Criteria evaluations of biometric systems がある。脆弱性評価サポート文書作成に当たっては、いずれも指紋を対象にしたものであるが、FSDEG 及び D 6.5 を調査し、それらの調査結果を考慮して素案を作成した。素案作成には、ベンダー各社に意見を求め、意見をまとめた結果を検討委員会で審議した。脆弱性評価サポート文書はまだ素案の段階であり、来年度のパイロット評価認証開始までに原案として完成させる。

(1)既存サポート文書の調査

FSDEG は、2009 年にドイツで開発された FSDPP（Fingerprint Spoof Detection Protection Profile）のサポート文書である。FSDEG は、非公開文書であるが、SC 27 に対してスタディピリオドの寄書として提供された。当該スタディピリオドは、SC 37 の ISO/IEC 30107 に対応してセキュリティの観点から検討するもので、ISO/IEC 19989 の開発の基になった。また、D6.5 は EU の BEAT（Biometric Evaluation And Testing）プロジェクトで作成した文書である。プロジェクト完了の 2016 年 3 月末の公式な文書公開前に、2015 年 10 月の SC 27 ジャイプール会議の直前に、ドイツとフランスから ISO/IEC 19989 プロジェクトへの寄書として提出された。

［FSDEG］

FSDEG は、Part A から Part C までの 3 つの部分から構成される。Part A は、スコープや用語定義など、全体の導入部分である。Part B と Part C が CC 評価ガイダンスで CEM を補うサポート文書に相当する内容であり、Part B は ATE 及び AVA を除く保証要件クラスである ASE クラス・ADV クラス・AGD クラス・ALC クラスについて、Part C は保証要件クラス ATE 及び AVA について、それぞれ記述している。

ASE クラスについては、ST の保証要件のクラスである。FSDEG が FSDPP のサポート文書であり、FSDPP の TOE が指紋認証のなりすまし防止機能に限定されたものであるため、本事業で作成した PP のサポート文書には適用できない。

ADV クラスについては、セキュリティアーキテクチャの保証要件を定める ADV_ARC、機能仕様の保証要件を定める ADV_FSP、及び TOE 設計の保証要件を定める ADV_TDS について、CEM を補足する要件を定めている。以下では、本事業で作成するサポート文書が対応すべき EAL2 相当の内容に限定して記述する。

ADV_ARC

ワークユニット ADV_ARC.1-5 への補足

評価者は、バイパス防止の観点から、センサーからの指紋情報と PAD 情報が同一の生体から得ることを確実にするメカニズムが記述されていることを、検査しなければならない。

ADV_FSP

ワークユニット ADV_FSP.2-1 への補足

評価者は、TSFI の観点から PAD に使われているメカニズムが記述されていることを、検査しなければならない。

ワークユニット ADV_FSP.2-3 への補足

評価者は、センサーが TOE に含まている場合は、ユーザがどのようにセンサーを使うか、センサーへの身体的特徴の提示方法が記述されていることを、検査しなければならない。

ワークユニット ADV_FSP.2-4 への補足

評価者は、TSFI のセキュリティに関連するパラメータの記述を、検査しなければならない。

ワークユニット ADV_FSP.2-7 への補足

評価者は、PAD で検知された場合のフィードバックが提供されていないことを、検査しなければならない。

ADV_TDS

ワークユニット ADV_TDS.1-4 への補足

評価者は、PAD に使われている身体的特徴とメカニズムがサブシステムレベルで記述され

ていること、PAD 特徴から PAD エビデンスへの処理が記述されていることを、検査しなければならない。

PAD エビデンスとしては、体温、湿度、伝導性、血流、血流酸素濃度、光学濃度などが挙げられている。

ワークユニット ADV_TDS.1-5 への補足

評価者は、PAD 機能とデータ採取機能の相互関係が記述されていることを、検査しなければならない。

AGD クラスについては、 利用者操作ガイダンスの保証要件を定める AGD_OPE、準備手続きの保証要件を定める AGD_PRE について、CEM を補足する要件を定めている。以下では、本事業で作成するサポート文書が対応すべき EAL2 相当の内容に限定して記述する。

AGD_OPE

ワークユニット AGD_OPE.1-2 及び AGD_OPE.1-3 への補足

評価者は、TOE への身体的特徴の提示のプロセス及び PAD のパラメータの設定方法が記述されていることを、検査しなければならない。

ワークユニット AGD_OPE.1-4 及び AGD_OPE.1-5 への補足

評価者は、PAD の結果をオペレータが手動で変更することが許可されている場合はその方法が記述されていることを、検査しなければならない。

AGD_PRE

ワークユニット AGD_PRE.1-2 への補足

評価者は、特に、PAD 機能を変更するパラメータ及び使用前の設定されなければならないパラメータについて設定方法が記述されていることを、検査しなければならない。

ALC クラスについては、 TOE の CM 範囲の保証要件を定める ALC_CMS、欠陥修正の保証要件を定める AGD_FLR について、CEM を補足する要件を定めている。以下では、本事業で作成するサポート文書が対応すべき内容に限定して記述する。

ALC_FLR

ワークユニット ALC_FLR.1-1 から ALC_FLR.1-5 への補足

評価者は、開発過程で PAD 機能が偽造生体を誤って受け入れられたことが欠陥とされていることを、検査しなければならない。

ATE クラスについては、 機能テストの保証要件を定める ATE_FUN、独立テストの保証要件を定める ATE_IND について、CEM を補足する要件を定めている。以下では、本事業で作成す

るサポート文書が対応すべき EAL2 相当の内容に限定して記述する。

ATE_FUN

ワークユニット ATE_FUN.1-2 への補足

評価者は、テスト計画に開発者がテストのために作成する偽造生体に関する情報（素材や作成マニュアル）について記述されていることを、検査しなければならない。

ワークユニット ATE_FUN.1-3 への補足

評価者は、ST に記載されている TOE の設定のとおりにテスト計画に PAD のパラメータが正しく設定されていることを、検査しなければならない。

ワークユニット ATE_FUN.1-7 への補足

評価者は､開発者は PAD 機能のテストに使った偽造生体の数とテスト数が適切であるか、テスト結果を検査しなければならない。

ATE_IND

ワークユニット ATE_IND.2-1 への補足

評価者は、ST に記載されている TOE の設定のとおりに PAD のパラメータが正しく設定されていることを、検査しなければならない。

ワークユニット ATE_IND. 2-4 への補足

評価者は、開発者が作った偽造生体を使って開発者テストを繰り返して、検査しなければならない。

ワークユニット ATE_IND. 2-6 への補足

評価者は、認証機関が提供する偽造生体作成方法を基に、独立テストのための偽造生体を作成しなければならない。

ワークユニット ATE_IND.2-8 への補足

評価者は、評価者が作成した偽造生体を使ってテストを実施しなければならない。

ワークユニット ATE_IND. 2-9 への補足

評価者は、偽造物の作成方法と使用方法を記録しなければならない。

ワークユニット ATE_IND. 2-11 への補足

評価者は、評価者が PAD 機能のテストに使った偽造生体の数とテスト数を、報告しなければならない。

AVA クラスについては、 脆弱性分析の保証要件を定める AVA_VAN について、CEM を補足する要件を定めている。以下では、本事業で作成するサポート文書が対応すべき EAL2 相当の内容に限定して記述する。

AVA_VAN

ワークユニット AVA_VAN.2-1 への補足

評価者は、PAD のパラメータについて、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を検査しなければならない。

ワークユニット AVA_VAN. 2-4 への補足

評価者は、TOE に存在する可能性がある潜在的な PAD 脆弱性を識別するために、ST、ガイダンス証拠資料、機能仕様、TOE 設計、及びセキュリティアーキテクチャ記述の証拠の探索を実施しなければならない。

ワークユニット AVA_VAN. 2-6 への補足

侵入テストの実行は、FSDEG が提供する手法を考慮すること。

ワークユニット AVA_VAN.2-8 への補足

評価者は、侵入テストのために作成した偽造生体の作成方法を侵入テスト証拠資料に含めなければならない。

ワークユニット AVA_VAN. 2-9 への補足

侵入テストの実行は、FSDEG が提供する手法を考慮すること。

ワークユニット AVA_VAN. 2-11 及び AVA_VAN. 2-12 への補足

PAD の攻撃能力計算は、FSDEG が提供するガイダンスを参照すること。

FSDEG では、以上に述べた CEM への補足に加えて、指紋認証の PAD メカニズムに対応する偽造生体作成の概要を紹介している。これは、ワークユニット AVA_VAN. 2-6 及び AVA_VAN. 2-9 で参照されている。ワークユニット AVA_VAN. 2-11 及び AVA_VAN. 2-12 から参照されている攻撃能力計算とその例が、FSDEG では提示されている。FSDEG の攻撃能力計算は、攻撃能力計算において考慮する要因と要因に割り当てられた値は CEM と同様であるが、攻撃のフェーズを CEM が識別と実行のふたつに分けているのに対し、FSDEG では攻撃準備・偽造生体作成準備・攻撃実施の 3 つに分けている。結果的に D 6.5 で改良案が示されたので、FSDEG の攻撃能力計算については報告しない。

[D 6.5]

D6.5 では、保証要件クラスは、FSDEG よりも簡単に扱われている。FSDEG が CEM のワークユニット毎に追加すべき評価方法を記述しているのに対して、D 6.5 では、ASE クラス・ADV クラス・AGD クラス・ALC クラスにおける評価観点を簡単にまとめているに過ぎない。D 6.5 の中心は、BEAT プロジェクトで検討した新しい攻撃能力計算の提案である。記述のとおり、FSDEG では攻撃能力計算において考慮する要因と要因に割り当てられた値は CEM と同様だった。しかし、D 6.5 では、攻撃能力計算において考慮するふたつの要因を新たに導入し、値も CEM とは異なるものを導入している。以下の表 5.2-8 に、CEM と D 6.5 に記載された BEAT との攻撃能力計算を比較する。

表 5.2-8　攻撃能力の計算

	要因	CEM	BEAT		
			識別	実行	注
1	所要時間				
	<= 1日	0	0	0	
	<= 1週間	1	1	2	
	<= 2週間	2	2	4	
	<= 1ヶ月	4	4	8	
	<= 2ヶ月	7	8	16	
	<= 3ヶ月	10	8	16	
	<= 4ヶ月	13	8	16	
	<= 5ヶ月	15	8	16	
	<= 6ヶ月	17	8	16	
	> 6ヶ月	19	8	16	
2	専門知識				
	しろうと	0	0	0	
	熟練者	3	2	4	
	エキスパート	6	4	8	
	複数のエキスパート	8	8	0 (Not Appl)	
3	TOEの知識				
	公開	0	0	0 (Not Appl)	
	限定的	3	2	0 (Not Appl)	
	機密	7	4	0 (Not Appl)	
	危機的	11	8	0 (Not Appl)	
4	機会				
	不必要/無制限のアクセス	0	-	-	
	容易	1	0	0	
	中	4	2	4	
	困難	10	4	8	
	なし	x	-	-	
5	機器				
	標準	0	0	0	
	特殊	4	2	4	
	特別注文	7	4	8	
	複数の特別注文	9	-	-	
6	身体的特徴へのアクセス				
	即時	-	0 (Not Appl)	0	2D, 3D(顔)
	容易	-	0 (Not Appl)	2	指紋
	中	-	0 (Not Appl)	4	虹彩
	難	-	0 (Not Appl)	8	静脈
7	成功率				
	70%-100%	-	0 (Not Appl)	0	
	30%-70%	-	0 (Not Appl)	2	
	<30%	-	0 (Not Appl)	4	

D 6.5 では、識別と実行では実行の方に大きな値が割り当てられている。これは、識別で攻撃方法に関する情報が得られた上に新たに攻撃を効率的に積み上げることができるを表現している。身体的特徴へのアクセスでは、攻撃実行時の偽造生体作成のための身体的特徴を入手の困難さを表したものである。昨年度から、静脈は他のモダリティに比べて偽造生体作成のための身体的特

徴を入手が困難であるにも関わらず、CC 評価認証において考慮されないことがベンダーから問題提起されていた。身体的特徴へのアクセスの要因の導入は、上記問題の解決策になるものである。成功率は、値の割当の再考は必要かも知れないが、種々の環境要因に影響され易いバイオメトリクスの技術においては、攻撃能力計算において考慮されるべき要因であろう。

D 6.5 における攻撃能力は､各要因の識別と実行の値の総和として計算される｡脆弱性及び TOE 抵抗力のレート付けについて、CEM の場合と D 6.5 の場合を、以下の表 5.2-9 に示す。

表 5.2-9　CEM の脆弱性及び TOE 抵抗力のレート付け

値	シナリオの悪用に必要な攻撃能力	TOE は、次の攻撃能力を持つ攻撃者に対抗する	満たされる保証コンポーネント	不合格になるコンポーネント
0-9	基本	レート付けなし	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10-13	強化基本	基本	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
14-19	中	強化基本	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	高	中	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>25	高より上	高	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

表 5.2-10　D 6.5 の脆弱性及び TOE 抵抗力のレート付け

値	シナリオの悪用に必要な攻撃能力	TOE は、次の攻撃能力を持つ攻撃者に対抗する	満たされる保証コンポーネント	不合格になるコンポーネント
0-10	基本	レート付けなし	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
11-20	強化基本	基本	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
21-30	中	強化基本	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
31-40	高	中	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>41	高より上	高	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

D 6.5 においては、各要因を識別と実行に分けてそれらの和を取るため、総和が大きくなる。そのため、各攻撃能力に割り当てられる値の範囲を変更して、是正している。こうした方法は、他の技術分野のサポート文書でも採用されている方法である。

D 6.5 では、攻撃能力計算の例がいくつか挙げられている。ここでは、本事業の参考になると考えられるふたつの例を挙げる。

［PAD 機能を持つ指紋製品への AVA_VAN.2 相当の攻撃］

次の条件を満たす攻撃を考える。

所要時間：攻撃のための適切な素材とそれをどのように提示するかが明確ではなく、試行錯誤が必要。攻撃識別に 1 ヶ月必要。TOE への攻撃は 1 日で実行する。

専門知識：公知の攻撃方法はあるが、攻撃には PAD 機能の概要を理解し、偽造物作成及び適用の検討が必要である。これは熟練者が実施する。熟練者が決定した攻撃を、しろうとが実行する。

TOE の知識：公開情報。PAD 機能の存在は宣伝などで知られている。PAD 機能の実現方法を攻撃者は推測できる。

機会: 中（個人は購入できず、購入には NDA が必要。TOE には何度でもアクセスできる）。

機器：標準機器だけを使う。

身体的特徴へのアクセス：指紋なので容易である。

成功率：攻撃は 60%成功する。

この場合は、攻撃能力計算の値は 12 になるので、AVA_VAN.2 相当の攻撃になる。

［高度な PAD 機能を持つ指紋製品への AVA_VAN.3 相当の攻撃］

次の条件を満たす攻撃を考える。

所要時間：攻撃のための適切な素材とそれをどのように提示するかが明確ではなく、試行錯誤が必要。攻撃識別に 1 ヶ月必要。TOE への攻撃は 1 日で実行する。

専門知識：公知の攻撃方法はなく、エキスパートが攻撃方法を新規に考案しなければならない。 攻撃は PAD 機能を理解した上で熟練者が実施する必要がある。

TOE の知識：TOE に関する制限的な情報が提供される。提供されないと、なりすましの成功は不可能である。

機会：難（提供先が限定されている。TOE には何度でもアクセスできる）。

機器：標準機器だけを使う。

身体的特徴へのアクセス：指紋なので容易である。

成功率：攻撃は 20%成功する。

この場合は、攻撃能力計算の値は 26 になり、AVA_VAN.3 相当の攻撃になる。

⑵素案作成

調査した FSDEG と D 6.5 のように、脆弱性評価サポート文書の含むべき内容は、ベンダーが作成し評価機関に提供する文書の記載内容に対する要件、評価機関における当該文書の評価方法、攻撃能力計算、及び攻撃能力計算例である。

評価のための文書への記載内容は、評価機関及び認証機関へ限定されるとはいえ、ベンダー技術の開示になるので、サポート文書の作成に当たってはベンダーが同意できる内容でなければならない。1 月にベンダー数社に対して、PAD 技術の評価のための文書への記載内容について、FSDEG の事例を示した上で、意見聴取を実施した。対象の文書は、セキュリティアーキテクチャ、機能仕様、TOE 設計とした。来年度のパイロット評価認証に向けてベンダーが準備を進めている文書なので、これらを意見聴取の対象にした。他文書については、別途意見聴取を実施する予定である。

意見聴取で提示した FSDEG の事例は、以下のとおりである。

セキュリティアーキテクチャ

バイパス防止の観点から、センサーからの指紋情報と PAD 情報が同一の生体から得られているとどのように判断できるかを記述しなければならない。

機能仕様

外部から TOE へ与えられる PAD に関する情報（体温、湿度、伝導性、血流、血流酸素濃度、光学濃度など）を記述しなければならない。

TOE 設計

外部から TOE へ与えられた PAD に関する情報を利用してどのように PAD をするか、及びその理論的背景を記述しなければならない。

意見聴取の結果をまとめると、以下のようになった。

セキュリティアーキテクチャ

バイパス防止の観点から、特徴抽出への入力と PAD 特徴抽出への入力が同一の生体から得られているとどのように判断するかを記述しなければならない。

機能仕様

外部から TOE へ与えられる PAD に関する情報（光学特性（反射/吸収、波長、照度）、画像特性、物理特性（温度、導電など））を記述しなければならない。

TOE 設計

外部から TOE へ与えられた PAD に関する情報を利用してどのように PAD をするか、及びその理論的背景を記述しなければならない。

サポート文書は公開文書になるので、攻撃者に対しての情報提供にならないように考慮すると、記載内容は粗いものになる。2 月に開催された検討委員会での記載レベルについての議論の結果、製品を分解などして容易にわかる情報については、評価機関での評価の効率化のために、文書に記載することが合意された。また、ベンダーによる製品のライフサイクル管理と記載内容の関係については、更に検討することになった。

攻撃能力計算及び攻撃能力計算例は、脆弱性評価における実際の攻撃内容の決定に大きく関わる内容である。D 6.5 における指紋の AVA_VAN.2 及び AVA_VAN.3 の攻撃例を基に、静脈の場合の身体的情報へのアクセスが困難であることを考慮した攻撃シナリオを、先ず検討した。12 月の検討委員会で案を提示し、2 月の検討委員会で合意した。12 月には 4 つのシナリオ案を検討したが、うち 2 つは 2 月の委員会で AVA_VAN.3 相当との結論になった。AVA_VAN.2 相当の攻撃シナリオ 2 つの内容は、本報告書には記載しない。それぞれのシナリオの要因は、以下のとおりである。

シナリオ 1

攻撃識別：

所要時間：1 ヶ月

専門知識：熟練者

TOE の知識：公開情報

機会：容易

機器：標準

攻撃実施：

所要時間：1 日

専門知識：しろうと

TOE の知識：不要

機会：容易

機器：標準

シナリオ 2

攻撃識別：

所要時間：1 ヶ月

専門知識：熟練者

TOE の知識：公開情報

機会：容易

機器：標準

攻撃実施：

所要時間：1 日

専門知識：しろうと

TOE の知識：不要

機会：容易

機器：標準

いずれのシナリオも、D 6.5 の攻撃能力計算に従えば、成功率が 60%であるとしても値の総和は 16 となり、AVA_VAN.2 相当である。以後の cPP 化や ISO/IEC 19989 への反映を考慮すると、D 6.5 に現れている BEAT プロジェクト成果との協調は重要である。現時点では、D 6.5 の攻撃能力計算の本事業への適用は問題ないと考えられる。

以後、来年度のパイロット評価認証に向けて、不足を補って、サポート文書原案を完成させる。

5.3　精度評価手法の研究

精度評価の手法として、評価機関が独立試験で使用できる共通的なツールに関する研究を行った。この活動は前年度作業の継続であり、今年度は前年度の開発成果物に対する機能追加を実施した。以下に、本活動内容について説明する。

5.3.1　精度評価ツールの概要

本ツールはバイオメトリック製品の精度評価を行うための標準的なツールとして開発するものである。主な特徴を以下に示す。

①用途：評価機関による独立試験

②評価の種類：

・FTE, FRR：シナリオ評価

・FAR：テクノロジ評価

③適用可能製品：SDK（ソフトウェア開発キット）

④対応インタフェース：BioAPI

⑤対応 OS：Windows

システム構成はクライアント／サーバ形式とし、サーバ上に登録や照合用の試験手順を示すスクリプトが格納され、これをバイオメトリック製品（TOE）がインストールされたクライアント側に転送したうえで、登録試験や照合試験を実行する。実行した結果生成された被験者のテンプレートや照合バイオメトリックデータ、および、試験結果などがサーバ上に記録され、評価機関により参照される。

本ツールを用いた試験の流れを図 5.3-1 に示す。

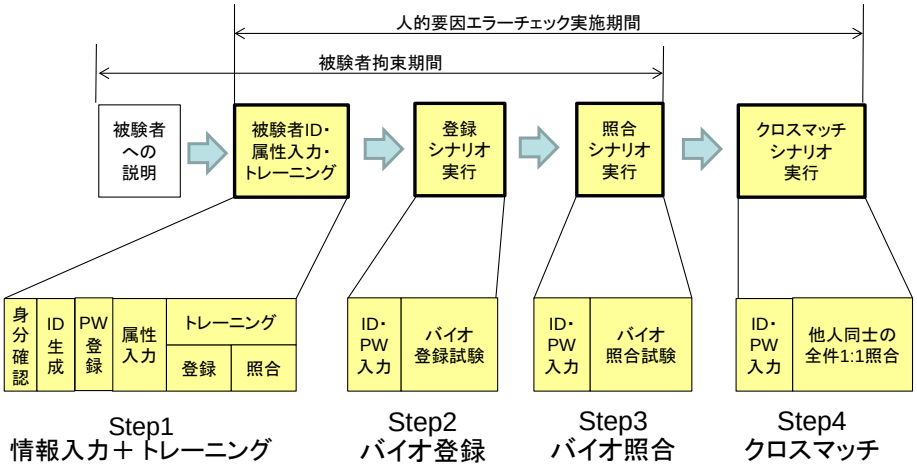


図 5.3-1 精度評価ツールを用いた試験の流れ

5.3.2　今年度の開発内容

前年度の事業では、精度評価の流れの中で、登録・本人トランザクション・偽者トランザクションを実行するための基本的な機能を開発した。今年度は、前年度の成果物に対する機能追加作業を実施した。この機能追加は、前述の 5.2.2 で示した精度評価のサポート文書素案の開発、および、有識者へのヒアリングにおいて精度評価ツールが持つべき機能として必要性が明らかになったものである。以下に追加機能の内容を説明する。

(1) BioAPI V1.1 対応

前年度の開発作業で対応した BioAPI のバージョンは V2.0 のみであった。有識者ヒアリングの中で BioAPI をインタフェースとしてサポートしているベンダーの SDK 製品には、BioAPI V2.0（ISO/IEC 規格）と BioAPI V1.1（ANSI 規格）の 2 種類が存在することが明らかになった。前年度の開発ではツールがサポートするインタフェースは BioAPI V2.0 のみだったが、V1.1 をサポートしている製品を考慮し、V1.1 へのサポート機能を追加した。

(2) ツールの柔軟性の向上

評価機関が独立試験として本ツールを使用する際に、試験官の操作の自由度や、様々な製品への対応が可能なようにツールの柔軟性の向上を行った。具体的な改善内容を以下に示す。

・トレーニングのタイミング

前年度に開発したツールは、登録や本人トランザクションを実行する際に実施する練習（登録トレーニング、照合トレーニング）は、本番の登録試験や本人トランザクション試験を実行する前にしかできないようになっていた。しかしながら、複数回実行される本人トランザクションを数週間など、ある程度の時間間隔を置いて実行するような評価方法を評価機関が選択した場合、被験者はそれらの複数回の照合トランザクションを実行する前に必ず照合トレーニングを行う必要性が生じる場合がある。精度評価を実施する際の環境などの制御要因のひとつに被験者の習熟度がある。対応製品が習熟度の高い被験者を想定している場合は、独立試験で募集した被験者に対して、本番の本人トランザクションを実行する前に十分な照合トレーニングを被験者が行うことにより習熟度が高い状態になっていることを試験官が確認する。このような試験手順に対応するため、被験者はいつでも登録や照合のトレーニングができるようにツールの機能を変更した。なお、被験者のトレーニングの実行は、管理者である評価機関の試験官の指示のもとで行うことが前提である。

・身体部分の順番

登録や照合に使用する身体部分が複数ある場合（例：左右の手、あるいは、手のそれぞれの指）、前年度に開発したツールの機能のでは、登録や照合の際に提示する身体部分の提示の順番をツールがあらかじめ決めていた。手順をツール側であらかじめ決めておくことは、試験官や被験者の負担を軽減し、人的要因ミスを低減することを意図したものであったが、実際

の独立試験においてはベンダーが希望する身体部分の提示順番はベンダー毎に異なる可能性があることがわかった。(指の場合、中指から始める場合や、人差し指から始める場合などが考えられる。) このため、ツールにより身体部分の提示順番の規定する機能を削除し、代わりにどの身体部分を提示するかを自由に変えられるように変更した。この機能を使用する前提として、評価機関の試験官が被験者に提示すべき身体部分を指示するとともに、試験官がどの身体部分が提示されたかをツールの画面操作で指定する方法に変更した。

・精度の実測値の出力内容

前年度に開発したツールでは、精度評価の評価尺度である FTE・FRR・FAR の実測値をツール内で計算し表示する機能があった。FTE・FRR・FAR は、分子をエラー数、分母を被験者数や実行されたトランザクション数として算出するが、実際の計算は製品や想定アプリケーション毎に異なる場合があり、単一な計算ができない場合があることが判明した。例えば登録失敗率を計算する場合、前年度の活動において行った定義では、分子は「登録に失敗した被験者数」であったが、今年度の活動ではこれを改め「登録ポリシーを満足できなかった被験者数」に変更した。登録ポリシーとはバイオメトリック製品あるいは想定アプリケーションによって定められる条件であり、例えばテンプレート生成が 2 つ以上の身体部分で成功しなければ登録成功としない、といったポリシーが挙げられる。このようなケースに対応するために、ツール内で FTE・FRR・FAR の算出をする機能を削除し、代わりに被験者毎の登録や本人トランザクションの実行結果、および、偽者トランザクションの実行結果を CSV 形式で出力する機能を開発した。評価機関は FTE・FRR・FAR の実測値を算出する際、この CSV ファイルを表計算ソフトなどで読み込み、評価対象製品の条件に沿った方法で算出できるようにした。

5.3.3 今後の予定

2017 年度に予定されているパイロット評価における評価機関による独立試験で使用されることを想定し、評価対象ベンダーが決定したのち、本ツールの適用が可能か否かを判断し、可能であった場合は評価対象ベンダー製品を本ツールに組み込むためのツールの変更作業を実施する。その後、独立試験で評価機関が使用する。

5.4 脆弱性評価手法の研究

本章は、攻撃者に対して有益な情報を与える可能性があるので、関係者限りの別文書に記述する。

5.5　パイロット評価・認証に向けた準備

来年度のパイロット評価・認証を実施するためには、評価・認証される側とする側それぞれの準備が必要である。今年度はその準備の年度とし、それぞれ準備を進めた。評価・認証される側はベンダーであり、準備の主な内容は CC 評価のための文書の準備である。来年度のパイロット評価・認証を希望するベンダーには CC 評価のための文書を作成していただいた。評価・認証する側は評価機関及び認証機関であり、実際の評価及び認証をどのように進めるかを決定する必要がある。バイオメトリクス製品の CC 評価・認証に関心を持つ評価機関と IPA に協力いただき、評価方法の検討を進めた。

