アプリポーター Security Kit

セキュリティターゲット

2005/ 2/ 5

Version 1.80

株式会社　日立製作所

はじめに

「アプリポーター」は、行政サービスのうち特に申請・届け出の手続きをオンライン化し、住民・企業（以下一般利用者）がインターネットなどのネットワークを介して利用可能な電子申請／電子窓口サービスの基盤機能を提供するソフトウェアである。本文書はアプリポーターのセキュリティ機能であるアプリポーター Security Kit を評価対象（Target of Evaluation：以下 TOE）としたセキュリティターゲット（Security Target：以下 ST）である。

本 ST は、アプリポーターに対して利用者の本人認証及び電子文書の原本性保証を含むセキュリティ機能を要求する。TOE が提供する利用者機能は、デフォルト設定時に適用される以下の機能を含む。

- 利用者の識別・認証機能：セッション管理サービス
- 電子申請受付事跡の管理機能：レシート管理サービス
- 申請書をバックオフィスに配信する機能：配信サービス
- ログ管理機能：アプリケーション動作支援サービスのログ管理機能

また、本 ST は、TOE が特定の運用環境で管理・運用されることを想定しており、TOE に対して最低限考慮すべきセキュリティ環境に基づいて実施されることを要求する。これらの要求を踏まえ、本 ST は、要求される TOE セキュリティ環境に対して識別された対策方針を満たすために有用かつ有効である機能及び保証の双方の IT セキュリティ要件及び TOE 要約仕様を設計したものである。

認証基準：

本 ST は、IT セキュリティ評価・認証プログラムが認証基準として認める以下の Common Criteria for Information Technology Security Evaluation に係る情報処理推進機構（IPA）または、製品評価技術基盤機能（NITE）の翻訳文書を適用する。

- 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 2.1 1999 年 8 月 CCIMB-99-031
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2:セキュリティ機能要件 バージョン 2.1 1999 年 8 月 CCIMB-99-032
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3:セキュリティ保証要件 バージョン 2.1 1999 年 8 月 CCIMB-99-033
- 補足－0210

用語及び略語：

（1）CC を下記の総称として使用する。

- Common Criteria for Information Technology Security Evaluation　Part 1 ~ Part 3 Version2.1, 99/8
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part1 ~ Part3, 99/12
- CCIMB Interpretations-0210
- JIS X5070, セキュリティ技術－情報技術セキュリティの評価基準－第 1 部：総則及び一般モデル、第 2 部：セキュリティ機能要件、第 3 部：セキュリティ保証要件、平成 12 年 7 月 20 日制定）

本 ST で使用する用語等が JIS 規格で用いられる用語等と異なる場合は、認証基準である上記翻訳文書に添付の対照表を参照のこと。

（2）本 ST で使用する「利用者」は、一般利用者（申請者の代理人を含む)、監査者、運用管理者を含む TOE を利用する者の総称とする。

（3）本 ST で使用する用語・略号の定義

・DD（Deployment Descripter）

アプリケーションを運用環境に配置するときの定義情報を記述した電子文書。EJB 用，Web アプリケーション用，Enterprise アプリケーション用などが Sun からの仕様で規定されている。

・UP（User Program）

電子申請業務の開発者が独自に作成したアプリポーター／フレームの制御下で動作するプログラム。

・標準パターン

アプリポーター／フレームで提供する標準的業務パターン。標準画面と標準関数のセットで提供する。

・ バックオフィス

アプリポーターでの電子申請受付後、申請書データを受けて個別の業務を行う環境

≪他社所有名称に対する表示≫

- Microsoft は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。
- Windows は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。
- Java 及びすべての Java 関連の商標及びロゴは、米国及びその他の国における米国 Sun Microsystems,Inc.の商標または登録商標です。
- iPlanet™および iPlanet™をベースとする商標は、米国およびその他の国における米国 Sun Microsystems, Inc.の商標または登録商標です。
- Netscape®は、米国およびその他の国における Netscape Communications Corporation の登録商標です。
- Netscape® Communicator は、Netscape Communications Corporation の商標です（一部の国では、登録商標となっています）。
- HP-UX は，米国 Hewlett-Packard Company のオペレーティングシステムの名称です。
- HP は、米国 Hewlett-Packard Company の会社名です。
- ORACLE は Oracle Corporation の登録商標です。
- ORACLE8i は，Oracle Corporation の商標です。
- MQSeries は，米国における米国 International Business Machines Corp.の商標です。

その他の製品名称などの固有名詞は、各社の登録商標、商標あるいは商品名称です。
なお、本文中では Microsoft®、™、®マークは表示しておりません

「アプリポーター Security Kit　セキュリティターゲット」

－目次－

1. ST 概説

1.1　ST 識別

（1）ST の識別情報

名称：アプリポーター Security Kit　セキュリティターゲット

バージョン： V 1.80

作成日： 2005 年　2 月 5 日

作成者： 株式会社　日立製作所

登録：（未評価及び未登録）

キーワード：電子政府、電子申請、電子窓口、電子文書、電子証明書、X.509 公開鍵認証書、電子署名、XML 署名、認証、セッション、Web サーバ、LDAP、DBMS、CRL、アクセス制御、ログ

（2）TOE の識別情報

名称：アプリポーター Security Kit

バージョン： 01-00

作成日： 2002 年 12 月 20 日

作成者： 株式会社日立製作所

（3）適合する CC のバージョン

CC バージョン 2.1 および補足－0210

（4）適合する PP

適合する PP は無い。

1.2　ST 概要

アプリポーターは、一般利用者に対して、電子証明書を利用した電子文書の認証と完全性保証を付加した電子申請サービスを提供するアプリケーション機能を具備した電子申請の基盤ソフトウェアである。

本STは、アプリポーターを構成するモジュールの中で、セキュリティ機能を実現するTOE「アプリポーター Security Kit」について記述している。

アプリポーター Security Kitはアプリポーターの以下の機能モジュールから構成される。

・セッション管理サービス

・レシート管理サービス

・配信サービス

・アプリケーション動作支援サービス(ログ管理)

・セッション管理サービス運用管理
・レシート管理サービス運用管理
・配信サービス運用管理

1.3　CC 適合

本 ST は以下の規格に準拠している。

- CC 第 2 部 適合
- CC 第 3 部 適合
- EAL 2 適合

1.4　参考資料

- JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第１部：総則及び一般モデル
- JIS X 5070-2:2000 セキュリティ技術－情報技術セキュリティの評価基準－第２部：セキュリティ機能要件
- JIS X 5070-3:2000 セキュリティ技術－情報技術セキュリティの評価基準－第３部：セキュリティ保証要件
- ISO/IEC 15408-1:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート1：概説と一般モデル
- ISO/IEC 15408-2:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート2：セキュリティ機能要件
- ISO/IEC 15408-3:1999 情報技術－セキュリティ技法－ITセキュリティのための評価基準 パート3：セキュリティ保証要件
- Common Criteria for Information Technology Security Evaluation Part1:Introduction and general model Version 2.1 August 1999 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation Part2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation Part3:Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- 補足－0210およびCCIMB Interpretations-0210

2. TOE 記述

2.1　TOE の種別

本 ST の TOE 種別は、ソフトウェア製品である。各種申請、情報提供等の行政サービスをインターネット経由で提供する電子申請／電子窓口システムの基本的機能であるアプリポーターのセキュリティ機能を提供する。

2.2　TOE の利用目的と利用方法

2.2.1　TOE の利用目的

一般利用者は、PC等のクライアントを使用してTOEにアクセスして識別・認証されることにより電子申請／電子窓口システムにアクセスすることが可能となり、申請・届出にともなう一連の電子申請サービスをインターネット経由で利用することができる。

一般利用者である申請者は、電子申請書に必要事項を入力し、申請書データに電子署名を付加し、オンラインで申請を行う。

運用管理者は、PC 等のクライアントを使用して TOE にアクセスして識別・認証されることにより運用管理ユティリティーにアクセスすることが可能になり、TOE を利用してユーザ情報の管理・申請書データ配信の管理・レシートの管理を行うことができる。

2.2.2　TOE の関連者

本 ST では、以下の関連者を想定する。

（1） 組織の責任者

役割：TOE の運営に関する意思決定を行う。TOE を含む業務システムの運用の基本方針を決定する。

権限：組織の経営、運用管理者及び監査者の任命に関する権限を持つ。

信頼度：組織の損失となる行為は行わない。

知識：情報システムに関する知識は少ない。組織のセキュリティ管理の責任者でありその推進活動を指揮する責任がある。

（2） 監査者

役割：TOE の監査を実施する。

権限：TOE の監査に係る機能は運用管理者が操作し、TOE の監査データのみを参照する。

信頼度：TOE の監査に係る行為のみ信頼できる。

知識：システム監査に必要な知識に精通している。

（3） 運用管理者

役割:TOE が利用する外部 IT サービスの選定･契約事務処理､TOE を導入する機器、ネットワーク及びソフトウェアの設置・接続・インストール、TOE のインストール・各種設定及び設定の変更、データベースの運用管理、TOE の起動・停止、システムトラブル対応及び日々のシステム運用管理、監査支援を行う。

権限：TOE のシステム運用に関する登録、変更、削除等の操作に関する権限を持つ。

信頼度:TOE のシステム管理全般に係る行為においてのみ信頼できる。所属する組織の規定する行動指針の遵守を管理される立場にある。

知識：情報技術及びシステム管理に精通している。

（4） 一般利用者

役割:一般利用者クライアントを用いて電子申請サービスを利用する。TOE を使って申請書を送信する。自らのパスワードを変更する。

権限：インターネットなど外部ネットワーク経由で TOE にアクセスし、申請書の送信、一般利用者自身のパスワードの変更に関する権限を持つ。

信頼度：原則として信頼できない。

知識：情報技術の利用に関して一般知識を有している。

2.2.3 TOE の利用方法

（1）運用管理者による準備

- 必要に応じてCAとの利用契約を締結する。
- TOEをインストールする機器の設置､接続､TOEの前提となるソフトウェア及びTOEのインストール、設定を行い、正しく動作することを確認する。
- 運用管理者は、TOEを運用する前に、受付処理主体の本人認証を行うための電子証明書をCAから取得する。

（2）一般利用者の準備

- 一般利用者は、TOEにアクセスする前に、一般利用者の本人認証を行うための電子証明書をCAから取得する。SSLクライアント証明書による利用者認証を行う場合には、SSLクライアント証明書を取得しておき使用するブラウザに組み込んでおく。

（3）一般利用者、運用管理者の電子申請業務

- 一般利用者は、電子申請に係る公開された情報を申請先のWebサイトからダウンロードすることにより取得する。
- 一般利用者は、TOEにて利用者認証された後、申請書を電子申請窓口へ送信する。申請書には、改ざん防止と本人確認のために電子署名を付加する。

- 運用管理者は、申請書と受付日時等を元に作成され、受付処理主体の電子署名が付加されたレシートを参照・管理することができる。
- 一般利用者は、メッセージを電子申請窓口から取得し申請ステータスの確認ができる。

（4）システム管理業務

運用管理者は、TOE の設定や日々のシステム管理を実施する。

（5）監査業務

監査者は、運用管理者の協力を得て TOE に保存された監査データを参照する。

（6）組織運営

組織の責任者は、セキュリティ対策方針に基づき組織を運営する。

2.3 TOE の利用形態

2.3.1 モデル図

TOE を適用したシステム構成のモデル図を以下に示す。TOE は受付サーバ内のソフトウェアの一部である。TOE のハードウェア上への配置と前提ソフトウェアの組合わせは様々なパターンが可能であるが、本 ST では以下２パターンの構成を対象とする。下図 2.3-1 はアプリポーターWindows 版および前提ソフトウェアを 1 台のハードウェアに搭載した構成である。

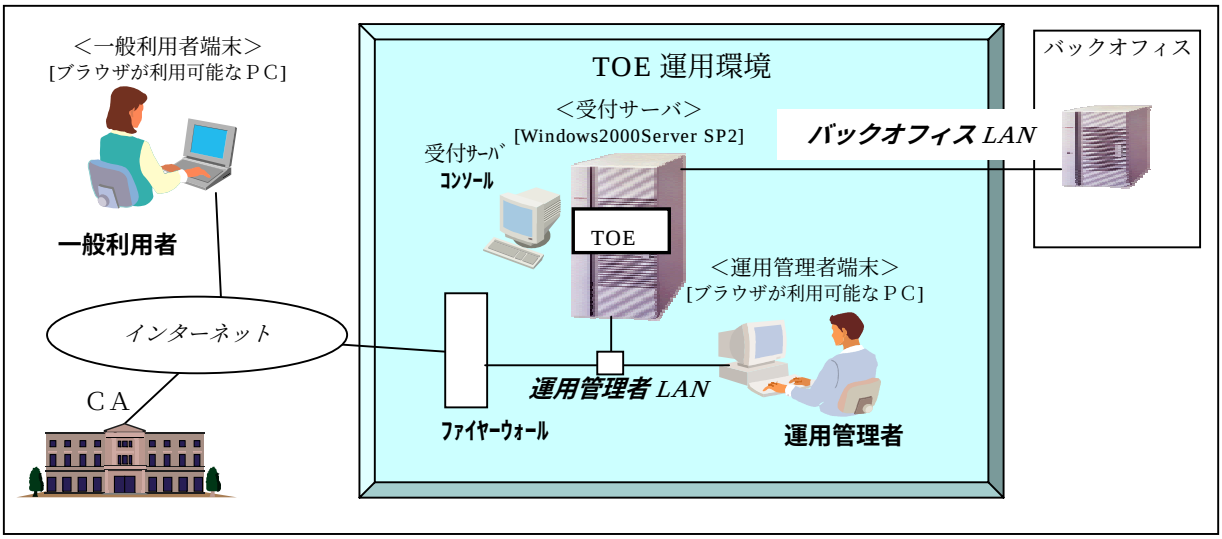


図 2.3-1　モデル図（Windows 版：最小構成）

下図 2.3-2 はアプリポーターHP-UX 版および前提ソフトウェアを 1 台のハードウェアに搭載した構成である。

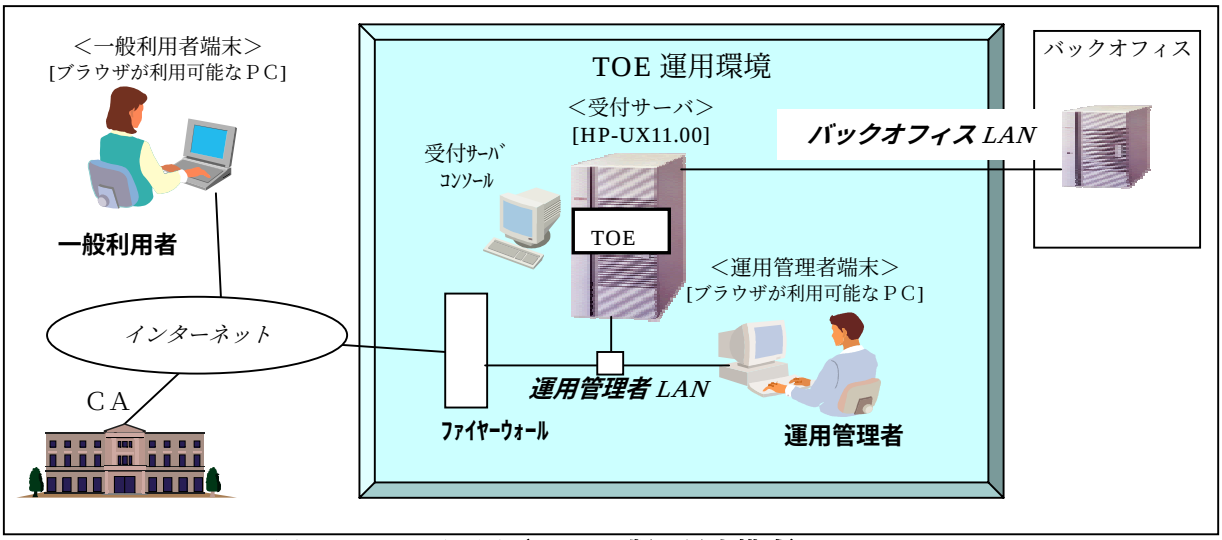


図 2.3-2　モデル図（HP-UX 版：最小構成）

2.3.2　ハードウェア構成

モデル図 2.3-1, 2.3-2 の TOE が搭載される受付サーバのハードウェア構成を以下の表 2.3-1, 2.3-2 に示す。

表 2.3-1ハードウェア構成(Windows 版：最小構成)

No	名称	ハードウェア仕様
1	受付サーバ	モデル：HA8000/70 プロセッサ（クロック）：Pentium III（700MHz） メモリ：512MB 内蔵ディスク容量：8.5GB コンソール：ディスプレイ装置・キーボード・マウス

表 2.3-2 ハードウェア構成(HP-UX 版：最小構成)

No	名称	ハードウェア仕様
1	受付サーバ	モデル：H9000V / C3600 プロセッサ（クロック）：PA-8600（552MHz） メモリ：1GB 内蔵ディスク容量：18GB コンソール：ディスプレイ装置・キーボード・マウス

2.3.3　ソフトウェア構成

モデル図 2.3-1, 2.3-2 の各構成要素に搭載されるソフトウェアコンポーネントの識別情報を以下の表 2.3-3, 2.3-4 に示す。

表 2.3-3 ソフトウェア構成(Windows 版：最小構成)

No	名称	搭載ソフトウェア	ﾊﾞｰｼﾞｮﾝ
1	受付サーバ	OS:Windows2000 Server Service Pack 2	2000 SP2
		Internet Information Services (IIS) 5	5.0
		Cosminexus Application Server - Version 5	05-00/B
		アプリポーター 03-02	03-02
		HiRDB/Single Server Version 6	06-00/C
		Oracle 8i Standard Edition	8.1.7
		セキュア通信基盤サーバ	03-00/A
		PKI Runtime Library for Windows Server	02-03
		Keymate/Crypto	02-00
		iPlanet Directory Server 5.1	5.1
		TP1/Message Queue	05-00/E
		TP1/Message Queue- Access	01-04
		TP1/Server Base	05-00/F
		Sendmail Advance Message Server	1.3J
2	運用管理者端末	OS:Windows(下記ブラウザが動作可能な OS)	
		Internet Explorer 5.5 SP2 または Netscape Communicator 4.7	5.5SP2/4.7
3	一般利用者端末	OS:Windows(下記ブラウザが動作可能な OS)	
		Internet Explorer 5.5 SP2 または Netscape Communicator 4.7	5.5SP2/4.7

表 2.3-4 ソフトウェア構成(HP-UX 版：最小構成)

No	名称	搭載ソフトウェア	ﾊﾞｰｼﾞｮﾝ
1	受付サーバ	OS: HP-UX11.00	11.00
		SORT	02-00/B
		Cosminexus Application Server - Version 5	05-00/B
		Hitachi Web Server（Cosminexus に同梱）	01-02/C
		アプリポーター 03-02	03-02
		HiRDB/Single Server Version 6(32)	06-01
		Oracle 8i Standard Edition	8.1.7
		セキュア通信基盤サーバ	03-02
		PKI Runtime Library for HP-UX	02-06
		Keymate/Crypto	03-00
		iPlanet Directory Server 5.1	5.1
		TP1/Message Queue	05-13
		TP1/Message Queue- Access	05-00
		TP1/Server Base	05-03/B
		Sendmail	8.8.6
2	運用管理者端末	OS:Windows(下記ブラウザが動作可能な OS)	
		Internet Explorer 5.5 SP2 または Netscape Communicator 4.7	5.5SP2/4.7
3	一般利用者端末	OS:Windows(下記ブラウザが動作可能な OS)	
		Internet Explorer 5.5 SP2 または Netscape Communicator 4.7	5.5SP2/4.7

各ソフトウェアコンポーネントが提供する機能の概要を以下に示す。

- Cosminexus Application Server
  J2EE 準拠のアプリケーションサーバ。TOE においては EJB コンテナ, Web コンテナ，JDBC 等 Web アプリケーションの実行環境を提供する。
- Web サーバ
  ・Internet Information Services (IIS) 5
  OS が Windows2000 ServerSP2 の場合の Cosminexus が前提とする Web サーバ。
  ・Hitachi Web Server
  OS が HP-UX11.00 の場合の Cosminexus が前提とする Web サーバ。Cosminexus に同梱される。
- DBMS（HiRDB/Single Server　または　Oracle8i）
  データベース管理ソフト。TOE からの指示によりデータの管理を行う。レシート情報、配信前の申請書データ（配信ジョブキュー）を格納する。TOE がユーザ情報管理を DBMS で行う設定の場合、ユーザ管理情報、アカウントロック情報も格納する。
  ・SORT
  OS が HP-UX の場合の HiRDB/Single Server の前提となるソフトウェア。ファイルの編成とテキストのソート・マージを行う。

- PKI サービス

  セキュア通信基盤サーバ、PKI Runtime Library、Keymate/Crypto の３つのソフトウェアからなるアプリポーターのサービスの一つ。レシート管理サービスにおいて、レシートに電子署名を付与する時に使用される。また、申請書に対する電子署名の署名検証・証明書の検証と有効性確認等に使用される。

  ・セキュア通信基盤サーバ

  署名（XML、PKCS#7 等）付与・検証、証明書の検証・有効性確認、クライアントとの暗号通信等の機能を持つ。PKI Runtime Library が前提プログラムとして必要。TOE はセキュア通信基盤の署名検証機能を使用し署名検証を行うことで、申請データの改ざん有無が確認可能。

  ・PKI Runtime Library

  PKI の技術を使ってセキュリティを確保するための実行用ライブラリと PKI 関連のツール群。セキュア通信基盤から呼び出されて、申請書データに付与された電子署名の検証、公開鍵証明書の検証、レシートへの電子署名付与を行う。また、秘密鍵管理、ルート CA 証明書管理、ユーザ証明書管理、鍵ペア生成、CRL 管理等のツール類を提供する。

  ・Keymate/Crypto

  セキュリティ基盤システム構築のための暗号ライブラリ。PKI Runtime Library の前提プログラム。公開鍵暗号、共通鍵暗号、ハッシュ関数の機能を提供する。また暗号鍵、秘密鍵、公開鍵の生成も行う。

