＜ST 作成説明会(2014/7/1)用抜粋版＞

参考資料

A 社個人情報処理システムアプリケーション
セキュリティターゲット

バージョン：1.4

発行日： 2014 年 6 月 27 日

作成者：X 社

注意事項：
・本文書は、個人情報処理システムアプリケーションの ST 作成時に、参考資料として利用してもらうことを目的に公開するものである。
・本文書は、他のシステムの ST 作成時に、本文書の一部またはすべてをそのままコピーして利用することを意図するものではない。
・本文書は、これを参考にして作成されたいかなる ST の評価や認証に影響を与えるものではない。
・本文書を参考として利用する限りにおいて、その利用方法を規制するものではない。

独立行政法人情報処理推進機構
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

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
0.7	新規作成	全体	ー	2007/4/23	X 社
0.8	レビューに伴う修正・追加	全体	ー	2007/6/19	X 社
0.9	・誤字・脱字の修正 ・ガイダンスへのバージョンの追加	全体 1.4.3	-	2007/6/29	X 社
1.0	・機能要件表記修正	6.1	V3.1 Part2 のコンポーネント表記に合わせた修正	2007/12/10	X 社
1.1	・CC バージョン表記の修正	2.1	改訂版の追記	2008/7/18	X 社
1.2	・CC バージョン表記の修正	2.1	改定版の更新	2009/7/1	X 社
1.3	・CC バージョン表記の修正 ・脅威の変更 ・ガイドライン表記の修正 ・前提条件の追加 ・TOE のセキュリティ対策方針の変更 ・セキュリティ対策方針根拠の変更 ・拡張機能コンポーネント ・セキュリティ機能要件（抜粋）の追加 ・セキュリティ機能要件根拠の修正 ・依存性の検証 ・TOE セキュリティ機能（抜粋）の修正	2.1 3.1.2、4.3 3.2 3.3、4.3 4.1 4.3 5.1 6.1 6.3.1 6.3.2 7.1	改定版の更新 対策方針に合わせた記述の変更、重複した名称を修正 改定版の更新 利用者に関する前提条件を追加 脅威に合わせた記述の追加 対策方針に合わせた記述の変更 CCv3.1R3 での変更に伴う修正 O.I&A に FMT クラスを追加 機能要件追加に伴う追加・更新 機能要件追加に伴う追加・更新 機能要件追加に伴う追加・更新	2010/7/27	X 社
1.4	・CC バージョン表記の修正	2.1	改定版の更新	2014/6/27	X 社

目次

1. ST 概説

本章では, ST 参照, TOE 参照, TOE 概要, およびTOE 記述について記述する。

コメント [CEM1]:
ASE_INT.1-1

1.1. ST 参照

コメント [CEM2]:
ASE_INT.1-2

本節ではST の識別情報を記述する。

タイトル　：A 社個人情報処理システムアプリケーション セキュリティターゲット
バージョン　：1.4
発行日　：2014 年 6 月 27 日
作成者　：X 社

1.2. TOE 参照

コメント [CEM3]:
ASE_INT.1-3
ASE_INT.1-4
ASE_INT.1-11

本節ではTOE の識別情報を記述する。

TOE　：A 社個人情報処理システムアプリケーション
TOE のバージョン　：1.0
キーワード　：個人情報、個人データ、保有個人データ、システム
開発者　：X 社

1.3. TOE 概要

1.3.1. TOE 種別および主要セキュリティ機能

コメント [CEM4]:
ASE_INT.1-5
ASE_INT.1-6
ASE_INT.1-7

TOE は、個人情報取扱事業者である A 社事業の一つである通信教育事業において、顧客の個人情報を管理するためのシステム「A 社個人情報処理システム」を構成するアプリケーションソフトウェアであり、基本機能（個人データの登録、更新、閲覧・検索、提供、預託、加工、削除の機能、未登録個人データの外部入力機能、提供・預託データの外部出力機能、及び監査証跡の退避機能）、及び個人データの漏えいを防止、改ざんを検出するためのセキュリティ機能を提供する。

TOE が提供するセキュリティ機能の概要を以下に示す。

［TOE が提供するセキュリティ機能］

監査機能：
TOE の監査証跡を採取し、参照・管理を可能にする

操作員管理・アクセス制御機能：
TOE にアクセスする利用者の管理、および各利用者に付与された権限に基づき TOE へのアクセスを制御する

識別認証機能：
TOE へアクセスする利用者の識別認証、端末の検証、パスワードの品質検証、及びアカウントロックを行う

暗号機能：
サーバ・クライアント間通信の暗号化、バックアップデータの暗号化・復号、及び個人データの提供データ・預託データの暗号化を行う

バックアップ・リカバリ機能：
TOE の復旧に必要なデータのバックアップ／リカバリを行う

1.3.2. TOE 利用環境

1.3.2.1. TOE 運用環境

TOE が稼動する端末と、関連する IT 機器構成を図 1-1 に示す。

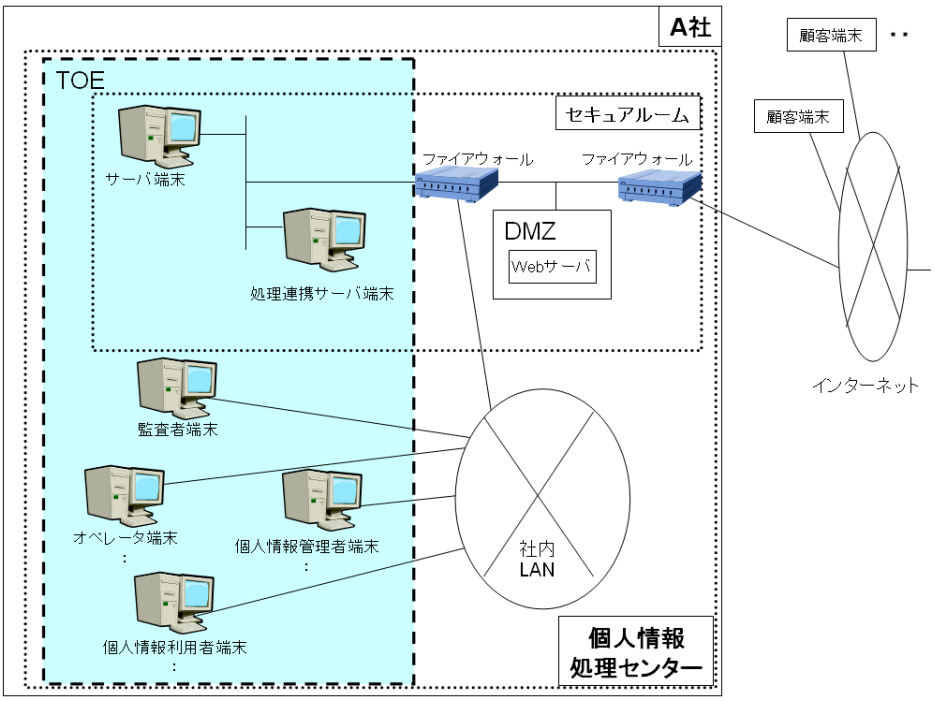


図 1-1 個人情報処理システム運用環境

(1) 物理配置及びネットワーク

A 社の通信教育事業の個人情報処理センターには、複数台のオペレータ端末、複数台の個人情報利用者端末、複数台の個人情報管理者端末、複数台の監査者端末と施錠可能なラック内に収納されているファイアウォール、Web サーバ、サーバ端末、及び処理連携サーバ端末が設置される。TOE の物理的範囲内にある端末は、オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末（図 1-1 の破線内）である。

個人情報処理センターは、A 社社員のみが入館できるよう入退館管理された建物に設置されており、個人データを保管するサーバ端末・処理連携サーバ端末は、個人情報処理センターの中で更に物理的に隔てられ別途入退室管理されたセキュアルームで管理される。セキュアルームへは、保管された端末を操作するサーバ管理者、サーバ管理者に許可された者、及び個人情報処理システム以外の機器における管理者等が入室を許可される。サーバ管理者やその他の機器の管理者は、それ以外の者の入室を許可した場合、その者に同行し行動を監視する。

顧客端末から送信されるデータは、インターネット、ファイアウォール、及び Web サーバを経由して処理連携サーバ端末へ格納される。通信内容や Web サーバへの各種攻撃については、ファイアウォールや Web サーバの管理者による各種セキュリティ対策が既に講じられており、安全に通信が行える状態を確保している。また、クライアント端末には個人データを保管しない。

コメント [CEM5]:
ASE_INT.1-8

(2) セキュアルームネットワーク

セキュアルーム内のサーバ端末、処理連携サーバ端末のみが接続するネットワークをセキュアルームネットワークと呼ぶ。

(2-1) サーバ端末

サーバ端末は、セキュアルームネットワークに接続される。サーバ管理者が、基本機能の起動／停止、鍵管理、システム環境設定、バックアップ／リカバリ、個人データの提供・預託データの外部出力、監査証跡参照、及び操作員管理を行うために用いる。基本機能利用者に対しては、役割毎に異なる基本機能を提供し、監査者に対しては、監査証跡参照・監査証跡管理・監査証跡退避機能を提供する。監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、サーバコンソールにその旨が通知される。また、処理連携サーバ端末のメールサーバを利用して、監査者にその旨を通知する。

(2-2) 処理連携サーバ端末

処理連携サーバ端末は、セキュアルームネットワークに接続される。DMZ 上の Web サーバを経由した顧客端末からの登録・更新・削除依頼を受付、処理連携サーバ端末内の DB に格納する。依頼を受け付けた際にはオペレータにメールで通知する。顧客からの登録・更新・削除依頼に基づくオペレータによる操作により、サーバ端末内の DB を更新する。その際は、オペレータ端末から、サーバ端末経由で処理連携サーバ端末にアクセスする。

(3) 社内 LAN

A 社のネットワークであり、ファイアウォールを介してインターネットと接続されている。セキュアルームネットワークを含み、オペレータ端末、個人情報利用者端末、個人情報管理者端末、及び監査者端末が接続するネットワークである。

(3-1) オペレータ端末

オペレータ端末は、社内 LAN に接続される。オペレータが、個人データを登録、更新、及び削除する際に、オペレータ端末から社内 LAN を介してサーバ端末にアクセスする。

(3-2) 個人情報利用者端末

個人情報利用者端末は、社内 LAN に接続される。個人情報利用者が、個人データを閲覧・検索、提供、預託、及び加工する際に、個人情報利用者端末から社内 LAN を介してサーバ端末にアクセスする。

(3-3) 個人情報管理者端末

個人情報管理者端末は、社内 LAN に接続される。個人情報管理者が、個人データを閲覧・検索する際、オペレータ・個人情報利用者の操作を承認する際、操作員管理を行う際に、個人情報管理者端末から社内 LAN を介してサーバ端末にアクセスする。

(3-4) 監査者端末

監査者端末は、社内 LAN に接続される。監査者が監査証跡参照、監査証跡管理、及び監査証跡退避を行う際に、監査者端末から社内 LAN を介してサーバ端末にアクセスする。監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、その

旨を警告するメールをサーバ端末から受信する。

1.3.2.2. ハードウェア構成

表 1-1 に、TOE の動作環境としてのハードウェア構成を示す。TOE は、表 1-1 を満たす動作環境で、正しく確実に動作する。尚、表 1-1 中の端末名に関しては、図 1-1 を参照されたい。

表 1-1 ハードウェア構成

端末・装置名	種別	説明
サーバ端末		
本体	ベンダ名	X 社
	製品名	ExpreZZ 5800/120Lh
	型名	P8100-1132P
	CPU	64 ビット インテリ eXeon プロセッサ（3.20 GHz）
	メモリ	1GB
	HDD	73.2GB × 3
DAT 装置	ベンダ名	X 社
	製品名	内蔵 DAT（DDS3/4/DAT72）（36GB）
	型名	N8151-51A
（中略）		

