平成 28 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２９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、本人固有の生体情報による認証という特性から、出入国管理や ATM など金融分野での本人確認などで使われている。また、その利便性の高さから、入退室管理・勤怠管理・携帯電話・PC/アプリケーション等でも使われている。

さらに、国内外における近年の行政および民間での電子サービスの拡充あるいは金融業界での 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に本人確認するシステムの必要性がますます増大し、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、ますます重要性を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、安全性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/パスワードのようには普及していない。これは、バイオメトリクス認証技術は、認証技術の提供ベンダーがそれぞれ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セキュリティ性を説明しているのが現状であり、社会的に認知された客観性を持つセキュリティ評価基準を基にして安全・安心な技術であるとの説明ができていないことが一因であると考えられる。

一方で、列車、自動車、医療機器や制御システムの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、これらのシステムにバイオメトリクス認証技術を組み込む場合、IEC 61508 シリーズと対の関係にある CC（Common Criteria）認証の重要性も増す可能性も出て来ている。

この状況を考えると、バイオメトリクス認証技術が客観的に評価された安全な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、適用市場も広がることが予想される。つまり、バイオメトリクス認証技術に対し、社会的に認知される客観性を持つセキュリティ評価基準を整備すると共に、国際標準に則ったセキュリティ評価を行うことができる環境を構築することが、今後のバイオメトリクス認証技術の普及にとって極めて重要と考え、本事業に取り組んだ。

最後になるが、本事業の実施にあたり、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　環境情報研究院）、内田 薫 委員（法政大学大学院 情報科学研究科）他の検討委員会委員各位、また、性能評価における独立試験手法の検討において統計学に関する貴重なご助言ならびにご支援を多数賜った鎌倉稔成先生（中央大学理工学部経営システム工学科　統計データ解析研究室）に、心から深く感謝申し上げる。

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および認証を得ること

平成 29 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

付録 1　バイオメトリック照合製品 PP（20160331）

付録 2　サポート文書

付録 3　サポート文書 性能評価別冊

付録 4　19989-1 目次

付録 5　19989-2 目次

付録 6　19989-3 目次

1. 事業の目的

本事業では、バイオメトリクス認証製品の CC（Common Criteria）認証に向け、①産業界が無理なく参加可能であり、②十分に有効性があり、③継続性のある、バイオメトリクス認証製品のセキュリティ評価基盤を整備する。本事業によって、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く、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。具体的には以下を実施する。

- 客観的な評価を可能とするため、セキュリティ評価基準（ISO/IEC 15408）に則って PP（Protection Profile）および PP に付随する性能評価手法および脆弱性評価手法を作成し確立する。併せて評価機関および認証機関が利用可能なセキュリティ評価・認証基盤を整備する。
- PP および PP に付随する評価手法の成果を ISO/IEC JTC 1/SC 27 に提案し、国際標準化を目指す。本活動にあたってはバイオメトリクス認証製品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しながら協力し、早期の発行を目指す。
- 本事業で開発した PP を基に各社製品の ST（Security Target、セキュリティ機能仕様書）およびエビデンス文書を作成し、パイロット評価・認証を実施する。
- 本事業で、確立したバイオメトリクス認証製品特有の評価および認証手法および手順を体系化して文書化し、本事業終了後も継続的に評価および認証を実施可能とする。

これらの取り組みによりセキュリティ評価・認証基盤を整備して、バイオメトリクス認証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認証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。

2. 事業の実施計画

バイオメトリクス認証製品の 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、平成 27 年度の 2 年間、下記の活動に取り組んだ。

なお、バイオメトリクス認証製品には、照合（１：１認証）と識別（1：N 認証）を行う 2 種類がある。活動開始時の検討により、本事業対象はバイオメトリック照合製品とした。

1）平成 26 年度（2014 年度）

・認証機関・評価機関・ベンダーおよび有識者からなる検討委員会の組織

・海外動向調査および方針検討

・セキュリティ評価手法の研究

- バイオメトリック照合製品 PP 開発および PP 認証取得
- 性能評価手法の研究と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・ベンダーおよ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

- バイオメトリック照合製品 PP の追加 PP 開発
- 性能評価手法の研究
- 脆弱性評価手法の研究
- サポート文書全体構成案の作成
- パイロット評価・認証に向けた準備

・国際標準化活動

平成 28 年度は、平成 26 年度、平成 27 年度の成果を基に、下記に取り組む。

1）平成 28 年度（2016 年度）

・認証機関・評価機関・ベンダーおよ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

- 性能評価手法の検証
- 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）
- サポート文書の検証および完成

・国際標準化活動

平成 28 年度は上記の計画に応じて以下を実施する。

(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、事業の実施に関係する事項、研究開発の検討方針、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、研究開発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認証製品の PP（バイオメトリック照合製品 PP）およ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、独立行政法人情報処理推進機構（以下 IPA）の協力の下、国内関係者の意見を参考にしながら、cPP（collaborative PP）化の活動を本格化させる。国内の関係企業はもとより、他国も巻き込むことでより大きな活動にして行く。

(3) セキュリティ評価手法の研究

（a）性能評価手法の研究

評価機関の独立評価に必要な性能試験手法を研究する。併せて評価機関の独立評価で使用を想定して、性能評価ツールのプロトタイプを完成させる。

（b）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 27 年度までに検討した偽造物検知の評価方針案に基づき、評価機関の独立評価に必要な偽造物作成方法・攻撃方法を研究する。

（c）パイロット評価・認証

パイロット評価・認証に適用する対象製品を選定し、IPA および国内評価機関と協力し、パイロット評価・認証を実施し、本事業で検討したセキュリティ評価方法・認証基盤の妥当性と改善点の確認を行う。

（d）サポート文書の検証および完成

性能評価手法と脆弱性評価手法の研究を反映して作成したパイロット評価・認証を通してサポート文書を完成し、その結果を cPP 活動に反映する。

(4) 国際標準化活動

本事業で作成した PP および脆弱性評価に関する内容を SC 27 の ISO/IEC 19989（Security evaluation of presentation attack detection for biometrics）開発プロジェクトへ反映させると共に、早期に CD 段階へ進めるために各国との合意形成を行う。

性能に関する CC 評価の国際標準化は現在スタディピリオドにあり、4 月の SC 27 の WG および総会にて、1. NP 提案して新規国際標準開発プロジェクトへ移行する、2. 開発中の ISO/IEC 19989 をパート分割して性能に関するパートを追加し、バイオメトリクス認証製品の CC 評価全体を扱

える規格にする、のいずれかを推進する。

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

3. 事業の実施体制

3.1 管理体制および研究体制

(1)管理体制および開発体制

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および[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およ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、バイオメトリクス認証技術に携わる機器ベンダー（富士通、NEC、日立ほか）および学識経験者により検討委員会を組織して、事業の実施に関係する事項、研究開発の検討方針、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、バイオメトリクス認証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

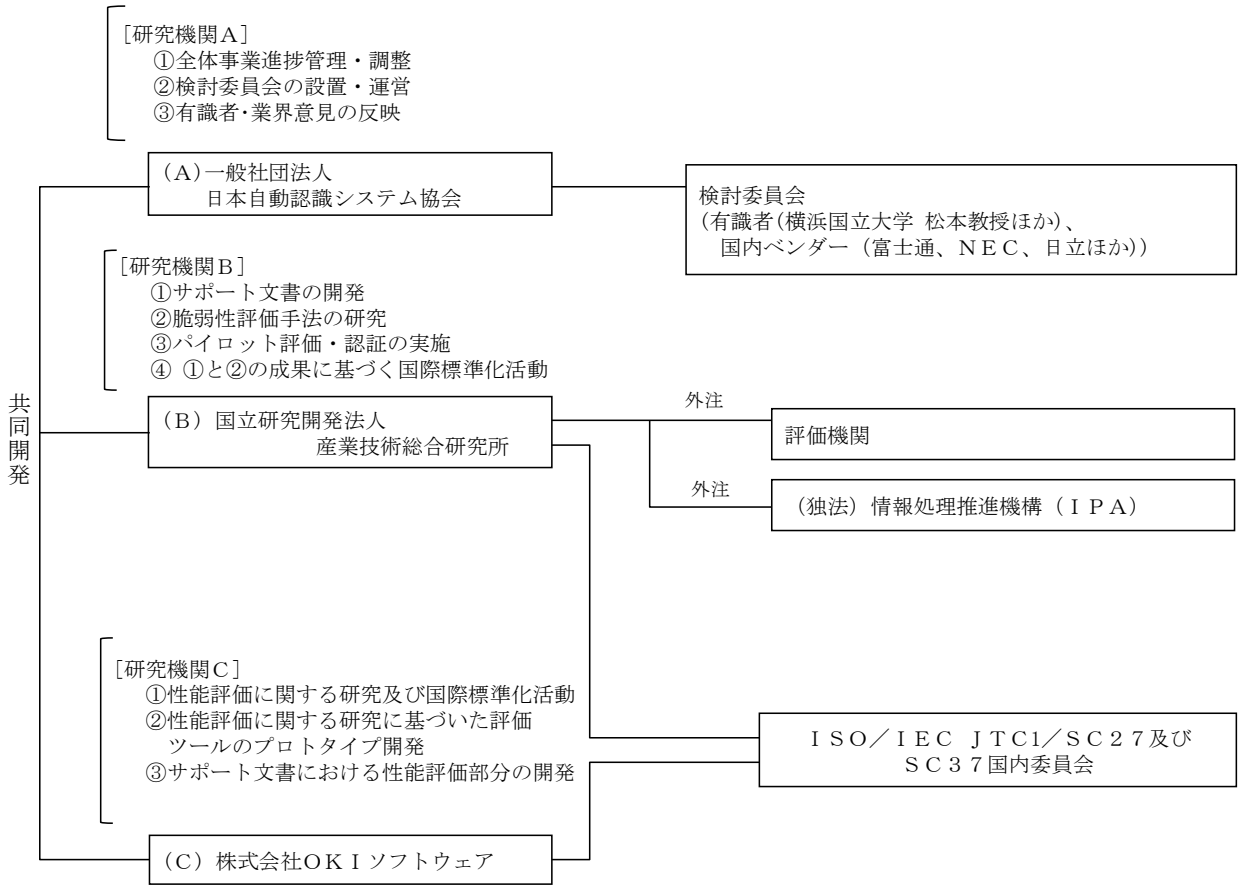


図 3.1-1　共同研究体制

2)個別の管理体制および研究体制

【一般社団法人日本自動認識システム協会（JAISA)】

(1) 管理体制

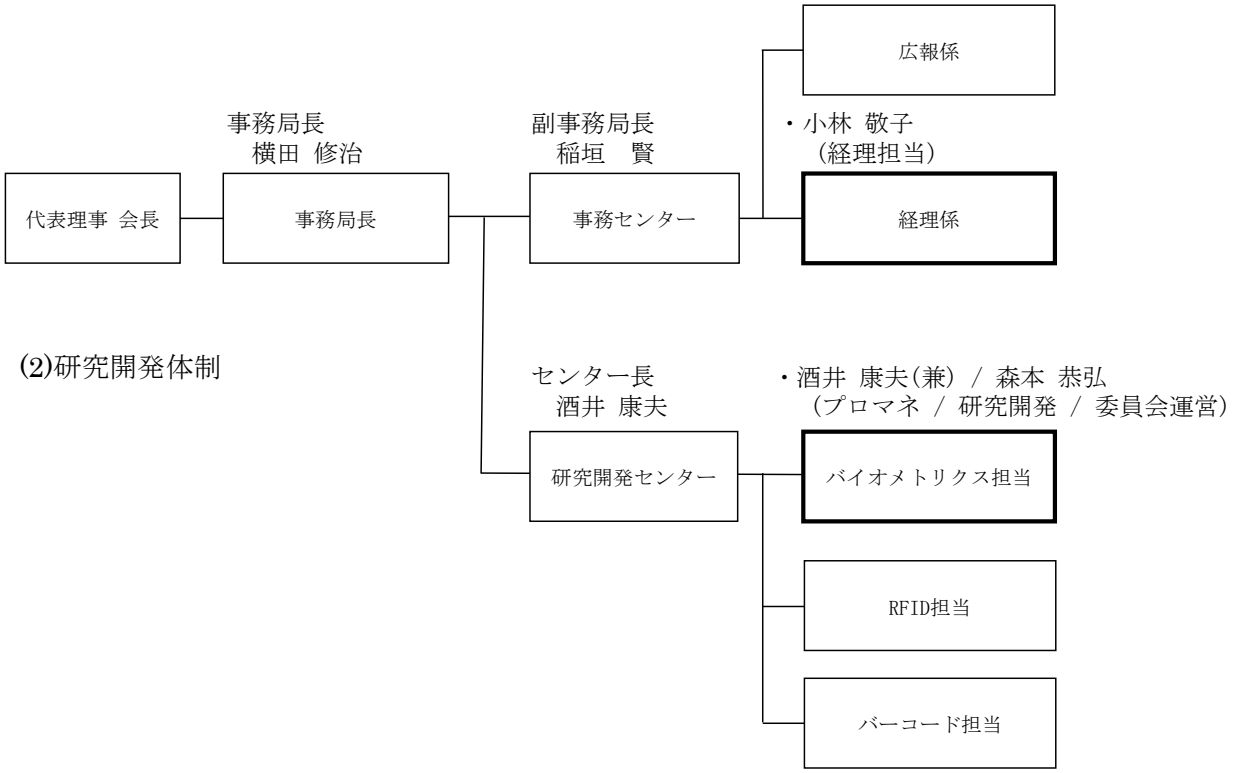


図 3.1-2　日本自動認識システム協会　管理体制・研究開発体制

【国立研究開発法人産業技術総合研究所（産総研)】

(1)管理体制

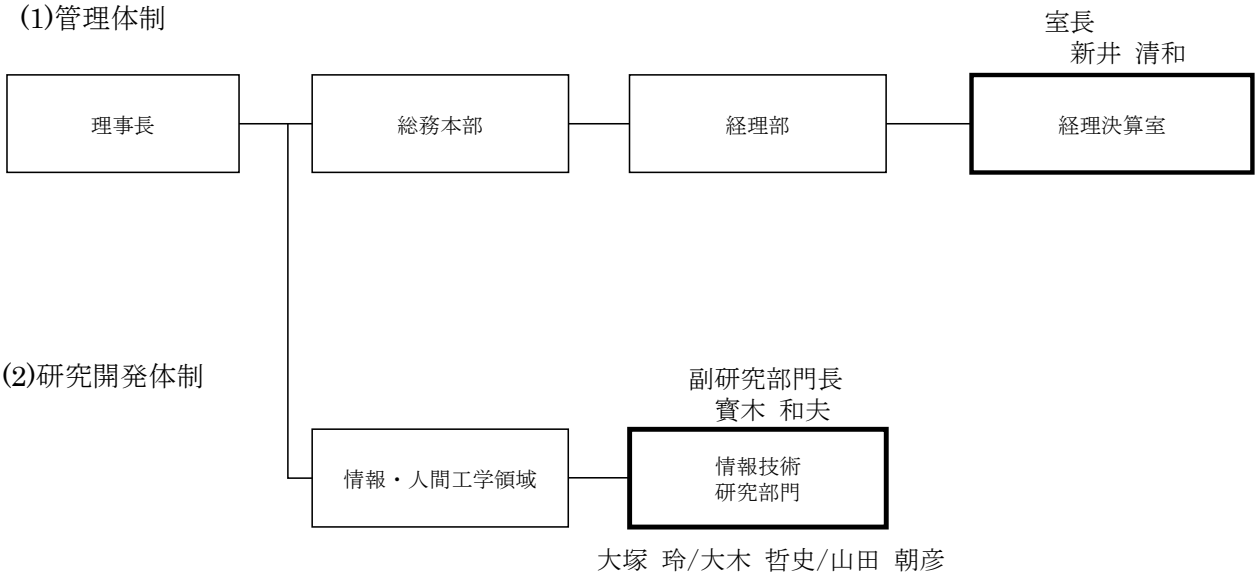


図 3.1-3　産業技術総合研究所　管理体制・研究開発体制

【株式会社 OKI ソフトウェア（OKI ソフト)】

(1)管理体制

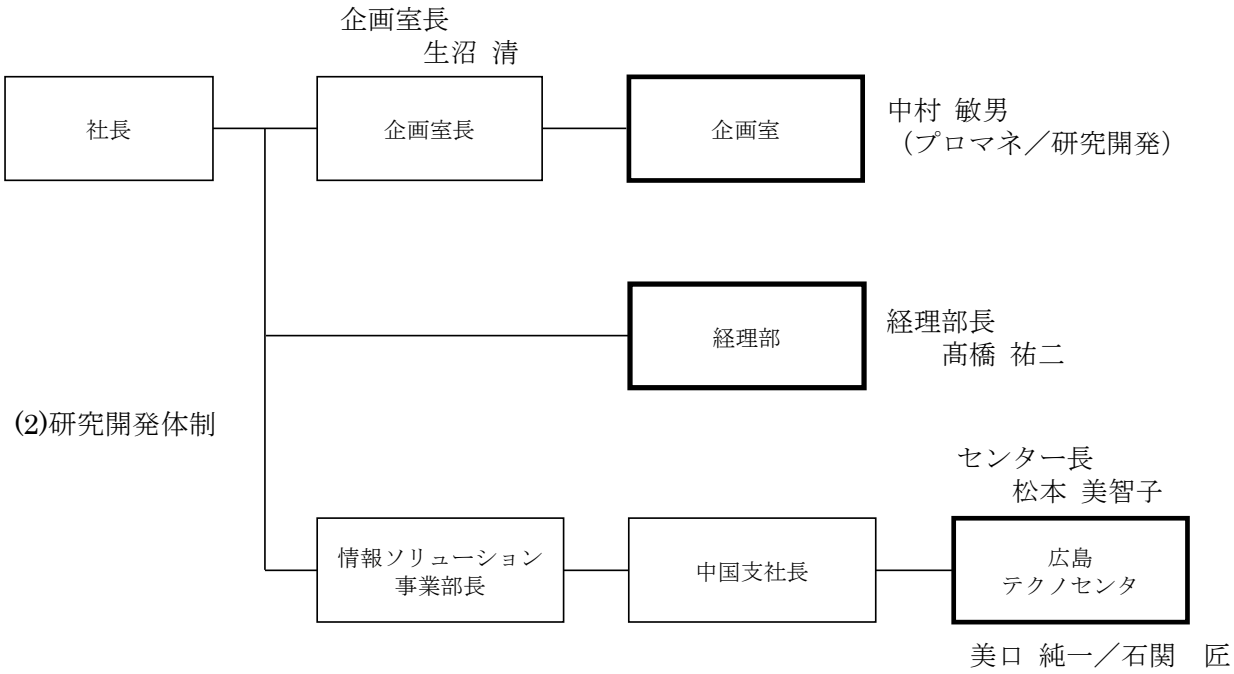


図 3.1-4　OKI ソフトウェア　管理体制・研究開発体制

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	役職	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	教授	
2	委員	内田　薫	法政大学大学院	教授	
3	委員	溝口 正典	日本電気株式会社	主席 技術主幹	SC37WG5 主査
4	委員	日間賀充寿	株式会社日立製作所	主任技師	SC37WG5 委員 SC37WG6 委員
5	委員	新崎　卓	株式会社富士通研究所	プロジェクト ディレクター	SC37WG3 主査
6	委員	岩田英三郎	ユニバーサルロボット株式会社	代表取締役 社長	
7	委員	須下 幸三	バイオニクス株式会社	代表取締役 社長	
8	委員	出口　豊	株式会社モフィリア	部長	
9	委員	甲斐 成樹	独立行政法人情報処理推進機構		
10	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	企画室	SC37WG2 委員
12	推進委員	寳木 和夫	国立研究開発法人産業技術総合研究所	副研究 部門長	
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	招聘研究員	SC37 委員長 SC37WG5 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	主任研究員	
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	特別研究員	
16	ｵﾌｻﾞｰﾊﾞ	金子 浩之	みずほ情報総研株式会社	室長	
17	ｵﾌｻﾞｰﾊﾞ	平野 誠治	凸版印刷株式会社	担当課長	SC37WG3 ｱﾄﾞﾊﾞｲｻﾞ
18	ｵﾌｻﾞｰﾊﾞ	齋藤　靖	日本電気株式会社		
19	ｵﾌｻﾞｰﾊﾞ	加藤 誠司	経済産業省　産業技術環境局	課長補佐	SC37 委員
20	ｵﾌｻﾞｰﾊﾞ	中山 和泉	経済産業省　製造産業局	課長補佐	
21	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	センター長	SC37 委員
22	事務局	森本 恭弘	一般社団法人日本自動認識システム協会	主任研究員	

