京セラミタ
Data Security Kit (E)
Software Type II
海外版
セキュリティターゲット

第 1.15 版

2010 年 08 月 27 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
2009/9/16	0.40	・新規作成（Type Ⅰより派生）	康	曽根
2010/8/10	1.10	・Type Ⅰの変更を反映	康	曽根
2010/8/27	1.15	・誤植修正	康	曽根

～ 目次 ～

1. ST 概説 1
1.1. ST 参照 1
1.2. TOE 参照 1
1.3. TOE 概要 1
1.3.1. TOE の種別 1
1.3.2. TOE の使用法及び主要なセキュリティ機能の特徴 2
1.3.3. 必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア 3
1.4. TOE 記述 3
1.4.1. TOE の関連者 3
1.4.2. TOE の物理的構成 4
1.4.3. TOE の論理的構成 6
1.4.3.1. TOE が提供する基本機能 6
1.4.3.2. TOE が提供するセキュリティ機能 7
1.4.4. ガイダンス 9
1.4.5. TOE の保護資産 9
2. 適合主張 10
2.1. CC 適合主張 10
2.2. PP 主張 10
2.3. パッケージ主張 10
2.4. 適合根拠 10
3. セキュリティ課題定義 11
3.1. 脅威 11
3.2. 組織のセキュリティ方針 11
3.3. 前提条件 11
4. セキュリティ対策方針 12
4.1. TOE のセキュリティ対策方針 12
4.2. 運用環境のセキュリティ対策方針 12
4.3. セキュリティ対策方針根拠 12

5. 拡張コンポーネント定義 15

6. セキュリティ要件 16

6.1. TOE セキュリティ機能要件 16
6.2. TOE セキュリティ保証要件 19
6.3. セキュリティ要件根拠 20
6.3.1. セキュリティ機能要件根拠 20
6.3.2. TOE セキュリティ機能要件間の依存関係 20
6.3.2.1. FCS_CKM.4 の依存性を必要としない根拠 21
6.3.3. セキュリティ保証要件根拠 21

7. TOE 要約仕様 22

7.1. 暗号化機能 22
7.2. 上書き消去機能 22

8. 略語・用語 24

8.1. 用語の定義 24
8.2. 略語の定義 25

～ 図目次 ～

図 1.1 一般的な利用環境 2
図 1.2 TOE の物理的構成図 4
図 1.3 TOE の論理的構造図 6

～ 表目次 ～

表 1.1 TOE の対象製品 3
表 4.1 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 12
表 6.1 TOE セキュリティ保証要件 19
表 6.2 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 20
表 6.3 TOE セキュリティ機能要件間の依存関係 20
表 7.1 TOE セキュリティ機能とセキュリティ機能要件 22
表 8.1 ST で使用される用語の定義 24
表 8.2 ST で使用される略語の定義 25

1. ST 概説

1.1. ST 参照

ST 名称：	京セラミタ Data Security Kit (E) Software Type II 海外版 セキュリティターゲット
ST バージョン：	第 1.15 版
作成日：	2010/8/27
作成者：	京セラミタ株式会社

1.2. TOE 参照

TOE 名称：	Data Security Kit (E) Software Type II
TOE バージョン：	V1.00E
作成者：	京セラミタ株式会社

1.3. TOE 概要

1.3.1. TOE の種別

本STが定義するTOEは、主としてコピー機能、スキャナ機能、プリンタ機能を有する複合機（Multi Function Printer：以下MFPと略称）を制御するファームウェアとセキュリティ演算機能を行うASICを含み、京セラミタ株式会社製MFP「TASKalfa 520i/420i、TASKalfa 520iG/420iG、CS 520i/420i、CD 1252/DC 2252 / CD 1242/DC 2242」に搭載され使用される。TOEが有する主なセキュリティ機能は、MFPの使用によりMFPが内蔵するHDDに格納された画像データを、不正なインタフェースより持ち出されることから保護するものである。

