認　証　報　告　書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

IT製品（TOE）

申請受付日（受付番号）	平成29年12月11日（IT認証7656）
認証識別	JISEC-C0597
製品名称	MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U
バージョン及びリリース番号	0210zc00
製品製造者	シャープ株式会社
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (認証識別: JISEC-C0553)
保証パッケージ	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1
ITセキュリティ評価機関の名称	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30年5月22日

技術本部
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　真鍋 史明

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 3.1 Release 4
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

評価結果：合格

「MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U 0210zc00」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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

この認証報告書は、シャープ株式会社が開発した「MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U バージョン 0210zc00」（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。）が平成 30 年 4 月に完了した 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 に関心を持つ調達者や消費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、第 10 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は第 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、CC パート 3 の以下の保証コンポーネントである。

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

1.1.2 TOEとセキュリティ機能性

本 TOE は IT 製品であり、コピー機能、プリンター機能、スキャナー機能、文書を保存/取り出す機能（本 TOE では、「ドキュメントファイリング機能」という。）等を備えたデジタル複合機（以下「MFD」という。）である。

本 TOE は、MFD が扱うデータの暴露や改ざんを防止するために、MFD 用のプロテクションプロファイルである Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 [14][15]（以下「適合 PP」という。）が要求するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で CEM に基づく評価と適合 PP の保証アクティビティに基づく評価が行われた。

本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威

本 TOE は、以下の脅威を想定している。

TOE の保護資産であるユーザの文書データ及びセキュリティ機能に影響するデータは、TOE の操作や、TOE が接続されているネットワークへのアクセスにより、不正に暴露や改ざんされる脅威がある。

また、TOE 自身の故障や、不正なソフトウェアのインストールにより、TOE が持つセキュリティ機能が損なわれる脅威がある。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

TOE は､不正な物理的アクセスが制限され､インターネットから保護された LAN に接続される環境で運用されることを想定している。

運用中の TOE の維持管理は、調達者から信頼されている管理者がガイダンス文書に従って適切に行わなければならない。また、TOE の利用者は、安全に TOE を使用するよう訓練を受けていなければならない。

1.1.3 免責事項

本評価では、以下に示す運用は保証の対象外である。

- 「4.3 運用環境における TOE 範囲」で示す TOE の運用環境がセキュアではない状態での運用
- 「7.5 評価構成について」で示す条件以外での TOE の運用

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 30 年 4 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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識別

本 TOE は、以下のとおり識別される。

TOE名称： MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U
バージョン： 0210zc00
開発者： シャープ株式会社

TOE 名称は、MFD の本体と必須オプションで構成される。TOE の構成品を表 2-1 に示す。

表 2-1 TOEの構成品

本体			必須オプション
型番	ファクス機能	販売地域	
MX-M6070, MX-M5070, MX-M4070, MX-M3570, or MX-M3070	オプション	日本以外	MX-FR57U

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

製品のガイダンスの記載に従って、TOE の筐体と操作パネルに表示された以下の情報を確認する。

・本体型番： 筐体に表示されている本体型番が、表 2-1 の「型番」に含まれる名称であること

・ファクス機能： 操作パネルに表示されるファクス機能が、表 2-1 の「ファクス機能」のとおり“オプション”であること

・必須オプション： 操作パネルに表示されるオプション名が、表 2-1 の「必須オプション」に含まれる名称と一致すること

・TOE バージョン： 操作パネルに表示される TOE バージョンが、TOE 識別のバージョンと一致すること

3 セキュリティ方針

本 TOE は、コピー機能、プリンター機能、スキャナー機能、ドキュメントファイリング機能といった MFD の基本機能を提供しており、利用者の文書データを TOE 内部に保存したり、ネットワークを介して利用者の端末や各種サーバーとやりとりしたりする機能を持つ。