3.3 実施スケジュール

平成 28 年度の活動は下記日程で実施した。

（A：JAISA, B：産総研, C：OKI ソフト）

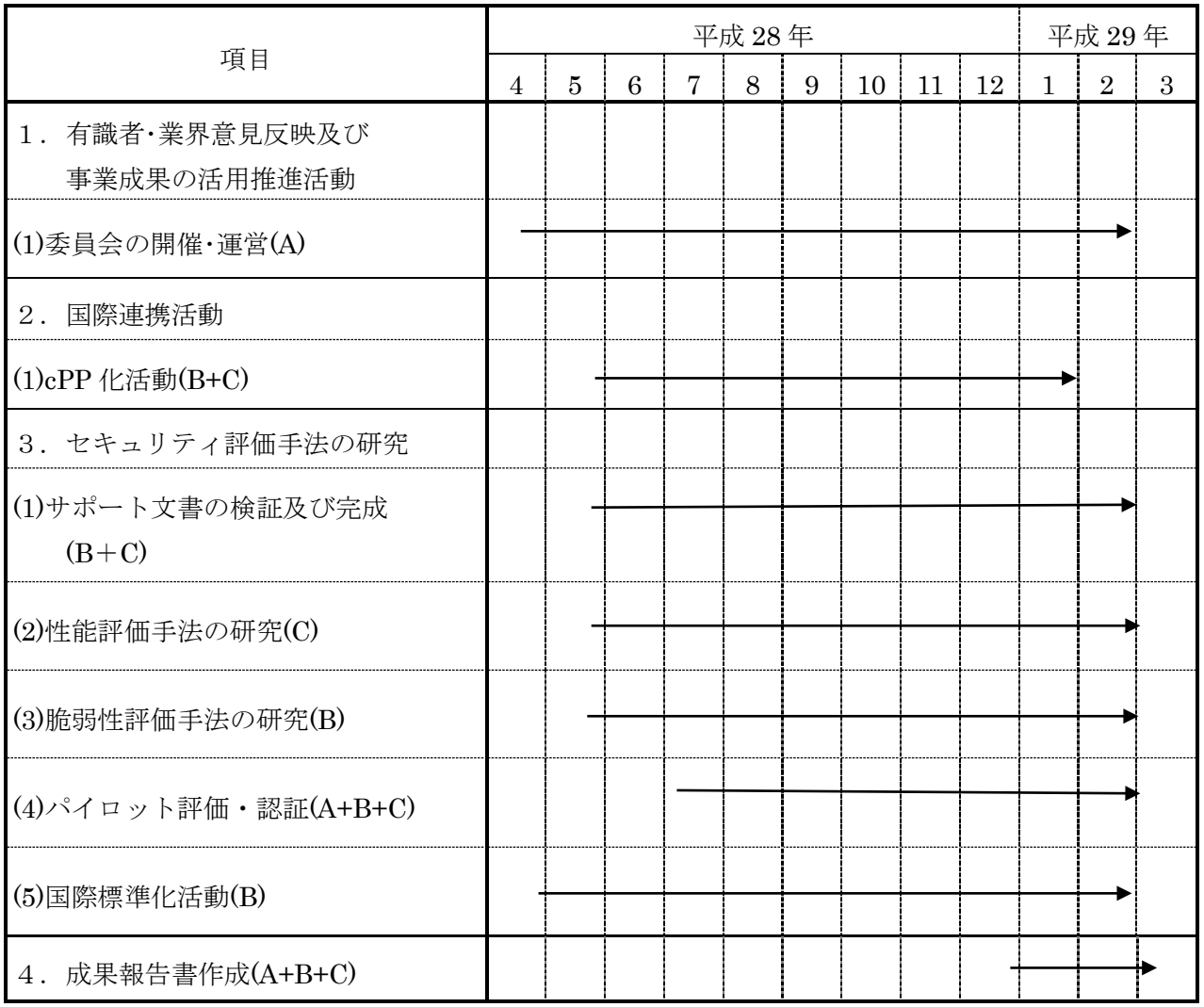


図 3.3-1　実施スケジュール

4. 実施内容概要

4.1 検討委員会

4.1.1 活動目的

バイオメトリクス認証技術に関係する、有識者・認証機関・評価機関・ベンダー・ユーザー・官公庁・実施者の知見を集め、事業の実施に関係する事項、研究開発の検討方針、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、研究開発にフィードバックすることを活動目的とした。

4.1.2 活動概要

有識者(2 団体 2 名)・認証機関(IPA 1 名)・評価機関(みずほ情報総研 2 名)・ベンダー(6 社 7 名)・ユーザー(1 社 1 名)・官公庁(2 名)・実施者（3 団体 7 名）から成る検討委員会(22 名)を組織した。

都合 4 回の委員会を開催した。各委員会の活動内容は下記である。

4.1.2.1 第 1 回検討委員会

平成 28 年 6 月 8 日(水) 9:30～12:40 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平成 28 年度計画概要審議

実施者より、資料を用いて、「クラウドセキュリティに資するバイオメトリクス認証製品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」事業について説明し、内容について審議した。

②登録および照合 PP 状況報告

実施者より、資料を用いて、登録および照合 PP 状況について報告した。

③脆弱性評価検討状況報告と審議

実施者より、資料を用いて、脆弱性評価検討状況について報告し、内容について審議した。

④性能評価検討状況報告と審議

実施者より、資料を用いて、性能評価検討状況について報告し、内容について審議した。

⑤パイロット評価・認証状況報告

実施者より、資料を用いて、パイロット評価・認証状況について報告した。

⑥cPP 提案活動状況報告

認証機関の委員より、資料を用いて、cPP 提案活動状況について報告した。

⑦国際標準化活動状況報告と審議

実施者より、資料を用いて、国際標準化活動状況について報告し、内容について審議した。

4.1.2.2　第 2 回検討委員会

平成 28 年 10 月 12 日(水)　14:00～17:30 に JAISA にて開催した。

前回の議事録の確認に引き続いて検討状況について審議した。

主な内容は下記であった。

①脆弱性評価検討状況報告と審議

実施者より、資料を用いて、脆弱性評価検討状況について報告し、内容について審議した。

②性能評価検討状況報告と審議

実施者より、資料を用いて、性能評価検討状況について報告し、内容について審議した。

③パイロット評価・認証状況報告

実施者より、資料を用いて、パイロット評価・認証状況について報告した。

④cPP 提案活動状況報告

認証機関の委員より、資料を用いて、cPP 提案活動状況について報告した。

⑤国際標準化活動状況報告と審議

実施者より、資料を用いて、国際標準化活動状況について報告し、内容について審議した。

4.1.2.3　第 3 回検討委員会

平成 28 年 12 月 16 日(金)　9:00～12:00 に JAISA にて開催した。

前回の議事録の確認に引き続いて検討状況について審議した。

主な内容は下記であった。

①脆弱性評価検討状況報告と審議

実施者より、資料を用いて、脆弱性評価検討状況について報告し、内容について審議した。

②性能評価検討状況報告と審議

実施者より、資料を用いて、性能評価検討状況について報告し、内容について審議した。

③パイロット評価・認証状況報告

実施者より、資料を用いて、パイロット評価・認証状況について報告した。

④cPP 提案活動状況報告

認証機関の委員より、資料を用いて、cPP 提案活動状況について報告した。

⑤国際標準化活動状況報告と審議

実施者より、資料を用いて、国際標準化活動状況について報告し、内容について審議した。

4.1.2.3　第 4 回検討委員会

平成 29 年 2 月 23 日(木)　9:00～12:00 に JAISA にて開催した。

前回の議事録の確認に引き続いて検討状況について審議した。

主な内容は下記であった。

①脆弱性評価検討状況報告と審議

実施者より、資料を用いて、脆弱性評価検討状況について報告し、内容について審議した。

②性能評価検討状況報告と審議

実施者より、資料を用いて、性能評価検討状況について報告し、内容について審議した。

③パイロット評価・認証状況報告

実施者より、資料を用いて、パイロット評価・認証状況について報告した。

④cPP 提案活動状況報告

認証機関の委員より、資料を用いて、cPP 提案活動状況について報告した。

⑤国際標準化活動状況報告と審議

実施者より、資料を用いて、国際標準化活動状況について報告し、内容について審議した。

4.1.3 活動成果

上記 4 回の検討委員会で、有識者・認証機関・評価機関・ベンダー・ユーザー・官公庁・実施者の知見を集め、研究開発の実施検討方針、検討内容や方向性について、専門的、具体的な検討を行い、研究開発にフィードバックした。

これにより、関係者の知見を集め、性能評価手法、脆弱性評価手法の検討・検証を進めることができ、サポート文書をまとめることができた。また、その内容を国際標準化活動に向けて、日本の代表者に提供することができた。

4.1.4 今後の課題

事業終了により検討委員会活動は終了するが、今回の事業で取り組んだバイオメトリック照合製品 PP とそれに基づく静脈認証製品に係わるサポート文書を用いて、静脈を用いたバイオメトリック照合製品の CC（Common Criteria）認証に沿ったセキュリティ評価・認証基盤が今後活用され、何件かの評価・認証の取り組みが進むに従い、本事業で開発したセキュリティ評価手法の見直しやサポート文書の改訂が必要になる場合が出てくることも予想される。

また、今回の事業で取り組んだ国際標準化活動や cPP 化活動は、国際の場で取り組みが始まったばかりであり、日本のバイオメトリクス認証業界として、今後も継続した取り組みが必要である。

これらの対応を行うために、バイオメトリクス認証製品のセキュリティ評価に係わる関係者が一堂に会して意見交換や合意形成をすることが必要になることも考えられる。

そのため、今回の事業関係者で対応体制の整備に取り組む。

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 化活動に集約されることになった。

4.2.1 cPP 化活動

4.2.1.1 活動目的

本事業の成果であるバイオメトリック照合製品 PP およ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。ここでの cPP 化の活動には、本事業の成果である性能評価およ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は決定しているが、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行くこととし、バイオメトリクス認証製品 PP を既に開発し CC 評価・認証を実施しているドイツおよびフランスを主たる連携候補とした。

4.2.1.2 活動概要

平成 27 年度開催された CCRA 会議において、IPA とスペイン認証機関共同で cPP 開発を申請し、Biometric Working Group の設立が承認された。cPP は、Biometrics Security iTC（international Technical Community）で議論される。Biometrics Security iTC を組織するために、2016 年 2 月 25 日以降、IPA 主催でオンライン会議を実施した。

Biometrics Security iTC は 6 月 8 日に第 1 回のオンライン会議を開催し、それ以降ほぼ 3 週間に 1 度の頻度で、合計 12 回のオンライン会議を開催した。ドイツ・フランスとの調整の結果、iTC の議長はフランスになったものの、テクニカルエディタは日本が務めることとなった。主な参加者は、バイオメトリック製品ベンダー、スマートフォン製造企業、評価機関、認証機関、研究機関からの参加者であり、国別では、フランス、ドイツ、米国、日本、オーストラリアなどである。

iTC では、今までに TOR（Terms Of Reference）、活動計画、ESR（Essential Security Requirement）、セキュリティ課題定義を作成し、本報告書執筆時点ではセキュリティ対策方針の作成を入ったところである。cPP は最終的に参加者全員が満足できるものになる必要があるが、本事業で作成した PP から内容が大きく外れることがないように、ESR およびセキュリティ課題定義に対して日本から多数のコメントを提出した。

DSC (Dedicated Security Components) iTC、米国のモバイルデバイスの PP である Protection Profile for Mobile Device Fundamentals を作成する活動との連携が進んでいる。また、CC 関係者のフォーラム CCUF（CC Users' Forum）でも紹介・普及活動を実施している。

4.2.1.3　活動成果

cPP 化の活動を本格化させることができ、フランスおよびドイツと主に連携して、合計 12 回の iTC オンライン会議を実施して、cPP の中間成果物である TOR（Terms Of Reference）、活動計画、ESR（Essential Security Requirement）、セキュリティ課題定義の作成を完了した。

4.2.2　その他の活動

バイオメトリック照合製品の CC 評価・認証を、産業界だけではなく、学界へも普及させるため、ポリシーベース認可の枠組みにバイオメトリック照合製品を組み込むためのソフトウェアアーキテクチャおよび CC 評価・認証結果の扱いについて、2016 年（平成 28 年）5 月 23 日から 25 日まで米国サンノゼで開催された 37th IEEE Symposium on Security and Privacy のポスターセッションで、Poster: A proposal for architecture of biometric authentication products を発表した。

また、2016 年（平成 28 年）9 月 19 日・20 日にドイツのダルムシュタットで開催された EAB Research Projects Conference (EAB-RPC) 2016 および 22 日・23 日に同地で開催された 2016 International Conference of the Biometrics Special Interest Group (BIOSIG)に参加し、バイオメトリック製品のセキュリティ評価を含む、主に欧米での研究およびプロジェクトの状況を調査し、関係者と意見交換した。

4.2.3　今後の課題

cPP の活動は、核となるメンバが積極的に活動し、Biometrics Security iTC への参加者も増えつつある。

平成 28 年度で事業は終了となるが、cPP の内容を拡充するため、今後も継続的に活動する。また、cPP は、性能と PAD とを個別にも評価し得るような柔軟なものを目指しているが、併せて評価する場合のオプションのひとつとして、本事業で作成した PP が実現されるように議論を進めることが必要である。

4.3 セキュリティ評価手法の研究

4.3.1 性能評価手法の研究

4.3.1.1 活動目的

評価機関の独立評価に必要な性能試験手法を研究する。併せて評価機関の独立評価で使用を想定して、性能評価ツールのプロトタイプを完成させる。

4.3.1.2 活動概要

前節の活動目的を達成するにあたり、以下の活動を実施した。

(1) 独立試験手法の研究

サポート文書 性能評価別冊の完成に向け、評価機関による独立試験手順および性能評価の合否判定方法に関する研究を行う。この研究結果に基づいて性能評価別冊に対する改訂作業を実施する。

(2) 性能評価ツールの開発

CC 評価の基盤のひとつとして、評価機関の独立評価で使用を想定して、性能評価ツールのプロトタイプを評価機関からの意見を取り入れながら完成する。

4.3.1.3 活動成果

前節で示した活動内容に関する活動成果についてまとめる。

(1) 独立試験手法の研究

従来、独立試験実施における課題であった、高性能なバイオメトリクス認証製品において多人数の被験者募集を必要とすることによる試験コストの問題を解決し、バイオメトリクス認証製品の性能に拠らず比較的少人数の被験者で実現可能な独立試験方法および合否判定方法を考案した。

(2) 性能評価ツールの開発

評価機関からの意見を反映させ、性能評価ツールのプロトタイプを完成した。

4.3.2 脆弱性評価手法の研究

4.3.2.1 活動目的

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に基づき、必要な偽造物作成方法・攻撃方法を研究する。

4.3.2.2 活動概要

パイロット評価・認証の実施に必要な脆弱性評価手法を研究した。具体的には、評価機関の評価作業を実施のための偽造物作成方法・攻撃方法の研究である。

これらとともに、より信頼性の高い脆弱性評価のため、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、認証機関 IPA に提供する脆弱性評価ツールセットの更新も働きかけた。

さらに、CC 評価の内容は製品の機微な情報を含むため、評価結果の開示範囲などの扱いについて、認証機関である IPA・各企業と調整の上、決定した。

脆弱性評価に必要な偽造生体作成手法等は、必要な関係者に開示したが、攻撃者に対して有益な情報を与える可能性があるので、本報告書には記載しない。

なお、本事業終了後の脆弱性評価手法の活用のため、認証機関である IPA への成果移管に向けた準備も進めている。

4.3.2.3　活動成果

パイロット評価対象の TOE（Target Of Evaluation）を考慮した脆弱性評価手法を研究し、評価機関に提供して、パイロット評価・認証に活用した。研究成果の活用によって、評価機関は、TOE を使った予備テストを経て、TOE に適した偽造生体を設定し、効率的に侵入テストを実施できた。

4. 3. 3　パイロット評価・認証

4.3.3.1　活動目的

パイロット評価・認証に適用する対象製品を選定して IPA および国内評価機関と協力し、パイロット評価・認証を実施し、本事業で検討したセキュリティ評価方法・認証基盤の妥当性と改善点の確認を行う。なお、評価結果の開示範囲などの扱いについては、認証機関である IPA・各企業と調整して決定する。

4.3.3.2　活動概要

本事業で検討したセキュリティ評価方法・認証基盤を適用し、パイロット評価・認証を実施した。実施にあたり、対象製品および評価機関は公募により選定した。

パイロット評価は平成 29 年 2 月 22 日に完了し、評価完了報告書が、産総研に納品され、認証機関である IPA にも送付された。

4.3.3.2.1　対象製品と評価機関の決定

受託 3 者は対象製品となるバオメトリツク照合製品を持たないため、受託者である産総研が静脈を用いたバイオメトリック照合製品を製造・販売する企業とパイロット評価・認証を実施するための共同研究契約を締結し、当該企業から製品を提供してもらい、パイロット評価・認証の対象製品とすることにした。公平を期すために、製品を公募して選定した。その結果、ユニバーサルロボット株式会社の製品を使用することになった。また、CC 評価の評価機関は、産総研での公開入札によって、みずほ情報総研株式会社に決定した。

4.3.3.2.2　パイロット評価・認証の実施

認証申請については、ユニバーサルロボット株式会社から認証申請して、8 月 4 日に IPA に受理された。

評価機関であるみずほ情報総研は、全ての保証クラスの全てのコンポーネントに対して、CC の評価方法論である CEM に規定されている内容に加え、サポート文書、性能評価別冊およびアタックメソッドで規定した評価を実施した。

ST の評価である ASE 評価は、一度は合格となったが、現時点では評価中となっている。理由は、ST 記載内容と他評価クラスのエビデンスとの間に不整合があるからである。評価報告書（案）は、みずほ情報総研から認証機関 IPA へ平成 29 年 2 月 14 日に提出され、産総研へは 2 月 17 日に納品された。

4.3.3.3　活動成果

パイロット評価・認証の実施により、本事業で作成したセキュリティ評価手法が妥当であることを確認した。

4. 3. 4　サポート文書の検証および完成

4.3.4.1　活動目的

性能評価手法と脆弱性評価手法の研究を反映して作成したサポート文書素案をパイロット評価・認証に活用することで検証して完成し、その結果を cPP 活動に反映する。

4.3.4.2　活動概要

パイロット評価・認証で得られた知見と関係者の意見を聴取し、サポート文書を完成した。

CCRA（CC Recognition　Arrangement）でのサポート文書の形式に合わせ、公開のサポート文書と開示先限定のアタックメソッドの二部構成とした。サポート文書については、性能評価の部分は、通常のサポート文書とは異なる詳細な内容を含むので、別冊として作成した。

このサポート文書は、cPP の審議において寄書提出を予定している。

4.3.4.2.1　サポート文書

本サポート文書（付録 2）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（IPA 認証番号 C0501）（付録 1）に適合する製品の評価ガイダンスであり、10 月の第 2 回検討委員会の後に提出されたコメントを反映し、完成させた。

4.3.4.2.2　性能評価別冊

前述 4.3.1 で示した性能評価手法の研究成果として作成した性能評価別冊をパイロット評価で検証した結果および検討委員会での審議を通じて、性能評価別冊（付録 3）を完成させた。記載内容には、開発者が実施する作業として開発者試験計画書・開発者試験報告書の記載事項、および、評価者が実施する作業として、評価者試験計画書の記載事項・独立試験の実施内容・開発者との協議事項が含まれる。

4.3.4.2.3　アタックメソッド

既存のアタックメソッドの構成に倣って、提示型攻撃について、攻撃の記述、攻撃の要点、TOE への影響、攻撃の特性、攻撃例をそれぞれ記述した。第 2 回検討委員会から第 4 回検討委員会にかけて審議し、完成させた。アタックメソッドは限定公開の文書であるが、参加者が限定されている iTC では、cPP およびサポート文書と併せて、アタックメソッドも作成する。今後、本アタックメソッドも iTC へ寄書提出する。

なお、アタックメソッドは、必要な関係者に開示したが、攻撃者に対して有益な情報を与える可能性があるので、本報告書には記載しない。

4.3.4.3　活動成果

バイオメトリック照合製品の CC 評価方法を決めるサポート文書一式を完成させた。パイロット評価に適用した結果、サポート文書に規定した評価手法が妥当であることを確認できた。

