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

申請受付年月日(受付番号)	**平成17年6月14日（IT認証5046）**
認証番号	C0033
認証申請者	**シャープ株式会社**
TOEの名称	AR-FR22
TOEのバージョン	VERSION S.10
PP適合	**なし**
適合する保証要件	EAL3+ADV_SPM.1
TOE開発者	**シャープ株式会社**
評価機関の名称	**社団法人　電子情報技術産業協会　ITセキュリティセンター**

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17年10月18日

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
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」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 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「AR-FR22 VERSION S.10」は、独立行政法人 情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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 はじめに

この認証報告書は、「AR-FR22 VERSION S.10」（以下「本TOE」という。）について「社団法人 電子情報技術産業協会 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シャープ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。

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:	AR-FR22
バージョン:	VERSION S.10
開発者:	シャープ株式会社

1.2.2 製品概要

本TOEは、デジタル複合機（Multi Function Device　以下「MFD」という。）のファームウェアアップグレードキットとして提供される。本TOEは、MFDの記憶デバイスに一時的に保存される実イメージデータに対して、そのデータの使用が終了した後に残存し漏洩することを防止する。実イメージデータが一時的に保存される記憶デバイスは、Flashメモリ及び揮発性メモリ(Random Access Memory)である。

本TOEは、MFDの機能である、PCFAX、ファクス送信、及びファクス受信が実施されたとき、実イメージデータがFlashメモリにスプールされる前に、暗号化を行う。またコピー、プリント、スキャン送信、PCFAX、ファクス送信、及びファクス受信のジョブ完了後、記憶デバイス内のスプールデータ領域を消去する。これらの暗号操作機能とデータ消去機能より、記憶デバイスに一時的に保存される実イメージデータの隠匿

性を確保し、不正な読み出しに対抗する。

1.2.3 TOEの範囲と動作概要

本TOEは、MFDのファームウェアアップグレードキットとして２枚のROM基板により提供される。本TOEとMFDの関係を図1-1に示す。なお、図1-1において本TOEは網掛けで示されている。