1.3.2.3. ソフトウェア構成

表 1-2 に、TOE のソフトウェア構成を示す。TOE は表 1-2 に識別されたソフトウェア構成によって、正しく確実に動作する。尚、表 1-2 中の端末名に関しては、図 1-1 を参照されたい。

表 1-2 ソフトウェア構成

端末名		
ベンダ名	製品名	備考
サーバ端末		
JISEC 社	JISEC Server 2006, Enterprise Edition; SP1	オペレーティングシステム
JISEC 社	Mailer Express 6.0	メールクライアント
JISEC 社	JISEC Database 10g Release 1(10.1.0)	DBMS
C 社	アンチウイルスソフト	ウイルス対策ソフト
X 社	個人情報処理システムサーバ用アプリケーションパッケージ V1.0	TOE の運用管理に必要となる、サーバ端末用アプリケーションパッケージ
（中略）		

1.4. TOE 記述

本章ではTOEの利用者役割、TOEの論理的範囲、およびTOEの物理的範囲について記述する。

1.4.1. TOE の利用者役割　*（抜粋）*

TOEで使用される各端末における利用者（以降、操作員と呼ぶ）の役割は以下のとおりである。操作員は、サーバ管理者、監査者、個人情報管理者、オペレータ、及び個人情報利用者のいずれかの操作員種別に分類され、操作員種別毎に付与された権限の範囲の業務を行うことができる。

（1）サーバ管理者

サーバ端末・処理連携サーバ端末の管理者となる。サーバ端末・処理連携サーバ端末に直接ログインできる権限を有する操作者である。サーバ管理者自身は、個人データの登録、更新、削除、閲覧・検索、提供、預託、及び加工を行わず、次の業務を行う。

- 基本機能の起動／停止
- 鍵管理（サーバ共通鍵・処理連携サーバ共通鍵・サーバ公開鍵・サーバ秘密鍵の生成・更新・削除、提供・預託先公開鍵のインポート・削除）
- システム環境設定（パスワード試行回数の管理、バナー表示メッセージの管理、操作員種別ごとのセション確立許可時間帯の管理）
- バックアップ／リカバリ
- 個人データの提供・預託データの外部出力
- 監査証跡参照
- 操作員管理（サーバ管理者、監査者、個人情報管理者の管理）

組織の責任者が、A 社通信教育事業部門員の中から適任者を厳重に人選し、サーバ管理者として任命する。

なおサーバ管理者は、自身の役割をサーバ端末、及び処理連携サーバ端末においてのみ実施することができる。

（2）監査者

監査者端末より、サーバサブシステム（詳細は、「1.3.2.3 ソフトウェア構成」で述べる。）が生成する監査証跡を検査する操作者である。監査者には、以下の権限のみが付与され、監査者自身は、個人データの登録、閲覧・検索、提供、預託、加工、更新、及び削除を行わず、次の業務を行う。

- 監査証跡参照
- 監査証跡管理
- 監査証跡退避

組織の責任者が、A 社通信教育事業部門員の中から適任者を厳重に人選し、監査者として任命する。

なお監査者は、自身の役割をクライアント端末においてのみ実施することができる。

（中略）

1.4.2. TOE の論理的範囲

コメント [CEM6]:
ASE_INT.1-10

本TOEは、顧客の個人情報の登録、更新、閲覧・検索、提供、預託、加工、及び削除を行うためのシステムである。A社個人情報処理システムの利用イメージを図1-2に示す。

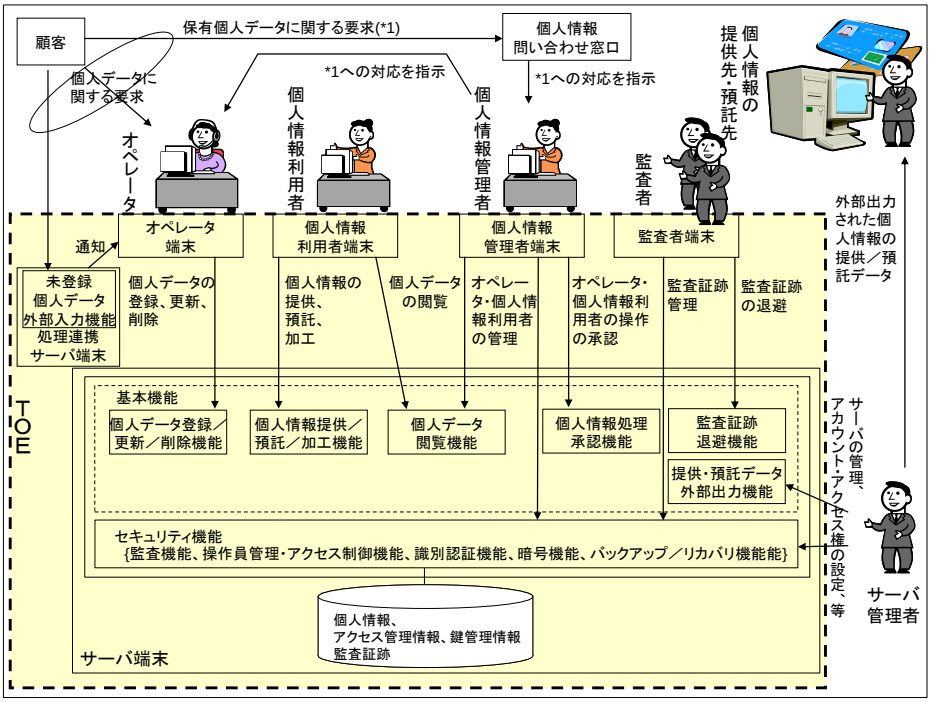


図 1-2　A 社個人情報処理システムの利用イメージ

A社個人情報処理システムで提供される機能は大別すると以下のように分類される。

(1) 基本機能

1. 個人情報処理メイン機能
   - 個人データ登録、更新、及び削除に関する機能、
   - 個人データ閲覧・検索に関する機能、
   - 個人データ提供、預託、及び加工に関する機能、
   - 個人情報処理承認に関する機能
2. 未登録個人データ外部入力機能
3. 提供・預託データ外部出力機能
4. 監査証跡退避機能

(2) セキュリティ機能

監査機能、操作員管理・アクセス制御機能、識別認証機能、暗号機能、及びバックアップ／リカバリ機能

1.4.2.1節、1.4.2.2節に述べる機能はすべて、TOEの範囲内である。

1.4.2.1. TOE によって提供される基本機能

表1-3は、TOEが提供する基本機能である、個人情報処理メイン機能、未登録個人データ外部入力機能、提供・預託データ外部出力機能、及び監査証跡退避機能についてその概要を記す。

表 1-3 TOE によって提供される基本機能

機能	概要
個人データ登録に関する機能	オペレータが、個人情報登録用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データが DB に登録される。
個人データ更新に関する機能	オペレータが、個人情報更新用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、DB 上のデータが更新される。
個人データ削除に関する機能	オペレータが、個人情報削除用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、DB 上のデータが削除される。
個人データ閲覧・検索に関する機能	個人情報利用者、個人情報管理者が、個人データ、及び個人データの加工データを閲覧・検索する。
個人データ提供に関する機能	個人情報利用者が、個人データ提供用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データは暗号化され、サーバ管理者に外部出力が依頼される。
個人データ預託に関する機能	個人情報利用者が、個人データ預託用のデータを生成し、個人情報管理者に承認を依頼する。個人情報管理者に承認されると、データは暗号化され、サーバ管理者に外部出力が依頼される。
個人データ加工に関する機能	個人情報利用者が、個人データを複写・加工する。
個人情報処理承認に関する機能	個人情報管理者が、オペレータ・個人情報利用者の操作を承認する。
未登録個人データ外部入力機能	顧客から送信されたデータを DMZ 上の Web サーバで未登録個人データとして生成し、これを処理連携サーバ端末へインポートする。
提供・預託データ外部出力機能	サーバ管理者が、暗号化された提供・預託データを TOE 外へエクスポートする。
監査証跡退避機能	監査者が、監査証跡を TOE 外へエクスポート、TOE 内へインポートする。

1.4.2.2. TOE によって提供されるセキュリティ機能

(1) 監査機能

TOEは、安定的な稼動維持、セキュリティ侵害の検知のために、自身の監査証跡を生成する。ただし、監査証跡に含まれるタイムスタンプは、TOE範囲外であるOSにより提供される。

＜アプリケーションの監査証跡＞

サーバ管理者、及び監査者は、監査証跡参照機能、及び監査証跡管理機能を使用して、アプリケーションの監査機能により採取・管理される監査証跡を使用する。

・監査証跡参照機能：

監査証跡の参照及び検索を行うための機能。サーバ管理者、及び監査者が利用可能。

・監査証跡管理機能：

DB上の監査証跡の削除を手動で行うための機能。監査証跡格納領域の枯渇の恐れがある場合に警告を発信する機能。セキュリティ侵害の可能性を検知するための機能。

- DB上の監査証跡の削除は、監査者のみが利用可能。
- 監査証跡を格納するための領域に枯渇の恐れがある時、及び監査対象事象に関して監査者の定めた重要度以上の重要度を含む監査証跡が生成された時には、その旨をサーバコンソールに通知するとともに、監査者へメールにより通知する。
- 監査証跡を格納するための領域が枯渇した場合は、領域の枯渇、及び作成日時が古い監査証跡から順番に削除する旨をサーバコンソールに通知するとともに、監査者へメールにより通知する。その上で、監査証跡の作成日時が古いものから順番に削除し、最新の監査証跡を生成する。
- セキュリティ侵害の可能性を検知するため、すべての監査対象事象に対して重要度を設定する。設定された重要度以上の監査証跡が生成された場合、サーバ管理者と監査者に通知する。

(2) 操作員管理・アクセス制御機能

TOEにアクセスする操作員の登録・削除・情報管理を行う。操作員管理を行うことができるのは、サーバ管理者及び個人情報管理者のみである。管理対象とできる操作員は、以下のとおりである。

・サーバ管理者が管理する操作者：サーバ管理者、監査者、及び個人情報管理者
・個人情報管理者が管理する操作者：オペレータ、及び個人情報利用者

管理できる情報は、識別認証機能によって利用される操作員ID及びパスワードである。操作員IDは、アクセス制御機能にも利用される。

サーバ管理者のID・パスワードの登録は、個人情報処理システムサーバ用アプリケーションパッケージのセットアップ時にサーバ管理者自身が行う。サーバ管理者は、サーバ管理者のID・パスワードの作成や、IDの削除は可能だが、TOEには必ず1名以上のサーバ管理者が存在する必要がある。

TOEの利用者役割に付与された権限に基づき、TOEへのアクセスを制御する。TOEに対してある一定の時間何の操作もしなかった場合には、対話セションを終了する。また、業務時間外に個人データを操作するのを防ぐため、利用時間帯を制限することができる。利用時間帯は、サーバ管理者のみが設定できる。クライアント操作員による個人データの持ち出し（サーバ端末以外への保存、画面コピー、印刷）を禁止する。

(3) 識別認証機能

TOEへアクセスする操作員の識別認証、端末の検証、パスワードの品質の検証、及びアカウントロックを行う。

クライアント操作員の識別認証では、以下のすべてが成功しなければならない。

1. 勧告的警告メッセージの表示
2. セション鍵の生成
3. クライアント端末用パッケージの正当性検証
4. クライアント操作員のID・パスワード認証

「クライアント端末用パッケージの正当性検証」では、クライアント端末がサーバ端末に対し、自身にインストールされる個人情報処理システムクライアント用アプリケーションパッケージが正当なものであることを証明する。

