認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付日（受付番号）	**平成19年3月14日** (IT認証7139)
認証番号	C0116
認証申請者	**シャープ株式会社**
TOEの名称	MX-FRX6
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19年8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　田渕　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。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「MX-FRX6 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 はじめに

この認証報告書は、「MX-FRX6 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-FRX6
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、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内に取り付けることにより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、データ消去機能、及び親展ファイル機能からなり、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。

暗号操作機能は、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。データ消去機能は、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。

親展ファイル機能は、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を付して保存することを可能とする。

1.2.3 TOEの範囲と動作概要

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。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。

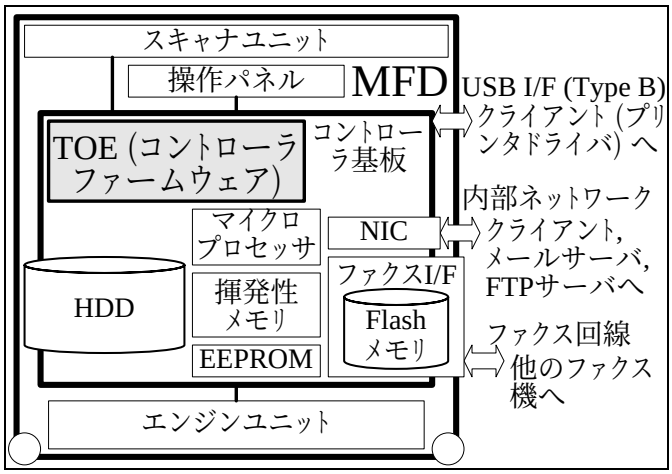

図1-1：MFDの物理的構成とTOEの物理的範囲

TOEの論理的構成を図1-2に示す。TOEの論理的範囲を太枠で示し、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。

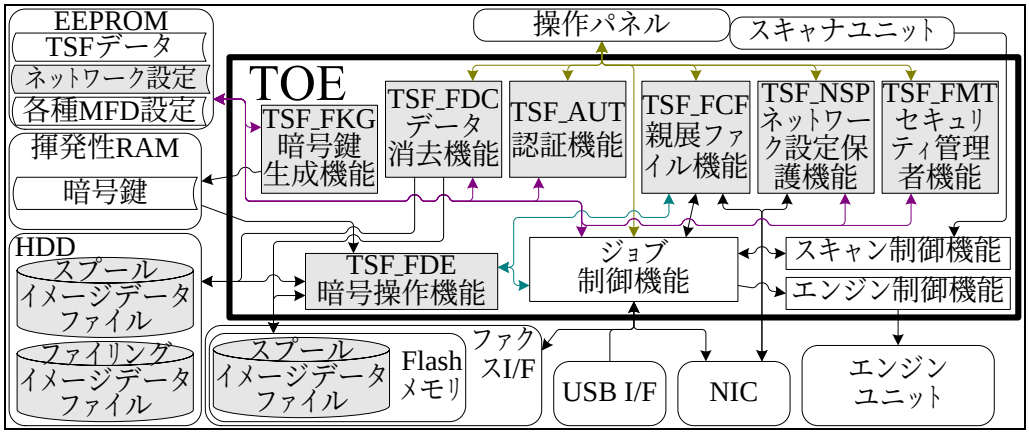

図1-2：TOEの論理的構成図

本TOEは、MFDの標準ファームウェアと同様にコピー、プリンタ、スキャナ、ファックス送受信及びPC-FAX等のMFD機能を持つ。TOEは各MFD機能の実行中にセキュリティ機能を実行する。

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)
MFD内のMSD (HDD及びFlashメモリ) を制御するデバイスドライバ機能に介在することにより, MSDに書き込む実イメージデータを暗号化し, MSDから読み出した実イメージデータを復号する。

b)暗号鍵生成機能 (TSF_FKG)
暗号操作機能 (前項) 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RAMに保存する。

c) データ消去機能 (TSF_FDC)
MFD内のMSDからの情報漏えいを防ぐため、データの上書き消去を実施する。データ消去の各プログラム（各ジョブ完了後の自動消去、全データエリア消去、ドキュメントファイリングデータ消去、及び電源ON時の自動消去)から構成される。

