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

1.2. PP 概要

本 PP は、CC の観点から、バイオメトリック照合製品に固有のセキュリティ機能要件及び保証要件を定める。バイオメトリック照合製品に固有のセキュリティ機能要件とは、パスワードや PKI などによる利用者認証製品にはない、誤受入及び誤拒否のエラーに対する要件、偽造生体検知に対する要件等である。従って、本 PP においては、誤受入及び偽造生体検知に関係しない脅威は、取り扱わない。
本 PP は、TOE が使用する身体的特徴（顔、指紋、虹彩、静脈など）と対応する身体部分（静脈の場合は、指、てのひら、手の甲など）を特定しない。

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

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

1.3. TOE 概要

1.3.1. TOE の種別

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

1.3.2. TOE が利用できる TOE 以外のハードウェア/ソフトウェア/ファームウェア

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

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

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

1.3.3. TOE の使用法

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

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

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

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

は、生データが登録生体情報として格納機能に保存される場合もある。

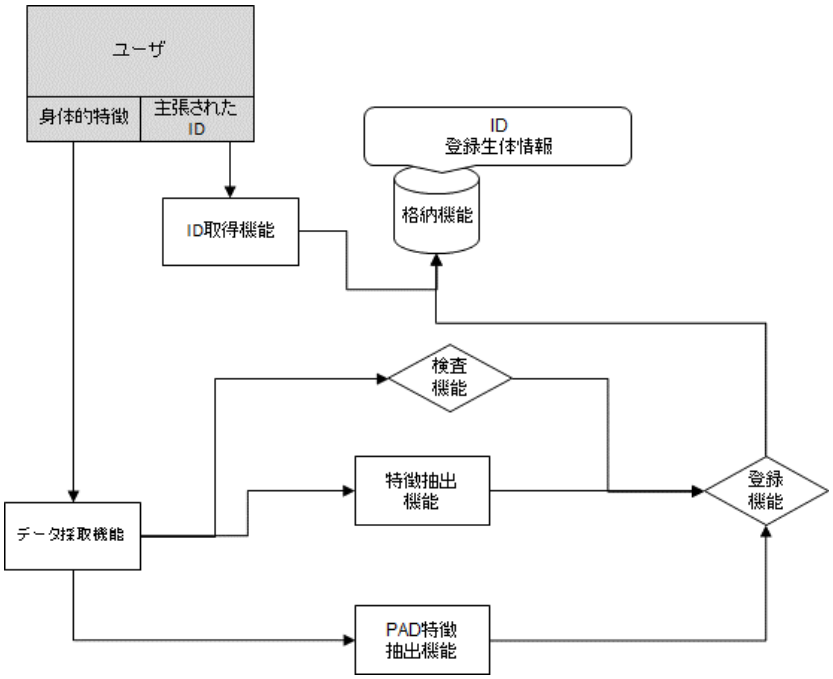


図 1 登録の処理

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

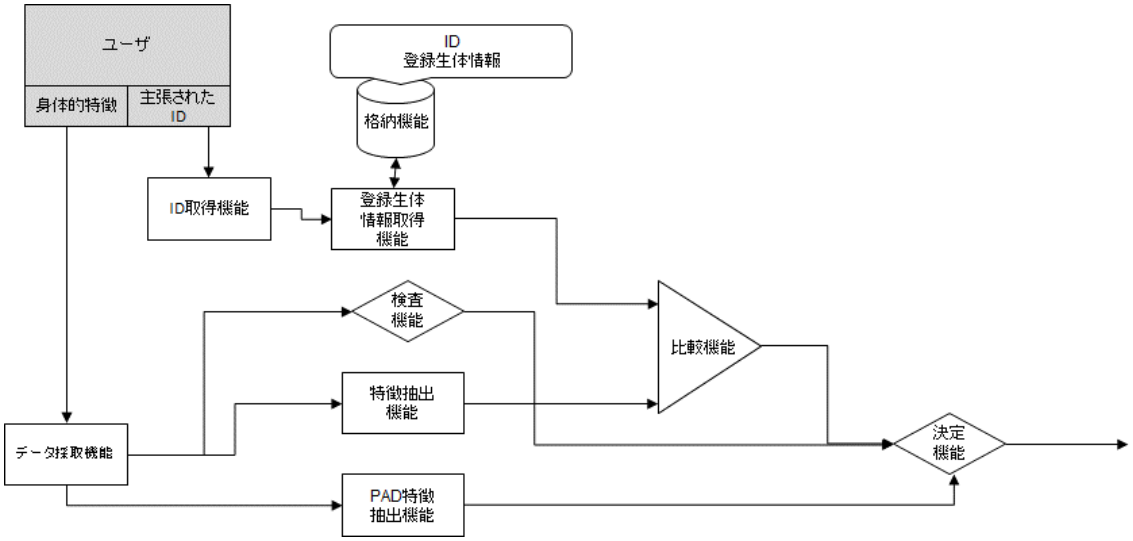


図 2 バイオメトリック照合の処理

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

1.3.4. TOE の主要なセキュリティ機能

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

1.3.4.1. バイオメトリック照合の特性

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

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

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

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

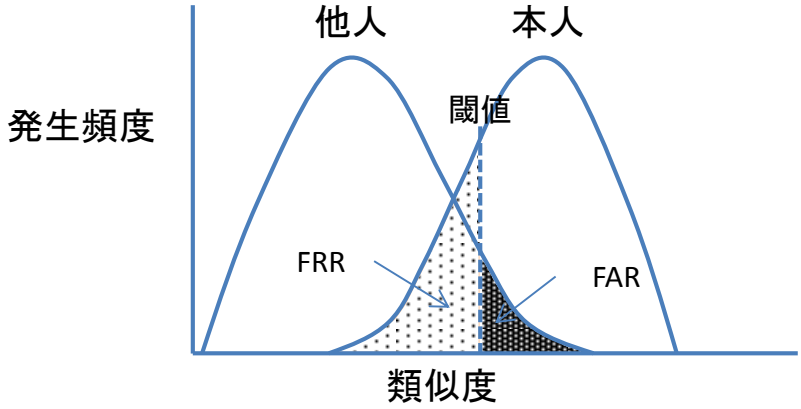


図 3 バイオメトリック照合の類似度分布

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

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

(2)偽造生体や品質の低い生体情報を用いた攻撃

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

1.3.4.2. TOE に対する攻撃手法と攻撃能力の想定

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

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

1.3.5. TOE の構成

TOE の構成は、以下のふたつである。本 PP は、いずれにも適用できる。

- 統合型：TOE の構成要素が物理的に分離していない。すなわち、TOE の構成要素が USB ケーブルやネットワークで接続されていることはない。
- 分離型：TOE の構成要素が物理的に分離している。すなわち、TOE の構成要素が USB ケーブルやネットワークで接続されている。

