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19年12月4日** (IT**認証**7186)
認証番号	C0188
認証申請者	**シャープ株式会社**
TOE**の名称**	MX-FRX8
TOE**のバージョン**	Version M.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	**みずほ情報総研株式会社 情報セキュリティ評価室**

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20年10月30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。

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-FRX8 Version M.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-FRX8 Version M.10」（以下「本TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（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、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-FRX8
バージョン： Version M.10
開発者： シャープ株式会社

1.2.2 製品概要

本TOEはシャープ製デジタル複合機（Multi Function Device 以下「MFD」という。）MX-M850、MX-M860、MX-M950及びMX-M1100 内のデータ保護機能を持つIT製品（オプション製品）であり、その主要部分は、ROMに格納されたMFD用ファームウェア製品である。MFD内蔵ハードウェア部品であるHDC（Hard Disk Controller）がTOEに含まれ、ファームウェア部分から呼び出される。

MFDすなわち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。MFD内の標準ファームウェアROMを外し、本製品と交換して使用する。

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

本TOEは2枚のROM基板とHDCにより提供される。TOEの範囲を図1-1に網掛けで示す。

- コントローラファームウェア:
  コントローラ基板に搭載する2枚のROM基板に格納されており、コントローラ基板を制御するファームウェアである。MFDのオプション品として提供される。
- HDC
  コントローラ基板に実装されている1個の集積回路部品である。コントローラファームウェアの制御下で動作する。

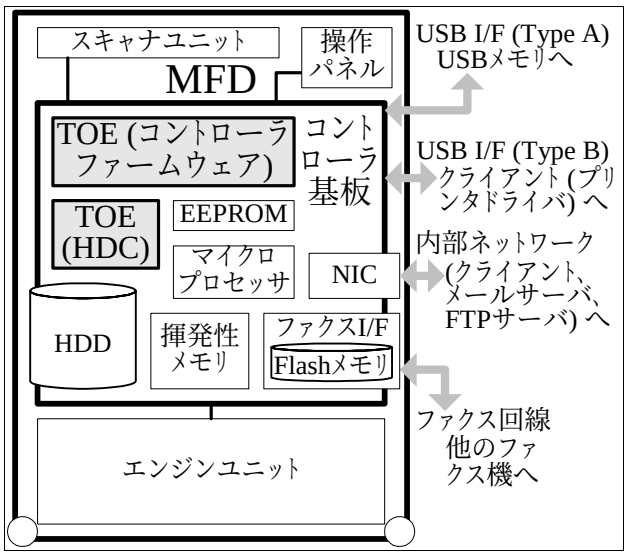

図 1-1 MFDの物理的構成とTOEの物理的範囲

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。図中、範囲を太い枠線内で示し、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、HDD、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。

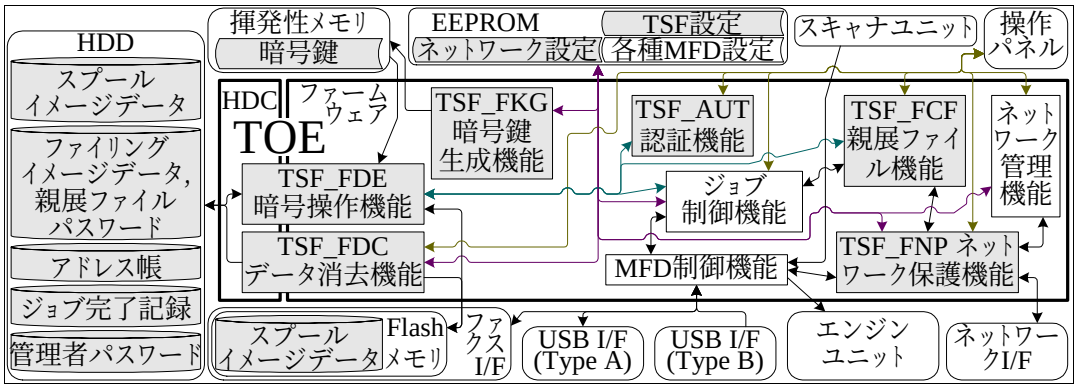

図 1-2　TOEの論理的構成図

TOEはイメージデータ等の利用者データを保護する目的で、以下の各機能を提供する。これらは、MFD内の不揮発性記憶装置 (HDD等) に保存あるいは残存する利用者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。また、当該利用者データをMFDがネットワーク (LAN) 経由で入出力する際、盗聴の試みに対抗することを目的とする。