d)認証機能 (TSF_AUT)
操作パネルにおける管理者パスワードにより管理者の識別認証を行う。この認証により管理者は管理者パスワードを含むTSFデータの管理が可能となる。

e)セキュリティ管理者機能 (TSF_FMT)
TOE の運用に必要となる、管理者向けセキュリティ管理機能を提供する。

f) ネットワーク設定保護機能 (TSF_NSP)
MFDのネットワーク関連設定を、管理者以外が変更できないよう保護する。

g)親展ファイル機能 (TSF_FCF)
利用者がドキュメントファイリング機能によりMFD内に保存したイメージデータ（親展ファイル）を利用者が印刷、送信する際、パスワードによる認証を要求する。連続して3回認証を失敗した場合、親展ファイルをロックする。

h)スキャン制御機能
コピー、スキャン送信、ファックス送信、及びスキャン保存の際、原稿を読み取るため、スキャナユニットの制御を行う。

i) エンジン制御機能
コピー、プリンタ、ダイレクトプリント、ファックス受信、及び再操作の印刷の際、実イメージデータをエンジンユニットに転送し印刷を行わせる。

j) ジョブ制御機能
ジョブ機能、ドキュメントファイリング機能において、ユーザインタフェースを提供し、動作を制御する。ジョブをキュー管理し、ジョブの完了記録を HDD 内に保持する。

k)ジョブ機能
イメージデータをMFDのスキャナユニットまたは外部から受け取り、MFD内のMSDにスプールし、イメージデータをMFDのエンジンユニット(印刷)または外部(送信)へ送る。ジョブ制御機能、スキャン制御機能及びエンジン制御機能により実現される。

l) ドキュメントファイリング機能
MFD内のHDDにイメージデータを保存し、そのイメージデータを操作パネル経由またはクライアントよりWeb経由で再操作するための機能を提供する。本機能はジョブ制御機能能により実現される。

m)ネットワーク管理機能
TOE のネットワーク機能を使用するために、MFD に付与する IP アドレス、TOE が参照すべき DNS サーバの IP アドレス、その他のネットワーク関連設定を行う機能を提供する。

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「(日本語版) MX-FRX6 セキュリティターゲット　(英語版) MX-FRX6 Security Target」（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-FRX6 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。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19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、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が設置される内部ネットワークは、外部ネットワークからのセキュリティの脅威から保護されている。このような環境下で想定される攻撃は、MFD（TOEを含む）への直接アクセスによるものか、または内部ネットワークを経由したものに制限される。つまりインターネット越しで外部からの攻撃を幅広く受け付けることは想定されない。したがって、攻撃者の攻撃能力を低（low attack potential）と想定することは妥当であり、最小機能強度としてSOF-基本を主張することは妥当である。

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、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、乱数値から作成したシードを基に必ず暗号鍵（共通鍵）を生成する。暗号鍵は、暗号化アルゴリズムAES Rijndaelを実施するための暗号鍵生成アルゴリズムであるMSN-D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する。生成されるシードは、設置の際MFD 1台ごとに異なる値が生成される。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。また、生成した暗号鍵は揮発性メモリ内に保存する。

(2) 暗号操作機能(TSF_FDE)

利用者データ及びTSFデータをMSDに書き込む場合、必ず暗号化を行い、それらのデータ利用時には復号し利用する。対象となる利用者データ及びTSFデータは、MSDにスプール保存されるイメージデータ、親展ファイル機能により保存されるイメージデータ、及び親展ファイルパスワードである。データは、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、FIPS PUB 197に基づき、AES Rijndaelアルゴリズムにより暗号化及び復号される。

(3) データ消去機能(TSF_FDC)

MSDに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を消去する機能を提供する。HDD内の保存データ消去時は、ランダム値をセキュリティ管理者機能（TSF_FMT）において設定した回数、Flashメモリ内の保存データ消去時は、固定値を1回上書きする。本機能は下記4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
本機能は以下の通り、実イメージデータを上書き消去する。
- 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実イメージデータを、当該ジョブ完了時に上書き消去する
- 親展ファイル機能によりHDDに保存された実イメージデータを、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
操作パネルにおける管理者の操作により、HDDにスプール保存またはファイリング保存されている実イメージデータ、及びFlashメモリにスプール

