



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

申請受付日（受付番号）	平成19年3月27日（IT認証7145）
認証番号	C0125
認証申請者	シャープ株式会社
TOEの名称	MX-FRX7
TOEのバージョン	VERSION S.10
PP適合	なし
適合する保証パッケージ	EAL3+ADV_SPM.1
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19年11月16日

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 鈴木 秀二

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 2.3

Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「MX-FRX7 VERSION S.10」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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	2
1.2.4	TOEの機能	3
1.3	評価の実施	4
1.4	評価の認証	4
1.5	報告概要	5
1.5.1	PP適合	5
1.5.2	EAL	5
1.5.3	セキュリティ機能強度	5
1.5.4	セキュリティ機能	5
1.5.5	脅威	7
1.5.6	組織のセキュリティ方針	7
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	8
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	15
4	結論	16
4.1	認証結果	16
4.2	注意事項	22
5	用語	23
6	参照	26

1 全体要約

1.1 はじめに

この認証報告書は、「MX-FRX7 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。

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： MX-FRX7
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)のセキュリティ機能を強化するためのファームウェアである。本TOEはオプション製品として提供され、MFD内に設置することにより、MFDの標準ファームウェアを置き換え、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。本TOEは、主として暗号操作機能、及びデータ消去機能からなり、TOEを搭載したMFD内部に残存する実イメージデータからの情報漏洩を防止することを目的とする。

暗号操作機能は、PC-Fax、ファクス送信、ファクス受信の各ジョブにおいて、実イメージデータをFlashメモリにスプール保存する前に暗号化する。データ消去機

能は、コピー、プリント、イメージ送信、PC-Fax、ファクス送信、ファクス受信の各ジョブの完了後、スプール保存されている実イメージデータが存在している領域に対しランダム値、または固定値を上書きする。

1.2.3 TOEの範囲と動作概要

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。

本TOEは、MFDのコントローラ基板に装着する2枚のROM基板に格納された、コントローラ基板を制御するファームウェア（コントローラファームウェア）である。

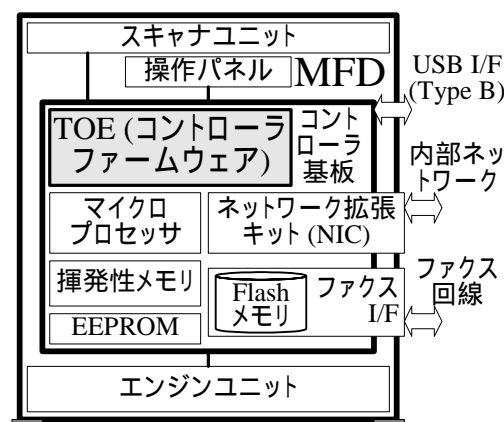


図1-1：MFDの物理的構成とTOEの物理的範囲

TOEの論理構成を図1-2に示す。TOEの論理範囲を太枠で示し、ソフトウェアの機能を長方形で示し、TOE外のハードウェアを角の丸い長方形で示す。本TOEの機能のうち、網掛け部分がセキュリティ機能である。また、データの流れを矢印で示す。