TOE は、適合 PP の要求を満足する以下のセキュリティ機能を提供する。

・利用者を識別認証する機能
・利用者データをアクセス制御する機能
・利用者データ等を暗号化して保存する機能
・LAN 利用時に通信経路上の利用者データを保護する機能
・セキュリティ管理を識別認証された利用者に制限する機能
・セキュリティ関連事象のログを記録する機能
・アップデートファームウェアを検証しインストールする機能
・起動時にセキュリティ機能が正常に動作することを検証する機能
・コピー機能等の処理中のデータを完了または中止時に上書き消去する機能
・利用者データ等を完全消去する機能

本 TOE の基本機能とセキュリティ機能の詳細は、5.1 節に示す。

TOE が想定する利用者役割、保護資産、脅威、組織のセキュリティ方針の詳細を 3.1 節から 3.4 節に示す。

3.1 利用者の役割

TOE の使用において、表 3-1 に示す利用者を想定する。

表 3-1 利用者の役割

名称	定義
U.NORMAL (一般利用者 / a normal user)	識別され、認証された利用者で、管理者役割を持たない利用者。
U.ADMIN (管理者 / an administrator)	識別され、認証された利用者で、管理者役割を持つ利用者。

3.2 保護資産

TOE の保護資産は、以下の表 3-2 の 2 種類に分類できる。 2 種類の保護資産のうち、利用者データは表 3-3、TSF データは表 3-4 のように、それぞれさらに 2 種類の保護資産で構成される。

表 3-2 TOEの保護資産

名称	種別	定義
D.USER	利用者データ	TSFの操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ。
D.TSF	TSF データ	TSFの操作に影響を与えるかもしれないTOEのためのTOEによって作成されたデータ。

表 3-3 保護資産(利用者データ)

名称	種別	定義
D.USER.DOC	利用者文書データ	電子的またはハードコピーの形式で、利用者の文書に含まれる情報
D.USER.JOB	利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報

表 3-4 保護資産(TSFデータ)

名称	種別	定義
D.TSF.PROT	保護された TSF データ	データの所有者でもなく、または管理者役割も持たない利用者によって、改ざんされた TSF データが TOE のセキュリティ影響を及ぼすかもしれないが、暴露については容認できるような TSF データ。
D.TSF.CONF	秘密の TSF データ	データの所有者でもなく、管理者役割も持たない利用者によって、暴露または改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないような TSF データ。

3.3 脅威

本 TOE は、表 3-5 に示す脅威を想定する。

表 3-5 想定する脅威

名称	定義
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 組織のセキュリティ方針

本 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 3-6 に示す。

表 3-6 組織のセキュリティ方針

名称	定義
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

名称	定義
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 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 4-1 前提条件

名称	定義
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 運用環境と構成

本TOEはオフィスに設置され、組織の内部ネットワークであるLANで接続され、同様にLANに接続されたクライアントPC及び各種サーバーと利用される。本TOEの一般的な運用環境を図 4-1 に示す。