a) 暗号操作機能

MFDがジョブ処理中のイメージデータをHDD等に一時的に書き込む際、また、利用者が文書のイメージデータをHDDにファイリング保存する際、書き込み前にデータを暗号化する。

b) データ消去機能

HDD等のイメージデータが用済みになった際、自動的に上書き消去する。MFD廃棄時もしくは運用中、必要に応じ、管理者の操作により全データを上書き消去する。

c) 親展ファイル機能

利用者がイメージデータをファイリングする際、パスワードによる保護を提供する。

d) ネットワーク保護機能

- IP/MACアドレスフィルタ機能

  ネットワーク経由の不正アクセスを拒む。

- SSL機能

  通信データを盗聴から守る。

1.2.3.3　TOE の保護資産

本TOEが対象とする保護資産は、以下の利用者データである。

- MFD機能がジョブ処理時にスプール保存するイメージデータ
- 利用者が親展ファイルとしてファイリング保存したイメージデータ
- アドレス帳データ
- ジョブ完了記録データ

- ネットワーク設定データ
- ネットワーク上の通信データ

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-FRX8 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、「MX-FRX8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、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20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。

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。
なお、攻撃者としては、以下の者を想定する。

- 脅威エージェント

  MFDの正規の利用者、または、第三者。

- 動機

  他人の文書のイメージデータ等、保護資産のいずれかを不正に入手する動機を持つ。

- 攻撃能力

  MFD及びTOEについて、取扱説明書を含む公開情報に基づく知識を有する。

表2-1 想定する脅威

識別子	脅 威
T.RECOVER	攻撃者がMSDをMFDから物理的に取り出し、簡単に入手することができるハードウェアやソフトウェアのツールを使用して、MSD内の利用者データ (削除後に残存しているデータを含む) を読み出し漏えいさせる。
T.REMOTE	MFDへのアクセスを認められていない攻撃者が、内部ネットワーク経由でMFD内のアドレス帳データを、まとめて読み出しまたは改変する。
T.SPOOF	攻撃者が、他の利用者になりすますことにより、操作パネルまたは内部ネットワーク経由で、利用者が親展ファイルとしてファイリング保存したイメージデータを、読み出し漏えいさせる。
T.TAMPER	攻撃者が、管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを、読み出しまたは改変する。
T.TAP	正当な利用者がMFDに対して通信する際、攻撃者が内部

	ネットワーク上を流れる利用者データを盗聴する。

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はない。

2.1.3 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2-2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2-2 TOE使用の前提条件

識別子	前提条件
A.NETWORK	MFDは、外部ネットワークからの攻撃から保護された内部ネットワークにおける、MFDとの通信を認める機器だけが接続されたサブネットワークに接続するものとする。(注) (注:MFDは、外部ネットワークからの攻撃から保護された内部ネットワーク内のサブネットワークに接続するものとし、当該サブネットワークにはMFDとの通信を認める機器だけが接続されていることを前提としている。)
A.OPERATOR	管理者は、MFD及び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。

表2-3 製品添付ドキュメント

	日本	日本以外
準備手続き	MX-FRX8 設置手順書 [TCADZ1969FCZZ]	MX-FRX8 Installation Manual [TCADZ1970FCZZ]
利用者操作	取扱説明書データセキュリティキット MX-FRX8 [CINSJ4234FC51]	MX-FRX8 Data Security Kit Operation Manual [CINSE4235FC51]
	注意書データセキュリティキット MX-FRX8 [TCADZ1967FCZZ]	MX-FRX8 Data Security Kit Notice [TCADZ1968FCZZ]