5.5.1　ベンダーにおける CC 評価のための文書の準備

CC 評価・認証の流れは、以下の図 5.5-1 のとおりである。

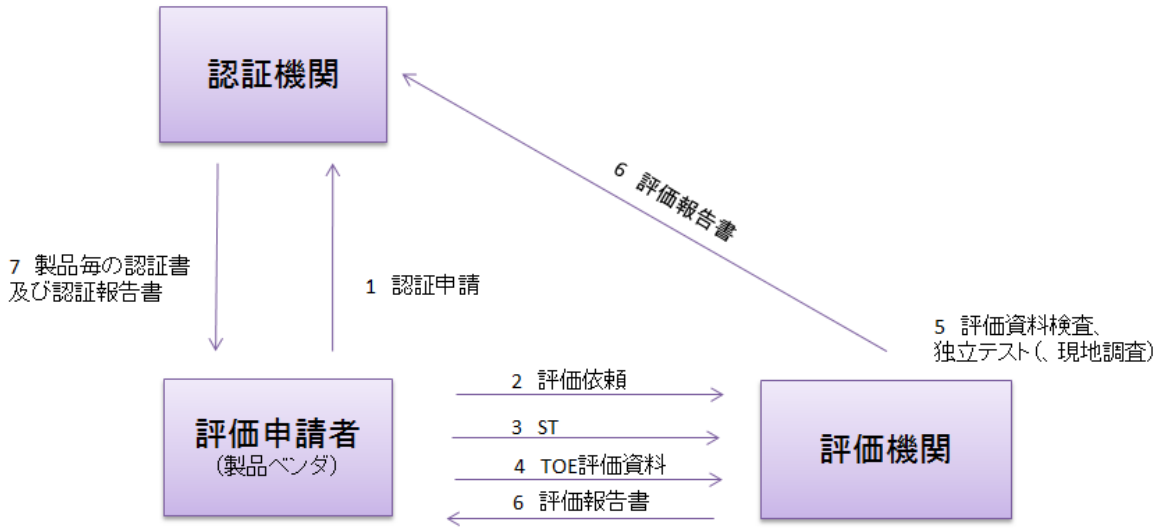


図 5.5-1　CC 評価・認証の流れ

ベンダーが先ず用意すべき CC 評価のための文書は、セキュリティ設計仕様書である ST（Security Target）である（図中の 3）。評価機関での ST の評価が終了すると、ベンダーは TOE 評価資料（図中の４）を評価機関に提出し、評価機関はそれらを評価する。本事業で作成した PP が求める TOE 評価資料は、機能仕様、TOE 設計、セキュリティアーキテクチャ記述、テスト証拠資料、テストカバレージ証拠、構成管理証拠資料、構成リスト、開発者の配付手続きの記述、配付証拠資料、ガイダンス証拠資料（利用者準備ガイダンス）、ガイダンス証拠資料（利用者操作ガイダンス）、欠陥修正手続き証拠資料である。来年度のパイロット評価・認証開始は 2016 年 7 月の予定なので、それまでにパイロット評価・認証を受けるベンダーはこれらの文書を準備する必要がある。ベンダーにおける文書作成は、パイロット評価・認証への準備の他に、本事業で作成した PP が各ベンダーの製品に適用できるかを検証する目的もあった。

今年度の開始時点では、来年度のパイロット評価・認証への参加意思を示したベンダーは 5 社あっ

た。各社にCC評価のための文書準備のスケジュールを提示した結果、1社はスケジュールが合わず、4社が文書の準備を開始した。ベンダー各社は文書の体系をIPAホームページにある資料で理解し、その後、機能仕様、TOE設計、セキュリティアーキテクチャ、STの順に、今年度は作成した。STは本来はじめに作成すべきものであるが、PPを並行して作成したため、各社には昨年度作成した認証PPを念頭においてST以外の文書を先行して作成してもらうことにした。今年度作成のPPが完成した時点でSTを作成し、他の文書に変更の必要が生じた場合は対応することにした。文書を作成する各社と産総研はNDAを締結した上で、各社が作成した文書を産総研に提供し、CEMに基づいて産総研が確認しフィードバックするという作業を繰り返した。最終的に3社が上記の4文書作成を完了した。

ベンダーの文書作成の過程で、いくつかの点で、作成したPPが各社製品へ適用できないことがわかった。昨年度作成した認証PPでは登録生体情報取得機能をTOEが含んでいたが、いくつかのベンダーの製品はこの機能を含んでいないことがわかった。また、管理者認証機能、設定機能についても、製品によっては機能を持たないことがわかった。これらは今年度作成したPPに反映され、各社の製品のST作成にPPが容易に適用できるように選択的なセキュリティ機能要件をPPの付録（最終的にはPP本体から削除）として作成した。

(1)CC評価のための文書体系理解

IPAホームページにある以下の資料を活用して、各社に文書体系を理解していただいた。

全体理解のために、「CC評価を理解するための開発者向け説明会」
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_eval_20120625.pdf

セキュリティアーキテクチャの理解のために、「CC評価のセキュリティアーキテクチャ」
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_eval_20140708.pdf

セキュリティアーキテクチャの概説書として、「開発者のためのセキュリティ解説書（セキュリティアーキテクチャ編）」
http://www.ipa.go.jp/security/jisec/apdx/documents/SecurityArchitectureGuide.pdf

文書体系全体の理解のために、以下のページの「CC評価証拠資料作成講座」の各資料
https://www.ipa.go.jp/security/jisec/seminar/apdx.html

CC評価のための文書のサンプルとして、以下のページの「開発証拠資料サンプル」
http://www.ipa.go.jp/security/jisec/apdx.html#ADV_ARC_GUIDE

STについて、以下のページの「ST作成に関する説明会」資料

http://www.ipa.go.jp/security/jisec/seminar/apdx.html

関連資料として、開発者のためのセキュリティ解説書（ガイダンス編）
http://www.ipa.go.jp/security/jisec/apdx/documents/SecureGuide.pdf

関連資料として、開発者のためのセキュリティ解説書（脆弱性評価編）
http://www.ipa.go.jp/security/jisec/apdx/documents/VulnerabilityAssessmentGuide.pdf

CC の概要理解のために、「CC 基礎講座」資料
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_20060222.pdf

文書作成に当たっては、上記の「開発証拠資料サンプル」を参考にするよう各社に依頼した。

(2)機能仕様

機能仕様は、TOE のインタフェース仕様書に相当する。各社とも、2 サイクルのレビューを経て、今年度の最終版を作成した。レビューの過程で見つかった問題点や指摘事項は、以下のとおりである。

BioAPI 用語や製品固有の用語等、一般的でない用語が使われていた。これらについては、第三者にもわかるような記述にするよう要求した。

SFR 実施アクションに関連する誤りメッセージは、セキュリティに関するもの以外も記述にするよう要求した。

ST（PP）の用語とのずれがあるものについては、対照表を作るよう要求した。

API の呼出しと返り値を別の TSFI と扱っている例があったので、ひとつの TSFI の入力と出力として記述するように要求した。

TSFI として TOE から運用環境へのアクセスを記述したものがあったが、TSFI に該当しないので不要であることを指摘した。

TSFI の使用方法のうち、入力パラメータの意味説明に不足があるものが多かった。

実施する SFR の記載があるのに、アクション記述にそのように読み取れる記載がないものがあった。

(3)TOE 設計

TOE 設計は、サブシステムレベルの設計書である。各社とも、1 サイクルまたは 2 サイクルのレビューを経て、今年度の最終版を作成した。レビューの過程で見つかった問題点や指摘事項は、以下のとおりである。

SFR 実施のサブシステムの記述で、PAD 機能や検査機能の記述が十分でないものがあった。

ふたつのコンポーネント間でそれぞれのサブシステムと連動する場合に、一方のコンポーネ

ントのサブシステムだけの記述をしている例があった。相互作用の記述も含め、両コンポーネントの記述を求めた。

TSFI とサブシステムのマッピングに TSFI でない API が含まれているものがあった。

(4)セキュリティアーキテクチャ

セキュリティアーキテクチャは、CC 特有の文書であり、TOE のセキュリティ機能が改ざんやバイパスされないように設計実装されていることを記述する文書である。各社とも、1 サイクルのレビューを経て、今年度の最終版を作成した。レビューの過程で見つかった問題点や指摘事項は、以下のとおりである。

TOE 設計と同等の詳細レベルで記述するよう依頼した。

セキュリティドメインに対する誤解が多かった。セキュリティドメインがない場合は、セキュリティドメインが不要であることを、または、TOE に対する入力が限定的であって TOE に有害でないことを、それぞれ主張するよう求めた。

初期化プロセスのセキュリティについては、製品初期設定を記述しているものが多かった。

バイパス防止については、TOE に対する入力のパスを具体的に列挙し、それらがバイパスできないことを論証するよう求めた。

(5)ST

ST 作成に当たっては、1 月 11 日時点での PP を基に各社の TOE の機能に合わせて、産総研から ST のたたき台を提供して、各社がたたき台に加筆して ST を完成した。加筆部分は、ST 概説の TOE 記述と ST の最後の部分である TOE 要約仕様である。レビューの過程で見つかった問題点や指摘事項は、以下のとおりである。

TOE 記述では TOE の物理的範囲及び論理的範囲を記述する必要があるが、一部のベンダーの ST では、両者が明確に記述されていないものがあった。

TOE 要約仕様には TOE がどのようにセキュリティ機能要件を満たすかを記述しなければならないが、一部のベンダーの ST では、十分な説明がなされていないものがあった。

各社から提出された ST を 1 回レビューし、レビュー結果を反映して今年度の ST 最終版とした。なお、PP は評価認証の過程で修正が必要になったため、ST は各社とも一部修正が必要である

5.5.2 評価機関・認証機関との評価方法の検討

来年度のパイロット評価・認証においてバイオメトリック製品の評価を実施するためには、CC 評価の仕組みに従った精度評価及び脆弱性評価の評価方法の確立が必要である。本節では、これらの評価方法確立に向けて、評価機関・認証機関と行った評価方法の検討結果を示す。

精度評価を担当する OKI ソフトウェアと評価機関・認証機関の間で行った活動として、精度評価のためのサポート文書案開発に関する検討結果について説明する。

① 概要

今年度の成果物として、精度評価サポート文書における社内試験エビデンス素案、および、独立試験方法素案の 2 つの文書の作成を完了した。

両文書の作成にあたり、評価機関・認証機関と OKI ソフトウェアとの間で 2015 年 7 月から 2016 年 3 月まで、7 回にわたって会議が開催され、サポート文書の全体構成、活動の推進方法、推進の途中段階における状況確認、両素案の各記述項目など、様々な意見交換が行われた。検討の詳細を以下に示す。

② 詳細

以下に精度評価の評価方法に関する評価機関・認証機関との検討結果の詳細について、時間的経緯とともに説明する。

・2015 年 7 月：評価方法確立のための活動方針として、精度評価のサポート文書案の作成方針ついて検討を実施した。本検討で、サポート文書の構成をベンダーによる社内試験エビデンスと評価機関による独立試験の 2 つとすることが決定した。また、社内試験エビデンスは精度評価のための国際標準規格である ISO/IEC 19795-1 及び ISO/IEC 19795-2 の記述内容に基づいて作成することになった。

・2015 年 9 月：社内試験エビデンスの項目を作成するための準備作業として、ISO/IEC 19795-1 及び ISO/IEC 19795-2 から抽出した項目表を OKI ソフトウェアが作成し、評価機関・認証機関とその内容について検討した。項目の中に社内試験として実施することが必ずしも容易ではないものが存在することが見込まれたことから、ベンダー各社に対して社内試験エビデンスの作成難易度に関する意見聴取を行うことが決定した。

・2015 年 10 月：社内試験エビデンス項目の作成難易度に関するベンダーへのアンケート調査案について、OKI ソフトウェアと評価機関・認証機関との間で検討を行い、アンケート調査表の各項目およびアンケート調査の形式を決定した。

・2015 年 11 月前半：ベンダー各社へのアンケート調査及び各社からの回答集計を OKI ソフトウェアが実施した上で、ベンダーから難易度が高いとの回答があった項目について評価機関・認証機関と意見交換を行った。その結果、難易度が高い項目についてはサポート文書における対応方法案を OKI ソフトウェアが別途検討するとともに、検討した結果を精度評価の国際標準規格の有識者から意見を頂き、最終案としてまとめることが決定した。

・2015 年 11 月後半：社内試験エビデンスとして難易度が高い項目に対する対応方法について、OKI ソフトウェアが精度評価の国際標準規格の有識者やベンダーとの間で意見交換を実施した。意見交換の結果に基づき、OKI ソフトウェアが社内試験エビデンス項目案として文書にまとめ、認証機関・認証機関との間で意見交換を行った。その結果、精度評価のサポート文書素案において、社内試験エビデ

ンスとして記載すべき項目が決定した。

・2016 年 1 月 : 評価機関による独立試験方法に関する検討資料を OKI ソフトウェアが作成し、評価機関・認証機関と意見交換を行った。評価機関・認証機関より、独立試験実施の際に多数の被験者を募集することについて、コスト増加などの懸念が示された。協議の結果、独立試験方法の検討においては多くの被験者募集を前提としない方針が決定した。また、方針案の検討においては、ベンダーおよび有識者と OKI ソフトウェアの間で意見交換を行うことが決定した。

・2016 年 3 月 : 独立試験方法確立のためにベンダーおよび精度評価の有識者との間で行った意見交換結果に基づいた独立試験方法を OKI ソフトウェアが作成した。その内容について評価機関・認証機関と意見交換を行い、精度評価のサポート文書における独立試験方法素案とすることが決定した。また、2017 年度における独立試験方法に関する検討方針として、統計的な手法の適用を含めて検討を推進すること決定した。

5.6 国際標準化活動

バイオメトリクスの国際標準化は ISO/IEC JTC 1/SC 37 で実施している。偽造生体などの提示型攻撃（presentation attack）の検知に関する国際標準化も 3 パートから成る ISO/IEC 30107 Biometric presentation attack detection シリーズとして SC 37 での活動がある。しかし、本事業の対象とする CC 評価認証の国際標準化は SC 27 で ISO/IEC 15408 として実施しており、提示型攻撃検知の CC 評価認証は SC 27 の ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics で国際標準化が進められている。精度評価を CC 評価認証でどう扱うかについても、SC 27 でスタディピリオドが開始された。

5.6.1 SC 27 での国際標準化

現在の SC 27 の活動の中で本事業と関連するのは、WG 3 における ISO/IEC 19989 と CC に基づく精度評価のスタディピリオドのふたつである。

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

本プロジェクトは、バイオメトリクスの偽造生体などの提示型攻撃の検知のセキュリティ評価を ISO/IEC 15408 の枠組みで実施可能とするためのセキュリティ要件及び評価方法の作成を目指しており、2014 年 10 月のメキシコ会議で産総研がエディタに就任した。

今年度の SC 27 国際会議は、5 月にマレーシアのクチンで、10 月にインドのジャイプールで開催された。クチン会議では WD 1 に対する審議、ジャイプール会議では WD 2 に対する審議が実施された。本成果報告書の作成時点では、WD 3 に対するコメント募集中である。

クチン会議では、5 月 5 日に 2 時間、5 月 6 日に 2 時間の審議を実施した。出席者は、ドイツ１、フランス２、日本２、韓国２、英国１、米国２だった。提出されたコメントは、ドイツ 4 件(ge1,te1)、フランス 9 件(ge5)、英国 53 件(ge10,te15)、日本 5 件（te4。うち 2 件はエディタから）、米国 10 件(te7)だった。コメント処理結果は最終的に参加者全員が満足するものとなったが、エディタが提出した 2 件のコメントは、参加者の賛成が得られず、却下せざるを得なかった。当該コメントは提示型攻撃検知以外の FAR 及び FRR を含む機能要件追加の内容であり、昨年度作成した認証 PP の内容へのスコープ拡張を狙ったものだった。エディタはスコープ拡張を求めたが、参加者の賛成は得られなかった。WD1 は、本プロジェクト開始前のドイツからの寄書から採用した記述が多かった。ドイツ寄書にあった攻撃に関する記述を WD1 からは削除したが、復活させるよう日本のエキスパートからコメントがあり、accept した。次のステージは、WD 2 と結論された。提出期限は 7 月 15 日、コメント提出期限は 9 月 30 日となった。

WD2 は、予定どおり 7 月 15 日に提出した。WD1 からの主な変更内容は、Annex に保証要件クラス ATE に関する記述を新たに設けたこと、上記の日本エキスパートのコメントを反映して Annex 中の保証要件クラス AVA の記述を補強したことである。

ジャイプール会議では、10 月 28 日に 4 時間、10 月 29 日に 2 時間の審議を実施した。出席者

は、ドイツ１、フランス１、インド２、日本２、韓国２、英国１だった。WD2 へのコメント提出はフランス 39 件(ge14，te7)、日本 5 件(ge3，te1)、イギリス 83 件(ge12，te24)だった。コメント処理はコメント提出の専門家の合意が得られた。イギリスからのコメントは、瑣末なコメントや現実から乖離したコメントもあったが、本質に迫るコメントも多く、本プロジェクトの品質向上に貢献した。論点の中心は、ATE と AVA がどのように分担して PAD のセキュリティを保証するかである。EU の BEAT（Biometric Evaluation And Testing）プロジェクトの寄書がドイツ及びフランスからあり、AVA における攻撃能力の計算をこの寄書を基に見直すことになった。また、上記寄書には精度評価に関する内容も含んでいたため、後述のスタディピリオドを開始することが WG 3 で決議された。国民 ID に指紋を採用している開催国インドが参加し、本プロジェクトに積極参加の姿勢を見せた。本プロジェクトの意味をより大きなものにすることが期待される。各国からのコメント・寄書がまだ多いので、次の段階は WD3 となった。提出期限は 12 月 15 日、コメント提出期限は 3 月 15 日となった。

WD3 は、予定から 10 日遅れ、12 月 25 日に提出した。BEAT プロジェクトの成果を反映することをジャイプール会議では結論したが、本事業での検証ができていないため、次のドラフトに持ち越すことにした。以下は、WD3 の目次である。

(2)SP on Security evaluation of biometric performance based on ISO/IEC 15408 and 18045

ISO/IEC 19989 は提示型攻撃検知のセキュリティ評価を対象にしているが、上記のとおり、フランス及びドイツからの寄書は、精度評価の CC 評価に関する内容も含んでいた。フランスのエキスパートから BEAT プロジェクトの成果に関するプレゼンテーションがあり、日本からの提案で SP（Study Period）を開始することが決定した。ISO/IEC 19989 のエディタとしては、クチン会議でのスコープ拡張に失敗したが、BEAT プロジェクトの寄書を根拠に再度スコープ拡張を提案することも可能だったかも知れない。スコープ拡張することは、本事業が目指すバイオメトリクス固有のセキュリティ評価をひとつの国際標準の中で扱えることになり、また本事業の成果とも対応するので、望ましい形である。しかし、スコープ拡張によって、ISO/IEC 19989 が混乱する可能性も考慮して、先ず SP から開始することを ISO/IEC 19989 エディタとして提案した。本 SP のラポータは日本が務め、コラポータは ISO/IEC 19989 のコエディタ（フランス）が務める。本 SP の寄書提出期限は 3 月 31 日に設定された。

本 SP に対しては、本事業の精度評価のサポート文書を寄書する予定である。

5.6.2 SC 37 での国際標準化

SC 37 での本事業に関わる国際標準化プロジェクトは、WG 3（パート 3 は WG 5 と共同）で開発している ISO/IEC 30107 Biometric presentation attack detection と WG 5 で開発が完了している ISO/IEC 19795 シリーズがある。

(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）

パート 1 は IS として 2016 年 1 月に発行された。パート 2 及びパート 3 は、現在 CD 段階にある。本事業に深く関わるのはパート 3 であり、パート 3 には今まで本事業からも多数のコメントを提出して来た。ISO/IEC 30107-3 と ISO/IEC 19989 との分担をどうするかの議論は今までなされて来なかった。1 月のマルティニー会議で、ISO/IEC 19989 エディタから ISO/IEC 19989 の状況を説明した。その結果、CC アプローチについては ISO/IEC 19989 が担当することが結論された。

(2) ISO/IEC 19795 Biometric performance testing and reporting

精度評価に関する提案活動については第 1 回委員会で新しい評価尺度を審議にかけたが、提示した概念は現行規格で言及済みとの指摘を受け、新規提案化の合意に至らなかった。また、現在までの精度評価手法の研究内容からは、ISO/IEC 19795 シリーズへの新規提案が必要な内容は見出していない。本事業における精度評価の成果は、SC 27 のスタディピリオドへの寄書提出することで国際標準に反映させる。

6. 平成２７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、平成 26 年度に活動をはじめ、平成 27 年度は、下記に取り組んだ。

・認証機関・評価機関・ベンダー及び有識者からなる検討委員会の組織
・国際連携活動
・セキュリティ評価手法の研究
- 追加 PP 開発とサポート文書全体構成案の作成
- 精度評価手法の研究
- 脆弱性評価手法の研究
- パイロット評価・認証に向けた準備
- 国際標準化活動

それぞれの活動成果は下記である。

(1) 委員会活動

認証機関(IPA 2 名)・評価機関(みずほ情報総研 2 名)・ベンダー(7 社 7 名)・有識者(3 団体 3 名)・官公庁(2 名)・実施者（2 団体 5 名）および事務局(１名)から成る検討委員会(22 名)を組織した。4 回の委員会を開催し、事業の実施検討方針、検討内容や今後の方向性について、専門的、具体的な検討を行い、事業の検討にフィードバックした。

(2) 国際連携活動

(a) PP 及び CC 評価・認証

本事業で作成の PP によりバイオメトリクス製品が CC 評価・認証される基準を世界統一基準とするためには、本事業で作成の PP を CCRA(*1)で cPP（*2）にする必要がある。IPA と協力し、今年度 9 月に CCRA へ cPP 化提案が完了した。

*1) CC Recognition Arrangement：CC を制定する各国の CC 認証機関からなる国際組織。日本は IPA が参加。CCRA は SC 27 と連携し、SC 27 が CC を ISO/IEC 国際標準化。

*2) collaborative PP：中立機関(CCRA)によって開発・保守され、ＣＣ評価認証制度を持つ世界 25 ヶ国で共通の調達基準となる PP（CC に基づくセキュリティ要件定義書）

(b) 精度評価

欧州におけるバイオメトリクスの評価と試験を研究する活動である BEAT（Biometric Evaluation And Testing）の文献調査を前年度に引き続いて実施した。BEAT は本事業で用い

る評価尺度と異なる性能指標を提案しており、評価方法についても大きく異なっている。前年度のヒアリングで日欧の連携に消極的だったこととあわせて、現時点では単独での実施が妥当と判断しているが、引き続き動向はウォッチし、連携の可能性を探った。今後の欧州の精度評価に関するプロジェクトへの本概念の採用や、国際標準化活動において欧州から本概念に関する標準化提案が行われる可能性もあるため、国際連携活動の推進において本概念に関する欧州の動きがないか今後注視する必要がある。

後述の精度評価のサポート文書素案を英訳して、上記の cPP 化のサポート文書のドラフトとして活用し、成果の国際活用を図る。

(3) 追加ＰＰ開発とサポート文書全体構成案の作成

(a) 追加 PP 開発

当初は登録だけの PP を作成する予定だったが、登録だけだとセキュリティ機能要件が作成できないことがわかった。その結果、昨年度作成した認証と合わせた PP にすることとし、より多くの製品に適用可能にするために認証から照合に変更して、登録と照合を対象とする PP を作成し完成させた。1 月 26 日に PP 評価に合格した。PP 認証は 2016 年 3 月末の予定である。

(b) 精度評価サポート文書素案の開発

静脈認証バイオメトリック製品に対する CC 評価の適用に向けて、バイオメトリック製品のセキュリティに関わる性能指標である誤受入率（FAR)、誤拒否率（FRR)、及び、登録失敗率（FTE）を評価するための精度評価に関するサポート文書素案を作成した。本素案は、静脈認証バイオメトリック製品の精度評価を CC 評価に適用するにあたり、静脈認証バイオメトリック製品に特有な必要事項をガイダンス文書としてまとめたものである。本素案では、ベンダーが静脈認証製品の精度評価を社内試験として実施した結果を評価機関に提示する際のエビデンス、及び、評価機関の社内試験エビデンスの適正さを確認するために実施する独立試験方法を記載した。精度評価サポート文書は 2017 年度に完成予定である。

(c) 脆弱性評価サポート文書素案の開発

脆弱性評価サポート文書は、精度評価サポート文書とは異なり、前例として、ドイツで作成さされたものと EU の BEAT（Biometric Evaluation And Testing）プロジェクトで作成されたものが 1 件ずつある。これらはいずれも指紋を対象にしたものであるが、両方を調査し、それらの調査結果を考慮して素案を作成した。素案作成には、ベンダー各社に意見を求め、意見をまとめた結果を検討委員会で審議した。評価のための文書に対する要件及び攻撃シナリオについて、サポート文書の骨格を作成した。攻撃シナリオ検討の結果、BEAT プロジェクトの成果と協調できる見通しである。脆弱性評価サポート文書はまだ素案の段階であり、来年度のパイロット評価認証開始までに原案を完成させ、パイロット評価認証で検証して完成させる。

(4) 精度評価手法の研究

評価機関が行う独立試験のために用いる精度評価ツールの開発を前年度から継続し取り組んだ。本ツールはバイオメトリック製品の精度評価を行うための標準的なツールとして開発するものである。ツールの主な特徴を以下に示す。

①用途：評価機関による独立試験

②評価の種類：

・FTE, FRR：シナリオ評価

・FAR：テクノロジ評価

③適用可能製品：SDK（ソフトウェア開発キット）

④対応インタフェース：BioAPI

⑤対応 OS：Windows

今年度は主に以下の 2 つの開発作業を実施した。

・BioAPI V1.1 対応：評価対象製品である静脈認証 SDK（ソフトウェア開発キット）がサポートするインタフェースの条件が、前年度は BioAPI V2.0 だったが、これに BioAPI V1.1 を追加した。

・ツールの柔軟性の向上：被験者の習熟度を上げるために試験官が被験者に対して行うトレーニングのタイミングの自由度を向上すること、複数の身体部分が存在する場合（左右の手、手のそれぞれの指など）の身体部分の順番の自由度を上げること、及び、ツールが生成する精度評価結果の実測値の出力内容を独立試験がしやすくなるよう柔軟性を向上させることの 3 つの対応を行った。

(5) 脆弱性評価手法の研究

偽造物作成のための装置を購入し、静脈の偽造物作成の研究を進めた。評価・認証に使用するための偽造物の品質について検討し、第 2 回委員会で議論した。今後、信頼できる安全性評価に向けた偽造物のバリエーションを検討すると共に、来年度の評価に使用する偽造物のセットを提案し、委員会の合意を得る予定である。

(6) パイロット評価・認証に向けた準備

来年度のパイロット評価・認証を実施するためには、評価・認証される側とする側それぞれの準備が必要である。評価・認証される側のベンダーと評価・認証する側の評価機関及び認証機関で、それぞれの準備を進めた。

