認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成23年6月23日 (IT認証1353)
認証番号	C0332
認証申請者	日立オムロンターミナルソリューションズ株式会社
TOEの名称	Finger Vein Authentication Device UBReader2
TOEのバージョン	Hardware: D, Software: 03-00
PP適合	なし
適合する保証パッケージ	EAL2
開発者	日立オムロンターミナルソリューションズ株式会社
評価機関の名称	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

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。

平成23年12月21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　山里　拓己

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 Common Criteria for Information Technology Security Evaluation
Version 3.1 Release 3
② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

評価結果：合格

「Finger Vein Authentication Device UBReader2」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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、日立オムロンターミナルソリューションズ株式会社が開発した「Finger Vein Authentication Device UBReader2、バージョン　Hardware: D , Software: 03-00」（以下「本 TOE」という。）について TÜV Informationstechnik GmbH, Evaluation Body for IT-Security（以下「評価機関」という。）が平成 23 年 12 月 8 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日立オムロンターミナルソリューションズ株式会社に報告するとともに、本 TOE に関心を持つ消費者や調達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、本書の付属書である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 を購入し本 TOE を含むシステム運用に責任を持つ運用者、及び本 TOE に関連するソフトウェアを開発する開発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 保証パッケージ

本 TOE の保証パッケージは、EAL2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、指の静脈パターンを用いた生体認証機能を提供する認証装置、及び認証装置を制御するためのソフトウェア（デバイスドライバ）である。TOE に入力された指の静脈パターンと、予め TOE に登録してある静脈パターンとを照合することにより、本人の認証を行う。

本 TOE は、登録済みの利用者に成りすまして、認証をパスしようとする試みを防ぐためのセキュリティ機能を提供する。

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 はシステムの一部として運用され、本 TOE が提供する認証機能により正当な利用者のみがシステムへのアクセスを許可される。本 TOE では正当な利用者以外の者がこの認証機能を通過し、背後のシステムに不正にアクセスを試みる行為を脅威として定義しており、以下のセキュリティ機能によりそれぞれの具体的な攻撃に対抗する。

本 TOE に登録された正当な利用者に成りすまし、認証をパスすることを目的として、様々な手法で認証機能を試行する攻撃に対抗するため、本 TOE では生体情報による認証機能を提供する。生体情報として指の静脈パターンを使用することにより、生体情報の偽造の難易度がより高くなり、よりセキュアな本人認証が可能となる。

TOE 自身が管理する各種情報（登録済みの静脈パターンデータ、閾値、認証結果等）に不正にアクセスし、それら情報を改ざん、または再利用することにより認証をパスしようとする攻撃に対抗するため、本 TOE は物理的な攻撃（デバイスの開封）に対抗するための機能、及び残存情報を消去する機能を提供する。

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 の構成要素である認証装置は USB により PC と接続され、PC 側に構築されたシステム（ポータルサイト等）のログイン処理等に使用されることを想定している。また、認証装置は PC 上に実装されたアプリケーションにより制御され動作する。このアプリケーションは TOE の構成要素である認証装置制御用ソフトウェア（デバイスドライバ）を使用して TOE の購入者によりセキュアに実装される。

本 TOE の運用においては、静脈パターンを用いた生体認証に適した物理的環境のもと、TOE が接続された PC や USB 接続経路の物理的な保護環境を確保することが TOE の運用者に求められる。

1.1.3 免責事項

本 TOE のセキュリティ機能は、通常運用中の認証装置に対する脅威に対抗するものであり、認証装置が接続された PC、USB ケーブルに対する脅威、及び運用状態にない TOE に対する脅威に対しては対抗しない。これらのセキュリティは TOE 運用者の責任となる。

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 セキュリティ認証申請手続等に関する規程」[1]、「IT セキュリティ評価機関承認申請手続等に関する規程」[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、平成 23 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[12]、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（[3][4][5]または[6][7][8]）及び CEM（ [9][10]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 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	Finger Vein Authentication Device UBReader2
バージョン：	Hardware: D , Software: 03-00
開発者：	日立オムロンターミナルソリューションズ株式会社

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。

認証装置の裏面にラベリングされたハードウェアバージョンと、CD-ROM により提供されるソフトウェア、及びマニュアル群のメディアにラベリングされたソフトウェアバージョンを管理者が確認し、マニュアルに記載されたバージョンと比較することにより運用中の製品が評価を受けた本 TOE であることを確認できる。