2.1.5 構成条件

本TOEは、シャープ製デジタル複合機 MX-M850、MX-M860、MX-M950及びMX-M1100で動作する。

2.2 セキュリティ対策

TOEは、2.1.1の脅威に対抗するために、以下のセキュリティ機能を具備する。

① 暗号鍵生成 (TSF_FKG)

本TSFは暗号鍵 (共通鍵) の生成を行い、利用者データ及びTSFデータの暗号化機能をサポートする。

本TSFは、TOE設置時にセキュアなシードを自ら生成し、このシードを元に、MFDの電源がオンになるたびに、128ビット長の鍵を生成する。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。生成した鍵は、揮発性メモリ内に保存し、電源オフにより消失する。

② 暗号操作 (TSF_FDE)

本TSFは、利用者データ及びTSFデータをMSDに書き込む必要が生じたときは、それらのデータを暗号化してから書き込む。また、それらのデータが必要になれば、MSDから読み出し、復号して利用する。暗号化及び復号には、暗号鍵生成 (TSF_FKG) により生成された暗号鍵を用いる。

対象となる利用者データは、HDD上及びFlashメモリ上にスプール保存されるイメージデータ、HDD上にファイリング保存されるイメージデータ、HDD上のアドレス帳データ及びジョブ完了記録データである。また対象となるTSFデータはHDD上の親展ファイルパスワード及び管理者パスワードである。

③ データ消去 (TSF_FDC)

本TSFは、スプール保存及びファイリング保存されたイメージデータファイル、またはアドレス帳データファイル、ジョブ完了記録データファイルを消去するデータ消去機能であり、以下のプログラムから構成される。各プログラムは、HDDではランダム値を1回以上、Flashメモリには固定値を1回上書きする。

a) 各ジョブ完了後の自動消去プログラム

ジョブ処理のためにHDD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、当該ジョブ完了または中止時に上書き消去する。また、ドキュメントファイリング機能 (親展ファイル機能を含む) によりHDDに保存されたイメージデータを、利用者の操作により削除される際に上書き

消去する。

b) 全データエリア消去プログラム

認証（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、HDD上にあるすべてのスプールイメージデータ及びファイリングイメージデータ、HDD上にあるジョブ完了記録データ、Flashメモリ上にあるすべてのスプールイメージデータを上書き消去する。アドレス帳データは消去しない。管理者の操作による全データエリア消去中断の場合、キャンセル操作を選択後に管理者認証を要求する。管理者はキャンセル操作により識別され、パスワードを入力することで認証される。パスワード入力時には入力文字を隠蔽する。この認証が連続３回の失敗した場合、認証入力受付を５分間停止する。

c) アドレス帳/本体内登録データ消去プログラム

認証（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、HDD上のアドレス帳データを上書き消去する。中止機能はない。

d) ドキュメントファイリングデータ消去プログラム

認証（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、HDD上にあるすべてのスプールイメージデータ/ファイリングイメージデータを上書き消去する。全データエリア消去プログラムと同様の中止機能を持つ。

e) ジョブ状況完了エリア消去プログラム

認証（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、HDD上のジョブ完了記録データを上書き消去する。中止機能はない。

f) 電源ON時の自動消去プログラム

TOEの電源ON時に上書き消去を実行する。ただし、スキャナまたはファクス送信の予約ジョブがある場合、及び未出力のファクス受信またはインターネットFax受信ジョブがある場合を除く。

電源ON時に本プログラムを実行するか否か、及び消去対象データは、予め設定された値に従う。消去対象データは、全データエリア消去プログラムの対象となるすべてのデータ、または指定されたHDDのデータのいずれかである。指定可能なHDDのデータは、スプールイメージデータ、ファイリングイメージデータ、及びジョブ完了記録データのうち一つ以上である。本プログラムは、全データエリア消去プログラムと同様の中止機能を持つ。

g) データ消去設定

上記の各プログラムに対し、認証（TSF_AUT）で識別認証された管理者に、以下の設定機能（問い合わせ、改変）を提供する。

- 各ジョブ完了後の自動消去回数

  各ジョブ完了後の自動消去プログラムのHDD上書き回数。1回以上7回以下。既定値は1回。

- データエリア消去回数

  全データエリア消去、アドレス帳/本体内登録データ消去、ドキュメントファイリングデータ消去、及びジョブ状況完了エリア消去の各プログラムのHDD上書き回数。1回以上7回以下。既定値は1回。

