ＳＴ確認報告書

評価対象

申請受付年月日(受付番号)	**平成**15**年**7**月**22**日**（ST**確認**3027）
確認番号	V023
ＳＴ確認申請者	**富士電機アドバンストテクノロジー株式会社**
ＳＴの名称	ForceSecure-Filing V01 **セキュリティターゲット**
ＳＴのバージョン	V01R21
ＰＰ適合	**なし**
適合する保証要件	ASE（ST**評価**）**クラス** （TOE**の保証パッケージは**EAL3）
ＳＴ開発者	**富士電機アドバンストテクノロジー株式会社**
評価実施機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

上記のSTについての評価は、以下のとおりであることを確認したので報告します。
平成17年2月9日

独立行政法人 情報処理推進機構
セキュリティセンター情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「セキュリティターゲットの確認業務実施規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0210

評価結果：合格

「ForceSecure-Filing V01 セキュリティターゲット」は、独立行政法人 情報処理推進機構が定めるセキュリティターゲットの確認業務実施規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

このST確認報告書は、「ForceSecure-Filing V01 セキュリティターゲット　V01R21」（以下「本ST」という。）について株式会社電子商取引安全技術研究所評価センター（以下「評価実施機関」という。）が行ったセキュリティ評価に対し、その内容の確認結果を申請者である富士電機アドバンストテクノロジー株式会社に報告するものである。

本ST確認報告書の読者は、本書とともに、対応する本ST[1]を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、本STにおいて詳述されている。

本ST確認報告書は、本STに対する確認結果を示すものであり、対応するTOEのいかなる実装についても言及していないことに留意されたい。

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

1.2 評価製品

1.2.1 製品名称

本STが対象とする製品は、以下のとおりである。なお、TOEの正確な範囲は、1.2.3節で定義される。

・名称:　　ForceSecure-Filing
・バージョン　V01
・開発者:　　富士電機アドバンストテクノロジー株式会社

1.2.2 製品概要

TOE(ForceSecure-Filing V01)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である。

本製品は、WWWサーバや暗号ツール、OSなどのソフトウェ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。