サーバ管理者の識別認証では、以下のすべてが成功しなければならない。

1. 勧告的警告メッセージの表示
2. サーバ管理者のID・パスワード認証

操作員のパスワードの品質は、低レベルの攻撃エージェントを想定した機能強度を持つことが検証される。

サーバ管理者が設定するパスワード試行回数以上、連続してパスワードを誤入力すると当該アカウントはロックされる。

(4) 暗号機能

サーバ端末と、クライアント端末間通信の暗号化、バックアップデータの暗号化・復号、及び個人データの提供データ・預託データの暗号化を行う。また暗号鍵の生成・インポート・破棄を行う。

＜暗号鍵の種別＞

・サーバ共通鍵：サーバ端末のバックアップデータの暗号操作に利用する。
・処理連携サーバ共通鍵：処理連携サーバ端末のバックアップデータの暗号操作に利用する。
・サーバ秘密鍵／公開鍵：サーバ端末ークライアント端末間の通信データの暗号操作に利用する。また、個人情報処理システムクライアント用アプリケーションパッケージ実行コードのハッシュ値に対する暗号操作に利用する。
・提供・預託先共通鍵：提供・預託データの暗号操作に利用する。

＜暗号化の対象となるデータ＞

・バックアップデータ
・通信データ（利用者データ）
・個人データの提供・預託データ

(5) バックアップ／リカバリ機能

TOEの障害に備えて、システムの復旧に必要なデータのバックアップを手動で行う。障害が発生した場合には、バックアップデータをリカバリすることによりTOEを復旧する。バックアップにおいては、DBのイメージコピーが作成される。

本機能は、不測の事態に運用を続けるためのデータのバックアップを目的とする。セキュリティ事故発生時の解析を行うことを目的とした監査証跡のバックアップには、基本機能における監査証跡退避機能が適している。

1.4.3. TOE の物理的範囲

コメント [CEM7]:
ASE_INT.1-9

図1-3の破線内に示されるコンポーネントがTOEの物理的範囲内である。

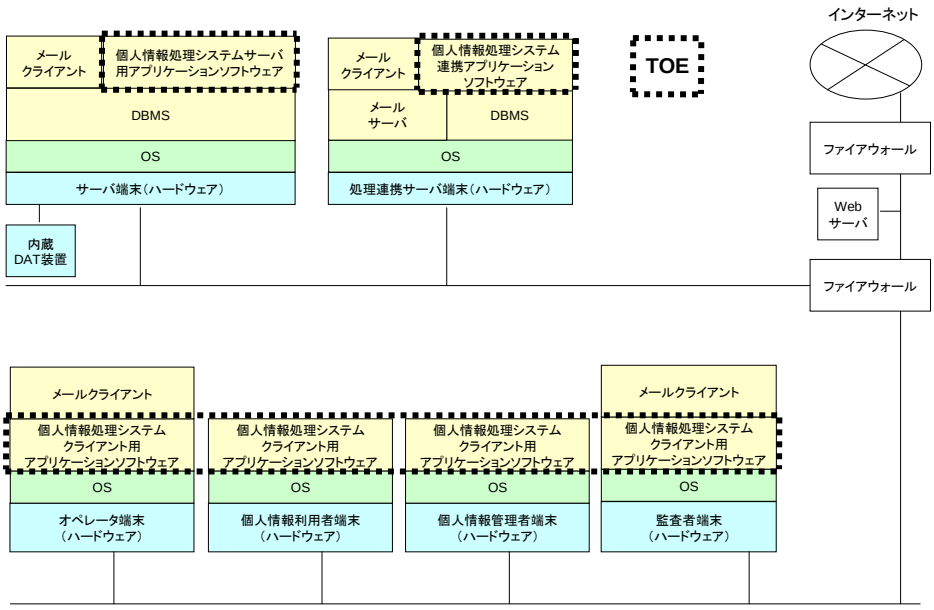


図 1-3　TOE 物理的範囲

図1-3に示したTOEを構成する各ツール、およびプログラムを以下に示す。

個人情報処理システムサーバ用アプリケーションソフトウェア：

サーバコンソール：

個人情報処理システムにおけるサーバを管理するために使われるGUI（グラフィカルユーザインタフェース）から構成される。システム管理GUI、サーバセットアップツール、及びデータベースセットアップツールがある。

システム管理GUI：基本機能、操作員管理機能、監査証跡参照機能、及びバックアップ／リカバリ機能についてのGUIを提供する。

サーバセットアップツール：

新規の個人情報処理システムのサーバをセットアップする。サーバのセットアップでは、監査証跡の最大容量の設定、個人情報処理システムサーバ用アプリケーションパッケージの管理者（サーバ管理者）の登録、及びサーバ公開鍵・秘密鍵の生成が行われる。

データベースセットアップツール：

サーバサブシステムからアクセスする各種データベースを作成する。このツールは、サーバセットアップに先立って実行される。

サーバサブシステム：

以下の機能を提供する。

基本機能、監査機能、操作員管理・アクセス制御機能、識別認証機能、暗号機能、及びバックアップ／リカバリ機能（1.4.2.2節参照）。

個人情報処理システム連携アプリケーションソフトウェア：

中継ツール：

顧客が行うインターネットを経由した個人情報の登録・更新・削除要求に対して、DMZ上のWebサーバから送信されてくるデータを受信し、処理連携サーバ端末のDBに格納する。さらに、オペレータの操作によってサーバ端末のDBに反映させる。

メール通知ツール：

DMZ上のWebサーバから受信したデータが、処理連携サーバ端末のDBに格納される都度、その旨をオペレータにメールで通知する。通知メールには、個人情報は含まれない。

バックアップ・リカバリツール：

処理連携サーバ端末上のDBをバックアップする。また、バックアップしたデータをリカバリする。

個人情報処理システムクライアント用アプリケーションソフトウェア：

持ち出し制御ツール：

個人データの持ち出しを制御する（個人データのクライアント端末・ネットワークドライブへの保存、画面コピーの禁止、印刷の禁止）。

暗号ツール：

サーバ端末との通信時に、通信データの暗号化/復号を行う。

※パッケージには、サーバ端末のセットアップ時に作成されたサーバ公開鍵が含まれる。サーバ公開鍵は、持ち出し制御ツールと同時にクライアント端末にインストールされる。

また、本 TOE を構成するガイダンス文書は以下の通りである。

- 個人情報処理システム インストールガイダンス
  [第一版 20070601]
- 個人情報処理システム 管理者ガイダンス [第一版 20070601]
- 個人情報処理システム 利用者ガイダンス [第一版 20070601]

2. 適合主張

2.1. CC 適合主張

本ST および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：

情報技術セキュリティ評価のためのコモンクライテリア
パート1: 概説と一般モデル バージョン 3.1 改訂第 4 版 ［翻訳第 1.0 版］
パート2: セキュリティ機能コンポーネント バージョン 3.1 改訂第 4 版 ［翻訳第 1.0 版］
パート3: セキュリティ保証コンポーネント バージョン 3.1 改訂第 4 版 ［翻訳第 1.0 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

EAL3適合

コメント [CEM8]:
ASE_CCL.1-1

コメント [CEM9]:
ASE_CCL.1-2
ASE_CCL.1-4

コメント [CEM10]:
ASE_CCL.1-3
ASE_CCL.1-5

コメント [CEM11]:
ASE_CCL.1-6

コメント [CEM12]:
ASE_CCL.1-7

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。
まず始めに、TOEのセキュリティに対する考え方について示す。

TOEに対する攻撃を行う者について、以下のとおり想定する。
1.4.1節で識別された人物のうち、TOEを管理する立場にあるサーバ管理者、監査者、及び個人情報管理者においては、信頼できる人物であり攻撃することは想定されない。ただし、意図せずTOEに対する攻撃となり得る操作を行うことは考えられる。一方、基本機能利用者のうち、個人情報利用者、及びオペレータにおいては、管理状態にない場合、不正な行為を行うことが想定される。また、サーバ管理者によりセキュアルームに入室が許可された者は、サーバ管理者にその行動が監視されるため、物理的な手法による攻撃は想定されない。
その他、攻撃が想定される者（以下、攻撃者と示す。）は、高度な専門知識を持たない、1.4.1節で識別された人物以外の者である。
これらの攻撃を行う者の主な動機としては、個人情報を入手することによって利益を得ることや、A社の業務妨害を目的として個人データを改ざん・破壊することが考えられる。

・機密性 : 保護資産である個人データは、顧客情報であり、故意・過失によらず暴露された時の影響は多大なものとなり、顧客からの信頼を損なう恐れがある。攻撃者は、社内 LAN 経由、または操作員の不在時に直接 TOE を利用することが考えられる。一方、リムーバブル媒体によって TOE より持ち出されたデータの盗難や紛失、ネットワークにおける伝送中データの取得による暴露が考えられる。よって、これらの TOE へのアクセスに関する機密性について考慮した。

・完全性 : 保護資産である個人データは、顧客情報でありサービス提供のために重要となる。顧客情報の改ざんやデータの紛失によって、顧客からの信頼を損なう恐れがある。攻撃者は、社内 LAN 経由による利用や、正当な操作員の不在時に直接 TOE を利用することが考えられる。また、顧客情報が保存されたリムーバブル媒体の紛失や、不正に改ざんされることが考えられる。一方、操作員の誤操作による顧客情報の改ざん、紛失が考えられる。よって、これらの改ざん、紛失に関する完全性について考慮した。

・可用性 : TOE はミッションクリティカルなシステムではないので、システムの二重化は考慮しない。また、システム構成上、DoS 攻撃については考慮不要である。一方、天災等によるデータ紛失によって、顧客情報が失われることは、以後のサービス提供に重大な影響を及ぼすため、データ紛失時にも確実に復旧できる必要がある。よって、不測の事態からの復旧が不可能とならないよう可用性について考慮した。

・責任追跡性 : 事件・事故時の原因究明や証拠保存のため、個人データの処理は誰が行ったのか、その処理の主体にたどるための記録の採取が必要となる。よって、TOE への操作に対する責任追跡性について考慮した。

・真正性 : 保護資産である個人データの受渡しが発生するのは、顧客から個人情報の提供を受ける際と、第三者に個人データを提供・預託する業務となる。顧客から個人情報の提供を受ける際、本人確認に関しては TOE の管理外であり、真正性については考慮不要である。提供・預託業務については、業務として真正性を要求する必要はないため、真正性については考慮不要である。

・信頼性 : TOE の意図した動作と結果に整合性を持たせるため、外部からの不正なプログラムや、ソフトウェアの既知の脆弱性による意図しない結果が生じないよう、システムの信頼性について考慮した。

3.1. 脅威

3.1.1. TOE 資産

本TOEの資産は、個人データから成る以下の利用者データである。

- 未登録個人データ（顧客が入力したDB未登録データ）
- 個人データ（保有個人データ）
- 個人データの提供データ
- 個人データの預託データ
- 個人データの加工データ
- 個人データに関する承認依頼データ（登録用）
- 個人データに関する承認依頼データ（更新用）
- 個人データに関する承認依頼データ（削除用）
- 個人データに関する承認依頼データ（提供用）
- 個人データに関する承認依頼データ（預託用）

TSFデータには、以下のようなデータがある。

- 識別・認証情報
- バナー表示メッセージ
- アクセスコントロール情報
- 監査証跡
- セキュリティ侵害の可能性を判断するために用いる監査証跡の重要度
- 操作員の最後に成功した認証以降の不成功認証試行回数
- 操作員種別毎のセション確立許可時間帯
- 暗号鍵

