認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成19年9月28日** (IT**認証**7175)
認証番号	C0160
認証申請者	**株式会社ディー・ディー・エス**
TOE**の名称**	**指紋認証ソフトウェア** EVE FA
TOE**のバージョン**	2.00
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**株式会社ディー・ディー・エス**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

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20年5月30日

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　鈴木　秀二

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 改訂第1版 (翻訳第1.2版)
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 改訂第1版 (翻訳第1.2版)

評価結果：合格

「指紋認証ソフトウェア EVE FA」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

1.1 はじめに

この認証報告書は、「指紋認証ソフトウェア EVE FA」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が行った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ディー・ディー・エスに報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　　指紋認証ソフトウェア EVE FA
バージョン：　2.00
開発者：　　株式会社ディー・ディー・エス

1.2.2 製品概要

本製品は、Windowsシステム向け指紋認証システムを制御するソフトウェアであり、Windowsシステム向け指紋認証ソリューションを提供する。

WindowsシステムにおいてクライアントPCのユーザがActive Directoryによってパスワード(Windowsログオンパスワード)認証され、Windowsドメインのコンピュータへのログオンが許可されている場合に、本製品の導入により、クライアントPCのユーザは、パスワード認証の代わりに指紋認証されることにより、上記許可がなされることとなり、識別・認証機能が強化される。

本製品は、クライアントPCと指紋照合を行うFA(Finger Authentication)サーバに分散して配置されて、指紋認証機能を実行する。

クライアントPCのユーザのWindowsログオン時、本製品はユーザ識別を行い、指紋の入力を求める。本製品は、周波数解析法により指紋の特徴量（サンプル）を抽出し、FAサーバに登録された指紋情報(参照テンプレート)と照合し、ユーザを認証する。指紋認証が成功すると、本製品は当該ユーザの予めFAサーバに登録されたWindowsログオンパスワードをActive Directoryに送信し、当該ユーザはWindowsドメインへのログオンが許可される。

本製品（TOE）のセキュリティ機能は、以下のとおりである。

(1) 識別・認証機能
(2) ユーザ情報及び指紋情報の管理機能
(3) 監査機能
(4) 通信路の情報保護機能

なお､本認証では指紋認証精度（他人受入率：FAR）は、評価の範囲外である。本TOEの構成における他人受入率：FAR、及び本人拒否率：FRRに関する参考値を表1-1に示す。

表1-1　1指3回登録時の他人受入率/本人拒否率(参考値)

他人受入率：FAR	本人拒否率：FRR
0.001%以下	0.1%以下

注）認証レベル（認証の厳しさ）が「標準的」での値

1.2.3　TOEの範囲と動作概要

本TOEは以下の3つのコンポーネントから構成される。

コンポーネント名称	コンポーネントの識別
サーバプログラム	EVE FA管理サーバ 2.00
ツールプログラム	EVE FA管理ツール 2.00
クライアントプログラム	EVE FAクライアント 2.00