1.3.2. TOE の使用法及び主要なセキュリティ機能の特徴

本TOEが搭載されるMFPは、利用者が扱う様々な文書をコピー（複製)、プリント（紙出力)、ネットワーク送信（電子化）することが可能である。MFPは、一般的なオフィスに設置され、単独で使用するだけでなく、LANやローカルポート（USBポート）に接続されて、ネットワーク環境でも使用される。ネットワーク環境では、ファイアウォールなどで外部ネットワークの不正アクセスから保護された内部ネットワークでクライアントPC、サーバと接続されて使用される事を想定している。

この利用環境において、操作パネル上のボタン操作やネットワーク上のクライアントPCからの操作により、上記機能を実施することが出来る。

図1.1 に一般的な利用環境を示す。

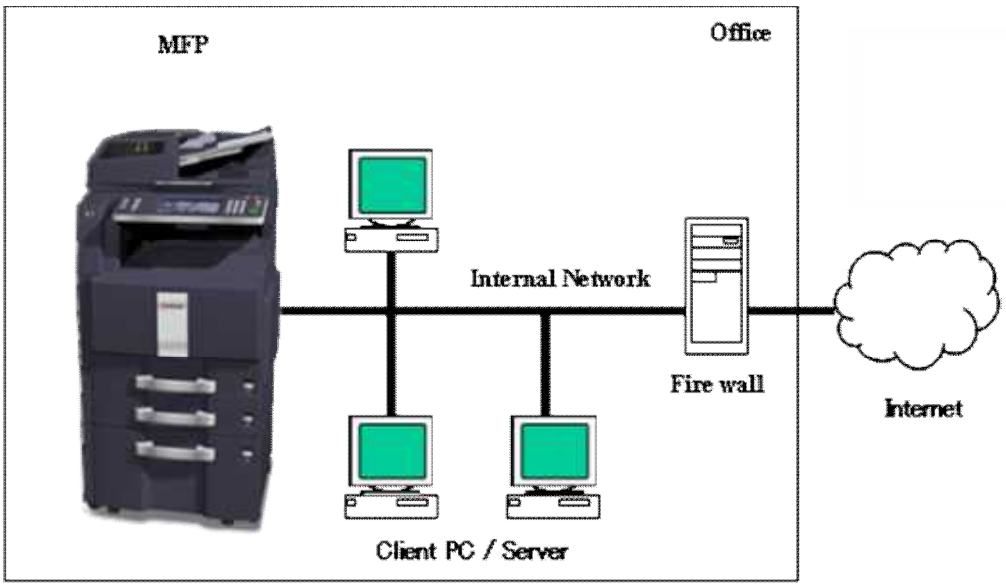

図 1.1 一般的な利用環境

TOEのセキュリティ機能は、MFP「TASKalfa 520i/420i、TASKalfa 520iG/420iG、CS 520i/420i、CD 1252/DC 2252 / CD 1242/DC 2242」使用におけるオプション「Data Security Kit (E)」を契約することによりライセンス登録することで活性化される。

TOEは、利用者が扱う画像データに対し、各機能の処理中/処理後にMFP 内に搭載されるHDDに一時的に保存される画像データの漏洩に対する保護機能を提供する。画像データが保存される際には暗号化を実施し、また、画像データの削除が指示された際にはデータ再利用を不可能な状態にすることで、HDDを持ち出し、HDDのインタフェースに直接アクセスすることによる画像データの漏洩を防止する。

1.3.3. 必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOEの動作には、京セラミタ株式会社製MFPの一部の機種が必要である。本TOEを搭載可能な製品を表2.1で示す。

表 1.1 TOE の対象製品

TOE 名称 / バージョン	対象製品
Data Security Kit (E) Software Type II / V1.00E	TASKalfa 520i TASKalfa 420i TASKalfa 520iG TASKalfa 420iG CS 520i CS 420i CD 1252/DC 2252 CD 1242/DC 2242

また、MFPの一般機能を使用するためには、図1.1で示す利用環境におけるクライアントPCおよびサーバに、プリンタドライバ及びTWAINドライバ（ガイダンスにて識別）、SMTPサーバ、SMBサーバ、FTPサーバが必要となる。

