# 認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太
原紙押印済

評価対象

| | |
|---|---|
| **申請受付日（受付番号）** | **平成17年9月21日** (IT**認証**5063) |
| **認証番号** | C0150 |
| **認証申請者** | **京セラミタ株式会社** |
| TOE**の名称** | Data Security Kit (C) Software |
| TOE**のバージョン** | V1.40 |
| PP**適合** | **なし** |
| **適合する保証パッケージ** | EAL3 |
| **開発者** | **京セラミタ株式会社** |
| **評価機関の名称** | **有限責任中間法人　ITセキュリティセンター　評価部** |

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年3月26日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

**評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。**

① Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 2.1

**評価結果：合格**

「Data Security Kit (C) Software」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

1 全体要約 ..... 1
1.1 はじめに ..... 1
1.2 評価製品 ..... 1
1.2.1 製品名称 ..... 1
1.2.2 製品概要 ..... 1
1.2.3 TOEの範囲と動作概要 ..... 1
1.2.4 TOEの機能 ..... 4
1.3 評価の実施 ..... 5
1.4 評価の認証 ..... 6
1.5 報告概要 ..... 6
1.5.1 PP適合 ..... 6
1.5.2 EAL ..... 6
1.5.3 セキュリティ機能強度 ..... 6
1.5.4 セキュリティ機能 ..... 6
1.5.5 脅威 ..... 8
1.5.6 組織のセキュリティ方針 ..... 8
1.5.7 構成条件 ..... 8
1.5.8 操作環境の前提条件 ..... 8
1.5.9 製品添付ドキュメント ..... 8
2 評価機関による評価実施及び結果 ..... 10
2.1 評価方法 ..... 10
2.2 評価実施概要 ..... 10
2.3 製品テスト ..... 11
2.3.1 開発者テスト ..... 11
2.3.2 評価者テスト ..... 13
2.4 評価結果 ..... 14
3 認証実施 ..... 15
4 結論 ..... 16
4.1 認証結果 ..... 16
4.2 注意事項 ..... 22
5 用語 ..... 23
6 参照 ..... 25

# 1 全体要約

## 1.1 はじめに

この認証報告書は、「Data Security Kit (C) Software」（以下「本TOE」という。）について有限責任中間法人　ITセキュリティセンター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である京セラミタ株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

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

## 1.2 評価製品

### 1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　Data Security Kit (C) Software
バージョン：　V1.40
開発者：　京セラミタ株式会社

### 1.2.2 製品概要

TOEは、京セラミタ株式会社の複合機「KM-3050、KM-4050、KM-5050、KM-3050i、KM-4050i、KM-5050i、CS-3050、CS-4050、CS-5050」に対するオプション製品として搭載され、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。