また、PC にインストールされているソフトウェアのコンポーネント毎の詳細なバージョン情報を表示するツールが別途用意される。管理者がこのツールを使用することで現在 PC にインストールされているソフトウェア構成の詳細情報を取得し、マニュアルに記載された詳細情報と比較することで評価対象の TOE が PC にインストールされていることを確認できる。

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。

本 TOE は、指の静脈パターンを用いた生体認証機能を提供する認証装置、及び認証装置を制御するためのソフトウェア（デバイスドライバ）であり、TOE に登録済みの利用者に成りすまして、認証をパスしようとする試みを防ぐためのセキュリティ機能を提供する。

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.BRUTEFORCE	An attacker may perform a brute force attack in order to get verified by the TOE using the identity of another user. In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE. This threat considers two different threat agents and corresponding adverse actions: - A not really hostile user who just tries to get verified with a wrong claimed identity a few times. The motivation of such a user is usually just curiosity. The hostile user does not need specific knowledge about the TOE to perform this attack. - A real attacker who uses a large amount of biometric

識別子	脅威
	characteristics and who really wants to get unauthorized access to the portal. This type of threat agent is supposed to have further public knowledge on biometric systems.
T.MODIFY_ASSETS	An attacker may try to modify secondary assets like biometric references, threshold, pairing key, or the boolean decision. Such attacks could compromise the integrity of the user security attributes resulting in an incorrect result that might give unauthorized access to the portal. This threat covers a number of distinct types of attacks: - An attacker may attempt to modify the threshold level used by the TOE to authenticate users. If the attacker is able to change the threshold (for one or more authorised users), the ability to verify the user(s) will be compromised and the attacker may succeed in gaining access to the portal or an authorised user may be denied entry to the portal. - An attacker may attempt to modify the Boolean match decision, the pairing key, or the biometric authentication data (the Biometric Reference Record) of an authorised user with the aim of enabling an attacker to masquerade as the authorized user and gain access to the portal. Alternatively, an authorised user may be denied access to the portal. The attacker may be able to insert a new biometric reference, containing biometric data belonging to an attacker, with the aim of enabling the impostor to gain access to the portal.This kind of attack presupposes that the attacker has further knowledge about the TOE and maybe special equipment.
T.REPRODUCE	An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised user. In this way the attacker is trying to get access to the assets residing in the environment that should be

識別子	脅威
	protected with the support of the TOE. The attacker will need further knowledge on biometric systems and the used biometric modality. Attackers may use technical equipment for analysing and generation of the biometric characteristics. The attacker may also be supported by an authorized user of the TOE (e.g. to imitate his biometric characteristic).
T.RESIDUAL	An attacker may try to take advantage of unprotected residual security relevant data (e.g. biometric data and settings) during a user's session or from a previous, already authenticated user. In this way the attacker tries to get access to the security relevant settings of the TOE. This threat covers a following scenario including: - An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data) using a flaw in a user visible interface of the TOE. The attacker needs further knowledge about the TOE to find and exploit a vulnerability regarding residual data in memory. Note: Because the TOE reads biometric characteristics from the vein structure of a finger, residual fingerprint images on the surface of the capture devices cannot be used by attackers to copy or replay the biometric characteristics. 【補足】 認証装置の表面に物理的に残存する情報については本TOEでは脅威にならないため、本脅威では認証装置内部に残存するデータに対するデバイスドライバ側からの論理的な不正アクセスを想定している。

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.BRUTEFORCE」への対抗

本脅威は、攻撃者が TOE の認証機能をパスしてシステムに不正にアクセスすることを目的として、TOE に登録されていない自身の指の静脈データや、その他の指の静脈データを認証装置に入力し、登録済みの静脈データの１つにマッチさせようとする試みを想定している。この脅威に対して、下記のセキュリティ機能により対抗する。

(a) 生体情報による認証機能

認証装置に入力された静脈パターンと、予め装置内に格納されている参照用静脈パターンとの照合処理を行い、同一の指から取得された静脈パターンかどうかの判断結果をデバイスドライバに通知する機能である。

認証プロセスの流れを以下に示す。

① 識別処理：

デバイスドライバから静脈パターンの識別情報（ID）が通知され、その ID に該当する参照用静脈パターンが抽出される。該当するデータが存在しない場合はこの時点でエラーが通知される。