1.4. TOE 記述

1.4.1. TOE の関連者

TOE が搭載されるMFP の利用に関連する人物の役割を以下に定義する。

- 機器管理者：
  TOE を搭載した MFP 本体の管理者として登録されている人。機器管理者は、MFP 本体に対する特権を有し、TOE を搭載した MFP を構成する機器、及び TOE に対する導入、運用管理を行う。

- TOE 利用者：
  TOE を搭載した MFP を利用する人。TOE 利用者は、コピー、プリント、ネットワーク送信、ボックスの機能を利用することが出来る。

- サービス担当者：
  TOE を搭載した MFP のサービス担当者として京セラミタが認めた人。サービス担当者は、TOE 導入時に、TOE の活性化を行い、TOE の立上げ（動作可能にする）を行う。また、TOE を搭載した MFP を構成する機器および TOE に対するメンテナンスを行う。

1.4.2. TOE の物理的構成

TOEの物理的構造の概念図を 図1.2 で示す。

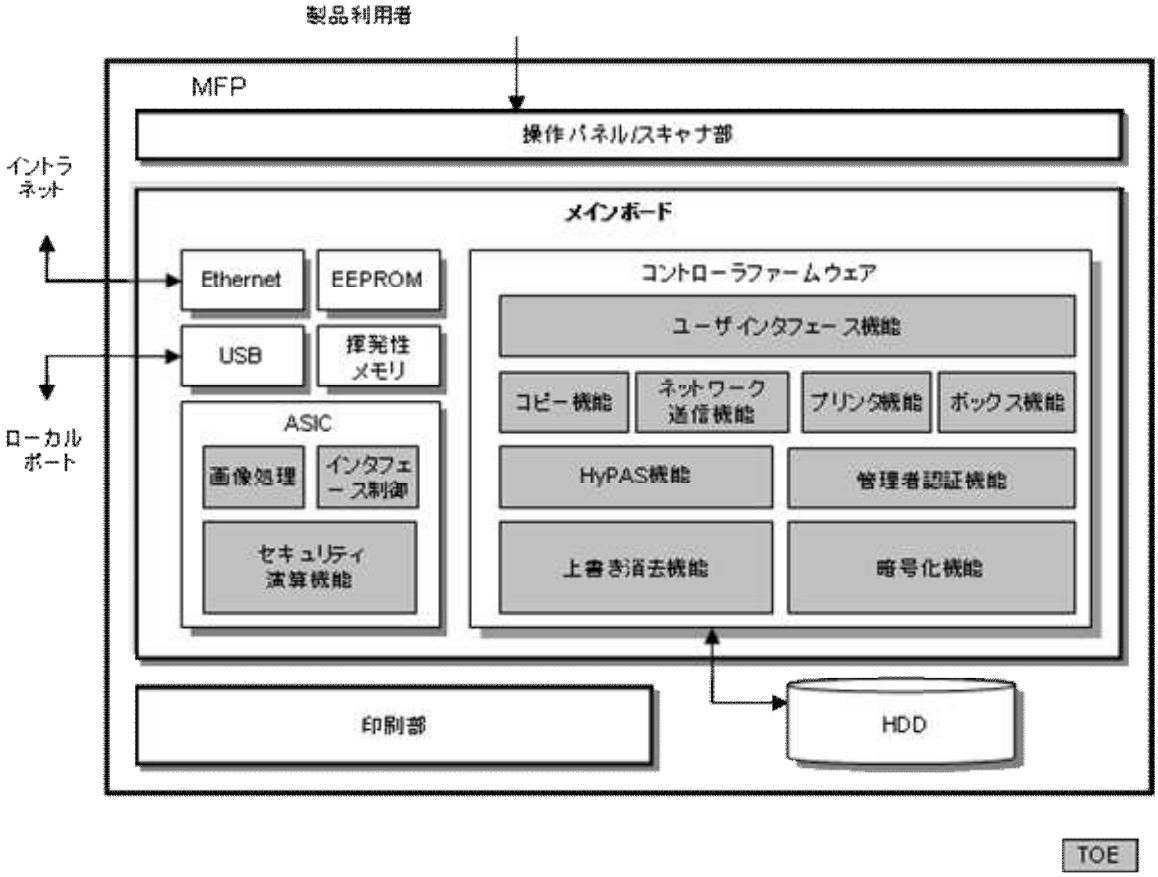

図 1.2 TOE の物理的構成図

TOE が搭載される MFP は、操作パネル、スキャナ部、印刷部、メインボード、HDD のハードウェアで構成される。
コピー機能制御、ネットワーク送信機能制御、プリンタ機能制御、ボックス機能制御、管理者認証機能制御、HyPAS 機能制御、上書き消去機能制御、暗号化機能制御を行うためのメインボード上のコントローラファームウェアは TOE に含まれる。
コントローラファームウエアと共にセキュリティ機能の実装を分担する専用カスタム IC（ASIC）も TOE に含まれる。ASIC には、セキュリティ演算機能部分、画像処理部分、インタフェース制御部分が含まれる。このうち、セキュリティ演算機能部分が、上書き消去機能においては、HDD の指定領域への上書き処理、暗号化機能では HDD に読み書きする際の暗号化処理を実現する。

