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

発行　　2008 年　5 月 15 日

株式会社　ディー・ディー・エス

DDS
DIGITAL DEVELOPMENT SYSTEMS

目次

変更履歴

変更日	バージョン	変更理由
2007-9-18	1.0	初版発行
2007-10-16	1.1	所見報告及び内部見直しの結果を反映
2007-10-23	1.2	所見報告及び内部見直しの結果を反映
2007-12-19	1.3	所見報告及び内部見直しの結果を反映
2007-12-21	1.4	所見報告及び内部見直しの結果を反映
2008-2-29	1.5	所見報告及び内部見直しの結果を反映
2008-3-4	1.06	内部見直しの結果を反映及びバージョン番号改訂
2008-3-31	1.07	内部見直しの結果を反映
2008-4-25	1.08	所見報告による見直しの結果を反映
2008-5-15	1.09	所見報告による見直しの結果を反映

1. ST 概説

本章では、 ST 参照、TOE 参照、TOE 概要、及び TOE 記述について記述する。

1.1 ST 参照

ST の識別情報を以下に記述する。

ST タイトル	指紋認証ソフトウェア EVE FA セキュリティターゲット
ST バージョン	1.09
ST 発行者	株式会社 ディー・ディー・エス
ST 発行日	2008 年 5 月 15 日

1.2 TOE 参照

TOE の識別情報を以下に記述する。

TOE タイトル	指紋認証ソフトウェア EVE FA
TOE バージョン	2.00
TOE 発行者	株式会社 ディー・ディー・エス

1.3 TOE 概要

1.3.1. TOE種別及び主要セキュリティ機能

本TOE は、Windows システム向け指紋認証ソリューションを提供する、指紋認証システムを制御するソフトウェアである。Active Directoryによってドメインのコンピュータにパスワード(Windowsログオンパスワード)でクライアントPCからログオンするWindowsシステムにおいて、識別・認証機能を強化するためにTOEが導入される。TOE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分散型TOEである。

クライアントPCからユーザがログオン時、TOEはユーザ識別を行い指紋の入力を求める。TOE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、TOEはActive Directory にWindowsログオンパスワードでログオンする。

本STでは、TOEのセキュリティ機能は以下の機能である。

(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ST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 に示す。

FAR:他人受入率	FRR:本人拒否率
0.001%以下	0.1%以下

注)認証レベルは標準的な条件での値である。

表 1 1指3回登録時の他人受入率/本人拒否率(参考値)

1.3.2. TOE利用環境

パスワードによる識別・認証方式では、安全な識別・認証サービスを提供するため必要なパスワードポリシーを全ユーザに強制し維持する必要があるがユーザにとってその負担は大きい。その結果、パスワード漏洩や強度不足のパスワードが使用されるリスクがある。

TOE は以下のハードウェア及びソフトウェアを既存のシステムに追加し識別・認証機能の強化を図る。

1)クライアントPCへの追加

①指紋認証ユニット(ハードウェア)の追加

②Windowsログオン画面に代わる、指紋によるログオンを行うソフトウェア(TOE)の追加。

TOEのインストールにより、クライアントPCのWindowsのログオン管理をおこなっているGina(Graphical Identification and Authentication)ライブラリをTOEのコンポーネントにリプレースする。その結果、指紋によるログオン制御機能を持つEVE FAログオン画面からのログオン操作が強制される。

2)FAサーバ及びデータベースサーバの追加

1.3.2.1 TOE運用環境

1) TOEの運用構成

TOEの運用時の構成を図 1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既存のWindowsシステムに追加するコンポーネントを示す)

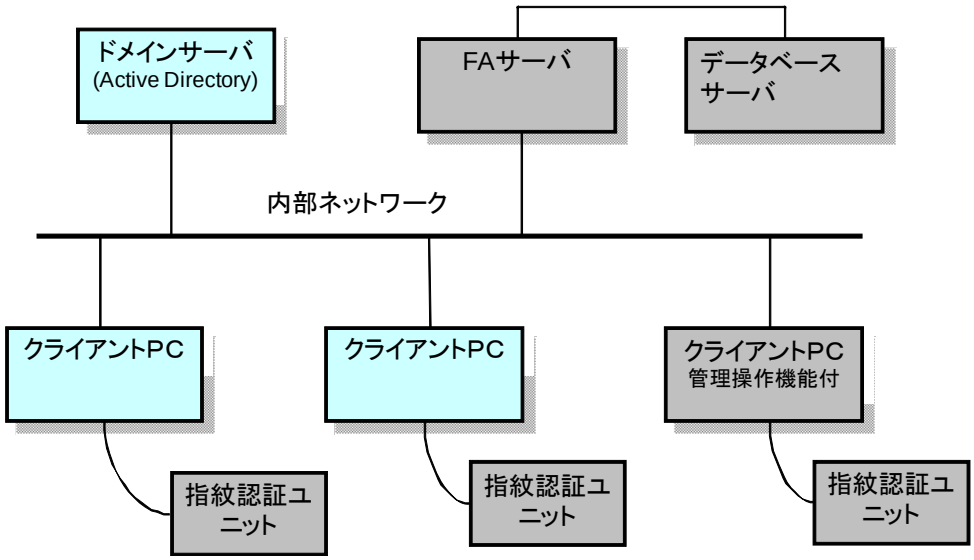

図 1 TOEの運用構成

【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。

2)TOEの運用時の物理的環境

(1)クライアントPC及び指紋認証ユニットは一般的なオフィスに置かれる。またクライアントPCは、TOE以外のソフトウェアも搭載され動作する。

(2) FAサーバと、クライアントPC間は、Windowsシステムで構築されたネットワーク環境であって、インターネットとはファイアウォールで接続された内部ネットワークである。

(3)FAサーバ及びデータベースサーバは、物理的なアクセス制御と入退出管理がされた環境に設置される。FAサーバとデータベースサーバの接続ケーブルは内部ネットワークと分離され、情報漏洩しないように物理的に保護される。またFAサーバ にはTOE及び本STに記述するソフトウェア以外は搭載しない。

3)TOEの使用方法

【ユーザ登録】

権限を持つ管理者は、ユーザ識別情報(ユーザ名及びログオン先)、Windowsログオンパスワードを TOEに登録する。また指紋登録するユーザに対し、ワンタイムパスワードをTOEで生成後、安全な方法でユーザに通知する。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。

ユーザはクライアント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)、TOEが生成したワンタイムパスワードは、ユーザ識別情報と関係付けられており、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確認し、本人と認める(認証)。その後TOEは登録されたWindowsログオンパスワードをActive Directoryに送りWindowsシステムにログオンする。

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。指紋情報の登録操作を、クライアントPCから行うと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。
TOEは権限を持つ管理者の操作により、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、誰も閲覧ができない。この結果指紋認証以外でWindowsシステムにログオンできずシステムのセキュリティは強化される。

【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いる。
指紋情報コードから登録された指紋情報の指紋特徴量(参照テンプレート)と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をActive Directoryに送りWindowsシステムにログオンする。

【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FAユーティリティにログオン後、指紋情報(指紋特徴量)を登録または変更及び削除をできる。また既に指紋情報を登録しているユーザが、指紋情報コードで識別された登録済み指紋情報を選択し、指紋認証ユニットで指紋入力し本人であることを確認できると、ユーザ情報と関係づけることができる。

【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のほか、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。

1.3.2.2. ハードウェア構成

表 2 にTOEの動作に必要なハードウェアを示す。

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
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

表 2 TOEが動作するハードウェア

1.3.2.3. ソフトウェア構成

TOEの動作に必要なソフトウェアを表 3に示す。

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

表 3 TOEの動作に必要なソフトウェア

1.4 TOE 記述

TOEの利用者役割、TOEの論理的範囲、及びTOEの物理的範囲について記述する。

1.4.1. TOEのユーザと役割

このSTでは、TOEの利用に関する関係者を以下の用語で表現する。

ユーザは TOE に登録され、TOE を利用する人である。

一般ユーザはクライアント PC から Windows ドメインにログオンするために TOE に登録された役割を指す。

管理者はユーザ情報及び指紋情報を管理するために TOE に登録された役割を指す。

システム管理者は、すべてのユーザ情報及び指紋情報の変更管理ができる。

TOE をインストール後、運用開始時点ではシステム管理者のユーザ情報がビルドイン登録されており、その情報を利用しシステム管理者がログオンして自身のユーザ情報を変更後他のユーザのユーザ情報を設定する。

システム管理者は、全ユーザ情報の変更管理ができると共に、ユーザ情報についてコンピュータ別またはコンピュータ内グループなどの範囲でユーザの変更管理権限を運用管理者に与えること(権限の委任)ができる。権限を委任された運用管理者は許可された範囲のユーザについて、ユーザ情報の変更管理ができる。またシステム管理者は、ユーザ情報の閲覧に限定した権限(参照管理)を運用管理者に与えることもできる。

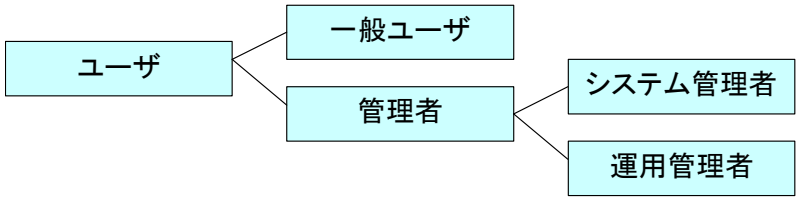

図 2　TOEのユーザの表現

TOE はシステム管理者、運用管理者及び、認証されたユーザを役割として識別する。

1.4.2. TOEの物理的範囲

(1) ソフトウェア構成

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

これらのコンポーネントを搭載した指紋認証システムの物理構成と TOE の境界を図 3 に示す。グレーの部分は TOE を表す。

【クライアント PC】

クライアント PC において TOE のコンポーネントは以下の機能を実行する。

①クライアントプログラム:

指紋認証ユニットとのインタフェース制御、FA サーバとの転送情報の通信暗号処理及び、FA ユーティリティのインタフェース、システムログオン機能を提供する。

システムログオン機能はシステムログオン画面を表示しログオンに必要な情報と指紋認証ユニットの操作を案内する。Windows のログオン画面を制御する Gina を TOE のライブラリで置き換える。

②ツールプログラム:

管理ユーティリティのインタフェースでユーザとの対話機能を提供する。

またクライアント PC 上の OS 及び指紋認証ユニットは TOE の範囲外である。

【FA サーバ】

FA サーバにおいて TOE のコンポーネントであるサーバプログラムは以下の機能を実行する。

①ユーザ識別・認証機能:

