認　証　報　告　書

評価対象

申請受付年月日（受付番号）	平成16年 4月19日　（IT認証4026）
認証申請者	シャープ株式会社
TOEの名称 （TOEのバージョン）	日本：　データセキュリティキットAR-FR4 version M.20 海外：　Data Security Kit AR-FR4 version M.20, Data Security Kit AR-FR5 version E.20
ＰＰ適合	なし
適合する保証要件	EAL4
TOE開発者	シャープ株式会社
評価機関の名称	株式会社富士総合研究所 情報セキュリティ評価センター

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16年9月15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 ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 － 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ 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
⑤ Common Methodology for Information Technology Security Evaluation Version 1.0
⑥ CCIMB Interpretations-0210
⑦ 認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「日本：データセキュリティキット AR-FR4 version M.20、海外：Data Security Kit AR-FR4 version M.20,Data Security Kit AR-FR5 version E.20」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

本認証報告書は、「日本：データセキュリティキット AR-FR4 version M.20、海外：Data Security Kit AR-FR4 version M.20,Data Security Kit AR-FR5 version E.20」（以下「本TOE」という。）を株式会社富士総合研究所 情報セキュリティ評価センター（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: 日本： データセキュリティキットAR-FR4 version M.20
海外： Data Security Kit AR-FR4 version M.20,
Data Security Kit AR-FR5 version E.20

・開発者: シャープ株式会社

製品名称については販売対象地域（言語）により異なるが、TOE自体は同一物である。

1.2.2 製品概要

本製品（デジタル複合機データセキュリティキット。以降「DSK」という。）は、デジタル複合機（Multi-Function Device。以降「MFD」という。）内に一時的に保存されるドキュメントデータやイメージデータが開示される危険性を減ずることを目的としたファームウェアである。

MFDとは、プリント機能ユニットに、コピー、イメージスキャニング、ファクス各機能ユニットを選択構成可能な事務機器である。プリンタ機能ユニットのみ搭載の場合はMFP(Multi-Function Printer)と呼びMFDの一種として取り扱う。DSKは、このMFDのファームウェアのアップグレードキットとして提供される。

1.2.3 TOEの範囲と動作概要

本TOEの物理的範囲はDSKとなる。DSKは**図 1**に示すようにMFD内のファームウェアROMとして標準装備のものに置き換わり装着される。

DSKを含むコントローラユニットはマイクロプロセッサとそれにより実行されるファームウェア、ファームウェア実行時に使用される揮発性RAM、セキュリティ設定を格納するEEPROMを有する。TOEの保護資産となるスプールデータは揮発性RAMの領域にRAMディスクとして保持され、この代わりにオプションとしてHDDを装着することもできる。オプションであるファクス機能についてはファクスインタフェース上のFlashメモリがスプール用として用いられる。これらHDD,RAM及びFlashメモリをMSD(Mass Storage Device)と呼ぶ。MFDの各種操作はDSKのセキュリティ設定を含め操作パネルを通して行われる。

