



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



評価対象

申請受付年月日(受付番号)	平成17年9月21日 (IT認証5064)
認証番号	C0056
認証申請者	京セラミタ株式会社
TOEの名称	Data Security Kit(D) Software
TOEのバージョン	V1.00J
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18年10月31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 田淵 治樹

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。

Common Criteria for Information Technology Security Evaluation Version 2.1
Common Methodology for Information Technology Security Evaluation Version 1.0
CCIMB Interpretations-0407

評価結果 : 合格

「Data Security Kit(D) Software」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、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	5
1.3	評価の実施	6
1.4	評価の認証	6
1.5	報告概要	7
1.5.1	PP適合	7
1.5.2	EAL	7
1.5.3	セキュリティ機能強度	7
1.5.4	セキュリティ機能	7
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	9
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	10
2.3.1	開発者テスト	10
2.3.2	評価者テスト	12
2.4	評価結果	14
3	認証実施	14
4	結論	14
4.1	認証結果	14
4.2	注意事項	20
5	用語	21
6	参照	23

1 全体要約

1.1 はじめに

この認証報告書は、「Data Security Kit(D) Software」（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。

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(D) Software

バージョン: V1.00J

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-C2520/KM-C3225/KM-C3232」に対するオプション製品として搭載され、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。

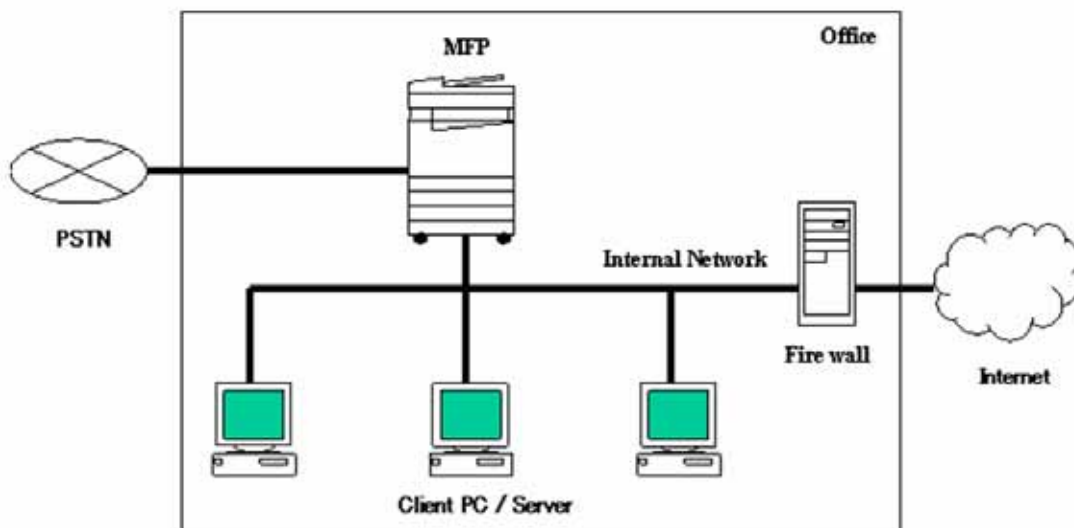


図1-1 複合機の利用環境

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。

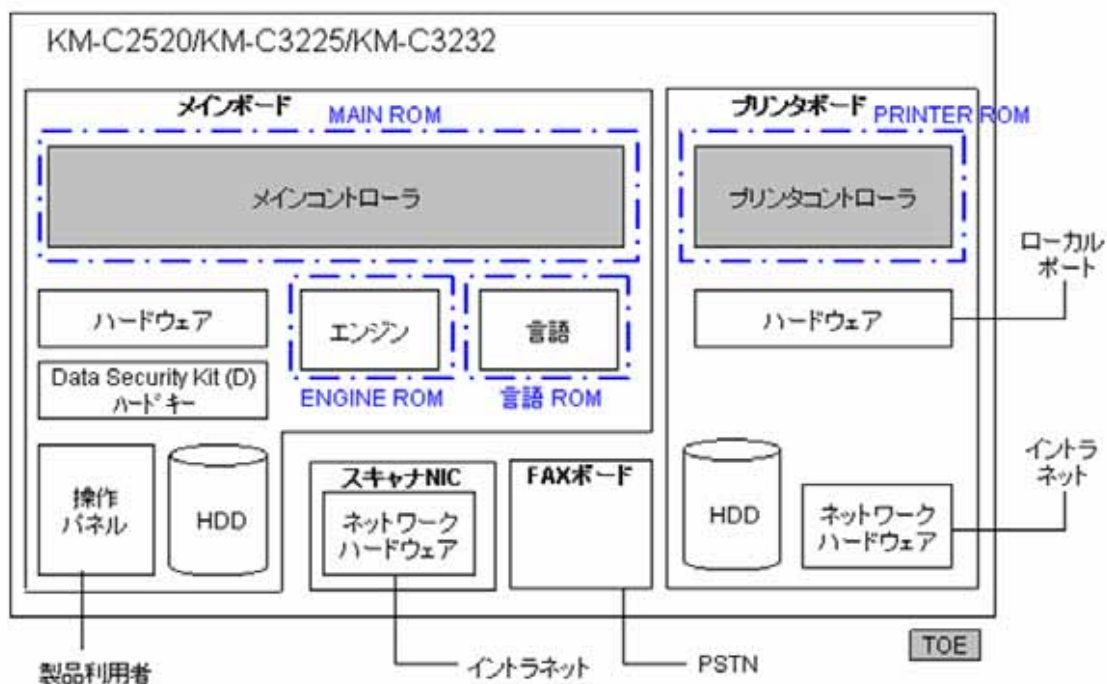


図1-2 TOE のハードウェア構成

TOEを動作させるには、図1-2に示されるData Security Kit (D) ハードキーが必要と

なる。仮に運用中にData Security Kit (D)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。

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
ENGINE ROM	エンジンモジュール	スキャナエンジン 印刷エンジン
言語ROM	言語モジュール	文字列データ 仕向け地に合わせる
FAX ROM	FAXモジュール	-
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。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。