保存されている実イメージデータに対する上書き消去を実行する。

本機能を途中で中止する場合、キャンセル操作を選択後、操作パネルにおける管理者パスワードの入力を要求する。操作パネルにおける管理者として識別認証された場合のみ、上書き消去を中止する。この操作パネルにおける管理者認証では、連続して3回認証に失敗した場合、認証入力受付を5分間停止する。

c) ドキュメントファイリングデータ消去
操作パネルにおける管理者の操作により上書き消去を実行する。その対象はHDDにスプール保存されているすべての実イメージデータ、HDDにファイリング保存されているすべての実イメージデータ、またはそれら両方のいずれかであり、操作パネルにおける管理者が指定する。本機能は、全データエリア消去と同様の中止機能を持つ。

d) 電源ON時の自動消去
TOEの電源ON時に上書き消去を実行する。ただし、スキャン送信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、本機能は実行されない。これらはガイダンスにて注意を喚起している。

電源ON時に本機能を実行するか否か、及び本機能を実行する際の消去対象領域はセキュリティ管理者機能(TSF_FMT)により設定される。また、本機能は全データエリア消去と同様の中止機能を持つ。

(4) 認証機能(TSF_AUT)

操作パネルにおける管理者パスワードにより、操作パネルにおける管理者の識別認証を行う。操作パネルにおける管理者パスワードは5文字の十進数字であり、認証に成功した場合のみ，TSF_FMTの各機能及びTSF_NSPのネットワーク設定UIにアクセスできる。

操作パネルにおける管理者パスワード入力時には入力文字を隠蔽し、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) セキュリティ管理者機能(TSF_FMT)

認証機能 (TSF_AUT) による識別認証の手順を経た後に、TOEの運用に必要となる、以下の管理者向けセキュリティ管理機能を提供する。

- 各ジョブ完了後の自動消去回数
- データエリア消去回数
- 電源ON時の自動消去
- 電源ON時の自動消去回数

- 操作パネルにおける管理者パスワードの変更
- ドキュメントファイリング再操作ロックの解除
- NICリセット（ネットワーク関連設定の工場出荷状態へのリセット）

(6) ネットワーク設定保護機能(TSF_NSP)

MFDのネットワーク関連設定を、管理者以外が設定できないよう保護する。本機能は、以下の2通りの設定機能で構成される。

- ネットワーク設定UI
  認証機能（TSF_AUT）における認証手順後にのみ操作が可能となるネットワーク設定UI
- ネットワーク管理ページ
  Web経由でのネットワーク設定機能を提供する管理ページ。ネットワーク管理ページへのアクセス時はWebにおける管理者の利用者識別名とパスワードによる識別認証を要求し、識別認証に成功した利用者のみにアクセスを許す。

ネットワーク設定データを改変する手段はTOEのROM内に実装された上記機能のみであるため、保護対象ネットワーク設定データは管理者以外による改変から保護される。

(7) 親展ファイル機能(TSF_FCF)

利用者が親展ファイルとして保存した実イメージデータを、そのデータの保存者が設定したパスワード（親展ファイルパスワード）により保護し、認証を経て再操作（印刷等）を許可する機能を提供する。親展ファイルパスワードは5文字の十進数字である。また本機能は、操作パネルまたはWeb経由で親展ファイル再操作を行う機能を提供し、その際にはパスワードが入力され、保存時に設定されたパスワードと一致することが確認された場合のみ再操作を許可する。

親展ファイルの再操作に先立つパスワード認証では、連続して3回認証に失敗した場合、そのファイルをロックし、再操作を禁止する。ロックの解除はセキュリティ管理者機能 (TSF_FMT)によって行う。

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	攻撃者がMFDから物理的にMSDを取り出し，MSD内の実イメージデータを読み出し再生する。
T.SHUNT	攻撃者がMFDのネットワーク関連設定を変更することにより、利用者がMFDに送信させようとしている実イメージデータを、攻撃者が攻撃の手段とする機材へ送信させる。
T.SPOOF	利用者がMFD内に保存している実イメージデータを、攻撃者がその利用者になりすますことにより、印刷または送信する。

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はない。

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-M350N，MX-M350NJ，MX-M350U，MX-M350UJ，MX-M450，MX-M450F，MX-M450N，MX-M450NJ，MX-M450U 及び MX-M450UJである。尚、型名にNを含まないMFDに関しては、HDDを含むシャープ純正オプションの装着が必要となる。

