認　証　報　告　書

東京都文京区本駒込2丁目28番8号
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

IT製品（TOE）

申請受付日（受付番号）	平成30年11月9日（IT認証8697）
認証識別	JISEC-C0662
製品名称	掌静脈認証ソフトウェア iOS 版
バージョン及びリリース番号	Ver2.00.b10
製品製造者	株式会社ノルミー
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	バイオメトリック照合製品プロテクションプロファイル第1.2版（JISEC認証番号C0501）
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
ITセキュリティ評価機関の名称	みずほ情報総研株式会社情報通信研究部マルチメディア技術チーム情報セキュリティ評価課

上記のTOE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。

令和2年1月9日

セキュリティセンター セキュリティ技術評価部
技術管理者　矢野 達朗

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5
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5
③ Evaluation Guidance for Biometric Verification Products Version 1.0
④ Annex for Evaluation Guidance for Biometric Verification Products Version 1.0

評価結果：合格

「掌静脈認証ソフトウェア iOS 版」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

この認証報告書は、株式会社ノルミーが開発した「**掌静脈認証ソフトウェア iOS 版 Ver2.00.b10**」（以下「本 TOE」という。）について、みずほ情報総研株式会社（以下「評価機関」という。）が令和元年 12 月に完了した 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株式会社ノルミーに報告するとともに、本 TOE 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、10 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 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、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE 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。

1.1 評価対象製品概要

本 TOE の機能、運用条件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 プロテクションプロファイルまたは保証パッケージ

本 TOE は、次のプロテクションプロファイル[16]（以下「適合 PP」という。）に適合する。

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）

本 TOE の保証パッケージは、EAL2 及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

TOE は、背面カメラを備えたスマートフォンや、前面カメラを備えたタブレット等、iOS 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。本 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。

本 TOE は、掌静脈と掌紋を用いて認証を行う機能とそのための登録機能を提供する。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。バイオメトリック照合機能は、その他の認証機能とは異なった特有の機能として、

十分に低い誤受入率・誤拒否率を満たすための機能と、偽造物等を用いた攻撃を防止できる機能がある。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

本 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タなどにアクセスすることを狙って、攻撃者は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しれない。これらを防止するために、本 TOE は背面カメラもしくは前面カメラで撮影された画像データから抽出した特徴データと登録生体情報との類似度が、ある閾値を超えた場合に照合成功とする機能と、偽造生体か否かを判定する機能を有する。

上記の機能によって品質の低い登録生体情報や偽造生体による登録を防止する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 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。

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。このため本 TOE は、モバイルデバイスのカメラで十分な画像が得られないほどの暗い環境に適さない。また本 TOE は、スマートフォンは片手持ち、タブレットは机上やテーブル、スタンド等に置かれた状態で使用される事を想定している。

TOE のインストール､設定及び運用の責任を持つバイオメトリックシステム管理者（以下「BS 管理者」という。）と、TOE を含むバイオメトリックシステムに生体情報を登録し TOE にバイオメトリック認証され利用者登録された登録ユーザによって利用される。

1.1.3 免責事項

「4.2 運用環境と構成」で特定された運用環境以外の TOE の動作は、本評価では保証されない。

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、評価機関によって本 TOE 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、令和元年 12 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]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE 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、TOE の評価が CC（[4][5][6]又は[7][8][9]）及び CEM（[10][11]のいずれか）及びサポート文書（[14][15]）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 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	掌静脈認証ソフトウェア iOS 版
バージョン：	Ver2.00.b10
開発者：	株式会社ノルミー