4. 3. 5　今後の課題

性能評価に関する今後の課題として、次の事項が考えられる。

- 照合スコアを用いた仮説検定の適用
- 静脈認証以外のモダリティへの対応
- 識別（1:N 認証）への対応
- 性能評価ツールの活用
- 開発者試験コスト低減のための性能評価方法の実現

脆弱性評価については、課題として、次の事項が考えられる。

- 性能評価と同様、静脈認証以外のモダリティへの対応
- 攻撃の進歩に応じた脆弱性評価手法の更新

パイロット評価・認証については、TOE の評価作業は完了したが、まだ合格になっていない。ユニバーサルロボット株式会社が、TOE を 3 月以降に改修の上、各エビデンスを改訂して、再度みずほ情報総研の評価を受ける。現時点では計画作成中であり、計画作成後、IPA に対して評価スケジュールを報告し、認証のスケジュールを決定する。

サポート文書については、cPP 活動に反映させるだけでなく、国際標準化活動にも反映させなければならない。これらの作成の過程で、サポート文書との乖離や齟齬が生じないようにして行く事業関係者を中心とする活動が必要である。

4.4 国際標準化活動

4.4.1 SC 27 および SC 37 での活動

4.4.1.1 活動目的

本事業で作成した PP および脆弱性評価に関する内容を日本がエディターを務める SC 27 の ISO/IEC 19989（Security evaluation of presentation attack detection for biometrics）開発プロジェクトへ反映させると共に、早期に CD 段階へ進めるため、各国との合意形成を行う。

性能に関する CC 評価の国際標準化は現在スタディピリオドにあり、4 月の SC 27 の WG および総会にて、1. NP 提案して新規国際標準開発プロジェクトへ移行する、2. 開発中の ISO/IEC 19989 をパート分割して性能に関するパートを追加し、バイオメトリクス認証製品の CC 評価全体を扱える規格にする、のいずれかを推進する。

また、SC 37 の ISO/IEC 30107 パート 3 は、CD 文書の品質向上に引き続き取り組む。

4.4.1.2 活動概要

SC 27 では、4 月と 10 月の国際会議に出席し、3 件の原案を作成し、3 件の原案に対してコメント作成し、2 件のコメント処理を実施し、4 月の国際会議では 1 件のスタディピリオドのラポータを務めた。

4 月のタンパ会議では、性能のセキュリティ評価を扱うためのスタディピリオド SP on Security evaluation of biometric performance based on ISO/IEC 15408 and 18045 のラポータを務めて、ISO/IEC 19989 のスコープを拡張して、スタディピリオドを統合した。その結果、タイトルを Criteria and methodology for security evaluation of biometric systems と変更し、2 パートに分割した。

10 月のアブダビ会議では、2 つのパートの内容に共通部分が多いとの意見がドイツとフランスで出され、3 パートに分割することが合意された。現在は、パート 1 が Framework、パート 2 が Biometric recognition performance、パート 3 が Presentation attack detection となっている。事業者が、パート 1 およびパート 3 のエディター、パート 2 のコエディターを担当している。パート分割によって、各パートとも WD から再出発した。本事業で作成した PP の拡張セキュリティ機能要件をアブダビ会議に向けてコメントとして提出し、原案に反映させた。現在の各パートの目次は、付録 4 から付録 6 のとおりである。

SC 37 では、7 月と 1 月から 2 月にかけての 2 回の国際会議に出席し、ISO/IEC 30107 パート 3 の文書の品質向上に取り組んだ。

4.4.1.3　活動成果

ISO/IEC 19989 のスコープを拡張して、性能のセキュリティ評価を扱えるようにできた。

また、本事業で作成した PP の拡張セキュリティ機能要件をコメントとして提出し、原案に反映させた。3 パートに分割された ISO/IEC 19989 のパート 1 およびパート 3 のエディターならびにパート 2 のコエディターに事業者が就任した。

SC 37 では、7 月と 1 月から 2 月にかけての 2 回の国際会議に出席し、ISO/IEC 30107 パート 3 の文書の品質向上に取り組み、DIS 段階にした。

4.4.2　今後の課題

ISO/IEC 19989 は、本事業で作成したサポート文書や cPP と共通する内容を含む。また、ISO/IEC 30107 パート 3 とも、できる限り内容の整合を取って進める必要がある。望ましい内容になるように、国内外の技術者と連携・協力して活動を進めて行くことが必要である。

5. 平成28年度活動まとめ

本事業は、バイオメトリクス認証製品の CC（Common Criteria）認証に向け、国内に、①産業界が無理なく参加可能であり、②十分に有効性があり、③継続性のある、バイオメトリクス認証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 28 年度は、下記に取り組んだ。

- ・認証機関・評価機関・ベンダーおよ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
  - - 性能評価手法の検証
  - - 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）
  - - サポート文書の検証および完成
- ・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

バイオメトリクス認証技術に関係する、有識者(2 団体 2 名)・認証機関(IPA 1 名)・評価機関(みずほ情報総研 2 名)・ベンダー(6 社 7 名)・ユーザー(1 社 1 名)・官公庁(2 名)・実施者（3 団体 7 名）から成る検討委員会(22 名)を組織し、都合 4 回の委員会を開催し、事業の実施に関係する事項、研究開発の検討方針、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、検討結果を研究開発にフィードバックした。

これにより、関係者の知見を集め、性能評価手法、脆弱性評価手法の検討・検証を進めることができ、平成 27 年度に認証取得したバイオメトリック照合製品 PP に基づく静脈認証製品に係わるサポート文書をまとめることができた。また、その内容を国際標準化活動に向けて、日本の代表者に提供することができた。

（2）国際連携活動

本事業の成果であるバイオメトリック照合製品 PP およ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 化の活動を本格化した。

cPP 化の活動には、本事業の成果である性能評価およ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も含めて取り組んだ。国内各社の議論への参加は決定しているが、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、より大きな活動にすることにも取り組んだ。この際、バイオメトリクス認証製品 PP を既に開発し CC 評価・認証を実施しているドイツおよびフランスを主たる連携候補として活動した。

合計 12 回の iTC オンライン会議を実施して、cPP の中間成果物である TOR（Terms Of Reference）、活動計画、ESR（Essential Security Requirement）、セキュリティ課題定義の作成を完了した。会議を重ねるに連れて、iTC 参加者間の信頼関係が形成された。

(3) セキュリティ評価手法の研究

（a）性能評価手法の研究

評価機関の独立評価に必要なバイオメトリック照合製品の性能試験手法を研究するとともに、評価機関の独立評価で使用を想定して評価機関からの意見を取り入れながら性能評価ツールのプロトタイプを完成することに取り組んだ。

独立試験手法の研究では、従来、独立試験実施における課題であった、高性能なバイオメトリクス認証製品において多人数の被験者募集を必要とすることによる試験コストの問題を解決し、バイオメトリクス認証製品の性能に拠らず比較的少人数の被験者で実現可能な独立試験方法および合否判定方法を考案した。

性能評価ツールの開発では、性能評価ツールのプロトタイプを完成した。

（b）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 27 年度までに検討した偽造物検知の評価方針案に基づき、評価機関の評価作業のための偽造物作成方法・攻撃方法を研究した。

パイロット評価対象の TOE を考慮した脆弱性評価手法を研究し、評価機関に提供して、パイロット評価に活用した。研究成果の活用によって、評価機関は、TOE を使った予備テストを経て、TOE に適した偽造生体を設定し、効率的に侵入テストを実施できた。

（c）パイロット評価・認証

パイロット評価・認証に適用する対象製品を選定して IPA および国内評価機関と協力し、パイロット評価・認証を実施し、本事業で検討した CC 認証に沿ったバイオメトリクス認証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った。

評価対象製品としてユニバーサルロボット株式会社の製品を選定し、評価機関であるみずほ情報総研は、全ての保証クラスの全てのコンポーネントに対して、CEM に規定されている内容に加え、サポート文書、別冊およびアタックメソッドで規定した評価を実施した。

これらにより、本事業で作成したセキュリティ評価手法が妥当であることを、実際の CC 評価への適用によって確認できた。

（d）サポート文書の検証および完成

性能評価手法と脆弱性評価手法の研究を反映して作成した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し、サポート文書と性能評価別冊ならびにアタックメ

ソットからなるサポート文書一式を完成した。

これらをパイロット評価に適用した結果、サポート文書に規定した評価手法が妥当であることを確認できた。

(4) 国際標準化活動

本事業で作成した PP および脆弱性評価に関する内容を SC 27 の ISO/IEC 19989 開発プロジェクトへ反映させると共に、早期に CD 段階へ進めるため、各国との合意形成を行い、スコープを拡張して､性能のセキュリティ評価を扱えるようにできた｡本事業で作成した PP の拡張セキュリティ機能要件をコメントとして提出し、原案に反映させた。3 パートに分割された ISO/IEC 19989 のパート 1 およびパート 3 のエディターならびにパート 2 のコエディターに事業者が就任した。

また、SC 37 の ISO/IEC 30107 Part3 は、7 月と 1 月から 2 月にかけての 2 回の国際会議に出席し、文書の品質向上に取り組んだ。

6. 今後に向けて

受託事業の終了により、今回の事業で取り組んだ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・普及基盤構築に向けた活動は終了する。今回の取り組みでは、バイオメトリック照合製品 PP とそれに基づく静脈認証製品に係わるサポート文書が整備できた。

しかしながら、全てのバイオメトリクス認証製品に対して、CC（Common Criteria）認証に沿ったセキュリティ評価・認証を行うための基盤が整備できた訳ではなく、まだまだ端緒についたばかりである。

以下、バイオメトリクス認証製品のセキュリティ評価・認証を行うための基盤を整備・活用してゆくために、今後の取り組みが必要と思われることを述べる。

（1）国際連携活動

cPP の活動は、核となるメンバが積極的に活動し、参加者も増えつつある。

平成 28 年度で事業は終了となるが、cPP の内容を拡充するため、今後も継続的に活動する。また、cPP は、性能と PAD とを個別にも評価し得るような柔軟なものを目指しているが、併せて評価する場合のオプションのひとつとして、本事業で作成した PP が実現されるように議論を進めることが必要である。

（2）セキュリティ評価手法の研究

（a）性能評価手法の研究

性能評価に関する今後の課題として、次の事項が考えられる。

- 照合スコアを用いた仮説検定の適用
- 静脈以外のモダリティへの対応
- 識別（1:N 認証）への対応
- 性能評価ツールの活用
- 開発者試験コスト低減のための性能評価方法の実現

（b）脆弱性評価手法の研究

脆弱性評価については、課題として、次の事項が考えられる。

- 性能評価と同様、静脈以外のモダリティへの対応
- 攻撃の進歩に応じた脆弱性評価手法の更新

（c）パイロット評価・認証

パイロット評価・認証については、TOE の評価作業は完了したが、まだ合格になっていない。ユニバーサルロボット株式会社が、TOE を 3 月以降に改修の上、各エビデンスを改訂して、再度みずほ情報総研の評価を受ける。現時点では計画作成中であり、計画作成後、IPA に対して評価スケジュールを報告し、認証のスケジュールを決定する。

（d）サポート文書

サポート文書については、cPP 活動に反映させるだけでなく、国際標準化活動にも反映させなければならない。これらの作成の過程で、サポート文書との乖離や齟齬が生じないようにして行く事業関係者を中心とする活動が必要である。

(3) 国際標準化活動

ISO/IEC 19989 は、本事業で作成したサポート文書や cPP と共通する内容を含む。また、ISO/IEC 30107 パート 3 とも、できる限り内容の整合を取って進める必要がある。望ましい内容になるように、国内外の技術者と連携・協力して活動を進めて行くことが必要である。

(4) 産業界としての取り組みの仕掛け

今回の事業で取り組んだバイオメトリック照合製品 PP とそれに基づく静脈認証製品に係わるサポート文書を用いて、静脈を用いたバイオメトリック照合製品の CC（Common Criteria）認証に沿ったセキュリティ評価・認証基盤が今後活用され、何件かの評価・認証の取り組みがされるに従い、本事業で開発したセキュリティ評価手法の見直しやサポート文書の改訂が必要になる場合が出てくることも予想される。

また、今回の事業で取り組んだ国際標準化活動や cPP 化活動は、国際の場で取り組みが始まったばかりであり、日本のバイオメトリクス認証業界として、継続した対応が必要である。

これらの対応を行うために、バイオメトリクス認証製品のセキュリティ評価に係わる関係者が一堂に会して意見交換や合意形成することが必要になることも考えられる。そのため、今回の事業関係者で対応体制の整備に取り組む。

付録１　バイオメトリック照合製品 PP（20160331）

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

1.2 版

2016/03/23

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 1.2
発行 平成 28 年 3 月 31 日
発行者 国立研究開発法人 産業技術総合研究所
登録 独立行政法人情報処理推進機構
認証番号 C0501
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、登録対象のユーザーに対して、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、ユーザー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。

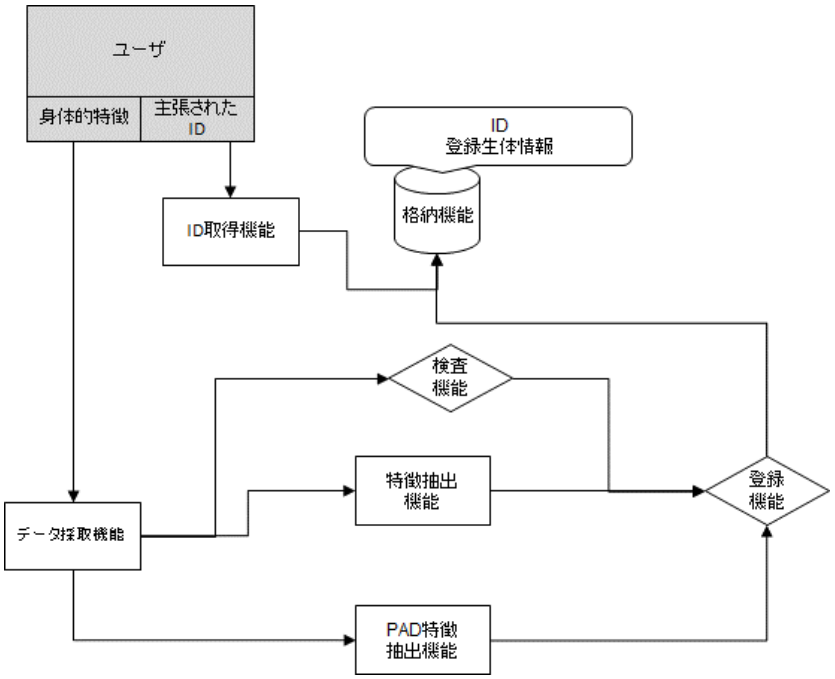


図 1 登録の処理

バイオメトリック照合処理は、ユーザーが提示した身体的特徴が登録生体情報と同一のユーザーのものであるかを判定する TOE の主機能である。登録ユーザーは 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ー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。

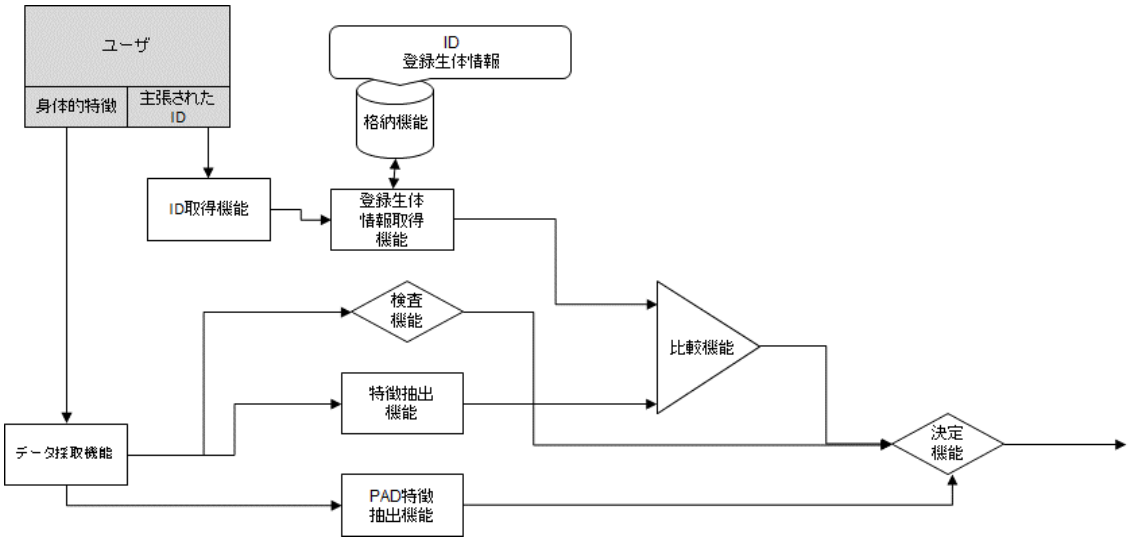


図 2 バイオメトリック照合の処理

本 PP では、登録ユーザーがバイオメトリック照合され利用者認証された結果、登録ユーザーは 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ーは ID 入力を必要としない。システムがユーザー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ー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ー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。

