ForceSecure-Filing V01

セキュリティターゲット

V01R21

2005 年 1 月 21 日

― 目次 ―

1 ST 概説

1.1 ST 識別

(1) セキュリティターゲット識別

名称　　：ForceSecure-Filing V01 セキュリティターゲット
バージョン：V01R20
作成日　　：2005 年 1 月 7 日
作成者　　：富士電機アドバンストテクノロジー（株）情報通信制御部

(2) 評価対象識別

名称　　：ForceSecure-Filing
バージョン：V01
製作者　　：富士電機アドバンストテクノロジー（株）情報通信制御部

(3) 作成に使用した CC

①JIS X 5070:2000 セキュリティ技術・情報技術セキュリティの評価基準
②補足－0210

1.2 ST 概要

この文書は、原本性保証ツール「ForceSecure-Filing V01」のセキュリティ仕様を定めたセキュリティターゲット（以下、ST）である。

ForceSecure-Filing V01 は、WWW サーバや暗号ツール、OS などのソフトウエアとともにファイルサーバを構成し、官公庁・自治体、民間企業のイントラネットにおいて、電子文書をセキュアに保存・管理するために使用される。

ForceSecure-Filing をインストールしたファイルサーバ PC に対する電子文書の書込み、読出しなどの命令は、SSL による暗号化およびクライアント認証を付加した HTTP (以下、HTTPS と示す) 経由で行う。

ForceSecure-Filing V01 は、以下の機能を提供する。

- 電子文書の改ざんを検知する。本機能は、電子文書単位で実行される。
- 業務アプリケーションに対し電子文書の保存先グループ単位で権限外の書込み、読出し, 削除を防止する。

さらに、ForceSecure-Filing V01 は、OS 等の外部機能を利用して以下の機能を実現する。

- 電子文書の不正な読出しによる機密情報漏洩防止のため、ファイルサーバ PC に書き込まれる電子文書を暗号化する。
- 電子文書に対する不正なアクセスを防止するため、業務アプリケーションの識別と認証を行う。

なお、電子文書ファイルの書込み、読出し、削除は、ForceSecure-Filing V01 では行わず WWW サーバで実行される。

1.3 CC 適合

本評価対象は、以下の情報セキュリティ評価基準に適合する。

- 機能要件は、JIS X 5070:2000 第 2 部適合である。
- 保証要件は、JIS X 5070:2000 第 3 部適合である。
- 保証レベルは EAL 3 適合である。
- 本 ST が適合している PP はない。

2 TOE 記述

2.1 製品の種別

TOE は、サーバークライアントシステム環境において、サーバ側で電子文書を管理するためのサーバソフトウェア製品 (ForceSecure-Filing V01) である。

2.2 TOE の説明

2.2.1 利用目的

官公庁・自治体においては電子政府が推進され、民間企業では電子商取引が実用化されつつある。これに伴い従来紙文書で行ってきた行政手続き、申請、契約などが電子文書で行われることが一般的な状況になってきている。

しかし、電子文書は、紙文書と比較して改ざんが容易でその痕跡が残りにくい等の特性を有しており、行政文書、申請書類、契約書などの保存・管理を紙文書から電子文書へ移行するためには、これらの問題を解決することが必要である。

TOE は、以下の機能を提供する。

- 電子文書の改ざんを検知する。本機能は、電子文書単位で実行される。
- 業務アプリケーションに対し電子文書の保存先グループ単位で権限外の書込み、読出し, 削除を防止する。

さらに、TOE は、OS 等の外部機能を利用して以下の機能を実現する。

- 電子文書の不正読出しによる機密情報漏洩防止のため、ファイルサーバ PC に書き込まれる電子文書を暗号化。
- 電子文書に対する不正なアクセス防止のため、業務アプリケーションの識別と認証。
- 電子文書ファイルの書込み、読出し、削除の実行。

2.2.2 利用環境

TOE は、電子文書を保存するファイルサーバ PC にインストールして利用される。

ファイルサーバ PC は、専用のサーバ室に設置される。サーバ室は入退室管理が行われ、TOE 運用管理者および TOE 許可利用者以外の者が、ファイルサーバ PC へ近づくことを制限される。また、ファイルサーバ PC は、外部ネットワークとの接続を持たない内部ネットワーク上に設置されるか、あるいはファイアウォールを介して外部ネットワークとの接続を行う。ファイルサーバ PC と業務アプリケーション間の通信には HTTPS を使用する。

2.2.3 利用方法

本 TOE は、TOE 運用管理者および TOE 許可利用者により、官公庁・自治体、あるいは民間企業内において、電子文書の安全な保存のために利用される。

TOE を利用した文書管理システムの概要を図 2-1 に示す。

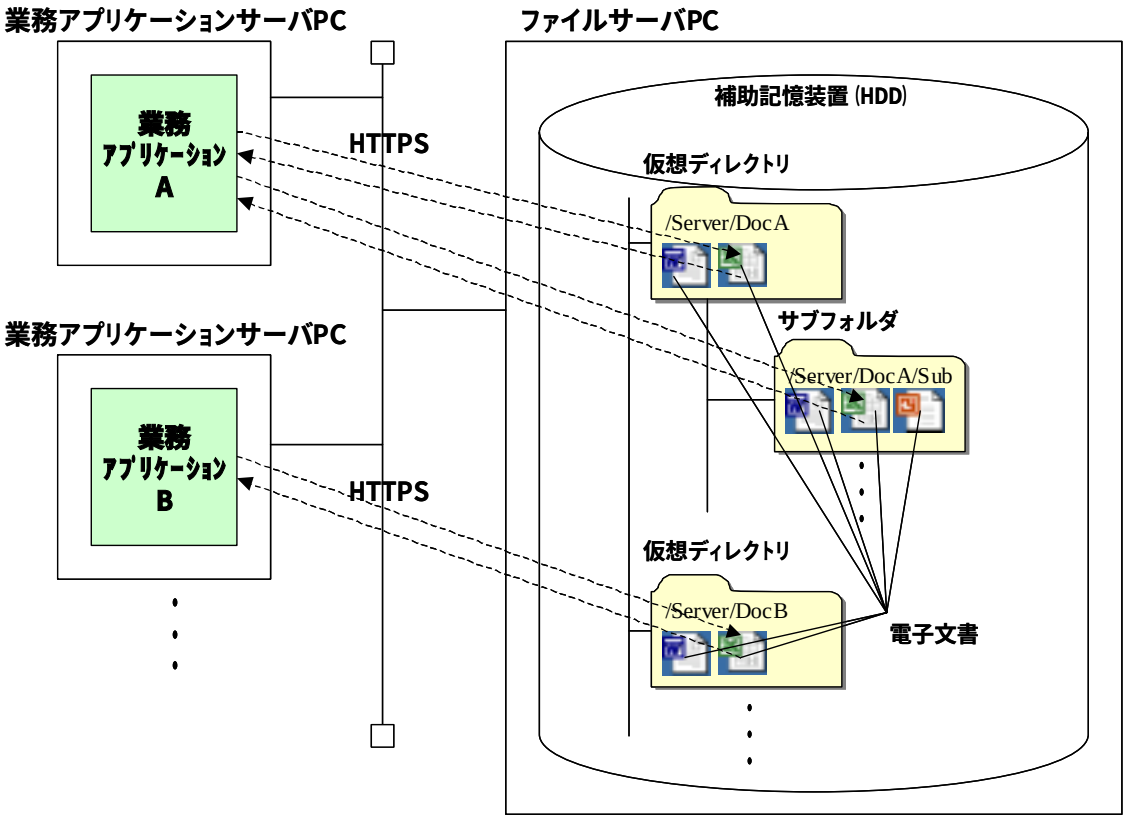

図 2-1　TOE を利用した文書管理システム概要

ファイルサーバ PC は、補助記憶装置（ハードディスクドライブ、以下 HDD）上の仮想ディレクトリまたは配下のサブフォルダに保存された電子文書をセキュアに管理する。

本 ST において使用されている用語について説明する。

業務アプリケーション

TOE に対し、HTTPS 経由でアクセスするアプリケーションソフトウェアのことである。

業務アプリケーションの識別情報は、TOE の起動前に TOE 運用管理者が、TOE に登録する必要がある。業務アプリケーションの利用者は業務アプリケーションを経由して TOE を利用するユーザであり、業務アプリケーションサーバ PC に接続されたクライアント PC を通じ電子文書の処理を行う。

業務アプリケーションサーバ PC

業務アプリケーションが搭載されたサーバ PC である。

ファイルサーバ PC

TOE が搭載されたサーバ PC である。

仮想ディレクトリ

ファイルサーバ PC 上のディレクトリであり、WWW サーバに登録され URL で指定されるディレクトリである。業務アプリケーションは対応する仮想ディレクトリに対して HTTPS 経由でサブフォルダの生成／削除または電子文書の書込み／読出し／削除を行う。

仮想ディレクトリは、業務アプリケーション毎に書込み／読出し／削除の権限を保持し権限は、仮想ディレクトリに属するサブフォルダおよび電子文書へのアクセス時に利用される。

業務アプリケーションに対応する仮想ディレクトリは必要に応じ、複数登録することができる。あるいは複数の業務アプリケーションが共有の仮想ディレクトリを使用することもできる。複数の業務アプリケーションが、共有の仮想ディレクトリを使用する場合、それぞれの権限に従って仮想ディレクトリに属するサブフォルダおよび電子文書へのアクセスをおこなう。

業務アプリケーションに対応する仮想ディレクトリ名と権限は、TOE 運用管理者または TOE 許可利用者が TOE に設定する。

サブフォルダ

仮想ディレクトリの配下に生成されるフォルダのことをいう。業務アプリケーションはサブフォルダを生成することができる。サブフォルダには、仮想ディレクトリの権限が適用される。業務アプリケーションは、仮想ディレクトリの権限に従いサブフォルダの生成／削除およびサブフォルダ内の電子文書の書込み／読出し／削除を行うことができる。

電子文書

仮想ディレクトリや、仮想ディレクトリ配下のサブフォルダに書き込まれ、保存されるファイルのことをいう。ファイルとは、Microsoft Word、Excel などのソフトウェアを使用して作成した、ハードディスクなどの記憶装置に記録されたデータのまとまりのことである。電子文書には、仮想ディレクトリの権限が適用される。

TOE 運用管理者

TOE の設定、管理を行う管理者。当該アカウントは、1 つの TOE に対してただ 1 つのアカウントしか存在せず、起動前に TOE に登録されている。

TOE 運用管理者は以下の機能を実行する。

- TOE 運用管理者のパスワードの登録･変更、およびパスワードの有効期限の設定。
- TOE 許可利用者のユーザ ID、パスワード、およびパスワードの有効期限の設定。