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

本 TOE を含むバイオメトリック照合製品の場合は、製品が格納されたメディアのラベルによって、その名称とバージョンを確認することができる。

TOE を構成する各ソフトウェアは、メディアに格納されたファイル名と、そのソフトウェアの機能を実行することで表示されるバージョンによって確認することができる。

3 セキュリティ方針

本章では、本 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。

TOE は、利用者の生体情報（掌静脈と掌紋）を用いて認証を行う機能とそのための登録機能を提供するソフトウェアライブラリである。TOE のセキュリティ機能性は、登録された生体情報との類似度照合機能によって十分に低い誤受入率・誤判定率を満たし、誤った利用者認証によるポータルへのアクセスを防止している。また、偽造生体か否かを判定することによって偽造物等を用いた攻撃を防止している。

なお、資産として以下の 2 点を定義する。

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。

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タなど。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 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具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

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に対し自分自身の身体的特徴を提示するかもしれない。登録ユーザのIDを使って1次資産にアクセスすることを狙っている。
T.PRESENTATION_ATTACK	品質の低い登録生体情報になるように、攻撃者は身体的特徴や偽造生体等を提示するかもしれない。誤った受け入れ判定によって1次資産にアクセスすることを狙っている。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.CASUAL_ATTACK」への対抗

十分に低い誤受入率を実現することで、攻撃者のバイオメトリック照合が成功してポータルへのアクセスを運用環境が許可する確率は十分に低い。さらに運用環境は、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これを攻撃と判断して当該ユーザのアカウントをロックすることで本脅威に対抗する。

(2) 脅威「T.PRESENTATION_ATTACK」への対抗

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、TOE はそれらの登録（注）やバイオメトリック照合を防止し、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。さらに運用環境は、生体情報登録の試行回数又は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これを攻撃と判断して登録を失敗としたり、当該ユーザのアカウントをロックすることで本脅威に対抗する。

注）登録の場合、運用を含む BS 管理者が、登録生体情報が掌を模した偽造物から得られたもので無いことを目視で確認する必要がある。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 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が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方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

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

アプリケーション開発の 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な機能を提供しなければならない。さらに 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運用しなければならない。これらによって本対応が実現される。

(2) 組織のセキュリティ方針「P. RESIDUAL」への対応

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る。運用環境が一時的に使用した生体情報があれば、それは必要がなくなった時点で削除される。これらによって本対応が実現される。

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

TOE が運用に支障のない誤拒否率を持つことで実現される。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 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

本 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、本 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無い。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、これを正しく実行する。
A.PROTECT_ASSETS	TOEの2次資産は、改訂、破棄、又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係わる機能と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各種機能は、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。

4.2 運用環境と構成

本 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バイオメトリック照合製品である。TOE は掌静脈と掌紋を用いて認証を行う機能とそのための登録機能を提供する。本 TOE の一般的な運用環境を図 4-1 に示す。

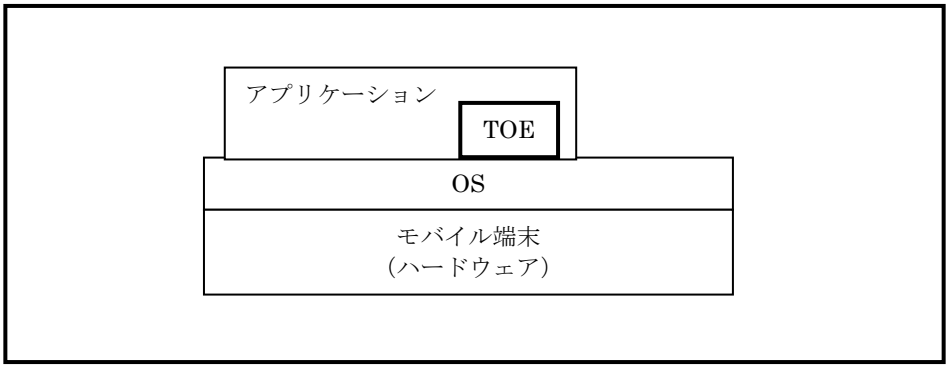

図 4-1 TOEの運用環境

TOE 及び TOE が組み込まれたアプリケーションの動作に必要なハードウェア・ソフトウェアを表 4-2 に示す。

表 4-2　動作に必要なハードウェア・ソフトウェア

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
機能及び仕様	
OS	iOS Version 9.3以降
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 ・カラーイメージセンサー ・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：4.0inch～6.0inch 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