  適用上の注釈：

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

1.3.6. TOE の使用が想定される環境

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

1.3.7. TOE の機能

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

太枠は、TOE の範囲を表す。

太枠内の実線四角（特徴抽出機能など）は、TOE が含む機能を表す。

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

太枠外の実線四角は、TOE の運用環境で提供される機能を表す。

影の付いた実線四角は、ユーザを表す。

なお、以下は、典型例であり、TOE によっては異なる処理を行う場合がある。

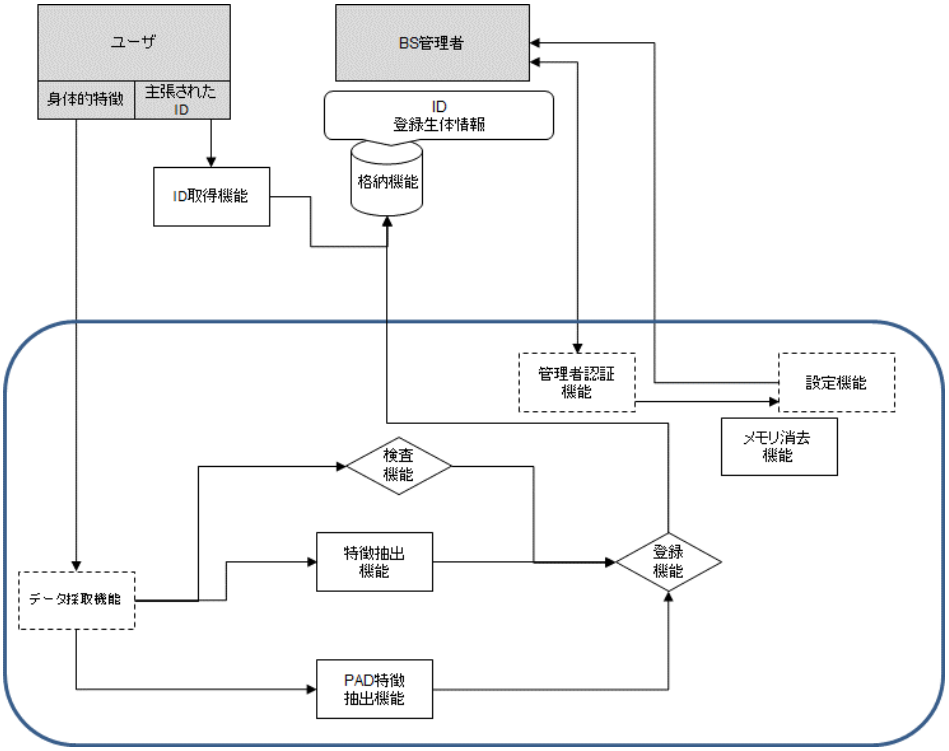


図 4　一般的な TOE の構成（登録の場合）

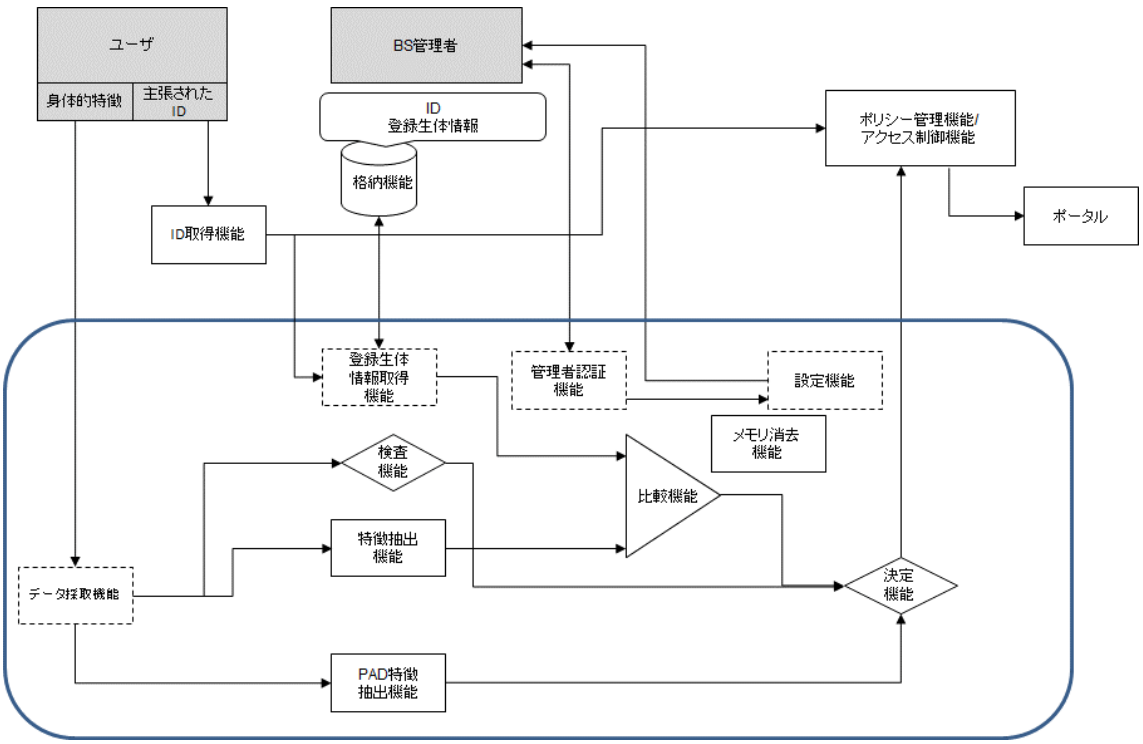


図 5 一般的な TOE の構成（照合の場合）

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

- 特徴抽出機能：登録や照合の前段階として、採取された生データから特徴が抽出される。これが、本機能の役割である。抽出されたデータは圧縮される場合もある。抽出されたデータを特徴データと呼ぶ。
- 検査機能：この機能は、データ採取機能から得られた生データが以後の処理のために十分な品質を持っているかを検査する。
- 登録機能：この機能は、検査機能によって登録に十分な品質を持つと判断され、PAD 特徴抽出機能からの PAD 特徴データを基に偽造生体などを使った攻撃でないと判断できる場合に、特徴抽出機能から得られた特徴データを登録生体情報として出力する。条件を満たさない場合は、登録生体情報となる特徴データを出力しない。なお、PAD（Presentation Attack Detection）とは、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、ユーザから生データを採取し、特徴抽出機能や検査機能に生データを送る役割を担う。
- 登録生体情報取得機能：この機能は、ユーザの ID に対応する既に登録された登録生体情報を取得する。
- 管理者認証機能：この機能は、BS の管理者に対する識別・認証を担う。この手段の例としては、スマートカードと PIN が挙げられる。BS 管理者は、認証された後に、TOE のセキュリティ関連設定を許可される。
- 設定機能：この機能は、BS 管理者に TOE のセキュリティに関連するパラメータの設定をするためのインタフェースを提供する。この機能は、TOE によっては、決定機能のための閾値設定に使われる。

TOE の運用環境にもセキュリティに関連する機能やインタフェースがある。

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

2. 適合主張

2.1. CC 適合主張

本 PP は、CC バージョン 3.1 改訂第 4 版（日本語版）適合を主張する。
本 PP は、CC パート 2 拡張を主張する。拡張するセキュリティ機能コンポーネントを第 5 章に定義する。
本 PP は、CC パート 3 適合を主張する。

2.2. PP 主張

本 PP は、他の PP に適合していない。

2.3. パッケージ主張

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

2.4. 適合ステートメント

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

3. セキュリティ課題定義

3.1. TOE に関連するエンティティ

以下の外部エンティティは、TOE に作用を及ぼす。

BS 管理者：

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

