京セラミタ

Data Security Kit (B)

海外版

セキュリティターゲット

第 0.15 版

2005 年 10 月 21 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
2004/4/26	0.01	・新規作成	吉岡	曽根
2004/6/23	0.02	・全般にわたり表現・記述の修正	吉岡	曽根
2004/8/6	0.03	・１章～３章において、指摘項目の修正	吉岡	曽根
2004/9/14	0.04	・TOE の識別を修正 ・１章～８章において、指摘項目の修正	吉岡	曽根
2004/9/17	0.05	・TOE 構成を修正 ・TOE 識別のバージョンを修正	吉岡	曽根
2004/10/21	0.06	・ASE001-01、ASE002-01、ASE003-01、ASE004-01、ASE005-01 対応	吉岡	曽根
2004/11/17	0.07	・ASE006-01、ASE007-01、ASE008-01、ASE009-01、ASE010-01 対応	吉岡	曽根
2004/11/26	0.08	・ASE011-01、ASE012-01、ASE013-01 対応	吉岡	曽根
2005/1/8	0.09	・ASE014-01 対応	吉岡	曽根
2005/1/19	0.10	・保証要件ドキュメントの名称を変更	吉岡	曽根
2005/4/6	0.11	・ASE015-01 対応 ・保証要件ドキュメントの名称を変更	吉岡	曽根
2005/4/26	0.12	・「保守担当者」を「サービス担当者」に変更	吉岡	曽根
2005/6/14	0.13	・O.METHOD に関する記述を修正 ・表 6.2 の名称を修正	吉岡	曽根
2005/8/4	0.14	・表 6.2 の記載を一部修正 ・8.3.3 保証手段の証拠資料を一部修正	吉岡	曽根
2005/10/21	0.15	・OE.POWER に関する記述を追加	吉岡	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 (B) 海外版 セキュリティターゲット

バージョン： 第 0.15 版

作成日： 2005/10/21

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 (B) Software

バージョン： V1.10E

作成者： 京セラミタ株式会社

注) バージョン V1.10E は次の ROM バージョンによって構成されている。

MAIN : 29101B-0210.00

PRINTER : 2FB_3F00.001.200

1.1.3. 適用する CC のバージョン

ISO/IEC 15408:1999

Interpretations-0210 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:概説を一般モデル バージョン2.1 1999年8月 CCIMB-99-031
  (平成13年1月翻訳 第1.2版 情報処理振興事業協会 セキュリティセンター)
- 情報技術セキュリティ評価のためのコモンクライテリア パート２:セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032
  (平成13年1月翻訳 第1.2版 情報処理振興事業協会 セキュリティセンター)
- 情報技術セキュリティ評価のためのコモンクライテリア パート３:セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033
  (平成13年1月翻訳 第1.2版 情報処理振興事業協会 セキュリティセンター)
- Common Criteria 補足-0210

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(MFP)、海外版 「KM-8030/KM-6030、CS-8030/CS-6030」に搭載する「Data Security Kit (B) Software」について記述し

ている。
複合機とは、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を有する製品である。(以後、コピー機能、プリンタ機能、及びネットワークスキャナ機能を通常機能と呼ぶ。) 利用者は、複合機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、複合機「KM-8030/KM-6030、CS-8030/CS-6030」にオプション製品として搭載され、通常機能、及び残存データ保護のためのセキュリティ機能を提供するソフトウェアモジュールである。

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の処理後、または複合機内部に保存されたデータの論理的な削除後の残存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 2.1 1999 年 8 月 CCIMB-99-031
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2:セキュリティ機能要件 バージョン 2.1 1999 年 8 月 CCIMB-99-032
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3:セキュリティ保証要件 バージョン 2.1 1999 年 8 月 CCIMB-99-033
- Common Criteria 補足-0210
- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 1999 Version 2.1 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 1999 Version 2.1 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements

August 1999 Version 2.1 CCIMB-99-033

- Common Criteria CCIMB Interpretations-0210
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part1, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part2, 99/12
- ISO/IEC 15408, Information Technology - Security techniques - Evaluation criteria for IT security - Part3, 99/12

2. TOE 記述

2.1. TOE 種別

本 TOE は、「Data Security Kit (B) Software」と呼ばれる、複合機にセキュリティ機能を提供するソフトウェアモジュール製品である。

※通常機能を提供するソフトウェアモジュールも TOE の範囲に含まれる。

2.2. 用語の定義

本 ST で使用される用語の定義を表 2.1 で示す。

表 2.1 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。
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。
PC 送信	スキャンされた画像をユーザが指定したファイルフォーマットで圧縮し、指定されたクライアント PC のユーティリティに向かって送信する処理。
E-mail 送信	スキャンされた画像をユーザが指定したファイルフォーマットで圧縮し、あらかじめ登録されている E-mail サーバに向かって、SMTP プロトコルに従って送信する処理。
TWAIN	TWAIN 対応のアプリケーションを利用することにより、複合機にセットされた原稿をクライアント PC からの操作でクライアント PC に取り込む処理。

ジョブ	コピー機能、プリンタ機能、ネットワークスキャナ機能の１つの処理の単位のこと。ジョブの中には原稿の画像データも含まれる。
印刷ジョブ	ジョブの中で、プリンタ機能として処理されるジョブのこと。
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。
プリンタドライバ	クライアントPCに表示された文字や画像を複合機のプリンタに転送するなど、複合機のプリンタ機能を制御するためにクライアントPCにインストールするソフト。
e-MPS	enhanced Multiple Printing Systemの略。 プリンタ機能の拡張機能で、クライアントPCからのデータをもとに各種の印刷ジョブを実行することが出来る。
Data Security Kit (B) ハードキー	セキュリティ機能を利用する際に、必須で取り付ける必要のある基板。Data Security Kit (B)の導入時にサービス担当者によって設置される。運用中にData Security Kit (B) ハードキーが取り外された場合、セキュリティ機能が無効になるのでは無く、複合機が何も動作しなくなる。
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。 外部インターフェイスであり、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。
NIC	Network Interface Cardの略。 TOEを内部ネットワーク(LAN)に接続するための拡張カード。
スキャナエンジン	原稿をスキャンする装置を制御するモジュール。
印刷エンジン	データを紙に出力し、印刷する装置を制御するモジュール。
フォーム	画像の重ね合わせ(イメージ合成)機能において、元画像となる合成元画像のことを指す。フォームに対し、読み取った原稿を重ね合わせてコピーすることが出来る。

2.3. TOE概要

2.3.1. TOEの利用目的

本TOEは、オフィスや学校で利用される複合機に搭載され、HDD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）の各処理後に HDD 上に残存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、様々な文書を扱うオフィスや学校で使用され、内部ネットワーク(LAN)に接続される。また、プリンタ出力用にローカルポート（パラレルポート、USB ポート、シリアルポート）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TOEマシン管理者は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。但し、外部から LAN/ローカルポートを通して複合機を利用する際は、画像データを入力し複合機から出力するのみの利用であり、LAN/ローカルポートを通して複合機に長期保存された画像データを取り出すことは出来ない。