ユーザは、TOE の操作パネル、LAN に接続された PC を操作して本 TOE を使用する。

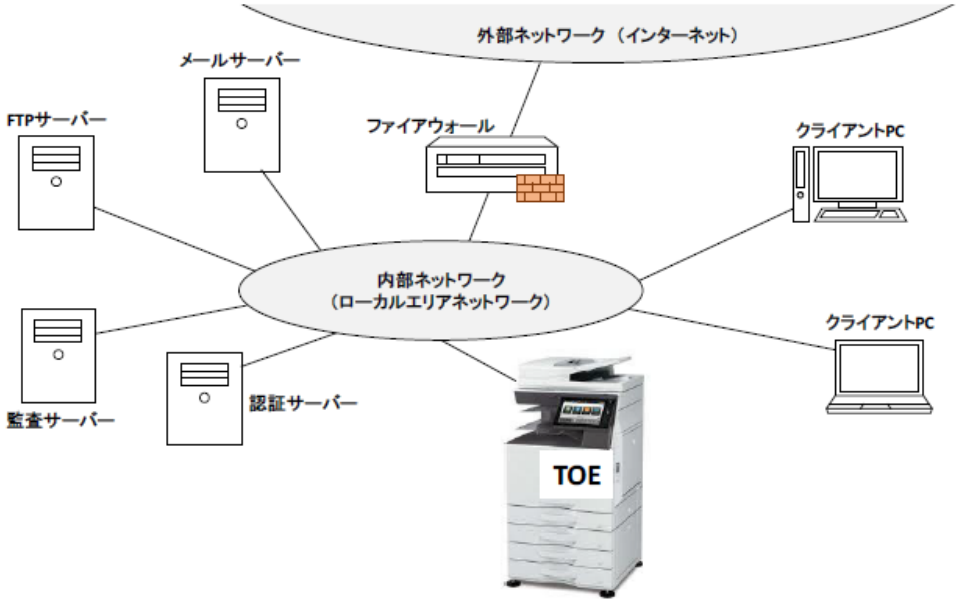

図 4-1 TOEの運用環境

TOE の使用環境の構成品について以下に示す。

(1) クライアント PC

ユーザが使用する汎用の PC である。

TOE の使用には、以下のソフトウェアが必要である。

・プリンタドライバ

名称は、「SHARP <本体型番> PCL6 ドライバー」である。 ここで、“<本体型番>”は、表 2-1 の本体型番のいずれかである。

・Web ブラウザ

(2) 監査サーバー

本 TOE により生成された監査ログを保存するために監査サーバーである。syslog プロトコルを使用し、TLS v1.2 に対応していなくてはならない。 本サーバーの設置は、必須である。

(3) 認証サーバー

5.1.2 節の「識別認証機能」で示す「外部認証方式」の場合、TLS v1.2 に対応し、認証プロトコルが LDAP 認証方式の認証サーバーが必要である。

(4) メールサーバー

「スキャナー機能」で、スキャンして読込んだ利用者文書データを E-mail 添付ファイルとして送信する場合に必要である。TLS v1.2 に対応していなくてはならない。

(5) FTP サーバー

「スキャナー機能」で、スキャンして読込んだ利用者文書データを指定のFTP サーバーに送信する場合に必要である。TLS v1.2 に対応していなくてはならない。

なお、本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本 TOE では、設置が必須である監査サーバー以外にも、認証サーバー等のサーバーを設置する場合がある。 また、外部ネットワークであるインターネットとの接続にはファイアウォールの設置が必要である。 これらのサーバー及びファイアウォールがセキュリティ対策方針に則りセキュアに運用されることは、運用者の責任となる。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。図 5-1 の TOE と示されている枠線で囲まれている部分が TOE であり、監査サーバー、メールサーバー、FTP サーバー、認証サーバー、クライアント PC、利用者は含まれない。

