認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司

原紙押印済

評価対象

申請受付日（受付番号）	**平成21年10月19日** (IT**認証**9273)
認証番号	C0255
認証申請者	**シャープ株式会社**
TOE**の名称**	MX-FR15
TOE**のバージョン**	C.10
PP**適合**	**なし**
適合する保証パッケージ	EAL3
開発者	**シャープ株式会社**
評価機関の名称	**一般社団法人　ITセキュリティセンター　評価部**

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22年5月26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　山里　拓己

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。

① 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 バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「MX-FR15 C.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 はじめに

この認証報告書は、「MX-FR15 C.10」（以下「本TOE」という。）について一般社団法人　ITセキュリティセンター　評価部（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とともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、デジタル複合機の調達者/管理者を読者と想定している。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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称：　MX-FR15
バージョン：　C.10
開発者：　シャープ株式会社

1.2.2 製品概要

TOEはMFD (デジタル複合機) 内データ保護機能を持つIT製品である。
TOEは、ROMに格納されたMFD用ファームウェアである。これはMFDの標準

ファームウェアを置き換えることにより､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。

デジタル複合機は事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能及びファクス機能を有する。

TOEの主要なセキュリティ機能は、暗号操作機能、データ消去機能であり、TOEを搭載したMFD内部のイメージデータを不正に取得する試みに対抗することを目的とする。

1.2.3 TOE範囲とセキュリティ機能

1.2.3.1 TOE の物理的範囲

TOEの物理的範囲を図1-1に網掛けで示す。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。

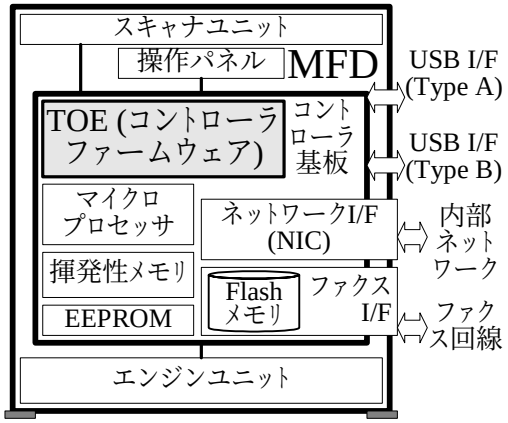

図1-1 MFDの物理的構成とTOEの物理的範囲

1.2.3.2 TOE の論理的範囲とセキュリティ機能

TOEの論理的構成を図1-2に示す。TOEの論理的範囲を太い枠線内として示す。TOE外のハードウェアを､角を丸くした長方形で示す｡TOEの機能を長方形で示し、その中のセキュリティ機能を網掛けで示す。また、揮発性メモリ、Flashメモリ、及びEEPROM上にあるデータのうち､セキュリティ機能が扱うデータ (利用者データ及びTSFデータ) を、同じく網掛けで示す。図中、データの流れを矢印で示す。また､TOEの機能間で受け渡されるデータは､一時的に揮発性メモリを経由するが､セキュリティ機能上の意味を持つ場合を除いて省略している。

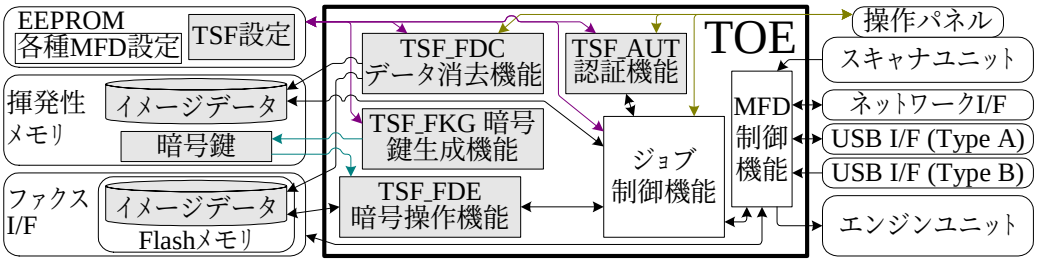

図1-2 TOEの論理的構成

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。以下のセキュリティ機能がTOEの論理的範囲に含まれる。