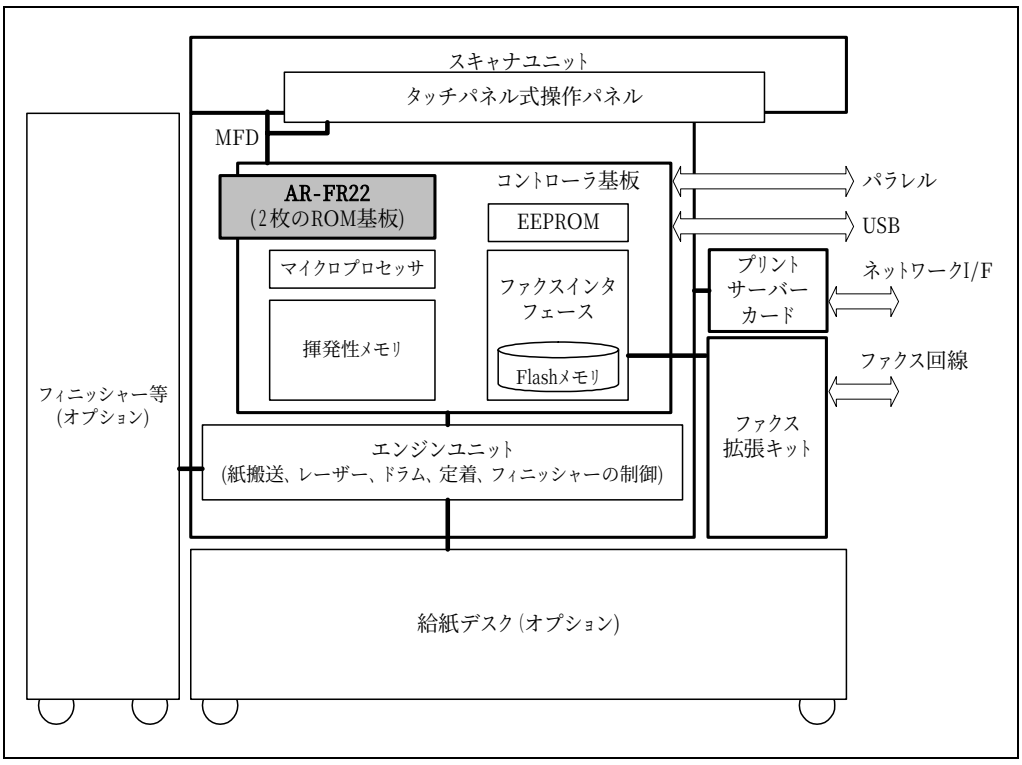

図1-1：MFDの物理的構成とTOEの物理的範囲

本TOEの論理的構成を図1-2に示す。図中、本TOEを太い枠線内として示す。長方形は本TOEの機能であり、角を丸くした長方形をハードウェアとして示す。本TOEの機能のうち、網掛け部がセキュリティ機能である。

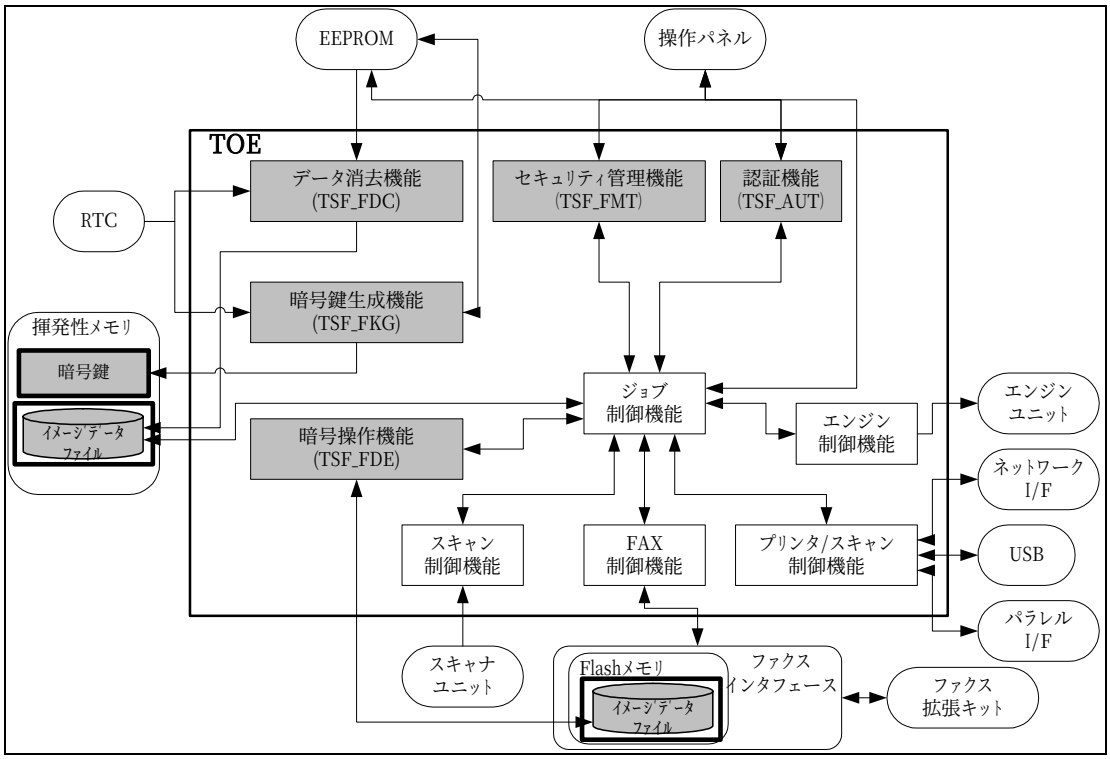

図1-2：TOEの論理的構成図

本TOEは、MFDにセキュリティ機能を追加するアップグレードキットであり、セキュリティ機能を提供すると共に、MFD全体の制御を行う。以下の機能が本TOEの論理的範囲に含まれる。

a) 暗号操作機能(TSF_FDE)