登録ユーザ：

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

攻撃者：

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

3.2. 資産

本 PP では、以下の資産を定義する。

1 次資産：

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

2 次資産：

TOE が生成するデータ及び BS 管理者が作成する TOE 内のデータ。

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

3.3. 前提条件

A.ADMINISTRATION

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

適用上の注釈：

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

A.PROTECT_ASSETS

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

適用上の注釈：

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

A.COMMUNICATION

運用環境のバイオメトリクスの処理に関わる機能と TOE との間の通信、TOE の構成要素が物理的に分離している場合は TOE の構成要素間の通信は、保護されている。

A.ENVIRONMENT

TOE が正しく動作可能になるためのセキュアな運用環境が提供されている。

適用上の注釈：

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

3.4. 脅威

T.CASUAL_ATTACK

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

T.PRESENTATION_ATTACK

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

3.5. 組織のセキュリティ方針

P.ENROL_ADMINISTERED

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

P.RESIDUAL

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

P.CONTROL_FALSE_REJECT

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

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.PAD_ENROL

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

O.CLEAR_RESIDUAL

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

O.CONTROL_FALSE_ACCEPT

TOE は、誤受入率(FAR)に対する基準を満たさなければならない。

O.PAD_VERIFY

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

O.CONTROL_FALSE_REJECT

TOE は、誤拒否率(FRR) に対する基準を満たさなければならない。

4.2. 運用環境のセキュリティ対策方針

OE.ENROL_ADMINISTERED

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

OE.PROTECT_RESIDUAL_ENVIRONMENT

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

OE.ACCESS_CONTROL

