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16年9月29日（IT認証4035）**
認証番号	C0035
認証申請者	**京セラミタ株式会社**
TOEの名称	Data Security Kit (B) Software
TOEのバージョン	V1.10E
PP適合	**なし**
適合する保証要件	EAL3
TOE開発者	**京セラミタ株式会社**
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11月2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-0210

評価結果：合格

「Data Security Kit (B) Software V1.10E」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、「Data Security Kit (B) Software V1.10E」（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。

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 (B) Software
バージョン:　V1.10E
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-8030/KM-6030/CS-8030/CS-6030」にセキュリティ機能を提供するソフトウェアモジュール製品である。本TOEは、オフィスや学校で利用される複合機に搭載され、HDD上書き消去機能を提供することにより、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）の各処理後にHDD上に残存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

(1) TOEの利用環境

TOEを搭載する複合機は、様々な文書を扱うオフィスや学校で使用され、内部ネットワーク(LAN)に接続される。また、プリンタ出力用にローカルポート（パラレルポート、USBポート、シリアルポート）に接続されて使用することも可能である。図1-1に

複合機の利用環境を示す。

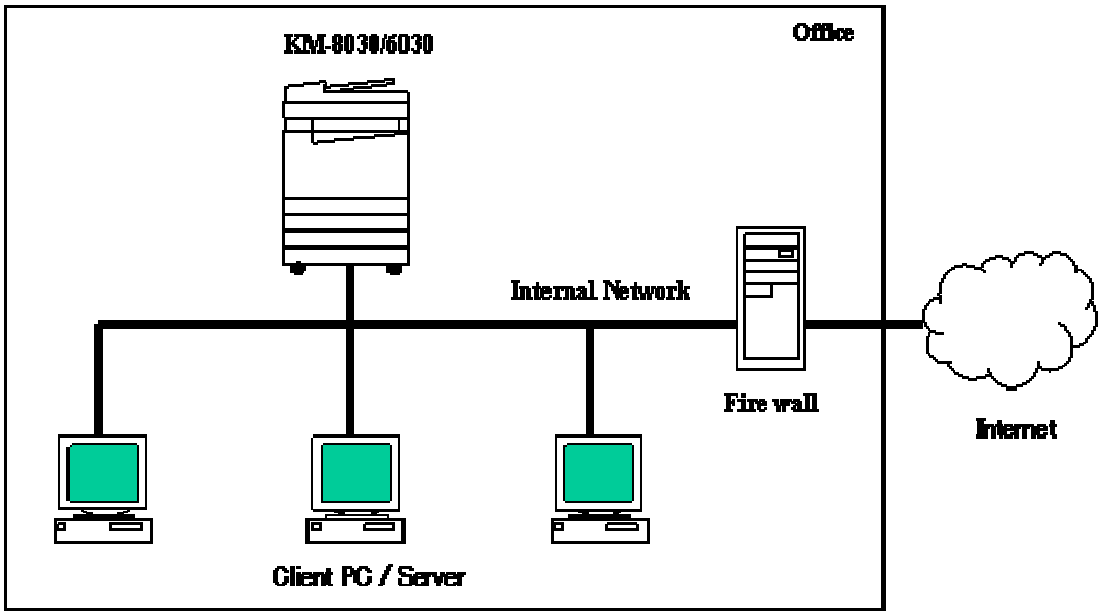

図1-1 複合機の利用環境

(2)TOE範囲と動作概要

TOEのハードウェア構成を図1-2 に示す。TOEはメインボードとプリンタボード上にある、MAIN ROMとPRINTER ROMのソフトウェアを指す。

