CRP-C0501-01

認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田 達夫

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	平成27年1月6日 (IT認証5529)
認証番号	C0501
認証申請者	国立研究開発法人　産業技術総合研究所
PPの名称	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
PPのバージョン	第1.2版
PP適合	他のPPへの適合主張なし
適合する保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.1
開発者	国立研究開発法人　産業技術総合研究所
評価機関の名称	みずほ情報総研株式会社　情報セキュリティ評価室

上記のPPについての評価は、以下のとおりであることを認証したので報告します。

平成28年3月31日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　近藤　潤一

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「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」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1　全体要約 1
1.1　評価PP 1
1.1.1　保証パッケージ 1
1.1.2　PP概要 1
1.1.3　セキュリティ機能概要 5
1.1.3.1　脅威とセキュリティ目標 6
1.1.4　認証に際しての免責事項 6
1.2　評価の実施 7
1.3　評価の認証 7
2　PP識別 8
3　セキュリティ方針 9
3.1　セキュリティ機能方針 9
3.1.1　脅威とセキュリティ機能方針 9
3.1.1.1　脅威 9
3.1.1.2　脅威に対するセキュリティ機能 9
3.1.2　組織のセキュリティ方針とセキュリティ機能 10
3.1.2.1　組織のセキュリティ方針 10
3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能と運用環境 11
4　前提条件と評価範囲の明確化 12
4.1　使用及び環境に関する前提条件 12
5　評価機関による評価実施及び結果 13
5.1　評価機関 13
5.2　評価方法 13
5.3　評価実施概要 13
5.4　評価結果 14
5.5　評価者コメント/勧告 15
6　認証実施 16
6.1　認証結果 16
6.2　注意事項 16
7　附属書 16
8　用語 17
8.1　CCに関する略語 17
8.2　本認証報告書で使用された用語及び略語 17
9　参照 19

1 全体要約

この認証報告書は、国立研究開発法人　産業技術総合研究所が開発した「バイオメトリック照合製品プロテクションプロファイル、バージョン　第 1.2 版」（以下「PP[12]」という。）についてみずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が平成 28 年 3 月 23 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である国立研究開発法人　産業技術総合研究所に報告するとともに、PP[12]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応する PP[12]を併読されたい。特に PP[12]に適合する TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、PP[12]において詳述されている。

本認証報告書は、PP[12]に適合したバイオメトリック照合製品を開発・納入する開発者及び適合したバイオメトリック照合製品の調達者を読者と想定している。本認証報告書は、PP[12]が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

本認証報告書で使用する用語については、8 章を参照されたい。

1.1 評価PP

PP[12]が要求するセキュリティ機能の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

PP[12]において要求される保証パッケージは、EAL2 追加である。追加の保証コンポーネントは、ALC_FLR.1 である。

また、PP[12]への適合を主張する PP、及び ST は正確適合を主張しなければならない。

1.1.2 PP概要

PP[12]は、オフィスでの PC のログインによる利用者認証、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に求められるセキュリティ要件を規定する。

TOE は、利用者認証のためのバイオメトリック照合、及びそのための利用者登録を実施する。バイオメトリック照合とは、ユーザが提示した身体的特徴（顔、指紋、虹彩、静脈など）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処理を指す。PP[12]は、照合する身体的特徴と対応す

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。また、バイオメトリック識別も対象としない。

以下に一般的な TOE の構成を、登録（図 1-1）とバイオメトリック照合（図 1-2）に分けて各々示す。下図の太枠は TOE の範囲を表し、太枠内の実線四角（特徴抽出機能など）は、TOE が含む機能を示す。太枠内の破線四角（データ採取機能など）は、PP[12]では提供されないとしているが TOE が含んでよい機能である。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。