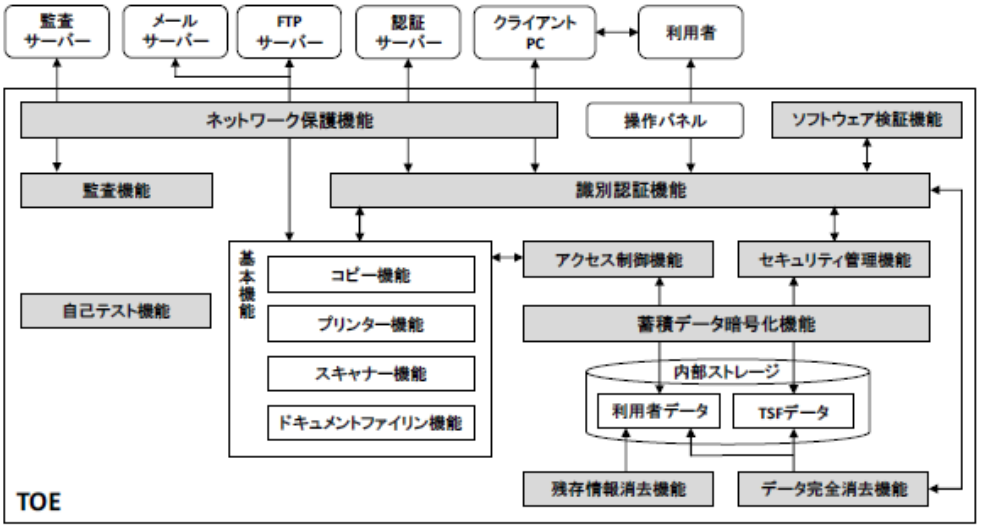

図 5-1 TOE境界

図 5-1 の TOE の基本機能（白抜きで示されている機能）とセキュリティ機能（網掛けで示されている機能）を以下で説明する。

5.1.1 基本機能

(1) コピー機能

利用者による操作パネルからの操作によって、紙文書をスキャンして読み込んだ利用者文書データを複写印刷する機能である。

(2) プリンター機能

クライアント PC のプリンタドライバから LAN 経由で利用者文書データを受信し、利用者による操作パネルからの操作によって印刷する機能である。

(3) スキャナー機能

利用者による操作パネルからの操作によって、紙文書をスキャンして読み込んだ利用者文書データをメールサーバー及び FTP サーバーに送信する機能である。

(4) ドキュメントファイリング機能

コピー機能等と同時に TOE 内部に利用者文書データを保存し、その保存されている利用者文書データを利用者による操作パネルからの操作、または LAN 経由によるクライアント PC からの操作によって、印刷等を行う機能である。

5.1.2 セキュリティ機能

(1) 識別認証機能

操作パネル、クライアント PC の Web ブラウザ、プリンタドライバにおいて、TOE の利用者をログイン名とパスワードにより識別認証する機能である。

- 管理者の設定した文字数以上で、アルファベットの大文字、小文字、数字、及び特殊文字のパスワードを要求する。
- TOE 内に保存されているユーザ情報を使用する「内部認証方式」と外部の認証サーバーを利用する「外部認証方式」をサポートする。
- パスワード入力時、入力された文字の代わりにアスタリスクを表示する。
- 連続してパスワード認証が失敗すると認証の受付を 5 分間停止する。
- 識別認証後、操作パネルの場合は管理者が設定した時間、Web ブラウザの場合は 5 分間、操作されないとセションを終了する。

(2) アクセス制御機能

TOE の基本機能で利用者データを操作するときに利用者データのアクセス制御を行う機能である。

- 利用者データの所有者や利用者役割などの利用者の種別ごとに定められているポリシーに基づき、利用者データへのアクセスを制御する。

(3) 蓄積データ暗号化機能

利用者データ等を TOE 内に暗号化して保存する機能である。

- 利用者データ及び TSF データは、鍵長 256 ビットの AES CBC モードで暗号化して保存する。
- 利用者データ等を暗号化するための暗号鍵は、十分なエントロピーを持つ乱数生成器により作成される。

(4) ネットワーク保護機能

LAN 利用時に通信経路上の利用者データを保護する機能である。

- 監査サーバー等の各種サーバーと TOE 間は、TLS v1.2 による暗号化通信を行う。
- 暗号化通信で用いられる暗号鍵は、十分なエントロピーを持つ乱数生成器により作成され、揮発性メモリのみに保存される。
- クライアント PC と TOE 間の通信のうち、プリンタドライバは、IPP over TLS 通信を、Web ブラウザでは HTTPS 通信を使用する。

(5) セキュリティ管理機能

TOE のセキュリティ管理を識別認証された利用者に制限する機能である。
- 内部認証利用者の登録/削除、最小パスワード長の変更、各種サーバーの設定、利用者データ及び TSF データの上書き消去等は、管理者役割を持つ利用者のみに提供される。
- 自身の利用者ログイン名及び利用者役割の問い合わせ、パスワードの変更は、全ての内部認証利用者に提供される。

(6) 監査機能

TOE の使用及びセキュリティに関連する事象のログを記録する機能である。
- 監査の起動と終了に加え、ジョブの終了、識別認証の失敗等の監査イベントのログを監査データとして生成する。 監査データには、イベント名、発生日時、利用者ログイン名、事象の結果、追加情報を記録する。
- 生成された監査データは、syslog プロトコル及び TLS v1.2 を用いて監査サーバーに送信する。