図 2.1 にオフィスにおける一般的な利用環境を示す。

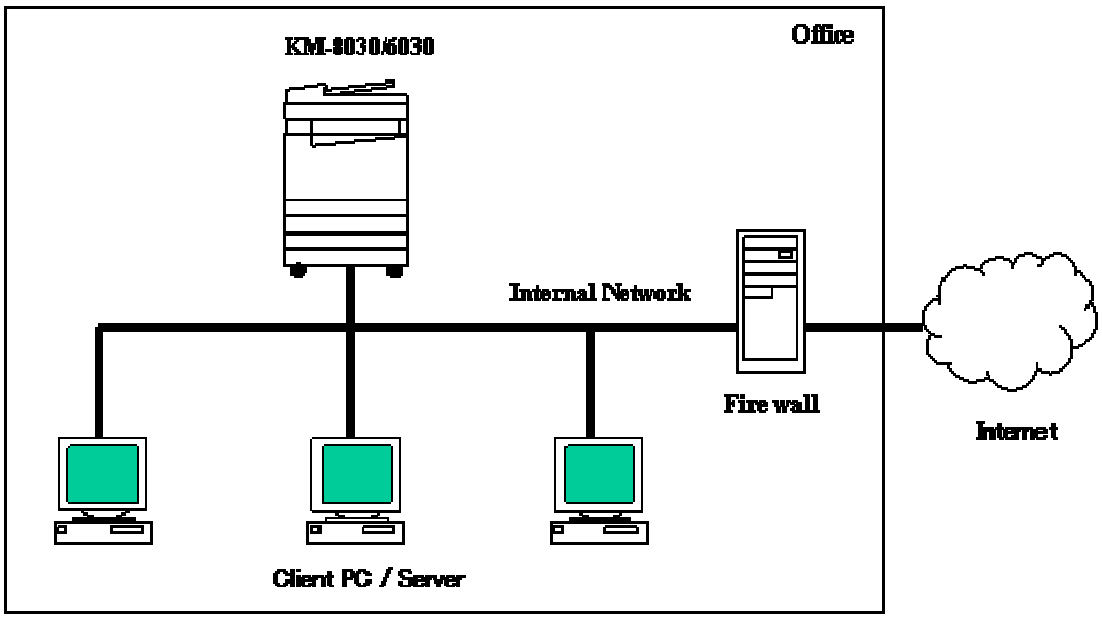

図 2.1 オフィスにおける一般利用

2.3.3. TOE の関連者

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

TOE マシン管理者：

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。TOE マシン管理者は、機械本体に対する特権を有する。

【 利用方法 】

TOE マシン管理者は、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 】

- TOE マシン管理者は、機器及び各ソフトウェア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 マシン管理者は、TOE 利用者が複合機を利用するために利用者個別の設定が必要な場合には、利用者情報の登録/設定を行う。
- TOE マシン管理者は、複合機の運用管理をするためにクライアント PC 等に必要なソフトウェアのインストールを行う。
- TOE マシン管理者は、TOE マシン管理者インタフェースを用いて上書き消去方式の設定値変更、HDD フォーマット機能の実行、TOE 管理者暗証番号の変更を行う。

TOE 利用者：

オフィスや学校内で 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等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、Data Security Kit (B) ハードキーを取り付け、TOE の立上げ（動作可能にする）を行い、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。その他、TOE マシン管理者としての役割も持ち、緊急の際に TOE マシン管理者の許可を得て、TOE マシン管理者インタフェースを用いて上書き消去方式の設定値変更、HDD フォーマット機

能の実行、TOE 管理者暗証番号の変更を行うことも出来る。(各機能の詳細は後述)

【 利用手順 】

- 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、Data Security Kit (B) ハードキーを取り付け、TOE を導入し、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。
- サービス担当者は、TOE マシン管理者の許可を得て、TOE マシン管理者インタフェースを用いて上書き消去方式の設定値変更、HDD フォーマット機能の実行、TOE 管理者暗証番号の変更を行う。

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 はメインボードとプリンタボード上にある、MAIN ROM と PRINTER ROM のソフトウェアのことを指す。

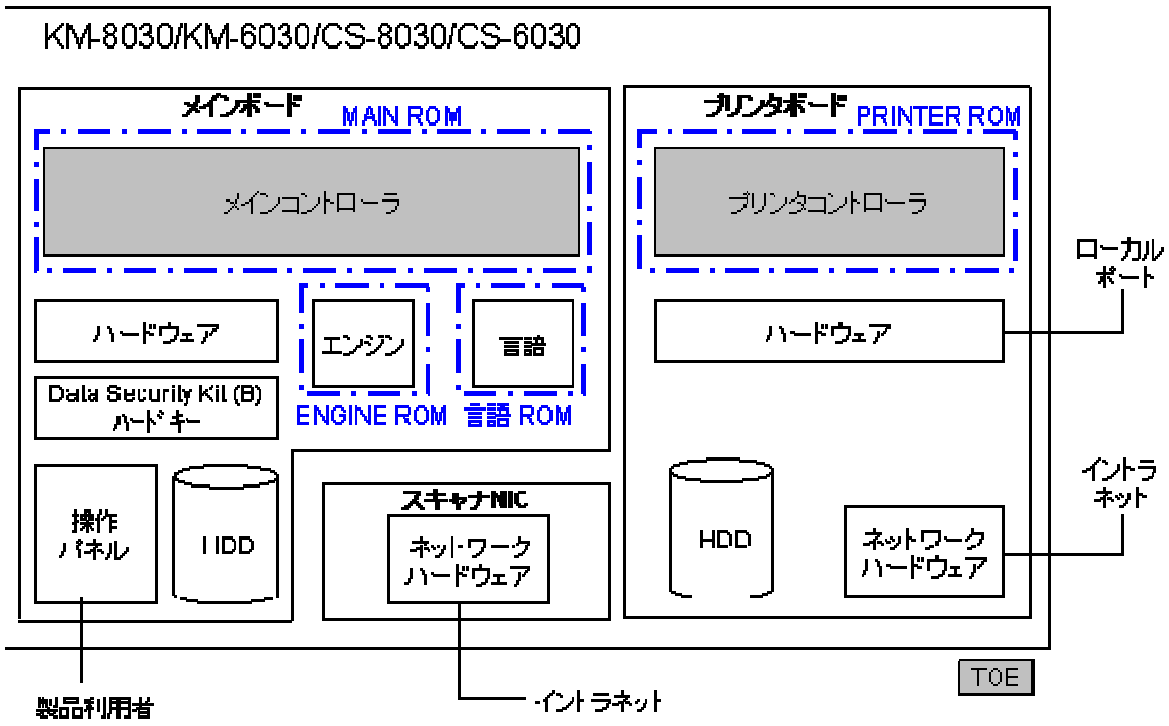

図 2.2 TOE の構成図

2.4.2. TOE の動作環境

「KM-8030/KM-6030、CS-8030/CS-6030」は、ハードウェアとソフトウェアで構成される。

ハードウェア部分は、メインボードとネットワークスキャナ用 NIC、プリンタボードから構成され、ボード毎に CPU が存在する。また、メインボードとプリンタボードにはそれぞれ HDD が存在し、ネットワークスキャナ用 NIC とプリンタボードにはそれぞれネットワーク接続用のネットワークハードウェアが存在する。プリンタボードには、ローカル接続用のローカルポート（パラレルポート、USB ポート、シリアルポート）が存在する。

また、TOE を動作させるには、Data Security Kit (B) ハードキーが必要となる。仮に運用中に Data Security Kit (B)ハードキーが取り外された場合、セキュリティ機能が無効になるのでは無く、複合機が何も動作しなくなる。

その他、CPU、Memory、スキャナ部、印刷部などは図 2.2 ではハードウェアとして総称する。

メインボード上の MAIN ROM 内にはメインコントローラが存在する。メインコントローラは、コピーモジュール、スキャナモジュール、ネットワークモジュール、コピー/ネットワークスキャナ共通のライブラリにより構成される。

また、その他に TOE を動作させる為の基本ソフトウェアとして、言語モジュールとエンジンモジュールが存在する。それぞれが、言語 ROM、ENGINE ROM 内に格納されている。言語 ROM は、必要に応じ変更することで、多言語に対応することが出来る。ENGINE ROM には、スキャナエンジンや印刷エンジンを制御するモジュールが含まれる。

プリンタボード上の PRINTER ROM 内にはプリンタコントローラが存在する。プリンタコントローラは、プリンタモジュール、ネットワークモジュール、プリンタ用ライブラリ、ネットワークサービスにより構成される。

図 2.2 に示したハードウェア、ネットワークハードウェア、HDD の諸元を表 2.2 に示す。

表 2.2 ハードウェア、ネットワークハードウェア、HDD の諸元

装置名称	種別	性能	備考
メインボード	CPU	源発振：８．２９MHz （内部１３２MHz）	－
	Memory	１２８Mbyte	－
	HDD	２０Gbyte	－

スキャナ NIC	ﾈｯﾄﾜｰｸﾊｰﾄﾞｳｪｱ	10Base-T/100Base-Tx	－
プリンタボード	CPU	６００MHz	－
	Memory	６４Mbyte	オプション RAM 32～256 MByte
	HDD	１０Gbyte	－
	ﾈｯﾄﾜｰｸﾊｰﾄﾞｳｪｱ	10Base-T/100Base-Tx	－