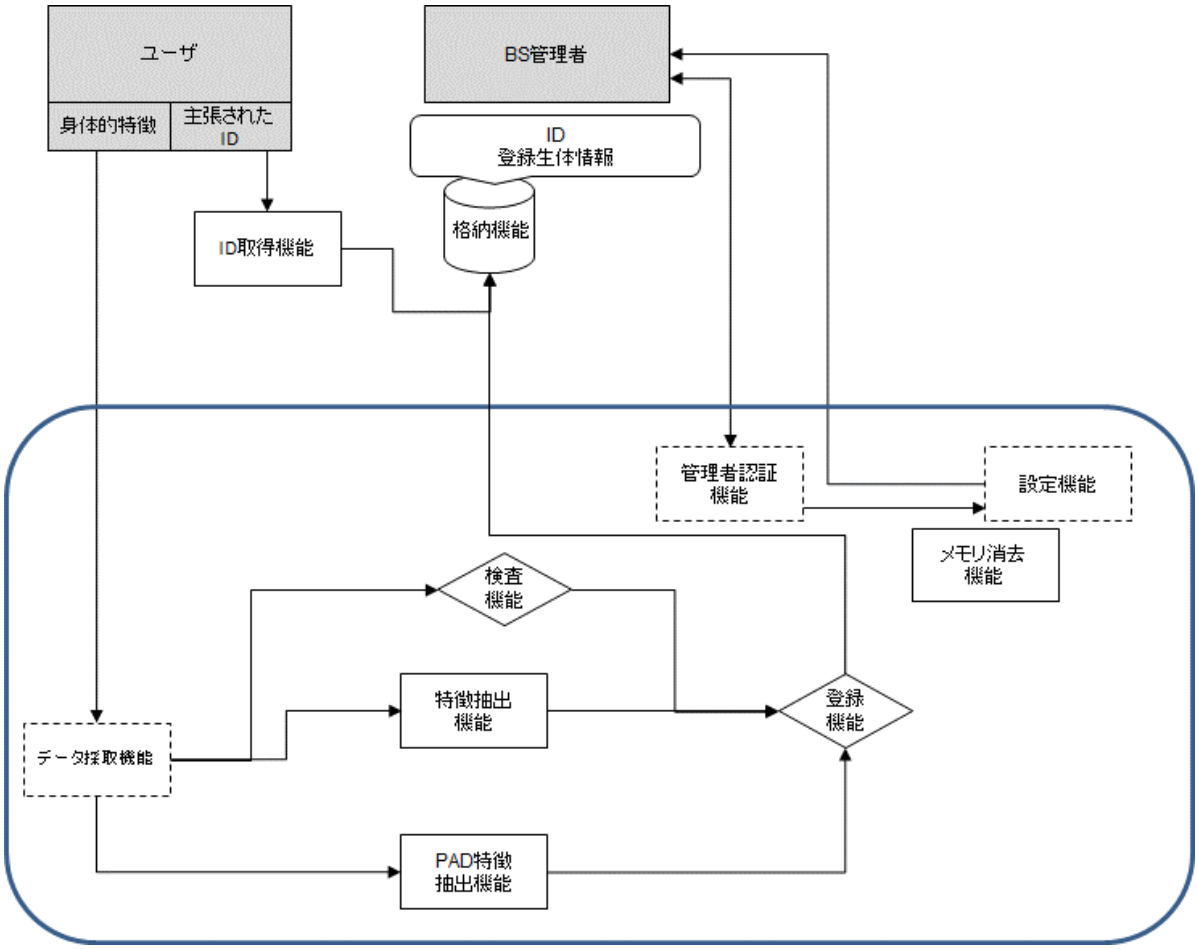

図 1-1 一般的なTOEの構成（登録の場合）

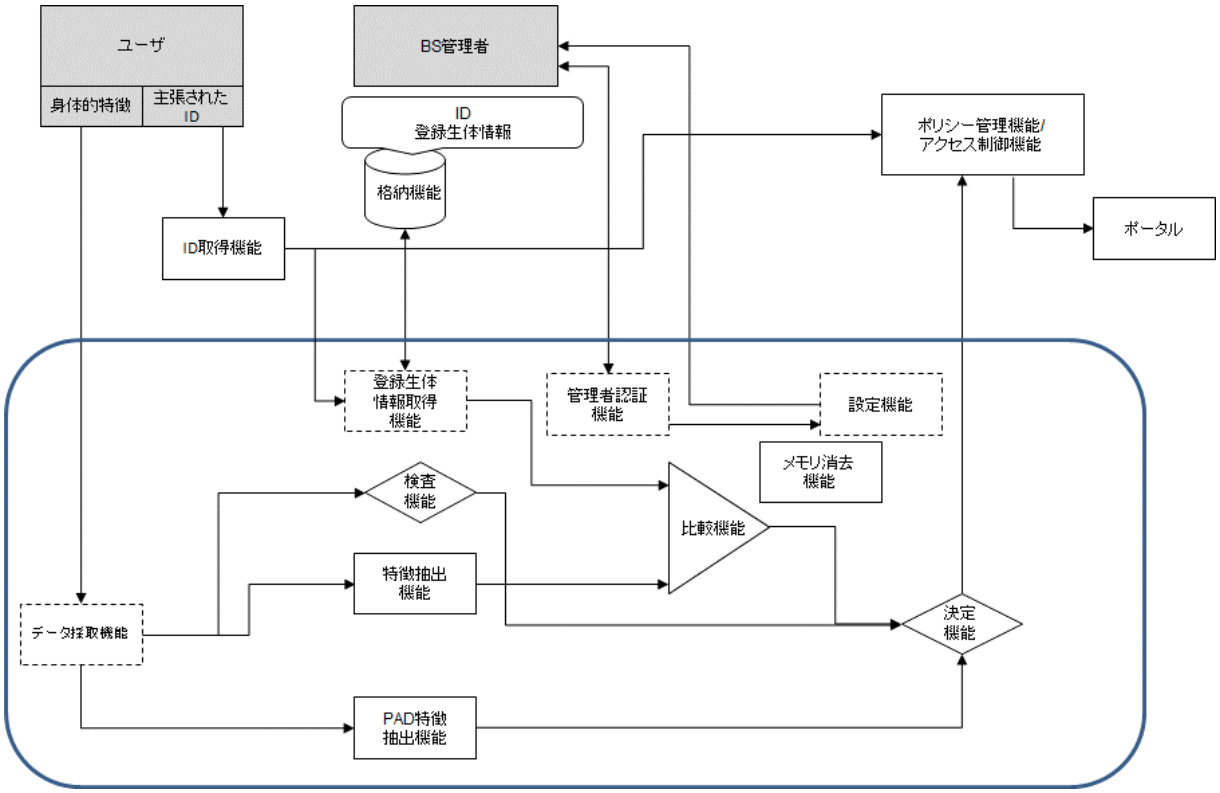

図 1-2 一般的なTOEの構成（照合の場合）

図 1-1、図 1-2 に示された各機能に関し、以下に説明する。

[TOE が含む機能]

以下は PP[12]で要求される機能であり、対応するセキュリティ機能要件が定義されている。各機能の内容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検知することを指す。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。

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

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

[TOE が提供可能な機能]

PP[12]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、バイオメトリックシステム（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 の運用環境により提供される機能等]

以下は、TOE の運用環境のセキュリティに関連する機能やインタフェースである。

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

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

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

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

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

1.1.3 セキュリティ機能概要

PP[12]では、バイオメトリック照合製品に求められる、以下のセキュリティ機能を規定する。その主要なものを以下に示す。

(1) 一定の基準を満たすバイオメトリック照合

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。この基準は、PP[12]に準拠する ST を作成する ST 作成者により指定される。また、誤拒否率（FRR）及び生体情報登録失敗率（FTE）は FAR とトレードオフの関係にあるため、この FRR と FTE もある一定の基準を満たす必要がある。それらの値も ST 作成者により指定される。

