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　齊藤　裕

原紙押印済

IT 製品（TOE）

申請受付日（受付番号）	令和 5 年 5 月 29 日（IT 認証 3848）
認証識別	JISEC-C0808
製品名称	SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U
バージョン及びリリース番号	0110M300
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)
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。
令和 6 年 3 月 8 日

セキュリティセンター セキュリティ技術評価部
技術管理者　矢野 達朗

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 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

評価結果：合格

「SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U バージョン 0110M300」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「SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U バージョン 0110M300」（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。）が令和 6 年 1 月 17 日に完了した 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、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 2 章以降を参照のこと。

1.1.1 プロテクションプロファイルまたは保証パッケージ

本 TOE は、次のプロテクションプロファイル[14][15]（以下「適合 PP」という。）に適合する。

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

1.1.2 TOE とセキュリティ機能性

本 TOE は、コピー機能、プリンター機能、スキャナー機能、ファクス機能、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 の扱う文書データやセキュリティに影響する設定データ等が暴露されたり改ざんされたりすることを防止するために、適合 PP 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適合 PP が要求する保証要件の範囲で評価が行われた。

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 脅威とセキュリティ対策方針

本 TOE は、以下の脅威を想定している。

TOE の保護資産である利用者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 の不正な操作や、TOE が接続されているネットワークへの不正なアクセスによって、暴露されたり改ざんされたりする脅威がある。

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 のセキュリティ機能が損なわれる脅威がある。

それらの脅威に対抗するために、本 TOE は、識別認証、アクセス制御、暗号化、電子署名などの、適合 PP が要求するセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

本 TOE 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。

TOE の設定及び維持管理は、信頼できる管理者がガイダンス文書に従って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、以下の運用を保証していない。

- 「4.2 運用環境と構成」の記載と異なる運用環境や構成
- 「7.5 評価構成について」の記載と異なる設定の TOE

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、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、令和 6 年 1 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。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。認証機関が指摘

した問題点は、すべて解決され、かつ、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： SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U

バージョン： 0110M300

本 TOE は日本以外で販売される製品である。

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、以下の情報を確認する。

・開発者名

TOE の筐体に表示されている開発者名が、「SHARP」であること

・本体型番

TOE の筐体に表示されている本体型番が、以下のいずれかであること

「BP-B550WD」
「BP-B547WD」
「BP-B540WR」
「BP-B537WR」

・ファクス機能

TOE の操作パネルの”FAX”欄に、「STANDARD」が表示されること

・必須オプション

TOE の操作パネルのオプション名に、「BP-FR12U」が表示されること

・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、MFD の基本機能としてコピー機能、プリンター機能、スキャナー機能、ファクス機能、ドキュメントファイリング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。

本 TOE は、MFD の扱う文書データやセキュリティに影響する設定データ等を保護するために、適合 PP の要求を満足するセキュリティ機能を提供する。

本 TOE の提供するセキュリティ機能の背景として、本 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を以下の 3.1 節から 3.4 節に示す。本 TOE のセキュリティ機能の詳細は、5 章に示す。

3.1 利用者の役割

本 TOE の想定する利用者の役割を表 3-1 に示す。

表3-1 利用者の役割

名称	定義
一般利用者 Normal User	識別認証された利用者で、管理者役割を持たない利用者 A User who has been identified and authenticated and does not have an administrative role
管理者 Administrator	識別認証された利用者で、管理者役割を持つ利用者 A User who has been identified and authenticated and has an administrative role

3.2 保護資産

本 TOE の想定する保護資産を表 3-2、表 3-3、表 3-4 に示す。TOE の保護資産には、表 3-2 に示すように利用者データと TSF データの 2 種類がある。また、利用者データは表 3-3、TSF データは表 3-4 に示すように、さらに細分される。

表3-2 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 Data created by and for Users that do not affect the operation of the TSF
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 Data created by and for the TOE that might affect the operation of the TSF

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 User Document Data	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 Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	利用者ジョブデータ User Job Data	利用者の文書または文書処理ジョブに関連する情報 Information related to a User's Document or Document Processing Job

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 Protected TSF Data	データの所有者でも管理者役割でもない利用者による改ざんが TOE のセキュリティに影響を及ぼすかもしれないが、暴露は許容できる TSF データ TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	秘密の TSF データ Confidential TSF Data	データの所有者でも管理者役割でもない利用者による暴露または改ざんが TOE のセキュリティに影響を及ぼすかもしれない TSF データ TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 脅威