(7) ソフトウェア検証機能

アップデート用のファームウェアを TOE が検証し、正規なファームウェアのみインストールを可能にする機能である。
- ファームウェアと同時に提供されるデジタル署名が付けられたファームウェアのハッシュ値と、TOE が SHA-256 で算出したハッシュ値を照合することにより、正規ファームウェアであることを検証する。
- 管理者役割を持つ利用者は、ファームウェアのバージョンを取得することができる。

(8) 自己テスト機能

TOE 起動時にセキュリティ機能の正常動作を検証する機能である。
- セキュリティ機能が正常に動作することの検証は、乱数生成器のエントロピー源のヘルステスト、暗号アルゴリズムの既知解テスト、ファームウェアに毀損が無いことの確認により行う。
- 検証において、全部もしくは一部にエラーが検出された場合は、TOE は起動を中止し、電源断まで動作を停止する。

(9) 残存情報消去機能

コピー機能等の処理中のデータを完了または中止時に上書き消去する機能である。
- 文書ジョブの終了時に利用者文書データを、管理者が設定した値で上書き消去する。

(10) データ完全消去機能

利用者データ等を完全消去する機能である。
- 管理者役割を持つ利用者の要求に応じ、内部ストレージ上にあるすべての利用者データ及び TSF データを上書き消去する。このとき、蓄積データ暗号化のための暗号鍵は、再生成する。

5.2 IT環境

TOE は、LAN を介して各種サーバーやクライアント PC と通信を行う。

TOE は、生成した監査データを監査サーバーに送信する。管理者は監査サーバーから監査データを読み出す。

外部認証方式の場合は、認証サーバーを使用して、利用者の識別認証を行う。

TOE は、スキャンして読込んだ利用者文書データをメールサーバー及び FTP サーバーに送信することができる。

6 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表 6-1 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。

表 6-1 添付ドキュメント

名称	バージョン	言語
Start Guide	TINSX5397FCZZ YT1	英語
Quick Start Guide	2018B-EX1	英語
User's Manual	2018B-EX1	英語
Web Page Settings Guide	2017H-EN1	英語
Software Setup Guide	2017L-EN1	英語
Troubleshooting	2018B-EN1	英語
MX-FR57U Data Security Kit Operation Guide	EX1	英語
MX-FR57U Data Security Kit Notice	2.0	英語
How to set up MX-FR57U to be the "Protection Profile for Hardcopy Devices" compliant	V1.0	英語

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した一般社団法人 IT セキュリティセンター 評価部は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CEM に規定された評価方法を用いた CC パート 3 の保証要件の評価及び適合 PP の保証アクティビティに対する評価が実施された。評価作業の詳細は、評価報告書において報告された。評価報告書は、本 TOE の概要、CEM のワークユニットと保証アクティビティごとの評価内容及び判断結果を説明する。

7.3 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 29 年 12 月に始まり、平成 30 年 4 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 30 年 2 月に開発者サイトで評価者テストを実施した。

7.4 製品テスト

評価者は、製品のセキュリティ機能が確実に実行されることを確信するための独立テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

本評価の保証要件には、開発者テストは含まれていない。

7.4.2 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を確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

独立テストの構成は、図 4-1 で示した TOE の運用環境に準じ、その構成要素は表 7-1 のとおりである。以下の点で相違があるが、これらの構成でも、ST において識別されている構成と同等であり、本 TOE の機能の確認において問題がないことが評価者により評価されている。

- 評価者がテストした TOE は、第 2 章の TOE 識別で示した TOE の構成品（表 2-1 参照）のうち、MFD 本体が MX-M3070 fax option model と MX-M6070 fax option model の場合である。MFD 本体の相違は、印字速度の違い（高速・低速）であり、セキュリティに影響しない。ただし、セキュリティ機能に影響しないことを確認するため、MX-M3070 fax option model (印刷速度：低速)と MX-M6070 fax option model (印刷速度：高速)をテスト対象とした。

- 外部ネットワークからの不正アクセスに対し TOE を保護するために設置するファイアウォールは、TOE の動作に影響を与えるものではないことからテスト環境には存在しない。

- TLS のテストでは、評価機関が作成した TLS テストツールを介して TOE とサーバー/クライアント PC 間の通信を行う。 TLS テストツールは、TLS ハンドシェイクメッセージのパケットデータの改変のみを行うため、TOE の機能に影響しない。

