京セラミタ

Data Security Kit (C) Type Ⅱ

セキュリティターゲット

第0.06版

2007年12月25日

京セラミタ株式会社

- 更新履歴 -

日付	Version	更新内容	承認者	作成者
2007/7/4	0.01	・新規作成	辻	曽根
2007/10/2	0.02	・適用する CC バージョンの修正	辻	曽根
2007/11/13	0.03	・対象製品の追加 ・バージョン情報の確定	辻	曽根
2007/11/27	0.04	・指摘事項に対する修正	辻	曽根
2007/12/10	0.05	・指摘事項に対する修正	辻	曽根
2007/12/25	0.06	・保証ドキュメント名称の修正	辻	曽根

～ 目次 ～

～ 図目次 ～

～ 表目次 ～

1. ST 概説

1.1. ST 識別

1.1.1. ST の識別と管理

名称： 京セラミタ Data Security Kit (C) Type Ⅱ セキュリティターゲット

バージョン： 第 0.06 版

作成日： 2007/12/25

作成者： 京セラミタ株式会社

1.1.2. TOE の識別と管理

名称： Data Security Kit (C) Type Ⅱ Software

バージョン： V2.40

作成者： 京セラミタ株式会社

1.1.3. 適用する CC のバージョン

ISO/IEC 15408:2005

CCIMB Interpretations-0512 適用

注) 日本語訳は以下の資料を利用する。

- 情報技術セキュリティ評価のためのコモンクライテリア パート１:概説と一般モデル バージョン2.3 2005年8月 CCIMB-2005-08-001
  (平成17年12月翻訳 第1.0版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室)
- 情報技術セキュリティ評価のためのコモンクライテリア パート２:セキュリティ機能要件 バージョン2.3 2005年8月 CCIMB-2005-002
  (平成17年12月翻訳 第1.0版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室)
- 情報技術セキュリティ評価のためのコモンクライテリア パート３:セキュリティ保証要件 バージョン2.3 2005年8月 CCIMB-2005-003
  (平成17年12月翻訳 第1.0版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室)
- 補足-0512

1.2. ST 概要

本STは、京セラミタ株式会社が提供する複合機 (Multi Function Printer 以下 MFP と略称) に搭載する「Data Security Kit (C) Type Ⅱ Software」について記述して

いる。
MFPとは、複写機としてのコピー機能のほかに、プリンタ機能、ネットワークスキャナ機能、FAX機能を有する製品である。利用者は、MFPを使用することにより、出力物としての紙文書を扱うだけでなく、電子化された文書としても扱うことが可能となる。本TOEは、このMFPにオプション製品として搭載され、保存データと残存データ保護のためのセキュリティ機能を提供するファームウェア製品である。

TOE が提供するセキュリティ機能：

・ コピー/プリント/ネットワークスキャナ/FAX の処理途上のデータ、又は複合機内部に保存されたデータ、及び前記処理の完了後、又は複合機内部に保存されたデータの論理的な削除時に残存するデータを保護する機能

1.3. CC 適合

パート 2 適合
パート 3 適合
EAL 3 適合
本 ST が適合している PP はない。

1.4. 参考資料

- 情報技術セキュリティ評価のためのコモンクライテリア パート 1:概説と一般モデル バージョン 2.3 2005 年 8 月 CCIMB-2005-08-001
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2:セキュリティ機能要件 バージョン 2.3 2005 年 8 月 CCIMB-2005-08-002
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3:セキュリティ保証要件 バージョン 2.3 2005 年 8 月 CCIMB-2005-08-003
- 補足-0512
- Common Criteria for Information Technology Security Evaluation
  Part 1： Introduction and general model
  August 2005 Version 2.3 CCIMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2： Security functional requirements
  August 2005 Version 2.3 CCIMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3： Security assurance requirements
  August 2005 Version 2.3 CCIMB-2005-08-003
- Interpretations-0512

1.5. 用語の定義

本 ST で使用される用語の定義を表 1.1 で示す。

表 1.1 TOE に関する用語の定義

用語	定義
スプール保存	受け取った画像データを、そのまま出力又は転送せずに一時的に HDD 上に保持すること。利用者が意識することなく複合機の処理過程で自動的に行う。長期保存と対比。
長期保存	受け取った画像データを、長期的に HDD 上に保持すること。利用者が意識して保存操作、取り出し操作を行う。スプール保存と対比。
PSTN	公衆交換電話網：Public Switched Telephone Networks の略。一般の加入電話回線ネットワークのこと。本 ST では「公衆回線」と訳す。
クライアント PC	ネットワークに接続された TOE に対して、ネットワークに接続して TOE のサービス(機能)を利用する側のコンピュータのことを指す。
ネットワークスキャナ	スキャンされた原稿を画像データとして、クライアント PC に送信する機能。LAN 経由で送信する PC 送信と、E-mail 経由で送信する E-mail 送信、クライアント PC からの操作でセットされた原稿を取り込む TWAIN 機能がある。
管理領域	画像データの中で、そのデータの管理情報が記された領域。画像データを論理的に削除するとは、この領域だけを認識不可能なものにすることを指す。
実データ領域	画像データの中で、実際の画像を構成するデータが記された領域。画像データを論理的に削除した場合には、この領域は残存してしまう。この残存した領域を指して「残存データ」と呼ぶ。
操作パネル	複合機の一番上部に設置され、液晶パネルで構成される。 外部インタフェースであり、利用者は、操作パネルを通して TOE を利用することが出来る。

2. TOE 記述

2.1. TOE 種別

本 TOE は、「Data Security Kit (C) Type Ⅱ Software」と呼ばれる、複合機に暗号化及び残存データの上書き機能を提供するファームウェア製品である。

2.2. 対象製品

本 TOE を搭載可能な製品を表 2.1 で示す。

表 2.1 TOE の対象製品

TOE 名称 / バージョン	対象製品
Data Security Kit (C) Type Ⅱ Software / V2.40	KM-2560、KM-3060 KM-2560i、KM-3060i CS-2560、CS-3060