ユーザ情報の識別及び指紋特徴量(サンプル)とユーザ情報に関係付けされた指紋情報の指紋特徴量(参照テンプレート)との照合処理をする。またワンタイムパスワードまたは管理者パスワードによる識別・認証を行う。

②通信暗号処理:

クライアント PC との転送情報の通信暗号処理をする。

③ユーザ情報管理機能:

管理者の識別・認証と権限に応じユーザ情報の変更管理または参照管理をする。

④指紋情報管理機能:

指紋情報を管理する。

⑤データベースアクセス制御:

データベースとの処理(ユーザ情報、指紋情報の書き込みと読み出し)

⑥監査機能:

監査事象の管理及びデータベースへの保存処理

⑦コマンドライン処理:

FA サーバの上でコマンドラインにより、ユーザ情報の管理処理をする。

また FA サーバ上の OS 及びデータベース機能は TOE の範囲外である。

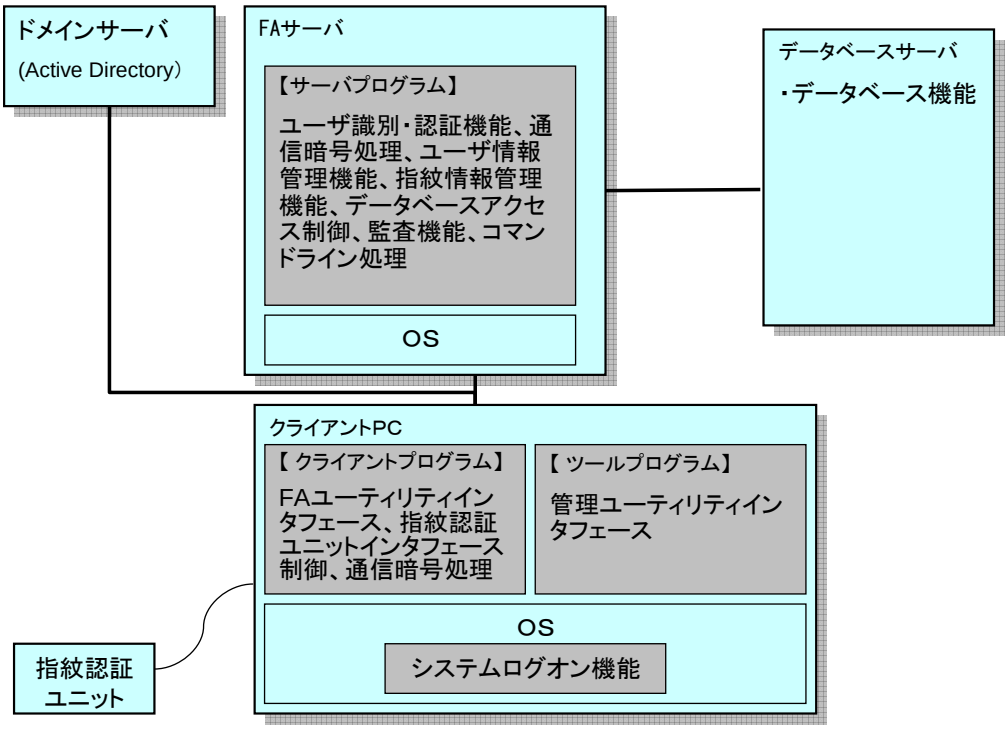

図 3　指紋認証システムの物理構成と TOE の境界

(2)ガイダンス文書

EVE FA ガイダンス資料 (D080630)がソフトウェアと共に提供される。

1.4.3. TOEの論理的範囲

1.4.3.1. TOEによって提供される基本機能

(1)Windows ドメインへのログオンの代行機能

TOEは、Windowsシステムのドメインサーバ(Active Directory)が管理するID・パスワード(Windowsログオンパスワード)の複製を持ち、一般ユーザのWindowsドメインへのログオンを代行する。

(2)Windows ログオンパスワードの更新機能

TOE は、一般ユーザの Windows ログオンパスワードを更新する機能を持つ。Active Directory での更新権限を持つ者がこの機能を使用した場合には、Windows ログオンパスワードは Active Directory でも同期をとって更新できる。更新方法として、新パスワードの設定、ランダム化の指定の二種類を提供する。

(3)FA サーバとクライアント PC 間の内部ネットワークの通信機能

内部ネットワークで情報転送を行う。

(4)データエクスポート機能

ユーザ一覧取得機能　一般ユーザ情報をコマンドラインでファイルに出力する。

ログエクスポート機能　監査証跡をログビューアまたはコマンドラインでファイルに出力する。

1.4.3.2. TOEによって提供されるセキュリティ機能

このSTではTOEにて認証を行い、Windowsドメインにログオンするために TOE内に保存されたWindows ログオンパスワードをActive Directoryに送るまでのセキュリティ対策を扱う。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保護は、Windowsシステムが分担し、TOEによるセキュリティ対策の範囲外である。Windowsログオンパスワード及びTSFデータを資産とし、許可された一般利用者または権限を持つ管理者以外のユーザによる権限外暴露及び改ざんを保護するTOEのセキュリティ機能を以下に示す。

(1)Windows ログオン代行時の識別・認証機能

TOE は、一般ユーザの識別・認証を行い、識別・認証に成功した場合にのみ、当該一般ユーザの Windows ログオンパスワードの読み出しを許可する。FA サーバから読みだした Windows ログオンパスワードは、クライアント PC 内の TOE によって Active Directory に自動的に送信される。クライアント PC －Active Directory 間の Windows ログオンパスワードは、Windows システムによって保護され、TOE によるセキュリティ対策の範囲外である。

TOE は、このための認証方式として、指紋認証、ワンタイムパスワード認証の二種類を提供する。

(2)ユーザ情報及び指紋情報の管理、及び TOE の構成設定の維持機能

TOEは、一般ユーザの識別・認証を行い、識別・認証に成功した場合にのみ、本人の指紋情報の管理(追加登録、更新、削除)を許可する。TOEは、このための認証方式として、指紋認証、ワンタイムパスワード認証の二種類を提供する。

TOEは、管理者を識別・認証し、識別認証に成功した場合に、その管理者に付与されている権限の範囲内の管理操作を許可する。TOEは、このための認証方式として、指紋認証、パスワード認証の二種類を提供する。

管理者にはシステム管理者、運用管理者の二種類が存在し、管理操作の対象は、ユーザ情報の管理、指紋情報の管理、TOEのふるまいの管理の3つに大別できる。以下に管理操作の概要を記す。

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。運用管理者が委任された権限は権限情報として TOE で管理され管理者の属性情報になる。権限情報は、管理者に許可された一般ユーザの管理範囲(コンピュータ名、コンピュータ内のグループなど)及び許可された変更管理権限からなり、管理者は権限の範囲内で、ユーザ情報の操作が可能である。

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。

またTOEは製品として持つ機能を制限して運用される。以下の機能制限は運用前にシステム管理者が設定し、運用中も変更してはならない。

・クライアントキャッシュ機能無効設定

モバイル使用などFAサーバと接続せずローカルログオンするため、クライアントPCに指紋情報をキャッシュする、クライアントキャッシュ機能は本TOEでは使用しない。

・Windowsログオンパスワードを直接入力しWindowsドメインにログオンすることの禁止設定

・ログ機能を有効設定(ログ削除しない)

「ログを保存しない」、「ログ保存期間指定」は本TOEでは使用せずログを削除しない状態で使用する

(3)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及び、指紋情報を暴露から防止する。

(4)監査機能

TOE のセキュリティ監査事象を記録・維持し、利用者が監査証跡の閲覧と管理(削除)を行える機能を提供する。

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

以下に(1)、(2)で使用する各認証方式の特徴を説明する。

・指紋認証

指紋の濃淡情報からTOEは指紋特徴量(サンプル)を抽出し、ユーザ識別情報から関係付けられた該当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。

・ワンタイムパスワード認証

一般ユーザ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においてユーザを認証する。

この様なケースでシステム管理者または該当する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該当するユーザ情報と関係づける。

一般ユーザはワンタイムパスワードによりWindows にログオン後、ワンタイムパスワードの有効範囲内で

FA ユーティリティを起動し、ワンタイムパスワードによる認証後、指紋認証が可能なように指紋情報(指紋特徴量)を登録することが期待される。

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。

(注)管理者に対しシステム管理者がワンタイムパスワードを設定できる機能をTOEは有するが、運用でワンタイムパスワードを管理者の認証のため設定することはしない。

・パスワードによる識別・認証機能

一般ユーザは、Windowsドメインにログオン時に指紋認証以外、直接Windowsログオンパスワードを入力しActive Directoryに送る機能を持つ(この機能は本TOEでは使用しない)。

パスワードは、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指紋登録前に管理ユーティリティを使用する管理者を認証する。

②管理ユーティリティを使用する管理者が登録した指が全て使用できない場合に、管理者を認証する(この場合、Windows ログオンにあたってはワンタイムパスワード認証が必要である)。

③指紋認証ユニットが使えない場合でも管理者を認証する(コマンドラインによる操作を含む)。

パスワードは権限を持つ管理者によって事前に登録されている必要がある。

2. 適合主張

2.1. CC 適合主張

本ST 及びTOE のCC 適合主張は、 以下のとおりである。

ST とTOE が適合を主張するCC のバージョン :

パート1: 概説と一般モデル 2006年9月 バージョン3.1 翻訳第1.2版

パート2: セキュリティ機能コンポーネント 2006年9月 バージョン3.1 翻訳第1.2版

パート3: セキュリティ保証コンポーネント 2006年9月 バージョン3.1 翻訳第1.2版

CC パート2 に対するST の適合 : CC パート 2 拡張

CC パート3 に対するST の適合 : CC パート3 適合

2.2. PP 主張、パッケージ主張

2.2.1. PP主張

本STが適合しているPPはない。

2.2.2. パッケージ主張

EAL2適合

3. セキュリティ課題定義

本章では脅威、組織のセキュリティ方針、前提条件について記述する。
本TOEではWindowsシステムのログオンパスワードを権限外の改ざんと暴露の脅威、及び関連し必要なユーザ情報と指紋情報の権限外改ざんと暴露の脅威を想定する。
指紋認証の精度については評価の範囲外として、指紋認証メカニズム自体の精度に関する脅威を想定から除外している。指紋認証精度(他人受入率:FAR)は、1.3.1.節の参考値を元に、TOEの使用者自身により判断されたい。