この ST では、ファームウエアの用語は、コントローラファームウエアに加えて ASIC を含む意味で使用する。

TOE の範囲外となるものは、表 1.1 で識別された MFP 本体、ユーザインタフェース機能で使用

される言語ファイル及び HyPAS 機能により搭載されるアプリケーションソフトウェアがこれに該当する。

また MFP を構成するハードウエア（ASIC を含む）の物理的な耐タンパー性は評価されない。

1.4.3. TOE の論理的構成

TOEの論理的構造の概念図を 図1.3 で示す。

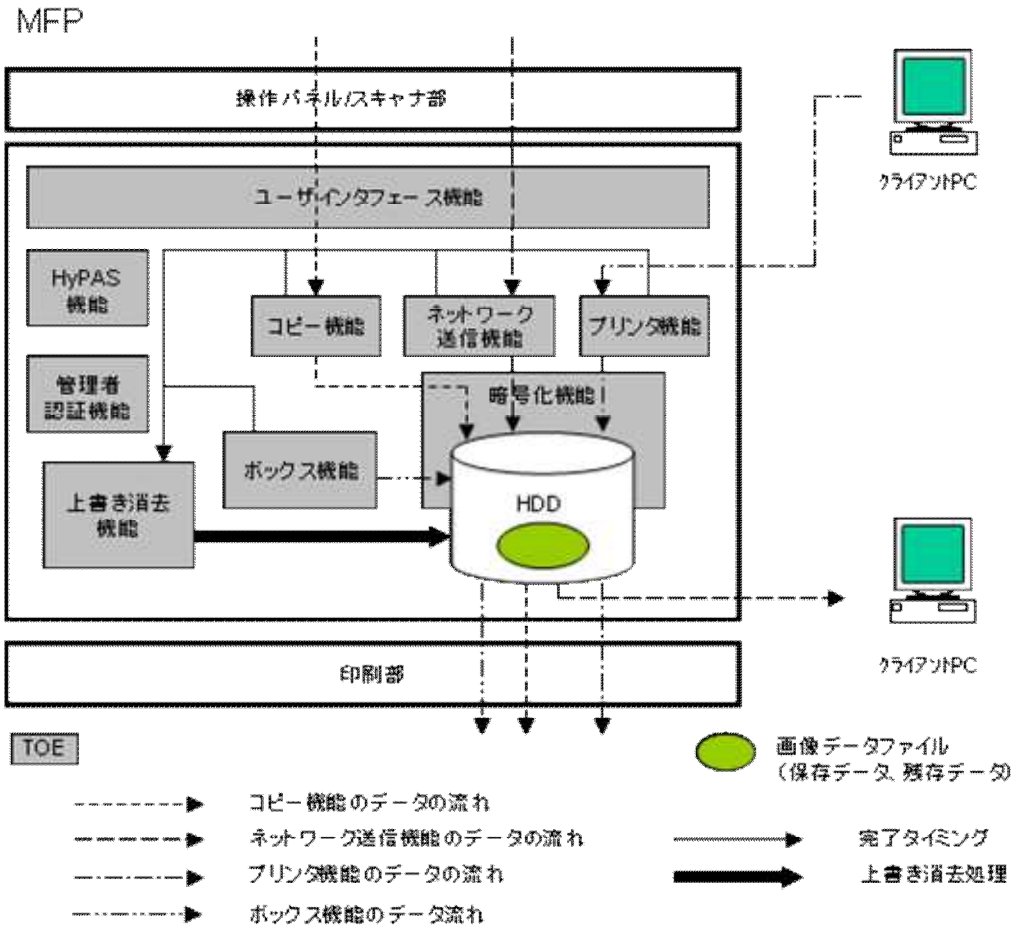

図 1.3 TOE の論理的構造図

1.4.3.1. TOE が提供する基本機能

TOEは、基本機能として以下の機能を提供する。

- ユーザインタフェース機能
  機器管理者、TOE 利用者、サービス担当が MFP の機能を利用するために、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。ただし、本機能は TOE が提供するセキュリティ機能ではない。
- コピー機能
  TOE 利用者が、操作パネルから入力/操作を行うことにより、画像データを MFP のスキャナから読込み、MFP の印刷部から出力する機能。
- ネットワーク送信機能
  TOE 利用者が、操作パネルから入力/操作を行うことにより、画像データをクライアント PC

に送信する機能。

- プリンタ機能
  TOE 利用者が、LAN 上、又はローカル接続されたクライアント PC から操作することにより、送信された画像データを MFP の印刷部から出力する機能。
- ボックス機能
  TOE 利用者が、画像データを HDD 上に長期保存する機能。
  TOE 利用者が、操作パネルからの入力/操作を行うか、もしくは、LAN 上、又はローカル接続されたクライアント PC から操作を行うことにより、入力された画像データを HDD 上に長期保存する。
  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。
  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。
- HyPAS 機能
  TOE が搭載される MFP は、日常の業務をより効率的に行うためのアプリケーションをインストールして使用することが出来る。HyPAS 機能とは、アプリケーションをインストールし、MFP 上で動作させるための機能である。
  ただし、インストールされるアプリケーションソフトウェアは、TOE の範囲外である。

1.4.3.2. TOE が提供するセキュリティ機能

TOEは、セキュリティ機能として以下の機能を提供する。

- 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。