- 仮想ディレクトリの生成･削除、および当該仮想ディレクトリの権限の設定･変更･削除。
- 電子文書の暗号化／復号に利用する共通鍵暗号のアルゴリズムおよび鍵長の変更。
- TOE にアクセスする業務アプリケーションの識別情報の設定・変更・削除。
- TOE 許可利用者の担当業務アプリケーションの設定・変更・削除。

TOE 許可利用者

TOE に設定された特定の業務アプリケーションについて、設定、管理を行うことができる利用者である。一人の TOE 許可利用者は、一つの業務アプリケーションの設定、管理を行うことができる。TOE 運用管理者により、TOE に設定される。

TOE 許可利用者は、以下の機能を実行することができる。

- 業務アプリケーションがアクセスする仮想ディレクトリの生成･削除、および当該仮想ディレクトリの権限の設定・変更・削除。

次に TOE の利用手順について説明する。TOE はファイルサーバ PC の WWW サーバ上で動作する。なお、ファイルサーバ PC と業務アプリケーションとの通信は HTTPS にて行う。HTTPS を使用することにより、一連の処理における業務アプリケーションとファイルサーバ PC 間の接続をセキュアに維持することが可能となる。また、複数の業務アプリケーションサーバにまたがる業務アプリケーションからの同時処理要求に対しても、業務アプリケーションと TOE 間の接続を適切に維持・処理することができる。

TOE を利用するにあたっては、TOE の起動時に以下の設定を行う。なお、TOE を設置・生成・スタートアップと考える操作は（TOE のインストール）と明示的に記述する。

はじめに、TOE 運用管理者は、TOE にアクセスする業務アプリケーションの識別に必要な、公開鍵証明書の識別情報を登録する。（TOE のインストール）

次に TOE 運用管理者または TOE 許可利用者は、業務アプリケーションがアクセスするファイルサーバ PC 上の仮想ディレクトリと、その仮想ディレクトリに対する業務アプリケーションの権限を設定する。但し、TOE 許可利用者が設定可能なのは、TOE 許可利用者が管理する特定の業務アプリケーションにアクセスを許可する仮想ディレクトリと、その権限である。これらの設定は、許可されていない業務アプリケーションによる不正アクセス、および権限外の操作から電子文書を保護するためのものであり、TOE 運用管理者、および TOE 許可利用者が行う。これらの設定は業務アプリケーションから行うことはできない。

さらに、必要に応じて、TOE 運用管理者は、電子文書の暗号化／復号に利用する共通鍵暗号のアルゴリズムおよび鍵長を設定する。（TOE のインストール）

上記設定が行われた後、許可された業務アプリケーションは、設定された権限に従い、対応する仮想ディレクトリ内の電子文書の書込み／読出し／削除を行うことができる。

業務アプリケーションは、対応する仮想ディレクトリの配下にサブフォルダを生成することができる。業務アプリケーションにより電子文書が書き込まれると、電子文書は暗号化されるとともに、電子文書の改ざん検証データを生成する。

業務アプリケーションにより電子文書が読出される際、電子文書は復号され、改ざん検証

データにより電子文書の改ざんの検証が行われる。

　これらの処理により、不正な電子文書の読出しによる機密情報の漏洩防止、および電子文書の改ざんの検知を行うことができる。

2.3 TOE の構成

2.3.1 ネットワーク環境

TOE のネットワーク構成を示す。

業務アプリケーションサーバ PC とファイルサーバ PC 間は、内部ネットワークで接続されるかあるいはファイアウォールを介して外部ネットワークと隔離して接続されている。業務アプリケーションとファイルサーバ PC 間の通信は HTTPS で行われる。

なお、TOE は、ファイルサーバ PC 上で動作するソフトウェア“ ForceSecure-Filing V01 ”であり、ファイルサーバ PC と業務アプリケーションまたはファイアウォールの間の HTTPS 通信は TOE 範囲外である。

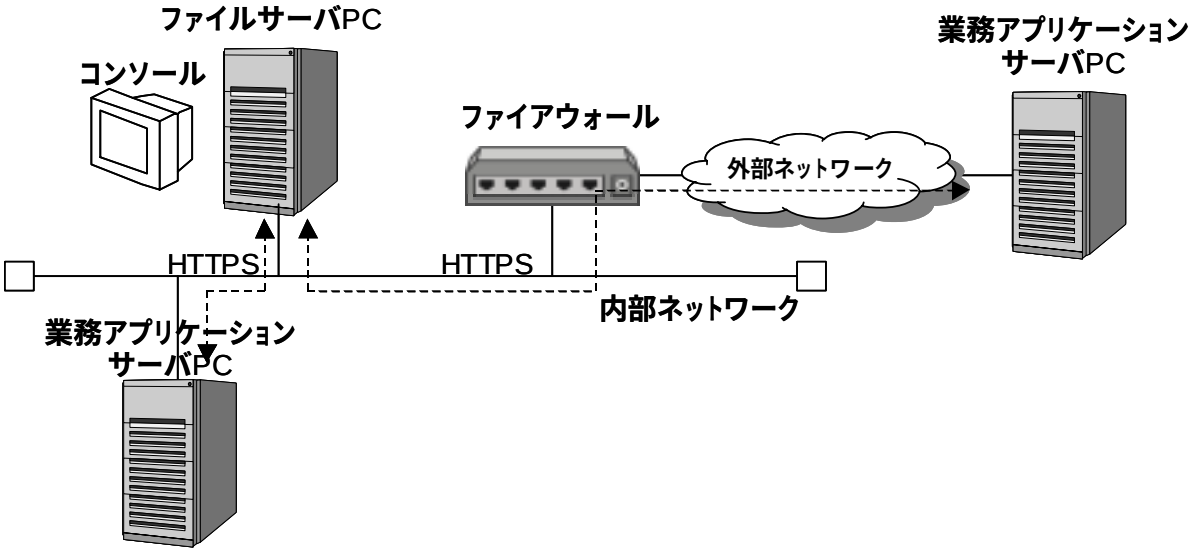

図 2-2　ネットワーク構成

2.3.2 ハードウェアとソフトウェアの構成

TOE を含むハードウェア・ソフトウェアの構成について説明する。

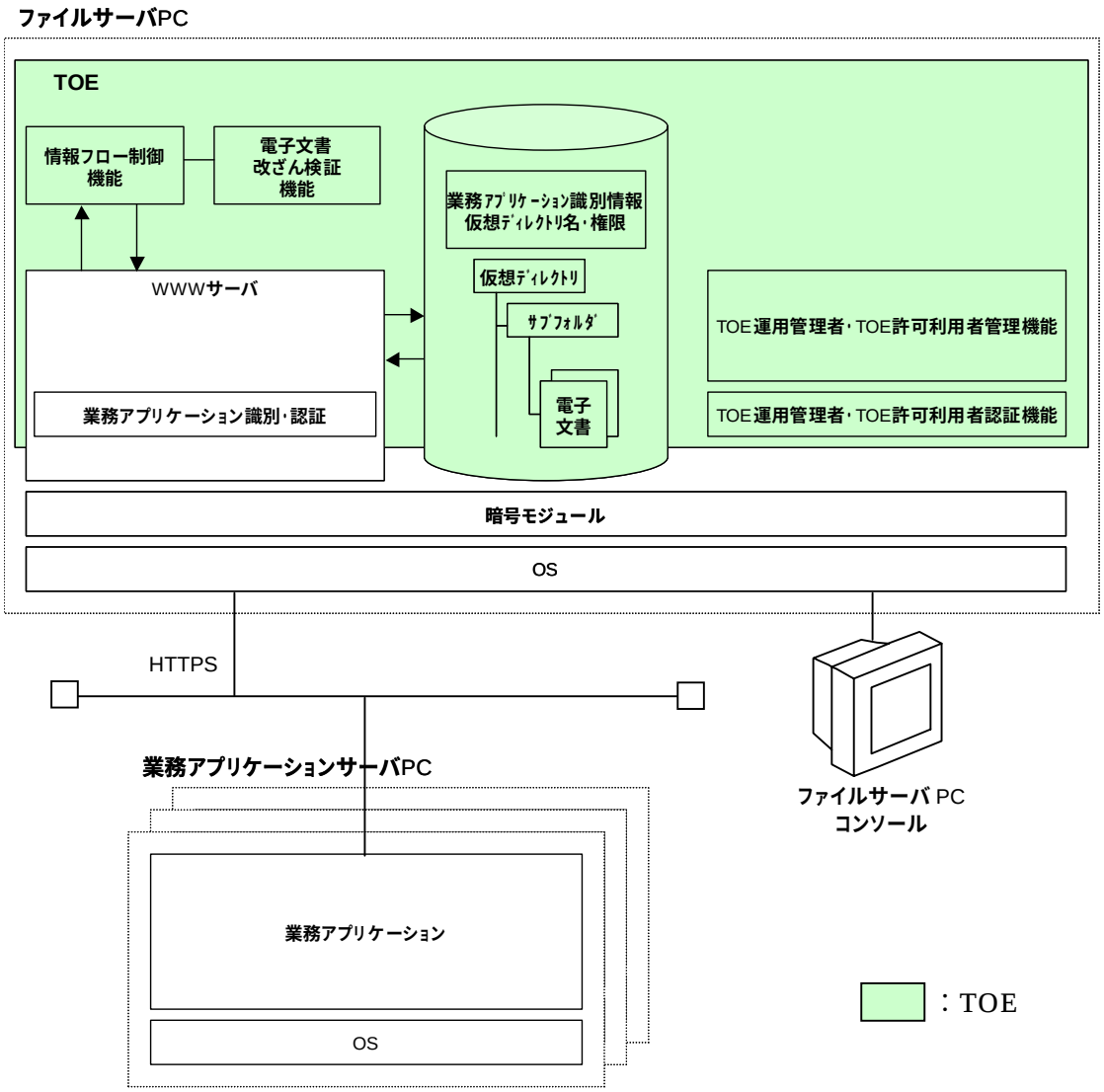

図 2-3　ハードウェア・ソフトウェア構成

2.3.2.1　ハードウェア

TOE はファイルサーバ PC 上にインストールされ、動作する。

ファイルサーバ PC のハードウェア環境を示す。

構成要素	要件
CPU	PentiumⅢ 700MHz 以上推奨

メインメモリ	1GB 以上推奨
ハードディスクドライブ	以下を保存する容量が必要 保存電子文書容量　　：保存文書総バイト数 電子文書属性情報容量　：保存文書数×約 200 バイト ログファイル容量　　：文書アクセス数×約 100 ﾊﾞｲﾄ
CD-ROM	必要（TOE のインストールに使用）
LAN カード	2（内部ネットワーク用と外部ネットワーク用）
キーボード／マウス	必要
ディスプレイ	必要
バックアップ装置	必要
UPS	必要