3.1 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。

3.2 組織のセキュリティ対策方針

組織のセキュリティ対策方針は無い。

3.3 前提条件

TOEの運用にあたり、使用者が守らなければならない条件を記述する。

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。

4. セキュリティ対策方針

本章では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及び、セキュリティ対策方針根拠について記述する。

4.1. TOE のセキュリティ対策方針

O.I&A

TOEはFAサーバの利用を許可された一般ユーザを識別・認証しなければならない。

O.I&A_ADMINI

TOE は、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権限を持つユーザを識別・認証しなければならない。

O.ENROLL_AUTH

TOE は、TOE により識別・認証された一般ユーザが、自分自身の指紋情報に限り管理(登録・変更・削除)をできることを保証しなければならない。

O.ADMINI_RIGHT

TOE は、TOE の構成設定の変更をシステム管理者に制限し TOE の構成設定を維持しなければならない。TOE は、ユーザ情報及び指紋情報の管理能力を複数の管理者に分割し許可範囲内の操作に制限し、許可範囲外の変更を防止することを保証しなければならない。

O.FALLBACK

TOE は指紋認証が利用できないユーザに対し、代替えの認証機能を提供しFA サーバを使用できるようにしなければならない。

O.AUDIT

TOEはバイオメトリックス識別・認証の不備をつく不正な認証の試みを検出しなければならない。
TOEは管理者パスワードまたはワンタイムパスワードによる不正な認証の試みを検出しなければならない。

O.COMM_PROTECT

TOE はクライアント PC と FA サーバ間の通信路からユーザ情報及び指紋情報の権限外の暴露及び改ざん防止を保証しなければならない。

4.2. 運用環境のセキュリティ対策方針

OE.TAMPER

システム管理者は TOE の構成を維持し、TOE の改ざんまたは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などを防止するセキュリティ対策を、実施しなければならない。

OE.SERVER_PROTECT
TOE が動作する FA サーバとデータベースサーバ、及び両者間の接続ケーブルは、物理的なアクセス制御がされた区画に設置されシステム管理者の監督下以外の入退出ができない環境制御が行われなければならない。

OE.DEDICARED
FA サーバには TOE とその関連するソフトウェア以外を稼働させず専用的に使用されなければならない。

OE.NO_EVIL
システム管理者には指紋認証システムの運用について十分な能力を持ち、知識に精通し信頼するものを任命する。またシステム管理者は委任する運用管理の責任範囲を明確にし、信頼できる人物に権限を委任し操作上の注意義務と責任を周知しなければならない。

OE.OBJECTIVE
管理者はユーザに指紋認証の特徴を十分に説明し、指紋登録時に指紋認証メカニズムを弱めるような意図を持った行動はしないように周知しなければならない。

OE.PASSWORD
管理者パスワード及びワンタイムパスワードは他人に漏洩しないように扱わなければならない。
管理者パスワードは十分強度のあるパスワードを設定する。

4.3. セキュリティ対策方針根拠

4.3.1. 必要性

脅威、組織のセキュリティ方針、及び前提条件に対するセキュリティ対策方針の対応関係を表 4 に示す。この表からセキュリティ対策方針が少なくても 1つ以上の脅威、組織のセキュリティ方針、及び前提条件に対応している。

セキュリティ課題 / セキュリティ対策方針	T.ILLEGAL_LOGON	T.ADMINI_RIGHT	T.COMM_DISC	T.FA_NOUSE	A.TAMPER	A.SERVER_PROTECT	A.DEDICARED	A.NO_EVIL	A.OBJECTIVE	A.PASSWORD
O.I&A	✓									
O.I&A_ADMINI		✓								
O.ENROLL_AUTH		✓								
O.ADMINI_RIGHT		✓								
O.FALLBACK				✓						
O.AUDIT	✓	✓		✓						
O.COMM_PROTECT			✓							
OE.TAMPER					✓					
OE.SERVER_PROTECT						✓				
OE.DEDICARED							✓			
OE.NO_EVIL								✓		
OE.OBJECTIVE									✓	
OE.PASSWORD										✓

表 4 脅威、組織のセキュリティ方針、前提条件とセキュリティ対策方針の対応関係

4.3.2. 脅威に対する十分性

各脅威がセキュリティ対策方針で対抗できることを説明する。

各脅威に対して攻撃者を明示し、想定される攻撃方法に対抗するための有効な対策を示し、それがすべて満たされることで脅威に対抗できる十分な対策であることを示す。

(1)T.ILLEGAL_LOGONに対して許可されていないユーザが

O.I&A により、一般ユーザを識別・認証し許可されていないユーザがFAサーバを不正利用しないことを保証する。

O.AUDITにより識別・認証の不備をつく不正な試みを検出できる。

このためこれらの対策方針が実施されれば脅威に対抗できる。

(2)T.ADMINI_RIGHTに対して権限を持たないユーザが

O.I&A_ADMINIにより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権限を持つユーザを識別・認証し許可されていないユーザが管理操作をしないことを保証する。

O.ENROLL_AUTHによりTOEは、TOEにより識別・認証された一般ユーザが自分自身の指紋情報に限り管理をできることを保証する。

O.ADMINI_RIGHTにより、TOEの構成設定変更能力をシステム管理者に制限することで権限のないユーザがTOEの構成設定を変更できないことを保証する。またユーザ情報及び指紋情報の管理能力を複数の管理者に分割し許可範囲内のユーザ管理に制限し許可範囲外の変更を防止することを保証する。これらにより許可されない管理操作によるリスクを緩和する。

しかし識別・認証の不備をつく不正な認証の試みも想定される。

O.AUDITにより識別・認証の不備をつく不正な試みを検出できる。

このためこれらの対策方針が実施されれば脅威に対抗できる。

(3) T.COMM_DISC に対して O.COMM_PROTECT は、脅威に対する直接的な対策方針であるため対策方針が実施されれば脅威に対抗できる。

(4) T.FA_NOUSE に対し O.FALLBACK は、指紋認証手段を利用できないユーザに、代替えの認証機能を提供し FA サーバを使用でき、また O.AUDIT により代替えの認証機能による認証を破ろうとする試みを検出できるため、脅威に対抗できる。

4.3.3. 組織のセキュリティ方針に対する十分性

この項は該当するものはない。

4.3.4. 前提条件に対する十分性

各前提条件がセキュリティ対策方針により実現できることを説明する。

(1) A.TAMPERが OE.TAMPERにより実現できる理由

ログオン成功後クライアントPC において、TOE の権限外改ざんまたは、認証システムを危殆化するハードウェア、ソフトウェアの権限外改造を防止するセキュリティ対策をシステム管理者に求める対策方針によって前提条件の想定は満たされている。

(2)A.SERVER_PROTECT が OE.SERVER_PROTECT により実現できる理由

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、及び両者の接続ケーブルは物理的なアクセス制御がされた区画に設置されシステム管理者の監督下以外で入退出が制限されるため、FA サーバ及びデータベースに保存された情報への直接アクセスまたは TOE の改ざんによるこれらの暴露、改ざんは阻止され対策方針によって前提条件の想定は満たされている。

(3)A.DEDICARED が OE.DEDICARED により実現できる理由

TOE が動作するFA サーバには評価されたソフトウェア以外を稼働させないことにより、TOE への干渉を防止できるため対策方針により前提条件は満たされている。

(4)A.NO_EVIL が OE.NO_EVIL により実現できる理由

システム管理者は指紋認証システムの運用について十分な能力を持ち知識に精通し、信頼するものが任命されるためシステム管理者に関する前提条件を満たす。また適切な運用管理の権限委任がさ

れると、運用管理者は操作可能な範囲が TOE の機能により制限され、権限を悪用する可能性を減らすことができる。運用管理者に権限を委任された操作はシステム管理者から操作上の注意義務と責任が周知されかつ信頼できる人物が任命されるため運用管理者に関する前提条件を満たし、従って前提条件は満たされている。

(5)A.OBJECTIVE が OE.OBJECTIVE により実現できる理由

指紋認証メカニズムの特徴をユーザに十分に説明し、ユーザ自身が指紋登録時に指紋認証メカニズムを弱めるような指紋登録はしないことを周知させる対策方針により前提条件は満たされている。

(6)A.PASSWORD が OE.PASSWORD により実現できる理由

指紋認証が使用できない場合、管理者パスワードの使用に関して、他人への漏洩を防止する対策方針により前提条件は満たされている。また指紋認証が使用できない場合、一般ユーザは、ワンタイムパスワードの他人への漏洩を防止する対策方針により前提条件は満たされている。

5. 拡張コンポーネント定義

5.1. 拡張機能コンポーネント

CCパート2に定義されたセキュリティ機能コンポーネントの拡張コンポーネントとしてFMT_SAC.1を定義する。このコンポーネントはFMT(セキュリティ管理)クラスの追加コンポーネントとして定義される。

セキュリティ属性有効回数制限付き許可(FMT_SAC)

ファミリのふるまい

このファミリは、セキュリティ属性の有効性に対して回数制限を実施する能力に対応する。

コンポーネントのレベル付け

FMT_SAC:セキュリティ属性有効回数制限付き許可	1

FMT_SAC.1 使用回数制限付き許可は、許可利用者が特定のセキュリティ属性について有効使用回数を特定するための権限を提供する。

管理: FMT_SAC.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:

· 有効使用回数制限付き許可がサポートされるセキュリティ属性のリストを管理すること;

· 使用回数が有効使用回数制限を過ぎたときにとられるアクション。

監査: FMT_SAC.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:

· 基本: 属性に対する使用回数制限の特定;

· 基本: 属性の有効使用回数制限を過ぎたときとられるアクション。

FMT_SAC.1使用回数制限付き許可

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SAC.1.1 TSF は、[割付: 使用回数制限がサポートされるセキュリティ属性のリスト]に対する有効使用回数を特定する能力を、[割付: 許可された識別された役割]に制限しなければならない。

FMT_SAC.1.2 これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する使用回数制限を超過後、[割付: 各々のセキュリティ属性に対してとられるアクションのリスト]を行えなければならない。

6. セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件、及びセキュリティ要件根拠を記述する。

6.1. セキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。 なお拡張機能コンポーネントを除いてセキュリティ機能要件は、 CC Part 2 に規定のセキュリティ機能要件から、引用する。