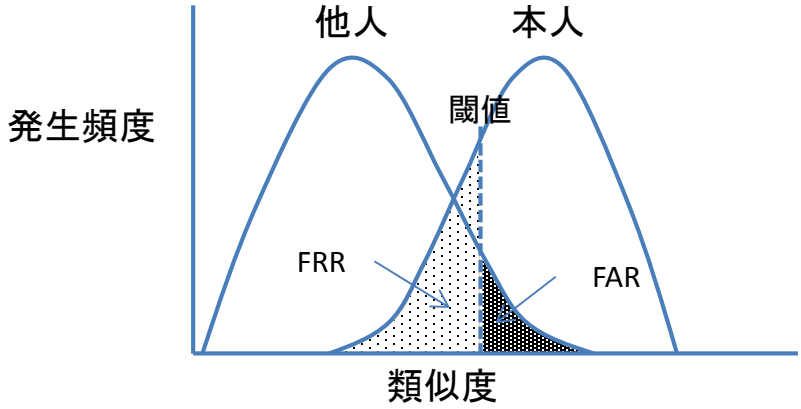


図 3 バイオメトリック照合の類似度分布

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、ユーザーを表す。

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。

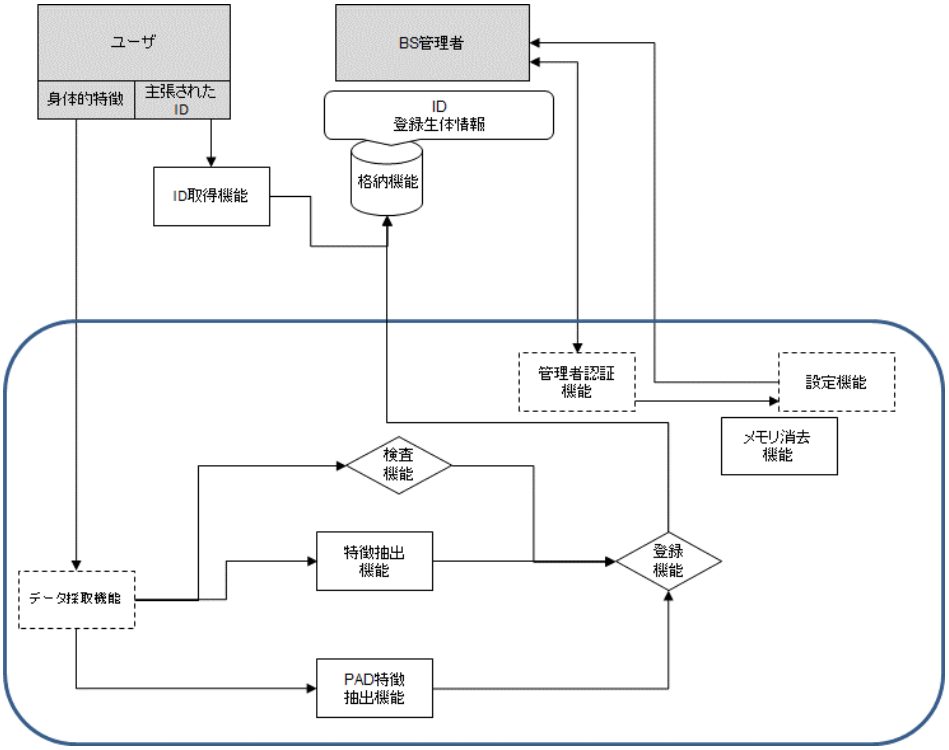


図 4　一般的な TOE の構成（登録の場合）

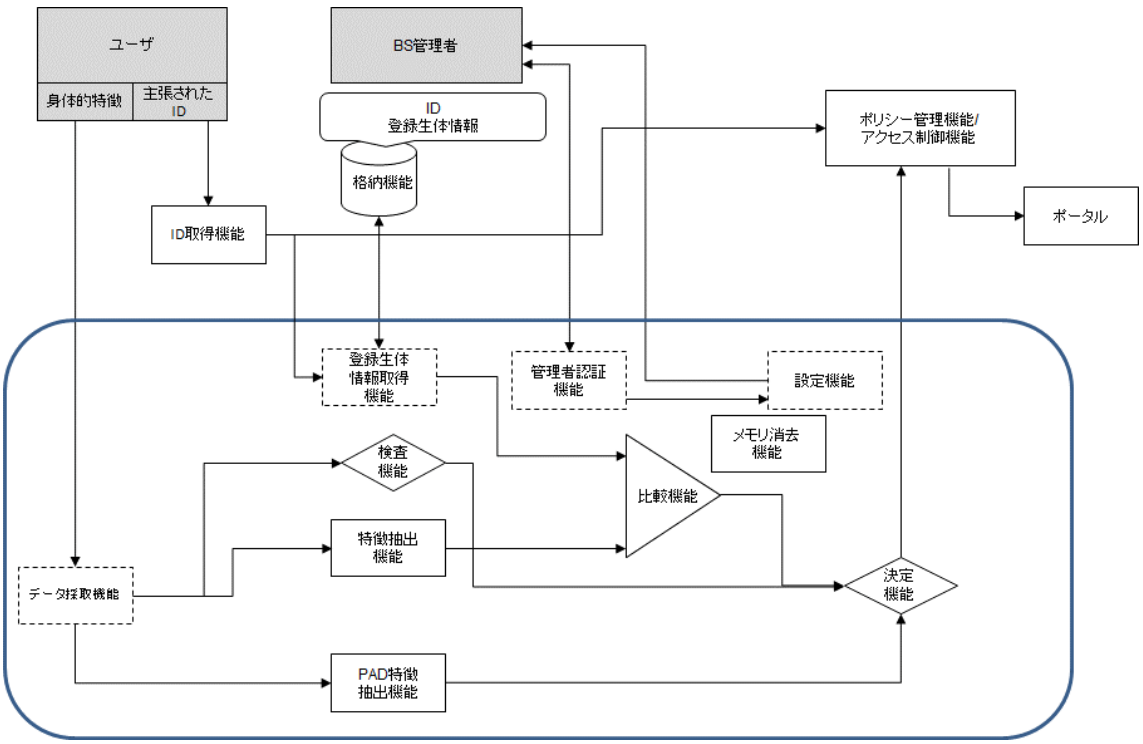


図 5 一般的な TOE の構成（照合の場合）

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、BS（Biometric System。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）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を指す。本 PP では、偽造生体と品質の低い生体情報の提示のみを対象としている。
- 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、ユーザー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、ユーザーの 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、ユーザー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、ユーザーが入力する 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、ユーザー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、ユーザー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、ユーザーの権利をチェックし､ユーザー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、ユーザー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 からユーザーの 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。

登録ユーザー：

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、登録ユーザーが 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、登録ユーザー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、登録ユーザーの 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、登録ユーザーの 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

登録ユーザーの生体情報登録は、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

登録ユーザー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

登録ユーザー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ー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、ユーザー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、当該ユーザー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、登録ユーザーの 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ー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、登録ユーザーの 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ー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ー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ー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ーのその他の情報は、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、登録ユーザー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：

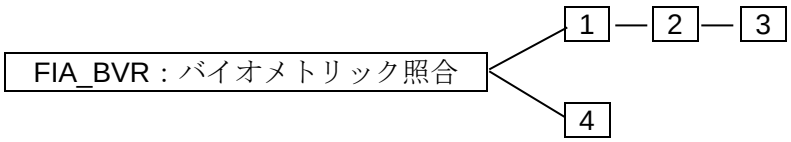
FTE の定義は、TOE の登録ポリシーに依存する。ST 作成者はそのポリシー概略を示さなければならない。

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。提示型攻撃には死体の身体部分を利用したデータの提示なども含まれるが、本 PP では偽造生体と品質の低い生体情報の提示のみを対象とする)
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

用語	意味
	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。
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。
登録ユーザー	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ー
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	ユーザー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ー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。
ユーザー	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

用語	意味
	ザーがその ID に対応する本人であることを確認する行為
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　サポート文書

Evaluation Guidance
for
Biometric Verification Products
Version 1.0

March 2017

National Institute of Advanced Industrial Science and Technology
OKI Software Co., Ltd.

Contents

1. Introduction

This document is the evaluation guidance for biometric verification products that claim a conformance to "Protection Profile for Biometric Vefirication Products" certified as C0501 by IPA (Information-technology Promotion Agency, Japan) and PPs or STs that define the same or similar SFRs.

This document contains evaluation guidance for both performance evaluation and presentation attack detection (PAD) evaluation. After addressing the relation between ATE class and AVA class for PAD evaluation, the complements of evaluation methodology for performance and PAD evaluations are specified. Because there are only five complements for performance evaluation at ATE_FUN.1-1, ATE_IND.2-6, ATE_IND.2-7, ATE_IND.2-8, and ATE_IND.2-10, the complements are for PAD evaluations unless otherwise specified as "for performance evaluation". The complements contain mandatory activities that the evaluator shall perform in order to assign verdicts. However all of them may not be applicable to all type of the TOEs. Evaluator can provide a justification to assign pass verdicts in such cases.

For the current version, there are two separate documents "Annex for Biometric Verification Product Evaluation Guidance" to specify the details of performance evaluation and "Attack Method for Vein Products" to specify more details of PAD evaluation for vein products.

Most of the contents of this document are based on Fingerprint Spoof Detection Evaluation Guidance (FSDEG), which was a contribution to ISO/IEC JTC 1/SC 27, and D6.5: Towards the Common Criteria evaluations of biometric systems of Biometric Evaluation and Testing (BEAT) project in EU.

2. Terms and definitions

biometric characteristic

biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition

modality

type of biometric data

3. Relation between ATE class and AVA class in PAD testing

This clause addresses relevant aspects for Class ATE and Class AVA.

It is the objective of any testing activity conducted in the course of the ATE class to

determine whether the PAD functionality is able to detect Presentation Attack Instruments (PAIs) as specifed in Security Target, Functional Specification, and TOE Design. In the deveopler testing (ATE_FUN), the developer prepares and constructs PAIs to test the PAD functionality to show that it works as specified. In the independent testing (ATE_IND), the evaluator samples and repeats the developer testing using and/or rebuilding the PAIs constructed by the developers. The evaluator also devises a test subset which is appropriate and effective to the TOE and conducts the testing, The evaluator should modify the PAIs created by the developer.

While the testing activities in context of ATE allow an overall assessment about the performance of the PAD mechanism for the tested PAIs, they do not provide any assurance about the PAD effectiveness for different PAIs. It falls to the vulnerability assessment to evaluate whether the use of additional PAIs that have not been part of the developer's PAIs can lead to exploitable vulnerabilities.

AVA testing extends the scope of ATE testing to add variations of the PAIs independently prepared by the evaluator investigating potential vulnerabilities based on the information that was found in the previous evaluation activities including ATE. The objective of AVA testing is to further explore and probe the boundaries of errors discovered during ATE testing, if there are, to estimate their applicability in the corresponding attack potential and to search for vulnerabilities that ATE testing does not uncover. The evaluator identifies possible areas of weakness and iteratively probes these areas using specially constructed PAIs, refining the PAIs and the presentation techniques in order to find vulnerabilities.

4. Workload for vulnerability evaluation

No rigid rules can be given on how much time should be spent on a typical biometric verification product of AVA_VAN.2 evaluation by a competent lab, but the following guidance shall none-the-less be provided in an effort to harmonise evaluations: Assuming the CC vulnerability analysis has already been performed the evaluation testing from scratch for a biometric verification product should take about 1 or 2 man weeks, depending on the characteristic and complexity of the product etc..

5. Complements to CEM on Class ASE: Security Target evaluation

5.1. Evaluation of sub-activity (ASE_INT.1)

Table 1 lists the complements to the work units in ASE_INT.

Table 1 — Complements to ASE_INT

Evaluator action element	Work unit	Complements
ASE_INT.1.1E	ASE_INT.1-1	None.
	ASE_INT.1-2	None.
	ASE_INT.1-3	None.
	ASE_INT.1-4	The evaluator ***shall also examine*** the TOE reference to determine that it clearly identifies the modality that the presentation attack detection system can be used for.
	ASE_INT.1-5	The evaluator ***shall also examine*** the TOE overview to determine that it states that the TOE provides presentation attack detection functionality. For performance evaluation, the evaluator **shall also examine** the TOE overview to determine that it states a specific user profile that the TOE is not designed to work with (e.g., over 65 years of age, right-handed or men).
	ASE_INT.1-6	None.
	ASE_INT.1-7	The evaluator ***shall also examine*** the TOE overview to determine that it does not claim error rates for presentation attack detection functionality.
	ASE_INT.1-8	None.
	ASE_INT.1-9	None.
	ASE_INT.1-10	None.

5.2. Evaluation of sub-activity (ASE_REQ.2)

Table 2 lists the complements to the work units in ASE_REQ.2-1E.

Table 2 — Complements to ASE_REQ.2.1E

Evaluator action element	Work unit	Complements
ASE_REQ.2.1E	ASE_REQ.2-1	None.
	ASE_REQ.2-2	None.
	ASE_REQ.2-3	The evaluator ***shall also examine*** the ST to determine that a value equal to or greater than the upper bound of

		the 90%, 95%, or 99% confidence interval is assigned for each of FTE, FAR, and FRR, and that a value equal to or greater than the upper bound of the 95% confidence interval is additionally described for each of FTE, FAR, and FRR if 90% or 99% is selected as the confidence level.

6. Complements to CEM on Class ADV: Development

6.1. Evaluation of sub-activity (ADV_ARC.1)

There are no complements to the work units in ADV_ARC.

6.2. Evaluation of sub-activity (ADV_FSP.2)

Table 3 lists the complements to the work units in ADV_FSP.2.1E. There are no complements in ADV_FSP.2.2E.

Table 3 — Complements to ADV_FSP.2.1E

Evaluator action element	Work unit	Complements
ADV_FSP.2.1E	ADV_FSP.2-1	The evaluator ***shall also check*** the functional specification to determine that the various mechanisms used for presentation attack detection are described in terms of TSFIs.
	ADV_FSP.2-2	None.
	ADV_FSP.2-3	The evaluator ***shall also examine*** the functional specification to determine how the capture devices are used when biometric characteristics are presented if they are part of the TOE.
	ADV_FSP.2-4	The evaluator ***shall also examine*** the presentation of the TSFI to determine that it completely identifies security relevant parameters for capture devices.
	ADV_FSP.2-5	The evaluator ***shall also examine*** the presentation of the TSFI to determine that it completely and accurately describes security relevant parameters for capture

		devices.
	ADV_FSP.2-6	None.
	ADV_FSP.2-7	The evaluator ***shall also examine*** the presentation of the TSFI to determine that it does not provide feedback on the decision of the presentation attack detection to the user.
	ADV_FSP.2-8	None.

6.3. Evaluation of sub-activity (ADV_TDS.1)

Table 4 lists the complements to the work units in ADV_TDS.1.1E. There are no complements in ADV_TDS.1.2E.

Table 4 — Complements to ADV_TDS.1.1E

Evaluator action element	Work unit	Complements
ADV_TDS.1.1E	ADV_TDS.1-1	None.
	ADV_TDS.1-2	None.
	ADV_TDS.1-3	None.
	ADV_TDS.1-4	The evaluator ***shall also examine*** the TOE design to determine that it describes biometric properties and mechanisms which are used to detect presentation attacks at the subsystem layer, i.e., the processing of signals acquired by the capture devices used for presentation attack detection and the transformation of these signals into classification of presentation attack.
	ADV_TDS.1-5	The evaluator ***shall also examine*** the TOE design to determine that the interactions between the presentation attack detection functionality and the capturing functionality are described at the subsystem layer.
	ADV_TDS.1-6	None.

7. Complements to CEM on Class AGD: Guidance documents

7.1. Evaluation of sub-activity (AGD_OPE.1)

Table 5 lists the complements to the work units in AGD_OPE.1.1E. There are no complements in AGD_OPE.1.2E.

Table 5 — Complements to AGD_OPE.1.1E

Evaluator action element	Work unit	Complements
AGD_OPE.1.1E	AGD_OPE.1-1	None.
	AGD_OPE.1-2	The evaluator ***shall also examine*** the operational user guidance to determine that it describes the process of presenting biometric characteristics to the TOE if the capture devices are part of the TOE.
	AGD_OPE.1-3	The evaluator ***shall also examine*** the operational user guidance to determine that it describes the secure configuration of presentation attack detection parameters.
	AGD_OPE.1-4	The evaluator ***shall also examine*** the operational user guidance to determine that it describes alternative procedures allow an operator to manually override the decision of the presentation attack detection.
	AGD_OPE.1-5	The evaluator ***shall also examine*** the operational user guidance to determine that it describes mode of operation of the TOE that an operator can manually override the decision of the presentation attack detection.
	AGD_OPE.1-6	None.
	AGD_OPE.1-7	None.
	AGD_OPE.1-8	None.

7.2. Evaluation of sub-activity (AGD_PRE.1)

Table 6 lists the complements to the work units in AGD_PRE.1.1E. There are no complements in AGD_PRE.1.2E.

Table 6 — Complements to AGD_PRE.1.1E

Evaluator action element	Work unit	Complements
AGD_PRE.1.1E	AGD_PRE.1-1	None.
	AGD_PRE.1-2	The evaluator ***shall also examine*** the provided installation procedures to determine that they describe, in particular, parameters that modify the security functionality of presentation attack detection (e.g. a threshold) and that have to be configured before the initial usage of the TOE.

8. Complement to CEM on Class ALC: Life-cycle support

8.1. Evaluation of sub-activity (ALC_DEL.1)

Table 7 lists the complements to the work units in ALC_DEL.1.1E.

Table 7 — Complements to ALC_DEL.1.1E

Evaluator action element	Work unit	Complements
ALC_DEL.1.1E	ALC_DEL.1-1	The evaluator ***shall also examine*** the delivery documentation to determine that it describes whether the TOE is readily available for all kind of customers or only purchased by restricted customers.
	ALC_DEL.1-2	None.

8.2. Evaluation of sub-activity (ALC_FLR.1)

The following shall be applied to all the work units in ALC_FLR.

The evaluator shall determine that PAIs which are falsely accepted by the presentation attack detection system are considered being security flaws in the developers' processes.

9. Complements to CEM on Class ATE: Tests

9.1. Evaluation of sub-activity (ATE_FUN.1)

Table 8 lists the complements to the work units in ATE_FUN.1.1E.

Table 8 — Complements to ATE_FUN.1.1E

Evaluator action element	Work unit	Complements
ATE_FUN.1.1E	ATE_FUN.1-1	For performance evaluation, the evaluator ***shall particularly check*** that the test documentation satisfies the relevant requirements from ISO/IEC 19795, listed in 1 of Annex. The evaluator ***shall explain*** any deviation from the requirements from ISO/IEC 19795, listed in 1 of Annex, in the test documentation.
	ATE_FUN.1-2	The evaluator ***shall also examine*** the test plan to determine that it provides information on the attack type that were created by the developer for the tests including detailed information on the PAI species such as material information and construction manuals, and method of interaction with the capture device.
	ATE_FUN.1-3	The evaluator ***shall also examine*** the test plan in particular to determine that potential presentation attack detection parameters are correctly configured according to the TOE configuration described in the ST.
	ATE_FUN.1-4	None.
	ATE_FUN.1-5	None.
	ATE_FUN.1-6	None.
	ATE_FUN.1-7	In particular, the evaluator ***shall also report*** the developer testing efforts for presentation attack detection functionality in terms of number and description of the attack types, PAI species, and test size.

9.2. Evaluation of sub-activity (ATE_IND.2)

Table 9 lists the complements to the work units in ATE_IND.2.

Table 9 — Complements to ATE_IND.2.1E

Evaluator action element	Work unit	Complements

	ATE_IND.2-1	The evaluator ***shall also examine*** to determine that potential presentation attack detection parameters are correctly configured according to the TOE configuration described in the ST.
	ATE_IND.2-2	None.
	ATE_IND.2-3	None.
ATE_IND.2.2E	ATE_IND.2-4	The evaluator ***shall also conduct*** testing using or rebuilding the PAIs created by the developer.
	ATE_IND.2-5	None.
ATE_IND.2.3E	ATE_IND.2-6	The evaluator ***shall particularly devise*** a test subset in which the evaluator uses or rebuilds PAIs created by the developer in a different manner from that done by the developer, such as presenting PAIs in a different manner. The evaluator ***shall consider*** modifying PAIs created by the developer for testing. The evaluator ***shall also consider*** disabling the PAD mechanism in the TOE to refine PAIs so that they can falsely accepted by the biometric verification mechanism of the TOE, if such TOE is available for testing. For performance evaluation, the evaluator ***shall devise*** independent performance testing as described in 2 in Annex.
	ATE_IND.2-7	For performance evaluation, the evaluator ***shall produce*** test documentation which satisfies the relevant requirements from ISO/IEC 19795, listed in 2 of Annex. The evaluator ***shall explain*** any deviation from the requirements in 2 of Annex in the test documentation.
	ATE_IND.2-8	For performance evaluation, the evaluator ***shall conduct*** independent performance testing as described in 2 in Annex.
	ATE_IND.2-9	The evaluator ***shall also record*** PAI modification and its usage.
	ATE_IND.2-10	For performance evaluation, the evaluator ***shall check*** the test result using the method described in 2 in Annex.
	ATE_IND.2-11	The evaluator ***shall particularly report*** in the ETR the

		evaluator testing effort on presentation attack detection functionality in terms of number and description of attack types, PAI species and test size.

10. Complements to CEM on Class AVA: Vulnerability assessment

The vulnerability analysis is an assessment to determine whether potential vulnerabilities (as identified during the evaluation of the development and anticipated operation of the TOE or by other methods) may allow attackers to violate the security functional requirements.

10.1. Evaluation of sub-activity (AVA_VAN.2)

Table 10 lists the complements to the work units in AVA_VAN.2.

Table 10 — Complements to AVA_VAN.2

Evaluator action element	Work unit	Complements
AVA_VAN.2.1E	AVA_VAN.2-1	The evaluator ***shall also examine*** the TOE to determine that potential presentation attack detection parameters are correctly configured according to the TOE configuration as described in the ST.
	AVA_VAN.2-2	None.
AVA_VAN.2.2E	AVA_VAN.2-3	None.
AVA_VAN.2.3E	AVA_VAN.2-4	The evaluator ***shall refer*** to Attack Method to identify possible potential vulnerabilities in the TOE.
	AVA_VAN.2-5	None.
AVA_VAN.2.4E	AVA_VAN.2-6	The evaluator ***shall refer*** to Attack Method to devise penetration tests.
	AVA_VAN.2-7	The evaluator ***shall produce*** penetration test documentation particularly including construction manuals of the PAIs.
	AVA_VAN.2-8	None.
	AVA_VAN.2-9	The evaluator ***shall also record*** the PAI construction and usage.
	AVA_VAN.2-10	None.
	AVA_VAN.2-11	The evaluator ***shall refer*** to 10.2 to determine ratings of

		presentation attacks.
	AVA_VAN.2-12	The evaluator ***shall refer*** to 10.2 to determine ratings of presentation attacks.

10.2. Calculating attack potential

To complete an attack potential calculation the points for identification and exploitation (see 10.2.1) have to be added as both phases together constitute the complete attack. When presenting the attack potential calculation, the evaluators will make an argument for the appropriateness of the parameter values used, and will therefore give the developer a chance to challenge the calculation before certification. The final attack potential result will therefore be based on discussions between the developer, the evaluator and the certification body, with the certification body making the final decision if agreement cannot be reached.

The calculation of attack potential given here is the one at the present and subject to change as the biometric technologies and the attacks against them progress.

