Android OS 版
掌静脈認証ソフトウェア
セキュリティターゲット

Version 1.27

PVA01a-CC-ST-127

ユニバーサルロボット株式会社

内容

更新履歴

Version	Date	Description
1.00	2016/02/18	初版
1.01	2016/07/08	PP に合わせて更新
1.02	2016/08/12	BS 管理者の説明を詳細化
1.03	2016/08/23	個人利用ユーザは ID を指定しなくて良く、“アプリケーションが定める ID が指定される”という表現に変更。
1.04	2016/09/01	文書全体の表現及び用語を統一。
1.05	2016/09/01	4.2 の BS 管理者毎の詳細説明部分を字下げした。
1.06	2016/09/13	TOE 物理的範囲明確化、および誤記の修正。
1.07	2016/09/24	FIA_BVR の選択を 3 から 2 に変更
1.08	2016/09/25	FIA_BVR.2 への変更漏れ、PAD の説明修正。
1.09	2016/09/30	FDP_RIP.1 の割付と 7.での説明の不整合修正。 7.における検査機能の説明修正。
1.10	2016/10/06	TOE 自身を.so ファイルと.jar ファイルに変更。
1.11	2016/10/24	FIA_UID.2 を FIA_UID.1 に変更
1.12	2016/10/27	TOE の物理的範囲を修正。誤字を修正。
1.13	2016/11/20	FIA_BVR の選択を 1 に変更。Android ver.変更
1.14	2016/11/27	ガイダンス文書を TOE の構成物に明記。
1.15	2016/11/29	ガイダンス文書名を修正
1.16	2016/11/30	7.の FAR,FRR 数値の誤記修正
1.17	2017/01/04	TOE の.jar ファイル名称誤記を修正、TOE ガイダンス文書にリファレンスマニュアルを追記。
1.18	2017/08/18	TOE 更新に伴う変更反映。
1.19	2017/08/24	1.3.3,1.4.2 の説明誤りを修正。
1.20	2017/09/06	検査機能、特徴抽出機能、PAD 機能の説明不整合を修正。
1.21	2017/09/15	TOE に関連しない PP 記載を削除。生体情報抽出の技術的説明を追加。使用が想定される環境の一部を TOE 要約に移動。
1.22	2017/10/17	TOE に必要なハードウエアの仕様の記載変更
1.23	2017/10/25	使用対象地域を再記載、誤記および“試行”の表現修正、TOE バージョン名変更、性能評価結果の反映

1.24	2017/11/07	FTE,FAR の誤り修正。性能評価のサポート文書との相違を追記。
1.25	2017/11/27	7.TOE 要約の Application Note の記述を修正。
1.26	2017/12/08	1.3.3.にユーザの正当性確認の記述を追加。 7.にて TOE がライブラリである事を強調。
1.27	2018/01/18	“ソフトウェア”の揺らぎを統一

1. ST 概説

1.1. ST 参照

タイトル: Android OS 版 掌静脈認証ソフトウェア　セキュリティーターゲット
版数 1.27
発行 2018/01/18
発行者 ユニバーサルロボット株式会社
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、静脈認証、プロテクションプロファイル、セキュリティターゲット

1.2. TOE 参照

開発者名 ユニバーサルロボット株式会社
TOE 名 Android OS 版 掌静脈認証ソフトウェア
TOE バージョン番号 Ver1.00.m01

1.3. TOE 概要

1.3.1. TOE の種別

本 TOE は、利用者認証に使用される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 はソフトウェアライブラリであり、アプリケーションに組み込まれて呼び出されることにより動作する。TOE は、利用者認証情報として個人に固有の生体情報である掌静脈と掌紋を用いることで、利便性が高く、本人でなければ認証されない特性を持つ認証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及びデータ採取機能は含まない。

1.3.2. TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE に必要なハードウェアは、スマートフォンなどのモバイルデバイスである。TOE は Android OS 上で動作するソフトウェアである。TOE はモバイルデバイス上の背面カメラ、撮影補助光(LED フラッシュ)及びディスプレイを使用する。
TOE を動作させ使用するために必要なハードウェア及びソフトウェア(OS)を以下に記載する。

本体	下記に列挙する機能や仕様を具備した スマートフォンまたはタブレット
機能および仕様	
OS	Android※1
API	Android 標準 API Level 22 をサポートしていること※1。
背面カメラ	◇スマートフォン 画素数：400 万画素以上 F 値：1.7～2.4 ・3 原色（RGB）色分解イメージセンサー ・VGA サイズで 10fps 以上のプレビューが可能 ◇タブレット 画素数：200 万画素以上 F 値：2.8 以下 ・3 原色（RGB）色分解イメージセンサー ・VGA サイズで 10fps 以上のプレビューが可能
LED フラッシュ	・赤色光を含むこと(白色 LED は赤色光を含む)。
ディスプレイ	◇スマートフォン サイズ：4.5inch～5.5inch 縦横比：16:9 発色：フルカラー約 1677 万色 その他：タッチスクリーン機能 ◇タブレット サイズ：7.0inch～10.5inch 縦横比：16:9 発色：フルカラー約 1677 万色 その他：タッチスクリーン機能

※１：Application Note

Camera2 API をサポートしている API Level22 以上である事。出荷時において API Level 22 未満を搭載したスマートフォンでバージョンアップにより API Level22 以上とした場合は対象外である。API Level22 をサポートしている Android OS のバージョンは、2017/10/31 現在、5.1.1,6.0-6.0.1,7.0-7.1.2,8.0 である。

1.3.3. TOE の使用法

TOE は、具体的には、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。TOE は生体情報の登録及びバイオメトリック照合を行うソフトウェアライブラリであり、モバイルバンキングや決済アプリケーション等に組み込まれて使用される。TOE はこれらのアプリケーションを開発する、アプリケーション開発者によってアプリケーションに組み込まれ、アプリケーションを使用するユーザに対する、利用者認証機能を提供する。ユーザは、これらアプリケーションが搭載された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の全体を含む最小のシステムを、本 ST では、バイオメトリックシステム(BS(Biometric System))と呼ぶ。TOE をユーザが BS の一部として利用するためには、上記のアプリケーション開発者、BS の設定や運用を管理する管理者が必要である。