2.3. TOE 概要

2.3.1. TOE の利用目的

本 TOE は、一般的な複合機に搭載され、暗号化機能と上書き消去機能を提供することにより、様々な文書のコピー（複製）、プリント（紙出力）、ネットワークスキャナ（電子化）、FAX（送受信）の各処理中/処理後に HDD 上に存在する画像データを不正な暴露から保護する目的のために利用される。

2.3.2. 複合機の利用環境

TOE を搭載する複合機は、LAN、FAX 用の公衆回線に接続される。また、ローカルポート（パラレルポート、USB ポート）に接続されて使用することも可能である。

LAN 内のクライアント PC やローカル接続されたクライアント PC にドライバや各種ユーティリティをインストールすることで機器管理者は LAN/ローカルポートを通して複合機の運用/管理を行うことが可能である。また TOE 利用者は LAN/ローカルポートを通して、複合機を利用することが可能である。

図 2.1 に一般的な利用環境を示す。

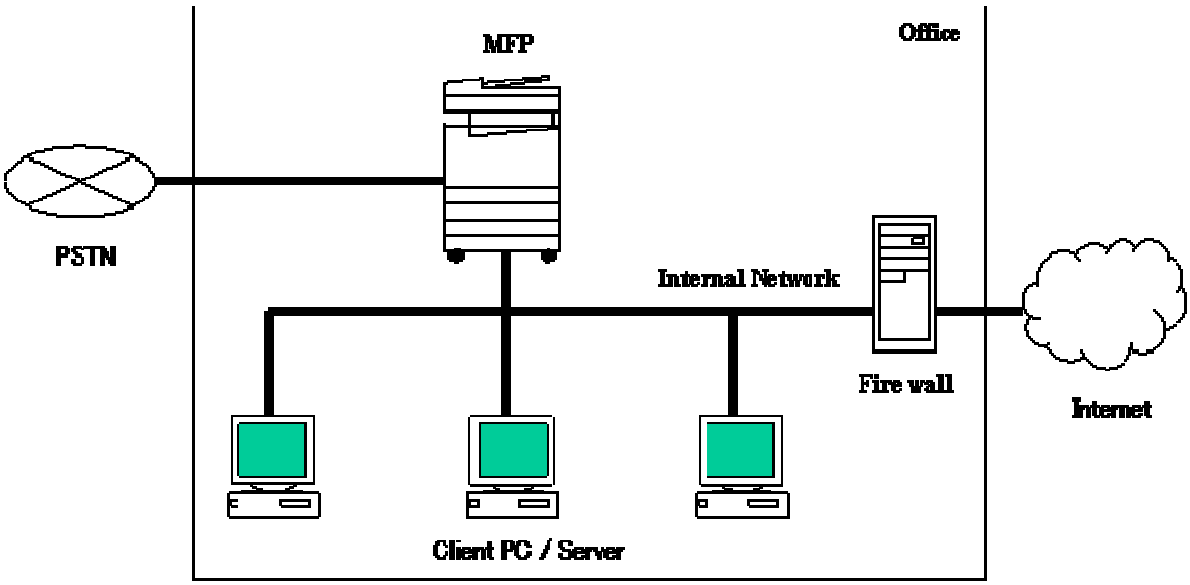

図 2.1 一般的な利用環境

2.3.3. TOE の関連者

TOE における、機器管理者、TOE 利用者、サービス担当者を以下に定義する。

機器管理者：

TOE を搭載した複合機本体の管理者として登録されている者。機器管理者は、機械本体に対する特権を有する。

【 利用方法 】

機器管理者は、TOE を搭載した複合機を構成する機器、及び TOE に対する導入、運用管理を行う。また、TOE のセキュリティを維持するための運用管理も行う。

【 利用手順 】

- 機器管理者は、複合機、及び TOE のマニュアルに従って、TOE を運用するために必要な各機器の設定・導入を行う。

TOE 利用者：

TOE を搭載した複合機の利用を許可された者。コピー、プリント、ネットワークスキャナ、FAX、及び文書管理の機能を利用することが出来る。また、TOE 利用者は、画像データの露顕に関して攻撃能力は低レベルである。

【 利用方法 】

TOE 利用者は、様々な文書のコピー、プリント、ネットワークスキャナ、FAX、及び文書管理を行う。

【 利用手順 】

- TOE 利用者は、複合機、及び TOE のマニュアルに従って、コピー、プリント、ネットワークスキャナ、FAX、及び文書管理の機能を使用する。

サービス担当者：

TOE を搭載した複合機のサービス担当者として京セラミタが認めた者。サービス担当者は TOE の導入及び、TOE を搭載した複合機の保守を行う。

【 利用方法 】

サービス担当者は、TOE 導入時に、TOE のインストールを行い、TOE の立上げ（動作可能にする）を行う。また、TOE を搭載した複合機を構成する機器および TOE に対するメンテナンスを行う。

【 利用手順 】

- サービス担当者は、TOE のマニュアルに従って、TOE をインストールし、TOE の立ち上げ（動作可能にする）を行う。
- サービス担当者は、複合機のサービスマニュアルに従って、TOE を搭載した複合機を構成する機器および TOE に対するメンテナンスを行う。

2.4. TOE 構成

2.4.1. TOE の物理的構成

TOE の物理的構造の概念図を 図 2.2 で示す。

TOE が搭載される MFP は、メインボード、FAX ボード、操作パネル、MFP 本体ハードウェアで構成される。

TOE である Data Security Kit (C) Type Ⅱ Software は、メインボード上のメインコントローラ内にある、セキュリティモジュールと暗号化チップで構成される。セキュリティ機能は全てセキュリティモジュールが行う。HDD データの暗号化は暗号化チップで行うが、暗号化チップの制御はセキュリティモジュールが行う。メインボード上のメインコントローラが MFP の全体制御を行っており、非セキュリティ機能に関しては全てメインモジュールが行う。また、メインボード上には、HDD が存在する。イントラネット、ローカルポートを通してのネットワーク制御はネットワークが行う。