PCFAX、ファクス送信、ファクス受信の各ジョブに関し実イメージデータを暗号化した後にFlashメモリにスプール保存し、イメージデータファイルとして管理する。また、Flashメモリにスプール保存されている実イメージデータを読み込み、復号した後に利用する。

b) 暗号鍵生成機能(TSF_FKG)

暗号操作機能で提供する暗号化、及び復号の暗号鍵を生成する。生成された暗号鍵は、揮発性メモリに保存する。

c) データ消去機能(TSF_FDC)

各ジョブによりMSD内にスプール保存され、イメージデータファイルとして管理されている対応する実イメージデータ領域に対して、ランダム値、または固定値を上書きすることにより、実イメージデータを消去する。(各ジョブ完了後の自動消去)

また、MSDにスプール保存することが可能な全領域に対して、ランダム値、

または固定値を上書きすることにより上書き消去を行う。（キーオペレーターの操作による全データエリア消去）

以下の２つのデータ消去機能を提供する。

- 各ジョブ完了後の自動消去
  （ジョブ完了後、ジョブが使用した実イメージデータ領域の消去）

  ジョブ処理において、揮発性メモリにスプール保存されている実イメージデータ格納領域についてはランダム値を上書き消去し、Flashメモリにスプール保存されている実イメージデータ格納領域については、固定値を上書き消去する。

- キーオペレーターの操作による全データエリア消去
  （注釈： ジョブが正常に完了しなかった場合､及びジョブが未完了の場合、実イメージデータ領域に対する消去機能であり、MFDの所有者変更、もしくはMFD廃棄等において、実イメージデータからの情報漏洩を防止するために使用する）

  揮発性メモリRAMの全ての実イメージデータ領域をランダム値で上書き消去し、Flashメモリの全ての実イメージデータ領域を固定値で上書き消去する。

  キーオペレーターの操作による全データエリア消去は、キーオペレーターにより上書き消去を中止することができる。

d) 認証機能(TSF_AUT)

キーオペレーターコード（パスワード）によりキーオペレーターの識別認証を行う。

e) セキュリティ管理機能(TSF_FMT)

キーオペレーターとして認証された場合において､キーオペレーターコードの変更（改変）機能を提供する。

f) エンジン制御機能

コピージョブ､プリントジョブ､ファクス受信ジョブにおいて､エンジンユニットの制御を行う。

g) スキャン制御機能

コピージョブ、スキャン送信ジョブ、ファクス送信ジョブにおいて、原稿を読み取るため、スキャナユニットの制御を行う。

h) プリンタ／スキャン制御機能

本TOEを搭載可能なMFDのうち、プリンタ機能を標準、もしくはオプションにより搭載した場合に実施が可能な機能である。また、ネットワークを利用する場合はネットワーク機能をオプションにより搭載した場合に実施が可能である。

- プリントジョブにおいては、パラレル、USB I/F、もしくはネットワークI/Fを介して、受信した印刷データをプリントするために、ビットマップイメージを作成する。
- スキャン送信ジョブにおいては、スキャンされた実イメージデータを、指定された形式に変換後にネットワークI/Fを介して、ネットワークに送出する。

i) FAX制御機能

PCFAXジョブ、ファクス送信ジョブにおいてFAX回線への送出、またファクス受信ジョブにおいてFAX回線からの受信を制御する。

j) ジョブ制御機能

ジョブには、コピージョブ、プリントジョブ、スキャン送信ジョブ、PCFAXジョブ、ファクス送信ジョブ、ファクス受信ジョブがあり、それぞれMFDのコピー、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信の各動作を制御する。