1.2.3 TOEの範囲

(1) TOEの動作環境

TOEが動作する環境について、図 1に示す。

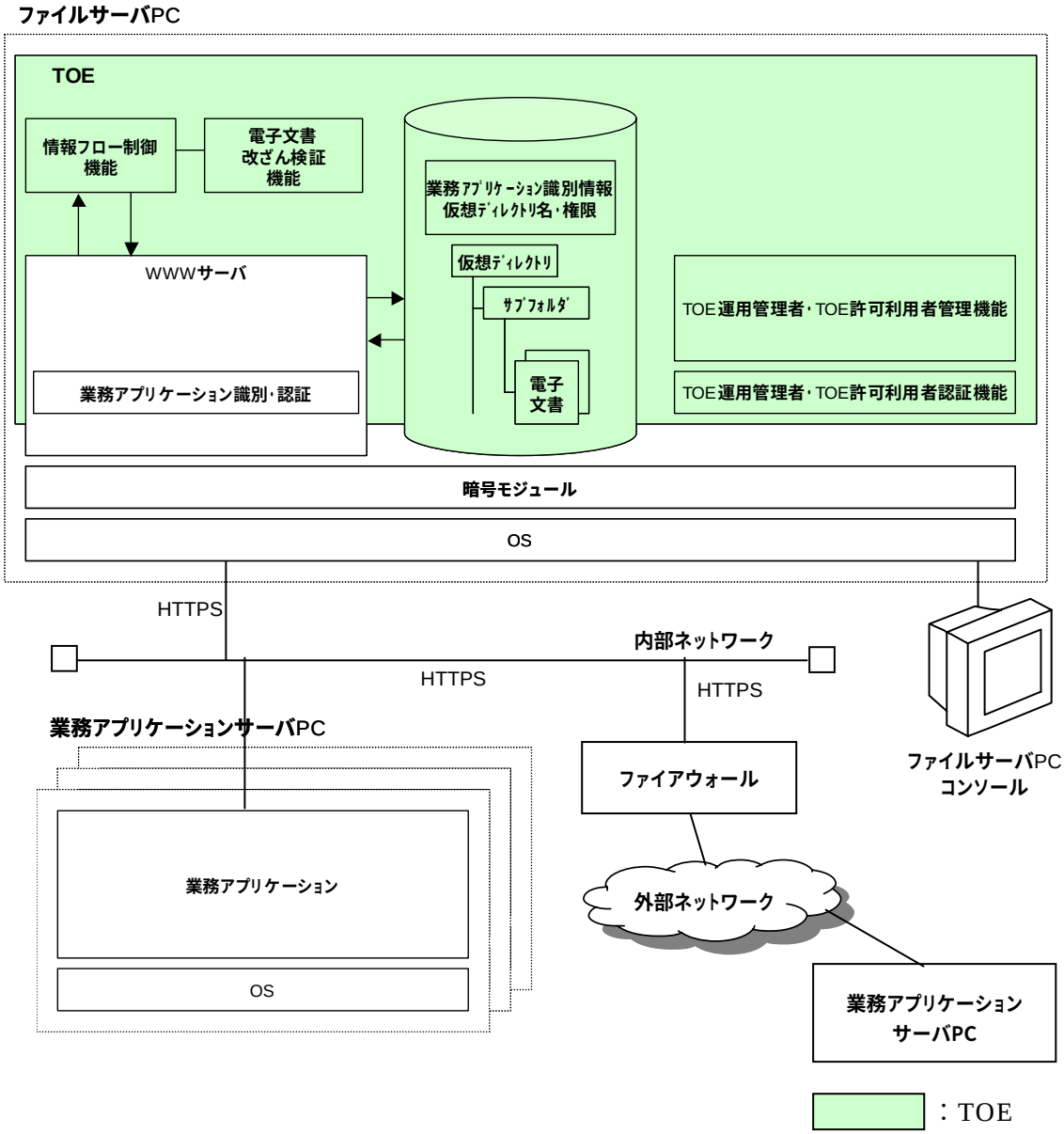

図 1　TOEの動作環境

TOEは、”ForceSecure-Filing V01”であり、ファイルサーバPC上で動作する。業務アプリケーション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ー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、HTTPS通信はTOEの範囲外である。

(2) TOEの機能範囲

TOEは、ファイルサーバPC上で、暗号モジュール、WWWサーバを利用して、電子文書をセキュアに管理する。以下に、TOE範囲内の機能と、TOE範囲外の機能を示す。

1) TOE範囲内の機能

・情報フロー制御機能

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

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

・ログ機能

業務アプリケーションからの処理履歴、及び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。

・TOE運用管理者・TOE許可利用者認証機能

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

・TOE運用管理者・TOE許可利用者管理機能

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

2) TOE範囲外の機能

・鍵生成機能

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／検証を行う電子署名用公開鍵ペア（RSA 1024bit またはRSA 2048bit）を生成する。