FAU_GEN.1 監査データ生成

下位階層: なし

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1

TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 指定なし]レベルのすべての監査対象事象; 及び

c) [割付: 表 5 個別に定義した監査事象]。

TOE にて選択した機能要件	CC パート2で規定された監査対象	監査事象
FAU_GEN.1	予見される監査対象事象はない。	
FAU_SAR.1	· 基本: 監査記録からの情報の読み出し。	ログビューアの起動
FAU_STG.1	予見される監査対象事象はない。	
FIA_UID.2	· 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; · 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	・指紋または管理者パスワードまたはワンタイムパスワード認証成功 ・指紋認証または管理者パスワードまたはワンタイムパスワード認証失敗の回数が閾値以上になった時
FIA_UAU.2	· 最小: 認証メカニズムの不成功になった使用; ·基本: 認証メカニズムのすべての使用。	・指紋または管理者パスワードまたはワンタイムパスワード認証成功 ・指紋認証または管理者パスワードまたはワンタイムパスワード認証失敗の回数が閾値以上になった時
FIA_UAU.5	· 最小: 認証の最終決定; · 基本: 最終決定でともに用いられた、各々の稼動したメカニズムの結果。	・指紋または管理者パスワードまたはワンタイムパスワード認証成功 ・指紋認証または管理者パスワードまたはワンタイムパスワード認証失敗の回数が閾値以上になった時
FIA_USB.1	・最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合; · 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗	無し
FIA_ATD.1	予見される監査対象事象はない。	
FDP_ACC.1	予見される監査対象事象はない。	
FDP_ACF.1	· 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 · 基本: SFP で扱われるオブジェクトに対す	

TOE にて選択した機能要件	CC パート2で規定された監査対象	監査事象
	る操作の実行におけるすべての要求。 ・ 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	
FIA_SOS.2	・ 最小: TSF による、テストされた秘密の拒否; ・ 基本: TSF による、テストされた秘密の拒否または受け入れ; ・ 詳細: 定義された品質尺度に対する変更の識別。	ワンタイムパスワードの発行時
FPT_ITT.1	予見される監査対象事象はない。	
FCS_COP.1	・ 最小: 成功と失敗及び暗号操作の種別。 ・ 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	無し
FCS_CKM.1	・ 最小: 動作の成功と失敗。 ・ 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	無し
FCS_CKM.4	・ 最小: 動作の成功と失敗。 ・ 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	無し
FMT_SMF.1	・ 最小: 管理機能の使用	管理ツール、FA ユーティリティの起動
FMT_SMR.1	・ 最小: 役割の一部をなす利用者のグループに対する改変; ・ 詳細: 役割の権限の使用すべて。	ユーザ識別情報、グループ情報の登録、改変、削除、インポート、権限情報の改変、削除
FMT_MSA.1	・ 基本: セキュリティ属性の値の改変すべて	ユーザ識別情報、グループ情報の登録、改変、削除、参照、インポート、権限情報の改変、削除
FMT_MSA.3	・ 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 ・ 基本: セキュリティ属性の初期値の改変すべて	ユーザ識別情報、グループ情報の登録、インポート
FMT_MTD.1(1)	・ 基本: TSF データの値のすべての改変	指紋情報、指紋情報コードの登録、改変、削除、インポート
FMT_MTD.1(2)	・ 基本: TSF データの値のすべての改変	指紋情報の登録、改変、削除
FMT_MTD.1(3)	・ 基本: TSF データの値のすべての改変	ワンタイムパスワードの生成、改変、削除
FMT_MTD.1(4)	・ 基本: TSF データの値のすべての改変	管理者パスワードの生成、改変、削除
FMT_MTD.1(5)	・ 基本: TSF データの値のすべての改変	監査記録の削除
FMT_SAE.1	・ 基本: 属性に対する有効期限の時間の特定; ・ 基本: 属性の有効期限切れによってとられるアクション。	ワンタイムパスワードの有効期限設定時
FMT_SAC.1	・ 基本: 属性に対する使用回数制限の特	ワンタイムパスワードの有効使用回

TOE にて選択した機能要件	CC パート2で規定された監査対象	監査事象
	定; ・ 基本: 属性の有効使用回数制限を過ぎたときとられるアクション。	数設定時
FMT_MOF.1	・基本: TSF の機能のふるまいにおけるすべての改変。	クライアントキャッシュ機能無効設定、Windows ログオンパスワードによる Windows ドメインにログオン禁止設定、ログ機能を有効設定(ログ削除しない)の改変時
FPT_STM.1	・ 最小: 時間の変更; ・ 詳細: タイムスタンプの提供。	無し OS のログで代行

表 5 個別に定義した監査事象

FAU_GEN.1.2

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: なし]

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_SAR.1 監査レビュー

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.1.1 TSF は、[割付: システム管理者]が、[割付: ユーザ識別情報、発生日時、事象種別、詳細情報]を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_STG.1 保護された監査証跡格納

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を[選択: 防止]できなければならない。

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

依存性: なし

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1 TSF は、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、各利用者に識別が成功することを要求しなければならない。

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSF は、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、各利用者に認証が成功することを要求しなければならない。

FIA_USB.1 利用者-サブジェクト結合

下位階層: なし

依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: グループ情報、権限情報]

FIA_USB.1.2 TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しけなければならない。:[割付: なし]

FIA_USB.1.3 TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: なし]

FIA_ATD.1 利用者属性定義

下位階層: なし

依存性: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付:グループ情報、権限情報]

FIA_UAU.5 複数の認証メカニズム

下位階層: なし

依存性: なし

FIA_UAU.5.1 TSF は、利用者認証をサポートするため、[割付: 表 6 の認証メカニズム]を提供しなければならない。

FIA_UAU.5.2 TSF は、[割付:表 6 の提供する認証内容]に従って、利用者が主張する識別情報を認証しなければならない。

認証メカニズム	提供する認証内容
ワンタイムパスワードメカニズム	指紋登録前のユーザを認証する。 登録した指が全て使用できないユーザを認証する。 指紋認証ユニットが使えない場合でユーザを認証する。
指紋認証メカニズム	Windows システムへのログオンまたは許可された管理操作を実行するためユーザを指紋認証により、認証する。
管理者パスワードメカニズム	許可された管理操作を実行するため、権限を持つ管理者を認証する。

表 6 認証メカニズムと提供する認証内容

FIA_SOS.2 TSF 秘密生成

下位階層: なし

依存性: なし

FIA_SOS.2.1 TSF は、[割付: 12 文字のアルファベットと数字の組み合わせ]に合致する秘密を生成するメカニズムを提供しなければならない。

FIA_SOS.2.2 TSF は、[割付: ワンタイムパスワードによる認証]に対し、TSF 生成の秘密の使用を実施できなければならない。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 TSF は、[割付: 表 7 に示す「サブジェクト」、「オブジェクト」、「サブジェクトとオブジェクト間の操作」]に対して[割付: FA アクセス制御 SFP]を実施しなければならない。

サブジェクト	ユーザを代行するプロセス
オブジェクト	Windows ログオンパスワードファイル
サブジェクトとオブジェクト間の操作	書込または、(Windows へログオンするため)読出し

表 7 FAアクセス制御SFPで制御されるサブジェクト、オブジェクト、操作

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

依存性: FDP_ACC.1 サブセットアクセス制御、FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 TSF は、以下の[割付: 表 8 に示すサブジェクト、オブジェクト及びサブジェクト、オブジェクトのセキュリティ属性]に基づいて、オブジェクトに対して、[割付: FA アクセス制御 SFP]を実施しなければならない。

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 表 9 の「操作の規則」]。

FDP_ACF.1.3 TSF は、次の追加規則、[割付: なし]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4 TSF は、[割付: なし]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

サブジェクト/オブジェクト	セキュリティ属性
サブジェクト:ユーザを代行するプロセス	グループ情報、権限情報
オブジェクト:Windows ログオンパスワードファイル	ユーザ識別情報、グループ情報

表 8 FAアクセス制御SFPで制御されるサブジェクト、オブジェクト及びサブジェクト、オブジェクトのセキュリティ属性

サブジェクトの処理	操作の規則	オブジェクトに対する操作
Windows ログオンパスワード書込処理	1) グループ情報より変更権限を持ち、権限情報よりシステム管理者の時、指定されたユーザ識別情報を持つオブジェクトに対し右の操作を許可。 2)グループ情報より変更権限を持ち、権限情報よりユーザ管理を許可された運用管理者の時、指定されたユーザ識別情報が許可された範囲内の場合オブジェクトに対し右の操作を許可。 3)上記の条件を満たさない場合書込を拒否。	(Windows へログオンのため)読出し 指定値の書込
Windows ログオンパスワードのランダム文字列書込処理	1) グループ情報より変更権限を持ち、権限情報よりシステム管理者の時、指定されたユーザ識別情報を持つオブジェクトに対し右の操作を許可。 2)上記の条件を満たさない場合書込を拒否。	(Windows へログオンのため)読出し 生成値を書込

表 9 FAアクセス制御SFPで制御されるサブジェクト、オブジェクト間の操作と操作の規則

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。:[割付:表 10 TSF によって提供される管理機能]

機能要件	管理対象（CC 定義）	管理機能
FIA_UID.2	・利用者識別情報の管理;	ユーザ情報の登録、改変、削除、インポート、参照 FMT_MSA.1
FIA_UAU.2	・管理者による認証データの管理; ・このデータに関係する利用者による認証データの管理;	指紋情報の登録、改変、削除、インポート、参照 FMT_MSA.1、FMT_MTD.1(1)
FIA_UAU.5	・認証メカニズムの管理; ・認証に対する規則の管理。	なし。認証メカニズムの変更や規則の管理はしないため。
FIA_USB.1	・許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 ・許可管理者は、サブジェクトのセキュリティ属性を変更できる。	サブジェクトのセキュリティ属性(権限情報)の管理 FMT_MSA.1
FIA_ATD.1	・もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし。追加のセキュリティ属性はないため。
FDP_ACC.1	予見される管理アクティビティはない。	
FDP_ACF.1	・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	セキュリティ属性の管理 FMT_MSA.1
FIA_SOS.2	・秘密の生成に使用される尺度の管理。	なし
FMT_MSA.1	・セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	なし。この要件自身が運用管理者の役割のグループを管理するため。
FMT_MTD.1(1)	・TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	権限情報の管理 FMT_MSA.1
FMT_MTD.1(2)	・TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし。全ての役割を要件で指定しているため。
FMT_MTD.1(3)	・TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	ユーザ識別情報、権限情報の管理 FMT_MSA.1
FMT_MTD.1(4)	・TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	ユーザ識別情報、権限情報の管理 FMT_MSA.1
FMT_MTD.1(5)	・TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし。システム管理者にのみ管理を許可しグループの概念はないため。
FMT_SAE.1	有効期限がサポートされるはずのセキュリティ属性のリストを管理すること; ・有効期限の時間が過ぎたときにとられるア	ワンタイムパスワードの生成 FMT_MTD.1(3)