- 暗号試験など一部のテストでは、TOE 内の暗号モジュールのテストのための呼び出しなどのために開発者が作成したテスト用ファームウェアを使用する。テスト用ファームウェアを使用したテストで呼び出されるモジュールは、TOE のモジュールと同一であることから、TOE の機能に影響しない。

表 7-1 独立テストの構成要素

要素	詳細
TOE	MX-M3070 fax option model ・オプション：MX-FR57U MX-M6070 fax option model ・オプション：MX-FR57U
監査サーバー	rsyslog　ver.8.24.0
メールサーバー	Postfix　ver.2.10.1
認証サーバー	openLDAP　ver2.4.44
FTPサーバー	Microsoft Internet Information Services　ver.8.5 9600.16384
クライアントPC	OS：Windows 8.1 / 10 Webブラウザ： ・Internet Explorer 11 ・Google Chrome 63.0.3239.132 プリンタドライバ： ・SHARP MX-M3070 PCL6ドライバー 07.01.06.19 ・SHARP MX-M6070 PCL6ドライバー 07.01.06.19

(2) 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である。

a) 独立テストの観点

評価者が、適合PPの保証アクティビティ及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① セキュリティ機能をSFRごとに確認する。

② 暗号実装が正しいことを確認する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

TOE の外部インタフェースについて、TOE の操作パネル、クライアントPC、テストツールを使用して入力を行い、そのふるまいを以下の手法で確認した。

- ふるまいが、TOE の外部インタフェースから確認可能な場合は、TOE の外部インタフェースを利用する。
- ふるまいが、TOE の外部インタフェースから確認できない場合は、監査サーバー内のログの調査、ネットワークアナライザや、テスト用ファームウェアを使用する。

＜独立テストの実施内容＞

独立テストは、評価者によって 34 項目実施された。

独立テストの観点とそれに対応したテスト内容を表 7-2 に示す。

表 7-2 実施した独立テスト

観点	テスト概要
①	セキュリティ機能の確認 ・適合PPの保証アクティビティまたはSFRの仕様から作成したテスト項目により、すべてのセキュリティ機能が仕様どおりであることをSFRごとに確認する。
②	暗号実装の確認 ・TOEにインストールしたテスト用ファームウェアを使用して、テスト対象の以下の暗号アルゴリズムの実装を確認する。 - RSA(鍵生成、署名生成/検証) - AES-CBC-128、AES-CBC-256、AES-ECB-256 - SHA-1、SHA-256 - HMAC-SHA-1、HMAC-SHA-256 - CTR_DRBG ・利用者文書データの暗号鍵とTOE内部に暗号化して保存された利用者文書データをテスト用ファームウェアにより取り出し、復号ツールにより復号することにより、正しく暗号化されていることを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者はTOEのふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 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となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

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。

① TOEの意図しないネットワークのポートが有効になっていたり、稼働しているネットワークサービスに公知の脆弱性が存在することにより悪用される懸念がある。
② TOEのWebインタフェースにおいて、URLの直接指定による識別認証機能等のバイパスやXSSなどの公知の脆弱性が存在することにより悪用される懸念がある。
③ TOEに入力される不正な印刷データにより、印刷ジョブの操作やバッファオーバーフローまたは任意のコードの実行が発生する懸念がある。
④ 操作パネル、プリンタドライバ及びWebインタフェースからの不正な入力により、識別認証機能がバイパスされる懸念がある。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者独立テストの環境に、以下の表 7 3 に示すテストツールを追加して実施した。