2.4.3. TOE を構成するソフトウェア

TOE を構成するソフトウェアを 表 2.3 に示す。網掛けは TOE を示す。

表 2.3 TOE を構成するソフトウェア

ROM 名称	種別	備考
MAIN ROM	メインコントローラ	－
	コピーモジュール	－
	スキャナモジュール	－
	ネットワークモジュール	－
	コピー/ネットワークスキャナ共通のライブラリ	HDD 上書き消去機能、管理者認証機能が含まれる
ENGINE ROM	エンジンモジュール	スキャナエンジン 印刷エンジン
言語 ROM	言語モジュール	文字列データ 仕向け地に合わせる
PRINTER ROM	プリンタコントローラ	－
	プリンタモジュール	－
	ネットワークモジュール	－
	プリンタ用ライブラリ	HDD 上書き消去機能が含まれる
	ネットワークサービス	－

2.4.4. TOE の論理的構成

TOE の論理的構造の概念図を 図 2.3 で示す。

TOE は、セキュリティ機能と共に、コピー機能のような通常の複合機としての機能も

有する。以下の機能が TOE の論理的範囲に含まれる。

- HDD 上書き消去機能
  HDD に保存されたデータの論理的な削除後に、実データ領域に対して、無意味な文字列を上書きすることにより、実データ領域を完全に消去する機能。
- 管理者認証機能
  TOE マシン管理者を操作パネルから入力された TOE 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。
  LAN 経由で送信する PC 送信と、E-mail 経由で送信する E-mail 送信がある。
  また、TWAIN 対応アプリケーションを利用することにより、複合機にセットされた原稿をクライアント PC からの操作でクライアント PC に取り込む TWAIN もある。
- 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。
- ジョブ管理機能
  HDD 上に保存されたジョブ/印刷ジョブを管理する機能。ジョブ/印刷ジョブの編集/出力/削除を行うことが出来る。

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。

- ユーザインターフェイス機能
  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。

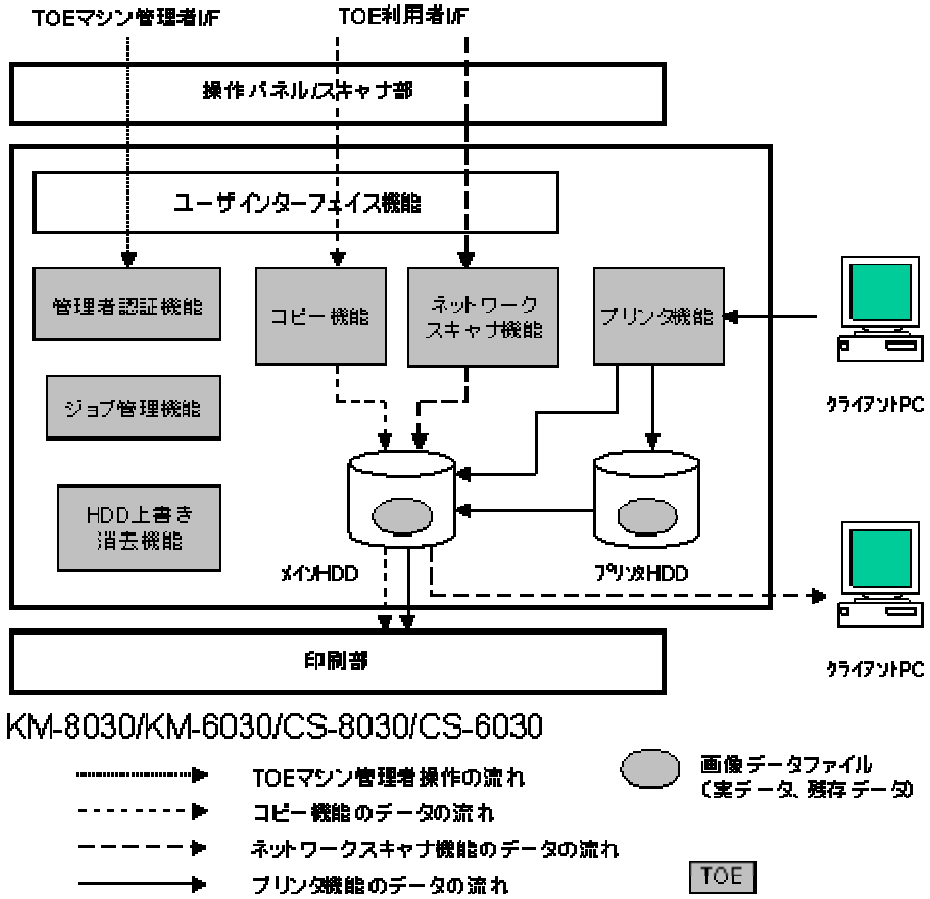

図 2.3 TOE の論理図

2.5. TOE の機能

TOE が提供する機能は以下である。

- セキュリティ機能
  - HDD 上書き消去機能
  - 管理者認証機能
- 複合機としての通常機能
  - コピー機能
  - ネットワークスキャナ機能
  - プリンタ機能
  - ジョブ管理機能

2.5.1. TOE のセキュリティ機能

2.5.1.1 HDD 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、HDD 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、プリンタ機能を使用し、HDD に保存された画像データを削除する際、画像データの論理的な削除後に、実データ領域に対して、無意味な文字列を上書きすることにより、実データ領域を完全に消去する。

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
上書き消去するデータの実データ領域全体に NULL（0x00）を書き込む

2.5.1.2 管理者認証機能

TOE マシン管理者を操作パネルからの TOE 管理者暗証番号により識別認証する。
識別認証された TOE マシン管理者は、HDD の全領域を上書き消去する「HDD フォーマット機能」の実行や、HDD 上書き消去機能において３回上書き方式と１回上書き方式を変更することが出来る。
ここで、３回上書き方式が初期値であり、処理効率よりも安全性を重視する場合に設定する。１回上書き方式は処理効率を重視する場合に設定する。また、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。

2.5.2. 通常機能

TOE は以下の基本機能を提供している。また、これらの機能を使用する上において、HDD に保持された画像データが論理的な従来の削除処理をされる際に、セキュリティ機能である「HDD 上書き消去機能」が機能することになる。

■コピー機能

TOE 利用者により、スキャナから読み込んだ原稿のコピーを行う。(通常コピー)
通常コピーを行う際には、メインボード上の HDD に画像データをスプール保存し、出力が完了した後、削除されることになる。
また、コピー機能は文書管理機能も有する。
文書管理機能には、蓄積共有ボックスとジョブ結合ボックス、フォーム用ボックスが存在する。各ボックスは全てメインボード上の HDD に存在する。
【文書管理機能】

- 蓄積共有ボックス -

スキャナから読み込んだ原稿の画像データをジョブとしてボックスに保存しておくことができ、保存されたジョブは必要な時に出力することが出来る。

- ジョブ結合ボックス -

スキャナから読み込んだ原稿、又はプリンタドライバから送信された画像データをジョブとしてボックスに保存しておくことが出来る。ジョブ結合ボックスの番号を指定して保存する。保存されたジョブは必要な時に出力することが出来る。保存されたジョブは、出力時に結合して出力することが出来る。また、ボックスに 1 日～7 日間の保存期間を設定することもでき、保存日から指定期間が過ぎると自動的に削除される。

- フォーム用ボックス -

コピー時に合成するフォームをあらかじめ登録しておくことが出来る。
スキャナから読み込んだ原稿、又はプリンタドライバから送信された画像データをフォームとしてボックスに登録する。

■ネットワークスキャナ機能

TOE 利用者により、スキャナから読み込んだ原稿の画像データをクライアント PC に送信することが出来る。LAN 経由で送信する PC 送信と、E-mail 経由で送信する E-mail 送信がある。
また、TWAIN 対応のアプリケーションを利用することにより、複合機にセットされた原稿をクライアント PC からの操作でクライアント PC に取り込むことも出来る。
ネットワークスキャナ機能を使用する際には、メインボード上の HDD に画像データをスプール保存し、送信が完了した後、削除されることになる。
【注意】文書管理機能により保存されているジョブを用いて PC 送信、E-mail 送信、TWAIN による取り込みを行うことは出来ない。