(2) 偽造生体及び品質の低い生体情報による登録・照合の防止

TOE は、品質の低い生体情報及び偽造生体による登録・照合を防止する必要がある。品質の低い生体情報とは、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。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。

1.1.3.1 脅威とセキュリティ目標[1]

PP[12]に適合する TOE は、前述したセキュリティ機能により以下の脅威に対抗する。

攻撃者は、自分の身体的特徴を使用し別の登録ユーザとしてバイオメトリック照合を試みるかもしれない。前述したように、他人なのに本人と誤認識され照合が成功する率を FAR と呼ぶが、TOE は一定の FAR 以下で照合を実施し、このような脅威を低減しなければならない。FRR や FTE も同様に一定の値以下に保つことは、この脅威から派生する要件として PP[12]に定義されている。

攻撃者は、意図的に身体部分を不適切に提示し品質の低い生体情報を登録することにより、他人として照合されることを成功させようとするかもしれない。また、同様の意図に基づき他人の身体的特徴を模して作成された偽造生体を登録しようとするかもしれない。TOE はそのような品質の低い生体情報や偽造生体の登録を防止しなければならない。また、照合の際にも同様の攻撃が想定されるため、TOE は品質の低い生体情報や偽造生体による照合を防止しなければならない。

1.1.4 認証に際しての免責事項

PP[12]は、TOE がある一定の精度（FAR、FRR、FTE）に関する基準を満たすことを求めており、FAR、FRR、FTE がゼロになることを求めているわけではなく、ST 作成者が指定した値以下になることを求めている。また PP[12]は、FAR、FRR、FTE はある特定の環境（例えば屋内・屋外など）で測定され評価されることを想定しており、全ての環境で評価されることを求めているわけではない。どのような環境で測定され評価されたのかに関しては、PP[12]に準拠した TOE 評価時に確認され、認証報告書に記載される。従って PP[12]に準拠し認証取得した TOE を購入する利用者は、認証報告書に記載された評価環境と自らの運用環境が異なる場合は、認証報告書に記載された精度が達成されない可能性があることに留意すべきである。