### 1.2.3 TOEの範囲と動作概要

- 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。

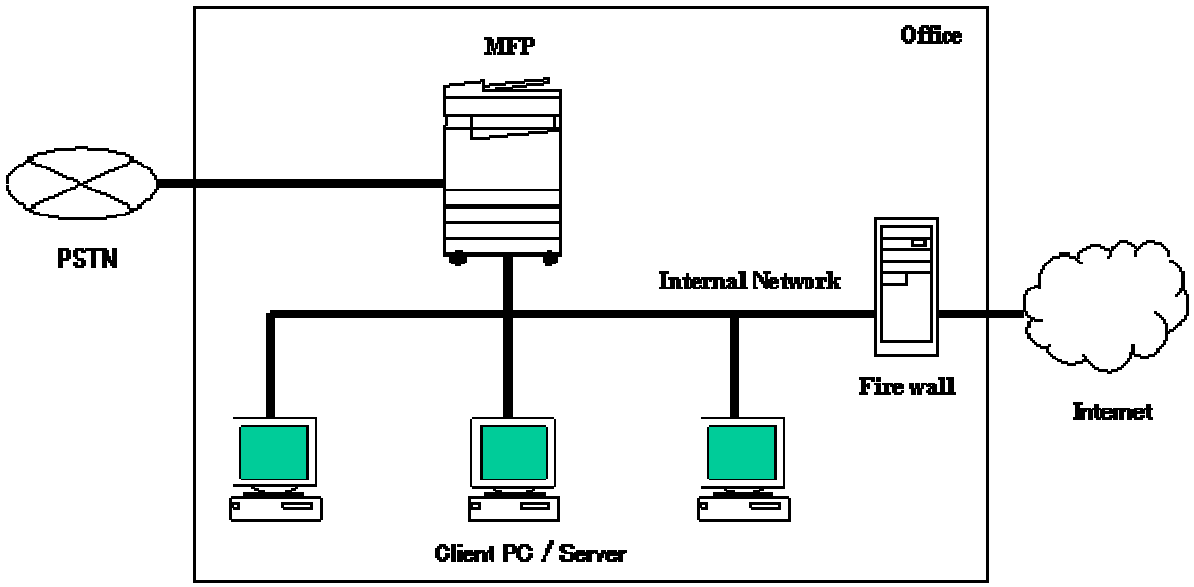


**図1-1　一般的な利用環境**

- TOEの範囲と動作概要

TOEの物理的構造の概念図を 図1-2 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) 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。

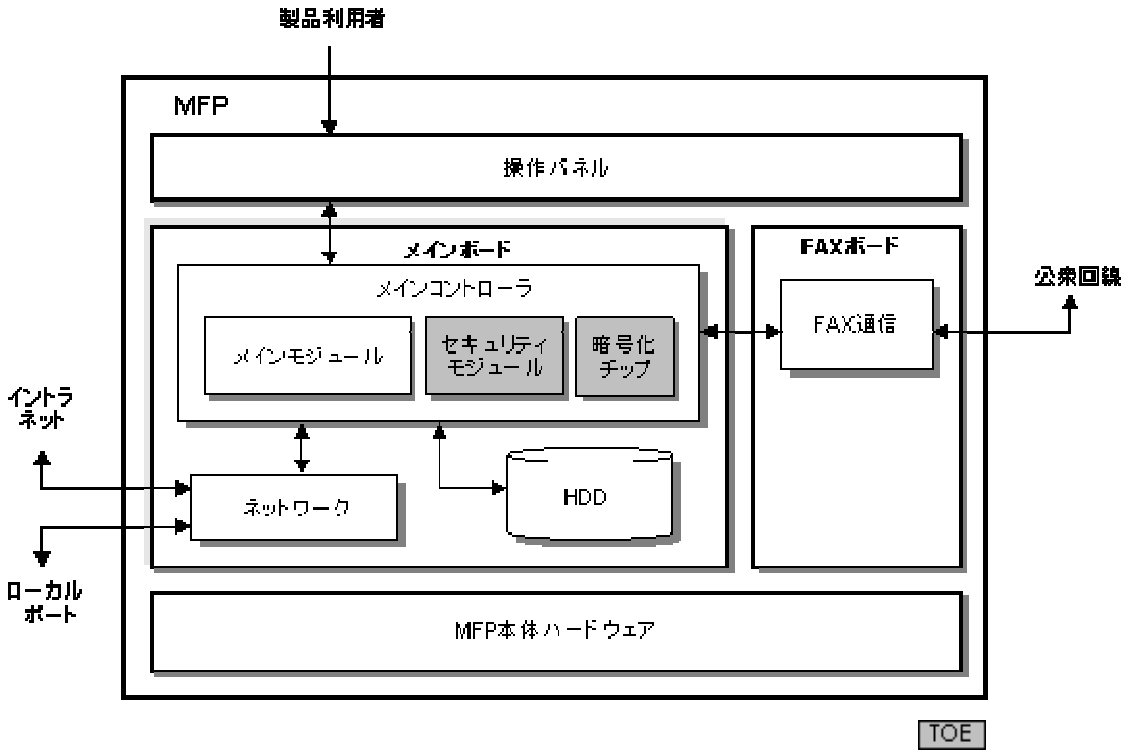


**図 1-2　TOE の構成図**

TOEの論理的構造の概念図を 図1-3 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。それぞれの機能の詳細については、「1.2.4 TOEの機能」、及び「1.5.4 セキュリティ機能」にて示す。