  暗号化機能は、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能という基本機能が処理され、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。また、同様の基本機能が処理され、HDD に保存された画像データを読み出す際に、暗号化された画像データを復号して読み出しも行う。

  暗号化に使用する暗号鍵は、MFP の電源 ON 時に機器ごとに一意な値で毎回生成され、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。

- 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。
  上書き消去機能は、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能という基本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の削除が指示された際に、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

することで、データ再利用を不可能な状態にする機能である。

1.4.4. ガイダンス

本TOEを構成するガイダンスを以下に示す。

種別	名称	バージョン	仕向地
取扱説明書	Data Security Kit (E) Operation Guide	Rev.2 2010.8	海外
	Notice	303MS56320 2010.1	海外
	Data Security Kit (E) Operation Guide Set-up Edition	303MS56710 2008.12	海外
	420i/520i Operation Guide	302KR56040 First edition 2009.7	海外
	CD 1242/DC 2242　CD 1252/DC 2252　Operation Guide	302KR56162 Rev. 2 2009.11	海外
サービスマニュアル	TASKalfa 420i/520i Service Manual	2KSSM063 Rev.3 2010.5	海外

1.4.5. TOE の保護資産

一般的な MFP は、コピー/プリント/ネットワーク送信の処理を行う際、一旦、一時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 上に画像データは一時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。一時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 が持ち出されると、これらデータを丸ごと持ち出されてしまうことが起こり得る。