本 TOE の想定する脅威を表 3-5 に示す。

表3-5 脅威

名称	定義
T.UNAUTHORIZED_ACCESS	攻撃者は、TOE のインタフェースを通じて、TOE 内の利用者文書データへアクセス（閲覧、改変、または削除)、または利用者ジョブデータを変更（改変または削除）するかもしれない。 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	攻撃者は、TOE のインタフェースを通じて、TOE 内の TSF データに不正アクセスするかもしれない。 An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	TOE の操作が許可された場合、TSF の誤作動によって、セキュリティの損失を引き起こすかもしれない。 A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	攻撃者は、TOE に不正なソフトウェアをインストールするかもしれない。 An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	攻撃者は、ネットワーク通信をモニタしたり操作したりすることで、通信中のデータにアクセスしたり、TOE のセキュリティを危殆化したりするかもしれない。 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 に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	利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。 Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	セキュリティ関連アクティビティは監査されなければならず、またこのようなアクションのログは保護され、外部 IT エンティティへ送信されなければならない。 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	TOE は、LAN 上の他のデバイスと自身を識別できなければならない。 The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOE はそれらのデバイス上の該当データを暗号化すること。 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	利用者文書データまたは秘密の TSF データの現地交換可能な不揮発性ストレージのための暗号鍵の生成に寄与するような、平文の鍵、サブマスク、乱数、またはその他のあらゆる値は、不正なアクセスから保護されなければならない、かつそのストレージデバイス上に保存されてはならない。 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.
P.FAX_FLOW	TOE が PSTN ファクス機能を提供する場合、PSTN ファクス回線と LAN の間の分離を保証する。 If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

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	TOE、及び TOE が保存または処理するデータの価値に見合った物理セキュリティが、環境によって提供されることを想定する。 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	運用環境は、LAN インタフェースへの外部からの直接のアクセスから TOE を保護することを想定する。 The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE 管理者は、サイトのセキュリティ方針に従って TOE を管理すると、信頼されている。 TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	許可された利用者は、サイトのセキュリティ方針に従って TOE を使用するよう教育訓練されている。 Authorized Users are trained to use the TOE according to site security policies.

4.2 運用環境と構成

本 TOE の想定する運用環境を図 4-1 に示す。本 TOE は一般的なオフィスに設置され、組織の内部ネットワークである LAN 及び公衆電話回線網に接続して使用される。利用者は、本 TOE の操作パネルや LAN に接続されたクライアント PC を操作して本 TOE を使用する。

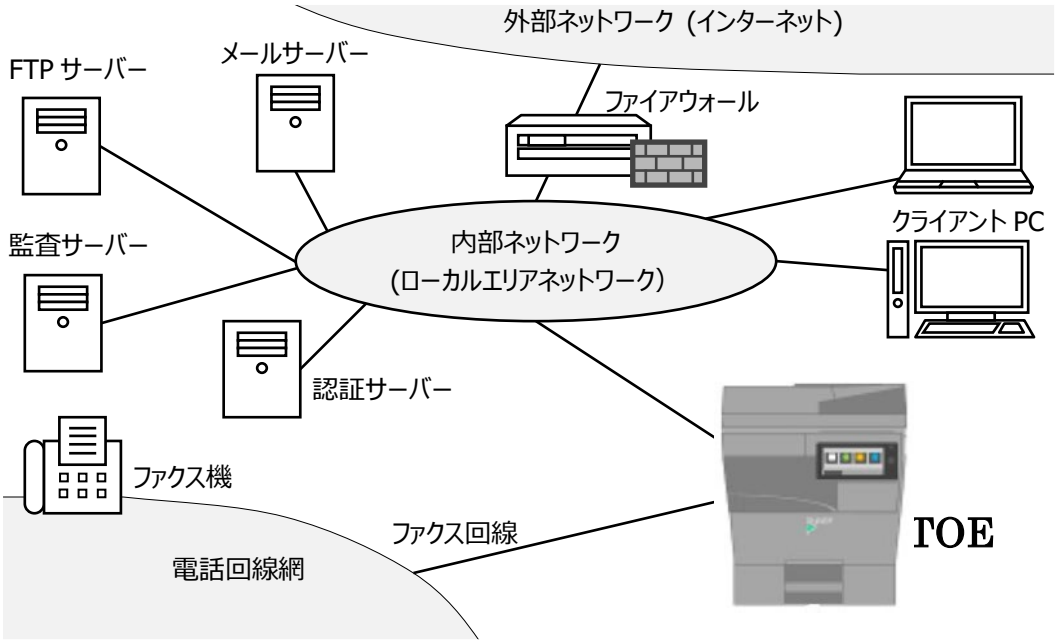

図4-1 TOE の運用環境

本 TOE の運用環境の構成品を以下に示す。

(1) クライアント PC

利用者が使用する汎用の PC である。 以下のソフトウェアが必要である。

・OS：Windows 10

・プリンタドライバ

SHARP <本体の型番> PCL6 ドライバー 04.00.08.17

・Web ブラウザ

Microsoft Edge 116

(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の監査サーバーである。syslog プロトコルを使用し、TLS 1.2 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。本評価では、rsyslog ver.8.24.0 を使用。