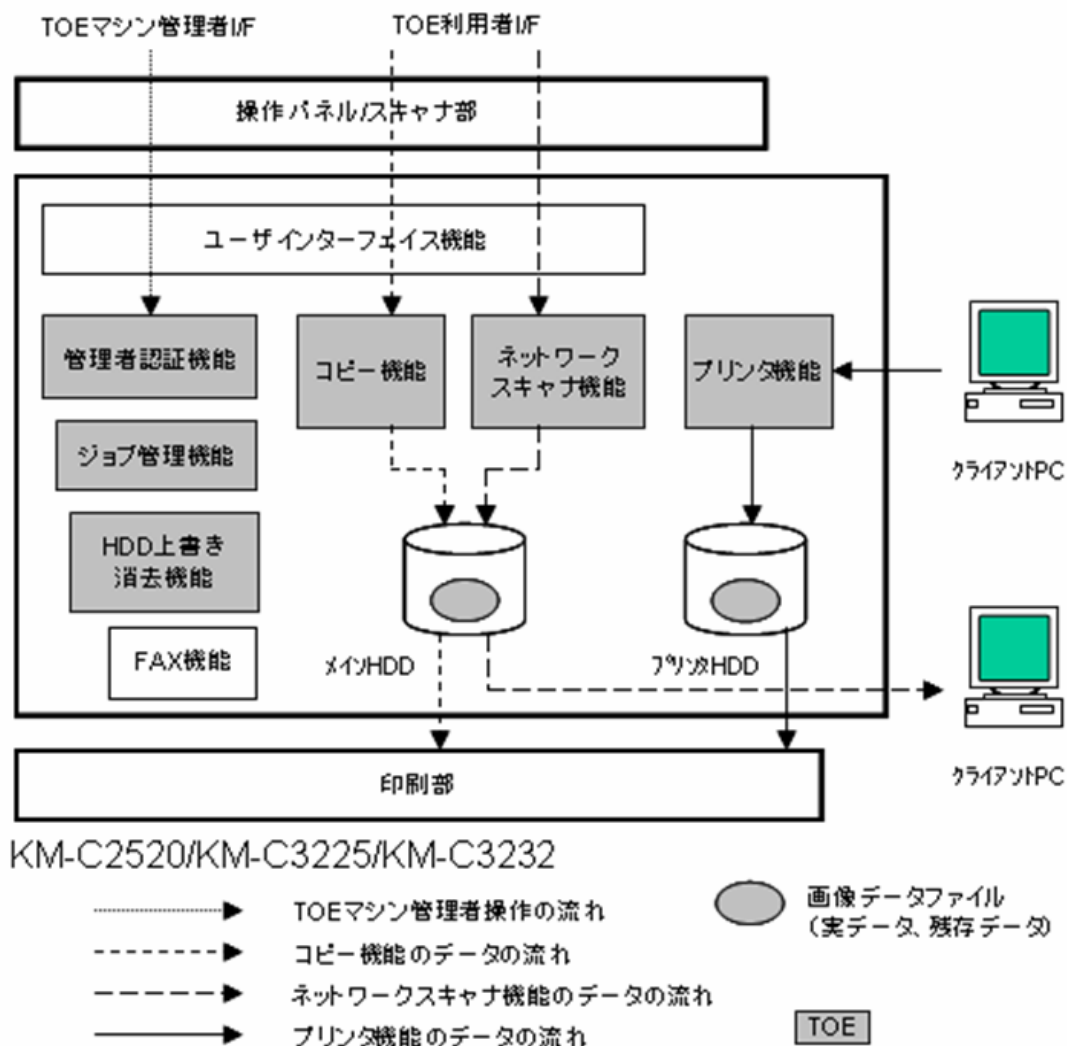


図1-3 TOEの論理的構成

これらの機能を利用することができる人物と、その概要を示す。

a. TOE管理者

TOEを搭載した複合機本体の管理者として登録されている者。TOE管理者は、機械本体に対する特権を有する。

b. TOE利用者

オフィスや学校内でTOEを搭載した複合機の利用を許可された者。コピー、プリント、ネットワークスキャナ、FAX等の機能を利用することができる。また、TOE利用者は、画像データの露頭に関して攻撃能力は低レベルである。

c. サービス担当者

TOEを搭載した複合機のサービス担当者として京セラミタが認めた者。サービス担当者はTOEの導入及び、TOEを搭載した複合機の保守を行う。

1.2.4 TOEの機能

TOEが提供する機能は以下のとおりである。

1)セキュリティ機能

a. HDD 上書き消去機能

HDDに保存された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機能。

b.管理者認証機能

TOE管理者を操作パネルから入力されたTOE管理者暗証番号により、識別認証する機能。

2)複合機としての通常機能

a.コピー機能

画像データを複合機のスキャナから読み込み、複合機の印刷部から出力する機能。

b.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み込み、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 送信がある。また、TWAIN 対応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 TWAIN もある。

c.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。

d.ジョブ管理機能

HDD 上に保存されたジョブ/印刷ジョブを管理する機能。ジョブ/印刷ジョブの編集/出力/削除を行うことができる。

TOE が搭載されていない複合機では、コピー/プリント/ネットワークスキャナの処理を行う際、一旦、スプール保存領域にデータを保持してから処理を行い、処理終了後にそのデータの管理領域を論理的に削除するだけである。このため、実データ領域が残存情報として残ってしまう。この残存情報には、データとしてはコピー/プリント/ネットワークスキャナ等の処理で行ったデータと同じデータが入っているため、何らかの方法によりアクセスされると、データを持ち出されてしまうことも起こり得る。場合によっては、このデータには利用者の機密情報が含まれることもあり、持ち出されると非常に重大な問題となる可能性もある。

そこで、TOE が保護すべき資産は、以下のとおりである。

- ・メインボード上 HDD 内にスプール保存又は長期保存された画像データが、論理的に削除された後の残存データ
- ・プリンタボード上 HDD 内に長期保存された画像データが、論理的に削除された

後の残存データ

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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 (D) 日本版 セキュリティターゲット 第0.07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 (D) Software (日本版) 評価報告書」(以下「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、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18年9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、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じ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、攻撃力を“低レベル”と想定することは妥当である。

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。

1)HDD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、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。

a. 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

b. 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

2)管理者認証機能

TOE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できる。

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。

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。

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-C2520/KM-C3225/KM-C3232」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-C2520/KM-C3225/KM-C3232 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 (D) 使用説明書 (303KM56010Rev.1.0)
- ・ Data Security Kit (D) 設置手順書 (303KM56711Rev.2.0)
- ・ FAX System (N) 設置手順書 (303KK56710Rev.1.0)
- ・ KM-C2520/KM-C3225/KM-C3232 サービスマニュアル (2GBSM002Rev.2)
- ・ KM-C2520/KM-C3225/KM-C3232 使用説明書 (302FZ56010Rev.1.0)
- ・ KM-C2520/KM-C3225/KM-C3232 使用説明書 応用編 (302FZ56020Rev.1.0)
- ・ FAX System (N) 使用説明書 (303KK56010Rev.1.0)
- ・ お知らせ (303KM56321Rev.2.0)

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、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、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18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18年8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18年8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。

