



KONICA MINOLTA

***bizhub C3850 / bizhub C3350 /
bizhub C3850FS /
ineo+ 3850 / ineo+ 3350 /
ineo+ 3850FS***

セキュリティターゲット

バージョン : 1.16

発行日 : 2016年3月11日

作成者 : コニカミノルタ株式会社

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2015/1/26	1.00	第2OPシステム制御開発部	山崎	小西	戸田	初版
2015/2/13	1.01	第2OPシステム制御開発部	山崎	小西	戸田	誤植の修正
2015/3/12	1.02	第2OPシステム制御開発部	山崎	小西	戸田	・ TOE識別、各種バージョンの見直し修正 ・ 誤植の修正
2015/4/7	1.03	第2OPシステム制御開発部	山崎	小西	戸田	・ 全体の見直し修正
2015/5/15	1.04	第2OPシステム制御開発部	山崎	小西	戸田	・ 全体の見直し修正
2015/6/9	1.05	第2OPシステム制御開発部	山崎	小西	戸田	・ 全体の見直し修正
2015/7/13	1.06	第2OPシステム制御開発部	山崎	小西	田向	・ 全体の見直し修正
2015/7/21	1.07	第2OPシステム制御開発部	山崎	小西	田向	・ 全体の見直し修正
2015/8/3	1.08	第2OPシステム制御開発部	山崎	小西	田向	・ 全体の見直し修正
2015/10/26	1.09	第2OPシステム制御開発部	山崎	小西	田向	・ 所見報告書に伴う修正
2015/11/17	1.10	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2015/12/17	1.11	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2015/12/22	1.12	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2016/1/22	1.13	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2016/2/17	1.14	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2016/3/1	1.15	第2OPシステム制御開発部	山崎	小西	田向	・ 指摘に伴う修正
2016/3/11	1.16	第2OPシステム制御開発部	山崎	小西	田向	・ ガイドンスのバージョン修正

— 【 目次 】 —

1. ST introduction	7
1.1. ST reference.....	7
1.2. TOE reference.....	7
1.3. TOE overview	7
1.3.1. TOE の種別.....	7
1.3.2. TOEに必要な TOE 以外のハードウェア/ソフトウェア.....	7
1.3.3. TOE の使用方法.....	8
1.3.4. TOE の主要な基本機能および主要なセキュリティ機能.....	9
1.4. TOE description	10
1.4.1. TOE の物理的範囲.....	11
1.4.2. ガイダンス.....	12
1.4.3. TOE の構成要素の識別.....	13
1.4.4. TOE の論理的範囲.....	13
1.4.5. TOE の利用者.....	16
1.4.6. 保護資産.....	16
1.4.7. 用語.....	17
2. Conformance claims	20
2.1. CC Conformance claims.....	20
2.2. PP claim.....	20
2.3. Package claim.....	20
2.3.1. SFR package reference.....	20
2.3.2. SFR Package functions.....	21
2.3.3. SFR Package attributes.....	21
2.4. PP Conformance rationale.....	22
2.4.1. PP の TOE 種別との一貫性主張.....	22
2.4.2. PP のセキュリティ課題とセキュリティ対策方針との一貫性主張.....	22
2.4.3. PP のセキュリティ要件との一貫性主張.....	22
3. Security Problem Definition	24
3.1. Threats agents.....	24
3.2. Threats to TOE Assets	24
3.3. Organizational Security Policies for the TOE	24
3.4. Assumptions	25
4. Security Objectives	26
4.1. Security Objectives for the TOE.....	26
4.2. Security Objectives for the IT environment.....	26
4.3. Security Objectives for the non-IT environment	27
4.4. Security Objectives rationale.....	28
5. Extended components definition (APE_ECD)	31
5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces.....	31
6. Security Requirements	33
6.1. Security functional requirements.....	33
6.1.1. Class FAU: Security audit	33
6.1.2. Class FCS: Cryptographic support.....	36

6.1.3. Class FDP: User data protection.....	37
6.1.4. Class FIA: Identification and authentication.....	42
6.1.5. Class FMT: Security management.....	45
6.1.6. Class FPT: Protection of the TSF.....	51
6.1.7. Class FTA: TOE access.....	52
6.1.8. Class FTP: Trusted path/channels.....	53
6.2. Security assurance requirements.....	53
6.3. Security requirements rationale.....	54
6.3.1. Common security requirements rationale (SFR Package is included).....	54
6.3.2. Security assurance requirements rationale.....	60
7. TOE Summary specification.....	61
7.1. FAUDIT(監査ログ機能).....	61
7.1.1. 監査ログ取得機能.....	61
7.1.2. 監査ログレビュー機能.....	61
7.1.3. 監査格納機能.....	62
7.1.4. 高信頼タイムスタンプ機能.....	62
7.2. FHDD_ENCRYPTION(HDD 暗号化機能).....	62
7.3. F.ACCESS_DOC(保存文書アクセス制御機能).....	63
7.4. F.ACCESS_FUNC(利用者制限制御機能).....	63
7.5. F.RIP(残存情報消去機能).....	64
7.5.1. 一時データ削除機能.....	64
7.5.2. データ完全削除機能.....	65
7.6. FI&A(識別認証機能).....	65
7.7. F.SEPARATE_EX_INTERFACE(外部インタフェース分離機能).....	67
7.8. F.SELF_TEST(自己テスト機能).....	67
7.9. F.MANAGE(セキュリティ管理機能).....	67
7.10. F.SECURE_LAN(ネットワーク通信保護機能).....	69

— 【 図目次 】 —

図 1-1 TOE の利用環境	8
図 1-2 TOE の物理的範囲	11
図 1-3 TOE の論理的範囲	13

— 【 表目次 】 —

Table 1-1 Users	16
Table 1-2 User Data	16
Table 1-3 TSF Data	17
Table 1-4 TSF Data	17
Table 1-5 用語	17
Table 2-1 SFR Package functions	21
Table 2-2 SFR Package attributes	22
Table 3-1 Threats to User Data for the TOE	24
Table 3-2 Threats to TSF Data for the TOE	24
Table 3-3 Organizational Security Policies for the TOE	24
Table 3-4 Assumptions for the TOE	25
Table 4-1 Security Objectives for the TOE	26
Table 4-2 Security Objectives for the IT environment	26
Table 4-3 Security Objectives for the non-IT environment	27
Table 4-4 Completeness of Security Objectives	28
Table 4-5 Sufficiency of Security Objectives	28
Table 6-1 Audit data requirements	34
Table 6-2 Cryptographic key algorithm key size	37
Table 6-3 Cryptographic operations algorithm key size standards	37
Table 6-4 Common Access Control SFP	38
Table 6-5 PRT Access Control SFP	38
Table 6-6 SCN Access Control SFP	38
Table 6-7 CPY Access Control SFP	38
Table 6-8 FAX Access Control SFP	38
Table 6-9 DSR Access Control SFP	39
Table 6-10 TOE Function Access Control SFP	39
Table 6-11 Management of Object Security Attribute	46
Table 6-12 Management of Subject Security Attribute	46
Table 6-13 Management of Subject Security Attribute	47
Table 6-14 Management of Object Security Attribute	47
Table 6-15 Characteristics Static Attribute Initialization	48
Table 6-16 Characteristics Static Attribute Initialization	49
Table 6-17 Operation of TSF Data	50
Table 6-18 Operation of TSF Data	50
Table 6-19 list of management functions	50
Table 6-20 IEEE 2600.2 Security Assurance Requirements	53

Table 6-21	Completeness of security requirements.....	54
Table 6-22	Sufficiency of security requirements	55
Table 6-23	The dependencies of security requirements	59
Table 7-1	TOE のセキュリティ機能の名称と識別子	61
Table 7-2	監査ログ	61
Table 7-3	HDD 暗号化機能における暗号アルゴリズム	62
Table 7-4	文書の操作	63
Table 7-5	一時データ上書き削除機能の動作設定	65
Table 7-6	データ完全削除機能の動作設定	65
Table 7-7	認証方式.....	65
Table 7-8	パスワードと品質	66
Table 7-9	認証失敗時の処理	66
Table 7-10	対話セッションの終了	67
Table 7-11	管理機能.....	68
Table 7-12	TOE が提供する暗号化通信	69

1. ST introduction

1.1. ST reference

- ・ ST名称 : bizhub C3850 / bizhub C3350 / bizhub C3850FS /
ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
セキュリティターゲット
- ・ STバージョン : 1.16
- ・ 作成日 : 2016年3月11日
- ・ 作成者 : コニカミノルタ株式会社

1.2. TOE reference

- ・ TOE名称 : bizhub C3850 / bizhub C3350 / bizhub C3850FS /
ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
- ・ バージョン : G0607-999
- ・ 製造者 : コニカミノルタ株式会社

1.3. TOE overview

TOEは、基本的に中程度の文書セキュリティ、ネットワークセキュリティ、情報保証が要求される商用情報処理環境で使用されるデジタル複合機（以下、mfpと称する）である。この環境では通常、日常の企業運営で扱う機密／非機密情報が処理される。

1.3.1. TOE の種別

TOEはネットワーク環境(LAN)で使用されるmfpであり、コピー、スキャン、プリント、ファクスといった機能に加えドキュメントを保存する機能を有する。なお、ファクス機能を使用するためには、FAXキット（オプション）の接続が必要である。

1.3.2. TOEに必要なTOE以外のハードウェア／ソフトウェア

TOEを利用するにあたって必要となるハードウェア／ソフトウェアとして、TOE評価に用いた構成を以下に示す。

ハードウェア／ソフトウェア	評価で使ったバージョン等
FAXキット	FK-512 (KONICA MINOLTA社製)
クライアントPC (OS)	Windows 7 Professional SP1
クライアントPC (Webブラウザ)	Internet Explorer Ver.11 Mozilla Firefox Ver.36
クライアントPC (プリンタドライバー)	KONICA MINOLTA C3850 Series PCL6 v3.0.1 XPS v3.0.2
(管理者用) クライアントPC (デバイス管理ソフトウェアツール)	KONICA MINOLTA Data Administrator with Device Set-Up and Utilities Ver. 1.0.06000

	KONICA MINOLTA Data Administrator Ver. 4.1.35000
外部認証サーバー	Microsoft Windows Server 2008 R2 Standard Service Pack1 に搭載されるActiveDirectory
DNSサーバー	Microsoft Windows Server 2008 R2 Standard Service Pack1 に搭載されるDNSサーバー
SMTPサーバー	XMail version 1.27

1.3.3. TOE の使用方法

TOEの利用環境を図示して、使用方法を記述する。

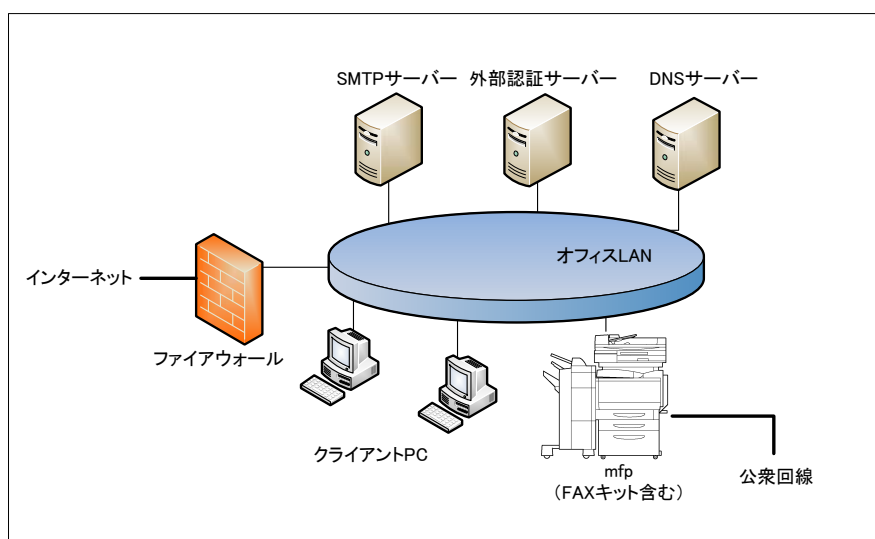


図 1-1 TOE の利用環境

TOEは図 1-1に示すようにLANと公衆回線に接続して使用する。利用者はTOEが備える操作パネルまたはLANを介して通信することによってTOEを操作することが出来る。以下にTOEであるmfpとTOE以外のハードウェア、ソフトウェアについて記述する。

(1) mfp (FAXキット含む)

TOE である。mfp はオフィス LAN に接続される。利用者は操作パネルから以下の処理を行うことができる。

- mfp の各種設定
- 紙文書のコピー・ファクス送信・電子文書としての保存・ネットワーク送信
- 保存文書の印刷・ネットワーク送信・削除

また、FAX キットが接続され、FAX 文書を送受信できる。

(2) LAN

TOE の設置環境で利用されるネットワーク。

(3) 公衆回線

FAX キットと接続され、外部ファクスと送受信するための電話回線。

(4) ファイアウォール

インターネットからオフィス内 LAN へのネットワーク攻撃を防止するための装置。

(5) クライアントPC

LANに接続することによってTOEのクライアントとして動作する。クライアントPCには、Web ブラウザ、プリンタドライバー、PSDA（管理者のみ）などをインストールすることができる。一般利用者は、これらを利用して mfp にアクセスし電子文書の保存・印刷、スキャン文書／ファクス受信文書のダウンロード・削除を行うことができる。また、管理者は、これらを利用して mfp にアクセスし mfp の各種設定を行うことができる。