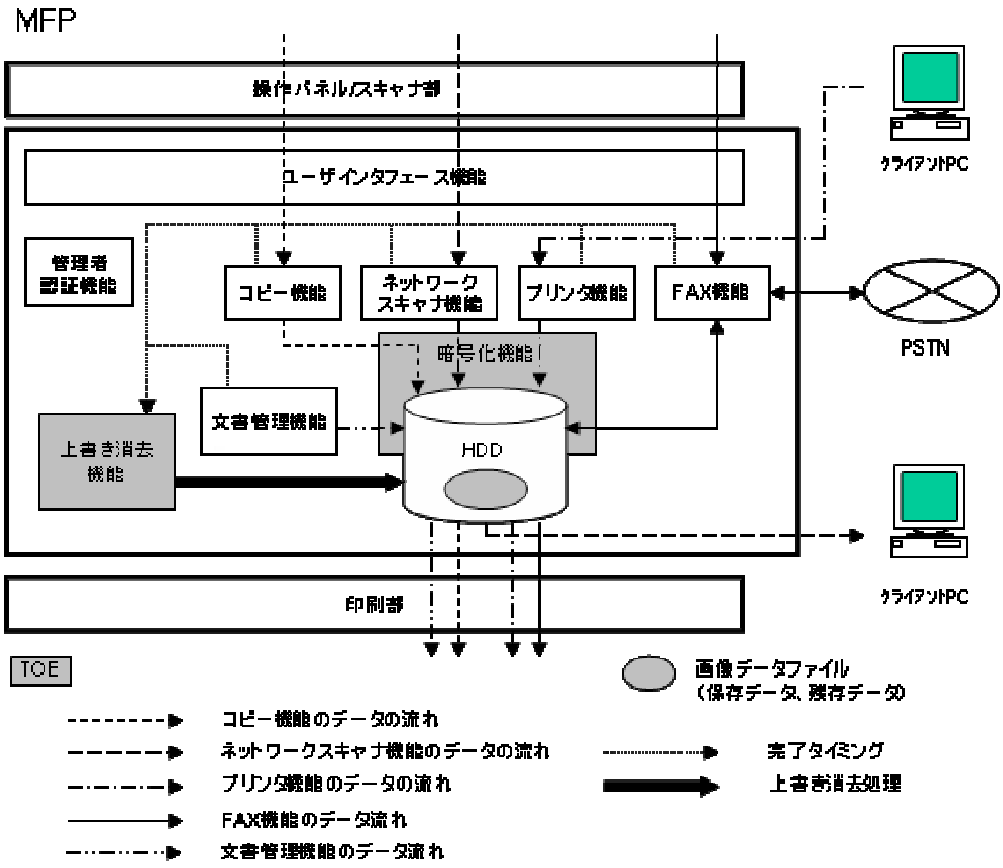


**図1-3 TOE の論理図**

### 1.2.4 TOEの機能

TOEが提供する機能は以下である。

- 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。

## 1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。
(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
(3) 本TOEがセキュリティ設計に基づいて開発されていること。
(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「京セラミタ　Data Security Kit (C) セキュリティターゲット 第0.17版」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11][14]のいずれか) 附属書C、CCパート2（[[6][9][12][15]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「京

セラミタ株式会社 Data Security Kit (C) Software 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[20][21]の内容を含む。

## 1.4 評価の認証

認証機関は、評価機関が作成した評価報告書・所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年2月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

## 1.5 報告概要

### 1.5.1 PP適合

適合するPPはない。

### 1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL3適合である。

### 1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、複合機にインストールを行われると自動的に動作するため、確率的な脆弱性となるインタフェースを持たない。よってSOF-基本で十分である。

### 1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

- 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。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。