これらのTOEコンポーネントを搭載した指紋認証システムとTOEの物理的範囲を図1-1に示す。グレーの部分がTOEを表す。

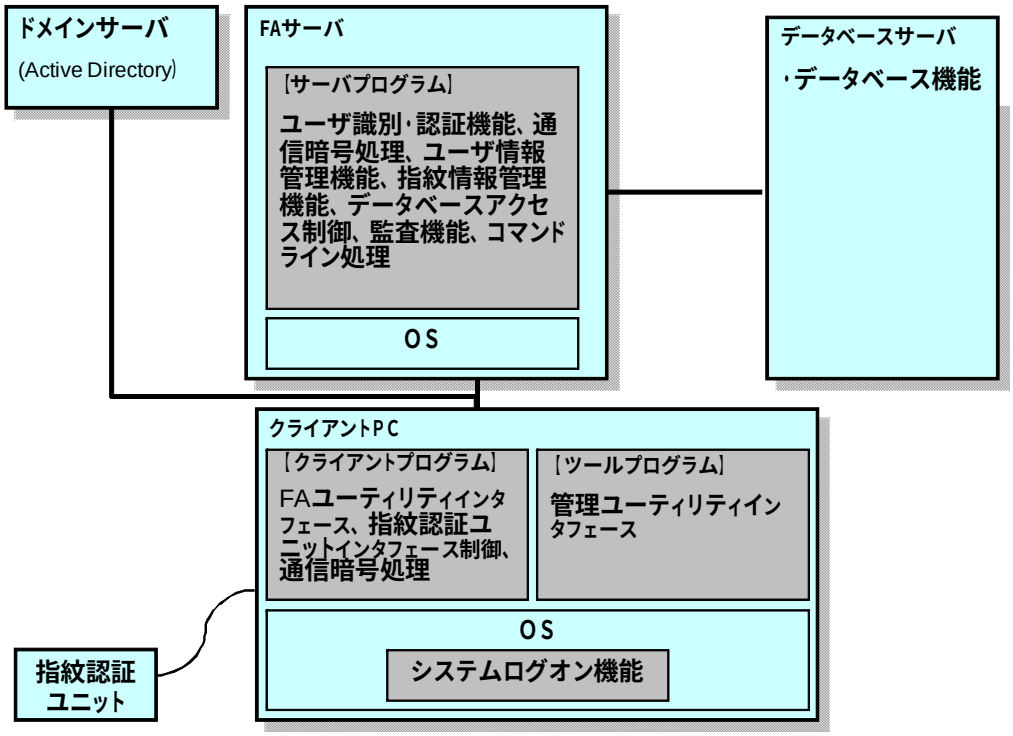

図1-1　TOE搭載の指紋認証システムとTOEの物理的範囲

なお、図1-1のシステムログオン機能は、TOEのインストールにより、クライアントPCのWindowsにおいてログオン管理を行っているGina（Graphical Identification and Authentication）ライブラリを、TOEのコンポーネント（指紋によるログオン制御機能）にリプレースしたものである。

また、TOEの運用構成（イメージ）を図1-2に示す。グレーの部分が、指紋認証システムを構築するために、既存のWindowsシステムに追加する必要がある部分を示す。

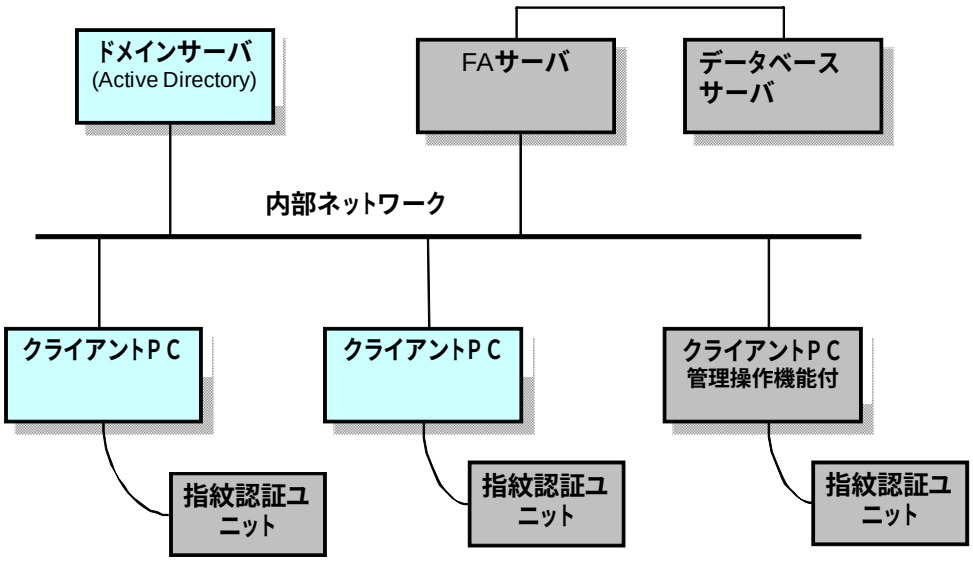

図1-2　TOEの運用構成

【説明】

(1)ドメインサーバ（Active Directory）

Windowsシステムのドメインへの参加（ログオン）を管理する。

(2)FAサーバ

ユーザ情報と指紋情報を管理するサーバ。複数台を使用した冗長化構成が可能（冗長化構成はTOEの機能には関係しない）。

(3)データベースサーバ

ユーザ情報と指紋情報を格納。FAサーバからのみアクセスされる。

(4)指紋認証ユニット

指紋を入力するユニット。UBF-blue（複数ユーザ共有可能）とUBF-mini（シングルユーザ使用）のタイプがあり、クライアントPCのUSBポートに接続して使用する。本TOEのセキュリティ機能に関して、UBF-blueとUBF-miniの機能面での違いは無い。

(5)クライアントPC

Windowsシステムのドメインにログオンするユーザが使用する端末。クライアントPCに、ユーザ情報の管理ユーティリティインタフェースを持つTOEのコンポーネントをインストールし、管理操作を行うこともできる。