- iPlanet　Directory　Server

  LDAP ディレクトリサーバソフト。TOE がユーザ情報管理を LDAP で行う設定の場合に使用する。ユーザ情報やユーザ権限を保持し，ユーザ認証時の照会先となる。パスワード長の制限、パスワード使用可能文字の制限、認証エラー回数によるアカウントロック機能等を持つ。

- MQ

  ・TP1/Message Queue

  TOE の配信サービスで MQ 配信機能を選択した場合配信先に必要となる。分散システム上のアプリケーション間でのメッセージキューを介した非同期蓄積型の通信手段を提供する。メッセージキューを管理してメッセージを送受信するプログラムをキューマネジャといい、TP1/Message Queue は、システム上でキューマネジャの役割を持つ。

  TP1/Message Queue を使用すると、OpenTP1（注）システム内のアプリケーション同士及び他システムのキューマネジャとの間でメッセージの送受信ができる。通信相手システムのキューマネジャは、TP1/Message Queue または他の MQSeries（IBM 社の製品）である。これらのキュー

マネジャと通信する場合、TCP/IP（Transmission Control Protocol/Internet Protocol）プロトコルを使用する。

（注）OpenTP1：オープンシステム上でオンライントランザクション処理（OLTP　Online Transaction Processing）をできるようにするソフトウェア（TP モニタ）。

・TP1/Message Queue- Access

クライアントアプリケーションから TP1/Message Queue のメッセージキューにメッセージを登録したり、取り出したりする機能を持つ。Java インタフェースを持つ。

・TP1/Server Base

TP1/Message Queue の前提ソフトウェア。TP1/Message Queue の動作基盤と各種設定機能を実現する。

- Sendmail Advance Message Server / sendmail

メールサーバ。配信サービスで E-mail 配信機能を選択した場合必要となる。E-mail の送受信管理機能を持つ。

2.4 TOE の範囲

2.4.1 物理的範囲

TOE の物理的範囲は、OS が Windows の場合図 2.4-1、HP-UX の場合図 2.4-2 にて示される以下のライブラリおよびユーティリティから構成される。

・セッション管理サービス
・レシート管理サービス
・配信サービス
・アプリケーション動作支援サービス(ログ管理)
・セッション管理サービス運用管理
・レシート管理サービス運用管理
・配信サービス運用管理

なお、TOE が Windows または HP-UX にて動作するのは、Java で記述された TOE が、アプリケーションサーバ Cosminexus Application Server - Version 5 により異なる OS 下でも同一の Java 動作基盤が提供されるためである。

TOE を含めたソフトウェア構成図を以下に示す。

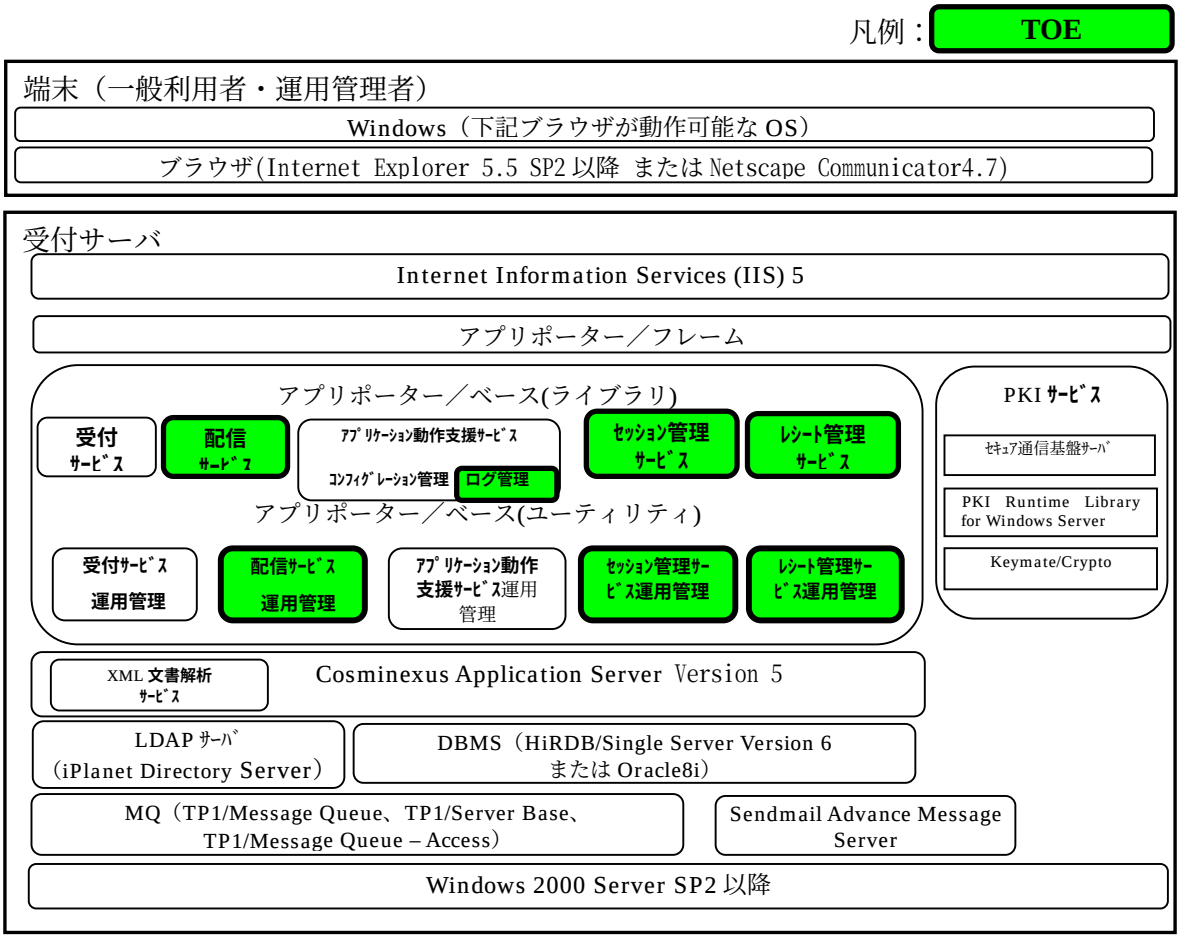


図 2.4-1 ソフトウェア構成図（アプリポーターWindows 版の構成例）

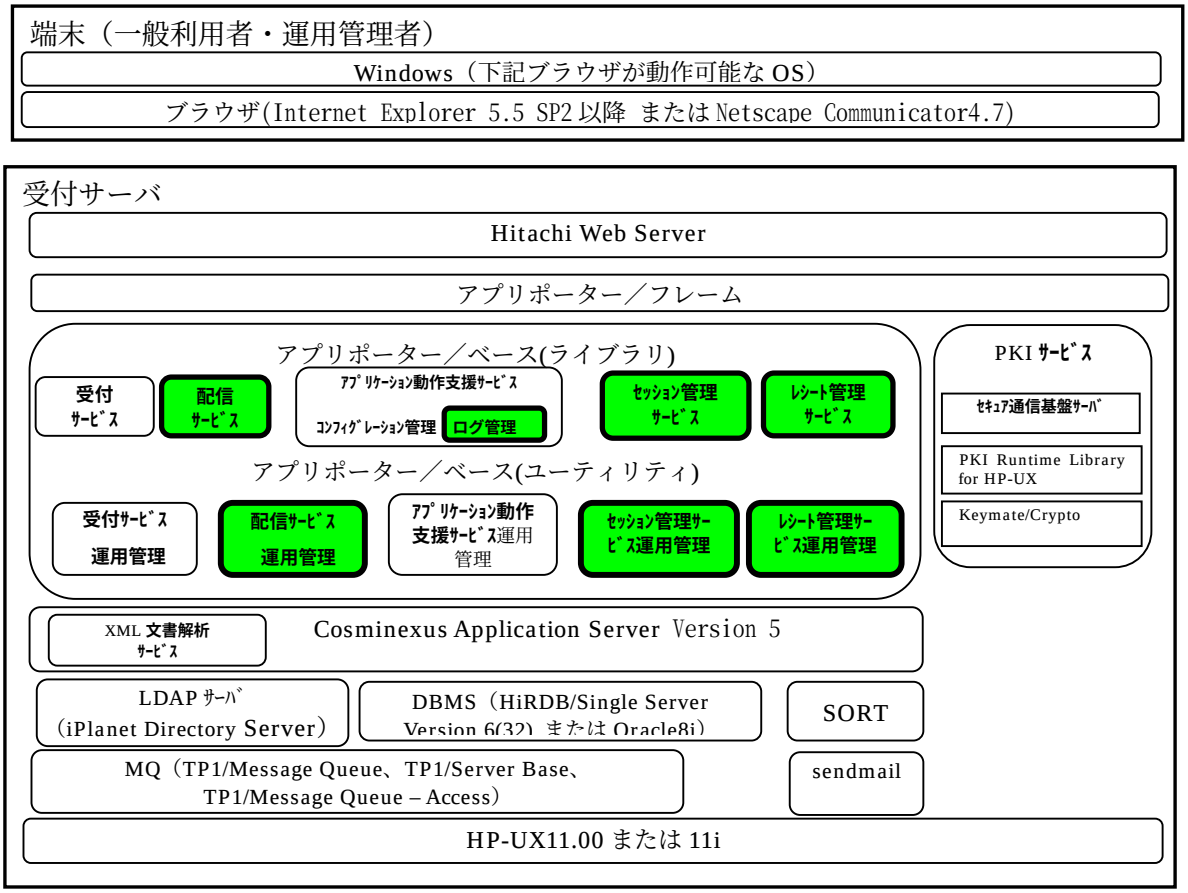


図 2.4-2　ソフトウェア構成図（アプリポーターHP-UX 版の構成例）

2.4.2　論理的範囲

TOE の機能は、以下の表 2.4-1 及び表 2.4-2 のアプリポーター／ベース機能の中の網掛けにて示した部分である。

表 2.4-1 アプリポーター／ベース（ライブラリ）の機能一覧

ライブラリ	機能		概要
セッション管理サービス	ユーザ認証	ユーザ ID／パスワード認証	ユーザ ID、パスワード方式でのセッション認証機能 パスワード変更機能
		SSL クライアント認証	SSL クライアント認証でのセッション認証機能
	ユーザ情報参照	固有情報参照	ユーザ情報に付与した業務固有情報の参照
		公開鍵証明書情報参照	クライアント証明書情報の参照※
	セッション情報保持		HTTP リクエスト間で引き継ぐ情報の登録・参照
受付サービス	申請ステータス管理		申請単位のステータス情報保持・更新・検索
	Web メール Box 管理		ユーザ単位のメール Box 内メッセージの登録・参照・更新
PKI サービス	＊このサービスはセキュア通信基盤サーバ、PKI Runtime Library 、Keymate/Crypto を使用します。		デジタル署名の検証 XML 署名の検証 公開鍵証明書の検証 証明書情報の参照 デジタル署名の付与 XML 署名の付与 暗号処理
XML 文書解析サービス	＊このサービスは Cosminexus を使用します。		XML 文書の構文解析 XML 文書の入力値の参照
レシート管理サービス	デジタルレシート発行		申請情報のデジタルレシート（デジタル署名付き受付記録）の発行・保管
	デジタルレシート参照		発行したデジタルレシート（デジタル署名付き受付記録）のアプリケーションへの引き渡し
配信サービス	メッセージ編集	MQ 配信用	申請データ、キュー名、メッセージ ID などの MQ メッセージ記述子に含まれる情報を設定して、MQ 配信用のメッセージを作成
		FTP 配信用	ホスト名、ファイルパス、申請書データを設定して FTP 配信用メッセージを作成
		Mail 配信用	題名、メール本文、宛先アドレス、申請書データを設定してメール配信用のメッセージを作成
		蓄積サーバ配信用	ホスト名、変換識別子、申請書データを設定して蓄積サーバ用メッセージを作成

	送信ジョブキューへの一時保管		メッセージ編集機能で作成されたメッセージを送信ジョブキューに一時保管
	配信機能	MQ 配信	送信ジョブキューに一時保管されている MQ 配信用のメッセージを TP1/Message Queue のメッセージキューイング機能を用いて配信
		FTP 配信	送信ジョブキューに一時保管されている FTP 配信用のメッセージを FTP で配信先に配信
		Mail 配信	送信ジョブキューに一時保管されている Mail 配信用のメッセージを sendmail のメール送信機能を用いて SMTP で配信
		蓄積サーバ配信	送信ジョブキューに一時保管されている蓄積サーバ用のメッセージを FTP で配信
	蓄積サーバ格納		蓄積サーバ配信によって配信されたデータおよび変換識別子により、蓄積サーバ上の HiRDB のテーブルにデータを登録する
アプリケーション動作支援サービス	コンフィグレーション管理		業務アプリケーション固有の構成・定義情報の管理
	ログ管理		メッセージレベル、メッセージ ID、種別、およびメッセージテキストを引数として、ログを取得。取得日時は自動取得

注：網掛け部分が TOE の範囲

表 2.4-2 アプリポーター／ベース（ユーティリティ）機能一覧

ユーティリティ	機能	概要
セッション管理サービス運用管理	利用者情報管理	利用者情報の登録・参照・編集・削除 ロックアウトユーザの参照・解除・強制ロックアウト ロックアウト条件の設定
受付サービス運用管理	申請ステータス管理	申請ステータス情報の参照・削除、 申請ステータス DB の利用状況の参照
	Web メール Box 管理	Web メール Box のメールエントリの参照、 メールエントリの削除、 Web メール Box DB の利用状況の参照
配信サービス運用管理	配信サービス管理	配信サービスの起動・停止
	配信データ管理	送信ジョブキューのエントリを一覧表示 送信済みエントリのデータを再送信 送信ジョブキューの配信データを削除

レシート管理サービス運用管理	レシートデータ管理	レシート DB の利用状況の参照 レシートデータのファイル出力 レシートデータの削除
アプリケーション動作支援サービス運用管理	コンフィグレーション管理	アプリケーションの任意情報の登録、 定義情報の参照・編集・削除
	システム監視	JVM の状態表示

注：網掛け部分が TOE の範囲

但し、上記表のセッション管理サービス及びセッション管理サービス運用管理機能は、TOE（ＲＤＢ）若しくは IT 環境（iPlanet Directory Server）のどちらかでの実施を選択可能である。両方を同時に使用することはできない。

2.4.3　TOE の機能概要

表 2.4-1 及び表 2.4-2 にて示した TOE の機能について以下に概要を示す。

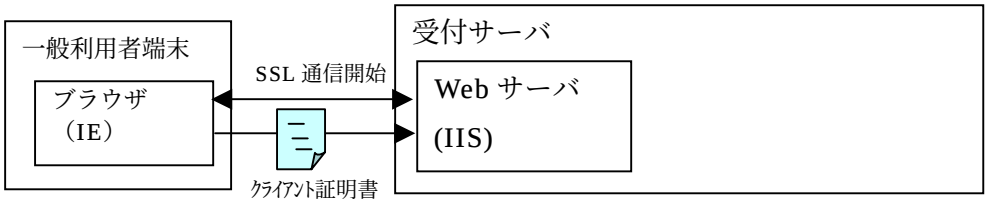
（1）一般利用者に対する TOE 機能

一般利用者による新規申請時の TOE 機能を、データフロー例にて以下に示す。

なお、一般利用者は CA から SSL ｸﾗｲｱﾝﾄ証明書を取得し、ブラウザに組込済み、申請書には電子署名付与済み、ﾊﾟｽﾜｰﾄﾞと SSL ｸﾗｲｱﾝﾄ証明書による認証を行う設定、ユーザ情報は RDB による管理とする。

① Web サーバとの SSL 通信開始

一般利用者は Web サーバにアクセスし SSL による暗号通信路を確保し、SSL クライアント証明書を Web サーバに渡す。

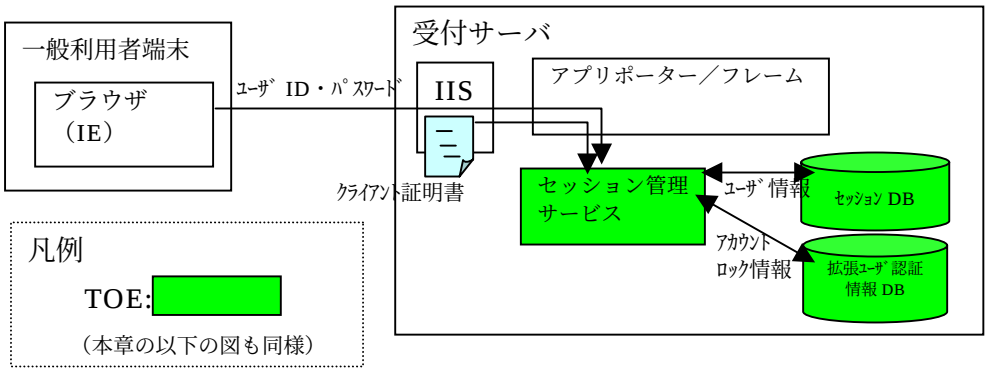


② ユーザ認証機能、ユーザ情報参照機能

一般利用者はログイン画面にユーザ ID とパスワードを入力する。

TOE のセッション管理サービスはセッション DB を検索し、利用者のロール、パスワードのハッシュ値と SSL クライアント証明書のハッシュ値を得る。

セッション管理サービスは、Web サーバから引き渡された利用者のパスワードと SSL クライアント証明書のハッシュ値を取りセッション DB との比較により認証を行う。次にセッション管理サービスは拡張ユーザ認証情報 DB を確認して利用者がロックアウトされていないか判定する。以上のログイン認証が正しく済んだらセッション管理サービスは認証済ユーザ情報（ユーザコンテクスト）を作成しセッションを開始、管理する。



③ 申請書受付

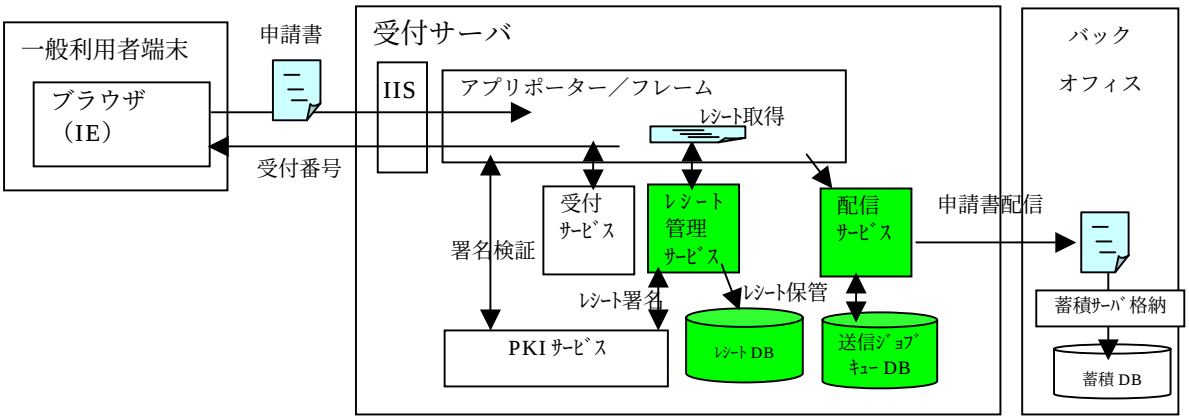
ログインが成功したらメニュー画面が表示される。一般利用者はメニュー画面から「新規申請」を選択し、新規申請画面にて送信する申請書を指定し送信する。
申請書を受けた受付サーバでは、申請書に対して署名検証を行う。署名検証処理には、PKI サービス（PKI Runtime Library およびセキュア通信基盤サーバ）を使用する。また、アプリポーターの受付サービスによって受付番号を取得し、一般申請者に返信する。受付け後、Web メール Box 管理と申請ステータス管理が開始される。

④ デジタルレシート発行機能

TOE のレシート管理サービスは、申請書類を受け付けた時点でレシートを発行する。レシート取得が行われると、レシート管理サービスは、PKI サービスを使いレシートにデジタル署名を施す。発行されたレシートデータはアプリポーター／ベースのレシート DB で管理される。

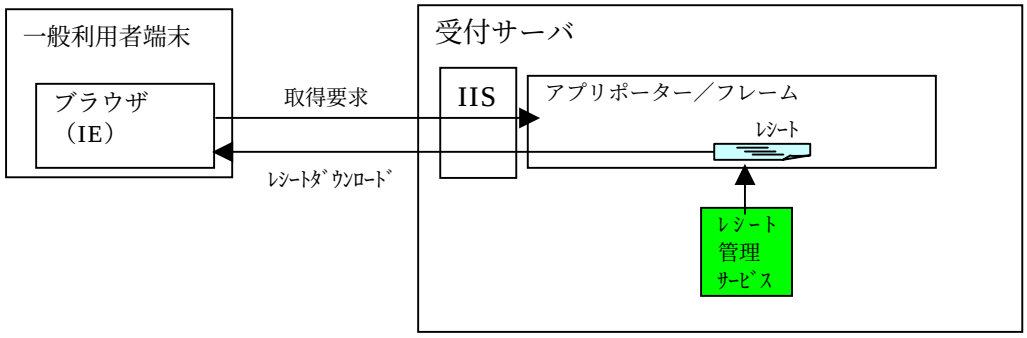
⑤ メッセージ編集機能、送信ジョブキューへの一時保管機能、配信機能

TOE の配信サービスは、受付けた申請書データに配信方法、配信先等の情報を付加して一時的に送信ジョブキューDB に格納し、その後指定された方法（FTP、MQ、Mail または蓄積サーバ配信）でバックオフィスへ配信する。



⑥ デジタルレシート参照機能

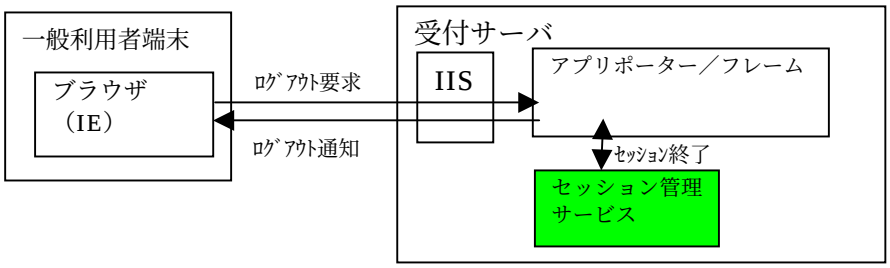
受付が完了すると、受付番号通知画面が一般利用者端末に表示され、受付番号が通知される。受付番号通知画面で「レシート取得」を押すとレシート管理サービスによって取得していたレシート情報がダウンロードされる。