- 電源ON時の自動消去

  電源ON時の自動消去プログラムの、対象別有効設定。既定値はすべて無効。

- 電源ON時の自動消去回数

  電源ON時の自動消去プログラムのHDD上書き回数。1回以上7回以下。既定値は1回。

④　認証 (TSF_AUT)

本TSFは、管理者パスワードにより管理者の識別認証を行う。管理者パスワードは5～32文字の英数記号であり、認証に成功した場合のみ、データ消去設定や管理者パスワード変更等の管理者向け機能のインタフェースを提供する。

管理者は操作パネルまたはWeb画面から管理機能の呼び出し、または管理者ログイン操作により識別され、パスワードを入力することで認証される。パスワード入力時には入力文字を隠蔽、または隠蔽を要求する。また、連続して3回認証に失敗した場合、認証受付を5分間停止する。

⑤　親展ファイル (TSF_FCF)

本TSFはMFD内に利用者が親展ファイルとして保存したイメージデータをパスワード保護し、操作パネルまたはWeb経由での認証を経て再操作 (印刷等) を許す機能を提供する。親展ファイルパスワードは5文字以上8文字以下の数字である。

親展ファイルの再操作に先立つ親展ファイルパスワード認証では、入力文字を隠蔽し、連続して3回認証に失敗した場合、当該親展ファイルをロックする。

また、暗号化されたデータをクライアントのWebブラウザへエクスポートし、

暗号化されたデータも暗号化されていないデータも共に、クライアントのWebブラウザよりインポートする機能も提供する。

本TSFは以下のドキュメントファイリング機能に関する管理機能を持ち、認証（TSF_AUT）で識別認証された管理者が実行できる。

- ドキュメントファイリング禁止設定

  ジョブ種類別に各保存モードを禁止できる。親展でない (パスワードのない) モードをすべて禁止する設定が既定値であり、推奨値である。

- ホールド以外のプリントジョブ禁止設定

  プリンタドライバからのジョブに対し、その場での印刷出力を禁止する。ホールド指定のないジョブは拒否し、ホールドするジョブは印刷の有無を無視してホールドのみ行う。出力された用紙が第三者に持ち去られるリスクの高い環境において推奨される。

- 親展ファイルのロック解除

  親展ファイルパスワード認証失敗によりロックされた親展ファイルに対し、ロックを解除する。

⑥ ネットワーク保護 (TSF_FNP)

本TSFはネットワーク保護に関する以下の3機能を提供する。

a) フィルタ機能

IPアドレス及びMACアドレスに基づき、意図しない通信相手との通信を拒絶する機能である。識別（TSF_AUT）で識別認証された管理者が許可/拒否のIPアドレス（4つまでの範囲）、許可するMACアドレス（10個まで）を設定する。

b) 通信データ保護機能

クライアントとWebとの通信を、盗聴より保護するための、HTTPS通信機能と、クライアントのプリンタドライバから送信される印刷データを、盗聴より保護するための、IPP-SSL通信機能である。

c) ネットワーク設定保護

識別（TSF_AUT）で識別認証された管理者のみが、操作パネル及びWebからネットワーク設定データの設定を行う機能である。

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19年12月に始まり、平成20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20年6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・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20年6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。

