認　証　報　告　書

評価対象

申請受付年月日(受付番号)	平成16年1月5日(IT認証4019):当初の申請を取り下げし、CCRA認証マーク対応のため、再申請があった申請受付日 平成15年9月18日(IT認証3012):当初の申請受付日
認証申請者	シャープ株式会社
TOEの名称	デジタル複合機データセキュリティキットAR-FR10 Version S.10
ＰＰ適合	なし
適合する保証要件	EAL3+ADV_SPM.1
TOE開発者	シャープ株式会社ドキュメントシステム事業本部 ドキュメントシステム事業部
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16年3月15日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
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.
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
⑥ 認証機関が公開する③および⑤の翻訳文書
⑦ 補足文書（補足-0210, CCIMB Interpretations-0210）

評価結果：合格

デジタル複合機データセキュリティキットAR-FR10 Version S.10は、独立行政法人製品評価技術基盤機構が定める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、「デジタル複合機データセキュリティキットAR-FR10 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「取扱説明書 データセキュリティキット AR-FR10」および「AR-FR10 設置手順書」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、動作条件および機能仕様は本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:　デジタル複合機データセキュリティキットAR-FR10
- バージョン:Version S.10

開発者: シャープ株式会社ドキュメントシステム事業本部ドキュメントシステム事業部

1.2.2 製品概要

本製品は、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は、コピー機能、ファクス機能で構成され販売される事務機器である。本製品は、このMFD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。

1.2.3 TOEの範囲と動作概要

本TOEの物理的範囲を図 1に示す。図１はMFDに搭載したTOEであるAR-FR10

の設置位置を網掛けで示している。TOEは、MFDのコントローラ基板上で動作し、セキュリティ機能を追加するファームウェアであり、物理的に２枚のROM基板として構成される。各ROM基板は、ROMチップ等を実装した約25mm×60mmのプリント基板であり、一辺にエッジコネクタを有し、エッジコネクタを介してMFD内のコントローラ基板に装着する。