本体	下記に列挙する機能や仕様を具備した タブレット
機能および仕様	
OS	iOS Version 9.3 以降
前面カメラ	◇タブレット 画素数：120 万画素以上 F 値：2.8 以下 ・カラーイメージセンサー ・VGA サイズで 10fps 以上のプレビューが可能
ディスプレイ	◇タブレット サイズ：7.0inch～13.0inch 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

なお、本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本 TOE の誤受入率・誤拒否率は、TOE 使用用途とそれに対応した想定使用環境に依存する。光源環境については標準的な室内環境を想定しており、夜間の車内ルームランプ点灯時相当から晴天日蔭相当での使用が想定される。モバイルデバイスのカメラで画像が撮影できないほどの暗い環境は適さない。

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。年齢はおよそ 18 歳～59 歳で 20 代、30 代を中心とする男女。

・温度：10℃～28℃

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1、図 5-2、図 5-3 に示す。太枠外のデータ採取機能、格納機能、ID 取得機能、ポリシー管理機能/アクセス制御機能は TOE に含まれない。

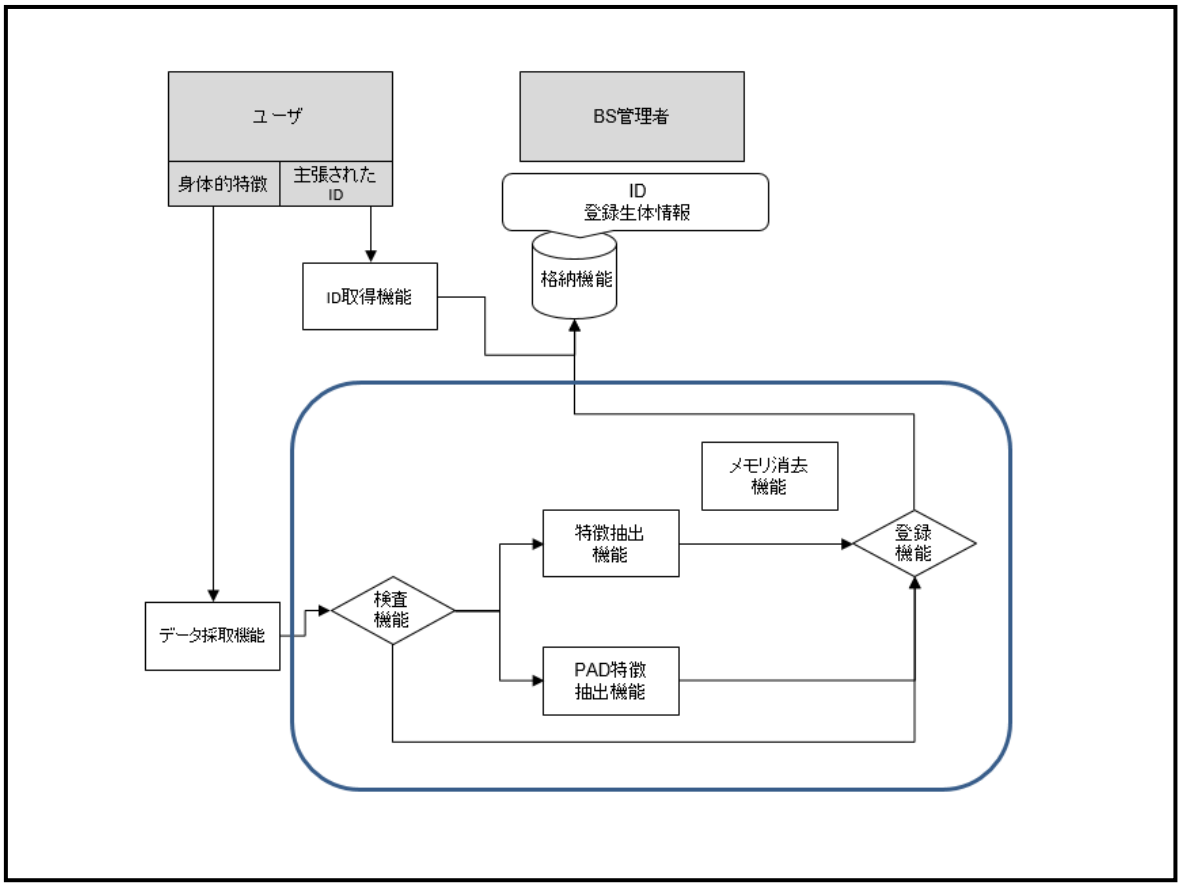