機能要件	管理対象（CC 定義）	管理機能
	クション。	
FMT_SAC.1	· 有効使用回数制限付き許可がサポートされるセキュリティ属性のリストを管理すること; · 使用回数が有効使用回数制限を過ぎたときにとられるアクション。	ワンタイムパスワードの生成 FMT_MTD.1(3)
FMT_SMF.1	予見される管理アクティビティはない。	
FMT_MOF.1	· TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること;	ユーザ識別情報、権限情報の管理 FMT_MSA.1
FMT_SMR.1	· 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	なし。システム管理者にのみ管理を許可しグループの概念はないため。
FAU_GEN.1	予見される管理アクティビティはない。	
FAU_SAR.1	· 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	なし。システム管理者に管理を許可しグループの概念はないため。
FAU_STG.1	予見される管理アクティビティはない。	
FPT_STM.1	· 時間の管理。	なし。OS にて変更され、TOE にそのインタフェースはないため。
FPT_ITT.1	· TSF が(その改変から)保護すべき改変の種別の管理; · TSF の異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムの管理。	なし。保護する種別やメカニズムの変更はないため。
FCS_COP.1	予見される管理アクティビティはない。	
FCS_CKM.1	· 暗号鍵属性の変更の管理。	なし。暗号鍵属性の変更はしないため。
FCS_CKM.4	· 暗号鍵属性の変更の管理。	なし。暗号鍵属性の変更はしないため。

表 10 TSFによって提供される管理機能

FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割[割付: システム管理者、運用管理者、認証された一般ユーザ]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

依存性: [FDP_ACC.1 サブセットアクセス制御/FDP_IFC.1 サブセット情報フロー制御]、
FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MSA.1.1 TSF は、セキュリティ属性[割付: 表 11 の「セキュリティ属性」]に対し[選択: [割付: 表 11 の「操作」]をする能力を[割付: 表 11 の「役割」]に制限する[割付: FA アクセス制御 SFP]を実施しなければならない。

役割	セキュリティ属性	操作
システム管理者	ユーザ識別情報、グループ情報	登録、改変、削除、参照、インポート
	権限情報	改変、削除、参照
システム管理者から権限を許可された運用管理者	システム管理者から、許可された範囲内のユーザ識別情報、グループ情報	登録、改変、削除、参照、インポート

表 11　セキュリティ属性の管理

FMT_MSA.3 静的属性初期化

下位階層: なし

依存性: FMT_MSA.1 セキュリティ属性の管理、FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: 制限的]デフォルト値を与える[割付: FA アクセス制御 SFP]を実施しなければならない。

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、[割付: 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]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

FMT_MTD.1(1) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 （1） TSF は、[割付:表 12 の「TSF データのリスト」に示した情報]を[選択:[割付:表 12 の「操作」に示した操作を実行]]する能力を[割付: システム管理者から権限を許可された運用管理者]に制限しなければならない。

役割	TSF データのリスト	操作
システム管理者	指紋情報及びユーザ情報に存在する指紋情報コード	登録、改変、削除、参照、インポート
システム管理者から権限を許可された運用管理者	システム管理者から、許可された範囲内の指紋情報及びユーザ情報に存在する指紋情報コード	登録、改変、削除、参照、インポート

注)登録された指紋特徴量の参照または指紋特徴量のインポートはできない

表 12システム管理者から権限を許可された運用管理者が管理するユーザ情報

FMT_MTD.1(2) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 (2) TSF は、[割付: 自分自身の指紋情報]を[選択: 改変、削除、[割付: 登録]]する能力を[割付:認証された一般ユーザ]に制限しなければならない。

FMT_MTD.1(3) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 (3) TSF は、[割付: ワンタイムパスワード]を[選択: 改変、削除、[割付:生成、問い合わせ]]する能力を[割付: 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]に制限しなければならない。

FMT_MTD.1(4) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 (4) TSF は、[割付:管理者パスワード]を[選択: 改変、削除、[割付: 生成]]する能力を[割付:システム管理者]に制限しなければならない。

FMT_MTD.1(5) TSF データの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(5) TSFは、[割付: 監査記録]を[選択:削除]する能力を[割付: システム管理者]に制限しなければならない。

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FMT_SMF.1 管理機能の特定

FMT_MOF.1.1 TSF は、機能[割付: 表 13 の「機能」][選択: のふるまいを決定する、のふるまいを改変する]能力を[割付: 表 13 の「役割」]に制限しなければならない。

役割	機能
システム管理者	・クライアントキャッシュ機能無効設定、 ・Windows ログオンパスワードによる Windows ドメインにログオン禁止設定 ・ログ機能を有効設定(ログ削除しない)

表 13 TOEセキュリティ機能のふるまいの制御

FMT_SAE.1 時限付き許可

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割、FPT_STM.1 高信頼タイムスタンプ

FMT_SAE.1.1 TSF は、[割付:ワンタイムパスワードの有効期限]に対する有効期限の時間を特定する能力を、[割付: 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]に制限しなければならない。

FMT_SAE.1.2 これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、[割付: ワンタイムパスワードの認証を拒否]を行えなければならない。

FMT_SAC.1 使用回数制限付き許可

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SAC.1.1 TSF は、[割付:ワンタイムパスワードの有効使用回数]に対する有効使用回数を特定する能力を、[割付: 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]に制限しなければならない。

FMT_SAC.1.2 これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する使用回数制限を超過後、[割付: ワンタイムパスワードの認証を拒否]を行えなければならない。

FPT_ITT.1 基本 TSF 内データ転送保護

下位階層: なし

依存性: なし

FPT_ITT.1.1 TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを[選択: 暴露、改変]から保護しなければならない。

FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1 TSF は、[割付: FIPS PUB 197]に合致する、特定された暗号アルゴリズム[割付: 表 14 の暗号アルゴリズム]と暗号鍵長[割付:表 14 の暗号鍵長]に従って、[割付:表 14 の暗号操作]を実行しなければならない。

暗号アルゴリズム	暗号鍵長	暗号操作
AES	256 bit	クライアントと FA サーバ間で転送されるユーザ情報、指紋情報の暗号化と復号。

表 14 TOEの暗号アルゴリズム、暗号鍵長、暗号操作

FCS_CKM.1 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2 暗号鍵配付、または FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.1.1 TSF は、以下の[割付: FIPS 180-2]に合致する、指定された暗号鍵生成アルゴリズム[割付: SHA-256]と指定された暗号鍵長[割付: 暗号鍵長 256bit]に従って、暗号鍵を生成しなければならない。

FCS_CKM.4 暗号鍵破棄

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または FCS_CKM.1 暗号鍵生成]

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4.1 TSF は、以下の[割付: なし]に合致する、指定された暗号鍵破棄方法[割付: 新たなセッション確立後新たな暗号鍵により上書き及び電源オフ時消去される]に従って、暗号鍵を破棄しなければならない。

6.2. セキュリティ保証要件

本節では TOE セキュリティ保証要件について記述する。

本 TOE が適合を主張する評価保証レベルは EAL2 である。表 15 に、TOE セキュリティ保証要件としてセキュリティ保証要件パッケージ(EAL2)の保証要件コンポーネントの参照を示す。 なお、全てのセキュリティ保証要件は、 CC Part 3 に規定のセキュリティ保証要件である。

保証クラス	保証要件コンポーネント	
開発(ADV)	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.2	セキュリティ実施機能仕様
	ADV_TDS.1	基本設計
ガイダンス文書(AGD)	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート(ALC)	ALC_CMC.2	CM システムの使用
	ALC_CMS.2	TOE の一部の CM 範囲
	ALC_DEL.1	配付手続き
セキュリティターゲット評価 (ASE)	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
テスト(ATE)	ATE_COV.1	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定(AVA)	AVA_VAN.2	脆弱性分析

表 15　TOEセキュリティ保証要件コンポーネントの参照【EAL2の場合】

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

6.3.1.1. 必要性

TOEのセキュリティ対策方針に対するセキュリティ機能要件(SFR)の対応関係を表 16 に示す。この表からセキュリティ機能要件が少なくても 1つ以上のセキュリティ対策方針に対応している。

対策方針 / SFR	O/I&A	O.I&A_ADMINI	O.ENROLL_AUTH	O.ADMINI_RIGHT	O.FALLBACK	O.AUDIT	O.COMM_PROTEC
FIA_UID.2	✓	✓			✓		
FIA_UAU.2	✓	✓			✓		
FIA_UAU.5	✓	✓			✓		
FIA_USB.1				✓			
FIA_ATD.1				✓			
FIA_SOS.2					✓		
FDP_ACC.1				✓			
FDP_ACF.1				✓			
FMT_MSA.1				✓			
FMT_MSA.3				✓			
FMT_MTD.1(1)				✓			
FMT_MTD.1(2)			✓				
FMT_MTD.1(3)					✓		
FMT_MTD.1(4)					✓		
FMT_MTD.1(5)						✓	
FMT_MOF.1				✓			
FMT_SAE.1					✓		
FMT_SAC.1					✓		
FMT_SMF.1			✓	✓	✓	✓	
FMT_SMR.1			✓	✓	✓	✓	
FAU_GEN.1						✓	
FAU_SAR.1						✓	
FAU_STG.1						✓	
FPT_STM.1					✓	✓	
FPT_ITT.1							✓
FCS_COP.1							✓
FCS_CKM.1							✓
FCS_CKM.4							✓

表 16 TOEのセキュリティ対策方針とセキュリティ機能要件の対応関係

6.3.1.2. 対策方針に対する十分性

TOEの各セキュリティ対策方針がセキュリティ機能要件の実施により実現できることを説明する。

(1)O.I&A

TOEはFAサーバの利用を許可された一般ユーザを識別・認証しなければならない。

FIA_UID.2

TOE はユーザ識別前に他の TSF 仲介アクションを許可しないことを求める要件により、Windows ドメインまたは FA ユーティリティへのログオン前にユーザ識別が最初に実施されることを保証する。

FIA_UAU.2

TOE はユーザ認証前に他の TSF 仲介アクションを許可しないことを求める要件によって Windows ドメインまたは FA ユーティリティへのログオン前にユーザ認証を必ず実施することを保証する。

FIA_UAU.5

指紋認証メカニズムによりユーザを認証することを保証する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.I&A は実現される。

(2)O.I&A_ADMINI

TOE は、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権限を持つユーザを識別・認証しなければならない。