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1-2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1-2　TOE使用の前提条件

識別子	前提条件
A.NETWORK	TOEを設置するMFDは、盗聴されないようセキュアに管理された内部ネットワークに接続するものとし、外部ネットワークからの任意のアクセスを認めないよう保護されているものとする。
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。
A.USER	TOEを設置するMFDの利用者 (管理者を含む) は、パスワードを以下のように扱うものとする。 • パスワードには容易に推測可能な値を設定しない。 • パスワードは定期的に更新する。 • パスワードは安全に管理する。

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-FRX6、バージョン 0.03 (CINSJ3969FC51)

・注意書データセキュリティキット MX-FRX5 MX-FRX6、バージョン 0.03 (TCADZ1924FCZZ)

・MX-FRX6 Webヘルプ (全般)、2007/5/28

・MX-FRX6 Webヘルプ (ドキュメントファイリング)、2007/5/28

・MX-FRX6 設置手順書、バージョン 0.01 (TCADZ1928FCZZ)

(2) 海外版

・MX-FRX6 Data Security Kit Operation Manual、Version 0.03 (CINSE3964FC51)

・MX-FRX5 MX-FRX6 Data Security Kit Notice、Version 0.03 (TCADZ1925FCZZ)

・MX-FRX6 Web Help (General)、2007/5/28

・MX-FRX6 Web Help (Document Filing)、2007/5/28

・MX-FRX6 Installation Manual、Version 0.01 (TCADZ1929FCZZ)

なお、本TOEの使用にあたっては、MFD本体に付属する以下の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、バージョン 1
(TINSJ3679FCZZ)
・取扱説明書デジタル複合機 共通編/コピー編、バージョン 1
(TINSJ3658FCZZ)
・取扱説明書デジタル複合機 プリンタ編、バージョン 1
(MXM450-JP1-PRINTER)
・取扱説明書デジタル複合機 イメージ送信編、バージョン 1
(MXM450-JP1-IMAGE SEND)
・取扱説明書デジタル複合機 ファクス編、バージョン 3
(TINSJ2785FCZZ)
・MX-M350/MX-M450/MX-M350F/MX-M450F/MX-M350N/MX-M450N
をお使いのお客様へ [MXモデル向けファクス編補足]、バージョン 1
(TINSJ3720FCZZ)

(2) 海外版

・Laser Printer Administrator Settings Guide、
Version 1 (TINSE3682FCZZ)
・Laser Printer Operation Manual、
(for general information and copier operation)、Version 1
(TINSE3662FCZZ)
・Laser Printer Operation Manual (for printer)、
Version 1 (MXM450-EX1-PRINTER)
・Digital Multifunctional System Operation Manual (for image send)、
Version 1 (MXM450-EX1-IMAGE SEND)
・AR-FX12 Facsimile Expansion Kit Operation Manual、Version 3
(TINSE2791FCZZ)
・To Users of the MX-M350U/MX-M450U/MX-M350N/MX-M450N
[Notes for facsimile of MX-models]、Version 1 (TINSE3802FCZZ)

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3月に始まり、平成19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19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。

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。図中の(122)decode.exeは、テスト用の復号ソフトウェアを示す。また、(110)デバッグターミナル用PCに接続されている(12)HDDは、(10)MFD内蔵の(12)HDDを取り外してPCに接続したものである。