■プリンタ機能

TOE 利用者により、プリンタドライバから送信された画像データを紙に出力する（通常プリント)。LAN 経由による出力と、ローカルポートによる出力がある。
また、プリンタ機能は、単に出力する他に、以下のような拡張機能(e-MPS)も有する。
プリンタ機能を使用する際には、通常プリント/拡張機能共に、一旦メインボード上の HDD に画像データをスプール保存し、出力が完了した後、削除されることになる。
【拡張機能(e-MPS)】

- 一時保存 -

印刷ジョブを一時的にプリンタボード上の HDD に保存する。一時保存領域を越えた場合に古いものから削除される。保存された印刷ジョブは必要な時に出力する

ことが出来る。

- 恒久保存 -

  印刷ジョブを恒久的にプリンタボード上の HDD に保存する。TOE 利用者によりジョブを削除するまでは削除されない。保存された印刷ジョブは必要な時に出力することが出来る。

- ジョブ結合ボックス -

  印刷ジョブを、メインボード上のジョブ結合ボックスに保存する。ジョブ結合ボックスのボックス番号を指定して送信する。

- フォーム集 -

  印刷ジョブを、メインボード上のフォーム用ボックスに保存する。

- クイックコピー -

  印刷ジョブを出力した後､再度出力出来るように一時的にプリンタボード上の HDD に保存する。保存された印刷ジョブは電源 OFF された時に削除される。(実際は、次回電源 ON 時に削除処理が行われる）また、保存領域を越えた場合に古いものから削除される。

- 試し刷り後、保留 -

  印刷ジョブの１部だけを出力し、内容を確認した後出力出来るようにプリンタボード上の HDD に保存される。保存された印刷ジョブは電源 OFF された時に削除される。(実際は、次回電源 ON 時に削除処理が行われる）また、保存領域を越えた場合に古いものから削除される。

- バーチャルメールボックス -

  印刷ジョブをプリンタボード上の HDD に設けられた仮想メールボックスに保存する。送信した時点では印刷されず、機械本体の操作パネルからメールボックス番号を指定された時に、保存された印刷ジョブを出力する。出力すると、その印刷ジョブは削除される。

- プライベートプリント -

  印刷ジョブにアクセスコードを付加し、一時的にプリンタボード上の HDD に保存する。送信した時点では印刷されず、機械本体の操作パネルから、該当アクセスコードが入力された時に、保存された印刷ジョブを出力する。出力すると、その印刷ジョブは削除される。保存された印刷ジョブは電源 OFF された時に削除される。(実際は、次回電源 ON 時に削除処理が行われる)

- ジョブ保留 -

  プライベートプリントと同等機能であるが、電源 OFF された時にでも、保存された印刷ジョブは削除されない。

■ジョブ管理機能

コピー機能、プリンタ機能に含まれる機能である。
それぞれの機能により、HDD に保存されたジョブ/印刷ジョブを管理する。ジョブ/印刷ジョブの、編集/出力/削除を行うことが出来る。
操作パネルからと、クライアント PC 上のユーティリティ(下記に記述)から操作することが出来る。

【ユーティリティについて】
クライアント PC に各種ツールをインストールすることにより、上述の機能をサポートする。

- 「KM-NET Printer Disk Manager」、「KM-NET for Clients」 -
  プリンタボード上の HDD に保存された印刷ジョブの編集/出力/削除を行うためにジョブ管理機能の操作を行う。
  「KM-NET Printer Disk Manager」が、TOE マシン管理者用のツールであり、「KM-NET for Clients」が、TOE 利用者用のツールである。
- プリンタドライバ -
  プリンタ機能を使用する場合に必要となる。
  拡張機能を使用する場合の設定も全てプリンタドライバから行う。
- Scanner File Utility -
  ネットワークスキャナ機能の、PC 送信を行う場合に必要となる。
  TOE から送信された画像データを受信し、指定されたフォルダにデータを保存する。(自 PC 内のフォルダでも、ネットワーク経由の共有フォルダでも可能)
- TWAIN ドライバ -
  ネットワークスキャナ機能の、TWAIN を行う場合に必要となる。
  画像処理を行う市販のアプリケーションから呼び出され、TWAIN ドライバからの操作により、TOE にセットされた原稿を読み込み、画像データを取り込む。

通常機能全体に渡り、コピー機能/プリント機能/ネットワークスキャナ機能の指示が同時、又は、重なって行われた場合、その時の優先順位に従って、順次処理を行う。従って、指示後すぐに処理が行えなかった場合でも、確実に最後まで処理は完了する。また、コピー機能/プリント機能/ネットワークスキャナ機能の処理が完了する前に、TOE 利用者からの指示により、処理を中止することも出来る。

TOE の機能と画像データの保存場所、削除手段の関係を示した表を表 2.4 に示す。

表 2.4 TOE の機能と保存場所と削除手段

基本機能	詳細機能	保存場所	保存形態	削除手段
コピー機能	通常コピー	メイン HDD	ｽﾌﾟｰﾙ保存	処理完了後、又は処理中止後
	蓄積共有ボックス	メイン HDD	長期保存	操作パネルからの削除操作、又は文書登録処理中止後
	ジョブ結合ボックス	メイン HDD	長期保存	操作パネルからの削除操作 又は 1 日～7 日間の保存期間経過後に自動削除 又は 文書登録処理中止後
	フォーム用ボックス	メイン HDD	長期保存	操作パネルからの削除操作、又は文書登録処理中止後
ネットワーク スキャナ機能	PC 送信/E-mail 送信 /TWAIN	メイン HDD	ｽﾌﾟｰﾙ保存	処理完了後、又は処理中止後
プリンタ機能	通常プリント	メイン HDD	ｽﾌﾟｰﾙ保存	処理完了後、又は処理中止後
	一時保存	プリンタ HDD	長期保存	ユーティリティからの削除操作 又は 保存領域を越えて保存しようとした時、最も古いジョブが削除される 又は ジョブ登録処理中止後
	恒久保存	プリンタ HDD	長期保存	ユーティリティからの削除操作 又は ジョブ登録処理中止後
	ジョブ結合ボックス	メイン HDD (ジョブ結合ボックス)	長期保存	操作パネルからの削除操作 又は 1 日～7 日間の保存期間経過後に自動削除 又は ジョブ登録処理中止後
	フォーム集	メイン HDD (フォーム用ボックス)	長期保存	操作パネルからの削除操作 又は ジョブ登録処理中止後
	クイックコピー	プリンタ HDD	長期保存	操作パネルからの削除操作 又は 電源 OFF されると次回電源 ON 時に削除 又は 保存領域を越えて保存しようとした時、最も古いジョブが削除される 又は ジョブ登録処理中止後
	試し刷り後、保留	プリンタ HDD	長期保存	操作パネルからの削除 又は 電源 OFF されると次回電源 ON 時に削除 又は 保存領域を越えて保存しようとした時、最も古いジョブが削除される 又は ジョブ登録処理中止後
	ﾊﾞｰﾁｬﾙﾒｰﾙﾎﾞｯｸｽ	プリンタ HDD	長期保存	操作パネル、ユーティリティからの削除操作 又は 出力完了後 又は ジョブ登録処理中止後
	ﾌﾟﾗｲﾍﾞｰﾄﾌﾟﾘﾝﾄ	プリンタ HDD	長期保存	操作パネルからの削除操作 又は

				出力完了後 又は 電源 OFF されると次回電源 ON 時に削除 又は ジョブ登録処理中止後
	ジョブ保留	プリンタ HDD	長期保存	操作パネルからの削除操作、又はジョブ登録処理中止後

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い、処理終了後にそのデータの管理領域を論理的に削除するだけである。このため、実データ領域が残存情報として残ってしまう。この残存情報には、データとしてはコピー/プリント/ネットワークスキャナ等の処理で行ったデータと同じデータが入っているため、何らかの方法によりアクセスされると、データを丸ごと持ち出されてしまうことも起こり得る。場合によっては、このデータには利用者の機密情報が含まれることもあり、持ち出されると非常に重大な問題となる可能性もある。