ベンダーにおける CC 評価のための文書の準備として、来年度のパイロット評価・認証への参加意思を示したベンダーに、来年度の準備と本事業で作成した PP の検証のふたつを目的に、設計関連の文書である、機能仕様、TOE 設計、セキュリティアーキテクチャ、ST を作成してもらった。文書を作成する各社と産総研は NDA を締結した上で、各社が作成した文書を産総研に提供し、CEM に基づいて産総研が確認しフィードバックするという作業を繰り返した。最終的に 3

社が上記の 4 文書作成を完了した。

ベンダーの文書作成の過程で、いくつかの点で、作成した PP が各社製品へ適用できないことがわかり、PP 作成にフィードバックした。

また、評価機関・認証機関との評価方法の検討として、精度評価を担当する OKI ソフトウェアと評価機関・認証機関の間で精度評価のためのサポート文書案開発に関する検討を行い、今年度の成果物として精度評価のサポート文書における社内試験エビデンス素案、および、独立試験方法素案の 2 つの文書の作成を完了した。

両文書の作成にあたり、評価機関・認証機関と OKI ソフトウェアとの間で 2015 年 7 月から 2016 年 3 月まで、7 回にわたって会議が開催され、サポート文書の全体構成、活動の推進方法、推進の途中段階における状況確認、両素案の各記述項目など、様々な意見交換を行った。

(7) 国際標準化活動

本事業の対象とする CC 評価認証の国際標準化は SC 27 で ISO/IEC 15408 として実施しており、提示型攻撃検知の CC 評価認証は SC 27 の ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics で国際標準化が進められている。精度評価を CC 評価認証でどう扱うかについても、SC 27 でスタディピリオドが開始された。

また、バイオメトリクスの国際標準化は ISO/IEC JTC 1/SC 37 で実施している。偽造生体などの提示型攻撃（presentation attack）の検知に関する国際標準化も 3 パートから成る ISO/IEC 30107 Biometric presentation attack detection シリーズとして SC 37 での活動がある。

今年度の SC 27 国際会議は、5 月にマレーシアのクチンで、10 月にインドのジャイプールで開催され、ISO/IEC 19989 については、各国からのコメント・寄書がまだ多く、WD 段階に留まっている。本事業の活動で、エディタとして WD2 及び WD3 を作成し、国際会議での審議を取りまとめた。WD2 に対しては、EU の BEAT（Biometric Evaluation And Testing）プロジェクトの寄書がドイツ及びフランスから提出された。この寄書には精度評価に関する内容も含んでいたため、スタディピリオド Security evaluation of biometric performance based on ISO/IEC 15408 and 18045 を開始することが WG 3 で決議された。本スタディピリオドのラポータも本事業の活動として実施する。

SC 37 での本事業に関わる国際標準化プロジェクトは、WG 3（パート 3 は WG 5 と共同）で開発している ISO/IEC 30107 Biometric presentation attack detection と WG 5 で開発が完了している ISO/IEC 19795 シリーズがある。ISO/IEC 30107-3 と ISO/IEC 19989 との分担をどうするかの議論は今までなされて来なかったが、SC 37 の 1 月のマルティニー会議で、ISO/IEC 19989 エディタから ISO/IEC 19989 の状況を説明し、CC アプローチについては ISO/IEC 19989 が担当することが結論された。また、本事業における精度評価の成果を ISO/IEC 19795 シリーズに反映させることを検討していたが、SC 27 のスタディピリオドへの寄書提出することで国際標準に反映させることとした。

7. 平成２８年度活動に向けて

平成２８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、セキュリティの観点から見た客観的な評価を可能にするために、セキュリティ評価基準に則って PP（Protection Profile）及び PP に付随する精度評価手法および脆弱性評価手法を作成し確立すること、ならび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ことに引き続き取り組む。

その場合、ＰＰ及びＰＰに付随する評価手法の成果は、国際標準化原案として、標準化機関である ISO/IEC JTC 1/SC 27 に提案することや、国際標準化の活動にあたっては、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、協力する。

特に平成 28 年度は、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の下、開発した PP を基に製品の ST（Security Target、セキュリティ機能仕様書）及びエビデンス文書を作成して、バイオメトリクス製品に対するパイロット評価・認証を認証機関・評価機関の協力のもとに実施したいと考えている。

また、本事業の過程で、本事業に関係する認証機関・国内評価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・手順を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評価及び認証を実施可能としたいと考えている。

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 認証取得可能としたいと考えている。

以上の取り組みのため、平成 28 年度も活動が継続できる場合は、バイオメトリクス製品の CC 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、以下の手順で研究を実施したいと考えている。

(1) 委員会活動

認証機関・国内評価機関・ベンダー・有識者 ・官公庁および事務局から成る検討委員会を組織し、委員会にて、事業の実施に関係する事項について、検討方針、検討内容や今後の方向性について、専門的、具体的な検討を行い、事業にフィードバックする。

(2) 国際連携活動

(a) cPP 化活動

本事業の成果であるバイオメトリクス製品の PP 及び評価方法論を反映した CC 評価・認証の国際的普及のために、IPA の協力の下、国内関係者の意見を参考にしながら、cPP 化の活動を本格化させる。cPP 化の活動には、本事業の成果である精度評価及び脆弱性評価のサポート文書をｃＰＰのサポート文書にする活動を含む。国内各社の議論への参加の内諾はいただいているが、海外については、現時点で活動に参加表明しているスペイン・トルコ・オーストラリアの他、潜在的要求があるアメリカ・ドイツ・フランス・インドなどを取り込んで、より大きな活動にしていく。この際、バイオメトリクス製品ＰＰを既に開発し CC 評価・認証を実施しているドイツ及びフランスを主たる連携候補として活動する。

(3) セキュリティ評価手法の研究

(a) サポート文書の検証

平成 27 年度に作成した精度評価並びに脆弱性評価に関わるサポート文書素案を、CC のパイロット評価・認証に活用することで、検証する。不足があれば補って、その結果を cPP 活動に反映させる。認証機関である IPA と協力し、また国内評価機関とも情報共有して、検証を進める。

(b) 精度評価手法の研究

平成 28 年度後半の独立評価で使用できるよう、精度評価ツールのプロトタイプを年度前半に完成させる。

平成 27 年度に作成した精度評価に関わるサポート文書素案は、ベンダーや評価機関による CC 評価の実施状況を確認し、修正の必要性があると判断された場合は適宜修正しサポート文書を完成させる。

(c) 脆弱性評価手法の研究

平成 28 年度にパイロット評価・認証に向けて、平成 27 年度までに検討した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・攻撃方法を研究する。この際、本年度に実施する評価・認証のため、国内企業の製品を使って評価を試行する。

また、より信頼性の高い脆弱性評価に資する活動として、偽造物のバリエーションの中で緊急性の高い偽造物を選択して試作し、脆弱性評価ツールセットの更新も働きかける。

また、平成 27 年度に作成した脆弱性評価に関わるサポート文書素案は、認証機関である IPA と連携して、ベンダーや評価機関による CC 評価の実施状況を確認し、修正の必要性があると判断された場合は適宜修正しサポート文書を完成させる。

更に、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。

(d) パイロット評価・認証

平成 28 年度のパイロット評価・認証に向けて、平成 27 年度に準備を進めた企業の製品から対象製品を選定し、IPA と国内評価機関と協力し、パイロット評価・認証を実施する。

これにより、本事業で検討した CC 認証に沿ったバイオメトリクス製品のセキュリティ評価・認証基盤の妥当性と改善点の確認を行う。

(e) 国際標準化活動

作成した PP の内容を SC 27 の ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics のプロジェクトへ反映させると共に、ISO/IEC 19989 を CD 段階へ進めることを目指す。精度に関する CC 評価については、スタディピリオドからプロジェクトへの移行を目標とする。ただし、ISO/IEC 19989 のスコープを拡張して、精度も含めた、バイオメトリクスの CC 評価全体を扱える規格にすることも検討する。

また、ISO／IEC 30107 Part3 は、CD 文書の品質向上に引き続き取り組む。

付録１　バイオメトリック照合製品プロテクション
プロファイル

バイオメトリック照合製品プロテクションプロファイル

1.1 版
2016/03/14
国立研究開発法人　産業技術総合研究所

目次

1. PP 概説

1.1. PP 参照

タイトル: バイオメトリック照合製品プロテクションプロファイル
版数 1.1
発行
発行者 国立研究開発法人　産業技術総合研究所
登録
認証番号
CC のバージョン 3.1 リリース 4
キーワード 認証、バイオメトリクス、バイオメトリック照合、顔照合、 指紋認証、虹彩認証、静脈認証、プロテクションプロファイル

1.2. PP 概要

本 PP は、CC の観点から、バイオメトリック照合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。バイオメトリック照合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 などによる利用者認証製品にはない、誤受入及び誤拒否のエラーに対する要件、偽造生体検知に対する要件等である。従って、本 PP においては、誤受入及び偽造生体検知に関係しない脅威は、取り扱わない。
本 PP は、TOE が使用する身体的特徴（顔、指紋、虹彩、静脈など）と対応する身体部分（静脈の場合は、指、てのひら、手の甲など）を特定しない。

本 PP は、バイオメトリック照合及びそのための利用者登録だけを対象とし、バイオメトリック識別を対象としない。
上記のバイオメトリック照合とバイオメトリック識別については、1.3.3 に詳述する。

本 PP は、バイオメトリック照合製品を調達する際に使用することを想定している。ST 作者は、製品に関する適切な記述を本 PP に加えて、ST を作成しなければならない。

1.3. TOE 概要

1.3.1. TOE の種別

本 PP が対象とする TOE は、バイオメトリック照合製品である。そのための登録は対象とするが、バイオメトリック識別の機能は対象としない。TOE は、利用者認証データとして身体的特徴(顔、指紋、虹彩、静脈など)を用いることで、利便性の高い利用者認証のための機能を提供することができる。TOE は、登録生体情報を格納する格納機能を含まない。

1.3.2. 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 を動作させ使用するためには、適切な運用環境を用意しなければならない。バイオメトリクスの機能としては、例えばデータベースソフトウェアなどの格納機能を実現する製品が、TOE から使えるようになっていなければならない。

TOE が使用できるハードウェアは、バイオメトリクスの専用機器、汎用的な PC、または、スマートフォンなどモバイルデバイスなどである。TOE が使用できるソフトウェアには、OS などがある。OS は、TOE が動作するハードウェアに応じて、専用機器の OS、Windows や Mac OS のような PC 用汎用 OS、または、iOS や Android のようなモバイルデバイス用の OS などがある。TOE が PC やモバイルデバイス上の汎用 OS で動作する場合は、ウィルスなどマルウェアなどから保護する対策ソフトが運用環境として使用できる。

例えば、PC に搭載される TOE を想定すると、TOE は、OS 上で動作するソフトウェアとなる。PC に組み込まれているカメラをデータ採取機器として利用する場合は、カメラを制御するドライバも運用環境となる。ST の作成に当たっては、TOE を動作させるために必要な運用環境を指定しなければならない。調達に当たっては、TOE が要求する運用環境を準備しなければならない。

1.3.3. TOE の使用法

TOE は、具体的には、オフィスでの PC のログインでの利用者認証、銀行の ATM や入退室管理の利用者認証、スマートフォンなどのモバイルデバイス上の利用者認証などに使われるバイオメトリック照合製品である。オフィスでの PC ログインに使用される場合は、TOE は施錠管理等された安全なオフィス環境で使用されるものとする。銀行の ATM や入退室管理に使用される場合には、建物や施設などに固定して設置され、監視カメラや警備員に監視された環境で使用されるものとする。TOE がモバイルデバイス上で動作する場合には、利用者はモバイルデバイスを適切に管理し、攻撃者が TOE や後述する 2 次資産を改竄できないことを想定している。

生体情報の登録及びバイオメトリック照合の処理全体を含む最小のシステムを、本 PP では、バイオメトリックシステム(BS)と呼ぶ。

以下に一般的な BS の使用の流れを示す。以下は、典型例であり、TOE によっては異なる処理を行う場合がある。

時系列的に、先ず、登録対象のユーザに対して、登録処理が行われる。TOE が指定する身体的特徴をデータ採取機能に提示し生データが採取され、特徴抽出機能によって生データから特徴データが抽出される。検査機能は得られた生データの品質を検査し、品質が十分でない場合は、ユーザは上記の処理を繰り返さなければならない。生データの十分な品質が得られ、偽造生体の提示ではないと登録機能が判断した場合、特徴データは、登録生体情報として、ID と対応付けられて、格納機能に保存される。生データが十分な品質を持たない場合または偽造生体が提示されたと判断された場合は、登録できない。TOE によって

は、生データが登録生体情報として格納機能に保存される場合もある。

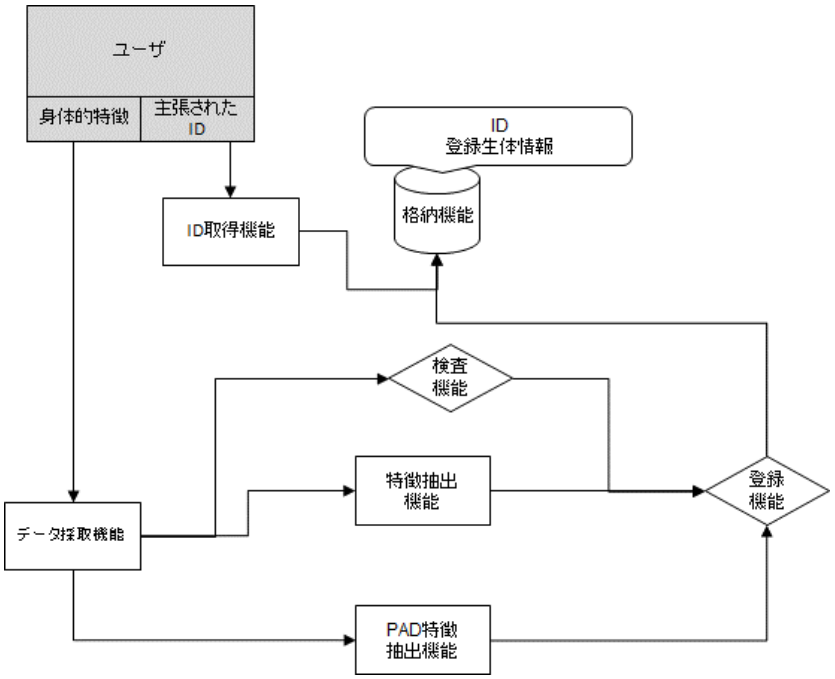


図 1 登録の処理

バイオメトリック照合処理は、ユーザが提示した身体的特徴が登録生体情報と同一のユーザのものであるかを判定する TOE の主機能である。登録ユーザは ID 取得機能に ID を提示する。登録生体情報取得機能は提示された ID に対応する登録生体情報を格納機能から取得し、データ採取機能はユーザの生データを取得する。検査機能は、得られた生データの品質を検査する。比較機能は、生データから特徴抽出機能が特徴抽出した特徴データを格納機能から取り出された登録生体情報と比較し、両者の類似度を算出する。決定機能は、データ採取された生データが十分な品質を持っていると検査機能が判断し、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃ではないと判断でき、特徴データと登録生体情報の類似度が要求される閾値を超える場合のみ、照合成功とする。そうでない場合は、照合失敗とする。なお、生データを登録生体情報としている場合には、登録生体情報は、特徴抽出された後、比較機能に渡される。

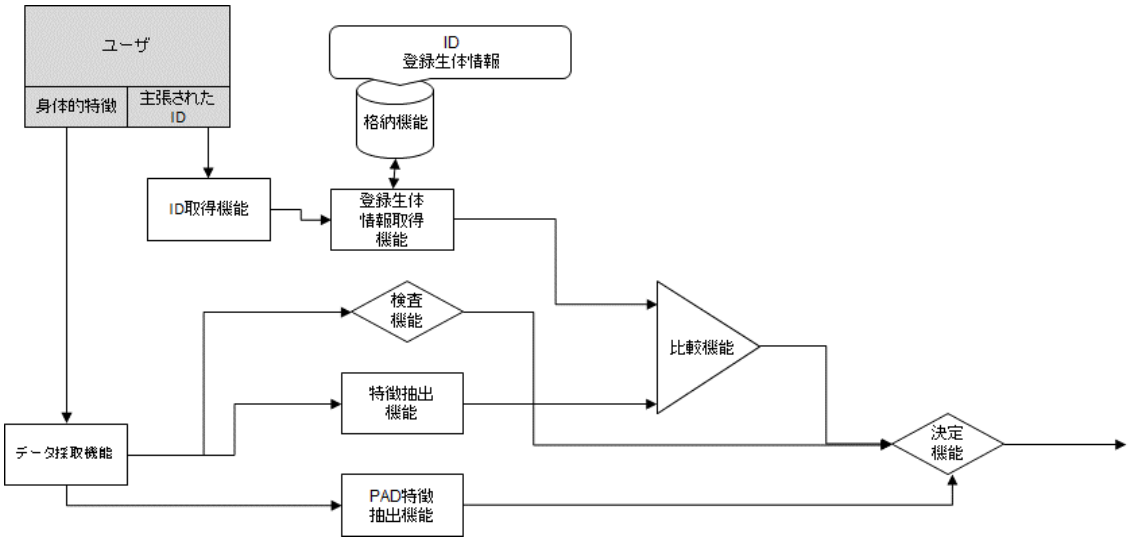


図 2 バイオメトリック照合の処理

本 PP では、登録ユーザがバイオメトリック照合され利用者認証された結果、登録ユーザは TOE 外の所望の物理的資産または論理的資産にアクセスできる。
物理的資産の例としては、バイオメトリック照合の結果、入室して使用可能になる場所がある。論理的資産の例としては、バイオメトリック照合の結果、使用可能になるデジタルデータやアプリケーションソフトウェアがある。バイオメトリック照合の使用シーンは、一般的な ID / パスワード方式の利用者認証機能が利用されるシーンと共通である。
バイオメトリクスの応用には、上記の他に、バイオメトリック識別がある。バイオメトリック照合とは異なり、バイオメトリック識別ではユーザは ID 入力を必要としない。システムがユーザの生データを採取し、格納機能の全ての登録生体情報と照合する。システムが十分に類似すると判定した登録生体情報に対応する ID が、システムから返される。

1.3.4. TOE の主要なセキュリティ機能

本 TOE の主要なセキュリティ機能は、バイオメトリック照合機能である。以下にその詳細を述べる。

1.3.4.1. バイオメトリック照合の特性

バイオメトリック照合機能は、他の認証機能とは異なった、特有の性質がある。それがセキュリティ上の脆弱性や脅威に関係している。以下にこれを説明する。

(1)誤受入率・誤拒否率
バイオメトリック照合は、生体情報に基づいており、あらかじめ登録された登録生体情報と照合時に得られる特徴データの類似度が閾値を超えれば、バイオメトリック照合を成功

させる。そのため、登録されているユーザが誤って拒否されてしまう、あるいは登録されていないユーザが誤って受け入れられてしまう現象が発生することがある。前者の発生率を FRR(False Reject Rate　誤拒否率)、後者の発生率を FAR(False Accept Rate　誤受入率)と呼ぶ。

FAR と FRR を下の図に示す。他人の曲線は、本人の登録生体情報と他人の特徴データを照合した場合の類似度の分布を表している。本人の曲線は、本人の登録生体情報と本人の特徴データを照合した場合の類似度の分布を表している。閾値を図のように設定した場合には、閾値より類似度が低い影のついた部分は本人であるにも関わらず拒否される割合を表すことになり、閾値より類似度が高い影のついた部分は本人でないにも関わらず照合される割合を表すことになる。

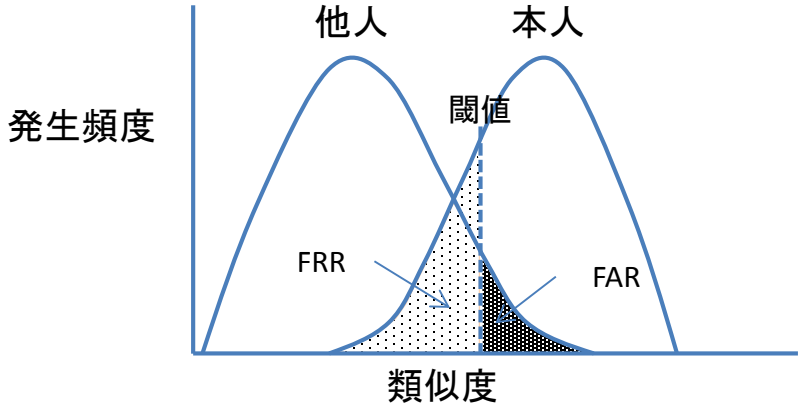


図 3 バイオメトリック照合の類似度分布

閾値を高くすれば、 FAR は低下するが、 FRR が増加する。その結果、使い難いシステムとなる。反対に閾値を低くすれば、FRR は低下するが、 FAR は増加する。その結果、システムのセキュリティは低下する。

FAR と FRR に関連する問題に対処するため、TOE は十分な FAR と FRR を満たすための機能を持たなければならない。また、FAR を良く見せるために、照合され易い登録生体情報だけを登録することがあってはならないので、TOE は FTE（Failure To Enrol（生体情報登録失敗率））が一定の割合よりも低くなくてはならない。

(2)偽造生体や品質の低い生体情報を用いた攻撃

BS に対する攻撃に、なりすましのために、生体を模した偽造生体や品質の低い生体情報となるように生体をデータ採取機器に提示する攻撃がある。これに対処するために、TOE は、偽造生体等を提示した攻撃を防止できるものとする。

1.3.4.2. TOE に対する攻撃手法と攻撃能力の想定

BS に対する典型的な攻撃は、1.3.4.1 で挙げた誤受入率を利用した手法と偽造生体等を利用

した手法である。これらの攻撃手法は、照合に用いられる身体的特徴や運用環境によって異なり、その攻撃に必要な能力も異なってくる。本 PP においては、1.2 のとおり、誤受入及び偽造生体検知に関係する脅威を取り扱う。1.3.3 にあるように、本 PP では、TOE は安全な環境で使用されることを想定しており、使用中の TOE を解析する、或いは物理的に改変する等を実施することは困難である。また、TOE を含む製品を購入可能な場合は、時間をかけて TOE を解析することは可能である。本 PP では、AVA_VAN.2 に相当する基本的な攻撃能力を想定し、脅威を記述する。

1.3.5. TOE の構成

TOE の構成は、以下のふたつである。本 PP は、いずれにも適用できる。

- 統合型：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。
- 分離型：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。

  適用上の注釈：

  本 PP が統合型・分離型のいずれにも適用できるのは、3 の前提条件 A.COMMUNICATION による。

1.3.6. TOE の使用が想定される環境

TOE の誤受入率・誤拒否率は、TOE の使用用途（オフィスでの PC ログイン、ビル入退出管理等）とそれに対応した想定使用環境（屋外・屋内、利用者の人口分布等）に依存する。ST 作成者は、評価で想定する TOE の使用用途及びその使用環境について、ST に詳細に記述しなければならない。

1.3.7. TOE の機能

本 PP の TOE 及び運用環境の機能の一例を図 4 及び図 5 に図示する。図中の表記は、以下のとおりである。

太枠は、TOE の範囲を表す。

太枠内の実線四角（特徴抽出機能など）は、TOE が含む機能を表す。

太枠内の破線四角（データ採取機能など）は、本 PP では提供されないとしているが、TOE が含んでよい機能を表す。

太枠外の実線四角は、TOE の運用環境で提供される機能を表す。

影の付いた実線四角は、ユーザを表す。

なお、以下は、典型例であり、TOE によっては異なる処理を行う場合がある。

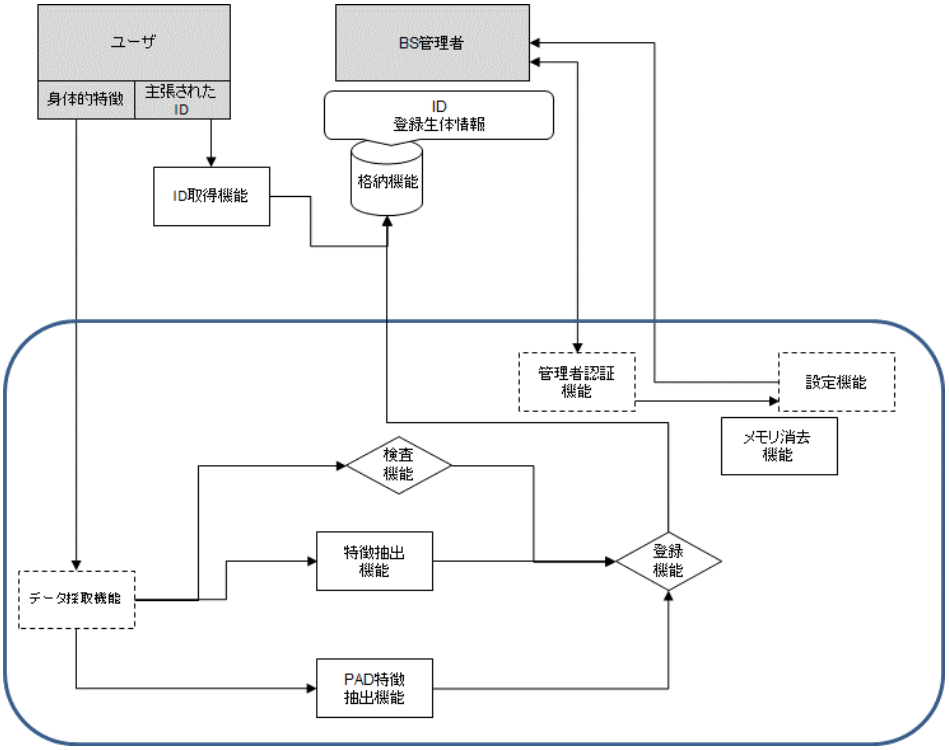


図 4　一般的な TOE の構成（登録の場合）

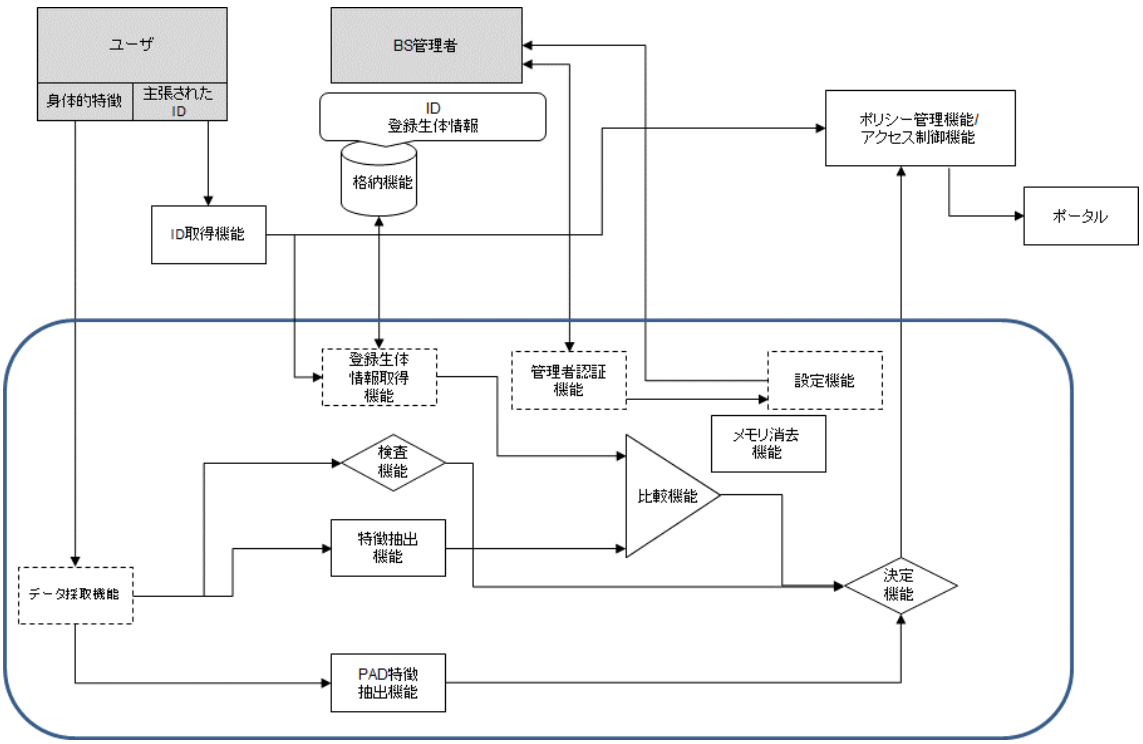


図 5 一般的な TOE の構成（照合の場合）

図 4 及び図 5 に示した機能に関し、以下に説明する。
TOE が含む機能は以下のとおりである。

- 特徴抽出機能：登録や照合の前段階として、採取された生データから特徴が抽出される。これが、本機能の役割である。抽出されたデータは圧縮される場合もある。抽出されたデータを特徴データと呼ぶ。
- 検査機能：この機能は、データ採取機能から得られた生データが以後の処理のために十分な品質を持っているかを検査する。
- 登録機能：この機能は、検査機能によって登録に十分な品質を持つと判断され、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃でないと判断できる場合に、特徴抽出機能から得られた特徴データを登録生体情報として出力する。条件を満たさない場合は、登録生体情報となる特徴データを出力しない。なお、PAD（Presentation Attack Detection）とは、採取された生データより偽造生体などを使った攻撃か否かを検知することを指す。
- 比較機能：この機能は、特徴抽出機能で抽出された特徴データを格納機能に登録されて登録生体情報取得機能で取り出された登録生体情報と比較し、両者の類似度を算出する。
- 決定機能：この機能は、検査機能、PAD 特徴抽出機能、及び比較機能の出力に基づき照合成功か照合失敗かを決定する。生データが十分な品質を持っていると検査機能が判断し、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃ではないと判断でき、特徴データと登録生体情報の類似度が要求される閾値を超える場合のみ、照合成功とする。いずれかの条件を満たさない場合は、照合失敗とする。また、完全一致は登録生体情報を特徴データとして再使用の可能性があるので失敗にすべきである。
- PAD 特徴抽出機能：PAD 特徴データは、データ採取機能が処理する生データから抽出される。PAD 特徴データは、データ採取機能への偽造生体などを使った攻撃の有無を決定するために使われ、登録時の登録機能における登録の成功/失敗の決定、照合時の決定機能における照合の成功/失敗の決定に使われる。
- メモリ消去機能：この機能は、攻撃からの保護のために、使用後のメモリの内容を消去する。消去されるべき情報は、登録生体情報、特徴データ、生データなどが含まれる。