(3) メールサーバー

TOE から利用者の文書データを E-mail 添付ファイルとして送信する場合に必要である。TLS 1.2 に対応していなくてはならない。

本評価では、Postfix　ver.2.10.1 を使用。

(4) FTP サーバー

TOE から利用者の文書データを FTP サーバーに送信する場合に必要である。TLS 1.2 に対応していなくてはならない。

本評価では、Windows 10 に搭載の Microsoft Internet Information Services ver.10.0.19041.2130 を使用。

(5) 認証サーバー

5.1.1 節の「識別認証機能」で示す「外部認証方式」の場合、TLS 1.2 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。

本評価では、openLDAP ver2.4.44 を使用。

なお、本構成に示されている TOE 以外のハードウェア及び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 の提供する機能、及び、本評価で保証される本 TOE の機能には、以下の制約がある。

(1) 各種サーバ及びクライアント PC

TOE と連携して動作する各種サーバーやクライアント PC がセキュアに運用されることは、管理者の責任である。

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 において、TOE は「TOE」と記述された部分であり、必要なオプションを搭載した MFD の全体である。

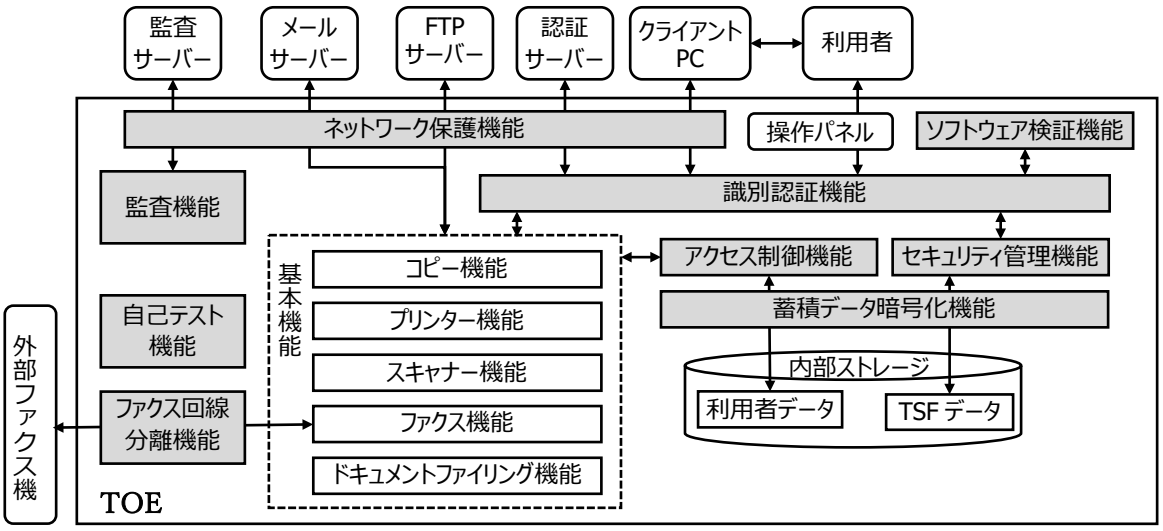

図5-1 TOE 境界

TOE の提供する機能は、MFD の基本機能とセキュリティ機能で構成される。図 5-1 で、TOE 内の色付きの部分がセキュリティ機能であり、TOE 内の他の機能は基本機能である。以下、TOE のセキュリティ機能について説明する。基本機能については 11 章を参照。

(1) 識別認証機能

本機能は、利用者が MFD の操作パネル、クライアント PC の Web ブラウザやプリンタドライバから TOE を利用するときに、ログイン名とパスワードで利用者を識別認証する機能である。

本機能は、識別認証を補強するために、以下の機能性を備えている。

・最小パスワード長の制限。
・連続した認証失敗時のアカウントのロックアウト。
・認証成功後、一定時間操作がない場合のセッション切断。

(2) アクセス制御機能

本機能は、MFD 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。

アクセス制御は、利用者データの所有者情報と、利用者の識別情報及び利用者役割に基づいて行われる。

(3) 蓄積データ暗号化機能

本機能は、TOE 内部に保存するデータを暗号化する機能である。暗号化は、鍵長 256 ビットの AES CBC モードを使用する。
暗号鍵は、推測の困難な十分なエントロピーを持つ乱数生成器を用いて生成される。