10.2.1. Phase (Identification/Exploitation)

Identification: corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. One of the outputs from Identification could be a script that gives a step-by-step description of how to carry out the attack. This script is assumed to be used in the exploitation part.

Exploitation: corresponds to achieving the attack on an instance of the TOE in its exploitation environment using the analysis and techniques defined in the identification part. Could be assumed that a different attacker carries out the exploitation, the technique (and relevant background information) could be available for the exploitation in the form of a script or set of instructions defined during the identification step. This type of script is assumed to identify the necessary equipment and, for example, mathematical techniques used in the analysis, or presentation attack methods. Furthermore, this same information may also reduce the exploitation requirement to one of time measurement, whereas the identification phase may have required reverse engineering of hardware or software information hence the expertise requirement may be reduced.

Notes:

For the evaluator, the work of the Identification phase has to be fully performed: developing HW and SW, creating presentation attack instruments (PAIs) if any, etc. The rating of this phase corresponds to the "real spending" in defining the attack. For the Exploitation, it is not necessary to perform the work again and the rating could correspond to an evaluation of the necessary effort for each factor.
Exploitation consisting in applying scripts, it is expected that some factor values will be reduced from the identification phase, in particular "Elapsed Time" and "Expertise". For the same reason, the "Knowledge of the TOE" factor is not applicable in the exploitation phase (all the knowledge is scripted).

10.2.2. Factors to be considered

Elapsed Time

In the Identification phase, it corresponds to the time required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary hardware or software equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. One of the outputs from Identification could be, for instance, a script that gives a step-by-step description of how to carry out the attack this script is assumed to be used in the exploitation part.
Applied to presentation attacks, elapsed time in identification corresponds to the time spent to find the so called "golden fake" and to define the method to build it from for example a fingerprint (with or without the collaboration of the user). "Golden fake" is defined as a PAI that is reproducibly accepted by the TOE as being genuine.
In the exploitation phase, Elapsed Time corresponds to the time necessary to apply the "script" to a specific biometrics. For example, for a presentation attack on fingerprints, it corresponds to the time required to create a PAI from an image of a print (and not the acquisition of this image which is taken into account in the "Access to biometric characteristics" factor).
Potential difficulties to have an access to the TOE in exploitation environment are taken into account in the " Window of opportunity / Access to the TOE " factor.

Expertise

This factor refers to the level of proficiency required by the attacker and the general knowledge that he possesses, not specific of the TOE being attacked. A suggested rating for this metric is:
Layman: no real expertise needed, any person with a regular level of education is capable of

performing the attack. For example, creating a PAI in a known (published) way without specific difficulties (specific or difficult to buy materials) is considered at a "Layman" level of expertise.

Proficient: some advanced knowledge in certain specific topics (biometrics) is required as well as good knowledge of the state-of-the-art of attacks. The person is capable of adapting known attack methods to his needs. For example, adapting a known PAI type (published) by the choice of specific (not published and sometimes difficult to find) materials in order to bypass a presentation attack detection mechanism and/or finding a non-evident way to present this PAI to the system can be considered at a "Proficient" level of expertise.

Expert: a specific preparation in multiple areas such as pattern recognition, computer vision or optimization is needed in order to carry out the attack. The person is capable of generating his own new attacking algorithms. For example, finding a new (unpublished) way of creating a PAI type using new and specific materials (unpublished) to counter an advanced presentation attack detection mechanism, can be considered at a "Expert" level. In addition, this level can be associated with specific equipment (bespoke)

Multiple experts: the attack needs the collaboration of several people with high level expertise in different fields (e.g., electronics, cryptanalysis, physics, etc.). It has to be noticed that a specific competence in biometrics is not considered as "multiple expertise". For example, building an "hill climbing" attack when the comparison score can only be accessed indirectly (for example using power or electromagnetic analysis) and when this attack requires electronic modification of the system (probing for example) can be considered at a "multi expertise" level.

Notes:

As previously noted, Exploitation expertise is usually lower that Identification expertise. Layman or Proficient can be considered as typical value for expertise in the exploitation phase. For the same reason, the multiple expert level is excluded from the exploitation phase.

As all the factors, higher rating would require specific justifications from the evaluator.

Knowledge for the TOE

This factor refers to the amount of knowledge of system required to perform the attack.

For instance, format of the acquired samples, size and resolution of acquisition systems, specific format of templates, but also specifications and implementation of countermeasures are knowledge that could be required to set up an attack.

This information could be publicly available at the website of the capture device manufacturer or protected (distributed to stakeholders under NDA or even classified inside

the company).
Ratings are:
Public: information which is fairly easy to obtain (e.g., on the web).
Restricted: information which is only shared by the developer and organizations which are using the system, usually under a non-disclosure agreement.
Confidential: information which is only available within the organization that develops the system and is in no case shared outside it.
Critical: it refers to information which is only available to certain people or groups within the organization which develops the system.
Special attention should be paid in this point to possible countermeasures that may be implemented in the system and whether it is necessary or not to have knowledge of their existence in order to be successful in a given attack.
It is assumed that all the knowledge required to perform the attack is gained during the identification phase and "scripted" for the exploitation. So, this factor is not used for the exploitation phase.

Window of Opportunity/ Access to the TOE
This factor refers to measuring the difficulty to access the TOE either to prepare the attack (Identification phase) or to perform it on the target system.
For the Identification phase, elements that should be taken into account include the easiness to buy the same biometrics equipment (with and without countermeasures).
For exploitation phase, both technical (such known/unknown tuning) and organizational measures (presence of a guard, ability to physically modify the target, limited number of tries, etc.) should be taken into account.
The number and the level of equipment requested to build the attack is also part of the rating.
This factor is not expressed in terms of time. Proposed values are:
Easy:
There is no strong constraint for the attacker to buy TOE (reasonable price) to prepare its attack (identification phase).
For the exploitation phase, there is no limit in the number of tries and the presentation attack is difficult to detect.
Medium:
For identification phase, specialized distribution schemes exist (not available to individuals).
For exploitation phase, either a tuning of the attack for the final system is required (unknown parameterization of countermeasures for example), or there is a supervision of the

biometrics system emitting, for example, an alert in case of numerous fail presentations.
Difficult:
For identification phase, the system is not available except for identified users and access requires compromising of one of the actors.
For exploitation, for example PAIs must be adapted to the (unknown) specific tuning, or there is a strong supervision (for example a guard), or the system needs physical modification (for example physically accessing a hidden signal significant of the comparison score). Compromising one actor involved in the use of the system (guard, administrator, and maintenance) is often required.

Window of Opportunity/ Access to Biometric characteristics

Common Criteria evaluations are dedicated to evaluate the intrinsic resistance of a system. Due to the potential number of attack paths (with or without the cooperation of a user for example) the evaluation does not take into account the way a real biometric characteristic is acquired. For presentation attack detection, the vulnerability analysis is based on the hypothesis that a real "image" is available, and the rating only concerns the creation and the presentation of a presentation attack instrument (PAI).
However, it seems important to be able to compare the resistance of various systems, even based on different biometrics. In addition, getting a real "image" to build a PAI is clearly part of an attack and it seems of interest, for the final user and the pertinence of a certificate to add a factor related to this topic.
2D images can be found even without direct contact with a user (an exploration of the web and the social networks is probably sufficient); 3D images require multiple acquisitions, probably in a controlled way, without user collaboration but probably with a direct contact with him; fingerprints are left on objects the user had in hand, but need to be revealed, acquired and the corresponding images need a preprocessing; Iris images can be acquired with a high resolution camera, but with some difficulties to get a complete high quality image without user cooperation; veins are a hidden characteristic, but infra-red cameras, close to the user, can acquire images to be used.
Multi-modality (e.g. finger and face) or multi-instances (e.g. several fingers) systems should be rated at the upper level of the higher rate. For example, 2D images and Iris are rated Difficult.
Note: As explained before, rating the resistance of a system is based on rating the successful attacks and verifying that no successful attack is found at the targeted level.
Some attacks do not need real biometrics data to be available, for example, attacks based on synthetic images or templates generation. In such a case, the value for this factor has to

be set to 0.

Note: The aforementioned explanations assume that the legitimate user(s) are noncooperative with the attacker. If - for some specific reason - there is reason to assume that a user will give deliberately give access to their biometric characteristic, the rating value for the access to this biometric characteristic would be 0.

Equipment

This factor refers to the type of equipment required to perform the attack. This includes the biometric databases used (if any). A suggested rating is:

Standard: equipment which is affordable, easy to obtain and simple to operate (e.g., computer, video cameras, mobile phones, "do it yourself" material, artistic leisure materials, ...).

Specialized: this refers to fairly expensive equipment, not available in standard markets and which require of some specific formation to be used (e.g., laboratory equipment, advanced printer specific materials and inks, advanced oscilloscopes, ...).

Bespoke: this refers to very expensive equipment with difficult and controlled access; for example, research printing systems with specific ink definition and flexible support adaptation. In addition, if more than one specialized equipment are required to perform different parts of the attack, this value should be used. Before using this value, it has to be carefully checked that no service is available (renting, limited time access, etc.). If such service exists, the rating has probably to be moved down to "Specialized".

10.2.3. Calculation of attack potential

Table 11 Calculation of attack potential

Factor	Value		
	Identification	Exploitation	Note
Elapsed Time			
<= one day	0	0	
<= one week	1	2	
<= two weeks	2	4	
<= one month	4	8	
> one month	8	16	
Expertise			
Layman	0	0	
Proficient	2	4	

Expert	4	8	
Multiple experts	8	Not Applicable	
Knowledge of TOE			
Public	0	Not Applicable	
Restricted	2	Not Applicable	
Sensitive	4	Not Applicable	
Critical	8	Not Applicable	
Window of Opportunity 1) Access to TOE			
Easy	0	0	
Moderate	2	4	
Difficult	4	8	
Window of Opportunity 2) Access to Biometric Characteristics			
Immediate	Not Applicable	0	2D, 3D（Face）
Easy	Not Applicable	2	Fingerprint
Moderate	Not Applicable	4	Iris
Difficult	Not Applicable	8	Vein
Equipment			
Standard	0	0	
Specialised	2	4	
Bespoke	4	8	

Important note: Where a factor falls close to the boundary of a range the evaluator should consider use of an intermediate value to those in the table. The table is also intended to be used as a guide.

10.2.4. Rating of vulnerabilities and TOE resistance

Table 12 Rating of vulnerabilities and TOE resistance

Values	Attack Potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components:	Failure of components:
< 10	Basic	No rating	-	AVA_VAN.1,

				AVA_VAN.2, AVA_VAN.3, VA_VAN.4, AVA_VAN.5
10-19	Enhanced-Basic	Basic	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
20-29	Moderate	Enhanced-Basic	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
30-39	High	Moderate	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
=>40	Beyond-High	High	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

11. Bibliography

[1] N. Tekampe, A. Merle, J. Bringer, M. Gomez-Barrero, J. Fierrez, J. Galbally, D6.5: Towards the Common Criteria evaluations of biometric systems, March 2016.

[2] National Institute of Advanced Industrial Science and Technology, Attack Method for Biometric Verification Products Version 0.43, November 2016.

付録３　サポート文書 性能評価別冊

Annex

for

Evaluation Guidance for Biometric Verification Products

Version 1.0

March 2017

OKI Software Co., Ltd.

はじめに

本書は、コモンクライテリアをはじめとする、開発者と評価者が関わるバイオメトリック性能評価において、開発者が作成する性能試験エビデンス、および、評価者が実施する独立試験方法について述べる。

目次

1. 開発者作業

1.1 概要

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や同様なセキュリティ機能要件を定義した PP/ST に基づき性能試験を実施する場合、開発者は、評価者にバイオメトリック性能試験のためのエビデンスを提出しなければならない。こ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。本書ではこれらの文書を総称して性能試験エビデンスと呼ぶ。ただし、性能試験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性能試験の報告書であり、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

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、実際に開発者が評価者に提出する性能試験エビデンス（性能試験計画書、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、性能試験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、開発者に対しその合理的な根拠を評価者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

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	評価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	評価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	評価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	評価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(1)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。

注）(1) 本書における FTE は、ISO/IEC　19795-1:2006 の定義に基づき、被験者のすべての有効な身体部分に対してテンプレート生成トランザクションを実行した結果、評価対象製品の登録ポリシーに従い 登録失敗となった被験者の割合を表す。

(2) 性能試験報告書

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	評価対象製品（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	評価対象製品、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	評価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	評価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

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

開発者が性能試験で使用した試験システムを特定する情報として、評価対象製品および性能試験ツールに関する以下の項目を記述する。評価者が性能試験を再現できるレベルの情報である必要がある。

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動作環境：評価対象製品の動作環境

④性能試験ツール：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

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。

(3) 性能試験方法の決定

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。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。

(4) 予定する試験実施者（監督者）

試験実施者の氏名、所属を記述するとともに、開発者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。性能試験の試験実施者は通常のケースでは開発者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

(6) 試験予定場所

1.3.2 システム情報

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、評価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) テンプレート生成時および照合時の出力情報の決定

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。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）。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。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。

(2) SDK（ソフトウェア開発キット）使用有無

試験実施時の SDK の使用有無を記述する。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。

(3) 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評価対象製品の修正有無を記述する。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。（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。）

(4) 他のテンプレートによる影響

評価対象製品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。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。

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。

(5) テンプレート学習の方法と内容

評価対象製品のテンプレート学習の有無について記述する（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。

(6) 閾値の定義

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、PAD に関係する閾値など）を記述する。あわせて、試験で使用する閾値の説明を記載する。

(7) データベース規模への依存性

データベース規模への依存性の有無について記述する（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、その依存性をどのように考慮して性能試験を計画したかに関し記載する。

(8) 性能試験方法の決定

試験システムによる試験方法が評価対象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。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。

(9) システム詳細

試験システムの詳細として以下の情報を記述する。

① 生体情報取得装置：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 生体情報取得装置の中心的取得構成要素が，指紋センサ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

開発者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。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（静脈認証、指紋認証など）などを含める。

1.3.4 影響要因の制御

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

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。

②性別：男女（生物学的性別）の分布を率で記述する。

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。

(2) 姿勢・位置決め

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ことが望ましい（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

試験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。

(4) 温度

試験システムが想定する温度条件の説明を記載する。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) 生体情報登録~照合間の経過時間

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。性能試験においては、想定される登録～照合までの経過時間を考慮して測定する。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。

(6) 利用者の習熟度

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。

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

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

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とともに、選定方法の説明を記載する。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、選定方法の説明、および、そのデータを今回の性能試験に使用してもよい根拠あわせて記載する。

(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

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。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。

(3) 被験者または取得データの汚染度合い

試験に参加した被験者や取得されたテンプレートや照合バイオメトリック・データの汚染の度合いに関する以下の情報を記述する。

① 取得されたテンプレートや照合バイオメトリック・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・調整に使用したテンプレートや照合バイオメトリック・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

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、テンプレートや照合バイオメトリック・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。

(2) 習熟度の確認

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、テンプレートや照合バイオメトリック・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。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性能試験ツールの記載などが含まれるべきである。

(3) 順化

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、テンプレートや照合バイオメトリック・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。

(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。

①被験者の初期登録方法

② 被験者の登録の一意性を保証する方法

③ 被験者を識別するために付与した識別子のタイプ

④ 収集された個人データの量およびタイプ

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）

(5) 少数の代表的でない利用者による偏りの防止

同一被験者が一度の性能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。(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

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

データ収集誤りの回避方法の概要の説明を記載する。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

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。

1.3.8 生体情報登録

生体情報登録に関する性能試験として FTE 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

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。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テンプレートや照合バイオメトリック・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、被験者によるテンプレートや照合バイオメトリック・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

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、トランザクション・アテンプト・プレゼンテーションの定義とともに説明を記載する。

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

注 1）あらかじめ蓄積されたテンプレートや照合バイオメトリック・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開発者の定義を用いる。

(3) 登録時の制御要因の制御方法

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。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。

(4) データ入力エラーの防止

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データ入力エラー防止対策の説明を記載する。

(5) 監督者の介入基準

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。

(6) 登録失敗者に対する助言又は救済策

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。

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

(7) 登録失敗の定義と失敗原因

利用者または運用者から見た登録失敗の定義、および、想定される登録失敗原因（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。

(8) 重みづけ

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。

(9) 試験前のデータ処理

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。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。

1.3.9 本人トランザクション

本人の照合に関する性能試験として誤拒否率 FRR 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

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。

(2) 誤拒否率算出のための照合処理方針

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、トランザクション・アテンプト・プレゼンテーションの定義とともに説明を記載する。

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

注 1) あらかじめ蓄積されたテンプレートや照合バイオメトリック･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開発者の定義を用いる。

(3) 収集過程での制御要因の制御方法

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。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。

(4) データ入力エラーの防止

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データ入力エラー防止対策の説明を記載する。

(5) 監督者の介入基準

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。

(6) 本人照合失敗者に対する助言又は救済策

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。

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

(7) 本人照合失敗の定義と失敗原因

運用者から見た本人照合失敗の定義、および、想定される本人照合失敗原因（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。

(8) 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。

(9) 試験前のデータ処理

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。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。

1.3.10 偽者トランザクション

偽者の照合に関する性能試験として誤受入率 FAR 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

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。

(2) 誤受入率算出のための照合処理方針

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、トランザクション・アテンプト・プレゼンテーションの定義とともに説明を記載する。

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

注 1) あらかじめ蓄積されたテンプレートや照合バイオメトリック･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合せを用いる（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開発者の定義を用いる。

(3) 個人内比較の実施有無

個人内比較の実施有無を記述する。有の場合、個人内比較の実施内容の説明を記載する。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

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。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。

(5) 偽者トランザクションのオフライン収集

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。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。)。
- 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) 収集過程での制御要因の制御方法

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。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。

(7) データ入力エラーの防止

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。

(8) 監督者の介入基準

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。

(9) 生体情報取得失敗者に対する助言又は救済策

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。

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

誤受入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。

(11) 評価前のデータ処理

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。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。

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

記録しようとする項目および内容の説明を記載する。 記録が推奨される項目を以下に示す。

①情報の記録方法を記述する。記録方法とは、性能試験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あるいは両方である。

②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）

③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）

④本人トランザクションごとの照合バイオメトリック・データ（バイオメトリック画像またはバイオメトリック特徴）

⑤偽者トランザクションで使用する照合バイオメトリック・データ（バイオメトリック画像またはバイオメトリック特徴）

⑥試験システムによる照合スコア及び判定出力

⑦性能尺度及び不確実性を導き出すために用いた方法（二項分布などを用いた区間推定）

⑧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

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。

(3) 保管状態

保管状態に関する計画の説明を記載する。 記録が推奨される項目を以下に示す。

①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

②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 性能試験報告書の記載事項

前節 1.3 で述べた性能試験計画書に従った試験を実施し、その結果を性能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。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) テンプレート生成時および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（コンピュータ名、フォルダ名など）。

(2) 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。

(3) 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評価対象製品の修正が有の場合、修正結果の説明を記載する。

(4) 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。

(5) 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。

(6) 閾値の定義

試験で使用した閾値の説明を記載する。

(7) 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。

(8) 性能試験方法の決定

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。

(9) システム詳細

試験計画と同様の項目について、試験結果を記述する。

1.4.3 想定アプリケーション

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 1.3.3 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。

1.4.4 影響要因の制御

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。

② 性別：男女（生物学的性別）の分布を被験者数で記述する。

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。

④ その他：身長、目や髪の色など開発者が記録したもの

(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。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

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。

(4) 温度

評価した温度条件の説明を記載する。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) 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。

(6) 被験者の習熟度

習熟度の分布を被験者数で示す。

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。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。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、選定方法、および、そのデータを今回の性能試験に使用してもよい根拠を記載する。

(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。

(3) 被験者または取得データの純粋性

再参加または再利用の有無を記述する。

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

被験者に対して行った各種説明内容の説明を記載する。

(2) 習熟度の確認

被験者の習熟度実施内容および習熟度確認結果の説明を記載する。

(3) 順化

被験者の順化方法の実施結果の説明を記載する。

(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。

(5) 少数の代表的でない利用者による偏りの防止

同一被験者の一度の性能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。

(6) 被験者一覧

性能試験に参加した全被験者の ID と各被験者の制御要因に関わる情報を表にまとめる（表 4 に例を示す)。本サポート文書が対象とする制御要因は、性別・年齢・民族的出身・習熟度・温度の 5 種類であ