上記のTOE運用構成におけるTOEの使用方法とTOEの動作概要は、以下のとおりである。

【ユーザ登録】

権限を持つ管理者は、指紋認証を行うユーザを登録するために、当該ユーザのユーザ識別情報（ユーザ名、ログオン先）、及びWindowsログオンパスワードをTOEに登録する。また、当該ユーザの指紋登録を行うために、ワンタイムパスワードをTOEで生成後、安全な方法で当該ユーザに通知する。ワンタイムパスワードは有効使用回数及び/または有効期限を制限した適切な強度のあるパスワードで、その制限内でTOEによるユーザ認証が可能になる。

ユーザがクライアントPCのEVE FAログオン画面から、ユーザ識別情報及びワンタイムパスワードを入力すると、TOEは、登録されたユーザ識別情報を確認（識別）し、さらに、当該ユーザ識別情報と関係付けられているTOEが生成したワンタイムパスワードとの使用制限内で入力されたワンタイムパスワードとの一致を確認し、本人と認める（認証）。その後、TOEは当該ユーザの登録されたWindowsログオンパスワードをActive Directoryに送り、当該ユーザはWindowsシステムへのログオンが許可される。

ユーザはログオン後、ユーザユーティリティ(FAユーティリティ)を起動し、指

紋情報をTOEに登録する。クライアントPCからユーザが指紋情報の登録操作を行うと、TOEは指紋認証ユニットによって指紋特徴量を抽出し、FAサーバにて指紋情報を登録し、指紋情報コードによりユーザ識別情報と関係付ける。

権限を持つ管理者の操作により、TOEは識別されたユーザ毎に異なる「ランダム文字列」を生成し、Active Directoryのログオンパスワードを置き換え、Windowsログオンパスワードを「ランダム文字列」に変更する。「ランダム文字列」は複雑な文字列の組み合わせからなり、誰も閲覧ができず、当初登録されたWindowsログオンパスワードに比べ、推測がより困難となる。

【ログオン（クライアント起動時及びスクリーンセーバから復帰時）】

TOEはEVE FAログオン画面から、ユーザ識別情報と指紋の入力を求める。ユーザの操作により、TOEは指紋特徴量を抽出し、FAサーバにてユーザ識別情報が登録されているか確認する（識別）。

ユーザ識別情報は、TOE内で当該ユーザの指紋情報と指紋情報コードで関係付けられており、TOEは、当該指紋情報コードで識別されている登録された指紋情報の指紋特徴量（参照テンプレート）と上記指紋特徴量との照合処理を行い、本人であることを確認する（認証）。その後、TOEは登録されたWindowsログオンパスワード（ランダム文字列）をActive Directoryに送り、当該ユーザはWindowsシステムへのログオンが許可される。

なお、TOEとActive Directory間で送信されるWindowsログオンパスワードの暴露及び改ざんからの保護は、Windowsシステムが行い、TOEによるセキュリティ対策の範囲外である。

【指紋情報の登録、変更、削除】

FAユーティリティはWindows上のアプリケーションのひとつで、Windowsにログオン後、起動可能になる。FAユーティリティを起動すると、TOEはユーザを識別・認証し、当該ユーザはFAユーティリティにログオン後、指紋情報(指紋特徴量)の登録（上記【ユーザ登録】参照））または変更及び削除を行うことができる。

【ユーザ情報及び指紋情報の管理】

管理ユーティリティ（管理ツール及びログビューア）：

Windows上のアプリケーションのひとつであり、Windowsにログオン後、起動可能になる。管理ユーティリティを起動すると、TOEはユーザを識別・認証し、管理ユーティリティにログオン後、管理操作が可能になる。

管理ユーティリティ起動時の認証は、指紋認証以外に指紋認証機能が使用でき

ない場合のために管理者パスワードによる認証も可能である。管理者パスワードは、システム管理者により設定される。システム管理者は十分強度のある管理者パスワードを設定し、権限を持つ管理者以外が管理ユーティリティを使用することを防止しなければならない。

コマンドライン：

FAサーバ上でコマンドプロンプトを起動しコマンドラインを入力して、ユーザ情報の管理操作を行うことができる。コマンドラインによる管理操作は、ユーザ名及び管理者パスワードが必要で、システム管理者の権限を持つユーザに操作が制限される。

1.2.4 TOEの機能

本TOEは「1.2.2　製品概要」に記載したように、Windowsシステムのドメインにログオンするユーザの認証を、パスワード認証から指紋認証に置き換えるためのソフトウェアであり、本質的に主たる機能がセキュリティ機能であるセキュリティ製品である。