以下に、本 TOE における BS の使用の流れを示す。

時系列的に、先ず、登録対象のユーザに対して、登録処理が行われる。

TOE が、主に個人が所有するモバイルデバイスで利用される場合には、登録対象のユーザが BS の設定や運用を管理する管理者を兼ねるため、登録処理は登録対象のユーザ自身が行う。但し、アプリケーション開発者は、登録対象ユーザの正当性を確認したのちに登録を可能とする運用方法を規定する必要がある。一方、主に法人が所有するモバイルデバイスで TOE を利用する場合には、登録対象のユーザとは別に、BS の設定や運用を管理する管理者を法人が任命して登録処理を実施させることもできる。

登録処理では、登録対象ユーザが手のひらをデータ採取機能に提示し、データ採取機能によって生データが採取される。得られた生データは、検査機能により色エッジ抽出処理による手のひら輪郭抽出と、中央矩形領域である特徴データ抽出領域の大きさの判定を行い、品質が検査される。生データが十分な品質であると判定された場合、特徴抽出機能は、生データから特徴データを抽出する。抽出した特徴データから、検査機能により特徴データの情報量を検査し、適正な範囲であるか否かにより品質を判定する。あわせて、検査機能により十分な品質が確認された当該生データを含む複数の生データは、PAD 特徴抽出機能に送られ、偽造生体を機械学習した判定器により、偽造生体判定スコアが PAD 特徴データとして抽出される。

登録機能は、PAD 特徴データが、偽造生体がデータ採取機能に提示された特徴を持たないことを判定した場合、特徴データを、登録生体情報として、ID と対応付けて、格納機能に保存する。

なお生データ及び特徴データが十分な品質を持たない場合、または PAD 特徴データから偽造生体がデータ採取機能に提示されたと判断された場合は、登録できない。

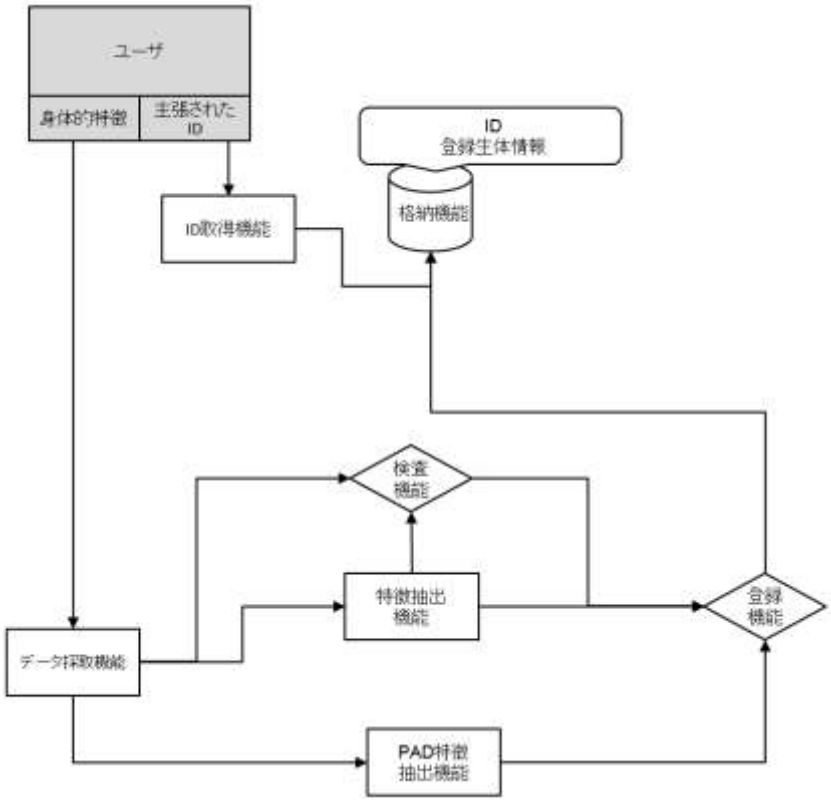


図 1 登録の処理

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

登録ユーザは ID 取得機能に ID を提示する。なお、TOE を含むアプリケーションが、個人が所有するモバイルデバイス上で動作する場合には、ユーザは ID を提示せずに、アプリケーションが定める ID が指定される。提示された ID に対応する登録生体情報は、登録生体情報取得機能により格納機能から取得される。

登録ユーザは手のひらをデータ採取機能に提示し、データ採取機能で生データを取得する。得られた生データは、検査機能により手のひらの有無及び品質判定を機械学習した判定器により、品質判定スコアを計算し、品質が検査される。当該生データが十分な品質であると判定された場合、データ採取機能から生データが特徴抽出機能に送られ、特徴抽出機能によって生データから特徴データを抽出する。

比較機能は、特徴抽出機能が特徴抽出した特徴データと格納機能から取り出された登録生体情報とを比較し、両者の類似度を算出する。特徴データと登録生体情報とを比較した類似度がある閾値を超えた場合、さらに当該生データを含む複数の生データが、PAD 特徴抽

出機能に送られ、偽造生体を機械学習した判定器により、偽造生体判定スコアを PAD 特徴データとして抽出する。
決定機能は、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にあって、PAD 特徴データが、偽造生体がデータ採取機能に提示された特徴を持たないことを判定した場合にのみ、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。