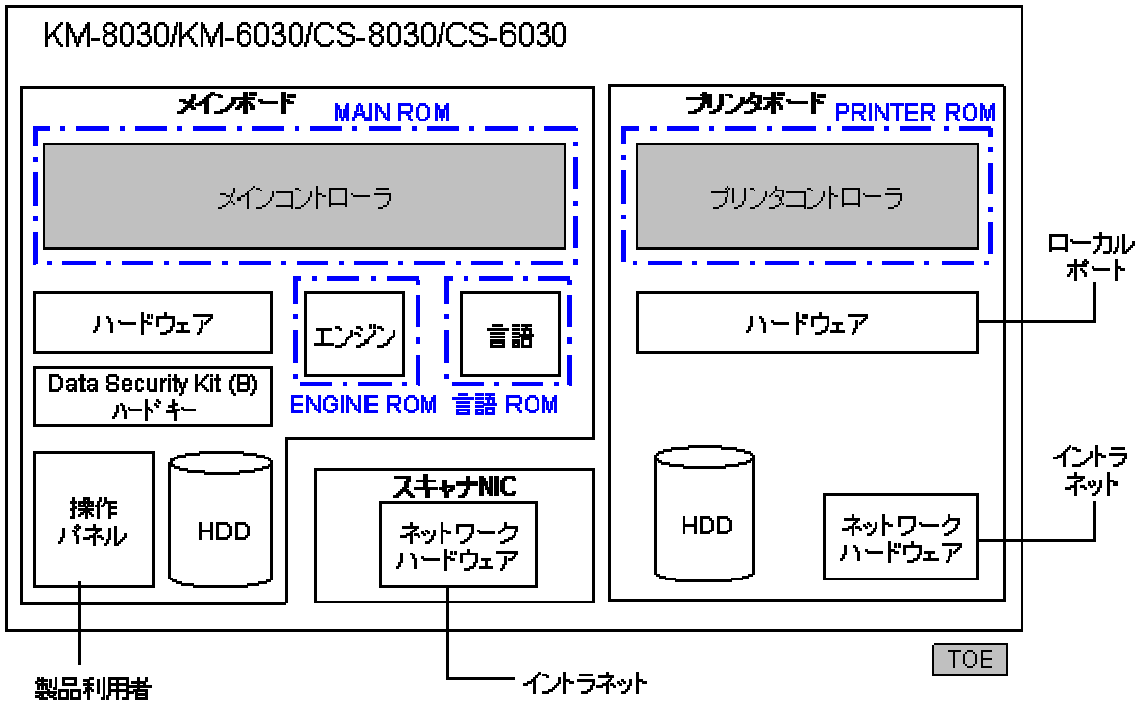

図1-2 TOE のハードウェア構成

TOEに含まれるソフトウェアモジュールの構成を表1-1に示す。

表1-1 TOEを構成するソフトウェアモジュール

ROM名称	種別		備考
MAIN ROM	メインコントローラ		―
		コピーモジュール	―
		スキャナモジュール	―
		ネットワークモジュール	―
		コピー/ネットワークスキャナ共通のライブラリ	HDD上書き消去機能、管理者認証機能が含まれる
PRINTER ROM	プリンタコントローラ		―
		プリンタモジュール	―
		ネットワークモジュール	―
		プリンタ用ライブラリ	HDD上書き消去機能が含まれる
		ネットワークサービス	―

TOEの論理的構成を図1-3 に示す。TOEは、セキュリティ機能と共に、コピー機能のような通常の複合機としても動作する。 以下の機能がTOEの論理的構成に含まれる。

- HDD 上書き消去機能　（セキュリティ機能）
  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、HDD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、プリンタ機能を使用し、HDDに保存された画像データを削除する際、画像データの論理的な削除後に、実データ領域に対して、無意味な文字列を上書きすることにより、実データ領域を完全に消去する。
  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。
- 管理者認証機能　（セキュリティ機能）
  TOEマシン管理者を操作パネルからのTOE管理者暗証番号により識別認証する。識別認証されたTOEマシン管理者は、HDDの全領域を上書き消去する「HDDフォーマット機能」の実行や、HDD上書き消去機能において３回上書き方式と１回上書き方式を変更することが出来る。ここで、３回上書き方式が初期値であり、処理効率よりも安全性を重視する場合に設定する。１回上書き方式は処理効率を重視する場合に設定する。また、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。
- コピー機能
  TOE利用者により、スキャナから読み込んだ原稿のコピーを行う。（通常コピー）

通常コピーを行う際には、メインボード上のHDDに画像データをスプール保存し、出力が完了した後、削除されることになる。また、コピー機能は文書管理機能も有する。文書管理機能には、蓄積共有ボックスとジョブ結合ボックス、フォーム用ボックスが存在する。各ボックスは全てメインボード上のHDDに存在する。 処理終了後、画像データは削除される