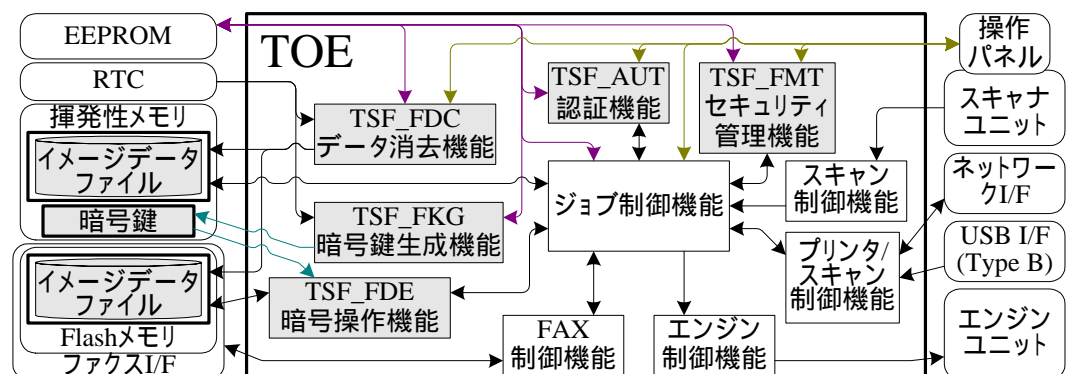


図1-2：TOEの論理的構成

本TOEはMFD用のファームウェアであり、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。

1.2.4 TOEの機能

TOEが提供する機能を以下に示す。

a) 暗号操作機能 (TSF_FDE)

ファクス機能で扱う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ための暗号鍵を生成する。生成された暗号鍵は、揮発性メモリ (FAX_RAM) に保存する。暗号鍵のシード (seed) はTOEの設置時に一度生成され、その後は、MFDの電源がオンになると、このシードを元に常に同じ暗号鍵を生成する。

c) データ消去機能 (TSF_FDC)

MSDからの情報漏えいを防ぐため、MSDに対し上書き消去する。各ジョブ完了後の自動消去、及び、全データエリア消去を行う。各ジョブ完了後の自動消去は、ジョブ制御機能により、ジョブ処理終了及び中止の際に呼び出される。

d) 認証機能 (TSF_AUT)

管理者パスワードにより管理者の識別認証を行う。

e) セキュリティ管理機能 (TSF_FMT)

管理者として認証された場合において、管理者パスワードの変更 (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

TOEを搭載可能なMFDのうち、PCL基板を標準また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、USB I/Fまたはネットワーク 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。
- イメージ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

PC-Faxジョブ、ファクス送信ジョブにおいてFAX回線への送付、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。

k) 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、イメージ送信ジョブ、PC-Fax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、イメージ送信、PC-Fax、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セキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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「MX-FRX7 セキュリティターゲット」(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]のいずれか) 附属書B、CCパート2 ([6][9][12]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]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、「MX-FRX7 VERSION S.10評価報告書」(以下「評価報告書」という。)[18]に示されている。なお、評価方法は、CEM ([14][15][16]のいずれか)に準拠する。また、CC及びCEMの各パートは補足[17]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。評価は、平成19年11月の評価機関による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

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 (TSF_FKG)

TOEは、暗号鍵 (共通鍵) の生成を行い、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。TOEは、セキュアなシードを元に、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し、暗号アルゴリズムAES Rijndaelで使用するために、揮発性メモリ内に保存する。MSN-J拡張アルゴリズムは、データセキュリティキット用暗号基準書を満たす暗号鍵生成アルゴリズムである。

暗号鍵のセキュリティ属性であるシードは、TOEセキュリティ方針 (TSP) モデルに従うセキュアな方法でTOEにより生成される。TOEは設置の際、MFD 1台ごとに異なるシードを生成する。これにより、各MFD内のTOEは常に同じシードから同じアルゴリズムで暗号鍵を生成する。

(2) 暗号操作機能 (TSF_FDE)

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。

暗号化及び復号にはFIPS PUBS 197に基づくAES Rijndaelアルゴリズムと、暗号鍵生成機能（TSF_FKG）により生成された128ビット長の暗号鍵を用いる。

(3) データ消去機能（TSF_FDC）

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機能を提供する。本機能は、下記2種類の消去プログラムにより構成される。

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、イメージ送信ジョブ完了後、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。

PC-Fax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) 全データエリア消去

本機能は、認証機能（TSF_AUT）で識別認証された管理者により操作パネルにて起動され、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し、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。

本機能を途中で中止する場合、キャンセル操作を選択後、管理者パスワードの入力による管理者の識別認証を必ず要求する。管理者として識別認証された場合についてのみ、上書き消去を中止する。