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

OE.LIMIT_NUM_TRIAL

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

OE.ADMINISTRATION

BS 管理者は、悪意を持たない者でなければならない。すなわち、攻撃者になったり、攻撃者に情報提供してはならない。BS 管理者は、TOE のインストール（ハードウェアがある場合はその設置を含む)、設定、運用の責任を持ち、実行しなければならない。

OE.PROTECT_ASSETS

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

OE.COMMUNICATION

BS 管理者は、運用環境のバイオメトリクスの処理に関わる機能と TOE との間の通信、TOE の構成要素が物理的に分離している場合は TOE の構成要素間の通信がセキュアな通信となる運用環境を提供しなければならない。

OE.ENVIRONMENT

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

4.3. セキュリティ対策方針根拠

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

表 1　セキュリティ対策方針根拠

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

4.3.1.　脅威への対抗

T.CASUAL_ATTACK

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

T.PRESENTATION_ATTACK

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

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

4.3.2. 組織のセキュリティ方針の実現

P. ENROL_ADMINISTERED

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

P.RESIDUAL

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

P.CONTROL_FALSE_REJECT

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

(FRR)を持つことで、実現される。

4.3.3. 前提条件への対応

A.ADMINISTRATION

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

A.PROTECT_ASSETS

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

A.COMMUNICATION

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

A.ENVIRONMENT

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

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

5. 拡張コンポーネント定義

クラス FIA（識別と認証）の拡張された機能ファミリ FIA_EBT（Enrolment of Biometric Template）及び FIA_BVR （Biometric VeRification）は、この PP の対象となる TOE のバイオメトリック照合の機能を記述するために定義される。TOE は、ポータルへのアクセスのために、バイオメトリック照合を提供しなければならない。CC パート 2 のクラス FIA（識別と認証）で定義された利用者認証とバイオメトリック照合には差異があるため、クラス FIA への拡張を選択した。