本 PP では、データ採取機能、登録生体情報取得機能、及び TOE のセキュリティに関連したパラメータ（閾値を含む）設定などのセキュリティ管理機能は、提供されていないものとしている。TOE がこれらの機能を持つ場合は、各機能の内容は以下のとおりである。

- データ採取機能：この機能は、ユーザから生データを採取し、特徴抽出機能や検査機能に生データを送る役割を担う。

- 登録生体情報取得機能：この機能は、ユーザの ID に対応する既に登録された登録生体情報を取得する。
- 管理者認証機能：この機能は、BS の管理者に対する識別・認証を担う。この手段の例としては、スマートカードと PIN が挙げられる。BS 管理者は、認証された後に、TOE のセキュリティ関連設定を許可される。
- 設定機能：この機能は、BS 管理者に TOE のセキュリティに関連するパラメータの設定をするためのインタフェースを提供する。この機能は、TOE によっては、決定機能のための閾値設定に使われる。

TOE の運用環境にもセキュリティに関連する機能やインタフェースがある。

- 格納機能：運用環境は TOE が使うデータベースを提供しなければならない。このデータベースは、ユーザの登録生体情報を格納する。登録生体情報以外の情報を含むこともある。
- ID 取得機能 ：この機能は、ユーザが入力する ID を獲得する。この機能は、入力された ID に基づき生体情報を登録し、入力された ID で照合に使う登録生体情報を決めるので、セキュリティに関連している。この機能は、ユーザに見えるインタフェースを提供する。運用環境がこの機能を含むかどうかは製品に依存する。個人利用の製品の場合は、ユーザは自動的に決まるため、この機能は必ずしも必要ではない。
- ポリシー管理機能/アクセス制御機能：バイオメトリック照合の結果は、運用環境のポリシー管理機能/アクセス制御機能に渡される。この機能は、ユーザの権利をチェックし、ユーザが十分な権限を持っていて TOE によるバイオメトリック照合が成功し、利用者認証された場合に、ユーザのポータルへのアクセスを許可する。すなわち、この機能は、ポータルへのアクセス制御を実現するものである。
- セキュア通信機能：運用環境は、セキュリティ関連データのセキュアな通信をサポートする。セキュアな通信は、TOE からの通信、TOE への通信、TOE の構成要素間の通信の場合がある。
- ポータル： 物理的または論理的な点であって、そこから先にある物理的または論理的な資産が運用環境のポリシー管理機能/アクセス制御機能で守られているような点である。ポリシー管理機能/アクセス制御機能は、上述のとおり、TOE からユーザの ID に対するバイオメトリック照合結果を受け取り、アクセス制御を実施する。

2. 適合主張

2.1. CC 適合主張

本 PP は、CC バージョン 3.1 改訂第 4 版（日本語版）適合を主張する。

本 PP は、CC パート 2 拡張を主張する。拡張するセキュリティ機能コンポーネントを第 5 章に定義する。

本 PP は、CC パート 3 適合を主張する。

2.2. PP 主張

本 PP は、他の PP に適合していない。

2.3. パッケージ主張

本 PP は、EAL2 追加を主張する。追加する保証要件は、ALC_FLR.1 である。

2.4. 適合ステートメント

本 PP は、他の PP/ST が本 PP への正確適合することを要求する。

3. セキュリティ課題定義

3.1. TOE に関連するエンティティ

以下の外部エンティティは、TOE に作用を及ぼす。

BS 管理者：

TOE のインストール（ハードウェアがある場合はその設置を含む）、設定、及び運用の責任を持つ。

登録ユーザ：

TOE を含む BS に生体情報を登録し、TOE にバイオメトリック照合され利用者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、登録時に偽造生体や品質の低い生体情報を意図的に登録することを試みたり、照合時に TOE に不正にバイオメトリック照合されることを試みる。

3.2. 資産

本 PP では、以下の資産を定義する。

1 次資産：

TOE 外に存在する資産であって、登録ユーザが TOE でバイオメトリック照合され利用者認証されることによってポータルを経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 BS 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照合のためのパラメータなど。

3.3. 前提条件

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、攻撃者に情報提供することはない。BS 管理者は、TOE のインストール（ハードウェアがある場合はその設置を含む）、設定、運用の責任を持ち、これらを正しく実行する。

適用上の注釈：

BS 管理者は、TOE が正しく稼動することに対して責任を持つ。しかし、攻撃者は、BS 管理者の目を盗み、偽造生体または品質の低い生体情報を登録するなどの可能性があり、そのような攻撃は、後述する T.PRESENTATION_ATTACK として定義されている。

A.PROTECT_ASSETS

TOE の 2 次資産は、改変、破壊、または収集されないように保護されている。

適用上の注釈：

例えば、閾値等のパラメータを変更する管理機能が運用環境より提供されている場合、そのような機能は BS 管理者だけが実施できるように管理されていなければならない。

A.COMMUNICATION

運用環境のバイオメトリクスの処理に関わる機能と TOE 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、保護されている。

A.ENVIRONMENT

TOE が正しく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。

適用上の注釈：

例えば、登録ユーザの登録生体情報を登録する格納機能は、適切に管理され、真正性と完全性が保たれている。また、TOE はウィルスなどマルウェアから保護されている。

3.4. 脅威

T.CASUAL_ATTACK

攻撃者が、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、自分自身の身体的特徴を提示するかも知れない。

T.PRESENTATION_ATTACK

攻撃者が、別の攻撃者に 1 次資産にアクセスさせることを狙い、品質の低い登録生体情報になるように身体的特徴を提示したり、偽造生体を提示して、登録を試みるかも知れない。また、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、品質の低い生体情報になるように身体的特徴を提示したり、偽造生体を提示するかも知れない。

3.5. 組織のセキュリティ方針

P.ENROL_ADMINISTERED

登録ユーザの生体情報登録は、BS 管理者だけが実行できるようにしなければならない。

P.RESIDUAL

登録ユーザの生体情報及びその他の関連データは、バイオメトリック登録及び照合の処理が終了して必要がなくなった時点で、削除するなどして利用できないようにしなければならない。

P.CONTROL_FALSE_REJECT

登録ユーザが身体的特徴の提示をした場合のバイオメトリック照合の失敗は、一定の割合以下にしなければならない。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.PAD_ENROL

TOE は、バイオメトリック登録において、入力されたデータが偽造生体から採取されたものであった場合または品質が低い登録生体情報となるように身体的特徴が提示された場合、それらの登録を防止しなければならない。

O.CLEAR_RESIDUAL

TOE は、バイオメトリック登録及び照合の処理が終了後に、TOE 内に残存する生体情報及びその他の関連データを、削除しなければならない。

O.CONTROL_FALSE_ACCEPT

TOE は、誤受入率(FAR)に対する基準を満たさなければならない。

O.PAD_VERIFY

TOE は、品質が低い生体情報となるように身体的特徴が提示された場合、及び偽造生体が提示された場合、バイオメトリック照合が成功することを防止しなければならない。

O.CONTROL_FALSE_REJECT

TOE は、誤拒否率(FRR) に対する基準を満たさなければならない。

4.2. 運用環境のセキュリティ対策方針

OE.ENROL_ADMINISTERED

BS 管理者は､BS 管理者だけが TOE の登録処理を実行できるようにしなければならない。

OE.PROTECT_RESIDUAL_ENVIRONMENT

BS 管理者は、一時的に使用した生体情報があれば、必要がなくなった時点で削除するなどして保護できる運用環境を登録ユーザに提供しなければならない。

OE.ACCESS_CONTROL

BS 管理者は、バイオメトリック照合が成功した場合に限って、ユーザのポータルへのアクセスを許可する運用環境を提供しなければならない。

OE.LIMIT_NUM_TRIAL

BS 管理者は、生体情報登録の試行失敗が一定回数以上に達した場合、登録を失敗とするアプリケーションを利用しなければならない。また、バイオメトリック照合の試行失敗が一定回数以上に達した場合、当該ユーザのアカウントをロックするアプリケーションを利用して、TOE に対する試行回数を制限しなければならない。

OE.ADMINISTRATION

BS 管理者は、悪意を持たない者でなければならない。すなわち、攻撃者になったり、攻撃者に情報提供してはならない。BS 管理者は、TOE のインストール（ハードウェア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.PROTECT_ASSETS

BS 管理者は、 TOE の 2 次資産が改変、破壊、または収集されないように保護する運用環境を提供しなければならない。

OE.COMMUNICATION

BS 管理者は、運用環境のバイオメトリクスの処理に関わる機能と TOE 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がセキュアな通信となる運用環境を提供しなければならない。

OE.ENVIRONMENT

BS 管理者は、TOE が正しく動作可能になるためのセキュアな運用環境を提供しなければならない。

4.3. セキュリティ対策方針根拠

セキュリティ対策方針は、セキュリティ課題定義で規定した前提条件、脅威、組織のセキュリティ方針に対応するものである。表 **1** に、セキュリティ対策方針と、脅威、組織のセキュリティ方針、前提条件との対応関係を示す。

表 1　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	OE.ENROL_ADMINISTERED	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_ASSETS	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x					x	x				
T.PRESENTATION_ATTACK	x			x				x	x				
P.ENROL_ADMINISTERED						x							
P.RESIDUAL		x					x						
P.CONTROL_FALSE_REJECT					x								
A.ADMINISTRATION											x		
A.PROTECT__ASSETS										x			
A.COMMUNICATION												x	
A.ENVIRONMENT													x

4.3.1.　脅威への対抗

T.CASUAL_ATTACK

T.CASUAL_ATTACK では、攻撃者が、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、自分自身の身体的特徴を提示することを、想定している。これに対しては、O.CONTROL_FALSE_ACCEPT と OE.ACCESS_CONTROL との組合せ及び OE.LIMIT_NUM_TRIAL によって、対抗する。TOE が十分に低い誤受入率(FAR)を持つので、攻撃者のバイオメトリック照合が成功して運用環境が攻撃者のポータルへのアクセスを許可する確率は十分に低い。更に、バイオメトリック照合の試行失敗が一定回数以上に達した場合に運用環境が攻撃と判断して当該ユーザのアカウントをロックするから、T.CASUAL_ATTACK に対抗する。

T.PRESENTATION_ATTACK

T.PRESENTATION_ATTACK では、攻撃者が、別の攻撃者に 1 次資産にアクセスさせることを狙い、品質の低い登録生体情報になるように身体的特徴を提示したり、偽造生体

を提示して、登録を試みることを想定している。また、攻撃者が、登録ユーザの ID を使い TOE にバイオメトリック照合されて 1 次資産にアクセスすることを狙って、品質の低い生体情報になるように身体的特徴を提示したり、偽造生体を提示することを、想定している。脅威の前半に対しては、O.PAD_ENROL で対抗する。登録時に、データ採取機能に偽造生体が提示された場合または品質が低い登録生体情報となるように身体的特徴が提示された場合等、TOE はそれらの登録を防止するので、別の攻撃者が品質の低い生体情報になるように身体的特徴を提示したり、偽造生体を提示したりしてバイオメトリック照合されることはない。更に、OE.LIMIT_NUM_TRIAL によって、生体情報登録の試行失敗が一定回数以上に達した場合に運用環境が攻撃と判断して当該ユーザの登録を失敗とする。脅威の後半に対しては、O.PAD_VERIFY と OE.ACCESS_CONTROL との組合せ及び OE.LIMIT_NUM_TRIAL によって、対抗する。データ採取機能に品質の低い生体情報になるように身体的特徴が提示されたり、偽造生体が提示された場合、TOE はバイオメトリック照合が成功することを防止させ、運用環境は攻撃者のポータルへのアクセスを許可しない。更に、OE.LIMIT_NUM_TRIAL によって、バイオメトリック照合の試行失敗が一定回数以上に達した場合に運用環境が攻撃と判断して当該ユーザのアカウントをロックする。よって、これらによって、T.PRESENTATION_ATTACK に対抗する。

4.3.2. 組織のセキュリティ方針の実現

P. ENROL_ADMINISTERED

P. ENROL_ADMINISTERED では、登録ユーザの生体情報登録を BS 管理者だけが実行できるようにしなければならないことを求めている。これは、OE.ENROL_ADMINISTERED によって、BS 管理者だけが TOE の登録処理にアクセスできるようにすることで、実現される。

P.RESIDUAL

P.RESIDUAL では、バイオメトリック登録及び照合の処理の後に残存する生体情報及び登録ユーザのその他の情報を削除するなどして利用できなくすることを求めている。これは、O.CLEAR_RESIDUAL、OE.PROTECT_RESIDUAL_ENVIRONMENT の組み合わせによって、実現される。O.CLEAR_RESIDUAL によって、TOE 内の処理に使用した生体情報及び登録ユーザのその他の情報は、バイオメトリック登録及び照合の処理終了後に、削除され、OE.PROTECT_RESIDUAL_ENVIRONMENT によって、運用環境が一時的に使用した生体情報があれば、必要がなくなった時点で削除するなどして保護されるからである。

P.CONTROL_FALSE_REJECT

P.CONTROL_FALSE_REJECT では、登録ユーザが身体的特徴の提示をした場合のバイオメトリック照合の失敗を、一定の割合以下にしなければならないことを求めている。これは、O.CONTROL_FALSE_REJECT によって、TOE が運用に支障のない誤拒否率

(FRR)を持つことで、実現される。

4.3.3. 前提条件への対応

A.ADMINISTRATION

A.ADMINISTRATION には、OE.ADMINISTRATION が対応する。

A.PROTECT_ASSETS

A.PROTECT_ASSETS には、OE.PROTECT_ASSETS が対応する。

A.COMMUNICATION

A.COMMUNICATION には、OE.COMMUNICATION が対応する。

A.ENVIRONMENT

A.ENVIRONMENT には、OE.ENVIRONMENT が対応する。

全ての前提条件に対して、対応するセキュリティ対策方針は前提条件の記述に対応するように記述されている。よって、それぞれのセキュリティ対策方針が有効であれば、対応する前提条件は満たされる。

5. 拡張コンポーネント定義

クラス FIA（識別と認証）の拡張された機能ファミリ FIA_EBT（Enrolment of Biometric Template）及び FIA_BVR （Biometric VeRification）は、この PP の対象となる TOE のバイオメトリック照合の機能を記述するために定義される。TOE は、ポータルへのアクセスのために、バイオメトリック照合を提供しなければならない。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とバイオメトリック照合には差異があるため、クラス FIA への拡張を選択した。

5.1. 生体情報の登録 FIA_EBT

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ック照合のための生体情報の登録のメカニズムを定義する。このファミリは、生体情報の登録の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_EBT.1　登録時の生体情報の検査は、偽造生体や品質の低い生体情報の使用を防止できることを要求する。

FIA_EBT.2　生体情報登録失敗率の低い生体情報の登録は、後のバイオメトリック照合における精度を良く見せるために、照合され易い生体情報だけ使用することを防止できることを要求する。

管理: FIA_EBT.1

以下のアクションは FMT における管理機能と考えられる:

管理者による TSF データ(登録時の生体情報の検査のための設定値)の管理

管理者による TSF データ(偽造生体検知のための設定値)の管理

管理: FIA_EBT.2

以下のアクションは FMT における管理機能と考えられる:

管理者による TSF データ(登録時の生体情報の検査のための設定値)の管理

監査: FIA_EBT.1
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: TSF による、検査及び偽造生体検知されたデータの拒否;
b) 基本: TSF による、検査及び偽造生体検知されたデータの拒否または受け入れ;
c) 詳細: 定義された TSF データ（検査及び偽造生体検知のための設定値）に対する変更の識別。

監査: FIA_EBT.2
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: TSF による、検査されたデータの拒否;
b) 基本: TSF による、検査されたデータの拒否または受け入れ;
c) 詳細: 定義された TSF データ（登録時の生体情報の検査のための設定値）に対する変更の識別。

FIA_EBT.1 登録時の生体情報の検査
下位階層: なし
依存性: なし

FIA_EBT.1.1 TSF は、TSF の利用者による品質が低い登録のための生体情報の使用を防止しなければならない。
適用上の注釈：
品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.1.2 TSF は、TSF の利用者による登録のための偽造生体の使用を防止しなければならない。
適用上の注釈：
偽造生体とは、TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

下位階層: なし
依存性: なし

FIA_EBT.2.1　TSF は、FTE[割付 : X]以下で動作する登録のための生体情報の受け入れメカニズムを提供しなければならない。

適用上の注釈：

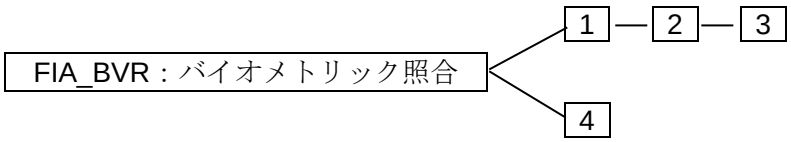
FTE の定義は、TOE の登録ポリシーに依存する。ST 作成者はそのポリシー概略を示さなければならない。

5.2.　バイオメトリック照合 FIA_BVR

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ック照合のメカニズムを定義する。このファミリは、バイオメトリック照合の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_BVR.1 精度の高いバイオメトリック照合は、TSF が利用者のバイオメトリック照合の誤受入及び誤拒否がそれぞれ一定の割合以下であることを要求する。

FIA_BVR.2 バイオメトリック照合による利用者認証のタイミングは、利用者の識別情報のバイオメトリック照合による利用者認証の前に、利用者があるアクションを実行することを認める。

FIA_BVR.3 アクション前のバイオメトリック照合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、バイオメトリック照合による利用者認証を要求する。

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合は、品質が低い生体情報や偽造生体の使用を、バイオメトリック照合のメカニズムが防止することを要求する。

管理: FIA_BVR.1
以下のアクションは FMT における管理機能と考えられる:
管理者による TSF データ(閾値を含む)の管理

管理: FIA_BVR.2
以下のアクションは FMT における管理機能と考えられる:
a) 管理者による TSF データ(閾値を含む)の管理;
b) 利用者が認証される前にとられるアクションのリストを管理すること。

管理: FIA_BVR.3
以下のアクションは FMT における管理機能と考えられる:
a) 管理者による TSF データ(閾値を含む)の管理;

管理: FIA_BVR.4
以下のアクションは FMT における管理機能と考えられる:
a) 管理者による TSF データ(偽造生体検知のための設定値)の管理

監査: FIA_BVR.1
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: バイオメトリック照合メカニズムの不成功になった使用
b) 基本:バイオメトリック照合メカニズムのすべての使用

監査: FIA_BVR.2
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: バイオメトリック照合による利用者認証メカニズムの不成功になった使用;
b) 基本: バイオメトリック照合による利用者認証メカニズムのすべての使用。
c) 詳細: バイオメトリック照合による利用者認証以前に行われた利用者のすべての TSF 仲介アクション。

監査: FIA_BVR.3
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:
a) 最小: バイオメトリック照合による利用者認証メカニズムの不成功になった使用;
b) 基本: バイオメトリック照合による利用者認証メカニズムのすべての使用。

監査: FIA_BVR.4
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを

監査対象にすべきである:
a) 最小:TSF による、検査及び偽造生体検知されたデータの拒否;
b) 基本: TSF による、検査及び偽造生体検知されたデータの拒否または受け入れ;
c) 詳細: 定義された TSF データ（検査及び偽造生体検知のための設定値）に対する変更の識別。

FIA_BVR.1 精度の高いバイオメトリック照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検査
　　FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.1.1 TSF は、各利用者に FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供しなければならない。

FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング
下位階層: FIA_BVR.1 精度の高いバイオメトリック照合
依存性: FIA_UID.1 識別のタイミング
　　FIA_EBT.1　登録時の生体情報の検査
　　FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.2.1 TSF は、利用者がバイオメトリック照合による利用者認証を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_BVR.2.2 TSF は、FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に当該メカニズムで認証が成功することを要求しなければならない。

FIA_BVR.3 アクション前のバイオメトリック照合による利用者認証
下位階層: FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング
依存性: FIA_UID.1 識別のタイミング
　　FIA_EBT.1　登録時の生体情報の検査
　　FIA_EBT.2 生体情報登録失敗率の低い生体情報登録
FIA_BVR.3.1 TSF は、FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し、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、その利用者に当該メカニズムで認証が成功することを要求しなければならない。

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検査

FIA_BVR.4.1 TSF は、TSF の利用者による品質が低い照合のための生体情報の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_BVR.4.2
TSF は、TSF の利用者による照合のための偽造生体の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

偽造生体とは、 TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

5.3.　機能ファミリ FIA_EBT 及び FIA_BVR 定義の理由

FIA_UAU が定義する利用者認証は、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。これに対し、バイオメトリック照合の場合は、FAR の存在が示すように、利用者の生体情報が提示された場合でも失敗する可能性がある。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、バイオメトリック照合では両者は明確に区別できない。また、バイオメトリック照合による利用者認証の場合は FIA_UAU と同様に利用者の ID を与えるが、バイオメトリック照合だけの場合は、利用者の ID は与えられず、照合時に得られ認証データに相当する特徴データと登録生体情報を比較するのみであるという差異がある。上記のとおり、クラス FIA にバイオメトリック照合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_BVR を定義した。

バイオメトリック照合を実行するためには、予め生体情報を登録する必要がある。登録生体情報が偽造生体によるものや品質が低いものであっては、正しいバイオメトリック照合が実行されない。また、バイオメトリック照合における精度を良く見せるために、照合され易い生体情報だけを登録することがあってはならない。これらの要件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_EBT を定義した。

6. セキュリティ要件

6.1. セキュリティ機能要件

表 **2** にこの PP のすべての TOE セキュリティ機能要件の一覧を示す。

表 2　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	生体情報登録失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合

操作内容は、各 SFR において以下の表記方法で示される。

・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。
・割付は　[割付：*XXX*]のように斜体で示す。
・選択は　 [選択：*XXX*] のように斜体で示す。選択対象外の項目は、~~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。
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。

FDP_RIP.1サブセット残存情報保護
下位階層: なし
依存性: なし

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　[選択: ~~*への資源の割当て、*~~*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。
　適用上の注釈：
　ST 作者は、割当て解除するオブジェクトを全て割り付けよ。

FIA_EBT.1　登録時の生体情報の検査
下位階層: なし
依存性: なし

FIA_EBT.1.1　TSF は、TSF の利用者による品質が低い登録のための生体情報の使用を防止しなければならない。
適用上の注釈：
品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.1.2　TSF は、TSF の利用者による登録のための偽造生体の使用を防止しなければならない。
適用上の注釈：
偽造生体とは、TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_EBT.2　生体情報登録失敗率の低い生体情報登録
下位階層: なし
依存性: なし

FIA_EBT.2.1　TSF は、FTE[割付：X]以下で動作する登録のための生体情報の受け入れメカニズムを提供しなければならない。
適用上の注釈：
FTE の定義は、TOE の登録ポリシーに依存する。ST 作成者はそのポリシー概略を示さなければならない。

FIA_BVR.1 精度の高いバイオメトリック照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検証
FIA_EBT.2 生体情報登録失敗率の低い生体情報登録

FIA_BVR.1.1　TSF は、各利用者に FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイ

オメトリック照合メカニズムを提供しなければならない。

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検査

FIA_BVR.4.1 TSF は、TSF の利用者による品質が低い照合のための生体情報の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

品質が低い生体情報とは、データ採取において、静止していない提示、データ採取機器に対して回転を加えた提示、データ採取機器が指示する距離に従わない提示、身体部分の一部が隠れている提示によって得られた生体情報等を言う。品質が低い生体情報に対する TOE の判断基準については、TOE 設計に記載すること。

FIA_BVR.4.2
TSF は、TSF の利用者による照合のための偽造生体の使用によるバイオメトリック照合の成功を防止しなければならない。

適用上の注釈：

偽造生体とは、 TOE が扱う身体的特徴やそれを含む身体部分の一部または全部を偽造されたものとする。偽造生体に対する TOE の判断基準については、TOE 設計に記載すること。

6.2.　セキュリティ保証要件

本 PP に適用される保証要件について、表 **3** に示す。保証コンポーネントは EAL2 を基本とし、ALC_FLR.1 を追加の要件としている。

表 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.　セキュリティ要件根拠

6.3.1.　セキュリティ機能要件根拠

本章では、定義された SFR 全体が 4 に記述された TOE のセキュリティ対策方針を適切に達成すること、6.3.1.1 では各 SFR がいずれかの TOE セキュリティ対策方針にさかのぼれることを示す。6.3.1.2 では、依存性が適切に満たされていることを示す。

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

TOE のセキュリティ対策方針が SFR で達成されることを表 **4** に示す。

表 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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X			
FIA_EBT.1	X				
FIA_EBT.2			X		X
FIA_BVR.1			X		X
FIA_BVR.4				X	