PP[12]は、品質の低い生体情報や偽造生体による登録や照合を防止することを求めているが、「品質の低い生体情報」や「偽造生体」そのものの正確な定義はして

---

[1] CC Part 1 [4]で定義されている"security objective"の訳語として、日本語翻訳版[7]では「セキュリティ対策方針」を割り当てているが、本認証報告書の中では、"security objective"の訳語として、「セキュリティ目標」を用いることとする。

いない。それは、PP[12]は照合する身体的特徴と対応する身体部分を特定していないため、「品質の低い生体情報」や「偽造生体」の定義が TOE により異なる可能性を考慮しているためである。従って「品質の低い生体情報」や「偽造生体」は TOE 評価時に定義され、その定義に従い TOE 評価が実施される。TOE 評価の認証報告書には、どのような「品質の低い生体情報」や「偽造生体」で TOE が評価されたのか記載されるが、利用者は、当該評価で使用されていない「品質の低い生体情報」や「偽造生体」が攻撃に利用された場合、その評価結果が適用できない可能性があることに留意すべきである。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[12]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 3 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書（[13][14]）、所見報告書（[15][16]）、及び関連する評価証拠資料を検証し、PP[12]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、PP の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

PP[12]は、以下のとおり識別される。

PP名称：	バイオメトリック照合製品プロテクションプロファイル
バージョン：	第1.2版
開発者：	国立研究開発法人　産業技術総合研究所

3 セキュリティ方針

本章では、PP[12]に適合する TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

PP[12]が TOE に要求するセキュリティ機能は、大きく次の 2 つである。

- 一定の精度（FAR、FRR、FTE）に関する基準を満たすバイオメトリック照合、
- 品質の低い生体情報、偽造生体を利用した攻撃への対抗

3.1 セキュリティ機能方針

PP[12]では、3.1.1.1 に示す脅威に対抗し、3.1.2.1 に示す組織のセキュリティ方針を満たすセキュリティ機能を規定している。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

PP[12]は、表 3-1 に示す脅威を想定し、これに対抗する機能を TOE に要求する。

表3-1 想定する脅威

識別子	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。

3.1.1.2 脅威に対するセキュリティ機能

PP[12]に適合する TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能で対抗する。

(1) 脅威「T.CASUAL_ATTACK」への対抗

脅威「T.CASUAL_ATTACK」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（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）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。

この脅威に対して、TOE が十分に低い FAR を達成することにより対抗する。また、運用環境が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 1 次資産へのアクセスを許可することを保証し、且つ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をロックするため、この脅威は充分に低減される。

⑵ 脅威「T.PRESENTATION_ATTACK」への対抗

脅威「T.PRESENTATION_ATTACK」は、攻撃者が、別の攻撃者に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。

登録に関する脅威に対しては、TOE が登録時に、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、TOE はそれらの登録を防止することにより対抗する。更に、運用環境が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攻撃と判断して当該ユーザの登録を失敗とするため、この脅威は充分に低減される。照合の脅威に対しては、TOE が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、バイオメトリック照合が成功することを防止させることにより対抗する。また運用環境は、照合が成功しない限り攻撃者の 1 次資産へのアクセスを許可しない、且つ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攻撃と判断して当該ユーザをロックするため、この脅威は充分に低減される。

3.1.2 組織のセキュリティ方針とセキュリティ機能

3.1.2.1 組織のセキュリティ方針

PP[12]に適合する TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

表 3-2　組織のセキュリティ方針

識別子	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。

3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能と運用環境

PP[12]は、表 3-2 の中で以下に示された組織のセキュリティ方針を満たす機能を TOE に要求する。

⑴ 組織のセキュリティ方針「P.RESIDUAL」への対応

本組織のセキュリティ方針は、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、TOE が使用した生体情報及び登録ユーザのその他の情報を、バイオメトリック登録及び照合の処理終了後に削除する機能を実装することにより実現される。

⑵ 組織のセキュリティ方針「P.CONTROL_FALSE_REJECT」への対応

本組織のセキュリティ方針は、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、TOE が運用に支障のない FRR を満たす照合機能を実装することにより実現される。

PP[12]は、表 3-2 の中で以下に示された組織のセキュリティ方針を満たす運用環境を TOE の利用者に要求する。

⑶ 組織のセキュリティ方針「P. ENROL_ADMINISTERED」への対応

本組織のセキュリティ方針は、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。これは運用環境が、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。

(4) 組織のセキュリティ方針「P.RESIDUAL」への対応

本組織のセキュリティ方針は、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。これは上記（1）に加え、運用環境においても一時的に使用した生体情報を必要がなくなった時点で削除することで実現される。