また、TOEが動作するMFDは、シャープ　デジタル複合機AR-555S、AR-625S、及びAR-705Sである。

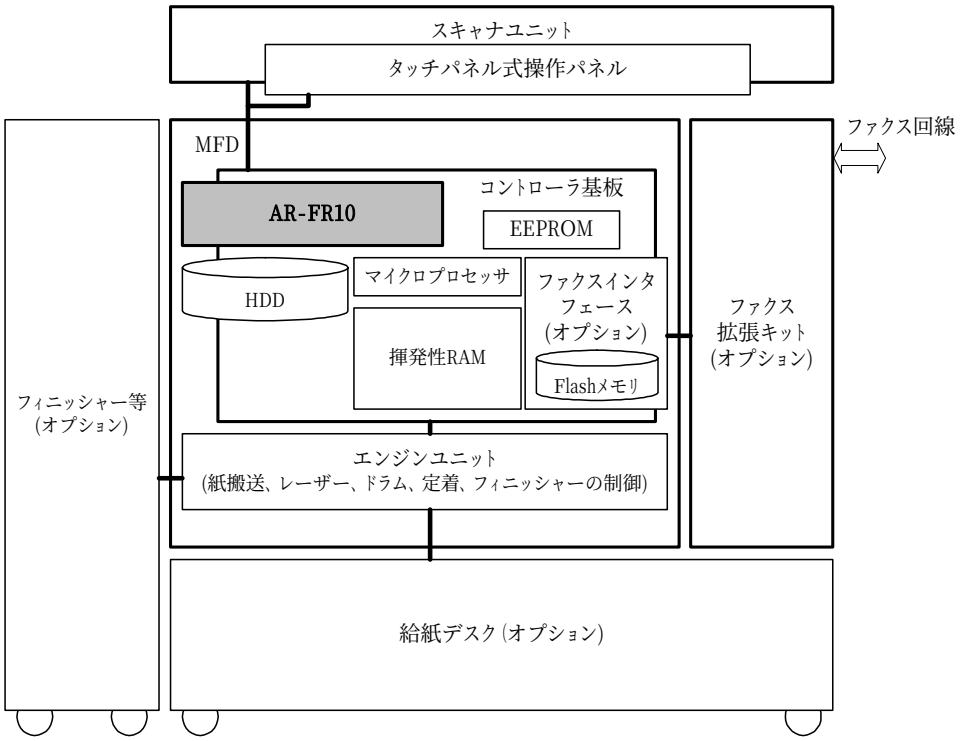

図 1　MFDの物理構成とTOEの物理的範囲

本TOEの論理的範囲を図 2に示す。図中、TOEを網掛けで示し、長方形はソフトウェアの機能、角を丸くした長方形をハードウェアとして示す。Flashメモリは、ファクスインタフェース基板上に搭載されていることを示したものである。

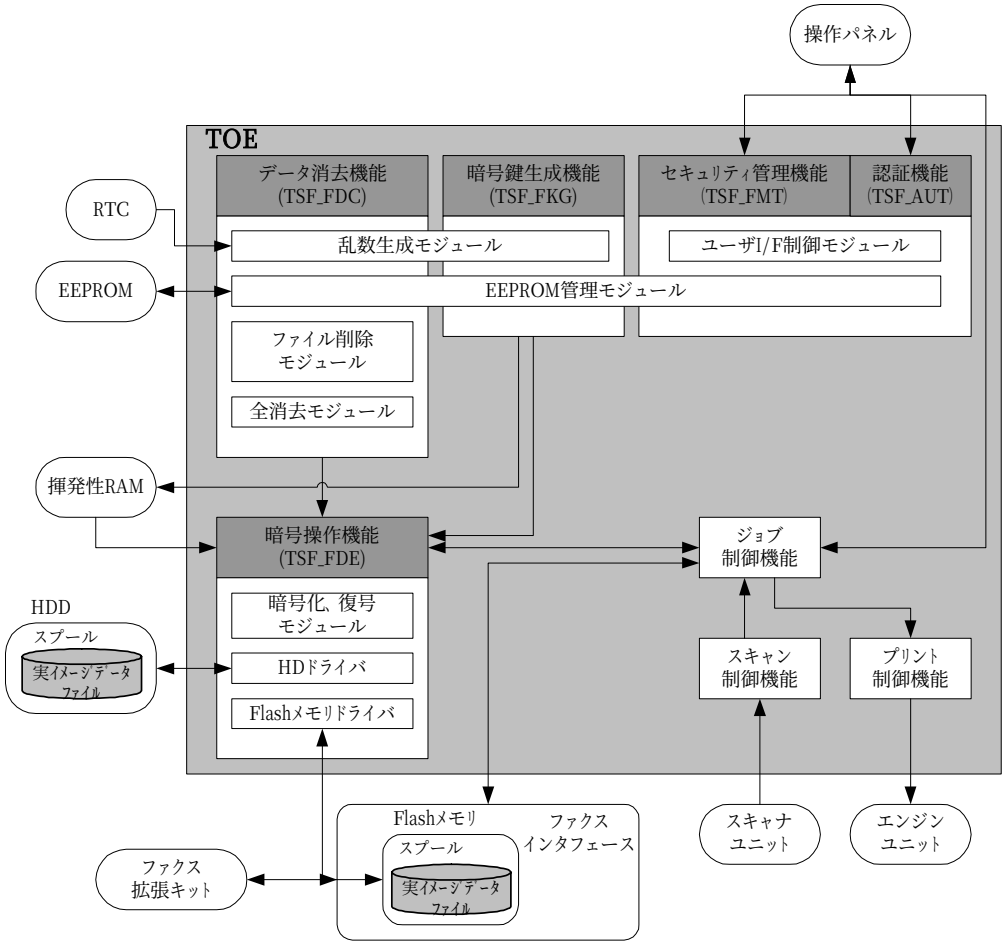

図 2　TOEの論理的範囲

TOEは、MFDにセキュリティ機能を追加するファームウェア 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のコントローラ基板の制御を行う。以下の機能がTOEの論理的範囲に含まれる。