以下に対応の詳細を記述する。

O.PAD_ENROL

このセキュリティ対策方針 O.PAD_ENROL は、登録時に、データ採取機能に偽造生体が提示された場合または品質が低い登録生体情報となるように身体的特徴が提示された場合、それらを TOE は登録を防止しなければならないとしている。このセキュリティ対策方針を満たすために、FIA_EBT.1 は登録されようとする情報を検査し、生体情報の品質が低い場合はそれを登録しないこと、偽造生体の場合はそれを登録しないことを、それぞれ要求している。

O.CLEAR_RESIDUAL

このセキュリティ対策方針は、バイオメトリック登録及び照合の処理が終了後に、TOE 内に残存する生体情報及びその他の関連データを、削除するとしている。このセキュリティ対策方針を満たすために、FDP_RIP.1 は、バイオメトリック登録及び照合の処理が終了後に、TOE 内に残存する生体情報及びその他の関連データを、TSF が削除することを要求している。

O.CONTROL_FALSE_ACCEPT

このセキュリティ対策方針 O.CONTROL_FALSE_ACCEPT は、TOE が誤受入率(FAR)の基準を満たすことを規定する。このセキュリティ対策方針を満たすために、FIA_BVR.1 は FAR[割付 : *X*]以下でバイオメトリック照合が成功することを要求する。この X は、ST

で具体的に規定される。しかし、FAR を良く見せるために、照合され易い生体情報だけを登録することがあってはならない。FIA_EBT.2 はこのことを要求する。

O.PAD_VERIFY

このセキュリティ対策方針は、品質が低い生体情報となるように身体的特徴が提示された場合、及び偽造生体が提示された場合、バイオメトリック照合が成功することを防止しなければならないとしている。このセキュリティ対策方針を満たすために、FIA_BVR.4 は品質の低い生体情報及び偽造生体の使用によるバイオメトリック照合の成功を防止することを要求している。

O.CONTROL_FALSE_REJECT

このセキュリティ対策方針 O.CONTROL_FALSE_REJECT は、TOE が誤拒否率(FRR)の基準を満たすことを規定する。このセキュリティ対策方針を満たすために、FIA_BVR.1 は、FRR[割付：Y]以下でバイオメトリック照合が成功することを要求する。この Y は、ST で具体的に規定される。しかし、FRR を良く見せるために、照合され易い生体情報だけを登録することがあってはならない。FIA_EBT.2 はこのことを要求する。

6.3.1.2. セキュリティ機能要件の依存性

本 PP の TOE のセキュリティ機能要件の依存性とその対応について表 **5** に示す。

表 5　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1

6.3.2. セキュリティ保証要件根拠

本 PP では保証レベル EAL2 を選択した。選択の理由は、想定するバイオメトリクス製品への攻撃能力が EAL2 に相当するからである。ALC_FLR.1 はセキュリティを維持するために必要である。

6.3.2.1. セキュリティ保証要件の依存性

セキュリティ保証要件は、ALC_FLR.1 を除き、EAL2 のとおりである。EAL2 からのセキュリティ保証要件については、依存性は EAL2 で定められたとおりである。ALC_FLR.1 については、依存性はない。よって、依存性は満たされる。

7. 用語集

以下において、CC で使われる略語については、フルスペルと日本語訳だけを示す。用語定義については、CC を参照せよ。

用語	意味
BS	Biometric System（バイオメトリックシステム）
CC（Common Criteria）	Common Criteria - Common Criteria for Information Technology Security Evaluation. コモンクライテリア（情報セキュリティ評価のためのコモンクライテリア）
EAL	Evaluation Assurance Level（評価保証レベル）
FAR	False Accept Rate（誤受入率。他人の身元確認要求の照合トランザクションにおいて、誤って受理する率）
FRR	False Reject Rate（誤拒否率。本人の身元確認要求の照合トランザクションにおいて、誤って拒否する率）
FTE	Failure To Enrol（生体情報登録失敗率。ある集団に対して登録処理を行った場合に、システムが登録処理を完了できなかった人数の割合）
OS	Operating System（オペレーティングシステム）
PAD	Presentation Attack Detection (提示型攻撃の検知。BS の操作を妨害することを目的としたデータ採取機能へのデータの提示の検知)
PP	Protection Profile（プロテクションプロファイル）
SFR	Security Functional Requirement（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOE セキュリティ機能）
攻撃者	権限なくポータルへアクセスすることを目的に、登録時に偽造生体や品質の低い生体情報を意図的に登録することを試みたり、照合時に TOE が正常に動作しないようにすることを試みる人
閾値	特徴データがある登録生体情報に対して一致と判定されるために必要な予め定められた類似や相関の度合い。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの一致の判定がなされる。

用語	意味
スマートカード	集積回路が組み込まれたクレジットカードの大きさのチップカード。認証用の鍵を格納するために使われることが多い。
生体情報	生データ、特徴データ、登録生体情報の総称
登録生体情報	のちの照合のための登録に適した特徴データまたは特徴データの組。TOE によっては、特徴データまたは特徴データの組でなく、生データまたは生データの組が用いられることがある。
登録ユーザ	BS に生体情報を登録され、TOE にバイオメトリック照合されることによって、ポータル経由で資産へアクセスするユーザ
特徴データ	生データから抽出した身体的特徴を表すデータ
生データ	データ採取機能によって得られるデータ
バイオメトリクス	人間の身体的特徴や行動的特徴に基づいて個人を自動的に認識する技術
バイオメトリック	バイオメトリクスの、バイオメトリクスを使った
バイオメトリック識別	与えられた特徴データに対して、格納された登録生体情報を検索して一致すると考えられる候補（複数の場合やない場合も含む）を返すアプリケーション。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの処理が実施される。
バイオメトリックシステム（BS）	バイオメトリック照合のメカニズムを含むシステムのうち最小のシステム
バイオメトリックシステム管理者（BS 管理者）	TOE のインストール（ハードウェアがある場合はその設置を含む）、設定、及び運用の責任を持つ管理者。TOE が管理機能を持つ場合は、TOE を含む 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管理者。
バイオメトリック照合	ユーザが提示した身体的特徴から得られる特徴データと登録生体情報とを比較して同一のユーザのものであるかを判定するアプリケーション。複数の特徴データを用いて、複数回の比較をして判定をすることもある。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの処理が実施される。
ユーザ	TOE に身体的特徴を提示し、登録及び照合される人間。本 PP では利用者とも呼んでいる。
利用者認証	システムや資産にアクセス許可される前に、ID を主張するユーザがその ID に対応する本人であることを確認する行為

用語	意味
類似度	特徴データとある登録生体情報との間の類似や相関の度合い。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの類似や相関が測られる。

付録２　選択的なセキュリティ機能要件

9.　選択的なセキュリティ機能要件

9.1.　TOE が管理機能を持ち BS 管理者の利用者管理機能（利用者認証機能含む）を運用環境が持つ場合

9.1.1.　概要

本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定める。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。ただし、BS 管理者の利用者管理機能は運用環境が管理する。

9.1.2.　セキュリティ課題定義の変更

9.1.2.1.　前提条件の変更

本編の A.PROTECT_ASSET を削除せよ。

9.1.2.2.　脅威の変更

T.PRESENTATION_ATTACK の後に次の脅威を追加せよ。

T.MODIFY__ASSETS

攻撃者が、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。

9.1.3.　セキュリティ対策方針の変更

9.1.3.1.　TOE のセキュリティ対策方針の変更

O.PAD_VERIFY と O.CONTROL_FALSE_REJECT の間に次のセキュリティ対策方針を追加せよ。

O.PROTECT_ASSETS

TOE は、BS 管理者だけが TOE 内の 2 次資産（バイオメトリックな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。

9.1.3.2.　運用環境のセキュリティ対策方針の変更

OE.LIMIT_NUM_TRIAL と OE.PROTECT_RESIDUAL_ENVIRONMENT の間に次のセキュリティ対策方針を追加せよ。

OE.AUTH_ADMIN

運用環境は、BS 管理者を利用者認証する手段を提供しなければならない。

OE.PROTECT_ASSETS を削除せよ。

9.1.3.3. セキュリティ対策方針根拠の変更

セキュリティ対策方針根拠の表を以下のものに置き換えよ。

表 6　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT	OE.ENROL_ADMINISTERED	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.AUTH_ADMIN	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x					x	x					
T.PRESENTATION_ATTACK	x			x				x	x					
T.MODIFY__ASSETS					x					x				
P.ENROL_ADMINISTERED							x							
P.CONTROL_FALSE_REJECT						x								
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

9.1.3.3.1. 脅威への対抗の変更

T.PRESENTATION_ATTACK への対抗の次に以下を追加せよ。

T.MODIFY_ASSETS

T.MODIFY_ASSETS では、ポータルへ権限なくアクセスする攻撃者が TOE 内の 2 次資産を改変、破壊、または収集し、悪用することを想定している。これに対しては、OE.AUTH_ADMIN、O.PROTECT_ASSETS の組み合わせによって、対抗する。

OE.AUTH_ADMIN によって、運用環境が BS 管理者を利用者認証する手段が提供される。

O.PROTECT_ASSETS によって、上記のように運用環境に利用者認証された BS 管理者

だけが 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する。よって、攻撃者の TOE 内の 2 次資産であるセキュリティ関連データへのアクセスを防き、TOE 内の 2 次資産の改変・破壊・収集に対抗する。

9.1.3.3.2. 前提条件への対抗の変更

A.PROTECT_ASSETS の記述を削除せよ。

9.1.4. セキュリティ要件の変更

9.1.4.1. セキュリティ機能要件の変更

セキュリティ機能要件の表を以下のものに置き換えよ。

表 7　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
クラス FMT: セキュリティ管理	
FMT_MTD.1	TSF データの管理
FMT_SMF.1	管理機能の特定

次のセキュリティ機能要件を追加せよ。

FMT_MTD.1 TSF データの管理

下位階層: なし

依存性: FMT_SMF.1 管理機能の特定

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。

Application Note：

TSF データの典型的な例として、閾値がある。割付は、ST 作者が実施する。

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

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***]**

9.1.4.2. セキュリティ要件根拠の変更

9.1.4.2.1. セキュリティ対策方針とセキュリティ機能要件の対応の変更

セキュリティ対策方針とセキュリティ機能要件の対応の表を以下で置き換えよ。

表 8　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X				
FIA_EBT.1	X					
FIA_EBT.2			X			X
FIA_BVR.1			X			X
FIA_BVR.4				X		
FMT_MTD.1					X	
FMT_SMF.1					X	

O.PAD_VERIFY の次の以下を追加せよ。

O.PROTECT_ASSETS

このセキュリティ対策方針は、TOE 内のセキュリティ関連データへのアクセスを TOE が BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求している。

9.1.4.2.2. セキュリティ機能要件の依存性の変更

SFR の依存性対応の表を以下に置き換えよ。

表 9　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	なし	不要

依存性から FMT_SMR.1 を削除した根拠は、利用者を BS 管理者に関連付けし、BS 管理者を維持するのは、運用環境が実施するからである。

9.2. TOE が管理機能を持ち BS 管理者の利用者識別機能を持たず利用者認証機能を持つ場合

9.2.1. 概要

本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定める。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。

TOE が、BS 管理者の利用者識別機能を持たないが、BS 管理者の利用者認証機能を持つ。

9.2.2. セキュリティ課題定義の変更

9.2.2.1. 前提条件の変更

本編の A.PROTECT_ASSET を削除せよ。

9.2.2.2. 脅威の変更

T.PRESENTATION_ATTACK の後に次の脅威を追加せよ。

T.MODIFY__ASSETS

攻撃者が、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。

9.2.3. セキュリティ対策方針の変更

9.2.3.1. TOE のセキュリティ対策方針の変更

O.PAD_VERIFY と O.CONTROL_FALSE_REJECT の間に次のセキュリティ対策方針を追加せよ。O.PROTECT_ENROLMEMT については、該当する場合だけ追加せよ。

O.AUTH_ADMIN

TOE は、BS 管理者を利用者認証する手段を提供しなければならない。

O.PROTECT_ENROLMEMT

TOE は、BS 管理者だけが登録処理にアクセスできるようにしなければならない。

O.PROTECT_ASSETS

TOE は、BS 管理者だけが TOE 内の 2 次資産（バイオメトリックな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。

9.2.3.2. 運用環境のセキュリティ対策方針の変更

OE.PROTECT_ASSETS を削除せよ。O.PROTECT_ENROLMEMT をセキュリティ対策方針に追加した場合は、OE.ENROL_ADMINISTERED も削除せよ。

9.2.3.3. セキュリティ対策方針根拠の変更

O.PROTECT_ENROLMEMT をセキュリティ対策方針に含まない場合は、セキュリティ対策方針根拠の表を表 10 に置き換えよ。O.PROTECT_ENROLMEMT をセキュリティ対策方針に含む場合は、セキュリティ対策方針根拠の表を表 11 に置き換えよ。

表 10　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT	OE.ENROL_ADMINISTERED	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x						x	x				
T.PRESENTATION_ATTACK	x			x					x	x				
T.MODIFY__ASSETS					x	x								
P.ENROL_ADMINISTERED								x						
P.CONTROL_FALSE_REJECT							x							
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

表 11 セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x						x	x				
T.PRESENTATION_ATTACK	x			x					x	x				
T.MODIFY__ASSETS					x		x							
P.ENROL_ADMINISTERED					x	x								
P.CONTROL_FALSE_REJECT								x						
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

9.2.3.3.1. 脅威への対抗の変更

T.PRESENTATION_ATTACK への対抗の次に以下を追加せよ。

T.MODIFY_ASSETS

T.MODIFY_ASSETS では、ポータルへ権限なくアクセスする攻撃者が TOE 内の 2 次資産を改変、破壊、または収集し、悪用することを想定している。これに対しては、O.AUTH_ADMIN、O.PROTECT_ASSETS の組み合わせによって、対抗する。

O.AUTH_ADMIN によって、TOE が BS 管理者を利用者認証する手段が提供される。

O.PROTECT_ASSETS によって、上記のように TOE に利用者認証された BS 管理者だけが 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する。よって、攻撃者の TOE 内の 2 次資産であるセキュリティ関連データへのアクセスを防き、TOE 内の 2 次資産の改変・破壊・収集に対抗する。

9.2.3.3.2. 組織のセキュリティ方針の実現の変更

O.PROTECT_ENROLMEMT を含む場合は、P. ENROL_ADMINISTERED の記述を以下に置き換えよ。

P. ENROL_ADMINISTERED

P. ENROL_ADMINISTERED では、運用環境に対して、登録ユーザの生体情報登録を BS 管理者だけが実行できるようにしなければならないことを求めている。これに対しては、O.AUTH_ADMIN、O.PROTECT_ ENROLMEMT の組み合わせによって、対抗する。O.AUTH_ADMIN によって、TOE が BS 管理者を利用者認証する手段が提供される。O.PROTECT_ ENROLMEMT によって、上記のように TOE に利用者認証された BS 管理者だけが登録処理にアクセスできるようにする。よって、BS 管理者だけが TOE の登録処理にアクセスできるようにすることが実現される。

9.2.3.3.3. 前提条件への対応の変更

A.PROTECT_ASSETS の記述を削除せよ。

9.2.4. セキュリティ要件の変更

9.2.4.1. セキュリティ機能要件の変更

9.2.4.1.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

セキュリティ機能要件の表を表 12 に置き換えよ。

表 12　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
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
クラス FMT: セキュリティ管理	
FMT_MTD.1	TSF データの管理
FMT_SMF.1	管理機能の特定

次のセキュリティ機能要件を追加せよ。

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
下位階層: FIA_UAU.1 認証のタイミング
依存性: ~~FIA_UID.1 識別のタイミング~~

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。

FMT_MTD.1 TSF データの管理
下位階層: なし
依存性: ~~FMT_SMR.1 セキュリティの役割~~
FMT_SMF.1 管理機能の特定

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。

Application Note:
TSF データの典型的な例として、閾値がある。O.PROTECT_ENROLMEMT を含む場合は、TSF データとして登録ユーザの登録生体情報、その他操作として登録を割り付けよ。その他の割付は、ST 作者が実施する。

FMT_SMF.1 管理機能の特定
下位階層: なし
依存性: なし

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***]**

9.2.4.1.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合
セキュリティ機能要件の表を表 13 に置き換えよ。

表 13　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1(1)	精度の高いバイオメトリック照合- 登録ユーザに対する照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
FIA_BVR.1(2)	精度の高いバイオメトリック照合 - BS 管理者に対する照合
クラス FMT: セキュリティ管理	
FMT_MTD.1	TSF データの管理
FMT_SMF.1	管理機能の特定

本編のセキュリティ機能要件 FIA_BVR.1 を次のように変更せよ。

FIA_BVR.1(1) 精度の高いバイオメトリック照合 – 登録ユーザに対する照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検証
　　FIA_EBT.2 登録失敗率の低い生体情報登録

FIA_BVR.1.1(1) 登録ユーザに対する照合　TSF は、エラー率 FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供しなければならない。

次のセキュリティ機能要件を追加せよ。

FIA_BVR.1(2) 精度の高いバイオメトリック照合 – BS 管理者に対する照合
下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検証
　　FIA_EBT.2 登録失敗率の低い生体情報登録

FIA_BVR.1.1(2) BS 管理者に対する照合　TSF は、エラー率 FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供しなければならない。

FMT_MTD.1 TSF データの管理
下位階層: なし
依存性: ~~FMT_SMR.1 セキュリティの役割~~

FMT_SMF.1 管理機能の特定

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。

Application Note:

TSF データの典型的な例として、閾値がある。O.PROTECT_ENROLMEMT を含む場合は、TSF データとして登録ユーザの登録生体情報、その他操作として登録を割り付けよ。その他の割付は、ST 作者が実施する。

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

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***]**

9.2.4.2. セキュリティ要件根拠の変更

9.2.4.2.1. セキュリティ対策方針とセキュリティ機能要件の対応の変更

9.2.4.2.1.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

セキュリティ対策方針とセキュリティ機能要件の対応の表を、セキュリティ対策方針がO.PROTECT_ENROLMEMT を含まない場合は表 14 で、含む場合は表 15 で、置き換えよ。

表 14　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X					
FIA_EBT.1	X						
FIA_EBT.2			X				X
FIA_BVR.1			X				X
FIA_BVR.4				X			
FIA_UAU.2					X		
FMT_MTD.1						X	
FMT_SMF.1						X	

表 15 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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X						
FIA_EBT.1	X							
FIA_EBT.2			X					X
FIA_BVR.1			X					X
FIA_BVR.4				X				
FIA_UAU.2					X			
FMT_MTD.1						X	X	
FMT_SMF.1						X	X	

O.PAD_VERIFY の次の以下を追加せよ。

O.AUTH_ADMIN

このセキュリティ対策方針は、BS 管理者の認証の機構を提供する。このセキュリティ対策方針を満たすために、FIA_UAU.2 は他のアクションを実行する前に BS 管理者の認証が成功することを要求する。

O.PROTECT_ ASSETS

このセキュリティ対策方針は、TOE 内のセキュリティ関連データへのアクセスを TOE が BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求している。

O.PROTECT_ENROLMEMT を含む場合は、O.AUTH_ADMIN の次に以下を追記せよ。

O.PROTECT_ENROLMEMT

このセキュリティ対策方針は、TOE は、登録処理を BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行す

ることを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求している。

9.2.4.2.1.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合

セキュリティ対策方針とセキュリティ機能要件の対応の表を、セキュリティ対策方針が O.PROTECT_ENROLMEMT を含まない場合は表 16 で、含む場合は表 17 で、置き換えよ。

表 16　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X					
FIA_EBT.1	X						
FIA_EBT.2			X				X
FIA_BVR.1(1)			X				X
FIA_BVR.4				X			
FIA_BVR.1(2)					X		
FMT_MTD.1						X	
FMT_SMF.1						X	

表 17 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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X						
FIA_EBT.1	X							
FIA_EBT.2			X					X
FIA_BVR.1(1)			X					X
FIA_BVR.4				X				
FIA_BVR.1(2)					X			
FMT_MTD.1						X	X	
FMT_SMF.1						X	X	

O.CONTROL_FALSE_ACCEPT 及び O.CONTROL_FALSE_ACCEPT における FIA_BVR.1 を FIA_BVR.1(1)に置き換えよ。O.PAD_VERIFY の次の以下を追加せよ。

O.AUTH_ADMIN

このセキュリティ対策方針は、BS 管理者の認証の機構を提供する。このセキュリティ対策方針を満たすために、FIA_BVR.1(2)は BS 管理者のバイオメトリック照合が成功することを要求する。

O.PROTECT_ ASSETS

このセキュリティ対策方針は、TOE 内のセキュリティ関連データへのアクセスを TOE が BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求している。

O.PROTECT_ENROLMEMT を含む場合は、O.AUTH_ADMIN の次に以下を追記せよ。

O.PROTECT_ENROLMEMT

このセキュリティ対策方針は、TOE は、登録処理を BS 管理者だけに制限するとしてい

る。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求している。

9.2.4.2.2. セキュリティ機能要件の依存性の変更

9.2.4.2.2.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

SFR の依存性対応の表を以下に置き換えよ。

表 18　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FIA_UAU.2	FIA_UID.1	なし
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	なし	不要

依存性から FIA_UID.1 を削除した根拠は、BS 管理者を利用者識別する機能を運用環境が持ち、TOE は持たないからである。
依存性から FMT_SMR.1 を削除した根拠は、利用者を BS 管理者に関連付けし、BS 管理者を維持するのは、運用環境が実施するからである。

9.2.4.2.2.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合

SFR の依存性対応の表を以下に置き換えよ。

表 19　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1(1)	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FIA_BVR.1(2)	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	なし	不要

依存性から FMT_SMR.1 を削除した根拠は、利用者を BS 管理者に関連付けし、BS 管理者を維持するのは、運用環境が実施するからである。

9.3.　TOE が管理機能も BS 管理者の利用者管理機能（利用者認証機能を含む）も持つ場合

9.3.1.　概要

本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定める。

TOE の 2 次資産に対する脅威が存在し、その対策として、BS 管理者に TOE の管理的操作の実行権限が与えられ、TOE の管理的機能を使用することができる。

BS 管理者の利用者管理機能も TOE が持つ。

9.3.2.　セキュリティ課題定義の変更

9.3.2.1.　前提条件の変更

本編の A.PROTECT_ASSET を削除せよ。

9.3.2.2.　脅威の変更

T.PRESENTATION_ATTACK の後に次の脅威を追加せよ。

T.MODIFY__ASSETS

攻撃者が、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。

9.3.3.　セキュリティ対策方針の変更

9.3.3.1.　TOE のセキュリティ対策方針の変更

O.PAD_VERIFY と O.CONTROL_FALSE_REJECT の間に次のセキュリティ対策方針を追

加せよ。O.PROTECT_ENROLMEMT については、該当する場合だけ追加せよ。

O.AUTH_ADMIN

TOE は、BS 管理者を利用者認証する手段を提供しなければならない。

O.PROTECT_ENROLMEMT

TOE は、BS 管理者だけが登録処理にアクセスできるようにしなければならない。

O.PROTECT_ASSETS

TOE は、BS 管理者だけが TOE 内の 2 次資産（バイオメトリックな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。

9.3.3.2. 運用環境のセキュリティ対策方針の変更

OE.PROTECT_ASSETS を削除せよ。O.PROTECT_ENROLMEMT をセキュリティ対策方針に追加した場合は、OE.ENROL_ADMINISTERED も削除せよ。

9.3.3.3. セキュリティ対策方針根拠の変更

O.PROTECT_ENROLMEMT をセキュリティ対策方針に含まない場合は、セキュリティ対策方針根拠の表を表 20 に置き換えよ。O.PROTECT_ENROLMEMT をセキュリティ対策方針に含む場合は、セキュリティ対策方針根拠の表を表 21 に置き換えよ。

表 20　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT	OE.ENROL_ADMINISTERED	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x						x	x				
T.PRESENTATION_ATTACK	x			x					x	x				
T.MODIFY__ASSETS					x	x								
P.ENROL_ADMINISTERED								x						
P.CONTROL_FALSE_REJECT							x							
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

表 21　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x						x	x				
T.PRESENTATION_ATTACK	x			x					x	x				
T.MODIFY__ASSETS					x		x							
P.ENROL_ADMINISTERED					x	x								
P.CONTROL_FALSE_REJECT								x						
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

9.3.3.3.1. 脅威への対抗の変更

T.PRESENTATION_ATTACK への対抗の次に以下を追加せよ。

T.MODIFY_ASSETS

T.MODIFY_ASSETS では、ポータルへ権限なくアクセスする攻撃者が TOE 内の 2 次資産を改変、破壊、または収集し、悪用することを想定している。これに対しては、O.AUTH_ADMIN、O.PROTECT_ASSETS の組み合わせによって、対抗する。

O.AUTH_ADMIN によって、TOE が BS 管理者を利用者認証する手段が提供される。

O.PROTECT_ASSETS によって、上記のように TOE に利用者認証された BS 管理者だけが 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する。よって、攻撃者の TOE 内の 2 次資産であるセキュリティ関連データへのアクセスを防き、TOE 内の 2 次資産の改変・破壊・収集に対抗する。

9.3.3.3.2. 組織のセキュリティ方針の実現の変更

O.PROTECT_ENROLMEMT を含む場合は、P. ENROL_ADMINISTERED の記述を以下に置き換えよ。

P. ENROL_ADMINISTERED

P. ENROL_ADMINISTERED では、運用環境に対して、登録ユーザの生体情報登録を BS 管理者だけが実行できるようにしなければならないことを求めている。これに対しては、O.AUTH_ADMIN、O.PROTECT_ ENROLMEMT の組み合わせによって、対抗する。O.AUTH_ADMIN によって、TOE が BS 管理者を利用者認証する手段が提供される。O.PROTECT_ ENROLMEMT によって、上記のように TOE に利用者認証された BS 管理者だけが登録処理にアクセスできるようにする。よって、BS 管理者だけが TOE の登録処理にアクセスできるようにすることが実現される。

9.3.3.3.3. 前提条件への対抗の変更

A.PROTECT_ASSETS の記述を削除せよ。

9.3.4. セキュリティ要件の変更

9.3.4.1. セキュリティ機能要件の変更

9.3.4.1.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

セキュリティ機能要件の表を表 22 に置き換えよ。

表 22　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
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_UID.2	アクション前の利用者識別 - BS 管理者に対する識別
クラス FMT: セキュリティ管理	
FMT_MTD.1	TSF データの管理
FMT_SMF.1	管理機能の特定
FMT_SMR.1	セキュリティの役割

次のセキュリティ機能要件を追加せよ。

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
下位階層: FIA_UAU.1 認証のタイミング
依存性: FIA_UID.1 識別のタイミング

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。

FIA_UID.2 アクション前の利用者識別
下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.2.1 BS管理者に対する識別　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
下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
　　FMT_SMF.1 管理機能の特定

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。

Application Note:
TSF データの典型的な例として、閾値がある。O.PROTECT_ENROLMEMT を含む場合は、TSF データとして登録ユーザの登録生体情報、その他操作として登録を割り付けよ。その他の割付は、ST 作者が実施する。

FMT_SMF.1 管理機能の特定
下位階層: なし
依存性: なし

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***]**

FMT_SMR.1 セキュリティの役割
下位階層: なし
依存性: FIA_UID.1 識別のタイミング

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。

9.3.4.1.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合
セキュリティ機能要件の表を以下のものに置き換えよ。

表 23　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
FIA_BVR.3	アクション前のバイオメトリック照合による利用者認証
FIA_UID.2	アクション前の利用者識別
クラス FMT: セキュリティ管理	
FMT_MTD.1	TSF データの管理
FMT_SMF.1	管理機能の特定
FMT_SMR.1	セキュリティの役割