FIA_UID.2

TOE はユーザ識別前に他の TSF 仲介アクションを許可しないことを求める要件により、管理ユーティリティのログオン前にユーザ識別が最初に実施されることを保証する。

FIA_UAU.2

TOE はユーザ認証前に他の TSF 仲介アクションを許可しないことを求める要件によって管理ユーティリティのログオン前にユーザ認証を必ず実施することを保証する。

FIA_UAU.5

TOE は指紋認証のメカニズムにより認証を行うことを保証する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.I&A_ADMINI は実現される。

(3)O.ENROLL_AUTH

TOE は、TOE により識別・認証された一般ユーザが、自分自身の指紋情報に限り管理(登録・変更・削除)をできることを保証しなければならない。

FMT_MTD.1 (2)

TOE により認証された一般ユーザは自分自身の指紋情報の 登録、改変、削除ができることを保証する。

FMT_SMF.1 は管理機能 FMT_MTD.1 (2) の実施を規定する。

FMT_SMR.1 は FMT_MTD.1 (2) を実施する役割を規定する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.ENROLL_AUTH は実現される。

(4)O.ADMINI_RIGHT

TOE は、TOE の構成設定の変更をシステム管理者に制限し TOE の構成設定を維持しなければならない。TOE は、ユーザ情報及び指紋情報の管理能力を複数の管理者に分割し許可範囲内の操作に制限し、許可範囲外の変更を防止することを保証しなければならない。

FIA_ATD.1

TOE は識別・認証後のユーザ識別情報に関係付けられたグループ情報、権限情報を維持することを保証する。

FIA_USB.1

TOE は識別・認証後、利用者のグループ情報、権限情報をセキュリティ属性として、サブジェクトと利用者を結合させることを保証する。

FDP_ACC.1 及び FDP_ACF.1

利用者の権限情報により許可された条件下の要求の場合、Windows ログオンパスワードファイルに指定または TOE 内で生成された値を書き込むことを保証する。

FMT_MSA.1

TOE はシステム管理者にユーザ識別情報、グループ情報の登録、改変、削除、参照、インポート操作を許可することにより一般ユーザ及び管理者のユーザ情報の管理を可能にする。

TOE はシステム管理者に管理者の権限情報の改変、削除、参照操作を許可することにより管理者の権限管理を可能にする。また TOE は一般ユーザの管理範囲とユーザ情報に関する管理権限をシステム管理者から許可された運用管理者に、許可された範囲内のユーザ識別情報、グループ情報を登録、改変、削除、参照、インポート操作を許可することによりユーザ情報の管理を可能にする。以上から、ユーザ情報の管理能力を複数の管理者に分割し許可範囲内の操作に制限することができる。

FMT_MSA.3

TOE はオブジェクトの生成時、SFP を実施するために使われるセキュリティ属性について、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が代替の初期値による制限的デフォルト値を与える。

FMT_MTD.1 (1)

TOE はシステム管理者に、指紋情報及びユーザ情報に存在する指紋情報コードの登録、改変、削除、参照、インポート操作を許可する。また一般ユーザの管理範囲と指紋情報に関する管理権限をシステム管理者から許可された運用管理者に許可範囲内の指紋情報及びユーザ情報に存在する指紋情報コードの登録、改変、削除、参照、インポート操作を許可する。ただし指紋情報のうち登録された指紋特徴量の参照または指紋特徴量のインポートは許可しない。

これによりユーザの指紋情報の管理能力を複数の管理者に分割し許可範囲内の操作に制限することを保証する。

FMT_MOF.1

TOE はシステム管理者に TOE の構成設定の改変を許可しそれ以外は制限し権限外の変更を防止する。

FMT_SMF.1 は管理機能 FMT_MSA.1、FMT_MSA.3、FMT_MTD.1 (1)、FMT_MOF.1 の実施を規定する。

FMT_SMR.1 は FMT_MSA.1、FMT_MSA.3、FMT_MTD.1 (1)、FMT_MOF.1 を実施する役割を規定する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.ADMINI_RIGHT は実現される。

(5)O.FALLBACK

TOE は指紋認証が利用できないユーザに対し、代替えの認証機能を提供しFA サーバを使用できるようにしなければならない。

FMT_MTD.1 (3)

該当ユーザの変更管理権限を持つシステム管理者または、 システム管理者から許可された権限を持つ運用管理者に、該当ユーザ用のワンタイムパスワードの生成及び問い合わせ、改変、削除を許可することを求める。

FIA_SOS.2

適切な強度を持つワンタイムパスワードの生成を TOE が実施する結果、弱い認証サービスの使用防止を保証する。

FMT_SAE.1

ワンタイムパスワードの有効期限の設定を、システム管理者または、一般ユーザの管理範囲とユーザ情報関する管理権限をシステム管理者から許可された運用管理者に制限し有効期限を超えた場合ワンタイムパスワードによる認証拒否を保証する。

FPT_STM.1 により、ワンタイムパスワードの認証時、有効期限後を判断するために信頼される時間情報が提供されることを保証する。

FMT_SAC.1

ワンタイムパスワードの有効使用回数制限の設定を、システム管理者または、一般ユーザの管理範囲とユーザ情報関する管理権限をシステム管理者から許可された運用管理者に制限しその使用回数が有効使用回数制限を超えた場合ワンタイムパスワードによる認証拒否を保証する。

FMT_MTD.1 (4)

システム管理者に、管理者パスワードの生成及び改変、削除を許可することを求める。

FMT_SMF.1 は管理機能 FMT_MTD.1 (3)、FMT_MTD.1(4)の実施を規定する。

FMT_SMR.1 は FMT_MTD.1 (3)、FMT_MTD.1(4)、FMT_SAE.1、FMT_SAC.1 を実施する役割を規定する。

FIA_UID.2

TOE はユーザ識別前に他の TSF 仲介アクションを許可しないことを求める要件により、Windows ドメインまたは管理ユーティリティ、FA ユーティリティにログオン前にユーザ識別が最初に実施することを保証する。

FIA_UAU.2

TOE はユーザ認証前に他の TSF 仲介アクションを許可しないことを求める要件によって Windows ドメインまたは管理ユーティリティ、FA ユーティリティにログオン前にユーザ認証を必ず実施することを保証する。

FIA_UAU.5

管理者パスワード及び、ワンタイムパスワードメカニズムによりユーザを認証することを規定する。

従ってこれらの機能要件が実装されれば、対策方針 O.FALLBACK は実現される。

(6)O.AUDIT

TOEはバイオメトリックス識別・認証の不備をつく不正な認証の試みを検出しなければならない。
TOEは管理者パスワードまたはワンタイムパスワードによる不正な認証の試みを検出しなければならない。

FAU_GEN.1

ユーザの識別・認証時の監査事象を監査証跡に記録する。管理者による操作結果も監査事象として発生日時とともに監査証跡に記録する。

FPT_STM.1

監査事象の発生時刻は信頼される情報であることを保証する。

FAU_SAR.1

システム管理者は監査記録を閲覧でき、また TOE はユーザ識別情報、発生日時、事象種別、詳細情報を文字形式の一覧形式により解釈に適した形式で監査記録を表示することを保証する。

FAU_STG.1

格納された監査記録は不正な削除から保護され、不正な改変を防止する。

FMT_MTD.1(5)

監査記録を削除をシステム管理者に制限する。

FMT_SMF.1 は管理機能 FMT_MTD.1 (5) の実施を規定する。

FMT_SMR.1 は FMT_MTD.1(5)、FAU_SAR.1 を実施する役割を定義する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.AUDIT は実現される。

(7)O.COMM_PROTECT

TOE はクライアント PC と FA サーバ間の通信路からユーザ情報及び指紋情報の権限外の暴露及び改ざん防止を保証しなければならない。

FPT_ITT.1

TSF データ(ユーザ情報、指紋情報)が、TOE の異なるパーツであるクライアント PC と FA サーバ間の通信路で 暴露及び改変保護を保証することを求める。

FCS_COP.1

クライアントPCとFAサーバは送信前にこれらの TSF データを暗号標準に従って暗号化し受信後復号する要件を規定し暴露及び改変から保護を具体化する。

FCS_CKM.1 及び FCS_CKM.4

TSF データを暗号化/復号に使用する暗号鍵の生成と廃棄について要求し暗号による脆弱性に対処する要件を規定する。

従ってこれらの機能要件がすべて実装されれば、対策方針 O.COMM_PROTECT は実現される。

6.3.2. セキュリティ機能要件の依存性根拠

セキュリティ機能要件(SFR)の依存性について表 17 に示す。表 17 は、CC が規定する依存性と TOE が依存性を満たす SFR、依存性を満たさない SFR、及び満たさなくて良い理由を記載する。

依存性 / SFR	SFR の依存性 (CC パート２規定)	ST で左記依存性を満たす SFR	依存性を満たさない SFR	依存性満たさなくて良い理由
FIA_UID.2	なし	なし	—	—
FIA_UAU.2	FIA_UID.1	FIA_UID.2	—	—

依存性 / SFR	SFR の依存性 (CC パート２規定)	ST で左記依存性を満たす SFR	依存性を満たさない SFR	依存性満たさなくて良い理由
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	—	—
FIA_ATD.1	なし	なし	—	—
FIA_UAU.5	なし	なし	—	—
FIA_SOS.2	なし	なし	—	—
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	—	—
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3		—
FMT_MSA.1	[FDP_ACC.1/FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	—	—
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	—	—
FMT_MTD.1 (1)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_MTD.1 (2)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_MTD.1 (3)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_MTD.1 (4)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_MTD.1 (5)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1 FPT_STM.1	—	—
FMT_SAC.1	FMT_SMR.1	FMT_SMR.1	—	—
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	—	—
FMT_SMF.1	なし	—	—	—
FMT_SMR.1	FIA_UID.1	FIA_UID.2	—	—
FAU_GEN.1	FPT_STM.1	FPT_STM.1	—	—
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	—	—
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	—	—
FPT_STM.1	なし	なし	—	—
FPT_ITT.1	なし	なし	—	—
FCS_COP.1	[FDP_ITC.1/ FDP_ITC.2 / FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 FCS_CKM.4	FMT_MSA.2	(1)
FCS_CKM.1	[FCS_CKM.2 / FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP.1 FCS_CKM.4	FMT_MSA.2	(1)
FCS_CKM.4	[FDP_ITC.1/FDP_ITC.2/FCS_CKM.1] FMT_MSA.2	FCS_CKM.1	FMT_MSA.2	(2)