操作パネルは、製品利用者からの入力を受付け、また製品利用者に情報を提供する。

MFP 本体ハードウェアは、印刷制御をつかさどる。

FAX ボード上の FAX 通信は、公衆回線との通信制御を行い、送受信データをメインコントローラへ受け渡す。

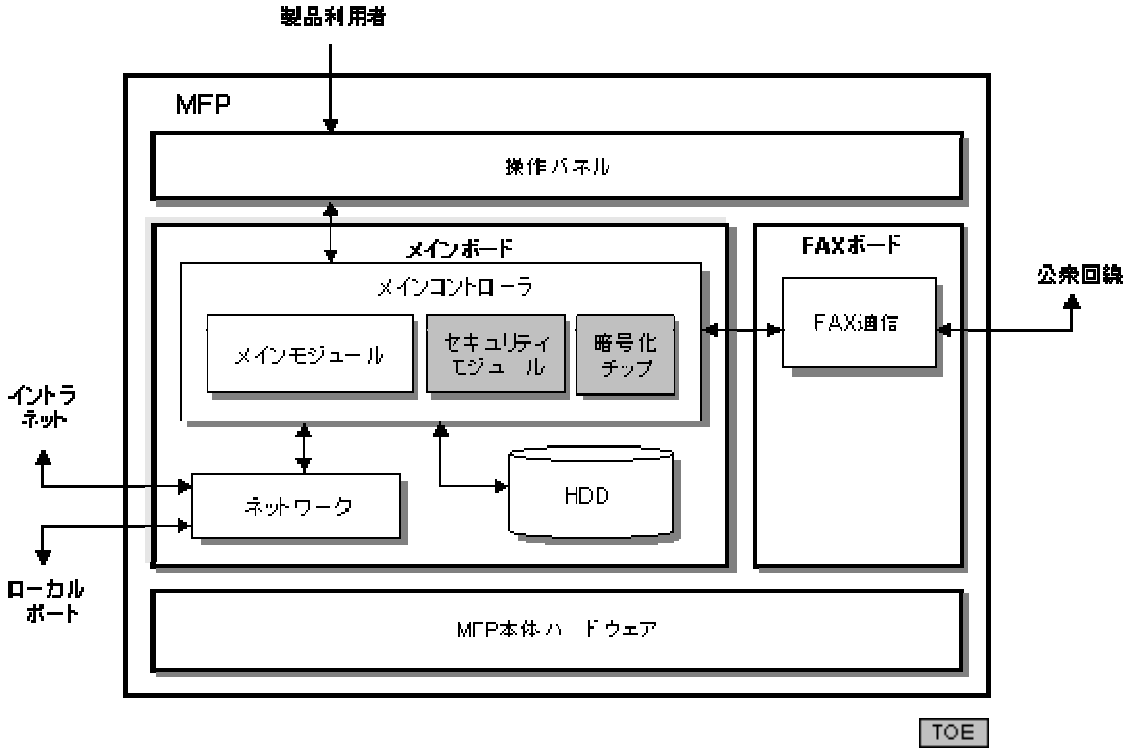

図 2.2 TOE の構成図

2.4.2. TOE の論理的構成と環境

TOE の論理的構造の概念図を 図 2.3 で示す。

TOE は、セキュリティ機能のみで構成される。MFP としては非セキュリティ機能として通常機能も有している。

以下の機能がセキュリティ機能として TOE の論理的範囲に含まれる。

- 暗号化機能
  コピー/プリント/ネットワークスキャナ/FAX/文書管理の各機能で処理される際に、TOE が HDD に保存される画像データを暗号化して保存する機能。また、暗号化されたデータを読み出す場合に、データの復号も行う。
- 上書き消去機能
  コピー/プリント/ネットワークスキャナ/FAX/文書管理の処理が完了し、または、これらの処理中の中止操作による中止処理の完了後、HDD に保存された画像データの論理的な削除を行う際に、TOE が実データ領域に対して無意味な文字列を上書きし、実データ領域を完全に消去する機能。

以下の機能は TOE 外の機能として論理的に構成されている。

- ユーザインタフェース機能
  操作パネルからの入力/操作を受け付ける機能。操作パネルへの表示も行う。
- 管理者認証機能
  機器管理者を操作パネルから入力された機器管理者暗証番号により、識別認証する機能。
- コピー機能
  画像データを複合機のスキャナから読込み、複合機の印刷部から出力する機能。
- ネットワークスキャナ機能
  画像データを複合機のスキャナから読込み、クライアント PC に送信する機能。
- プリンタ機能
  LAN 上、又はローカル接続されたクライアント PC から送信された画像データを複合機の印刷部から出力する機能。
- FAX 機能
  公衆回線を通して、他の FAX とデータの送受信を行う機能。

- 文書管理機能
  画像データを HDD 上に長期保存する機能。
  長期保存された画像データは、印字出力、クライアント PC への転送、FAX 送信することが出来る。また、誰でも自由にアクセスすることが出来る。
  入力手段として、操作パネル、クライアント PC からの転送、FAX 受信がある。
  また、長期保存された画像データを削除することも可能である。