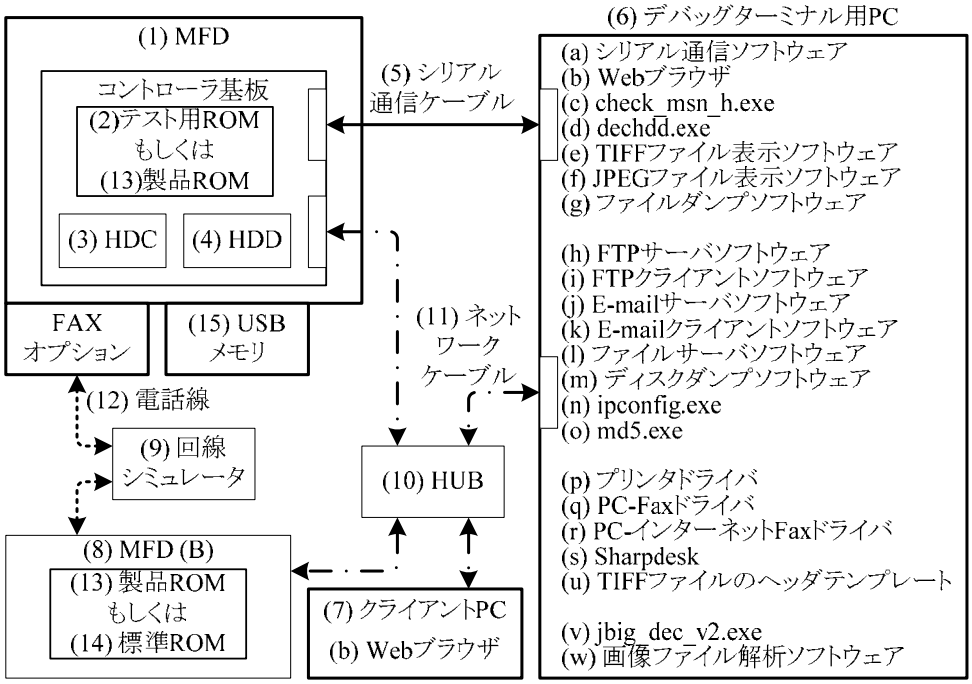

図3-1　開発者テストの構成図

開発者テストは本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。

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

開発者テストで実施されたテストの概要は以下のとおり。

開発者テスト構成図に示した環境下で、2種類のROMをテストの特性により使い分け実施した。

① 製品ROM

セキュリティ機能性が外部から観測可能なテスト。

② テストROM

暗号操作やデータ消去等のセキュリティ機能性が外部から観測不可能なテスト。デバッグターミナルPCから機能特性観察のためのコマンド操作や、内部情報を出力して確認する。

テスト手法は、開発者の手動操作により、MFDの電源のON/OFF、操作パネルでの操作、TOEのWebでの操作、論理的外部I/Fを刺激する操作（プリンタドライバの操作、PC-FAXドライバの操作、FAXでの操作)等、テストROMを用いたデバッグターミナルPCでの操作、及びテスト用に特別に行う操作（トレイを引き出す/戻す、HDの取り出し/接続、ファクス回線を外す/接続）

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51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、TOE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。

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。評価者テストは本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。

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、インタフェースに対する開発者テストの厳密性、十分性を補足するために以下の観点での独立テストを考案した。

① 開発者テストでは実施していないパラメタで、同じタイプのテストを行うことにより、インタフェースをさらに厳密にテストする。

② 開発者テストでは実施していないインタフェースの起動法を用いて、インタフェースを刺激し、同じタイプのテストを行うことにより、インタフェースをさらに十分にテストする。（特に論理的外部I/F）

③ 開発者テストでは実施していないモードで、同じタイプのテストを行うことにより、インタフェースをさらに十分にテストする。

④ 開発者テストでは実施していないテスト手法で、異なるタイプのテストを行うことにより、インタフェースをさらに十分にテストする。

⑤ 開発者テストでは実施していない初期条件で、同じタイプのテストを行うことにより、インタフェースをさらに十分にテストする。

⑥ 開発者テストのテストツールのみではインタフェースを刺激できない、またはインタフェースのふるまいを観察できないケースについて、特別のテストツールを用いることにより、インタフェースをさらに十分にテストする。