a) 暗号操作機能 (TSF_FDE):
Flashメモリに書き込むイメージデータを暗号化する。また、Flashメモリから読み出したイメージデータを復号する。ジョブ制御機能により、ジョブ処理の際に呼び出される。

b) 暗号鍵生成機能 (TSF_FKG):
暗号操作機能で使用する暗号鍵を生成する。生成された暗号鍵は、揮発性メモリに保存する。

c) データ消去機能 (TSF_FDC):
MFD内の揮発性メモリ、及びFlashメモリ（以下MSDという。）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機能から構成される。各ジョブ完了後の自動消去は、ジョブ制御機能が呼び出すことにより自動的に起動する。全データエリア消去は、管理者が操作することにより起動する。

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。管理者パスワードを変更する管理機能を持つ。

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-FR15 セキュリティターゲット」（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]のいずれか） 附属書A、CCパート2（[6][9]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]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、「シャープ株式会社 MX-FR15 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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及び所見報告書、その他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22年5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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅 威
T.RECOVER	攻撃者が、MFD内のFlashメモリを取り外して持ち出し、他の装置 (そのFlashメモリを搭載したMFD以外の装置)を接続することにより、Flashメモリ内に残存するイメージデータを読み出し漏えいさせる。

2.1.2 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2-2に示す。

表2-2 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	ジョブ完了または中止時、MSDにスプール保存されたイメージデータの領域は、少なくとも1回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、MSDのスプール領域はすべて、少なくとも1回上書き消去されなければならない。

2.1.3 運用環境の前提条件

本TOEを使用する環境において有する前提条件を表2-3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2-3 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。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

・MX-FR15 Data Security Kit Operation Manual [CINSE4812FC51]
本TOEの取扱説明書として提供され、セキュリティ機能の使い方、設定方法等TOEの管理、運用に必要な事項が記載される。

・MX-FR15 Data Security Kit Notice [CINSE4813FC51]
本TOEをセキュアに利用するための注意事項、及び本TOEを複合機本体に取り付ける際の作業手順等が記載される。

2.1.5 構成条件

本TOEは、シャープ製デジタル複合機 MX-M363U、MX-M363UJ、MX-M453U、MX-M453UJ、MX-M503U、及びMX-M503UJで動作する。

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

2.2.1 脅威「T.RECOVER」への対抗

「T.RECOVER」ではMFDから取り外されたFlashメモリから、内部に残存するデータが漏えいすることを想定している。この脅威に対して下記のセキュリティ機能により対抗する。

① 暗号鍵生成機能（TSF_FKG）

暗号鍵（共通鍵）の生成を行い、暗号操作機能（TSF_FDE）をサポートする機能である。TOEは、MFDの電源がオンになると必ず128ビット長のセキュアな暗号鍵（共通鍵）を生成し、揮発性メモリ内に保存する。

② 暗号操作機能（TSF_FDE）

ジョブ処理の途上において、ジョブのイメージデータをFlashメモリに書き込む際に必ず暗号化後に書き込み処理を行い、データ読出しの際には復号処理を行う機能である。暗号化、及び復号にはFIPS PUB 197に基づくAES Rijndaelアルゴリズム、及び暗号鍵生成機能（TSF_FKG）により生成された128ビット長の暗号鍵を用いる。

2.2.2 組織のセキュリティ方針「P.RESIDUAL」の実現

「P.RESIDUAL」は揮発性メモリ、及びFlashメモリの保存データに対して上書き消去を求めている。この組織のセキュリティ方針を下記のセキュリティ機能により実現する。

① データ消去機能（TSF_FDC）

スプール保存されたイメージデータを消去する機能を提供する。本機能は、以下の各機能により構成される。各機能とも揮発性メモリにはランダム値を、Flashメモリには固定値を上書きすることにより、イメージデータの再生を不能とする。

a) 各ジョブ完了後の自動消去
ジョブ処理のため揮発性メモリまたはFlashメモリにスプール保存されたイメージデータを、当該ジョブ完了時に上書き消去する機能である。

b) 全データエリア消去
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、揮発性メモリまたはFlashメモリにスプール保存された全てのイメージデータを上書き消去する機能である。

