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3月31日** (IT**認証**9253)
認証番号	C0227
認証申請者	**シャープ株式会社**
TOE**の名称**	MX-FR11
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21年7月27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-FR11 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-FR11 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-FR11
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の主要部分は、ROM及びHDD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。MFD内蔵ハードウェア部品であるHDCがTOEに含まれ、ファームウェア部分から呼び出される。

MFD (Multi Function Device) 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。

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、親展ファイル機能、ネットワーク保護機能、ファクスフロー制御機能であり、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の主要部分はMFDのコントローラファームウェアである。これは2枚のROM及びUSBメモリにて提供される。セキュリティ機能の一部をMFDのHDC内に実装しており、これもTOEの範囲に含む。

- ROM
  コントローラファームウェアの一部を格納する。MFDにTOEを設置する際、コントローラ基板から標準ファームウェアROM 2枚を取り外し、代わりにDSKのROM 2枚を取り付ける。
- MAIN
  コントローラファームウェアの一部。DSKのUSBメモリからMFD内のHDDへ設置する。
- HDC
  1個の集積回路部品であり、コントローラ基板の一部として予めMFDに内蔵されている。

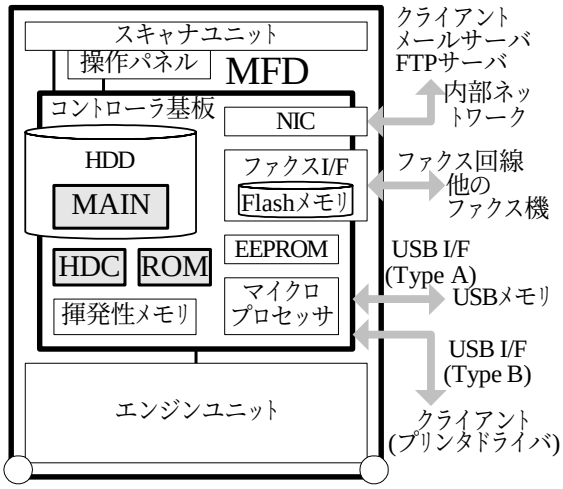

図1-1 MFDの物理的構成とTOEの物理的範囲

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、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。

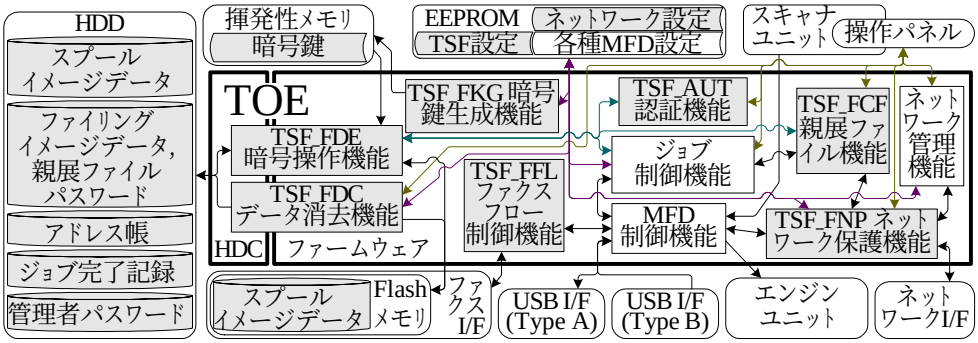

図1-2　TOEの論理的構成図

TOEの主要部分は、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。また、TOEセキュリティ機能 (TSF) の一部はHDC内に実装され、ファームウェア内のTSFから呼び出される。以下がセキュリティ機能である。

a) 暗号操作機能

MFDが扱うイメージデータ等をMFD内のHDDまたはFlashメモリに書き込む前に暗号化する。

b) 暗号鍵生成機能

暗号操作機能で使用する暗号鍵を生成する。

c) データ消去機能

MFD内のHDDまたはFlashメモリに保存された暗号データの領域に対し、ランダム値または固定値を上書きする。

d) 認証機能

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。

e) 親展ファイル機能

利用者がHDDにイメージデータをファイリング保存する際、他人が無断で再利用しないよう、パスワードによる保護を提供する。

f) ネットワーク保護機能

ネットワーク経由の不正アクセス、通信データの盗聴、及び、ネットワーク

設定の不正な改変を防ぐ。

g) ファクスフロー制御機能

MFDのファクスI/Fに接続される電話回線網から、MFDのネットワークI/Fを経由して内部ネットワークにアクセスすることを防ぐ。

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-FR11 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-FR11 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21年7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。