(4) ネットワーク保護機能

本機能は、TOE と各種 IT 機器との間の通信データを、暗号通信プロトコル TLS 1.2 で保護する機能である。
暗号鍵は、推測の困難な十分なエントロピーを持つ乱数生成器を用いて生成される。

(5) セキュリティ管理機能

本機能は、セキュリティ機能の設定等を、管理者に制限する機能である。
ただし、一般利用者は、自身の利用者ログイン名及び権限グループの問い合わせ、パスワードの変更が可能である。

(6) 監査機能

本機能は、セキュリティ機能に関する監査事象を監査ログとして生成し、監査サーバーに送信する機能である。
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保存されずに破棄される。

(7) ソフトウェア検証機能

本機能は、ファームウェア更新時に更新用ファームウェアの電子署名を検証する機能である。

(8) 自己テスト機能

本機能は、TOE 起動時に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をテストする機能である。

(9) ファクス回線分離機能

本機能は、公衆電話回線網(PSTN)と LAN を分離する機能である。 PSTN の利用はファクスに制限され、それ以外の通信はできない。

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 の「(4) ネットワーク保護機能」は、それら IT 機器と連携して実現され、以下のプロトコルを使用する。

・クライアント PC(Web ブラウザ)：HTTP over TLS
・クライアント PC(プリンタドライバ)：IPP over TLS
・監査サーバー：syslog over TLS
・メールサーバー：SMTP over TLS
・FTP サーバー：FTP over TLS
・認証サーバー：LDAP over TLS

6 製品添付ドキュメント

本 TOE のガイダンスの識別を表 6-1 及び表 6-2 に示す。本体型番が BP-B550WD または BP-B540WR である TOE のガイダンスが表 6-1、本体型番が BP-B547WD または BP-B537WR である TOE のガイダンスが表 6-2 である。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 ガイダンス (BP-B550WD または BP-B540WR)

名称	バージョン
Start Guide	TINSE2441QSZZ YT1
Quick Start Guide	bpb550wd_qsg_01a_us
User's Manual	bpb550wd_usr_01a_en
Software Setup Guide	software-setup_a30-02a_en
Data Security Kit Operation Guide	bp70C65_dk1_01a_en
Data Security Kit Notice	Q1-1
How to set up this product to be the "Protection Profile for Hardcopy Devices" compliant	m3-1

表6-2 ガイダンス (BP-B547WD または BP-B537WR)

名称	バージョン
Start Guide	TINSM2442QSZZ CR1
Quick Start Guide	bpb547wd_qsg_01a_en
User's Manual	bpb547wd_usr_01a_en
Software Setup Guide	software-setup_a30-02a_en
Data Security Kit Operation Guide	bp70C65_dk1_01a_en
Data Security Kit Notice	Q1-1
How to set up this product to be the "Protection Profile for Hardcopy Devices" compliant	m3-1

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、適合 PP が要求する 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及び適合 PP の保証アクティビティを用いて行われた。

評価作業の詳細は、評価報告書において報告された。評価報告書では、本 TOE の概要と、CEM のワークユニット及び適合 PP の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、令和 5 年 5 月に始まり、令和 6 年 1 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、令和 5 年 8～9 月に開発者サイトで評価者テストを実施した。

認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、製品のセキュリティ機能が確実に実現されていることを保証するための評価者独立テスト及び脆弱性評定に基づく評価者侵入テストを実行した。

7.4.1 開発者テスト

本評価において、開発者テストは保証要件には含まれない。

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現されていることを保証するための評価者独立テスト(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

独立テストの環境は、図 4-1 に示した TOE の運用環境に準じた構成である。独立テストの環境で使用した構成品を表 7-1 に示す。

表7-1 独立テスト環境の構成品

構成品	詳細
TOE	・SHARP BP-B550WD fax-standard model with BP-FR12U バージョン 0110M300 ・SHARP BP-B537WR fax-standard model with BP-FR12U バージョン 0110M300
監査サーバー	rsyslog ver.8.24.0
メールサーバー	Postfix ver.2.10.1
FTP サーバー	Microsoft Internet Information Services ver.10.0.19041.2130
認証サーバー	openLDAP ver.2.4.44
クライアント PC	OS：Windows 10 Web ブラウザ： ・Microsoft Edge 116 プリンタドライバ： ・SHARP BP-B550WD PCL6 04.00.08.17 ・SHARP BP-B537WR PCL6 04.00.08.17