図 5-1 TOE の構成（登録の場合）

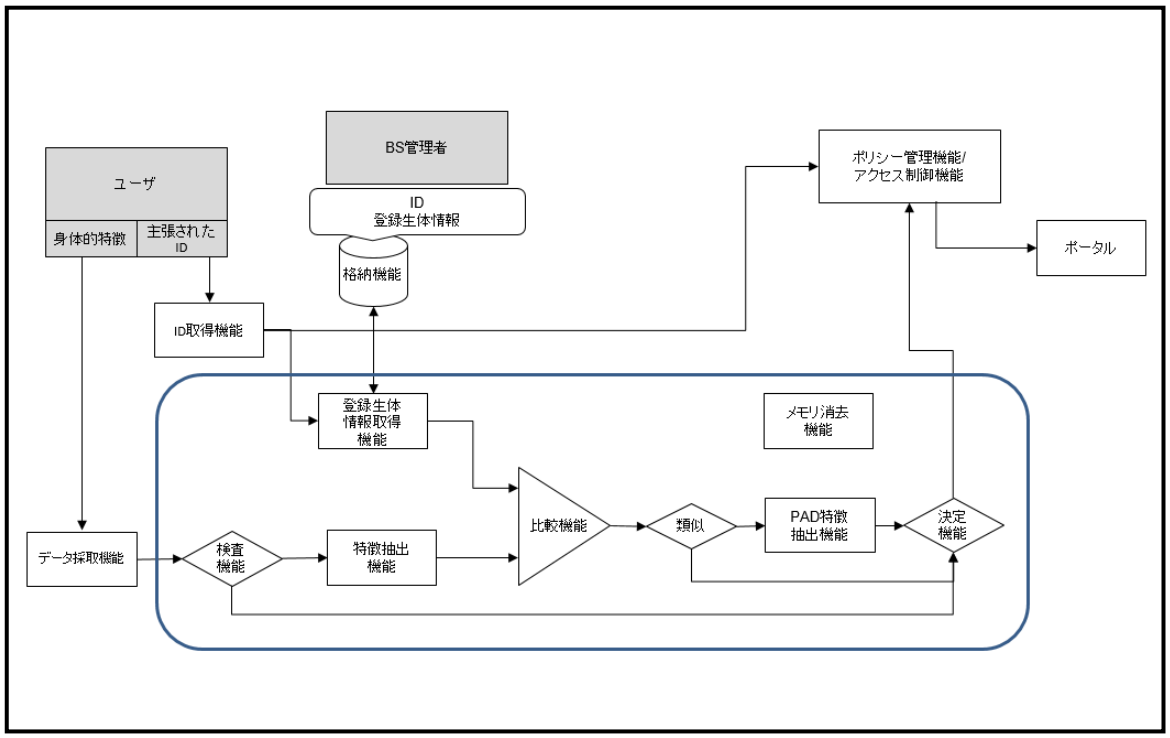

図 5-2　TOE の構成（照合の場合）

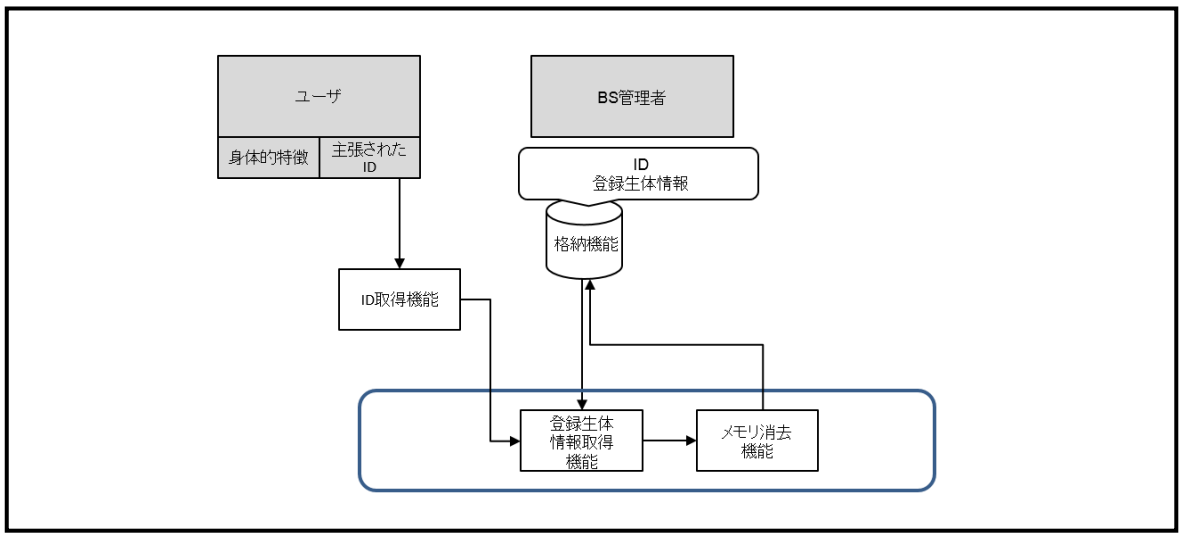

図 5-3　TOEの構成（登録生体情報削除の場合）

TOE が含む機能は以下のとおりである。

・特徴抽出機能：採取された生データから特徴を抽出する。

・検査機能：データが十分な品質を持っているか検査を行う。

・登録機能：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。

・登録生体情報取得機能：ユーザ ID に対応する登録生体情報を取得する。

・比較機能：特徴データと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 : PAD 特徴抽出機能及び比較機能を出力に基づき照合成功か失敗かを決定する。

・PAD 特徴抽出機能 : PAD（Presentation Attack Detection）を判定するための特徴データを抽出する。

・メモリ消去機能：使用後のメモリの内容を消去する。

5.2 IT環境

本 TOE は、データ採取機能、セキュリティに関連したパラメタ（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 の運用環境にある機能やインタフェースは以下のとおりである。

・データ採取機能：ユーザから生データを採取する機能。

・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。このデータベースにユーザの登録生体情報などを格納する機能。

・ID 取得機能：ユーザが入力する ID を獲得する機能。

・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を受けて、ユーザのポータルへのアクセスコントロールを実現する機能。

・セキュア通信機能 : TOE からの通信、TOE への通信、TOE 構成要素間の通信をサポートする機能。

・ポータル : 物理的又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物理的又は論理的な場所。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を表 6-1 に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

表 6-1 TOEに添付されるドキュメント

評価証拠資料	バージョン
掌静脈認証ソフトウェアiOS版準備ガイダンス	2.01
掌静脈認証ソフトウェアiOS版運用ガイダンス	2.02
掌静脈認証ソフトウェアiOS版I/F解説書	2.00
掌静脈認証ソフトウェアiOS版アプリケーション開発マニュアル	2.00
掌静脈認証ソフトウェアiOS版リファレンスマニュアル	2.00
納品物一覧	2.03