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からMSDを取り出し、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利用者データの領域は、少なくとも1回上書き消去されなければならない。 MSDにおいて、利用者が削除した利用者データの領域は、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の利用者データの領域はすべて、少なくとも1回上書き消去されなければならない。
P.FAXTONET	MFDのファクスI/Fに接続される電話回線網からは、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを、できないようにしなければならない。

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2-3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.NETWORK	TOEを搭載する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。
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。

日本向け	取扱説明書データセキュリティキット MX-FR11 [CINSJ4570FC51]	注意書データセキュリティキット MX-FR11 [TCADJ2013FCZZ]
日本以外向け	MX-FR11 Data Security Kit Operation Manual [CINSZ4571FC51]	MX-FR11 Data Security Kit Notice [TCADZ2014FCZZ]

2.1.5 構成条件

本TOEは、シャープ製デジタル複合機 MX-3600FN、MX-4100FN、MX-4100N、MX-4101FN、MX-4101N、MX-4101NJ、MX-5000FN、MX-5000N、MX-5001FN、MX-5001N及びMX-5001NJ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。

① 暗号鍵生成 (TSF_FKG)

TOE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。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、128ビット長及び256ビット長のセキュアな鍵を生成し、揮発性メモリ内に保存する。

② 暗号操作 (TSF_FDE)

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、必ず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。暗号鍵は、暗号鍵生成(TSF_FKG)で生成された鍵を用いて暗号操作を行う。

対象となる利用者データは、HDD上にスプール保存されるイメージデータ、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、HDD上の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、HDD上の管理者パスワードである。

③ データ消去 (TSF_FDC)

TOE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、以下のプログラムに含まれる。各プログラムともHDDにはランダム値を1回以上上書きする。また、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、HDD上にあるすべての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。

本プログラムを途中で中止する場合、キャンセル操作を選択後、管理者の

パスワード入力を必ず要求する。パスワード入力では、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。正しいパスワード入力の場合のみ、上書き消去を中止する。連続して3回認証に失敗した場合、管理者パスワードをロックする。ロックからの経過時間が5分に達すれば、自動的にロックを解除する。

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の操作により、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の操作により、HDD上のイメージデータを上書き消去する。対象データは、HDD上にあるすべてのスプールイメージデータ、HDD上にあるすべてのファイリングイメージデータの選択肢から一つ以上を、起動時に管理者が指定する。全データエリア消去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は、予め設定された値に従う。本プログラムを実行する際の消去対象データも同様である。消去対象データは、全データエリア消去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。全データエリア消去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のみに以下の設定機能(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を有効にする消去対象データの設定。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)

管理者パスワードにより管理者の識別認証を行う。長さ5文字以上32文字以下で、英字52種、数字10種、記号33種の95種の文字から成るパスワードのみを受け入れる。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。操作パネルでの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。

管理者パスワード認証において、連続して3回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が5分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

管理者のみに管理者パスワードの変更 (改変) 機能を提供することにより、役割の維持管理を図る。

⑤ 親展ファイル (TSF_FCF)

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。失敗回数は、各ファイルについて数える。認証に成功したとき、当該ファイルの失敗回数をゼロに戻す。ロックの解除は、認証(TSF_AUT)で識別認証された管理者

のみに許される。

再操作の一種として親展ファイルパスワード変更の機能を、本TSFで識別認証された親展ファイル保存者のみに提供し、新パスワードが5文字以上8文字以下の数字であることを検査する。また、属性変更の機能として、親展以外の属性に変更すれば、親展ファイルパスワードは削除される。この逆に、属性を親展に変更する場合、5文字以上8文字以下の数字からなる親展ファイルパスワードを要求する。

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する。本TSFはまた、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。

なお、以下のとおり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に実行を許す。

【親展ファイルによる保護の実効性を高めるための管理機能】

- 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に関する管理機能】

- 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)

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

管理者による事前の設定に基づき、意図しない通信相手との通信を拒絶する。IPアドレスによる条件とMACアドレスによる条件を設定できる。条件に合わない通信相手からのネットワークパケットを、必ず破棄し、レスポンス