表 17 セキュリティ機能要件(SFR)の依存性

(1)FMT_MSA.2 の依存性を必要としない理由
暗号鍵は、クライアント PC と FA サーバ間の通信セッション毎に鍵シーズから生成され TOE 内部において制御される。そのため暗号鍵に対して管理されるべきセキュリティ属性を必要としないため、セキュアなセキュリティ属性の管理要件を必要としない。

6.3.3. セキュリティ保証要件根拠

TOEが保護するWindowsログオンパスワード、ユーザ情報及び指紋情報は、権限外暴露及び改ざんがされると認証機能自体の信頼性が損なわれる。また個人のバイオメトリックス情報が漏洩し再利用されると、その認証情報の変更ができないため、高いセキュリティの品質が求められる。しかし識別・認証で使用するこれらの情報は、物理的保護対策が取られている、FAサーバが制御するデータベース上に置かれる。
そのため攻撃者が利用可能な手段は、指紋認証ユニット、クライアント及びネットワークからの読み取りと置き換えになり論理的インタフェースを通じてのみ可能になる。クライアント上はこれらの情報が通過するだけで不揮発性メモリに残さないように実装され、また実行形式でインストールされたプログラムを解読することは困難である。また指紋認証ユニットから指紋情報を読み出せたとしてもそれをクライアント通じ登録させるためにはクライアントと認証ユニット間のプロトコルの詳細を再現させる技術と、設備が必要でありこの方法による脅威レベルは想定しない。結局想定する脅威は論理的インタフェースの利用を想定し、これらのセキュリティ品質の確認は、設計資料とテスト及び脆弱性評定で十分である。
EAL2はTOEにおける開発段階のセキュリティ対策の系統だったテストの実施と分析、安全に使用するための十分なガイダンスの評価、及び製品のユーザの手許に間違いなく配付することを保証する評価により、達成できるため、EAL2は妥当な選択である。

7. TOE 要約仕様

本章では、TOEが提供するセキュリティ機能の要約仕様について述べる。

7.1. TOE セキュリティ機能

7.1.1 指紋認証機能

ユーザがクライアント PC を起動すると、TOE は Windows ドメインにログオンするために、ログオン画面を表示する。またWindowsドメインにログオン後、FA ユーティリティまたは管理ユーティリティを起動すると、TOE はログオン画面を表示する。

(1) Windows ドメインにログオン

TOE はユーザ名と Windows システムのドメインのログオン先(コンピュータ名またはアプリケーション名)と指紋認証ユニットより指紋の入力をユーザに要求する。

指紋の入力後、TOE はユーザ識別情報によりユーザを識別する。

次に、TOE は指紋の濃淡情報から抽出した指紋特徴量(サンプル)と、登録された該当するユーザの指紋情報とを照合しユーザの認証を行う。

(2) FA ユーティリティにログオン

Windowsドメインにログオン後、FA ユーティリティを起動するとTOE はユーザ名の入力及び、指紋認証ユニットより指紋の入力をユーザに要求する。

指紋の入力後、TOE はユーザ識別情報によりユーザを識別する。

次に、TOE は指紋の濃淡情報から抽出された指紋特徴量と、登録された該当するユーザの指紋情報とを照合しユーザの認証を行う。

(3)管理ユーティリティにログオン

Windows ドメインにログオン後、管理ユーティリティを起動すると TOE はユーザ名の入力及び、指紋認証ユニットより指紋の入力をユーザに要求する。

指紋の入力後、TOE はユーザ識別情報によりユーザを識別する。

次に、TOE は指紋の濃淡情報から抽出した指紋特徴量と、登録された該当するユーザの指紋情報とを照合しユーザの認証を行う。

・FIA_UID.2 は以下のように実現される。

TOE は起動されるとログオン画面を表示しログオン画面以外は表示せず、他の TSF 仲介アクションは行わない。

TOE は入力されたユーザ名とログオン先が、TOE に登録されたユーザ情報に存在するか確認しユーザを識別する。

・FIA_UAU.2 は以下のように実現される。

指紋によるユーザ認証前にユーザ識別以外の TSF 調停アクションは実施しない。

・FIA_UAU.5 の指紋認証メカニズムについて以下のように実現される。

指紋認証ユニットから入力された指紋の濃淡情報から指紋特徴量を抽出し、ユーザ識別情報により関係付けられた指紋情報とを照合しユーザの認証を行う。

7.1.2 ワンタイムパスワードによる識別・認証機能

ユーザが指紋認証手段を利用できない場合、以下の方法による代替えの認証機能によりユーザの認証を行う。

(1)該当するユーザ情報の変更管理権限を持つ管理者が、該当ユーザに有効期限または有効使用回数を設定しワンタイムパスワードを発行する。

(2)Windows ドメインにログオン

TOE はユーザ名と Windows システムのドメインのログオン先及びワンタイムパスワードの入力をユーザに要求する。

ユーザが入力すると、TOE はユーザ識別情報によりユーザを識別する。

次に、TOE はユーザのワンタイムパスワードの有効期限と使用回数が制限内の時、ワンタイムパスワードによるユーザの認証を行う。また同時にそのワンタイムパスワードの使用回数を更新する。

(3) FA ユーティリティにログオン

Windows ドメインにログオン後、FA ユーティリティを起動すると、TOE はログオン先とワンタイムパスワード入力をユーザに要求する。

ユーザが入力すると、TOE はユーザ識別情報によりユーザを識別する。

次に、TOE はユーザのワンタイムパスワードの有効期限と使用回数が制限内の時、ワンタイムパスワードによるユーザの認証を行う。また同時にそのワンタイムパスワードの使用回数を更新する。

・FIA_UID.2 は以下のように実現される。

TOE は起動されるとログオン画面を表示しログオン画面以外は表示せず、他の TSF 仲介アクションは行わない。

TOE は入力されたユーザ名とログオン先が、TOE に登録されたユーザ情報に存在するか確認しユーザを識別する。

・FIA_UAU.2 は以下のように実現される。

ワンタイムパスワードによるユーザの認証を行う前にユーザ識別以外の TSF 調停アクションは実施しない。

・FIA_UAU.5 のワンタイムパスワードメカニズムについて以下のように実現される。

ユーザのワンタイムパスワードの属性から、有効期限と有効使用回数が制限内かどうか確認し有効な場合、該当するユーザ識別情報と関係付けられたワンタイムパスワードをログオン画面から入力されたワンタイムパスワードと照合しユーザを認証する。また同時にそのワンタイムパスワードの属性のうち使用回数を更新する。

・FMT_SAE.1 は以下のように実現される。

システム管理者または、一般ユーザの管理範囲とユーザ情報に関する管理権限をシステム管理者から許可された運用管理者は、管理ツールで該当するユーザに対しワンタイムパスワードの有効期限の設定がされており、ワンタイムパスワードによるユーザ認証時に有効期限を超えていると、ワンタイムパスワードによる認証を拒否する。

・FMT_SAC.1 は以下のように実現される。

システム管理者または、一般ユーザの管理範囲とユーザ情報に関する管理権限をシステム管理者から許可された運用管理者は、管理ツールで該当するユーザに対しワンタイムパスワードの有

効使用回数の設定がされており、ワンタイムパスワードによるユーザ認証時にワンタイムパスワードの使用回数が有効使用回数を超えた場合、ワンタイムパスワードによる認証を拒否する。

・FPT_STM.1 は以下のようにして実現される。

TOEはワンタイムパスワードによる認証要求時、ワンタイムパスワードの有効期限を超えたかどうか判定するためOSの時刻情報を獲得する。OSの時刻は、システム管理者が設定し、さらにOSを含むFAサーバはシステム管理者以外がアクセスすることは物理的に制限されていることから、獲得した時刻は信頼できる。

7.1.3 管理者パスワードによる識別・認証機能

管理ユーティリティまたは FA サーバのコマンドラインを入力しログオンする管理者は、指紋認証に代わり、システム管理者が設定した管理者パスワードによる認証ができる。

・FIA_UID.2 は以下のように実現される。

管理ユーティリティが起動されると TOE はログオン画面を表示しログオン画面以外は表示せず他の TSF 仲介アクションは行わない。

コマンドラインが入力されるとシステム管理者名が TOE に登録されたユーザ情報に存在しないと TOE は何も実行せず、他の TSF 仲介アクションは行わない。

・FIA_UAU.2 は以下のように実現される。

管理ユーティリティのログオン用画面またはコマンドラインから入力された管理者パスワードにより TOE はユーザの認証を行いユーザ認証前にユーザ識別以外の TSF 調停アクションは実施しない。

・FIA_UAU.5 の管理者パスワードメカニズムは以下のように実現される。

TOE は該当ユーザの管理者パスワードを入力された値と照合し管理者を認証する。

7.1.4 ユーザ情報及び指紋情報の管理機能

管理者の権限に応じ TOE は以下を実行する。

1) システム管理者は、管理者または一般ユーザのユーザ情報の管理、指紋情報の管理ができる。また運用管理者に一般ユーザの管理範囲とユーザ情報、指紋情報に関する管理権限を許可することができる。
2) 運用管理者は、システム管理者から許可された範囲と許可された操作の権限に従い、グループの作成またはグループに所属する一般ユーザのユーザ情報の管理、指紋情報の管理、ワンタイムパスワードの管理ができる。

また認証されたユーザは TOE により自身の指紋情報を管理できる。

・FIA_ATD.1、FIA_USB.1 は以下のように実現される。

管理ユーティリティまたは FA ユーティリティによる識別・認証成功後、ユーザ識別情報に関係付けられたグループ情報、権限情報を維持し、グループ情報、権限情報をセキュリティ属性とし利用者を代行するプロセスを呼び出す。利用者を代行するプロセスはユーザが操作可能な画面を表示

する。

コマンドラインによる識別・認証成功後、ユーザ識別情報に関係付けられたグループ情報、権限情報を維持し、グループ情報、権限情報をセキュリティ属性とし利用者を代行するプロセスを呼び出す。

・FMT_SMR.1 は以下のように実現される。

ユーザ識別情報とグループ情報及び権限情報により、次の役割を維持する。

1)全ての設定情報の管理権限を持つシステム管理者役割

2)グループ情報及び権限情報により一般ユーザの管理範囲とユーザ情報、指紋情報に関する管理権限を許可された運用管理者役割

3)一般ユーザ役割

・FMT_MSA.1、FMT_MSA.3、FMT_SMF.1 は、以下のように実現される。

管理ツールの画面またはコマンドラインからログオン先の管理(登録、改変、削除、参照、インポート)、ログオン先のグループの管理(登録、改変、削除、参照、インポート)、及びこれらに所属する一般ユーザのユーザ識別情報の管理(登録、改変、削除、参照、インポート)操作をシステム管理者が行うことができる。