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報通信研究部 マルチメディア技術チーム 情報セキュリティ評価課は、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）の相互承認に加盟している認定機関（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。

7.2 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、本TOE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を説明する。

7.3 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 30 年 11 月に始まり、令和元年 12 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。また、令和元年 6 月に評価者テストを実施した。

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。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成は、次に示す点を除き「4.2 運用環境と構成」と同じである。「4.2 運用環境と構成」の構成は ST において保証の対象とされている構成である。

・「図 4-1 TOE の運用環境」に示されているアプリケーションは、開発者テストでは､TOE に伴う配付物として ST に記載されているサンプルアプリケーションが使われている。TOE に変更はなく、テスト構成として問題ないことが評価者によって判断されている。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

生体情報登録、生体照合実行、登録生体情報削除の各インタフェースを刺激することで、その応答と動作及び実装が正しいことを確認した。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-1 に示す。

表 7-1 開発テストツール

ツール名称	概要・利用目的
MAC	MAC：OS: High Sierra 10.13.6 Xcode：Ver.9.4.1 スマートフォンやタブレット上のプログラムをPCから実行するための使用

＜開発者テストの実施内容＞

応答は､表示されるメッセージによって結果を確認した｡各機能の動作は､ログによって結果を確認した。また TOE のふるまいを観察することで各機能が確かに実装されていることを確認した。これらの確認は､期待するテスト結果と実際の結果を画像ファイルとログによって比較し一致を確認した。

テストケースは、生体情報登録、生体照合実行、登録生体情報削除の 3 種類に分類される。生体照合実行､登録生体情報削除は生体情報登録を前提とするため「順序依存」が存在する。この順序依存性に関してもテストで確認した。

b) 開発者テストの実施範囲

開発者テストは開発者によって69項目実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースがテストされたことが検証された。

カバレージ分析によって､機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。

c) 結果

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプリングテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、開発者テストと同様の構成である。評価者がテストを実施するにあたって、追加したテストツール等は存在しない。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

TOEの特性から評価者は、インタフェースに対する以下の観点で独立テストを実施した。

＜独立テストの観点＞

① 誤使用の観点

開発者テストと異なる入力でテストを実施する。

② SFR の観点

TOE のふるまいによる確認が困難な機能を確認する。

b) 独立テスト概要

評価者は、開発者テスト及び提供された評価証拠資料から、TSFIとSFRの観点で15項目のサンプリングテストを実施した。評価者は、開発者テスト及び提供された評価証拠資料から、上記の観点で4項目の追加の独立テストを考案した。評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストと異なる入力を考慮して 3 項目、ふるまいの観察による確認が困難な機能についてはソースコードレビューとして 1 項目の合計 4 項目のテストを実施した。

＜独立テストツール＞

独立テストにおいて利用したツールは、表 7-1 と同じである。

＜独立テストの実施内容＞

独立テストは、評価者によって 4 項目実施された。

独立テストの観点とそれに対応したテスト内容を表 7-2 に示す。

表 7-2 実施した独立テスト

観点	テスト概要

①誤使用の観点について	手をかざす方向を故意に不正にした時の登録と照合のふるまいを確認し、期待した結果と比較した。
②SFRの観点について	ソースコードレビューを実施しFDP_RIP.1が正確かつ完全に実装されていることを確認した。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまい及び実装を確認した。評価者は、すべてのテスト結果と期待されるふるまい及び実装が一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

①偽造物の提示や品質の低い提示等によって強制的にTOEを一般的でない状況又は期待されない状況に至らせ、その結果、誤登録及び／又は誤照合を引き起こす可能性が懸念された。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者が実施した侵入テストの構成は、開発者テストと同様の構成である。評価者がテストを実施するにあたって、追加したテストツール等は存在しない。