- ネットワークスキャナ機能
  TOE利用者により、スキャナから読み込んだ原稿の画像データをクライアントPCに送信することが出来る。LAN経由で送信するPC送信と、E-mail経由で送信するE-mail送信がある。また、TWAIN対応のアプリケーションを利用することにより、複合機にセットされた原稿をクライアントPCからの操作でクライアントPCに取り込むことも出来る。ネットワークスキャナ機能を使用する際には、メインボード上のHDDに画像データをスプール保存し、送信が完了した後、削除されることになる。
- プリンタ機能
  TOE利用者により、プリンタドライバから送信された画像データを紙に出力する（通常プリント）。LAN経由による出力と、ローカルポートによる出力がある。また、プリンタ機能は、単に出力する他に、拡張機能も有する。通常プリントを使用する際には、一旦メインボード上のHDDに画像データをスプール保存し、出力が完了した後、削除されることになる。拡張機能を使う場合には、画像データをプリンタボード上のHDD、またはメインボード上のHDDに保存し、処理終了後、画像データは削除される。
- ジョブ管理機能
  コピー機能、プリンタ機能に含まれる機能である。それぞれの機能により、HDDに保存されたジョブ/印刷ジョブを管理する。ジョブ/印刷ジョブの、編集/出力/削除を行うことが出来る。操作パネルからと、クライアントPC上のユーティリティから操作することが出来る。

TOEを動作させるには、図1-2に示されるData Security Kit (B) ハードキーが必要となる。仮に運用中にData Security Kit (B)ハードキーが取り外された場合、セキュリティ機能が無効になるのでは無く、複合機が何も動作しなくなる。

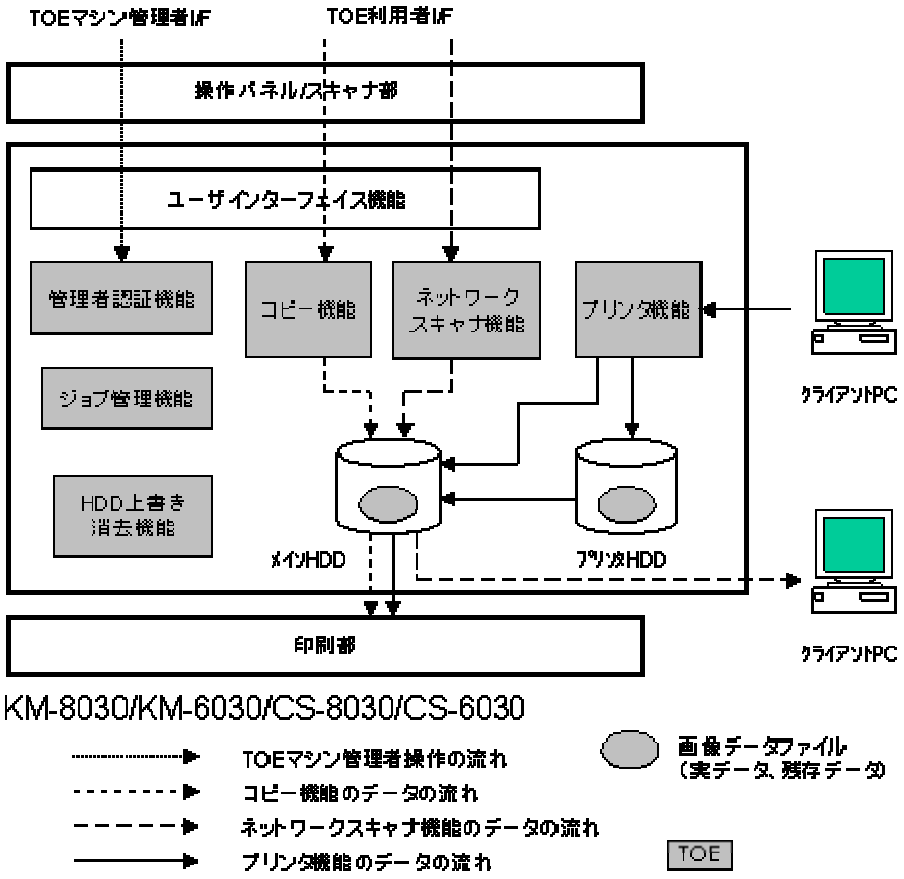

図1-3　TOEの論理的構成

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「京セラミタ Data Security Kit(B) 海外版 セキュリティターゲット 第0.15版」（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、「京セラミタ　Data Security Kit(B) Software （海外版）評価報告書　第2.3版」（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。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10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、オフィスや学校において複合機に搭載されて利用され、LANやローカルポートに接続されることも想定しているが、LAN/ローカルポートを通したネットワークから、複合機内部の残存データを読み出すことはできない。また、複合機は入退室管理された場所に設置されるため、TOEの運用環境に中レベル以上の攻撃力を持つ攻撃者を含む不特定多数の攻撃者は存在しない。このため、攻撃力は“低レベル”であり、これに対応できる最小機能強度レベルは、“SOF-基本”が適切と判断された。