また管理ツールの画面から管理者の権限の改変、削除、参照操作をシステム管理者が行うことができる。

管理ツールに許可された範囲の画面を表示し、その範囲内でログオン先の管理(登録、改変、削除、参照、インポート)、ログオン先のグループの管理(登録、改変、削除、参照、インポート)、及びこれらに所属する一般ユーザのユーザ識別情報の管理(登録、改変、削除、参照、インポート)操作をシステム管理者から権限を許可された運用管理者が行うことができる。

一般ユーザのユーザ識別情報の登録またはインポート時 Windows ログオンパスワード(オブジェクト)が生成される。オブジェクト生成時のセキュリティ属性(ユーザ識別情報、グループ情報)は、システム管理者または権限を持つ運用管理者により設定された初期値が与えられる。

・FDP_ACC.1、FDP_ACF.1 は、以下のように実現される。

Windows ログオンパスワードについて TOE は、以下のように読み出し及び書込を制御する。

1)管理者の識別認証後呼び出されたプロセスは、グループ情報より変更権限を持ち、権限情報よりシステム管理者の権限を持つ場合、一般ユーザのユーザ識別情報を指定し「パスワード変更」操作により指定された Windows ログオンパスワードに対し読み出し及び指定値の書込を行う。

2)管理者の識別認証後呼び出されたプロセスは、グループ情報より変更権限を持ち、権限情報よりシステム管理者の権限を持つ場合、ログオン先、ログオン先のグループ、所属するユーザ識別情報のいずれかを指定し「ランダムパスワード発行」操作により指定された Windows ログオンパスワード読み出し及び生成値の書込を行う。

3)管理者の識別認証後呼び出されたプロセスは、グループ情報より変更権限を持ち、権限情報よりユーザ情報の管理を許可された運用管理者の場合、許可された一般ユーザの管理範囲にある一般ユーザのユーザ識別情報を指定し「パスワード変更」操作ができ、Windows ログオンパスワードに対し読み出し及び指定値の書込を行う。

・FMT_MTD.1(1)、FMT_SMF.1 は、以下のように実現される。

管理ツールの画面から指定された指紋情報(指紋特徴量)の登録、改変、削除操作をシステム管理者が行うことができる。

管理ツールの画面から指定された指紋情報(登録された指の指紋特徴量除く)及び指紋情報コードの登録、改変、削除、参照、インポート操作をシステム管理者が行うことができる。

コマンドラインから指紋情報コード及び指紋情報(指紋特徴量)の削除操作をシステム管理者が行うことができる。

コマンドラインから指紋情報コードのインポート、改変操作をシステム管理者が行うことができる。

許可された一般ユーザの管理範囲または指紋情報に関する管理権限範囲のユーザ情報を管理ツールの画面に表示し、該当ユーザの指紋情報(指紋特徴量)の登録、改変、削除操作をシステム管理者から管理権限を許可された運用管理者が行うことができる。

許可された一般ユーザの管理範囲または指紋情報に関する管理権限範囲のユーザ情報を管理ツールの画面に表示し、指紋情報(登録された指の指紋特徴量除く)及び指紋情報コードの登録、改変、削除、参照、インポート操作をシステム管理者から管理権限を許可された運用管理者が行うことができる。

・FMT_MTD.1(2)、FMT_SMF.1 は以下のように実現される。

FA ユーティリティにより自分自身の指紋情報の登録、改変、削除操作を識別・認証された一般ユーザができる。

・FMT_MTD.1(3)、FMT_SMF.1 は以下のように実現される。

管理ツールにより、指定されたユーザのワンタイムパスワードの生成、参照、改変、削除操作をシステム管理者ができる。また管理ツールにより、許可されたユーザの管理範囲のユーザ識別情報と関係付けられたワンタイムパスワードの生成、参照、改変、削除操作を、システム管理者から権限を許可された運用管理者ができる。

・FIA_SOS.2 は以下のように実現される。

ワンタイムパスワードは 12 桁のアルファベット及び数字の組み合わせとして TOE が生成する。

・FMT_SAE.1、FMT_SMF.1、FMT_SMR.1 は以下のように実現される。

システム管理者または、一般ユーザの管理範囲とユーザ情報に関する管理権限をシステム管理者から許可された運用管理者は、管理ツールで該当するユーザに対しワンタイムパスワードの有効期限の設定操作ができる。

・FMT_SAC.1、FMT_SMF.1 、FMT_SMR.1 は以下のように実現される。

システム管理者または、一般ユーザの管理範囲とユーザ情報に関する管理権限をシステム管理者から許可された運用管理者は、管理ツールで該当するユーザに対しワンタイムパスワードの有効使用回数の設定操作ができる。

・FMT_MTD.1 (4)、FMT_SMF.1 は以下のように実現される。

管理ツールまたはコマンドラインにより、全ての管理者パスワードを生成・改変・削除操作をシステム管理者ができ、この能力はシステム管理者に制限される。

・FMT_MOF.1、FMT_SMF.1 は以下のように実現される。

管理ツールにより、クライアントキャッシュ機能無効設定と改変、Windows ログオンパスワードによる

Windows ドメインにログオン禁止設定と改変、ログ機能を有効設定(ログ削除しない)と改変操作ができ、この能力はシステム管理者に制限される。

7.1.5 監査機能

ログビューアにログオン後、システム管理者は、TOE により監査記録を閲覧できる。

・FIA_ATD.1、FIA_USB.1 は以下のように実現される。

識別・認証成功後、ユーザ識別情報に関係付けられたグループ情報、権限情報を読み込み維持し、グループ情報、権限情報をセキュリティ属性とし利用者を代行するプロセス(サブジェクト)が起動する。利用者を代行するプロセスはセキュリティ属性に従い、システム管理者が閲覧できるログビューア画面を表示する。

・FAU_SAR.1、FMT_SMR.1 は以下のようにして実現される。

ログビューアにより、TOE は以下の監査記録を日付別に解釈するのに適した一覧表形式によるキャラクタ表示を行い、閲覧をシステム管理者に可能にする。

監査記録の表示

(1)ユーザ識別情報　　:ユーザ名＋ログオン先

(2)発生日時　　:発生日時(クライアント)、受信時(FA サーバ)

(3)監査事象種別　　:ログ種別、ログ分類

(4)詳細情報　　:詳細な事象の発生内容

・FAU_GEN.1は以下のようにして実現される。

FA サーバが起動されると監査機能も起動しシャットダウンによって監査機能が終了する。監査機能の起動と終了は FA サーバの OS のログに記録され代替できる。

監査事象発生時、発生時刻とユーザ識別情報及びログ分類、エラーコードをデータベースに記録する。

機能要件毎の監査事象は、以下に示す監査事象をログ分類とエラーコードとして監査証跡に記録することで実現される。

①ログの読み出し(FAU_SAR.1)はログビューア起動時を監査事象として記録

②ログオンの成功時、ログオン失敗の回数が閾値以上の時(FIA_UID.2、FIA_UAU.2、FIA_UAU.5)は、「ログ分類(ログオン先)とエラーコード(指紋認証または管理者パスワードまたはワンタイムパスワード認証成功/認証失敗)」を監査事象として記録

(注)TOE ではログオン失敗回数の閾値は1回である。

③管理機能の起動(FMT_SMF.1)は、管理ツール、FA ユーティリティの起動を監査事象として記録

④ユーザ識別情報及びグループ情報の登録、改変、削除、インポート時、ワンタイムパスワードの生成、改変、削除時、指紋情報及び指紋情報コードの登録、改変、削除、インポート時、管理者パスワードの生成、改変、削除時、権限情報の改変、削除時、監査記録の削除時(FMT_SMR.1、FMT_MSA.1、FMT_MTD.1(1)、 FMT_MTD.1 (2)、 FMT_MTD.1 (3)、 FMT_MTD.1 (4) 、FMT_MTD.1 (5))はそれぞれの事象発生時を監査事象として記録

⑤ワンタイムパスワードの有効期限設定時(FMT_SAE.1)を監査事象として記録
⑥ワンタイムパスワードの有効使用回数設定時(FMT_SAC.1)を監査事象として記録
⑦秘密の生成時(FIA_SOS.2)は、ワンタイムパスワードの発行時を監査事象として記録
⑧TSF の機能のふるまいにおけるすべての改変時(FMT_MOF.1)は、クライアントキャッシュ機能無効設定、Windows ログオンパスワードによる Windows ドメインにログオン禁止設定、ログ機能を有効設定(ログ削除しない)の改変時を監査事象として記録

・FPT_STM.1 は以下のようにして実現される。
監査事象発生時、TOE は OS の時刻情報を獲得し、監査事象と共に記録する。
OS の時刻は、システム管理者が設定し、さらに OS を含む FA サーバはシステム管理者以外がアクセスすることは物理的に制限されていることから、獲得した時刻は信頼できる。

・FAU_STG.1、FMT_MTD.1(5)は以下のようにして実現される。
ログビューアにより、監査記録の削除操作をシステム管理者ができる。これ以外に監査記録を削除あるいは改変するインタフェースは存在しない。

7.1.6 通信路の情報保護機能

TOE は生成した暗号鍵により、ユーザ情報または指紋情報を通信前に暗号化し受信後復号する。
またドメインの資源にログオン可能な「ランダム文字列」を通信前に暗号化し受信後復号する。

・FCS_CKM.1 は以下のように実現される。
暗号化/復号に使用するクライアント PC と FA サーバのパーツの共通鍵は、FIPS 180-2 に従い AES の 256bit の暗号鍵を、通信毎に変化するセッションデータから共通の鍵シーズを生成し、鍵シーズをハッシュ演算して生成する。

・FCS_COP.1 は以下のように実現される。
TOE はユーザ情報及び指紋情報を FIPS PUB 197 に従った、AES に暗号鍵長 256bit で暗号化及び復号を行う。

・FCS_CKM.4 は以下のように実現される。
暗号化及び復号で使用された暗号鍵は、新たなセッションの確立後に、次の暗号操作が行われると新しい暗号鍵により、使用された暗号鍵は上書きされて利用することはできない。
さらに暗号鍵は揮発性メモリでのみ使用され、不揮発性メモリには残さないため電源オフ後の再利用は防止される。

・FPT_ITT.1 は以下のように実現される。
TOE の異なるパーツ間で TSF データ(ユーザ情報、指紋情報)の転送時、暗号化されて送られるため暴露及び改ざんからの保護が保証される。

付録　用語の定義

解説付き用語	説明(定義)
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。
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に使用する。 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は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場合。
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。