⑦ セッション情報保持機能

セッション管理サービスは、ログイン認証にて作成した認証済ユーザ情報（ユーザコンテクスト）をセッション確立中は保持管理する。

一般利用者がログアウトボタンを押すとセッション管理サービスは、ユーザ認証によって生成されたセッションを終了する。ログアウト処理が一定時間行われなかった場合は、タイムアウトでセッションを終了する。ログアウト後、ログアウト通知画面が表示される。



（2）運用管理者に対する TOE 機能

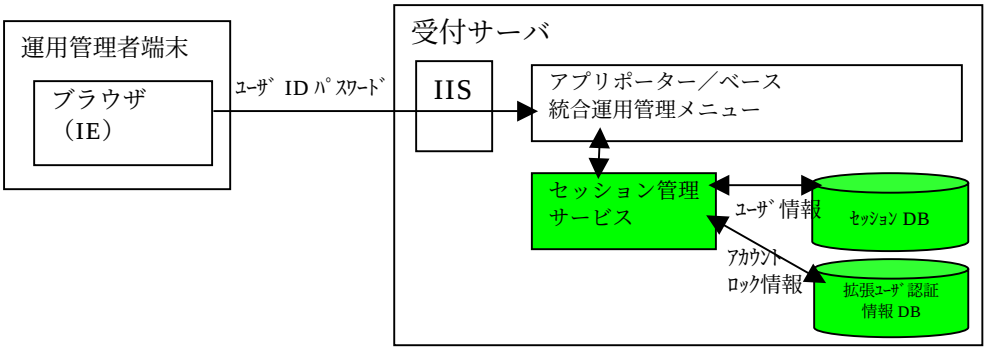
運用管理者による運用管理業務の TOE 機能をデータフロー例にて以下に示す。ユーザ情報は RDB による管理とする。

① ユーザ認証機能、ユーザ情報参照機能

運用管理者は統合運用管理ログイン画面にユーザ ID とパスワードを入力する。

TOE のセッション管理サービスはセッション DB を検索し、利用者のロール、パスワードのハッシュ値を得る。セッション管理サービスは、利用者のパスワードのハッシュ値を取りセッション DB との比較により認証を行う。次にセッション管理サービスは拡張ユーザ認証情報 DB を確認して利用者がロックアウトされていない

か判定する。以上のログイン認証が正しく済んだらセッション管理サービスは認証済ユーザ情報（ユーザコンテクスト）を作成しセッションを開始、管理する。ログインが成功したら統合運用管理メニュー画面が表示される。

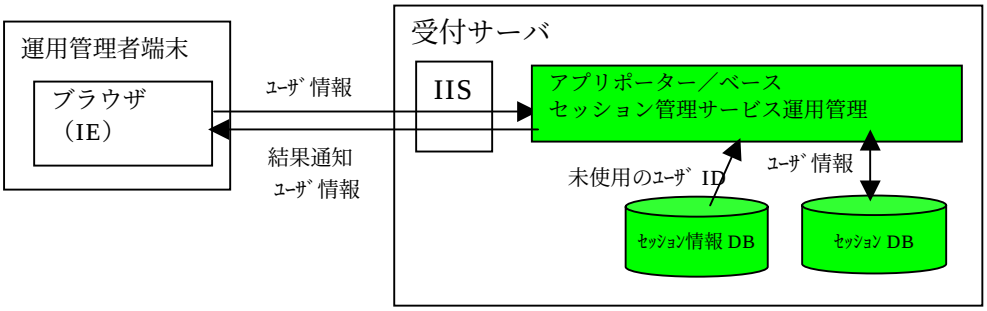


② 利用者情報管理機能

運用管理者が統合運用管理メニュー画面からセッション管理サービスを選択すると、セッション管理サービス運用管理が開始される。セッション管理サービス運用管理メニュー画面で、「ユーザ登録」のラジオボタンを選び、「実行」を押すと新規ユーザ登録画面が表示される。

ユーザ ID の自動生成の設定の場合、セッション管理サービス運用管理はセッション情報 DB からユーザ ID を取り出し、ユーザ ID 欄に表示される。ユーザ ID を任意指定する場合は運用管理者が任意のユーザ ID を入力する。SSL クライアント証明書はファイルパスを指定する。パスワード等ユーザ情報を入力して「登録」ボタンを押すと、セッション管理サービス運用管理は、パスワードポリシー（最小文字数・最大文字数、利用可能文字）に従ってパスワードチェックを行い、問題なければ確認画面を表示し「登録」ボタンを押すとユーザ情報をユーザ情報 DB に登録する。パスワード・SSL クライアント証明書についてはハッシュ値を取りハッシュ値のみを登録する。

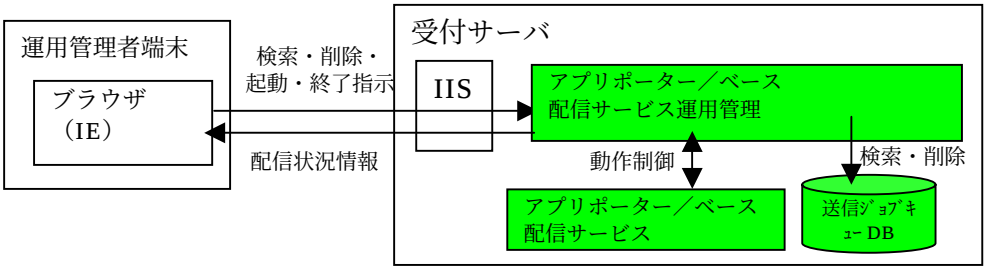
セッション管理サービス運用管理のメニューからは他に、ユーザ情報の検索・更新・削除等を行うことができる。



③ 配信サービス管理機能、配信データ管理機能

運用管理者が統合運用管理メニュー画面から配信サービスを選択すると、配信管理サービス運用管理が開始される。

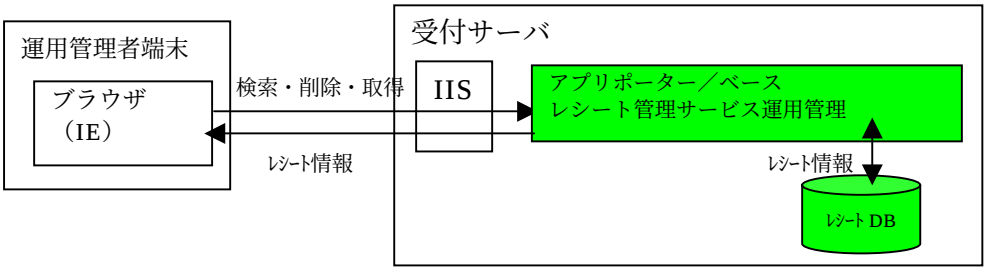
配信管理サービス運用管理メニューで業務を選択して送信ジョブキューのエントリ（配信先が指定された申請書データ）の検索・削除、配信サービスの配信機能の起動・終了を行うことができる。



④ レシートデータ管理機能

運用管理者が統合運用管理メニュー画面からレシート管理サービスを選択すると、レシート管理サービス運用管理が開始される。

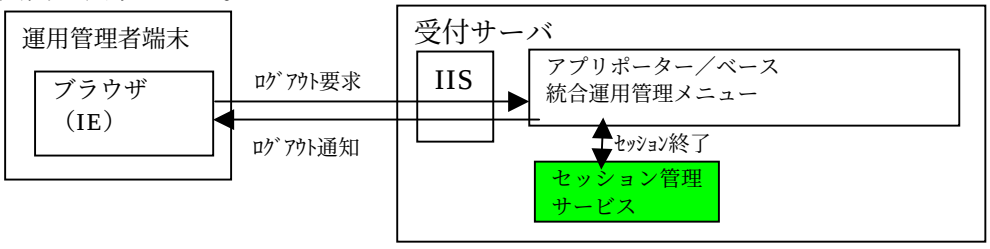
レシート管理サービス運用管理メニューで業務を選択してレシートの検索・削除・ダウンロードを行う。



⑤ セッション情報保持機能

セッション管理サービスは、ログイン認証にて作成した認証済ユーザ情報（ユーザコンテクスト）を、セッション確立中は保持管理する。

運用管理者がログアウトボタンを押すとセッション管理サービスは、ユーザ認証によって生成されたセッションを終了する。ログアウト処理が一定時間行われなかった場合は、タイムアウトでセッションを終了する。ログアウト後、ログアウト通知画面が表示される。

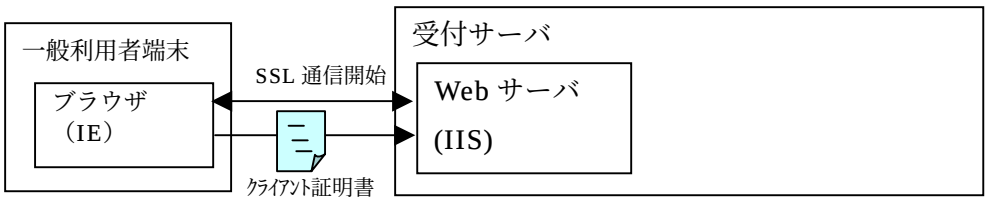


（3）LDAP を使う場合のユーザ認証

ユーザ情報管理については RDB または LDAP を選択できる。以下に LDAP サーバ（iPlanet Directory Server）を使った場合のユーザ認証についての例を示す。

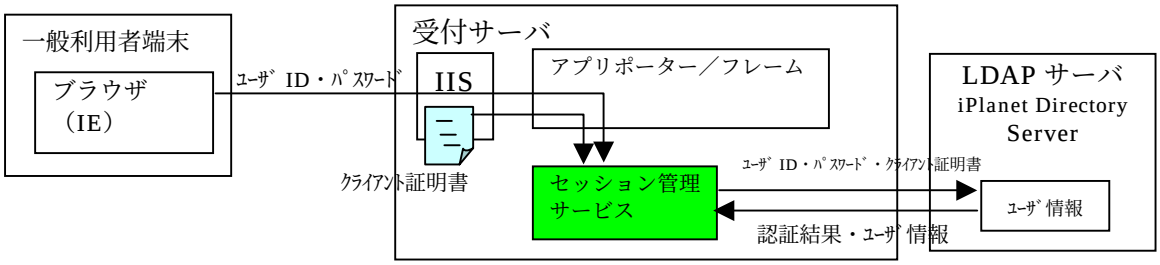
① Web サーバとの SSL 通信開始

一般利用者は Web サーバにアクセスし SSL による暗号通信路を確保し、SSL クライアント証明書を Web サーバに渡す。



② ユーザ認証機能、ユーザ情報参照機能

一般利用者はログイン画面にユーザ ID とパスワードを入力する。TOE のセッション管理サービスは LDAP サーバにユーザ ID・パスワード・SSL クライアント証明書を引渡す。LDAP サーバではパスワード・SSL クライアント証明書により認証を行う。また利用者がロックアウトされていないか判定する。LDAP サーバで認証が成功すると、セッション管理サービスは認証成功の通知と利用者のロール等ユーザ情報を得る。以上のログイン認証が正しく済んだらセッション管理サービスは認証済ユーザ情報（ユーザコンテクスト）を作成しセッションを開始、管理する。



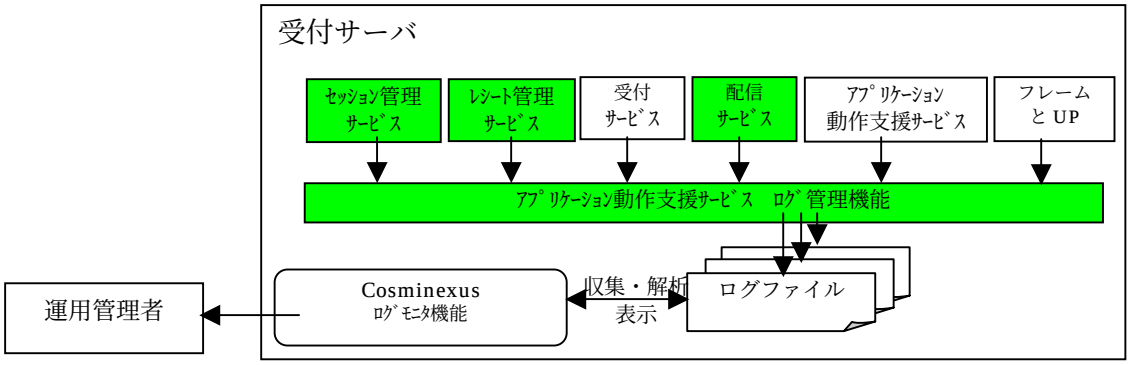
（4）ログ管理機能

アプリケーション動作支援サービスのログ管理機能について、データフローの概要を以下に示す。

・ログファイル出力

アプリケーション動作支援サービスのログ管理機能はアプリポーターの各サービスのメッセージについて DD（Deployment Descriptor）システム定義で定義されたログ出力事象種別、出力先ディレクトリ等を元に該当するレベルのログを出力する。同様にフレームの標準プログラムと UP（ユーザが開発したプログラム）についても DD 定義を元にログを出力する。

運用管理者は受付サーバの Cosminexus ログモニタ機能により、ログの収集・表示・検索等を行う。



2.5　物理条件及び利用制限

TOE の物理条件及び利用制限を以下に示す。

- TOE 運用環境は、入退室管理された開発棟内のサーバ室に設置し、関係者以外は立ち入りできない。
- 運用管理者端末が接続する TOE 運用環境の運用管理者 LAN はネットワーク構成上、バックオフィスと接続するバックオフィス LAN とは別の独立したネットワークとする。
- TOE 運用環境の運用管理者 LAN とインターネットなど一般利用者の接続する外部ネットワークの間にはファイアウォールを設置する。
- 一般利用者端末の設置場所は任意とするが、一般利用者は自らの責任において、TOE の利用規則に従って TOE にアクセスするために必要な秘密情報を管理する責務を負う。
- 運用規則にて定められた所定期間毎に定期保守を実施する。定期保守時は、TOE 運用環境外部とのネットワーク接続を一時的に遮断する。
- 一般利用者端末から Web サーバへの通信は、SSL による通信路の暗号化を行うよう Web サーバを設定する。また TOE の認証において SSL クライアント証明書による認証を行う場合は SSLv3 によるサーバ認証、クライアント認証及び通信路の暗号化を行う設定とする。

TOE の運用環境及び特定したアプリポーターの設定及び使用方法を以下に示す。

- 申請書には一般利用者により PKCS#7 電子署名または XML 電子署名が付与されることとする。
- 暗号処理に適用するアルゴリズムは、TripleDES　168 ビット、RSA 1024 ビット、SHA-1 160 ビットを利用する。

3. TOE セキュリティ環境

3.1 保護資産

申請書データ

資産の性質

一般利用者が作成した申請書データで、TOE が受信する以前に一般利用者により電子署名が付加されている。

TOE は申請書データ受領証拠としてレシートデータを作成する為に、申請書データを一時的に保持する。TOE 範囲であるレシート管理サービスは申請書データにアクセスする。

TOE 内において、
申請書データは、運用管理者以外への暴露から守られなければならない。
申請書データは、不当な改ざん、削除から守られなければならない。

ユーザ管理情報

資産の性質

一般利用者・運用管理者の識別・認証情報、及び一般利用者のＳＳＬクライアント証明書。識別にはユーザ ID、認証にはパスワードが使われる。また一般利用者の認証においては、ＳＳＬクライアント証明書による認証も合わせて実施することが可能。
TOE はユーザ管理情報を保管する。TOE は、個々のユーザ管理情報の変更処理とユーザ情報作成・削除の管理機能を持つ。

TOE 内において、
ユーザ管理情報は、本人、運用管理者以外への暴露から守られなければならない。
ユーザ管理情報は、不当な改ざん、削除から守られなければならない。

レシートデータ

資産の性質

申請書データに対する電子署名値と受付番号、受付日時、申請者のユーザ ID 等管理情報からなる。電子署名は TOE 外で保管される受付秘密鍵を使って行われる。レシートデータは申請書の受領証拠として生成される。TOE 内で生成・保管・参照・削除等を管理する。

TOE 内において
レシートデータは、本人、運用管理者以外への暴露から守られなければならない。
レシートデータは、不当な改ざん、削除から守られなければならない。

3.2 前提

A.BACKUP

運用規定に沿って資産のバックアップが行われており、以下にあげる資産を一定時間前の状態に戻すことができるようになっている。

- 申請書データ、ユーザ管理情報、レシートデータ
- 監査データ、秘密鍵

A.PHYSICAL_ACCESS

受付サーバ（及び受付サーバコンソール)、資産のバックアップが保管されたメディア、運用管理者端末、及び運用管理者 LAN とバックオフィス LAN が収容された場所は、入退出管理を実施する。

A.ADMINISTRATOR

監査者、運用管理者は、それぞれに課せられた役割に対して許可された一連の行為に関して悪意を持った行為は行わない。

A.TRUST_CERT

電子証明書と対応する秘密鍵の発行及び失効は、TOE の範囲外において信頼できる CA によって行われる。発行された電子証明書と対応する秘密鍵は信頼できる。

A.NETWORK

TOE へのネットワークからのアクセスを許可する箇所は､特定箇所のみに限定されており、TOE とバックオフィス、運用管理者端末は専用の LAN で結ばれている。また、バックオフィスでの運用は信頼できる。

A.VIRUS

TOE 外部からのウィルスなど不正プログラムの侵入を検出するよう、定期的にウィルスチェックが実施されている。

3.3 脅威

本 TOE では、脅威をもたらす攻撃者として“ 運用管理者以外 ”の以下の者を想定する。

- 一般利用者として TOE の利用権限を持つが、他の利用者（運用管理者または他の一般利用者）に成りすまそうとする者
- TOE の利用権限を持たない者
  （一般利用者以外のインターネット上のユーザ及び、運用組織内の他システム関連者）

T.INTERNAL_USER_DATA_ACCESS

TOE 内部で保管される申請書データが、攻撃者の行為により運用管理者端末から削除、改ざん、暴露される。
これにより TOE は申請処理そのものを実施しない、正規の申請内容と異なった申請処理を実施する、申請内容の漏洩、という不具合が発生する。

T.INTERNAL_AUTH_DATA_ACCESS

TOE 内部で保管されるユーザ管理情報が、攻撃者の行為によりインターネットまたは運用管理者端末から削除、改ざん、暴露される。
これにより、正当な利用者が TOE を利用出来ない、TOE へログインする際になりすましが発生する、という不具合が発生する。

T.INTERNAL_RECEIPT_DATA_ACCESS

TOE 内部で保管されるレシートデータが、攻撃者の行為によりインターネットまたは運用管理者端末から削除、改ざん、暴露される。
これにより、一般利用者本人が申請処理内容の確認が出来ない、TOE が処理した結果と異なる処理内容が一般利用者本人に通知される、申請内容の漏洩、という不具合が発生する。

T.DISCLOSE_NW_DATA

TOE と一般利用者端末間のインターネット上の通信において、ネットワーク上でやり取りされるユーザ管理情報、レシートデータ、及び申請書データが暴露される。
これにより、TOE への成りすましの発生、申請結果及び申請書データ内容の漏洩といった不具合が発生する。

3.4 組織のセキュリティ方針

OSP.REPUDIATION

運用管理者は一般利用者に対して、以下を証明しなければならない。

・TOE が申請書データを受け付けたことを否認できない為の証明。

OSP.IMPORT_USER_DATA_INTEGRITY

運用管理者は、TOE にインポートされる一般利用者からの申請書に対して以下を実施しなければならない。

・申請者である一般利用者を正しく識別・認証し、申請書が改ざんされていないことを確認する。

（申請者本人の意図しない申請内容となっていないことの確認）

4. セキュリティ対策方針

認証情報の管理と識別認証機能は、TOE、IT 環境のどちらでも実現可能とする。また、上記の対策方針は TOE、IT 環境の何れかで実施するものとし、TOE の対策方針と IT 環境の対策方針の双方に記述を行う。

4.1 TOE のセキュリティ対策方針

O.ID_AUTH

TOE は、IT 環境で識別・認証しない場合、正しく一般利用者、運用管理者の識別・認証を行わなければならない。
また、識別・認証されたユーザ情報をセッション確立中は維持しなければならない。

O.ADMIN

TOE は、IT 環境で識別・認証しない場合、ユーザ管理情報の管理を運用管理者に、または一般利用者のパスワード変更をその一般利用者本人に限定しなければならない。

O.AUDIT

TOE は、セキュリティに関連したイベントを適切に記録する手段を提供しなければならない。

O.NON_REPUDIATION

TOE は、TOE が申請書データを受け付けたことを証明する証拠としてレシートデータを作成しなければならない。

4.2　環境のセキュリティ対策方針

（1）運用管理面を規定する環境対策方針

OE.ACCOUNT
運用管理者は、組織で定められた役割に割り当てられる人員に変更があった場合、TOE 内のアカウントや認証情報にすみやかに反映させなければならない。

OE.AUTH
運用管理者は、自身の認証情報や TOE 所有の認証情報の推測や暴露を防ぐように管理しなくてはならない。

OE.BACKUP
運用管理者は、定められた時点以降の状態に戻せるように、運用規定に沿って資産のバックアップを行わなければならない。

OE.PHYSICAL_ACCESS
受付サーバ（及び受付サーバコンソール）、資産のバックアップが保管されたメディア、運用管理者端末が設置される場所は、入退出管理、又は施錠管理されたボックス内など、組織内のものだけが物理的にアクセスできるように管理しなければならない。運用管理者 LAN とバックオフィス LAN の管理も同様である。
また、監査者が監査を実施する際は、運用管理者による操作のもとで実施するものとする。

OE.ADMINISTRATOR
監査者、運用管理者がそれぞれに課せられた役割に対して許可された一連の行為に関して悪意を持った行為を行わないことを保証するために、組織の責任者は適切な人選を行い、管理や教育を実施しなければならない。

OE.TRUST_CERT
信頼できる CA を利用しなければならない。

OE.NETWORK

運用管理者は、以下の点を管理しなければならない。

- TOE とインターネットなどの外部ネットワークは識別された特定個所のみで接続されていることを保証し、ファイアウォールにより TOE と一般利用者端末または CA 以外の通信を禁止する。
- 運用管理者 LAN とバックオフィス LAN はそれぞれ、一般利用者と TOE を結ぶ外部ネットワークから独立し、受付サーバと運用管理者端末またはバックオフィスとの通信はインターネットへ漏れないように管理する。
  また、バックオフィスでの運用は信頼できるよう管理されなければならない。