本機能は途中での中止機能を提供する。キャンセル操作が選択されると、管理者の識別認証を必ず要求し、正しく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。

② 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機能である。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、及び管理者パスワードの改変は、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。パスワード改変の際には、新しく設定されるパスワードが長さ、文字種の観

点から必要な品質が確保されていることをTOEが検査する。

3 評価機関による評価実施及び結果

3.1 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。

3.2 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21年10月に始まり、平成22年5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22年2月、及び4月に開発現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティ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22年2月、及び4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。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

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3-1　開発者テストの構成図に示す。

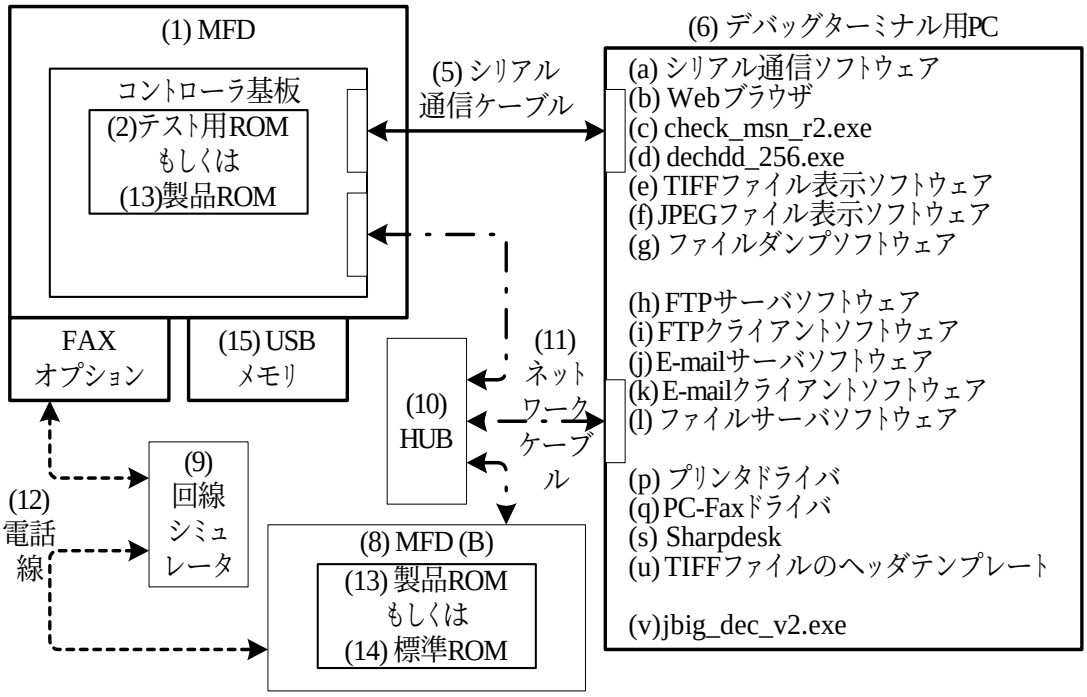

図3-1　開発者テストの構成図

テストで使用されたMFDはSTで識別されている複数のMFDの一部の機種(MX-M503U)が使用された。TOEの動作する各MFDは処理能力等が異なるが、TOEは全て同一なものが使用される。よって、テスト環境は、STにおいて識別された環境と同等の構成であるとみなすことができる。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

図3-1に示した環境下で、製品ROM、テスト用ROMの2種類のROMをテストの特性により使い分けて実施した。テスト用ROMは、テストの結果確認のためにシリアルポート出力、暗号鍵の種及び暗号鍵の出力、暗号操作の有効無効の切り替え、上書き消去データの指定を可能にしたものであり、テスト対象のセキュリティ機能性には影響がない。

テスト手法は、インタフェースを刺激する手法(MFDの電源操作、MFDの操作パネルからの手動操作、クライアントPCからの手動操作等)と、応答を観察する手法(MFDの操作パネルからの観察、デバッグターミナルからの観察等)により実施した。

b. 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。

カバレージ分析が実施され、機能仕様に記述されたすべてのTSFI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、TOE設計に記述されたすべてのTSFサブシステムのふるまいと相互作用が十分にテストされたことが検証されている。

c. 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。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