(4) 認証機能（TSF_AUT）

本機能は、管理者パスワードにより管理者の識別認証を行う。TOEは、管理機能の起動操作によって管理者を識別し、かつ、正しい管理者パスワードによって管理者認証に成功した場合に限り、管理者向け機能へのインタフェースを提供する。これにより管理者を特定し、管理者の役割を利用者に関連付ける。管理者パスワード入力時、入力した文字と同数のアスタリスク（星型記号）を表示するが、入力した文字は表示しない。

連続して3回認証に失敗した場合、認証受付を停止する。認証受付停止からの経過時間が5分に達すれば、自動的に認証受付停止を解除、すなわち、認証失敗回数をクリアして通常状態に復帰する。

データ消去機能(TSF_FDC)の全データエリア消去の実行、及びセキュリティ管理機能(TSF_FMT)の管理者パスワードの問い合わせと変更は、操作を許可する前に必ず管理者として認証されなければならない。

(5) セキュリティ管理機能 (TSF_FMT)

管理者パスワードは、本機能により管理されている。本機能の使用を許可する前に必ず認証機能(TSF_AUT)による管理者識別認証を行い、成功した場合に限り本機能の使用を許可する。このため、認証機能(TSF_AUT)と同じく、管理者を特定し、利用者と役割を関連付けている。また、管理者パスワードを変更(変更)後も、管理者として役割が維持される。

本機能は管理者パスワード変更機能を提供する。これにより管理者パスワードの変更(変更)が可能で、新しい管理者パスワードが5文字の数字であることを必ず検査する。設定値はMFD内のEEPROMに保存する。

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えいさせる。

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、イメージ送信、PC-Fax、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、管理者により、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

TOEが動作するMFDはシャープ社製のMX-M350, MX-M350F, MX-M350U, MX-M350UJ, MX-M450, MX-M450F, MX-M450U及びMX-M450UJ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	管理者は、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 MX-FRX7

バージョン : CINSJ3965FC51

対象者 : 管理者、利用者

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 MX-FRX7

バージョン : TCADZ1930FCZZ

対象者 : 管理者、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。

MX-FRX7 設置手順書

バージョン : TCADZ1932FCZZ

対象者 : 管理者、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、管理者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

MX-FRX7 Data Security Kit Operation Manual

バージョン : CINSE3966FC51

対象者 : 管理者、利用者

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

MX-FRX7 Data Security Kit Notice

バージョン : TCADZ1931FCZZ

対象者 : 管理者、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。

MX-FRX7 Installation Manual

バージョン : TCADZ1933FCZZ

対象者 : 管理者、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、管理者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。

なお、本TOEの使用にあたっては、MFD本体に付属する下記ドキュメントも併読する必要がある。

(1) 日本語版

- ・取扱説明書デジタル複合機 管理者設定編
(TINSJ3679FCZZ)

(2) 海外版（表記言語は英語）

- ・Laser Printer Administrator Settings Guide
(TINSE3682FCZZ)

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19年6月に始まり、平成19年11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19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19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。