(6) SMTPサーバー

TOE 内の電子文書を E メール送信する場合に使用されるサーバー。

(7) 外部認証サーバー

TOE の一般利用者を識別認証するサーバー。外部サーバー認証方式で運用する場合だけ必要となる。外部サーバー認証方式においては Kerberos 認証を用いる。

(8) DNSサーバー

ドメイン名を IP アドレスに変換するサーバー。

1.3.4. TOE の主要な基本機能および主要なセキュリティ機能

TOEの主な基本機能は以下の通りである。

(1) 印刷機能

印刷データを印刷する機能。

(2) スキャン機能

文書（紙）を読み取って文書ファイルを生成する機能。

(3) コピー機能

文書（紙）を読み取って、読み取った画像を複写印刷する機能。

(4) ファクス機能

紙文書を読み込んで外部ファクスに送信する機能、および、外部ファクスから文書を受信する機能。

(5) 文書の保存と取り出しの機能

TOE 内に文書を保存し、保存した文書を取り出す機能。

(6) 共有メディアインタフェース機能

TOE の利用者がクライアント PC から TOE をリモート操作する機能。

TOE の主なセキュリティ機能は以下の通りである。

(1) 識別認証機能

TOE の利用者を識別認証する機能。

(2) 保存文書アクセス制御機能

保存文書の操作を制御する機能。

(3) 利用者制限制御機能

TOE の機能の操作の制御、実行中のジョブに含まれる保存文書以外の文書への操作の制御をする機能。

(4) HDD暗号化機能

HDD に記録するデータを暗号化する機能。

(5) 監査ログ機能

TOE の使用およびセキュリティに関連する事象のログを監査ログとして記録し参照するための機能。

(6) 残存情報消去機能

TOE 内の削除された文書、一時的な文書あるいはその断片の再利用を不可能とする機能。

(7) ネットワーク通信保護機能

LAN 利用時にネットワーク上の盗聴による情報漏えいを防止する機能。

(8) 自己テスト機能

TSF 実行コードの完全性及び、暗号化ワードの完全性を mfp 起動時に検証し、全体制御機能の正常動作を実証する機能。

(9) セキュリティ管理機能

TSF データに対する操作を制御する機能。

(10) 外部インターフェース分離機能

USB インタフェースを含む外部インターフェースからの入力をそのまま Shared-medium Interface へ転送することができないようにし、また、電話回線から LAN への侵入を防止する機能。

1.4. TOE description

本章ではTOEの物理的範囲、利用者定義、TOEの論理的範囲、保護資産の概要を記述する。

1.4.1. TOE の物理的範囲

TOEは「図 1-2」に示すように、主電源・副電源、操作パネル、スキャナユニット・自動原稿送り装置、制御コントローラユニット、プリンタユニット、HDDで構成されるmfpである。

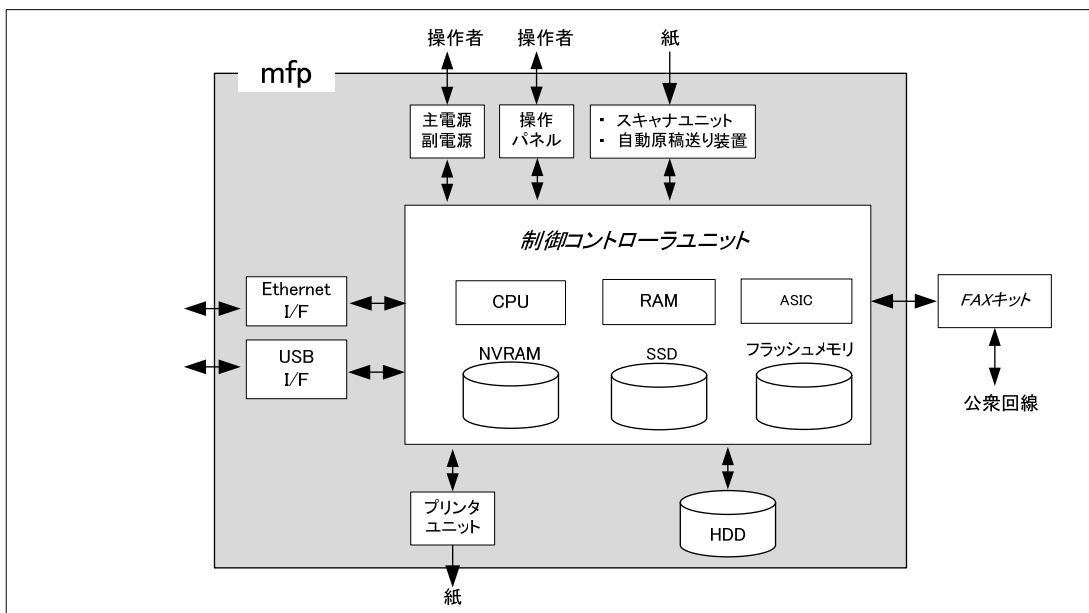


図 1-2 TOE の物理的範囲

- (1) 主電源・副電源
mfp を動作させるための電源スイッチ。
- (2) 操作パネル
タッチパネル液晶ディスプレイとテンキー¹やスタートキー、ストップキー、画面の切り替えキー等を備えた mfp を操作するための専用コントロールデバイス。
- (3) スキャナユニット／自動原稿送り装置
紙から図形、写真を読み取り、電子データに変換するためのデバイス。
- (4) 制御コントローラユニット
mfp を制御する装置。
- (5) CPU
中央演算処理装置。
- (6) RAM
作業領域として利用される揮発メモリ。
- (7) ASIC
画像処理全般を行うために設計された集積回路。また、画像を印刷する時に画像の展開と色合いの調整等の処理も行う。

¹ テンキーはタッチパネル内の表示となっており、ハードテンキーはオプション(TOE 外)である。

- (8) **NVRAM**
mfp の動作を決定する TSF データが保存される不揮発メモリ。
- (9) **SSD**
制御ソフトウェアのオブジェクトコード（操作パネルやネットワークからのアクセスに対するレスポンス等で表示するための各国言語メッセージデータを含む）が保存される記憶媒体。
- (10) **フラッシュメモリ**
TOE（Boot 制御部）のオブジェクトコードが保存される不揮発性メモリ。
- (11) **プリンタユニット**
制御コントローラからの指示により、印刷用に変換された画像データを印刷出力するデバイス。
- (12) **HDD**
容量 320GB のハードディスクドライブ。電子文書がファイルとして保存されるほか、作業領域としても利用される。本 TOE において HDD は着脱可能な不揮発性記憶装置ではない。
- (13) **Ethernet I/F**
10BASE-T、100BASE-TX、Gigabit Ethernet をサポートするインタフェース。
- (14) **USB I/F**
TOE のアップデートなどを実施できるインタフェース。なお、USB のローカルプリンター接続は 1 対 1 であり、USB I/F は共有メディアインタフェースには該当しない。
- (15) **FAXキット**
公衆回線を介して FAX の送受信や遠隔診断機能の通信に利用されるデバイス。これは TOE 外である。

1.4.2. ガイダンス

TOE のガイダンスは英語版と日本語版があり、販売地域に応じて配付する。以下にガイダンスの一覧を示す。

名称	Ver.
bizhub C3850 ユーザーズガイド	2015.3 Ver. 1.00
bizhub C3850 ユーザーズガイド セキュリティ機能編	2.02
bizhub C3850FS/C3850/C3350 user's Guide	2015.4 Ver. 1.00
bizhub C3850FS/C3850/C3350 user's Guide [Security Operations]	2.02
ineo+ 3850FS/3850/3350 User's Guide	2015.4 Ver. 1.00
ineo+ 3850FS/3850/3350 User's Guide [Security Operations]	2.02

1.4.3. TOE の構成要素の識別

TOE を構成する mfp 本体、ファームウェア、mfp 基板、SSD 基板はそれぞれ識別を持つ。それぞれの識別と mfp 本体に内蔵される構成要素の関係は以下の通りである。

mfp 本体	mfp 基板	ファームウェア	SSD 基板
bizhub C3850	A3GNH010-07	A3GN30G0607-999	A3GNM71A-01
ineo+ 3850			
bizhub C3350			
ineo+ 3350			
bizhub C3850FS			
ineo+ 3850FS			

1.4.4. TOE の論理的範囲

以下に TOE のセキュリティ機能と基本機能を記述する。

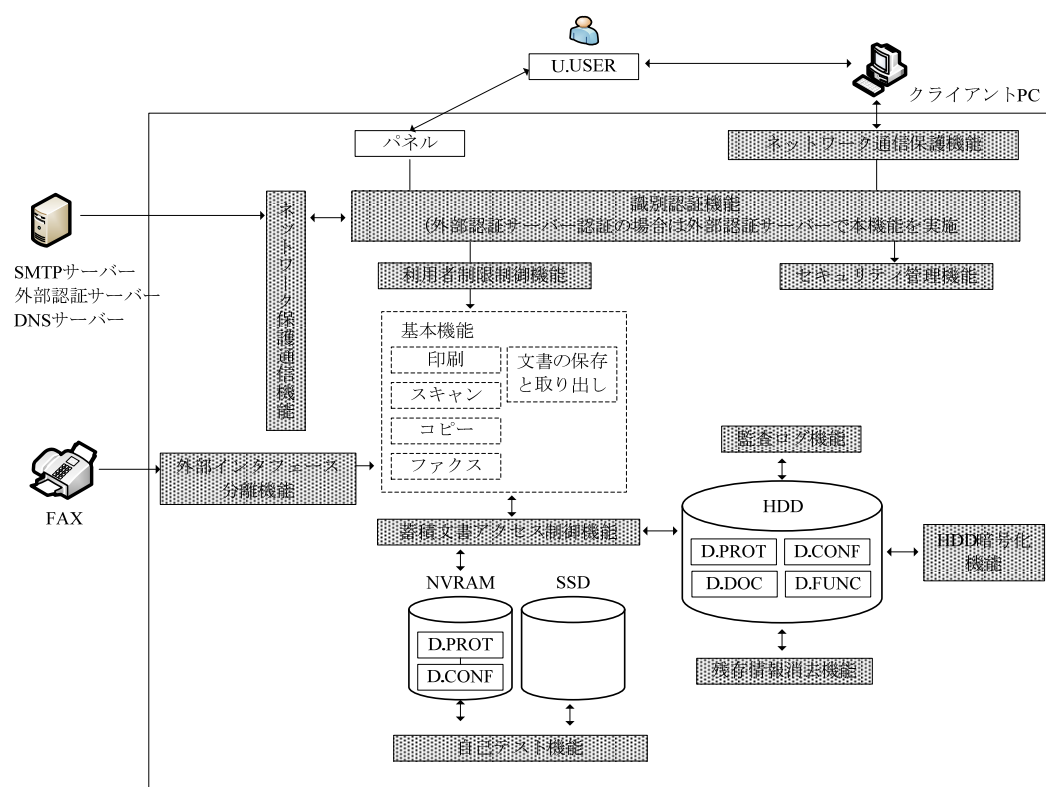


図 1-3 TOE の論理的範囲

1.4.4.1. 基本機能

以下に、TOEの基本機能を記述する。

(1) 印刷機能

クライアントから LAN を経由して受信した印刷データおよび USB インタフェースから受信した印刷データを印刷する機能。

(2) スキャン機能

一般利用者による操作パネルからの操作によって、文書（紙）を読み取って文書ファイルを生成する機能。

(3) コピー機能

一般利用者による操作パネルからの操作によって、文書（紙）を読み取って読み取った画像を複写印刷する機能。

(4) ファクス機能

紙文書を読み込んで外部ファクスに送信する機能（ファクス送信機能）および外部ファクスから文書を受信する機能（ファクス受信機能）。

- ファクス送信機能

紙文書およびファクス送信文書を電話回線から外部のファクス装置に送信する機能。
紙文書は操作パネルからの操作によってスキャンしファクス送信する。

- ファクス受信機能

外部ファクスから電話回線を介して文書を受信する機能。

(5) 文書の保存と取り出しの機能

TOE 内に文書を**保存**し、**保存**した文書を取り出す機能。印刷データやスキャン機能によって生成される文書ファイル、ファクス受信した文書なども保存と取り出しの対象となる。

(6) 共有メディアインタフェース機能

TOE の利用者がクライアント PC から TOE をリモート操作するための機能。ガイダンスにしたがって指定の Web ブラウザやアプリケーション等をインストールし、TOE とは LAN 経由で接続する。