4 前提条件と評価範囲の明確化

本章では、PP[12]に適合する TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

PP[12]に適合する TOE を運用する際の前提条件を**表** 4-1 に示す。これらの前提条件が満たされない場合、PP[12]に適合する TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	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。

識別子	前提条件
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。

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した株式会社 みずほ情報総研株式会社　情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、PP[12]の概要と、CEM のワークユニットごとの評価内容及び判断結果が説明されている。

5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 27 年 1 月に始まり、平成 28 年 3 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

5.4 評価結果

評価者は、PP[12]が CEM のワークユニットすべてを満たしていると判断した。

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、APE_REQ.2

評価では以下について確認された。

表 5-1 評価結果概要

評価結果概要
APE_INT.1　　PP 概説
PP[12]の PP 概説には、PP 識別情報、PP 概要、CC 適合が明確に記述されている。略語、専門用語が付加され一般読者が PP[12]を理解するために十分な情報を与えている。これらの記述内容は、明確であり、矛盾や曖昧な表現はなく、PP[12]その他の部分とも一貫している。よって合格と判定した。
APE_CCL.1　　適合主張
PP[12]の適合主張には、CC 適合主張で許可された用語で PP と TOE が CC に適合する内容が適切に記述されている。これらの記述内容は、明確であり、矛盾や曖昧な表現はなく、PP[12]その他の部分とも一貫している。よって合格と判定した。
APE_SPD.1　　セキュリティ課題定義
PP[12]のセキュリティ課題定義には、脅威、OSP（組織のセキュリティ方針)、前提条件、が記述されている。これらの記述内容は、明確であり、矛盾や曖昧な表現はなく、消費者が十分理解できるレベルである。よって合格と判定した。
APE_OBJ.2　　セキュリティ目標
PP[12]のセキュリティ対策方針には、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針が記述されている。これらの記述内容は、明確で矛盾や曖昧な表現はなく完全であり、根拠の正当化においても一貫している。よって合格と判定した。
APE_ECD.1　　拡張コンポーネント定義
PP[12]は拡張コンポーネントを明確に、曖昧さなく定義しており、当該拡張コンポーネントは既存のコンポーネントを使用して明確に表現できないものである。よって合格と判定した。
APE_REQ.2　　セキュリティ要件
PP[12]のセキュリティ要件は、セキュリティ機能要件(SFR)、SFR とセキュリティ

方針の関係、セキュリティ保証要件(SAR)、セキュリティ要件根拠が記述されている。これらの記述内容は、明確で矛盾や曖昧な表現はなく完全であり、根拠の正当化においても一貫している。よって合格と判定した。

5.5 評価者コメント/勧告

調達者に喚起すべき評価者勧告は特にない。

6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の項目について確認した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの確認において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[12]及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を作成した。

6.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、PP[12]が CC パート 3 の APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及び APE_REQ.2 に対する保証要件を満たすものと判断する。

6.2 注意事項

PP[12]に適合する TOE の評価を行う際には、評価機関は予め適切な評価手法を定め、それに従った評価を実施することが要求される。

7 附属書

特になし。

8 用語

8.1 CCに関する略語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
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）

8.2 本認証報告書で使用された用語及び略語

本報告書で使用された用語の定義及び略語を以下に示す。

BS	Biometric System（バイオメトリックシステム）
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)
攻撃者	権限なくポータルへアクセスすることを目的に、登録時に偽造生体や品質の低い生体情報を意図的に登録することを試みたり、照合時にTOEが正常に動作しないようにすることを試みる人
閾値	特徴データがある登録生体情報に対して一致と判定されるために必要な予め定められた類似や相関の度合い。生データまたは生データの組が登録生体情報として使われる場合は、登録生体情報

	は、特徴抽出された後、特徴データとの一致の判定がなされる。
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
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。

9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

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

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

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

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] バイオメトリック照合製品プロテクションプロファイル, バージョン 第1.2版, 2016年3月23日, 国立研究開発法人　産業技術総合研究所

[13] 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評価報告書 136601-01-R003-07, 2016年3月23日, みずほ情報総研株式会社 情報セキュリティ評価室

[14] 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評価報告書 付属書A 136601-01-R004-07, 2016年3月23日, みずほ情報総研株式会社 情報セキュリ

ティ評価室

[15] 所見報告書 136601-01-R008-01, 2015年1月30日, みずほ情報総研株式会社 情報セキュリティ評価室

[16] 所見報告書 136601-01-R009-01, 2016年1月14日, みずほ情報総研株式会社 情報セキュリティ評価室