そこで、TOE が保護すべき資産を以下に示す。

■残存データ

メインボード上 HDD 内に、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の残存データ

及び、プリンタボード上 HDD 内に、長期保存された画像データが、論理的に削除された後の残存データ

対象となるデータは以下のファイルに格納されている。

（以下は HDD に保存される画像データの種別）

◆ メインボード上 HDD の画像データファイル

・通常コピー時のスプール保存ジョブ
・蓄積共有ボックス内のジョブ
・ジョブ結合ボックス内のジョブ
・フォーム用ボックス内のジョブ
・ネットワークスキャナ時(PC 送信/E-mail 送信/TWAIN)のスプール保存ジョブ
・プリンタの通常プリント機能、及び全てのプリンタ拡張機能を使用した際のスプール保存ジョブ

◆ プリンタボード上 HDD の画像データファイル

・プリンタ拡張機能：一時保存機能の印刷ジョブ
・プリンタ拡張機能：恒久保存機能の印刷ジョブ

・プリンタ拡張機能：クイックコピー機能の印刷ジョブ
・プリンタ拡張機能：試し刷り後、保留機能の印刷ジョブ
・プリンタ拡張機能：バーチャルメールボックス機能の印刷ジョブ
・プリンタ拡張機能：プライベートプリント機能の印刷ジョブ
・プリンタ拡張機能：ジョブ保留機能の印刷ジョブ

3. TOE セキュリティ環境

3.1. 前提条件

TOE が安全な使用環境に配置されるための使用環境として、以下の前提条件を必要とする。

A.PHYSICAL ： TOE と資産の物理的安全性

TOE を搭載する複合機は、TOE の関連者のみが利用可能な物理的に保護された場所に設置されていること。

A.ADMIN ： 管理者の信頼性

TOE マシン管理者は、信用できる人物であり、不正を行わない人物であること。

A.CE ： サービス担当者の信頼性

TOE のサービス担当者は、不正を行わないこと。

3.2. 脅威

前提条件で示した使用環境下にて、想定される脅威について述べる。
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 ： 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 に保持されている残存データを閲覧/出力する。また、上書き消去中における複合機の電源の切断により、上書き消去が未完状態となった HDD 上の残存データを閲覧/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.METHOD ： 上書き消去方式の適用

HDD の上書き消去に際し、安全性と処理効率の兼ね合いを考慮し、３回上書き方式、または１回上書き方式を適用する。

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.REMAIN ： 残存データの上書き消去

TOE は、HDD に保存されている残存データが不正に閲覧／出力されないように、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。

O.METHOD ： 上書き消去方式の設定機能

TOE は、HDD の上書き消去方式を３回上書き方式、または 1 回上書き方式のいずれかに設定できる機能を TOE マシン管理者に提供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を述べる。

OE.PHYSICAL ： TOE と資産の物理的防護

TOE マシン管理者は、不審人物が勝手に TOE を利用することの無いよう、TOE が搭載された複合機を、入退室管理された TOE の関連者のみが利用可能な場所に設置する。

OE.ADMIN ： 管理者の人選

TOE を導入する組織は、課せられた役割を忠実に実行し、不正を行わない適切な人物を TOE マシン管理者として人選する。

OE.CE ： サービス担当者の監視

サービス担当者が TOE のメンテナンス等を行う際は、必ず TOE マシン管理者が監視する。

OE.POWER ： 電源の切断防止

TOE を搭載した複合機の使用中に電源の切断が発生した際には、TOE 利用者は速やかに電源の再投入を行う。

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

FIA_UAU.2	アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.7　　保護された認証フィードバック

下位階層：なし

FIA_UAU.7.1

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

[割付：フィードバックのリスト]
・ダミー文字（＊）
※入力した文字数分のダミー文字

依存性：FIA_UAU.1 認証のタイミング

FIA_UID.2　　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

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

依存性：なし

FIA_SOS.1　　秘密の検証

下位階層：なし

FIA_SOS.1.1

TSF は、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

［割付：定義された品質尺度］
・数字（0～9）　８文字固定

［詳細化：秘密］
・TOE 管理者暗証番号

依存性：なし

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]
・メインボード上 HDD の画像データファイル
・プリンタボード上 HDD の画像データファイル

依存性：なし

FMT_MTD.1　　TSF データの管理

下位階層：なし

FMT_MTD.1.1

TSFは、[割付：TSFデータのリスト]を[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]する能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：TSFデータのリスト]
・TOE管理者暗証番号

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

[割付：その他の操作]
・なし

[割付：許可された識別された役割]
・TOEマシン管理者

依存性：FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_MOF.1　　セキュリティ機能のふるまいの管理

下位階層：なし

FMT_MOF.1.1

TSFは、機能[割付：機能のリスト][選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：機能のリスト]
・HDD上書き消去機能

[選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]
・のふるまいを改変する、を動作させる

[割付：許可された識別された役割]
・TOEマシン管理者

依存性：FMT_SMR.1 セキュリティ役割
FMT_SMF.1 管理機能の特定

FMT_SMR.1　　セキュリティ役割

下位階層：なし

FMT_SMR.1.1

TSFは、役割[割付：許可された識別された役割]を維持しなければならない。

[割付：許可された識別された役割]

・TOEマシン管理者

FMT_SMR.1.2

TSFは、利用者を役割に関連付けなければならない。

依存性：FIA_UID.1 識別のタイミング

FMT_SMF.1　　管理機能の特定

下位階層：なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：TSF によって提供されるセキュリティ管理機能のリスト]

[割付：TSF によって提供されるセキュリティ管理機能のリスト]
・表 5.1 にセキュリティ管理機能のリストを示す

表 5.1 管理項目一覧

機能要件	管理対象項目	実際の管理項目
FIA_UAU.2	管理者による認証データの管理	管理者による TOE 管理者暗証番号の管理
FIA_UAU.7	予見される管理アクティビティはない	なし
FIA_UID.2	利用者識別情報の管理	なし(識別の対象は TOE マシン管理者だけであり、TOE は管理者専用の操作を行うことにより、TOE マシン管理者を識別するため、利用者識別情報を管理する必要はない)
FIA_SOS.1	秘密の検証に使用される尺度の管理	なし（秘密の尺度は、数字８文字固定であり、管理行為は不要である）
FDP_RIP.1	いつ残存情報保護を実施するかの選択（すなわち、割当てあるいは割当て解除において）が、TOEにおいて設定可能にされる	なし（割当て解除時にのみ残存情報保護を実施するため、残存情報保護のタイミングを管理する必要はない）
FMT_MTD.1	TSFデータと相互に影響を及ぼし得る役割のグループを管理すること	なし(役割はTOEマシン管理者だけであり、管理行為は不要であるため)
FMT_MOF.1	TSFの機能と相互に影響を及ぼし得る役割のグループを管理すること	なし(役割のTOEマシン管理者だけであり、管理行為は不要であるため)

機能要件	管理対象項目	実際の管理項目
FMT_SMR.1	役割の一部をなす利用者のグループの管理	なし(利用者のグループはなく、役割に関連付けられる利用者は「TOEマシン管理者」のみであり、管理行為は不要であるため)
FMT_SMF.1	予見される管理アクティビティはない	なし
FPT_RVM.1	予見される管理アクティビティはない	なし

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 5-2 で識別する。なお、EAL3 を超える特定の保証対策は無い。

表 5.2 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。

セキュリティ機能強度が要求される機能要件は以下の通りであり、また、それぞれに対し、明示された機能強度を以下に示す。

・FIA_UAU.2　-　機能強度　:　SOF-基本
・FIA_UAU.7　-　機能強度　:　SOF-基本
・FIA_SOS.1　-　機能強度　:　SOF-基本

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.AGAIN	SPF.ADMIN
FIA_UAU.2		○
FIA_UAU.7		○
FIA_UID.2		○
FIA_SOS.1		○
FDP_RIP.1	○	
FMT_MTD.1		○
FMT_MOF.1		○
FMT_SMR.1		○
FMT_SMF.1		○
FPT_RVM.1	○	○

6.1.1. HDD 上書き消去機能

HDD 上書き消去機能は、以下の機能を提供する。

SPF.AGAIN

HDD 上書き消去機能は、HDD 上に保存されたデータを、論理的に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。