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。

- **HDD上書き消去機能　SPF.AGAIN**

HDD上書き消去機能は、HDD上に保存されたデータを、論理的に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機能である。
上書き消去の方式は以下の２通りであり、TOEマシン管理者のみ変更が可能である。

- ３回上書き方式
  上書き消去する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
  上書き消去するデータの実データ領域全体にNULL（0x00）を書き込む

また、HDD上書き消去機能は、メインボードとプリンタボードのぞれぞれのHDDに対して独自に実行される。但し、上書き消去方式の設定値と、下記HDDフォーマット機能の実行に対しては、メインボード/プリンタボードの区別なく、統一して行う。

また、HDD上書き消去機能は、下記のいずれかのタイミングで実行出来る。

・出力又は 電源OFF 又は 削除操作により、ジョブが削除された時
・TOEマシン管理者により、HDDフォーマット機能が実行された時
※ 電源OFFによる上書き消去は、実際には次回電源ON時に消去処理が実行される。このHDD上書き消去機能は、上記のタイミングにおいて必ず呼び出され迂回されずに実行される。

a)メインボード HDD 上書き消去機能
メインボード上 HDD の画像データファイルに保存される各ジョブに対する上書き消去機能がある。
・HDD上にスプール保存されたデータを完全に消去する機能
・HDD上に長期保存されたデータをTOE利用者の削除操作により完全に消去する機能

b)プリンタボード HDD 上書き消去機能
プリンタボード上 HDD の画像データファイルに保存される各ジョブに対する上書き消去機能がある。
・HDD上に長期保存されたデータをTOE利用者の削除操作により完全に消去する機能
・HDD上に長期保存されたデータが出力により完全に消去される機能
・HDD上に長期保存されたデータが電源OFFにより完全に消去される機能

c)HDD フォーマット機能
TOE マシン管理者から、HDD フォーマット機能が実行された時、メインボード HDD、プリンタボード上のデータを完全に消去する機能

・メインボード上HDD、プリンタボード上HDD内の全領域を上書き消去する。

● 管理者認証機能　SPF.ADNIN

管理者認証機能は、TOEマシン管理者を確実に識別認証する機能である。
TOEマシン管理者権限の機能にアクセスする際に、TOEマシン管理者であることを識別し、TOE管理者暗証番号が要求され、操作パネルからTOE管理者暗証番号を入力する。入力されたTOE管理者暗証番号が一致すればアクセスを許可するが、一致しない限りはアクセスを許可しない。認証を行っている間、操作パネルには入力した文字数分のダミー文字(＊)だけが表示される。
TOE管理者暗証番号の尺度は、数字（0～9）８文字固定で構成される。この管理者認証機能は、TOEマシン管理者権限の機能にアクセスする際には必ず呼び出され、迂回されずに実行される。

また、TOE管理者暗証番号の値は、一定の場所に保管されており、機械設置時のデフォルト値は存在するが、TOEマシン管理者だけが変更出来るようになっている。変更する際には、数字以外が入力されても入力を受け付けず、また８文字未満のTOE管理者暗証番号では変更を受け付けない。

TOEマシン管理者に与えられた権限は以下の通りである。
・上書き消去方式の設定値変更 （３回上書き方式 / １回上書き方式）
・HDDフォーマット機能の実行
・TOE管理者暗証番号の変更

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に保持されている残存データを閲覧/出力する。また、上書き消去中における複合機の電源の切断により、上書き消去が未完状態となったＨＤＤ上の残存データを閲覧/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.METHOD	HDDの上書き消去に際し、安全性と処理効率の兼ね合いを考慮し、3回上書き方式、または1回上書き方式を適用する。

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-8030/KM-6030/CS-8030/CS-6030」に提供されるソフトウェアモジュールとして提供される。なお、ソフトウェアモジュールは、KM-8030/KM-6030/CS-8030/CS-6030 のMAIN ROM およびPRINTER ROM 内部に含まれている。

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.PHYSICAL	TOEを搭載する複合機は、TOEの関連者のみが利用可能な物理的に保護された場所に設置されていること。
A.ADMIN	TOEマシン管理者は、信用できる人物であり、不正を行わない人物であること。
A.CE	TOEのサービス担当者は、不正を行わないこと。

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。

・Data Security Kit (B) Operation Guide
　バージョン： Revision 1.0 2005.6 303J056013
・INSTALLATION GUIDE for Data Security Kit (B)
　バージョン： 2005.2 303J056710