及び処理をしない。

IPアドレスによる条件は、範囲を四つまで指定し、それらを許可するかまたは拒否するかを指定する。MACアドレスによる条件は、許可するMACアドレスを10個まで指定する

b) 通信データ保護機能

次の通信データ保護機能を提供する。

- クライアントとTOEのWebとの通信を、盗聴より保護できるよう、HTTPS通信機能を提供する。
- 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、盗聴より保護できるよう、IPP-SSL通信機能を提供する。
- クライアントとTOEとのSNMPを利用した通信を、盗聴より保護できるよう、SNMP v3機能を提供する。
- クライアントとTOEとのIPを利用したすべての通信を、盗聴より保護できるよう、IPsec機能を提供する。

上記設定の問い合わせ及び改変を、認証(TSF_AUT)で識別認証された管理者のみに許す。また、各通信の使用/未使用 (無効) の設定によって、ネットワーク保護機能の動作を変更することができる。

c) ネットワーク設定保護

ネットワーク設定データを扱うインタフェースを、操作パネル及びTOEのWebで提供する。これらのインタフェースは管理者のみに対して提供し、他の利用者のアクセスより保護する。

⑦ ファクスフロー制御 (TSF_FFL)

ファクス回線からの通信データに対し、内部ネットワークへ中継することを決して許可しないようなフロー制御を実施する。これにより、MFDのファクスI/Fに接続される電話回線網からの、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを防ぐ。

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4月に始まり、平成21年7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21年5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21年5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。

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。

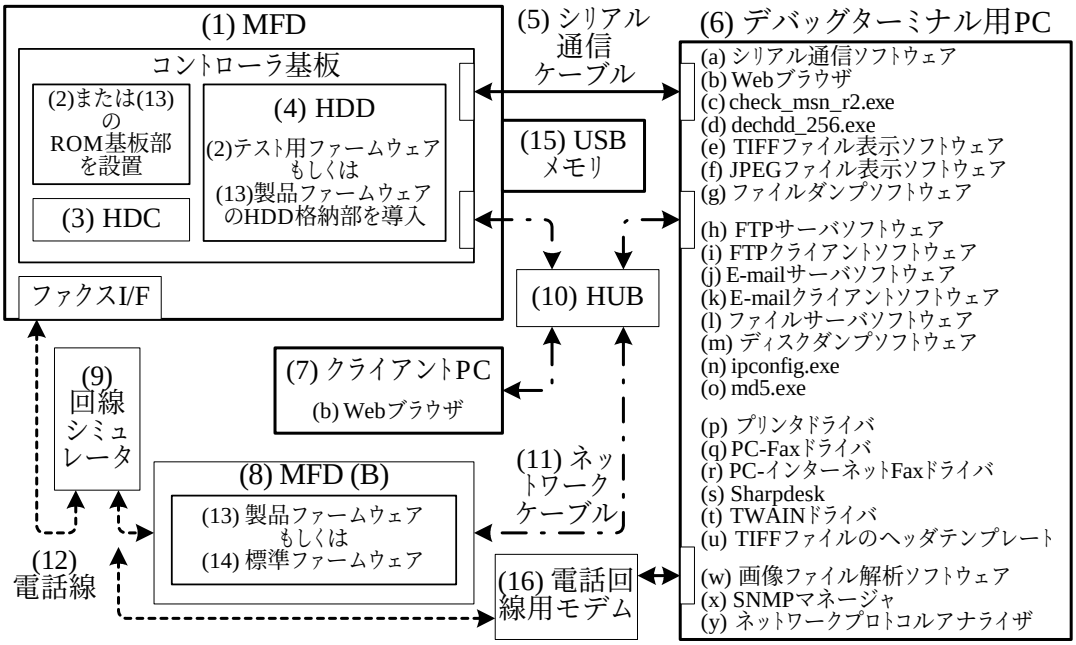

図3-1　開発者テストの構成図

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-4101FN)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

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。

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(クライアントPCからの観察、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62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。

- 主要なTSFIを選定することで、全てのTSFがテスト対象に含まれるようにサンプリングした。
- 開発者テストとは異なるパラメタやテスト方法(手順)を使用する。
- 各インタフェースのテストでは、考慮されていないと考えられるタイミング、及び操作において動作可能かの観点によるテストする。
- 操作パネルとWebブラウザのインタフェースタイプが存在するので、これらが網羅できるように考慮する。

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。

テストの種別	テスト対象TSFの数	項目数
評価者考案テスト	6	11
サンプリングテスト	(すべて)7	18
計		29

評価者考案テストにおいては、暗号鍵生成(TSF_FKG)を除く6つのセキュリティ機能が網羅されており、外部インタフェースは、操作パネル、Webブラウザ、ネットワークインタフェース及びファクスインタフェース経由の4種類のテストを実施している。テスト対象から除いた暗号鍵生成(TSF_FKG)機能は、TSFIが電源ONのみであり、このTSFIに対するテストはサンプリングテストで実施することから、対象からは外すこととした。評価者考案テストの具体的なテスト項目としては、PCリストア時の暗号化正常テスト、ドキュメントファイリング消去中止後の電源ON時の自動消去テスト、ファクスフロー制御受信拒否テストなどである。