a) 暗号操作機能

スプール保存する実イメージデータを暗号化し、MSD（Mass Storage Deviceの略。本書ではHDDもしくはFlashメモリを意味する。）に保存する。また、MSDにスプール保存されている実イメージデータを復号する。

b) 暗号鍵生成機能

暗号操作機能で使用する暗号鍵を生成する。生成した暗号鍵は、揮発性RAMに保存する。

c) データ消去機能

コピージョブによりHDD内に、もしくはファクス送受信ジョブによりFlashメモリ内にスプール保存された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、実イメージデータ領域を消去

する。また、ジョブが正常に完了しなかった場合、消去されなかった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上書き消去を行う。以下の３つのデータ消去機能を提供する。

① 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HDDあるいはFlashメモリの実イメージデータ領域の消去。

② 電源ON時の自動消去
　ジョブが正常に完了せずに消去されなかったHDDの実イメージデータ領域を含むスプール領域全体に対する消去。

③ キーオペレータの操作による全データエリア消去
　ジョブが正常に完了せず、あるいはジョブの未完了により消去されなかったHDDあるいはFlashメモリの実イメージデータを含むスプール領域全体に対する消去。これはMFDの所有者変更、もしくはMFD廃棄等における実イメージデータからの情報漏洩を防止するための機能である。

d) 認証機能
　キーオペレータコード（パスワード）によりキーオペレータの認証を行う。

e) セキュリティ管理機能
セキュリティ管理のために、以下の設定を可能にする。

① 「電源ON時の自動消去」の実行もしくは不実行の設定

② 「各ジョブ完了後の自動消去」時のHDDへの上書きデータ消去回数の設定

③ 「キーオペレータの操作による全データエリア消去」時のHDD全データエリア消去回数の設定

④ 「電源ON時の自動消去」時のHDDへの上書き消去回数の設定

⑤ キーオペレータコードの変更

f) スキャン制御機能
　コピージョブ、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。スキャンされたイメージデータは揮発性RAMに格納される。

g) プリント制御機能
　コピージョブ、ファクス受信ジョブにおいて、揮発性RAMに格納されている実イメージデータを、印刷のためにエンジンユニットに転送する。

h) ジョブ制御機能

ジョブには、コピージョブ、ファクス送信ジョブ、ファクス受信ジョブがあり、それぞれ以下のような機能を提供する。

① コピージョブ
MFDのコピー動作を制御する。

② ファクス送信ジョブ
MFDのファクス送信動作を制御する。

③ ファクス受信ジョブ
MFDのファクス受信動作を制御する。

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 (平成15年)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「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14年4月)」[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、本TOEのセキュリティ設計である「デジタル複合機データセキュリティキット AR-FR10 セキュリティターゲット Version 0.21」(以下「本ST」という。) 6、本TOE開発に関連する評価用提供物件及び本TOEの開発環境・製造・出荷の現場を調査し、本TOEとその開発環境等が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）の機能要件及び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することである。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-FR10 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および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、評価機関である社団法人　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16年3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が判明した。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、一般のオフィスで利用される。攻撃者は公開情報を利用した低レベルの攻撃能力を有することを想定している。攻撃者はTOEへの直接的な攻撃によりTOEのセキュリティ機能を阻害することはできず、保護資産はかならず暗号化される。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。

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) 暗号鍵生成機能

TOEは、イメージデータを暗号化するための暗号鍵（共通鍵）の生成を行う。MFDの電源がオンになると２つの暗号鍵（共通鍵）が生成される。一つは、循環付き遅延フィボナッチ乱数拡張アルゴリズムを用いて、MFD内のHDDに