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16年10月に始まり、平成17年10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16年12月、平成17年1月、および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16年12月および平成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構成を図2-1に示す。

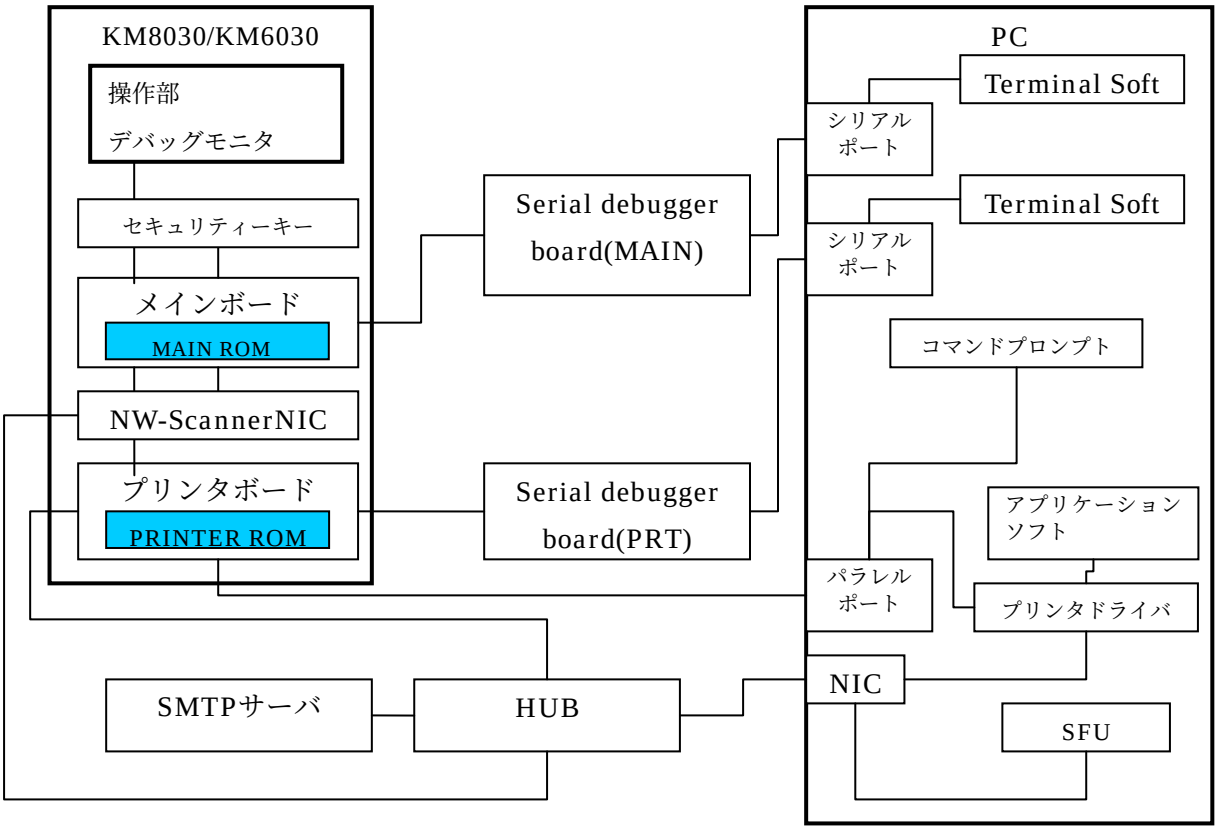

図2-1　開発者テスト及び評価者テストの構成

TOE：京セラミタ　Data Security Kit(B) Software	TOEはメインボードとプリンタボード上にある、MAIN ROMとPRINTER ROMのソフトウェアのことを指す。(図中青色表示)
メインボード	以下のサブシステムが動作する基板。 MMI、JOB管理、プリンタ制御、画像入出力制御、ファイル管理
プリンタボード	以下のサブシステムが動作する基板。 プリンタ
セキュリティーキー	メイン基板に接続することによりセキュリティ機能を有効にする基板。
PC	OS:Windows95以上、RAM:128MB以上
HUB	PCからLAN経由でのプリンタ印字、NWスキャナを使用するためのローカルネットワーク構築に使用する。
SMTPサーバ	NWスキャナのメール送信機能を使用するためのサーバ。
操作部デバッグモニタ	操作部で特定キーの同時押し下げにより、操作部LCDにデバッグ情報を表示することができる。
Serial debugger board (MAIN/PRT)	メイン基板用とプリンタ基板用がある。ターミナルソフトとシリアルポートを介して接続し、接続した基板に対して、ログ出力、メモリダンプ等が可能である。さらに、プリンタに対してはブレークポイントの設定が