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。

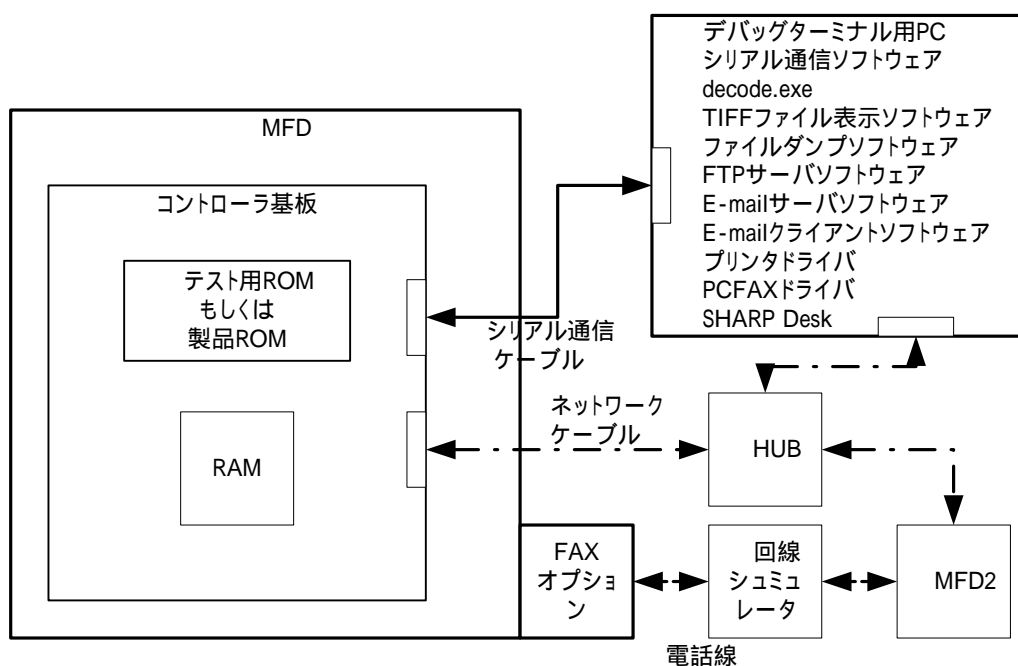


図2-1 開発者テストの構成図

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において識別されてい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MFDは、STで動作環境として複数識別されている機種のうちの一機種(MX-M450F)がテストにおいて使用された。STで識別されているMFD間の差異はエンジンスピード(1分間当たりの印字速度)及びオプション機能に起因するものである。TOEのセキュリティ機能はこれらの影響を受けず、またテストで使用した機種(MX-M450F)は全ての機能を搭載したものであるため、本テスト環境は、STにおいて識別されたTOEと同等の構成であるとみなすことができる。

図2-1のテスト用ROMは、STで識別されるTOEとは異なるが、これらは製品ROMにテスト用のデバッグ機能を追加したものであり、TOEと同等の構成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。