1.4.4.2. セキュリティ機能

以下に、TOEのセキュリティ機能を記述する。

(1) 識別認証機能

TOE を利用しようとする者が TOE の許可利用者であるかどうかをユーザー名とパスワードによって検証し、TOE の許可利用者であることが確認できた場合に TOE の利用を許可する機能。検証方法には本体認証（管理者と一般利用者）と外部サーバー認証（一般利用者のみ）があり、管理者があらかじめ設定した方式で認証する。

本機能には、操作パネルからパスワードを入力する際にパスワードをダミー文字で表示する機能が含まれる。さらに、連続した認証失敗回数が設定値に達した場合に認証機能をロックするロック機能、パスワードの品質を確保するため管理者があらかじめ設定したパスワードの最小桁等の条件を満たしたパスワードだけを登録する機能が本機能に含まれる。

(2) 保存文書アクセス制御機能

識別認証機能で認証された TOE の許可利用者に対して、その利用者の役割に対して与えられた権限または利用者毎に与えられた権限に基づいて**保存**文書への操作を許可する機能。

(3) 利用者制限制御機能

識別認証機能で認証された TOE の許可利用者に対して、その利用者の役割に対して与えられた操作権限または利用者毎に与えられた操作権限に基づいて、印刷機能、スキャン機能、コピー機能、ファクス機能、文書の保存と取り出し等の機能、共有メディアインタフェース機能の操作を許可する機能。および、実行中のジョブに含まれる**保存**文書以外の文書への操作の制御をする機能。

(4) HDD暗号化機能

HDD に記録されているデータを漏洩から保護するために、それらを暗号化する機能。

(5) 監査ログ機能

TOE の使用およびセキュリティに関連する事象（以下、監査事象という）のログを日時情報等とともに監査ログとして記録し、記録した監査ログを監査できる形式で提供する機能。監査ログは TOE 内の HDD に格納するが、格納領域が満杯になった場合は管理者による設定にしたがって、ジョブの受付停止または最も古くに格納された監査記録へ上書きを行う。さらに、記録した監査ログは管理者だけに読み出し、削除の操作を許可する。

(6) 残存情報消去機能

TOE 内の削除された文書、一時的な文書あるいはその断片に対して、特定のデータを上書きすることにより、残存情報の再利用を不可能とする機能。

(7) ネットワーク通信保護機能

LAN 利用時にネットワーク上の盗聴による情報漏えいを防止する機能。クライアント PC と mfp の間の通信データ、外部認証サーバー、DNS サーバー、SMTP サーバーと mfp の間の通信データを暗号化する。

(8) 自己テスト機能

TSF 実行コードの完全性及び、暗号化ワードの完全性を mfp 起動時に検証し、全体制御機能の正常動作を実証する機能。

(9) セキュリティ管理機能

識別認証機能で認証された TOE の許可利用者に対して、その利用者の役割に対して与えられた権限または利用者毎に与えられた権限に基づいて TSF データに対する操作に関する制御をおこなう機能。

(10) 外部インタフェース分離機能

USB インタフェースを含む外部インタフェースからの入力をそのまま Shared-medium Interface へ転送することができないようにし、また、電話回線から LAN への侵入を防止する機能。電話回線については入力情報をファクス受信のみに限定することにより電話回線からの侵入を防止し、受信ファクスの転送を禁止することにより電話回線から LAN への侵入を防止する。

1.4.4.3. 制限

以下に、禁止される機能ならびに使用できない機能を記述する。

- (1) 認証&プリント以外のプリント機能（プリント機能は認証&プリントに制限される）
- (2) インターネットFAX
- (3) FTP送信、SMB送信、WebDAV送信、SNMP機能、LPD設定、RAW印刷

※(1)は、セキュリティ強化設定が有効な場合、禁止される機能である。

(2)は、セキュリティ強化設定が有効な場合、禁止される機能であるが、管理者のみに変更が可能な機能である。

(3)は、管理者のみに変更が可能な機能である。

1.4.5. TOE の利用者

TOE の利用者 (U.USER) は、以下のように分類される。

Table 1-1 Users

Designation	Definition
U.USER (許可利用者)	Any authorized User.
U.NORMAL (一般利用者)	A User who is authorized to perform User Document Data processing functions of the TOE.
U.ADMINISTRATOR (管理者)	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

1.4.6. 保護資産

保護資産は、User Data, TSF Data, Functionsである。

1.4.6.1. User Data

User Data は許可利用者が作成するか、許可利用者のために作成され、TOE セキュリティ機能の操作に影響を与えないデータである。User Data は以下のように分類される。

Table 1-2 User Data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

1.4.6.2. TSF Data

TSF Data は TOE が作成するか、TOE 用に作成されたデータであり、TOE の操作に影響を与えるデータである。TSF Data は以下のように分類される。

Table 1-3 TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

本 TOE で扱う TSF Data を以下に示す。

Table 1-4 TSF Data

Designation	Definition
D.PROT	オートリセット時間 自動ログアウト時間 アクセス制御にかかわるデータ（認証失敗回数等） 外部サーバー認証設定データ 日時情報 ネットワーク設定（SMTPサーバーのIPアドレス、ポート番号等、mfpのIPアドレス等） 送信宛先設定（メールによる送信の宛先等） パスワード規約 Admin ID User ID Permission Role Allocation Role FAXIN Box Word
D.CONF	ログインパスワード 暗号化ワード 監査ログ

1.4.6.3. Functions

2.3.2 SFR Package functions に示す機能。

1.4.7. 用語

本 ST で使用する用語の意味を定義する。

Table 1-5 用語

Designation	Definition
Allocation Role	一般利用者に関連付けられる属性。mfpの機能を実行する際に参照される。
Copy Role	コピーを実行できる役割。
Data Administrator	クライアントPCから管理者設定を行うためのアプリケーションソフト。

DSR Role	データのHDDへの保存、HDDに保存されているデータの読み出し、削除ができる役割。
Fax Role	ファクス機能を実行できる役割。
FTP送信	スキャンしたデータを、コンピューターで扱えるファイルに変換して、FTPサーバーにアップロードする機能。
HDDデータ上書き削除機能	HDD上のデータを上書き削除する機能。
HDDデータ上書き削除機能の動作設定機能	HDDデータ上書き削除機能において使用する削除方式（消去方式）を設定する機能。
Panel Operation	操作パネルからログインし、操作パネルからTOEを操作している状態。
Permission Role	mfpの機能に関連付けられる属性。
Print Role	クライアントPCからプリントを実行できる役割。
Scan Role	スキャンを実行できる役割。
SMB送信	スキャンしたデータを、コンピューターで扱えるファイルに変換して、コンピューターやサーバーの共有フォルダーへ送信する機能。
User Role	プリント、スキャン、コピー、ファクス、文書ファイルの保存といった機能を実行する際に必要な役割。
Web Connection	ネットワーク上のコンピューターでWebブラウザを起動しMFPの設定変更や状態確認をするための機能。
WebDAV送信	スキャンしたデータを、コンピューターで扱えるファイルに変換して、WebDAVサーバーにアップロードする機能。
遠隔診断機能	FAX公衆回線口やE-mailといった接続方式を利用して、コニカミノルタ株式会社が製造するmfpのサポートセンターと通信し、mfpの動作状態、印刷数等の機器情報を管理する。また必要に応じて適切なサービス（追加トナーの発送、課金請求、故障診断からサービスエンジニアの派遣など）を提供する。
オートリセット	ログイン中に、予め設定されたオートリセット時間でアクセスがなかった場合に自動的にログアウトする機能。
オートリセット時間	管理者が設定する時間。この時間が経過すると自動的にログアウトする。
ジョブ	ハードコピー装置に送出される文書処理タスク。単一の処理タスクは1本以上の文書を処理できる。
セキュリティ強化設定	セキュリティ機能のふるまいに関係する設定をセキュアな値に一括設定しその設定を維持する機能。この機能が有効になっていることによりネットワークを介したTOEの更新機能、遠隔診断機能による設定変更などの利用が禁止され、または利用の際に警告画面が表示されるほか、設定値の変更の際にも警告画面が表示される。
プリントジョブ投入機能	TOEがクライアントPCから送信されたユーザーID、ログインパスワード、印刷データを受け入れる機能。ユーザーID、ログインパスワードによる識別認証が成功した場合のみ印刷データを受け入れる。
ユーザーID (User ID)	一般利用者にあてられている識別子。TOEはその識別子により利用者を特定する。
管理者ID (Admin ID)	管理者にあてられている識別子。管理者IDはTOEに組込まれているIDであり、そのIDに対する操作は提供されていない。
ユーザー管理機能	ユーザーの登録／削除、権限の付与／削除／変更を行う機能。
ユーザー認証機能	TOEの利用者を認証する機能。 本体認証（INTERNALLY AUTHENTICATION）と外部サーバー認証

	(EXTERNALLY AUTHENTICATION) の2種類がある。 管理者は本体認証のみで認証される
ユーザー認証の管理機能	認証方式 (本体認証/外部サーバー認証) の設定を行う機能。
ログイン	TOEにおいて、ユーザーIDとログインパスワードによって識別認証を実行すること。
ログインパスワード (LOGIN PASSWORD)	TOEにログインするためのパスワード。
暗号化ワード	HDDの暗号化において使用する暗号鍵の生成において使用するデータ。TOEは暗号化ワードを使用して暗号鍵を生成する。
外部サーバー認証設定データ	外部認証サーバーに関する設定データ (外部サーバーが所属するドメイン名などを含む)。
監査ログ管理機能	監査ログ満杯時の動作の設定や、監査ログを読み出し・削除等を行う機能。
監査ログ機能	監査ログを取得する機能。
高信頼チャネル機能	LANを経由してやり取りするデータを暗号化して保護する機能
高信頼チャネル管理機能	高信頼チャネル機能の実行のほか、SSL/TLSサーバー証明書や暗号方式の管理を行う機能。
残存情報消去機能	HDDデータ上書き削除機能によりHDD上のデータを削除する機能。
日時情報	日時の情報。監査対象事象が発生した場合、この日時情報が監査ログに記録される。
自動ログアウト時間	管理者が設定する時間。この時間が経過すると自動的にログアウトする。Web Connectionが対象。
セッションの自動終了機能	セッションを自動的に終了する機能。 操作パネル、Web Connectionについてそれぞれ一定時間操作がおこなわれないとセッションを自動的に終了する。
認証&プリント機能 (AUTH PRINT)	ネットワーク上のコンピューターから送信されたユーザー名、パスワードを伴う文書をプリント指示された文書として保存する機能。
TOEの状態確認および表示等の設定	利用者は識別認証が成功する前にレポート出力 (設定情報リスト、統計ページ、フォントリストなど)、消耗品残量表示、カウンタ表示の状態確認、およびタッチパネル輝度調整、ページ印字位置設定などの設定をすることができる。
全体制御機能	この機能は、mfp全体を制御する機能であり、監査ログ機能、HDD暗号化機能、保存文書アクセス制御機能、利用者制限制御機能、残存情報消去機能、識別認証機能、外部インタフェース分離機能、自己テスト機能、セキュリティ管理機能、ネットワーク通信保護機能が含まれる。
FAXIN Box Word	強制メモリ受信文書にアクセスするために必要な情報であり、管理者によって設定される。

2. Conformance claims

2.1. CC Conformance claims

本STは、以下のCommon Criteria（以降、CCと記す）に適合する。

CC version : Version 3.1 Release 4
CC conformance : CC Part 2 extended, CC Part 3 conformant
Assurance level : EAL2 augmented by ALC_FLR.2

2.2. PP claim

本STは、以下のPPに適合する。

PP identification : IEEE Std 2600.2-2009
PP Title : 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B
PP registration : BSI-CC-PP-0058-2009
PP version : 1.0
Date : March 2009

2.3. Package claim

本STは、以下のSFR Packageに適合する。

- 2600.2-PRT 適合
- 2600.2-SCN 適合
- 2600.2-CPY 適合
- 2600.2-FAX 適合
- 2600.2-DSR 適合
- 2600.2-SMI 適合

2.3.1. SFR package reference

Title : 2600.2-PRT SFR Package for Hardcopy Device Print Functions, Operational Environment B

Package version : 1.0

Date : March 2009

Title : 2600.2-SCN SFR Package for Hardcopy Device Scan Functions, Operational Environment B

Package version : 1.0

Date : March 2009

- Title : 2600.2-CPY SFR Package for Hardcopy Device Copy Functions, Operational Environment B
 Package version : 1.0
 Date : March 2009
- Title : 2600.2-FAX SFR Package for Hardcopy Device Fax Functions, Operational Environment B
 Package version : 1.0
 Date : March 2009
- Title : 2600.2-DSR SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment B
 Package version : 1.0
 Date : March 2009
- Title : 2600.2-SMI SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
 Package version : 1.0
 Date : March 2009

2.3.2. SFR Package functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-1.

Table 2-1 SFR Package functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.3.3. SFR Package attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that

depend on the function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-2.

Table 2-2 SFR Package attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a Shared-medium interface.