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り、製品ROM、テスト用ROMを使用している。

評価者が実施したテストの構成を図3-1に示す。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

- 入力パラメタの網羅性の観点から開発者テストが不足していると判断されるTSFに関して、入力パラメタの種類、組み合わせを追加し、TSF毎にテストを実施する
- 利用者操作のタイミング、組み合わせを追加し、TSFの振る舞いをより厳密に確認するためのテストを実施する
- クライアントPCとの接続方法に関して、開発者テストとは異なるインタフェースを使用しTSFの振る舞いを確認するためのテストを実施する
- TOEが提供する全てのインタフェースタイプ、及び全てのセキュリティ機能を網羅できるように考慮する

b. テスト概要

上記観点を考慮し、サンプリングテスト9件、独立テスト5件の評価者テストが実施された。評価者が実施した独立テストにおいて使用されたツール、テスト手法は開発者テストと同様のものが用いられている。

c. 結果

実施したすべての評価者独立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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した主な侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

- 意図しないネットワークポートインタフェースが存在し、そこからTOEにアクセスできる可能性がある、もしくはオープンポートへの不正なデータ送信により保護資産が暴露される可能性がある
- 保守インタフェース、テスト用インタフェース等通常使用されることが想定されないインタフェースを使用してセキュリティ機能をバイパスされる可能性がある
- 必要以上の情報がインタフェースから出力され、秘密情報が暴露される可能性がある
- メモリに対する物理的な操作により、セキュリティ機能がバイパスされる可能性がある
- 複数台の複合機が連携して処理を実施する際に、TOEが未設置の複合機から保護資産が漏えいする可能性がある
- 管理者パスワードの文字種の特殊な組合せが正しく検証されず、セキュリティ機能がバイパスされる可能性がある

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

・ポートスキャン用のツールを使用し、必要としないネットワークポートが開いていないことを確認する
・オープンポートに対する不正パケットの送信により、保護資産の暴露に繋がる脆弱性が存在しないことを確認する
・サービスマン用のインタフェースに対する操作からセキュリティ機能への侵害に繋がる脆弱性が存在しないことを確認する
・秘密情報の暴露に繋がる情報がTOEのインタフェースから出力されないことを確認する
・ROM基板、揮発性メモリボード、EEPROM搭載基板の差換え、抜き取り等によりセキュリティ機能のバイパスに繋がる脆弱性が存在しないことを確認する
・連結印刷実施時に、TOEが設置されない複合機から保護資産が漏えいしないことを確認する
・管理者パスワードの文字種の組合せが特殊であっても、セキュリティ機能がバイパスされないことを確認する

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告はとくにない。

4 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。

① 所見報告書でなされた指摘内容が妥当であること。
② 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評価報告書で示されたように評価されていること。
④ 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 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及び評価報告書において、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、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3に対する保証要件を満たすものと判断する。

5.2 注意事項

特になし。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）
TSFI	TSF Interface（TSFインタフェース）

本報告書で使用されたTOEに関する略語を以下に示す。

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	Electronically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM。
MFD	Multi Function Device — デジタル複合機。事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。
MSD	Mass Storage Device — 大容量ストレージ装置。本書では特にMFD内の、揮発性メモリの一部、および、Flashメモリを指す。
ROM	Read Only Memory — 読み出し専用メモリ。

本報告書で使用された用語の定義を以下に示す。

Flashメモリ	不揮発性メモリの一種で、電気的な一括消去および任意部分の再書き込みを可能にしたROM。
イメージデータ	本書では特に、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。
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。
ジョブ	MFDのコピー、プリンタ、スキャナ、ファクス送受信および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、スキャナおよ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。
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、機能キーおよ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はTOEのコントローラファームウェアに置き換えられる。
連結印刷	大量の印刷部数を、2台のMFDで折半することにより倍速でこなす機能。

7 参照

[1] MX-FR15 セキュリティターゲット バージョン 0.04 2010年3月10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 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] シャープ株式会社 MX-FR15 評価報告書 第2.8版 2010年5月14日
一般社団法人 ITセキュリティセンター 評価部