表 2-1　ハードウェア環境

TOE は、ファイルサーバ PC 上で動作するソフトウェア“ ForceSecure-Filing V01 ”であり、ファイルサーバ PC および業務アプリケーションサーバ PC は、TOE 範囲外である。

2.3.2.2 ソフトウェア

TOE はファイルサーバ PC の OS 上で、OS の持つ暗号モジュールおよび WWW サーバを利用して動作する。暗号モジュールは、ForceSecure-Filing V01 に動的に結合される。

ファイルサーバ PC のソフトウェア構成を示す。

OS	Microsoft Windows 2000 Server Service Pack3 Microsoft Windows 2000 Advanced Server Service Pack3
WWW サーバ	Microsoft Internet Information Service 5.0
暗号モジュール	Microsoft CryptoAPI version1.0
TOE	ForceSecure-Filing V01

表 2-2　ソフトウェア環境

なお、OS（オペレーティングシステム）、暗号モジュールおよび WWW サーバは TOE の範囲外である。

2.4 TOE の機能

TOE の機能を以下に説明する。

2.4.1 TOE 範囲内の機能

情報フロー制御機能

TOE は、WWW サーバで認証された業務アプリケーションから命令（情報）を受け、業務アプリケーションを識別し、命令の中のディレクトリ名とファイル操作命令が対応する仮想ディレクトリに設定された権限を満たす場合、情報を通過させる。満たさない場合は業務アプリケーションにエラーを返し命令を破棄する。

電子文書改ざん検証機能

TOE は、業務アプリケーションから書込み要求された電子文書の改ざん検証データを生成する。また、読出し要求された電子文書の改ざん検証データから、電子文書の改ざんの有無を検証する。

改ざん検証データに含まれる電子署名の生成および検証は TOE 範囲外である電子署名機能にて実行する。

ログ機能

TOE は、業務アプリケーションからの処理履歴、および TOE 運用管理者・TOE 許可利用者による管理機能操作の履歴を記録する。

記録した監査データは、ファイルサーバ PC コンソールより参照することができる。

監査データの参照は、TOE 運用管理者にのみ許可される。また、監査データの変更、削除を行なうことはできない。

TOE 運用管理者・TOE 許可利用者認証機能

TOE は、TOE にアクセスする TOE 運用管理者および TOE 許可利用者の識別・認証を行う。

TOE 運用管理者または TOE 許可利用者が、ファイルサーバ PC のコンソール経由で TOE にアクセスする際、TOE 運用管理者および TOE 許可利用者のユーザ ID とパスワードにより識別・認証を行う。入力された TOE 運用管理者および TOE 許可利用者のユーザ ID、パスワードが TOE に登録されている場合アクセスを許可し、そうでない場合アクセスは拒否される。

TOE 運用管理者・TOE 許可利用者管理機能

TOE 運用管理者の識別・認証に使用する、TOE 運用管理者のパスワードの登録・変更、およびパスワードの有効期限を設定する。

また、TOE 許可利用者の識別・認証に使用する、TOE 許可利用者のユーザ ID、パスワード、およびパスワードの有効期限の設定を行う。

TOE 運用管理者および TOE 許可利用者のパスワード有効期限が過ぎた場合、TOE 運用

管理者および TOE 許可利用者の識別・認証時にパスワードの有効期限が過ぎていることがガイダンス表示され、パスワードの変更が強制される。パスワードの変更を行わない場合、TOE 運用管理者および TOE 許可利用者の識別・認証が必要な機能を実行することはできない。

TOE 運用管理者のパスワードの登録・変更、パスワードの有効期限設定、および TOE 許可利用者のユーザ ID、パスワード、およびパスワードの有効期限設定は、TOE 運用管理者が行う。

2.4.2 TOE **範囲外の機能**

鍵生成機能

鍵生成機能は、電子文書の暗号化／復号用共通鍵（RC4 128bit または Triple DES 168bit）を生成する。

また、電子文書の電子署名の生成／検証をおこなう電子署名用公開鍵ペア（RSA 1024bit または RSA 2048bit）を生成する。

生成する鍵のアルゴリズム、鍵長、ハッシュアルゴリズムは、起動時に登録した値を使用する。

鍵生成は TOE 起動時に行われる。

暗号化機能

TOE からの要求により電子文書を暗号化あるいは復号する。暗号化／復号に使用する共通鍵は、鍵生成機能にて生成される。

電子署名機能

TOE からの要求により、以下の機能を実現する。

電子文書と日付時刻情報（電子文書作成日時）のハッシュ値をとり電子署名用公開鍵ペア秘密鍵で暗号化して電子署名を生成する。

電子署名用公開鍵ペア公開鍵により電子署名を復号し電子文書と日付時刻情報の完全性を検証する。

電子署名生成および復号に使用する公開鍵ペアは、鍵生成機能にて生成される。

SSL 機能

ファイルサーバ PC と業務アプリケーション間で SSL によるクライアント認証を行う。また、TOE と業務アプリケーション間の通信を暗号化する。

ファイル操作機能

TOE を通過した業務アプリケーションからの命令をもとにディレクトリで指定されたサブフォルダを生成／削除，電子文書の書込み／読出し／削除を実行する。

3 TOE セキュリティ環境

本章では、本 TOE に対するセキュリティ環境について記述する。

3.1 前提条件

A.SVR_PLACE

ファイルサーバ PC は専用のサーバ室に設置される。サーバ室は入退室管理が行われ、TOE 運用管理者、TOE 許可利用者および入室を許可された者以外は入退室することはできない。

A.COMM

ファイルサーバ PC は、外部ネットワークとの接続を持たない内部ネットワーク上に設置される。または、ファイルサーバ PC はファイアウォール等により保護されたネットワーク上に設置される。

A.DEDICATED_SVR

ファイルサーバ PC は、OS、WWWサーバ、暗号モジュールおよび TOE 以外のアプリケーションソフトウェアがインストールされない。また、TOE が使用しないサービスは停止される。

A.MANAGER

TOE 運用管理者および TOE 許可使用者は、TOE の運用に関して不正を行わない。

A.PASSWORD_MANAGE

TOE 運用管理者および TOE 許可利用者が TOE にアクセスするために用いるパスワードは、他人に知られないよう本人によって管理される。パスワードは推測・解析されにくいものが設定され、適正な間隔で変更される。

3.2 脅威

3.2.1 資産

TOE が保護対象とする資産は以下のとおりである。

- サブフォルダ、電子文書

3.2.2 脅威

T.REGIST_APL

不正な業務アプリケーションにより、権限のない電子文書を操作（書き換え、読出し、削除）またはサブフォルダを削除する。

1)登録されていない業務アプリケーションによる電子文書の操作またはサブフォルダの削除

2) 登録された業務アプリケーションによる意図しない電子文書に対する操作またはサブフォルダの削除

T.DIRECT_USERDATA_ACCESS

ファイルサーバの OS にコンソールを使用してログインする者が、直接電子文書を書き換え、読出し、削除またはサブフォルダを削除する。

T.DIRECT_TSFDATA_ACCESS

TOE 運用管理者または TOE 許可利用者以外の者が TOE 運用管理者及び TOE 許可利用者になりすまし、仮想ディレクトリの権限を改ざんし、電子文書へのアクセス権が変更されることによって、不正に電子文書を変更、読出し、削除またはサブフォルダを削除する。

3.3 組織のセキュリティ方針

本 ST では、組織のセキュリティ方針はない。

4 セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

4.1 TOE のセキュリティ対策方針

O.ACCESS_PRIVILEGE

TOE は、不正な業務アプリケーションによる権限のない電子文書の書込み、読出し、削除、サブフォルダの削除を防止する制御を行う。

O.AUDIT_ACCESS

TOE は、業務アプリケーションによる電子文書への処理履歴を記録し、設定データへの操作履歴を記録し、不正なアクセスを特定可能とする。

O.DETECT_MODIFY

TOE は、電子文書の改ざん検証データを生成し、改ざん検証データから電子文書の改ざんを検証する。

O.I&A_USER

TOE は、ファイルサーバ PC コンソールから TOE にアクセスする利用者の識別と認証を行い TOE 運用管理者あるいは TOE 許可利用者以外のユーザが業務アプリケーションの仮想ディレクトリの権限を変更し、不正に電子文書へアクセスすることを防止する

4.2 環境のセキュリティ対策方針

OE.SSL

ファイルサーバ PC と業務アプリケーションは、HTTPS プロトコルによって保護されたチャネルが確立され業務アプリケーションの識別と認証をおこない TOE 運用管理者が登録したもの以外は接続を拒否する。

OE.CRYPT

暗号モジュールは、電子文書を秘匿するために電子文書を暗号化する。

OE.SIGNATURE

暗号モジュールは、改ざん検証データに含まれる電子署名を生成および検証する。

OE.BACKUP

TOE 運用管理者は、TOE が管理する電子文書のバックアップを定期的に行う。バックアップには CD-R 等の書き換え不可媒体を使用し、媒体は施錠された保管庫にて管理する。

OE.SVR_PLACE

ファイルサーバ PC は、TOE 運用管理者、TOE 許可利用者および入室を許可された者以外

の人による直接的なアクセスを防止するために、専用のサーバ室に設置されなければならない。

OE.COMM

ファイルサーバ PC は、外部ネットワークとの接続を持たない内部ネットワーク上に設置されなければならない。または、ファイルサーバ PC は、ファイアウォール等により保護されたネットワーク上に設置されなければならない。

OE.DEDICATED_SVR

ファイルサーバ PC には、OS、WWW サーバ、暗号モジュールおよび TOE 以外のアプリケーションソフトウェアはインストールされない。また、TOE が使用しないサービスは停止されなければならない。

OE.MANAGER

TOE 運用管理者および TOE 許可利用者は、信頼できる人をアサインし、不正防止を契約に織りこみ、また監査を実施することで TOE の運用に関して不正をおこなわないようにしなければならない。

OE.PASSWORD_MANAGE

TOE 運用管理者および TOE 許可利用者は、TOE 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。

5 IT セキュリティ要件

本章では、TOE またはその環境が満たしていなければならない詳細な IT セキュリティ要件について記述する。

5.1 TOE セキュリティ要件

本章では、TOE が満たすべき IT セキュリティ要件について記述する。

5.1.1 TOE セキュリティ機能要件

本章では、CC パート 2 から該当する機能コンポーネントを抜き出して、TOE に対する IT セキュリティ機能要件を定義する。

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:

1) 監査機能の起動と終了;
2) 監査の[選択: 指定なし]レベルのすべての監査対象事象; および
3) [割付: 表 5-1 に示す監査対象事象]