スプール保存される実イメージデータの暗号化、および読出される実イメージデータの復号に用いる暗号鍵である。もう一つは、MSN拡張アルゴリズムを用いて、MFD内のFlashメモリにスプール保存される実イメージデータの暗号化、および読出される実イメージデータの復号に用いる暗号鍵である。鍵は、いずれも128ビット長である。これらの暗号鍵は揮発性RAM内に保存する。

(2) 暗号操作機能

通常の動作の間、ジョブ処理の途上において、MFDはジョブのデータである実イメージデータをMSDにスプール保存する。ファクス回線からの送受信における実イメージデータはFlashメモリ領域に、コピーの対象となる実イメージデータはHDD領域にそれぞれ保存する。スプール保存するにあたり、揮発性RAM内に保存している暗号鍵を用いAES Rijndaelアルゴリズムによって暗号化の後、MSDにスプール保存する。また、スプール保存された実イメージデータを実際に処理（利用）する際には、ジョブ処理の過程で必要となるデータ断片（処理中ジョブ1件の実イメージデータの一部）を必要の都度、MSDから読み出し、暗号鍵により復号する。

(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を消去する機能を有する。本機能は、以下の３プログラムで構成される。

① 各ジョブ完了後の自動消去

コピージョブ完了後、コピージョブが利用した実イメージデータファイルが存在していたHDD上の領域に、ランダム値をセキュリティ管理機能により設定されている回数繰り返して上書き消去し、ファクスの送受信ジョブ完了後、ファクスの送受信ジョブが利用した実イメージデータファイルが存在していたFlashメモリ上の領域に、Flashメモリの各ビットに固定値”0”を上書き消去する機能。

② 電源ON時の自動消去

電源ON時の自動消去がセキュリティ管理機能により実行状態に設定されている場合において、MFDの電源がONになった際、ジョブが正常に完了せず消去されなかった実イメージデータを含むHDD上のスプール領域全体に、ランダム値をセキュリティ管理機能により設定されている回数繰り返して上書き消去する機能。

③ キーオペレータの操作による全データエリア消去

キーオペレータ認証後、キーオペレータの操作により、スプール保存のために利用されるHDD上の全てのスプール領域に、ランダム値をセキュリティ管理機能により設定されている回数繰り返して上書き消去する機能。また、スプール保存のために利用されるFlashメモ

リ上の全スプール領域について、Flashメモリの全ビットをデバイスのブロック消去機能により固定値”1”で埋める機能。単に、全データエリア消去とも呼ぶ。

電源ON時の自動消去、及びキーオペレータの操作による全データエリア消去を中断させる場合、キーオペレータコードの入力を要求し、認証された場合についてのみ上書き消去を中断する。

(4) 認証機能

TOEは、キーオペレータに対し、キーオペレータプログラムへのアクセスのために５桁の暗証番号、即ち、キーオペレータコードの入力を要求する。キーオペレータコードを正しく入力する手順によって、キーオペレータとして認証される。キーオペレータ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。

データ消去機能のうち、キーオペレータの操作による全データエリア消去の起動と中断、電源ON時の自動消去の中断、及びセキュリティ管理は、キーオペレータとして認証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

TOEは、キーオペレータコードの入力により、キーオペレータが認証される手順を経た後に、以下のセキュリティ機能に関わる設定を提供する。各設定値はMFD内のEEPROM内に保存される。

① 「電源ON時の自動消去」実行、もしくは不実行の設定
出荷時設定では、電源ON時の自動消去は実行と設定されている。設定値の問合せ、及び変更ができる。

② 「各ジョブ完了時の自動消去」におけるHDD上の実イメージデータファイルに対する上書きの回数
消去回数は、１回から７回までの間で設定でき、設定値の問合せ及び変更ができる。

③ 「キーオペレータの操作による全データエリア消去」におけるHDD上の全ての実イメージデータファイルに対する上書きの回数
消去回数は、１回から７回までの間で設定でき、設定値の問合せ、及び変更ができる。

④ 「電源ON時の自動消去」におけるHDD上の実イメージデータファイルに対する上書きの回数
消去回数は、１回から７回までの間で設定でき、設定値の問合せ、及び変更ができる。