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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「データセキュリティキットAR-FR22　セキュリティターゲット」（以下「本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、「データセキュリティキットAR-FR22 評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[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]のいずれか）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、本評価報告書、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17年9月の評価機関による本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

本STが規定するTOEの評価保証レベルは、EAL3追加である。

追加されるコンポーネントはADV_SPM.1である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃である。このため、攻撃者の攻撃力は“ 低レベル ”である。したがって、最小機能強度は“ 低レベル ”に対抗できる “ 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。

(1) 暗号鍵生成機能

TOEは、暗号鍵（共通鍵）の生成を行い、実イメージデータの暗号化機能をサポートする。MFDの電源がオンになると、必ず暗号鍵（共通鍵）を生成する。暗号鍵は、データセキュリティキット用暗号基準書に基づき、暗号化アルゴリズムAES Rijndaelを実施するための暗号鍵生成アルゴリズムであるMSN-J拡張アルゴリズムを用いて、128ビット長のセキュアな鍵を生成する。MSN-J拡張アルゴリズムで生成する鍵は、Flashメモリにスプール保存するための暗号操作で利用する。この暗号鍵は揮発性メモリ内に保存する。

(2) 暗号操作機能

ジョブ処理の途上において、ジョブのデータである実イメージデータをFlashメモリに、必ず暗号化後にスプール保存する。また、実イメージデータを実際に処理（利用）する際は、Flashメモリから暗号化後にスプール保存されている実イメージデータを読み出し、必ず復号後に利用する。

暗号化、復号については、暗号鍵生成（TSF_FKG）により生成された128ビット長の暗号化鍵を用い、FIPS PUBS 197に基づき、AES Rijndaelアルゴリズムにより実イメージデータを暗号化、もしくは復号する。Flashメモリへの暗号操作には

MSN-J拡張アルゴリズムで生成された鍵を利用する。

(3) データ消去機能

TOEは、スプール保存された実イメージデータファイルを消去するデータ消去機能を有する。本機能は、以下の２プログラムで構成される。

a) 各ジョブ完了後の自動消去

コピージョブ、プリントジョブ、スキャン送信ジョブ完了後、揮発性メモリにスプール保存されている実イメージデータファイルをランダム値で上書き消去する。

PCFAXジョブ、ファクス送信ジョブ、ファクス受信ジョブにおいては、実イメージデータとしてFlashメモリにスプール保存されている実イメージデータファイルを固定値で上書き消去する。

b) キーオペレーターの操作による全データエリア消去

キーオペレーターの操作による全データエリア消去実行の場合、認証(TSF_AUT)によるキーオペレーターの識別認証後、キーオペレーターの操作により、揮発性メモリのスプール保存のために利用される全ての実イメージデータをランダム値で上書き消去する。また、Flashメモリ上のスプール保存のために利用される全ての実イメージデータを固定値で上書き消去する。

キーオペレーターの操作による全データエリア消去中断の場合、キャンセル操作を選択後キーオペレーターコードの入力によるキーオペレーターの識別認証を要求する。キーオペレーター認証において、キーオペレーターに対する最後の認証成功以降の不成功認証試行回数が連続３回の認証失敗である場合、認証入力受付を５分間停止する。認証入力停止から通常状態へは自動的に復帰し、再認証入力を受け付ける。キーオペレーターコードを入力している間、TOEは入力した文字を隠蔽、及び入力文字数を示すため、入力数に対応し”＊”を表示する。

キーオペレーターコードは、入力文字と比較するための認証データとしてEEPROM内に管理されており、キーオペレーターの識別認証機能、及び文字の隠蔽機能は必ず実施され、キーオペレーターとして識別認証された場合についてのみ、上書き消去を中断する。

各ジョブ完了後の自動消去、キーオペレーターの操作による全データエリア消去のタイミングは、各ジョブ完了後、キーオペレーターの操作による全データエリア消去発動時に実施するよう管理されている。また、各ジョブ完了後の自動消去およびキーオペレーター操作による全データエリア消去は必ず実施される。