本認証におけるTOEの評価範囲として、下記のセキュリティ機能が定義されている。詳細は「1.5.3　セキュリティ機能」に記す。

(1) 識別・認証機能
　指紋認証機能、ワンタイムパスワードによる識別・認証機能、及び管理者パスワードによる識別・認証機能。

(2) ユーザ情報及び指紋情報の管理機能
　システム管理者、またはシステム管理者から権限を付与された運用管理者にユーザ情報及び指紋情報の管理を行わせるための機能。

(3) 監査機能
　監査証跡の記録・維持・閲覧と管理を行うための機能。

(4) 通信路の情報保護機能
　内部ネットワークで通信されるクライアントPCとFAサーバ間のユーザ情報、指紋情報を暗号化する機能。

上記以外のTOEの機能としては、上記セキュリティ機能(4)が適用される基本機能（FAサーバとクライアントPC間の内部ネットワーク通信機能）、及び補助的な基本機能（ユーザ一覧取得機能、ログエクスポート機能、ランダム文字列発生機能）等がある。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[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」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「指紋認証ソフトウェア EVE FA セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「指紋認証ソフトウェア EVE FA v2.00 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成20年5月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能の詳細は以下のとおりである。

(1)識別・認証機能

・指紋認証によるユーザの識別・認証機能

ユーザ（一般ユーザ、管理者）がWindowsにログオンする時、TOEはEVE FAログオン画面を表示し、ユーザ識別情報（ユーザ名、ログオン先）及び指紋認証ユニットから指紋の入力を要求する。

また、Windowsにログオンしたユーザは、FAユーティリティ（一般ユーザ、管理者）または管理ユーティリティ（管理者）が起動可能となり、FAユーティリティまたは管理ユーティリティ起動時、TOEはEVE FAログオン画面を表示して、ユーザ名及び指紋認証ユニットからの指紋の入力を要求する。

TOEは、指紋の濃淡情報から指紋特徴量（サンプル）を抽出し、ユーザ識別情報に関係付けられた当該ユーザの登録済み指紋情報をデータベースから獲得し、照合する。照合成功後、TOEは登録された当該ユーザのWindowsログオンパスワードをActive Directoryに送り、当該ユーザはWindowsシステムにログオンする。Windowsシステムでユーザを識別・認証する機能は、TOEの範囲外である。

・ワンタイムパスワードによる識別・認証機能

ユーザ（一般ユーザ、管理者）が指紋認証手段を利用できない以下のケースで使用される。

①指紋登録前のユーザを認証する。
②登録した指が全て使用できない場合のユーザを認証する。
③指紋認証ユニットが使えない場合でもユーザを認証する。

この様なケースで、システム管理者または当該ユーザの変更管理権限を持つ運用管理者は、ワンタイムパスワードの発行機能の操作を実行する。TOEは管理者の設定に従い、有効使用回数または有効期限の属性を持つワンタイムパスワードを生成し、当該ユーザ情報と関係付ける。

TOEはワンタイムパスワードが使用される度に使用回数をカウントする。有効期限経過後または使用可能回数超過後のワンタイムパスワード認証は行わない。

ただし、管理者の管理ユーティリティ使用に関して、システム管理者がワンタ

イムパスワードを設定できるTOEの機能は、本TOEの運用では使用しないことにする。

・パスワードによる識別・認証機能

TOEは、一般ユーザのWindowsドメインへのログオン時に、指紋認証機能以外に直接Windowsログオンパスワードを入力させ、Active Directoryに送る機能を持つ（この機能は本TOEでは使用しない運用にする）。

また、管理者の管理ユーティリティへのログオン時に、指紋認証に代わり、権限を持つ管理者が設定したパスワードによる認証ができる。

(2)ユーザ情報及び指紋情報の管理機能

システム管理者、またはシステム管理者から権限を許可された運用管理者に、ユーザ情報及び指紋情報の管理を行わせる機能である。

管理されるユーザ情報及び指紋情報の内容は、以下のように構成される。

ユーザ情報：ユーザ識別情報（ユーザ名、ログオン先）、Windowsログオンパスワード、ワンタイムパスワード、グループ情報、指紋情報コード、権限情報、管理者パスワード

指紋情報：登録者名、指紋認証レベルの設定値及び登録した指の指紋特徴量（参照テンプレート）のセット（これらは指紋情報コードで識別される）

指紋情報コードによってユーザ情報と指紋情報は関係付けられ、ユーザ情報と指紋情報の変更操作に応じ、これらの関係を維持する。

一般ユーザのグループ情報は、運用管理者の管理が可能な一般ユーザの集合（グループ）を特定する情報である。また、管理者のグループ情報は、Administrators（変更権限を持つ）かAdministrators以外（参照権限だけを持つ）のいずれかに区別される。