顧客が送信した未登録個人データは処理連携サーバ端末のDBに、これ以外の資産はすべてサーバ端末のDBに保存され、TOEによる保護対象となる。

上記の他、バックアップデータ（上記利用者データ、TSFデータ）がTOEによる保護対象資産である。バックアップデータ、及び提供・預託データが保存されたリムーバブル媒体は、不正に持ち出されないよう保管されるので、バックアップ媒体中のデータの完全性・機密性はセキュアルームに設置されるサーバ端末のDB内のデータと同等で十分である。

以降、特に断りのない限り、利用者データ、TSFデータ、及びバックアップデータは上記で記述した内容を指すものとする。

また、TOEが保護する個人データは、TOEの範囲内で管理された電子データに限り、TOEに登録される前などの紙媒体による個人データに関しては保護の対象とならない。考えられる脅威についても同様である。

3.1.2. 脅威

コメント [CEM13]:
ASE_SPD.1-1
ASE_SPD.1-2

T.ILLEGAL_LOGON（不正なログオン）
攻撃者が、許可なく TOE を利用したり、TOE の正当な利用者になりすまして TOE を利用したりすることにより、利用者データを破壊・改ざん・暴露するかもしれない。

T.UNAUTHORIZED_ACCESS（不正なアクセス）
TOE（クライアント端末）の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、故意に許可されていない操作（生成、参照、更新、削除、印刷、及び保存）を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。

T.MISUSE（誤操作）
TOE で利用される各端末の正当な操作員が、誤操作により利用者データを破壊・改ざん・暴露するかもしれない。

T.INJUSTICE（不正行為）
TOE（クライアント端末）の正当な基本機能利用者のうち、個人情報利用者、及びオペレータが、業務時間外など明らかに管理状態にない場合、TOE を利用し利用者データを暴露するかもしれない。

T.ILLEGAL_USE（不正な利用）
個人情報利用者、オペレータ、及び攻撃者が、TOE（クライアント端末）の正当な基本機能利用者の離席時にクライアント端末を利用して、利用者データを破壊・改ざん・暴露するかもしれない。

T.DISCLOSE_NW_DATA（ネットワークデータ暴露）
個人情報利用者、オペレータ、及び攻撃者が、サーバ端末とクライアント端末間のネットワーク上でやりとりされる通信データを、不正に入手することで利用者データを改ざん・暴露するかもしれない。

T.REMOVABLE_MEDIA（リムーバブル媒体）
個人情報利用者、オペレータ、及び攻撃者が、バックアップデータ、及び提供・預託データが保存されたリムーバブル媒体を不正に入手することで利用者データを改ざん・暴露するかもしれない。

T.UNEXPECTED_ACCIDENT（不測の事態）
火災、天災、ディスク障害、その他の不測の事態により、TOE の動作のために必要なデータが失われるかもしれない。

3.2. 組織のセキュリティ方針 *（抜粋）*

コメント [CEM14]: ASE_SPD.1-3

TOE が従うべき事項として、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（最終改訂：平成 21 年 10 月） 2.法令解釈指針・事例 2-2.個人情報取扱い事業者の義務等 2-2-3.個人データの管理（法第１９条～２２条関連）2-2-3-2.安全管理措置（法第２０条関連）」に規定される、「講じなければならない事項」を考慮する。

P.SAFE_PLACE（安全な建物）
TOE に関連するハードウェア（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、処理連携サーバ端末）は、A 社社員のみが入館できる建物内に設置され、個人データを取り扱う業務は、同所にて実施する。
[ガイドライン]の規程（物理的安全管理措置【各項目を実践するために講じることが望まれる手法の例示】①「入退館（室）管理」を実践するために講じることが望まれる手法の例示：個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施）を参考とする。

P.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
個人データが格納されている HDD は簡単に取り外されないように保護し、バックアップデータや外部出力された提供・預託データは権限のない者に持ち去られることがないように保護するため、個人データが保存される機器は許可された信頼できる者、または許可された者に認められその行動が監視される者のみが入室できる物理的に隔てられた場所に設置する。
[ガイドライン]の規程（物理的安全管理措置【各項目を実践するために講じることが望まれる手法の例示】①「入退館（室）管理」を実践するために講じることが望まれる手法の例示：個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置）を参考とする。

P.NETWORK（ネットワーク環境）
社内 LAN とインターネットとは、外部からの不正な侵入を防ぐ装置なしでの接続は許可しない。また、セキュアルームネットワークは、アプリケーションの機能に必要な通信以外の通過を禁止された特定箇所で社内 LAN に接続する。
[ガイドライン]の規程（技術的安全管理措置【各項目を実践するために講じることが望まれる手法の例示】②「個人データへのアクセス制御」を実践するために講じることが望まれる手法の例示：個人データを格納した情報システムへの無権限アクセスからの保護）を参考とする。

（中略）

3.3. 前提条件

コメント [CEM15]: ASE_SPD.1-4

A.TRUST_SEVER_ADMIN（信頼できるサーバ管理者）
サーバ管理者は TOE の利用に際して課せられた役割に責任を持ち、不正な行為を行わないものとする。

A.TRUST_AUDITOR（信頼できる監査者）
監査者は TOE の利用に際して課せられた役割に責任を持ち、不正な行為を行わないものとする。

A.TRUST_INFO_ADMIN（信頼できる個人情報管理者）
個人情報管理者は TOE の利用に際して課せられた役割に責任を持ち、不正な行為を行わないものとする。

A. COMPLICATED_PASSWORD（推測しにくいパスワード）
すべての操作員は、他から推測しにくい認証情報（パスワード）を設定するものとする。

4. セキュリティ対策方針

コメント [CEM16]:
ASE_OBJ.2-1

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、およ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（操作員の識別認証）
TOEは、操作員がTOEを利用する時は必ず識別認証されることを保証し、指定された回数以内に識別認証に成功した操作員のみTOEの利用を許可しなければならない。また、認証情報の推測を防止するために、設定する認証情報の品質を保証しなければならない。

O.ACCESS_CONTROL（アクセスコントロール）
TOEは、操作員または操作員を代行するプロセスに対して、各操作員の種別とその操作対象に応じて設定･付与された権限に従った、保護資産へのアクセスを保証しなければならない。

O.TAKE_OUT（クライアント端末を経由したTOE外への利用者データの持ち出し）
TOEは、クライアント端末を経由した利用者データのTOE外への持ち出し（保存、印刷）を禁止しなければならない。

O.AUDIT（監査）
TOEは、特定の事象が発生した場合これを監査証跡として保管しなければならない。監査証跡は、TOEのセキュリティ侵害の事後調査における記録として利用されるため、以下を満たすことが必要となる。
・監査証跡には、事象の日付・時刻、事象個所、及び事象に責任を持つ主体を含め生成されること。
・対象となるすべての監査事象を監査証跡として取得すること。
・監査証跡の改ざんを防御し、これを検出できること。
・監査証跡は許可された利用者である監査者及びサーバ管理者のみが許可された範囲の利用ができること。

O.ALERT（アラート）
TOEは、TOEに対するセキュリティ侵害の可能性を検知しなければならない。またセキュリティ侵害の可能性を検知した場合、サーバ管理者及び監査者に対してその可能性について通知しなければならない。

O.RECOMMEND（勧告）
TOEは、利用者セション確立前に、TOEの不正な使用に関する勧告的警告メッセージを表示しなければならない。

O.AUTO_LOGOUT（自動ログアウト）
TOEは、TOEにログオンした操作員から、一定時間TOEへのアクセスがないとき、自動的にログアウトを行わなければならない。

O.USERDATA_PROTECTION（利用者データの保護）
TOEは、以下のデータを秘匿し、改ざんを検出できなければならず、それぞれに対し許可された操作員や端末のみがデータを利用することができなければならない。
・サーバ管理者が、バックアップデータを利用することができる。
・個人情報管理者、及び個人情報利用者が、個人データの提供・預託データを利用することができる。

・サーバ端末ークライアント端末間で通信される利用者データは、当該端末が利用することができる。

O.BACKUP_RECOVERY（バックアップ／リカバリ）
TOEは、TOEが正常に動作するために必要な利用者データ及びTSFデータをバックアップする手段を提供しなければならない。また、バックアップした利用者データ及びTSFデータを、TOEの動作を復旧させるためにTOEへリカバリする手段を提供しなければならない。

O.AVAILABLE_TIME_RESTRICTION（利用時間制限）
TOEは、管理されたセション確立可能な時間に基づき、セションの確立を制限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 *（抜粋）*

OE.AUTHORIZATION_SETTING（権限の設定）
組織の責任者は、TOEに関連する権限・役割をもつ操作員として個人情報管理者、サーバ管理者、及び監査者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当てなければならない。個人情報管理者は、オペレータ、及び個人情報利用者の任命・管理を組織の責任者から委任され、TOEに関連する権限・役割をもつ操作員としてオペレータ、及び個人情報利用者を任命し、それぞれの権限付与の規定が載っている規則を参照して、それに基づいて権限を付与することにより、TOEに対し行える操作を割り当てなければならない。

OE.TRUSTED_ROLE（信頼される役割）
組織の責任者は、サーバ管理者、監査者、及び個人情報管理者の役割に適した者を人選し、その上で、それぞれの役割を理解させる。

OE.PASSWORD_MANAGEMENT（操作員によるパスワードの管理）
すべての操作員は、TOEサービスを提供するシステムにアクセスするための認証情報（パスワード）を記憶し、他人に漏らしてはならない。 また推測・解析されやすい認証情報（パスワード）を設定してはならず、適正な間隔で変更しなければならない。

OE.TRAINING（教育・訓練）
すべての操作員は、個人データ及びTOEの安全管理に関する操作員の役割及び責任についての教育・訓練を受けなければならない。

OE.BACKUP_MEDIA（バックアップ媒体）
TOEのバックアップデータ、及び提供・預託データが保存されたリムーバブル媒体は、入退室管理を実施している物理的に保護された室内、及びTOEの遠隔地に所在し入退室管理を実施している物理的に保護された室内において施錠保管され、耐用年数を考慮した運用がなされなければならない。

OE.TIME_STAMP（高信頼タイムスタンプ）
TOEでは、監査証跡を生成する際、及び利用時間制限を行う際に、高信頼タイムスタンプが利用できなければならない。

OE.SAFE_PLACE（安全な建物）
オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末は、A社社員のみが入館できるよう入退館管理される建物内に設置され、個人データを取り扱う業務は同所にて実施されなければならない。

OE.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
サーバ端末、処理連携サーバ端末、及び個人データが格納されたリムーバブル媒体は、入退室管理（サーバ管理者として許可されている者、及びサーバ管理者に許可された者に制限）されている室内に設置されなければならない。なおサーバ管理者は、自身が許可した者を入室させた場合、その者の行動を監視する必要がある。

OE.NETWORK（ネットワーク環境）
社内LANと外部ネットワークとの間には、必要な通信のみに制限する設定がなされたファイアウォールを設置し、不要なパケットの流入を防ぐ。またセキュアルームネットワークは、TOEの機能に必要な通信のみに制限する設定がなされたファイアウォールを介して社内LANと接続する。

（中略）

4.3. セキュリティ対策方針根拠　*（抜粋）*

コメント [CEM17]:
ASE_OBJ.2-2
ASE_OBJ.2-3

セキュリティ対策は、セキュリティ課題定義で規定した脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針の対応関係を表 4-1 に示す。