② 読み取り処理：

認証装置が待ち状態となり、指が装置上に置かれたことを検出すると、静脈パターンの読み取り処理が開始される。読み取り処理では、装置上部からの近赤外線を指に透過させて得られる静脈パターンを、装置下部カメラで記録する。

指の設置個所にはタッチセンサが組み込まれ、指が置かれたことを確認するまでは読み取り処理を開始しない。

③ 照合処理：

読み取った静脈パターンデータと、参照用のデータを照合し、両データの差異が閾値以下の場合は成功、閾値より大きい場合は失敗と判断し、結果をデバイスドライバに通知する（但し、2 つのデータが全く一致した場合（差異が 0 の場合）には、照合が失敗する。）。

上記の各処理はデバイスドライバからの制御により実施されるが、その制御を行うアプリケーションは、TOE の購入者により実装される。このアプリケーションが、本 TOE の認証機能を適切なタイミングで実行し、通知された認証結果に従って適切なアクセス制御を行うことで、本脅威が想定する攻撃に対抗することが可能となる。

(2) 脅威「T.MODIFY_ASSETS」への対抗

本脅威は、攻撃者が TOE の認証機能をパスすることを目的として、認証装置のメモリ等に不正にアクセスし、認証機能に関連する情報を改ざんする試みを想定している。

想定される具体的な攻撃内容の例を以下に示す。

- 静脈パターンの照合処理の際に使用される閾値を不正に操作し、異なる指の静脈パターンでも照合処理を成功し易くする
- 照合処理の結果を不正に操作して、常に成功の結果をデバイスドライバに通知させる
- 攻撃者の静脈パターンデータを参照用のデータとして不正に認証装置内に格納する

この脅威に対して、下記のセキュリティ機能により対抗する。

(a) 耐タンパ機能

本機能は、運用中の認証装置に対する物理的な不正アクセスに対抗するものであり、認証装置の内部に設置されたセンサが、認証装置のカバーが開けられたことを検知すると、内部のメモリ（SDRAM,フラッシュ ROM）に格納された、静脈パターンデータやソフトウェアモジュール等を自動的に消去する。

運用中の TOE においてこの機能が動作することにより、TOE の動作に必要なデータが消去され、再びカバーが閉じられた後も正常に起動することができなくなる。

本機能が実装されることにより、認証装置の内部に不正アクセスするという攻撃者の攻撃に対抗することが可能となる。

(3) 脅威「T.REPRODUCE」への対抗

本脅威は、攻撃者が TOE の認証機能をパスすることを目的として、偽造した静脈データを認証装置に入力する試みを想定している。データの入力は偽造した人工指を使用して認証装置の外から行う場合や、作成した偽造データを認証装置の内部メモリ等に直接書き込む場合等が想定される。この脅威に対して、下記のセキュリティ機能により対抗する。

(1) 生体情報による認証機能

本機能で使用されるタッチセンサにより、指を正しく設置するまで、静脈パターンの読み取り処理は開始されない。また、静脈パターンの照合処理を高精度で行うことにより、偽造されたデータの認証を拒否することができる。これらの処理の組

み合わせにより、偽造した入力データを用いた装置外部からの攻撃に対抗することができる。

(2) 耐タンパ機能

偽造したデータを装置の内部メモリに直接書き込むためには装置のカバーを開けて内部メモリに直接アクセスする必要があるため、本機能を実装することにより脅威に対抗することができる。

(4) 脅威「T.RESIDUAL」への対抗

本脅威は、デバイスドライバ経由で認証装置内に残存する関連データ（照合処理に使用した静脈パターンデータや設定情報等）が再利用されることを想定している。この脅威に対して下記のセキュリティ機能により対抗する。

(1) 残存データ保護機能

本機能は、認証機能において、静脈パターンの照合処理が終了した時点で、照合に使用したデータ及び関連する設定情報を消去する機能である。本機能により、過去に使用した静脈パターンデータ等を不正に取得して再利用することを防ぐことが可能となる。

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
OSP.ERROR	The TOE shall meet recognised national and/or international criteria for its security relevant error rates (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)). For the TOE a FAR of less than 0.001 is claimed.