OE.VIRUS

運用管理者は、受付サーバ内に保存される申請書に対するウィルスチェックを実施するなどし、申請書を経由して TOE 内に不正なプログラムが持ち込まれることを防止しなければならない。

（2）IT 環境の製品により実現する環境対策方針

OE.ID_AUTH
IT 環境は、TOE で識別・認証しない場合、正しく一般利用者、運用管理者の識別・認証を行わなければならない。

OE.FILE_ACCESS
IT 環境は、申請書データ、ユーザ管理情報およびレシートデータが入ったファイルに直接アクセスすることを、ＯＳアドミニストレータ権限を持つ運用管理者に限定しなければならない。

OE.AUDIT
IT 環境は、セキュリティに関連したイベントを適切に記録する手段を提供しなければならない。

OE.ACCESS_SEC_KEY
IT 環境は、秘密鍵・公開鍵に対する参照、更新、廃棄などの操作を、ＯＳアドミニストレータ権限を持つ運用管理者に限定するようアクセス制御しなければならない。

OE.SIGNATURE
IT 環境は、本人確認や、否認防止、改ざんを検出するための署名機能、及び検証機能を以下の場合に提供しなくてはならない。
・ 一般利用者から送信される申請書データが TOE にインポートされる場合の署名検証
・ 申請書データ受信証拠であるレシートデータ生成時に署名を付与

OE.ADMIN
IT 環境は、TOE で識別・認証しない場合、ユーザ管理情報の管理を運用管理者に、または一般利用者のパスワード変更をその一般利用者本人に限定しなければならない。
また、識別・認証動作を決定する設定はＯＳアドミニストレータ権限を持つ運用管理者に限定しなければならない。

OE.MONITOR
IT 環境は、TOE が生成する監査データに対し、データの検索など効率的な監査を実施する機能を提供しなければならない。

OE.ACCESS_AUDIT_DATA

IT 環境は、TOE が生成した監査データに対する参照、更新、削除などの操作を運用管理者に限定するようアクセス制御しなくてはならない。

OE.SSL

IT 環境は、一般利用者端末と TOE 間の通信においての暴露を防止する為に、Secure Socket Layer（SSL）を適用した、HTTPS プロトコルを使用した暗号化通信を実施しなくてはならない。また SSL のバージョンは、一般的な WWW ブラウザの具備する SSLv3 を使用する。

5. IT セキュリティ要件

5.1 TOE セキュリティ機能要件

FAU_GEN.1　監査データ生成

下位階層: なし

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: 最小、基本、詳細、指定なし*]のすべての監査対象事象; 及び
c) *上記以外の個別に定義した監査対象事象*

[*選択: 最小、基本、詳細、指定なし*]

指定なし

[詳細化:]

c)の*上記以外の個別に定義した監査対象事象* を以下に示す。

表 5-1 監査対象事象

コンポーネント	選択	個別に定義した監査対象事象
FAU_GEN.1	—	なし
FAU_SEL.1	指定なし	なし
FCO_NRR.2	指定なし	FCO_NRR.2(T)に関する、 ①レシートデータ作成の成功と失敗の記録
FIA_AFL.1	指定なし	FIA_AFL.1(T)に関する、 ①連続認証失敗回数が閾値に達した場合のロックアウト開始記録 ②及び時間経過によりロックアウト解除後の最初の認証成功記録
FIA_ATD.1	—	なし
FIA_SOS.1	指定なし	FIA_SOS.1(T)で定義した品質尺度に照し合せた、 ①パスワード登録・変更の成功／失敗の記録 ②登録・変更内容の記録 ③登録者・変更者の記録 ④登録・変更が発生した時刻の記録
FIA_UAU.2	指定なし	FIA_UAU.2(T)に関する、 ①認証における失敗の記録 ②失敗者の記録 ③失敗が発生した時刻の記録
FIA_UAU.5	指定なし	FIA_UAU.5(T)に関して、２つの複合認証において、 ①パスワード認証での成功／失敗の記録 ②ＳＳＬクライアント認証での成功／失敗の記録 ③複合認証でのトータルな認証の成功／失敗の記録 ④成功者／失敗者の記録 ⑤成功／失敗が発生した時刻の記録
FIA_UAU.7	—	なし
FIA_UID.2	指定なし	FIA_UID.2(T)に関して、 ①識別における失敗の記録

		②失敗者の記録 ③失敗が発生した時刻の記録
FIA_USB.1	指定なし	なし
FMT_MTD.1	指定なし	a)FMT_MTD.1(T)(1)に関する、 ①ロックアウト閾値の変更の成功／失敗の記録 ②変更者の記録 ③および時刻の記録 b)FMT_MTD.1(T)(2)に関する、 ①ロックアウトフラグ変更後の値の記録 ②変更の成功／失敗の記録 ③変更者の記録 ④時刻の記録 C)FMT_MTD.1(T)(3)に関する、 ①認証失敗回数クリア間隔値の変更の成功／失敗の記録 ②変更者の記録 ③時刻の記録 d)FMT_MTD.1(T)(4)に関する、 ①ロックアウト期間の値の変更成功／失敗の記録 ②変更者の記録 ③時刻の記録 e)FMT_MTD.1(T)(6)に関する、 ①レシートデータ削除、ダウンロードの成功／失敗の記録 ②対象者の記録 ③時刻の記録 f)FMT_MTD.1(T)(7)に関する、 ①パスワード、ユーザＩD、証明書、ロールに関する変更後の値の記録 ②変更の成功／失敗記録 ③変更者の記録 ④時刻の記録 g)FMT_MTD.1(T)(9)に関する、 ①一般利用者による本人パスワード変更後のハッシュ値の記録 ②変更の成功／失敗記録 ③変更者の記録 ④時刻の記録
FMT_SMF.1	指定なし	a)FMT_SFM.1(T)(1)に関する、 ①セッション管理サービス運用管理におけるアカウント（ユーザＩD、パスワード及び SSL クライアント証明書)、ロールへ全操作記録 ②セッション管理サービスにおける一般利用者本人のパスワード変更に関する操作記録 ③ロックアウト設定値の操作記録 b)FMT_SMF.1(T)(2)に関する、

		①レシート管理サービス運用管理におけるレシートデータへの全操作記録
FMT_SMR.1	指定なし	FMT_SMR.1(T)に関する、 ①ロールへの全操作記録
FPT_RVM.1	―	なし

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: *その他の監査関連情報*]

[割付: *その他の監査関連情報*]

存在しない

依存性: FPT_STM.1 高信頼タイムスタンプ

補足：FAU_GEN.1.1 の a) 監査機能の起動と終了　は、TOE の機能ではなく IT 環境にて実施される機能である。

FAU_SEL.1　選択的監査

下位階層: なし

FAU_SEL.1.1　TSFは以下のような属性に基づいて、監査事象のセットから監査対象事象を含めたり、除外したりすることができなければならない:

a)[選択: *オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別*]
b)[*割付: 監査の選択性の基礎となる追加属性リスト*]

[選択: *オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別*]

事象種別

[*割付: 監査の選択性の基礎となる追加属性リスト*]

なし

依存性: FAU_GEN.1 監査データ生成
FMT_MTD.1 TSF データの管理

FCO_NRR.2　受信の強制的証明

下位階層: FCO_NRR.1

FCO_NRR.2.1　TSFは、受信した[割付: *情報種別のリスト*]の受信の証拠生成を実施しなければならない。

[割付: *情報種別のリスト*]

一般利用者からの申請書データ

FCO_NRR.2.2　TSFは、情報の受信者の[割付: *属性のリスト*]を証拠が適用される情報の[割付: *情報フィールドのリスト*]に関係付けることができなければならない。

[割付: *属性のリスト*]

TOE の電子署名、受付番号、受付日時、申請者のユーザ ID

[割付: *情報フィールドのリスト*]

申請書データ

FCO_NRR.2.3　TSFは、[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]へ、[割付: 受信の証拠における制限]の範囲で、情報受信の証拠を検証する能力を提供しなければならない。

[選択: *発信者*、*受信者*、[割付: *第三者のリスト*]]

発信者、受信者

[割付: 受信の証拠における制限]

運用管理者によりレシートデータが削除されるまで（運用サイト側の運用ルールにてレシート保存期限を決め、その期間内においては受信証拠を検証できる。）

依存性: FIA_UID.1 識別のタイミング

FIA_AFL.1　認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1　TSFは、[割付: *認証事象のリスト*]に関して、[割付: *回数*]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*]

１０分間（デフォルト）以内の間隔での連続した、運用管理者と一般利用者に関する認証（但し、運用管理者はパスワード認証のみ。一般利用者はパスワード認証のみの場合とパスワード＋ＳＳＬクライアント証明書認証の複合認証の両方に関して対象とする。）

[割付: *回数*]

３回（デフォルト）

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]

該当ユーザを６０分間（デフォルト）ロックアウトし、ログイン出来なくする。

その後、上記ロックアウト期間経過後に、自動的に該当ユーザはログイン可能となる。
また、ロックアウト期間経過を待たずとも以下の運用管理者の操作によっても該当ユーザはログイン可能となる。

・ロックアウトユーザ一覧からユーザを指定するか、ユーザＩＤを直接指定してロックアウトフラグを解除する。

依存性: FIA_UAU.1 認証のタイミング

FIA_ATD.1　利用者属性定義

下位階層: 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[割付: *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*]

ロール

依存性: なし

FIA_SOS.1　秘密の検証

下位階層: 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*]

繰返	対象	定義された品質尺度
1	パスワードによる認証	パスワードとして使用できる文字列に関しての基準を、 ①最小文字数６文字 かつ ②使用可能文字を英字（a～z、Ａ～Ｚ）と数字（０～９）、記号（!"#$%&'()*+,-./:;<>=?@[\]^_`{}¦~）の計９４文字以上とする

依存性: なし

FIA_UAU.2　アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.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、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.5　複数の認証メカニズム

下位階層: なし

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

[割付: *複数の認証メカニズムのリスト*]

パスワード認証とＳＳＬクライアント認証での複合認証

FIA_UAU.5.2　TSFは、[割付: *複数の認証メカニズムがどのように認証を提供するかを記述する規則*]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。

[割付:*複数認証メカニズムがどのように認証を提供するかを記述する規則*]

運用管理者によるＤＤファイルの設定（一般利用者認証方式フラグの設定）によって、一般利用者に対してはパスワード認証とＳＳＬクライアント認証の複合認証を実施することが出来る（デフォルトはパスワード認証のみ)。その場合、両方に合格した場合のみ認証成功となる。(該当者がロックアウト中であった場合は、両者の認証で成功となっても認証失敗となる。)

依存性: なし

FIA_UAU.7　保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1　TSFは、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付: *フィードバックのリスト*]

入力されたパスワード文字を＊（アスタリスク）で表示

依存性: FIA_UAU.1 認証のタイミング

FIA_UID.2　アクション前の利用者識別

下位階層: FIA_UID.1

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。

依存性: なし

FIA_USB.1　利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1　TSFは、適切な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。

依存性: FIA_ATD.1 利用者属性定義

FMT_MTD.1　TSFデータの管理

下位階層: なし

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。

繰返	TSFデータのリスト	操作	許可された識別された役割
1	ロックアウト閾値	デフォルト値変更､問い合わせ、改変	運用管理者
2	ロックアウトフラグ	改変、消去	運用管理者
3	認証失敗回数クリア間隔	デフォルト値変更､問い合わせ、改変	運用管理者
4	ロックアウト期間	デフォルト値変更､問い合わせ、改変	運用管理者
5	ロックアウト対象者一覧	問合せ	運用管理者
6	レシートデータ	問い合わせ､削除､ダウンロード（『その他の操作』を選択）	運用管理者
7	運用管理者･一般利用者のユーザＩＤ、パスワード、ロール及び一般利用者のＳＳＬクライアント証明書	問合せ、改変、削除、消去生成（『その他の操作』を選択）	運用管理者
8	パスワード最小文字数､最大文字数､使用可能文字種類	デフォルト値変更､問い合わせ、改変	運用管理者
9	一般利用者のパスワード	改変	一般利用者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1　管理機能の特定

下位階層: なし

FMT_SMF.1.1　TSFは､以下のセキュリティ管理機能を行う能力を持たねばならない:[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]。

[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]

繰返	TSFによって提供されるセキュリティ管理機能のリスト
1	セッション管理サービス運用管理における①アカウント（ユーザＩＤ、パスワード及び一般利用者のSSLクライアント証明書）、ロールへのアクセス管理②ロックアウト情報（閾値、ロックアウトフラグ、クリア間隔、ロックアウト期間、対象者）の管理機能③パスワード品質定義値（最小文字数、最大文字数、使用可能文字種類）の管理 セッション管理サービスにおける、一般利用者本人のパスワード変更機能
2	レシート管理サービス運用管理における、レシートデータ管理機能

依存性: なし

FMT_SMR.1　セキュリティ役割

下位階層: なし

FMT_SMR.1.1　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*]

運用管理者、一般利用者

FMT_SMR.1.2　TSFは、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FPT_RVM.1　TSPの非バイパス性

下位階層: なし

FPT_RVM.1.1　TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

5.2　IT 環境に対するセキュリティ機能要件

FAU_GEN.1　監査データ生成

下位階層: なし

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: 最小、基本、詳細、指定なし*]のすべての監査対象事象; 及び
c)*上記以外の個別に定義した監査対象事象*

[*選択: 最小、基本、詳細、指定なし*]

指定なし

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: *その他の監査関連情報*]

[割付: *その他の監査関連情報*]

存在しない

●TSF に関する詳細化

本要件は Cosminexus Application Server に対する機能要件である。

依存性: FPT_STM.1 高信頼タイムスタンプ

補足：IT 環境は TOE の監査機能の起動と終了に関する監査データを生成する。従って、FAU_GEN.1 の a)のみが IT 環境の機能要件であり、他は TOE の機能要件である。

FAU_SAR.1　監査レビュー

下位階層: なし

FAU_SAR.1.1　TSFは、[割付: *許可利用者*]が、[割付: *監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付: *許可利用者*]

運用管理者

[割付: *監査情報のリスト*]

全ての TOE 監査データ

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。

●TSF に関する詳細化

本要件は Cosminexus Application Server に対する機能要件である。

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.2　限定監査レビュー

下位階層: なし

FAU_SAR.2.1　TSFは、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

●TSF に関する詳細化

本要件は OS に対する機能要件である。

依存性: FAU_SAR.1 監査レビュー

FAU_SAR.3　選択可能監査レビュー

下位階層: なし

FAU_SAR.3.1　TSFは、[割付: *論理的な関連の基準*]に基づいて、監査データを[選択: *検索、分類、並べ替え*]する能力を提供しなければならない。

[割付: *論理的な関連の基準*]

取得日付、取得時刻、プロセスＩＤ、スレッド識別子、メッセージＩＤ、イベント種別

[選択: *検索、分類、並べ替え*]

検索、分類、並べ替え

●TSF に関する詳細化

本要件は Cosminexus Application Server に対する機能要件である。

依存性: FAU_SAR.1 監査レビュー

FAU_STG.1　保護された監査証跡格納

下位階層: なし

FAU_STG.1.1　TSFは、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、監査記録の改変を[選択: *防止*、*検出*]できねばならない。

[選択: *防止*、*検出*]

防止

●TSF に関する詳細化

本要件は OS に対する機能要件である。

依存性: FAU_GEN.1 監査データ生成

FCS_COP.1　暗号操作

下位階層: なし

FCS_COP.1.1　TSFは、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。

繰返	TSF	標準のリスト	暗号アルゴリズム	暗号鍵長	暗号操作のリスト
1	PKI サービス	PKCS#1	RSA	1024 ビット	・レシートデータへのデジタル署名 ・申請書の署名検証
2	PKI サービス	FIPS 180-2	SHA-1	なし	・パスワード、SSL クライアント証明書のハッシュ値算出
3	Web サーバ	PKCS#1 FIPS 180-2 FIPS 46-3	RSA SHA-1 TripleDES	1024 ビット なし 168 ビット	・SSL 通信によるクライアント認証 ･通信の暗号化/復号化

依存性: [FDP_ITC.1 セキュリティ属性なし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_CKM.4　暗号鍵廃棄

下位階層: なし

FCS_CKM.4.1　TSFは、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵廃棄方法[割付*: 暗号鍵廃棄方法*]に従って、暗号鍵を廃棄しなければならない。

繰返	TSF	標準のリスト	暗号鍵廃棄方法
1	PKI サービス	なし	新しい電子証明書の登録によるファイルの上書き。
2	PKI サービス	なし	セッション終了時にメモリ領域を開放する。

3	Web サーバ	なし	セッション終了時にメモリ領域を開放する。

依存性　: [FDP_ITC.1 セキュリティ属性なし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

FDP_ACC.1　サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1　TSFは、[割付: *サブジェクト、オブジェクト、及び**SFP**で扱われるサブジェクトとオブジェクト間の操作のリスト*]に対して[割付: *アクセス制御**SFP***]を実施しなければならない。

[割付: *サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト*]及び[割付: *アクセス制御 SFP*]

繰返	TSF	サブジェクト	オブジェクト	SFP で扱われるサブジェクトとオブジェクト間の操作	アクセス制御 SFP
1	OS	運用管理者の OS 管理プロセス	・申請者データディレクトリファイル ・ユーザ情報管理ファイル ・レシートデータファイル	参照、変更、削除	OS ファイルアクセス制御 SFP
2	PKI サービス	TOE 電子証明書管理プロセス	媒体に保管された秘密鍵および TOE 電子証明書保管ファイル	登録	TOE 電子証明書アクセス制御 SFP

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

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

FDP_ACF.1.1　TSFは、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]に基づいて、オブジェクトに対して、[割付: *アクセス制御**SFP***]を実施しなければならない。

[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]及び[割付: *アクセス制御 SFP*]

繰返	TSF	セキュリティ属性、 名前付けされたセキュリティ属性のグループ	アクセス制御 SFP
1	OS	サブジェクトのセキュリティ属性：OS アドミニストレータ権限	OS ファイルアクセス制御 SFP

2	PKI サービス	サブジェクトのセキュリティ属性：OS アドミニストレータ権限 オブジェクトのセキュリティ属性：TOE 電子証明書の有効期間、失効情報	TOE 電子証明書アクセス制御 SFP

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: *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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]。

[割付: *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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則*]

繰返	TSF	アクセス制御 SFP	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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則
1	OS	OS ファイルアクセス制御 SFP	運用管理者のOS管理プロセスにOSアドミニストレータ権限が有れば、申請者データディレクトリファイル、ユーザ情報管理ファイル、レシートデータファイルの参照、変更、削除を許可する。
2	PKI サービス	TOE 電子証明書アクセス制御 SFP	TOE 電子証明書管理プロセスは、OS アドミニストレータ権限のある運用管理者が「登録キー」を押すと、媒体に保管された秘密鍵および TOE 電子証明書保管ファイルをアクセスし TOE 電子証明書が有効であればPKI サービスに登録を許可する。

FDP_ACF.1.3　TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]

なし

FDP_ACF.1.4　TSFは、[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]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。

[割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則*]

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_DAU.1　基本データ認証

下位階層: なし

FDP_DAU.1.1　TSFは、[割付: *オブジェクトまたは情報種別のリスト*]の有効性の保証として使用できる証拠を生成する能力を提供しなければならない。

[割付: *オブジェクトまたは情報種別のリスト*]

申請書データ

FDP_DAU.1.2　TSFは、示された情報の有効性の証拠を検証する能力を[割付: *サブジェクトのリスト*]に提供しなければならない。

[割付: *サブジェクトのリスト*]

申請書を送信した一般利用者、運用管理者

●TSF に関する詳細化

本要件は PKI サービスに対する機能要件である。

依存性: なし

FDP_IFC.1　サブセット情報フロー制御

下位階層: なし

FDP_IFC.1.1　TSFは、[割付: *サブジェクト、情報、及び、SFPによって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]に対して[割付: *情報フロー制御SFP*]を実施しなければならない。

[割付: サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]及び[割付: 情報フロー制御 SFP]

繰返	TSF	サブジェクト	情報	SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作	情報フロー制御 SFP
1	PKI サービス	受信プロセス	申請書データ	申請書受信、破棄	申請書情報フロー制御 SFP
2	Web サーバ	SSL 通信プロセス	SSL クライアント証明書およびセッション鍵	SSL クライアント証明書とセッション鍵のインポートおよび通信の開始	SSL クライアント証明書インポート情報フロー制御 SFP

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFF.1　単純セキュリティ属性

下位階層: なし

FDP_IFF.1.1　TSFは、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御**SFP***]を実施しなければならない: [割付: *セキュリティ属性の最小数及び種別*]。

繰返	TSF	セキュリティ属性の最小数	セキュリティ属性種別	情報フロー制御 SFP
1	PKI サービス	4	・サブジェクトのセキュリティ属性：送信情報 ・情報のセキュリティ属性：申請書データの電子署名値、申請者の電子証明書の有効期間、失効情報	申請書情報フロー制御 SFP
2	Web サーバ	3	・サブジェクトのセキュリティ属性：一般利用者からの接続開始要求 ・情報のセキュリティ属性：SSL クライアント証明書の有効期間、失効情報	SSL クライアント証明書インポート情報フロー制御 SFP

FDP_IFF.1.2　TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]。

[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

繰返	TSF	各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係
1	PKI サービス	受信プロセスの送信情報が ” 一般利用者の申請書送信 ” であれば、申請者の電子証明書をインポートし申請書データの電子署名値を検査する。その結果、申請者の電子証明書が有効かつ申請書データに改ざんが検出されなければ申請書データを受信し、電子証明書が無効または申請書データに改ざんが検出されれば申請書データを破棄する。
2	Web サーバ	SSL 通信プロセスは一般利用者からの接続開始要求であれば、SSL クライアント証明書が有効な場合、SSL クライアント証明書とセッション鍵をインポートし通信を開始する。

FDP_IFF.1.3　TSFは、[割付: *追加の情報フロー制御**SFP**規則*]を実施しなければならない。

[割付: *追加の情報フロー制御 SFP 規則*]