・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。

・電子署名機能

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。

・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

1.2.4 TOEの動作概要

(1) TOEの利用方法

TOEは、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に示す

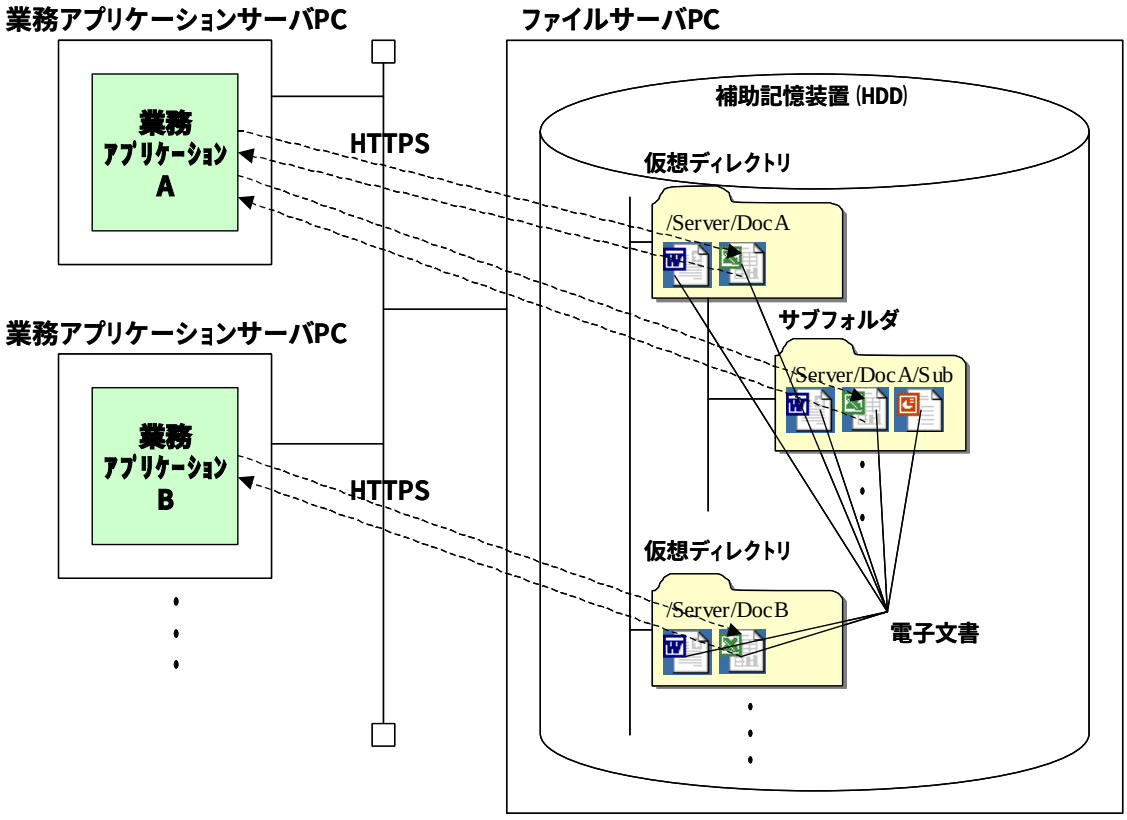

図 2 TOEを利用した文書管理システム概要

ファイルサーバPCは、補助記憶装置（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。

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。

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。

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、及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、及びTOE許可利用者が行う。

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、及び電子文書の改ざんの検知を行うことができる。

(2) TOEの利用者

・TOE運用管理者

TOE の設定、管理を行う管理者。TOE 運用管理者は以下の機能を実行する。

1)TOE 運用管理者のパスワードの登録・変更、及びパスワードの有効期限の設定。

2)TOE 許可利用者のユーザ ID、パスワード、及びパスワードの有効期限の設定。

3)仮想ディレクトリの生成・削除、及び当該仮想ディレクトリの権限の設定・変更・削除。

4)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。

5)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。TOE 許可利用者は、以下の機能を実行することができる。
1) 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、及び当該仮想ディレクトリの権限の設定・変更・削除。

・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。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。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。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。

1.3 評価実施

「ForceSecure-Filing V01 セキュリティターゲット V01R21」のセキュリティ評価は、認証機関が運営するITセキュリティ評価・認証プログラムに基づき、「セキュリティターゲットの評価・確認申請等の手引き」[2]、「セキュリティターゲット 評価実施機関に対する要求事項」[3]、「セキュリティターゲットの確認申請者・登録者に対する要求事項」[4]に規定された内容に従い、評価実施機関によって実施された。

本評価の目的は、申請者から提出された本ST[1]が、CCパート1([5][8][11][14]のいずれか)附属書C、CCパート2([6][9][12][15]のいずれか)の機能要件及びCCパート3([7][7][10][13][16]のいずれか)のASEクラスの規定を満たしており、セキュリティ機能設計の基本文書として技術的に妥当なものであるかどうかを評価することである。ただし、ASEクラスの規定の中で、TOE評価と関連する要求事項については、評価の項目に含まれていない。なお、評価方法は、CEMパート2([17][18][19]のいずれか)に準拠する。また、CC及びCEMの各パートは補足（[21][22]）の内容を含む。

認証機関は、評価実施機関が実施するSTの評価を監督し、ST評価が所定の手続きに沿って行われたことを確認した。評価は、平成17年1月の評価実施機関による「ST評価報告書 6.0版」（以下「本評価報告書」という。）[20]の提出をもって完了し、同報告書に基づき、認証機関は本ST確認報告書を作成した。

1.4 報告概要

1.4.1 PP適合

適合するPPはない。

1.4.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3適合である。

1.4.3 セキュリティ機能強度

本STにおいてTOEに要求される最小機能強度レベルは、SOF-基本である。

1.4.4 セキュリティ機能

本STで扱うTOEのセキュリティ機能は以下のとおりである。

・ 情報フロー制御機能

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

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、及び検証はTOE範囲外である電子署名機能にて実行する。

・ ログ機能

業務アプリケーションからの処理履歴、及び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。

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にアクセスするTOE運用管理者、及び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、及び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、及び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、及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、及びパスワードの有効期限の設定を行う。

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

1.4.5 脅威

TOEは、表 1に示す脅威を想定し、本製品は、これに対抗する機能を備える。

表 1　想定する脅威

識別子	内　容
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。

1.4.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.4.7 構成条件

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、及び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。

1.4.8 動作環境の前提条件

TOEを使用する環境において有する前提条件を表 2に示す。

これらの前提条件が満たされない場合、TOEのセキュリティ機能が有効に動作することは保証されない。

表 2　TOE使用の前提条件

識別子	内　容
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.COM	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.DEDICATE_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。

1.5 ST確認に関わる注意事項

ST確認は、CCで規定された評価の全過程から、ST評価の部分だけを抜き出した評価に基づいて行われるものである。したがって、ST評価を規定したASEクラスの要件の中で、TOE評価と関連する事項についてはST評価の対象になっていない。また、ASEクラス以外の保証クラスに属する事項、例えば、STの記載事項がそのとおりに設計されTOEに実装されているかどうか、TOEに悪用可能な脆弱性が残っていないかどうか、あるいはTOEの製造・配付が安全な手続きに基づいて行われているかなども評価の範囲外である。これら評価対象外の事項については確認も行われていないことに、本報告書の読者は留意すべきである。