＜侵入テスト手法＞

偽造物の提示並びに品質の低い提示による検査を行うため、サポート文書に従って偽造物を作成し、登録と照合のテストを行い、脆弱性がないことを確認する。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-3 に示す。

表 7-3　侵入テスト概要

脆弱性	テスト概要
①偽造物の提示や品質の低い提示等によって強制的にTOEを一般的でない状況又は期待されない状況に至らせる	・偽造物を提示した試行では、一部の偽造生体を除いては登録に失敗することを確認した。 ・生体の掌を登録する際に故意に品質の低いデータを登録し、その後偽造物を提示した試行で照合に失敗することを確認した。

c) 結果

一部の偽造物においては登録が成功している。しかしながら[ST]に記載されている通り、運用を含むBS管理者が登録生体情報が偽造物から得られたもので無いことを目視で確認するため、偽造物の提示による登録が成功することはない。評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本評価では、「4.2 運用環境と構成」に示す動作環境を想定して評価を行った。この構成は ST における保証の対象としている動作環境と同じである。

7.6　評価結果

評価者は、評価報告書をもって本 TOE 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。

評価では以下について確認された。

PP 適合：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）

セキュリティ機能要件：　コモンクライテリア　パート２　拡張

セキュリティ保証要件：　コモンクライテリア　パート３　適合

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。

EAL2 パッケージのすべての保証コンポーネント

追加の保証コンポーネント　ALC_FLR.1

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7　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。

8 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、以下の認証を実施した。

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サンプリングし、その内容を検査し、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。

これらの認証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、本 ST 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、本認証報告書を発行した。

8.1 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、本 TOE が CC パート 3 の EAL2 及び保証コンポーネント ALC_FLR.1 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE の調達者は、「1.1.3 免責事項」及び「4 前提条件と評価範囲の明確化」の記載事項を参照し、本 TOE の制約事項が各自の想定する運用条件に合致しているかを確認する必要がある。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり提供される。

掌静脈認証ソフトウェア　iOS 版 セキュリティターゲット　バージョン 1.20
2019 年 12 月 6 日　株式会社ノルミー

11 用語

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）
SFR	Security Functional Requirement（セキュリティ機能要件）
TSFI	TOE Security Functionality Interface（TOEセキュリティ機能インタフェース）

本報告書で使用された TOE に関する略語を以下に示す。

BS	Biometric System
ID	Identification
OS	Operating System
API	Application Programming Interface
LED	Light Emitting Diode
PAD	Presentation Attack Detection

本報告書で使用された用語の定義を以下に示す。

攻撃者	権限なくポータルに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。
生体情報	本TOEが対象とする掌静脈と掌紋の生データ、特徴データ、登録生体情報を示す
偽造生体	身体的特徴やそれを含む身体部分の一部又は全部を偽造したもの。本TOEでは掌静脈や掌自身が偽造されたものを示す。
登録生体情報	照合のために登録に適した特徴データ又は特徴データの組。
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を比較して同一のユーザの物であるかを判定するアプリケーション。
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
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

12 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30年7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30年9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30年9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 Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[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5版, 2017年4月, CCMB-2017-04-001 (平成29年7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5版, 2017年4月, CCMB-2017-04-002 (平成29年7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5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[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5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] 掌静脈認証ソフトウェア　iOS版　セキュリティターゲット　バージョン 1.20 2019年12月6日　株式会社ノルミー

[13] 164753-02-R003-06, 2019年12月9日, みずほ情報総研株式会社情報通信研究部 マルチメディア技術チーム情報セキュリティ評価課

[14] Evaluation Guidance for Biometric Verification Products Version 1.0, March 2017, National Institute of Advanced Industrial Science and Technology OKI Software Co., Ltd.

[15] Annex for Evaluation Guidance for Biometric Verification Products Version 1.0, March 2017, OKI Software Co., Ltd.

[16] 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）