なし

FDP_IFF.1.4　TSFは、以下の[割付: *追加の**SFP**能力のリスト*]を提供しなければならな

い。

[割付: *追加の SFP 能力のリスト*]

なし

FDP_IFF.1.5 TSFは、以下の規則に基づいて、情報フローを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]

なし

FDP_IFF.1.6 TSFは、次の規則に基づいて、情報フローを明示的に拒否しなければならない: [割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]

なし

依存性: FDP_IFC.1 サブセット情報フロー制御

FMT_MSA.3 静的属性初期化

FDP_ITC.1 セキュリティ属性なしの利用者データのインポート

下位階層: なし

FDP_ITC.1.1 TSFは、SFPに従って制御され、TSC外から利用者データをインポートするときは、[割付: *アクセス制御SFP及び/または情報フロー制御SFP*]を実施しなければならない。

繰返	TSF	アクセス制御 SFP 及び/または情報フロー制御 SFP
1	PKI サービス	TOE 電子証明書アクセス制御 SFP
2	PKI サービス	申請書情報フロー制御 SFP
3	Web サーバ	SSL クライアント証明書インポート情報フロー制御 SFP

FDP_ITC.1.2 TSFは、TSC外からインポートされるとき、利用者データに関連付けられたいかなるセキュリティ属性も無視しなければならない。

FDP_ITC.1.3 TSFは、SFPに従って制御され、TSC外から利用者データをインポートするときは、以下の規則を実施しなければならない: [割付: *追加のインポート制御規則*]

[割付: *追加のインポート制御規則*]
なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_MSA.3 静的属性初期化

FIA_AFL.1　認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1　TSFは、[割付: *認証事象のリスト*]に関して、[割付: *回数*]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*]
１０分間（デフォルト）以内の間隔での連続した、運用管理者と一般利用者に関する認証（但し、運用管理者はパスワード認証のみ。一般利用者はパスワード認証のみの場合とパスワード＋ＳＳＬクライアント証明書認証の複合認証の両方に関して対象とする。）
[割付: *回数*]
３回（デフォルト）

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]
該当ユーザを６０分間（デフォルト）ロックアウトし、ログイン出来なくする。
その後、上記ロックアウト期間経過後に、自動的に該当ユーザはログイン可能となる。
また、ロックアウト期間経過を待たずとも以下の運用管理者の操作によっても該当ユーザはログイン可能となる。
・ロックアウトユーザ一覧からユーザを指定するか、ユーザＩＤを直接指定してロックアウトフラグを解除する。

●TSF に関する詳細化
本要件は iPlanet　Directory　Server に対する機能要件である。
依存性: FIA_UAU.1 認証のタイミング

FIA_ATD.1　利用者属性定義

下位階層: 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[割付: *セキュリティ属性のリスト*]を維持しなければならない。

●TSF に関する詳細化及び割付

繰返	TSF	セキュリティ属性のリスト
1	iPlanet Directory Server	ロール（TOE ログイン時）
2	OS	アドミニストレータ権限（OS ログイン時）

依存性: なし

FIA_SOS.1 秘密の検証

下位階層: 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。

●TSFに関する詳細化及び割付

繰返	TSF	対象	定義された品質尺度
1	iPlanet Directory Server	パスワードによる認証	パスワードとして使用できる文字列に関しての基準を、 ①最小文字数６文字 かつ ②使用可能文字を英字（a～z、Ａ～Ｚ）と数字（０～９）、記号（!"#$%&'()*+,-./:;<>=?@[\]^_`{}|~）の計９４文字以上とする
2	Cosminexus Application Server	SSL クライアント証明書による認証	ハッシュ関数 SHA-1 で取得される１６０ビットのメッセージ要約値による証明書検証

依存性: なし

FIA_UAU.2　アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.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、各利用者に認証が成功することを要求しなければならない。

●TSFに関する詳細化

繰返	TSF
1	iPlanet Directory Server
2	OS

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.5　複数の認証メカニズム

下位階層: なし

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

[割付: *複数の認証メカニズムのリスト*]

パスワード認証とＳＳＬクライアント認証での複合認証

FIA_UAU.5.2　TSFは、[割付: *複数の認証メカニズムがどのように認証を提供するかを記述する規則*]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。

[割付:*複数の認証メカニズムがどのように認証を提供するかを記述する規則*]

運用管理者によるＤＤファイルの設定（一般利用者認証方式フラグの設定）によって、一般利用者に対してはパスワード認証とＳＳＬクライアント認証の複合認証を実施することが出来る（デフォルトはパスワード認証のみ)。その場合、両方に合格した場合のみ認証成功となる。(該当者がロックアウト中であった場合は、両者の認証で成功となっても認証失敗となる。)

●TSF に関する詳細化

本要件は iPlanet　Directory　Server に対する機能要件である。

依存性: なし

FIA_UAU.7　保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1　TSFは、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付: *フィードバックのリスト*]

入力されたパスワード文字を＊（アスタリスク）で表示

●TSF に関する詳細化

本要件は iPlanet　Directory　Server に対する機能要件である。

依存性: FIA_UAU.1 認証のタイミング

FIA_UID.2　アクション前の利用者識別

下位階層: FIA_UID.1

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。

●TSFに関する詳細化

繰返	TSF
1	iPlanet Directory Server
2	OS

依存性: なし

FIA_USB.1　利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1　TSFは、適切な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。

●TSF に関する詳細化

本要件は OS に対する機能要件である。

依存性: FIA_ATD.1 利用者属性定義

FMT_MSA.1　セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1　TSFは、セキュリティ属性[割付: *セキュリティ属性のリスト*]に対し[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付: *その他の操作*]]をする能力を[割付: *許可された識別された役割*]に制限するために[割付: *アクセス制御SFP*、*情報フロー制御SFP*]を実施しなければならない。

[割付: *セキュリティ属性のリスト*]

OS アドミニストレータ権限

[選択: *デフォルト値変更*、*問い合わせ*、*改変*、*削除*、[割付: *その他の操作*]]

生成（その他の操作を選択）、問い合わせ、改変、削除

[割付: *許可された識別された役割*]

OS アドミニストレータ権限を持つ運用管理者

[割付: *アクセス制御 SFP*、*情報フロー制御 SFP*]

OS ファイルアクセス制御 SFP、TOE 電子証明書アクセス制御 SFP

●TSF に関する詳細化

本要件は OS に対する機能要件である。

依存性: [FDP_ACC.1 サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MSA.2　セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1　TSF は、セキュアな値だけがセキュリティ属性として受け入れられることを保証しなければならない。

●TSFに関する詳細化

繰返	TSF
1	PKI サービス
2	Web サーバ

依存性: ADV_SPM.1 非形式的 TOE セキュリティ方針モデル

[FDP_ACC.1 サブセットアクセス制御または

FDP_IFC.1 サブセット情報フロー制御]

FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティ役割

FMT_MTD.1　TSFデータの管理

下位階層: なし

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。

●TSFに関する詳細化及び割付

繰返	TSF	TSFデータのリスト	操作	許可された識別された役割
1	Cosminexus Application Server	一般利用者認証方式フラグ	デフォルト値変更、問い合わせ、改変	OS アドミニストレータ権限を持つ運用管理者
2	iPlanet Directory Server	ロックアウト閾値	デフォルト値変更、問い合わせ、改変	運用管理者
3	iPlanet Directory Server	ロックアウトフラグ	改変、消去	運用管理者
4	iPlanet Directory Server	認証失敗回数クリア間隔	デフォルト値変更、問い合わせ、改変	運用管理者
5	iPlanet Directory Server	ロックアウト期間	デフォルト値変更、問い合わせ、改変	運用管理者

6	iPlanet Directory Server	ロックアウト対象者一覧	問合せ	運用管理者
7	iPlanet Directory Server	運用管理者・一般利用者のユーザＩＤ、パスワード、ロール及び一般利用者のSSLクライアント証明書	問合せ、改変、削除、消去 生成（『その他の操作』を選択）	運用管理者
8	Cosminexus Application Server	ログ出力事象種別	デフォルト値変更、問い合わせ、改変	OS アドミニストレータ権限を持つ運用管理者
9	iPlanet Directory Server	パスワード最小文字数、最大文字数、使用可能文字種類	デフォルト値変更、問い合わせ、改変	運用管理者
10	Cosminexus Application Server	ユーザ情報管理方式フラグ	デフォルト値変更、問い合わせ、改変	OS アドミニストレータ権限を持つ運用管理者
11	iPlanet Directory Server	一般利用者のパスワード	改変	一般利用者
12	Cosminexus Application Server	セッションタイムアウトまでの時間	デフォルト値変更、問い合わせ、改変	OS アドミニストレータ権限を持つ運用管理者

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1　管理機能の特定

下位階層: なし

FMT_SMF.1.1　TSFは、以下のセキュリティ管理機能を行う能力を持たねばならない:[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]。

●TSF に関する詳細化及び割付

繰返	TSF	TSFによって提供されるセキュリティ管理機能のリスト
1	Cosminexus Application Server	Cosminexus管理機能を用いた①一般利用者認証方式フラグの管理機能②TOEのログ出力事象種別の管理機能③ユーザ情報管理をTOE／iPlanet Directory Serverのどちらで実施するか決定するユーザ情報管理方式フラグの管理機能④セッションタイムアウト時間間隔の管理機能
2	OS	運用管理者のOSアカウント管理機能
3	iPlanet Directory Server	セッション管理サービス運用管理機能における①アカウント（ユーザＩＤ、パスワード及び一般利用者のSSLクライアント証明書）、ロールへのアクセス管理②ロックアウト情報（閾値、ロックアウトフラグ、クリア間隔、ロックアウト期間、対象者）の管理機能③パ

		スワード品質定義値（最小文字数、最大文字数、使用可能文字種類）の管理 セッション管理サービスにおける、一般利用者本人のパスワード変更機能

依存性:なし

FMT_SMR.1　セキュリティ役割

下位階層: なし

FMT_SMR.1.1　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。

●TSF に関する詳細化及び割付

繰返	TSF	許可された識別された役割
1	iPlanet Directory Server	運用管理者、一般利用者
2	OS	OS アドミニストレータ権限を持つ運用管理者

FMT_SMR.1.2　TSFは、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FPT_STM.1　高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1　TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

●TSF に関する詳細化

本要件は OS に対する機能要件である。

依存性:なし

FTA_SSL.3　TSF起動による終了

下位階層: なし

FTA_SSL.3.1 TSFは、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

[割付: *利用者が非アクティブである時間間隔*]

1,800 秒（デフォルト）

●TSF に関する詳細化

本要件は Cosminexus Application Server に対する機能要件である。

依存性: なし

FTP_TRP.1　高信頼パス

下位階層: なし

FTP_TRP.1.1　TSFは、それ自身と[選択: *リモート*、*ローカル*]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別及び改変や暴露からの通信データの保護を提供する通信パスを提供しなければならない。

[選択: *リモート*、*ローカル*]

リモート

FTP_TRP.1.2　TSFは、[選択: *TSF*、*ローカル利用者*、*リモート利用者*]が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択: *TSF*、*ローカル利用者*、*リモート利用者*]

リモート利用者

FTP_TRP.1.3　TSFは、[選択: *最初の利用者認証*、[割付: *高信頼パスが要求される他のサービス*]]に対して、高信頼パスの使用を要求しなければならない。

[選択: *最初の利用者認証*、[割付: *高信頼パスが要求される他のサービス*]]

・ 最初の利用者認証

及び

・ 一般利用者端末との間で通信されるユーザ管理情報(ユーザ ID、パスワード)、申請データ、レシートデータの暗号化。

●TSF に関する詳細化

本要件は Web サーバに対する機能要件である。

依存性:なし

5.3　TOE セキュリティ保証要件

保証レベルは、EAL2である。拡張保証コンポーネントは存在しない。

（１）構成管理

ACM_CAP.2 構成要素

（２）配付と運用

ADO_DEL.1 配付手続き

ADO_IGS.1 設置、生成、及び立上げ手順

（３）開発

ADV_FSP.1 非形式的機能仕様

ADV_HLD.1 記述的上位レベル設計開発

ADV_RCR.1 非形式的対応の実証

（４）ガイダンス文書

AGD_ADM.1 管理者ガイダンス

AGD_USR.1 利用者ガイダンス

（６）テスト

ATE_COV.1 カバレージの証拠

ATE_FUN.1 機能テスト

ATE_IND.2 独立試験- サンプル

（７）脆弱性評定

AVA_SOF.1 TOE セキュリティ機能強度評価

AVA_VLA.1 開発者脆弱性分析

5.4　TOE セキュリティ機能強度主張

TOE 機能強度主張が対象とするものはパスワードメカニズムであり、本 ST において対象とする TOE の機能コンポーネントは、

・FIA_SOS.1 のパスワード品質定義機能

及び

・FIA_AFL.1 のアカウントロック機能

である。

両者はそれぞれ最小機能強度レベル SOF－基本を主張する。

これにより、TOE は FIA_SOS.1 と FIA_AFL.1 の組み合わせにより TOE としてのセキュリティ機能強度の最小機能強度レベルは SOF－基本を主張する。

（補足：パスワード認証の他に SSL クライアント証明書による複合認証を実施することも可能である。SSL クライアント証明書認証の強度規定は IT 環境が持つ要件のため本節では対象外である。）

6. TOE 要約仕様

本章では､5.1 の TOE セキュリティ機能要件を満足する TOE の具体的なセキュリティ機能、5.3 の TOE セキュリティ保証要件を満足する具体的な保証手段、及びセキュリティ機能強度分析の対象となる TOE の具体的なセキュリティ機能の識別について記述する。

本章で述べる各セキュリティ機能と、5 章に記述した各 TOE 機能要件の関係を下表 6-1-1 に示す。

表 6-1-1　各セキュリティ機能と TOE 機能要件の関係

セキュリティ機能 ／機能要件	FAU_GEN.1	FAU_SEL.1	FCO_NRR.2	FDP_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.5	FIA_UAU.7	FIA_UID.2	FIA_USB.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1
SF-1：識別･認証				○			○	○	○	○				
SF-2：ｾｯｼｮﾝ情報保持											○			
SF-4：ﾚｼｰﾄ管理			○									○	○	
SF-5：ﾛｸﾞ生成	○	○												
SF-6：ﾕｰｻﾞ情報管理					○	○						○	○	○
SF-7：ｱｶｳﾝﾄﾛｯｸ管理												○	○	

6.1　TOE セキュリティ機能

TOE は以下に示すセキュリティ機能を持つ。

SF-1：識別・認証

（1）利用者識別・認証

TOE を一般利用者または運用管理者が利用する際には、①ログイン、②TOE 操作、③ログアウト、といった手順で実施する必要がある。ログインの際には、まず利用者識別・認証に成功しなければならない。

利用者識別はユーザ ID により行なう。利用者認証の方法はパスワードによる認証、パスワードおよび SSL クライアント証明書による認証の２つの方法がある。利用者認証方法は運用管理者が DD ファイル内の一般利用者認証方式フラグに指定しておき、TOE は一般利用者認証方式フラグに事前に定義してある方法で認証を行う。一般利用者認証方式フラグに指定がない場合はパスワードによる認証を行う。ただし、運用管理者の使う運用管理者用ユティリティではパスワードによる認証のみが利用可能である。（一般利用者認証方式フラグへの設定機能そのものは IT 環境で実施される機能である。）

パスワード認証ではTOEが管理するユーザ管理情報の中のパスワードと利用者の入力したパスワードを比較することで認証する。SSL クライアント証明書方式では、TOE が管理するユーザ管理情報の中のSSLクライアント証明書と利用者がWebサーバに送ったSSL クライアント証明書を比較することで認証する。但し、パスワード及び SSL クライアント証明書はユーザ管理情報にはハッシュ値をエンコードした状態で保管されているので、IT 環境の機能を用いてハッシュを取りエンコードしてから、TOE で比較する。

（2）複数の認証メカニズム

パスワードおよび SSL クライアント証明書による認証では、パスワードによる認証とSSL クライアント証明書による認証の両方で認証成功した場合のみ認証成功となる。

（3）保護された認証フィードバック

パスワード認証時に利用者が入力したパスワードは画面上では＊（アスタリスク）で表示する。

（4）認証失敗時の取り扱い

TOE は利用者がパスワードまたは SSL クライアント証明書による認証に失敗すると、認証失敗回数をカウントアップする。認証失敗回数が「ロックアウト閾値」に達した場合はその利用者のアカウントがロックアウトされる。ロックアウトされた利用者はパスワードや SSL クライアント証明書による認証が成功しても認証失敗としログインできなくする。最後の認証失敗からの経過時間が、「認証失敗回数クリア間隔」の指定時間を超えると認証失敗回数はクリアされる。また、「ロックアウト期間」の指定時間を経過するとアカウントのロックアウトは解除されログイン可能となる。ロックアウト閾値はデフォルトでは３回である。認証失敗回数クリア間隔はデフォルトで 10 分である。ロックアウト期間はデフォルトで 60 分である。

ユーザ情報の管理は RDB(HiRDB または Oracle)による方法と LDAP サーバ（iPlanet Directory　Server）による方法がある。RDB によるユーザ管理の場合、TOE が上記のロックアウトの管理を行う。LDAP によるユーザ管理を選択した場合には、TOE 外のLDAP サーバの機能によってロックアウトの管理を行う。

SF-2：セッション情報保持

利用者識別・認証が成功すると、TOE は認証済みの利用者情報を保持するユーザコンテクストを生成し、ユーザ ID 、ロール等ユーザ管理情報をセットする。識別・認証成功後のTOE ではこのユーザコンテクストのロールを参照することで運用管理者用 Web ページ、ユーザ管理情報、レシート、申請書データ等へのアクセス管理を行う。いったん確立されたセッションは、そのセッションに対して識別・認証済み利用者から明示的にログアウトが

行われるか、もしくはセッションタイムアウトが発生するまで持続される。

SF-4：レシート管理

TOE は申請書の受信証拠として、申請書データに受付番号、受付日時、申請者のユーザ ID を付与したレシートデータを作成し、IT 環境である PKI サービスへ TOE の電子署名の付与を依頼する。PKI サービスから受け取ったレシートデータは、レシート管理サービスにて保管すると同時に、アプリポーター／フレームに渡され申請者にダウンロードされる。また、TOE はレシート管理サービス運用管理機能にて運用管理者に、レシートデータを管理する機能を提供する。識別・認証で正しく認証された運用管理者（ロールが運用管理者）は、レシート DB に蓄積されたレシートについて、レシート ID、取得日、受付番号、ユーザ ID をキーにして検索・一覧表示できる。また表示後にレシートを指定して削除またはダウンロード（レシート DB からの取り出し）ができる。

SF-5：ログ生成

TOE は以下の監査ログを生成する。

- レシートデータ作成の成功／失敗の記録
- 連続認証失敗回数が閾値に達した場合のロックアウト開始記録、及びアカウントロック閾値に達しロックアウトされた者が、時間経過後にロックアウトが解除された後の最初の認証成功記録
- パスワード登録・変更の成功／失敗の記録、登録・変更内容の記録、登録者・変更者の記録、登録・変更が発生した時刻の記録
- セッション管理サービスでの識別、認証の失敗の記録、失敗者の記録、失敗が発生した時刻
- 複合認証において、パスワード認証での成功／失敗の記録、ＳＳＬクライアント認証での成功／失敗の記録、複合認証としての最終的な認証の成功／失敗の記録、成功者／失敗者の記録、成功／失敗が発生した時刻
- ロックアウト閾値の変更の成功／失敗の記録、変更者の記録、および時刻の記録
- ロックアウトフラグ変更後の値の記録、変更の成功／失敗の記録、変更者の記録、時刻の記録
- 認証失敗回数クリア間隔値の変更の成功／失敗の記録、変更者の記録、時刻の記録
- ロックアウト期間の値の変更成功／失敗の記録、変更者の記録、時刻の記録
- セッション管理サービス運用管理機能における運用管理者の TOE アカウント（ユーザ ID、パスワード）、ロールの検索・表示、更新、削除への全アクセス記録
- レシート管理サービス運用管理機能におけるレシートデータの検索、参照、ダウンロード、削除の全操作記録
- セッション管理サービスにおける一般利用者本人のパスワード変更に関する操作記録

ログデータは、イベントごとに、番号（トレースレコード番号)、日付、時刻、AP 名（アプリケーション識別名)、プロセス ID、スレッド識別子、メッセージ ID、種別及びテキスト情報を出力する。

これらの監査ログは、表 6-1-2 に示す事象種別によって監査ログ生成の可否が決定される。

表 6-1-2　監査対象事象と事象種別の関係

監査対象事象	監査ログが生成される事象種別
①レシートデータ作成の成功／失敗の記録	INFO または DEBUG
①連続認証失敗回数が閾値に達した場合のロックアウト開始記録 ②及び時間経過によりロックアウト解除後の最初の認証成功記録	CAUTION または INFO または DEBUG
①パスワード登録・変更の成功／失敗の記録 ②登録・変更内容の記録 ③登録者・変更者の記録 ④登録・変更が発生した時刻の記録	INFO または DEBUG
①認証における、失敗の記録 ②失敗者の記録 ③失敗が発生した時刻の記録	ERROR または WARN または CAUTION または INFO または DEBUG
①パスワード認証での成功／失敗 ②ＳＳＬクライアント認証での成功／失敗 ③複合認証でのトータルな認証の成功／失敗 ④成功者／失敗者の記録 ⑤成功／失敗が発生した時刻	INFO または DEBUG （但し、④失敗者に関するユーザＩＤは DEBUG での出力）
①識別における失敗の記録 ②失敗者の記録 ③失敗が発生した時刻の記録	ERROR または WARN または CAUTION または INFO または DEBUG
①ロックアウト閾値の変更の成功／失敗の記録 ②変更者の記録 ③および時刻の記録	INFO または DEBUG
①ロックアウトフラグ変更後の値の記録 ②変更の成功／失敗の記録 ③変更者の記録 ④時刻の記録	CAUTION または INFO または DEBUG
①認証失敗回数クリア間隔値の変更の成功／失敗の記録 ②変更者の記録 ③時刻の記録	INFO または DEBUG
①レシートデータ削除、ダウンロードの成功／失敗の記録 ②対象者の記録 ③時刻の記録	INFO または DEBUG
①ロックアウト期間の値の変更成功／失敗の記録 ②変更者の記録 ③時刻の記録	INFO または DEBUG