表 7-3 侵入テストで使用したツール

ツール名称	概要・利用目的
ポートスキャンツール nmap　7.60	ポートを検索するために使用
脆弱性スキャンツール Nessus　6.11.1	公知の脆弱性を検出するために使用
Web脆弱性スキャンツール OWASP ZAP　2.7.0	Webの一般的な脆弱性を検出するために使用
Webアプリケーション解析ツール Fiddler　5.0.20173.50948	Webアプリケーションがやり取りする通信データを捕捉、もしくは発行するために使用
プリンタセキュリティテストツール PRET　0.39	印刷デバイスに対しプリンタ言語を用いて脆弱性を検出するために使用
TCP/UDPデータ通信ツール Netcat　1.12	識別認証の脆弱性を検出するために使用
侵入テスト用ツール Metasploit Framework v4.6.2	不正な印刷用ファイルの作成を行うために使用

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-4 に示す。

表 7-4 侵入テスト概要

脆弱性	テスト概要
①	ポートスキャンツールと脆弱性スキャンツールを使用して、想定しないポートが開いていないこと及び使用可能なポートに公知の脆弱性が存在しないことを確認する。
②	Web脆弱性スキャンツールとWebアプリケーション解析ツールを使用して、Webインタフェースに公知の脆弱性がないことを確認する。
③	不正なふるまいを発生させることを意図したPostscriptやPJL言語、TIFF形式、PDF形式の印刷データを使用することにより、意図しないふるまいが発生しないことを確認する。
④	識別認証機能において入力される文字列により、不正なふるまいが発生しないことを確認する。

c) **結果**

評価者が実施した侵入テストでは、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。

7.5 評価構成について

本評価の前提となる TOE の構成条件は、第 6 章に示したガイダンスに記述されているとおりである。 本 TOE のセキュリティ機能を有効にし、安全に使用するためには、ガイダンスの記述のとおりに TOE を設定しなければならない。 ガイダンスと異なる設定にした場合は、本評価による保証の対象ではない。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニットと適合 PP の保証アクティビティのすべてを満たしていると判断した。

評価では以下について確認された。

PP 適合：

Protection Profile for Hardcopy Devices
1.0 dated September 10, 2015

Protection Profile for Hardcopy Devices - v1.0
Errata #1, June 2017

セキュリティ機能要件： コモンクライテリア パート２ 拡張

セキュリティ保証要件： コモンクライテリア パート３ 適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 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または保証アクティビティ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及び保証アクティビティで示されている方法に適合していること。

8.1 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 の以下の保証コンポーネント及び適合 PP の保証アクティビティを満たすものと判断する。

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

8.2 注意事項

本 TOE に興味のある調達者は、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価対象範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

本 TOE で生成された監査データは、監査サーバーへの送信が成功するまで TOE 内に暗号化して保存する。 TOE 内には、4 万件の監査データの保存が可能であるが、4 万件を超えて新たに生成された監査データは削除される。 監査サーバーへの送信が失敗した場合、TOE は再送信を試みるが、操作パネル及び Web ページに表示される警告メッセージに運用者は注意する必要がある。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり提供される。

名称：	MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57Uセキュリティターゲット
バージョン：	1.04
発行日：	2018年3月27日
作成者：	シャープ株式会社

11 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）
PP	Protection Profile（プロテクションプロファイル）
SFR	Security Functional Requirement（セキュリティ機能要件）
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。

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
FTP	File Transfer Protocol
HCD	Hardcopy Device
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL/TLS
IPP	Internet Printing Protocol
LDAP	Lightweight Directory Access Protocol
MFD	Multifunction Device
NVS	Nonvolatile Storage
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
XSS	Cross Site Scripting

本報告書で使用された用語の定義を以下に示す。

Field Replaceable (Unit)	故障を修理するために現場で交換可能な最小サブアセンブリ。 The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	電子的文書または画像の物理的媒体を生成または取り扱うシステム。このようなシステムはプリンター、スキャナー、ファクス装置、ディジタルコピー機、ディジタル複合機,「オールインワン」及びその他の同様な製品を含む。 A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), “all-in-ones” and other similar products.

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 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4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57Uセキュリティターゲット, バージョン 1.04, 2018年3月27日, シャープ株式会社

[13] シャープ株式会社 MX-M6070 / M5070 / M4070 / M3570 / M3070 fax option model with MX-FR57U 評価報告書, 第1.2版, 2018年4月4日, 一般社団法人 ITセキュリティセンター 評価部

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (認証識別: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017