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

独立テストとして、31件のテストを実施した。テストの考案に当たっては、開発者テストで実施していないパラメタ（管理者パスワード、親展ファイルパスワードのバリエーション等）、インタフェースの起動法（USB接続によるプリントジョブの起動等）、モード（Fax夜間モード等）、テスト手法（Webからの同時操作等）、ならびに初期条件(ドキュメントファイリングデータのリストア直後等)を考慮することにより、開発者テストの厳密性、十分性を補足した。さらに、開発者テストで使用していないツール（OpenSSLコマンド、Wireshark等）を使用してインタフェースを刺激し、ふるまいを観察することにより、深さの観点（サブシステムの内部インタフェースのふるまい）も考慮した。独立テストは全てのセキュリティ機能を網羅し、インタフェースについては、TSFIの約半数に相当する28個のインタフェースをカバーした。カバーしていないインタフェース（データ消去の各タイプのインタフェース、一括印刷等のインタフェース等）は開発者テストで十分にふるまいを確認していることから、必要ないと判断した。

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、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。

公知の脆弱性の探索の結果からは、IPAの公開情報である、Webアプリケーションのチェックポイント7件（クライアント側スクリプトによる入力データのチェック、クロスサイトスクリプティング、セションＩＤの推測、クエリストリング等）を識別し、CEMの「一般的な脆弱性に関するガイダンス」の確認事項を証拠資料より探索を行って、バイパス、改ざんや誤使用に関する13件の侵入テストの候補となる脆弱性の識別を行った。

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。

上記、探索結果をもとに、Webアプリケーションのチェックポイントのテストに関しては、Webブラウザの設定（スクリプトの有効/無効）を変更したテストや、認証が必要なURLへの直接アクセスのテスト等のWebブラウザからのテストを実施した。バイパスに関しては、ポートスキャンツールを使用しての不要なポートの確認テストや、管理者がログインしている状態でMFDの状態を変更（電源断等）し、認証状態の不適切な継続テスト等を実施した。また、改ざんや誤使用に関しては、パスワードの特殊文字のテストや、MFDの操作パネルやWebからのアクセスの組み合わせによる同時利用の混乱のテスト、ネットワークプロトコル解析ツールを使用して、指定された暗号化通信が行われているかのテストを実施した。

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超える潜在的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特にない。

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）

本報告書で使用されたTOEに関する略語を以下に示す。

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。
HDC	Hard Disk Controller (ハード ディスク コントローラ)
HDD	Hard Disk Drive (ハード ディスク ドライブ)
HTTPS	HTTP over SSL — SSLにより保護されたHTTP。
IPP-SSL	IPP over SSL — SSLにより保護されたIPP。
LAN	Local Area Network (ローカルエリアネットワーク)
MFD	Multi Function Device – デジタル複合機、すなわちコピー機能、プリンタ機能、スキャナ機能、ファクス機能等を有する事務機。
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HDD及びFlashメモリを指す。
ROM	Read Only Memory (読み出し専用メモリ)
SSL	Secure Socket Layer – 計算機ネットワーク用暗号通信プロトコルの名称。
UI	User Interface (ユーザーインタフェース)

本報告書で使用された用語の定義を以下に示す。

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。
コントローラ基板	MFD全体を制御する基板。TOEのファームウェアを実行するためのマイクロプロセッサ、揮発性メモリ、HDC、HDD等を有する。
コントローラファームウェア	MFDのコントローラ基板を制御するファームウェア。ROM基板に格納してコントローラ基板に搭載する。

サブネットワーク	内部ネットワークのうち、ルータで区切られた範囲。
ジョブ	MFDのコピー、プリンタ、スキャナ、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。
ドキュメントファイリング	MFDが取り扱うイメージデータを、利用者が後で再操作(印刷、送信、等) できるようMFD内のHDDに保存する機能。
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。本報告書では特に、コントローラファームウェアを指す。
ホールド	プリンタドライバからのジョブを、ファイリング保存すること。
ホールド以外のプリントジョブ禁止	プリンタドライバからのジョブに対し、その場での印刷出力を禁止する。ホールド指定のないジョブは拒否し、ホールドするジョブは印刷の有無を無視してホールドのみ行う。
Flashメモリ	不揮発性メモリの一種で、電気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)。

7 参照

[1] MX-FRX8 セキュリティターゲット Version 0.07 2008年6月30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-2007-09-04 (平成20年3月翻訳第2.0版)

[13] MX-FRX8 評価報告書 2008年9月29日 みずほ情報総研株式会社 情報セキュリティ評価室