表 4-1　セキュリティ対策方針と対抗する脅威、組織セキュリティ方針及び前提条件

	T.ILLEGAL_LOGIN	T.UNAUTHORIZED_ACCESS	T.MISUSE	T. INJUSTICE	T.ILLEGAL_USE	T.DISCLOSE_NW_DATA	T.REMOVABLE_MEDIA	T.UNEXPECTED_ACCIDENT	P.SAFE_PLACE	P.FACILITIES_IN_SECURE_ROOM	P.NETWORK	P.UNJUST_SOFTWARE	P.RECOMMEND	A.TRUST_SEVER_ADMIN	A.TRUST_AUDITOR	A.TRUST_INFO_ADMIN	A.COMPLICATED_PASSWORD
O.I&A	×																
O.ACCESS_CONTROL		×	×														
O.TAKE_OUT		×	×														
O.AUDIT		×		×													
O.ALERT		×		×													
O.RECOMMEND													×				
O.AUTO_LOGOUT					×												
O.USERDATA_PROTECTION						×	×										
O.BACKUP_RECOVERY								×									
O.AVAILABLE_TIME_RESTRICTION				×													
OE.AUTHORIZATION_SETTING		×															
OE.TRUSTED_ROLE		×		×										×	×	×	
OE.PASSWORD_MANAGEMENT	×																×
OE.TRAINING			×	×										×	×	×	
OE.BACKUP_MEDIA								×									
OE.TIME_STAMP		×		×													
OE.SAFE_PLACE									×								
OE.FACILITIES_IN_SECURE_ROOM										×							
OE.NETWORK											×						
OE.UNJUST_SOFTWARE												×					

表 4-1 により、各セキュリティ対策方針は一つ以上の脅威、及び組織のセキュリティ方針に対応している。

次に、各脅威がセキュリティ対策方針で対抗できること、各組織のセキュリティ方針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。

説明の中では、各脅威に対して攻撃者を明示し、攻撃者が行う想定される攻撃方法を分析する。次に、攻撃方法に対抗するための有効な対策内容を示し、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。なお、対策内容は、一つ以上のセキュリティ対策方針がそれを満たし、脅威に対するセキュリティ対策方針として必要であることを示す。

○脅威

コメント [CEM18]:
ASE_OBJ.2-4

T.ILLEGAL_LOGON（不正なログオン）

この脅威は、1.4.1 節で識別された者以外の高度な専門知識を持たない攻撃者によって実行される。この脅威には以下の 2 つの内容が含まれる。それぞれに有効な対抗策について以下に述べる。

a. 利用を許可されていない者が、許可なく TOE を利用する。

この攻撃に対しては、TOE の利用において識別・認証を行い、TOE の利用を正当な者のみに制限することにより対抗できる。この対抗策に該当するセキュリティ対策方針は、O.I&A である。

b. 正当な利用者になりすまして TOE を利用する。

a の対抗策が有効に働くためには、識別･認証に用いられる情報を管理し、不正利用による利用許可者へのなりすましを防止する必要がある。識別・認証情報の不正取得の方法は、正当な操作員からの取得、攻撃者による類推の 2 種類がある。

正当な操作員からの識別・認証情報の取得、及び類推による識別認証情報の取得については、正当な操作員に対して認証情報の決定方法（認証情報を他人に教えない。認証情報は推測・類推されにくいものにする。認証情報は適切な間隔で変更する。）を教育することで対抗できる。また、類推により識別・認証情報を不正に取得されないように、設定する認証情報の品質を保証すると共に、誤った識別認証の連続試行を制限する。この対抗策に該当するセキュリティ対策方針は、O.I&A、及び OE.PASSWORD_MANAGEMENT である。

以上、a、b すべての攻撃方法に対抗することは、T.ILLEGAL_LOGIN に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.I&A、及び OE.PASSWORD_MANAGEMENT によって、T.ILLEGAL_LOGIN に対抗できる。

T.UNAUTHORIZED_ACCESS（不正なアクセス）

この脅威は、基本機能利用者（個人情報利用者、及びオペレータ）によって実行される。個人情報利用者、及びオペレータがとり得る具体的な不正アクセスの方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 許可されていない操作を行う。

この攻撃に対しては、TOE の各操作に対して権限を設定し、操作員毎に許可／禁止される操作を明確にすることで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.ACCESS_CONTROL である。

b. クライアント端末を用いて TOE 外へ利用者データを持ち出す。

この攻撃は、上記 a により参照可能な権限が付与された利用者に対し、参照した利用者データを TOE 外へ持ち出すことであり、この攻撃に対しては、クライアント操作員が用いるクライアント端末を経由したサーバ端末外部への保存と印刷を禁止することで対抗できる。この対抗策に該当するセキュリティ対策方針は、O.TAKE_OUT である。

c. 許可されていない操作について、許可するように権限を改ざんする。

この攻撃に対しては､TOE の各操作に対する権限設定を行える者を制限することによって対抗できる。この対抗策に該当するセキュリティ対策方針は、OE.AUTHORIZATION_SETTING である。

d. 許可されている操作を総当りで探索する。

この攻撃に対しては、許可されている操作を探索している操作を検出することが有効である｡TOE で発生した事象についての正確な時刻に裏づけされた記録を採取し、その記録の中から攻撃の可能性を検知した時、その結果を TOE の保護に責務がある者に通知することにより、TOE の保護のための適切な事前処置を促す。この対抗

策に該当するセキュリティ対策方針は、記録の採取については O.AUDIT、及び OE.TIME_STAMP、通知については O.ALERT、TOE 保護の責務に関しては OE.TRUSTED_ROLE である。

以上、a、b、c、d すべての攻撃方法に対抗することは、T.UNAUTHORIZED_ACCESS に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.ACCESS_CONTROL、O.TAKE_OUT、O.AUDIT、O.ALERT、OE.TRUSTED_ROLE、及び OE.AUTHORIZATION_SETTING によって、T.UNAUTHORIZED_ACCESS に対抗できる。

（中略）

○組織のセキュリティ方針

コメント [CEM19]: ASE_OBJ.2-5

P.SAFE_PLACE（安全な建物）

この組織のセキュリティ方針は、TOE に関連するハードウェアが設置される場所、及び個人データを取り扱う業務が実施される場所に関するものである。それぞれに有効な対策方針について以下に述べる。

a. TOE を設置する建物を制限する。

TOE（オペレータ端末、個人情報利用者端末、個人情報管理者端末、サーバ端末、監査者端末、及び処理連携サーバ端末）は、入退館管理される建物内に設置し、A 社社員のみが入館できるように管理される。この方針に応じるための環境セキュリティ対策方針は、OE.SAFE_PLACE である。

b. 個人データを取り扱う業務は、同所にて実施する。

TOE を設置した建物内においてのみ、個人データを取り扱うことを許可する。この方針に応じるための環境セキュリティ対策方針は、OE.SAFE_PLACE である。

以上、a、b すべてに応じることは、P.SAFE_PLACE に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.SAFE_PLACE の達成によって P.SAFE_PLACE が実装される。

P.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）

この組織のセキュリティ方針は、個人データが格納された HDD またはリムーバブル媒体の、持ち出し保護に関するものである。有効な対策方針について以下に述べる。

a. 個人データが格納される機器を設置する、及びリムーバブル媒体を保管する部屋を制限する。

個人データが格納されるサーバ端末、処理連携サーバ端末、及びリムーバブル媒体は、許可された者のみ入室が可能な室内に設置・保管する。この方針に応じるための環境セキュリティ対策方針は、OE.FACILITIES_IN_SECURE_ROOM である。

b. 入室を許可するものを制限する。

入室が許可されるものは、サーバ管理者として許可されている者、及びサーバ管理者に許可された者のみとする。この方針に応じるための環境セキュリティ対策方針は、OE.FACILITIES_IN_SECURE_ROOM である。

以上、a、b すべてに応じることは、P.FACILITIES_IN_SECURE_ROOM に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.FACILITIES_IN_SECURE_ROOM の達成によって

P.FACILITIES_IN_SECURE_ROOM が実装される。

（中略）

○前提条件

コメント [CEM20]:
ASE_OBJ.2-6

A.TRUST_SEVER_ADMIN（信頼できるサーバ管理者）

この前提条件は、サーバ管理者は TOE の利用に際して課せられた役割に責任を持ち、不正な行為を行わないとするものである。有効な対策方針について以下に述べる。

a. 組織の責任者は、サーバ管理者の役割に適した者を人選する。

この方針に応じるための環境セキュリティ対策方針は、OE.TRUSTED_ROLE である。

b. 人選したサーバ管理者に対して役割を理解させるため教育を実施する。

この方針に応じるための環境セキュリティ対策方針は、OE.TRAINING である。

以上、a、b すべてに応じることは、A.TRUST_SEVER_ADMIN に応じることである。したがって OE.TRUSTED_ROLE、及び OE.TRAINING の実施により、A.TRUST_SEVER_ADMIN が保証される。

（中略）

5. 拡張コンポーネント定義

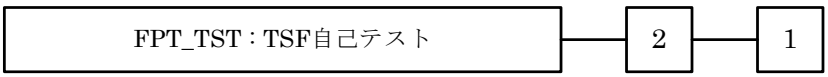
5.1. 拡張機能コンポーネント

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 FPT_TST.2 を定義する。このコンポーネントは FPT（TSF の保護）クラス、FPT_TST（TSF 自己テスト）ファミリの拡張コンポーネントとして定義される。また、本コンポーネントは完全性を検証する範囲を TSF データ、TSF データの一部、TSF、もしくは TSF の一部から選択が可能であり、完全性検証の範囲を TSF データ、もしくは TSF データの一部から選択、且つ、TSF、もしくは TSF の一部から選択としている FPT_TST.1 の簡易版（下位階層）という位置付けとして定義される。

以下に、CC パート 2 で定義される FPT_TST ファミリに対して、変更が生じる箇所を示す。

TSF 自己テスト（FPT_TST）

コンポーネントのレベル付け



FPT_TST.2　簡易 TSF テストは、TSF の正しい運用をテストする能力を提供する。これらのテストは、作動すべき条件が満たされた時に実行することができる。また、このテストは、（一部もしくは全ての）TSF の完全性を検証する能力、および（一部もしくは全ての）TSF データの完全性を検証する能力を提供する。

管理：FPT_TST.2
以下のアクションは FMT における管理機能と考えられる:

- TSF 自己テストが動作する条件の管理

監査：FPT_TST.2
FAU_GEN1 セキュリティ監査データ生成が 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：
- 最小：TSF 自己テストが成功した場合のテスト結果
- 基本：TSF 自己テストの実行とテスト結果
- 詳細：自己テストが作動すべき条件の変更

FPT_TST.2　簡易 TSF テスト
下位階層：　なし
依存性：　　なし

FPT_TST.2.1　TSF は、[割付：自己テストが作動すべき条件]下で、自己テストを実行しなければならない。
FPT_TST.2.2　TSF は、自己テストを行うことによって、[選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]の完全性を検証することができなければならない。

コメント [CEM21]:
ASE_ECD.1-1
ASE_ECD.1-2
ASE_ECD.1-3
ASE_ECD.1-4
ASE_ECD.1-5
ASE_ECD.1-12
ASE_ECD.1-13

6. セキュリティ要件

コメント [CEM22]:
ASE_REQ.2-13

本章では、セキュリティ要件を記述する。

6.1. セキュリティ機能要件 *（抜粋）*

コメント [CEM23]:
ASE_REQ.2-1
ASE_REQ.2-3
ASE_REQ.2-4
ASE_REQ.2-5
ASE_REQ.2-6
ASE_REQ.2-7
ASE_REQ.2-8

TOE が提供するセキュリティ機能要件を記述する。

○セキュリティ監査（FAU）

FAU_ARP.1 セキュリティアラーム

下位階層： なし
依存性： FAU_SAA.1 侵害の可能性の分析

FAU_ARP.1.1 TSF は、セキュリティ侵害の可能性が検出された場合、[割付: アクションのリスト]を実行しなければならない。

[割付：アクションのリスト]：サーバ管理者、監査者へのアラート通知

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。

[詳細化]：格納された → サーバ端末の DB に格納された

FAU_STG.1.2 TSF は、監査証跡内の監査記録への不正な改変を[選択：防止、検出：から一つのみ選択]できねばならない。

[詳細化]：監査証跡内の → サーバ端末の DB に格納された監査証跡内の

[選択：防止、検出：から一つのみ選択]：防止

＜CC パート 2 より抜粋＞

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、検出*: から 1 つのみ選択]できなければならない。**