上書き消去の方式は以下の２通りであり、TOE マシン管理者のみ変更が可能である。デフォルト値は、３回上書き方式である。

□ 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

□ 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) を書込む

また、HDD 上書き消去機能は、メインボードとプリンタボードのぞれぞれの HDD に対して独自に実行される。
但し、上書き消去方式の設定値と、下記 HDD フォーマット機能の実行に対しては、メインボード/プリンタボードの区別なく、統一して行う。

また、HDD 上書き消去機能は、下記のいずれかのタイミングで実行出来る。
・出力 又は 電源 OFF 又は 削除操作により、ジョブが削除された時
・TOE マシン管理者により、HDD フォーマット機能が実行された時
※ 電源 OFF による上書き消去は、実際には次回電源 ON 時に消去処理が実行される。
この HDD 上書き消去機能は、上記のタイミングにおいて必ず呼び出され、迂回されずに実行される。

メインボード HDD 上書き消去機能

メインボード上HDDの画像データファイルに保存される各ジョブに対する上書き消去機能は以下の通りである。

■ HDD 上にスプール保存されたデータを完全に消去する機能
HDD 上にスプール保存されるデータは以下の通り。
・コピー時のスプール保存ジョブ
・ネットワークスキャナ時(PC 送信/E-mail 送信/TWAIN)のスプール保存ジョブ
・プリンタの通常プリント、及び全てのプリンタ拡張機能を使用した際のスプール保存ジョブ

HDD 上にスプール保存されるデータが上書き消去されるタイミングは以下のパターンである。
・コピー/プリント（通常プリント機能、及び全てのプリンタ拡張機能を含む）/ネットワークスキャナの処理の正常終了後
・これらの処理中の、中止操作による中止処理後

■ HDD 上に長期保存されたデータを TOE 利用者の削除操作により完全に消去する機能
削除操作は、操作パネルから行うことが可能。
また、ジョブ結合ボックスで、保存期間を指定した場合は、TOE 利用者の削除操作だけではなく、指定期間経過後にデータが削除される
HDD 上に長期保存されるデータは以下の通り。

・蓄積共有ボックス内のジョブ
・ジョブ結合ボックス内のジョブ
・フォーム用ボックス内のジョブ

また、上記のデータを HDD に保存中に、中止操作により中止処理を行った後にも上書き消去が行われる。

プリンタボード HDD 上書き消去機能

プリンタボード上HDDの画像データファイルに保存される各ジョブに対する上書き消去機能は以下の通りである。

■ HDD 上に長期保存されたデータを TOE 利用者の削除操作により完全に消去する機能
削除操作は、操作パネルからと関連ユーティリティから行うことが可能。
HDD 上に長期保存されるデータは以下の通り。
・プリンタ拡張機能：一時保存機能の印刷ジョブ
・プリンタ拡張機能：恒久保存機能の印刷ジョブ
・プリンタ拡張機能：クイックコピー機能の印刷ジョブ
・プリンタ拡張機能：試し刷り後、保留機能の印刷ジョブ
・プリンタ拡張機能：バーチャルメールボックス機能の印刷ジョブ
・プリンタ拡張機能：プライベートプリント機能の印刷ジョブ
・プリンタ拡張機能：ジョブ保留機能の印刷ジョブ

また、上記のデータを HDD に保存中に、中止操作により中止処理を行った後にも上書き消去が行われる。

■ HDD 上に長期保存されたデータが出力により完全に消去される機能
HDD 上に長期保存されるデータは以下の通り。
・プリンタ拡張機能：バーチャルメールボックス機能の印刷ジョブ
・プリンタ拡張機能：プライベートプリント機能の印刷ジョブ

■ HDD 上に長期保存されたデータが電源 OFF により完全に消去される機能
HDD 上に長期保存されるデータは以下の通り。
・プリンタ拡張機能：クイックコピー機能の印刷ジョブ
・プリンタ拡張機能：試し刷り後、保留機能の印刷ジョブ
・プリンタ拡張機能：プライベートプリント機能の印刷ジョブ

HDD フォーマット機能

TOE マシン管理者から、HDD フォーマット機能が実行された時、メインボード HDD、プリンタボード上のデータを完全に消去する機能

■ メインボード上 HDD、プリンタボード上 HDD 内の全領域を上書き消去する。
上書き消去処理は、実行のタイミングでそれぞれ並行して行われる。

【備考】

メインボード HDD 上書き消去機能/プリンタボード HDD 上書き消去機能/HDD フォーマット機能共に、上書き消去中に電源 OFF が発生すると、上書き消去中の残存データはそのまま HDD 上に残ってしまうが、次回電源 ON 時に上書き消去処理を再開し、完全に残存データを上書き消去する。

6.1.2. 管理者認証機能

管理者認証機能は、以下の機能を提供する。

SPF.ADMIN

管理者認証機能は、TOE マシン管理者を確実に識別認証する機能である。
TOE マシン管理者権限の機能にアクセスする際に、TOE マシン管理者であることを識別し、TOE 管理者暗証番号が要求され、操作パネルから TOE 管理者暗証番号を入力する。入力された TOE 管理者暗証番号が一致すればアクセスを許可するが、一致しない限りはアクセスを許可しない。認証を行っている間、操作パネルには入力した文字数分のダミー文字(＊)だけが表示される。
TOE 管理者暗証番号の尺度は、数字（0～9）８文字固定で構成される。
この管理者認証機能は、TOE マシン管理者権限の機能にアクセスする際には必ず呼び出され、迂回されずに実行される。

また、TOE 管理者暗証番号の値は、一定の場所に保管されており、機械設置時のデフォルト値は存在するが、TOE マシン管理者だけが変更出来るようになっている。変更する際には、数字以外が入力されても入力を受け付けず、また８文字未満の TOE 管理者暗証番号では変更を受け付けない。

TOE マシン管理者に与えられた権限は以下の通りである。

- 上書き消去方式の設定値変更 （３回上書き方式 / １回上書き方式）
- HDD フォーマット機能の実行

・ TOE 管理者暗証番号の変更

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

３回上書き方式とは、不揮発性メモリ上のデータ消去アルゴリズムの１つである。
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 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

１回上書き方式とは、不揮発性メモリ上のデータ消去アルゴリズムの１つである。
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 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。

■TOE 管理者暗証番号

TOE 管理者暗証番号による管理者認証機能は、認証メカニズムを使用している。
数字(0～9) ８文字固定で構成される。

なお、本 TOE では本方式を以下の機能で使用している。

・管理者認証機能

TOE マシン管理者権限の機能にアクセスする際、TOE 管理者暗証番号により、識別認証を行う。

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、FIA_UAU.2、FIA_UAU.7、FIA_SOS.1 に対応する管理者認証機能 (SPF.ADMIN) であり、この機能のセキュリティ機能強度は SOF-基本である。

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	・KM-8030/KM-6030 構成管理計画書 ・KM-8030/KM-6030 構成管理規約書 ・KM-8030/KM-6030 海外版 構成リスト
	ACM_SCP.1	・KM-8030/KM-6030 構成管理計画書 ・KM-8030/KM-6030 構成管理規約書
配付と運用	ADO_DEL.1	・KM-8030/KM-6030 配付手順説明書
	ADO_IGS.1	・Data Security Kit (B) Operation Guide ・INSTALLATION GUIDE for Data Security Kit (B) ・Printing System (V) Operation Guide Set-up Edition ・Scan System (G) Operation Guide Set-up Edition ・8030/6030 SERVICE MANUAL
開発	ADV_FSP.1	・KM-8030/KM-6030 機能仕様書
	ADV_HLD.2	・KM-8030/KM-6030 上位レベル設計書
	ADV_RCR.1	・KM-8030/KM-6030 機能対応表
ガイダンス文書	AGD_ADM.1	・Data Security Kit (B) Operation Guide
	AGD_USR.1	・Data Security Kit (B) Operation Guide ・6030/8030 Operation Guide ・6030/8030 Advanced Operation Guide