2.4. PP Conformance rationale

2.4.1. PP の TOE 種別との一貫性主張

PP が対象とする製品の種別は、ハードコピー装置(以下、HCDと言う)である。HCDは、ハードコピー文書をデジタルフォームに変換するか(スキャン)、デジタル文書をハードコピーフォームに変換するか(印刷)、電話回線を介してハードコピー文書を送信するか(ファクス)、ハードコピー文書の複製を作成する(コピー)するために使用する製品である。

HCDは目的に応じて多数の異なる構成で実装され、機能を拡張するためにハードディスクドライブや他の不揮発性記憶システム、ドキュメントサーバー機能などを追加しているものもある。

本 TOE の種別は mfp である。mfp は、追加装置も含めて HCD が持つ装置を備え、HCD が搭載する機能を搭載している。よって、本 TOE 種別は PP の TOE 種別と一貫している。

2.4.2. PP のセキュリティ課題とセキュリティ対策方針との一貫性主張

本STはPPのセキュリティ課題に加えOSPとObjectivesを各1つ追加しているがPPとは一貫している。その理由を記載する。

STで追加しているOSPはP.HDD.CRYPTOである。これはHDDに記録されるデータの暗号化を求めるものであり運用環境にかかる制約をあたえるものではなくTOEを制約するものである。またSTで追加しているObjectives (O.HDD.CRYPTO) は追加したOSPに対応するものでこれも運用環境にかかる制約をあたえるものではなくTOEを制約するものである。したがってSTはTOEに対してPPと同等以上の制限を課し、TOEの運用環境に対してはPPと同等の制限を課しており、PPに対して同等またはより制限的であるという条件を満たす。

2.4.3. PP のセキュリティ要件との一貫性主張

本 TOE の SFR は、Common Security Functional Requirements と 2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-FAX、2600.2-DSR、2600.2-SMI からなる。

Common Security Functional Requirements は、PP が指定する必須 SFR であり、2600.2-PRT、2600.2-SCN、2600.2-CPY、2600.2-FAX、2600.2-DSR、2600.2-SMI は PP が指定する SFR Package から選択したものである。

本 ST のセキュリティ要件は、PP のセキュリティ要件に対して追加、具体化している箇所があるが、PP とは一貫している。以下に、追加、具体化している箇所と、それらが PP と一貫している理由を記載する。

Common Access Control SFP

本 TOE では D.FUNC の Modify を行うことはできない。これは PP より制限的なアクセス制御である。

PP は+FAXIN の属性をもつ D.DOC の Delete、および D.FUNC の Delete に関するアクセス制御を定義しているが、TOE が受信中の FAX 通信のキャンセルは管理者のみが可能であり、これにより受信中の FAX の D.DOC、D.FUNC は削除される。しかしながらこれは D.DOC、D.FUNC の Delete を意図した処理ではなく通信キャンセルに伴う Delete であり、受信が完了した後は FAX Access Control SFP の対象となり保護されることから PP の要求を損なうものではない。また受信が完了した後、+FAXIN の属性をもつ D.DOC、および D.FUNC は全て+DSR として保存される。それらは DSR Access Control SFP の対象となり保護されることから、PP が指定するセキュリティ要件の内容を変更するものではない。

さらに、PP は+DSR の属性をもつ D.DOC の Delete、および D.FUNC の Delete に関するアクセス制御を定義しているが、本 TOE では、D.DOC の具体化に伴い、DSR Access Control SFP の中で定義していることから、PP のアクセス制御に抵触するものではない。

FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4(1)、FAU_STG.4(2)の追加

本 TOE が監査ログを保持管理するために、PP APPLICATION NOTE 5.および PP APPLICATION NOTE 7.に従い、FAU_SAR.1、FAU_SAR.2、FAU_STG.1、FAU_STG.4(1)、FAU_STG.4(2)を追加する。

FCS_CKM.1、FCS_COP.1、FIA_SOS.1(3)の追加

本 TOE は Objectives として O.HDD.CRYPTO を追加しており、それにともなって FCS_CKM.1、FCS_COP.1、FIA_SOS.1(3)を追加するが、これは、PP が指定するセキュリティ要件の内容を変更するものではない。

FIA_AFL.1、FIA_SOS.1(1)、FIA_SOS.1(2)、FIA_UAU.6、FIA_UAU.7 の追加

本体認証は本 TOE が実装する機能である。そこで、PP APPLICATION NOTE 38.に従い、FIA_AFL.1、FIA_SOS.1(1)、FIA_SOS.1(2)、FIA_UAU.6、FIA_UAU.7 を追加する。

FMT_MOF.1 の追加

TOE はセキュリティ強化設定を有効にした状態で運用することをそのガイダンスで求めており、セキュリティ強化設定の変更を U.ADMINISTRATOR に制限することで、不正にセキュリティ強化設定が改変されることを防止しているものであり、PP が指定するセキュリティ要件の内容を変更するものではない。

ユーザー認証機能、HDD データ上書き削除機能、監査ログ機能、高信頼チャネル機能の管理、ならびにユーザー管理機能の管理を U.ADMINISTRATOR に制限することで、管理機能が不正に実行されることを防止しているものであり、PP が指定するセキュリティ要件の内容を変更するものではない。

上述の通り、いくつかの SFR を追加したが、PP では監査のレベルが定義されていないため、これらの SFR に対する監査ログは FAU_GEN.1 では定義しない。

3. Security Problem Definition

3.1. Threats agents

This security problem definition addresses threats posed by four categories of threat agents:

- a) Persons who are not permitted to use the TOE who may attempt to use the TOE.
- b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
- c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.
- d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Protection Profile address the threats posed by these threat agents.

3.2. Threats to TOE Assets

This section describes threats to assets described in clause in 1.4.6.

Table 3-1 Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC_REST.DIS	D.DOC	User Document Data at rest (stored) in the TOE may be disclosed to unauthorized persons
T.DOC_REST.ALT	D.DOC	User Document Data at rest (stored) in the TOE may be altered by unauthorized persons
T.FUNC_REST.ALT	D.FUNC	User Function Data at rest (stored) in the TOE may be altered by unauthorized persons

Table 3-2 Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.3. Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 3-3 Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be

	authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.CRYPTO	The Data stored in an HDD must be encrypted to improve the secrecy.

3.4. Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Protection Profile are based on the condition that all of the assumptions described in this section are satisfied.

Table 3-4 Assumptions for the TOE

Assumptions	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4. Security Objectives

4.1. Security Objectives for the TOE

This section describes the Security Objectives that the TOE shall fulfill.

Table 4-1 Security Objectives for the TOE

Objective	Definition
O.DOC_REST.NO_DIS	The TOE shall protect User Document Data at rest (stored) in the TOE from unauthorized disclosure.
O.DOC_REST.NO_ALT	The TOE shall protect User Document Data at rest (stored) in the TOE from unauthorized alteration.
O.FUNC_REST.NO_ALT	The TOE shall protect User Function Data at rest (stored) in the TOE from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.
O.HDD.CRYPTO	The TOE shall encrypt data at the time of storing it to an HDD.

4.2. Security Objectives for the IT environment

This section describes the Security Objectives that must be fulfilled by IT methods in the IT environment of the TOE.

Table 4-2 Security Objectives for the IT environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3. Security Objectives for the non-IT environment

This section describes the Security Objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

Table 4-3 Security Objectives for the non-IT environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer's guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4. Security Objectives rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 4-4 Completeness of Security Objectives

Threats, policies, And assumptions	Objectives																				
	O.DOC_REST.NO_DIS	O.DOC_REST.NO_ALT	O.FUNC_REST.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT_REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	
T.DOC_REST.DIS	✓						✓	✓													
T.DOC_REST.ALT		✓					✓	✓													
T.FUNC_REST.ALT			✓				✓	✓													
T.PROT.ALT				✓			✓	✓													
T.CONF.DIS					✓		✓	✓													
T.CONF.ALT						✓	✓	✓													
P.USER.AUTHORIZATION							✓	✓													
P.SOFTWARE.VERIFICATION									✓												
P.AUDIT.LOGGING										✓		✓	✓	✓							
P.INTERFACE.MANAGEMENT															✓		✓				
P.HDD.CRYPTO											✓										
A.ACCESS.MANAGED																✓					
A.ADMIN.TRAINING																		✓			
A.ADMIN.TRUST																				✓	
A.USER.TRAINING																					✓

Table 4-5 Sufficiency of Security Objectives

Threats, Policies, and assumptions	Summary	Objectives and rationale
T.DOC_REST.DIS	User Document Data at rest in the TOE may be disclosed to unauthorized persons.	O.DOC_REST.NO_DIS protects D.DOC at rest in the TOE from unauthorized disclosure. O.USER.AUTHORIZED establishes user identification and authentication as the basis for T.DOC_REST.DIS authorization.

		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC_REST.ALT	User Document Data at rest in the TOE may be altered by unauthorized persons.	O.DOC_REST.NO_ALT protects D.DOC at rest in the TOE from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for T.DOC_REST.ALT authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC_REST.ALT	User Function Data at rest in the TOE may be altered by unauthorized persons.	O.FUNC_REST.NO_ALT protects D.FUNC at rest in the TOE from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for T.FUNC_REST.ALT authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.

		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events and prevents unauthorized disclosure or alteration.
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion, and modifications.
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
P.HDD.CRYPTO	Cryptographic operation will be controlled by TOE.	O.HDD.CRYPTO encrypts data stored in HDD by TOE.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures.	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5. Extended components definition (APE_ECD)

This Protection Profile defines components that are extensions to Common Criteria 3.1 Revision 2, Part 2. These extended components are defined in the Protection Profile but are used in SFR Packages and, therefore, are employed only in TOEs whose STs conform to those SFR Packages.

5.1. FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces	1
---------------	--	---

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: **FPT_FDI_EXP.1**

The following actions could be considered for the management functions in FMT:

- a) Definition of the role(s) that are allowed to perform the management activities
- b) Management of the conditions under which direct forwarding can be allowed by an administrative role
- c) Revocation of such an allowance

Audit: **FPT_FDI_EXP.1**

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external

interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 **Restricted forwarding of data to external interfaces**

Hierarchical to: No other components

Dependencies: **FMT_SMF.1** Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

6. Security Requirements

本章では、セキュリティ要件について記述する。

6.1. Security functional requirements

この章では、4.1 章で規定されたセキュリティ対策方針を実現するための、TOE のセキュリティ機能要件を記述する。なお、セキュリティ機能要件は、CC Part2 に規定のセキュリティ機能要件から、引用する。CC Part2 に規定されていないセキュリティ機能要件は、5 章を参照。

<セキュリティ機能要件“操作”の明示方法>

以下の機能エレメントの記述の中において、**ボールド**で示される表記は、PP で操作完了または詳細化したことを示す。**イタリック且つボールド**で示される表記は、本 ST で“割付”、または“選択”されていることを示す。アンダーラインで示される原文の直後に**括弧書きでイタリック且つボールド**で示される表記は、アンダーラインされた原文箇所が本 ST で“詳細化”されていることを示す。ラベルの後に括弧付けで示される番号は、当該機能要件が本 ST で“繰返し”されて使用されていることを示す。

また、PP で定義されたセキュリティ機能要件のコンポーネントは**ボールド**で、ST で追加されたコンポーネントは**イタリック且つボールド**で示す。

6.1.1. Class FAU: Security audit

FAU_GEN.1 Audit data generation

Hierarchical to : No other components

Dependencies : FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions; and
- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 6-1; [assignment: *other specifically defined auditable events*]** [selection, choose one of: *minimum, basic, detailed, not specified*]
not specified
[assignment: *other specifically defined auditable events*]

なし

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 6-1: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*]
[assignment: *other audit relevant information*]

なし

Table 6-1 Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information	Details
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required	<ul style="list-style-type: none"> ・ログインの成功 ・ログインの失敗
The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	FIA_AFL.1	Minimum	None required	<ul style="list-style-type: none"> ・認証の停止 ・通常状態への復帰
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available	<ul style="list-style-type: none"> ・ログインの成功 ・ログインの失敗
Failure of reauthentication	FIA_UAU.6	Minimum	None required	<ul style="list-style-type: none"> ・再認証の失敗
Use of the management functions	FMT_SMF.1	Minimum	None required	<ul style="list-style-type: none"> ・管理機能の使用
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required	役割としてのユーザーのグループは存在しないので記録はない。
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required	<ul style="list-style-type: none"> ・通信の失敗
Changes to the time	FPT_STM.1	Minimum	None required	<ul style="list-style-type: none"> ・日時の変更
Locking of an interactive session by the	FTA_SSL.3	Minimum	None required	<ul style="list-style-type: none"> ・対話セッションの終了

session locking mechanism				
---------------------------	--	--	--	--

FAU_GEN.2 User identity association

Hierarchical to : No other components
 Dependencies : FAU_GEN.1 Audit data generation
 FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to : No other components
 Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.
 [assignment: *authorised users*]

U.ADMINISTRATOR

[assignment: *list of audit information*]