次のセキュリティ機能要件を追加せよ。

FIA_BVR.3 アクション前のバイオメトリック照合による利用者認証
下位階層: FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング
依存性: FIA_UID.1 識別のタイミング
　　FIA_EBT.1　登録時の生体情報の検査
　　FIA_EBT.2 登録失敗率の低い生体情報登録

FIA_BVR.3.1 TSF は、エラー率 FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し、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、その利用者に当該メカニズムで認証が成功することを要求しなければならない。

FIA_UID.2 アクション前の利用者識別
下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.2.1 BS管理者に対する識別　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
下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
　　FMT_SMF.1 管理機能の特定

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。
Application Note:
TSF データの典型的な例として、閾値がある。O.PROTECT_ENROLMEMT を含む場合は、TSF データとして登録ユーザの登録生体情報、その他操作として登録を割り付けよ。その他の割付は、ST 作者が実施する。

FMT_SMF.1 管理機能の特定
下位階層: なし
依存性: なし

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***]**

FMT_SMR.1 セキュリティの役割
下位階層: なし
依存性: FIA_UID.1 識別のタイミング

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。

9.3.4.2. セキュリティ要件根拠の変更

9.3.4.2.1. セキュリティ対策方針とセキュリティ機能要件の対応の変更

9.3.4.2.1.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

セキュリティ対策方針とセキュリティ機能要件の対応の表を、セキュリティ対策方針が O.PROTECT_ENROLMEMT を含まない場合は表 24 で、含む場合は表 25 で、置き換えよ。

表 24　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X					
FIA_EBT.1	X						
FIA_EBT.2			X				X
FIA_BVR.1			X				X
FIA_BVR.4				X			
FIA_UAU.2					X		
FIA_UID.2					X		
FMT_MTD.1						X	
FMT_SMF.1						X	
FMT_SMR.1						X	

表 25　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X						
FIA_EBT.1	X							
FIA_EBT.2			X					X
FIA_BVR.1			X					X
FIA_BVR.4				X				
FIA_UAU.2					X			
FIA_UID.2					X			
FMT_MTD.1						X	X	
FMT_SMF.1						X	X	
FMT_SMR.1						X	X	

O.PAD_VERIFY の次の以下を追加せよ。

O.AUTH_ADMIN

このセキュリティ対策方針は、BS 管理者の識別・認証の機構を提供する。このセキュリティ対策方針を満たすために、FIA_UID.2 は他のアクションを実行する前に BS 管理者の識別が成功することを要求し、FIA_UAU.2 は他のアクションを実行する前に BS 管理者の認証が成功することを要求する。

O.PROTECT_ ASSETS

このセキュリティ対策方針は、TOE 内のセキュリティ関連データへのアクセスを TOE が BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求し、FMT_SMR.1 は BS 管理者の役割の維持を要求している。

O.PROTECT_ENROLMEMT を含む場合は、O.AUTH_ADMIN の次に以下を追記せよ。

O.PROTECT_ENROLMEMT

このセキュリティ対策方針は、TOE は、登録処理を BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求し、FMT_SMR.1 は BS 管理者の役割の維持を要求している。

9.3.4.2.1.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合

セキュリティ対策方針とセキュリティ機能要件の対応の表を、セキュリティ対策方針が O.PROTECT_ENROLMEMT を含まない場合は表 26 で、含む場合は表 27 で、置き換えよ。

表 26　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X					
FIA_EBT.1	X						
FIA_EBT.2			X				X
FIA_BVR.1			X				X
FIA_BVR.4				X			
FIA_BVR.3					X		
FIA_UID.2					X		
FMT_MTD.1						X	
FMT_SMF.1						X	
FMT_SMR.1						X	

表 27　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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.AUTH_ADMIN	O.PROTECT_ENROLMEMT	O.PROTECT_ASSETS	O.CONTROL_FALSE_REJECT
FDP_RIP.1		X						
FIA_EBT.1	X							
FIA_EBT.2			X					X
FIA_BVR.1			X					X
FIA_BVR.4				X				
FIA_BVR.3					X			
FIA_UID.2					X			
FMT_MTD.1						X	X	
FMT_SMF.1						X	X	
FMT_SMR.1						X	X	

O.PAD_VERIFY の次の以下を追加せよ。

O.AUTH_ADMIN

このセキュリティ対策方針は、BS 管理者の認証の機構を提供する。このセキュリティ対策方針を満たすために、FIA_UID.2 は他のアクションを実行する前に BS 管理者の識別が成功することを要求し、FIA_BVR.3 は他のアクション前を実行する前にバイオメトリック照合による BS 管理者の利用者認証が成功することを要求する。

O.PROTECT_ ASSETS

このセキュリティ対策方針は、TOE 内のセキュリティ関連データへのアクセスを TOE が BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求し、FMT_SMR.1 は BS 管理者の役割の維持を要求している。

O.PROTECT_ENROLMEMT を含む場合は、O.AUTH_ADMIN の次に以下を追記せよ。

O.PROTECT_ENROLMEMT

このセキュリティ対策方針は、TOE は、登録処理を BS 管理者だけに制限するとしている。このセキュリティ対策方針を満たすために、FMT_SMF.1 は TSF が管理機能を実行することを要求し、FMT_MTD.1 は管理機能の対象となるデータの操作を BS 管理者に制限することを要求し、FMT_SMR.1 は BS 管理者の役割の維持を要求している。

9.3.4.2.2. セキュリティ機能要件の依存性の変更

9.3.4.2.2.1. BS 管理者に対する利用者認証機能がバイオメトリクス以外の場合

SFR の依存性対応の表を以下に置き換えよ。

表 28　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	なし	不要
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.2

9.3.4.2.2.2. BS 管理者に対する利用者認証機能がバイオメトリクスの場合

SFR の依存性対応の表を以下に置き換えよ。

表 29　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FIA_BVR.3	FIA_UID.1、FIA_EBT.1、FIA_EBT.2	FIA_UID.2、FIA_EBT.1、FIA_EBT.2
FIA_UID.2	なし	不要
FMT_MTD.1	FMT_SMR.1、FMT_SMF.1	FMT_SMR.1、FMT_SMF.1
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.2

9.4.　TOE が登録生体情報取得機能を持つ場合

9.4.1.　概要

本編に加えて、以下のような場合に対するセキュリティ機能要件を定める。

利用者が入力した ID を基に TOE が格納機能から登録生体情報を取得してバイオメトリック照合による利用者認証を実行する。

9.4.2.　セキュリティ要件の変更

9.4.2.1.　セキュリティ機能要件の変更

セキュリティ機能要件の表を以下のものに置き換えよ。

表 30　セキュリティ機能要件

クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.3	アクション前のバイオメトリック照合による利用者認証
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合
FIA_UID.2	アクション前の利用者識別 - 許可された利用者の識別

FIA_BVR.1 を次のセキュリティ機能要件で置き換えよ。

FIA_BVR.3 アクション前のバイオメトリック照合による利用者認証
下位階層: FIA_BVR.2 バイオメトリック照合による利用者認証のタイミング
依存性: FIA_UID.1 識別のタイミング
　　FIA_EBT.1　登録時の生体情報の検査
　　FIA_EBT.2 登録失敗率の低い生体情報登録

FIA_BVR.3.1 TSF は、エラー率 FAR[割付：*X*]以下、FRR[割付：*Y*]以下で動作するバイオメトリック照合メカニズムを提供し、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、その利用者に当該メカニズムで認証が成功することを要求しなければならない。

次のセキュリティ機能要件を追加せよ。

FIA_UID.2 アクション前の利用者識別
下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.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、各利用者に識別が成功することを要求しなければならない。

Application Note：
個人が使用するスマートフォンなどのモバイルデバイスで ID が固定的に使われる場合は、当該個人の識別が成功しているものとみなして良い。

9.4.2.2. セキュリティ要件根拠の変更

9.4.2.2.1. セキュリティ対策方針とセキュリティ機能要件の対応の変更

セキュリティ対策方針とセキュリティ機能要件の対応の表を以下で置き換えよ。

表 31　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.PAD_ENROL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL
FDP_RIP.1					X
FIA_EBT.1	X				
FIA_EBT.2		X		X	
FIA_BVR.3		X		X	
FIA_BVR.4			X		
FIA_UID.2		X		X	

O.CONTROL_FALSE_ACCEPT と O.CONTROL_FALSE_REJECT を、それぞれ以下で置き換えよ。

O.CONTROL_FALSE_ACCEPT

このセキュリティ対策方針 O.CONTROL_FALSE_ACCEPT は、TOE が他人受入率(FAR)の基準を満たすことを規定する。このセキュリティ対策方針を満たすために、FIA_UID.2 は他のアクションを実行する前に識別が成功することを要求し、FIA_BVR.3 はエラー率 FAR[割付 : *X*]以下でバイオメトリック照合による利用者認証が成功することを要求する。このエラー率 X は、ST で具体的に規定される。しかし、FAR を良く見せるために、照合され易い生体情報だけを登録することがあってはならない。FIA_EBT.2 はこのことを要求する。

O.CONTROL_FALSE_REJECT

このセキュリティ対策方針 O.CONTROL_FALSE_REJECT は、TOE が本人拒否率(FRR)の基準を満たすことを規定する。このセキュリティ対策方針を満たすために、FIA_BVR.3 は、エラー率 FRR[割付：*Y*]以下でバイオメトリック照合による利用者認証が成功することを要求する。このエラー率 Y は、ST で具体的に規定される。しかし、FRR を良く見せるために、照合され易い生体情報だけを登録することがあってはならない。FIA_EBT.2 はこのことを要求する。

9.4.2.2.2. セキュリティ機能要件の依存性の変更

SFR の依存性対応の表を以下に置き換えよ。

表 32　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.3	FIA_UID.1、FIA_EBT.1、FIA_EBT.2	FIA_UID.2、FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1
FIA_UID.2	なし	不要

9.5.　TOE のコンポーネントが暗号化機能を持つ場合

9.5.1.　概要

本編に加えて、以下のような場合に対する前提条件・脅威・セキュリティ対策方針及びセキュリティ機能要件を定める。

TOE 間のデータ授受に脅威が存在し、その対策として、TOE のコンポーネントが TOE の他のコンポーネントと授受するデータを暗号化する。

Application Note：

以下の記述はデータ採取機能と特徴抽出機能の間としたが、TOE に合わせて、適切に変更せよ。

9.5.2.　セキュリティ課題定義の変更

9.5.2.1. 前提条件の変更

本編の A.COMMUNICATION を以下に置き換えよ。

A.COMMUNICATION

TOE と運用環境のバイオメトリクスの処理に関わる機能との間の通信は、保護されている。

9.5.2.2. 脅威の変更

次の脅威を追加せよ。

T.COMMUNICATION

攻撃者が、データ採取機能と特徴抽出機能の間の通信を盗聴し、登録ユーザの生体情報を搾取するなどして、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。

Application Note:

上記では、 データ採取機能と特徴抽出機能の間としたが、TOE に応じて、データ採取機能と PAD 特徴抽出機能の間とする、または加える等せよ。

9.5.3. セキュリティ対策方針の変更

9.5.3.1. TOE のセキュリティ対策方針の変更

O.CLEAR_RESIDUAL の後に次のセキュリティ対策方針を追加せよ。

O.PROTECT_COMMUNICATION

TOE は、データ採取機能と特徴抽出機能の間の通信を保護しなければならない。

9.5.3.2. 運用環境のセキュリティ対策方針の変更

本編の OE.COMMUNICATION を以下に置き換えよ。

OE.COMMUNICATION

TOE と運用環境のバイオメトリクスの処理に関わる機能との間の通信は、保護されていなければならない。

9.5.3.3. セキュリティ対策方針根拠の変更

セキュリティ対策方針根拠の表を以下のものに置き換えよ。

表 33　セキュリティ対策方針根拠

	O.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	O.PROTECT_COMMUNICATION	OE.ENROL_ADMINISTERED	OE.ACCESS_CONTROL	OE.LIMIT_NUM_TRIAL	OE.PROTECT_ASSETS	OE.PROTECT_RESIDUAL_ENVIRONMENT	OE.ADMINISTRATION	OE.COMMUNICATION	OE.ENVIRONMENT
T.CASUAL_ATTACK			x					x	x					
T.PRESENTATION_ATTACK	x			x				x	x					
T.MODIFY__ASSETS										x				
T.COMMUNICATION						x								
P.ENROL_ADMINISTERED							x							
P.CONTROL_FALSE_REJECT					x									
P.RESIDUAL		x									x			
A.ADMINISTRATION												x		
A.COMMUNICATION													x	
A.ENVIRONMENT														x

9.5.3.3.1. 脅威への対抗の変更

T.PRESENTATION_ATTACK への対抗の次に以下を追加せよ。

T.COMMUNICATION

T.COMMUNICATION では、攻撃者が、データ採取機能と特徴抽出機能の間の通信を盗聴し、登録ユーザの生体情報を搾取するなどして、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ことを想定している。これに対しては、O.PROTECT_COMMUNICATION によって、対抗する。

O.PROTECT_COMMUNICATION によって、TOE は、データ採取機能と特徴抽出機能の間の通信を保護することで対抗する。

9.5.4. セキュリティ要件の変更

9.5.4.1. セキュリティ機能要件の変更

セキュリティ機能要件の表を以下のものに置き換えよ。

表 34　セキュリティ機能要件

クラス FCS: 暗号サポート	
FCS_CKM.1	暗号鍵生成
FCS_CKM.4	暗号鍵破棄
FCS_COP.1	暗号操作
クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合

次のセキュリティ機能要件を追加せよ。

FCS_CKM.1 暗号鍵生成
下位階層: なし
依存性: [~~FCS_CKM.2 暗号鍵配付、または~~ FCS_COP.1 暗号操作]
　　FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。

FCS_CKM.4 暗号鍵破棄
下位階層: なし
依存性: [~~FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~ FCS_CKM.1 暗号鍵生成]

FCS_CKM.4.1 TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵破棄方法[割付: *暗号鍵破棄方法*]に従って、暗号鍵を破棄しなければならない。

FCS_COP.1 暗号操作
下位階層: なし
依存性: [~~FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2~~

~~セキュリティ属性を伴う利用者データのインポート、または~~ FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 TSF は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。

Application Note:

暗号化操作のリストへは、 T.COMMUNICATION に対応して、データ採取機能から特徴抽出機能へ送る生体情報の保護、データ採取機能から PAD 特徴抽出機能へ送る生体情報の保護、等を割り当てよ。

TOE が暗号鍵配付機能を持つ場合は、表 34 を表 35 で置き換えて、上記の FCS_CKM.1 の後に以下のセキュリティ機能要件 FCS_CKM.2 を追加せよ。

表 35　セキュリティ機能要件

クラス FCS: 暗号サポート	
FCS_CKM.1	暗号鍵生成
FCS_CKM.2	暗号鍵配付
FCS_CKM.4	暗号鍵破棄
FCS_COP.1	暗号操作
クラス FDP: 利用者データ保護	
FDP_RIP.1	サブセット残存情報保護
クラス FIA: 識別と認証	
FIA_EBT.1	登録時の生体情報の検査
FIA_EBT.2	失敗率の低い生体情報登録
FIA_BVR.1	精度の高いバイオメトリック照合
FIA_BVR.4	偽造生体等を受け入れないバイオメトリック照合

FCS_CKM.2 暗号鍵配付

下位階層: なし

依存性: [~~FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~ FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FCS_CKM.2.1 TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵配付方法[割付: *暗号鍵配付方法*]に従って、暗号鍵を配付しなければならない。

9.5.4.2. セキュリティ要件根拠の変更

9.5.4.2.1. セキュリティ対策方針とセキュリティ機能要件の対応の変更

セキュリティ対策方針とセキュリティ機能要件の対応の表を表 36 で置き換えよ。TOE が暗号鍵配付機能を持つ場合は、表 37 で置き換えよ。

表 36　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.PAD_ENROL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	O.CLEAR_RESIDUAL	O.PROTECT_COMMUNICATION
FCS_CKM.1						X
FCS_CKM.4						X
FCS_COP.1						X
FDP_RIP.1					X	
FIA_EBT.1	X					
FIA_EBT.2		X		X		
FIA_BVR.1		X		X		
FIA_BVR.4			X			

表 37 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.PAD_ENROL	O.CLEAR_RESIDUAL	O.CONTROL_FALSE_ACCEPT	O.PAD_VERIFY	O.CONTROL_FALSE_REJECT	O.PROTECT_COMMUNICATION
FCS_CKM.1						X
FCS_CKM.2						X
FCS_CKM.4						X
FCS_COP.1						X
FDP_RIP.1		X				
FIA_EBT.1	X					
FIA_EBT.2			X		X	
FIA_BVR.1			X		X	
FIA_BVR.4				X		

O.CONTROL_FALSE_REJECT の次に以下を追加せよ。

O.PROTECT_COMMUNICATION

このセキュリティ対策方針は、TOE のデータ採取機能と特徴抽出機能の間の通信を保護するとしている。このセキュリティ対策方針を満たすために、FCS_CKM.1 は適切なアルゴリズムの適切な長さの暗号鍵の生成を、FCS_COP.1 は適切なアルゴリズムを使った暗号化操作を、FCS_CKM.4 は適切な方法による暗号鍵の破棄を、それぞれ要求している。

TOE が暗号鍵配付機能を持つ場合は、O. CONTROL_FALSE_REJECT の次に、上記ではなく、以下を追加せよ。

O.PROTECT_COMMUNICATION

このセキュリティ対策方針は、TOE のデータ採取機能と特徴抽出機能の間の通信を保護するとしている。このセキュリティ対策方針を満たすために、FCS_CKM.1 は適切なアルゴリズムの適切な長さの暗号鍵の生成を、FCS_CKM.2 は適切な方法による暗号鍵配付を、FCS_COP.1 は適切なアルゴリズムを使った暗号化操作を、FCS_CKM.4 は適切な方法による暗号鍵の破棄を、それぞれ要求している。

9.5.4.2.2. セキュリティ機能要件の依存性の変更

SFR の依存性対応の表を表 38 に置き換えよ。TOE が暗号鍵配付機能を持つ場合は、表 39 で置き換えよ。

表 38　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1]、FCS_CKM.4	FCS_COP.1、FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FCS_CKM.4	FCS_CKM.1、FCS_CKM.4
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1

表 39　SFR の依存性対応

SFR	規格における依存性の要求	本 PP 内での対応
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1]、FCS_CKM.4	FCS_COP.1、FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1] 、FCS_CKM.4	FCS_CKM.1、FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]、FCS_CKM.4	FCS_CKM.1、FCS_CKM.4
FDP_RIP.1	なし	不要
FIA_EBT.1	なし	不要
FIA_EBT.2	なし	不要
FIA_BVR.1	FIA_EBT.1、FIA_EBT.2	FIA_EBT.1、FIA_EBT.2
FIA_BVR.4	FIA_EBT.1	FIA_EBT.1

付録３　精度評価のための社内試験エビデンス素案

この付録の見方を以下に示す。背景に色が付いた部分は本付録を読みやすくするためのものであり、本素案がサポート文書として完成するまでに削除する予定である。
背景色があるものは以下の意味を持つ。
①背景色が水色のものは、ISO/IEC 19795-1 及び ISO/IEC 19795-2 の該当する箇所として章や節番号を付記したもの、あるいは、補足説明として付記したものである。
②背景色が黄色のものは、各項目が必須項目であるか（shall）、あるいは、推奨項目であるか（should）を区別するために付記したものである。

以下、付録本文：

1. 社内試験エビデンス

1.1 概要（ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当項目なし）

バイオメトリック登録及び照合のプロテクションプロファイルに基づいてベンダーが評価機関に提出するバイオメトリック性能試験のための社内試験のエビデンスは、バイオメトリック性能試験の国際規格である ISO/IEC 19795-1:2006 および ISO/IEC 19795-2:2007 に記載されている性能試験における重要項目に基づき作成することとする。エビデンスは以下に示す 2 種類の文書により構成されるものとする。ただし、このエビデンスは上記規格書に対する準拠性を満足することを保証するものではない。

(1) バイオメトリック性能試験計画書：性能試験実施前に作成される計画書であり、試験準備・実施手順・分析方法などについて記載した文書である。（以下、性能試験計画書と略す。）
(2) バイオメトリック性能試験報告書：性能試験計画書に基づいて実行された精度評価の報告書であり、試験準備・実施手順・分析などの結果について記載した文書である。（以下、性能試験報告書と略す。）

注）ISO/IEC 19795-1:2006 において性能試験における報告項目と本サポート文書における報告項目の対応を別紙-1 に示す。

1.2 記載項目概要（ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当項目なし）

性能試験計画書、性能試験報告書それぞれに記載すべき項目の概要を以下に示す。なお、実際に評価機関に提出する社内試験のエビデンス（バイオメトリック性能試験計画書、バイオメトリック性能試験報告書）の名称やフォーマットは、本サポート文書に従う必要はない。性能試験計画書と性能試験報告書が一つの文書にマージされていても構わないし、各々が複数の文書に分割されていても構わない。また下記の表の順番通りに記載する必要も無い。しかしながら本サポート文書で記載が求められる内容に関しては、エビデンスのどこかには記載されている必要がある。また、記載できないものがある場合は、何故記載しなくてもよいのか、開発者からその合理的な根拠を評価機関より求められるケースがあることに留意すべきである。

(1) 性能試験計画書（ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当箇所あり。各節を参照の事）

表-1 に、性能試験計画書に記載すべき項目と各項目の概要を示す。

表-1 性能試験計画書の記載項目

No	項目	説明
1	一般的事項	試験対象製品（製品名、型番など）、および、実施する性能試験に関する一般的事項を記載する。
2	システム情報	試験対象製品および試験システムの性能試験に関わる考慮事項を記載する。
3	想定アプリケーション	試験対象製品が想定するアプリケーションについて記載する。
4	影響要因の制御	試験対象製品に関する試験者による制御要因（被験者の年齢分布、性別分布、温度など）を記載する。
5	被験者選定	被験者選定方法など被験者を集めるための計画を記載する。
6	被験者管理	選定した被験者への試験内容の説明、習熟度確認、順化など被験者の管理方法について記載する。
7	データ収集誤りの回避	データ収集時に考えられる誤りの回避策を記載する。
8	生体情報登録	生体情報登録の性能試験（FTE の試験）の試験方法・手順を記載する。
9	本人トランザクション	本人トランザクションの性能試験（FRR の試験）の試験方法・手順を記載する。
10	偽者トランザクション	偽者トランザクションの性能試験（FAR の試験）の試験方法・手順を記載する。
11	記録管理	収集された情報の記録管理方法を記載する。

(2) 性能試験報告書（ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当箇所あり。各節を参照の事）

表-2 に、性能試験報告書に記載すべき項目と各項目の内容を示す。

表-2 性能試験報告書の記載項目

No	項目	説明
1	一般的事項	試験対象製品（製品名、型番など）、および、実施した性能試験に関する一般的事項を記載する。
2	システム情報	試験対象製品、および、試験システムの性能試験に関わる考慮事項に関する実施結果を記載する。
3	想定アプリケーション	試験対象製品が想定するアプリケーションについて記載する。
4	影響要因の制御	試験対象製品に関する試験者による制御要因（被験者の年齢分布、性別分布、温度など）に関する制御結果を記載する。
5	被験者選定	被験者の選定結果を記載する。
6	被験者管理	選定した被験者への試験内容の説明、習熟度確認、順化など被験者の管理結果について記載する。
7	データ収集誤りの回避	データ収集時に発生した誤りの回避結果を記載する。
8	生体情報登録	生体情報登録の性能試験（FTE の試験）の結果を記載する。
9	本人トランザクション	本人トランザクションの性能試験（FRR の試験）の結果を記載する。
10	偽者トランザクション	偽者トランザクションの性能試験（FAR の試験）の結果を記載する。
11	記録管理	収集された情報の記録管理結果を記載する。

1.3 性能試験計画書の記載事項

1.3.1 一般的事項(19795-1 6.1)

試験システムや性能尺度など、実施する性能試験に関する一般的な情報を記載する。内容は以下のとおりである。

(1) 試験システム情報(19795-1 6.1 (a))

製品を特定する情報として以下の項目を記述する[shall]。

①製品情報：製品名称、バージョン、製品コードなど。なおここで記載された製品情報は、セキュリティターゲットに記載された製品情報と一貫している必要がある。

②生体認証方法：モダリティ、対象となる身体部分、照合方式（照合機能をサポートしていること）

③試験システム：試験ツールの名称、機能、入出力情報、動作環境など。

(2) 測定する性能尺度(19795-1 6.1 (b))

測定する性能尺度が、評価対象製品のセキュリティターゲットのセキュリティ機能要件に記載されている FTE・FAR・FRR の 3 つであることを記述する[shall]。

(3) 性能試験方法の決定(19795-1 6.1 (c))

実施する性能試験の方法が、テクノロジ評価・シナリオ評価のいずれか一方あるいは両方であることを記述する[shall]。両方である場合、性能試験方法の種類と上記(2)の測定する性能尺度との対応付けをあわせて記述する[shall]。

(4) 予定する試験実施者（監督者）19795-2 8.1

試験実施者の氏名、所属を記述するとともに、ベンダーとの利害関係の有無（独立・非独立）について説明を記載する[shall]。社内試験の試験実施者は通常のケースではベンダーの従業員であることが多いと思われるが、中立的な評価組織によって実行される場合もある。

(5) 試験予定期間 (ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当なし) [shall]

(6) 試験予定場所 (ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当なし) [shall]

1.3.2 システム情報(19795-1 6.3)

試験結果の分析や再現に関わる性能試験ツールが持つ機能や、対象製品の機能の中で性能試験の方法や手順に関わる機能の有無など、試験システムに関する試験実施にあたっての考慮事項を記載する。内容は以下のとおりである。

(1) トランザクション情報保存の方法と内容(19795-1 6.3(a))

試験実施時の登録のためのテンプレート生成トランザクションや本人トランザクションあるいは偽者トランザクションの、ログの記録方法を記述する。記録方法とは、ツールなどを用いて機械的に記録する方法か、あるいは手操作で記録する方法のいずれかである [shall]。あわせて、記録する情報の中で性能に関わる情報の項目とその内容の説明を記載する[shall]。

(2) 画像または特徴の保存の方法と内容(19795-1 6.3(b))

試験実施時のバイオメトリック画像またはバイオメトリック特徴の記憶媒体への保存有無を記述する[shall]。有の場合、保存される情報の項目とその内容について説明を記載する[shall]。

(3) 照合時の出力情報の決定(19795-1 6.3(c))

試験システムが照合スコアを出力するか、照合判定結果（照合成功・照合失敗）を出力するかを記述する[shall]。照合スコア出力の場合、スコアの説明を記載する（最小値・最大値など）[shall]。同様に、登録においてテンプレート品質スコアを出力するか、テンプレート生成判定結果（テンプレート生成成功・失敗）を出力するかを記述する[shall]。テンプレート品質スコア出力を出力する場合、スコアの説明を記載する[shall]。

(4) SDK（ソフトウェア開発キット）使用有無(19795-1 6.3(d))

試験実施時の SDK の使用有無を記述する[shall]。有の場合、SDK を特定する情報、および、性能試験における用途の説明を記載する[shall]。

(5) 試験のためのシステム修正有無(19795-1 6.3(e))

性能試験実施を目的とした製品の修正有無を記述する[shall]。有の場合、システムの性能特性を変えない理由について説明を記載する[shall]。（例：修正箇所が照合判定処理の後にあるため、性能試験結果には影響しない。）