- 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。

### 1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

**表1-1 想定する脅威**

| 識別子 | 脅 威 |
|---|---|
| T.AGAIN | 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。 |

### 1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

**表1-2 組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.REMAIN | 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。 |

### 1.5.7 構成条件

本製品は、京セラミタ株式会社の複合機「KM-3050、KM-4050、KM-5050、KM-3050i、KM-4050i、KM-5050i、CS-3050、CS-4050、CS-5050」に提供されるファームウェアとして提供される。

### 1.5.8 操作環境の前提条件

本TOEを使用する環境において有する想定される前提条件はない。

### 1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- KM-4050/KM-5050 使用説明書　応用編 (302GW56021 Rev.2.0)
- 3050/4050/5050 Advanced Operation Guide (Rev.2.1, Rev.3.0)
- KM-4050/KM-5050 使用説明書 (302GW56011 Rev.2.0)
- FAX System (M) 使用説明書 (303KH56050 2007.6)
- 3050/4050/5050 Operation Guide (302GN56014 Rev.3.0)
- 3050i/4050i/5050i Operation Guide (302GN56212 Rev.3.0)

- FAX System (M) Operation Guide (303KH56060 2007.6)

# 2 評価機関による評価実施及び結果

## 2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

## 2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成17年10月に始まり、平成20年2月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成19年12月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成19 年12月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