Table 6-1 に示す監査ログ

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to : No other components
 Dependencies : FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components
 Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

[selection, choose one of: *prevent, detect*]

prevent

FAU_STG.4(1) Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss

- Dependencies : FAU_STG.1 Protected audit trail storage
- FAU_STG.4.1(1) The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full(監査証拠が満杯になった時の動作が「上書き禁止」に設定された状態で、監査証拠が満杯になった場合).
- [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”]
- prevent audited events, except those taken by the authorised user with special rights**
- [assignment: other actions to be taken in case of audit storage failure]
- ・管理者による監査ログの削除
 - ・管理者による監査ログのエクスポート (エクスポートにより TOE 上の監査ログは削除される)
 - ・管理者による「上書き禁止」から「上書き許可」への設定変更

FAU_STG.4(2) Prevention of audit data loss

- Hierarchical to : FAU_STG.3 Action in case of possible audit data loss
- Dependencies : FAU_STG.1 Protected audit trail storage
- FAU_STG.4.1(2) The TSF shall [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full(監査証拠が満杯になった時の動作が「上書き許可」に設定された状態で、監査証拠が満杯になった場合).
- [selection, choose one of: “ignore audited events”, “prevent audited events, except those taken by the authorised user with special rights”, “overwrite the oldest stored audit records”]
- overwrite the oldest stored audit records**
- [assignment: other actions to be taken in case of audit storage failure]
- なし

6.1.2. Class FCS: Cryptographic support

FCS_CKM.1 Cryptographic key generation

- Hierarchical to : No other components.
- Dependencies : [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
- FCS_CKM.1.1 The TSF shall generate cryptographic keys (**cryptographic keys for HDD encryption**) in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: cryptographic key generation algorithm]

refer to Table 6-2

[assignment: cryptographic key sizes]

refer to Table 6-2

[assignment: list of standards]

refer to Table 6-2

Table 6-2 Cryptographic key algorithm key size

list of standards	cryptographic key generation algorithm	key sizes
FIPS180-3	SHA-256	・ 256bit

FCS_COP.1 Cryptographic operation

Hierarchical to : No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
 FDP_ITC.2 Import of user data with security attributes, or
 FCS_CKM.1 Cryptographic key generation]
 FCS_CKM.4 Cryptographic key destruction

..FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following:

[assignment: list of standards].

[assignment: list of cryptographic operations]

refer to Table 6-3

[assignment: cryptographic algorithm]

refer to Table 6-3

[assignment: cryptographic key sizes]

refer to Table 6-3

[assignment: list of standards]

refer to Table 6-3

Table 6-3 Cryptographic operations algorithm key size standards

Standard	cryptographic algorithm	key sizes	cryptographic operations
FIPS PUB197	AES	・ 256 bit	HDD の暗号化

6.1.3. Class FDP: User data protection

FDP_ACC.1(a) Subset access control

Hierarchical to : No other components

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the Common Access Control SFP in Table 17 (Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9) on the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 17 (the list of users as subjects, objects, and operations among subjects and objects covered by the Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9).

Table 6-4 Common Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+PRT +SCN +CPY +FAXOUT	User ID	Delete	U.NORMAL	User ID	User ID が一致する場合のみ操作を許可する。
D.FUNC	+PRT +SCN +CPY +FAXOUT	User ID	Delete	U.NORMAL	User ID	User ID が一致する場合のみ操作を許可する。

Table 6-5 PRT Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+PRT	User ID	Read	U.NORMAL	User ID	User ID が一致するもののみ操作を許可する。

Table 6-6 SCN Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+SCN	User ID	Read	U.NORMAL	User ID	User ID が一致するもののみ操作を許可する。

Table 6-7 CPY Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+CPY	User ID	Read	PP に従い、アクセス制御制限を特定しない。		

Table 6-8 FAX Access Control SFP

Object	Attribute	Operation(s)	Subject	Subject	Access control rule
--------	-----------	--------------	---------	---------	---------------------

	Function Attribute	Object Attribute			Attribute	
D.DOC	+ FAXIN	FAXIN Box Word	Read	U.NORMAL	FAXIN Box Word	FAXIN Box Word が一致する場合操作を許可する。
D.DOC	+FAXOUT	User ID	Read	U.NORMAL	User ID	User ID が一致するもののみ操作を許可する。

Table 6-9 DSR Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+DSR (+SCN からの保存)	User ID	Read Delete	U.NORMAL	User ID	User ID が一致するもののみ操作を許可する。
	+DSR (+FAXIN からの保存)	FAXIN Box Word	Read Delete	U.NORMAL	FAXIN Box Word	FAXIN Box Word が一致する場合操作を許可する。
D.FUN C	+DSR (+SCN からの保存)	User ID	Delete	U.NORMAL	User ID	User ID が一致するもののみ操作を許可する。
	+DSR (+FAXIN からの保存)	FAXIN Box Word	Delete	U.NORMAL	FAXIN Box Word	FAXIN Box Word が一致する場合操作を許可する。

なお、Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9 では、PP APPLICATION NOTE 19.に従い、「Create」操作に関するアクセス制御規則は指定しない。

FDP_ACC.1(b) Subset access control

Hierarchical to : No other components

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP (TOE Function Access Control SFP in Table 6-10)** on **users as subjects, TOE functions as objects, and the right to use the functions as operations (the list of users as subjects, objects, and operations among subjects and objects covered by the TOE Function Access Control SFP in Table 6-10)**.

Table 6-10 TOE Function Access Control SFP

Object (TOE Function)	Object Attribute	Operation(s)	Subject	Subject Attribute	Access control rule
F.PRT	Permission	実行	U.NORMAL	Allocation Role	Subject の Allocation

	Role				Role が Object の Permission Role を含んでいる場合、機能の実行を許可する。
F.SCN	Permission Role	実行	U.NORMAL	Allocation Role	Subject の Allocation Role が Object の Permission Role を含んでいる場合、機能の実行を許可する。
F.CPY	Permission Role	実行	U.NORMAL	Allocation Role	Subject の Allocation Role が Object の Permission Role を含んでいる場合、機能の実行を許可する。
F.FAX	Permission Role	実行	U.NORMAL	Allocation Role	Subject の Allocation Role が Object の Permission Role を含んでいる場合、機能の実行を許可する。
F.DSR	Permission Role	実行	U.NORMAL	Allocation Role	Subject の Allocation Role が Object の Permission Role を含んでいる場合、機能の実行を許可する。

FDP_ACF.1(a) Security attribute based access control

: Hierarchical to : No other components
 Dependencies : FDP_ACC.1 Subset access control
 FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17 (Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 17, and for each, the indicated security attributes in Table 17 (the list of users as subjects and objects controlled under the Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9 and for each, the indicated security attributes in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)**.

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 17 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects (rules specified in the Document Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects)**.

FDP_ACF.1.3(a) The TSF shall explicitly authorize access of subjects to objects based on the following

additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

[assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]

- ・ *U.ADMINISTRATOR* はすべての *D.DOC*、*D.FUNC* の *Delete* が可能
- ・ *U.ADMINISTRATOR* は +*FAXIN*、+*DSR* の属性をもつ *D.DOC* の *Read* が可能

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
なし

FDP_ACF.1(b) Security attribute based access control

Hierarchical to : No other components

Dependencies : FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** (*TOE Function Access Control SFP in Table 6-10*) to objects based on the following: **users and** [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*].

[assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]

the list of users as subjects and objects controlled under the TOE Function Access Control SFP in Table 6-10, and for each, the indicated security attributes in Table 6-10

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*].

[selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]

[assignment: *other conditions*]

Table 6-10

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **the user acts in the role U.ADMINISTRATOR:** [assignment: *other rules, based on security attributes, that explicitly authorise access of subjects to objects*].
[assignment: *other rules, based on security attributes, that explicitly authorise access of subjects to objects*].
なし

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules based on security attributes that explicitly deny access of subjects to objects*].
The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules based on security attributes that explicitly deny access of subjects to objects*].
なし

FDP_RIP.1 Subset residual information protection

Hierarchical to : No other components

Dependencies : No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC**, [assignment: *list of objects*].
[selection: *allocation of the resource to, deallocation of the resource from*]
deallocation of the resource from
[assignment: *list of objects*].
なし

6.1.4. Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components

Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *assignment: positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[selection: *assignment: positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]
an administrator configurable positive integer within [assignment: range of acceptable values]
[assignment: *range of acceptable values*]
3
[assignment: *list of authentication events*]
ログインパスワードによる認証

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*]
met
[assignment: *list of actions*]
ログインパスワードによる認証の停止
<通常復帰のための操作>
管理者の認証の場合: TOE の起動処理を行う。(起動処理から管理者認証の操作禁止解除時間を経過後に解除処理が行なわれる。)
それ以外の場合: 管理者による認証失敗回数の消去機能の実行

FIA_ATD.1 User attribute definition

Hierarchical to : No other components

Dependencies : No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].
[assignment: *list of security attributes*].
AdminID
User ID
Allocation Role
FAXIN Box Word

FIA_SOS.1(1) Verification of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that secrets (ログインパスワード (U.ADMINISTRATOR)) meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*]

- ・桁数 : 8桁以上
- ・文字種 : 95文字の中から選択可能
- ・規則 : ① 同一の文字だけで構成されていない。
② 変更する場合、変更後の値が現在設定されている値と合致しない。

FIA_SOS.1(2) Verification of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.1.1(2) The TSF shall provide a mechanism to verify that secrets (ログインパスワード (U.NORMAL)) meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*]

- ・桁数 : 8桁以上
- ・文字種 : 93文字の中から選択可能
- ・規則 : ① 同一の文字だけで構成されていない。
② 変更する場合、変更後の値が現在設定されている値と合致しない。

FIA_SOS.1(3) Verification of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.1.1(3) The TSF shall provide a mechanism to verify that secrets (暗号化ワード) meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*]

- ・桁数 : 20桁
- ・文字種 : 95文字の中から選択可能
- ・規則 : ① 同一の文字だけで構成されていない。
② 同一文字種のみで構成されていない。

FIA_UAU.1	Timing of authentication
	Hierarchical to : No other components
	Dependencies : FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [assignment: <i>list of TSF-mediated actions that do not conflict with access-controlled Functions of the TOE</i>] on behalf of the user to be performed before the user is authenticated. [assignment: <i>list of TSF-mediated actions that do not conflict with access-controlled Functions of the TOE</i>] ファクス受信 TOEの状態確認および表示等の設定
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.6	Re-authenticating
	Hierarchical to : No other components
	Dependencies : No dependencies
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions [assignment: <i>list of conditions under which re-authentication is required</i>]. [assignment: <i>list of conditions under which re-authentication is required</i>] 自身のログインパスワードの変更
FIA_UAU.7	Protected authentication feedback
	Hierarchical to : No other components
	Dependencies : FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [assignment: <i>list of feedback</i>] to the user while the authentication is in progress. [assignment: <i>list of feedback</i>] 入力された文字データ 1文字毎に秘匿文字の表示
FIA_UID.1	Timing of identification
	Hierarchical to : No other components
	Dependencies : No dependencies
FIA_UID.1.1	The TSF shall allow [assignment: <i>list of TSF-mediated actions that do not conflict with access-controlled Functions of the TOE</i>] on behalf of the user to be performed before the user is identified. [assignment: <i>list of TSF-mediated actions that do not conflict with access-controlled Functions of the TOE</i>] ファクス受信 TOEの状態確認および表示等の設定
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1	User-subject binding
	Hierarchical to : No other components
	Dependencies : FIA_ATD.1 User attribute definition
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: <i>list of user security attributes</i>]. [assignment: <i>list of user security attributes</i>]. AdminID User ID Allocation Role FAXIN Box Word
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [assignment: <i>rules for the initial association of attributes</i>]. [assignment: <i>rules for the initial association of attributes</i>] なし
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [assignment: <i>rules for the changing of attributes</i>]. [assignment: <i>rules for the changing of attributes</i>] なし

6.1.5. Class FMT: Security management

FMT_MOF.1	Management of security functions behaviour
	Hierarchical to : No other components
	Dependencies : FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i>] the functions [assignment: <i>list of functions</i>] to [assignment: <i>the authorised identified roles</i>]. [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i>] modify the behaviour of [assignment: <i>list of functions</i>] ・セキュリティ強化設定 ・ユーザー認証機能 ・HDD データ上書き削除機能 ・監査ログ機能 ・高信頼チャネル機能 ・ユーザー管理機能 [assignment: <i>the authorised identified roles</i>]. U.ADMINISTRATOR

FMT_MSA.1(a) Management of security attributes

- Hierarchical to : No other components
- Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17 (Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, and Table 6-9)**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

なし

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

Refer to Table 6-11, Table 6-12

[assignment: *list of security attributes*]

Refer to Table 6-11, Table 6-12

[assignment: *the authorized identified roles*]