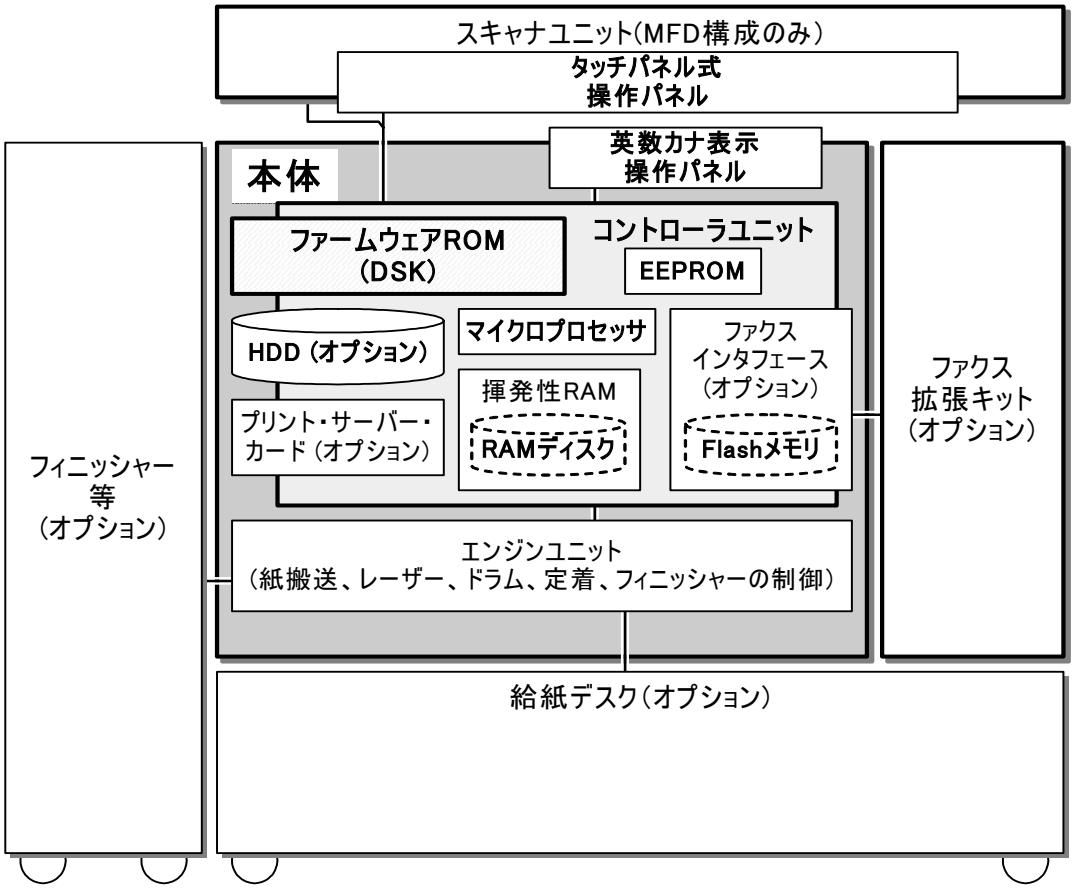

図 1 デジタル複合機におけるDSKの位置づけ

本TOEの論理的範囲を図 2の枠線に示す。TOEはMFDのコントローラユニットのファームウェアであり、既成のMFDの機能に対し操作パネルからの入力あるいは

MSDへの書き込みに介在しセキュリティ機能遂行のためのコードが呼び出される。

TOE中のセキュリティ機能については白抜き文字で略称を示す。これらについては1.5.4で詳述する。網掛け部分は操作パネルに関連するユーザインタフェースでのパラメータ設定、メッセージ機能である。その他はMSD中のスプールデータに対する暗号化及び消去のための機能となる。