る。評価者の確認の利便性のためCSVなどコンピュータで編集しやすい形式とすることが推奨される。

表 4　被験者及び制御要因一覧表（例）

被験者 ID	性別	年齢	民族的出身	習熟度	温度（登録時、照合時）
0001					
0002					
0003					
NNNN					

図 1 に被験者及び制御要因一覧の CSV 表現の例を示す。

```
SubjectID, Gender, Age, Ethnicity, Habituation, Temperature(C)
0001, Female, 30-35, Asian(Japanese), 3, 20-30,
0002, Male, 30-35, Asian(Japanese), 3, 20-30,
0003, Male, 40-45, Caucasian(German), 3, 20-30,

…

NNNN, Female, 25-30, Asian(Indonesian), 3, 20-30
```

図 1　テンプレート生成結果の CSV 表現例

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。

(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。

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

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。

(2) 生体情報登録方針

生体情報登録方針の実施結果の説明を記載する。

(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。

(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。

(5) 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。

(6) 登録失敗者に対する助言又は救済策

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。

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) 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。

(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。

(9) 評価前のデータ処理

評価前のデータ処理結果の説明を記載する。

(10) テンプレート生成結果一覧

各被験者の各身体部分のテンプレート生成トランザクション実行結果を表にまとめる（表 5 に指静脈の例を示す）。本サポート文書においてテンプレート生成トランザクション実行結果として対象とする情報は、被験者を識別するための ID・テンプレート生成対象となった身体部分・テンプレート生成成否・テンプレート生成トランザクション内の総アテンプト数（またはトランザクションの開始から終了までの所要時間）である。評価者の確認の利便性のため CSV などコンピュータで編集しやすい形式とすることが強く推奨される。

表 5　テンプレート生成結果一覧表例（指静脈の場合）

被験者 ID	左右	指	成否	総アテンプト数 または トランザクション所要時間
0001	右	中指		
		人差し指		
		薬指		
	左	中指		
		人差し指		
		薬指		
0002	右	中指		
NNNN	左	薬指		

図 2 にテンプレート生成結果の CSV 表現の例を示す。

```
SubjectID, LR, Finger, Result, Attempts,
0001, R, Middle, Success, 3,
0001, R, Point, Fail, 10,
0001, R, Ring, Success, 1,
0001, L, Middle, Success, 3,
0001, L, Point, Success, 5
0001, L, Ring, Success, 7,
0002, R, Middle, Success, 4,

…

NNNN, L, Ring, Success, 1
```

図 2 テンプレート生成結果の CSV 表現例（指静脈の場合）

(11) 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（評価対象製品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。

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

(12) 登録失敗率（FTE）の宣言値

登録失敗率の宣言値を記述するとともに、区間推定における上側信頼限界を記述する。登録失敗率の宣言値は、ST に記載する FTE である。上側信頼限界は、宣言値に対して同じか下回らなければならない。具体的には、二項分布を適用した場合、FTE の実測値に 95%、99%あるいは 90%のいずれかから選択した信頼区間を二項分布に基づいて算出し、その上側信頼限界が登録失敗率の宣言値以下になっていることが示されなければならない。宣言値および上側信頼限界の記述とあわせて、二項分布を適用した旨の記載、および、選択した信頼区間（95%、99%、90%のいずれか）を記述する。本書では、選択すべき信頼区間として 95%を強く推奨する。開発者が信頼区間として 95%を選択しなかった場合、

宣言値に加えて、95%信頼区間の上側信頼限界以上の値を登録失敗率の参考性能値として記述する。信頼区間の算出方法として二項分布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とともに、二項分布を適用した場合に記載する情報と同等の情報を記述する。なお、宣言値、及び参考性能値（95%信頼区間を選択しなかった場合）は、ST に記載された値と一致している必要がある。

(13) 人口統計グループ毎の集計（推奨）

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，又はその他の条件に基づいた登録結果を集計する。

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

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。

(2) 誤拒否率算出のための照合処理方針の実施結果

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。

(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。

(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。

(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。

(6) 本人照合失敗者に対する助言又は救済策

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。

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。

(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。

(9) 評価前のデータ処理

評価前のデータ処理結果について説明を記載する。

(10) 本人トランザクション実行結果一覧

各被験者の各身体部分の本人トランザクション実行結果を表にまとめる（表 6 に指静脈の例を示す）。

本サポート文書において本人トランザクション実行結果として対象とする情報は、被験者を識別するための ID・照合対象となった身体部分・照合判定結果・トランザクション内の総アテンプト数（またはトランザクションの開始から終了までの所要時間）である。評価者の確認の利便性のため CSV などコンピュータで編集しやすい形式とすることが強く推奨される。

表 6　本人トランザクション実行結果一覧表例（指静脈の場合）

被験者 ID	左右	指	判定結果	照合スコア値(1)	総アテンプト数 または トランザクション所要時間
0001	右	中指			
		人差指			
		薬指			
	左	中指			
		人差指			
		薬指			
0002	右	中指			
NNNN	左	薬指			

注）(1) 照合スコア値は、その本人トランザクションの結果が受入だった場合、受入が発生したアテンプトの照合スコア値を用いる。結果が拒否で、そのトランザクション内に複数のアテンプトが存在した場合、複数の照合スコアの中から最良のスコア値を用いる。

図 3 に本人トランザクション実行結果の CSV 表現の例を示す。

```
SubjectID, LR, Finger, Result, Score, Attempts,
0001, R, Middle, Accept, 100, 1,
0001, R, Point, Accept, 101, 3,
0001, R, Ring, Reject, 28, 10,
0001, L, Middle, Accept, 95, 2,
0001, L, Point, Accept, 118, 1,
0001, L, Ring, Accept, 105, 3,
0002, R, Middle, Accept, 120, 1

…

NNNN, L, Ring, Accept, 99, 2
```

図 3　本人トランザクション実行結果の CSV 表現例（指静脈の場合）

(11) 誤拒否率（FRR）の実測値

誤拒否率 FRR の実測値を記述するとともに、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。

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

(12) 誤拒否率（FRR）の宣言値

誤拒否率の宣言値を記述するとともに、区間推定における上側信頼限界を記述する。誤拒否率の宣言値は、ST に記載する FRR である。上側信頼限界は、宣言値に対して同じか下回らなければならない。具体的には、二項分布を適用した場合、FRR の実測値に 95%、99%あるいは 90%のいずれかから選択した信頼区間を二項分布に基づいて算出し、その上側信頼限界が誤拒否率の宣言値以下になっていることが示されなければならない。宣言値および上側信頼限界の記述とあわせて、二項分布を適用し

た旨の記載、および、選択した信頼区間（95%、99%、90%のいずれか）を記述する。本書では、選択すべき信頼区間として 95%を強く推奨する。開発者が信頼区間として 95%を選択しなかった場合、宣言値に加えて、95%信頼区間の上側信頼限界以上の値を誤拒否率の参考性能値として記述する。信頼区間の算出方法として二項分布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とともに、二項分布を適用した場合に記載する情報と同等の情報を記述する。なお、宣言値、及び参考性能値（95%信頼区間を選択しなかった場合）は、ST に記載された値と一致している必要がある。

(13) スコア分布グラフ

被験者の各身体部分に対する本人トランザクション実行時に生成された最良スコアを用いたスコア分布グラフを後述 1.4.10 の偽者トランザクションのスコア分布とともに作図する。

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

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。

(2) 誤受入率算出のための照合処理方針の実施結果

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。

注 1) あらかじめ蓄積されたテンプレートや照合バイオメトリック･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合せを用いる（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開発者の定義を用いる。

(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。行われた場合、個人内比較の内容の説明を記載する。

(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。

(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。

(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。

(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。

(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。

(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。

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。

(11) 評価前のデータ処理

評価前のデータ処理結果について説明を記載する。

(12) 偽者トランザクション実行結果一覧

各被験者の各身体部分の偽者トランザクション実行結果を表にまとめる（表 7 に指静脈の例を示す）。本サポート文書において偽者トランザクション実行結果として対象とする情報は、テンプレート側の被験者を識別するための ID・テンプレートの身体部分・偽者側の被験者を識別するための ID・偽者側の身体部分・判定結果・トランザクション内で生成された最良スコア値・トランザクション内の総アテンプト数（またはトランザクションの開始から終了までの所要時間）である。評価者の確認の利便性のため CSV などコンピュータで編集しやすい形式とすることが強く推奨される。

表 7　偽者トランザクション実行結果一覧表の例（指静脈の場合）

被験者 ID	左右	指	偽者 被験者 ID	左右	指	判定 結果	照合 スコア値(1)	総アテンプト数 または トランザクション所要時間
0001	右	中指	0002	右	中指			
					人差指			
					薬指			
				左	中指			
					人差指			
					薬指			
			0003	右	中指			
NNNN	左	薬指	…	…	…			

注）(1) 照合スコア値は、その偽者トランザクションの結果が受入だった場合、受入が発生したアテンプトの照合スコア値を用いる。結果が拒否で、そのトランザクション内に複数のアテンプトが存在した場合、複数の照合スコア値の中から最良のスコア値を用いる。

図 4 に偽者トランザクション実行結果の CSV 表現の例を示す。

```
SubjectID, LR, Finger, ImpostorID, LR, Finger, Result, Score, Attempts,
0001, R, Middle, 0002, R, Middle, Reject, 15, 10,
0001, R, Middle, 0002, R, Point, Reject, 33, 10,
0001, R, Middle, 0002, R, Ring, Reject, 7, 10,
0001, R, Middle, 0002, L, Middle, Reject, 22, 10,
0001, R, Middle, 0002, L, Point, Reject, 21, 10,
0001, R, Middle, 0002, L, Ring, Reject, 38, 10,
0001, R, Middle, 0003, R, Middle, Accept, 95, 6,

…

NNNN, L, Ring, NNNN-1, L, Ring, Reject, 30, 10
```

図 4　偽者トランザクション実行結果の CSV 表現例（指静脈の場合）

(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。

$$\text{FAR の実測値} = \frac{\text{受入が発生した偽者トランザクション総数}}{\text{本人以外の身体部分間あるいは本人の異なる身体部分間の偽者トランザクション総数}}$$

(14) 誤受入率（FAR）の宣言値

誤受入率の宣言値を記述するとともに、区間推定における上側信頼限界を記述する。誤受入率の宣言値は、ST に記載する FAR である。上側信頼限界は、宣言値に対して同じか下回らなければなければならない。具体的には、二項分布を適用した場合、FAR の実測値に 95%、99%あるいは 90%のいずれかから選択した信頼区間を二項分布に基づいて算出し、その上側信頼限界が誤受入率の宣言値以下になっていることが示されなければならない。宣言値および上側信頼限界の記述とあわせて、二項分布を適用した旨の記載、および、選択した信頼区間（95%、99%、90%のいずれか）を記述する。本書では、選択すべき信頼区間として 95%を強く推奨する。開発者が信頼区間として 95%を選択しなかった場合、宣言値に加えて、95%信頼区間の上側信頼限界以上の値を誤受入率の参考性能値として記述する。信頼区間の算出方法として二項分布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とともに、二項分布を適用した場合に記載する情報と同等の情報を記述する。なお、宣言値、及び参考性能値（95%信頼区間を選択しなかった場合）は、ST に記載された値と一致している必要がある。

(15) スコア分布グラフ

被験者の各身体部分に対する偽者トランザクション実行時に生成された最良スコアを用いたスコア分布グラフを前述 1.4.9 の本人トランザクションのスコア分布とともに作図する。

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。あわせて、試験環境における保存場所の説明を記載する（コンピュータ名、フォルダ名など）、および、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。

(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。

(3) 保管状態

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（コンピュータ名、フォルダ名など）とともに保管状態の説明を記載する。

2. 評価者作業

2.1 概要

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や同様なセキュリティ機能要件を定義したPP/STに基づいて行う評価者作業は、開発者が提出した性能試験エビデンスの一貫性確認、および、バイオメトリック性能評価のための独立試験の実施である。独立試験は、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実施することとする。評価者は独立試験の実施において、前述1で示した開発者によって実施される性能試験において作成される性能試験計画書、および、性能試験報告書の内容に準ずる内容の文書を、独立試験計画立案時および独立試験実施時に作成することとする。

2.2 記載項目概要

バイオメトリック性能評価のための独立試験の試験計画立案および性能試験実施それぞれにおいて考慮すべき事項の概要を以下に示す。

(1) 性能試験計画立案

表8に、バイオメトリック性能評価のための独立試験計画立案時の作業項目概要を示す。

表8　計画立案時の作業項目

No	項目	説明
1	性能試験エビデンスの一貫性確認	開発者が作成した性能試験エビデンスが独立試験を実施するための十分な一貫性を持っているか確認する。確認対象には、FTE・FRR・FARそれぞれの実測値および宣言値、本人トランザクションや偽者トランザクションのスコア分布などが含まれる。
2	性能試験計画書の作成	開発者が作成した性能試験計画書の項目に準ずる内容の独立性能試験計画書を作成する。

(2) 性能試験実施

表9に、バイオメトリック性能評価のための独立試験実施時の作業項目概要を示す。

表9 試験実施時の作業項目

No	項目	説明
1	試験実施	独立試験を実施する。本作業には、評価対象製品のセットアップ、被験者募集、性能評価のための各種トランザクションの実行などが含まれる。
2	エラー率棄却限界値確認	独立試験で検出されたエラー事象（登録失敗・誤拒否・誤受入）に対して二項分布に基づくエラー率棄却限界値確認を実施する。棄却限界値5%を判定基準とし、5%未満を検出した場合上記1を再度実施する（被験者の追加募集）。
3	性能試験実施報告書の作成	開発者が作成した性能試験実施報告書の項目に準ずる内容の独立性能試験報告書を作成する。

2.3 性能試験計画時の作業内容

独立試験のための性能試験計画時の作業内容を以下に示す。

2.3.1 性能試験エビデンスの一貫性確認

(1) 使用する情報

開発者が提出した性能試験エビデンスのうち、評価者は主に以下の情報を用いて一貫性確認を行う。

- ・設定された各種閾値
- ・登録失敗率（FTE）の実測値および宣言値
- ・誤拒否率（FRR）の実測値および宣言値
- ・誤受入率（FAR）の実測値および宣言値
- ・本人トランザクションスコア分布
- ・偽者トランザクションスコア分布
- ・被験者及び制御要因一覧情報
- ・テンプレート生成結果一覧情報
- ・本人トランザクション実行結果一覧情報
- ・偽者トランザクション実行結果一覧情報

(2) 確認項目

評価者は、開発者試験において各性能尺度（FTE、FAR、FRR）が正しく導出されたことを検証するために、開発者試験エビデンスの一貫性を確認しなければならない。確認の際には、最低限以下の項目をチェックしなければならない。下記に加えて、評価者の判断により確認項目を追加することができる。

① 性能試験エビデンスで示された各種閾値（照合スコアの判定閾値、画像品質閾値、PAD に関連した閾値など）が、登録失敗率・誤拒否率・誤受入率のための試験において一貫性を持って設定されていることを確認しなければならない。

② 性能試験エビデンスで示された被験者及び制御要因一覧における被験者集団の人口統計分布が、開発者の評価対象製品の想定利用者の人口統計分布と一貫性があることを確認しなければならない。

③ 性能試験エビデンスで示された FTE・FRR・FAR それぞれの実測値算出に用いた値（例；計算式の分母の値や分子の値）と、同じく性能試験エビデンスで示されたテンプレート生成結果一覧・本人トランザクション実行結果一覧・偽者トランザクション実行結果一覧に含まれる情報との間で一貫性があることを確認しなければならない。

④ 性能試験エビデンスで示された FTE・FRR・FAR それぞれの宣言値の算出結果が、開発者が使用した信頼区間の算出方法において正確であることを確認しなければならない。

⑤ 性能試験エビデンスで示された本人トランザクションのスコア分布・偽者トランザクションのスコア分布と、同じく性能試験エビデンスで示された本人トランザクション実行結果一覧の照合スコア値・偽者トランザクション実行結果一覧の照合スコア値との間に一貫性があることを確認しなければならない。

⑥ 性能試験エビデンスで示された上記以外の内容に、情報の不足・誤り・不明点などがなく、独立試験に進めることを評価者は確認しなければならない。

以上の項目をひとつでも満足しなかった場合、評価者は開発者に性能試験エビデンス、あるいは、適切さを満足するための関連文書の再提出を要求しなければならない。これを受けて開発者が評価者に資料の再

提出を行った場合、評価者は上記項目を再度確認し、条件を満足したかどうか判定しなければならない。

2.3.2 性能試験計画書の作成

評価者は、前述 1 で示した開発者によって実施される性能試験において作成される性能試験計画書に準ずる内容の性能試験計画書を作成しなければならない。

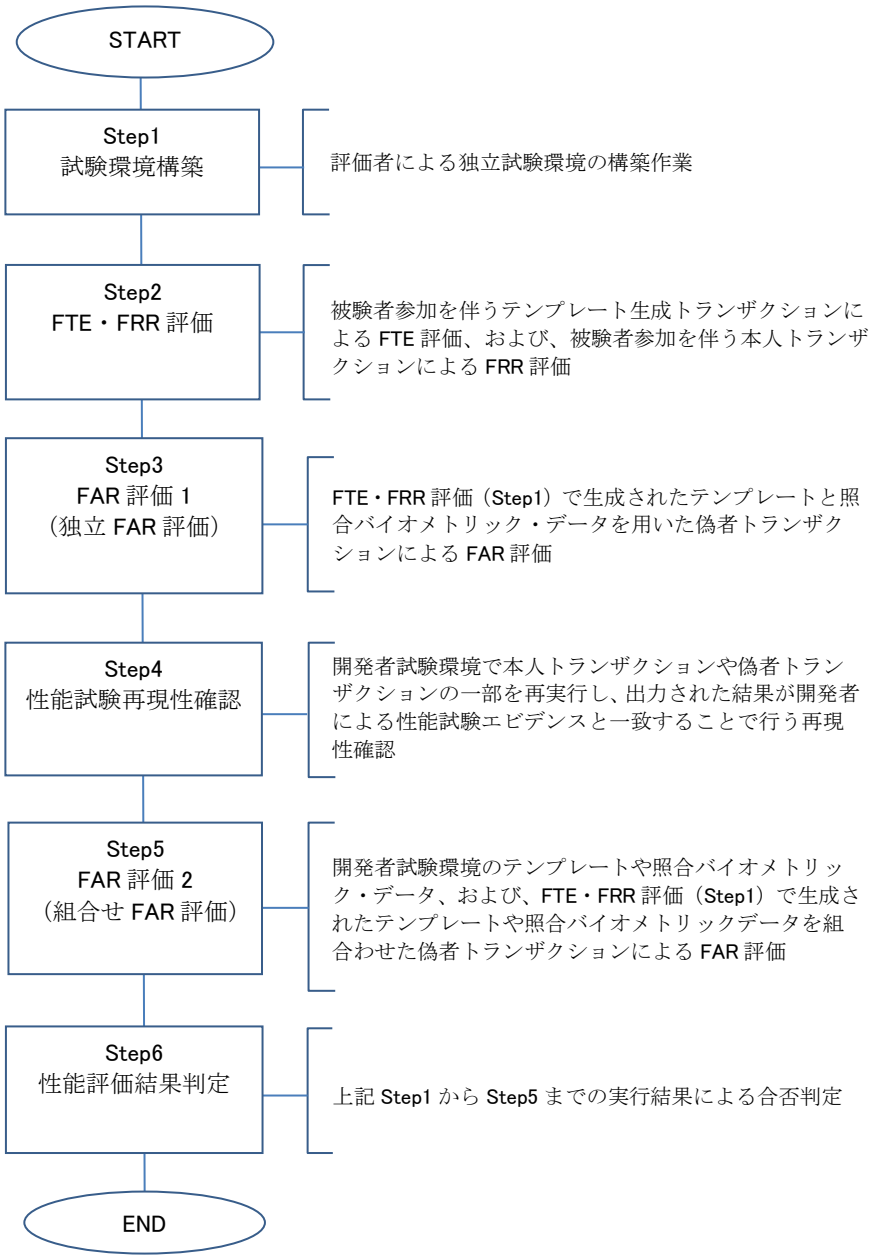
なお、被験者が募集する被験者数の初期値は 100 人とする。評価者は計画書の中で、募集する被験者の人口統計分布を決定しなければならない。この分布は、一貫性があることが確認された性能試験エビデンスで示される被験者の人口統計分布に従うことが推奨される。