Refer to Table 6-11, Table 6-12

Table 6-11 Management of Object Security Attribute

Access Control SFP	Object Security Attribute	Authorized Identified Roles	Operations
Common Access Control SFP PRT Access Control SFP SCN Access Control SFP CPY Access Control SFP FAX Access Control SFP (FAXOUT) DSR Access Control SFP (SCN)	User ID	Nobody	Any operation
FAX Access Control SFP (FAXIN) DSR Access Control SFP (FAXIN)	FAXIN Box Word	U.ADMINISTRATOR	登録 Modify

Table 6-12 Management of Subject Security Attribute

Access Control SFP	Subject Security Attribute	Authorized Identified Roles	Operations
Common Access Control SFP PRT Access Control SFP SCN Access Control SFP CPY Access Control SFP	User ID	U.ADMINISTRATOR	Delete Modify

FAX Access Control SFP (FAXOUT) DSR Access Control SFP (SCN)			
FAX Access Control SFP (FAXIN) DSR Access Control SFP (FAXIN)	FAXIN Box Word	Nobody	Any operation

FMT_MSA.1(b) Management of security attributes

- Hierarchical to : No other components
- Dependencies : [FDP_ACC.1 Subset access control, or
 FDP_IFC.1 Subset information flow control]
 FMT_SMR.1 Security roles
 FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP (TOE Function Access Control SFP in Table 6-10)**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

なし

[selection: *change_default, query, modify, delete, [assignment: other operations]*]

Refer to Table 6-13, Table 6-14

[assignment: *list of security attributes*]

Refer to Table 6-13, Table 6-14

[assignment: *the authorised identified roles*]

Refer to Table 6-13, Table 6-14

Table 6-13 Management of Subject Security Attribute

Access Control SFP	Subject Security Attribute	Authorized Identified Roles	Operations
TOE Function Access Control SFP	Allocation Role	U.ADMINISTRATOR	Delete Modify

Table 6-14 Management of Object Security Attribute

Access Control SFP	Object Security Attribute	Authorized Identified Roles	Operations
TOE Function Access Control SFP	Permission Role	Nobody	Any operation

FMT_MSA.3(a) Static attribute initialisation

Hierarchical to : No other components

Dependencies: : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17 (Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *access control SFP, information flow control SFP*]

なし

[selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

[assignment: *other property*]

refer to Table 6-15

FMT_MSA.3.2(a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

nobody

Table 6-15 Characteristics Static Attribute Initialization

Access Control SFP	Object	Function Attribute	Object Attribute	Default values for Object Security Attribute
Common Access Control SFP / PRT Access Control SFP /	D.DOC D.FUNC	+PRT +SCN +CPY +FAXOUT	User ID	オブジェクトを生成した U.NORMAL の User ID
SCN Access Control SFP / CPY Access Control SFP /	D.DOC D.FUNC	+DSR(+SCN からの保存)	User ID	オブジェクトを生成した U.NORMAL の User ID
FAX Access Control SFP / DSR Access Control SFP / DSR Access Control SFP	D.DOC D.FUNC	+FAXIN +DSR(+FAXIN からの保存)	FAXIN Box Word	FAXIN Box Word は、U.ADMINISTRATOR が設定した値を関連付ける

※Function Attribute はオブジェクトを生成する機能（プリント、スキャンなど）に対応して付与されるため同時に複数付与されることはない。

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to : No other components

Dependencies: : FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

- FMT_MSA.3.1(b) The TSF shall enforce the **TOE Function Access Control Policy (TOE Function Access Control SFP (TOE Function Access Control SFP in Table 6-10))**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP. [assignment: *access control SFP, information flow control SFP*]
なし
[selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[assignment: other property]
Refer to Table 6-16
- FMT_MSA.3.2(b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.
[assignment: *the authorized identified roles*]
nobody

Table 6-16 Characteristics Static Attribute Initialization

Object (TOE Function)	Object Attribute	Characteristics which restricts access only to Subject which any of the following attributes
F.PRT	Permission Role	Print Role
F.SCN	Permission Role	Scan Role
F.CPY	Permission Role	Copy Role
F.FAX	Permission Role	Fax Role-
F.DSR	Permission Role	DSR Role

FMT_MTD.1 Management of TSF data

Hierarchical to : No other components
Dependencies: : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

- FMT_MTD.1.1(a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]*].
[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
refer to Table 6-17
[assignment: *other operations*]
refer to Table 6-17
[assignment: *list of TSF data*]
refer to Table 6-17
[selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]*]
refer to Table 6-17
- FMT_MTD.1.1(b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete,*

clear, [assignment: other operations] the [assignment: list of TSF data associated with a U.NORMAL or TSF data associated with documents or jobs owned by a U.NORMAL] to [selection, choose one of: Nobody, [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated]].

refer to Table 6-18

Table 6-17 Operation of TSF Data

TSF Data	Authorized Identification Roles	Operations
U.NORMAL のログインパスワード	U.ADMINISTRATOR	登録
U.ADMINISTRATOR のログインパスワード	U.ADMINISTRATOR	Modify
暗号化ワード	U.ADMINISTRATOR	設定
日時情報	U.ADMINISTRATOR	Modify
オートリセット時間	U.ADMINISTRATOR	Modify
自動ログアウト時間	U.ADMINISTRATOR	Modify
認証失敗回数 (管理者以外)	U.ADMINISTRATOR	Clear
パスワード規約	U.ADMINISTRATOR	Modify
外部サーバー認証設定データ	U.ADMINISTRATOR	登録 Modify
ネットワーク設定	U.ADMINISTRATOR	登録 Modify
送信宛先設定	U.ADMINISTRATOR	登録 Modify
監査ログ	U.ADMINISTRATOR	Query Delete

Table 6-18 Operation of TSF Data

TSF Data	Authorized Identification Roles	Operations
U.NORMAL のログインパスワード	当該パスワードに関連付けられたユーザー (U.NORMAL) U.ADMINISTRATOR	Modify

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components

Dependencies: : No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[assignment: list of management functions to be provided by the TSF].

[assignment: list of management functions to be provided by the TSF]

refer to Table 6-19

Table 6-19 list of management functions

management functions
U.ADMINISTRATOR によるセキュリティ強化設定の管理機能
U.ADMINISTRATOR によるユーザー認証機能の管理機能
U.ADMINISTRATOR による HDD データ上書き削除機能の動作設定機能
U.ADMINISTRATOR による監査ログ管理機能
U.ADMINISTRATOR による高信頼チャンネル管理機能
U.ADMINISTRATOR によるユーザー管理機能*
U.NORMAL による自身のログインパスワードの変更機能
U.ADMINISTRATOR による自身のログインパスワードの変更機能
U.ADMINISTRATOR による暗号化ワードの設定機能
U.ADMINISTRATOR による日時情報の変更機能
U.ADMINISTRATOR によるオートリセット時間の変更機能
U.ADMINISTRATOR による自動ログアウト時間の変更機能
U.ADMINISTRATOR による外部サーバー認証設定データの登録・変更機能
U.ADMINISTRATOR による認証失敗回数（管理者以外）の消去機能
U.ADMINISTRATOR によるパスワード規約変更機能
U.ADMINISTRATOR によるネットワーク設定の登録・変更機能
U.ADMINISTRATOR による送信宛先の登録・変更機能
U.ADMINISTRATOR による FAXIN Box Word の登録・変更機能

※ユーザー管理機能には、U.ADMINISTRATOR による U.NORMAL のログインパスワードの管理、サブジェクトのセキュリティ属性の管理が含まれる。

FMT_SMR.1 Security roles

Hierarchical to : No other components
Dependencies: : FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR**, **U.NORMAL**, [selection: **Nobody**, [assignment: *the authorised identified roles*]].
[selection: **Nobody**, [assignment: *the authorised identified roles*]]
Nobody

FMT_SMR.1.2 The TSF shall be able to associate users with roles, **except for the role “Nobody” to which no user shall be associated.**

6.1.6. Class FPT: Protection of the TSF

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to : No other components
Dependencies: : FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface.**

FPT_STM.1	<p>Reliable time stamps</p> <p>Hierarchical to : No other components</p> <p>Dependencies: : No dependencies</p>
FPT_STM.1.1	TSF shall be able to provide reliable time stamps.
FPT_TST.1	<p>TSF testing</p> <p>Hierarchical to : No other components</p> <p>Dependencies: : No dependencies</p>
FPT_TST.1.1	<p>The TSF shall run a suite of self tests [selection: <i>during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions</i> [assignment: <i>conditions under which self test should occur</i>]] to demonstrate the correct operation of [selection: [assignment: <i>parts of TSF</i>], <i>the TSF</i>].</p> <p>[selection: <i>during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions</i> [assignment: <i>conditions under which self test should occur</i>]]</p> <p><i>during initial start-up</i></p> <p>[selection: [assignment: <i>parts of TSF</i>], <i>the TSF</i>]</p> <p><i>[assignment: parts of TSF]</i></p> <p>全体制御機能、HDD 暗号化機能 (暗号化ワード)</p>
FPT_TST.1.2	<p>The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: <i>parts of TSF</i>], <i>TSF data</i>].</p> <p>[selection: [assignment: <i>parts of TSF</i>], <i>TSF data</i>].</p> <p><i>[assignment: parts of TSF]</i></p> <p>暗号化ワード</p>
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.7. Class FTA: TOE access

FTA_SSL.3	<p>TSF-initiated termination</p> <p>Hierarchical to : No other components</p> <p>Dependencies: : No dependencies</p>
FTA_SSL.3.1	<p>The TSF shall terminate an interactive session after a [assignment: <i>time interval of user inactivity</i>].</p> <p>[assignment: <i>time interval of user inactivity</i>]</p> <ul style="list-style-type: none"> ・操作パネルの場合、最終操作および最終操作による処理が完了してからオートリセット時間によって決定される時間 ・Web Connection の場合、最終操作および最終操作による処理が完了してから自動ログアウト時間によって決定される時間 ・Data Administrator の場合、60 分 ・プリンタドライバーの場合、対話セッションはない

6.1.8. Class FTP: Trusted path/channels

FTP_ITC.1	Inter-TSF trusted channel
	Hierarchical to : No other components
	Dependencies: : No dependencies
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit the TSF, another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for communication of D.PROT, and D.CONF over any Shared-medium Interface.

6.2. Security assurance requirements

Table 6-20 lists the security assurance requirements for 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B, and related SFR packages, EAL 2 augmented by ALC_FLR.2.

Table 6-20 IEEE 2600.2 Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing—sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3. Security requirements rationale

6.3.1. Common security requirements rationale (SFR Package is included)

Table 6-21 and Table 6-22 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 6-21 Completeness of security requirements

SFRs	Objectives										
	O.DOC_REST.NO_DIS	O.DOC_REST.NO_ALT	O.FUNC_REST.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO
FAU_GEN.1										P	
FAU_GEN.2										P	
FAU_SAR.1										P	
FAU_SAR.2										P	
FAU_STG.1										P	
FAU_STG.4(1)										P	
FAU_STG.4(2)										P	
FCS_CKM.1											S
FCS_COP.1											P
FDP_ACC.1(a)	P	P	P								
FDP_ACC.1(b)							P				
FDP_ACF.1(a)	S	S	S								
FDP_ACF.1(b)							S				
FDP_RIP.1	P										
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1(1)							S				
FIA_SOS.1(2)							S				
FIA_SOS.1(3)											S
FIA_UAU.1							P	P			
FIA_UAU.6							S	S			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	P	P	S	S	
FIA_USB.1							P				
FMT_MOF.1	S	S	S	S	S	S	S	S	S	S	S
FMT_MSA.1(a)	S	S	S	P							
FMT_MSA.1(b)				P			S				
FMT_MSA.3(a)	S	S	S								
FMT_MSA.3(b)							S				
FMT_MTD.1				P	P	P					S
FMT_SMF.1	S	S	S	S	S	S	S	S	S	S	S

SFRs	Objectives										
	O.DOC_REST.NO_DIS	O.DOC_REST.NO_ALT	O.FUNC_REST.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO
FMT_SMR.1	S	S	S	S	S	S	S	S		S	S
FPT_FDI_EXP.1								P			
FPT_STM.1										S	
FPT_TST.1									P		
FTA_SSL.3							P	P			
FTP_ITC.1	P	P	P	P	P	P					

Table 6-22 Sufficiency of security requirements

Objectives	Description	SFRs	Purpose
O.DOC_REST.NO_DIS, O.DOC_REST.NO_ALT, O.FUNC_REST.NO_ALT	Protection of User Data at rest in the TOE from unauthorized disclosure or alteration	FDP_ACC.1(a)	Enforces protection by establishing an access control policy.
		FDP_ACF.1(a)	Supports access control policy by providing access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(a)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(a)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.DOC_REST.NO_DIS	Protection of User Document Data at rest in the TOE from unauthorized	FDP_RIP.1	Enforces protection by making residual data unavailable.

	disclosure		
O.PROT.NO_ALT	Protection of TSF Data from unauthorized alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(a)	Enforces protection by control of security attributes.
		FMT_MSA.1(b)	Enforces protection by control of security attributes.
		FMT_MTD.1	Enforces protection by restricting access.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.CONF.NO_DIS, O.CONF.NO_ALT	Protection of TSF Data from Unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MTD.1	Enforces protection by restricting access.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.USER_AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	FDP_ACC.1(b)	Enforces authorization by establishing an access control policy.
		FDP_ACF.1(b)	Supports access control policy by providing access control function.
		FIA_AFL.1	Supports authorization by requiring access control.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_SOS.1(1)	Supports authorization by requiring by specification of secrets.