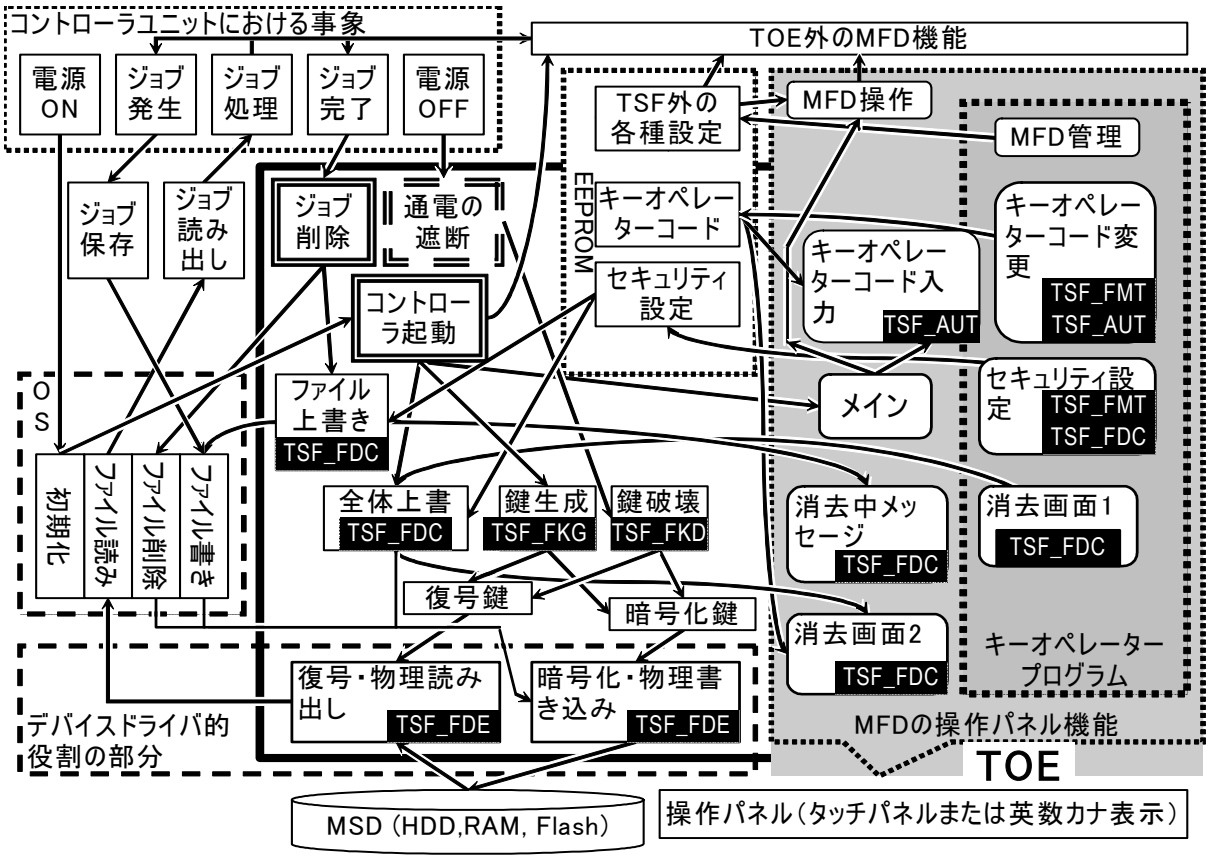

図 2 TOEの論理的範囲

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って、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「デジタル複合機データセキュリティキット AR-FR4/AR-FR5 セキュリティターゲット Version 0.04」（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、「デジタル複合機データセキュリティキット AR-FR4/AR-FR5 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。評価は、平成16年8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、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、**EAL4**適合である。

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、一般のオフィスで利用されることを想定する。TOEへの直接的な攻撃手法・時間は想定環境によって制限される。このため、低レベルの攻撃力に対抗できるレベルである”SOF-基本”で満足される。

また、MSDを利用環境から持ち出した場合にも、データ消去及び暗号化の機能により低レベルの攻撃力に対抗可能である。ただし、暗号化機能は本評価における機能強度の対象でない。

1.5.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。各セキュリティ機能項目の略称は図 2 中のものと対応する。

(1) データ消去機能(TSF_FDC)

MFDはドキュメントやイメージデータを、プリンタ、コピー、イメージスキャニング処理ではHDDまたはRAMディスク領域内に、ファクス処理ではFlashメモリ領域にスプールする。ジョブ完了時にそれらの領域はメモリ管理上フリーとなるが、実際にはメモリ上に残存している。

TOEのデータ消去機能は、スプール領域(HDD、RAMディスク、Flashメモリ)のデータを上書きによる消去を行う。データ消去機能は、ジョブの完了時に対象となるデータの領域に対して自動的に行う「各ジョブ完了後の自動消去」、TOEの電源ON時にHDDまたはRAMディスクのスプール領域全体に対して上書きによる消去を自動的に行う「電源ON時の自動消去」、そして手動操作によりHDDまたはRAMディスク、及びFlashメモリの領域全体に対して上書きによる消去を行う「全データエリア消去」がある。

データ消去機能は操作パネルより設定を行う。各ジョブ完了後の自動消去、全データエリア消去あるいは電源ON時の自動消去の実行の際それぞれ、消去中メッセージ、消去画面１、消去画面２が表示される。

(2) 暗号操作機能(TSF_FDE)

MFDはデータ処理の際、MSDにデータファイルを作成し、ジョブ毎に該当するデータを読み出す。暗号操作機能ではデータファイル作成に際してデータを後述の暗号鍵生成機能により作成した暗号鍵で暗号化した後MSDに書き込み、データ処理の際に読み出しに必要なデータを同暗号鍵にて復号する。

(3) 暗号鍵生成機能(TSF_FKG)・暗号鍵破壊機能(TSF_FKD)

暗号鍵の生成機能及び破壊機能は、上記暗号操作機能で用いる鍵の生成、破壊を行う。暗号鍵生成機能では、MFDの起動時に日時及びティック時間を基に暗号鍵を生成し、揮発性RMA上に保存する。この鍵は操作パネル及びその他の外部インタフェースからアクセスすることはできない。暗号鍵破壊機能は、電源オフか停電により揮発性RAMへの通電が遮断されることで実現される。暗号鍵生成機能によって生成された暗号鍵は、暗号鍵破壊機能により破壊されるまで使用される。

(4) 認証機能(TSF_AUT)

後述のセキュリティ管理機能へのアクセスを、キーオペレータというMFD

管理者のみが可能とするため、認証機能を持つ。キーオペレータは、キーオペレータコードを操作パネルより入力し、これがMFDのEEPROMに保存されている値と一致することで認証される。

(5) セキュリティ管理機能(TSF_FMT)