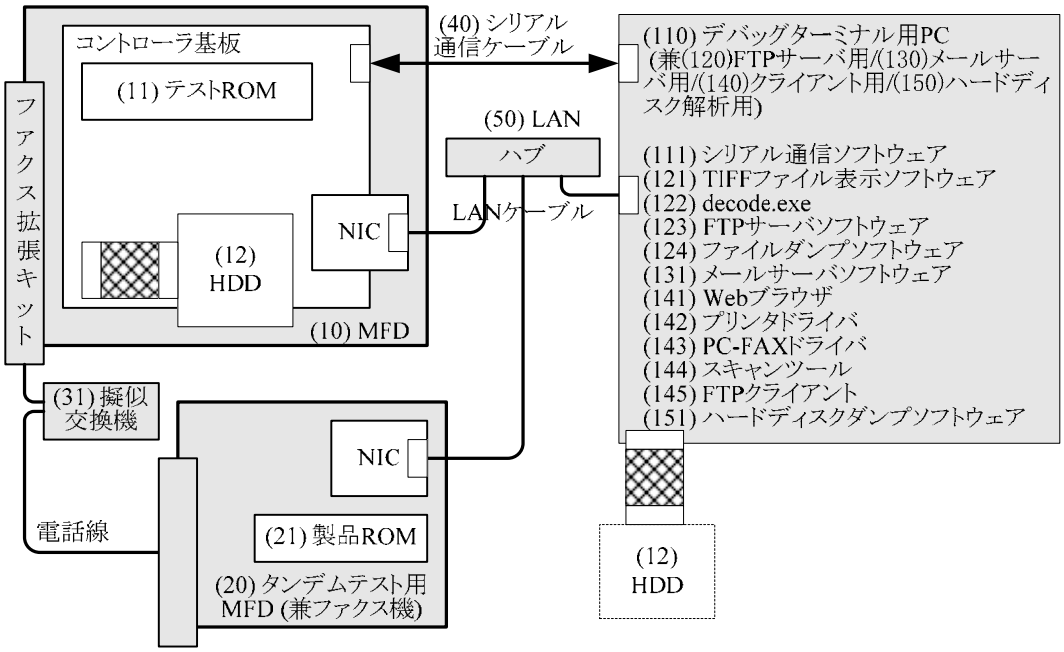

図2-1　開発者テストの構成図

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(10)MFDは、STで動作環境として識別されている複数のMFDの機種のうちの一部の機種(MX-M450N)がテストにおいて使用された。STで識別されるMFD間の違いは、エンジンスピードすなわち1分間当たりの印字速度に起因するものである。TOEのセキュリティ機能はMFDの印字速度とは無関係であり、TSFの実装はこれらの影響を受けない。よって本MFDのテスト環境で行われたテストは、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中の(11)テストROMは、STで識別されるTOEとは異なるが、これは製品ROM(TOE)にテスト用のデバッグ機能のみ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

テストには、以下の手法が使用された。

① MFD（操作パネル、電源など）を手動で操作することによりセキュリティ

機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

② TOEのWebを操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びTOEのWebの出力内容からセキュリティ機能のふるまいを観察する。

③ MFDに実イメージデータの読み取り・受信、及び印刷・送信を行わせることによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びMFDから取り外したHDDのダンプ内容からセキュリティ機能のふるまいを観察する。

c.実施テストの範囲

テストは開発者によって49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、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