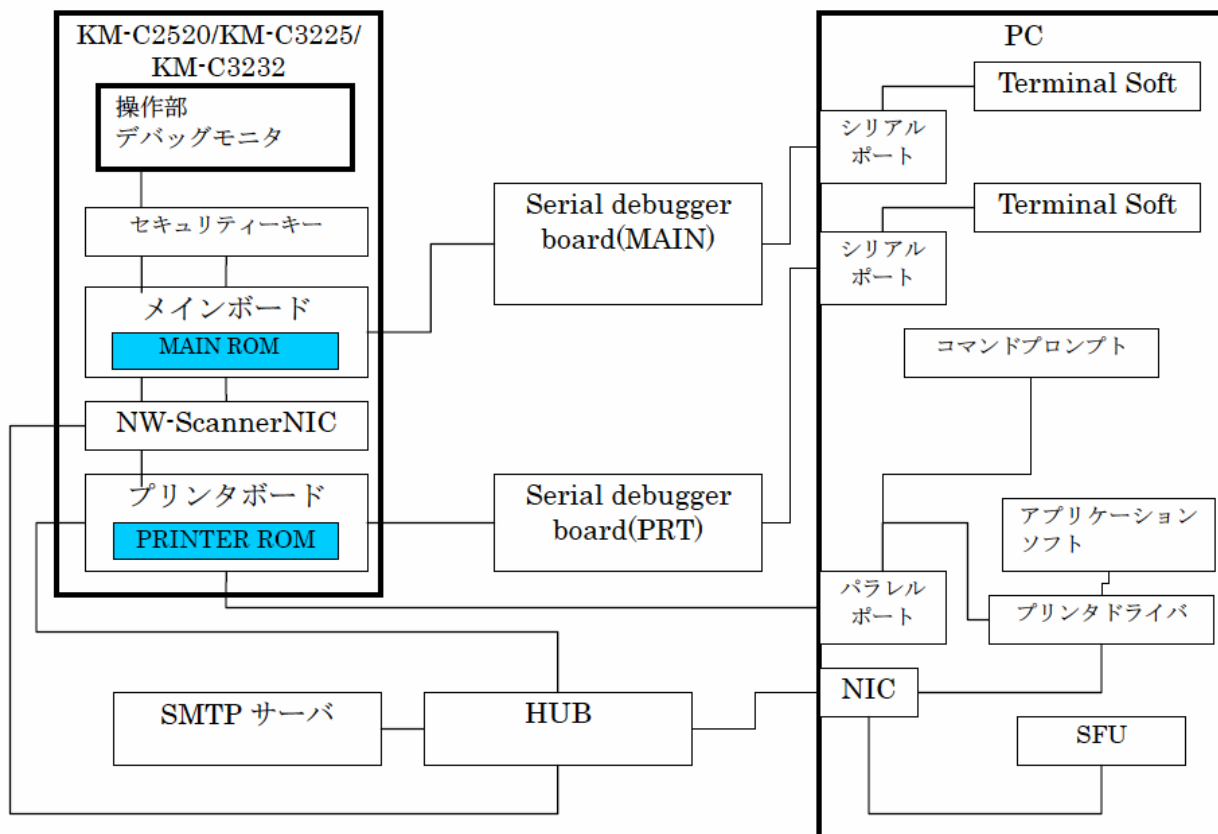


図2-1 開発者テストの構成図

TOE : 京セラミタ Data Security Kit(D) 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な。
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。

・ 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ugg (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。

・ 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ugg (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ugg情報をLCDに表示するデバugg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45項目、サブシステムテスト145項目が実施されている。

カバレッジ分析が実施され、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（侵入テストを含む）を19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59項目のテストを実施した。

評価者が独自に考案したテストは、以下を考慮している。

- ・ 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
 - ・ 電源OFF2回（電源再々投入時）でも上書き消去を実施すること
 - ・ メンテナンスモード起動中に、セキュリティモードが動作しないこと
 - ・ 上書き消去実施後に、残存データ復元ソフトウェアを用いても復元可能なファイルがないこと
 - ・ RAMから残存データが読み出せず、電源OFF時にはデータが消失すること
 - ・ Flashメモリ内に保護資産が保存されていないこと
 - ・ 不揮発性メモリ上の設定値を、取得・改ざんできないこと
- 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

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。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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。
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

	<p>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、当評価に至るまでになされた所見報告書による指摘も適切と判断される。</p>
ASE_REQ.1.2E	<p>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。</p>
ASE_SRE.1.1E	<p>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。</p>
ASE_SRE.1.2E	<p>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。</p>
ASE_TSS.1.1E	<p>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。</p>
ASE_TSS.1.2E	<p>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。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。</p>
構成管理	適切な評価が実施された
ACM_CAP.3.1E	<p>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。</p>
ACM_SCP.1.1E	<p>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。</p>
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。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。
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。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、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。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。
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。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_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。
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。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.1.2E	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。

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を利用することができる。
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。
プリンタドライバ	クライアントPCに表示された文字や画像を複合機のプリンタに転送するなど、複合機プリンタ機能を制御するためにクライアントPCにインストールするソフト。
スキャナエンジン	原稿をスキャンする装置を制御するモジュール。
印刷エンジン	データを紙に出力し、印刷する装置を制御するモジュール。

6 参照

- [1] 京セラミタ Data Security Kit (D) 日本版 セキュリティターゲット 第0.07版
(2006年6月26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17年7月 独立行政法人 情報処理推進機構 EC-01
- [3] ITセキュリティ認証手続規程 平成17年7月 独立行政法人 情報処理推進機構 EC-03
- [4] 評価機関承認手続規程 平成17年7月 独立行政法人 情報処理推進機構 EC-05
- [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 model
- [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] 京セラミタ株式会社 Data Security Kit (D) Software (日本版) 評価報告書 第1.6版
2006年9月29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