ユーザによる管理が可能なTOEのセキュリティ機能の設定とそのインタフェースを提供する。ユーザインタフェースは操作パネルであり、セキュリティ管理機能は次の通りである。

- データ消去機能設定

  データ消去機能(TSF_FDC)のふるまいを設定する。設定可能項目は、電源ON時の自動消去の実行・不実行、各ジョブ完了後の自動消去の消去回数、全データエリア消去の消去回数、電源ON時の自動消去の消去回数。設定値はEEPROMに保持されている。

- キーオペレータコード設定

  認証に用いるキーオペレータの変更を行なう。このときTOEは入力された新たなキーオペレータコードが5桁の値を持つことを検査する。設定値はEEPROMに保存される。

1.5.5 脅威

本TOEは、表 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 想定する脅威

識別子	脅威
T.RECOVER	悪意の利用者が、MFDからMSDを物理的に取り出した後、市販のツールを使用して内容を読み出して、コピー、プリント、イメージスキャニング、ファクスの各ジョブのMSD内の残存データからドキュメントデータやイメージデータの再生を試みる可能性がある。
T.ALTER	悪意の利用者が、TOEのセキュリティ管理機能の設定値を改変する可能性がある。

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はない。

1.5.7 構成条件

本TOEは、既製品であるMFDのアップグレードキットとして、対象MFDのROMの一部を差し替える交換用ROM製品という形態をとる。本TOEが対象とするMFDのモデルのリストを表 2に示す。

表 2 TOEの対象MFDモデル

DSKモデル・バージョン	対象MFDモデル
AF-FR4 Version M.20	海外向けMFD-model AR-M350, AR-M450, AR-M280N, AR-M350N, AR-M450N, AR-M280U, AR-M350U, AR-M450U, AR-M300U, AR-M300N, DM-3551, DM-4551 国内向けMFD-model AR-310M, AR-350M, AR-450M, AR-310S, AR-350S, AR-450S, AR-310F, AR-350F, AR-450F, DM-3551, DM-4551
AF-FR5 Version E.20	海外向けプリンタmodel AR-P350, AR-P450, DM-3500, DM-3501, DM-4500, DM-4501

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 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 3 TOE使用の前提条件

識別子	前提条件
A.OFFICE	TOEが組み込まれたMFDは、一般的なオフィス環境に設置される。オフィスに働く従業員が不在の場合､オフィスは施錠等による防犯対策が実施されている。また、従業員不在時の入室の際は、適切な従業員であることを確認するようオフィスは管理されている。
A.PROCEDURE	キーオペレータは、以下の事項を遵守するものとする。 ・TOEがインストールされていることを確認する。 ・消去ふるまい設定、消去回数設定を適切に行なう。 ・キーオペレータコードを定期的に変更する。

	・キーオペレータコードは容易に推測できないものを設定する。 ・キーオペレータコードを他者に開示しない。

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。

●AR-FR4　日本語版

・ドキュメント名：取扱説明書 データセキュリティキット AR-FR4
・バージョン　　：2003L DSC1 CINSJ2300FC53
・対象者　　：キーオペレータ（利用サイトの管理者）
・内容　　：本TOEを利用するガイドとして提供され、TOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は日本語。

・ドキュメント名：AR-FR4 設置手順書※
・バージョン　　：TCADZ6011FCZ1①
・対象者　　：DSKサービスマン（販売会社から派遣される保守管理者）
・内容　　：AR-FR4 日本語版の提供形態はROM（BOOT ROMとMAIN ROMの2つ）であり、これをMFPに取り付ける作業要領が述べられている。表記言語は、日本語を始めとして、英語、仏語、独語、西語の5ヶ国語。

・ドキュメント名：SHARP MFP Data Security Kit Version:M.20 E.20　設置チェックリスト　取扱説明書追補版 Models:AR-FR4 AR-FR5
・バージョン　　：1.0
・対象者　　：キーオペレータ、DSKサービスマン
・内容　　：本TOEの設置に伴い、DSKサービスマン及びキーオペレータが行うべきTOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は、日本語。

●AR-FR4　海外版

・ドキュメント名：AR-FR4 Data Security Kit Operation Manual
・バージョン　　：2003M DSC1 CINSZ2302FC53
・対象者　　：キーオペレータ（利用サイトの管理者）
・内容　　：本TOEを利用するガイドとして提供され、TOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は英語、仏語、独語、西語の4ヶ国語。

・ドキュメント名：AR-FR4 設置手順書※

・バージョン　：TCADZ6011FCZ1①
・対象者　：DSKサービスマン（販売会社から派遣される保守管理者）
・内容　：AR-FR4 海外版の提供形態はROM（BOOT ROMとMAIN ROMの2つ）であり、これをMFPに取り付ける作業要領が述べられている。表記言語は、日本語を始めとして、英語、仏語、独語、西語の5ヶ国語。