⑤ キーオペレータコードの変更

キーオペレータコードは十進数字5桁であり、TOEは桁数が5桁であることを検査する。キーオペレータコードの設定値の問合せ、及び変更ができる。

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

項番	脅威
1	攻撃者が、MFD内のMSDに、MFD以外の装置を使用することによりMSD内の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に装着するプリント基板製品という形態をとる。本TOEが動作する対象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

TOE	対象MFDモデル
AF-FR10 VERSION S.10	AR-555S、AR-625S、AR-705S

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

項番	前提条件
1	キーオペレータは、TOEに対して不正な行為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。

■取扱説明書　データセキュリティキット AR-FR10

バージョン　：CINSJ2569FC51

対象者　　：キーオペレータ

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

■AR-FR10 設置手順書

バージョン　：TCADZ1614FCZZ

対象者　　：キーオペレータ、サービスマン

内容　　：本TOEの設置に伴い、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

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15年10月に始まり、平成16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15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実施した。また、開発者のテスト環境にて、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記録され、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、評価に反映された。

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。

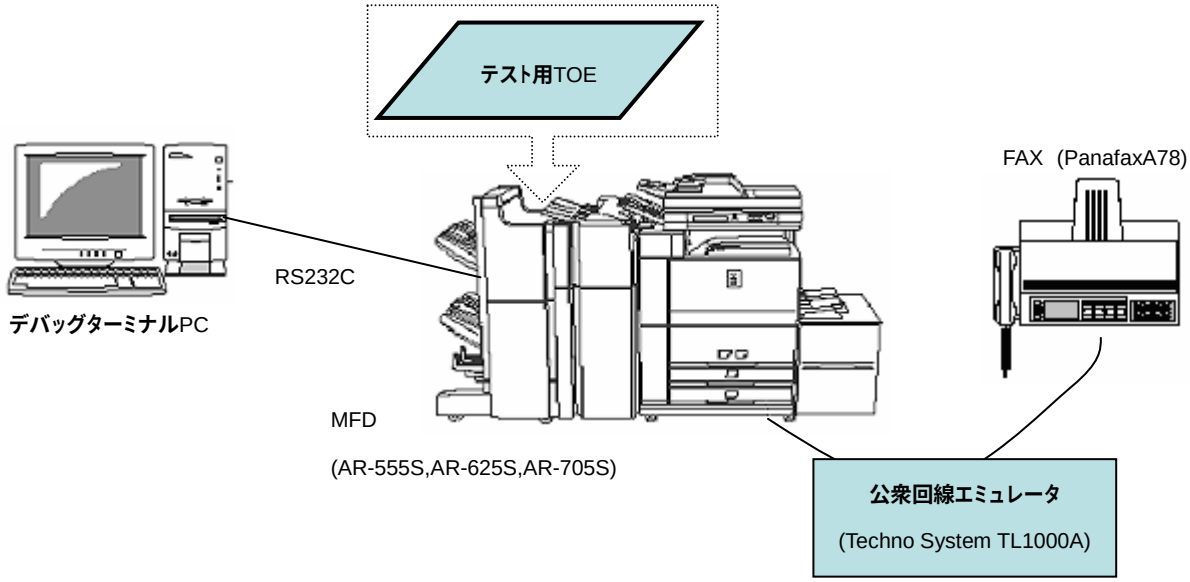

図 3 開発者テストシステム構成図

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	
MFD	TOEを搭載するMFD (AR-625S,AR-555S,AR-705S)
テスト用TOE	デバッグ用にコンパイルされたTOE (AR-FR10 VERSION S.10)
公衆回線エミュレータ	公衆回線の擬似交換機(Techno System TL1000A)
ファクス	TOEファクス機能テスト用ファックス(Panafax A78)
デバッグターミナルPC	MSD内容を確認するためのテストツールを動作させるPC(PC/AT)
テストツール	

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(秀 Term)
暗号データ復号ツール	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(Decode.exe)
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)
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)