評価者が実施した独立テスト、及び侵入テストの構成をそれぞれ図2-2、図2-3に示す。

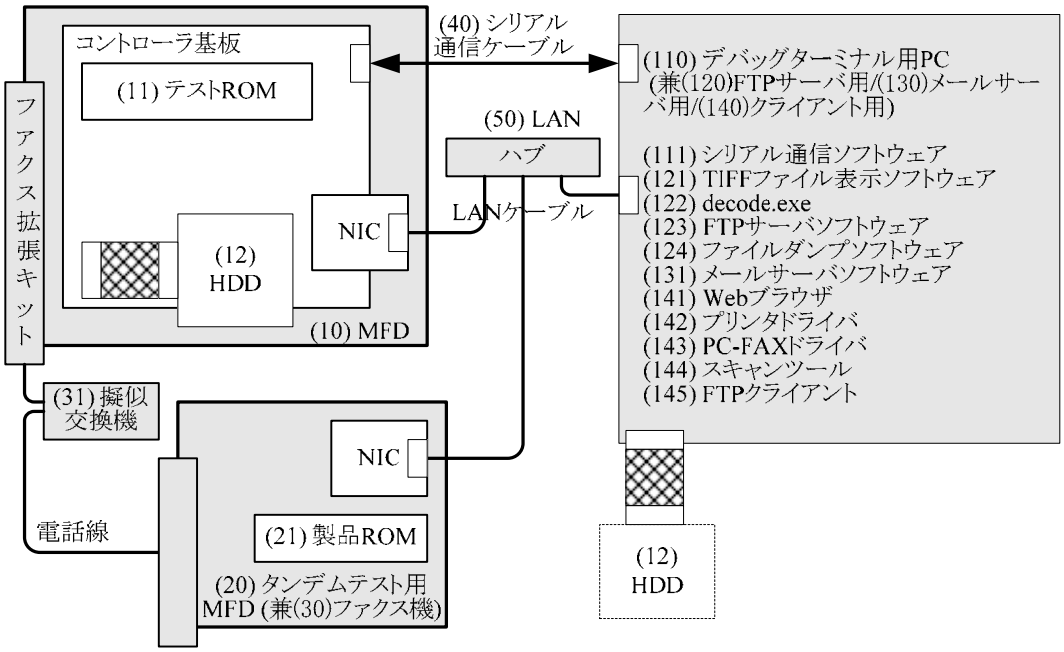

図2-2　独立テストの構成図

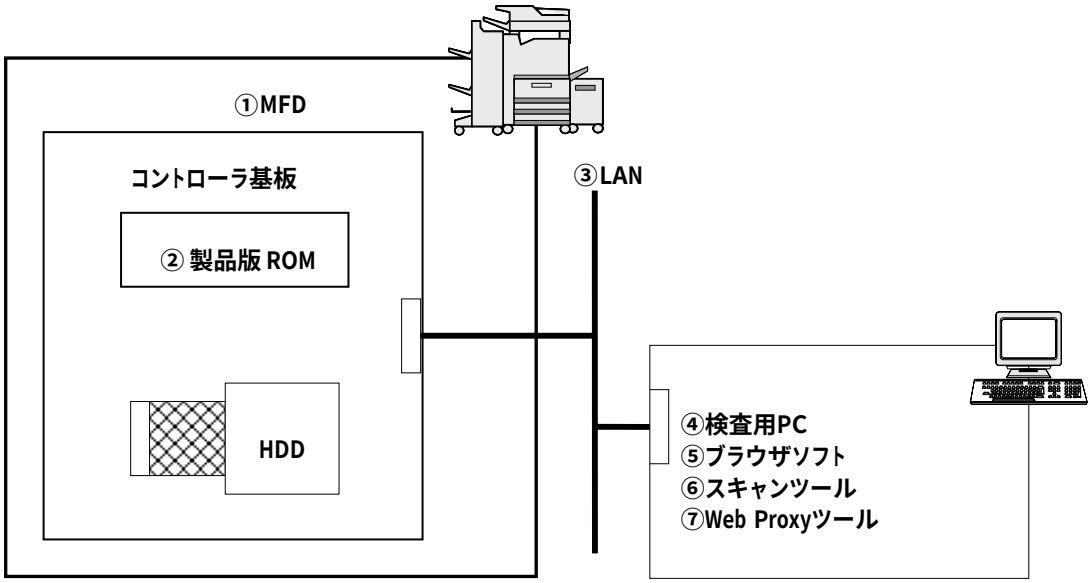

図2-3　侵入テストの構成図

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、及び図2-3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

テストには、以下の手法が使用された。

① MFD（操作パネル、電源など）を手動で操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

② TOEのWebを操作することによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、ログファイルの内容、及びTOEのWebの出力内容からセキュリティ機能のふるまいを観察する。

③ MFDに実イメージデータの読み取り・受信、及び印刷・送信を行わせることによりセキュリティ機能の外部インタフェースを刺激し、操作パネルへの表示内容、デバッグターミナルへの出力内容、及びログファイルの内容からセキュリティ機能のふるまいを観察する。

④ MFDのNICに対してポートスキャンを行い、その応答を観察する。

c.実施テストの範囲

評価者が独自に考案したテストを13項目、開発者テストのサンプリングによるテストを15項目、侵入テストを5項目、計33項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

【独自に考案した独立テスト】

① すべてのセキュリティ機能をテスト対象とすること

② すべての論理的TSFIをテスト対象とすること

③ 操作パネル一般UI及び操作パネル管理者UIの両方を対象とすること

④ セキュリティ機能が実施されるタイミング、使用されるパラメータの組み合わせ等を考慮し、開発者テストをより厳密にテストすべき内容を対象とすること

【開発者テストのサンプリングによるテスト】

① 開発者テスト項目数(49項目)の20%以上を確保すること
② すべてのセキュリティ機能を網羅すること
③ 対象とするMSDとして、スプール領域（HDD、Flashメモリ）及びファイリング領域（HDD）を含めること
④ 開発者テストの各分類（HDD取り外しテストを除く）からそれぞれ選択すること