○識別と認証（FIA）

FIA_AFL.1 認証失敗時の取り扱い

下位階層： なし
依存性： FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト] ：
・最後に成功した認証以降の各クライアント操作員の認証
・最後に成功した認証以降の各サーバ管理者の認証
[選択：[割付：正の整数値], 「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：「1～5 回内における管理者設定可能な正の整数値」

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：アクションのリスト]をしなければならない。

[割付：アクションのリスト]：表 6-1 に示す。

表 6-1 TOE へのアクセスを管理する規則

認証事象	アクション
最後に成功した認証以降の各クライアント操作員の認証	アカウントをロックし、解除不可能にする。
最後に成功した認証以降の各サーバ管理者の認証	アカウントを 5 分間無効化する。その後、不成功認証試行回数を 0 にする。

＜注釈＞
ロックされたアカウントを復旧する場合は､個人情報管理者もしくはサーバ管理者が当該アカウントを削除し、再度アカウントを作成する。
・個人情報管理者が復旧できるアカウント：オペレータ、個人情報利用者
・サーバ管理者が復旧できるアカウント：個人情報管理者、監査者

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: セキュリティ属性のリスト]

[割付：セキュリティ属性のリスト]：

{操作員種別（オペレータ、個人情報利用者、個人情報管理者、サーバ管理者、監査者）}

FIA_SOS.1 秘密の検証

下位階層： なし
依存性： なし

FIA_SOS.1.1　TSF は、秘密が[割付 : 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]：　以下の品質尺度

＜品質尺度＞

・操作員のパスワードは 6 文字以上 10 文字以下の、以下の範囲の ASCII 文字が使用できる。

・アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字。

・数字は、[0-9]の合計 10 文字。

・記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字。

・1 文字以上の数字または記号を含む。

・2 文字以上のアルファベットを含む（大文字、小文字は区別される）。

・新しいパスワードは、直前のパスワードと同一であってはならない。

FIA_UAU.1a 認証のタイミング（クライアント操作員）

下位階層：　なし
依存性：　FIA_UID.1 識別のタイミング

FIA_UAU.1.1.a　TSF は、利用者が認証される前に利用者を代行して行われる[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化] : 利用者 → クライアント操作員

[割付 : TSF 仲介アクションのリスト] :
・勧告的警告メッセージの表示
・セション鍵生成
・クライアント端末用パッケージの正当性検証
・クライアント操作員の識別

FIA_UAU.1.2.a　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、各利用者に認証が成功することを要求しなければならない。

[詳細化]：　利用者 → クライアント操作員

FIA_UAU.1b 認証のタイミング（サーバ管理者）

下位階層：　なし
依存性：　FIA_UID.1 識別のタイミング

FIA_UAU.1.1.b　TSF は、利用者が認証される前に利用者を代行して行われる[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]：　利用者 → サーバ管理者

[割付 : TSF 調停アクションのリスト] :
・勧告的警告メッセージの表示
・サーバ管理者の識別

FIA_UAU.1.2.b　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、各利用者に認証が成功することを要求しなければならない。

[詳細化]：　利用者 → サーバ管理者

FIA_UID.1a 識別のタイミング（クライアント操作員）

下位階層： なし
依存性： なし

FIA_UID.1.1a TSF は、利用者が識別される前に利用者を代行して実行される[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]： 利用者 → クライアント操作員

[割付：TSF 仲介アクションのリスト]：
・勧告的警告メッセージの表示
・セション鍵生成
・クライアント端末用パッケージの正当性検証

FIA_UID.1.2a 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。

[詳細化]： 利用者 → クライアント操作員

FIA_UID.1b 識別のタイミング（サーバ管理者）

下位階層： なし
依存性： なし

FIA_UID.1.1b TSF は、利用者が識別される前に利用者を代行して実行される[割付：TSF 仲介アクションのリスト]を許可しなければならない。

[詳細化]：利用者 → サーバ管理者

[割付：TSF 仲介アクションのリスト]：
・勧告的警告メッセージの表示

FIA_UID.1.2b TSF は､その利用者を代行する他の TSF 調停アクションを仲介する前に、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。

[詳細化]： 利用者 → サーバ管理者

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: 利用者セキュリティ属性のリスト]

[割付：利用者セキュリティ属性のリスト]：操作員種別

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない：[割付：属性の最初の関連付けに関する規則]

[割付：属性の最初の関連付けに関する規則]：

表 6-2 に示す

表 6-2　属性の最初の関連付けに関する規則

利用者	利用者を代行して動作するサブジェクト	利用者セキュリティ属性（操作員種別）
サーバ管理者	サーバ管理者プロセス	サーバ管理者
監査者	監査者プロセス	監査者
個人情報管理者	個人情報管理者プロセス	個人情報管理者
オペレータ	オペレータプロセス	オペレータ
個人情報利用者	個人情報利用者プロセス	個人情報利用者

FIA_USB.1.3　TSF は、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：　属性の変更に関する規則]

[割付：属性の変更に関する規則] :

操作員種別を変更する役割は存在しない。

○セキュリティ管理（FMT）

FMT_MTD.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　TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]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。

[割付：TSF データのリスト] : 表 6-3 に示す。

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]] : 表 6-3 に示す。

[割付：その他の操作] : 表 6-3 に示す。

[割付：許可された識別された役割] : 表 6-3 に示す。

表 6-3　TSF データの管理

TSF データ	選択：デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
セキュリティ侵害の可能性を判断するために用いる監査証跡の重要度	改変	監査者
サーバ管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
サーバ管理者のパスワード	作成	サーバ管理者

TSF データ	選択：デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
監査者、個人情報管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
監査者、個人情報管理者のパスワード	削除、作成	サーバ管理者
オペレータ、個人情報利用者の 操作員 ID	問い合わせ、削除、作成	個人情報管理者
オペレータ、個人情報利用者の パスワード	削除、作成	個人情報管理者
操作員自身のパスワード	改変	オペレータ 個人情報利用者 個人情報管理者 サーバ管理者 監査者
サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
処理連携サーバ共通鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ秘密鍵	問い合わせ、改変、削除、作成	サーバ管理者
サーバ公開鍵	問い合わせ、改変、削除、作成	サーバ管理者
	問い合わせ	オペレータ 個人情報利用者 個人情報管理者 監査者
提供・預託先共通鍵	問い合わせ、削除、インポート	サーバ管理者
	問い合わせ	個人情報管理者
セション鍵	問い合わせ、削除、作成	オペレータ 個人情報利用者 個人情報管理者 監査者
操作員の最後に成功した認証以降の不成功認証試行回数の定義	問い合わせ、改変	サーバ管理者
バナー表示メッセージ	問い合わせ、改変、作成	サーバ管理者
操作員種別毎のセション確立許可時間帯	問い合わせ、改変、作成	サーバ管理者
監査証跡	問い合わせ、削除、エクスポート、インポート	監査者
	問い合わせ	サーバ管理者

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: TSF によって提供される管理機能のリスト]

[割付：TSF によって提供されるセキュリティ管理機能のリスト]：表 6-4 に示す。

表 6-4　セキュリティ管理機能の特定

機能要件	管理要件	管理項目
FAU_ARP.1	1）アクションの管理(追加、除去、改変)。	なし（アクションは固定であり、管理対象とならない）
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAA.1	1）規則のセットから規則を(追加、改変、削除)することによる規則の維持。	セキュリティ侵害の可能性の判断に用いる監査データの重要度の管理
FAU_SAR.1	1）監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	なし（アクションは固定であり、管理対象とならない）
FAU_SAR.2	なし	なし
FAU_SAR.3	なし	なし
FAU_STG.1	なし	なし
FAU_STG.3	1）閾値の維持; 2）監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。	なし（閾値、アクションは固定であり、管理対象とならない）
FAU_STG.4	1）監査格納失敗時にとられるアクションの維持（削除、改変、追加）。	なし（アクションは固定であり、管理対象とはならない）
FCS_CKM.1	1）暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし（アクションは固定であり、管理対象とならない）
FCS_CKM.4	1）暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし（アクションは固定であり、管理対象とならない）
FCS_COP.1	なし	なし
FDP_ACC.1a	なし	なし
FDP_ACC.1b	なし	なし
FDP_ACF.1a	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。	なし （変更不可のため管理項目はない）
FAU_ARP.1	1）アクションの管理(追加、除去、改変)。	なし（アクションは固定であり、管理対象とならない）

機能要件	管理要件	管理項目
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAA.1	1) 規則のセットから規則を(追加、改変、削除)することによる規則の維持。	セキュリティ侵害の可能性の判断に用いる監査データの重要度の管理
FAU_SAR.1	1) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	なし（アクションは固定であり、管理対象とならない）
FDP_ACF.1b	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	なし （変更不可のため管理項目はない）
FDP_ETC.2	なし	なし
FDP_ITC.2	1) インポートに対して使用される追加の制御規則の改変。	なし（アクションは固定であり、管理対象とならない）
FIA_AFL.1	1) 不成功の認証試行に対する閾値の管理 2) 認証失敗の事象においてとられるアクションの管理	1) 不成功の認証試行に対する閾値の管理 2) なし（アクションは固定であり、管理対象とならない）
FIA_ATD.1	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（アクションは固定であり、管理対象とならない）
FIA_SOS.1	1) 秘密の検証に使用される尺度の管理	なし（アクションは固定であり、管理対象とならない）
FIA_UAU.1a	1) 管理者による認証データの管理 2) 関係する利用者による認証データの管理 3) 利用者が認証される前にとられるアクションのリストを管理すること	1) クライアント操作員のパスワードの登録 2) クライアント操作員のパスワードの改変 3) なし（アクションは固定であり、管理対象とならない）
FIA_UAU.1b	1) 管理者による認証データの管理 2) 関係する利用者による認証データの管理 3) 利用者が認証される前にとられるアクションのリストを管理すること	1) サーバ管理者のパスワードの登録 2) サーバ管理者のパスワードの改変 3) なし（アクションは固定であり、管理対象とならない）
FIA_UID.1a	1) 利用者識別情報の管理 2) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	1) クライアント操作員 ID の作成、問い合わせ、削除 2) なし（アクションは固定であり、管理対象とならない）
FIA_UID.1b	1) 利用者識別情報の管理 2) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること	1) サーバ管理者 ID の作成、問い合わせ、削除 2) なし（アクションは固定であり、管理対象とならない）

機能要件	管理要件	管理項目
FIA_USB.1	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 2) 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変更できる	1) サーバ管理者はサーバ管理者、監査者、個人情報管理者の操作員種別を付与でき、個人情報管理者はオペレータと個人情報利用者の操作員種別を付与できる 2) なし（許可する役割はない）
FMT_MSA.3	1) 初期値を特定できる役割のグループを管理すること 2) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること	1) なし（初期値を特定できる役割は存在しない） 2) なし（管理する役割はない）
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	なし（TSF データと相互に影響を及ぼし得る役割のグループは固定）
FMT_SMF.1	なし	なし
FMT_SMR.2	1) 役割の一部をなす利用者のグループを管理すること 2) 役割が満たさなければならない条件を管理すること	なし（役割の一部をなす利用者のグループ、役割が満たさなければならない条件は固定）
FTA_SSL.3	1) 個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定 2) 対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定	なし（アクションは固定であり、管理対象とならない）
FTA_TAB.1	1) 許可管理者によるバナーの維持	1) バナー表示メッセージの管理
FTA_TSE.1	1) 許可管理者によるセション確立条件の管理	1) 操作員種別毎のセション確立許可時間帯の管理
FPT_TST.2	1) TSF 自己テストが動作する条件の管理	なし（アクションは固定であり、管理対象とはならない）
FPT_STM.1	1) 時間の管理	なし（システム内時刻の管理は、OS により行われるため、管理対象とならない）