運用管理者が、システム管理者から権限を委任（許可）される一般ユーザの管理範囲、またはユーザ情報、指紋情報の管理権限は、権限情報に保存される。運用管理者は自身の権限情報とグループ情報によって、一般ユーザの管理範囲と可能な操作（ユーザ情報や指紋情報の登録・変更・削除など）を行うことができる。

(3)監査機能

監査証跡の記録・維持・閲覧と管理（削除）を行う機能。

システム管理者は、以下の事象を監査証跡から閲覧でき、セキュリティ機能のふるまいを追跡できる。

①ユーザの識別・認証の成功/不成功の事象の発生
②管理者が行ったユーザ情報の操作
③ユーザが行った指紋情報の登録

(4)通信路の情報保護機能

クライアントPCとFAサーバ間の内部ネットワークで通信されるユーザ情報、指紋情報を通信前に暗号化し、受信後に復号する機能。

1.5.4 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 想定する脅威

識別子	脅 威
T.ILLEGAL_LOGON	許可されていないユーザが利用者ガイダンスのログオン手順に従い、FAサーバを不正利用するかも知れない。
T.ADMINI_RIGHT	権限を持たないユーザが、許可されていない管理操作を行い、不正にTOEの構成設定の変更またはユーザ情報及び指紋情報を変更するかも知れない。許可されていない管理操作とは次の操作である。 1)TOEに登録されたユーザの指紋情報を本人以外が不正に変更する 2)管理者が、許可範囲外のユーザ情報及び指紋情報を変更する 3) TOEの構成設定を変更する
T.COMM_DISC	クライアントPCとFAサーバ間の通信路にて、ユーザ情報及び指紋情報を盗聴し、権限外の暴露及び改ざんを行うかも知れない。
T.FA_NOUSE	指紋未登録または指紋認証を利用できないユーザは、FAサーバを使用できないかも知れない。

1.5.5 組織のセキュリティ方針

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はない。

1.5.6 構成条件

本TOEの動作に必要なハードウェアを表1-3に示す。

表1-3 TOEが動作するハードウェア

ハードウェア構成要素	仕様
FAサーバ	下記要件を満たすPC/AT互換機 CPU Pentium4相当 1GHz以上 HDD プログラム50MB + データサイズ メモリ容量 1GB以上 ネットワークインタフェース

ハードウェア構成要素	仕様
クライアントPC	下記要件を満たすPC/AT互換機 CPU Pentium3相当 600MHz以上 HDD プログラム40MB + データサイズ メモリ容量128MB以上 ネットワークインタフェース USB 1ポート以上
指紋認証ユニット	DDS製 UBF-blue : 型番 UB-P301 UBF-mini : 型番 UB-P501-M64-A00

また、本TOEの動作に必要なソフトウェアを表1-4に示す。

表1-4 TOEが動作するソフトウェア

ソフトウェア構成要素	製品識別
クライアントPC	Windows XP SP2
FAサーバ	Windows 2003R2 SP2
データベースサーバ	Microsoft SQL Server 2005 SP4 Oracle Database 10g Release 2
Active Directory	Windows 2003R2 SP2

1.5.7 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-5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1-5 TOE使用の前提条件

識別子	前提条件
A.TAMPER	Windowsログオン後クライアントPCにおいて、TOEの認証システムを危殆化する不正なハードウェア、ソフトウェアの追加がされないものと想定する。
A.SERVER_PROTECT	TOEが動作するFAサーバとユーザ情報と指紋情報を保存するデータベースサーバ、及び両者間を接続するケーブルは、物理的なアクセス制御がされ、保存された情報が暴露または改ざんされたり、TOE自身が改ざんされたり、または運用が直接的に妨害されない環境にて運用されることと想定する。
A.DEDICARED	FAサーバは専用であり、TOEとその関連するソフト

	ウェア以外が稼働することはないものと想定する。
A.NO_EVIL	システム管理者はシステムの運用について十分な能力を持ち、指紋認証システムの運用知識に精通し、信頼するものと想定する。またシステム管理者から権限を委任された運用管理者は、任された範囲内において悪意を持った行動を行わず、権限を乱用する操作をしないものと想定する。
A.OBJECTIVE	ユーザは自身の指紋を登録する際、指紋認証を不正に弱める意図や興味で登録することはしないものと想定する。
A.PASSWORD	指紋認証の代わりに認証に使用する管理者パスワード及びワンタイムパスワードは他人に知られないように扱われるものと想定する。

1.5.8 製品添付ドキュメント

本TOEに添付されるドキュメントを表1-6に示す。

表1-6　TOEのガイダンス文書

種類	ガイダンス文書名
利用者準備・操作ガイダンス	EVE FAガイダンス資料 (D080630)