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

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

依存性: FPT_STM.1 高信頼タイムスタンプ

下線は TOE で監査対象としているアクションを示す。

監査対象事象	機能要件	監査対象とすべきアクション
・ 業務アプリケーション命令の処理エラー結果 ・ 電子文書の書込み／読出し／削除の成功 ・ サブフォルダの生成／削除の成功 ・ 電子文書の書込み／読出し／削除の失敗 ・ サブフォルダの生成／削除の失敗	FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセッ

監査対象事象	機能要件	監査対象とすべきアクション
		ト。
・ 電子文書の書込みの成功 ・ 改ざん検証データ生成失敗	FDP_DAU.1	a) 最小: 有効性の証拠の生成成功。 b) 基本: 有効性の証拠の生成不成功。 c) 詳細: 証拠を要求したサブジェクトの識別情報。
・ 識別認証された業務アプリケーションと業務アプリケーションプロセスの WWW サーバ異常による結合失敗	FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。
・ 設定情報の設定／変更	FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。

表 5-1　監査対象事象

FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1　TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

依存性:　FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1　TSF は、[割付: TOE 運用管理者]が、[割付: 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)]を監査記録から読出せるようにしなければならない。

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

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出しアクセスを禁止しなければならない。

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]できねばならない。

依存性: FAU_GEN.1 監査データ生成

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層: なし

FAU_STG.3.1 TSF は、監査証跡が[割付: TOE 運用管理者がインストール時に指定した容量]を超えた場合、[割付: TOE の動作停止のアクション]をとらなければならない。

依存性: FAU_STG.1 保護された監査証跡格納

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: 表 5-2 のサブジェクト、情報、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]に対して[割付: ForceSecure-Filing V01 情報フロー制御ポリシー]を実施しなければならない。

依存性: FDP_IFF.1 単純セキュリティ属性

サブジェクト	操作	情報
業務アプリケーション識別と関連付けられた、業務アプリケーションプロセス	通過または業務アプリケーションにエラーを通知し破棄	業務アプリケーションからの命令

表 5-2 ｻﾌﾞｼﾞｪｸﾄ、情報、ｻﾌﾞｼﾞ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

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: ForceSecure-Filing V01 情報フロー制御ポリシー]を実施しなければならない: [割付:

1) セキュリティ属性の最小数：3（最小限 1 つの仮想ディレクトリは設定されているため）
2) サブジェクトのセキュリティ属性：業務アプリケーション識別と関連付けられた仮想ディレクトリの権限
3) 情報のセキュリティ属性：業務アプリケーションからの命令に含まれる電子文書やサブフォルダに対するファイル操作命令]。

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:
1) TOE は業務アプリケーション識別と関連付けられた、仮想ディレクトリの権限をチェックし、「書込み」が存在する場合、ファイル操作命令が、サブフォルダの生成命令または電子文書の書込み命令なら通過させ、「書込み」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄。
2) TOE は業務アプリケーション識別と関連付けられた、仮想ディレクトリの権限をチェックし、「読出し」が存在する場合、ファイル操作命令が、電子文書の読出し命令なら通過させ、「読出し」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄。
3) TOE は業務アプリケーション識別と関連付けられた、仮想ディレクトリの権限をチェックし、「削除」が存在する場合、ファイル操作命令が、サブフォルダの削除命令または電子文書の削除命令なら通過させ、「削除」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄。]。

FDP_IFF.1.3 TSF は、[割付: なし]を実施しなければならない。

FDP_IFF.1.4 TSF は、以下の[割付: なし]を提供しなければならない。

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: 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: 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

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: 表 5-3 のセキュリティ属性]に対し[選択: 表 5-3 のセキュリティ属性に対する操作]をする能力を[割付: 表 5-3 の許可された役割]に制限するために[割付: ForceSecure-Filing V01 情報フロー制御ポリシー]を実施しなければ

ならない。

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

セキュリティ属性	セキュリティ属性に対する操作	許可された役割
業務アプリケーション識別、業務アプリケーションと関連付けられる仮想ディレクトリ名と権限	設定、変更、削除	TOE 運用管理者
該当する業務アプリケーションに関連付けられる仮想ディレクトリ名と権限	設定、変更、削除	TOE 許可利用者

表 5-3　セキュリティ属性、セキュリティ属性に対する操作、許可された役割一覧

FMT_MSA.3 静的属性初期化

下位階層: なし

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択: 許可的]デフォルト値を与える[割付: ForceSecure-Filing V01 情報フロー制御ポリシー]を実施しなければならない。

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

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

FDP_DAU.1 基本データ認証

下位階層: なし

FDP_DAU.1.1 TSF は、[割付: 電子文書]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。

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: 業務アプリケーションプロセス]に提供しなければならない。

依存性: なし

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:業務アプリケーション ID、仮想ディレクトリ名、権限]を維持しなければならない。

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: 以下の品質尺度]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。

依存性:　なし

［ 品質尺度 ］

TOE 運用管理者および TOE 許可利用者のパスワード認証におけるパスワードは、8 個以上の英数字である。

FIA_UAU.2(1) 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 調停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_UID.2(1) 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 調停アクションを許可する前に、各利用者に自分自身を識別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:

1) TOE 運用管理者のパスワード

2) TOE 許可利用者のユーザ ID

3) TOE 許可利用者のパスワード

]を[選択: [割付: 登録]、改変、削除]する能力を[割付: TOE 運用管理者]に制限しなければならない。

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_SAE.1 時限付き許可

下位階層: なし

FMT_SAE.1.1 TSF は、[割付: TOE 運用管理者および TOE 許可利用者のパスワード有効期限]に対する有効期限の時間を特定する能力を、[割付: TOE 運用管理者]に制限しなければならない。

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

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

FMT_SMF.1 管理機能の特定

下位階層: 他のコンポーネントはない

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 データ（TOE 運用管理者パスワード、TOE 許可利用者のユーザ ID・パスワード）の管理機能]。

依存性: 依存性なし

機能要件	管理要件	管理有無	管理項目	管理機能要件
FAU_GEN.1	管理項目要請なし	しない	なし	なし
FAU_GEN.2	管理項目要請なし	しない	なし	なし
FDP_IFC.1	管理項目要請なし	しない	なし	なし
FDP_IFF.1	明示的なアクセスに基づく決定に使われる属性の管理	しない	なし	なし
FDP_DAU.1	データ認証が適用され得るオブジェクトに対する割付や改変が、システムにおいて設定可能である。	しない	なし	なし
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義すること	しない	なし	なし

機能要件	管理要件	管理有無	管理項目	管理機能要件
	ができる。			
FIA_SOS.1	秘密の検証に使用される尺度の管理。	しない	なし	なし
FIA_UAU.2(1)	管理者による認証データの管理; 関係する利用者による認証データの管理; 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。	する	TOE 運用管理者パスワード、TOE 許可利用者パスワード	FMT_MTD.1 FMT_SMF.1
FIA_UID.2(1)	利用者識別情報の管理。	する	TOE 許可利用者のユーザ ID	FMT_MTD.1 FMT_SMF.1
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	しない	なし	なし
FMT_MSA.1	初期値を制御する役割を特定する。	する	役割	なし
FMT_MSA.3	初期値を特定できる役割を管理する。 初期値の許可的あるいは制限的設定を管理する。	する	初期値	なし
FMT_MTD.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。	しない	なし	なし
FMT_SAE.1	有効期限がサポートされるはずのセキュリティ属性のリストを管理すること; 有効期限の時間が過ぎたときにとられるアクション。	しない	なし	なし
FMT_SMF.1	管理項目要請なし	しない	なし	なし
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	しない	なし	なし
FPT_RVM.1	管理項目要請なし	しない	なし	なし
FPT_SEP.1	管理項目要請なし	しない	なし	なし

機能要件	管理要件	管理有無	管理項目	管理機能要件
FPT_STM.1	時間の管理。	しない	なし	なし

表 5-4　TOE の管理項目

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:
1) TOE 運用管理者
2) TOE 許可利用者
]を維持しなければならない。

FMT_SMR.1.2　TSF は、利用者を役割に関連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

FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1　TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2　TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性:　なし

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。

依存性:　なし

5.1.2 TOE セキュリティ保証要件

本章では TOE のセキュリティ保証要件を定義する。

この TOE の保証要件は EAL3 である。これらの要件は JIS X 5070:2000 第 3 部から選択されている。

表 5-5 に選択された保証コンポーネントを示す。なお、ASE クラスは JIS X 5070:2000 によるセキュリティ評価にあたっては常に必要な保証クラスである。

保証クラス	保証コンポーネント	
ACM クラス： 構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
ADO クラス： 配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、および立上げ手順
ADV クラス： 開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
AGD クラス： 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
ALC クラス： ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
ATE クラス： テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト：上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト－サンプル
AVA クラス： 脆弱性評定	AVA_MSU.1	ガイダンスの検査
	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

表 5-5　選択された保証コンポーネント

5.1.3 最小機能強度（SOF）宣言

本 TOE における最小機能強度は SOF－基本である。但し、暗号アルゴリズムは本機能強度の対象としない。

5.2 IT 環境に対するセキュリティ要件

本章では、TOE の IT 環境セキュリティ要件について記述する、

5.2.1 IT 環境のセキュリティ機能要件

本章では、IT 環境が提供する IT セキュリティ機能要件を定義する。

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1　暗号モジュールは、以下の[割付: 表 5-6　暗号鍵リストにおける標準]に合致する、指定された暗号鍵生成アルゴリズム[割付:表 5-6 暗号鍵リストにおけるアルゴリズム]と指定された暗号鍵長[割付:表 5-6　暗号鍵リストにおける鍵長]にしたがって、暗号鍵を生成しなければならない。

依存性:　[FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

	種類	標準	ｱﾙｺﾞﾘｽﾞﾑ	鍵長
1	電子文書暗号化／復号用共通鍵	なし	RC4	128bit
		FIPS PUB 46-3	Triple DES	168bit
2	電子署名用公開鍵ペア	PKCS#1	RSA	1024/2048bit

表 5-6　暗号鍵リスト

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1　暗号モジュールは、[割付:表 5-7　暗号操作リストにおける標準]に合致する、特定された暗号アルゴリズム[割付:表 5-7　暗号操作リストにおけるアルゴリズム]と暗号鍵長[割付:表 5-7　暗号操作リストにおける鍵長]にしたがって、[割付:表 5-7　暗号操作リストにおける操作]を実行しなければならない。

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

	種類	標準	ｱﾙｺﾞﾘｽﾞﾑ	鍵長	操作
1	電子文書暗号化／復号用共通鍵	なし	RC4	128bit	電子文書の暗号化
		FIPS PUB 46-3	Triple DES	168bit	電子文書の復号
2	電子署名用公開鍵ペア	PKCS#1	RSA	1024/ 2048bit	電子署名生成
3	電子文書のハッシュ計算	FIPS180-1	SHA-1	――	電子文書のハッシュ値の生成