製品ROM使用環境

ユーザ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。

テスト用ROM使用環境

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。

c.実施テストの範囲

テストは開発者によって15項目実施されている。

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を図2-2に示す。

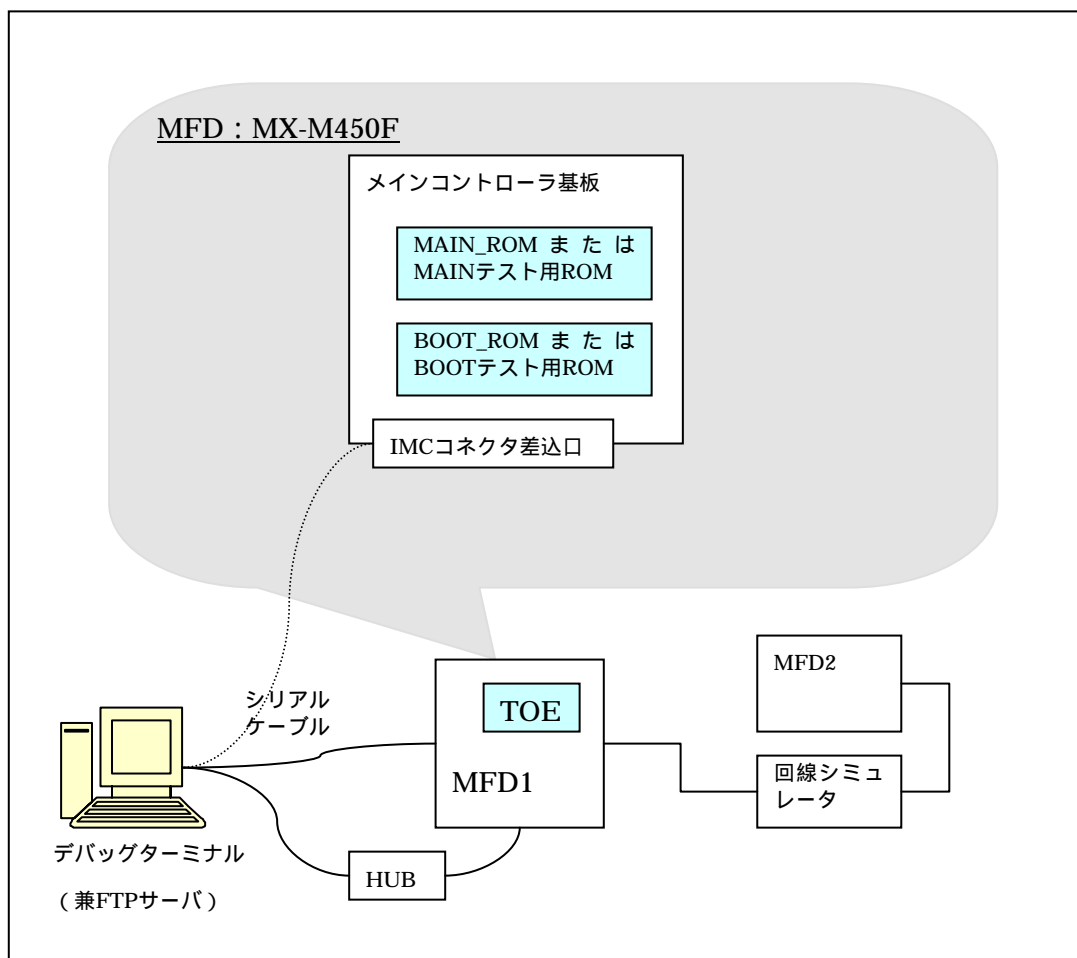


図2-2 評価者テストの構成図

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2-2に示すとおりである。評価者テストはSTにおいて識別されているTOE構成と同等のTOE動作環境で実施された。評価者テスト構成においても、STにおいて識別されるTOE構成とは完全に一致しない部分が存在するが、開発者テスト環境と同様の理由により、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。

製品ROM使用環境

ユーザ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。

テスト用ROM使用環境

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。

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、侵入テストを9項目、計22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、以下に示す観点を考慮している。

5つのセキュリティ機能すべてが含まれること

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

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

認証取得済みTOEに追加された機能

開発者が実施していない消極的テスト

TOEが対応するとした他機種種の複合機に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も、5つのセキュリティ機能すべてを選択の対象とし、かつ、データ消去機能（TSF_FDC）が実施されるさまざまな場合がテストされるよう配分を行っている。

侵入テストは、開発者が考慮していない明白な脆弱性が存在しないかの確認のため、4つのセキュリティ機能（暗号操作機能、データ消去機能、認証機能、セキュリティ管理機能）に加え、TOEとTOEの環境全体を対象とするテスト項目が考案された。

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

認証機関は、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。

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。

認証機関は、ST及び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。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_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_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。
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。
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において明示的方针をもたないこと、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	<p>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ータ、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。</p>
AGD_USR.1.1E	<p>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。</p>
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	<p>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。</p>
ALC_DVS.1.2E	<p>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。</p>
テスト	適切な評価が実施された
ATE_COV.2.1E	<p>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。</p>
ATE_DPT.1.1E	<p>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。</p>

ATE_FUN.1.1E	<p>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。</p>
ATE_IND.2.1E	<p>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。</p>
ATE_IND.2.2E	<p>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。</p>
ATE_IND.2.3E	<p>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。</p>
脆弱性評価	適切な評価が実施された
AVA_MSU.1.1E	<p>評価はワークユニットに沿って行われ、提供されたガイドランスが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、ガイドラ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。</p>
AVA_MSU.1.2E	<p>評価はワークユニットに沿って行われ、提供されたガイドラ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。</p>
AVA_MSU.1.3E	<p>評価はワークユニットに沿って行われ、提供されたガイドランスが、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。</p>

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。
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。