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 3及び表 4に示す。TOEはAR-FR10 version S.10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。

また、TOEが対象とするMFD３機種(AR-555S、AR-625S、AR-705S)は印刷スピード以外のメカニズムは同様のため、特にAR-625Sを用いテストを実施し、AR-555SおよびAR-705Sはいくつかのテストをサンプリングして実施した。

b.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した。

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、PCへ転送される。これらのデータはPC上でダンプツールにより確認される。また、ファックスに出力することで画像データを確認する。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。

c.実施テストの範囲

すべてのTOEセキュリティ機能(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、機能仕様に記載されているインタフェースはすべてテストされ、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12（総テスト数48）であり、HDD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。

d.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システム構成及びテストシステムの各機器の構成は開発者テストと同等である。

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構成は図 3及び表 4に示す開発者テスト環境と同等のものを使用した。本構成は本STの記述と一致する。

b.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採用した。

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で確認した。

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、PCへ転送される。これらのデータはPC上でダンプツールにより確認した。また、ファックスに出力することで画像データを確認した。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。

d.実施テストの範囲

評価者テストは、すべてのセキュリティ機能を網羅し、かつ認証機能とセキュリティ管理機能に着目し8項目（16テスト）を開発者テストから抽出した。また異常系13項目（13テスト）をこれに追加し、総計29のテストを実施した。これは開発者テストに対する網羅度、サンプル数として十分である。

e.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。

2.4 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

認証は、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

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調査した結果、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EAL3及び保証コンポーネントADV_SPM.1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アクションエレメントについての確認結果を表 5にまとめる。

表 5 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	確認結果
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。また、当評価に至るまでになされた指摘(所見報告書)も適切と判断される。

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。また、当評価に至るまでになされた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。当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでになされた指摘)も適切と判断される。
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。また、当評価に至るまでになされた指摘も適切と判断される。
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。また、当評価に至るまでなされた指摘も適切と判断される。
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。また、当評価に至るまでなされた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。また、当評価に至るまでなされた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、完結しており、かつ一貫していることを確認している。当評価に至るまでになされた指摘も適切と判断される。
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、当評価に至るまでなされた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。また、当評価に至るまでなされた指摘も適切と判断される。
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、当評価に至るまでなされた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、CMシステムにCCで必要とされるものが、構成要素リストに記述されて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。また、当評価に至るまでなされた指摘も適切と判断される。
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、当評価に至るまでなされた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。
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。また、当評価に至るまでなされた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、当評価に至るまでなされた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。また、当評価に至るまでなされた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。当評価に至るまでなされた指摘も適切と判断される。
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。また、当評価に至るまでなされた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、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に関して、利用者に関連する事項は存在しない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、当評価に至るまでなされた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.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。また、当評価に至るまでなされた指摘も適切と判断される。
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が記述され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.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。

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
MFD	Multi-Function Device
MSD	Mass Storage Device
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。

イメージデータ	MFDにてコピー、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。ファクス受信においては、電話回線を通じて受信したデータ、及びこのデータを伸張したデータ。また、これらを圧縮したデータもイメージデータと呼ぶ。
エンジンユニット	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。
キーオペレータ	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。
キーオペレータコード	キーオペレータの認証の際に用いられるパスワード。
キーオペレータプログラム	TOEのセキュリティ管理機能。MFD管理機能でもある。キーオペレータプログラムにアクセスす

	るためには、キーオペレータとして識別認証されなければならない。
サービスマン	TOE設置時に販売会社から派遣されるTOE保守管理者。
ジョブ	MFD機能（コピー、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。
実イメージデータ	MFDで作成され、スプール領域に展開されたイメージデータ。

6 参照

[1] デジタル複合機データセキュリティキット AR-FR10 セキュリティターゲット Version 0.21 2004年2月21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15年 独立行政法人 製品評価技術基盤機構 適合性評価センター ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02

[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14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02

[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-FR10 評価報告書 第1.4版 2004年2月27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