①パスワード、ユーザＩＤ、証明書、ロールに関する変更後の値の記録 ②変更の成功／失敗記録 ③変更者の記録 ④時刻の記録	CAUTION または INFO または DEBUG

また上記の監査事象に関して、監査機能の起動と終了に関するログは含まれていない。起動と終了に関するログは、TOE 範囲ではない IT 環境（Cosminexus Application Server）にて生成しているため本章には記述しない。

SF-6：ユーザ情報管理

ユーザ情報の管理方法は、運用管理者が DD ファイル中のユーザ情報管理方式フラグに指定しておくことで LDAP を使う方法と RDB を使う方法を選択できる。デフォルトでは LDAP を使用する。本記述は、TOE で管理した場合の記述である。

ユーザ情報の管理は、運用管理者のみが管理できる。運用管理者による管理機能はセッション管理サービス運用管理機能である。

（1）アカウント情報の管理

利用者のユーザ ID、パスワード、SSL クライアント証明書の新規登録・更新・削除・検索・参照は TOE を使って行うことができる。この機能を使用できるのは、TOE によりロールが運用管理者である利用者のみに限定される。

ただし、パスワード変更のみはパスワードを所有する一般利用者自身にも変更権限を与える。

（2）ロールの管理

ロールはユーザ情報登録時の必須項目である。ロールには下記の二つがあり、本 ST で示す役割と関連付けられている。

- 運用管理者（本 ST での運用管理者）
- 申請者（本 ST での一般利用者）

ロールの初期登録と変更・追加・削除は運用管理者のみが可能とする。本機能で同一ユーザに上記のロールを両方設定できるが、ロール「なし」には設定できない。

（3）パスワードの制限

ユーザ情報管理に RDB を使う方法の場合は、TOE の機能でパスワードとして使用できる文字列について、最小文字数・最大文字数、英数字以外の使用可能文字の限定ができる。パスワードの最小文字数はデフォルトで 6 文字、パスワードの最大文字数はデフォルトで 32 文字である。

パスワードに使用可能な文字は英数字（a～z,A～Z,0～9）と記号（デフォルトでは　!"#$%&'()*+,-./:;<>=?@[\]^_`{}¦~　）である。

パスワードの新規登録、変更時に TOE は以上のパスワード制限を判定し、適合しない

パスワードについては登録、変更を拒否する。

LDAP を使う方法の場合、これらのパスワードの制限は TOE 外である LDAP ソフトウェアの機能と設定に従う。

SF-7：アカウントロック管理

ユーザ情報管理を RDB で行う方法を選択した場合、TOE はセッション管理サービス運用管理機能の一機能としてアカウントロック管理機能を提供する。アカウントロック管理機能を使用できるユーザは、TOE の識別・認証機能により運用管理者のみに限定される。アカウントロック管理では以下の機能を提供する。

- 現在ロックアウトされているユーザを検索し一覧表示する。
- ロックアウトユーザ一覧からユーザを指定するか、ユーザＩＤを直接指定してロックアウトフラグを解除する。
- ロックアウトに関する設定値である、ロックアウト閾値、ロックアウト期間、認証失敗回数クリア期間について設定値の参照、変更を行う。

6.2　セキュリティ強度

確率的順列的メカニズムに基づくセキュリティ機能は、先述の SF-1：識別・認証、及び SF-6：ユーザ情報管理である。SF-1 は、認証失敗時のアクションとして FIA_AFL.1 によるアカウントロックを実施し、SF-6 は、アカウント作成時のパスワードに関して品質定義を実施する。両者ともそのセキュリティ強度は、SOF-基本である。

6.3　TOE 保証手段

以下の TOE 保証手段により、TOE セキュリティ保証要件が満たされる。

保証コンポーネント	分類	保証手段
ACM_CAP.2 構成要素 ADO_DEL.1 配付手続き	文書	「構成管理規則」
	構成リスト	「プログラム一覧表」 「ドキュメント一覧表」 「ソフトウエア一覧表」 「ハードウエア一覧表」 「構成要素一覧表」
	文書	「アプリポーター配付規則」 「試送連絡票」 「試送時添付資料一覧」 「製品複写適合／合否判定票」 「入庫票」 「記録媒体入庫票」 「ソフトウェア使用許諾契約書」 「ソフトウェア添付資料」
ADO_IGS.1 設置、生成、及び立上げ手順	文書	「アプリポーター環境構築手順書(Windows/HiRDB 版)」 「アプリポーター環境構築手順書(Windows/Oracle 版)」 「アプリポーター環境構築手順書(HP-UX/HiRDB 版)」 「アプリポーター環境構築手順書(HP-UX/Oracle 版)」 「SSL サーバー設定」 「SSL ｸﾗｲｱﾝﾄ設定」 「蓄積サーバ構築手順」
ADV_FSP.1 非形式的機能仕様	文書	「外部インターフェース仕様書」
ADV_HLD.1 記述的上位レベル設計開発	文書	「サブシステム間インターフェース仕様書」
ADV_RCR.1 非形式的対応の実証	文書	「ADV.RCR_表現対応」 「ADV.RCR 確認方法」
AGD_ADM.1 管理者ガイダンス	文書	「アプリポーター／ベース　アドミニストレーターズガイド(Windows 版)」 「アプリポーター／ベース　アドミニストレーターズガイド(HP-UX 版)」
AGD_USR.1 利用者ガイダンス	文書	「アプリポーター／ベース　アドミニストレーターズガイド(Windows 版)」 「アプリポーター／ベース　アドミニストレーターズガイド(HP-UX 版)」
ATE_COV.1	文書	「TSF-テスト項目対応表」

カバレージの証拠		
ATE_FUN.1 機能テスト	文書・記録	「テスト計画書」 「SCL（Windows 版）」 「SCL（HP-UX 版）」 「M票（問題点票）一覧（Windows 版）」 「M票（問題点票）一覧（HP-UX 版）」
ATE_IND.2 独立試験- サンプル	—	評価者が独立テストを実施
AVA_SOF.1 TOE セキュリティ機能強度評価	文書	「TOE セキュリティ機能強度分析書」
AVA_VLA.1 開発者脆弱性分析	文書	「脆弱性分析書」

7. PP主張

本 ST では主張すべき PP は存在しない。

8. 根拠

8.1 セキュリティ対策方針根拠

（1）必要性

セキュリティ対策方針は、TOE セキュリティ環境で規定した TOE の前提と組織のセキュリティ方針を実現するため、あるいは脅威に対抗するためのものである。セキュリティ対策方針と前提条件、脅威または組織のセキュリティ方針の対応関係を以下に示す。

脅威等 ＼ 対策方針	O.ID_AUTH	O.ADMIN	O.AUDIT	O.NON_REPUDIATION	OE.ACCOUNT	OE.AUTH	OE.BACKUP	OE.PHYSICAL_ACCESS	OE.ADMINISTRATOR	OE.TRUST_CERT	OE.NETWORK	OE.VIRUS	OE.ID_AUTH	OE.FILE_ACCESS	OE.AUDIT	OE.ACCESS_SEC_KEY	OE.SIGNATURE	OE.ADMIN	OE.MONITOR	OE.ACCESS_AUDIT_DATA	OE.SSL
A.BACKUP							○														
A.PHYSICAL_ACCESS								○													
A.ADMINISTRATOR									○												
A.TRUST_CERT										○											
A.NETWORK											○										
A.VIRUS												○									
T.INTERNAL_USER_DATA_ACCESS	○		○		○	○	○						○	○	○				○	○	
T.INTERNAL_AUTH_DATA_ACCESS	○	○	○		○	○	○						○	○	○			○	○	○	
T.INTERNAL_RECEIPT_DATA_ACCESS	○		○		○	○	○						○	○	○				○	○	
T.DISCLOSE_NW_DATA																					○
OSP.REPUDIATION				○												○	○				
OSP.IMPORT_USER_DATA_INTEGRITY	○		○		○	○							○		○		○		○	○	

（2）十分性

セキュリティ対策方針は、TOE セキュリティ環境で規定した TOE の前提条件と組織のセキュリティ方針を実現できること、また脅威に対抗できることを説明する。

①前提条件を実現できることについて

「3.2 前提」で識別した前提に対して、セキュリティ対策方針が十分であることを説明する。

前提	対策方針
A.BACKUP	**OE.BACKUP** により、資産を一定時間前の状態に戻すことができるようにバックアップの管理及び運用が行われる。また、資産のバックアップは複数世代または複数個が保管されるように管理及び運用が行われる。
A.PHYSICAL_ACCESS	**OE.PHYSICAL_ACCESS** により **A.PHYSICAL_ACCESS** は実現される。
A.ADMINISTRATOR	**OE.ADMINISTRATOR** により、監査者、運用管理者として適切な人選が行われ、管理や教育が実施されるので、**A.ADMINISTRATOR** が実現される。
A.TRUST_CERT	**OE.TRUST_CERT** により信頼できる CA を利用するので、そこが発行する電子証明書と対応する秘密鍵は信頼できる。

A.NETWORK	**OE.NETWORK** より、TOE と外部ネットワークであるインターネットの接点、及び、内部ネットワークである２つの LAN を管理するので、**A.NETWORK** を実現できる。また、バックオフィスでの運用は信頼できる。
A.VIRUS	**OE.VIRUS** より、外部ネットワークであるインターネットからインポートされる申請書データに対して定期的にウィルスチェックを実施するので、TOE にウィルスが侵入した場合も検出可能である。

②脅威に対抗できることについて

「3.3 脅威」で識別したセキュリティ脅威に対して、セキュリティ対策方針が十分であることを説明する。

脅威	対策方針
T.INTERNAL_USER_DATA_ACCESS	送信ジョブキューに格納された申請書データへのアクセスは運用管理者の総合運用管理ログイン画面からに限られる。総合運用管理メニューでは最初にログインユーザの識別・認証により運用管理者であることを確認する。即ち、TOE の機能 **O.ID_AUTH** 或いは IT 環境の機能 **OE.ID_AUTH** より運用管理者の識別・認証を行う。 認証されたユーザ情報は、**O.ID_AUTH** によりセッション確立中は維持される。 また、認証情報の運用面での管理に関して、**OE.AUTH** により認証情報が正当な所有者以外に暴露することを軽減する。**OE.ACCOUNT** により、運用管理者、一般利用者とそれぞれの認証情報の対応が正確であることを保証する。 **O.AUDIT** にて申請書データアクセスに関する監査ログを収集し、不正アクセスの証拠を検出する。また、TOE の監査機能の起動終了に関する記録は **OE.AUDIT** にて実施する。 これらの監査データに対して、監査データの編集である **OE.MONITOR**、監査データへのアクセス制御である **OE.ACCESS_AUDIT_DATA** は IT 環境の OS により実現する。 さらに、**OE.FILE_ACCESS** により OS から申請書データを直接アクセスすることは、OS アドミニストレータ権限を持つ運用管理者に限定する。 万が一、申請書データに改ざんが発生した場合は、**OE.BACKUP** によりできる限り最新の状態に復元する。
T.INTERNAL_AUTH_DATA_ACCESS	ユーザ管理情報へのアクセスは、運用管理者の場合は総合運用管理ログインから、一般利用者の場合はログイン画面からに限られる。これらの画面では最初にログインユーザの識別・認証により利用者本人であることを確認する。即ち、TOE の機能 **O.ID_AUTH** 或いは IT 環境の機能 **OE.ID_AUTH** より識別・認証を行う。

	認証されたユーザ情報は、**O.ID_AUTH** によりセッション確立中は維持される また、認証情報の運用面での管理に関して、**OE.AUTH** により認証情報が正当な所有者以外に暴露することを軽減する。**OE.ACCOUNT** により、運用管理者、一般利用者とそれぞれの認証情報の対応が正確であることを保証する。 ユーザ管理情報は、TOE で管理する場合は **O.ADMIN** により、IT 環境で管理する場合は **OE.ADMIN** により管理される。即ち、ユーザ管理情報管理は運用管理者に、一般利用者が本人のパスワードを変更する場合はその一般利用者に限定する。 ユーザ管理情報の管理を TOE または IT 環境のいずれかで実施するかの決定を **OE.ADMIN** により OS アドミニストレータ権限を持つ運用管理者に限定する。 **O.AUDIT** にてユーザ管理情報への不正アクセスに関する監査ログを収集し、不正アクセスの証拠を検出する。また、TOE の監査機能の起動終了に関する記録は **OE.AUDIT** にて実施する これらの監査データに対して、監査データの編集である **OE.MONITOR**、監査データへのアクセス制御である **OE.ACCESS_AUDIT_DATA** は IT 環境の OS により実現する。 さらに、**OE.FILE_ACCESS** により OS からユーザ管理情報を直接アクセスすることは、OS アドミニストレータ権限を持つ運用管理者に限定する。 万が一、ユーザ管理情報に改ざんが発生した場合は、**OE.BACKUP** によりできる限り最新の状態に復元する。
T.INTERNAL_RECEIPT_DATA_ACCESS	レシートデータへのアクセスは運用管理者の総合運用管理ログイン画面からに限られる。総合運用管理メニューでは最初にログインユーザの識別・認証により運用管理者であることを確認する。即ち、TOE の機能 **O.ID_AUTH** 或いは IT 環境の機能 **OE.ID_AUTH** より運用管理者の識別・認証を行う。 認証されたユーザ情報は、**O.ID_AUTH** によりセッション確立中は維持される。 また、認証情報の運用面での管理に関して、**OE.AUTH** により認証情報が正当な所有者以外に暴露することを軽減する。**OE.ACCOUNT** により、運用管理者、一般利用者とそれぞれの認証情報の対応が正確であることを保証する。 **O.AUDIT** にてレシートデータへの不正アクセスに関する監査ログを収集し、不正アクセスの証拠を検出する。また、TOE の監査機能の起動終了に関する記録は **OE.AUDIT** にて実施する。 これらの監査データに対して、監査データの編集である **OE.MONITOR**、監査データへのアクセス制御である **OE.ACCESS_AUDIT_DATA** は IT 環境の OS により実現する。 さらに、**OE.FILE_ACCESS** により OS からレシートデータを直接アクセスすることは、OS アドミニストレータ権限を持つ

	運用管理者に限定する。 万が一、レシートデータに改ざんが発生した場合は、**OE.BACKUP** によりできる限り最新の状態に復元する。
T.DISCLOSE_NW_DATA	**OE.SSL** により、一般利用者端末と TOE 間の通信路は SSL により暗号化通信がなされるので、TOE と一般利用者端末間で送信される、ユーザ管理情報（ユーザＩD、パスワード）、申請書データ、レシートデータの暴露を防ぐことが出来る。

③組織のセキュリティ方針に対抗できることについて

「3.4 組織のセキュリティ方針」で識別したセキュリティ方針に対して、セキュリティ対策方針が十分であることを説明する。

脅威	対策方針
OSP.REPUDIATION	**O.NON_REPUDIATION** により、TOE は申請書データを受け付けた証拠としてレシートデータを作成する。**OE.SIGNATURE** により、レシートデータへ電子署名を付与し、一般利用者へレシートデータを返却するため、TOE で受付処理が実施されたことを TOE は否認できない。またその為の TOE の受付秘密鍵は、**OE.ACCESS_SEC_KEY** により IT 環境での特権機能で OS アドミニストレータ権限を持つ運用管理者のみが変更可能とすることにより正しい秘密鍵で常に署名付与及び署名検証が行われる。
OSP.IMPORT_USER_DATA_INTEGRITY	申請書データが TOE にインポートされる際に、申請者が許可された一般利用者であることを認証・識別する。 即ち、TOE の機能 **O.ID_AUTH** 或いは IT 環境の機能 **OE.ID_AUTH** より一般利用者の識別・認証を行う。 認証されたユーザ情報は、**O.ID_AUTH** によりセッション確立中は維持される。 また、認証情報の運用面での管理に関して、**OE.AUTH** により認証情報が正当な所有者以外に暴露することを軽減する。 **OE.ACCOUNT** により、一般利用者とそれぞれの認証情報の対応が正確であることを保証する。 **O.AUDIT** にて申請者の認証・識別に関する監査ログを収集し、不正な申請の証拠を検出する。また、TOE の監査機能の起動終了に関する記録は **OE.AUDIT** にて実施する。 これらの監査データに対して、監査データの編集である **OE.MONITOR**、監査データへのアクセス制御である **OE.ACCESS_AUDIT_DATA** は IT 環境の OS により実現する。 さらに、IT 環境の PKI サービスは申請書データに付与されている一般利用者の署名に対して、**OE.SIGNATURE** により署名検証を実施する。これによって、TOE が申請書データの改ざんに気付かずに申請処理を実施することを防止する。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ機能要件根拠

TOE と IT 環境のセキュリティ機能要件がそれぞれセキュリティ対策方針に対して適切であることを示す。又、セキュリティ保証要件が TOE に対して適切であることも示す。

（1）必要性

「5.1 TOE セキュリティ機能要件」「5.2 IT 環境に対するセキュリティ機能要件」で示したセキュリティ機能要件は、セキュリティ対策方針で規定した TOE のセキュリティ対策方針、及び、IT 環境のセキュリティ製品である Cosminexus、PKI サービス、OS（Windows2000 Ｓerver　又は　HP-UX11.00）のセキュリティ対策方針を実現するための物である。

IT 環境が持つセキュリティ機能要件は、IT 環境が持つセキュリティ対策方針のうち、上記前提製品が持つべき対策方針である、「4.2 環境のセキュリティ対策方針(2)IT 環境の製品により実現する環境対策方針」に規定した、**OE.ID_AUTH**、**OE.FILE_ACCESS**、**OE.AUDIT**、**OE.ACCESS_SEC_KEY** 、 **OE.SIGNATURE** 、 **OE.ADMIN** 、 **OE.MONITOR** 、 **OE.ACCESS_AUDIT_DATA**、**OE.SSL** を実現する為の物である。

TOE、IT 環境のセキュリティ機能要件と各セキュリティ対策方針の対応関係を、表 8-2-1 に示す。各セキュリティ対策方針に対し、それぞれ 1 つ以上のセキュリティ機能要件が対応することにより、この TOE と IT 環境のセキュリティ機能要件セットによって、セキュリティ対策方針はすべて対応付けられる。

本節以降では、

- TOEが持つ機能要件に識別子“T”、IT環境が持つ機能要件に識別子“E”を付けて、機能要件を識別する。
  例）FAU_GEN.1(T)：TOEが持つFAU_GEN.1
  FAU_GEN.1(E)：IT環境が持つFAU_GEN.1

- 同じ機能要件に対して複数回繰返し操作を行っている場合、識別する為に機能要件に識別子として、ST5章の該当機能要件の繰返し番号を加える。
  例）FDP_ACC.1(T)(2)：TOE が持つ FDP_ACC.1 の繰返し操作 2 番目のアクセス制御

- 但し、繰返し操作が 1 回しか無い場合は、繰返し番号を省略する。
  例）FAU_GEN2(T)：TOE が持つ FAU_GEN.2 には繰り返し操作が無い為。

表 8-2-1 セキュリティ機能要件と対応するセキュリティ対策方針

#	機能要件 ／対策方針	O.ID_AUTH	O.ADMIN	O.AUDIT	O.NON_REPUDIATION	OE.ID_AUTH	OE.FILE_ACCESS	OE.AUDIT	OE.ACCESS_SEC_KEY	OE.SIGNATURE	OE.ADMIN	OE.MONITOR	OE.ACCESS_AUDIT_DATA	OE.SSL
T-1	FAU_GEN.1(T)			○										
T-2	FAU_SEL.1(T)			○										
T-3	FCO_NRR.2(T)				○									
T-4	FIA_AFL.1(T)	○												
T-5	FIA_ATD.1(T)	○												
T-6	FIA_SOS.1(T)	○												
T-7	FIA_UAU.2(T)	○												
T-8	FIA_UAU.5(T)	○												
T-9	FIA_UAU.7(T)	○												
T-10	FIA_UID.2(T)	○												
T-11	FIA_USB.1(T)	○												
T-12	FMT_MTD.1(T)(1)		○											
T-13	FMT_MTD.1(T)(2)		○											
T-14	FMT_MTD.1(T)(3)		○											
T-15	FMT_MTD.1(T)(4)		○											
T-16	FMT_MTD.1(T)(5)		○											
T-17	FMT_MTD.1(T)(6)				○									
T-18	FMT_MTD.1(T)(7)		○											
T-19	FMT_MTD.1(T)(8)		○											
T-20	FMT_MTD.1(T)(9)		○											
T-21	FMT_SMF.1(T)(1)		○											
T-22	FMT_SMF.1(T)(2)				○									
T-23	FMT_SMR.1(T)		○		○									
E-1	FAU_GEN.1(E)							○						
E-2	FAU_SAR.1(E)											○		
E-3	FAU_SAR.2(E)												○	
E-4	FAU_SAR.3(E)											○		
E-5	FAU_STG.1(E)												○	
E-6	FCS_COP.1(E)(1)									○				
E-7	FCS_COP.1(E)(2)					○					○			
E-8	FCS_COP.1(E)(3)													○

#	機能要件 ／対策方針	O.ID_AUTH	O.ADMIN	O.AUDIT	O.NON_REPUDIATION	OE.ID_AUTH	OE.FILE_ACCESS	OE.AUDIT	OE.ACCESS_SEC_KEY	OE.SIGNATURE	OE.ADMIN	OE.MONITOR	OE.ACCESS_AUDIT_DATA	OE.SSL
E-9	FCS_CKM.4(E)(1)									○				
E-10	FCS_CKM.4(E)(2)									○				
E-11	FCS_CKM.4(E)(3)													○
E-12	FDP_ACC.1(E)(1)						○							
E-13	FDP_ACC.1(E)(2)								○					
E-14	FDP_ACF.1(E)(1)						○							
E-15	FDP_ACF.1(E)(2)								○					
E-16	FDP_DAU.1(E)									○				
E-17	FDP_IFC.1(E)(1)									○				
E-18	FDP_IFC.1(E)(2)													○
E-19	FDP_IFF.1(E)(1)									○				
E-20	FDP_IFF.1(E)(2)													○
E-21	FDP_ITC.1(E)(1)									○				
E-22	FDP_ITC.1(E)(2)									○				
E-23	FDP_ITC.1(E)(3)													○
E-24	FIA_AFL.1(E)					○								
E-25	FIA_ATD.1(E)(1)					○								
E-26	FIA_ATD.1(E)(2)						○		○					
E-27	FIA_SOS.1(E)(1)					○								
E-28	FIA_SOS.1(E)(2)					○								
E-29	FIA_UAU.2(E)(1)					○								
E-30	FIA_UAU.2(E)(2)						○		○					
E-31	FIA_UAU.5(E)					○								
E-32	FIA_UAU.7(E)					○								
E-33	FIA_UID.2(E)(1)					○								
E-34	FIA_UID.2(E)(2)						○		○					
E-35	FIA_USB.1(E)						○		○					
E-36	FMT_MSA.1(E)						○		○					
E-37	FMT_MSA.2(E)(1)									○				
E-38	FMT_MSA.2(E)(2)													○
E-39	FMT_MTD.1(E)(1)										○			
E-40	FMT_MTD.1(E)(2)										○			