【侵入テスト】
① TOEのWebへのアクセス時における認証セッションの脆弱性の確認
② 公知の脆弱性が顕在化していない論拠の実地検査

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。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 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。
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、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。
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。
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。
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ている。但し、過去の同系機の評価における実績、及び配布証拠資料の調査により実地検査は不要であると判断し、関係者へのインタビューをもって、実際に配付手続きが使用されていることを確認している。
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。
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。
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。
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。
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。
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。
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。
HDD	Hard Disk Drive (ハード ディスク ドライブ)。
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。
RAM	Random Access Memory — 任意順に読み書き可能なメモリ。
ROM	Read Only Memory — 読み出し専用メモリ。
UI	User Interface (ユーザインタフェース)。
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。
Webにおける管理者	TOEがリモート操作用に提供するWebで、成功裏に管理者として識別し認証された利用者。
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。

外部ネットワーク	組織の管理が及ばない、内部ネットワーク以外のネットワーク。
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。ジョブ完了の際、ジョブ中止の際、及び、ファイリングされたデータが利用者の操作により削除される際に、呼び出される。
管理者	組織の責任者の信頼を得て、TOEを含むMFDを管理する利用者。本利用者はWebにおける管理者あるいは操作パネルにおける管理者として、TOEを操作する。
揮発性	記憶装置に関し、電源を切れば記憶内容が消失する性質。
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。
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RAM, 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。
実イメージデータ	イメージデータファイルから管理領域を除いた実イメージデータ部分。
ジョブ	MFD機能 (コピー、プリンタ、ダイレクトプリント、スキャン送信, PC-FAX送信, ファクス送信、ファクス受信) 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。
親展ファイル	利用者がファイリング保存したデータのうち、他人に無断で再利用されないよう、パスワード (親展ファイルパスワード) によって保護されたもの。
親展ファイルパスワード	親展ファイルを、他人に無断で再利用されないよう、保護するためのパスワード。
親展ファイル保存者	イメージデータを親展ファイルとしてファイリング保存した利用者。
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、スキャン送信、ファクス送信及びスキャン保存の際に使用する。
スキャン保存	ファイリング機能の一つ。原稿を読み取って得たイメージデータをHDDに保存するが、印刷や送信は実行しない。

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が搭載しているすべてのMSDについて、保存されているすべての実イメージデータを上書き消去する処理。
操作パネル	表示部、ボタンキー、タッチパネル上に形成されたボタンを含む、利用者I/Fのためのデバイス。または、そのユニット。
操作パネルにおける管理者	操作パネルで成功裏に管理者として識別し認証された利用者。
操作パネルにおける管理者パスワード	操作パネルで管理者を認証する際に用いられるパスワード。
電源ON時の自動消去	MFDの電源ON時にMSD上のデータを上書き消去するための機能。管理者による事前の設定に基づき、MFDの電源ON時に呼び出される。
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STでは、ファイリングとも呼ぶ。
ドキュメントファイリングデータ消去	HDD上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。ファイリングされたイメージデータの消去が主な目的だが、スプールされたイメージデータの消去も可能。
内部ネットワーク	組織の内部にあり、外部ネットワークからのセキュリティの脅威に対して保護されたネットワーク。
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もコントローラファームウェアであり、TOE設置時に標準ファームウェアを取り外す。
ファイリング	ドキュメントファイリングの略。また、ドキュメントファイリング機能によりイメージデータを保存すること。
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)。
保護対象ネットワーク設定データ	MFDのネットワーク関連設定データのうち、本STが保護資産とするもの。
未消去データ	コピー、ファクスのジョブについて、ジョブのキャンセルを含み、

	ジョブの終了前に何らかのトラブルにより、MSD内に残存しているデータ。また、ジョブが正常に終了する前にスプール保存されているデータ。
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。
ロック	誤ったパスワードが連続して入力されたとき、パスワードの受付を停止する機能。

6 参照

[1] (日本語版) MX-FRX6 セキュリティターゲット バージョン 0.04（2007年7月10日）
シャープ株式会社
(英語版) MX-FRX6 Security Target Version 0.04 (2007-07-10) Sharp Corporation

[2] ITセキュリティ評価及び認証制度の基本規程 平成18年9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18年9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18年9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 2.3 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-FRX6 評価報告書 第1版 2007年7月12日
みずほ情報総研株式会社 情報セキュリティ評価室