		FIA_SOS.1(2)	Supports authorization by requiring by specification of secrets.
		FIA_UAU.1	Enforces authorization by requiring user authentication.
		FIA_UAU.6	Supports authorization by requiring user authentication.
		FIA_UAU.7	Supports authorization by requiring user authentication.
		FIA_UID.1	Enforces authorization by requiring user identification.
		FIA_USB.1	Enforces authorization by distinguishing subject security attributes associated with user roles.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(b)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(b)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports authorization by requiring security roles.
		FTA_SSL.3	Enforces authorization by terminating inactive sessions.
O.INTERFACE.MANAGED	Management of external interfaces	FIA_UAU.1	Enforces management of external interfaces by requiring user authentication.
		FIA_UAU.6	Supports authorization by requiring user authentication.
		FIA_UID.1	Enforces management of external interfaces by requiring user authentication.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports authorization by requiring security roles.
		FPT_FDI_EXP.1	Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces

			to Shared-medium Interfaces.
		FTA_SSL.3	Enforces management of external interfaces by terminating inactive sessions.
O.SOFTWARE.VERIFIED	Verification of software integrity	FPT_TST.1	Enforces verification of software by requiring self-tests.
O.AUDIT.LOGGED	Logging and authorized access to audit events	FAU_GEN.1	Enforces audit policies by requiring logging of relevant events.
		FAU_GEN.2	Enforces audit policies by requiring logging of information associated with audited events.
		FAU_SAR.1	Enforces audit policies by providing security audit record.
		FAU_SAR.2	Enforces audit policies by restricting reading of security audit records.
		FAU_STG.1	Enforces audit policies by protecting from unauthorised deletion and/or modification.
		FAU_STG.4(1)	Enforces audit policies by preventing audit data loss.
		FAU_STG.4(2)	Enforces audit policies by preventing audit data loss.
		FIA_UID.1	Supports management of external interfaces by requiring user authentication.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports authorization by requiring security roles.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.HDD.CRYPTO	The encryption of data	FCS_CKM.1	暗号鍵生成を要求してHDD暗号化を支援する。
		FCS_COP.1	暗号操作を要求してHDD暗号化を実施する。
		FIA_SOS.1(3)	暗号鍵のもととなるデータの品質を検証し、暗号化を支援する。
		FIA_UID.1	Supports authorization by requiring user identification.
		FMT_MOF.1	Supports the encryption of data by management of security functions behavior.
		FMT_MTD.1	Supports the encryption of data by

			management of TSF data.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports authorization by requiring security roles.

6.3.1.1. The dependencies of security requirements

セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 で規定される依存性を満たさない場合、「本 ST における依存関係」の欄にその理由を記述する。

Table 6-23 The dependencies of security requirements

本 ST の機能要件 コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4(1)	FAU_STG.1	FAU_STG.1
FAU_STG.4(2)	FAU_STG.1	FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 <FCS_CKM.4 を適用しない理由> ・暗号鍵は HDD のデータを暗号化するために使用するものであり、電源 ON 時に生成される。生成された鍵は揮発メモリに格納されるが、当該鍵にアクセスする外部インタフェースを提供しておらず、電源 OFF によって消滅するため、破棄を考慮する必要性はない。
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 <FCS_CKM.4 を適用しない理由> ・暗号鍵は HDD のデータを暗号化するために使用するものであり、電源 ON 時に生成される。生成された鍵は揮発メモリに格納されるが、当該鍵にアクセスする外部インタフェースを提供しておらず、電源 OFF によって消滅するため、破棄を考慮する必要性はない。
FDP_ACC.1(a)	FDP_ACF.1	FDP_ACF.1(a)
FDP_ACC.1(b)	FDP_ACF.1	FDP_ACF.1(b)
FDP_ACF.1(a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(a) FMT_MSA.3(a)
FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(b) FMT_MSA.3(b)
FDP_RIP.1	なし	なし
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	なし	なし
FIA_SOS.1(1)	なし	なし
FIA_SOS.1(2)	なし	なし
FIA_SOS.1(3)	なし	なし
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.6	なし	なし
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1

本 ST の機能要件 コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FIA_UID.1	なし	なし
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(a)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(b)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1
FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	なし	なし
FPT_TST.1	なし	なし
FTA_SSL.3	なし	なし
FTP_ITC.1	なし	なし
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

6.3.2. Security assurance requirements rationale

This Protection Profile has been developed for Hardcopy Devices to be used in commercial information processing environments that require a moderate level of document security, network security, and security assurance. The TOE will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7. TOE Summary specification

TOE のセキュリティ機能要件より導かれる TOE のセキュリティ機能の一覧を Table 7-1 に示す。詳細は、後述の項にて説明する。

Table 7-1 TOE のセキュリティ機能の名称と識別子

No.	TOE のセキュリティ機能	
1	F.AUDIT	監査ログ機能
2	F.HDD_ENCRYPTION	HDD 暗号化機能
3	F.ACCESS_DOC	保存文書アクセス制御機能
4	F.ACCESS_FUNC	利用者制限制御機能
5	F.RIP	残存情報消去機能
6	F.I&A	識別認証機能
7	F.SEPARATE_EX_INTERFACE	外部インタフェース分離機能
8	F.SELF_TEST	自己テスト機能
9	F.MANAGE	セキュリティ管理機能
10	F.SEUCRE_LAN	ネットワーク通信保護機能

7.1. F.AUDIT（監査ログ機能）

F.AUDIT は監査ログを取得するとともに取得した監査ログを改ざん・暴露から保護する。

7.1.1. 監査ログ取得機能

- 対応する機能要件：FAU_GEN.1、FAU_GEN.2
- TOE は以下のログを生成する。

Table 7-2 監査ログ

事象	ログ
監査ログ取得機能の開始	事象の日時
監査ログ取得機能の終了	事象の識別情報
ログイン操作の成功と失敗	サブジェクト識別情報（AdminID、User ID）
再認証の失敗	事象の結果（成功・失敗）
認証停止	
認証停止状態からの復帰	
Table 6-19 の管理機能の使用	
ネットワークを介した通信の失敗	
セッションの自動終了機能によるセッションの終了	

7.1.2. 監査ログレビュー機能

- 対応する機能要件：FAU_SAR.1、FAU_SAR.2

TOE は監査ログの読み出しを U.ADMINISTRATOR のみに制限する。TOE は監査ログを、ログの日時、操作者、操作内容、結果などを含む XML 形式のファイルとして、クライアント PC にダウンロードする機能を提供する。

7.1.3. 監査格納機能

- － 対応する機能要件：FAU_STG.1、FAU_STG.4(1)、FAU_STG.4(2)

TOE は監査ログの許可されていない削除や改変を制限する。また、TOE は監査ログを TOE 内の HDD に格納するが、格納領域が満杯になった場合、以下の処理を行う。

- (1). 「上書き禁止」に設定されている場合
 - 以下の操作以外を禁止する。また、PC からの印刷、FAX 受信も受け付けない。
 - 監査ログの削除、エクスポート（エクスポートにより TOE 上の監査ログは削除される）
 - 「上書き禁止」から「上書き許可」への設定変更
 - (2). 「上書き許可」に設定されている場合
 - 最も古くに格納された監査記録へ上書きする。
- (1)、(2)の設定は U.ADMINISTRATOR が行う。

7.1.4. 高信頼タイムスタンプ機能

- － 対応する機能要件：FPT_STM.1

TOE はクロック機能を有する。TOE はクロック機能によるタイムスタンプを監査ログ生成時に発行する。

7.2. F.HDD_ENCRYPTION (HDD 暗号化機能)

- － 対応する機能要件：FCS_CKM.1、FCS_COP.1、FIA_SOS.1(3)

TOE は HDD に保存されているデータを漏洩から保護するため暗号化を行う。使用する暗号鍵とアルゴリズムは以下の通りである。

(1). 暗号鍵

FIPS180-3 によって規定される SHA-256 アルゴリズムより、暗号鍵を生成する。（暗号鍵長は、256 bit）

暗号鍵は、U.ADMINISTRATOR が設定した暗号化ワードをもとにして生成することで TOE 毎に固有の暗号鍵を生成する。暗号化ワードは F.MANAGE により以下の品質を満たすもののみを受け入れる。

- 桁数 : 20 桁
- 文字種 : 95 文字以上の中から選択可能
- 規則 :
 - ◇ 同一の文字だけで構成されていない。
 - ◇ 同一文字種のみで構成されない。

(2). 暗号アルゴリズム

Table 7-3 に示す暗号アルゴリズム。

Table 7-3 HDD 暗号化機能における暗号アルゴリズム

暗号鍵長	暗号アルゴリズム
256 bit	FIPS PUB197 に準拠する暗号化アルゴリズム (AES)

7.3. F.ACCESS_DOC（保存文書アクセス制御機能）

－ 対応する機能要件：FDP_ACC.1(a)、FDP_ACF.1(a)

この節では、HDD に保存される文書に対するアクセス制御機能のみを記述して、それ以外の D.DOC に対するアクセス制御機能は F.ACCESS_FUNC にて記述する。

TOE は文書を保存するための機能を提供する。文書は HDD に保存され、文書に関連付けられた属性を参照してアクセス制御され PC へのダウンロード、削除を実施することができる。

以下に文書に関するアクセス制御の内容を示す。

Table 7-4 文書の操作

文書		文書の操作			
		Create	Modify	Read	Delete
強制メモリ受信 文書 (+FAXIN から +DSR に保存)	ファクス機能の受信により保存される文書である。 保存された D.DOC には FAXIN Box Word が関連付けられる。	—	なし	PC へのダウンロード U.USER or U.ADMIN	U.USER or U.ADMIN
スキャン保存文書 (+SCN から +DSR に保存)	スキャン(HDD)により保存される文書である。 保存された D.DOC には User ID が関連付けられる。	login_id	なし	PC へのダウンロード login_id or U.ADMIN	login_id or U.ADMIN

※ U.USER：指定した FAXIN Box Word が一致し、機能利用が許可された U.USER が操作可能であることを表す。

U.ADMIN：U.ADMINISTRATOR が操作可能であることを表す。

login_id：ログイン中のユーザーの User ID と文書の User ID が一致する場合に操作可能であることを表す。

強制メモリ受信文書は、FAX 受信することにより生成されるため、Create を定義する必要がない。

7.4. F.ACCESS_FUNC（利用者制限制御機能）

－ 対応する機能要件：FDP_ACC.1(a)、FDP_ACF.1(a)、FDP_ACC.1(b)、FDP_ACF.1(b)、FMT_MSA.3(a)、FMT_MSA.3(b)

F.MANAGE のユーザー管理機能により、一般利用者は権限が付与されたうえで登録される。TOE は識別認証された一般利用者の権限にしたがって、F.PRT、F.SCN、F.CPY、F.FAX、F.DSR の操作を許可する。なお、これらの属性である Permission Role に対する操作はできない。これにより識別認証された一般利用者は自身に許可された機能のみ実行できる。

各機能により生成される D.DOC、D.FUNC は、生成時に F.MANAGE により対応する属性が付与される。

また機能の実行中に発生する D.DOC、D.FUNC に対しては以下の操作が可能である。

なお実行者とは、操作対象の D.DOC、D.FUNC と同じ属性か、または許可された属性を持つ利用者を指す。TOE はこれらと比較し一致する場合にその利用者を実行者として扱う。

また U.ADMINISTRATOR の場合は、ジョブの削除によりすべての D.DOC、D.FUNC の削除が可能である。さらに、U.NORMAL による DSR 属性を持つ D.FUNC の Delete は、F.ACCESS_DOC の D.DOC の Delete と同様に削除が可能である。

- ・プリントの場合(+PRT)
以下の操作が可能（認証&プリント機能を利用）。
 - ・認証&プリントジョブの登録
クライアント PC 上のプリンタドライバーからの印刷操作で、ユーザー認証に成功するとジョブが登録される。
 - ・印刷
そのプリントを実行した U.NORMAL が印刷可能。(Read)
 - ・削除
そのプリントを実行した U.NORMAL が削除可能。(Delete)
- ・スキャンの場合(+SCN)
以下の操作が可能。
 - ・D.DOC の操作
そのスキャンを実行した U.NORMAL は読み込んだ原稿データを(Read して)メールで送信することが出来る。F.ACCESS_DOC により、HDD へ保存(+DSR の Create)することや HDD に保存した D.DOC(+DSR)を操作することが出来る。ここで送信待ち状態が生じることがあるがその場合以下の操作が可能
 - ・削除
そのメール送信を実行した U.NORMAL はその送信待ちのジョブを削除することができる。(Delete)
- ・コピーの場合(+CPY)
以下の操作が可能。
 - ・印刷
そのコピーを実行した U.NORMAL が印刷可能。
 - ・削除
そのコピーを実行した U.NORMAL はそのジョブを削除することができる。(Delete)
- ・ファクス受信の場合(+FAXIN)
FAX 受信した D.DOC は、FAXIN Box Word に関連付けて HDD に保存される。指定した FAXIN Box Word が一致した U.USER、U.ADMIN が FAX を印刷することができる。それ以外は保存文書として扱われるため、F.ACCESS_DOC により操作可能となる。
- ・ファクス送信の場合(+FAXOUT)
以下の操作が可能。
 - ・ファクス送信操作
ファクス送信を許可された U.NORMAL は読み込んだ原稿データを(Read して)ファクス送信することができる。
 - ・削除
そのファクス送信を実行した U.NORMAL はそのジョブを削除することができる。(Delete)