#	機能要件 ／対策方針	O.ID_AUTH	O.ADMIN	O.AUDIT	O.NON_REPUDIATION	OE.ID_AUTH	OE.FILE_ACCESS	OE.AUDIT	OE.ACCESS_SEC_KEY	OE.SIGNATURE	OE.ADMIN	OE.MONITOR	OE.ACCESS_AUDIT_DATA	OE.SSL
E-41	FMT_MTD.1(E)(3)										○			
E-42	FMT_MTD.1(E)(4)										○			
E-43	FMT_MTD.1(E)(5)										○			
E-44	FMT_MTD.1(E)(6)										○			
E-45	FMT_MTD.1(E)(7)										○			
E-46	FMT_MTD.1(E)(8)							○						
E-47	FMT_MTD.1(E)(9)										○			
E-48	FMT_MTD.1(E)(10)										○			
E-49	FMT_MTD.1(E)(11)										○			
E-50	FMT_MTD.1(E)(12)					○								
E-51	FMT_SMF.1(E)(1)					○		○			○			
E-52	FMT_SMF.1(E)(2)						○		○					
E-53	FMT_SMF.1(E)(3)										○			
E-54	FMT_SMR.1(E)(1)										○			
E-55	FMT_SMR.1(E)(2)						○	○	○		○			
E-56	FPT_STM.1(E)							○						
E-57	FTA_SSL.3(E)					○								
E-58	FTP_TRP.1(E)													○

（2）十分性

「5.1 TOE セキュリティ機能要件」により、「4.1 TOE のセキュリティ対策方針」を実現でき、「5.2 IT 環境に対するセキュリティ機能要件」により、「4.2 環境のセキュリティ対策方針(2)IT 環境の製品により実現する環境対策方針」を実現できることを説明する。

セキュリティ対策方針	セキュリティ機能要件
O.ID_AUTH	TOE にて識別認証とユーザ管理情報をもつ場合は、**FIA_SOS.1(T)**及び **FIA_AFL.1(T)**により、パスワード検証能力に不成功試行回数に基づく品質尺度を適用することで機能強度を適正化する。（この時、複合認証を実施する場合には、IT 環境 Cosminexus Application Server にて SSL クライアント証明書に関して **FIA_SOS.1(E)(2)**のハッシュ関数 SHA-1 により証明書検証強度を高める。） **FIA_UAU.2(T)、FIA_UID.2(T)**により TOE 利用の前に必ず識別・認証を要求し **FIA_UAU.7(T)**により、パスワード情報の暴露を防御することにより、識別・認証時の非許可者による認証情報を分析するために利用可能な情報を極小化する。 **FAU_UAU.5(T)**によりパスワード認証とＳＳＬ証明書認証の組み合わせで複合認証を行うことも可能である。 (なお、識別・認証で使用するパスワードと SSL クライアント証明書は IT 環境の **FCS_COP.1(E)(2)**にてハッシュ値を算出する。) **FIA_ATD.1(T)**により識別・認証時に、権限（=ロール）をセキュリティ属性として運用管理者、一般利用者へ結び付け、**FIA_USB.1(T)**にて以降の保護資産へのアクセス制御を可能とする。 (なお、IT 環境の Cosminexus Application Server により一定時間非アクティブとなったセッションは終了される。)
O.ADMIN	識別認証に関する TSF データの管理機能は **FMT_SMF.1(T)(1)**にて提供し、以下の機能要件にて運用管理者に操作を限定する。 認証失敗ユーザのアカウントロック機能は、**FMT_MTD.1(T)(1)～(5)**であらわされる、各種 TSF データにより、ロックアウトを開始する連続認証失敗回数の指定、該当ユーザのロックアウトの解除設定、アカウントロッククリア間隔の設定、ロックアウトに達した場合のロックアウト期間の設定、ロックアウト対象者情報の管理である。 また **FMT_MTD.1(T)(7)、FMT_SMR.1(T)**にて TOE のアカウントであるユーザ管理情報、及びロールのデータ管理を実施している。但し、**FMT_MTD.1(T)(9)**にて、一般利用者に本人のパスワード変更を許可している。 また、パスワードの品質定義値の設定は **FMT_MTD.1(T)(8)**であらわされる、パスワード最小文字数、最大文字数、使用可能文字種類をデフォルト値から変更することが可能である。 **FMT_SMR.1(T)**にて運用管理者、一般利用者の役割を定義・維持する。これらにより、識別・認証時に正しく運用管理者

	と一般利用者を判別でき、TSF データ、セキュリティ属性への不当なアクセスを防いでいる。
O.AUDIT	**FAU_GEN.1(T)**にて TOE が提供するサービスに関して表 6-1-2 で示した監査データを生成する。 **FAU_SEL.1(T)**により上記 TOE 監査事象に対して、IT 環境にて設定されるログ出力事象種別（ワーニングレベル、エラーレベルなど）の設定を受け、監査ログとして生成する事象を選択可能である。（ログレベルの設定改変を管理するデータは IT 環境 Cosminexus Application Server にて管理される。また、IT 環境の OS によりタイムスタンプが提供される。）
O.NON_REPUDIATION	**FCO_NRR.2(T)**により TOE は、受け付けた申請書データを用いて、レシートデータを作成する。作成するレシートデータには、TOE での受付証拠としての電子署名を付与する。 このレシートデータの管理機能は、**FMT_SMF.1(T)(2)**：レシート管理サービス運用管理機能であり、以下の機能要件にて運用管理者に操作を限定する。 **FMT_SMR.1(T)**にて運用管理者、一般利用者の役割を定義・維持する。これらにより、識別・認証時に正しく運用管理者と一般利用者を判別でき、**FMT_MTD.1(T)(6)**にて TOE 内で保管するレシートデータへの問合せ（検索、参照）、削除（削除）、その他（ダウンロード）の操作を運用管理者に限定している。
OE.ID_AUTH	識別・認証で使用するパスワードと SSL クライアント証明書は **FCS_COP.1(E)(2)**にてハッシュ値を算出する。 また、IT 環境である iPlanet Directory Server は、TOE が持つべきセッション管理サービス運用管理機能を TOE と同等に実現することが出来る。以下に、セッション管理サービス運用管理機能が TOE ではなく iPlanet Directory Server にて実現される場合の機能要件に関して検証する。 **FIA_SOS.1(E)(1)**及び **FIA_AFL.1(E)**により、パスワード検証能力に不成功試行回数に基づく品質尺度を適用することで機能強度を適正化する。同様に SSL クライアント証明書についてはハッシュ関数 SHA-1 によるハッシュ値を比較することで、IT 環境 Cosminexus Application Server にて **FIA_SOS.1(E)(2)**の証明書検証強度を高める。 **FIA_UAU.2(E)(1)**、**FIA_UID.2(E)(1)**により TOE 利用の前に必ず識別・認証を要求し **FIA_UAU.7(E)**により、パスワード情報の暴露を防御することにより、識別・認証時の非許可者による認証情報を分析するために利用可能な情報を極小化する。 **FAU_UAU.5(E)**によりパスワード認証とＳＳＬ証明書認証の組み合わせで複合認証を行うことも可能である。 **FIA_ATD.1(E)(1)**により識別・認証時に、権限（=ロール）をセキュリティ属性として運用管理者、一般利用者へ結び付ける。 **FTA_SSL.3(E)**により非アクティブな状態で一定の時間間隔を過ぎたセッションを終了することができる。セッション終了までの時間間隔の管理は、**FMT_MTD.1(E)(12)** および **FMT_SMF.1(E)(1)**により OS アドミニストレータ権限を持つ

	運用管理者に限定している。
OE.FILE_ACCESS	**FDP_ACC.1(E)(1)、FDP_ACF.1(E)(1)**により OS 直接操作による申請書データ、ユーザ管理情報、レシートデータの格納ファイルへのアクセスはセキュリティ属性 OS アドミニストレータ権限を持つ運用管理者に限定する。 **FIA_UAU.2(E)(2)、FIA_UID.2(E)(2)**により OS アドミニストレータ権限を持つ運用管理者を認証・識別し、**FIA_ATD.1(E)(2)**および **FIA_USB.1(E)**にて運用管理者に OS アドミニストレータ権限を結び付け、上記のアクセス制御を有効にする。 このセキュリティ属性である、OS アドミニストレータ権限は**FMT_SMF.1(E)(2)**および **FMT_MSA.1(E)** にて、OS アドミニストレータ権限をもつ運用管理者に管理を限定させる。 実際 **FMT_SMR.1(E)(2)**により OS アドミニストレータ権限は維持されるため識別時に正しく OS アドミニストレータ権限を持つ運用管理者であるかを特定できる。
OE.AUDIT	**FAU_GEN.1(E)**にて Cosminexus Application Server は TOE の監査機能の起動と停止に関する監査データを生成する。 監査機能は **FMT_SMF.1(E)(1)**および **FMT_MTD.1(E)(8)**にて、ログ出力事象種別の切り替え（監査とする範囲を変更できる）を OS アドミニストレータ権限を持つ運用管理者に操作を限定する。これらは、**FMT_SMR.1(E)(2)**により OS アドミニストレータ権限はアカウント内に維持されるため識別時に正しく OS アドミニストレータ権限を持つ運用管理者であるかを特定できるため、保証される。 また IT 環境 OS により、監査データに対して、**FPT_STM.1(E)**にてタイムスタンプを実施し、監査事象の発生時刻を正確に記録する。
OE.ACCESS_SEC_KEY	TOE がレシートデータに署名、検証するための秘密鍵および公開鍵の管理は、IT 環境である PKI サービスの**FDP_ACC.1(E)(2)、FDP_ACF.1(E)(2)**により実現される。 PKI サービスは秘密鍵および公開鍵へのアクセスを OS アドミニストレータ権限を持つ運用管理者に限定する。すなわち、**FIA_UAU.2(E)(2)、FIA_UID.2(E)(2)**により OS アドミニストレータ権限を持つ運用管理者を認証・識別し、**FIA_ATD.1(E)(2)**および **FIA_USB.1(E)**にて運用管理者に OS アドミニストレータ権限を結び付け、上記のアクセス制御を有効にする。 このセキュリティ属性である、OS アドミニストレータ権限は**FMT_SMF.1(E)(2)**および **FMT_MSA.1(E)** にて、OS アドミニストレータ権限をもつ運用管理者に管理を限定させる。 実際 **FMT_SMR.1(E)(2)**により OS アドミニストレータ権限は維持されるため識別時に正しく OS アドミニストレータ権限を持つ運用管理者であるかを特定できる。 以上により特権者以外からの秘密鍵および公開鍵への不当なアクセスを防いでいる。そのため、署名及び署名検証のセキュリティ機能は正しい鍵にて実施される。

OE.SIGNATURE	電子署名付与、及び検証は IT 環境である PKI サービスにより実現される。 申請書データが TOE 内にインポートされる場合に、PKI サービスは **FDP_IFC.1(E)(1)、FDP_IFF.1(E)(1)**にて申請書データの改ざん有無をチェックする。その後その検証結果の証拠として **FDP_DAU.1(E)** にて TOE からの指示によりレシートデータに署名する。 このために PKI サービスは**FCS_COP.1(E)(1)**にて申請書データの改ざんチェックおよびレシートへの署名のための暗号化を実施する。 申請書データの改ざんチェックに使用される暗号鍵は、**FDP_ITC.1(E)(2)**により申請書に付加された申請者の電子証明書をインポートし、チェック終了後は **FCS_CKM.4(E)(2)**により廃棄される。 レシートデータへの署名のための暗号鍵は、**FDP_ITC.1(E)(1)**により媒体からインポートされ、**FCS_CKM.4(E)(1)**により廃棄される。なお、TOE および申請者の電子証明書は、インポート時に **FMT_MSA.2(E)(1)**にて有効性が検証される。 以上により TOE は、申請書データの改ざんに気付かずに申請処理を実施することはなく、一般利用者に対して TOE が申請を受け付けたことを否認できなくなる。
OE.ADMIN	識別認証に関する TSF データの管理を iPlanet Directory Server で実現する場合には **FMT_SMF.1(E)(3)**にて提供する。このとき、**FMT_SMR.1(E)(1)**にて維持される運用管理者、一般利用者の役割から運用管理者に操作を限定する。認証失敗ユーザのアカウントロック機能の設定は、**FMT_MTD.1(E)(2)～(6)**であらわされる各種 TSF データにより、ロックアウトを開始する連続認証失敗回数の指定、該当ユーザのロックアウトの解除設定、アカウントロッククリア間隔の設定、ロックアウトに達した場合のロックアウト期間の設定、ロックアウト対象者情報の管理を運用管理者に限定している。 また **FMT_MTD.1(E)(7)、FMT_SMR.1(E)(1)**にて TOE のアカウントであるユーザ管理情報、及びロールのデータ管理を運用管理者に限定している。但し、**FMT_MTD.1(E)(11)**では、一般利用者に本人のパスワード変更を許可している。この時、パスワードと SSL クライアント証明書は **FCS_COP.1(E)(2)**にてハッシュ値を算出し、ハッシュ値がユーザ管理情報に登録される。 パスワード品質定義は、**FMT_MTD.1(E)(9)**のパスワード最小文字数、最大文字数、使用可能文字種類の変更を運用管理者に限定している。 Cosminexus Application Server は以下のセキュリティ機能に関する管理機能 **FMT_SMF.1(E)(1)**を提供する。このとき、**FMT_SMR.1(E)(2)**にて OS アドミニストレータ権限をもつ運用管理者に管理を限定する。 TOE 或いは iPlanet Directory Server の機能である、パスワードとＳＳＬクライアント認証の複合認証を実施する決定

	は、**FMT_MTD.1(E)(1)**にて一般利用者認証方式フラグの設定変更を OS アドミニストレータ権限を持つ運用管理者に限定している。 ユーザ情報管理方式を TOE で実施するか iPlanet Directory Server で実施するかの決定は、**FMT_MTD.1(E)(10)**のユーザ情報管理方式フラグの変更を OS アドミニストレータ権限を持つ運用管理者に限定している。
OE.MONITOR	監査データの読み出し時の編集機能は IT 環境である Cosminexus Application Server により実現される。 **FAU_SAR.1(E)、FAU_SAR.3(E)**により TOE の監査データを、読み出し編集や監査効率を挙げるための検索機能を提供する。（参照時の編集機能は Cosminexus Application Server によるが、実際の監査データへのアクセス制御は次の OS により実施される）
OE.ACCESS_AUDIT_DATA	監査データへのアクセス制御に関しては OS のアクセス制御にて実現する。 **FAU_SAR.2(E)、FAU_STG.1(E)**にて TOE 監査データへのアクセスを運用管理者に限定し、不当な削除を防止する。（監査データへのアクセス制御は OS が実施するが、データ編集や検索などの機能は Cosminexus Application Server が実施する）
OE.SSL	**FTP_TRP.1(E)**により、一般利用者と TOE との通信は SSL 通信が使用され、申請書データ、レシートデータ、ユーザＩＤ及びパスワードは暗号化通信により、インターネット上での暴露から守られる。 SSL 通信のための暗号化・復号化は、**FCS_COP.1(E)(3)**により実施される。 暗号鍵は **FDP_ITC.1(E)(3)** 、**FDP_IFC.1(E)(2)** 、**FDP_IFF.1(E)(2)**により SSL クライアント証明書およびセッション鍵をインポートし、通信終了時に **FCS_CKM.4(E)(3)** により廃棄される。なお、SSL クライアント証明書は、**FMT_MSA.2(E)(2)**にてセッション確立時に有効性が検証される。

（３）セキュリティ機能要件の依存性

表8-2-2に、セキュリティ機能要件の依存性を示す。

セキュリティ機能要件間の依存性は、CC Part2に完全に準拠している。（インタープリテーションズを含む）

表 8-2-2　セキュリティ機能要件と**依存関係**

#	機能要件	依存先	項番	備考
T-1	FAU_GEN.1 (T)	FPT_STM.1(E)	E-56	時刻取得はOSに依存
T-2	FAU_SEL.1(T)	FAU_GEN.1 (T)	T-1	
		FMT_MTD.1(E)(8)	E-46	TSF ﾃﾞｰﾀであるﾛｸﾞ出力ﾚﾍﾞﾙは Cosminexus で管理
T-3	FCO_NRR.2(T)	FIA_UID.2 (T)	T-10	TOE でユーザ識別･認証を実施する場合。上位の UID.2 を選択
		FIA_UID.2 (E)(1)	E-33	LDAP で識別･認証を実施する場合。上位の UID.2 を選択
T-4	FIA_AFL.1 (T)	FIA_UAU.2 (T)	T-7	上位の UAU.2 を選択
T-5	FIA_ATD.1 (T)	-	-	
T-6	FIA_SOS.1 (T)	-	-	
T-7	FIA_UAU.2 (T)	FIA_UID.2 (T)	T-10	上位の UID.2 を選択
T-8	FIA_UAU.5 (T)	-	-	
T-9	FIA_UAU.7 (T)	FIA_UAU.2 (T)	T-7	上位の UAU.2 を選択
T-10	FIA_UID.2 (T)	-	-	
T-11	FIA_USB.1 (T)	FIA_ATD.1 (T)	T-5	
T-12	FMT_MTD.1 (T) (1)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-13	FMT_MTD.1 (T) (2)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-14	FMT_MTD.1 (T) (3)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-15	FMT_MTD.1 (T) (4)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-16	FMT_MTD.1 (T) (5)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-17	FMT_MTD.1 (T) (6)	FMT_SMR.1 (T)	T-23	
		FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(T)(2)	T-22	
T-18	FMT_MTD.1 (T) (7)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-19	FMT_MTD.1 (T) (8)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-20	FMT_MTD.1 (T) (9)	FMT_SMR.1 (T)	T-23	
		FMT_SMF.1(T)(1)	T-21	
T-21	FMT_SMF.1(T)(1)	-	-	
T-22	FMT_SMF.1(T)(2)	-	-	
T-23	FMT_SMR.1 (T)	FIA_UID.2 (T)	T-10	上位の UID.2 を選択
T-24	FPT_RVM.1 (T)	-	-	
E-1	FAU_GEN.1 (E)	FPT_STM.1(E)	E-56	時刻取得はOSに依存
E-2	FAU_SAR.1(E)	FAU_GEN.1 (T)	T-1	TOE が生成したﾛｸﾞに対して Cosminexus が読み出し編集する
E-3	FAU_SAR.2(E)	FAU_SAR.1(E)	E-2	
E-4	FAU_SAR.3(E)	FAU_SAR.1(E)	E-2	
E-5	FAU_STG.1(E)	FAU_GEN.1 (T)	T-1	TOE が生成したﾛｸﾞに対して OS がｱｸｾｽ制御する
E-6	FCS_COP.1(E)(1)	【FDP_ITC.1(E)(1)	E-21	
		FDP_ITC.1(E)(2)	E-22	

#	機能要件	依存先	項番	備考
		FCS_CKM.1】	×	FDP_ITC.1 との 2 者択一
		FCS_CKM.4(E)(1)	E-9	
		FCS_CKM.4(E)(2)	E-10	
		FMT_MSA.2(E)(1)	E-37	
E-7	FCS_COP.1(E)(2)	【FDP_ITC.1	×	鍵が不要な為、鍵のｲﾝﾎﾟｰﾄも不要。依存採用せず
		FCS_CKM.1】	×	ﾊｯｼｭ計算のため鍵は不要な為、依存を採用せず
		FCS_CKM.4	×	鍵が不要な為、廃棄も不要。依存採用せず
		FMT_MSA.2	×	上記により採用せず
E-8	FCS_COP.1(E)(3)	【FDP_ITC.1(E)(3)	E-23	
		FCS_CKM.1】	×	FDP_ITC.1 との 2 者択一
		FCS_CKM.4(E)(3)	E-11	
		FMT_MSA.2(E)(2)	E-38	
E-9	FCS_CKM.4(E)(1)	【FDP_ITC.1(E)(1)	E-21	
		FCS_CKM.1】	×	FDP_ITC.1 との 2 者択一
		FMT_MSA.2(E)(1)	E-37	
E-10	FCS_CKM.4(E)(2)	【FDP_ITC.1(E)(2)	E-22	
		FCS_CKM.1】	×	FDP_ITC.1 との 2 者択一
		FMT_MSA.2(E)(1)	E-37	
E-11	FCS_CKM.4(E)(3)	【FDP_ITC.1(E)(3)	E-23	
		FCS_CKM.1】	×	FDP_ITC.1 との 2 者択一
		FMT_MSA.2(E)(2)	E-38	
E-12	FDP_ACC.1(E)(1)	FDP_ACF.1(E)(1)	E-14	
E-13	FDP_ACC.1(E)(2)	FDP_ACF.1(E)(2)	E-15	
E-14	FDP_ACF.1(E)(1)	FDP_ACC.1(E)(1)	E-12	
		FMT_MSA.3	×	OS ｱﾄﾞﾐﾆｽﾄﾚｰﾀ権限にﾃﾞﾌｫﾙﾄ値は存在しない
E-15	FDP_ACF.1(E)(2)	FDP_ACC.1(E)(2)	E-13	
		FMT_MSA.3	×	ｾｷｭﾘﾃｨ属性が存在しない為依存を採用せず
E-16	FDP_DAU.1(E)	-	-	
E-17	FDP_IFC.1(E)(1)	FDP_IFF.1(E)(1)	E-19	
E-18	FDP_IFC.1(E)(2)	FDP_IFF.1(E)(2)	E-20	
E-19	FDP_IFF.1(E)(1)	FDP_IFC.1(E)(1)	E-17	
		FMT_MSA.3	×	セキュリティ属性の保管管理が不要なため初期値の保証をしない
E-20	FDP_IFF.1(E)(2)	FDP_IFC.1(E)(2)	E-18	
		FMT_MSA.3	×	ｾｷｭﾘﾃｨ属性は付与されていない為管理不要。依存採用せず
E-21	FDP_ITC.1(E)(1)	【FDP_ACC.1(E)(2)	E-13	
		FDP_IFC.1】	×	FDP_ACC.1 との 2 者択一
		FMT_MSA.3	×	ｾｷｭﾘﾃｨ属性の発生が無い為、依存を採用せず
E-22	FDP_ITC.1(E)(2)	【FDP_ACC.1	×	FDP_IFC.1 との 2 者択一
		FDP_IFC.1(E)(1)】	E-17	
		FMT_MSA.3	×	ｾｷｭﾘﾃｨ属性は発生しない為、依存を採用せず
E-23	FDP_ITC.1(E)(3)	【FDP_ACC.1	×	FDP_IFC.1 との 2 者択一
		FDP_IFC.1(E)(2)】	E-18	
		FMT_MSA.3	×	TOE で新たなｾｷｭﾘﾃｨ属性を付与しない為、依存採用せず
E-24	FIA_AFL.1（E）(1)	FIA_UAU.2（E）(1)	E-29	上位の UAU.2 を選択。LDAP による認証でのｱｶｳﾝﾄﾛｯｸ
E-25	FIA_ATD.1（E）(1)	-	-	