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「OSP.ERROR」への対応

このセキュリティ方針は、本 TOE が提供する生体情報を用いた認証機能の精度に関する要求である。特に本 TOE では、他人の認証要求を誤って受け入れる確率を示す FAR(False Accept Rate)の値が要求されている。

本 TOE では、指静脈を用いた認証機能に関して FAR が要求を満たしていることを、開発者、及び評価者がテストを実施しその結果をもって保証する（「7.3 製品テスト」参照)。

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	The administrator is well trained, non hostile, and reads the guidance documentation carefully, completely understands and applies it. The administrator is responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.
A.ENROLMENT	The enrolment is assumed to be already securely performed and therefore, the biometric reference for each authorized user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user.
A.ENVIRONMENT	It is assumed, that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, database, LAN, and guardian). Specifically the following things are assumed: - It is assumed that the direct environment of the TOE supports the functionality of the TOE. Regarding the request of the claimed identity, which is necessary for the biometric authentication, the environment offers the possibility to integrate a claimed identity into the biometric verification process. - The environment is assumed to implement the access control functionality for the protected portal. Specifically, if the environment has more than one

識別子	前提条件
	portal that is secured using the services of the TOE the environment is assumed to ensure that after authentication of a user (by the TOE) a portal is only opened if the user has the necessary permission. - The environment is assumed to ensure a secure communication of security relevant data from and to the TOE. - The environment ensures a secure communication between the TOE components by physical means. - It is assumed that the TOE environment is free of viruses, trojans, and malicious software. - The TOE is a piece of equipment that uses near-infrared light to capture finger vein data without being in physical contact with the finger. Thus the near-infrared light from natural light (sunlight), incandescent lamps, mercury lamp and halogen lamps in the environment can reduce the authentication accuracy. Therefore it is assumed that the capture device is not exposed to direct sunlight, incandescent lamps, mercury lamp and halogen lamps. - The UBReader2 device is assumed to be stored in a secure environment (e.g. locked storage room) whenever it is not in use and powerless. Before the powerless device is brought into operation, the administrator is assumed to check the security seal and verify that the device has not been opened.
A.PHYSICAL_DRIVER	It is assumed that the UBReader2 device driver installed on the PC is physically protected against unauthorized access or destruction. Physical access to PC is only allowed for authorized administrators. This does not cover the UBReader2 device that has to be accessible for every user.
A.FALLBACK	It is assumed that a fall-back mechanism for the TOE is available that reaches at least the same level of

識別子	前提条件
	security as the TOE does. This fall-back system is used in cases where an authorized user is rejected by the TOE (False Rejection).
A.ROLES	An application using the TOE shall restrict its management functionality to authenticated and authorized administrators. Other users are not allowed to manage the TOE.
A.AUTH_ADMIN	An application using the TOE shall provide a mechanism to authenticate an administrator with other means than the biometric verification process. This authentication process may be realized via a user name/password or a smartcard/pin based mechanism.

4.2 運用環境と構成

本 TOE の構成要素である認証装置は USB を用いて PC に接続されて運用され、PC 側に構築されたシステム（ポータルサイト等）のログイン時に本人確認を行うための認証装置として使用されることを想定している。図 4-1 に認証装置のイメージを示す。