7.5. FRIP（残存情報消去機能）

7.5.1. 一時データ削除機能

- － 対応する機能要件：FDP_RIP.1

TOE は HDD 上の削除された文書、一時的な文書あるいはその断片に対して、上書き削除を実行することで残存情報の再利用を防止する。本機能は以下のタイミングで実行される。

- (1). プリントやスキャンなどのジョブの完了、停止時
ジョブ実行中に生成される一時的な文書あるいはその断片を削除する。
- (2). 削除操作実行時
指定された文書を削除する。
- (3). 電源オン時に残存情報が存在する時
(1)、(2)の削除実行中に電源がオフされて削除が完了しておらず残存情報が存在する場合、電源オン時にそれらを削除する。

上書きにおいて書き込むデータ、書き込む回数は、HDD データ上書き削除機能の動作設定機能によって U.ADMINISTRATOR が設定する。可能な設定とその内容は以下の通りである。

Table 7-5 一時データ上書き削除機能の動作設定

設定	内容 (上書きされるデータタイプとその順序)
Mode:1	0x00 で一回上書き
Mode:2	0x00、0xFF、0x61 の順に上書きを行い結果を検証

7.5.2. データ完全削除機能

- － 対応する機能要件 : FDP_RIP.1

U.ADMINISTRATOR は HDD 上の画像データを含むデータ領域に対する上書き削除を実行することが出来る。これに HDD 上の文書は削除されかつ残存情報の再利用が防止される。上書きにおいて書き込むデータ、書き込む回数は、HDD データ上書き削除機能の動作設定機能によって U.ADMINISTRATOR が設定する。可能な設定とその内容は以下の通りである。

Table 7-6 データ完全削除機能の動作設定

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	乱数 ⇒ 乱数 ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
Mode:4	乱数 ⇒ 0x00 ⇒ 0xFF
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

7.6. F.I&A (識別認証機能)

- － 対応する機能要件 : FIA_AFL.1、FIA_ATD.1、FIA_SOS.1(1)、FIA_SOS.1(2)、FIA_UAU.1、FIA_UAU.6、FIA_UAU.7、FIA_UID.1、FIA_USB.1、FTA_SSL.3、FMT_SMR.1

TOE は TOE を利用しようとする者が許可利用者であることを利用者から取得した識別認証情報を使って検証し、許可利用者と判断された者だけに TOE の利用を許可する。識別認証機能は、TOE 自身が識別認証を行う本体認証方式と外部の認証サーバーを使用する外部サーバー認証方式が存在する。

Table 7-7 認証方式

認証方式	識別認証成功前に可能な操作	SFR
本体認証	ファクス受信	FIA_UID.1
外部サーバー認証	TOE の状態確認および表示等の設定	FIA_UAU.1

※ 認証方式の設定は U.ADMINISTRATOR が行う。本体認証方式と外部サーバー認証方式は両方を同時に有効にすることはできない。

U.ADMINISTRATOR が外部サーバー認証方式の使用を設定した場合、一般利用者自身が、認証時に外部認証サーバーの接続先を選択できる。

また、再認証は、許可利用者が F.MANAGE により、自身のパスワードを変更する際に限定される。
FIA_UAU.6。

さらに、TOE は入力されたパスワードに対して、1 文字毎隠匿文字を表示する。FIA_UAU.7。

識別認証が成功した場合、当該利用者を代行するプロセスには指定された FAXIN Box Word、User ID、Allocation Role を結合する。FIA_ATD.1、FIA_USB.1

さらに、TOE は認証に使用するパスワードを F.MANAGE により以下の品質を満たすものに制限することで、強度の低いパスワードが設定されることを防止する。

Table 7-8 パスワードと品質

対象	条件	SFR
ログイン パスワード (U.ADMINISTRATOR)	TOE は下記の条件を満たすパスワードのみを受け入れる ・桁数 : 8 桁以上 ・文字種 : 95 文字以上の中から選択可能 ・規則 : ① 同一の文字だけで構成されていない。 ② 変更する場合、変更後の値が現在設定されている値と合致しない。	FIA_SOS.1(1)
ログイン パスワード (U.NORMAL)	TOE は下記の条件を満たすパスワードのみを受け入れる ・桁数 : 8 桁以上 ・文字種 : 93 文字以上の中から選択可能 ・規則 : ① 同一の文字だけで構成されていない。 ② 変更する場合、変更後の値が現在設定されている値と合致しない。	FIA_SOS.1(2)

また、認証が失敗した場合、TOE は以下の処理を行う。

Table 7-9 認証失敗時の処理

対象	処理	SFR
ログイン パスワード による認証 の失敗	連続した認証失敗回数が、3 回に達した場合認証を停止する。 管理者の認証が停止した場合は TOE の起動処理を行うことで、起動処理から管理者認証の操作禁止解除時間を経過後に認証停止を解除する。それ以外の場合は、F.MANAGE により管理者が認証失敗回数の消去機能を実行することで認証停止を解除する。	FIA_AFL.1

さらに、識別認証されたユーザーの操作が一定時間ない場合、そのセッションを終了する。詳細は以

下の通りである。FTA_SSL.3

Table 7-10 対話セッションの終了

対象	セッション終了	備考
操作パネル	最終操作および最終操作による処理が完了してから、オートリセット時間によって決定される時間経過した場合	オートリセット時間は工場出荷時に設定されており、管理者が変更可能である。
Web Connection	最終操作および最終操作による処理が完了してから、自動ログアウト時間によって決定された時間経過した場合	自動ログアウト時間は工場出荷時に設定されており、管理者が変更可能である。
Data Administrator	最終操作による処理が完了してから、60分間経過した場合※	時間は固定である。
プリンタドライバー		要求された処理の受け付けが開始、処理の完了が終了となるため、対話セッションはない。

※登録情報のダウンロードなど時間を要する処理を考慮した時間

7.7. F.SEPARATE_EX_INTERFACE (外部インタフェース分離機能)

－ 対応する機能要件：FPT_FDI_EXP.1

TOE は電話回線からの入力情報をファクス受信と遠隔診断機能のみに限定することにより電話回線からの侵入を防止するとともに受信ファクスの転送を禁止している。さらに USB インタフェースを含む外部インタフェースからの入力をそのまま Shared-medium Interface へ転送することはできない構造となっている。

7.8. F.SELF_TEST (自己テスト機能)

－ 対応する機能要件：FPT_TST.1

TOE は電源 ON 時に暗号化ワードの生成時と mfp 起動時に算出した値を比較することにより、暗号化ワードの完全性が検証され、暗号化機能の正常動作が実証される。暗号化ワードの完全性検証において完全性の喪失が検出された場合、TOE は操作パネルに警告を表示し、HDD への操作を受け付けない。さらに TOE は電源 ON 時に制御ソフトウェアのハッシュ値を計算し、記録している値との一致を確認することで TSF 実行コードの完全性が検証され、全体制御機能の正常動作が実証される。制御ソフトウェアの完全性検証において完全性の喪失が検出された場合、TOE は操作パネルに警告を表示し、操作を受け付けない。

7.9. F.MANAGE (セキュリティ管理機能)

－ 対応する機能要件：FIA_SOS.1(1)、FIA_SOS.1(2)、FMT_MOF.1、FMT_MSA.1(a)、FMT_MSA.1(b)、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FIA_SOS.1(3)

TOE は以下の管理機能を提供する。

Table 7-11 管理機能

管理機能	内容	操作者
セキュリティ強化設定の管理機能	セキュリティ強化設定の有効化／無効化を行う。	U.ADMINISTRATOR
ユーザー認証機能の管理機能	認証方式の設定を行う。	U.ADMINISTRATOR
HDD データ上書き削除機能の動作設定機能	HDD データ上書き削除機能の動作設定 (Mode の設定) を行う	U.ADMINISTRATOR
監査ログ管理機能	監査ログ満杯時の動作の設定 (上書き禁止／上書き許可)、監査ログを読み出し・削除を行う。	U.ADMINISTRATOR
高信頼チャンネル管理機能	通信暗号強度設定 (通信暗号方式の変更)	U.ADMINISTRATOR
ユーザー管理機能	TOE への U.NORMAL (UserID)の登録、削除、変更、権限 (Allocation Role) の変更・削除を行う。 Allocation Role の各 Role の Default を以下に示す。 <ul style="list-style-type: none"> ・ Print Role (Default: Allow) ・ Scan Role (Default: Allow) ・ Copy Role (Default: Allow) ・ Fax Role (Default: Restrict) ・ DSR Role (SCN) (Default: Allow) ・ DSR Role (FAXIN) (Default: Restrict) また、U.NORMAL のログインパスワードの登録・変更を行う。 この際、パスワードの品質が検査される。	U.ADMINISTRATOR
属性の初期化機能 (D.DOC および D.FUNC)	TOE は D.DOC および D.FUNC のセキュリティ属性を Table 6-15 に示した通り初期化する。	+DSR(+FAXIN)の場合： U.ADMINISTRATOR が設定した FAXIN Box Word それ以外の場合：U.NORMAL
属性の初期化機能 (F.PRT、F.SCN、F.CPY、F.FAX、F.DSR)	TOE は F.PRT、F.SCN、F.CPY、F.FAX、F.DSR の属性は Table 6-16 の通り固定で設定されているため、この初期化処理に介入する機能は存在しない。	なし
U.NORMAL のログインパスワードの変更機能	自身のパスワードを変更する。 この際、パスワードの品質が検査される。	U.NORMAL
U.ADMINISTRATOR のログインパスワード変更機能	U.ADMINISTRATOR が自身のパスワードを変更する。(工場出荷時に初期値が設定されているため、設定の機能はない。) この際、パスワードの品質が検査される。	U.ADMINISTRATOR
暗号化ワードの設定機能	HDD 暗号化機能で使用する暗号鍵のもととなるデータである暗号化ワードを設定する。 この際、暗号化ワードの品質が検査される。	U.ADMINISTRATOR

日時情報の変更機能	日時情報を設定する。	U.ADMINISTRATOR
オートリセット時間の変更機能	オートリセット時間の変更を行う。 (工場出荷時に初期値が設定されているため、設定の機能はない。)	U.ADMINISTRATOR
自動ログアウト時間の変更機能	自動ログアウト時間の変更を行う。	U.ADMINISTRATOR
外部サーバー認証設定データの登録・変更機能	外部認証サーバーに関する設定データ (外部サーバーが所属するドメイン名などを含む) の登録・変更を行う。	U.ADMINISTRATOR
認証失敗回数 (管理者以外) の消去機能	認証失敗回数 (管理者以外) を消去する。 これにより認証機能のロックが解除される。	U.ADMINISTRATOR
パスワード規約の変更機能	パスワード規約の設定・変更を行う。	U.ADMINISTRATOR
ネットワーク設定の登録・変更機能	ネットワーク設定 (SMTP サーバー、DNS サーバーの IP アドレス、ポート番号等、mfp の IP アドレス、NetBIOS 名等) の設定・変更を行う。	U.ADMINISTRATOR
送信宛先の登録・変更機能	送信宛先設定 (メールによる送信の宛先等) の登録・変更を行う。	U.ADMINISTRATOR
FAXIN Box Word の登録・変更機能	受信した FAX 文書を格納する強制メモリ受信の FAXIN Box Word の登録・変更を行う。	U.ADMINISTRATOR

7.10. F.SECURE_LAN (ネットワーク通信保護機能)

ー 対応する機能要件：FTP_ITC.1

TOE は IT 機器との通信において暗号化通信を行う。TOE が提供する暗号化通信は以下の通りである。(セキュリティ強化設定が有効な場合)

Table 7-12 TOE が提供する暗号化通信

通信先	プロトコル	暗号アルゴリズム
クライアント PC	TLSv1.0,TLSv1.1,TLSv1.2	3DES(168 bits)、AES(128bits、256bits)
外部認証サーバー	IPsec	3DES(168 bits)、AES(128bits、192bits、256bits)
DNS サーバー	IPsec	3DES(168 bits)、AES(128bits、192bits、256bits)
SMTP サーバー	IPsec	3DES(168 bits)、AES(128bits、192bits、256bits)

以上