## 2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

### 2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1、図2-2に示す。

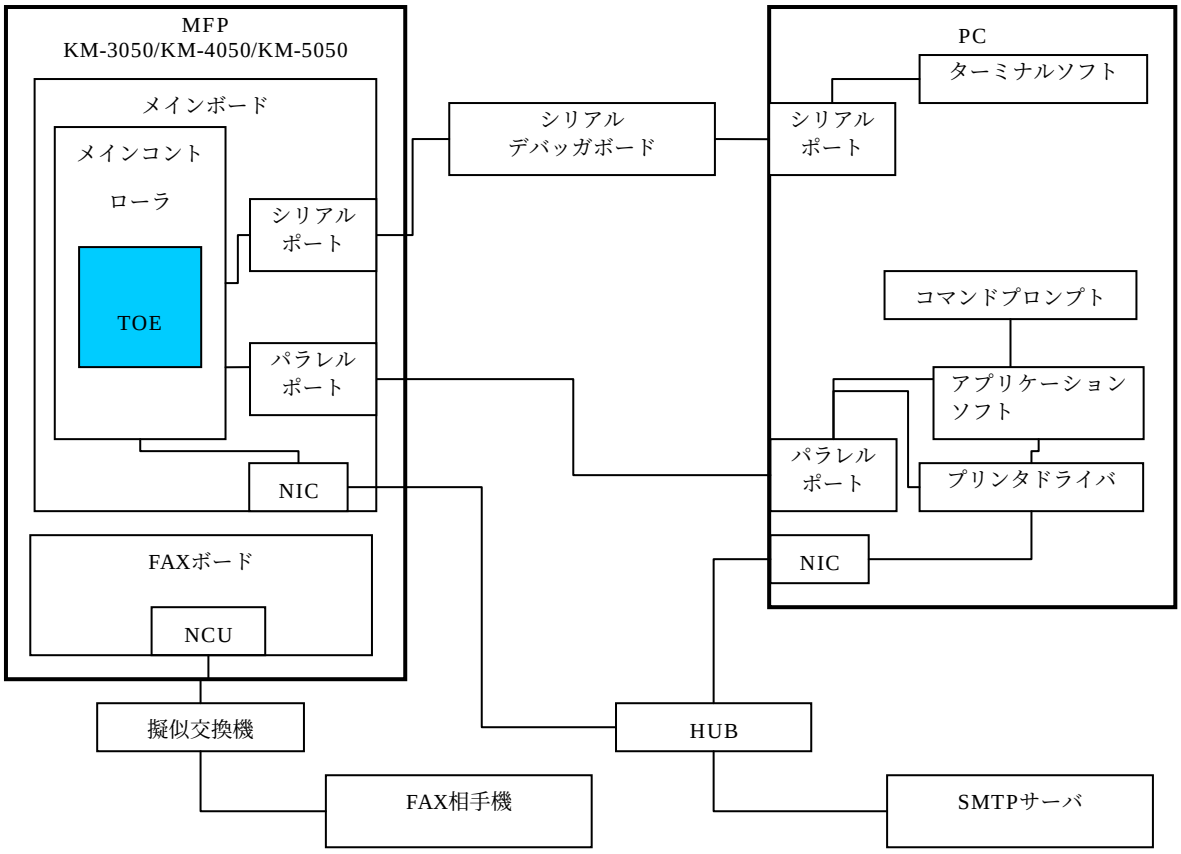


**図2-1　開発者テストの構成図1**

**※テストの対象とするMFPについて**

TOEは、複数のMFPに対応する。しかしながら、それらMFPの違いは、処理速度（30枚/40枚/50枚機）及びブランド（京セラミタ/IKON/コピスタ）の違いであり、TOEのセキュリティ機能は同一であるので、本テストではTOEが搭載されるMFPは、それぞれ、

どれか1台に対し、テストすることで問題ないものと判断する。

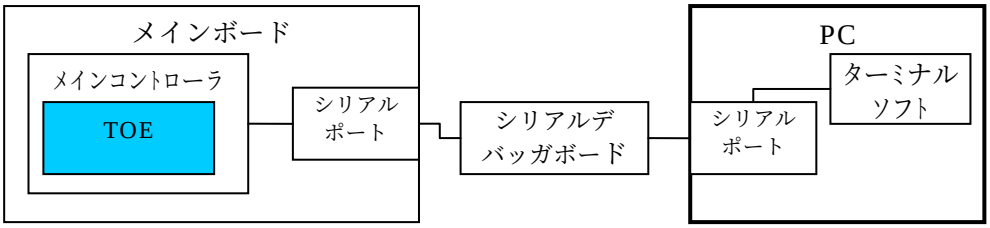


**図2-2　開発者テストの構成図2**

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1、図2-2に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