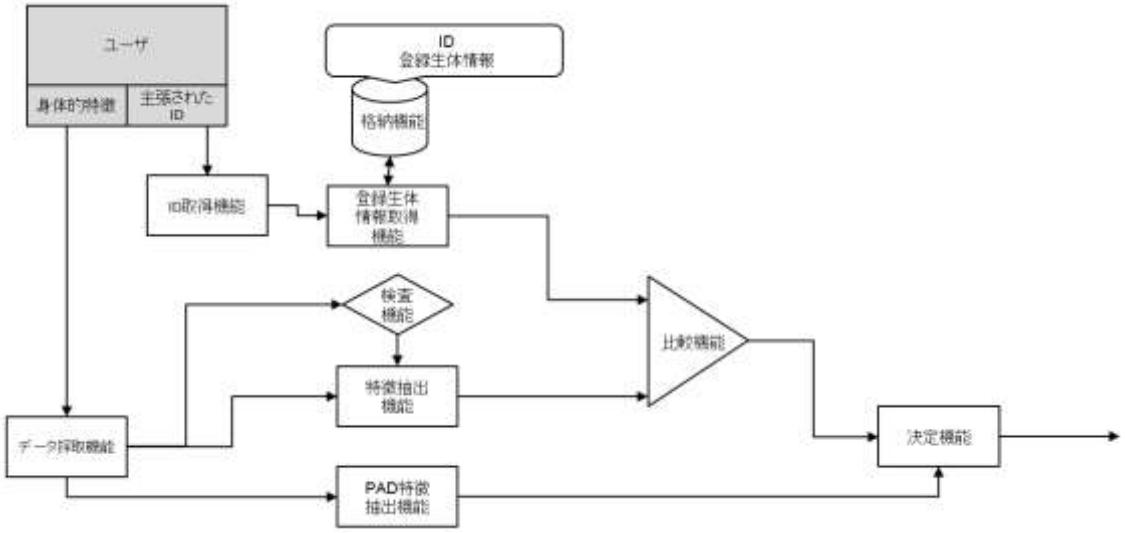


図 2 バイオメトリック照合の処理

本 ST では、登録ユーザがバイオメトリック照合され利用者認証された結果、登録ユーザは TOE 外の所望の論理的資産にアクセスできる。
利用者認証を個人が利用するアプリケーションの例としては、バイオメトリック照合の結果、使用可能になるモバイルバンキングアプリへのログインによる各種取引やオンライン決済などがある。法人利用の場合の例としては、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。

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機能の特性

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

(1)誤受入率・誤拒否率

バイオメトリック照合は、生体情報に基づいており、あらかじめ登録された登録生体情報と照合時に得られる特徴データの類似度が閾値を超えれば、バイオメトリック照合を成功させる。そのため、登録されているユーザが誤って拒否されてしまう、あるいは登録されていないユーザが誤って受け入れられてしまう現象が発生することがある。前者の発生率を FRR(False Reject Rate　誤拒否率)、後者の発生率を FAR(False Accept Rate　誤受入率)と呼ぶ。

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

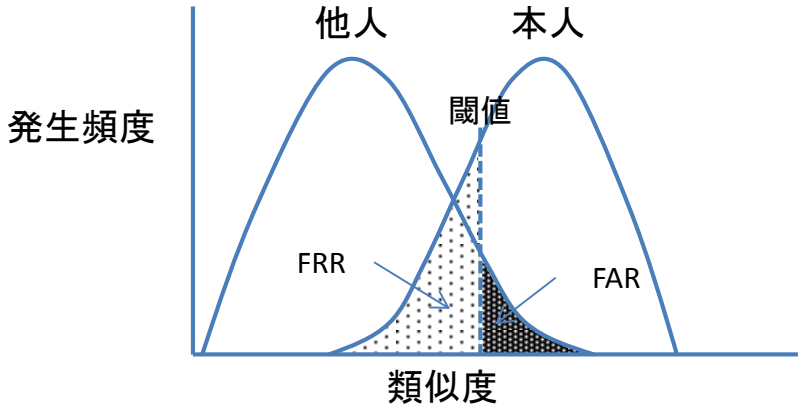


図 3 バイオメトリック照合の類似度分布

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、TOE は FTE（Failure To Enrol（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)偽造物等を用いた攻撃
BS に対する攻撃には、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 で挙げたエラー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 TOE は、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、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 TOE は、AVA_VAN.2 に相当する基本的な攻撃能力を想定し、脅威に記述する。

1.3.4.3. セキュリティに関する管理機能

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、提供されない。

1.3.5. TOE の構成

TOE は、スマートフォンやタブレットなどモバイルデバイス上のソフトウェアである。TOE の構成要素は物理的に分離していない。

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 の使用用途とそれに対応した想定使用環境に依存する。本 TOE はモバイルデバイス上で動作するモバイルバンキングやモバイル決済のアプリケーションに組み込まれて使用される。こうした金融サービスでは、ユーザは「いつでも、どこでも」サービスの利用をすることが想定される。法人の業務アプリケーションに組み込まれて使用される場合でも、通常のビジネス時間であれば、場所や時間の制約を厳格に設けることが難しい。
TOE の使用において、モバイルデバイス上のカメラをデータ採取機能として使用することから、使用場所の光源環境が誤受入率・誤拒否率に影響を与えることになる。
本 TOE では、標準的な室内環境（約 1000lx）から夜間車内ルームランプ点灯時相当の 100lx、さらに晴天日陰相当の約 10000lx での使用が想定される(90～11000lx を使用可能範囲とする)。モバイルデバイスのカメラで画像の撮影ができない程の暗い環境では、本 TOE の使用は適さない。

また TOE は、モバイルデバイスを片手持ちの状態で使用される事を想定している。
その他、以下要因について変化する環境・条件での使用を想定している。

- 使用対象者は、ほぼ毎日スマートフォンを使用していて、モバイルバンキング等の金融サービスや、モバイルショッピング等を頻繁に利用しているスマートフォンユーザ。年齢はおおよそ 18 歳～59 歳で、20 代、30 代を中心とする男女。
- 温度：10℃～28℃
- 東アジアや東南アジアを中心に、国内外での利用を想定。

1.4. TOE 記述

TOE は、スマートフォンやタブレット等、背面カメラを備え Android OS を搭載したモバイル端末上で動作する生体認証ソフトウェアである。モバイル端末の背面カメラで撮影された手のひら画像の生データを取得して、特徴データを抽出し、登録生体情報を作成し、格納機能へ保存する。照合時にはモバイル端末の背面カメラから手のひら画像の生データを取得して、特徴データを抽出し、登録生体情報と特徴データとの類似度を算出し、類似度がある閾値を超えた場合、バイオメトリック照合の成功とするものである。また、TOE は保存された登録生体情報を削除する機能を備えている。