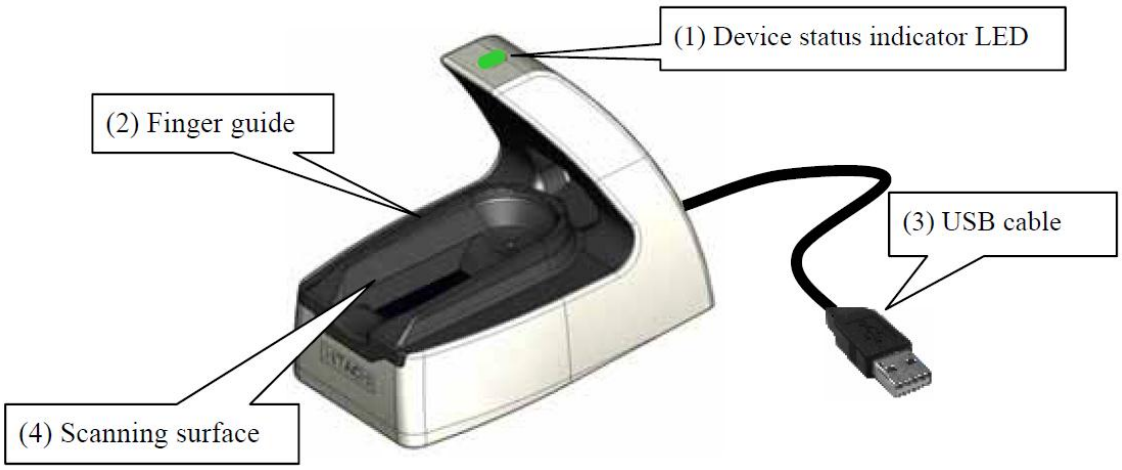

図 4-1 認証装置（TOEの構成要素）

USB cable（図 4-1(3)）を使用して PC に接続された認証装置は、PC 上のアプリケーションからの制御により動作する。このアプリケーションはアプリケーション

開発者により、TOE の構成要素である制御用ソフトウェア（デバイスドライバ）を使用して実装される。

アプリケーションからの指示により認証処理が開始されると、Finger guide(図 4-1(2))に添って置かれた利用者の指に対して、装置の上部から赤外線が照射され、Scanning surface(図 4-1(4))において指の静脈パターンが読み取られ、予め認証装置内に格納されている静脈パターンとの照合処理が行われる。

Device status indicator LED(図 4-1(1))に点灯する異なる色によって、認証装置の各状態（情報読み取り中、各種エラー発生等）が示される。

本 TOE の運用に関連する役割を以下に示す。

アプリケーション開発者：
TOE に添付されるガイダンスに従い、認証装置を制御するためのアプリケーションを開発する。

管理者：
TOE の運用に際して環境構築、及び管理作業等全般に対して責任を持つ。
運用中は静脈認証に適した環境のもと、PC 等の物理的な保護についても責任を持つ。

一般利用者：
PC 上のシステムを使用するために認証装置を用いて本人確認処理を行う利用者。

また、デバイスドライバをインストールする PC の OS として下記をサポートする。

Windows XP Professional (32bit), Windows Vista Business (32bit),
Windows 7 Professional (32bit)

4.3 運用環境におけるTOE範囲

本 TOE には USB による PC との接続経路に関する保護機能として暗号化通信機能が実装されているが、この機能は本評価の範囲外である。したがって認証装置と PC 間の通信の保護手段は TOE 運用者の責任において用意する必要がある。

また、本 TOE が提供する認証機能は、予め選択された静脈パターン同士を照合する機能のみであり、必要な静脈パターンを選択する処理（識別処理）や関連するパラメタを設定する処理等は TOE の範囲外となり、これらはアプリケーションにより提供する必要がある。

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 に示す。TOE は PC に接続される認証装置（図 5-1 中 UBR2 Device）と PC にインストールされる制御用ソフトウェア（図 5-1 中 UBR2 Driver）で構成される。