AES	Advanced Encryption Standard — 米国の商務省標準技術局 (NIST) が制定した米国政府標準暗号。
EEPROM	Electrically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電氣的に任意部分の書き換えを可能にしたROM。
I/F	Interface (インタフェース)
MSD	Mass Storage Device — 大容量ストレージ装置。本報告書では特にMFD内のIMC_RAM, PCL_RAM及びFlashメモリを指す。
NIC	Network Interface Card (ネットワークインタフェースカード) — または — Network Interface Controller (ネットワークインタフェースコントローラ)
ROM	Read Only Memory — 読み出し専用メモリ。
UI	User Interface (ユーザーインタフェース)
USB	Universal Serial Bus — IT機器間を接続するシリアルバス標準の名称。

イメージデータ	本STでは特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
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。
各ジョブ完了後の自動消去	MFD内のMSDに保存された、個々のジョブに対応するイメージデータを上書き消去するための機能。ジョブ完了または中止の際に呼び出される。
揮発性メモリ	電源を切れば記憶内容が消失する記憶装置。
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	本TOEの保護資産であり、MFDの各処理終了後に揮発性メモリ、もしくはFlashメモリ内に残存するイメージそのもののデータ。
実イメージデータファイル	実イメージデータを管理するファイルシステムが取り扱うためのオブジェクトであり、実イメージデータそのものである。
ジョブ	MFDのコピー、プリンタ、イメージ送信、ファクス送受信及びPC-Faxの各機能において、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。
スキャナユニット	原稿をスキャンしてイメージデータを得る装置。コピー、イメージ送信及びファクス送信の際に使用する。
スプール	入出力効率のため、ジョブのイメージデータを一時的にMSDに保持すること。
全データエリア消去	MFD内のMSD上にあるすべてのイメージデータを上書き消去するための機能。管理者の操作により呼び出される。
操作パネル	MFDの正面にあるUI用ユニット。スタートキー、数字キー、機能キー及びタッチ操作式の液晶ディスプレイを含む。
標準ファームウェア	TOE設置前のMFDに搭載されているコントローラファームウェア。TOEはコントローラファームウェアを含んでおり、TOE設置時に標準ファームウェアを取り外す。
ファームウェア	機器のハードウェアを制御するために、機器に組み込まれたソフトウェア。本STでは特に、コントローラファームウェアを指す。
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記憶装置。

Flashメモリ	不揮発性メモリの一種で、電氣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 (Flash Memory)。
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。

6 参照

- [1] MX-FRX7 セキュリティターゲット バージョン 0.04 (2007年11月7日)
シャープ株式会社
- [2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報
処理推進機構 CCS-01
- [3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報
処理推進機構 CCM-02
- [4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政
法人 情報処理推進機構 CCM-03
- [5] Common Criteria for Information Technology Security Evaluation Part1:
Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001
- [6] Common Criteria for Information Technology Security Evaluation Part2:
Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002
- [7] Common Criteria for Information Technology Security Evaluation Part3:
Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003
- [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2.3 2005年8月 CCMB-2005-08-001 (平成17年12月翻訳第1.0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2.3 2005年8月 CCMB-2005-08-002 (平成17年12月翻訳第1.0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2.3 2005年8月 CCMB-2005-08-003 (平成17年12月翻訳第1.0版)
- [11] ISO/IEC 15408-1:2005 Information technology - Security techniques -
Evaluation criteria for IT security - Part 1: Introduction and general model
- [12] ISO/IEC 15408-2:2005 Information technology - Security techniques -
Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:2005 Information technology - Security techniques -
Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] Common Methodology for Information Technology Security Evaluation :
Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004
- [15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8
月 (平成17年12月翻訳第1.0版)
- [16] ISO/IEC 18045:2005 Information technology - Security techniques -
Methodology for IT security evaluation
- [17] 補足-0512 平成17年12月
- [18] MX-FRX7 VERSION S.10 評価報告書 第2.2版 2007年11月8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