	できる。
Terminal Soft	Hyper Terminal等のターミナルソフト。ログ確認、ブレークポイント設定に用いる。
コマンドプロンプト	MS-DOSのコマンドプロンプト。パラレルポートを介して、プリンタ基板にprescribeコマンドを転送する。
プリンタドライバ	プリンタ印字に必要。
SFU	ScannerFileUtility。NWスキャナのデータファイルを受信するソフト。
アプリケーションソフト:	プリンタ印字のテストに用いるWord/Excel等。

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。テスト環境として下記の２種類の環境が存在する。

①外部インタフェースを使用するテスト

ユーザが実際に使用する環境と同じ構成。Serial debugger Boardを介するデバッガ（PC）へは未接続。操作パネルやLCDの表示、エラー音、複合機の印刷出力により結果を確認する。

②内部インタフェースを使用するテスト

メインボードとプリンタボードそれぞれにSerial debugger boardを接続し、シリアルケーブルを通してデバッガ（PC）へセキュリティ機能の状態、サブシステム間の要求や通知内容、カウンタ値などのログを出力し結果を確認する。本機能はテスト用のみコンパイルスイッチにより実装されている。ユーザが実際に使用する場合はコンパイルスイッチの無効化により使用できない。また一部テストでは、TOEに組み込まれたテスト用のメモリダンプ機能によりデバッグ情報をLCDに表示するデバッグモニタを利用して結果を確認する。

c.実施テストの範囲

テストは開発者によって、機能テスト（FTテスト） 45項目、サブシステムテスト（JTテスト） 145項目が実施されている。

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構成は、開発者テストと同様の構成である。

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を図2-1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

テスト手法は、開発者テストと同じ方法がとられた。

c.実施テストの範囲

評価者が独自に考案したテストを14項目、開発者テストのサンプリングによるテストを40項目、計54項目のテストを実施した。

①評価者が独自に考案したテストは、下記を考慮している。

・開発者が実施していない、残存データ発生に対するテスト
・管理者暗証番号の変更に対する消極的なテスト
・全てのセキュリティ機能をテストすること

②開発者テストのサンプリングテストは以下を考慮し選択された。

・２つのセキュリティ機能を網羅する各テスト項目の中から、STに記述されていないふるまいのテスト(FTテスト)
・ハードキー基板（セキュリティハードキー基板）の有無でのセキュリティ機能のふるまいのテスト(FTテスト)
・各サブシステムを網羅するテスト項目の中からそれぞれのセキュリティ機能の主幹部分をテストしている項目(JTテスト)
・セキュリティ機能の期待される典型的なふるまいが確認できる項目(JTテスト)

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。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.1.2E	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、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_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、実地検査相当の方法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あることを確認している。
テスト	**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、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。

4.2 注意事項

TOEの保護資産は残存データであり、残存データの発生以前のファイル、データはTOEにより保護されていない。製品の利用に際して、セキュリティ上の注意を利用者に伝えることを勧める。

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
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。

スプール保存	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	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。
TWAIN	TWAIN対応のアプリケーションを利用することにより、複合機にセットされた原稿をクライアントPCからの操作でクライアントPCに取り込む処理。
ジョブ	コピー機能、プリンタ機能、ネットワークスキャナ機能の１つの処理の単位のこと。ジョブの中には原稿の画像データも含まれる。
印刷ジョブ	ジョブの中で、プリンタ機能として処理されるジョブのこと。
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。
残存データ	実データ領域の画像データを論理的に削除した後に、画像データが残存する領域。
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。外部インターフェイスであり、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。
NIC	Network Interface Cardの略。TOEを内部ネットワーク(LAN)に接続するための拡張カード。
フォーム	画像の重ね合わせ(イメージ合成)機能において、元画像となる合成元画像のことを指す。フォームに対し、読み取った原稿を重ね合わせてコピーすることが出来る。

6 参照

[1] 京セラミタ Data Security Kit(B) 海外版　セキュリティターゲット 第0.15版（2005年10月21日）京セラミタ株式会社

[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] 京セラミタ Data Security Kit(B) Software（海外版） 評価報告書 第2.3版 2005年10月25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