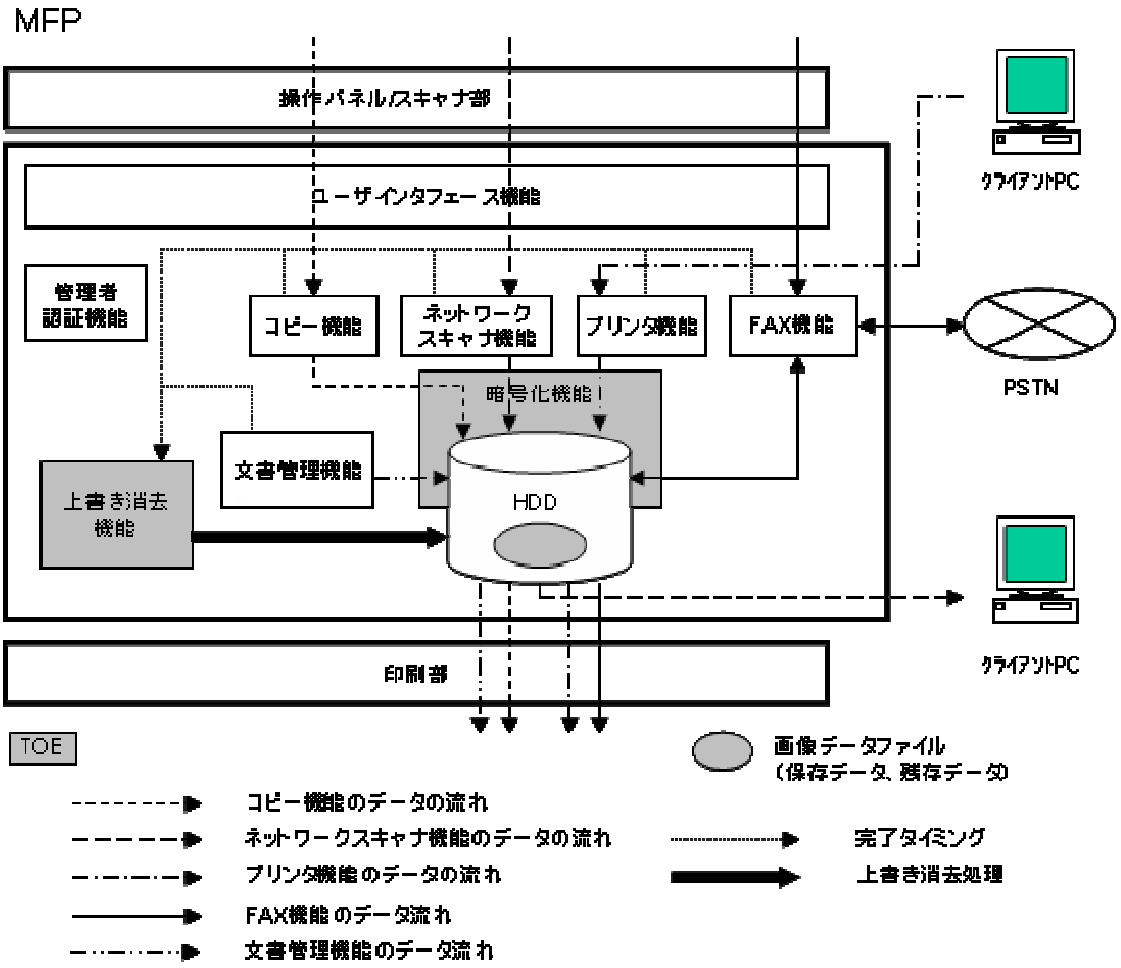

図 2.3 TOE の論理図

2.5. TOE の機能

TOE が提供する機能は以下である。

- 暗号化機能
- 上書き消去機能

2.5.1. 暗号化機能

HDD に保存された画像データに対し、データの漏洩に対する脅威に対抗することを目的として、暗号化機能が存在する。

コピー機能、ネットワークスキャナ機能、プリンタ機能、FAX 機能、及び文書管理機能という通常機能が処理され、画像データを HDD に保存する際に、TOE は保存する画像データを暗号化し HDD に書き込む。また、同様の通常機能が処理され、HDD に保存された画像データを読み出す際に、TOE は暗号化された保存データを復号して画像デ

ータを読み出す。

暗号化に使用する暗号鍵は、複数の情報を元に、MFP の電源 ON 時に毎回生成され、揮発性メモリに保持される。つまり、MFP の電源が OFF された状態で MFP 内部に暗号鍵が保持されていることはない。暗号鍵の元となる情報の１つは機器管理者が登録することが出来る。ただし、この情報を登録しなくても、暗号鍵は一意に生成される。

2.5.2. 上書き消去機能

論理的な従来の削除処理に加え、更に安全性を向上させることを目的として、上書き消去機能が存在する。

コピー機能、ネットワークスキャナ機能、プリンタ機能、FAX 機能、及び文書管理機能という通常機能の処理が完了し、または、これらの処理中の中止操作による中止処理の完了後、HDD に保存された画像データを削除する際に、TOE は画像データの実データ領域に対して無意味な文字列を上書きし、実データ領域を完全に消去した上で画像データの管理情報を削除する。

また、機器管理者がフォーマットを実行した際に、上書き消去機能は HDD の全領域に対して無意味な文字列を上書きし、それにより全領域を完全に消去する。

HDD に対する上書き消去の方式には、３回上書き方式と１回上書き方式がある。

- ◆ ３回上書き方式

  上書き消去する画像データの実データ領域全体に、ランダムデータ（１）、ランダムデータ（２）、NULL（0x00）を順次書き込む

- ◆ １回上書き方式

  上書き消去する画像データの実データ領域全体に NULL（0x00）を書き込む

３回上書き方式は処理効率よりも安全性を重視する場合に設定し、１回上書き方式は処理効率を重視する場合に設定する。必ずどちらか一方の方式が設定されることになり、デフォルト値は３回上書き方式である。機器管理者のみが、設定値を変更することが出来る。

2.6. 保護対象となる資産

一般的な複合機は、コピー/プリント/ネットワークスキャナ/FAX の処理を行う際、一旦、スプール保存領域にデータを保持してから処理を行う。また、処理終了後にそのデータの削除を行うが、管理領域を論理的に削除するだけである。このため、各機能の処理中や、用紙切れ等で即時処理(出力)が出来ない場合には HDD 上に画像データはスプール保存されたままであり、また処理終了後でも、実データ領域が残存情報として残ってしまう。元々長期的に保存されている画像データや上述のようにスプール保

存されている画像データはもちろんのこと、この残存情報にもデータとしては各機能の処理で行ったデータと同じデータが入っているため、HDD に不正な解読装置をつけられたり、HDD が持ち出されたりすると、これらデータを丸ごと持ち出されてしまうことも起こり得る。

そこで、TOE が保護すべき資産を以下に示す。

■ 保存データ

コピー/プリント/ネットワークスキャナ/FAX の処理を行う際、HDD 上にスプール保存された画像データ。

文書管理機能を使用し、HDD 上に長期保存された画像データ。

なお、長期保存された画像データは、再印刷など複合機上で再使用するために保存するデータであるので、複合機の一般機能（2.4.2 節で TOE 外の機能としてリストされている機能）でアクセスされることは、脅威とはみなさないものとする。