そこで、TOE が保護すべき資産を以下に示す。

■ 残存データ

HDD 上に、一時保存又は長期保存された画像データを、HDD から論理的に削除した後に残存するデータ。

■ 一時保存データ

コピー/プリント/ネットワーク送信の処理を行う際、HDD 上に一時保存する画像データ。

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。

2. 適合主張

2.1. CC 適合主張

本ST およびTOE のCC 適合主張は、以下のとおりである。

ST とTOE が適合を主張するCC のバージョン：
パート1： 概説と一般モデル
2007 年3 月 バージョン3.1 翻訳第1.2 版
パート2： セキュリティ機能コンポーネント
2008 年3 月 バージョン3.1 翻訳第2.0 版
パート3： セキュリティ保証コンポーネント
2008 年3 月 バージョン3.1 翻訳第2.0 版
CC パート2 に対するST の適合： CC パート2 適合
CC パート3 に対するST の適合： CC パート3 適合

2.2. PP 主張

本ST が適合するPP はない。

2.3. パッケージ主張

本ST は、パッケージ：EAL3 に適合する。

2.4. 適合根拠

なし。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威

TOE に対する脅威を以下のように識別する。また、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.RESIDUAL ： 残存データへの不正アクセス

攻撃者が、HDD を持ち出し、容易に入手可能なツールを利用して、画像データの削除後も HDD に残存しているデータを不正に復元/解読し、読み出して持ち出すかもしれない。

T.TEMP ： 一時保存データへの不正アクセス

攻撃者が、HDD を持ち出し、容易に入手可能なツールを利用して、HDD 上に一時保存している画像データを不正に読み出して持ち出すかもしれない。

3.2. 組織のセキュリティ方針

本 TOE が遵守しなければならない組織のセキュリティ方針は無い。

3.3. 前提条件

本 TOE の前提条件は以下の通りである。

A.LOCATION ： 運用環境における TOE の安全性の確保

MFP のハードウエアに対し行われるかもしれない攻撃による TOE のセキュリティ侵害を防ぐため、相互監視が可能な管理された環境にて運用するものと想定する。ハードウエアに対する攻撃では MFP 内部を開き機器を接続し解析する、あるいは MFP の基板を交換するようなことを想定する。

A.NETWORK ：TOE の外部ネットワークからの安全性

TOE は外部ネットワークの不正アクセスから保護された内部ネットワークに接続されて使用されるものと想定する。

A.CE ：サービス担当者の信頼性

TOE のサービス担当者は、信頼出来る人物であり、不正は行わないものと想定する。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に示す。

O.REMAIN ： 残存データの上書き消去

TOE は、削除する HDD の画像データファイルにおいて資源割り当てから解放された領域（実データ領域）の以前のどの情報も再利用できないことを保証しなければならない

O.ENCRYPT ：保存データの解読防止

TOE は、HDD に保存する画像データを暗号化し、不正にデータが解読されないことを保証しなければならない。

4.2. 運用環境のセキュリティ対策方針

TOE の運用環境が実施するセキュリティ対策方針を以下に示す。

OE.LOCATION ：TOE と資産の環境による保護

MFP は相互監視が可能な管理された環境で運用し、相互監視により、MFP を構成するハードウエアに対する解析、改ざんを行う攻撃を防止しなければならない。

OE.NETWORK ：TOE の外部ネットワークからの防護

TOE が設置される内部ネットワークは、ファイアウォールなどの機器を設置して、外部ネットワークから TOE への攻撃を制限しなければならない。

OE.CE ：サービス担当者の確認

サービス担当者が TOE のメンテナンスを行う際は、その人物が正規のサービス担当者であることを確認しなければならない。

4.3. セキュリティ対策方針根拠

前提条件、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関係を下表に示す。セキュリティ対策方針が少なくとも 1 以上の前提条件、脅威、組織のセキュリティ方針に対応していることを示している。

表 4.1 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.RESIDUAL	T.TEMP	A.LOCATION	A.NETWORK	A.CE
O.REMAIN	✔				
O.ENCRYPT		✔			
OE.LOCATION			✔		
OE.NETWORK				✔	
OE.CE					✔

以下に、『表 4.1 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.RESIDUAL

T.RESIDUAL の脅威に対抗するためには、HDD に保存されている残存データに対し、その情報が復元/解読され、読み出されないようにする必要がある。
この脅威に対して、O.REMAIN の対策方針により対抗することが出来る。すなわち、HDD に保存されている画像データファイルにおいて、資源割り当てから解放された領域の以前のどの情報も再利用できないことを保証するので、残存データが復元/解読され、読み出されることを防止することが出来る。