5.1. 生体情報の登録 FIA_EBT

ファミリのふるまい

このファミリは、TSF がサポートするバイオメトリック照合のための生体情報の登録のメカニズムを定義する。このファミリは、生体情報の登録のメカニズムが基づかねばならない、要求された属性も定義する。

コンポーネントのラベル付け

FIA_EBT.1　登録時の生体情報の検査は、偽造生体や品質の低い生体情報の使用を防止できることを要求する。

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

管理: FIA_EBT.1

以下のアクションは FMT における管理機能と考えられる:

管理者による TSF データ(登録時の生体情報の検査のための設定値)の管理

管理者による TSF データ(偽造生体検知のための設定値)の管理

管理: FIA_EBT.2

以下のアクションは FMT における管理機能と考えられる:

管理者による TSF データ(登録時の生体情報の検査のための設定値)の管理

監査: FIA_EBT.1

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

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

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

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

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

FIA_EBT.2 生体情報登録失敗率の低い生体情報登録
下位階層: なし

依存性: なし

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

適用上の注釈：

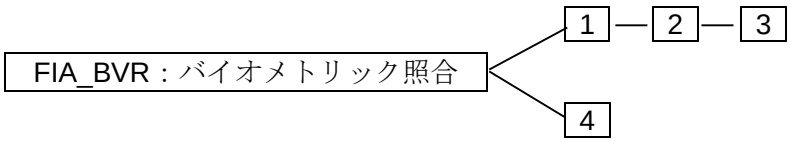
FTE の定義は、TOE の登録ポリシーに依存する。ST 作成者はそのポリシー概略を示さなければならない。

5.2.　バイオメトリック照合 FIA_BVR

ファミリのふるまい

このファミリは、TSF がサポートするバイオメトリック照合のメカニズムを定義する。このファミリは、バイオメトリック照合のメカニズムが基づかねばならない、要求された属性も定義する。

コンポーネントのラベル付け



FIA_BVR.1 精度の高いバイオメトリック照合は、TSF が利用者のバイオメトリック照合の誤受入及び誤拒否がそれぞれ一定の割合以下であることを要求する。

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

FIA_BVR.3 アクション前のバイオメトリック照合による利用者認証は、TSF がその他のアクションを許可する前に、バイオメトリック照合による利用者認証を要求する。

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

管理: FIA_BVR.1

以下のアクションは FMT における管理機能と考えられる:

管理者による TSF データ(閾値を含む)の管理

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

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

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

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

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

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

監査: FIA_BVR.4
セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:

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

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

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

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

FIA_BVR.2.1 TSF は、利用者がバイオメトリック照合による利用者認証をされる前に利用者を代行して行われる[割付: *TSF 仲介アクションのリスト*]を許可しなければならない。

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

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

FIA_BVR.4 偽造生体等を受け入れないバイオメトリック照合

下位階層: なし
依存性: FIA_EBT.1　登録時の生体情報の検査

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

適用上の注釈：

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

FIA_BVR.4.2

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

適用上の注釈：

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

5.3.　機能ファミリ FIA_EBT 及び FIA_BVR 定義の理由

FIA_UAU が定義する利用者認証は、認証データが正しければ、認証は必ず成功しなければならない。これに対し、バイオメトリック照合の場合は、FAR の存在が示すように、利用者の生体情報が提示された場合でも失敗する可能性がある。FIA_UAU では認証データの偽造とコピーが別に扱われているが、バイオメトリック照合では両者は明確に区別できない。また、バイオメトリック照合による利用者認証の場合は FIA_UAU と同様に利用者の ID を与えるが、バイオメトリック照合だけの場合は、利用者の ID は与えられず、照合時に得られ認証データに相当する特徴データと登録生体情報を比較するのみであるという差異がある。上記のとおり、クラス FIA にバイオメトリック照合を適切に表現するファミリがなかったので、新しいファミリ FIA_BVR を定義した。