FMT_SMR.2 セキュリティ役割における制限

下位階層： FMT_SMR.1

依存性： FIA_UID.1 識別のタイミング

FMT_SMR.2.1 TSF は、役割[割付：許可された識別された役割]を維持しなければならない。

[割付：許可された識別された役割]：

・オペレータ

・個人情報利用者

・個人情報管理者

・サーバ管理者

・監査者

FMT_SMR.2.2 TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.2.3 TSF は、条件[割付：異なる役割に対する条件]が満たされていることを保証しなければならない。

[割付：異なる役割に対する条件]：

一つの操作員アカウントは、オペレータ、個人情報利用者、個人情報管理者、サーバ管理者、監査者を兼ねられない。

○TSF の保護（FPT）

FPT_TST.2 簡易 TSF テスト

下位階層： なし
依存性： なし

FPT_TST.2.1 TSF は、[割付：自己テストが作動すべき条件]下で、自己テストを実行しなければならない。

[割付：自己テストが作動すべき条件]：
クライアント操作員がクライアント端末を利用してサーバ端末に対しアクセスする時の、識別認証が行われる前

FPT_TST.2.2 TSF は、自己テストを行うことによって、[選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]の完全性を検証することができなければならない。

[選択：[割付：TSF の一部]、TSF 全体、[割付：TSF データの一部]、TSF データ全体]：

[割付：TSF の一部]：個人情報処理システムクライアント用アプリケーションパッケージ

6.2. セキュリティ保証要件

コメント [CEM24]:
ASE_REQ.2-2

TOE セキュリティ保証要件を示す。
本 TOE の評価保証レベルは EAL3 である。全てのセキュリティ保証要件は CC パート 3 に規定されているセキュリティ保証コンポーネントを直接使用する。

(1) 開発（ADV）
- ADV_ARC.1 ：セキュリティアーキテクチャ記述
- ADV_FSP.3 ：完全な要約を伴う機能仕様
- ADV_TDS.2 ：アーキテクチャ設計

(2) 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

(3) ライフサイクルサポート（ALC）
- ALC_CMC.3 ：許可の管理
- ALC_CMS.3 ：実装表現の CM 範囲
- ALC_DEL.1 ：配付手続き
- ALC_DVS.1 ：セキュリティ手段の識別
- ALC_LCD.1 ：開発者によるライフサイクルモデルの定義

(4) 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

(5) テスト（ATE）
- ATE_COV.2 ：カバレージの分析
- ATE_DPT.1 ：テスト：基本設計
- ATE_FUN.1 ：機能テスト
- ATE_IND.2 ：独立テスト – サンプル

(6) 脆弱性評定（AVA）
- AVA_VAN.2 ：脆弱性分析

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

コメント [CEM25]:
ASE_REQ.2-10
ASE_REQ.2-11

セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 6-5 に示す。この表で示す通り、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対抗している。

表 6-5 セキュリティ機能要件とセキュリティ対策方針の対応関係（抜粋）

	O.I&A	O.ACCESS_CONTROL	O.TAKE_OUT	O.AUDIT	O.ALERT	O.RECOMMEND	O.AUTO_LOGOUT	O.USERDATA_PROTECTION	O.BACKUP_RECOVERY	O.AVAILABLE_TIME_RESTRICTION
FAU_ARP.1					×					
FAU_GEN.1				×						
FAU_GEN.2				×						
FAU_STG.1				×						
FAU_STG.3				×						
FAU_STG.4				×						
FCS_CKM.1								×		
FCS_CKM.4								×		
FCS_COP.1								×		
FDP_ITC.2									×	
FIA_AFL.1	×									
FIA_ATD.1	×	×								
FIA_SOS.1	×									
FIA_UAU.1a	×									
FIA_UAU.1b	×									
FIA_UID.1a	×									
FIA_UID.1b	×									
FIA_USB.1	×	×								
FMT_MSA.3		×	×							
FMT_MTD.1	×	×		×				×		
FMT_SMF.1	×	×								
FMT_SMR.2	×	×								
FTA_SSL.3							×			
FTA_TAB.1						×				
FTA_TSE.1										×
FPT_TST.2			×							

次に、各 TOE セキュリティ対策方針が、セキュリティ機能要件により実現できることを説明する。

各セキュリティ対策方針に対し、必要な対策の詳細を分析する。次に、それぞれの対策に対し、要求される機能を示し、それがすべて満たされることでセキュリティ対策方針を実現することができることを示す。なお、要求される機能については、一つ以上のセキュリティ機能要件がそれを満たし、セキュリティ対策方針に対する機能要件として必要であることを示す。

O.I&A（識別認証）

この TOE セキュリティ対策方針は、正当な操作員が TOE を利用するための、利用者の制限を求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. TOE 利用前に、操作員を識別する。

操作員が TOE を利用する前には、利用を許可されている者であることが識別されなければならない。よって、操作員が識別される前に実行が許可される TSF は、操作員を識別するための TSF のみである。ただし、クライアント操作員の識別時には、勧告的警告メッセージの表示、セション鍵生成、及びクライアント端末用パッケージの正当性検証も許可される。また、サーバ管理者の識別時には、勧告的警告メッセージの表示も許可される。この要件に該当するセキュリティ機能要件は、FIA_UID.1a、及び FIA_UID.1b である。

b. TOE 利用前に、操作員を認証する。

操作員が TOE を利用する前には、利用を許可されている者であることが認証されなければならない。よって、操作員が認証される前に実行が許可される TSF は、操作員を認証するための TSF のみである。この要件に該当するセキュリティ機能要件は、FIA_UAU.1a、及び FIA_UAU.1b である。

c. 認証情報の品質を検証する。

識別認証の機能強度を確保するためには、利用者認証情報が、利用者本人以外に予測されることが困難でなければならない。予測されることが困難であるためには、利用者認証情報に対し、必要なレベルの品質を明確に定義し、その品質が満たされていることを検証しなければならない。この要件に該当するセキュリティ機能要件は、FIA_SOS.1 である。

d. 識別認証に成功した時に、TOE の利用を許可する。

識別認証に成功した操作員は、同じく成功した端末を用いて TOE を利用できなければならない。TOE 利用に際しては、TOE は操作員を代行するサブジェクトを生成し、操作員は TSF を実施するために使用するセキュリティ属性を関連付けられる。この要件に該当するセキュリティ機能要件は、FIA_ATD.1、及び FIA_USB.1 である。

e. 指定回数以内に識別・認証に成功しない場合、TOE の利用を無効とする。

識別認証に失敗した操作員は、TOE の正当な利用者ではないとみなす必要がある。TOE は指定した回数識別認証に失敗した操作員に対し、あらかじめ定義されたアクション(アカウントのロック、または一定期間の無効化)を実施しなければならない。この要件に該当するセキュリティ機能要件は、FIA_AFL.1 である。

f. 識別・認証の可否を決定する TSF データの管理者を制限する。

識別・認証で用いられる TSF データは、その値によって識別認証の可否が決定されるため、その値の管理者を限定しなければならない。よって、TOE が提供する TSF データの問合せや改変等の操作を、TOE が維持する特定の役割の利用者のみに制限する。この要件に該当するセキュリティ機能要件は、FMT_MTD.1、FMT_SMF.1、及び FMT_SMR.2 である。

以上、a、b、c、d、e、f すべての対策を満たすことは、O.I&A を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FIA_AFL.1、FIA_ATD.1、FIA_SOS.1、FIA_UAU.1a、FIA_UAU.1b、FIA_UID.1a、FIA_UID.1b、FIA_USB.1、FMT_MTD.1、FMT_SMF.1、及び FMT_SMR.2 の達成により、O.I&A を実現できる。

O.ALERT（アラート）

この TOE セキュリティ対策方針は、セキュリティ侵害の可能性を検出した際のアラート通知について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. セキュリティ侵害の可能性を検出する。

取得した監査証跡から、セキュリティ侵害の可能性について検出しなければならない。よって、監査対象事象の発生に際し、あらかじめ決められた閾値を監査証跡に付加し、閾値に応じてセキュリティ侵害の可能性を検出する。すべての監査対象事象に関して、監査者が定めた重要度を含む監査証跡が生成された場合に、セキュリティ侵害の可能性があると判断する。この要件に該当するセキュリティ機能要件は、FAU_SAA.1 である。

b. 検出したセキュリティ侵害の可能性について通知する。

セキュリティ侵害の可能性が検出された時、自動的な応答を返さなければならない。よって、セキュリティ侵害の可能性の検出によって、サーバ管理者と監査者に対するアラート通知を行う。この要件に該当するセキュリティ機能要件は、FAU_ARP.1 である。

以上、a、b すべての対策を満たすことは、O.ALERT を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FAU_ARP.1、及び FAU_SAA.1 の達成により、O.ALERT を実現できる。

O.RECOMMEND（勧告）

この TOE セキュリティ対策方針は、操作員に対する勧告的警告メッセージの表示について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 操作員に勧告的警告メッセージを表示する。

操作員が不正な操作を試みた際には、勧告的警告メッセージを表示しなければならない。利用者セッション確立前に、不正な利用に関する勧告的警告メッセージを表示する。この要件に該当するセキュリティ機能要件は、FTA_TAB.1 である。

以上、a の対策を満たすことは、O.RECOMMEND を満たすことである。したがって、その対策に必要な機能要件として該当する、FTA_TAB.1 の達成により、O.RECOMMEND を実現できる。

O.AUTO_LOGOUT（自動ログアウト）

この TOE セキュリティ対策方針は、TOE と操作員との対話セションの自動終了について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 対話セションを終了する。

操作員が一定時間 TOE を操作しない状態が続くと、TOE と操作員との対話セションを終了しなければならない。操作員が TOE を操作しない時間があらかじめ決められた時間間隔を超えると、TOE と操作員との対話セションを切断する。この要件に該当するセキュリティ機能要件は、FTA_SSL.3 である。

以上、a の対策を満たすことは、O.AUTO_LOGOUT を満たすことである。したがって、その対策に必要な機能要件として該当する、FTA_SSL.3 の達成により、O.AUTO_LOGOUT を実現できる。

（中略）

6.3.2. 依存性の検証

コメント [CEM26]: ASE_REQ.2-9

セキュリティ要件のコンポーネントの依存性を表 6-6 に示す。

表 6-6　セキュリティ要件のコンポーネントの依存性

項番	セキュリティ要件	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされないコンポーネント	妥当性
1	FAU_ARP.1	FAU_SAA.1	FAU_SAA.1	なし	
2	FAU_GEN.1	FPT_STM.1	なし	FPT_STM.1	*4
13	FCS_COP.1	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1	なし	
		FCS_CKM.4	FCS_CKM.4	なし	
		FMT_MSA.2	なし	FMT_MSA.2	*1
14	FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	なし	
15	FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	なし	
19	FDP_ITC.2	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1b	なし	
		[FTP_ITC.1、または FTP_TRP.1]	なし	[FTP_ITC.1、または FTP_TRP.1]	*2
		FPT_TDC.1	なし	FPT_TDC.1	*2
20	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1a FIA_UAU.1b	なし	
28	FMT_MSA.3	FMT_MSA.1	なし	FMT_MSA.1	*3
		FMT_SMR.1	なし	FMT_SMR.1	*3
29	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.2 (左記の上位階層)	なし	
30	FMT_SMF.1	なし	なし	なし	
31	FMT_SMR.2	FIA_UID.1	FIA_UID.1a FIA_UID.1b	なし	