・ドキュメント名：SHARP MFP Data Security Kit Version:M.20 E.20　Installation Checklist Supplemental Sheet　Models:AR-FR4 AR-FR5
・バージョン　：1.0
・対象者　：キーオペレータ、DSKサービスマン
・内容　：TOEの設置に伴い、DSKサービスマン及びキーオペレータが行うべきTOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は、英語。

●AR-FR5　海外版

・ドキュメント名：AR-FR5 Data Security Kit Operation Manual
・バージョン　：2003M DSC1 CINSZ2304FC53
・対象者　：キーオペレータ（利用サイトの管理者）
・内容　：本TOEを利用するガイドとして提供され、TOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は英語、仏語、独語、西語の4ヶ国語。

・ドキュメント名：AR-FR4 設置手順書※

・バージョン　：TCADZ6011FCZ1①
・対象者　：DSKサービスマン（販売会社から派遣される保守管理者）
・内容　：AR-FR5 海外版の提供形態はROM（MAIN ROMのみ）であり、これをMFPに取り付ける作業要領が述べられている。表記言語は、日本語を始めとして、英語、仏語、独語、西語の5ヶ国語。

・ドキュメント名：SHARP MFP Data Security Kit Version:M.20 E.20　Installation Checklist Supplemental Sheet Models:AR-FR4 AR-FR5
・バージョン　：1.0
・対象者　：キーオペレータ、DSKサービスマン
・内容　：TOEの設置に伴い、DSKサービスマン及びキーオペレータが行うべきTOEのセキュアな管理・運用に必要な事項が述べられている。表記言語は、英語。

※　設置手順書はAR-FR4日本語版とAR-FR4/FR5の英語版、独語版、仏語版、西語版[AR-FR4/FR5 Installation Manual]の共通ドキュメントである。

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、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16年5月に始まり、平成16年8月本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16年5月に開発・製造現場へ赴き、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、記録及びスタッフへのヒアリングにより実施し、同年5月に評価機関で開発者のテスト環境と同等の環境を構築し開発者サンプリングテスト及び評価者テストも実施している。

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、本TOEは認証番号C0004[23]で認証されたTOEと同製品であり、適用可能な評価については認証番号C0004の評価結果を本評価に適用する。

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システムの構成を図 3に示す。また、テスト環境で使用された機器およびソフトウェアツールを表 4に示す。