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

6. セキュリティ要件

6.1. セキュリティ機能要件

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

表 2 セキュリティ機能要件

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

操作内容は、各 SFR において以下の表記方法で示される。

・繰返し操作は、SFR 名称の後ろにカッコ付きで区別のための情報を示し、さらに短縮名に(1)、(2)のように番号を付けて示す。
・割付は [割付：*XXX*]のように斜体で示す。
・選択は [選択：*XXX*] のように斜体で示す。選択対象外の項目は、~~抹消線~~で示す。
・詳細化は、詳細化を施した部分を下線で示す。
本 PP では、一部操作が未了であり、その個所をマーカーで示す。ST 作者は、未了部分の操作を完了させなければならない。

FDP_RIP.1サブセット残存情報保護
下位階層: なし
依存性: なし

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

適用上の注釈：
ST 作者は、割当て解除するオブジェクトを全て割り付けよ。

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

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

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

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

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

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

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

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

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

適用上の注釈：

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

FIA_BVR.4.2

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

適用上の注釈：

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

6.2. セキュリティ保証要件

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

表 3　セキュリティ保証要件

保証クラス	保証コンポーネント
開発	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.1

セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
テスト	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.2

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

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

6.3.1.1. セキュリティ対策方針とセキュリティ機能要件の対応

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

表 4　セキュリティ対策方針とセキュリティ機能要件の対応

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

以下に対応の詳細を記述する。

O.PAD_ENROL

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

O.CLEAR_RESIDUAL

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

O.CONTROL_FALSE_ACCEPT

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

O.PAD_VERIFY

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

O.CONTROL_FALSE_REJECT

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

6.3.1.2. セキュリティ機能要件の依存性

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

表 5　SFR の依存性対応

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

6.3.2. セキュリティ保証要件根拠

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

6.3.2.1. セキュリティ保証要件の依存性

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

7. 用語集

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

用語	意味
BS	Biometric System（バイオメトリックシステム）
CC（Common Criteria）	Common Criteria - Common Criteria for Information Technology Security Evaluation. コモンクライテリア（情報セキュリティ評価のためのコモンクライテリア）
EAL	Evaluation Assurance Level（評価保証レベル）
FAR	False Accept Rate（誤受入率。他人の身元確認要求の照合トランザクションにおいて、誤って受理する率）
FRR	False Reject Rate（誤拒否率。本人の身元確認要求の照合トランザクションにおいて、誤って拒否する率）
FTE	Failure To Enrol（生体情報登録失敗率。ある集団に対して登録処理を行った場合に、システムが登録処理を完了できなかった人数の割合）
OS	Operating System（オペレーティングシステム）
PAD	Presentation Attack Detection (提示型攻撃の検知。BS の操作を妨害することを目的としたデータ採取機能へのデータの提示の検知。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

用語	意味
	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
特徴データ	生データから抽出した身体的特徴を表すデータ
生データ	データ採取機能によって得られるデータ
バイオメトリクス	人間の身体的特徴や行動的特徴に基づいて個人を自動的に認識する技術
バイオメトリック	バイオメトリクスの、バイオメトリクスを使った
バイオメトリック識別	与えられた特徴データに対して、格納された登録生体情報を検索して一致すると考えられる候補（複数の場合やない場合も含む）を返すアプリケーション。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの処理が実施される。
バイオメトリックシステム（BS）	バイオメトリック照合のメカニズムを含むシステムのうち最小のシステム
バイオメトリックシステム管理者（BS 管理者）	TOE のインストール（ハードウェアがある場合はその設置を含む）、設定、及び運用の責任を持つ管理者。TOE が管理機能を持つ場合は、TOE を含む BS の管理的操作の実行権限があり、TOE を含む BS の管理的機能を使用することができる管理者。
バイオメトリック照合	ユーザが提示した身体的特徴から得られる特徴データと登録生体情報とを比較して同一のユーザのものであるかを判定するアプリケーション。複数の特徴データを用いて、複数回の比較をして判定をすることもある。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報は、特徴抽出された後、特徴データとの処理が実施される。
ユーザ	TOE に身体的特徴を提示し、登録及び照合される人間。本 PP では利用者とも呼んでいる。
利用者認証	システムや資産にアクセス許可される前に、ID を主張するユーザがその ID に対応する本人であることを確認する行為

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