サンプリングテストにおいては、7つすべてのセキュリティ機能が網羅されており、外部インタフェースは、電源ON、操作パネル、Webブラウザ、ネットワークインタフェース及びファクスインタフェース経由の5種類が含まれているため、サンプリングとしては十分である。

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、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、公知の脆弱性情報、公知の一般的攻撃、及び提供された証拠資料の情報より、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。

公知の脆弱性情報（JVN、US-CERT、CVE の各Webサイト）を情報源としたST等の証拠資料に示されたTOEの製品分類、機能に関連したキーワードによる分析結果からは侵入テストの候補となる脆弱性は検出出来なかったため、当該TOEのシリーズにおいて今回新規に追加した機能やネットワークに関する潜在的脆弱性を4件、IPA資料「脆弱性分析ガイダンス 第1.0版(2007年5月16日)」を参照して公知の一般的攻撃に基づく潜在的脆弱性を10件、証拠の探索に基づく潜在的脆弱性を10件、合計24件の侵入テストの対象とす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。

侵入テストでは、上記、探索結果をもとに24件のテストが実施された。

主な侵入テストは以下のとおりである。

① 公知の脆弱性情報に基づく潜在的脆弱性のテスト
- FTPでの保護資産のアクセスによる暴露がないことを確認する。
- IPsec、SNMPv3の設定におけるセキュリティ機能の無効化が起きないことを確認する。
- SSLポートへの無意味なパケット入力によるアクセスによってTOEが誤動作して保護資産が暴露されないことを確認する。

② 公知の一般的攻撃に基づく潜在的脆弱性のテスト
- サービスマン用のインタフェースからセキュリティが侵害されないことを確認する。
- 電源on後、コピースタートに表示された操作パネルの画面から秘密情報を取得できないことを確認する。
- 操作中にネットワーク接続が遮断された時に以降の消去が実施されることを確認する。

③ 証拠の探索に基づく潜在的脆弱性のテスト
- 連結コピー時、TOE未設置の子機でイメージデータの漏洩が起きないことを確認する。
- ROM差し替えによりセキュリティ機能が無効化されないことを確認する。
- 揮発性メモリ無で動作し暗号鍵が生成されずセキュリティ機能が無効化されないことを確認する。
- Webブラウザからの認証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 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。
② 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。
③ 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。

5 結論

5.1 認証結果

提出された評価報告書、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。

DSK	データセキュリティキットMX-FR11 – MFDの別売オプション品。TOEのファームウェア部分を含む。
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) – MFD内のHDCはTOEのハードウェア部分を含む。
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。
IPsec	Security Architecture for Internet Protocol — AH (Authentication Header) による完全性、認証機構、ESP (Encapsulated Security Payload) によるデータ暗号化、IKE (Internet Key Exchange protocol) による鍵交換から構成される、IPパケット単位でデータの改竄防止や秘匿機能を提供する通信プロトコルの名称。
MAC	Media Access Control (媒体アクセス制御) – 多数の通信機器が単一の通信媒体を共有できるよう、各機器を識別し、通信どうしが衝突しないよう調停する通信プロトコルの総称。
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、スキャナ機能及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ST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。

USB	Universal Serial Bus– IT機器間を接続するシリアルバス標準の名称。
SNMP	Simple Network Management Protocol ― ネットワーク機器を管理するための通信プロトコルの名称。
SNMP v3	SNMP version 3 ― ネットワーク上を流れるSNMPパケットを認証、暗号化することにより、盗聴、なりすまし、改ざん、再送などの危険から保護する機能を実装したSNMP。

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、電気的な一括消去及び任意部分の再書き込みを可能にしたROM (Flash Memory)。
IPアドレス	IPにおいて通信相手となる各機器を識別するための呼出符号。
MACアドレス	MACにおいて通信媒体上の各機器を識別するための呼出符号。
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、及びHDD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。本書では、ファイリングとも呼ぶ。
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。
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。

7 参照

[1] MX-FR11 セキュリティターゲット Version 0.03　2009年4月24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-FR11 評価報告書 第2.0版 2009年7月21日 一般社団法人 ITセキュリティセンター