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

申請受付年月日(受付番号)	**平成17年9月26日（IT認証5067）**
認証番号	C0054
認証申請者	**シャープ株式会社**
TOEの名称	MX-FRX1
TOEのバージョン	Version M.10
PP適合	**なし**
適合する保証要件	EAL3+ADV_SPM.1
TOE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18年9月5日

独立行政法人 情報処理推進機構
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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「MX-FRX1 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-FRX1 Version M.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。

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-FRX1
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、オプション製品であり、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、および、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の各ジョブにおいて、イメージデータをHDDまたはFlashメモリにスプールする前に暗号化する。データ消去機能は、コピー、プリンタ、スキャナ、ファクス送受信およびPC-Faxの各ジョブの完了後、スプールされている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。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のファームウェアアップグレードキットとして２枚のROM基板およびHDCにより提供される。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。

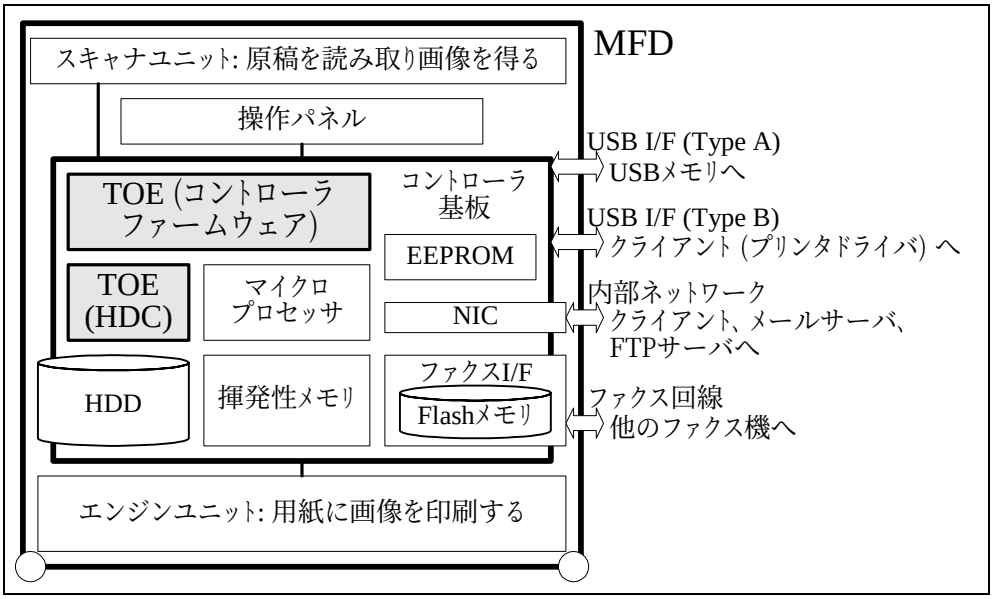

図1-1：MFDの物理的構成とTOEの物理的範囲

本TOEの論理的構成を図1-2に示す。図中、本TOEを太い枠線内として示す。長方形は本TOEの機能であり、角を丸くした長方形をハードウェアとして示す。本TOEの機能のうち、網掛け部がセキュリティ機能である。データの流れを矢印で示す。