表 6-6 より、TOE セキュリティ機能要件は後述する例外を除きそれぞれの必要な依存関係をすべて満たしている。すべての例外について、依存関係は満たされなくても問題がない根拠を以下に示す。

*1) FCS_CKM.1、FCS_CKM.4、FCS_COP.1 → FMT_MSA.2

FCS_CKM.1、FCS_CKM.4、及び FCS_COP.1 で取り扱うセキュリティ属性は、各暗号鍵に関するものである。それぞれが標準化されたアルゴリズムに従って、属性の値が決定されており、操作員が設定・改変する値を受け入れることはない。よって、これらの依存関係は不要である。

*2) FDP_ITC.2 → FTP_ITC.1、FTP_TRP.1、FPT_TDC.1

リムーバブル媒体は、物理的に保護された室内に保管され、攻撃者によるデータの改ざんに対する脅威は想定されないため、インポートされるデータは正確なものである。また、インポートされるデータは暗号化されて保存されており、通信路上において完全性が満たされていることを、ハッシュ値を用いて確認することができる。よって、この依存関係は不要である。

*3) FMT_MSA.3a、FMT_MSA.3b → FMT_MSA.1、FMT_SMR.1

FMT_MSA.3a、及び FMT_MSA.3b の対象となるセキュリティ属性は、TOE により管理されており、操作員に対しデフォルト値変更・問い合わせ・改変・削除などの役割は存在せず、役割を維持する必要性もない。よって、この依存関係は不要である。

*4) FAU_GEN.1 → FPT_STM.1

4.2 運用環境のセキュリティ対策方針 に示されるとおり、OE.TIME_STAMP の実現により、本 TOE が監査証跡を生成する際に利用する高信頼タイムスタンプは、TOE の運用環境によって提供される。よって、この依存関係は不要である。

6.3.3. セキュリティ保証要件根拠

本システムは、個人データを登録、閲覧・検索、提供、預託、加工、更新、及び削除するためのシステムである。2005 年 4 月には、個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）が完全施行されて社会の意識も高まり、個人情報に関する事故は、故意・ミスを問わず、大きな社会的・経営的問題に発展するケースがある。このため、本システムのセキュリティ機能には高い信頼性が要求される。EAL3 は TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、及び開発環境や開発生産物の管理状況の評価）を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれるので妥当な選択であるといえる。

コメント [CEM27]:
ASE_REQ.2-12

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 *（抜粋）*

コメント [CEM28]:
ASE_TSS.1-1
ASE_TSS.1-2

表 7-1 に TOE セキュリティ機能とセキュリティ機能要件（SFR）との対応関係について示す。ここで示される通り、本節で説明するセキュリティ機能は、6.1 節に記述される全ての SFR を満たすものである。

表 7-1　TOE セキュリティ機能とセキュリティ機能要件の対応関係

	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_STG.1	FAU_STG.3	FAU_STG.4	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FDP_ETC.2	FDP_ITC.2	FIA_AFL.1	FIA_ATD.1
SF.Audit	×	×	×	×	×		×		×	×											
SF.ACC					×	×		×						×	×	×	×	×	×		×
SF.I&A																				×	
SF.Crypto											×	×	×								
SF.Import_Export																		×	×		

	FIA_SOS.1	FIA_UAU.1a	FIA_UAU.1b	FIA_UID.1a	FIA_UID.1b	FIA_USB.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.2	FTA_SSL.3	FTA_TAB.1	FTA_TSE.1	FPT_TST.2
SF.Audit									×					
SF.ACC						×	×	×	×	×				
SF.I&A	×	×	×	×	×			×	×	×	×	×	×	×
SF.Crypto														
SF.Import_Export														

以下では各 TOE セキュリティ機能に関して、その概要および対応する SFR の具体的な実現方法について説明する。

7.1.1. 識別認証機能（SF.I&A）

識別認証機能は、TOE にアクセスする操作員を識別し、登録されている操作員本人であることを確認するための機能を提供する。また本機能は、操作員の識別認証に加え、操作員が使用するクライアント端末にインストールされたソフトウェアの正当性検証を行う機能を提供する。以下では識別認証機能について、SFR の実現方法という観点から説明する。

7.1.1.1. 対応する SFR の実現方法

(1) FIA_UID.1a 識別のタイミング、FIA_UAU.1a 認証のタイミング
（クライアント操作員）

TOE は、クライアント操作員の識別認証に関して以下の機能を提供する。

- TOE は、クライアント操作員の識別認証前に勧告的警告メッセージの表示、セション鍵生成、及びクライアント端末用パッケージの正当性検証のみを許可する
- 下記処理が 1→2→3→4 の順番ですべて成功した場合のみ、クライアント操作員の識別認証成功となる
    1. 勧告的警告メッセージの表示
    2. セション鍵の生成
    3. クライアント端末用パッケージの正当性検証
    4. クライアント操作員の識別認証

上記機能の実装により、FIA_UID.1a および FIA_UAU.1a を実現する。

(2) FIA_UID.1b 識別のタイミング、FIA_UAU.1b 認証のタイミング
（サーバ管理者）

TOE は、サーバ管理者の識別認証に関して以下の機能を提供する。

- TOE は、サーバ管理者の識別認証前に勧告的警告メッセージの表示のみを許可する
- 下記処理が 1→2 の順番ですべて成功した場合のみ、サーバ管理者の識別認証成功となる
    1. 勧告的警告メッセージの表示
    2. サーバ管理者の識別認証

上記機能の実装により、FIA_UID.1b および FIA_UAU.1b を実現する。

(3) FIA_SOS.1 秘密の検証

TOE は、ID・パスワード方式を用いるクライアント操作員、及びサーバ管理者の識別認証において下記機能を提供する。

- TOE は、操作員のパスワードが以下の条件を満たしていることを検証する
    - 6 文字以上 10 文字以下の、以下の範囲の ASCII 文字である
        - アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字
        - 数字は、[0-9]の合計 10 文字
        - 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字
    - 1 文字以上の数字または記号を含む
    - 2 文字以上のアルファベットを含む（大文字、小文字は区別される）
    - 新しいパスワードは、直前のパスワードと同一ではない
- TOE は、操作員の登録時及びパスワードの変更時において、新たなパスワードの候補として入力された文字列が上記の基準を満たさない場合には、パスワードの候補の再入力を要求する

この機能の実装により、FIA_SOS.1 を実現する。

(4) FIA_AFL.1 認証失敗時の取り扱い

TOE は、クライアント操作員、及びサーバ管理者の識別認証に関して以下の機能を提供する。

- 操作員が入力した ID に対するパスワードが異なる場合、操作員 ID 毎にパスワード誤り回数をカウントする
- 連続パスワード誤り回数が、サーバ管理者によって指定される最後の認証以降の不成功認証試行回数（1～5 回）に達すると、そのアカウントがサーバ管理者のものである場合には、当該アカウントを 5 分間無効化する（無効化が解除されると、不成功認証試行回数は 0 回に変更される）
- アカウントがクライアント操作員のものである場合には、当該アカウントをロックし、解除不可能とする
- 上記クライアント捜査員のアカウントを再び使用するためには、個人情報管理者もしくはサーバ管理者が当該アカウントを一度削除し再度アカウントを作成する

上記機能の実装により、FIA_AFL.1 を実現する。

(5) FPT_TST.2 簡易 TSF テスト

TOE は、クライアント操作員の識別認証に関して以下の機能を提供する。

- 上記「クライアント端末用パッケージの正当性検証」において、クライアント端末がサーバ端末に対し、自身にインストールされる個人情報処理システムクライアント用アプリケーションパッケージが正当なものであることを証明する

上記機能の実装により、FPT_TST.2 を実現する。

(6) FTA_TAB.1 デフォルト TOE アクセスバナー

TOE は、クライアント操作員、及びサーバ管理者の識別認証処理において、TOE 利用の前に、不正な利用に関する勧告的警告メッセージを表示する。
この機能の実装により、FIA_TAB.1 を実現する。
また、勧告的警告メッセージの作成、更新は、操作員管理・アクセス制御機能の実装により、サーバ管理者に限定される。

(7) FTA_SSL.3 TSF 起動による終了

TOE は、クライアント端末、サーバ端末間に確立するセションに関して以下の機能を提供する。

- TOE は、操作員 ID 毎に TOE への最後の操作時間を保持し、現在時刻との差が 15 分になるとセションを切断する
- 操作時間は、セションの切断により、0 に再設定される

上記機能の実装により、FTA_SSL.3 を実現する。

(8) FTA_TSE.1 TOE セション確立

TOE は、クライアント端末、サーバ端末間に確立するセションに関して以下の機能を提供する。

- TOE は、セション確立前に、セション確立要求時刻を、操作員種別毎のセション確立許可時間帯と照合する
- セション確立時刻が操作員種別毎のセション確立許可時間帯外の場合、セション確立を拒否する

上記機能の実装により、FTA_TSE.1 を実現する。
また、セション確立許可時間帯の設定、更新は、操作員管理・アクセス制御機能の実装により、サーバ管理者に限定される。

(9) FMT_SMF.1 管理機能の特定

TOE は、識別認証機能において表 7-2 に示すセキュリティ管理機能を提供する。

表 7-2 提供セキュリティ管理機能

特定されたセキュリティ管理項目	セキュリティ管理機能
不成功の認証試行回数の管理	不成功の認証試行に対する閾値の管理
バナー表示メッセージの管理	バナー表示メッセージの管理
操作員種別毎のセション確立許可時間帯の管理	操作員種別毎のセション確立許可時間帯の管理
操作員管理 自身によるパスワードの改変	クライアント操作員のパスワードの登録 クライアント操作員のパスワードの改変 クライアント操作員 ID の作成、問い合わせ、削除 サーバ管理者のパスワードの登録 サーバ管理者のパスワードの改変

これは FMT_SMF.1 で要求される管理機能の一部であり、従って、この機能の実装および監査機能、操作員管理・アクセス制御機能の実装により、FMT_SMF.1 を実現する。

(10) FMT_MTD.1 TSF データの管理

TOE は、表 7-3 に示すように左列に示す識別・認証用 TSF データに対して、右列に示された対応する各操作員が、中列に示された各操作を実行する事のみを許可する。

表 7-3 識別・認証用 TSF データの管理

TSF データ	操作	許可された識別された役割
サーバ管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
サーバ管理者のパスワード	作成	サーバ管理者
監査者、個人情報管理者の操作員 ID	問い合わせ、削除、作成	サーバ管理者
監査者、個人情報管理者の パスワード	削除、作成	サーバ管理者
オペレータ、個人情報利用者の 操作員 ID	問い合わせ、削除、作成	個人情報管理者
オペレータ、個人情報利用者の パスワード	削除、作成	個人情報管理者
操作員自身のパスワード	改変	オペレータ 個人情報利用者 個人情報管理者 サーバ管理者 監査者
操作員の最後に成功した認証以降の不成功認証試行回数の定義	問い合わせ、改変	サーバ管理者

これは FMT_MTD.1 で要求される管理機能の一部であり、従って、この機能の実装および暗号鍵管理機能、監査証跡管理機能の実装により、FMT_MTD.1 を実現する。

(11) FMT_SMR.2 セキュリティ役割における制限

TOE は、操作員登録に関して以下の機能を提供する。

・ 操作員は、登録時に以下のセキュリティ属性を持つ

（セキュリティ属性）

- 操作員 ID
- パスワード
- 操作員種別

・ 以下の操作員種別を定義する

（操作員種別）
- オペレータ
- 個人情報利用者
- 個人情報管理者
- サーバ管理者
- 監査者

・ すべての操作員は、登録時に上記のいずれかの操作員種別に分類される
・ 一つの操作員を複数の操作員種別に重複して分類できない

この機能の実装により、FMT_SMR.2 を実現する。

（中略）