		・Printing System (V) Operation Guide Function Edition ・Printing System (V) Operation Guide Set-up Edition ・Scan System Operation Guide Function Edition ・Scan System (G) Operation Guide Set-up Edition
ライフサイクルサポート	ALC_DVS.1	・KM-8030/KM-6030 開発セキュリティ規定書
テスト	ATE_COV.2	・KM-8030/KM-6030 カバレージテスト分析書
	ATE_DPT.1	・KM-8030/KM-6030 上位レベル設計テスト仕様書
	ATE_FUN.1	・KM-8030/KM-6030 機能テスト仕様書
	ATE_IND.2	・TOE
脆弱性評定	AVA_MSU.1	・Data Security Kit (B) Operation Guide ・6030/8030 Operation Guide ・6030/8030 Advanced Operation Guide ・Printing System (V) Operation Guide Function Edition ・Printing System (V) Operation Guide Set-up Edition ・Scan System Operation Guide Function Edition ・Scan System (G) Operation Guide Set-up Edition
	AVA_SOF.1	・KM-8030/KM-6030 脆弱性分析書
	AVA_VLA.1	・KM-8030/KM-6030 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.METHOD
O.REMAIN	✔	
O.METHOD		✔
OE.POWER	✔	

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 に保持されている残存データに対し、以後その残存データにアクセスすることが出来ないようにする必要がある。

この脅威に対して、O.REMAIN、及び OE.POWER の対策方針により対抗することが出来る。すなわち、O.REMAIN 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ことで、残存データが不正に閲覧／出力されることを防止することが出来る。

また、上書き消去中に複合機の電源が切断された場合は上書き消去処理が中断され、

上書き消去が完了しない状態の残存データが HDD 上に残る可能性がある。この脅威を防止するために、OE.POWER により TOE 利用者は複合機の使用中に電源の切断が発生した際には、速やかに電源の再投入を行う。電源を入れることで自動的に上書き消去処理が再実行されるため、残存データが不正に閲覧／出力されることを防止することが出来る。

P.METHOD

組織のセキュリティ方針 P.METHOD により、管理者が安全性と処理効率の兼ね合いを考慮することにより HDD の上書き消去方式として、３回上書き方式、または１回上書き方式が適用されなければならない。その対策として、O.METHOD の対策方針により、HDD の上書き消去方式を、３回上書き方式、または１回上書き方式のいずれかに設定できる機能を TOE マシン管理者に提供するので、P.METHOD を実現することが出来る。

8.1.2. 前提条件に対する環境のセキュリティ対策方針の適合性

前提条件に対応する環境のセキュリティ対策方針を『表 8.2 前提条件と環境のセキュリティ対策方針の対応』に示す。

表 8.2 前提条件と環境のセキュリティ対策方針の対応

前提条件 / 環境のセキュリティ対策方針	A.PHYSICAL	A.ADMIN	A.CE
OE.PHYSICAL	✔		
OE.ADMIN		✔	

OE.CE			✔

以下に、『表 8.2 前提条件と環境のセキュリティ対策方針の対応』の根拠を示す。

A.PHYSICAL

A.PHYSICAL は、TOE を搭載する複合機が、TOE の関連者のみが利用可能な物理的に保護された場所に設置されていることを必要とする。このことは、TOE やその資産に対して、不特定多数の脅威エージェントによる攻撃方法、及び攻撃機会を制限するために不特定多数の人物に TOE を利用させないことが目的となる。OE.PHYSICAL の対策により、TOE マシン管理者は TOE が搭載された複合機を、入退室管理された TOE の関連者のみが利用可能な場所に設置することを行うので、不特定多数の脅威エージェントによる攻撃方法、攻撃機会が制限されるため、A.PHYSICAL を実現することが出来る。

A.ADMIN

A.ADMIN は、TOE マシン管理者が、信用できる人物であり、不正を行わない人物であることを必要とする。OE.ADMIN の対策により、TOE マシン管理者が不正な操作を行わないことを実現するために、TOE を導入する組織は、課せられた役割を忠実に実行し、不正を行わない適切な人物を TOE マシン管理者として人選することを行うので、A.ADMIN を実現することが出来る。

A.CE

A.CE は、TOE のサービス担当者（京セラミタが認める人物）は、不正を行わないことを必要とする。OE.CE の対策により、TOE マシン管理者は、TOE のサービス担当者が不正を行わないことを実現するために、サービス担当者が TOE のメンテナンス等を行う際は、必ず TOE マシン管理者が立会うことを行うので、A.CE 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 8.3 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 8.3 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.REMAIN	O.METHOD
TOE セキュリティ機能要件	FIA_UAU.2		✔
	FIA_UAU.7		✔
	FIA_UID.2		✔
	FIA_SOS.1		✔
	FDP_RIP.1	✔	
	FMT_MTD.1		✔
	FMT_MOF.1	✔	✔
	FMT_SMR.1		✔
	FMT_SMF.1		✔
	FPT_RVM.1	✔	✔

以下に、『表 8.3 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.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。
HDD 上書き消去機能の実行についての役割を FMT_MOF.1 によって TOE マシン管理者に任せる。
また、FPT_RVM.1 により、FDP_RIP.1、FMT_MOF.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。

O.METHOD

まず、正当な許可された TOE マシン管理者を FIA_UID.2 及び FIA_UAU.2 によって識別認証する。この時、TOE 管理者暗証番号を秘匿にするため、FIA_UAU.7 により、入力された文字数分のダミー文字（＊）を表示する。TOE マシン管理者は、HDD 上書き消去機能の上書き消去方式の動作の決定についての役割を FMT_MOF.1 によって任される。この役割は、FMT_SMR.1 によって常に適切な TOE マシン管理者に維持される。TSF データである TOE 管理者暗証番号の問い合わせ、改変する能力を、FMT_MTD.1 によって TOE マシン管理者のみに制限する。また、認証のための尺度は、FIA_SOS.1 によって数字８文字固定であることを検証する。
また、TOE 管理者暗証番号の管理を FMT_SMF.1 によって特定し、FPT_RVM.1 により、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FIA_SOS.1、FMT_MTD.1、FMT_MOF.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、HDD 上書き消去機能の上書き消去方式を、３回上書き方式、または１回上書き方式のいずれかに変更する権限を TOE マシン管理者に制限することによって、確実に O.METHOD 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 8.4 TOE セキュリティ機能要件間の依存関係』に示す。

表 8.4 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	**FIA_UAU.2**	FIA_UAU.1	FIA_UID.1	3	FIA_UID.2 は FIA_UID.1 の上位コンポーネントのため依存性は満たされている。
2	**FIA_UAU.7**	なし	FIA_UAU.1	1	FIA_UAU.2 は FIA_UAU.1 の上位コンポーネントのため依存性は満たされている。
3	**FIA_UID.2**	FIA_UID.1	なし	－	
4	**FIA_SOS.1**	なし	なし	－	
5	**FDP_RIP.1**	なし	なし	－	
6	**FMT_MTD.1**	なし	FMT_SMR.1 FMT_SMF.1	8 9	
7	**FMT_MOF.1**	なし	FMT_SMR.1 FMT_SMF.1	8 9	
8	**FMT_SMR.1**	なし	FIA_UID.1	3	FIA_UID.2 は FIA_UID.1 の上位コンポーネントのため依存性は満たされている。
9	**FMT_SMF.1**	なし	なし	－	
10	**FPT_RVM.1**	なし	なし	－	

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 8.5 セキュリティ要件の相互作用』に示す。

表 8.5 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

FIA_UAU.2	FPT_RVM.1	N/A	N/A
FIA_UAU.7	FPT_RVM.1	N/A	N/A
FIA_UID.2	FPT_RVM.1	N/A	N/A
FIA_SOS.1	FPT_RVM.1	N/A	N/A
FDP_RIP.1	FPT_RVM.1	N/A	N/A
FMT_MTD.1	FPT_RVM.1	N/A	N/A
FMT_MOF.1	FPT_RVM.1	N/A	N/A
FMT_SMR.1	N/A	N/A	N/A
FMT_SMF.1	N/A	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A

N/A : Not Applicable

迂回

FPT_RVM.1

TOE マシン管理者の識別認証に関する FIA_UAU.2、FIA_UAU.7、FIA_UID.2 は、TOE マシン管理者の識別認証時に必ず呼び出されるため迂回出来ない。