1.4.1. TOE 境界

TOE はソフトウェアライブラリであり、アプリケーション開発者によってアプリケーションに組み込まれて使用される。
TOE は、ハードウェアを含まない。
TOE の物理的範囲を以下に示す。

図 4 TOE の物理的範囲

TOE は以下の.so ファイルと.jar ファイルである。

- LibURpalmvein.so (TOE 自身)
- URpalmLib.jar (TOE 自身、Java ライブラリ)

TOE を構成するガイダンス文書は以下の通りである。

・Android OS 版掌静脈認証ソフトウェア準備ガイダンス
・Android OS 版掌静脈認証ソフトウェア運用ガイダンス
・Android OS 版掌静脈認証ソフトウェア I/F 解説書
・Android OS 版掌静脈認証ソフトウェアアプリケーション開発マニュアル
・Android OS 版掌静脈認証ソフトウェアリファレンスマニュアル

TOE に伴う配付物は以下である。
・サンプルアプリケーションソースコード
(URSampleP/app/src/main/java/jp/co/urobot/ursamplep フォルダ以下に格納の java ファイル)

TOE の論理的範囲及び運用環境の機能の一例を図 5、図 6 及び図 7 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 に含まれる機能を表す。
　太枠外の実線四角は、TOE の運用環境で提供される機能を表す。
　影の付いた実線四角は、ユーザを表す。
図のとおり、データ採取機能、格納機能、ID 取得機能は、TOE に含まれない。これらは、モバイル端末上で提供される。