■ 残存データ

HDD 上に、スプール保存又は長期保存された画像データが、論理的に削除された後に残存するデータ。

対象となるデータは HDD 上の画像データファイルに格納されている。

3. TOE セキュリティ環境

3.1. 前提条件

本 TOE の利用にあたり、想定される前提条件はない。

3.2. 脅威

本 TOE が想定している攻撃者の攻撃能力は、低レベルである。

T.AGAIN ：保存データ/残存データへの不正アクセス

悪意を持った TOE 利用者が、HDD に不正な解読装置を接続したり、HDD を持ち出したりして、HDD に保持されている保存データ/残存データを閲覧/出力する。

3.3. 組織のセキュリティ方針

TOE が従わなければならない組織のセキュリティ方針として以下を必要とする。

P.REMAIN ： 残存データの上書き消去

組織からの要求として、保存データの使用後に HDD には実データを一切残さないようにするために、HDD に残存するデータは、上書き消去されなければならない。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

TOE が実施する、脅威に対抗するためのセキュリティ対策方針を述べる。

O.ENCRYPT ：保存データの解読防止

TOE は、HDD に保持されている保存データが不正に閲覧/出力されないように、保存データを解読されないようにしなければならない。

O.REMAIN ： 残存データの上書き消去

TOE は、HDD に保持されている残存データの保存領域を上書き消去しなければならない。

4.2. 環境のセキュリティ対策方針

TOE の環境が実施する、脅威に対抗もしくは前提条件を実現するためのセキュリティ対策方針はない。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

FCS_CKM.1　　暗号鍵生成

下位階層：なし

FCS_CKM.1.1

TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付：標準のリスト]

・京セラミタ標準

[割付：暗号鍵生成アルゴリズム]

・京セラミタ標準の暗号鍵生成アルゴリズム

[割付：暗号鍵長]

・128 bit

依存性：[FCS_CKM.2 暗号鍵配付 または FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1　　暗号操作

下位階層：なし

FCS_COP.1

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

[割付：標準のリスト]
・FIPS PUB 197

[割付：暗号アルゴリズム]
・AES

[割付：暗号鍵長]
・128 bit

[割付：暗号操作のリスト]
・HDD 上の保存データファイルの暗号化
・HDD 上の保存データファイルの復号

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データインポート
または FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FDP_RIP.1　　サブセット残存情報保護

下位階層：なし

FDP_RIP.1.1

TSF は、以下のオブジェクト[選択：への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない：[割付：オブジェクトのリスト]。

[選択：への資源の割当て、からの資源の割当て解除]
・からの資源の割当て解除

[割付：オブジェクトのリスト]
・HDD 上の画像データファイル

依存性：なし

FPT_RVM.1　　TSP の非バイパス性

下位階層：なし

FPT_RVM.1.1

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

依存性：なし

5.1.2. TOE セキュリティ保証要件

TOE セキュリティ保証要件の保証レベルは EAL3 である。選択した TOE セキュリティ保証要件一覧表を 表 5.1 で識別する。なお、EAL3 を超える特定の保証対策は無い。

表 5.1 TOE セキュリティ保証要件

クラス	コンポーネント名(ファミリ含む)	
構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立ち上げ手順
開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
テスト	ATE_COV.2	ガバレージの分析
	ATE_DPT.1	テスト：上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テストーサンプル
脆弱性評定	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.2. IT 環境に対するセキュリティ要件

TOE が従わなければならない IT 環境によるセキュリティ要件は存在しない。

5.3. 最小機能強度

本 TOE の全体のセキュリティ機能要件に対する最小機能強度主張は SOF-基本である。
ただし、該当する機能は存在しない。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

ここでは、本 TOE が提供すべきセキュリティ機能を定義する。

表 6.1 は、各 TOE 要約仕様とセキュリティ機能要件の関係を示す。

表 6.1 TOE 要約仕様とセキュリティ機能要件

仕様概要 / 機能要件	SPF.ENCRYPT	SPF.AGAIN
FCS_CKM.1	○	
FCS_COP.1	○	
FDP_RIP.1		○
FPT_RVM.1	○	○

6.1.1. 暗号化機能

暗号化機能は、以下の機能を提供する。

SPF.ENCRYPT

暗号化機能は、画像データを HDD に保存する際に、画像データを暗号化して保存する機能である。

TOE は保存する画像データを AES アルゴリズムを用いて暗号化し HDD に書き込む。また、暗号化された保存データを復号して画像データを読み出す。

TOE は、AES アルゴリズムに使用する 128bit 暗号鍵を京セラミタ標準の暗号鍵生成アルゴリズムを用いて生成する。この鍵は、複数の情報を元に、MFP の電源 ON 時に毎回生成され、揮発性メモリに保持される。揮発性メモリは、電荷が無くなると記憶内容が失われる半導体メモリであるので、MFP の電源が OFF された時点で MFP 内部に暗号鍵が保持されていることは無くなり、暗号鍵を読み出すことは出来ない。

6.1.2. 上書き消去機能

上書き消去機能は、以下の機能を提供する。

SPF.AGAIN

上書き消去機能は、HDD に保存された画像データを、論理的に画像データの管理情報だけを削除するのではなく、実データ領域も全て上書き消去する機能である。
TOE は、HDD に保存された画像データの実データ領域に対して上書き消去を行い、実データ領域を完全に消去してから画像データの管理情報を削除する。
また、上書き消去機能は、MFP の起動時にも削除対象となっている画像データが存在する場合に上書き消去を実行する。

6.2. セキュリティメカニズム

TOE は、以下のセキュリティメカニズムを採用する。

■３回上書き方式

上書き消去するデータの実データ領域全体に、ランダムデータ(１)、ランダムデータ(２)、NULL(0x00)を順次書き込むアルゴリズムである。

なお、本 TOE では本方式を以下の機能で使用している。

・HDD に対する上書き消去機能

HDD 上に保存されたデータを削除する際、３回上書き方式により、実データ領域を確実に上書き消去する。
１回上書き方式よりも安全に上書き消去される。

■１回上書き方式

上書き消去するデータの実データ領域全体に、NULL(0x00)を書き込むアルゴリズムである。

なお、本 TOE では本方式を以下の機能で使用している。

・HDD に対する上書き消去機能

HDD 上に保存されたデータを削除する際、１回上書き方式により、実データ領域を確実に上書き消去する。

6.3. セキュリティ機能強度

本 TOE の確率的または順列的セキュリティメカニズムに基づくセキュリティ機能はない。

6.4. 保証手段

開発者は、CC の保証要件および社内の開発規約に従って開発を行う。EAL3 セキュリティ保証要件のコンポーネント及び各保証要件を満足する保証ドキュメントを 表 6.2 に示す。