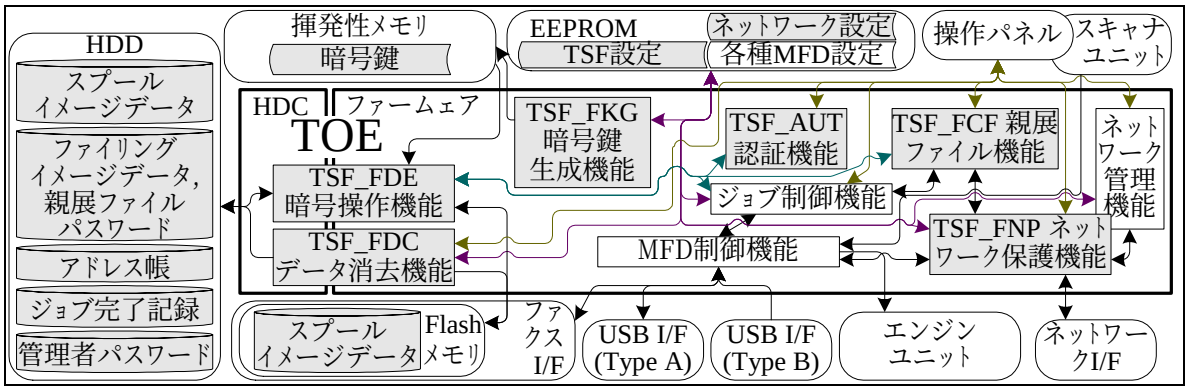

図1-2：TOEの論理的構成図

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

クス送受信およびPC-Fax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。TOEの機能およびMFD機能を以下に示す。

(ア) TOE機能

以下の機能が本TOEの論理的範囲に含まれる。

a) 暗号操作機能(TSF_FDE)

MFD内のHDDおよびFlashメモリに書き込む利用者データおよびTSFデータを暗号化する。また、HDDおよびFlashメモリから読み出すデータを復号する。

b) 暗号鍵生成機能(TSF_FKG)

暗号操作機能で提供する暗号化、及び復号の暗号鍵を生成する。生成された暗号鍵は、MFD内の揮発性メモリに保存する。

c) データ消去機能(TSF_FDC)

MFD内のHDDおよびFlashメモリ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、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、ジョブ状況完了エリア消去、および、電源ON時の自動消去) ならびに、その設定機能 (データ消去設定) からなる。各ジョブ完了後の自動消去は、MFD機能であるジョブ機能およびドキュメントファイリング機能 により呼び出される。

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。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) 親展ファイル機能(TSF_FCF)

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）を印刷や送信する際、利用者パスワード（親展ファイルパスワード）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。ロックは管理者のみが解除できる。

f) ネットワーク保護機能(TSF_FNP)

以下の３つの要素からなる。

・フィルタ機能
IPアドレスまたはMACアドレスによる通信相手の制限

・通信データ保護機能
SSLによるデータ保護。クライアントがSSLをサポートする必要がある。

・ネットワーク設定保護
ネットワーク管理機能を管理者のみに制限する。

g) ジョブ制御機能

MFD機能であるジョブ機能、アドレス帳機能および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。

h) MFD制御機能

各種MFDハードウェアの制御をし、通信を伴うジョブにおいて、送受信するデータとMFD内のイメージデータとの間でデータ形式を変換する。

i) ネットワーク管理機能

MFDのネットワークの機能を使用するための、アドレス、ポートおよびDNSの設定を行う管理機能。ネットワーク保護機能(TSF_FNP)により呼び出される。

(イ) MFD機能

MFD機能の多くはMFDの操作パネルを通じて行われる。一部の機能はリモート操作用Webの操作時あるいはデータ受信時に発動する。

a) ジョブ機能

イメージデータをMFDのスキャナユニット、FTP、USBメモリまたはファクス受信から受け取り、MFD内のHDDまたはFlashメモリにスプールする。スプールしたデータは印刷またはネットワークにより外部へ送信される。これはジョブ制御機能およびMFD制御機能により実現される。

b) ドキュメントファイリング機能

MFD内のHDDにジョブによるイメージデータを保存しておき、そのデータを再利用可能な状態にする。データの管理としてデータ上書き消去やバックアップおよび属性が指定されていた場合、親展ファイル機能の呼び出しを行う。

c) アドレス帳機能

送信先ファクス番号やEmailアドレスを登録しておき、送信の際の送信先指定をアドレス帳により行える機能。アドレス帳データはHDD内に保存され、操作パネルまたはリモート操作用Webから登録、変更または削除する。ジョブ制御により呼び出される。