なお、揮発性メモリに対する上書き消去で使用するランダム値は、循環付き遅延フィ

ボナッチアルゴリズムに基づいて生成する。

(4) 認証機能

TOEは、TOEのセキュリティ管理機能であるキーオペレータープログラムの操作は、必ずキーオペレーターの識別認証を必要とする。これにより、キーオペレーターを特定し、利用者と役割を関連付けている。キーオペレーターの識別認証は、キーオペレータープログラムの選択後キーオペレーターコードの入力によるキーオペレーターの識別認証を要求する。キーオペレーター認証において、キーオペレーターに対する最後の認証成功以降の不成功認証試行回数が連続３回の認証失敗である場合、認証入力受付を5分間停止する。認証入力停止から通常状態へは自動的に復帰し、再認証入力を受付を受け付ける。キーオペレーターコードを入力している間、TOEは入力した文字を隠蔽、及び入力文字数を示すため、入力数に対応し“ *“ を表示する。キーオペレーターの識別認証機能、及び文字の隠蔽機能は必ず実施され、キーオペレーターとして識別認証された場合についてのみ、キーオペレータープログラムの操作が可能である。

データ消去 (TSF_FDC)のうちのキーオペレーターの操作による全データエリア消去の実行、及びセキュリティ管理(TSF_FMT)のキーオペレーターコードの問い合わせと改変は、必ずキーオペレーターとして認証(TSF_AUT)された場合についてのみ操作を可能とする。

(5) セキュリティ管理機能

キーオペレーターコードは、セキュリティ管理(TSF_FMT)により管理されている。セキュリティ管理(TSF_FMT)は、必ず認証（TSF_AUT）によりキーオペレーターを識別認証された後に実施可能とする。このため、認証（TSF_AUT）と同じく、キーオペレーターを特定し、利用者と役割を関連付けている。また、キーオペレーターコードを改変（変更）後も、キーオペレーターとして役割が維持される。

a) キーオペレーターコードの変更

キーオペレーターコードの問合せ、及び改変（変更）ができる。変更されるキーオペレーターコードについて、必ず5文字の数字であることを検査する。

各設定値を変更すると、MFD内のEEPROM内に保存される。

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.RECOVER	低レベルの攻撃者が、MFD内のFlashメモリに、MFD以外の装置を使用することにより、Flashメモリ内に残存する実イメージデータを読み出し漏洩させる。

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.RESIDUAL	コピー、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信ジョブ終了、もしくはジョブを中止した場合、MSDにスプール保存された実イメージデータ領域は上書き消去されなければならない。MFDの廃棄または所有者変更の際、キーオペレーターにより、MSDのスプール領域全体は上書き消去されなければならない。

1.5.7　構成条件

本TOEが動作するMFDは、シャープ デジタル複合機AR-M351U, AR-M451U, AR-M355U, AR-M455U, AR-M355UJ, AR-M455UJ, AR-311S, AR-351S, AR-451S, AR-311FP, AR-351FP, AR-451FPである。

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前提条件を表1-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-3 TOE使用の前提条件

識別子	前提条件
A.OPERATOR	キーオペレーターは、TOEに対して不正をせず信頼できるものとする。

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。

(1) 日本語版

■取扱説明書データセキュリティキット AR-FR22

バージョン ：CINSJ3105FC51
対象者 ：キーオペレーター（利用者サイトの管理者）
内容 ：本TOEを利用するガイドとして提供され、セキュリティ機能の使い方、設定方法などTOEの管理、運用に必要な事項が述べられている。表記言語は日本語

■注意書データセキュリティキット AR-FR22

バージョン ：TCADZ6053FCZZ
対象者 ：キーオペレーター、利用者
内容 ：本TOEをセキュアに利用するために、管理者や利用者が注意しておかなければならない事項や運用方法が述べられている。表記言語は日本語。