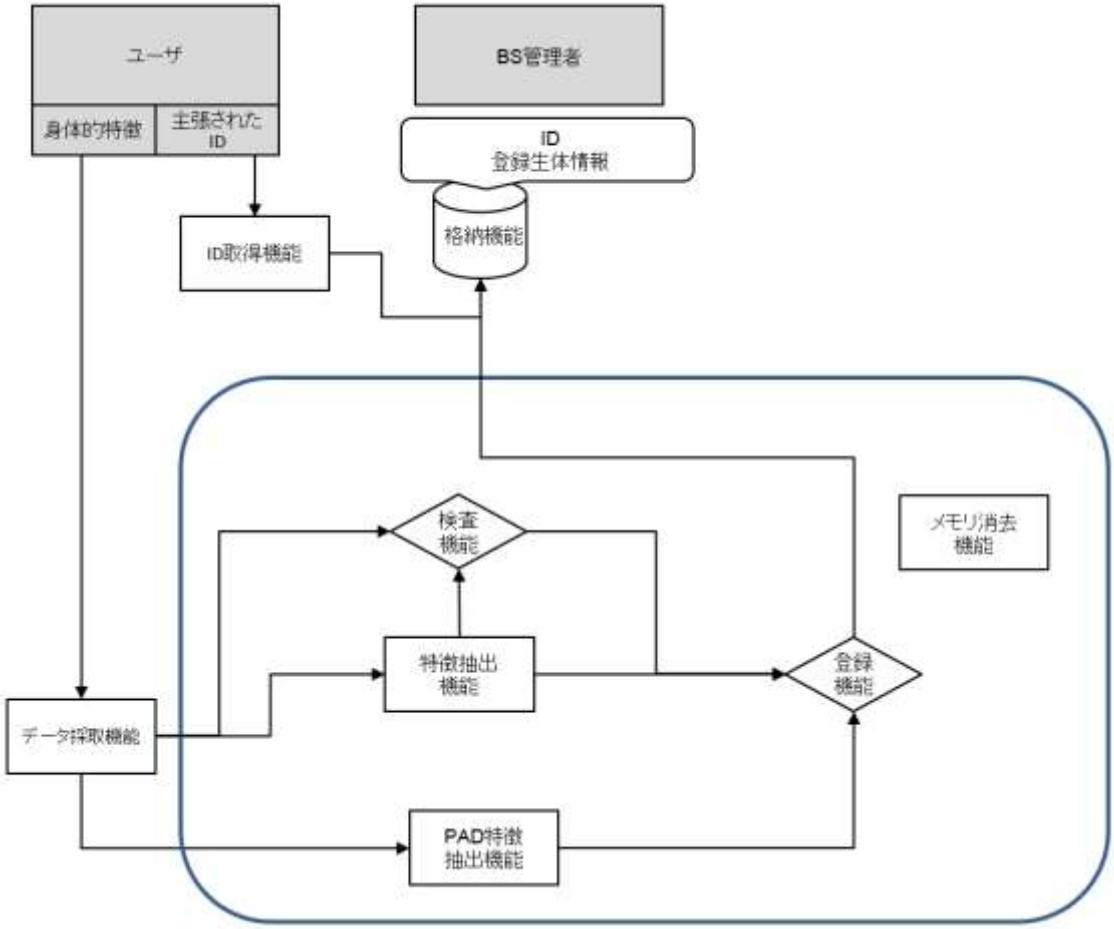


図 5　TOE の構成（登録の場合）

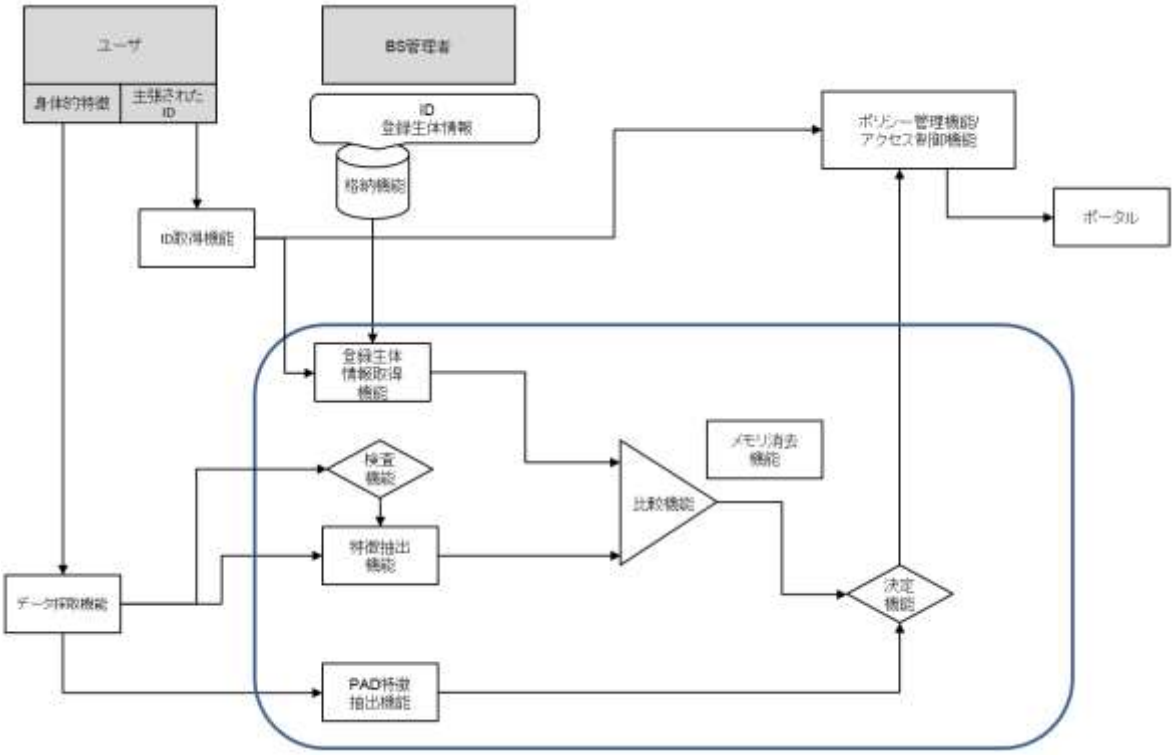


図 6 TOE の構成（照合の場合）

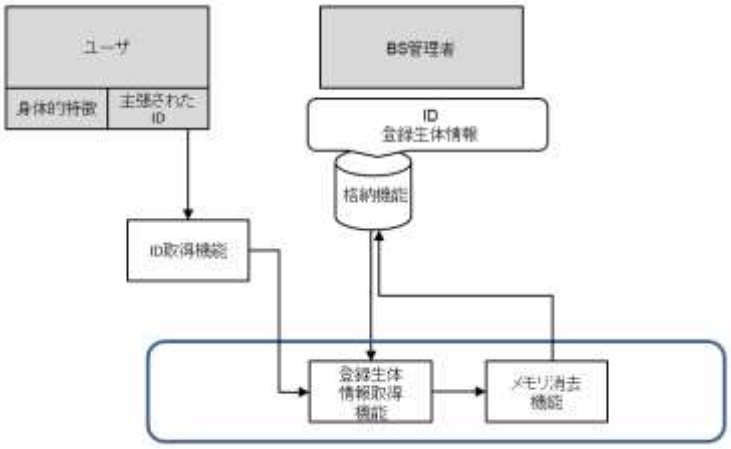


図 7 TOE の構成（登録生体情報削除の場合）

1.4.2. TOE の機能

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。抽出されたデータを特徴データと呼ぶ。抽出されたデータは圧縮される場合もある。
  特徴の抽出は、検査機能により生データが十分な品質であると判断された生データに対して特徴抽出を行う。

- 検査機能：この機能は、登録時には、データ採取機能から得られた生データに含まれる色エッジ抽出処理による手のひら輪郭抽出や、矩形マッチング処理による特徴データ抽出領域の大きさの判定、抽出した特徴データの情報量の検査により、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。また照合時には、手のひらの有無及び品質判定を機械学習した判定器により、品質判定スコアを計算し品質を検査する。
- 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、撮影生データを画面に表示してユーザに確認を促し、ユーザが適正と判断した場合に、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。品質が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 ST 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。
- 登録生体情報取得機能：この機能は、ユーザの ID に対応する既に登録された登録生体情報を取得する。
- 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と、格納機能に登録されており登録生体情報取得機能で取り出された登録生体情報とを比較し、両者の類似度を算出する。
- 決定機能：この機能は、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。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。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とする。
- PAD 特徴抽出機能：PAD 特徴データは、データ採取機能から得られる生データから抽出される。PAD 特徴データは、機械学習した偽造生体判定器を使い、生データを偽造生体判定器へ入力する事により得られる偽造生体判定スコアである。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/失敗の決定に直接的または間接的に使われる。
- メモリ消去機能：この機能は、攻撃からの保護のために、使用後のメモリの内容を消去する。消去されるべき情報は、登録生体情報、特徴データ、生データなどが含まれる。

TOE は、データ採取機能、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を、提供しない。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。各機能の内容は以下のとおりである。

- データ採取機能：この機能は、ユーザから生データを採取し、検査機能、特徴抽出機能や PAD 特徴抽出機能に生データを送る役割を担う。
- 格納機能：運用環境は TOE が使うデータベースを提供しなければならない。このデータベースは、ユーザの登録生体情報を格納する。登録生体情報以外の情報を含むこともある。
- ID 取得機能：この機能は、ユーザが入力する ID を獲得する。この機能は、入力された ID 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。また、右手・左手を本 TOE ではサブ ID と捉える。個人利用の製品の場合は、ID の入力は明示的でなくても良く、アプリケーションが定める ID およびサブ ID が TOE に入力されても良い。法人利用の場合は ID の入力は明示的であるが、サブ ID はアプリケーションが定めるサブ ID が TOE に入力されても良い。
- ポリシー管理機能/アクセス制御機能：バイオメトリック照合の結果は、運用環境のポリシー管理機能/アクセス制御機能に渡される。この機能は、ユーザの権利をチェックし、ユーザが十分な権限を持っていて TOE によるバイオメトリック照合が成功し、利用者認証された場合に、ユーザのポータルへのアクセスを許可する。すなわち、この機能は、ポータルへのアクセスコントロールを実現するものである。
- セキュア通信機能：運用環境は、セキュリティ関連データのセキュアな通信をサポートする。セキュアな通信は、TOE からの通信、TOE への通信、TOE の構成要素間の通信の場合がある。
- ポータル：物理的または論理的な点であって、そこから先にある物理的または論理的な資産が運用環境のポリシー管理機能/アクセス制御機能で守られているような点である。ポリシー管理機能/アクセス制御機能は、上述のとおり、TOE からユーザの ID に対するバイオメトリック照合結果を受け取り、アクセス制御を実施する。