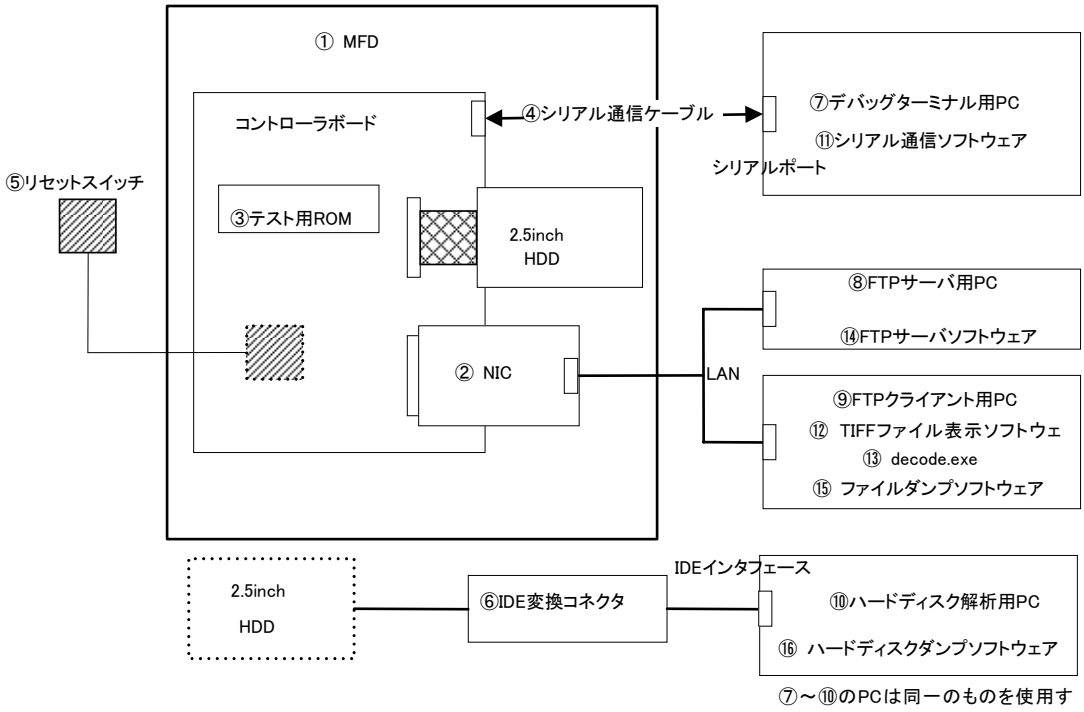

図 3 開発者テストシステム構成図

表 4 開発者テスト使用機器・ツール

名称	概要（種別）
テスト機器	
①MFD	TOEを搭載するMFD （AR-350S）
②NIC	MFDをLANに接続するための基板
③テスト用ROM	TOE (AR-FR4 version.M20)
④シリアル通信ケーブル	MFDとデバッグターミナル用PCを接続するためのRS-232C準拠のケーブル
⑤リセットスイッチ	MFDのコントローラボードのCPUを手動でリセットする為の押しボタンスイッチ
⑥変換コネクタ	2.5inchのIDEインタフェースを3.5inchのIDEインタフェースへ変換するコネクタ

⑦～⑩PC	MSD内容を確認するためのツールを動作させるPC
テストツール	
⑪シリアル通信ソフトウェア	MFDとシリアル通信を介して操作するためのターミナルエミュレータソフトウェア(TeraTerm Pro 2.3 19J)
⑫TIFFファイル表示ソフトウェア	MFDで作成される圧縮画像をPC上で表示するための画像表示ソフトウェア(IFAX VIEW version 3.0)
⑬decode.exe	MFDで暗号化し作成されたデータファイルを任意の鍵で復号するための開発者作成ソフトウェア
⑭FTPサーバソフトウェア	MFDで作成されたデータをファイルとしてFTP転送するためのサーバソフトウェア（WAR-FTPD version 1.65)
⑮ファイルダンプソフトウェア	PC上のファイルを16進数でダンプするバイナリエディタ(Stirling version 1.31)
⑯ハードディスクダンプソフトウェア	ハードディスク内の任意の指定のセクタを読み込んでその内容を表示、編集できるソフトウェア(DiskDump version 1.20)

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。

1. テスト構成

開発者が実施したテストの構成は図 3及び表 4に示す。TOEはAR-FR4 version.M20のデバッグ用ROMを用いた。これはテスト結果をPCにて確認するためのインタフェースを持ち、テストを容易かつ確実にするためのものであり、このインタフェースを除き製品ROMと同等である。よって本構成は本STの記述と一致している。

2. テスト手法

開発者は各セキュリティ機能（データ消去機能、暗号操作機能、暗号鍵生成機能、認証機能、セキュリティ管理機能）を操作パネルあるいはジョブや電源ONにより完了あるいはそれらの中断により未完了の状態とし、その結果をTOEあるいはMFDから直接データを読み出し、その内容をデバッグ用のPCで確認する方法で実施された。

MSDの内容は接続されたシリアルケーブル接続のターミナルからMFDのデバッグコマンドを操作することにより、LANケーブルを経由しPCへ転送される。またHDDを直接MFDから外しデバッグ用PCにIDEにて接続し内容を確認する方法もとられた。これらのデータはPC上で画像ツール、ダンプ

ツールにより確認される。暗号化データはテスト用暗号鍵を使用し、暗号化に使用した暗号鍵を用いてPC側で復号し確認を行った。

3. 実施テストの範囲

TOEセキュリティ機能のうち暗号鍵破壊を除くすべての機能(データ消去、暗号操作、暗号鍵生成、認証、セキュリティ管理)が対象となるように実施された。また、機能仕様に識別されているインタフェースはすべてテストされ、また各機能と外部インタフェースの対応も確認されている。

テストの総項目数は28項目であり、HDD/RAMおよびFlashメモリに対し、それぞれ暗号化、復号およびデータ消去という一連の手順が含まれており、開発者テスト数としては妥当と判断した。

なお、暗号鍵破壊については、同機能が揮発性RAMの電源遮断時に保持している内容が失われるという特性によるものであるため、TOEのセキュリティ機能としてのテストを除外した。

4. 結果

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機能テスト仕様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システム構成を図 4に示す。また、テストシステムの各機器の構成を表 5に示す。