■AR-FR22設置手順書

バージョン ：TCADZ6049FCZZ
対象者 ：キーオペレーター、サービスマン（販売会社から派遣される保守管理者）
内容 ：本TOEを複合機本体に取り付ける際の作業要領、及びTOEの設置に伴い、サービスマン、キーオペレーターが行うべき事項が述べられている。表記言語は日本語。

(2) 海外版

■AR-FR22 Data Security Kit Operation Manual

バージョン　：CINSZ3106FC51

対象者　　：キーオペレーター（利用者サイトの管理者）

内容　　：本TOEを利用するガイドとして提供され、セキュリティ機能の使い方、設定方法などTOEの管理、運用に必要な事項が述べられている。表記言語は英語

■AR-FR22 Data Security Kit Notice

バージョン　：TCADZ6054FCZZ

対象者　　：キーオペレーター、利用者

内容　　：本TOEをセキュアに利用するために、管理者や利用者が注意しておかなければならない事項や運用方法が述べられている。表記言語は英語。

■AR-FR22設置手順書（英独仏西語版）

バージョン　：TCADZ6050FCZZ

対象者　　：キーオペレーター、サービスマン（販売会社から派遣される保守管理者）

内容　　：本TOEを複合機本体に取り付ける際の作業要領、及びTOEの設置に伴い、サービスマン、キーオペレーターが行うべき事項が述べられている。表記言語は英語、独語、仏語、スペイン語の4ヶ国語。

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パート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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、本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6月に始まり、平成17年9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17年7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17年7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環境を図2-1に示す。

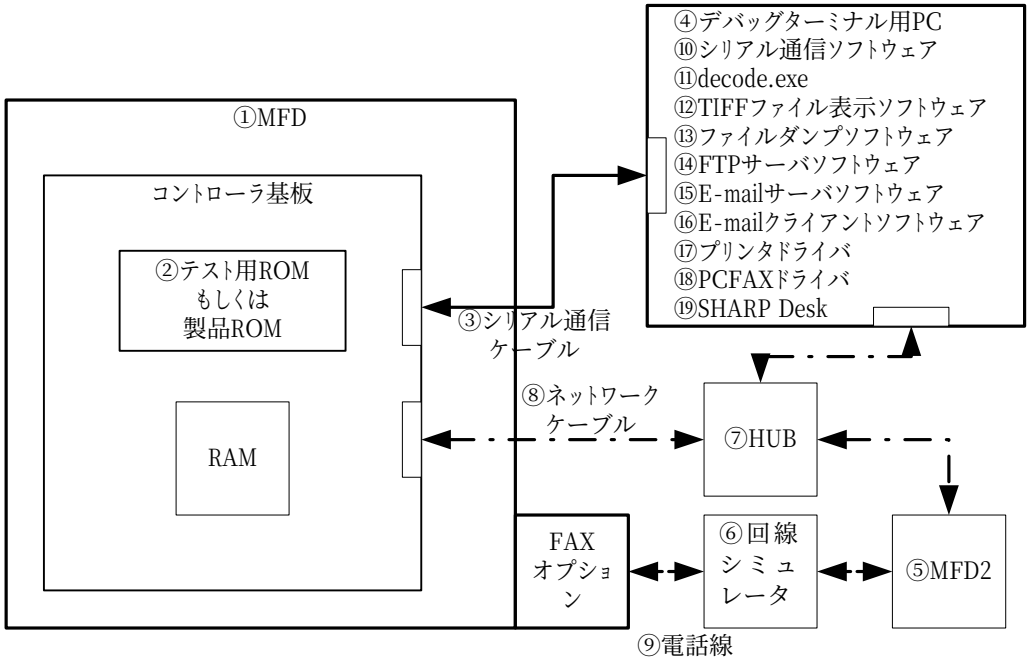

図2-1　開発者テスト及び評価者テストの構成図

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は図2-1のとおりである。

開発者テストは、STにおいて識別されているTOE構成と同等のハードウェア及びソフトウェア構成のテスト環境で実施された。以下は、テスト構成がSTにおいて識別される構成と完全には一致しない部分について、同等であるとみなせる理由である。