① 操作パネル等の目にみえる入出力インタフェースでセキュリティ機能を刺激し、観察する

② 目にみえる入出力インタフェースでは確認できない、暗号化や上書き消去されているデータを内部インタフェースから確認する

c.実施テストの範囲

テストは開発者によって43項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

### 2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施した開発者テストの構成を、図2-3、図2-4に示す。

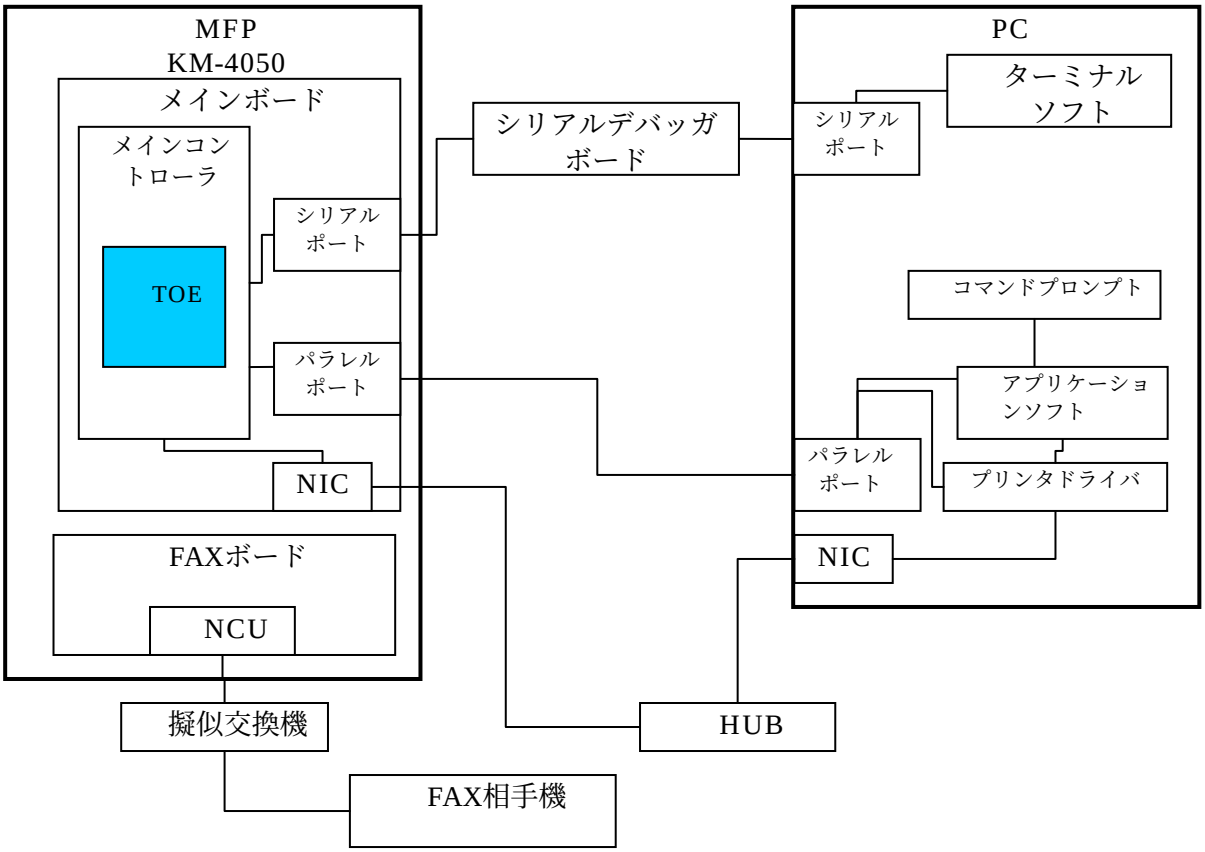


**図2-3　評価者テストの構成図1**

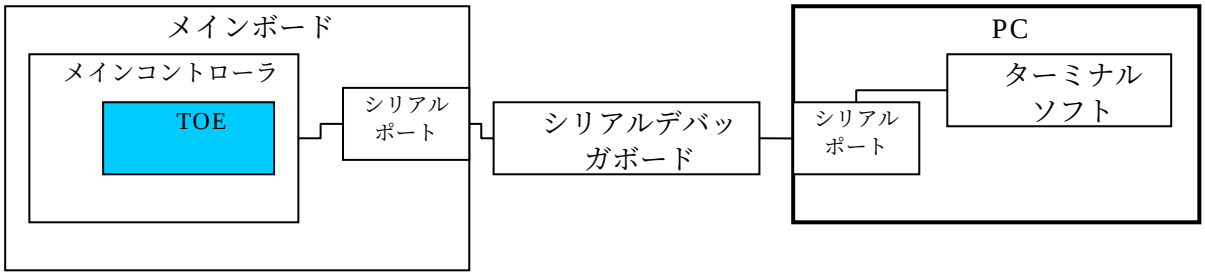


**図2-4　評価者テストの構成図2**

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-3、図2-4に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①一つは標準的な運用操作インタフェースの入出力を必要とする場合にMFPを使った環境

② 評価者テストに関しては操作パネルとクライアントインタフェース両方を使用する。

c.実施テストの範囲

評価者が独自に考案したテストを6項目、開発者テストのサンプリングによるテストを13項目、計19項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 評価者のテストに関しては上書き消去機能と暗号化機能両方を網羅する

② 評価者テストに関しては操作パネルとクライアントインタフェース両方を使用する。

③ サンプルテストに関しては、２つすべてのセキュリティ機能が網羅されている

④ サンプルテストに関しては、MFP機能の外部インタフェースは、コピー/プリンタ/FAX/スキャナ機能インタフェースを全て考慮している。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