(6) 他のテンプレートによる影響(19795-1 6.3(f))

試験対象システムのテンプレートが他のテンプレートの存在により影響を受けるか否かについて記述する[shall]影響を受ける場合、他のテンプレートによる影響内容、および、この機能に基づいた性能試験計画の説明を記載する[shall]。

注他のテンプレートとは本人以外の、あるいは、本人の他の身体部分のテンプレートを指す。

(7) テンプレート学習の方法と内容(19795-1 6.3(g))

試験対象システムのテンプレート学習の有無について記述する[shall]（テンプレート学習とは、複数の

本人同士の照合トランザクションの実施結果を考慮してテンプレートの内容を更新する機能である)。有の場合、学習機能、および、この機能に基づいた性能試験計画の説明を記載する[shall]。

(8) 閾値の定義(19795-1 6.3(h))

利用者または運用者が設定可能な閾値の種類（判定閾値、画像品質閾値、など）を記述する[shall]。あわせて、試験で使用する閾値の説明を記載する[shall]。

(9) データベース規模への依存性(19795-1 6.3(k))

データベース規模への依存性の有無について記述する[shall]（データベース規模への依存性が有るとは、登録している被験者のテンプレート数の違いにより性能に影響が出る場合である)。有の場合、依存性の内容、および、この機能に基づいた性能試験計画の説明を記載する[shall]。

(10) 性能試験方法の決定 **19795-2 6.1.4**

試験システムによる試験方法が製品の実装方法から独立していることについて説明を記載する [shall]。独立しているとは、管理者あるいは利用者向説明資料に記載されていない実装上の特性を考慮した試験が、性能試験計画の中に盛り込まれていないことを意味する。

(11) システム詳細 **19795-2 7.4.2.2**

試験システムの詳細として以下の情報を記述する[shall]。

① 取得装置：製造者，モデル，バージョン，可能な場合はファームウェア。

② 取得装置の中心的取得構成要素が，指紋センサーの周辺装置への組込みの場合など，サードパーティの装置内に統合される場合，中心的取得構成要素の製造者，モデル，バージョン，リビジョン

③ 比較アルゴリズムについて：プロバイダ，バージョン，改訂番号

④ システムが試験されたプラットフォームの仕様。プラットフォーム，OS，処理能力，メモリ，製造者，データベースのタイプ，データベースのサイズ，モデルなど

1.3.3 想定アプリケーション **19795-2 7.1.1.1**

ベンダーの評価タイプがシナリオ評価の場合もテクノロジ評価の場合も、評価システムが想定するアプリケーションについて説明を記載する[shall]。説明には、汎用・特定用途の別、想定アプリケーションの機能概要、使用する生体認証技術などを含める。

1.3.4 影響要因の制御 **19795-2 6.2.5 はこの節に含まれる(19795-1 6.4)**

シナリオ評価における影響要因の考慮、あるいは、テクノロジ評価におけるデータ収集中の環境条件について記載する。内容は以下のとおりである。以下の内容の記載ができない場合、その理由について説明を記載する。

(1) 母集団の人口統計(19795-1 C.2.1)

①年齢層：任意の年齢単位（1 年、5 年、10 年など）で区切った年齢層の分布を率で記述する[shall]。

②性別：男女（生物学的性別）の分布を率で記述する[shall]。

③民族的出身（海外市場が対象の場合）：民族的出身に応じた分類を定義した上で、分類毎の分布を率で記述する[shall]。

(2) 姿勢・位置決め(19795-3 Table 7 Posture)

習熟度が低の被験者が含まれる場合、試験システムの生体情報取得装置の仕様に基づいた姿勢や位置決めに関する被験者の分布情報の収集方法の説明を記載する[shall]（カメラの正面や角度など・ずれ及び回転・カメラまでの距離・高すぎ低すぎなど)。習熟度が低の被験者が含まれない場合、本項目は

記載する必要はない。

(3) 屋内・屋外 19795-2 6.2.10, 7.1.1.3

システムの使用環境が屋内か屋外かの別。屋内の場合は施設のタイプの説明を記載する[shall]。屋外の場合は性能に関わる条件の説明を記載する[shall]。

(4) 温度(19795-3 Table 7 Temperature)

試験システムが想定する温度条件の説明を記載する[shall]。屋内環境の場合の最低限の記述例は「空調が効いた室内環境であり、何℃～何℃の温度環境で評価を実施する」である。

(5) データの使用順序 19795-2 6.1.8

FTE・FRR・FAR それぞれの試験において使用するバイオメトリックデータの順序（テクノロジ評価の場合）あるいは被験者の順序（シナリオ評価の場合）が、対象アプリケーションにおいて適切であることについて説明を記載する[shall]。具体的には、ひとりの被験者が複数のトランザクションを実行する場合、それぞれのトランザクション処理が時間的に分離されていること（オーバーラップしていないこと）や、テンプレート作成トランザクションを実行した後で、本人トランザクションや偽者トランザクションを実行することなど、データの順序に関する説明を記載する。

(6) 生体情報登録~照合間の経過時間(19795-3 Table 7 Time interval)

試験システムを利用する母集団の想定される登録～照合までの経過時間に関する情報（最短時間あるいは平均時間）を記述する[shall]。対象アプリケーションの習熟度が高でない場合、異なる日の測定を推奨する。

(7) 利用者の習熟度(直接関連しないが 19795-1 C.2.2 に従えば、level of user familiarity かもしくは habituation)

習熟度を表 3 の 3 段階に分け、母集団として想定される分布を率で示す[shall]。

表-3 習熟度の分類と定義

No	分類	定義
1	低	正しい提示方法を理解していない。 試行に失敗しても、提示方法の誤りかどうか確実に判断できない。以降の試行で、提示方法をどのように修正すべきか確実に判断できない。
2	中	正しい提示方法を理解している。 提示方法の誤りにより試行に失敗することがあるが、以降の入力試行では正しい提示方法に修正していくことができる。
3	高	正しい提示方法をよく理解している。 ほとんどの場合、正しい方法で提示できる。 提示方法の誤りにより試行に失敗することがあるが、以降の入力試行では正しい提示方法に修正していくことができる。

1.3.5 被験者選定(19795-1 6.5)

性能試験実施にあたり募集を計画する被験者の選定方法や被験者の振る舞いについての項目を記載する。内容は以下のとおりである。

(1) 被験者の人数および選定方法 19795-2 7.2.1 の内容を含む

試験の実施にあたり募集を計画する被験者の人数、身体部分の数、サンプル数を記述する[shall]とともに、選定方法の説明を記載する[shall]。過去に開発や試験のために収集され蓄積されたテンプレートや

照合用バイオメトリックデータの利用が試験計画に含まれる場合、蓄積済みデータの被験者数、身体部分の数、サンプル数および選定方法の説明もあわせて記載する[shall]。

(2) 人工的に生成したサンプルまたは特徴データの使用有無(19795-1 6.5.1)

テクノロジ評価において人工的に生成したデータの使用有無を記述する[shall]。有の場合、計画している人工データが想定する被験者数、身体部分の数、サンプル数、および、人工データを用いる妥当性の説明を記載する[shall]。

(3) 被験者または取得データの汚染度合い **19795-2 6.2.7**

試験に参加した被験者や取得されたバイオメトリックデータの汚染の度合いに関する以下の情報を記述する[shall]。

① 取得されたバイオメトリックデータの試験実施者による所有権保持の有無（過去に保持していた場合も含む）

② 過去に試験・調整に使用したバイオメトリックデータの再利用の有無

③ 過去に試験・調整に参加した被験者の再参加の有無

1.3.6 被験者管理

被験者に対する試験前後の説明や習熟度確認や順化など、被験者に対する管理についての項目を記載する。内容は以下のとおりである。

(1) 被験者説明 **19795-2 7.1.2.1**

登録作業や本人あるいは偽者トランザクションの実行前後、あるいは、バイオメトリックデータ取得の実行前後で被験者に対して行う各種説明内容について説明を記載する[shall]。

(2) 習熟度の確認 **19795-2 7.1.2.2**

登録作業や本人あるいは偽者トランザクションの実行前、あるいは、バイオメトリックデータ取得の実行前に行う被験者の習熟度確認の方法について説明を記載する[shall]。被験者への練習によって習熟度を確認する場合、説明の中には各被験者が行う練習の一貫性の確保方法や、練習のために用意されたツールの記載などが含まれるべきである[should]。

(3) 順化 **19795-2 7.1.2.5**

登録作業や本人あるいは偽者トランザクションの実行前、あるいは、バイオメトリックデータ取得の実行前に被験者が屋外環境から室内環境に入った直後の急激な温度変化などの影響を受けないようにするための、被験者の順化方法について説明を記載する[shall]。

(4) 管理プロセス

被験者の管理プロセスとして以下の項目について説明を記載する[shall]。

①被験者の初期登録方法 **19795-2 7.2.4**

② 被験者の登録の一意性を保障する方法 **19795-2 7.2.4**

③ 被験者を識別するために付与した識別子のタイプ **19795-2 6.2.4**

④ 収集された個人データの量およびタイプ **19795-2 7.2.4**

⑤ シナリオ評価における識別子の提示方法（トークン又は標章など） **19795-2 7.2.4**

(5) 少数の代表的でない利用者による偏りの防止 （19795-1 7.4.5）

同一被験者が一度の社内試験に複数回参加することはないことに関する説明を記載する[shall]（例：「一部の被験者のみ、照合を規定回数以上実施するようなことはない」）

1.3.7 データ収集誤りの回避(19795-1 7.1)

性能試験実施中に発生しうる人的要因エラーを含んだデータ収集誤りを回避するための方法および、データ収集誤りが発生した場合の除外基準について記載する。内容は以下のとおりである。

(1) データ収集誤り回避方法(19795-1 7.1.1、7.1.4)

データ収集誤りの回避方法の概要の説明を記載する[shall]。回避方法として記載すべき項目には、データ収集ソフトウェアによるキー入力作業の低減、複数のデータ収集要員による二重チェック、試験に精通した監督者の配置、サンプルの誤取得に関する客観的な基準の準備、二重登録防止のための ID 管理およびその工程、などがある。

(2) データ除外基準(19795-1 7.1.6)

バイオメトリック登録または照合時のデータ除外の基準の説明を記載する[shall]。

1.3.8 生体情報登録(19795-1 7.3)

生体情報登録に関する性能試験として FTE（Failure-To-Enrol）を測定するための計画を記載する。内容は以下のとおりである。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**(ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当なし)

オンラインまたはオフラインのいずれの方法で実施するかを記述する[shall]。オンラインとは、試験において被験者が生体認証装置を用いてバイオメトリックデータを取得する過程を含んだものである。オフラインとは、被験者によるバイオメトリックデータの取得を含まず、あらかじめ記憶媒体に蓄積してあったバイオメトリックデータを用いて評価を実施するものである。

(2) 生体情報登録方針 **19795-2 7.1.3.1**

生体情報登録失敗率を算出するための生体情報登録の処理方針に関する以下の内容について説明を記載する[shall]。

①登録失敗率算出のための品質スコアの閾値

②テンプレート生成トランザクションの処理内容（フローチャートなど）

③テンプレート生成トランザクションの最短・最長時間

④テンプレート生成トランザクションの最小・最大アテンプト回数

⑤テンプレート生成トランザクションの最小・最大プレゼンテーション回数

⑥テンプレート生成のための最小必要・最大許容サンプル数 **19795、-2 6.3.1**

注 1）あらかじめ蓄積されたバイオメトリックデータを用いてテンプレート生成トランザクションをシミュレートして FTE を算出する場合も、上記と同等の内容の説明を記載する。トランザクションのシミュレートに関する説明を別紙-2 に示す。

注 2) 人単位で算出し（身体部分単位ではない）、ひとりの被験者が登録に参加できるのは 1 回とする（二重登録は許されない）。

注 3）ひとりの被験者のひとつの身体部分のテンプレート生成トランザクション数はそれぞれ 1 回とする。

注 4）テンプレート生成トランザクションはベンダーの定義を用いる。

(3) 登録の一般条件下での実行（19795-1 7.3.2.2）

テンプレート生成トランザクション実行時、あるいは、オフライン試験のためのデータ収集時の制御要

因がすべての被験者で一様になるか、一様にならない場合被験者全員で無作為に変わるかを記述する[shall]。それぞれの場合において、制御要因の制御の方法の説明を記載する[shall]。本項における制御要因は、温度である。

(4) 監督者の介入基準（19795-1 7.3.2.3）

生体情報登録における監督者の介入基準の説明を記載する[shall]。

(5) 登録失敗者に対する助言又は救済策 **19795-2 6.2.6, 7.1.2.4 を追加**（19795-1 7.3.3.1）

テンプレート生成トランザクション実行時、あるいは、オフライン試験のためのデータ収集時に被験者が何らかのエラーを発生した際の再登録試行前の助言や救済策について以下の情報を含めて説明を記載する[shall]。

①アプリケーションと一貫性があること

②以下のガイダンス方針の説明を記載すること

- ガイダンスが許可されるポイント又はガイダンスが要求されるポイント
- 運用責任者が被験者に提供することになっている固有のガイダンス
- 運用責任者の裁量によって被験者にガイダンスを与える局面

(6) 登録失敗の定義と失敗原因（19795-1 7.3.3.2）

利用者または運用者から見た登録失敗の定義、および、登録失敗原因（生体特徴をもっていない、サンプルが取得できない、練習入力試行で照合できない、など）の説明を記載する[shall]。

(7) 重みづけ（19795-1 8.1.2）

登録失敗率において何らかの重みづけ（被験者集団の分布、実行されたトランザクション回数の分布など）を行う場合、その方法の説明を記載する[shall]。

(8) 試験前のデータ処理 **19795-2 6.2.11**

保存されたテンプレートのデータ処理内容について説明を記載する[shall]。原画像から特徴量データに変換されている場合はその処理の概要や、大よそのデータサイズなどについて記載する[shall]。

1.3.9 本人トランザクション（19795-1 7.4）

本人の照合に関する性能試験として誤拒否率 FRR（False Reject Rate）を測定するための計画を記載する。内容は以下のとおりである。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**

オンラインまたはオフラインのいずれの方法で実施するかを記述する[shall]。

(2) 誤拒否率算出のための照合処理方針 **19795-2 7.1.3.2, 7.1.5**

誤拒否率を算出するための本人トランザクションの処理方針に関する以下の内容について説明を記載する[shall]。

①拒否率算出のための照合スコアと品質スコアの閾値

②本人トランザクションの処理内容（フローチャートなど）

③本人トランザクションの最短・最長時間

④本人トランザクションの最小・最大アテンプト回数

⑤本人トランザクションの最小・最大プレゼンテーション回数

⑥本人トランザクションのための最低必要・最大許容サンプル数 **19795-2 6.3.1 を照合に適用**

注 1）あらかじめ蓄積されたバイオメトリックデータを用いて本人トランザクションをシミュレートし

て FRR を算出する場合も、上記と同等の内容について説明を記載する。トランザクションのシミュレートに関する説明を別紙-2 に示す。

注 2）身体部分単位で算出し、ひとりの被験者のひとつの身体部分の本人トランザクション数は 1 回とする。

注 3）本人トランザクションはベンダーの定義を用いる。

(3) 収集過程の一般条件下での実行（19795-1 7.4.2）

本人トランザクション実行時、あるいは、オフライン試験のためのデータ収集時の制御要因がすべての被験者で一様になるか、一様にならない場合被験者全員で無作為に変動させる方法を記述する[shall]。それぞれの場合において、制御要因の制御の方法について説明を記載する[shall]。本項における制御要因は、温度である。

(4) 監督者の介入基準（19795-1 7.3.2.3）

本人トランザクション実行時、あるいは、オフライン試験のためのデータ収集時の監督者の介入基準の詳細について説明を記載する[shall]。

(5) 本人照合失敗者に対する助言又は救済策 **19795-2 6.2.6, 7.1.2.4 を追加**（19795-1 7.3.3.1）

本人トランザクション実行時、あるいは、オフライン試験のためのデータ収集時にエラーが発生した際の再試行前の助言や救済策を以下の情報を含めて説明を記載する[shall]。

①アプリケーションと一貫性があること

②以下のガイダンス方針の説明を記載すること

- ガイダンスが許可されるポイント又はガイダンスが要求されるポイント
- 運用責任者が被験者に提供することになっている固有のガイダンス
- 運用責任者の裁量によって被験者にガイダンスを与える局面

(6) 本人照合失敗の定義と失敗原因（19795-1 7.3.3.2）

運用者から見た本人照合失敗の定義、および、本人照合失敗原因（生体特徴をもっていない、サンプルが取得できない、テンプレートと合致しない、など）の説明を記載する[shall]。

(7) 重みづけ（19795-1 8.1.2）

誤拒否率において何らかの重みづけ（被験者集団の分布、実行されたトランザクション回数の分布など）を行う場合、その方法の説明を記載する[shall]。

(8) 試験前のデータ処理 **19795-2 6.2.11**

テクノロジ評価およびシナリオ評価において、保存された照合用バイオメトリックデータが FRR 算出のための試験に使用される前の段階でのデータ処理の内容について説明を記載する[shall]。原画像から特徴量データに変換されている場合はその処理の概要や、大よそのデータサイズなどの説明を記載する[shall]。

1.3.10 偽者トランザクション（19795-1 7.6）

偽者の照合に関する性能試験として誤受入率 FAR（False Accept Rate）を測定するための計画を記載する。内容は以下のとおりである。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**

オンラインまたはオフラインのいずれの方法で実施するかを記述する[shall]。

(2) 誤受入率算出のための照合処理方針 19795-2 7.1.3.2, 7.1.5

誤受入率を算出するための偽者トランザクションの処理方針に関する以下の内容について説明を記載する[shall]。

① 受入率算出のための照合の閾値

②偽者トランザクションの処理内容（フローチャートなど）

③偽者トランザクションの最短・最長時間

④偽者トランザクションの最小・最大アテンプト回数

⑤偽者トランザクションの最小・最大プレゼンテーション回数

⑥偽者トランザクションのための最低必要・最大許容サンプル数 19795-2 6.3.1 を照合に適用

注 1）あらかじめ蓄積されたバイオメトリックデータを用いて偽者トランザクションをシミュレートして FAR を算出する場合も、上記と同等の内容について説明を記載する。トランザクションのシミュレートに関する説明を別紙-2 に示す。

注 2）身体部分単位で算出し、ひとりの被験者のひとつの身体部分の偽者トランザクション数は 1 回とする。

注 3）テンプレートと照合バイオメトリックデータの組は順列ではなく組み合わせを用いる（あるテンプレートと照合バイオメトリックデータの組を逆にして照合トランザクションに加えてはならない）。

注 4）偽者トランザクションはベンダーの定義を用いる。

(3) 個人内比較の実施有無（19795-1 7.6.1.3）

個人内比較の実施有無を記述する[shall]。有の場合、個人内比較の実施内容の説明を記載する[shall]。個人内比較とは、利用者ひとりあたり複数の身体部分がある場合（指、手、目など）、同一の個人の異なる身体部分間での試験を偽者トランザクションに含めることを表す。

(4) 偽者トランザクションのオンライン収集（19795-1 7.6.2）

トランザクションをオンラインで実施する場合、計画の詳細について説明を記載する[shall]。蓄積媒体に記憶された複数の非自己テンプレート（利用者自身以外のテンプレート）の中から無作為に抽出したテンプレートを用いてトランザクションを実行する場合は、説明の中に無作為抽出方法の詳細も含める[shall]。

(5) 偽者トランザクションのオフライン収集（19795-1 7.6.3）

偽者トランザクションをオフラインで実施する場合、非自己比較のためのサンプルとテンプレートの抽出方法を含めた実施計画の説明を記載する[shall]。抽出方法には大きく分けて以下の 3 種類のいずれかが考えられる。

－ 非自己比較のためにサンプルとテンプレートとの両方を無作為に復元抽出する。

－ 本人サンプルごとに，生体情報登録されたすべての非自己テンプレートの中から若干数のものをサンプル特徴と比較するために無作為に抽出する（テンプレートの無作為抽出は，サンプルごとに独立して行う。）。

－ 完全相互比較を実行する。すなわち，各サンプル特徴をすべての非自己テンプレートと比較する。

(6) 収集過程の一般条件下での実行 この項目は 19795-1 において、テンプレート生成トランザクションにのみ記載されていますが偽者トランザクションにも適用しました。

偽者トランザクション実行時、あるいは、オフライン試験のためのデータ収集時の制御要因がすべての被験者で一様になるか、一様にならない場合被験者全員で無作為に変動させる方法を記述する[shall]。それぞれの場合において、制御要因の制御の方法の説明を記載する[shall]。本項における制御要因は、

温度である。

(7) データ入力エラーの防止　**この項目は 19795-1 において、本人トランザクションにのみ記載されています（1.3.9 (4)）が偽者トランザクションにも適用しました。**

偽者トランザクション実行時、あるいは、オフライン試験のためのデータ収集時のデータ入力エラー防止対策の説明を記載する[shall]。

(8) 監督者の介入基準　**上記(6)と同様の考えで追加しました**

偽者トランザクション実行時、あるいは、オフライン試験のためのデータ収集時の監督者の介入基準の説明を記載する[shall]。

(9) 生体情報取得失敗者に対する助言又は救済策　**上記(6)と同様の考えで追加しました**

被験者が偽者トランザクション実行時、あるいは、オフライン試験のためのデータ収集時に生体情報取得に失敗した際の再照合試行前の助言や救済策について以下の情報を含めて説明を記載する[shall]。

①アプリケーションと一貫性があること

②以下のガイダンス方針の説明を記載すること

- ガイダンスが許可されるポイント又はガイダンスが要求されるポイント
- 運用責任者が被験者に提供することになっている固有のガイダンス
- 運用責任者の裁量によって被験者にガイダンスを与える局面

(10) 重みづけ

誤拒否率において何らかの重みづけ（被験者集団の分布、実行されたトランザクション回数の分布など）を行う場合、その方法の説明を記載する[shall]。

(11) 習熟度の実現方法 **19795-2 7.2.2**

偽者トランザクション実行時、あるいは、オフライン試験のためのデータ収集時、募集する被験者が想定する習熟度に従っていることを実現するための方法の説明を記載する[shall]。評価前に事前練習を行うといった方法が例として考えられる。

(12) 評価前のデータ処理 **19795-2 6.2.11**

テクノロジ評価およびシナリオ評価において、保存された照合用バイオメトリックデータが FAR 算出のための試験に使用される前の段階でのデータ処理の内容の説明を記載する[shall]。原画像から特徴量データに変換されている場合はその処理の概要や、大よそのデータサイズなどについて記載する[shall]。

1.3.11 記録管理

評価結果を記録管理するための計画を記載する。内容は以下のとおりである。

(1) 記録方法 **19795-1 9**

記録しようとする項目および内容の説明を記載する[shall]。　記録が推奨される項目を以下に示す。

- データ容量が非現実的でなければ、原サンプル画像（収集される場合）
- 生体情報登録ごとのテンプレート（入手可能な場合、照合入力試行ごとの特徴データも蓄積するのが望ましい）
- 入手可能な場合、バイオメトリックシステムによる照合スコア及び判定出力
- 性能尺度及び不確実性を導き出すために用いた方法
- 生体情報登録を実施すること及び本人や偽者トランザクションデータの収集を監督することに責任を負う者の身元

(2) 保管情報の有効性 19795-2 7.1.6

保管された情報の有効性が確認できるプロセスの説明を記載する[shall]。

(3) 保管状態 19795-1 9

保管状態に関する計画の説明を記載する[shall]。 記録が推奨される項目を以下に示す。

・試験で実行されたオフラインの本人トランザクションや偽者トランザクションを再現できるよう保管すること

・記録されたデータがバックアップなどにより損失や変更の回避が行われること

1.4 試験報告書の記載事項

前節 1.3 で述べた試験計画書に従った試験を実施し、その結果を試験報告書に記載する。しかし結果を報告書に記載する際には以下の点に留意すること

1.4.1 一般的事項

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.1 の一般的事項に関する試験後の情報を記載する[shall]。記載項目は 1.3.1 節の記載内容に従う。

1.4.2 システム情報

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.2 のシステム情報に関する試験後の情報を記載する。記載項目は 1.3.2 節の記載内容に従う。

(1) トランザクション情報保存の有無

ログなどによる保存が有の場合、試験環境における保存場所の説明を記載する[shall]（コンピュータ名、フォルダ名など）。

(2) 画像または特徴の保存有無

バイオメトリック画像またはバイオメトリック特徴の記憶媒体への保存が有の場合、試験環境における保存場所の説明を記載する[shall]（コンピュータ名、フォルダ名など）。

(3) 照合時の出力情報の決定

判定結果や各種スコアの試験環境における保存場所の説明を記載する[shall]（コンピュータ名、フォルダ名など）。

(4) SDK（ソフトウェア開発キット）使用有無

試験計画と同様の項目について、試験結果の説明を記載する[shall]。

(5) 試験のためのシステム修正有無

性能試験実施を目的とした製品の修正が有の場合、修正結果の説明を記載する[shall]。

(6) テンプレートの独立性の有無

テンプレートの独立性が無の場合、非自己、すなわち本人以外あるいは本人の異なる身体部分のテンプレートへの影響を考慮して実施した試験結果の説明を記載する[shall]。

(7) テンプレート学習の有無

テンプレート学習が有の場合、実施した学習結果の説明を記載する[shall]。

(8) 閾値の定義

試験で使用した閾値の説明を記載する[shall]。

(9) データベース規模への依存性の有無

データベース規模への依存性が有の場合、依存性を考慮して実施した試験結果の説明を記載する[shall]。

(10) 性能試験方法の決定 **19795-2 6.1.4**

試験計画と同様の項目について、試験結果の説明を記載する[shall]。

(11) システム詳細 **19795-2 7.4.2.2**

試験計画と同様の項目について、試験結果を記述する[shall]。

1.4.3 想定アプリケーション **19795-2 7.1.1.1**

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.3 の想定アプリケーションに関する試験後の特記事項などがあれば記載する[shall]。

1.4.4 影響要因の制御 **19795-2 6.2.5 はこの節に含まれる**

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.4 の影響要因の制御に関する試験後の情報を記載する。記載項目は 1.3.4 節の記載内容に従う。

(1) 母集団の人口統計

① 年齢層:任意の年齢単位(1 年、5 年、10 年など)で区切った年齢層の分布を被験者数で記述する[shall]。

② 性別:男女(生物学的性別)の分布を被験者数で記述する[shall]。

③ 民族的出身(海外市場が対象の場合):民族的出身に応じた分類を定義した上で、分類毎の分布を被験者数で記述する[shall]。

④ その他:身長、目や髪の色などベンダーが記録したもの

(2) 姿勢・位置決め

試験システムの生体情報取得装置の仕様に基づいた姿勢や位置決めに関する被験者の分布情報の収集結果の説明を記載する[shall]。習熟度が低の被験者が含まれない場合、本項目は記載する必要はない。

(3) 屋内・屋外 **19795-2 6.2.10, 7.1.1.3**

システムの使用環境が屋内か屋外かの別。屋内の場合は施設のタイプの説明を記載する。屋外の場合は性能に関わる条件の説明を記載する[shall]。

(4) 温度

評価した温度条件の説明を記載する[shall]。屋内環境の場合の最低限の記述例は「空調が効いた室内環境であり、何℃～何℃の温度環境で評価を実施した」である。

(5) データの使用順序 **19795-2 6.1.8**

データの使用順序の結果の説明を記載する[shall]。

(6) 生体情報登録~照合間の経過時間

登録～照合までの最短時間あるいは平均時間を記述する。あわせて経過時間の結果の根拠の説明を記載する[shall]。

(7) 被験者の習熟度

習熟度の分布を被験者数で示す[shall]。

1.4.5 被験者選定

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.5 の被験者選定に関する試験後の情報を記載する[shall]。記載項目は 1.3.5 節の記載内容に従う。