(ウ) TOE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。

a) MFD機能がジョブ処理時にスプールするイメージデータ

利用者がMFD機能を利用したときに、TOE自身が各ジョブ処理のためにMFD内のHDDまたはFlashメモリに一時的に保存したイメージデータ。ジョブ完了時またはジョブキャンセル時の論理的削除がなされた後にも物理的にHDDまたはFlashメモリに残存するイメージデータを含む。

本データには各利用者にとっての重要情報が含まれる可能性がある。

b) 利用者が親展ファイルとしてファイリングしたイメージデータ

利用者がドキュメントファイリング機能時に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。利用者が削除操作をした後の物理的残存データも含む。

本データには各利用者にとっての重要情報が含まれる可能性がある。

c) アドレス帳データ

利用者がアドレス帳機能により登録しHDD内に保存されるアドレス帳データ。MFDの正当な利用者たちが共同で扱う個人情報（名前、メールアドレス、ファクス番号など）。操作パネルでの1件ずつの目視確認は可能とする。

d) ジョブ完了記録データ

ジョブ制御機能がプリンタドライバからの利用者名、文書名、ファクス送受信相手先などの情報をHDD内に保存するジョブ完了の記録データ。操作パネルでの１件ずつの目視確認は可能とする。

e) ネットワーク設定データ

MFDがネットワークに接続するために必要となるネットワーク設定に関する情報。本データが改ざんされた場合、意図しないネットワーク上への資産の流出やTSF機能への脅威となる可能性がある。

ネットワーク設定データは、TCP/IP設定（TCP/IP有効設定、DHCP有効設定、IPアドレス設定)、DNS設定（プライマリ/セカンダリDNSサーバ、ドメイン名）、WINS設定（WINS有効設定、プライマリ/セカンダリWINSサーバ、WINSスコープID）、SMTP設定（SMTPサーバ）、LDAP設定（LDAP有効設定、LDAPサーバ）、タンデム設定（子機IPアドレス、タンデム送信禁止）、ポート設定（各ネットワークサービスの有効設定、対応ポート番号）。

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「MX-FRX1 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][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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-FRX1 評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]のいずれか）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、本評価報告書、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18年8月の評価機関による本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

本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

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、外部ネットワークからの攻撃から保護された、一般のオフィス環境での利用を想定している。TOEへの直接的なアクセスあるいは内部ネットワークを経由した攻撃は、管理者による監視下にあり複雑な攻撃を想定されない。このため、攻撃者の攻撃力を“低レベル”とすることは妥当であり、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、利用者データおよび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、データセキュリティキット用暗号基準書に基づき、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-R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。MSN-R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を満たす暗号鍵生成アルゴリズムである。生成する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)

利用者データおよびTSFデータをHDDまたはFlashメモリに書き込む場合、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はHDD上、Flashメモリ上にスプールされるイメージデータ、HDD上に保存されるイメージデータ、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および管理者パスワードである。

データは、暗号鍵生成（TSF_FKG）により生成された128ビット長の暗号化鍵を用い、FIPS PUBS 197に基づき、AES Rijndaelアルゴリズムにより暗号化および復号される。

(3) データ消去機能(TSF_FDC)

TOEは、スプールおよびファイリング保存されたイメージデータファイル、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を有する。本機能は、以下のMFDのプログラムから呼び出される。

MFDの各消去プログラムは、HDDではランダム値をデータ消去設定で指定した回数、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メモリにスプールされたイメージデータを、該当ジョブ完了時に消去する。また、親展ファイル機能を含むドキュメントファイリング機能により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する際に上書き消去をする。

b) 全データエリア消去プログラム

認証(TSF_AUT)による識別認証された管理者により操作パネルから起動され、HDD上のスプールイメージデータ、ファイリング保存されたイメージデータ、ジョブ完了記録データおよびFlashメモリ上のスプールイメージデータが上書き消去される。なお、アドレス帳データは下記c)により消去する。

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。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)による識別認証された管理者により操作パネルから起動され、HDD上のアドレス帳データを上書き消去する。中断機能はない。