2 評価機関による評価実施及び結果

2.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 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19年10月に始まり、平成20年5月の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、平成20年3月に開発・製造・配付の現場へ赴き、現物・記録の確認、及びスタッフへのヒアリングにより、ライフサイクルの各ワークユニットに関するプロセスの施行状況の検査を行った。また、平成20年3月に開発者サイトで開発者のテスト環境を借用し、評価者テスト（評価者独立テストと侵入テスト）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、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

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2-1に示す。

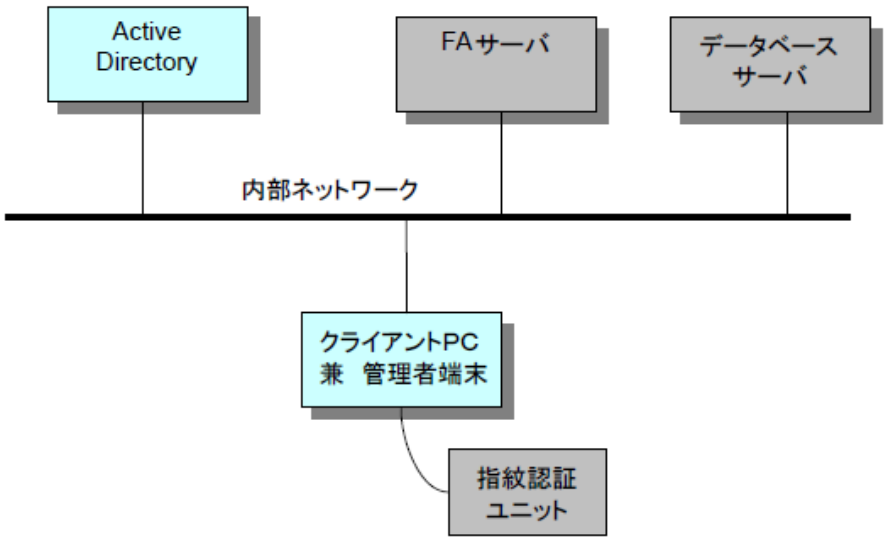

図2-1　開発者テストの構成図

FAサーバ、クライアントPCにTOEをインストールしている。STでは2種のデータベースと2種類の指紋認証ユニットがTOEの動作環境として識別されており、開発者テストは、それらを組み合わせた4 パターンのテスト構成で行われている。

なお、暗号化機能のテストを行う際には、クライアントPCにパケットキャプチャ用のツール（Ethereal）を追加している。

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成に関しては、上記「1) 開発者テスト環境」を参照の事。開発者テストは、STにおいて識別されているTOEバージョン、及びTOE動作環境と同一、かつ、TOE運用構成と同等であるTOEテスト環境で実施されている。

b.テスト手法

TOEの外部インタフェース（Windowsログオン画面、FAユーティリティ、管理ツール、ログビューア、コマンドラインI/F）から操作を行い、各操作に対応するTSFIを通じて、TOEのSFRを実施するTSFのふるまいを確認している。

同様に、外部インタフェースを通じて動作が確認できないもの（通信の暗号化機能）に関しては、パケットをキャプチャして取得したデータにより、通信電文のボディ部が常に、平文ではなく暗号文らしきものに変換されて送信され

ていることを確認している。

c.実施テストの範囲

TOEの外部インタフェースを用いたテストには51個の手順があり、各手順にはそれぞれ1～11項目のTSFIテストが含まれていた。上記51手順は全体として、37個のTSFIすべてをカバーし、項目数としては257項目が存在した。1つのテスト構成にて257項目（すべて）、残りの3つの構成で17、38、17項目が実施された。

パケットキャプチャでは、1つのテスト項目が実施された。このテストによって、通信路の情報の暗号化機能がテストされ、通信電文のボディ部が常に、平文ではなく暗号文らしきものに変換されていることが確認された。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

「2.3.1 開発者テスト環境 1）テスト構成」に示したテスト構成と同一である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

「2.3.1 開発者テスト環境 2）a. 開発者テスト環境」に示したテスト環境と同一である。

b.テスト手法

TOEの外部インタフェースから操作を行い、ふるまいを確認した。

c.実施テストの範囲

評価者独立テストとして、評価中にテストしたインタフェースは、インタフェース37個中15個である。

開発者テストは、指紋情報、ワンタイムパスワード等のインポートのインタフェースに関するテスト以外のテストについては、インタフェースの仕様を確

認するための十分なテストが実施されていることから、評価者テストは少なめのサイズであっても妥当であると判断した。上記インポートのインタフェースに関するテストは不十分だと判断したため、同じインタフェースのテストにおいて19個のテストを実施している