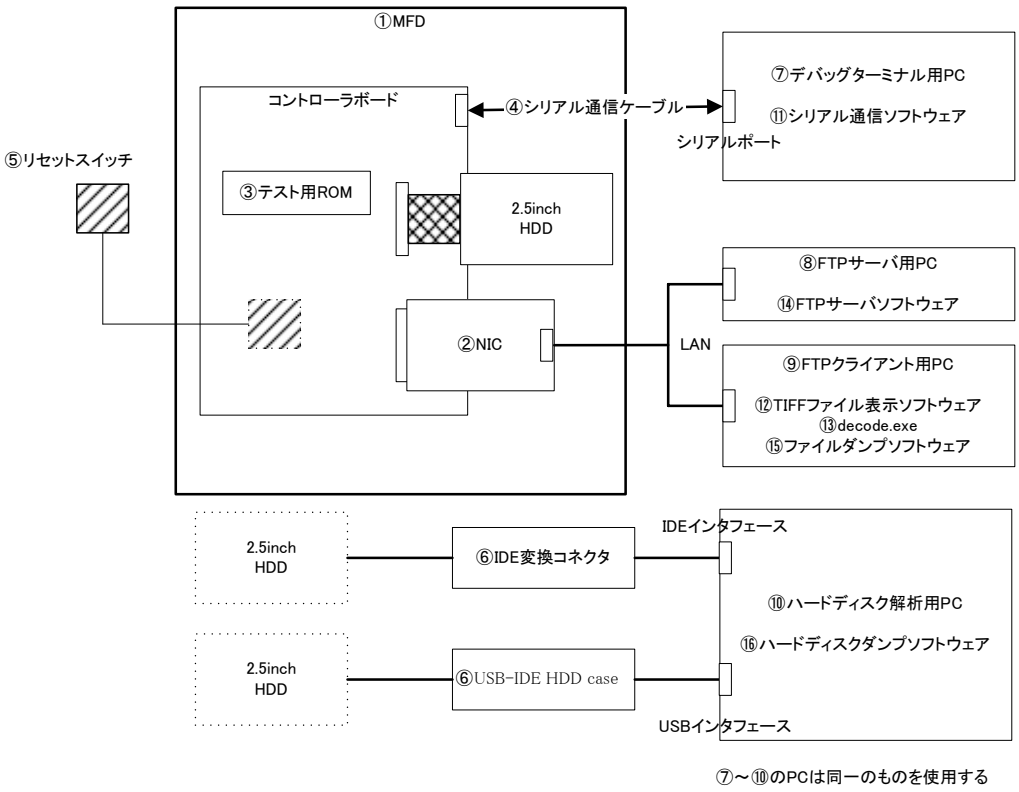

図 4 評価者テストシステム構成図

表 5 評価者テスト使用機器・ツール

名称	概要（種別）
テスト機器	
①MFD	TOEを搭載するMFD （AR-310M）
②NIC	MFDをLANに接続するための基板
③テスト用ROM	TOE (AR-FR4 version.M20)
④シリアル通信ケーブル	MFDとデバッグターミナル用PCを接続するためのRS-232C準拠のケーブル
⑤リセットスイッチ	MFDのコントローラボードのCPUを手動でリセットする為の押しボタンスイッチ
⑥変換コネクタ	2.5inchのIDEインタフェースを3.5inchのIDEインタフェース・USBインタフェースへ変換するコネクタ

⑦～⑩PC	MSD内容を確認するためのツールを動作させるPC
テストツール	
⑪シリアル通信ソフトウェア	MFDとシリアル通信を介して操作するためのターミナルエミュレータソフトウェア(TeraTerm Pro version 2.3 1.9J)
⑫TIFFファイル表示ソフトウェア	MFDで作成される圧縮画像をPC上で表示するための画像表示ソフトウェア(IFAX VIEWER version 3.0)
⑬decode.exe	MFDで暗号化し作成されたデータファイルを任意の鍵で復号するための開発者作成ソフトウェア
⑭FTPサーバソフトウェア	MFDで作成されたデータをファイルとしてFTP転送するためのサーバソフトウェア(WAR-FTPD version 1.65)
⑮ファイルダンプソフトウェア	PC上のファイルを16進数でダンプするバイナリエディタ(Stirling version 1.31)
⑯ハードディスクダンプソフトウェア	ハードディスク内の任意の指定のセクタを読み込んでその内容を表示、編集できるソフトウェア(DiskDump version 1.20)

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。

1. テスト構成

評価者が実施したテストの構成は図 4及び表 5に示す。本構成は本STの記述と一致しており、開発者のテスト環境とも一致する。なお、テスト効率を上げるため、USBインタフェースを使用した。