2. 適合主張

2.1. CC 適合主張

本 ST 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 ST 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 ST は、CC パート 3 適合を主張する。

2.2. PP 主張

本 ST 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第 1.2 版（JISEC 認証番号 C0501）に正確適合している。

2.2.1. 適合根拠

本 ST の TOE 種別はバイオメトリック照合製品であり、上記 PP の TOE 種別であるバイオメトリック照合製品と一致している。

2.3. パッケージ主張

本 ST は、EAL2 追加を主張する。追加される保証要件は、ALC_FLR.1 である。

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。

（本 ST が準拠する PP である C0501 の BS 管理者の定義は上記のとおりであるが、本 ST では、TOE のインストールに至るアプリケーションの開発に当たるアプリケーション開発者も BS 管理者とする。特に断らない限りは、アプリケーション開発は、TOE のインストールに含めて考える。以下において、両者を識別する必要がある場合は、アプリケーション開発者をアプリケーション開発の BS 管理者、アプリケーション開発より後のインストール、設定、及び運用に当たる管理者を運用を含む BS 管理者、と表現する。）

登録ユーザ：

TOE を含む BS に生体情報を登録し、TOE にバイオメトリック照合され利用者認証されることによって、ポータルへアクセスする。

攻撃者：

権限なくポータルへアクセスすることを目的に、登録時に偽造生体や品質の低い生体情報を意図的に登録することを試みたり、照合時に TOE に不正にバイオメトリック照合されることを試みる。

3.2. 資産

本 ST では、以下の資産を定義する。

1 次資産：

TOE 外に存在する資産であって、登録ユーザが TOE でバイオメトリック照合され利用者認証されることによってポータルを経てアクセスできる資産。この資産は、物理的資産の場合も、論理的資産の場合もある。

2 次資産：

TOE が生成するデータ及び BS 管理者が作成する TOE 内のデータ。

TOE 内で処理され使用される生体情報、閾値などのバイオメトリック照合のためのパラメータなど。

3.3. 前提条件

A.ADMINISTRATION

BS 管理者は、悪意を持たない。すなわち、攻撃者になったり、攻撃者に情報提供することはない。

運用を含む 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。

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。

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。

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

3.4. 脅威

T.CASUAL_ATTACK

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

T.PRESENTATION_ATTACK

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

3.5. 組織のセキュリティ方針

P.ENROL_ADMINISTERED

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

P.RESIDUAL

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

P.CONTROL_FALSE_REJECT

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

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.PAD_ENROL

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

O.CLEAR_RESIDUAL

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

O.CONTROL_FALSE_ACCEPT

TOE は、誤受入率(FAR)に対する基準を満たさなければならない。

O.PAD_VERIFY

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

O.CONTROL_FALSE_REJECT

TOE は、誤拒否率(FRR)に対する基準を満たさなければならない。

4.2. 運用環境のセキュリティ対策方針

OE.ENROL_ADMINISTERED

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

アプリケーション開発の BS 管理者は、運用を含む BS 管理者だけが TOE の登録処理を実行できるような機能を提供しなければならず、運用を含む BS 管理者は、運用を含む BS 管理者だけが TOE の登録処理を実行できるように運用しなければならない。

OE.PROTECT_RESIDUAL_ENVIRONMENT

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

アプリケーション開発の 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ように、アプリケーションを開発しなければならない。

OE.ACCESS_CONTROL

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

アプリケーション開発の BS 管理者は､バイオメトリック照合が成功した場合に限って、ユーザのポータルへのアクセスを許可するアプリケーションを開発しなければならない。運用を含む BS 管理者は、そのアプリケーションを使用して、バイオメト

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

OE.LIMIT_NUM_TRIAL

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

アプリケーション開発の BS 管理者は、生体情報登録の試行回数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開発しなければならない。また、アプリケーション開発の BS 管理者は、バイオメトリック照合の試行失敗が一定回数以上に達した場合、当該ユーザのアカウントをロックするようアプリケーションを開発しなければならない。

運用を含む BS 管理者は、そのアプリケーションを利用して、生体情報登録の試行回数が一定回数以上に達した場合、登録を失敗としなければならない。運用を含む BS 管理者はその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。

アプリケーション開発の BS 管理者及び運用を含む 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。運用を含む 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 内の 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。

アプリケーション開発の BS 管理者は、TOE 内の 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で動作するアプリケーションを開発しなければならない。運用を含む BS 管理者は TOE 内の 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保護される運用環境を提供しなければならない。

上記において、BS 管理者は、運用を含む BS 管理者である。

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。

上記において、BS 管理者は、運用を含む BS 管理者である。

4.3. セキュリティ対策方針根拠

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

表 1　セキュリティ対策方針根拠

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

4.3.1.　脅威への対抗

T.CASUAL_ATTACK

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

T.PRESENTATION_ATTACK

T.PRESENTATION_ATTACK では、攻撃者が、別の攻撃者に 1 次資産にアクセスさせる

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

4.3.2. 組織のセキュリティ方針の実現

P. ENROL_ADMINISTERED

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

P.RESIDUAL

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

P.CONTROL_FALSE_REJECT

P.CONTROL_FALSE_REJECT では、登録ユーザが身体的特徴の提示をした場合のバイ

オメトリック照合の失敗を、一定の割合以下にしなければならないことを求めている。これは、O.CONTROL_FALSE_REJECT によって、TOE が運用に支障のない誤拒否率(FRR)を持つことで、実現される。