図2-1の①「MFD」は、STで動作環境として識別されている複数のMFDの機種のうちの一部の機種がテストにおいて使用された。この機種はSTで動作環境として識別されるすべてのMFDの機種の機能を含むため、テスト構成におけるMFDはSTで動作環境として識別されているMFDと同等であるとみなすことができる。

図2-1の②「テスト用ROM」はSTで識別されるTOEとは異なるが、これは製品ROM(TOE)に対し、テストの便宜のためにデバッグ機能の追加及び一部のセキュリティ機能の変更がなされたものである。テストの便宜のために変更されたセキュリティ機能に関しては、変更される前のセキュリティ機能が正しく動作することが製品ROMを使用してテストが行われた。したがって、テスト用ROMと

製品ROMを使用して行われたテストは、STにおいて識別されたTOEをテストしたことと同等であるとみなすことができる。

b.テスト手法

TOEのセキュリティ機能のすべてのテストは、TOEテスト環境構成の環境下で実施する。TOEのテスト環境として下記の2種類の環境が存在する。

①製品ROM使用

利用者が実際に使用する環境と同じ構成。

デバッグ用のシリアル通信ケーブルは未接続。

②テスト用ROM使用

製品ROM使用環境に対して、コントローラ基板にシリアル通信ケーブルを接続し、RAM上の実イメージデータおよび上書き消去後のデータをデバッグターミナルに読み出すためのテスト用ROMを使用している。また、暗号鍵RAM上の外部変数領域およびFlashメモリ内のデータをデバッグターミナルに出力する機能を備えている。

テストの便宜上、暗号鍵をall0、上書き消去の乱数を上書き消去回数を表す値に切り替える機能も備えている。

c.実施テストの範囲

テストは開発者によって28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

評価者が実施したテストの環境は、図2-1に示す環境から「⑮E-mailサーバソフトウェア」と「⑯E-mailクライアントソフトウェア」を除いたものである。

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環境は、図2-1に示す環境から「⑮E-mailサーバソフトウェア」と「⑯E-mailクライアントソフトウェア」を除いたものである。

評価者テストにはE-mailを利用するテストは含まれないため、これらのソフトウェアが除かれたことによるテスト結果への影響はない。したがって、評価者テストは、開発者テストと同等の構成で実施されたとみなすことができる。

b.テスト手法

評価者が実施したテストには、TOEのテスト環境として下記の２種類の環境が存在する。

①製品ROM使用

利用者が実際に使用する環境と同じ構成。

デバッグ用のシリアル通信ケーブルは未接続。

②テスト用ROM使用

製品ROM使用環境に対して、コントローラ基板にシリアル通信ケーブルを接続し、RAM上の実イメージデータおよび上書き消去後のデータをデバッグターミナルに読み出すためのテスト用ROMを使用している。また、暗号鍵RAM上の外部変数領域およびFlashメモリ内のデータをデバッグターミナルに出力する機能を備えている。

テストの便宜上、暗号鍵をall0、上書き消去の乱数を上書き消去回数を表す値に切り替える機能も備えている。

c.実施テストの範囲

評価者が独自に考案したテストを7項目、開発者テストのサンプリングによるテストを6項目、計13項目のテストを実施した。

独立テスト項目の選択基準として、下記を考慮している。

① 識別されたすべてのセキュリティ機能(5個)のテストを含むこと。

② セキュリティ対策方針から重要と考えられる機能（暗号鍵生成）のテスト

③ 異常系の処理に対してもTOEが機能仕様書どおりに動作すること

④ 前回認証を取得したAR-FR12Mから新たに追加された機能

⑤ 開発者が実施していない消極的テスト

⑥ TOEが対応するとした他機種の複合機にTOEを設置してのテスト

開発者テストのサンプリングについては、5つのセキュリティ機能のうち大部分が含まれるよう、かつ、重要なセキュリティ機能であるデータ消去機能が実施されるさまざまな場合がテストされるよう考慮している。