2. テスト手法

評価者は、開発者が行ったテスト手法が、セキュリティ機能の期待されたふるまいを検証するのに適していると判断し、開発者のテスト手法を踏襲した。

評価者は各セキュリティ機能を操作パネルあるいはジョブや電源ONにより完了あるいはそれらの中断により未完了の状態とし、その結果をTOEあるいはMFDから直接データを読み出し、その内容をデバッグ用のPCで確認する方法で実施された。

MSDの内容は接続されたシリアルケーブル接続のターミナルからMFDのデバッグコマンドを操作することにより、LANケーブルを経由しPCへ転送される。またHDDを直接MFDから外しデバッグ用PCにIDEあるいはテストの効率化のためにUSBにて接続し内容を確認する方法もとられた。これらの

データはPC上で画像ツール、ダンプツールにより確認された。暗号化データはテスト用暗号鍵を使用し、暗号化に使用した暗号鍵を用いてPC側で復号し確認を行った（図 4参照)。

3. 実施テストの範囲

評価者テストは、暗号鍵破壊を除くすべてのセキュリティ機能に対し通常動作と操作取り消しを含む代表的なテストパターンが実施された。テスト項目数は15項目であり、MSDのデータ消去に関してはデータ暗号化、復号、消去の一連の手順が含まれている。

また、開発者テスト項目から暗号鍵破壊を除くすべてのセキュリティ機能とすべての対象スプール（HDD、RAMディスク、Flashメモリ）を網羅する方針により6項目を抽出し実施した。

4. 結果

評価者テストを実施し、その実施結果において評価者テストでは期待される結果となり、開発者テストのサンプリングテストでは機能テスト仕様書に示されたものと一致することを確認した。

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 該所見報告書でなされた指摘事項が妥当であること。

② 当該所見報告書でなされた指摘事項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理にかなっていること。

⑤ 本評価報告書に示された評価者の評価手法がCEMに適していること。

これらの認証において発見された問題事項はない。

認証機関は、本ST及び本評価報告書において、所見報告書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（[7][10][13][16]のいずれか）に規定されたEAL4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アクションエレメントについての調査結果を表 6にまとめる。

表 6 評価者アクションエレメント調査結果

評価者アクションエレメント	調査結果
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記述が理路整然と一貫性のあ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、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明記され、それらが脅威、組織のセキュリティ、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、完結しており、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理路整然とし、完結しており、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。
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結しており、理路整然とし、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_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	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.2.1E	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.2.1E	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.2.2D	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.2.1E	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.2.2E	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_IMP.1.1E	評価はワークユニットに沿って行われ、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが内部的に一貫していることを確認している。
ADV_IMP.1.2E	評価はワークユニットに沿って行われ、実装表現のサブセットがその関連するTOEセキュリティ機能要件を正しく具体化したものであることを確認している。

ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。
ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計が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り、下位レベル設計が上位レベル設計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。
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。
ALC_LCD.1.1E	評価はワークユニットに沿って行なわれ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義していることを確認している。
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が含まれて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.2.1E	評価はワークユニットに沿って行われ、管理者ガイダンス及びインストールガイドが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.2.2E	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.2.3E	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が記述されていることを確認している。
AVA_MSU.2.4E	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の全ての操作モードにおいてのセキュアな操作を提供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主張が正しことを確認している。
AVA_VLA.2.1E	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.2.2E	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。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく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の概要について報告がなされている。

AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

4.2 注意事項

本TOEの守るべき資産はMFDから取り出されたMSDのデータであり、対抗する脅威はそのMSDからの残存データの再生である。よってTOEの運用中において正当な手段を擬して再生を試みる脅威（たとえばジョブリテンション機能によりホールドされたスプールデータを、不正に入手したパスコードにより印刷等を行う）には対抗しないことに留意し、TOE使用にあたって、使用者はガイダンスにより想定される使用環境を理解しTOEを管理しなければならない。

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
DSK	Data Security Kit
EAL	Evaluation Assurance Level
MFD	Multi-Function Device
MFP	Multi-Function Printer
MSD	Mass Storage Device
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

6 参照

[1] デジタル複合機 データセキュリティキット AR-FR4/AR-FR5 セキュリティターゲット Version 0.04 2004年7月30日 シャープ株式会社

[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-0210

[21] 補足-0210

[22] デジタル複合機 データセキュリティキットAR-FR4/AR-FR5 評価報告書 2004年8月3日　03002795-01-R002-02 株式会社富士総合研究所 情報セキュリティ評価センター

[23] JISEC ホームページ 認証製品リスト (http://www.ipa.go.jp/security/jisec/cert-list.html)