T.TEMP

T.TEMP の脅威に対抗するためには、HDD に一時保存されている画像データに対し、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 に保存されている画像データを暗号化し、同一の暗号鍵で復号すること以外にはデータを解読されないことを保証することで、不正に閲覧/出力されることを防止することが出来る。

A.LOCATION

A.LOCATION の前提条件は、MFP のハードウエアに対し行われるかもしれない攻撃による TOE のセキュリティ侵害を防ぐため、相互監視が可能な管理された環境にて運用されることを必要とする。このことは、MFP のハードウェアに対する不正な解析や改ざんによるセキュリティ侵害から TOE を守るため、攻撃方法、及び攻撃機会を制限することが目的となる。OE.LOCATION の対策により、MFP は相互監視が可能な管理された環境で運用し、相互監視により MFP を構成するハードウェアに対する解析、改ざん等を行う攻撃を制限することを行うので、攻撃方法、攻撃機会が制限され、A.LOCATION を実現することが出来る。

A.NETWORK

A.NETWORK の前提条件は、TOE が外部ネットワークの不正アクセスから保護された内部ネットワークに接続されて使用されることを必要とする。このことは、TOE に対して、外部ネットワークからの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 にアクセスさせないことが目的となる。OE.NETWORK の対策により、TOE が設置される内部ネットワークは、ファイアウォールなどの機器を設置して、外部ネットワークからの TOE への攻撃を制限することを行うので、外部ネットワークからの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、A.NETWORK を実現することが出来る。

A.CE

A.NETWORK の前提条件は、TOE のメンテナンスを行うサービス担当者が信頼出来る人物であることを必要とする。このことは、TOE のメンテナンスを行うサービス担当者は不正を働かないことが目的となる。OE.CE の対策により、サービス担当者が TOE のメンテナンスを行う際には、その人物が正規のサービス担当者であることの確認を行うので、TOE のメンテナンスを行うサービス担当者が不正を働かない人物であることに制限され、A.CE を実現することが出来る。

5. 拡張コンポーネント定義

拡張コンポーネントは定義しない。

6. セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

6.1. 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

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

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

FCS_COP.1　　暗号操作

下位階層：なし

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
FDP_ITC.2 セキュリティ属性を伴う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

FCS_COP.1.1

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 へ書き込み時の画像データを暗号化
・HDD から読み出し時の画像データの復号

FDP_RIP.1　　サブセット情報保護

下位階層：なし

依存性：なし

FDP_RIP.1.1

TSF は、[割付：オブジェクトのリスト]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]
・HDD 上の画像データファイル

[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

6.2. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL3 であり、本 TOE の評価保証レベルは EAL3 である。

表 6.1 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)	
開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.3	完全な要約を伴機能仕様
	ADV_TDS.2	アーキテクチャ設計
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート	ALC_CMC.3	許可の管理
	ALC_CMS.3	実装表現の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_DVS.1	セキュリティ手段の識別
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト : 基本設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定	AVA_VAN.2	脆弱性分析

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

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示す。

表 6.2 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.REMAIN	O.ENCRYPT
TOE セキュリティ機能要件	FCS_CKM.1		✔
	FCS_COP.1		✔
	FDP_RIP.1	✔	

以下に、『表 6.2 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.REMAIN

FDP_RIP.1 のサブセット情報保護方針により、削除する HDD の画像データファイル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いことを保証することが出来る。

従って、O.REMAIN は残存データに対して再利用できないことを保証することが出来る。

O.ENCRYPT

FCS_COP.1 の暗号操作方針により、HDD に保存する画像データの暗号化を保証することが出来る。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とが保証される。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。

従って、O.ENCRYPT は保存データに対して不正にデータが解読されないことを保証することが出来る。

6.3.2. 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以下に示す。

表 6.3 TOE セキュリティ機能要件間の依存関係

No	TOE	下位階層	依存関係	参照 No	備考

	セキュリティ機能要件				
1	FCS.CKM.1	なし	FCS_COP.1 FCS_CKM.4	2 不要	6.3.2.1 節参照
2	FCS_COP.1	なし	FCS_CKM.1 FCS_CKM.4	1 不要	6.3.2.1 節参照
3	FDP_RIP.1	なし	なし	―	