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

本評価報告書をもって、評価者は本TOEがCEMパート2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

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本評価報告書で示されたように評価されていること。

④ 本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 本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、本ST及び本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

提出された本評価報告書、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及び保証コンポーネントADV_SPM.1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種別、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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概説が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、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理路整然とし、完全であり、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。IT環境の要件は規定されていないことを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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理路整然とし、完全であり、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が理路整然とし、完全であり、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、実地検査及び録画された音声・映像の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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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環境に対する要求はないためIT環境に対する要件は不適用であること、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
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いることを確認している。IT環境に対するセキュリティ要件はないので、それに関しては管理者ガイダンスへの記述は不要であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、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いることを確認している。対応すべき機能や特権に関する警告、IT環境に対するセキュリティ要件は、それらの記述が不要で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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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主張が正しことを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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
AES	Advanced Encryption Standard NIST(米国商務省標準技術局)で制定された米国政府標準暗号
DSK	Data Security Kit
EEPROM	Electronically Erasable Programmable ROM 不揮発性メモリの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM
I/F	Interface
IFAX	Internet FAX
MSD	Mass Storage Device 本TOEの場合、ファイルシステムにより管理されている揮発性メモリ、及びFlashメモリがMSDに相当する。
OS	Operating System
RAM	Random Access Memory
ROM	Read Only Memory

TIFF-FX	Tag Image File Format Fax eXtended. インターネットFAX規格で規定された画像フォーマット。

本報告書で使用された用語を以下に示す。

イメージデータ	MFDにてコピー、プリント、スキャン、もしくはファクス送信のため、原稿画像を読み込みデジタル化したデータ。PCFAX、ファクス送信、ファクス受信においては、電話回線への送信、もしくは電話回線から受信したデータを含み、このデータをMFDで取扱可能な様に変換したデータもイメージデータと呼ぶ。
エンジン	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。プリントエンジン、エンジンユニットともいう。
キーオペレーター	TOEのセキュリティ管理機能、あるいはMFD管理機能にアクセス可能な、認証された利用者。
キーオペレーターコード	キーオペレーターの認証の際に用いられるパスワード。
キーオペレータープログラム	TOEのセキュリティ管理機能。MFD管理機能でもある。キーオペレータープログラムにアクセスするためには、キーオペレーターとして識別認証されなければならない。
ジョブ	MFD機能（コピー、プリント、スキャン送信、PCFAX、ファクス送信、ファクス受信）において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
データセキュリティキット	シャープのデジタル複合機専用のアップグレード キット AR FR22。
メモリ	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。
基板	プリント基板に部品を半田付け実装したものを指す。
実イメージデータ	イメージデータから管理領域を除いた実イメージデータ部分。

全データエリア消去	MFDが搭載しているMSDについて、スプール保存に利用される全ての実イメージデータ領域に対する上書き消去処理。キーオペレーターのみが実施可能であるため、キーオペレーターの操作による全データエリア消去ともいう。
操作パネル	表示部、ボタンキー、タッチパネル上に形成されたボタンを含む、ユーザI/Fのためのデバイス。または、そのユニット。
揮発性メモリ	電源を切ると記憶内容が失われるメモリのこと。
不揮発性メモリ	電源を切っても記憶内容を保持することができるメモリのこと。半導体素子、あるいは磁気記憶を用いたものがある。
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去及び任意部分の再書き込みを可能にしたROM

6 参照

[1] データセキュリティキットAR-FR22　セキュリティターゲット バージョン 0.09（2005年7月29日）

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-08

[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

[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

[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

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[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

[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

[21] 補足-0210 第2版 及び 補足-0407

[22] データセキュリティキット AR-FR22 評価報告書 第2.2版 2005年9月9日 社団法人 電子情報技術産業協会　ITセキュリティセンター