2.4 試験実施時の作業内容

独立試験のための性能試験実施時の作業内容を以下に示す。

2.4.1 試験実施の流れ

独立試験実施の概要を図 5 に示す。本図は評価実施の大まかな工程をステップとしてまとめたものである。図の右側の想定実施場所は、各項目を実施する際に想定される場所として評価者が管理する場所か、あるいは、開発者が管理する場所かを示す。評価者の判断により、本図で示された想定実施場所以外の場所で評価を実施することができる。



想定実施場所	
評価者	開発者
○	
○	
○	
	○
	○
○	

図 5　独立試験実施の概要

図 5 における FTE・FRR 評価（Step2）、FAR 評価 1（Step3）、FAR 評価 2（Step5）の詳細手順を図 6 に示す。

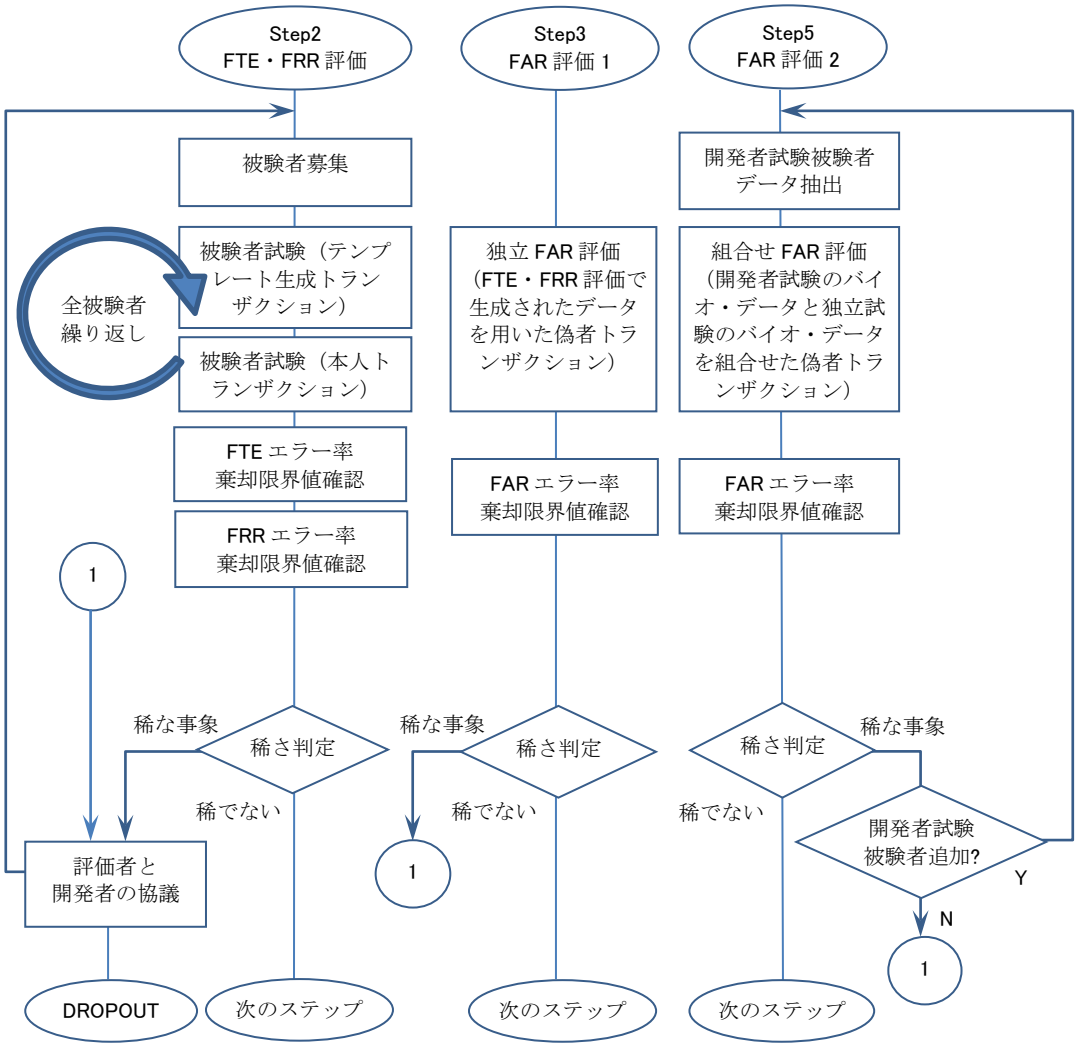


図 6　独立試験における FTE・FRR 評価、FAR 評価 1 および FAR 評価 2 の詳細な流れ

評価者が合理的だと判断した場合、本図で示された作業の順番を変えることができる。（例：FTE・FRR 評価において、エラー率棄却限界値確認で稀な事象が発生していることが明確な場合、評価者と開発者の協議を実施する。）

(1) 試験環境構築

評価者が、独立試験実施場所を確保し、装置の配置や性能試験ツールのセットアップなど試験実施のための環境構築を行う。

(2) FTE・FRR 評価

試験実施場所に被験者を募集し、評価者による管理のもと、被験者が FTE 評価のためのテンプレート生成トランザクションや FRR 評価のための本人トランザクションを実行する。

(3) FAR 評価 1（独立 FAR 評価）

評価者は、前述(2)の FTE・FRR 評価で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・データを用いた偽者トランザクションを実行する。実行結果より、評価者は次に取るべきアクションを決定する。

(4) 性能試験再現性確認

評価者は、開発者の性能試験実施環境を訪問し、開発者の性能試験が正しく再現されることを確認する。確認結果より、評価者は次に取るべきアクションを決定する。

(5) FAR 評価 2（組合せ FAR 評価）

評価者は、開発者による性能試験で生成された被験者のテンプレートまたは照合バイオメトリック・データと、前述(2)の FTE・FRR 評価で収集された被験者のテンプレートまたは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を実行する。実行結果より、評価者は次に取るべきアクションを決定する (1)。

(6) 性能評価結果判定

評価者は、前述(2)、(3)、(5)の結果から、開発者が ST に記載した宣言性能である FTE 値・FRR 値・FAR 値が独立試験の結果と乖離していないか確認する。さらに、前述(4)の結果から、開発者の性能試験の環境が正しいか確認する。これらの確認において、開発者による試験結果と独立試験結果の間に乖離がなく、独立試験の試験環境に問題がなく、かつ、性能試験再現性確認結果が正しいと判断された場合、合格とする。

注）(1) 開発者の性能試験の本人トランザクションと独立試験の本人トランザクションを組合せた評価（これを組合せ FRR 評価と呼ぶ）は実施する必要はない。上記(3) FAR 評価 1（独立 FAR 評価）に加え(5)FAR 評価 2（組合せ FAR 評価）を実施するのは、この組合せ FAR 評価により、開発者と評価者が個別に収集したテンプレートと照合バイオメトリック・データを組み合わせて照合し、独立 FAR 評価では実施されていない新規の偽者トランザクションを実行できるからである。評価者は、独立 FAR 評価に加え、この新規のトランザクションの実行結果も考慮することにより、より精度の高い評価を実施することが出来る。これに対し、組合せ FRR 評価では、開発者のデータと評価者のデータが組み合わされ照合されることはない。単に開発者のデータと評価者のデータが個別に照合されるため、組合せ FAR 評価と異なり新規の本人トランザクションが実行されることはない。従って組合せ FRR 評価を実施する必要はなく、独立 FAR 評価のみで問題はない。組合せ FTE 評価についても同様の理由で実施する必要はない。

2.4.2 詳細説明

前述 2.4.1 で示した試験実施の流れの各項目の詳細について以下に説明する。

2.4.2.1 試験環境構築

評価者は、開発者による性能試験の実施環境に準ずる試験環境を構築しなければならない。特に以下の点に注意する。

(1) 生体情報取得装置の設置環境：設置位置や設置環境の温度などが開発者の推奨使用環境との間で一貫性

を持っていること。

(2) セットアップ時の各種パラメータ：バイオメトリック性能に影響を与える各種閾値（照合スコアの判定閾値、画像品質閾値、PAD に関連した閾値など）が開発者の性能試験エビデンスで示された設定値と一致していること。

なお、構築した試験環境における環境条件（結果に影響を与える制御要因など）が、開発者による性能試験の実施環境に準じていることを、開発者も確認し同意することが強く推奨される。

2.4.2.2 FTE・FRR 評価

(1) 被験者募集

評価者は、評価方針に基づいて決定した人口統計分布に従って、あらかじめ決定した人数分の被験者を募集しなければならない。

(2) テンプレート生成トランザクションの実行

評価者は、FTE 評価のためのテンプレート生成トランザクションを実行し、以下の情報を収集する。

・被験者及び制御要因一覧情報

・テンプレート生成結果一覧情報

(3) 本人トランザクションの実行

評価者は、FRR 評価のための本人トランザクションを実行し、本人トランザクション実行結果一覧情報を収集する。

(4) エラー率棄却限界値確認

評価者は、テンプレート生成トランザクションの実行、および、本人トランザクションの実行それぞれについて、発生したエラー（登録失敗、あるいは誤拒否）の回数から確率計算を行う。

①FTE の場合

開発者が定めた登録ポリシーを満足しなかった被験者数と評価に参加した全被験者数を用いて、二項分布に基づくエラー率棄却限界値確認を実施する。確率計算の結果が棄却限界値である 5%未満であり且つ評価者がその結果を妥当と認めた場合、稀な事象が発生したと判断する。確率計算結果が棄却限界値である 5%以上だった場合、稀な事象は発生しなかったと判断する。ただし、1.4.8 における登録失敗率（FTE）の宣言値算出時に、開発者が二項分布以外の方法を使用した場合、評価者は二項分布を用いず開発者が適用した方法に従ってエラー率棄却限界値確認を実施する。なお、独立試験における初期被験者数 100 人で収集されるサンプル数が、開発者が使用した方法の適用条件を満たさない場合、評価者は開発者と協議し、開発者が使用した方法が適用できるよう初期被験者数を設定するか、あるいは、独立試験において二項分布を適用するかをあらかじめ決定しておく。図 7 に FTE・FRR 評価における FTE に関するエラー率棄却限界値確認の考え方を、FTE の宣言値が 0.1%の評価対象製品を例にとって説明する。

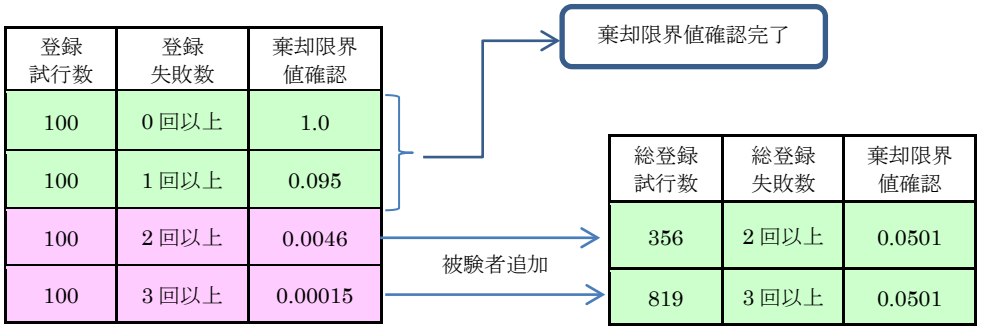


図 7　FTE の宣言値が 0.1%の場合の計算方法

本図の左側の表の登録試行数が 100 となっているのは、独立試験の初期被験者数として評価者が 100 人の被験者を募集して登録試行を行ったことを示す。左側の表の各行は発生した登録失敗数ごとに事象発生確率を二項分布に従って計算した結果を示す。この事象発生確率の値が有意水準である 0.05 未満だった場合、稀な事象が発生したと判断する。左側の表では、登録失敗回数が 2 回以上だった場合、事象発生確率は 0.05 を下回る。下回った場合、評価者は開発者と協議し、双方が納得すれば評価者が新たに被験者を追加募集する。追加募集して再度登録試行を実施した結果、追加被験者において登録失敗が発生しなかった場合に有意水準以上となる条件を本図の右側の表に示す。

図 8 に FTE の宣言値が 0.1%の評価対象製品における FTE のための評価の具体例を示す。

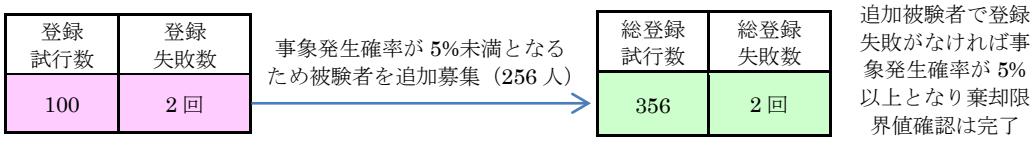


図 8　FTE の宣言値が 0.1%の場合の具体例

初期被験者 100 人での登録試行において 2 回の登録失敗が発生した場合、事象発生確率は有意水準を下回るため稀な事象と判断される。被験者追加が決定された場合、256 人の被験者を追加することで総登録試行数は 356 回となる。登録失敗数が 2 回のままであれば、事象発生確率は有意水準以上の値となる。この結果、FTE のエラー率棄却限界値確認の試験は完了となり、次の項目（②FRR の場合）に進む。被験者追加の際の人数は、追加被験者を加えた総登録試行において総登録失敗数が変らなかった場合（すなわち追加被験者での登録失敗が 0 件だった場合）に、総登録試行および総登録失敗数による二項分布を用いたエラー率棄却限界値確認の結果が、有意水準以上となる人数とする。

②FRR の場合

本人トランザクションで発生した誤拒否件数と実行した総本人トランザクション数より、二項分布に基づくエラー率棄却限界値確認を実施する。確率計算の結果が棄却限界値である 5%未満であり且つ評価者がその結果を妥当と認めた場合、稀な事象が発生したと判断する。確率計算結果が棄却限界値である 5%以上だった場合、稀な事象は発生しなかったと判断する。ただし、1.4.9 における誤拒否率（FRR）の宣言値算出時に、開発者が二項分布以外の方法を使用した場合、評価者は二項分布を

用いず開発者が適用した方法に従ってエラー率棄却限界値確認を実施する。なお、独立試験における初期被験者数 100 人で収集されるサンプル数が開発者が使用した方法の適用条件を満たさない場合、評価者は開発者と協議し、開発者が使用した方法が適用できるよう初期被験者数を設定するか、あるいは、独立試験において二項分布を適用するかをあらかじめ決定しておく。図 9 に FTE・FRR 評価における FRR に関するエラーエラー率棄却限界値確認の考え方を、FRR の宣言値が 0.1%で身体部分の数が 2 の評価対象製品を例にとって説明する。

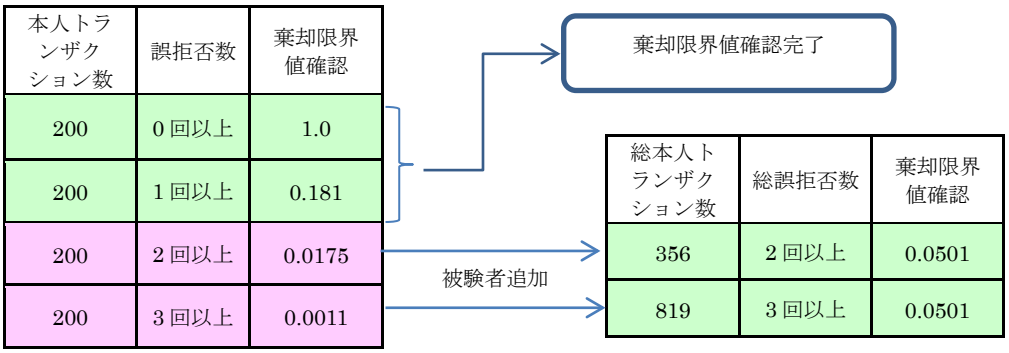


図 9　FRR の宣言値が 0.1%の場合の計算方法（身体部分数が 2 個の場合）

本図の左側の表の本人トランザクション数が 200 となっているのは、独立試験の初期被験者数として評価者が 100 人の被験者を募集し、各被験者がそれぞれの身体部分を使って本人トランザクションを行ったことを示す。本人トランザクション数の計算式は、100×2＝200 である。左側の表の各行は発生した誤拒否数ごとに事象発生確率を二項分布に従って計算した結果を示す。この事象発生確率の値が有意水準である 0.05 未満だった場合、稀な事象が発生したと判断する。左側の表では、誤拒否数が 2 回以上だった場合、事象発生確率は 0.05 を下回る。下回った場合、評価者は開発者と協議し、双方が納得すれば評価者が新たに被験者を追加募集する。追加募集して再度本人トランザクションを実施した結果、追加被験者において誤拒否が発生しなかった場合に有意水準以上となる条件を本図の右側の表に示す。

図 10 は、FRR の宣言値が 0.1%で身体部分の数が 2 の評価対象製品における FRR のための評価の具体例を示す。

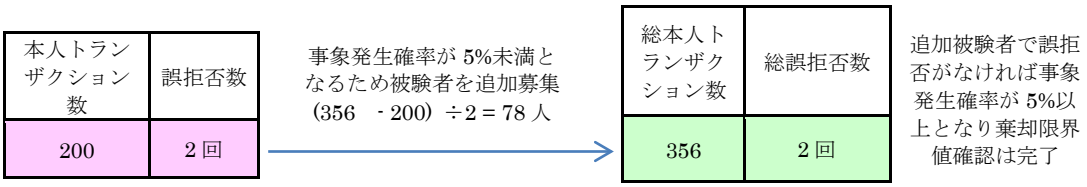


図 10　FRR の宣言値が 0.1%の場合の具体例（身体部分数が 2 の場合）

初期被験者 100 人での 200 回の本人トランザクションにおいて 2 回の誤拒否が発生した場合、事象発生確率は有意水準を下回るため稀な事象と判断される。被験者追加が決定された場合、78 人の被験者を追加することで総本人トランザクション数は 356 回となる（計算式は、178×2＝356 である）。誤拒否数が 2 回のままであれば、事象発生確率は有意水準以上の値となる。この結果、FRR のエラー率棄却限界値確認の試験は完了となり、次の項目（(5) 稀さ判定）に進む。被験者追加の際の人数は、追加被験者を加えた総本人トランザクションにおいて総誤拒否数が変らなかった場合（すなわち追加

被験者での誤拒否件数が 0 件だった場合）に、総本人トランザクション数および総誤拒否数による二項分布を用いたエラー率棄却限界値確認の結果が、有意水準以上となる人数とする。

(5) 稀さ判定

上記(4)のエラー率棄却限界値確認で稀な事象が発生した場合、評価者は被験者の追加による再評価が必要と判断し、追加被験者数を検討する。追加被験者数は、被験者を追加して再評価を実施した結果、追加被験者による試験でエラー事象が発生しなかった場合に、累積のエラー率棄却限界値確認結果が 5%以上となる最少人数とする。評価者は、追加被験者による再評価の実施について開発者と協議した上で、上記(1)の被験者募集以降を再度実施する。これに対して、稀な事象が発生しなかった場合、FTE・FRR 評価は完了となり、次の評価である FAR 評価 1（独立 FAR 評価）に進む。なお、協議の際に開発者は独立試験と乖離しないよう宣言値を変更することにより、被験者の追加をせずに合格条件を満たすことができる。

2.4.2.3 FAR 評価 1（独立 FAR 評価）

(1) 偽者トランザクションの実行

評価者は、前述の FTE・FRR 評価で収集した被験者のテンプレートおよび照合バイオメトリック・データを用いて偽者トランザクションを実行し、偽者トランザクション実行結果一覧情報を収集しなければならない。

(2) エラー率棄却限界値確認

評価者は、発生したエラー（誤受入）の回数から事象発生の確率計算を行う。すなわち、偽者トランザクションで発生した誤受入件数と、実行した総偽者トランザクション数より、二項分布に基づく事象発生確率を計算する。確率計算の結果が棄却限界値である 5%未満であり且つ評価者がその結果を妥当と認めた場合、稀な事象が発生したと判断する。確率計算結果が棄却限界値である 5%以上だった場合、稀な事象は発生しなかったと判断する。ただし、1.4.10 における誤受入率（FAR）の宣言値算出時に、開発者が二項分布以外の方法を使用した場合、評価者は二項分布を用いず開発者が適用した方法に従ってエラー率棄却限界値確認を実施する。なお、独立試験における初期被験者数 100 人で収集されるサンプル数が、開発者が使用した方法の適用条件を満たさない場合、評価者は開発者と協議し、開発者が使用した方法が適用できるよう初期被験者数を設定するか、あるいは、独立試験において二項分布を適用するかをあらかじめ決定しておく。図 11 に FAR 評価 1 におけるエラー率棄却限界値確認の考え方を、FAR の宣言値が 0.0001%で身体部分の数が 2 の評価対象製品を例にとって説明する。