評価者独立テスト項目の選択基準として、下記を考慮している。

① 多くのインタフェースについて、入力パラメタの有効範囲、有効文字、入力なし、全角文字に関するエラー系のテストが実施されていないと判断し、テスト（セキュリティ機能の厳密なテスト）

② 開発者テストのテスト結果において、ログの確認による動作検証のみが行われているものがあったため、当該動作検証を確認する手段として画面インタフェースから動作を確認するためのテストを追加（開発者テスト方策の補足）

また、開発者テストで実施されたテストはサンプリングをせず全て実施した。

また、侵入テストについては、下記判断基準により、5個のインタフェースに関して12件実施した。

① 評価者が分析した潜在的脆弱性に基づき、侵入テストが必要と判断したものを実施（ワンタイムパスワード及びパスワードの不正な規定外の仕様の入力に関する自己保護、すべてのシステム管理者の削除）

d.結果

サンプリングテストに関しては、すべてのテスト結果が開発者の提示したテスト結果と同等であることを確認し、開発者の提供したテスト結果が妥当であると判断した。

また、独立テストに関しては、すべてのテスト結果が、機能仕様に記載された仕様、またはガイダンスに記述されている内容に沿ったものであることからTOEの仕様が妥当であると判断した。

また、侵入テストに関しては、すべて悪用不能脆弱性であることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本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。

3 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
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、ST及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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保証コンポーネントに対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_INT.1.1E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が正しく記述されていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、TOE参照、TOE概要、及びTOE記述が相互に一貫していること確認している。
ASE_CCL.1.1E	評価はワークユニットに沿って行われ、CCの適合主張の有効性を確認している。
ASE_SPD.1.1E	評価はワークユニットに沿って行われ、セキュリティ課題が明確に定義されていることを確認している。
ASE_OBJ.2.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針が明確に定義されていることを確認している。
ASE_ECD.1.1E	評価はワークユニットに沿って行われ、CCを参照しない要件の明示が必要である根拠が示されていること、それらの要件はCCの要件と同様のスタイルと詳細度で記述されていること、及びそれらの要件は評価可能であることを適切にサポートする根拠が示されていることを確認している。
ASE_ECD.1.2E	評価はワークユニットに沿って行われ、既存のコンポーネントを使用して、提示された拡張機能コンポーネントが明らかに表現できないことを確認している。

ASE_REQ.2.1E	評価はワークユニットに沿って行われ、SFR、SARは明確に、曖昧さなく十分に定義され、また内部的に一貫していること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がどのように各SFRを満たすかを示していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がTOE概要及びTOE記述と一貫していることを確認している。
ライフサイクルサポート	**適切な評価が実施された。**
ALC_CMC.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ALC_CMS.2.1E	評価はワークユニットに沿って行われ、TOEの構成リストが管理され、構成要素が一意に識別可能なことを確認している。
ALC_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
開発	**適切な評価が実施された。**
ADV_FSP.2.1E	評価はワークユニットに沿って行われ、機能仕様にTSFが完全に表現されていること、機能仕様にすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていることを確認している。
ADV_FSP.2.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_TDS.1.1E	評価はワークユニットに沿って行われ、TOE設計にてすべてのサブシステムが記述され、各サブシステムの特性が識別されていることを確認している。
ADV_TDS.1.2E	評価はワークユニットに沿って行われ、TOE設計にすべての機能要件が含まれ、具体化されていることを確認している。

ADV_ARC.1.1E	評価はワークユニットに沿って行われ、アーキテクチャ設計に自己保護、ドメイン分離、非バイパス性が記述され、TSFが保護されていることを確認している。
ガイダンス文書	**適切な評価が実施された。**
AGD_OPE.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しており運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を記述してあることを確認している。
AGD_PRE.1.1E	評価はワークユニットに沿って行われ、準備手続きがTOEのセキュアな準備を記述し、STの運用環境のITセキュリティ方針に従った環境が構築可能であることを確認している。
AGD_PRE.1.2E	評価はワークユニットに沿って行われ、準備手続きを元に評価者がセキュアにTOEと準備環境を構築可能なことを実行し確認している。
テスト	**適切な評価が実施された。**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテスト項目が正確にTFSIと関連付けられていることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。