ST確認は、TOEに対する、潜在的なものを含めたあらゆるセキュリティ上の脅威が完全に対策されていることを保証するものではない。評価完了後にTOEやそのIT環境にあらたな脅威が発見される可能性は常に考慮されるべきであり、TOE利用者は、TOEに関わる最新のセキュリティ関連情報に継続的な注意を払うことが必要である。

STの中で前提条件として記述されたものは、TOEを安全に使用する上での必須事項である。これらの条件が満たされないと、TOEのセキュリティ機能は、期待される効果を発揮

することができない。前提条件を満たすためのTOEの安全な運用管理は、TOE利用者の責務である。

本ST確認報告書は、認証機関が該当するTOEを保証し、その使用を推奨することを意図したものではない。

2 TOE構成

TOEが動作するファイルサーバPCのハードウェア、及びソフトウェア構成について以下に示す。

(1) ForceSecure-Filing V01 に必要なハードウェア

TOE（ForceSecure-Filing V01）が動作するファイルサーバPCのハードウェア構成を、表 3に示す。

表 3 ForceSecure-Filing V01 に必要なハードウェア

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 ドライブ	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

(2) ForceSecure-Filing V01 に必要なソフトウェア

TOE（ForceSecure-Filing V01）が動作するファイルサーバPCのソフトウェア構成を、表 4に示す

表 4 ForceSecure-Filing V01 に必要なソフトウェア

構成要素	要 件
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

3 評価実施機関による評価結果

評価は、CCパート3のASEクラスの規定に基づき、CEMパート2に規定された評価方法を用いて行われた。評価作業の詳細は、ST評価報告書[20]において報告されている。ST評価報告書には、TOEの概要説明、CEMパート2のワークユニットごとの評価内容及び判断が記載されている。各ワークユニットの評価作業において発見された問題点及びその対処の経過・結果も記載されている。

評価実施機関が評価中に発見した問題点は、すべて、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

総合判定は、「合格」である。

4 結論

4.1 ST確認実施

認証機関は、評価の過程で評価実施機関より提出される各資料をもとに、以下の確認を実施した。

① 評価実施機関が評価作業中に指摘した所見報告書の内容が妥当であること。

② 所見報告書でなされた指摘内容が正しくSTに反映されていること。

③ 提出されたSTの内容を確認し、関連する評価者アクションエレメントが本評価報告書で示されたように評価されていること。

④ 本評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 本評価報告書に示された評価者の評価方法がCEMに準拠していること。

これらの確認において発見された問題事項を認証レビューとして記載し、評価実施機関に送付した。

認証機関は、本STにおいて、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4.2 ST確認結果

提出されたST評価報告書及び所見報告書を調査した結果、認証機関は、本STがCCパート3に規定されたASEクラスの保証要件を満たしていることを確認した。

評価実施機関の実施した各評価者アクションエレメントについての調査結果を表 5にまとめる。

表 5　評価者アクションエレメント調査結果

評価者アクションエレメント	調査結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

評価者アクションエレメント	調査結果
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が明記され、それらが脅威、組織のセキュリティ、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

評価者アクションエレメント	調査結果
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完結しており、理路整然とし、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

4.3 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用された用語の定義を以下に示す。

HTTPS	Hypertext Transfer Protocol Security：Webサーバとクライアントがデータを送受信するのに使用されるHTTPにSSLによるデータの暗号化機能を付加したプロトコル。
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。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。
業務アプリケーションPC	業務アプリケーションが搭載されたサーバPC。
ファイルサーバPC	TOEが搭載されたサーバPC。
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。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。
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。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、及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。
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。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

6 参照

[1] ForceSecure-Filing V01 セキュリティターゲット V01R21 2005年1月21日 富士電機アドバンストテクノロジー株式会社

[2] セキュリティターゲットの評価・確認申請等の手引き 平成16年4月 独立行政法人 情報処理推進機構 ITQM-21

[3] セキュリティターゲット 評価実施機関に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-13

[4] セキュリティターゲットの確認申請者・登録者に対する要求事項 平成16年4月 独立行政法人 情報処理推進機構 ITQM-12

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

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

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

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] 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

[15] 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

[16] 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

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] ST評価報告書 6.0版 2005年1月24日 NYC-ETRST-0006-00 株式会社電子商取引安全技術研究所 評価センター

[21] CCIMB Interpretations-0210

[22] 補足-0210