表 5-7　暗号操作リスト

FIA_UID.2(2) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1　WWW サーバは、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性:　なし

FIA_UAU.2(2) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1　WWW サーバは、その利用者を代行する他の TSF 調停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

5.2.2 IT 環境のセキュリティ保証要件

本 ST では、IT 環境のセキュリティ保証要件は定義しない。

6 TOE 要約仕様

本章では、TOE の要約仕様を記述する。

6.1 IT セキュリティ機能

本章では、TOE の IT セキュリティ機能を説明する。以下の IT セキュリティ機能は、5.1.1 章で記述した TOE セキュリティ機能要件を満たすものである。

6.1.1 IT セキュリティ機能

SF.IFC

業務アプリケーションとファイルサーバ PC 間の HTTPS プロトコルによる保護されたチャネルが確立され、識別および認証された業務アプリケーションのみを受け入れる。

（この機能は TOE の範囲外である）

識別された業務アプリケーションは、TOE で維持された業務アプリケーション識別をもとに業務アプリケーションプロセスに関連付けられる。

業務アプリケーションから受けた命令から、仮想ディレクトリを読み該当する仮想ディレクトリの権限をチェックする。

1) 「書込み」が存在する場合、ファイル操作命令が、サブフォルダの生成命令または電子文書の書込み命令なら通過させ、「書込み」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄。
   なお電子文書の書込み命令に対し、TOE は電子文書の改ざん検証データを生成するがその実施は SF.DETECT_MODIFY のセキュリティ機能で識別される。
2) 「読出し」が存在する場合、ファイル操作命令が、電子文書の読出し命令なら通過させ、「読出し」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄。
3) 「削除」が存在する場合、ファイル操作命令が、サブフォルダの削除命令または電子文書の削除命令なら通過させ、「削除」が存在しない場合、業務アプリケーションにエラー通知し情報を破棄する

SF.IFC を通過した業務アプリケーションからの命令に従ってサブフォルダの生成／削除、電子文書の書込み／読出し／削除が実行されるがこれは TOE 範囲外の WWW サーバにて実施される。

TOE 運用管理者は、業務アプリケーション識別、仮想ディレクトリ名と権限（書込み・読出し・削除）を設定、変更、削除する。TOE 許可利用者は、TOE 許可利用者が管理する特定の業務アプリケーションに関する仮想ディレクトリ名と、その権限を設定、変更、削除する。運用状態への反映は TOE の起動時におこなわれる。

SF.DETECT_MODIFY

TOE は、電子文書の改ざんの検証を行うため、電子文書の書込み時、当該電子文書の改ざん検証データを生成する。改ざん検証データは電子文書および電子文書書込み日時およ

び電子署名からなる。なお、改ざん検証データに含まれる電子署名の生成は、TSF の範囲外である電子署名機能によって実現されている。

TOE は、電子文書の読出し時、当該電子文書の改ざん検証データの検証を行う。改ざん検証は、改ざん検証データである電子文書および電子文書書込み日時を読出し、電子署名を検証することにより行う。なお、電子署名の検証は、TOE の範囲外である電子署名機能によって実現されている。

SF.LOG

TOE は、TOE がセキュアに運用されていることを監査するために必要な情報の採取、および管理を行うために、監査の対象となる事象が発生した場合に、当該事象を監査データとして採取する。

監査データは以下の項目で構成される。

ここに取得する監査事象を列挙する。ただし監査事象は対策方針(O.AUDIT_ACCESS)を満たすために必要な監査事象のみを記述する。

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

サブジェクト識別情報は、TOE 運用管理者または TOE 許可利用者のユーザ ID、および業務アプリケーション識別情報である。

監査データは、以下の監査対象事象の発生時に採取する。

- 業務アプリケーション命令の処理エラー結果
- 電子文書の書込み／読出し／削除の成功
- 電子文書の書込み／読出し／削除の失敗
- サブフォルダの生成／削除の成功
- サブフォルダの書込み／削除の失敗
- 改ざん検証データ生成失敗
- 識別認証された業務アプリケーションと業務アプリケーションプロセスの WWW サーバ異常による結合失敗
- 設定情報の設定／変更

ログ機能は TOE の起動と同時に開始され、監査機能の開始は“ ForceSecure-Filing 初期化完了 ”として記録される。ログ機能は TOE の停止時に停止され、監査機能の停止は“ ForceSecure-Filing 正常終了 ”として記録される。

監査データは、ファイルサーバ PC コンソールより参照することができる。

監査データの参照は、TOE 運用管理者にのみ許可される。また、監査データの変更、削除を行なうことはできない。

TOE 運用管理者が TOE のインストール時に指定した監査データ格納用の領域サイズを監査証跡が越えた場合は、TOE の運用を停止する。

運用の再開は、TOE 運用管理者が監査証跡をバックアップ後、再立上げをすることが必要である。

SF.I&A_USER

TOE は、TOE にアクセスする TOE 運用管理者および TOE 許可利用者を識別し、識別した TOE 運用管理者、TOE 許可利用者が TOE に登録されている TOE 運用管理者および TOE 許可利用者であることを確認する。

識別認証方式は、以下の認証メカニズムと認証を提供する規則を用いる。

- 認証メカニズム
  パスワード認証
- 認証を提供する規則
  ファイルサーバ PC において、TOE 運用管理者および TOE 許可利用者を識別認証する場合、ファイルサーバ PC のコンソールより入力されたパスワードと、TOE が管理するパスワードが一致することを確認する。

TOE 運用管理者および TOE 許可利用者の認証にあたっては、TOE は TOE 運用管理者および TOE 許可利用者に識別認証前のいかなる操作も許可しない。

パスワード認証方式において、TOE は以下のように TOE 運用管理者および TOE 許可利用者を一意に識別・認証する。

1) ファイルサーバ PC のコンソールで、TOE 運用管理者または TOE 許可利用者のユーザ ID とパスワードの入力を要求する。
2) ユーザ ID とパスワードを入力すると、TOE は、入力された TOE 運用管理者・TOE 許可利用者のユーザ ID が存在するかどうか確認する。
3) 該当するユーザ ID が存在した場合、ユーザ ID に対応するパスワードと入力されたパスワードが一致するかどうか確認する。

TOE は、管理機能の動作が許可される前に、SF.I&A_USER を呼び出す。

SF.USER_MANAGE

SF.I&A_USER で識別・認証後ユーザの役割（TOE 管理者または TOE 許可利用者）を決定する。

(1) TOE 運用管理者のパスワード登録・変更、およびパスワードの有効期限の設定

TOE は、TOE 運用管理者のパスワード登録・変更、およびパスワードの有効期限

の設定を行う機能を提供する。
TOE 運用管理者のパスワード登録・変更、およびパスワードの有効期限の設定は、TOE 運用管理者しか行うことができない。

TOE は、登録・変更する TOE 運用管理者のパスワードの条件を検証する。以下の条件を満たすものが設定可能である。
・ 8 個以上の英数字

TOE 運用管理者のパスワード登録・変更時、指定したパスワードが上記を満たさない場合には、パスワードの再入力を要求し、TOE 運用管理者のパスワード登録・変更を行うことはできない。
また、TOE は、TOE 運用管理者のパスワードの有効期限を検証する。パスワードの有効期限を過ぎた場合、TOE はパスワードの変更を強制する。

(2) TOE 許可利用者のユーザ ID・パスワード、およびパスワードの有効期限の設定
TOE は、TOE 許可利用者のユーザ ID・パスワード、およびパスワードの有効期限の設定を行う機能を提供する。
TOE 許可利用者のユーザ ID・パスワード、およびパスワードの有効期限の設定は、TOE 運用管理者しか行うことができない。

TOE は、登録・変更する TOE 許可利用者のパスワードの条件を検証する。以下の条件を満たすものが設定可能である。
・ 8 個以上の英数字

TOE 許可利用者のパスワード登録・変更時、指定したパスワードが上記を満たさない場合には、パスワードの再入力を要求し、TOE 許可利用者のユーザ ID・パスワード登録・変更を行うことはできない。
また、TOE は、TOE 許可利用者のパスワードの有効期限を検証する。パスワードの有効期限を過ぎた場合、TOE はパスワードの変更を強制する。

6.1.2 IT セキュリティ機能と機能要件の対応関係

表 6-1 にIT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示す。表中の「X」は、対応関係にあることを示している。

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.3	FDP_IFC.1	FDP_IFF.1	FDP_DAU.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2(1)	FIA_UID.2(1)	FIA_USB.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SAE.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1
SF.IFC							X	X		X				X	X	X					X	X	
SF.DETECT_MODIFY									X														X
SF.LOG	X	X	X	X	X	X																	X
SF.I&A_USER												X	X								X		
SF.USER_MANAGE											X						X	X	X	X			

表 6-1　IT セキュリティ機能と機能要件の対応関係

6.1.3 IT セキュリティ機能とセキュリティメカニズムの対応関係

本 ST では以下のセキュリティメカニズムが参照されている。

- パスワード認証メカニズム

これらのセキュリティメカニズムは、SF.I&A_USER の実装で使用されている。

6.1.4 機能強度主張

SF.I&A_USER だけが確率的あるいは順列的メカニズムに基づくセキュリティ機能である。SF.I&A_USER はセキュリティ機能強度として SOF-基本を持つ。

6.2 保証手段

本章では、TOE のセキュリティ保証手段を説明する。以下のセキュリティ保証手段は、5.1.2 章で記述した TOE セキュリティ保証要件を満たすものである。

6.2.1 保証手段に関わる文書

保証手段として次の文書が提供される。

- ForceSecure-Filing V01 セキュリティターゲット V01R20 2005 年 1 月 7 日
- ForceSecure-Filing V01 ﾕｰｻﾞｲﾝﾀｰﾌｪｰｽ仕様書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 システム構造設計書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 表現対応分析書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 開発環境ｾｷｭﾘﾃｨ仕様書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 ソフトウェア説明書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 運用手引書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 システムプログラマ手引書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 テストカバレージ分析書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 テスト深さ分析書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 テスト仕様書・成績書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 ｾｷｭﾘﾃｨ機能強度分析書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 脆弱性分析書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 構成管理仕様書 V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 構成管理システム V01R20 2003 年 6 月 28 日
- ForceSecure-Filing V01 配布手順書 V01R20 2003 年 6 月 28 日