#	機能要件	依存先	項番	備考
E-26	FIA_ATD.1 (E) (2)	-	-	
E-27	FIA_SOS.1 (E) (1)	-	-	
E-28	FIA_SOS.1 (E) (2)	-	-	
E-29	FIA_UAU.2 (E) (1)	FIA_UID.2 (E)(1)	E-33	上位の UID.2 を選択。LDAP による識別･認証
E-30	FIA_UAU.2 (E) (2)	FIA_UID.2 (E)(2)	E-34	上位の UID.2 を選択。OS による識別･認証
E-31	FIA_UAU.5 (E)	-	-	
E-32	FIA_UAU.7 (E)	FIA_UAU.2 (E) (1)	E-29	上位の UAU.2 を選択。LDAP による認証ﾌｨｰﾄﾞﾊﾞｯｸ
E-33	FIA_UID.2 (E) (1)	-	-	
E-34	FIA_UID.2 (E) (2)	-	-	
E-35	FIA_USB.1 (E)	FIA_ATD.1 (E) (2)	E-26	OS による OS ﾕｰｻﾞへの関連付け
E-36	FMT_MSA.1(E)	【FDP_ACC.1(E)(1)	E-12	
		FDP_ACC.1(E)(2)	E-13	
		FDP_IFC.1】	×	FDP_ACC.1 との 2 者択一
		FMT_SMF.1(E)(2)	E-52	
		FMT_SMR.1(E)(2)	E-55	
E-37	FMT_MSA.2(E)(1)	ADV_SPM.1	×	
		【FDP_ACC.1(E)(2)	E-13	
		FDP_IFC.1(E)(1)】	E-17	
		FMT_MSA.1	×	
		FMT_SMR.1	×	
E-38	FMT_MSA.2(E)(2)	ADV_SPM.1	×	
		【FDP_ACC.1	×	FDP_IFC.1 との 2 者択一
		FDP_IFC.1(E)(2)】	E-18	
		FMT_MSA.1	×	
		FMT_SMR.1	×	
E-39	FMT_MTD.1(E)(1)	FMT_SMR.1(E)(2)	E-55	
		FMT_SMF.1(E)(1)	E-51	
E-40	FMT_MTD.1(E)(2)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-41	FMT_MTD.1(E)(3)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-42	FMT_MTD.1(E)(4)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-43	FMT_MTD.1(E)(5)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-44	FMT_MTD.1(E)(6)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-45	FMT_MTD.1(E)(7)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-46	FMT_MTD.1(E)(8)	FMT_SMR.1(E)(2)	E-55	
		FMT_SMF.1(E)(1)	E-51	
E-47	FMT_MTD.1(E)(9)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-48	FMT_MTD.1(E)(10)	FMT_SMR.1(E)(2)	E-55	
		FMT_SMF.1(E)(1)	E-51	

#	機能要件	依存先	項番	備考
E-49	FMT_MTD.1(E)(11)	FMT_SMR.1(E)(1)	E-54	
		FMT_SMF.1(E)(3)	E-53	
E-50	FMT_MTD.1(E)(12)	FMT_SMR.1(E)(2)	E-55	
		FMT_SMF.1(E)(1)	E-51	
E-51	FMT_SMF.1(E)(1)	-	-	
E-52	FMT_SMF.1(E)(2)	-	-	
E-53	FMT_SMF.1(E)(3)	-	-	
E-54	FMT_SMR.1(E)(1)	FIA_UID.2（E)(1)	E-33	上位の UID.2 を選択
E-55	FMT_SMR.1(E)(2)	FIA_UID.2（E)(2)	E-34	上位の UID.2 を選択
E-56	FPT_STM.1(E)	-	-	
E-57	FTA_SSL.3(E)	-	-	
E-58	FTP_TRP.1(E)	-	-	

表にある通り、各機能要件の依存関係は TOE と IT 環境に跨ることはあっても全体で依存性を満たす。特に、依存を拒否している（表中の項番欄に“×”が付いている）箇所について、以下に記述する。

・E-7 の FCS_COP.1(E)(2)から FDP_ITC.1、FCS_CKM.1、FCS_CKM.4、FMT_MSA.2 への依存

本機能はハッシュ値算出のための機能であるため暗号鍵はない。従って、暗号鍵生成、破棄および暗号鍵のセキュリティ属性のセキュリティ確保に関する依存は必要ない。

・E-14 の FDP_ACF.1(E)(1)から FMT_MSA.3 への依存

運用管理者のセキュリティ属性である OS アドミニストレータ権限にはデフォルト値が存在しないため本要件への依存性は不要である。

・E-15 の FDP_ACF.1(E)(2)から FMT_MSA.3 への依存

TOE 電子証明書は、PKI サービスのインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

同様に、運用管理者のセキュリティ属性である OS アドミニストレータ権限にはデフォルト値が存在しないため本要件への依存性は不要である。

・E-19 の FDP_IFF.1(E)(1)から FMT_MSA.3 への依存

セキュリティ属性である送信情報は通信パケット受信時に自動的に設定されサブジェクトによる変更操作はできない。また、電子署名値、電子証明書はインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

・E-20 の FDP_IFF.1(E)(2)から FMT_MSA.3 への依存

SSL クライアント証明書およびセッション鍵は、Web サーバのインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

・E-21 の FDP_ITC.1(E)(1)から FMT_MSA.3 への依存

TOE 電子証明書および秘密鍵は、PKI サービスのインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

・E-22 の FDP_ITC.1(E)(2)から FMT_MSA.3 への依存

申請者の電子証明書は、PKI サービスのインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

・E-23 の FDP_ITC.1(E)(3)から FMT_MSA.3 への依存

SSL クライアント証明書は、Web サーバのインポートにより新たなセキュリティ属性を付与されない。したがって、セキュリティ属性のデフォルト設定に関する本要件への依存性は不要である。

・E-37 の FMT_MSA.2(E)(1)から ADV_SPM.1、FMT_MSA.1、FMT_SMR.1 への依存

TOE の電子証明書および秘密鍵、申請者の電子証明書は信頼された認証局により発行されたものであり、IT 環境である PKI サービスによりセキュリティ属性である有効期間や失効状況などを検証することで安全性が確認される。したがって、TOE のセキュリティ方針モデルを表現する ADV_SPM.1 への依存性は不要である。

また、これらセキュリティ属性はサブジェクトによる値の変更操作はできない。したがって、セキュリティ属性の管理要件である FMT_MSA.1 への依存性は不要である。

さらに、これらセキュリティ属性は IT 環境によって自動的に検証されるため、本機能実行に関するセキュリティ役割を規定する FMT_SMR.1 への依存性は不要である。

・E-38 の FMT_MSA.2(E)(2)から ADV_SPM.1、FMT_MSA.1、FMT_SMR.1 への依存

IT 環境である Web サーバが実施する SSL ハンドシェイクプロトコルは、申請者から受付けた SSL クライアント認証書およびセッション鍵の有効性を検証しセッションを開始する。したがって、セキュリティ属性は安全であり TOE のセキュリティ方針モデルを表現する ADV_SPM.1 への依存性は不要である。

また、SSL クライアント証明書やセッション鍵のセキュリティ属性はサブジェクトに

よる値の変更操作はできない。したがって、セキュリティ属性の管理要件である FMT_MSA.1 への依存性は不要である。
さらに、これらセキュリティ属性は IT 環境によって自動的に検証されるため、本機能実行に関するするセキュリティ役割を規定する FMT_SMR.1 への依存性は不要である。

（4）TOE セキュリティ機能要件の相互作用

表 8.2-3 に、TOE セキュリティ機能要件の相互作用の関係について検証する。

8-2-3　TOE セキュリティ機能要件の相互作用

#	機能要件	防御を提供している要件		
		迂回	破壊	非活性化
T-1	FAU_GEN.1(T)	N/A	N/A	FMT_MTD.1(E)(8)
T-2	FAU_SEL.1(T)	N/A	N/A	FMT_MTD.1(E)(8)
T-3	FCO_NRR.2(T)	N/A	N/A	N/A
T-4	FIA_AFL.1(T)	FPT_RVM.1 (T)	N/A	FMT_MTD.1(T)(1)
T-5	FIA_ATD.1(T)	FPT_RVM.1 (T)	N/A	N/A
T-6	FIA_SOS.1(T)	N/A	N/A	FMT_MTD.1(T)(8)
T-7	FIA_UAU.2(T)	FPT_RVM.1 (T)	N/A	N/A
T-8	FIA_UAU.5(T)	FPT_RVM.1 (T)	N/A	FMT_MTD.1(E)(1)
T-9	FIA_UAU.7(T)	FPT_RVM.1 (T)	N/A	N/A
T-10	FIA_UID.2(T)	FPT_RVM.1 (T)	N/A	N/A
T-11	FIA_USB.1(T)	FPT_RVM.1 (T)	N/A	N/A
T-12	FMT_MTD.1(T)(1)	N/A	N/A	N/A
T-13	FMT_MTD.1(T)(2)	N/A	N/A	N/A
T-14	FMT_MTD.1(T)(3)	N/A	N/A	N/A
T-15	FMT_MTD.1(T)(4)	N/A	N/A	N/A
T-16	FMT_MTD.1(T)(5)	N/A	N/A	N/A
T-17	FMT_MTD.1(T)(6)	N/A	N/A	N/A
T-18	FMT_MTD.1(T)(7)	N/A	N/A	N/A
T-19	FMT_MTD.1(T)(8)	N/A	N/A	N/A
T-20	FMT_MTD.1(T)(9)	N/A	N/A	N/A
T-21	FMT_SMF.1(T)(1)	N/A	N/A	N/A
T-22	FMT_SMF.1(T)(2)	N/A	N/A	N/A
T-23	FMT_SMR.1(T)	N/A	N/A	N/A

N/A：Not Applicable

迂回

一般利用者、運用管理者が TOE を利用する場合は、必ず先に FIA_UID.2(T)、FIA_UAU.2(T)（運用側の設定によっては FIA_UAU.5(T)）が呼び出され、識別認証を迂回することは出来ず、認証失敗時にも FIA_UAU.7(T)、FIA_AFL.1(T)が呼び出される。
さらに TOE は上記利用者が認証に成功した際、常に FIA_ATD.1(T)、FIA_USB.1(T)を適用し、ユーザ情報はセッション確立中、維持される。

破壊
本 TOE のサブジェクトとなるのは一般ユーザと運用管理者のみである。
運用管理者のインタフェースは、TOE のインタフェースおよび OS からアクセスするインタフェースのいずれも内部に閉じられたインタフェースからの利用で、認証識別機能にて運用管理者を特定することにより不信なサブジェクトは存在しない。
一般利用者のインタフェースは、TOE 内において特定データの登録に限定されたインタフェースであり、プログラムの改ざんを可能とするインタフェースではない。
従って、破壊への対応を必要としない。

非活性化
各機能要件の設定変更は、以下の様に非活性化から保護されている。
FUA_GEN.1(T)　：FMT_MTD.1(E)(8)のログ出力事象種別のデータ管理
FAU_SEL.1(T)　：FMT_MTD.1(E)(8)のログ出力事象種別のデータ管理
FIA_AFL.1(T)　：FMT_MTD.1(T)(1) TOE でのロックアウト閾値のデータ管理
FIA_SOS.1(T)　：FMT_MTD.1(T)(8)のパスワード最小文字数・使用文字種のデータ管理
FIA_UAU.5(T)　：FMT_MTD.1(E)(1)の一般利用者認証方式フラグのデータ管理
にて設定変更は、運用管理者および OS アドミニストレータ権限を持つ運用管理者に限定されている。

8.2.2　TOE セキュリティ機能強度主張の根拠

本 TOE の最小機能強度レベル主張は SOF－基本であり、機能強度に関連するメカニズムは、パスワードによる識別認証である。本 TOE は電子政府における電子申請にて利用される。そのため不特定のユーザからの技術的攻撃にさらされる可能性がある。一度攻撃を受けてしまうと、電子政府における電子申請の安全性が損なわれる。

本 TOE の SOF 主張は“ SOF－基本 ”である。これは EAL４までのコマーシャル製品では“ SOF－基本 ”で十分とされる点だけでなく、下記 2 点の根拠から TOE の SOF 主張は妥当である。

（1）対象となる TOE の機能要件、FIA_AFL.1 のアカウントロック、FIA_SOS.1 のパスワード品質定義はともに“ SOF－基本 ”を満たす品質である。（TOE の認証には、パスワード認証とＳＳＬクライアント認証の複合認証のケースも有り得るが、パスワードだけでの認証でも“ SOF‐基本 ”を満たす）

（2）TOE の脅威は運用管理者および一般利用者の公開インタフェースを利用した攻撃であり、その攻撃力は“低レベル”である。従って TOE の主張する機能強度“SOF-基本”で十分に対抗できる。

8.2.3　TOE セキュリティ保証要件の根拠

「5.3 TOE セキュリティ保証要件」で記述した TOE セキュリティ保証要件が必要かつ十分であることを述べる。

本 TOE は電子政府向けの電子申請窓口業務を実現する物であり、申請された文書の保管など運用側での業務主体を定義する物ではない。また TOE 範囲は、識別認証、監査データ生成、管理機能であり、一般利用者と TOE の接点は、識別認証機能だけである。また TOE のセキュリティ機能は、全て運用管理者による設定のみによりセキュリティを実現しており、運用／管理面で十分セキュリティが確保できる。このため、評価保証レベルは EAL2 とする。また、EAL2 に追加すべき保証コンポーネントは存在しない。

8.3　TOE 要約仕様根拠

8.3.1　TOE セキュリティ機能と TOE 機能要件の根拠

（1）必要性

「6.1　TOE セキュリティ機能」で示した TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係を検証する。

表 6-1-3　各セキュリティ機能と TOE 機能用件の関係により、各 TOE セキュリティ機能要件に対し、それぞれ 1 つ以上の TOE セキュリティ機能が対応し、この TOE セキュリティ機能セットによって、TOE セキュリティ機能要件はすべて対応付けられる。また、TOE セキュリティ機能は、これらが一体となってそれぞれの TOE セキュリティ機能要件を満たすことになる。運用管理者は、すべての TOE セキュリティ機能動作のための設定と監査のためのアクションを実施することができる。
これらにより、TOE セキュリティ機能は適切である。

（2）十分性

TOE セキュリティ機能要件	TOE セキュリティ機能
FAU_GEN.1	SF-5：ログ生成にて、DD ファイルに定義されるログ出力事象種別に従って以下の監査データを生成する。 ・ レシートデータ作成の成功／失敗の記録 ・ セッション管理サービスにおける、一般利用者、運用管理者のアカウントロック到達及び、ロックアウト解除後の最初の認証成功記録 ・ パスワード登録・変更の成功／失敗の記録、登録・変更内容の記録、登録者・変更者の記録、登録・変更が発生した時刻の記録 ・ セッション管理サービスの識別認証失敗記録 ・ 複合認証において、パスワード認証での成功／失敗の記録、ＳＳＬクライアント認証での成功／失敗の記録、複合認証としての最終的な認証の成功／失敗の記録、成功者／失敗者の記録、成功／失敗が発生した時刻 ・ ロックアウト閾値の変更の成功／失敗の記録、変更者の記録、および時刻の記録 ・ ロックアウトフラグ変更後の値の記録、変更の成功／失敗の記録、変更者の記録、時刻の記録 ・ 認証失敗回数クリア間隔値の変更の成功／失敗の記録、変更者の記録、時刻の記録 ・ ロックアウト期間の値の変更成功／失敗の記録、変更者の記録、時刻の記録 ・ 運用管理者のセッション管理サービス運用管理機能を用いた、TOE アカウント（ユーザ ID、パスワード）、ロールへの

	操作記録 ・ 運用管理者のレシート管理サービス運用管理機能を用いた、レシートデータへの参照、ダウンロード、削除の操作記録 ・ セッション管理サービスにおける一般利用者本人のパスワード変更に関する操作記録
FAU_SEL.1	SF-5：ログ生成にて、監査事象変更を管理する TSF データである DD ファイルに指定されたログ出力事象種別に応じて、FAU_GEN.1 が定義する各監査事象に関して監査データを生成する／しないの変更が出来る。
FDP_NRR.2	SF-4：レシート管理機能にて申請書データの受領証拠として、受付番号、受付日時、申請者のユーザＩＤを付加したレシートデータの作成を行う。（その後、IT 環境にて電子署名がされ TOE に返送され、）保管・管理は TOE にて検索、表示、削除、ダウンロードの操作を運用管理者に限定している。
FIA_AFL.1	SF-1：識別認証機能にて、連続認証試行への制限を設ける。これにより識別認証のセキュリティ機能を保護している。
FIA_ATD.1	SF-6：ユーザ情報管理機能にて利用者アカウントの一部としてロールを維持し一般利用者と運用管理者を区別している。
FIA_SOS.1	SF-6：ユーザ情報管理機能にてパスワードに対して品質定義を持ち、TOE 利用のアカウントを作成・変更する場合に、適用し、推測されやすいパスワードの生成を防ぐ。これにより識別認証のセキュリティ機能を保護している。
FIA_UAU.2	SF-1：識別認証機能にて運用管理者、一般利用者の認証を実施する。
FIA_UAU.5	SF-1：識別認証機能にて、一般利用者に対してパスワードとＳＳＬクライアント認証の複合認証を実施することができる。これにより識別認証のセキュリティ機能をより強化することが出来る。（この設定は Cosminexus の管理機能を用いて DD ファイル内の一般利用者認証方式フラグ値を変更することにより実施できる。）
FAI_UAU.7	SF-1：識別認証機能にて、認証失敗時にパスワード情報の推測がされるようなメッセージ等の出力を行わない。入力されたパスワードは＊(アスタリスク)で表示され、パスワードの推測を防いでいる。
FIA_UID.2	SF-1：識別認証機能にて運用管理者、一般利用者の識別を実施する。
FIA_USB.1	SF-2：セッション情報保持機能にて運用管理者、一般利用者の各操作にてロール(一般利用者、運用管理者)を識別・認証後の各ユーザに対してセッション確立中、維持している。
FMT_MTD.1	SF-4：レシート管理機能にて、TSF データであるレシートデータに対する検索、参照、削除、ダウンロードの操作は運用管理者の

	みが可能である。 SF-6：ユーザ情報管理機能にて、TSF データである TOE アカウント（ユーザ ID、パスワード）に対する新規登録、更新、削除、検索、参照の操作は運用管理者のみが可能である。但し、一般利用者は本人のパスワードに関してのみ変更可能としている。またパスワード品質定義値（最小文字数、最大文字数、使用可能文字種類）に関する問合せ、変更（デフォルト値からの変更も含む）を運用管理者に限定している。 SF-7：アカウントロック管理機能にて、運用管理者はロックアウトに関する設定値である、ロックアウト閾値、ロックアウト期間、認証失敗回数クリア期間について設定値への参照、変更を行う。 その他にロックアウト対象者の検索、参照、ロックアウト状態を示すロックアウトフラグの参照、変更が可能である。
FMT_SMF.1	SF-4：レシート管理機能にて、レシートデータの検索・一覧表示、削除と言う管理機能を、レシート管理サービス運用管理機能として実現している。 SF-6：ユーザ情報管理機能にて、ユーザＩＤ、パスワード、ＳＳＬクライアント証明書、ロールの生成、改変、削除の管理機能を、セッション管理サービス運用管理機能、セッション管理サービス機能として実現している。 SF-7：アカウントロック管理機能にて、ロックアウト対象者の検索参照、ロックアウト解除、各種ロックアウト機能設定の管理機能を、セッション管理サービス運用管理機能として実現している。
FMT_SMR.1	SF-6：ユーザ情報管理機能にて、TOE のアカウント（ユーザ ID、パスワード）に対して組織の役割としてセキュリティ属性であるロールを維持する。これにより一般利用者、運用管理者が常に正しく判別され、セキュリティ機能は正しく動作する。

8.3.2　セキュリティ強度実装根拠

「6.2 セキュリティ機能強度」で示した通り、TSF である SF-1：識別・認証、及び SF-6：ユーザ情報管理は、ST5 章の識別認証時の FIA_AFL.1 によるアカウントロック、アカウント作成時のパスワードに関しての品質定義を実装している。この２つのセキュリティ機能のセキュリティ強度は、5 章での強度主張 SOF-基本と一致している。

8.3.3　保証手段根拠

「6.3 保証手段」で示した保証手段は、設定した TOE セキュリティ保証要件を実現するためのものである。

各 TOE セキュリティ保証要件に対しそれぞれ 1 つ以上の保証手段が対応することにより、この保証手段セットによって、TOE セキュリティ保証要件はすべて対応付けられる。
また、保証手段に示された文書及び帳票・記録により、本 ST に規定した EAL2 のすべての TOE セキュリティ保証要件が要求する証拠を網羅している。これらにより、保証手段は適切である。