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)による識別認証された管理者により操作パネルから起動され、指定されたHDD上のスプールイメージデータ、ファイリング保存されたイメージデータを上書き消去する。全データエリア消去時と同様の中断機能を持つ。

e) ジョブ状況完了エリア消去プログラム

認証(TSF_AUT)による識別認証された管理者により操作パネルから起動され、HDD上のジョブ完了記録データを上書き消去する。中断機能はない。

f) 電源ON時の自動消去プログラム

TOEの電源ON時に自動的に消去対象データに対する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や未出力のファクス・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時に本プログラムを実行するか否か、および実行する消去対象データは予め設定する。消去対象データは、上記の全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上のデータである。指定可能なHDD上のデータは、スプールイメージデータ、ファイリングイメージデータおよびジョブ完了記録データのうちのひとつ以上である。本プログラムは中断機能を持つ。

g) データ消去設定

上記各消去プログラムに対し、認証機能(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　[1～7回：既定値 1回]

各ジョブ完了後に実施される自動消去プログラムのHDD上書き回数。

・データエリア消去回数　[1～7回：既定値 1回]

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、ジョブ状況完了消去共通のHDD上書き回数。

・電源ON時の自動消去有効化 [有効 / 無効：既定値 無効]

電源ON時の自動消去プログラムの対象別有効設定。

・電源ON時の自動消去回数 [1～7回：既定値 1回]

電源ON時の自動消去プログラムのHDD上書き回数。

(4) 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など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画面から識別および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。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) 親展ファイル機能(TSF_FCF)

ドキュメントファイリング機能により保存されるデータを、そのデータの保存者が設定したパスワードにより保護する機能を提供する。親展ファイルパスワードは5

～8文字の数字である。

利用者が当該データを再操作（プレビュー、印刷など）する際、操作パネルまたはWeb画面で親展パスワードを要求し、合致した場合のみ再操作を許す。パスワード入力時の入力文字は隠蔽する。また、連続して3回認証に失敗した場合、当該親展ファイルへの認証機能をロックする。

親展ファイルでは、以下の管理機能を持つ。いずれもTSF_AUTで識別認証された管理者のみが実行できる。

a) ドキュメントファイリング禁止設定：親展ファイルでないつまりパスワードを設定しない保存をすべて禁止する。ジョブ種類別に保存設定ができ、既定値および推奨値はドキュメントファイリング禁止である。

b) 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、ホールドジョブは印刷の有無に関わらずホールドのみ行う。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。

c) 親展ファイルロックの解除：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) ネットワーク保護機能(TSF_FNP)

ネットワークに関する以下の3つの機能を有する。

a) フィルタ機能

IPアドレスおよびMACアドレスに基づき通信を制限する機能。予め通信を拒否あるいは許可するアドレス条件を管理者により設定しておき、条件に合致するアドレスを持つパケットとの通信を拒否または許可する。

b) 通信データ保護機能

クライアントとのWeb通信の秘匿性を保つためにHTTPS通信機能を提供する。また、クライアントのプリンタドライバからの送信データの秘匿性保持のためのIPP-SSL通信機能を提供する。秘匿性は暗号化により実現し、採用されるアルゴリズムはRSA、DES、Triple-DES、AESおよびSHA-1である。

c) ネットワーク設定保護

MFDが通信するために必要なネットワーク設定データに対する操作をWebで提供する。操作の前にTSF_AUT機能により管理者の識別認証を行う。

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HDDまたはFlashメモリを取り出し、HDDまたはFlashメモリ内の利用者データ（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。

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	ジョブ完了または中止時、HDDまたはFlashメモリ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。 HDDまたはFlashメモリにおいて、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、HDDまたはFlashメモリ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。

1.5.7 構成条件

TOE が動作する MFD はシャープの MX-2300FG, MX-2300G, MX-2300N, MX-2300NJ, MX-2700FG, MX-2700G, MX-2700NおよびMX-2700NJ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.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。
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-FRX1 MX-FRX2