表 6.2 保証手段

セキュリティ保証要件		保証手段
構成管理	ACM_CAP.3	・Data Security Kit (C) Type Ⅱ 構成管理計画書 ・Data Security Kit (C) Type Ⅱ 構成管理規約書 ・Data Security Kit (C) Type Ⅱ 構成リスト
	ACM_SCP.1	・Data Security Kit (C) Type Ⅱ 構成管理計画書 ・Data Security Kit (C) Type Ⅱ 構成管理規約書
配付と運用	ADO_DEL.1	・Data Security Kit (C) Type Ⅱ 配付手順説明書
	ADO_IGS.1	・Date Security Kit (C) 複合機用設置手順書 ・KM-2560/KM-3060 使用説明書　応用編 ・2560/3060 Advanced Operation Guide ・KM-2560/KM-3060 サービスマニュアル ・KM-2560/KM-3060 SERVICE MANUAL ・FAX System (M) ファクスシステム設置手順書 ・FAX System (M) サービスマニュアル ・FAX System (M) SERVICE MANUAL
開発	ADV_FSP.1	・Data Security Kit (C) Type Ⅱ 機能仕様書
	ADV_HLD.2	・Data Security Kit (C) Type Ⅱ 上位レベル設計書
	ADV_RCR.1	・Data Security Kit (C) Type Ⅱ 機能対応表
ガイダンス文書	AGD_ADM.1	・KM-2560/KM-3060 使用説明書　応用編 ・2560/3060 Advanced Operation Guide
	AGD_USR.1	・KM-2560/KM-3060 使用説明書 ・KM-2560/KM-3060 使用説明書　応用編 ・FAX System (M) 使用説明書 ・2560/3060 Operation Guide ・2560/3060 Advanced Operation Guide ・2560i/3060i Operation Guide ・FAX System (M) Operation Guide
ライフサイクルサポート	ALC_DVS.1	・Data Security Kit (C) Type Ⅱ 開発セキュリティ規定書

テスト	ATE_COV.2	・Data Security Kit (C) Type Ⅱ カバレージテスト分析書
	ATE_DPT.1	・Data Security Kit (C) Type Ⅱ 上位レベル設計テスト仕様書
	ATE_FUN.1	・Data Security Kit (C) Type Ⅱ 機能テスト仕様書
	ATE_IND.2	・TOE
脆弱性評定	AVA_MSU.1	・KM-2560/KM-3060 使用説明書 ・KM-2560/KM-3060 使用説明書　応用編 ・FAX System (M) 使用説明書 ・2560/3060 Operation Guide ・2560/3060 Advanced Operation Guide ・2560i/3060i Operation Guide ・FAX System (M) Operation Guide
	AVA_SOF.1	・Data Security Kit (C) Type Ⅱ 脆弱性分析書
	AVA_VLA.1	・Data Security Kit (C) Type Ⅱ 脆弱性分析書

7. PP 主張

本 ST が準拠する PP は存在しない。

8. 根拠

8.1. セキュリティ対策方針根拠

8.1.1. 脅威及び組織のセキュリティ方針に対するセキュリティ対策方針の適合性

脅威及び組織のセキュリティ方針に対応するセキュリティ対策方針の関係を『表 8.1 脅威及び組織のセキュリティ方針とセキュリティ対策方針の対応』に示す。

表 8.1 脅威及び組織のセキュリティ方針とセキュリティ対策方針の対応

脅威/組織のセキュリティ方針 ＼ セキュリティ対策方針	T.AGAIN	P.RAMAIN
O.ENCRYPT	✔	
O.REMAIN		✔

以下に、『表 8.1 脅威及び組織のセキュリティ方針とセキュリティ対策方針の対応』の根拠を示す。

T.AGAIN

T.AGAIN の脅威に対抗するためには、HDD に保持されている保存データ/残存データに対し、その情報が閲覧/出力できないようにする必要がある。

この脅威に対して、O.ENCRYPT の対策方針により対抗することが出来る。すなわち、HDD に保持されている保存データを解読されないように暗号化することで、不正に閲覧/出力されることを防止することが出来る。

P.REMAIN

組織のセキュリティ方針 P.REMAIN により、組織からの要求として、保存データの使用後に HDD には実データを一切残さないようにするために、HDD に保存されるデータは、各機能の使用後に、論理的な削除だけでなく、実データ領域も全て上書き消去されなければならない。その対策として、O.REMAIN の対策方針により、HDD に保持されている残存データの保存領域を上書き消去する機能を提供するので、P.REMAIN を実現することが出来る。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ対策方針に対するTOEセキュリティ機能要件の適合性

セキュリティ対策方針に対するTOEセキュリティ機能要件の対応を『表 8.2 セキュリティ対策方針とTOEセキュリティ機能要件の対応』に示す。

表 8.2 セキュリティ対策方針とTOEセキュリティ機能要件の対応

種別	セキュリティ対策方針 / TOEセキュリティ機能要件	O.ENCRYPT	O.REMAIN
TOE セキュリティ機能要件	FCS_CKM.1	✔	
	FCS_COP.1	✔	
	FDP_RIP.1		✔
	FPT_RVM.1	✔	✔

以下に、『表 8.2 セキュリティ対策方針と TOE セキュリティ機能要件の対応』の根拠を示す。

O.ENCRYPT

FCS_COP.1 の暗号操作方針により、HDD に保存されたデータが AES アルゴリズムを用いて暗号化されるため、データが不正に解読されることを防ぐことが出来る。

FCS_COP.1 を実施するために、FCS_CKM.1 により、暗号化を行うための暗号鍵が生成される。この時、暗号鍵は電源 ON 時に京セラミタ標準の暗号鍵生成アルゴリズムを用いて毎回生成される。