秘密の検証に関する FIA_SOS.1 は、TOE 管理者暗証番号の変更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、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、または、TOE マシン管理者による HDD フォーマット機能が実行操作された後に必ず呼び出されるため迂回出来ない。

TSF データの管理に関する FMT_MTD.1 は、TOE 管理者暗証番号の変更時に必ず呼び出されるため迂回出来ない。セキュリティ機能のふるまい管理に関する FMT_MOF.1 は、HDD 上書き消去方式の設定値変更時に、必ず TOE マシン管理者の識別認証が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。また管理機能へのインタフェースは TOE マシン管理者インタフェースのみであり、TSF および TSF データにアクセスするその他のサブジェクトは存在しない。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 は、オフィスや学校において複合機に搭載されて利用され、LAN やローカルポートに接続されることも想定しているが、LAN/ローカルポートを通したネットワークから、複合機内部の残存データを読み出すことはできない。また、複合機は入退室管理された場所に設置されるため、TOE の運用環境に中レベル以上の攻撃力を持つ攻撃者を含む不特定多数の攻撃者は存在しない。このため、攻撃力は“低レベル”であり、これに対応できる最小機能強度レベルは、“SOF-基本”で満足される。

8.2.5. 保証要件根拠

本 TOE は、オフィスや学校において複合機に搭載されて利用される。ただし、利用者は不特定多数ではなく、不正行為は、オフィスや学校内部における攻撃であるため、画像データの露顕に関して攻撃能力は低レベルである。このため商用の複合機として十分なレベルである 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 8.6 TOE 要約仕様とセキュリティ機能要件の対応』に示す。

表 8.6 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.AGAIN	SPF.ADMIN
FIA_UAU.2		✔
FIA_UAU.7		✔
FIA_UID.2		✔
FIA_SOS.1		✔
FDP_RIP.1	✔	
FMT_MTD.1		✔
FMT_MOF.1		✔
FMT_SMR.1		✔
FMT_SMF.1		✔
FPT_RVM.1	✔	✔

以下に、『表 8.6 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。

FIA_UAU.2

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、TOE マシン管理者に許可された機能にアクセスする際に、必ず認証を行うため、アクション前の利用者認証というふ

るまいを規定したセキュリティ機能要件 FIA_UAU.2 は満たされている。

FIA_UAU.7

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、認証を行っている間、操作パネルには入力した文字数分のダミー文字(＊)だけを表示することを行うため、保護された認証フィードバックというふるまいを規定したセキュリティ機能要件 FIA_UAU.7 は満たされている。

FIA_UID.2

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、TOE マシン管理者に許可された機能にアクセスする際に、TOE 管理者暗証番号が要求されることで、必ず TOE マシン管理者であることが識別されるため、アクション前の利用者識別というふるまいを規定したセキュリティ機能要件 FIA_UID.2 は満たされている。

FIA_SOS.1

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、TOE 管理者暗証番号の品質尺度の検証を、定義された構成で行うため、秘密の検証というふるまいを規定したセキュリティ機能要件 FIA_SOS.1 は満たされている。

FDP_RIP.1

セキュリティ機能 SPF.AGAIN「HDD 上書き消去機能」は、メインボード上、及びプリンタボード上 HDD 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、及び、TOE マシン管理者により、HDD フォーマット機能が実行された時、ディスク全体を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。

FMT_MTD.1

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、TOE マシン管理者の TOE 管理者暗証番号の値の表示と変更を、TOE マシン管理者にのみ許可することを行うため、TSF データの管理というふるまいを規定したセキュリティ機能要件 FMT_MTD.1 は満たされている。

FMT_MOF.1

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、PSF.AGAIN「HDD 上書き消去機能」の上書き消去方式の設定値を３回上書き方式または１回上書き方式に変更する役割、

及び、HDD のディスク全体を初期化する HDD フォーマット機能の実行操作の役割を、TOE マシン管理者にのみ許可することを行うため、セキュリティ機能のふるまいの管理というふるまいを規定したセキュリティ機能要件 FMT_MOF.1 は満たされている。

FMT_SMR.1

セキュリティ機能 SPF.ADMIN「管理者認証機能」は、TOE マシン管理者の識別認証を確実に行い、且つ TOE 管理者暗証番号の変更を TOE マシン管理者にのみ許可することにより、役割が TOE マシン管理者に維持される。また、識別認証に成功した者を TOE マシン管理者という役割に関連付けることが出来る。以上により、セキュリティ役割というふるまいを規定したセキュリティ機能要件 FMT_SMR.1 は満たされている。

FMT_SMF.1

FMT_SMF.1 は、FIA_UAU.2 の管理項目である、SPF.ADMIN「管理者認証機能」による TOE 管理者暗証番号を管理する能力を持っている。

なお、保護された認証フィードバックはダミー文字で固定であり、FIA_UAU.7 の管理項目は無い。アクション前の利用者識別についても、識別の対象は TOE マシン管理者だけであり、TOE は管理者専用の操作を行うことにより、TOE マシン管理者を識別するため、FIA_UID.2 に対する管理項目は無い。秘密の検証尺度についても、数字８文字固定であるため、FIA_SOS.1 に対する管理項目は無い。また、サブセット残存情報保護についても、割当て解除時にのみ残存情報保護を実施するため、タイミングは固定であり、FDP_RIP.1 の管理項目は無い。TSF の機能や TSF データと相互に影響を及ぼす役割グループは TOE マシン管理者だけであるため管理の必要は無く、FMT_MTD.1、FMT_MOF.1 の管理項目は無い。役割の一部をなす利用者は TOE マシン管理者のみであり管理の必要は無いため、FMT_SMR.1 の管理項目は無い。

以上により、SPF.ADMIN「管理者認証機能」を実装することにより、管理機能の特定というふるまいを規定したセキュリティ機能要件 FMT_SMF.1 は満たされている。

FPT_RVM.1

セキュリティ機能 SPF.ADMIN「管理者認証機能」及び PSF.AGAIN「HDD 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. セキュリティ機能強度根拠

“6.3 セキュリティ機能強度”において、管理者認証機能のセキュリティメカニズムに対しては、SOF-基本を主張している。一方、“5.3 最小機能強度”において、TOE の最小機能強度は SOF-基本を主張している。従って、両者の機能強度は一貫しており、セキュリ

ティ機能強度 SOF-基本は妥当である。

8.3.3. 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】 ・KM-8030/KM-6030 構成管理計画書
・KM-8030/KM-6030 構成管理規約書
・KM-8030/KM-6030 海外版 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】 ・KM-8030/KM-6030 構成管理計画書
・KM-8030/KM-6030 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】 ・KM-8030/KM-6030 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 (B) 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】 ・Data Security Kit (B) Operation Guide
・INSTALLATION GUIDE for Data Security Kit (B)
・Printing System (V) Operation Guide Set-up Edition
・Scan System (G) Operation Guide Set-up Edition
・8030/6030 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】 ・KM-8030/KM-6030 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、TOE マシン管理者や 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】 ・KM-8030/KM-6030 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】 ・KM-8030/KM-6030 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】 ・Data Security Kit (B) Operation Guide

【内容】 TOE マシン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】 ・Data Security Kit (B) Operation Guide
・6030/8030 Operation Guide
・6030/8030 Advanced Operation Guide
・Printing System (V) Operation Guide Function Edition
・Printing System (V) Operation Guide Set-up Edition
・Scan System Operation Guide Function Edition
・Scan System (G) Operation Guide Set-up Edition

【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】 ・KM-8030/KM-6030 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】 ・KM-8030/KM-6030 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】 ・KM-8030/KM-6030 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】 ・KM-8030/KM-6030 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】 ・Data Security Kit (B) Operation Guide
・6030/8030 Operation Guide
・6030/8030 Advanced Operation Guide
・Printing System (V) Operation Guide Function Edition
・Printing System (V) Operation Guide Set-up Edition
・Scan System Operation Guide Function Edition
・Scan System (G) Operation Guide Set-up Edition

【内容】 TOE マシン管理者や 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】　・KM-8030/KM-6030 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】　・KM-8030/KM-6030 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)