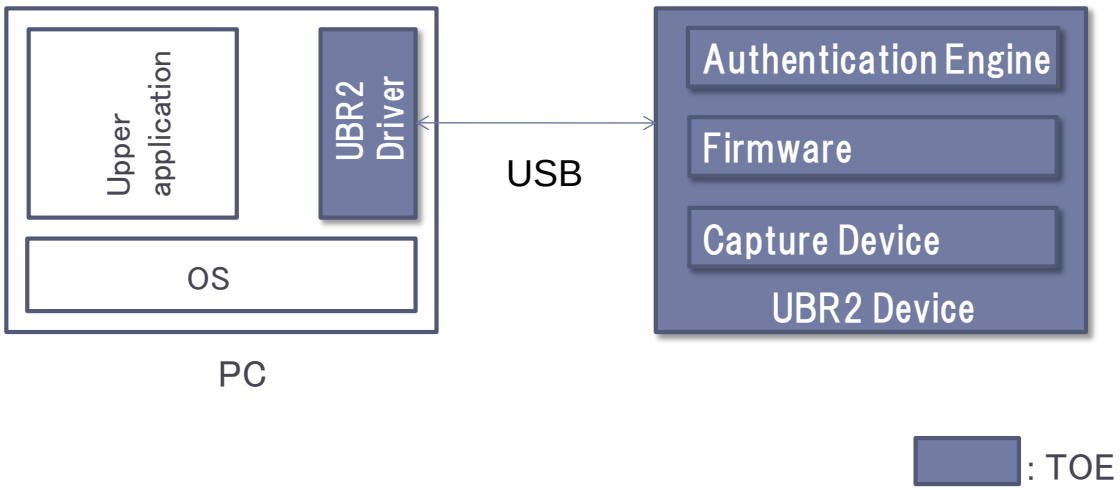

図 5-1 TOE構成

図 5-1 の TOE 各構成要素の概要について以下に示す。

UBR2 Driver

認証装置を制御するためのデバイスドライバ。認証装置が接続されるPCにインストールされ、認証装置の各機能を実行するためのインタフェースがAPIとして提供される。

アプリケーション開発者はこのAPIを使用して、アプリケーションを開発する。

Authentication Engine

認証装置に実装されるソフトウェアモジュールで、内部に登録された静脈パターンと新たに入力された静脈パターンの照合処理を行う。

Firmware

PCとの通信を制御し、デバイスドライバからの要求に従いCapture Device等のハードウェアを始め、装置全体を制御する。

Capture Device

認証装置に置かれた指から静脈パターンを読み取るためのハードウェアモジュールで、赤外線モジュール、カメラモジュール、各種センサ等で構成される。

認証装置には、その他 CPU、メモリ（SDRAM、フラッシュ ROM）、USB インタフェース等のハードウェアが搭載される。フラッシュ ROM には各種ソフトウェアモジュールが格納される他、認証を行う際に使用される参照用静脈パターンが予め格納される。

5.2 IT環境

本 TOE は PC に実装されたアプリケーションからの制御により動作する。PC 上のアプリケーションは TOE をセキュアに運用するためのセキュリティ機能が求められ、アプリケーション開発者はガイダンスに従ってこれらの機能を適切に実装する。

TOE をセキュアに運用するために必要となる主な機能としては下記のものが挙げられる。

認証装置の初期化、終了機能：
認証装置を正常に立ち上げ、終了させるための制御機能

認証機能の実行：
認証装置で静脈パターンの照合処理を開始するための制御機能

各種設定機能：
認証に関する各種パラメタの設定を行う機能やエラーハンドリングに関する処理

管理者認証、及びアクセス制御：
上記設定等を行う権限を持つ管理者を認証する機能、及び管理者のみに各種機能を実行させるアクセス制御機能（管理者の認証には生体認証とは別の方式を用いた認証機能が求められる）

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以下に示す。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。

ドキュメント名	バージョン
CC Guidance Addendum	1.6
Finger Vein Authentication Device UBReader2 User's Manual	05
Finger Vein Authentication Device UBReader2 Driver Interface Specifications	08
Finger Vein Authentication Device UBReader2 Device Driver Installation Manual	03

7 評価機関による評価実施及び結果

7.1 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。

7.2 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 23 年 6 月に始まり、平成 23 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、構成管理・配付の各ワークユニットの評価に関して、実際に TOE を購入しその配付経路、構成管理に関するセキュリティ手段の確認を行うと共に、関連する評価者テストによりセキュリティ手段が確実に適用されていることを確認した。また、平成 23 年 7 月、8 月に評価機関において開発者テストのサンプリングチェック及び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。