バージョン ：CINSJ3651FC51
対象者 ：管理者
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-FRX1

バージョン ：TCADZ1825FCZZ
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-FRX1 設置手順書

バージョン ：TCADZ1823FCZZ
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-FRX1 MX-FRX2 Data Security Kit Operation Manual

バージョン　：CINSZ3652FC51

対象者　　：管理者

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-FRX1 Data Security Kit Notice

バージョン　：TCADZ1826FCZZ

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-FRX1 設置手順書（英独仏西語版）

バージョン　：TCADZ1824FCZZ

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。

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パート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成17年10月に始まり、平成18年8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18年5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、同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。

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

開発者テスト環境

開発者が実施したテストの環境を図2-1に示す。

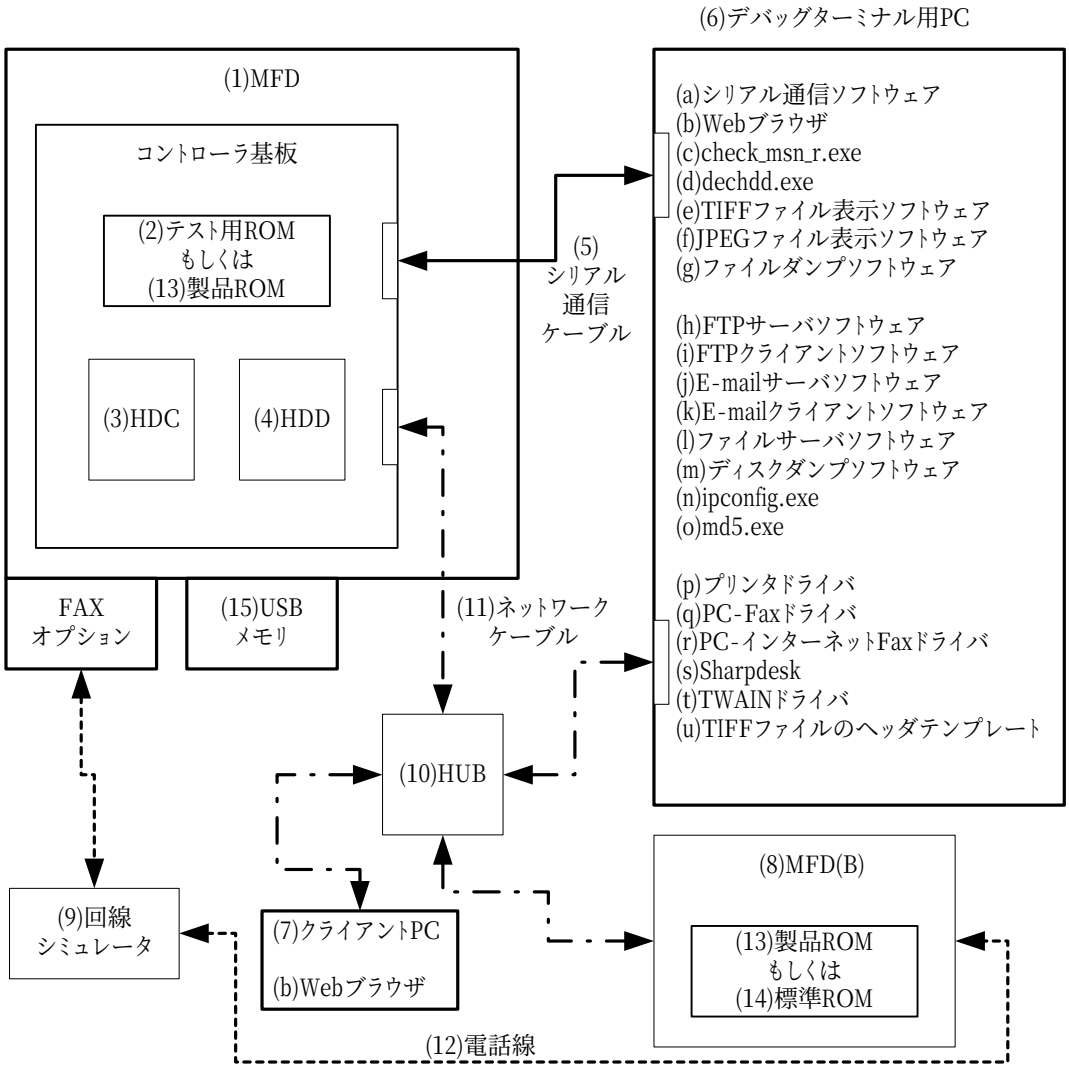

図2-1　開発者テスト及び評価者テストの構成図

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「(1)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-2700FG)がテストにおいて使用された。TOEの動作する各MFDでは、TOEの一部であるHDCが実装されるが、このHDC部分につ

いてはすべての機種で同等のものが使用される。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の「(2)テスト用ROM」はSTで識別されるTOEとは異なるが、これは製品ROM(TOE)に対し、テストの便宜のためにデバッグ機能の追加及び一部のセキュリティ機能の変更がなされたものである。テストの便宜のために変更されたセキュリティ機能に関しては、変更される前のセキュリティ機能が正しく動作することが製品ROMを使用してテストが行われた。したがって、テスト用ROMと製品ROMを使用して行われたテストは、STにおいて識別されたTOEをテストしたことと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。