また、FPT_RVM.1 により、FCS_COP.1、FCS_CKM.1 が迂回されずに必ず実行させることが出来る。

以上により、O.ENCRYPT である、保存データに対して不正に閲覧/出力されることを防止することを実現することが可能となる。

O.REMAIN

FDP_RIP.1 のサブセット残存情報保護方針により、HDD から削除された情報が二度とアクセスされないことを保証することが出来る。

また、FPT_RVM.1 により、FDP_RIP.1 が迂回されずに必ず実行させることが出来る。
以上により、O.REMAIN である、残存データに対して印刷/閲覧されることを防止することを実現することが可能となる。

8.2.2. TOE セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間の依存関係を『表 8.3 TOE セキュリティ機能要件間の依存関係』に示す。

表 8.3 TOE セキュリティ機能要件間の依存関係

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
1	**FCS.CKM.1**	なし	FCS_COP.1 FCS_CKM.4 FMT_MSA.2	2 不要 不要	 8.2.2.1 節参照 8.2.2.2 節参照
2	**FCS_COP.1**	なし	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	1 不要 不要	 8.2.2.1 節参照 8.2.2.2 節参照
3	**FDP_RIP.1**	なし	なし	―	
4	**FPT_RVM.1**	なし	なし	―	

8.2.2.1. FCS_CKM.4 の依存性を必要としない根拠

暗号鍵は、電源 ON 時に毎回生成され揮発性メモリに保持されるが、電源が OFF された時に揮発性メモリの電荷がなくなると記憶内容が失われ、暗号鍵は破棄されるため依存性を必要としない。

8.2.2.2. FMT_MSA.2 の依存性を必要としない根拠

暗号化に使用する暗号鍵は共通鍵１つであり、タイプや期限などといった属性が存在しないため依存性を必要としない。

8.2.3. TOE セキュリティ機能要件の相互作用

以下に、セキュリティ要件の相互作用の関係性について検証する。セキュリティ要件の相互作用の関係を『表 8.4 セキュリティ要件の相互作用』に示す。

表 8.4 セキュリティ要件の相互作用

機能要件	防御を提供している要件		
	迂回	破壊	非活性化
FCS_CKM.1	FPT_RVM.1	N/A	N/A

FCS_COP.1	FPT_RVM.1	N/A	N/A
FDP_RIP.1	FPT_RVM.1	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A

N/A : Not Applicable

迂回

FPT_RVM.1

暗号化に関する FCS_COP.1 は、画像データが HDD に保存される時に必ず呼び出されるため迂回は出来ない。また、暗号鍵を生成する FCS_CKM.1 は、電源 ON 時に必ず呼び出されるため迂回出来ない。

利用者のデータ保護に関する FDP_RIP.1 は、HDD に保存された画像データを削除しようとする際に必ず呼び出されるため迂回出来ない。

破壊

本 TOE は、すべての利用者に対して保存データ及び残存データにアクセスする機能をもっていないため、アクセス制御または情報フロー制御を実施する必要がない。従って、不正なサブジェクトによる TSF の破壊を考慮する必要はない。

非活性化

本 TOE には、セキュリティ機能をオフにする仕組は存在しないため、TSF が非活性化されることはない。

8.2.4. セキュリティ対策方針に対する最小機能強度レベル根拠

本 TOE に対する攻撃者の攻撃能力は低レベルであり、最小機能強度レベル SOF-基本と一貫している。低レベルの攻撃者が行える攻撃は公開情報を利用したものであり、本セキュリティ対策方針が公開されたインタフェースを使って HDD を読み出す攻撃に対抗出来る暗号化と上書き消去であるため、セキュリティ対策方針の内容と最小機能強度レベルは一貫している。

8.2.5. 保証要件根拠

本 TOE は、低レベルの攻撃者による画像データの露顕の脅威に対抗することを目的としているため、低レベルの攻撃への対抗性の保証が必要となる。

このため、EAL3 の選択は妥当である。

また、EAL3 を超える特定の保証対策はない。

8.3. TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』に示す。

表 8.5 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / TOE セキュリティ機能要件	SPF.ENCRYPT	SPF.AGAIN
FCS_CKM.1	✔	
FCS_COP.1	✔	
FDP_RIP.1		✔
FPT_RVM.1	✔	✔

以下に、『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』の根拠を示す。

FCS_CKM.1

セキュリティ機能 SPF.ENCRYPT「暗号化機能」は、電源が ON された際に京セラミタ標準の暗号鍵生成アルゴリズムを用いて必ず鍵長 128bit の暗号鍵の生成を行うため、暗号鍵生成というふるまいを規定したセキュリティ機能要件 FCS_CKM.1 は満たされている。

FCS_COP.1

セキュリティ機能 SPF.ENCRYPT「暗号化機能」は、画像データファイルを HDD に保存する際に、FIPS PUB 197 に合致する、鍵長 128bit の AES アルゴリズムを用いて必ず暗号化することを行い、また HDD に保存された画像データファイルを読み出す際に、必ず復号することを行うため、暗号操作というふるまいを規定したセキュリティ機能要件 FCS_COP.1 は満たされている。

FDP_RIP.1

セキュリティ機能 SPF.AGAIN「上書き消去機能」は、HDD 上の画像データファイルを

削除する際に、論理的な削除だけでなく、実データ領域も上書き消去することを行うため、サブセット残存情報保護というふるまいを規定したセキュリティ機能要件 FDP_RIP.1 は満たされている。

FPT_RVM.1

セキュリティ機能 SPF.ENCRYPT「暗号化機能」、SPF.AGAIN「上書き消去機能」は、迂回されずに必ず実行されるため、TSP の非バイパス性というふるまいを規定したセキュリティ機能要件 FPT_RVM.1 は満たされている。

8.3.2. 保証手段根拠

ここでは、“6.4 保証手段”の有効性について検証する。

表 6-2 に示すように、全ての TOE セキュリティ保証要件は保証手段により示されたドキュメントのセットによって対応付けられる。

また、保証手段に示されたドキュメントによって、本 ST が規定した TOE セキュリティ保証要件 EAL3 が要求する証拠を網羅している。

◆ ACM_CAP.3 許可の管理

【保証手段】 ・Data Security Kit (C) Type Ⅱ 構成管理計画書
・Data Security Kit (C) Type Ⅱ 構成管理規約書
・Data Security Kit (C) Type Ⅱ 構成リスト