7.3 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。

7.3.1 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を図 7-1 に示す。

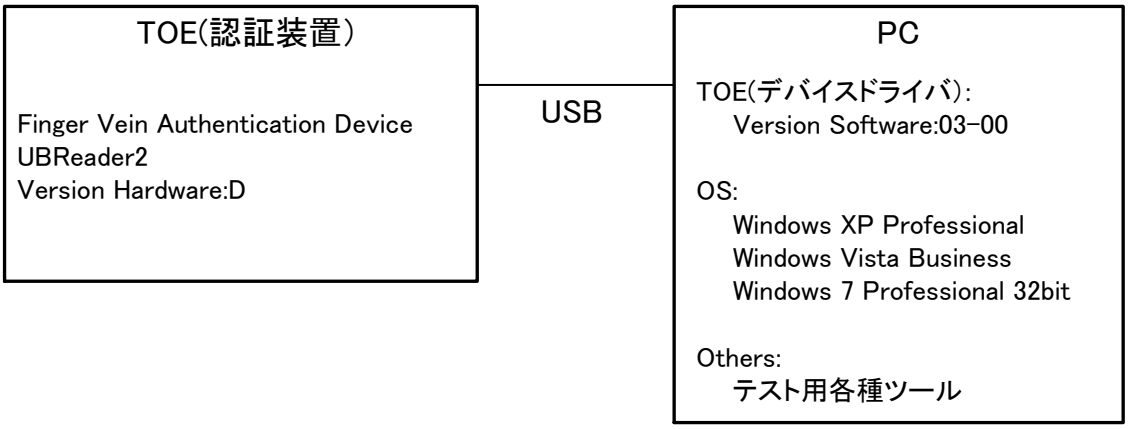

図 7-1 開発者テストの構成図

開発者テストは本 ST において識別されている TOE 構成と同一の TOE テスト環境で実施されている。なお、PC 上にはテスト用のアプリケーションがインストールされる。このアプリケーションは本 TOE の構成要素であるデバイスドライバを使用して認証装置の制御や、認証装置からの応答の確認のために使用される。

⑵ 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＞

開発者テストは通常のTOEの使用において想定される外部インタフェース（デバイスドライバが提供するAPI、認証装置の静脈パターン読み取り部）を刺激し、結果を目視観察する方法の他、耐タンパ機能のテストに関しては実際に認証装置を開封し、その結果の観察が行われている。

＜開発者テストの実施内容＞

外部インタフェースのテストについては、デバイスドライバが提供する各APIを実行し、戻り値を確認するための専用アプリケーションが使用された。認証処理を実施する際は認証装置に静脈パターンを入力し、アプリケーションに通知される認証結果の内容、及び認証装置のLEDの状態を観察し、予め期待されたテスト計画書の値との比較を行った。その結果期待されるテスト結果の値と実際のテスト結果の値が一致していることが確認された。

認証精度の確認については、静脈パターンの入力、登録データとの比較結果の集計を自動的に実施する専用アプリケーションが使用され、開発者が事前に準備したサンプルの登録データ群を用いてFARを算出し、要求を満たしていることが確認された。なお、テストでは約6,000,000回の照合処理を行い、全ての照合結果において正しい結果が得られたことを確認している。

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12項目実施された。各項目には正常系、異常系等複数の確認項目が含まれる。

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。

7.3.2 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ル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、図 7-1 に示した開発者テストと同様の構成である。

(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。

＜独立テストの観点＞

① 外部インタフェースから入力される、生体情報という多様性を考慮し、独自に用意した入力データを使用し、バリエーションを増やしたテスト項目を実施する。

② テスト結果の確認方法についてバリエーションを増やし、開発者テスト結果の妥当性についてより高い確信を得る。

③ サンプリングテストにおいては、網羅性の観点から全ての TSF、TSFI が含まれるように項目を選択する。

b) 独立テスト概要

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＞

独立テストは、開発者テストとは異なる初期条件の設定や異なる入力データを使用した上で、通常の TOE の使用において想定される外部インタ

フェース（デバイスドライバが提供する API、認証装置の静脈パターン読み取り部）を刺激し、結果を目視観察する方法の他、耐タンパ機能のテストに関しては実際に認証装置を開封し、その結果の観察が行われている。

＜独立テストの実施内容＞

独立テストの観点に基づき、独立テスト 6 件、サンプリングテスト 12 件のテストが実施された。

実施された主な独立テスト概要と、対応する独立テストの観点を表 7-1 に示す。

表 7-1 実施した主な独立テスト

独立テストの観点	テスト概要
①	・認証装置に入力する静脈データのバリエーションを増やすため、評価者の知見に基づき、独自に作成された人工指、静脈パターンデータを組み合わせたものを認証装置に入力し、TOEのふるまいが仕様通りであることを確認する。 ・認証精度の算出結果についてより高い確信を得るため、評価者が用意した静脈パターンの入力データと、開発者テストで使用されたサンプルデータ群を使用してFARを算出し、要求値を満たしていることを確認する。
②	・耐タンパ機能の実施結果についてより高い確信を得るため、開発者テストで使用されたものとは別のアプリケーションを用いてTOEの状態を確認し、そのふるまいが仕様通りであることを確認する。 ・耐タンパ機能のテストを実施する初期条件、物理的環境のバリエーションを増やし、そのふるまいが仕様通りであることを確認する。