ATE_IND.2.2E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_VAN.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
AVA_VAN.2.2E	評価はワークユニットに沿って行われ、潜在的脆弱性を識別するために公知の情報源に関する脆弱性探索を実施している。
AVA_VAN.2.3E	評価はワークユニットに沿って行われ、TOEの潜在的な脆弱性を識別するために、ガイダンス証拠資料、機能仕様、TOE設計、及びセキュリティアーキテクチャ記述を使用して、TOEの独立脆弱性分析を実施している。
AVA_VAN.2.4E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

本報告書で使用された用語を以下に示す。

FAサーバ	ユーザ情報と指紋情報を管理しユーザの識別と指紋認証を行うサーバ。
指紋認証ユニット	指紋を入力するスイープ型指紋センサユニット。周波数分析方式を採用している。
EVE FAログオン画面	指紋認証のログオンを案内する画面。ログオン先、ユーザ名、及び許可時におけるワンタイムパスワードの入力が可能。
ランダム文字列	指紋認証後Windowsにログオンするために TOEが発行する文字列。誰も閲覧することができない。
Windows ログオンパスワード	Windowsドメインにパスワードでログオンするユーザを認証するパスワード。
管理者パスワード	管理ツールを起動時、指紋情報が未登録または登録済みの指が使えない時、指紋認証ユニットが使えない時など、指紋認証機能を使えないとき管理者を認証するため使用するパスワード。
ワンタイムパスワード	有効使用回数あるいは有効期限を制限し一時的に権限を与えるため発行するパスワード。Windowsのログオンまたは FAユーティリティの起動時とTOEのアンインストール時に使われる。 Windowsのログオン時には、ユーザの指紋情報が未登録または登録済みの指が使えない時、指紋認証ユニットが使えない時など、指紋認証機能を使えないときを救済するため使用する。 ネットワーク上にてパスワードの暴露を防止する目的で、通信の度にパスワードが異なる値にする時の用語と異なる。
ユーザ情報	TOEにてユーザを管理するために用いる情報でありユーザ識別

	情報（ユーザ名、ログオン先)、Windowsログオンパスワード、ワンタイムパスワード、管理者パスワード、グループ情報、権限情報、指紋情報コード等からなる。
指紋情報	指紋情報コードで識別され指紋特徴量（参照テンプレート）を管理する情報であり登録者名、指紋認証ユニット名、作成/更新日、認証レベル、登録された指の指紋特徴量（参照テンプレート）からなる。
指紋特徴量（サンプル）	指紋認証ユニットで読み取り、抽出した指紋の特徴を示す情報。
指紋特徴量（参照テンプレート）	登録時に指紋から抽出された指紋特徴量（サンプル）より構成され、指紋情報コードで識別されTOEに保存され照合に使われる。
照合 (Verification)	利用者が登録者と一致することを検証するために、提示されたバイオメトリックスサンプルを参照テンプレートと比較すること。
他人受入（False Acceptance）	指紋認証システムが、誤って個人を識別したり、提示された識別情報に対して他人詐称者を間違って照合したりすること。
他人受入率(False Acceptance Rate : FAR）	他人詐称者を間違って照合する確率。下記のように表現できる。 FAR ＝ 他人受入の場合の数 ／ 他人詐称者が照合を試みた回数
本人拒否率(False Rejection Rate : FRR）	登録者が提示した正当な指紋情報の照合に失敗する確率。下記のように表現できる。 FRR ＝ 本人拒否の場合の数／ 登録者本人が照合を試みた回数
他人詐称者 (Impostor)	指紋認証システムに対して、認証情報に関する偽の提示をすることにより、正当な登録者として通過しようとする人。
認証レベル	正しく指紋入力を行っても、個人差により指紋情報の照合が成功しない場合がある。認証レベルは、指紋認証時の認証の厳しさを表したもの。 TOEにおいては「非常に厳しい」から「非常に緩やか」まで5段階で指定が可能。認証レベルを緩やかにすれば、本人拒否率(FRR)は低下するが他人受入率(FAR)は高くなる。

6 参照

[1] 指紋認証ソフトウェア EVE FA セキュリティターゲット バージョン 1.09（2008年5月15日）株式会社ディー・ディー・エス

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] 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19年5月 独立行政法人 情報処理推進機構 CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 3.1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 3.1 September 2006 CCMB-2006-09-003

[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1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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2: セキュリティ機能要件 バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-002 (平成19年3月翻訳第1.2版)

[10] 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: セキュリティ保証要件 バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-003 (平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 September 2006 CCMB-2006-09-004

[12] 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1版 2006年9月 CCMB-2006-09-004 (平成19年3月翻訳第1.2版)

[13] 指紋認証ソフトウェア EVE FA v2.00 評価報告書 第2版 2008年5月22日 株式会社電子商取引安全技術研究所 評価センター