①製品ROM使用

利用者が実際に使用する環境と同じ構成。

②テスト用ROM使用

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、HDDまたはFlashメモリ上の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。

テスト実施にあたっては、テストの特性に応じて使い分ける。標準的な外部インタフェースの入出力で確認を行うものについては製品ROM使用構成を用い、入出力の結果確認のため特殊なインタフェースが必要となる場合にはテスト用ROM使用構成を用いる。

c.実施テストの範囲

テストは開発者によって表2-1の63項目が実施されている。

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。

表2-1 開発者テスト概要

テスト分類	主なテスト対象TSF	項目数
事前テスト	なし	1
管理者認証テスト	TSF_AUT	4
鍵生成テスト	TSF_FKG	1

HDD内の暗号化格納、復号出力、消去テスト	TSF_FDE, TSF_FDC	24
Flashメモリの暗号化格納、復号出力、消去テスト	TSF_FDE, TSF_FDC	8
消去中止不能テスト	TSF_FDC	3
ドキュメントファイリング機能テスト	TSF_FCF	17
ネットワーク保護テスト	TSF_FNP	5

d.結果

評価者は以下のことを確認し、開発者テストは正しく実施された。

・開発者テストのTOEテスト構成がSTで定義されているTOEの構成と一貫している。

・開発者テストのテスト手法がTSF及びTSFIのふるまいを確認するために妥当である。

・開発者テストで実行されたテスト量と範囲について、TSF、TSFI及びサブシステムが網羅されている。

・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。

・テスト結果がすべて期待されたふるまいであり、残存問題はない。

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環境は、図2-1に示す環境と同等のものを用いた。

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

評価者テストは、開発者テストと同等の構成で実施された。

b.テスト手法

評価者が実施したテストは、開発者テストと同じ環境であり、下記の２種類の環境が存在する。

①製品ROM使用
利用者が実際に使用する環境と同じ構成。
②テスト用ROM使用

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、HDDまたはFlashメモリ上の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。

テスト実施にあたっては、テストの特性に応じて使い分ける。標準的な外部インタフェースの入出力で確認を行うものについては製品ROM使用構成を用い、入出力の結果確認のため特殊なインタフェースが必要となる場合にはテスト用ROM使用構成を用いる。

c.実施テストの範囲

評価者が独自に考案したテスト（評価者作成独立テスト）と、開発者テストのサンプリングによるテストを実施した。テストの対象となったセキュリティ機能と項目数は表2-2のとおり。