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が一致していることを確認した。

7.3.3 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 TOEに実装されるソフトウェア、ファームウェアが不正に改ざんされることで、セキュリティ機能がバイパスされる可能性がある。
② TOE運用中にUSBケーブルが外される等､想定外の物理的環境でTOEが運用されることによりセキュリティ機能がバイパスされる可能性がある。
③ デバイスドライバが不適切なアプリケーションにより通常想定されない使われ方をされた場合に、セキュリティ機能がバイパスされる可能性がある。
④ 実際の静脈パターンデータに近い入力データを偽造することにより、登録済みのデータに成りすまし、結果として認証機能をバイパスされる可能性がある。
⑤ 過負荷状態でTOEを運用することにより、セキュリティ機能がバイパスされる可能性がある。

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＞

侵入テストは、図 7-1 に示した開発者テスト、及び評価者独立テストと同様の環境で実施された。

＜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 7-2 に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、8 件の侵入テストを実施した。

表 7-2　侵入テスト概要

脆弱性	テスト概要
①	一部が改ざんされたファームウェアや認証モジュールが認証装置に格納された場合でも、TOE自身が適切に検出を行うことで、セキュリティ機能がバイパスされないことを確認する。
②	TOEの初期化処理中にUSBケーブルを抜く等、通常の運用では想定されない状況が発生した場合でも、セキュリティ機能がバイパスされないことを確認する。
③	想定されないようなAPI呼び出し（不正なパラメタの設定やAPIの非同期呼び出し等）が行われても、セキュリティ機能がバイパスされないことを確認する。
④	TOEに登録済みの指と同じ静脈パターンデータを様々な手法で偽造し、認証装置に入力しても認証機能がバイパスされないことを確認する。
⑤	リソース枯渇状態でTOEを運用しても、TOEがアンセキュアな状態にならないことを確認する。

c) 結果

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。

7.4　評価構成について

本評価では、図 7-1 に示す構成において、評価を行った。本 TOE は、この構成と構成要素が大きく異なる環境において、運用される場合はない。よって、評価者は、上記の評価構成は適切であると判断した。

また、認証精度に関するテストにおいて、開発者がテスト用に構築したサンプル静脈パターンデータベース（サンプルデータ群）を用いて FAR の算出が行われた。このデータ数、及び評価者からの入力データとの照合結果等から、今回使用されたサンプルデータ群は、ST の要求を満たす認証精度を保証するテスト環境として適切であると評価者は判断している。

7.5 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：なし

セキュリティ機能要件：　コモンクライテリア　パート２　適合

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

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。

7.6 評価者コメント/勧告

消費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 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

「5.2 IT 環境」にも示した通り、本 TOE をセキュアに運用するためには、アプリケーション開発者がガイダンスに従って適切なアプリケーションを構築する必要があり、この中で、TOE に関連する複数のセキュリティ機能を新たに実装する必要がある。

また、上記アプリケーション、及び PC 側に構築するシステムにおいて、本 TOE が提供する認証機能を適切なタイミングで実行し、認証の結果を踏まえた利用者のアクセス制御を適切に行うことによって、初めて TOE が提供するセキュリティ機能性が実現されることに TOE 運用者は注意する必要がある。

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本認証報告書とともに提供される。

UBReader2 Security Target　version 1.12 ,2011-12-05
Hitachi-Omron Terminal Solutions, Corp.

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）

本報告書で使用された TOE に関する略語を以下に示す。

FAR	False Acceptance Rate (他人受入率)

本報告書で使用された用語の定義を以下に示す。

参照用静脈パターン	予めTOEの認証装置内に登録されている、正当な利用者の指の静脈パターン。 STではBRR(Biometric Reference Record)と記述される。
静脈パターン	近赤外線を照射して撮影された静脈の画像から作成された、照合用のデータ。本TOEでは指の静脈パターンを使用して照合を行う。
生体認証	人間の身体的特徴や行動的特徴の情報を用いて行う個人認証技術の総称。バイオメトリクス認証とも呼ばれる。本TOEでは身体的特徴として指の静脈パターンを使用する。

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23年2月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証申請手続等に関する規程, 平成23年2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申請手続等に関する規程, 平成23年2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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[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3版, 2009年7月, CCMB-2009-07-001, (平成21年12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3版, 2009年7月, CCMB-2009-07-002, (平成21年12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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] UBReader2 Security Target version 1.12, 2011-12-05, Hitachi-Omron Terminal Solutions, Corp.

[13] UBReader2 Evaluation Technical Report, Version 2 , 2011-12-08, TÜV Informationstechnik GmbH, Evaluation Body for IT-Security