6.2.2 保証手段と保証要件の対応関係

表 6-2 に、保証手段と保証要件の対応関係を示す。

保証クラス	保証要件 ｺﾝﾎﾟｰﾈﾝﾄ	保証手段
ASE クラス： セキュリティターゲット 評価	ASE_INT.1 ASE_DES.1 ASE_ENV.1 ASE_OBJ.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1 ASE_PPC.1	ForceSecure-Filing V01 ｾｷｭﾘﾃｨﾀｰｹﾞｯﾄ V01R20 2005 年 1 月 7 日
ACM クラス： 構成管理	ACM_CAP.3 ACM_SCP.1	ForceSecure-Filing V01 構成管理仕様書 V01R20 2003 年 6 月 28 日 ForceSecure-Filing V01 構成管理ｼｽﾃﾑ V01R20 2003 年 6 月 28 日
ADO クラス： 配付と運用	ADO_DEL.1	ForceSecure-Filing V01 配布手順書 V01R20 2003 年 6 月 28 日
	ADO_IGS.1	ForceSecure-Filing V01 ｿﾌﾄｳｪｱ説明書 V01R20 2003 年 6 月 28 日 ForceSecure-Filing V01 運用手引書 V01R20 2003 年 6 月 28 日
ADV クラス： 開発	ADV_FSP.1	ForceSecure-Filing V01 ﾕｰｻﾞｲﾝﾀｰﾌｪｰｽ仕様書 V01R20 2003 年 6 月 28 日
	ADV_HLD.2	ForceSecure-Filing V01 ｼｽﾃﾑ構造設計書 V01R20 2003 年 6 月 28 日
	ADV_RCR.1	ForceSecure-Filing V01 表現対応分析書 V01R20 2003 年 6 月 28 日
AGD クラス： ガイダンス文書	AGD_ADM.1 AGD_USR.1	ForceSecure-Filing V01 ｿﾌﾄｳｪｱ説明書 V01R20 2003 年 6 月 28 日 ForceSecure-Filing V01 運用手引書 V01R20 2003 年 6 月 28 日 ForceSecure-Filing V01 ｼｽﾃﾑﾌﾟﾛｸﾞﾗﾏ手引書 V01R20 2003 年 6 月 28 日
ALC クラス： ライフサイクル サポート	ALC_DVS.1	ForceSecure-Filing V01 開発環境ｾｷｭﾘﾃｨ仕様書 V01R20 2003 年 6 月 28 日
ATE クラス： テスト	ATE_COV.2	ForceSecure-Filing V01 ﾃｽﾄｶﾊﾞﾚｰｼﾞ分析書 V01R20 2003 年 6 月 28 日
	ATE_DPT.1	ForceSecure-Filing V01 テスト深さ分析書 V01R20 2003 年 6 月 28 日
	ATE_FUN.1	ForceSecure-Filing V01 テスト仕様書・成績書 V01R20 2003 年 6 月 28 日
	ATE_IND.2	TOE（ForceSecure-Filing V01）
AVA クラス： 脆弱性評定	AVA_MSU.1	ForceSecure-Filing V01 ｿﾌﾄｳｪｱ説明書 V01R20 2003 年 6 月 28 日 ForceSecure-Filing V01 運用手引書 V01R20 2003 年 6 月 28 日
	AVA_SOF.1	ForceSecure-Filing V01 ｾｷｭﾘﾃｨ機能強度分析書 V01R20 2003 年 6 月 28 日
	AVA_VLA.1	ForceSecure-Filing V01 脆弱性分析書 V01R20 2003 年 6 月 28 日

表 6-2　保証手段と保証要件の対応関係

7 PP 主張

本章では、PP 主張の記述を行う。

7.1 PP 参照

参照した PP はない。

8 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠、PP 主張根拠について記述する。

8.1 セキュリティ対策方針根拠

セキュリティ対策は、TOE セキュリティ環境で規定した脅威に対抗するためのものである。あるいは、TOE の前提条件と組織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および前提条件の対応関係を表 8-1 に示す。表中の「X」は対応関係にあることを示している。

	T.REGIST_APL	T.DIRECT_USERDATA_ACCESS	T.DIRECT_TSFDATA_ACCESS	A.SVR_PLACE	A.COMM	A.DEDICATED_SVR	A.MANAGER	A.PASSWORD_MANAGE
O.ACCESS_PRIVILEGE	X							
O.AUDIT_ACCESS	X		X					
O.DETECT_MODIFY		X						
O.I&A_USER			X					
OE.SSL	X							
OE.CRYPT		X						
OE.SIGNATURE		X						
OE.BACKUP		X						
OE.SVR_PLACE				X				
OE.COMM					X			
OE.DEDICATED_SVR						X		
OE.MANAGER							X	
OE.PASSWORD_MANAGE								X

表 8-1　セキュリティ対策方針と対抗する脅威・対応する前提条件

表 8-1 により、各セキュリティ対策方針は 1 つ以上の TOE セキュリティ環境に対応していることが分かる。

次に、各 TOE セキュリティ環境に対して、セキュリティ対策方針が当該 TOE セキュリティ環境を満たしていることを示す。

T.REGIST_APL

T.REGIST_APL は、O.ACCESS_PRIVILEGE、O.AUDIT_ACCESS、OE_SSL によって対抗される。

OE.SSL によって登録されていない業務アプリケーションを識別し操作要求を排除する。

O.ACCESS_PRIVILEGE により、TOE は業務アプリケーションからの権限のない電子文書へのファイル操作またはサブフォルダの削除を防止する。

O.AUDIT_ACCESS により、業務アプリケーションからの TOE に対する処理履歴を記録し、権限のない命令を特定することを可能にし、不正な処理を抑止することができる。

T.DIRECT_USERDATA_ACCESS

T.DIRECT_USERDATA_ACCESS は、O.DETECT_MODIFY、OE.CRYPT、OE.SIGNATURE、OE.BACKUP によって対抗される。

OE.CRYPT

電子文書を暗号化することで、電子文書の読出を無効にする。

O.DETECT_MODIFY および OE.SIGNATURE により、電子文書の不正改ざんを検出し改ざんされた電子文書の使用を抑止する。

OE.BACKUP により、電子文書の不正改ざんや不正削除から電子文書の復元を可能にする。

T.DIRECT_TSFDATA_ACCESS

T.DIRECT_TSFDATA_ACCESS は、O.I&A_USER、O.AUDIT_ACCESS によって対抗される。

O.I&A_USER により、ファイルサーバ PC コンソールから TOE にアクセスする利用者の識別と認証を行い TOE 運用管理者あるいは TOE 許可利用者以外のユーザが業務アプリケーションの仮想ディレクトリの権限を変更し、不正に電子文書へアクセスすることを防止する。また O.AUDIT_ACCESS により仮想ディレクトリの権限の改ざんを追跡可能とする。

A.SVR_PLACE

A.SVR_PLACE は、OE.SVR_PLACE によって対抗されている。

OE.SVR_PLACE により、ファイルサーバ PC は専用のサーバ室に設置され、サーバ室への入退室は、TOE 運用管理者、TOE 許可利用者および入室を許可された者に限られるからである。

A.COMM

A.COMM は、OE.COMM によって対抗されている。

OE.COMM により、TOE は外部ネットワークに直接接続されることはなく、外部ネットワークとの接続をもたない内部ネットワーク上に設置されるか、またはファイアウォール等により保護されたネットワーク上に設置される。

A.DEDICATED_SVR

A.DEDICATED_SVR は、OE.DEDICATED_SVR によって対抗されている。

OE.DEDICATED_SVR により、TOE が動作するファイルサーバ PC には、OS、WWW サーバ、暗号モジュールおよび TOE のみインストールされ、利用するサービスだけが実行されるからである。

A.MANAGER

A.MANAGER は、OE.MANAGER によって対抗されている。

OE.MANAGER により、TOE 運用管理者および TOE 許可利用者には信頼できる人をアサインし不正防止を契約により抑制し監査を実施することにより TOE の運用に関する不正を防止するからである。

A.PASSWORD_MANAGE

A.PASSWORD_MANAGE は、OE.PASSWORD_MANAGE によって対抗されている。

OE.PASSWORD_MANAGE により、TOE 運用管理者および TOE 許可利用者は、TOE にアクセスするための認証情報（パスワード）を他人に漏らさないよう管理し、推測・解析されやすい認証情報（パスワード）を設定せず、また、認証情報（パスワード）は適正な間隔で変更されるからである。

8.2 セキュリティ要件根拠

本章では、セキュリティ要件（TOE および環境）がセキュリティ対策方針を満たすのに適し、かつセキュリティ対策方針にまでたどれることを実証する。

8.2.1 TOE の機能要件による TOE の対策方針の充足

表 8-2 は、TOE の IT セキュリティ機能要件と TOE のセキュリティ対策方針との対応関係を示した表である。表中の「X」は、対応関係にあることを示している。

	O.ACCESS_PRIVILEGE	O.AUDIT_ACCESS	O.DETECT_MODIFY	O.I&A_USER
FAU_GEN.1		X		
FAU_GEN.2		X		
FAU_SAR.1		X		
FAU_SAR.2		X		
FAU_STG.1		X		
FAU_STG.3		X		
FDP_IFC.1	X			
FDP_IFF.1	X			
FDP_DAU.1			X	
FIA_ATD.1	X			
FIA_SOS.1				X
FIA_UAU.2(1)				X
FIA_UID.2(1)				X
FIA_USB.1	X			
FMT_MSA.1	X			
FMT_MSA.3	X			
FMT_MTD.1				X
FMT_SAE.1				X
FMT_SMF.1				X
FMT_SMR.1				X
FPT_RVM.1	X			X
FPT_SEP.1	X			X
FPT_STM.1		X	X	

表 8-2　TOE の IT セキュリティ機能要件と TOE のセキュリティ対策方針との対応関係

表 8-2 により、各 IT セキュリティ機能要件は 1 つ以上の TOE セキュリティ対策方針に対応していることが分かる。

次に、各 TOE セキュリティ対策方針に対して、IT セキュリティ機能要件が当該 TOE セキュリティ対策方針を満たしていることを示す。

O.ACCESS_PRIVILEGE

O.ACCESS_PRIVILEGE は、FDP_IFC.1、FDP_IFF.1、FIA_ATD.1、FMT_MSA.1、FMT_MSA.3、FIA_USB.1、FPT_RVM.1、FPT_SEP.1 によって実現される。

FDP_IFC.1、FDP_IFF.1、FMT_MSA.1、FMT_MSA.3 により、「ForceSecure-Filing V01 情報フロー制御ポリシー」に従い、TOE 運用管理者または TOE 許可利用者が設定したセキュリティ属性に基づき業務アプリケーションからの命令（情報）が制御される。