(1) 被験者の人数および選定方法

募集した被験者の人数、収集した身体部分の数、サンプル数を記述するとともに、実施した被験者選定方法の説明を記載する[shall]。過去に収集され蓄積されたデータが評価に使われた場合、蓄積済みデータの被験者数、身体部分の数、サンプル数および選定方法もあわせて説明を記載する[shall]。

(2) 人工的に生成したサンプルまたは特徴データの使用有無

人工的に生成したデータが有の場合、生成した人工データが想定する被験者数、身体部分の数、サンプル数の説明を記載する[shall]。

(3) 被験者または取得データの純粋性 **19795-2 6.2.7**

再参加または再利用の有無を記述する[shall]。

1.4.6 被験者管理

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.6 の被験者管理に関する試験後の情報を記載する。記載項目は 1.3.6 節の記載内容に従う。

(1) 被験者説明 **19795-2 7.1.2.1**

被験者に対して行った各種説明内容の説明を記載する[shall]。

(2) 習熟度の確認 **19795-2 7.1.2.2**

被験者の習熟度確認の実施結果の説明を記載する[shall]。

(3) 順化 **19795-2 7.1.2.5**

被験者の順化方法の実施結果の説明を記載する[shall]。

(4) 管理プロセス

被験者の管理プロセスの各実施結果の説明を記載する[shall]。

(5) 少数の代表的でない利用者による偏りの防止 （19795-1 7.4.5）

同一被験者の一度の社内試験への複数回参加に対する防止結果の説明を記載する[shall]。

1.4.7 データ収集誤りの回避

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.7 のデータ収集誤りの回避に関する試験後の情報を記載する。記載項目は 1.3.7 節の記載内容に従う。

(1) データ収集誤り回避方法

データ収集誤りの回避結果の説明を記載する[shall]。

(2) 除外サンプルの報告

登録時の人単位の除外が FTE として集計されていること、および、身体部分単位の除外数を記述する[shall]。除外サンプル報告の詳細を以下に示す。① 登録時のサンプル除外

- ある身体部分のサンプルがすべて除外され、その身体部分のテンプレートが生成されなかった場合、そのように失敗した身体部分の総数を、サンプル収集の対象となったすべての被験者の身体部分の総数とともに報告しなければならない。
- 登録ポリシーを満足できなかった被験者のエラー要因にサンプル除外が含まれている場合、そのように失敗した被験者の総数を、登録に参加したすべての被験者の総数とともに報告しなければならない。なお、このような被験者は登録失敗者として扱い、FTE に含めなければならない。

② 本人トランザクションあるいは偽者トランザクション実行時のサンプル除外

・本人トランザクションあるいは偽者トランザクションにおいて、ある身体部分のサンプルがすべて除外され、その身体部分の照合バイオメトリックデータが生成されなかった場合、そのように失敗した身体部分の総数を、サンプル収集の対象となったすべての被験者のすべての身体部分の数とともに報告しなければならない。

・本人トランザクションの失敗において、その失敗要因が身体部分のサンプル除外だった場合、そのように失敗したトランザクションの総数を、本人トランザクションの総数とともに報告しなければならない。なお、このようなトランザクションは誤拒否として扱い、FRR に含めなければならない。

1.4.8　生体情報登録

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.8 のデータ収集誤りの回避に関する試験後の情報を記載する。記載項目は 1.3.8 節の記載内容に従う。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**

オンラインまたはオフラインのいずれで試験を実施したか記述する[shall]。

(2) 生体情報登録方針 **19795-2 7.1.3.1**

生体情報登録方針の実施結果の説明を記載する[shall]。

(3) 登録の一般条件下での実行

一様制御あるいは無作為制御の結果の説明を記載する[shall]。

(4) 監督者の介入基準

監督者の介入結果の詳細の説明を記載する[shall]。

(5) 登録失敗者に対する助言又は救済策 **19795-2 6.2.6, 7.1.2.4 を追加**

再登録試行前の助言や救済策の実施結果の説明を記載する[shall]。

ガイダンス結果として提示した件数、提示したガイダンスの種類、種類ごとの比率などの説明を記載することを推奨する。

(6) 登録失敗の定義と失敗原因（推奨）

発生した登録失敗の原因（生体特徴をもっていない、サンプルが取得できない、練習入力試行で照合できない、など）の説明を記載することを推奨する[should]。

(7) 重みづけ

重みづけを行った場合、結果の説明を記載する[shall]。

(8) 習熟度の実現方法 **19795-2 7.2.2**

習熟度の実現結果の説明を記載する[shall]。

(9) 評価前のデータ処理 **19795-2 6.2.11**

評価前のデータ処理結果の説明を記載する[shall]。

(10) 登録失敗率（FTE）の実測値

登録失敗率 FTE の実測値を記述するとともに、計算式の分子（試験対象システムの登録ポリシーを満足できなかった人の総数）と計算式の分母（登録に参加した総人数）を記述する[shall]。

$$\text{FTE の実測値} = \frac{\text{登録ポリシーを満足できなかった人の総数}}{\text{登録に参加した総人数}}$$

(11) 登録失敗率（FTE）の諸元値

FTE の実測値に信頼区間を適用した、登録失敗率の諸元値を記述する。あわせて、宣言値を定めた根拠の説明を記載する。[shall] 静脈認証技術に二項検定を適用した場合、FTE のベンダーが定める信頼区間の上限値を記述する。[shall]信頼区間の算出方法として二項検定以外の方法を使用する場合、信頼区間の算出方法およびその方法が適用できる根拠の説明を記載する[shall]。

(12) 人口統計グループ毎の集計（推奨）19795-2 6.3.3 を登録に適用

異なる人口統計グループに対する登録結果，異なる環境条件に関連する登録結果，又はコーパスの他の論理セグメントに対する登録結果を集計する[should]。

1.4.9　本人トランザクション

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.9 のデータ収集誤りの回避に関する試験後の情報を記載する。記載項目は 1.3.9 節の記載内容に従う。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**

オンラインまたはオフラインのいずれの方法で実施したか記述する[shall]。

(2) 誤拒否率算出のための照合処理方針の実施結果 **19795-2 7.1.3.2, 7.1.5**

誤拒否率算出のための照合処理方針の実施結果の説明を記載する[shall]。

(3) 収集過程の一般条件下での実行

一様制御あるいは無作為制御の結果について説明を記載する[shall]。

(4) データ入力エラーの防止

データ入力エラー防止対策の実施結果の説明を記載する[shall]。

(5) 監督者の介入基準

監督者の介入結果の説明を記載する[shall]。

(6) 本人照合失敗者に対する助言又は救済策 **19795-2 6.2.6, 7.1.2.4 を追加**

再照合試行前の助言や救済策の実施結果について説明を記載する[shall]。

ガイダンス結果として提示した件数、提示したガイダンスの種類、種類ごとの比率などの説明を記載することを推奨する。

(7) 本人照合失敗の定義と失敗原因

発生した本人照合失敗の原因（生体特徴をもっていない、サンプルが取得できない、テンプレートと合致しない、など）の説明を記載する[shall]。

(8) 重みづけ

重みづけを行った場合、結果の説明を記載する[shall]。

(9) 習熟度の実現方法 **19795-2 7.2.2**

習熟度の実現結果の説明を記載する[shall]。

(10) 評価前のデータ処理 **19795-2 6.2.11**

評価前のデータ処理結果について説明を記載する[shall]。

(11) 誤拒否率（FRR）の実測値

誤拒否率 FRR の実測値を記述する[shall]とともに、計算式の分子（拒否が発生した本人トランザクション総数）と計算式の分母（本人トランザクション総数）を記述する[shall]。

$$\text{FRR の実測値} = \frac{\text{拒否が発生した本人トランザクション総数}}{\text{本人トランザクション総数}}$$

(12) 誤拒否率（FRR）の諸元値

FRR の実測値に信頼区間を適用した、誤拒否率の諸元値を記述する。あわせて、宣言値を定めた根拠の説明を記載する。[shall] 静脈認証技術に二項検定を適用した場合、FRR のベンダーが定める信頼区間の上限値を記述する。[shall]信頼区間の算出方法として二項検定以外の方法を使用する場合、信頼区間の算出方法およびその方法が適用できる根拠の説明を記載する[shall]。

1.4.10　偽者トランザクション

前節 1.3 の試験計画に従って実施した試験において、前節 1.3.10 のデータ収集誤りの回避に関する試験後の情報を記載する。記載項目は 1.3.10 節の記載内容に従う。

(1) オンラインまたはオフラインによる実行 **シミュレーテッド・トランザクションか否かを区別するためにこの項目を追加しました**

オンラインまたはオフラインのいずれの方法で実施したか記述する[shall]。

(2) 誤受入率算出のための照合処理方針の実施結果 **19795-2 7.1.3.2, 7.1.5**

誤受入率算出のための照合処理方針の実施結果の説明を記載する[shall]。

(3) 個人内比較の実施有無

評価が個人内比較を含めて行われたか否かを記述する[shall]。行われた場合、個人内比較の内容の説明を記載する[shall]。

(4) 偽者トランザクションのオンライン収集

トランザクションをオンラインで実施した場合の実施結果の説明を記載する[shall]。

(5) 偽者トランザクションのオフライン収集

トランザクションをオフラインで実施した場合の実施結果の説明を記載する[shall]。

(6) 収集過程の一般条件下での実行

制御要因の制御結果について内容の説明を記載する[shall]。

(7) データ入力エラーの防止

データ入力エラー防止対策の実施結果の説明を記載する[shall]。

(8) 監督者の介入基準

偽者照合における監督者の介入結果の説明を記載する[shall]。

(9) 生体情報取得失敗者に対する助言又は救済策

生体情報取得失敗者に対する助言や救済策の実施結果について説明を記載する[shall]。

ガイダンス結果として提示した件数、提示したガイダンスの種類、種類ごとの比率などの説明を記載することを推奨する。

(10) 重みづけ

重みづけを行った場合、結果の説明を記載する[shall]。

(11) 習熟度の実現方法

習熟度の実現結果の説明を記載する[shall]。

(12) 評価前のデータ処理 **19795-2 6.2.11**

評価前のデータ処理結果について説明を記載する[shall]。

(13) 誤受入率（FAR）の実測値

誤受入率 FAR の実測値を記述するとともに、計算式の分子（受入が発生した偽者トランザクション総数）と計算式の分母（本人以外の身体部分間あるいは本人の異なる身体部分間の偽者トランザクション総数）を記述する[shall]。

$$\text{FAR の実測値} = \frac{\text{受入が発生した偽者トランザクション総数}}{\text{本人以外の身体部分間あるいは本人の異なる身体部分間の偽者トランザクション総数}}$$

(14) 誤受入率（FAR）の諸元値

FAR の実測値に信頼区間を適用した、誤受入率の諸元値値を記述する。あわせて、宣言値を定めた根拠の説明を記載する。[shall] 静脈認証技術に二項検定を適用した場合、FAR のベンダーが定める信頼区間の上限値を記述する。[shall]信頼区間の算出方法として二項検定以外の方法を使用する場合、信頼区間の算出方法およびその方法が適用できる根拠の説明を記載する[shall]。

1.4.11 記録管理

(1) 記録方法

記録された項目および内容の概要の説明を記載する[shall]。あわせて、スクリーンショットか複製かは問わず，表及び実験記録などのデータ収集要素の例を提出する[shall]。

(2) 保管情報の有効性

有効性の確認結果の説明を記載する[shall]。

(3) 保管状態

保管状態の説明を記載する[shall]。

別紙-1: ISO/IEC 19795-1 の報告項目と本サポート文書の報告項目の対応表

ISO/IEC 19795-1:2006 において性能試験における報告項目と、本サポート文書における報告項目の対応を下表に示す。

No	分類	項目名	必須
1	基本的な尺度	生体情報登録失敗率	✓
		取得失敗率	
		誤合致率及（FMR）及び誤非合致率（FNMR）	
		個々の誤り率のヒストグラム	
2	システム性能尺度	生体情報登録失敗率（FTE）	✓
		取得失敗率（FTA）	✓ （シナリオのみ）
		誤受入率（FAR）誤拒否率（FRR）	✓
		一般化の方法の詳細と一般化した誤受入率と誤拒否率	
		個々の誤り率のヒストグラム	
3	試験詳細の報告	試験したシステムの性能に関係する詳細	✓
		評価形式（テクノロジ、シナリオ）	✓
		試験の規模（被験者数、被験者がテンプレート生成する指、手の数）	✓
		被験者が行う訪問の回数	✓
		各訪問時の被験者（又は被験者の身体部分）ごとのトランザクション数	✓
		被験者集団の人口統計（年齢、性別、民族的出身）	✓
		試験環境の詳細	✓
		生体情報登録から照合試験トランザクションまでの経過時間	✓
		データ収集時に用いた（利用者が設定可能な）品質・判定閾値	✓
		性能に影響を与える制御要因（温度）の制御	✓
		試験手順の詳細（登録処理、照合処理とも）	✓
		被験者集団のシステム使用上の訓練・精通・習熟水準の詳細（習熟度）	✓
		分析から除外した異常な事例及びデータの詳細	✓
		不確実性推定値（及び推定方法）	✓
		本ガイドラインからの逸脱事項	✓
4	結果のグラフ表示	DET 曲線	
		ROC 曲線	

別紙-2：トランザクションのシミュレートによる評価

記憶媒体に蓄積された被験者ごとの（複数の）テンプレート、および、複数のバイオメトリック照合データを用いて、テンプレート生成トランザクションや本人トランザクション、偽者トランザクションをシミュレートすることにより精度値を算出する場合の記載事項を以下に示す。

1. バイオメトリックトランザクションの一般的な説明（19795-1 5.4）

バイオメトリック処理におけるトランザクションは一般的に、提示と入力試行の 2 つから構成される。ISO/IEC 19795-1 に記載されているトランザクションの一般的な概念を以下に示す。この概念はテンプレート生成トランザクション、本人トランザクション、偽者トランザクションのいずれにも適用することが可能だが、ベンダーが製品に実装するトランザクションは、製品が取り扱う身体部分やモダリティ、あるいは、エルゴノミクス（センサーへの接触があるかないか、など）によりベンダー毎に異なる場合がある。

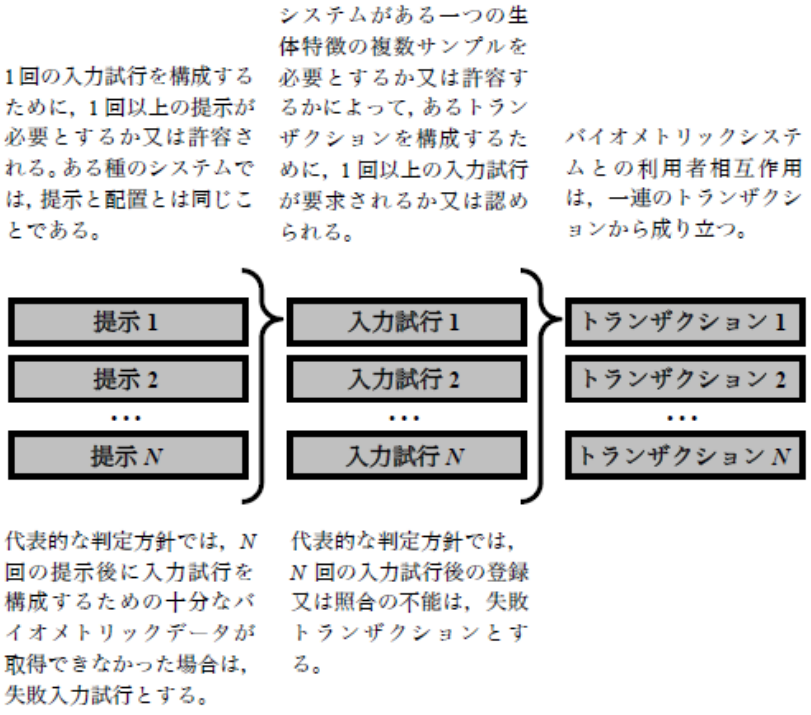


図-1 バイオメトリックトランザクションの概念図

2. トランザクションのシミュレートについて（ISO/IEC 19795-1 及び ISO/IEC 19795-2 に該当なし）

ベンダーが実施する精度評価のための社内試験においては、FTE や FRR・FAR などの性能尺度の評価をデータベースに蓄積されたバイオメトリックデータをトランザクションにシミュレートすることにより実現する場合がある。蓄積されたデータからトランザクションをシミュレートする場合に評価機関への提示が要求される情報を以下に示す。

(1) トランザクションの構成要素

・シミュレートするテンプレート生成トランザクションまたは本人トランザクション、偽者トランザクションの処理フロー
・1 回のトランザクションで用いられるひとりの被験者のひとつの身体部分毎の最大テンプレート数、最大バイオメトリック照合データ数
・1 回のトランザクションで実行される最大アテンプト数、プレゼンテーション数

(2) シミュレートされたトランザクションに基づく性能算出根拠

・被験者総数
・総身体部分数
・テンプレート生成トランザクション総数および失敗トランザクション数
・本人トランザクション総数および拒否発生トランザクション数
・偽者トランザクション総数および受入発生トランザクション数

(3) 性能値の算出における考慮事項

・データの独立性を考慮し、順列（P）ではなく組み合わせ（C）を用いられたことの説明（例：「偽者トランザクションおよび本人トランザクションで用いられるテンプレートと照合バイオメトリックデータの組は、順列ではなく組み合わせが用いられた。」）
・データベースからのデータの取り出し順番が性能に不当に有利になるような配慮がされていないことの説明（例：「時間順に機械的にデータを取り出した。」あるいは、「ランダムにデータを取り出した。」）
・シミュレートに端数が出た場合（完結したトランザクションにならない場合）、これを有効なデータとみなして、集計結果に含められていることの説明（例：「トランザクションのシミュレートにおいて発生した端数は、集計データに含まれている。」）
・シミュレーションが偽者トランザクションに基づいてシミュレートされていることの説明（本人トランザクションに基づいてシミュレートされる場合、その合理的な根拠が説明されなければならない）。

＜用語に関する補足説明＞

19795-1,2 およびこれらに対応する JIS 規格で用いられている表現とサポート文書案における表現について

No	サポート文書案の今までの表現	19795 原文の表現	翻訳 JIS の表現	サポート文書案での変更案
1	「精度評価」	“performance test”と”performance evaluation”が混在している。	それぞれ「性能試験」と「性能評価」に翻訳している。	19795-1 規格書タイトルの「性能試験」に統一する。
2	「評価」、「試験」	“test”と”evaluation”が文書内に混在している。	「test」を「試験」、「evaluation」を「評価」に翻訳している。	基本的に「試験」に統一するが、19795-2 規格書のタイトルにある「テクノロジ評価」「シナリオ評価」のみ「評価」を用いる。
3	「登録」、「テンプレート生成」	2 つの概念を”enrol”のみで表現している。	「enrol」を「登録」に翻訳しているため、2 つの概念が区別されていない。	文脈に応じて「登録」と「テンプレート生成」を使い分ける。
4	「部位」	“body part”という言葉が使われている。	「身体部分」に翻訳している。	「身体部分」を用いる。
5	「スコア」、「スコア値」	“score”が使われている。	「得点」あるいは「スコア」に翻訳している。	「スコア」を用いる。
6	「バイオメトリックデータ」、「バイオメトリック情報」	“biometric data”が使われている。	「バイオメトリックデータ」に翻訳している。	「バイオメトリックデータ」に統一する。

付録４　評価機関による独立試験方法素案

バイオメトリック性能試験の社内試験エビデンスを受領後、評価機関が実施する独立試験の実施方法に関する素案を以下に示す。

1. 独立試験の種類

社内試験結果のエビデンスをベンダーから受領後、評価機関は原則として以下の 2 種類の独立試験の両方を実施することとする。

① 被験者試験：評価機関が独自に募集した少人数の被験者（想定人数数人～200 人程度）を用いて行うシナリオ評価である。

② 立ち入り試験：ベンダーの社内環境に評価機関が立ち入り、ベンダーが構築した試験環境を用いて行うテクノロジ評価である。

(1) 被験者試験

評価機関の施設内で、評価機関が独自に募集した被験者を用いて行うシナリオ評価である。試験の独立性を高めるために、ベンダーが提供した評価ツールではなく、標準的なツールが用いることが推奨される。被験者試験における被験者数は、数人から 200 人程度であり、以下を得ることを目的とする。

① 登録失敗率（FTE）に関する情報
- 登録ポリシーを満足できなかった人の総数
- 登録に参加した総人数

② 誤拒否率（FRR）に関する情報
- 拒否が発生した本人トランザクション総数
- 本人トランザクション総数

③ 誤受入率（FAR）に関する情報
- 全被験者の登録テンプレート
- 全被験者の照合バイオメトリックデータ

(2) 立ち入り試験

ベンダーの施設内で、ベンダーの試験環境を用いて行うテクノロジ評価である。

上記(1)で取得した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を、ベンダーの社内試験環境に書き込んだあと、誤受入率の評価を実行する。なお、ベンダーが社内試験で蓄積したデータ項目は、適宜評価機関の判断で項目の並べ替えを行う。評価実施時にあたっては、ベンダーの操作説明を受けて実際の操作は評価機関が実施する。評価完了後、評価機関が持ち込んだバイオメトリックデータは、評価機関の操作により削除する。

2. 独立試験の判定手順

FTE・FRR・FAR それぞれについて以下のとおり判定する。

2.1 登録失敗率（FTE）

ベンダーの社内試験のエビデンスに含まれる登録ポリシーを満足できなかった人の総数に、独立試験で得られた登録ポリシーを満足できなかった人の総数を加算する。同様に、ベンダーの社内試験のエビデンスに含まれる登録に参加した総人数に、独立試験で得られた登録に参加した総人数を加算する。こうして得られた分子と分母から算出される登録失敗率が、ベンダーの登録失敗率の諸元値以下であることを確認する。独立試験の実施手順を以下に示す。

(1) FTE 実測値および諸元値の入手

ベンダーから提示された社内試験エビデンスから以下の値を得る。

- 登録ポリシーを満足しなかった人の総数　= EF(V)
- 登録に参加した総人数 = EP(V)
- FTE 諸元値: FTE(V)

(2) 被験者試験の実施

評価機関が独自に集めた、評価機関が定めた数の被験者による登録試験を実施する（独立試験の客観性を高める方法として、試験ツールとして標準的なツールを用いることが推奨される)。試験の結果として以下の 2 つの数値を得る。

- 登録ポリシーを満足しなかった人の総数　= EF(I)
- 登録に参加した総人数 = EP(I)

(3) 合算 FTE の算出

独立試験結果および社内試験エビデンスの値を合算した FTE を算出する。

$$FTE(VI) = \frac{EF(V) + EF(I)}{EP(V) + EP(I)}$$

(4) 判定

ベンダーの FTE 諸元値 FTE(V)と合算 FTE である FTE（VI）を比較し、合算 FTE が FTE 諸元値以下であれば合格とする。すなわち、以下の条件を満足すれば合格とする。

$$FTE(V) \geqq FTE(VI)$$

注）略号はそれぞれ、EP: Enrolment Participants, EF: Enrolment Failures, V: Vendor, I: Independent を意味する。

2.2 誤拒否率（FRR）

ベンダーの社内試験エビデンスに含まれる拒否が発生した本人トランザクション総数に、独立試験で得られた拒否が発生した本人トランザクション総数を加算する。同様に、ベンダーの社内試験エビデンスに含まれる本人トランザクション総数に、独立試験で得られた本人トランザクション総数を加算する。こうして得られた分子と分母から算出される誤拒否率が、ベンダーの誤拒否率の諸元値以下であることを確認する。なお、独立試験の実施においては、社内試験とトランザクションの同質性の保証されなければならない。独立試験の実施手順を以下に示す。

(1) FRR 実測値および諸元値の入手

ベンダーから提示された社内試験エビデンスから以下の値を得る。

・拒否が発生した本人トランザクションの総数 = VF(V)

・本人トランザクションの総数 = VT(V)

・FRR 諸元値: FRR(V)

(2) 被験者試験の実施

評価機関が独自に集めた、評価機関が定めた数の被験者による本人トランザクション試験を実施する（独立試験の客観性を高める方法として、試験ツールとして標準的なツールを用いることが推奨される）。試験の結果として以下の 2 つの数値を得る。

・拒否が発生した本人トランザクションの総数 = VF(I)

・本人トランザクションの総数 = VT(I)

(3) 合算 FRR の算出

独立試験結果および社内試験エビデンスの値を合算した FRR を算出する。

$$FRR(VI) = \frac{VF(V) + VF(I)}{VT(V) + VT(I)}$$

(4) 判定

ベンダーの FRR 諸元値 FRR(V)と合算 FRR である FRR（VI）を比較し、合算 FRR が FRR 諸元値以下であれば合格とする。すなわち、以下の条件を満足すれば合格とする。

$$FRR(V) \geqq FRR(VI)$$

注）略号はそれぞれ、VF: Verification Failures, VT: Verification Transactions, V: Vendor, I: Independent を意味する。

2.3 誤受入率（FAR）

立ち入り試験より、受入が発生した偽者トランザクション総数、および、本人以外の身体部分間あるいは本人の異なる身体部分間の偽者トランザクション総数を得る。これらをそれぞれ分子と分母とした式から算出される誤受入率が、ベンダーの誤受入率の諸元値以下であることを確認する。独立試験の実施手順を以下に示す。

(1) FAR 諸元値の入手

ベンダーから提示された社内試験エビデンスから以下の値を得る。

FAR 諸元値: FAR(V)

(2) 被験者試験の実施

評価機関が独自に集めた、評価機関が定めた数の被験者による登録試験および本人あるいは偽者トランザクションの実施により、以下の 2 種類のデータを入手する。

・各被験者の各身体部分のテンプレート

・各被験者の各身体部分の照合バイオメトリックデータ

(3) 合算 FAR の算出

ベンダーの社内試験環境に評価機関の担当者が立ち入り、社内試験で使用したデータベースに上記(1)のテンプレートおよびバイオメトリックデータを追加した上で、偽者トランザクションを実行し、社内試験で収集されたバイオメトリックデータと独立試験で収集されたバイオメトリックデータを組み合わせた合算 FAR を算出する。得られた値を FAR（VI）とする。

(4) 判定

ベンダーの FAR 諸元値 FAR(V)と立ち入り試験で得られた FAR である FAR（VI）を比較し、合算 FAR が FAR 諸元値以下であれば合格とする。すなわち、以下の条件を満足すれば合格とする。

$$FAR(V) \geqq FAR(VI)$$

3. 偽者トランザクションに関する社内試験の適正さの検証

独立試験で募集した被験者に由来する偽者トランザクション以外の偽者トランザクション、すなわち、ベンダーが社内試験で募集した被験者のテンプレートや照合バイオメトリックデータを用いた立ち入り試験において実行されたすべての偽者トランザクションによる判定結果が、ベンダーの社内試験エビデンスの内容にすべて一致することで、社内試験の適正さを確認する。

4. 補足

収集したバイオメトリックデータが評価対象システムの構成要素であるセンサーとは異なるセンサーを用いて収集されている社内試験の許容可否や条件についても今後検討する予定です(2017 年度検討項目とする予定)。

平成２７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２８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
国立研究開発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