4.3.3. 前提条件への対応

A.ADMINISTRATION

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

A. PROTECT_ASSETS

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

A.COMMUNICATION

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

A.ENVIRONMENT

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

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

5. 拡張コンポーネント定義

クラス FIA（識別と認証）の拡張された機能ファミリ FIA_EBT（Enrolment of Biometric Template）及び FIA_BVR（Biometric VeRification）は、この ST 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。

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。

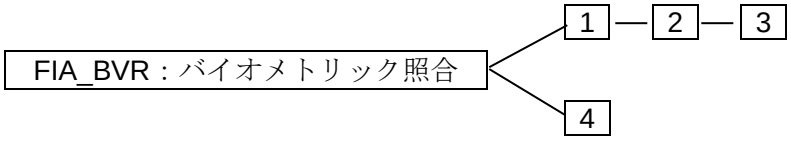
FIA_EBT.2 生体情報登録失敗率の低い生体情報登録
下位階層: なし
依存性: なし

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。

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れ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。

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。

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 ST 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。

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: *データ採取機能（カメラ）から取得した生データ、生データから抽出した特徴データ、格納機能より取得した登録生体情報、生データから抽出した PAD 特徴データ、生体特徴類似度計算、偽造物判定計算、生体情報品質判定計算の結果及び用いたパラメータ*]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。

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。

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。

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：*0.4%]*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。

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：*0.0006%*]以下、FRR[割付：*0.2%*]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。

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。

6.2. セキュリティ保証要件

本 ST 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 0.0006%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。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、FRR0.2%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。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 ST 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 ST 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 ST 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. TOE 要約仕様

TOE は、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。スマートフォンやタブレットの背面カメラを使って手のひらを撮影することにより得られた画像から、色成分を処理して血管を強調することにより抽出される掌静脈情報からなる生体情報を抽出して登録及びバイオメトリック照合を行うソフトウェアライブラリである。TOE はソフトウェアライブラリであるので、アプリケーション開発者によって以下のようなアプリケーションに組み込まれて使用されるものである。

・モバイルバンキングのアプリケーションソフトウェアであって、モバイルバンキングへのログインや各種サービスを提供する際の、本人認証を行うために TOE を使用する。
・モバイル決済を行うソフトウェアであって、決済時の本人認証を行うために TOE を使用する。
・法人においては、社内の機密情報を取り扱うソフトウェアであって、機密情報へのアクセス権限をもつユーザの認証のために TOE を使用する。

個人が所有するモバイル機器上での使用も想定するため、歩行時や乗り物に乗りゆれる状態や、手が濡れていたりハンドクリームが塗られている状態でも使用されることを想定している。TOE はアジアを中心とした国内外での利用を想定しており、様々な人種が使用する事も想定している。生体情報の登録及びバイオメトリック照合の処理の全体を含む最小のシステムを、本 ST では、バイオメトリックシステム(BS(Biometric System))と呼ぶ。

TOE はこれらのアプリケーションを開発するアプリケーション開発者によってアプリケーションに組み込まれ、アプリケーションを使用するユーザに対する利用者認証機能を提供する。このアプリケーション開発者を、ここではアプリケーション開発の BS 管理者という。また、ユーザは、これらアプリケーションが搭載された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。こうした BS の設定や運用を管理する管理者を、ここでは運用を含む BS 管理者という。

TOE は、登録対象のユーザに対して、登録処理を行う。

TOE が、主に個人が所有するモバイルデバイスで利用される場合には、登録対象のユーザが運用を含む BS 管理者を兼ねるため、登録処理は登録対象のユーザ自身が行う。一方、主に法人が所有するモバイルデバイスで TOE を利用する場合には、登録対象のユーザとは別に、BS の設定や運用を管理する管理者を法人が任命して登録処理を実施させることもできる。

登録処理では、登録対象ユーザが手のひらをデータ採取機能に提示して、画面に表示されている登録ボタンをタップすることにより、データ採取機能が生データを採取する。得られた生データは、検査機能により色エッジ抽出処理による手のひら輪郭抽出や、中央矩形領域である特徴データ抽出領域の大きさの判定を行い、品質が検査される。その結果、手のひらが提示されていない状態、位置が適正でない状態、手のひらとはかけ離れた、色成

分や輪郭、テクスチャを持つ提示物は、品質が十分でないと判定する。生データが十分な品質であると判定された場合、特徴抽出機能は、生データから特徴データを抽出する。抽出した特徴データから、検査機能によりの情報量を検査し、所定の範囲内に入っていないものについては再度撮影を行うために、登録ボタンのタップを促す。あわせて、当該生データを含む複数の生データは、PAD 特徴抽出機能に送られ、生データから、機械学習による偽造生体判定スコアを計算し PAD 特徴データとして抽出する。特徴データの情報量が所定の範囲に入っており、PAD 特徴データから偽造生体で無いと判定された場合に、撮影生データを画面へ表示し、ユーザの目視による適正位置の確認を行なう。ユーザの目視により適正な画像と判断された後、該特徴データを登録生体情報とする。TOE は、前記登録対象ユーザに対し、手のひらをデータ採取機能に提示し、撮影生データをユーザが目視で確認する操作を、登録生体情報取得が 3 回成功するまで、最大 15 回要求する。
登録生体情報取得が 3 回成功した場合、登録生体情報として、ID と対応付ける。併せて、認証時に使用する位置品質検査のために掌紋データを抽出して、登録生体情報と共に格納機能に保存する。
最大 15 回の登録生体情報取得のうちに、3 回の登録生体情報取得が成功出来なかった場合は登録できず、再度、最大 15 回の登録生体情報取得を要求する。最大 15 回の登録生体情報取得を 3 回繰り返しても登録出来ない場合は､アプリケーションへ登録失敗を出力する。
検査機能が生データが十分な品質でないと判断した場合には特徴データの抽出は行わず登録も行わないこと、および PAD 特徴データによる生体と偽造生体の判定により偽造生体がデータ採取機能に提示されたと判断された場合には登録を失敗とすることで、FIA_EBT.1 を満足する。
一方、FIA_EBT1 が要求する、品質の低いデータや偽造生体が提示されたデータでなければ排除されないことや、前記登録の一連の試行において、登録の失敗は２回まで許容することから、低い登録失敗率を実現しており、アジアを中心とした国内外を想定した人口統計に基づいた被験者による性能評価試験において、FTE 実測値 0.13%、95%信頼区間の上限 0.38%であった。ISO19795 では 95%信頼区間の上限値を採用することを求めることから、TOE は登録失敗率 FTE0.4%を宣言値とすることにより、FIA_EBT.2 を満足する。