FIA_USB.1 により識別認証された業務アプリケーションと業務アプリケーションプロセスが関連付けされる。

FIA_ATD.1 により業務アプリケーションとプロセスに関するセキュリティ属性を維持する。

FPT_RVM.1 により、業務アプリケーションによって電子文書にアクセスする前に情報フロー制御機能が呼び出される。

FPT_SEP.1 により、TSF を信頼できない利用者による干渉と改ざんから保護するため、セキュリティドメインを分離する。

O.AUDIT_ACCESS

O.AUDIT_ACCESS は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.3、FPT_STM.1 によって実現される。

FAU_GEN.1 により、監査対象事象の監査記録を生成する。

FAU_GEN.2 により、各監査対象事象を、その原因となった識別情報に関連付ける。

FAU_SAR.1 は監査記録を読出せるようにする。

FAU_SAR.2 は、明示的に読出しアクセスを許可した利用者を除き、すべての利用者に監査記録の読出しアクセスを禁止しなければならない。

FAU_STG.1 は、保管された監査記録が不正に削除されないように保護し、また監査記録の改変を防止する。

FAU_STG.3 は、監査証跡が事前に定義された限界値を超えた場合、TOE 停止のアクションをとるようにする。

FPT_STM.1 により、監査記録に必要な、高信頼タイムスタンプを提供する。

O.DETECT_MODIFY

O.DETECT_MODIFY は、FDP_DAU.1、FPT_STM.1 によって実現される。

FDP_DAU.1 により、電子文書の有効性を検知するための証拠データ（改ざん検証データ）を生成する能力を提供する。

FPT_STM.1 により、改ざん検証データに必要な高信頼タイムスタンプを提供する。

O.I&A_USER

O.I&A_USER は、FIA_SOS.1、FIA_UAU.2(1)、FIA_UID.2(1)、FMT_MTD.1、FMT_SAE.1、FMT_SMF. 1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 によって実現される。

FIA_SOS.1 により、秘密（TOE 運用管理者および TOE 許可利用者のパスワード）を設定する際、秘密が品質尺度にあっていることを TSF が検証することを要求する。

FIA_UAU.2(1)により、セキュリティ管理機能の実行を許可する前に、TOE 運用管理者および TOE 許可利用者に自分自身の認証が成功することを要求する。

FIA_UID.2(1)により、TOE 運用管理者および TOE 許可利用者の利用者識別において、TSF が何らかのアクションを許す前に、各利用者に識別に成功することを要求する。

FMT_MTD.1、FMT_SMF.1、FMT_SMR.1 により、正当な役割を有する利用者が、セキュリティ管理機能である TOE 運用管理者・TOE 許可利用者管理機能を用いて、TOE 運用管理者・TOE 許可利用者の識別に用いる TSF データ（TOE 運用管理者のパスワード、TOE 許可利用者のユーザ ID・パスワード）を管理することを許可する。

FMT_SAE.1 により TOE 運用管理者または、TOE 許可利用者のパスワード有効期限が切れた場合パスワードの更新を強制される。

FPT_RVM.1 により、TOE の機能を動作させる前に、TOE 運用管理者・TOE 許可利用者認証機能が呼び出され、成功することを保証する。

FPT_SEP.1 により､TSF を信頼できない利用者による干渉と改ざんから保護するため、セキュリティドメインを分離する。

8.2.2 IT 環境の機能要件による TOE の対策方針の充足

表 8-3 は、IT 環境のセキュリティ機能要件と TOE のセキュリティ対策方針との対応関係を示した表である。表中の「X」は、対応関係にあることを示している。

	OE.CRYPT	OE.SIGNATURE	OE.SSL
FCS_CKM.1	X	X	
FCS_COP.1	X	X	
FIA_UID.2(2)			X
FIA_UAU.2(2)			X

表 8-3　IT 環境のセキュリティ機能要件と TOE のセキュリティ対策方針との対応関係

表 8-3 より、各 IT 環境セキュリティ機能要件が１つ以上の IT 環境セキュリティ対策方針に対応している。

OE.CRYPT

OE.CRYPT は、FCS_CKM.1、FCS_COP.1 によって実現される。

FCS_CKM.1 により、電子文書暗号化／復号用共通鍵を生成する。

FCS_COP.1 により、生成した電子文書暗号化／復号用共通鍵を使用して電子文書の暗号化を行う。

OE.SIGNATURE

OE.SIGNATURE は、FCS_CKM.1、FCS_COP.1 によって実現される。

FCS_CKM.1 により、電子署名用公開鍵ペアを生成する。

FCS_COP.1 により、生成した電子署名用公開鍵ペアを使用して電子文書の改ざん検証データに含まれる電子署名を生成/検証する。

OE.SSL

OE.SSL は FIA_UID.2(2)、FA_UAU.2(2)によって実現される。

FIA_UID.2(2)により業務アプリケーションが識別される。

FIA_UAU.2(2)により業務アプリケーションが認証される。

8.2.3 最小機能強度レベルの適合性

TOE は､A.COMM に挙げているように閉じた保護されたネットワークを前提としており、TOE が高度な経験・設備・意思（high attack potential）を持つ攻撃者からの攻撃に対して備えることは想定していない。また TOE が利用されている、閉じた通信環境としては政府・地方公共団体、医療機関、民間企業等が考えられるが、これらの内部からの攻撃は、動機や高度な経験・設備を同時に備えるとは考えにくく、したがって SOF-基本が妥当といえる。

8.2.4 セキュリティ機能要件依存性

8.2.4.1 TOE セキュリティ機能要件依存性

表 8-4 は TOE で選択された TOE セキュリティ機能要件の依存性を示す。IT 環境で依存性を満たしている機能要件は斜体で、満たしていない機能要件は下線で表記する。

機能要件	ST で選択した依存する機能要件	満たしていない機能要件
FAU_GEN.1	FPT_STM.1	－
FAU_GEN.2	FAU_GEN.1 FIA_UID.1(1)	－
FAU_SAR.1	FAU_GEN.1	－
FAU_SAR.2	FAU_SAR.1	－
FAU_STG.1	FAU_GEN.1	－

機能要件	ST で選択した依存する機能要件	満たしていない機能要件
FAU_STG.3	FAU_STG.1	―
FDP_IFC.1	FDP_IFF.1	―
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	―
FDP_DAU.1	―	―
FIA_ATD.1	―	―
FIA_SOS.1	―	―
FIA_UAU.2(1)	FIA_UID.2(1)	―
FIA_UID.2(1)	―	―
FIA_USB.1	FIA_ATD.1	―
FMT_MSA.1	FDP_IFC.1 FMT_SMR.1	―
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	―
FMT_MTD.1	FMT_SMR.1	―
FMT_SMR.1	FIA_UID.1(1)	―
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	―
FMT_SMF.1	―	―
FPT_RVM.1	―	―
FPT_SEP.1	―	―
FPT_STM.1	―	―

表 8-4　セキュリティ機能要件の依存性

FAU_GEN.2、FIA_UAU.2(1)、FMT_SMR.1 から導かれる FIA_UID.1 への依存性

FIA_UID.2(1)を選択しているので、依存性は満たされている。

8.2.4.2 IT 環境に対するセキュリティ機能要件依存性

表 8-5 は IT 環境で選択されたセキュリティ機能要件の依存性を示す。IT 環境で依存性を満たしている機能要件は斜体で、満たしていない機能要件は下線で表記する。

機能要件	ST で選択した依存する機能要件	満たしていない機能要件
FCS_CKM.1	FCS_COP.1	FCS_CKM.4 FMT_MSA.2
FCS_COP.1	FCS_CKM.1	FCS_CKM.4 FMT_MSA.2
FIA_UAU.2(2)	FIA_UID.2(2)	―
FIA_UID.2(2)	―	―

表 8-5　IT 環境に対するセキュリティ機能要件の依存性

依存関係が満たされていない部分について、問題がない根拠を以下に示す。

FCS_CKM.1、FCS_COP.1 から導かれる FCS_CKM.4 への依存性

TOE 運用管理者が暗号アルゴリズムと鍵長の変更を行った場合、TOE の起動時に暗号モジュール（TOE 範囲外）で暗号鍵を生成する。

生成された鍵はファイルに保存される。暗号アルゴリズムと鍵長の変更を TOE 運用管理者が行った後起動しない限り、変更あるいは廃棄することはない。したがって、この依存関係は不要である。

FCS_CKM.1、FCS_COP.1 から導かれる FMT_MSA.2 への依存性

TOE 運用管理者が暗号アルゴリズムと鍵長の変更を行った場合、TOE の起動時に暗号モジュール（TOE 範囲外）で暗号鍵を生成する。生成された鍵はファイルに保存される。鍵ファイルはひとつしか存在せず暗号操作の実行時鍵を識別しなくても安全である。

生成された鍵を保存するファイルは OS の機能で安全に維持されるためセキュリティ属性に割り付けられた値はセキュアに維持できる。

したがって、この依存関係は不要である。

8.2.5 セキュリティ要件の相互補完

前節より、TOE セキュリティ機能要件および IT 環境セキュリティ機能要件は、一部の例外を除き、それぞれと依存関係のある機能要件と相互補完している。

これらの機能要件以外で、明示的な依存関係はないが、以下の観点から相互補完する機能要件について記述する。

＜バイパス防止＞

FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、識別・認証機能（FIA_UAU.2(1)、FIA_UID.2(1)）、情報フロー制御機能（FDP_IFC.1、FDP_IFF.1）、TSP 実施機能（FMT_MTD.1、FMT_SAE.1）が呼び出され成功することが保証される。

＜改ざん防止＞

FPT_SEP.1 により、TOE に登録されていない信頼できないサブジェクトによるセキュリティドメインの改ざんを防止する。したがって、その TOE 上で動作する TOE のセキュリティ機能（すべての TOE 機能要件）の改ざんも防止する。

8.2.6 TOE 保証要件の妥当性

ForceSecure-Filing V01 で扱う電子文書は、行政文書や医療情報も対象とすることができるため、実装されるセキュリティ機能には高い信頼性が要求される。しかしながらファイルサーバ PC は物理的に入退出制限されかつ業務アプリケーションサーバ PC との接続は外部ネットワークとファイアウオールで隔離された環境に置かれ運用することを考慮すると攻撃レベルは“低”と想定する。一方で、高い保証レベルの評価にはそれなりのコストがかかるため、製品の価格に影響を及ぼすことも事実である。それらを考慮すると EAL3 は TOE の細部分析（下位設計書とソースコードの評価）を除いては、より確かな品質を保証するという点で妥当な選択であると考える。

8.3 TOE 要約仕様根拠

8.3.1 セキュリティ機能の根拠

表 8-6 にIT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示す。表中の「X」は、対応関係にあることを示している。

	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.3	FDP_IFC.1	FDP_IFF.1	FDP_DAU.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2(1)	FIA_UID.2(1)	FIA_USB.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SAE.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1
SF.IFC							X	X		X				X	X	X					X	X	
SF.DETECT_MODIFY									X														X
SF.LOG	X	X	X	X	X	X																	X
SF.I&A_USER												X	X								X		
SF.USER_MANAGE											X						X	X	X	X			