6.3.2.1. FCS_CKM.4 の依存性を必要としない根拠

暗号鍵は主電源 ON 時に生成され、電源 ON 中は画像データを HDD に読み書きする暗号処理のために保存されこの目的以外にアクセスするインタフェースはない。このため暗号鍵を破棄する要件は必要としない

6.3.3. セキュリティ保証要件根拠

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。

EAL3 は TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、及び開発環境や開発生産物の管理状況の評価)を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれる。保証要件は、EAL3 適合であるため、EAL3 の選択は妥当である。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。
表 6.1 は、TOE セキュリティ機能とセキュリティ機能要件の関係を示す。

表 7.1 TOE セキュリティ機能とセキュリティ機能要件

セキュリティ機能 / 機能要件	TSF.ENCRYPT	TSF.AGAIN
FCS_CKM.1	○	
FCS_COP.1	○	
FDP_RIP.1		○

7.1. 暗号化機能

TSF.ENCRYPT

暗号化機能は、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能という基本機能が処理され、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。

(1) FCS_CKM.1 暗号鍵生成

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 時に機器ごとに一意な値で毎回生成され、揮発性メモリに保持される。尚、暗号鍵の元となる情報は運用開始時にのみ設定され、運用中に変更されることは無い。

(2) FCS_COP.1 暗号操作

TOE は、HDD に画像データを保存する際、起動時に生成した暗号鍵生成(FCS_CKM.1)により作成した 128bit 暗号鍵を用い、FIPS PUBS 197 に基づく AES 暗号アルゴリズムに従って画像データの暗号化を行い、HDD に書込む。また、HDD に保存された画像データを読み出す際、同様に起動時に作成した暗号鍵を用い、AES 暗号アルゴリズムに従って画像データを復号する。

7.2. 上書き消去機能

TSF.AGAIN

上書き消去機能は、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能と

いう基本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の削除が指示された際に、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ことでデータ再利用を不可能な状態にする機能である。

(1) FDP_RIP.1 サブセット残存情報保護

TOE は、上書き消去の対象となる利用済み画像データを HDD 上の特定の領域に置き、それを監視するプロセスにより上書き消去を実行する。別の基本機能が指示され、上書き消去が待機状態になった場合や、上書き消去中の電源断により、未了となった利用済み画像データがある場合も、待機状態が解除された時点や、電源が起動された時点で、監視プロセスにより上書き消去を実行する。

8. 略語・用語

8.1. 用語の定義

本 ST で使用される用語の定義を表 8.1 で示す。

表 8.1 ST で使用される用語の定義

用語	定義
画像データ	TOE 利用者が、コピー機能、ネットワーク送信機能、プリンタ機能、及びボックス機能を利用した際に、MFP 内部で処理される画像情報のことを指す。
一時保存	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 上に保持したり、画像処理において一時的に 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	画像データを、利用者が意識して保存操作を行い、HDD 上に保持すること。一時保存と対比。
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。
ネットワーク送信	スキャンされた画像データやボックスに保存された画像データを、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。
上書き消去	HDD に保存された画像データの削除が指示された際に、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ことを指す。こうすることでデータ再利用を不可能な状態にすることが出来る。
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。

8.2. 略語の定義

本 ST で使用される略語の定義を表 8.2 で示す。

表 8.2 ST で使用される略語の定義

用語	定義
CC	Common Criteria (コモンクライテリア)
ST	Security Target (セキュリティターゲット)
EAL	Evaluation Assurance Level (評価保証レベル)
SFR	Security Functional Requirement (セキュリティ機能要件)
SAR	Security Assurance Requirement (セキュリティ保証要件)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functions (TOE セキュリティ機能)
AES	Advanced Encryption Standard
EEPROM	Electronically Erasable Programmable ROM
HDD	Hard Disk Drive
MFP	Multi Function Printer
USB	Universal Serial Bus

(最終ページ)