## 2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

# 3 認証実施

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

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

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

# 4 結論

## 4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

**表4-1 評価者アクションエレメント検証結果**

| 評価者アクションエレメント | 検証結果 |
|---|---|
| **セキュリティターゲット評価** | **適切な評価が実施された。** |
| ASE_DES.1.1E | 評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。 |
| ASE_DES.1.2E | 評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。 |
| ASE_DES.1.3E | 評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。 |
| ASE_ENV.1.1E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。 |
| ASE_ENV.1.2E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.1E | 評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。 |
| ASE_INT.1.2E | 評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.3E | 評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。 |

| | |
|---|---|
| ASE_OBJ.1.1E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。 |
| ASE_OBJ.1.2E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_PPC.1.1E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_PPC.1.2E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_REQ.1.1E | 評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。 |
| ASE_REQ.1.2E | 評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_SRE.1.1E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_SRE.1.2E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_TSS.1.1E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。 |

| | |
|---|---|
| ASE_TSS.1.2E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| **構成管理** | **適切な評価が実施された** |
| ACM_CAP.3.1E | 評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。 |
| ACM_SCP.1.1E | 評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。 |
| **配付と運用** | **適切な評価が実施された** |
| ADO_DEL.1.1E | 評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。 |
| ADO_DEL.1.2D | 評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。 |
| ADO_IGS.1.1E | 評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。 |
| ADO_IGS.1.2E | 評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。 |
| **開発** | **適切な評価が実施された** |
| ADV_FSP.1.1E | 評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。 |
| ADV_FSP.1.2E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。 |

| | |
|---|---|
| ADV_HLD.2.1E | 評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。 |
| ADV_HLD.2.2E | 評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。 |
| ADV_RCR.1.1E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。 |
| **ガイダンス文書** | **適切な評価が実施された** |
| AGD_ADM.1.1E | 評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| AGD_USR.1.1E | 評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| **ライフサイクルサポート** | **適切な評価が実施された** |
| ALC_DVS.1.1E | 評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。 |

| | |
|---|---|
| ALC_DVS.1.2E | 評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。 |
| **テスト** | **適切な評価が実施された** |
| ATE_COV.2.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。 |
| ATE_DPT.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。 |
| ATE_FUN.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。 |
| ATE_IND.2.1E | 評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。 |
| ATE_IND.2.2E | 評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。 |

| | |
|---|---|
| ATE_IND.2.3E | 評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。 |
| **脆弱性評定** | **適切な評価が実施された** |
| AVA_MSU.1.1E | 評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。 |
| AVA_MSU.1.2E | 評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。 |
| AVA_MSU.1.3E | 評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。 |
| AVA_SOF.1.1E | 評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。 |
| AVA_SOF.1.2E | 評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。 |
| AVA_VLA.1.1E | 評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。 |

| | |
|---|---|
| AVA_VLA.1.2E | 評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。 |

## 4.2 注意事項

特になし。

# 5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用された用語を以下に示す。

| | |
|---|---|
| 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。 |
| 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。 |
| セキュリティキット | セキュリティ機能を利用する際に、必須でダウンロードする必要のあるデータ。セキュリティキットは、導入時にサービス担当者によって設置される。 |
| 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。<br>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。 |
| MFP | Multi Function Printer の略。<br>複合機。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。 |
| NIC | Network Interface Card の略。<br>TOEを内部ネットワーク(LAN)に接続するための拡張カード。 |

# 6 参照


[1] 京セラミタ Data Security Kit (C) セキュリティターゲット 第0.17版 （2008年1月16日）京セラミタ株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

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

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

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

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031 (平成13年1月翻訳第1.2版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032 (平成13年1月翻訳第1.2版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033 (平成13年1月翻訳第1.2版)

[11] ISO/IEC15408-1: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general mode

[12] ISO/IEC15408-2: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC15408-3: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

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

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月 (平成13年2月翻訳第1.0版)

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

[20] CCIMB Interpretations-0407　平成16年8月

[21] 補足-0210 第2版、補足-0407　平成16年8月

[22] Data Security Kit (C) Software 評価報告書 第3.3版 2008年2月27日
有限責任中間法人　ITセキュリティセンター　評価部