表 8-6　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

SF.IFC は、FDP_IFC.1、FDP_IFF.1、FMT_MSA1、FMT_MSA.3、FIA_USB.1、FIA_ATD.1、FPT_RVM.1、FPT_SEP.1 の 8 個の機能要件に対応している。

SF.DETECT_MODIFY は、FDP_DAU.1、FPT_STM.1 の 2 個の機能要件に対応している。

SF.LOG は、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.3、FPT_STM.1 の 7 個の機能要件に対応している。

SF.I&A_USER は、FIA_UAU.2(1)、FIA_UID.2(1)、FPT_RVM.1 の３個の機能要件に対応している。

SF.USER_MANAGE は、FIA_SOS.1、FMT_MTD.1、FMT_SAE.1、FMT_SMF.1、FMT_SMR.1 の５個の機能要件に対応している。

したがって、各 IT セキュリティ機能は、少なくとも 1 つの TOE セキュリティ機能要件に対応しているといえる。

次に、各セキュリティ機能要件が、TOE セキュリティ機能で実現できることを説明する。

FAU_GEN.1

SF.LOG は、以下の監査対象事象の監査記録を生成する。

各機能要件を選択した場合の監査対象とすべきアクションと、SF.LOG にて記録する監査事象の対応関係を以下に示す。

下線は選択した機能要件の監査対象事象を示す。

機能要件	監査対象とすべきアクション	監査対象事象
FDP_IFC.1	無し	無し
FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット。	・ 業務アプリケーション命令の処理エラー結果 ・ 電子文書の書込み／読出し／削除の成功 ・ サブフォルダの生成／削除の成功 ・ 電子文書の書込み／読出し／削除の失敗 ・ サブフォルダの生成／削除の失敗
FDP_DAU.1	a) 最小: 有効性の証拠の生成成功。 b) 基本: 有効性の証拠の生成不成功。 c) 詳細: 証拠を要求したサブジェクトの識別情報。	・ 電子文書の書込みの成功 ・ 改ざん検証データ生成失敗
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合（例えば、サブジェクトの生成）。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功及び失敗)。	・ 識別認証された業務アプリケーションと業務アプリケーションプロセスのWWW サーバ異常による結合失敗
FIA_ATD.1	無し	無し
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	設定情報の設定／変更
FMT_MSA.3	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	無し

表 8-7　各機能要件における監査対象とすべきアクションと監査対象事象の対応関係

FDP_IFF.1 を選択した場合の監査対象とすべきアクション“ 情報フローに対する要求に関するすべての決定 ” に対して、SF.LOG では電子文書の書込み／読出し／削除の成功, サブフォルダの生成／削除の成功,電子文書の書込み／読出し／削除の失敗, サブフォルダの生成／削除の失敗を記録しているが、これは、情報フローが成功して行われるため情報フローの成功を意味している。

FDP_DAU.1 を選択した場合の監査対象とすべきアクション“ 有効性の証拠の生成成功 ” に対して、SF.LOG では電子文書の書込み成功を記録しているが、これは、TOE が有効性の証拠（改ざん検証データ）の生成を電子文書の書込み時に行うからである。電子文書の

書込み時、改ざん検証データの生成に失敗した場合は、“改ざん検証データ生成失敗”が監査証跡に記録されるため、電子文書の書込みの成功は、有効性の証拠の生成成功をも意味することになる。

FMT_MSA.3 の監査対象事象は、“無し”であるがサブフォルダまたは文書ファイル生成時に、仮想ディレクトリの仮想ディレクトリ名および権限を継承するため、監査事象が存在しなくても追跡性の問題は発生しない。

また、SF.LOG では、各監査記録において以下の情報を記録する。

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

したがって、FAU_GEN.1 は SF.LOG により実現されている。

FAU_GEN.2

SF.LOG は、監査記録時に業務アプリケーション識別情報を記録することにより、各監査対象事象をその原因となった業務アプリケーションに関連付けている。

したがって、FAU_GEN.2 は SF.LOG により実現されている。

FAU_SAR.1

SF.LOG は、TOE 運用管理者に限り監査データへの参照を許可する。

したがって、FAU_SAR.1 は SF.LOG により実現されている。

FAU_SAR.2

SF.LOG は、TOE 運用管理者に限り監査データへの参照を許可しており、TOE 許可利用者は監査データを参照することができない。

したがって、FAU_SAR.2 は SF.LOG により実現されている。

FAU_STG.1

SF.LOG は、監査データにアクセス可能な利用者を TOE 運用管理者に制限する。

また、TOE 運用管理者には監査データの参照のみ許可されるため、監査データの変更、および削除を行うことはできない。

したがって、FAU_STG.1 は SF.LOG により実現されている。

FAU_STG.3

SF.LOG は、監査証跡が、TOE 運用管理者が TOE のインストール時に指定した監査データ格納用の領域サイズを超えた場合、TOE の運用を停止する。

したがって、FAU_STG.3 は SF.LOG により実現されている。

FDP_IFC.1

SF.IFC は、業務アプリケーションプロセスがサブフォルダと電子文書に対しおこなう業務アプリケーションからの命令に対しディレクトリの権限に基づく情報フローを制御する。従って FDP_IFC.1 は SF.IFC により実現されている。

FDP_IFF.1

SF.IFC は、業務アプリケーションと関連付けられた業務アプリケーションプロセスにおいて、業務アプリケーションからの命令に対し、そこで指定された仮想ディレクトリの権限に基づき、業務アプリケーションからの命令を通過させるかエラーを返して破棄するかの情報フロー制御をおこなう。そのルールは FDP_IFF.1 と SF.IFC で一致する。

SF.IFC は、TOE 運用管理者または TOE 許可利用者が、業務アプリケーション識別に対する仮想ディレクトリ名と権限を設定、変更、消去する。

したがって、FDP_IFF.1 は SF.IFC により実現されている。

FDP_DAU.1

SF.DETECT_MODIFY は、電子文書の書込み時に生成された改ざん検証データより、電子文書の有効性の証拠を検証する。

したがって、FDP_DAU.1 は SF.DETECT_MODIFY により実現されている。

FIA_ATD.1

SF.IFC は業務アプリケーション ID と仮想ディレクトリ名を維持する。

したがって、FIA_ATD.1 は SF.IFC により実現されている。

FIA_SOS.1

SF.USER_MANAGE は、TOE 運用管理者および TOE 許可利用者の認証に使用するパスワードが以下の品質尺度を満たすことを検証するメカニズムを提供する。

・パスワードは 8 個以上の英数字

したがって、FIA_SOS.1 は SF.USER_MANAGE により実現されている。

FIA_UAU.2(1)

SF.I&A_USER は、TOE 運用管理者および TOE 許可利用者の認証にあたり、TOE は、TOE 運用管理者および TOE 許可利用者に対し認証前のいかなる操作も許可しない。

したがって、FIA_UAU.2(1)は SF.I&A_USER により実現されている。

FIA_UID.2(1)

SF.I&A_USER は、TOE 運用管理者および TOE 許可利用者が TOE を利用する前に、TOE 運用管理者および TOE 許可利用者の識別を行う。

したがって、FIA_UID.2(1)は SF.I&A_USER により実現されている。

FIA_USB.1

SF.IFC は、識別認証に成功した業務アプリケーションをサブジェクトである業務アプリケーションプロセスと関連付ける。

したがって、FIA_USB.1 は SF.IFC により実現されている。

FMT_MSA.1

SF.IFC は、仮想ディレクトリの権限の設定を TOE 運用管理者に制限し、TOE 許可利用者が管理する特定の業務アプリケーションの仮想ディレクトリに対する権限の設定を TOE 許可利用者に制限する。

したがって、FMT_MSA.1 は SF.IFC により実現されている。

FMT_MSA.3

SF.IFC は、「書込み／読出し／削除」の権限を仮想ディレクトリに関連付けており、TOE 運用管理者または TOE 許可利用者が設定できる。

したがって、FMT_MSA.3 は SF.IFC により実現されている。

FMT_MTD.1

SF.USER_MANAGE は、TSF データ（TOE 運用管理者パスワード、TOE 許可利用者ユーザ ID）の管理機能を、TOE 運用管理者に制限する。

したがって、FMT_MTD.1 は SF.USER_MANAGE により実現されている。

FMT_SAE.1

SF.USER_MANAGE は、TOE 運用管理者および TOE 許可利用者のパスワード有効期限に対する有効期限の時間を特定する能力を TOE 運用管理者に制限し、TOE 運用管理者または TOE 許可利用者のパスワード有効期限が切れた場合、パスワードの変更を強制する。

したがって、FMT_SAE.1 は SF.USER_MANAGE により実現されている。

FMT_SMF.1

SF.USER_MANAGE は、TSF データ（TOE 運用管理者パスワード、TOE 許可利用者のユーザ ID・パスワード）の管理機能を特定する。

したがって、FMT_SMF.1 は SF.USER_MANAGE により実現されている。

FMT_SMR.1

SF.USER_MANAGE は、TOE 運用管理者・TOE 許可利用者の役割を特定する。

したがって、FMT_SMR.1 は SF.USER_MANAGE により実現されている。

FPT_RVM.1

SF.I&A_USER による利用者（TOE 運用管理者および TOE 許可利用者）の識別認証が完了しないと TOE の操作ができない。

したがって、FPT_RVM.1 は SF.I&A_USER、SF.IFC により実現されている。

FPT_SEP.1

SF.IFC は､信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのドメインを維持している。

したがって、FPT_SEP.1 は SF.IFC により実現されている。

FPT_STM.1

SF.LOG は、監査データに記録する日付時刻情報を、OS から取得する。

SF.DETECT_MODIFY は、改ざん検証データに含まれる電子署名を構成する日付時刻情報を、OS から取得する。

したがって、FPT_STM.1 は SF.LOG、SF.DETECT_MODIFY により実現されている。

8.3.2 機能強度の根拠

本 TOE において、確率的あるいは順列的メカニズムを持つセキュリティ機能は SF.I&A_USER だけである。SF.I&A_USER のセキュリティ機能強度は 6.1.4 章において「SOF-基本」と宣言されている。一方、本 TOE の最小機能強度は 5.1.3 章において「SOF-基本」と宣言されている。これらが矛盾していないことは明らかである。

8.3.3 保証手段の根拠

ASE クラスおよび EAL3 からなる保証要件と､それぞれのコンポーネントに対応する保証手段とを表 6-2 に示す。表にある各保証手段により、それぞれ対応する保証要件は満たされる。

8.4 PP 主張根拠

この ST で参照される PP はない。