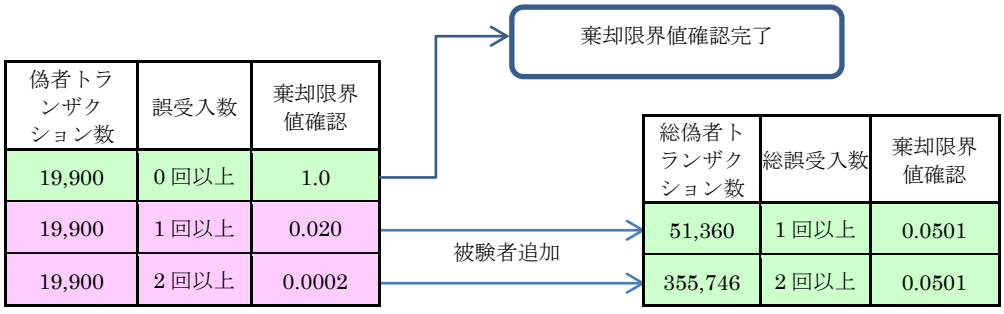


図 11　FAR の宣言値が 0.0001%の場合の計算方法（身体部分数が 2 の場合）

本図の左側の表の偽者トランザクション数が 19,900 となっているのは、独立試験の初期被験者数として評価者が 100 人の被験者を募集し、各被験者がそれぞれの身体部分を使って実施した FTE・FRR 評価で収集されたテンプレートおよび照合バイオメトリック・データを使って偽者トランザクションを性能試験ツールなどを用いて行ったことを示す。偽者トランザクション数の計算式は、100×2×（100×2－1）÷2＝19,900 である。左側の表の各行は発生した誤受入数ごとに事象発生確率を二項分布に従って計算した結果を示す。この事象発生確率の値が有意水準である 0.05 未満だった場合、稀な事象が発生したと判断する。左側の表では、誤受入数が 1 回以上だった場合、事象発生確率が 0.05 を下回る。下回った場合、評価者は開発者と協議し、双方が納得すれば評価者が新たに被験者を追加募集する。追加募集された被験者が FTE・FRR 評価を実施し、その際に収集されたテンプレートおよび照合バイオメトリック・データを追加することで再度偽者トランザクションを実施した結果、追加被験者において誤受入が発生しなかった場合に有意水準以上となる条件を本図の右側の表に示す。

図 12 は、FAR の宣言値が 0.0001%で身体部分の数が 2 の評価対象製品における FAR 評価 1 の具体例を示す。

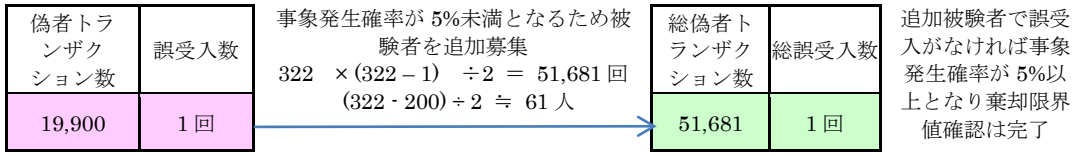


図 12　FAR の宣言値が 0.0001%の場合の具体例（身体部分数が 2 の場合）

初期被験者 100 人での 19,900 回の偽者トランザクションにおいて 1 回の誤受入が発生した場合、事象発生確率は有意水準を下回るため稀な事象と判断される。被験者追加が決定された場合、61 人の被験者を追加することで総被験者数は 161 人となる。この場合の総偽者トランザクション数は 51,681 回となる（計算式は 161×2×（161×2－1）÷2＝51,681 である）。誤受入数が 1 回のままであれば、事象発生確率は有意水準以上の値となる。この結果、FAR 評価 1 のエラー率棄却限界値確認の試験は合格となる。被験者追加の際の人数は、被験者を加えた総偽者トランザクションにおいて誤受入数が変らなかった場合（すなわち追加被験者での誤受入件数が 0 件だった場合）に、総偽者トランザクション数および総誤受入数による二項分布を用いたエラー率棄却限界値確認の結果が、有意水準以上となる人数とする。

(3) 稀さ判定

上記(2)のエラー率棄却限界値確認で稀な事象が発生した場合、評価者は被験者の追加による再評価が必要と判断し、追加被験者数を検討する。追加被験者数は、被験者を追加して再試験を実施した結果、追加被験者においてエラー事象が発生しなかった場合に、累積のエラー率棄却限界値確認結果が 5%以上となる最少人数とする。評価者は、追加被験者による再評価の実施について開発者と協議した上で、FTE・FRR 評価の被験者募集以降を再度実行する。これに対して、稀な事象が発生しなかった場合、FAR 評価 1 は完了となり、次の評価である性能試験再現性確認に進む。なお、協議の際に開発者は独立試験と乖離しないよう宣言値を変更することにより、被験者の追加をせずに合格条件を満たすことができる。

2.4.2.4 性能試験再現性確認

評価者は、開発者の性能試験環境の所在地に移動する。（この際、FTE・FRR 評価に参加した被験者のテンプレートや照合バイオメトリック・データを帯同する。）評価者は、開発者の性能試験の再現性を確認するため、開発者による性能試験に参加した被験者の被験者 ID と身体部分を評価者が十分と考える数だけ抽出し、開発者による性能試験環境に保存されている被験者のテンプレートや照合バイオメトリック・データによる本人トランザクションまたは偽者トランザクションを実行する。

評価者は、得られた判定結果と照合スコア値を、開発者が独立試験前に提出した性能試験エビデンスの該当情報と比較し、一致することを確認する。この作業を、評価者が十分と考える数だけ繰り返すことで、開発者による性能試験の結果が正しく再現されることを確認する。性能試験が正しく再現されないと評価者が判断した場合、評価者は開発者に試験環境の是正が必要なことを通知する。例えば、評価者は開発者の試験環境を訪問する時、開発者性能試験に参加した被験者の中から人口統計分布に従いある割合（例：1%程度）を抽出し、抽出した被験者のテンプレートおよび照合バイオメトリック・データを用いて本人トランザクションおよび偽者トランザクションを実行する。実行して得られた照合判定結果および照合スコアを性能試験エビデンスの該当する情報と比較し、一致することを確認することにより、性能試験が正しく再現されるかを確認することができる。評価者が独立試験で使用しているコンピュータを開発者の試験環境を訪問する時に帯同し、開発者による性能試験のデータを評価者のコンピュータにコピーすることを開発者が認めた場合、評価者は開発者から受け取った被験者データを用いて本人トランザクションおよび偽者トランザクションを実行し、得られた結果を開発者が提出した性能試験エビデンスの該当する情報と比較することで、開発者の性能試験の再現性とあわせて、独立試験環境の正しさを確認することができる。再現性に問題がないと判断された場合、FAR 評価 2（組合せ FAR 評価）に進む。

2.4.2.5 FAR 評価 2（組合せ FAR 評価）

(1) 偽者トランザクションの実行

評価者は、開発者が性能試験で収集した被験者のテンプレートまたは照合バイオメトリック・データと、評価者が独立試験における FTE・FRR 評価（前述）で収集した被験者のテンプレートまたは照合バイオメトリック・データを組合わせて偽者トランザクションを実行し、偽者トランザクション実行結果一覧情報を収集しなければならない。この際評価者は、誤受入数が 3 件以上だったときにエラー率棄却限界値確認結果が 5%未満となる偽者トランザクション数を最小トランザクション数とし、この数を満足する人数分の被験者のテンプレートまたは照合バイオメトリック・データを開発者の性能試験環境から抽出した上で評価を実施する。（開発者の性能試験に参加したすべての被験者のテンプレートまたは照合バイオメトリック・データを使う必要はない。）評価者は、抽出する被験者の人口統計分布が 1.3.4 の母集団の人口統計に従うことを考慮する。実際に抽出する人数は、評価者が開発者と協議して決定する。独立試験で収集されたテンプレートや照合バイオメトリック・データを、開発者試験で収集されたテンプレートや照合バイオメトリック・データとどのように組合わせて使用するかは、評価機関が判断し決定する。

(2) エラー率棄却限界値確認

評価者は、発生したエラー（誤受入）の回数から確率計算を行う。すなわち、偽者トランザクションで

発生した誤受入件数と実行した総偽者トランザクション数より、二項分布に基づく発生確率を計算する。確率計算の結果が棄却限界値である 5%未満であり且つ評価者がその結果を妥当と認めた場合、稀な事象が発生したと判断する。確率計算結果が棄却限界値である 5%以上だった場合、稀な事象は発生しなかったと判断する。ただし、1.4.10 における誤受入率（FAR）の宣言値算出時に、開発者が二項分布以外の方法を使用した場合、評価者は二項分布を用いず開発者が適用した方法に従ってエラー率棄却限界値確認を実施する。なお、独立試験における初期被験者数 100 人で収集されるサンプル数が開発者が使用した方法の適用条件を満たさない場合、評価者は開発者と協議し、開発者が使用した方法が適用できるよう初期被験者数を設定するか、あるいは、独立試験において二項分布を適用するかをあらかじめ決定しておく。図 13 に FAR 評価 2 におけるエラー率棄却限界値確認の考え方を、FAR の宣言値が 0.0001%で身体部分の数が 2 の評価対象製品を例にとって説明する。

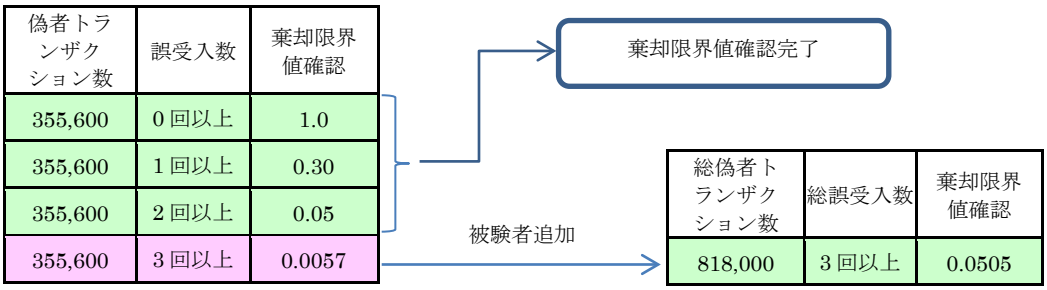


図 13　FAR の宣言値が 0.0001%の場合の計算方法（身体部分数が 2 の場合）

本図の左側の表の偽者トランザクション数が 355,600 となっているのは、開発者試験の被験者として 3000 人が参加し、かつ、独立試験の初期被験者数として評価者が 100 人を募集した場合、開発者試験の被験者から 889 人を評価者が抽出し、これらの被験者のテンプレートと独立試験の FTE・FRR 評価で収集された 100 人分の照合バイオメトリック・データを使って偽者トランザクションを性能試験ツールなどを用いて行ったことを示す。偽者トランザクション数の計算式は、889×2×100×2＝355,600 である。左側の表の各行は発生した誤受入数ごとに事象発生確率を二項分布に従って計算した結果を示す。この事象発生確率の値が有意水準である 0.05 未満だった場合、稀な事象が発生したと判断する。左側の表では、誤受入数が 3 回以上だった場合、事象発生確率が 0.05 を下回る。評価者は開発者と協議し、双方が納得すれば評価者が開発者試験のデータを追加することによる被験者追加、あるいは、新たに被験者を追加募集することで被験者追加を行う。いずれかの方法で追加されたテンプレートおよび照合バイオメトリック・データを用いて再度偽者トランザクションを実施した結果、追加被験者において誤受入が発生しなかった場合に有意水準以上となる条件を本図の右側の表に示す。
図 14 は、FAR の宣言値が 0.0001%で身体部分の数が 2 の評価対象製品における FAR 評価 2 の具体例を示す。

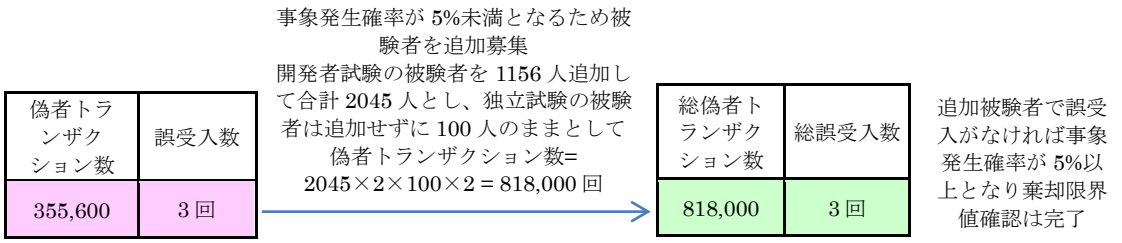


図 14　FAR の宣言値が 0.0001%の場合の具体例（身体部分数が 2 の場合）

開発者試験の被験者として 3000 人が参加し、独立試験の初期被験者として 100 人が参加した場合、開発者試験の被験者から 889 人を評価者が抽出し、これらの被験者のテンプレートと独立試験の FTE・FRR 評価で収集された 100 人分の照合バイオメトリック・データを使った偽者トランザクションにおいて 3 回の誤受入が発生した場合、事象発生確率は有意水準を下回るため稀な事象と判断される。被験者追加として開発者試験に参加した被験者からのテンプレート追加が決定された場合、評価者は 1,156 人分のテンプレートを追加抽出することで、総被験者数は 2045 人となる（計算式は 2045×2×100×2=818,000 である）。誤受入数が 3 回のままであれば、事象発生確率は有意水準以上の値となる。この結果、FAR 評価 2 のエラー率棄却限界値確認の試験は合格となる。被験者追加の際の人数は、被験者を加えた総偽者トランザクションにおいて誤受入数が変らなかった場合（すなわち追加被験者での誤受入件数が 0 件だった場合）に、総偽者トランザクション数と総誤受入数の二項分布を用いたエラー率棄却限界値確認の結果が、有意水準以上となる人数とする。

(3) 稀さ判定

上記(2)のエラー率棄却限界値確認で稀な事象が発生した場合、評価者は被験者の追加による再評価が必要と判断し、追加被験者数を検討する。追加被験者数は、被験者を追加して再試験を実施した結果、追加被験者においてエラー事象が発生しなかった場合に、累積のエラー率棄却限界値確認結果が 5%以上となる最少人数とする。評価者は、追加被験者による再評価の実施について開発者と協議した上で、開発者が実施した性能試験で募集された被験者のテンプレートや照合バイオメトリック・データを再抽出することにより追加して FAR 評価 2 を再実行するか、あるいは、FTE・FRR 評価のための被験者を追加募集して、それ以降の評価を再度実行する。いずれの方法を選択するかは、評価者が開発者と協議したうえで決定する。これに対して、稀な事象が発生しなかった場合、FAR 評価 2 は合格となり、次の作業である合否判定に進む。なお、協議の際に開発者は独立試験と乖離しないよう宣言値を変更することにより、被験者の追加をせずに合格条件を満たすことができる。

2.4.2.6 性能評価結果判定

前述までで示した試験内容において以下に示す①および②の結果が得られた場合、性能評価の試験に合格とする。

① FTE・FRR 評価、FAR 評価 1、および、FAR 評価 2 におけるエラー率棄却限界値確認において、稀な事象が検出されなかった。
② 性能試験再現性確認で、結果が正しいと評価者が判断した。

上記②の条件を満足したが、①の条件を満足しなかった場合、開発者は①において稀さが検出されないように ST に記載する宣言値を変更することができる。評価者は、開発者によるこの変更が妥当と判断した場合、判定結果を合格とする。

2.5 評価者と開発者間の協議

評価者は必要に応じて開発者と協議しながら独立試験を実施する。試験の実施において、特に開発者との協議が重要な項目を以下に示す。

(1) 試験開始前

① 独立試験の実施に先立ち、開発者が必要と考えるすべての事前説明を、開発者は評価者に対して行うことができる。事前説明の終了条件は、開発者及び評価者が相互に納得するまでとする。事前説明には、少なくとも、被験者に対する装置の操作説明、被験者がしがちな操作誤り、エラー発生時の被験者へのガイダンス方法、登録や照合における除外ケースなど、開発者の性能試験において評価担当者が行っている試験実施上の考慮事項や注意事項が含まれる。

② 構築した試験環境における環境条件（結果に影響を与える制御要因など）が、開発者による性能試験の実施環境に準じていることを開発者と評価者が協議し、同意することが強く推奨される。

(2) 試験実施中

① 開発者は評価者による独立試験に立ち会い、必要に応じて評価者と協議することができる。ある被験者の試験実施中に、集計対象外とすべき事象が発生したと開発者が判断した場合、開発者は評価者に対する提案のために、一時的な試験の中断を求めることができる。開発者からの提案には、正当な理由を伴った、その被験者の試験のやり直しや、試験からの除外が含まれる。評価者は開発者の提案の正当性を確認したうえで、該当被験者に対する試験方法を決定する。なお、開発者は被験者に対して直接働きかけることはできない。

② エラー率棄却限界値確認で稀さが見つかった場合、評価者は開発者と協議したうえでその妥当性を判断する。

③ 稀さの妥当性が認められた後の被験者追加、あるいは、使用する開発者が実施した性能試験の被験者データについて、評価者は開発者と協議したうえで評価方法を決定する。

- FTE・FRR 評価および FAR 評価 1（独立 FAR 評価）において稀さが検出された際の追加被験者数とコスト
- FAR 評価 2（組合せ FAR 評価）において使用する開発者が実施した性能試験の被験者数、被験者を部分抽出する際の抽出方法、および、稀さが検出された際の被験者追加方法（開発者が実施した性能試験の被験者データを追加する、あるいは、FTE・FRR 評価のための被験者を評価者が追加募集する）

④ 稀さが検出された後、ST に記載した宣言値を独立試験の結果と乖離しないように変更することにより、被験者を追加せずに合格することを開発者が希望した場合、評価者と開発者は協議したうえで合格条件を満たす宣言値を決定する。

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以下に示す。

表 10　ISO/IEC 19795-1:2006 の報告項目と本サポート文書における報告項目の対応

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）	
		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、複数の照合バイオメトリック・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

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、開発者が評価対象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（センサへの接触があるかないか、など）により開発者毎に異なる場合がある。

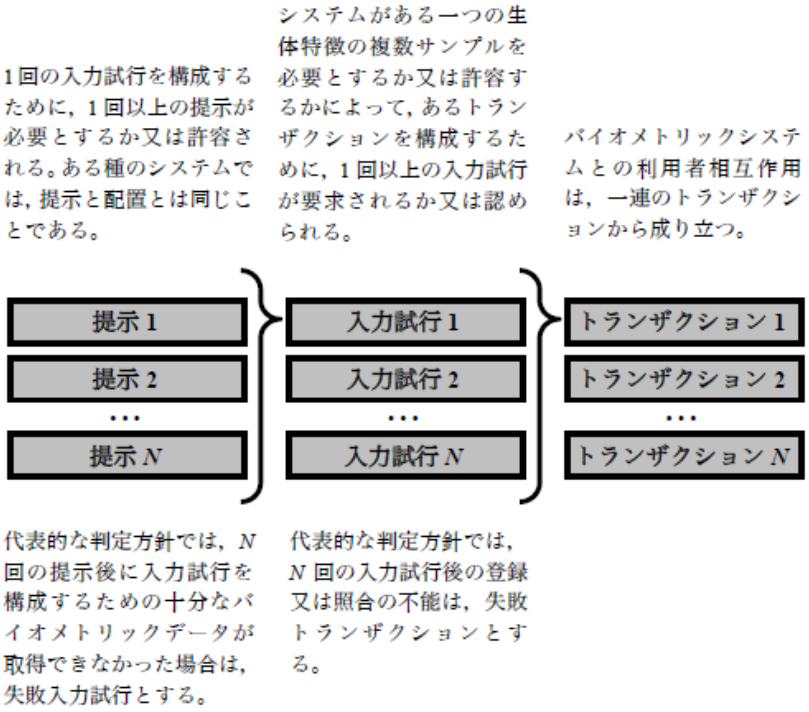


図 15 トランザクションと入力試行と提示の関係

2. トランザクションのシミュレートについて

開発者が実施する性能試験においては、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テンプレートや照合バイオメトリック・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者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、最大照合バイオメトリック・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）。

付録４　19989-1 目次

付録５　19989-2 目次

Contents Page

付録６　19989-3 目次

平成 28 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 29 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