バイオメトリック照合は、ユーザが提示した身体的特徴が登録生体情報と同一のユーザのものであるかを判定する TOE の主機能である。
登録ユーザは ID 取得機能に ID を提示する。なお、TOE を含むアプリケーションが、個人が所有するモバイルデバイス上で動作する場合には、ユーザは ID を提示せずに、アプリケーションが定める ID が指定される。提示された ID に対応する登録生体情報は、登録生体情報取得機能により格納機能から取得される。
登録ユーザは手のひらをデータ採取機能に提示し、データ採取機能で生データを取得する。得られた生データは、検査機能により手のひらの有無及び品質判定を機械学習した判定器

により、品質判定スコアを計算し、品質が検査される。その結果、手のひらが提示されていない状態、位置が適正でない状態、手のひらとはかけ離れた、色成分や輪郭、テクスチャを持つ提示物は、品質が十分でないと判定する。
認証当該生データが十分な品質であると判定された場合は、さらに掌紋データとの類似度判定に基づく位置品質の検査を行う。十分な位置品質であると判定された場合は、データ採取機能から生データが特徴抽出機能に送られ、特徴抽出機能よって生データから特徴データを抽出する。
比較機能は、特徴抽出機能が特徴抽出した特徴データと格納機能から取り出された登録生体情報とを比較し、両者の類似度を算出する。特徴データと登録生体情報とを比較した類似度がある閾値を超えた場合、さらに当該生データを含む複数の生データが PAD 特徴抽出機能に送られ、偽造生体を機械学習した判定器により、偽造生体判定スコアを PAD 特徴データとして抽出する。
本 TOE では、検査機能により十分な品質が確認されたのち、生データは随時特徴抽出機能に送られ、特徴抽出機能は随時特徴データを生成し、比較機能に送られる。比較機能は、随時、登録生体情報と特徴データを比較し、類似度のスコアを算出することを繰り返す。
決定機能は、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にあって、PAD 特徴データが、偽造生体がデータ採取機能に提示された特徴を持たないことを判定した場合にのみ、照合成功とする。前記、データ採集から特徴抽出までの一連の処理は、照合成功、もしくは一定時間までに照合が成功しない場合に照合失敗とするまで、繰り返される。内部的に適切な閾値を設定することによって、高いセキュリティ性能を実現しており、アジアを中心とした国内外を想定した人口統計に基づいた被験者による性能評価試験において、FRR 実測値 0.065%、FAR 実測値 0.000294%であった。ISO19795 では 95%信頼区間の上限値を採用することを求めることから、前記 FRR の実測値から算出した 95%信頼区間の上限は 0.192%、FAR の 95%信頼区間の上限は 0.000513%であった。本 TOE では誤拒否率 FRR0.2%、誤受入率 FAR0.0006%を宣言値とすることにより、FIA_BVR.1 を満足する。
また、検査機能が生データが十分な品質でないと判断した場合には特徴データの抽出は行わず照合も行わないこと、および PAD 特徴データによる生体と偽造生体の判定により偽造生体がデータ採取機能に提示されたと判断された場合には登録を失敗とすることで、FIA_BVR.4 を満足する。
生体情報登録時、生体情報と特徴データの照合時および登録生体情報の削除時において生成される、データ採取機能（カメラ）から取得した生データ、生データから抽出した特徴データ、格納機能より取得した登録生体情報、生データから抽出した PAD 特徴データ、生体特徴類似度計算、偽造物判定計算、生体情報品質判定計算の結果及び用いたパラメータを、それぞれの処理が完了した時点で、それぞれに対応するメモリ領域を一旦乱数データで書き換えた後にゼロクリアして開放することにより、FDP_RIP.1 を満足する。

Application Note:
信頼区間は、サポート文書ではなく ISO/IEC19795-1 Appendix B3,B4 に従って算出した。また、本 TOE は、テンプレートとバイオメトリック・データとでは、トランザクションの構成やデータの品質を検査する項目、また画像からデータを抽出する範囲やデータ数が異なるので、テンプレートとバイオメトリック・データを入れ替えた場合の照合結果は一致しない。よって、FAR の実測値は、計算式の分子を「受入が発生した偽者トランザクション総数」、計算式の分母を「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」として算出した。

8. 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 ST 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	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
登録実行指示	アプリケーションが TOE に対し行う実行指示であり、これにより登録処理が開始される。
登録生体情報削除	すでに登録されている登録生体情報の削除処理を行うこと。アプリケーションが TOE に対し行う指示により、処理が実行される。
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。TOE のインストールに至るアプリケーション開発も TOE のインストールに含めて考え、アプリケーション開発者も BS 管理者（アプリケーション開発の BS 管理者）と呼ぶ。アプリケーション開発より後のインストール、設定、及び運用に当たる管

用語	意味
	理者を運用を含む BS 管理者と呼ぶ。
バイオメトリック照合	ユーザが提示した身体的特徴から得られる特徴データと登録生体情報とを比較して同一のユーザのものであるかを判定するアプリケーション。複数の特徴データを用いて、複数回の比較をして判定をすることもある。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの処理が実施される。
ユーザ	TOE に身体的特徴を提示し、登録及び照合される人間。本 ST では利用者とも呼んでいる。
利用者認証	システムや資産にアクセス許可される前に、ID を主張するユーザがその ID に対応する本人であることを確認する行為。
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。
品質が低い生体情報	データ採取において、静止しない提示、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を言う。
偽造生体	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である。即ち、掌静脈や手のひら自身が偽造されたものである。