【内容】 TOE のバージョンを識別するための命名規則、構成要素の一覧表、構成要素の一意の識別を規定し、TOE の修正に対する保証、TOE の完全性維持を保証する。

◆ ACM_SCP.1 TOE の CM 範囲

【保証手段】 ・Data Security Kit (C) Type Ⅱ 構成管理計画書
・Data Security Kit (C) Type Ⅱ 構成管理規約書

【内容】 構成要素リストで識別されている構成要素に対しての適切な許可を伴う変更管理方法について規定する。

◆ ADO_DEL.1 配付手続き

【保証手段】 ・Data Security Kit (C) Type Ⅱ 配付手順説明書

【内容】 TOE 及び TOE を動作させるための Data Security Kit (C) ハードキーが開発元からユーザに配送されるまでの TOE のセキュリティ維持のために使用される手段、設備、手続きについて規定する。

◆ ADO_IGS.1 設置、生成、及び立上げ手順

【保証手段】 ・Date Security Kit (C) 複合機用設置手順書
・KM-2560/KM-3060 使用説明書 応用編
・2560/3060 Advanced Operation Guide
・KM-2560/KM-3060 サービスマニュアル
・KM-2560/KM-3060 SERVICE MANUAL
・FAX System (M) ファクスシステム設置手順書
・FAX System (M) サービスマニュアル
・FAX System (M) SERVICE MANUAL

【内容】 TOE がセキュアな方法で、設置/起動を行うための手順と確認方法を規定する。

◆ ADV_FSP.1 非形式的機能仕様

【保証手段】 ・Data Security Kit (C) Type Ⅱ 機能仕様書

【内容】 TOE のセキュリティ機能の全ての振る舞いと、機器管理者や TOE 利用者から見える外部インタフェースの詳細な内容を記述する。

◆ ADV_HLD.2 セキュリティ実施上位レベル設計

【保証手段】 ・Data Security Kit (C) Type Ⅱ 上位レベル設計書

【内容】 TOE の機能仕様をサブシステムに詳細化し、その各サブシステムについて、目的、機能を記述し、セキュリティ機能を識別する。また、サブシステム間の相互関係も定義する。

◆ ADV_RCR.1 非形式的対応の実証

【保証手段】 ・Data Security Kit (C) Type Ⅱ 機能対応表

【内容】 TOE のセキュリティ機能の各レベル（要約仕様－機能仕様－上位レベル設計）での完全な対応を記述する。

◆ AGD_ADM.1 管理者ガイダンス

【保証手段】 ・KM-2560/KM-3060 使用説明書 応用編
・2560/3060 Advanced Operation Guide

【内容】 機器管理者が利用できる管理機能とインタフェースの記述、TOE のセキュアな運用に関連する利用者のふるまいについての前提条件などを記述する。

◆ AGD_USR.1 利用者ガイダンス

【保証手段】 ・KM-2560/KM-3060 使用説明書
・KM-2560/KM-3060 使用説明書 応用編
・KM-2560/KM-3060 FAX System (M) 使用説明書
・2560/3060 Operation Guide
・2560/3060 Advanced Operation Guide
・2560i/3060i Operation Guide
・FAX System (M) Operation Guide

【内容】 TOE 利用者が利用できるセキュリティ機能とインタフェースの記述、TOE のセキュアな運用のための警告を含む使用方法、ガイドラインについて記述する。

◆ ALC_DVS.1 セキュリティ手段の識別

【保証手段】 ・Data Security Kit (C) Type Ⅱ 開発セキュリティ規定書

【内容】 TOE を保護するために開発環境で使用される、物理的、手続き的、人的、及びその他のセキュリティ手段を規定する。

◆ ATE_COV.2 カバレージの分析

【保証手段】 ・Data Security Kit (C) Type Ⅱ カバレージテスト分析書

【内容】 TOE のセキュリティ機能のテストの十分性/完全性について記述する。

◆ ATE_DPT.1 テスト：上位レベル設計

【保証手段】 ・Data Security Kit (C) Type Ⅱ 上位レベル設計テスト仕様書

【内容】 TOE のセキュリティ機能のテストを、内部メカニズムの正常な動作から保証することを提供する。

◆ ATE_FUN.1 機能テスト

【保証手段】 ・Data Security Kit (C) Type Ⅱ 機能テスト仕様書

【内容】 TOE のセキュリティ機能のテストを、セキュリティ機能要件を満たすことから保証することを提供する。

◆ ATE_IND.2 独立テスト - サンプル

【保証手段】 ・TOE

【内容】 TOE のセキュリティ機能のテスト環境の再現及びテスト資材を提供する。

◆ AVA_MSU.1 ガイダンスの検査

【保証手段】 ・KM-2560/KM-3060 使用説明書
・KM-2560/KM-3060 使用説明書　応用編
・KM-2560/KM-3060 FAX System (M) 使用説明書
・2560/3060 Operation Guide
・2560/3060 Advanced Operation Guide
・2560i/3060i Operation Guide
・FAX System (M) Operation Guide

【内容】 機器管理者やTOE利用者が、誤使用によりTOEのセキュリティ機能を非セキュアな状態にしてしまう危険性の無いようにTOEの使用方法、運用の前提条件を記述する。

◆ AVA_SOF.1 TOEセキュリティ機能強度評価

【保証手段】 ・Data Security Kit (C) Type Ⅱ 脆弱性分析書

【内容】 TOEのセキュリティ機能のセキュリティメカニズムに対してのTOEセキュリティ機能強度分析について記述する。

◆ AVA_VLA.1 開発者脆弱性分析

【保証手段】 ・Data Security Kit (C) Type Ⅱ 脆弱性分析書

【内容】 TOEの意図する環境において、セキュリティ機能の脆弱性が悪用され得ないことについて記述する。

8.4. PP主張根拠

本STでは、準拠するPPはない。

(最終ページ)