表2-2　評価者テスト範囲

テストの種別	テスト対象TSFの数	項目数
評価者作成独立テスト	5	10
サンプリングテスト	6（すべて）	19
計	11	29

評価者作成独立テストの考案においては、主要なセキュリティ機能を網羅すること、すべての外部インタフェースが含まれることを考慮した。ただし暗号生成機能(TSF_FKG)は、唯一のTSFIが電源ONによるものであり、運用中のセキュリティ機能の使用度合いからもサンプリングテストのみで実施することとした。

サンプリングテストについては、すべてのセキュリティ機能とTSFIが含まれるものとし、同様機能については代表的なデータを抽出し、開発者テストの30%を越えるテスト項目を実施した。

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

本評価報告書をもって、評価者は本TOEがCEMパート2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

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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本評価報告書において、所見報告書及び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

提出された本評価報告書、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。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.1.2E	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。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_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。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_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。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.1.1E	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、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。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_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理路整然とし、完全であり、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。
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。IT環境の要件は規定されていない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_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理路整然とし、完全であり、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。
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要約仕様の記述が理路整然とし、完全であり、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。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。
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。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。
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、実地検査及び録画された音声・映像の検査により確認している。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。
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。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。
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。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。
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環境に対する要求はないためIT環境に対する要件は不適用であること、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。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。
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において明示的方針をもたないこと、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	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いることを確認している。IT環境に対するセキュリティ要件はないので、それに関しては管理者ガイダンスへの記述は不要であ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。

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、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いることを確認している。対応すべき機能や特権に関する警告、IT環境に対するセキュリティ要件は、それらの記述が不要であ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。
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。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。
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。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。
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。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。
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。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。
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。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。
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。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。
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
AES	Advanced Encryption Standard NIST(米国商務省標準技術局)で制定され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
HDC	Hard Disk Controller
HDD	Hard Disk Drive
I/F	Interface
IPP	Internet Printing Protocol 印刷用通信プロトコル
IPP-SSL	IPP over SSL SSLにより保護されたIPP
LDAP	Lightweight Directory Access Protocol ディレクトリサービス用通信プロトコル
OS	Operating System
ROM	Read Only Memory
SMTP	Simple Mail Transfer Protocol
WINS	Windows Internet Name Server NetBIOS名からIPアドレスを求める機能

本報告書で使用された用語を以下に示す。

イメージデータ	MFDにてコピー、プリント、スキャン、もしくはファクス送信のため、原稿画像を読み込みデジタル化したデータ。PC-Fax、ファクス送信、ファクス受信においては、電話回線への送信、もしくは電話回線から受信したデータを含み、このデータをMFDで取扱可能な様に変換したデータもイメージデータと呼ぶ。
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。
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。
再操作	ファイリング保存したイメージデータに対する印刷等の操作。
サブネットワーク	内部にルータを含まない単一ネットワーク。
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、他人に利用されないようパスワードによって保護されたもの。
ジョブ	MFD機能（コピー、プリント、スキャン送信、PC-Fax、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。
スプール	入出力効率化のため、ジョブのイメージデータを一時的にHDDまたはFlashメモリに保持すること。スプール保存。
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、ユーザI/Fのためのデバイス。または、そのユニット。
タンデム	印刷の効率化のため、2台のMFDで作業を折半すること。
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、利用者が後で利用可能なようにMFD内のHDDに保存する機能。ファイリング。
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。

ホールド	プリンタドライバからのジョブを、ファイリングすること。
メモリ	記憶装置、特に半導体素子による記憶装置。
揮発性メモリ	電源を切ると記憶内容が失われるメモリのこと。
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メモリのこと。半導体素子、あるいは磁気記憶を用いたものがある。
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
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-FRX1　セキュリティターゲット Version 0.14 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17年7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17年7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17年7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 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 :1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2 :1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999　Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版 及び 補足-0407

[22] MX-FRX1 評価報告書 第2.4版 2006年8月28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