独立テストの構成は、ST において識別されている TOE の構成と以下のような違いがある。評価者は、それらの違いに問題はなく、評価者の実施した独立テストによって、ST において識別されている TOE の構成のセキュリティ機能が適切にテストされたと見なすことができると判断している。

① テスト対象の機種

2 章の TOE 識別で示した TOE の機種には、以下のような相違により、複数の機種が含まれている。

・印刷速度の違い

各機種のセキュリティ機能は同じであり、上記の相違点を考慮して代表する 2 機種をテストすることで、TOE 全機種のセキュリティ機能がテストされたと見なすことができると、評価者は判断している。

② テスト用に変更されたファームウェアの使用

独立テストでは、暗号機能の確認のために、TOE のファームウェアの代わりに、テスト用に変更されたファームウェアが使用された。テスト対象の暗号機能のモジュールは同一であり、テスト用に変更された部分は影響を与えないため、テスト用ファームウェアによるテストは妥当であると、評価者は判断している。

③ テスト用ツールの追加使用

独立テストでは、通信データの確認や変更、暗号機能の確認などのために、テスト用のツールが使用された。それらのテスト用ツールの妥当性は評価者によって確認されている。

⑵ 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 の要求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セキュリティ機能要件（SFR）ごとに確認する。

② 暗号アルゴリズムの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 に対して、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、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 35 項目実施された。

独立テストの観点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 SFR ごとに指定された保証アクティビティ、または、SFR の要件に基づいて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に動作することを確認する。
②	暗号アルゴリズムの実装の確認 TOE にインストールしたテスト用プログラムを使用して、以下の暗号アルゴリズムが仕様どおりに実装されていることを確認する。 - RSA(鍵生成、署名生成/検証) - ECDSA(署名検証) - AES-ECB-128, AES-ECB-256, AES-CBC-128, AES-CBC-256, AES-GCM-128, AES-GCM-256 - SHA-1、SHA-256、SHA-384、SHA-512 - HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384 - CTR_DRBG

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、想定される運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、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 に意図しないネットワークポートが開いている懸念がある。また、TOE で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懸念がある。
② TOE の Web インタフェースに公知の脆弱性が存在する懸念がある。
③ TOE の印刷処理に公知の脆弱性が存在する懸念がある。
④ TOE の操作パネル、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。
⑤ TOE が TLS クライアントとして動作する際に通信先のサーバ証明書の確認処理に脆弱性が存在する可能性がある。

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＞

侵入テストの環境は、独立テストの環境に、侵入テスト用のツールを追加した環境である。侵入テストで使用したツールを表 7-3 に示す。

表7-3 侵入テスト用ツール

名称	概要・利用目的
Nmap 7.93	利用可能なネットワークポートを検出するツール
Nessus 10.4.1	ネットワークポートの公知の脆弱性を検出するツール
OWASP ZAP 2.12.0 Active scanner rules(beta) バージョン 40.0.0 を追加	Web アプリケーションの脆弱性を診断するツール
PRET 0.40	印刷処理の様々な脆弱性を検査するツール

＜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	・Nmap を使用して、TOE に想定外のネットワークポートが開いていないことを確認する。 ・Nessus を使用して、TOE で稼働しているネットワークサービスに公知の脆弱性がないことを確認する。
②	・OWASP ZAP を使用して TOE の Web インタフェースに公知の脆弱性が存在しないことを確認する。
③	・PRET やインターネットで入手した攻撃コードを使用して、TOE の印刷処理に公知の脆弱性がないことを確認する。
④	・TOE の操作パネル、プリンタドライバ及び Web インタフェースにおいて、不正な処理を発生させる可能性のある文字列を入力しても、TOE に不正なふるまいが発生しないことを確認する。
⑤	・TLS のサーバ証明書の検証処理を TOE が正しく実施していることをメール処理において確認する。

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、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 を評価で保証されたとおりに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 のワークユニット及び適合 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

「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン[16]

- FCS_RBG_EXT.1 のテストに関連する措置について
- FCS_TLS_EXT.1.1 のテストに関する措置について

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、適合 PP が要求する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、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、以下の観点で認証を実施した。

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 CEM のワークユニット及び適合 PP の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 及び適合 PP の保証アクティビティに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

評価機関より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 の評価が適合 PP の要求する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「4.2 運用環境と構成」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。

監査データの監査サーバーへの送信が失敗した場合、操作パネル及び Web ページに警告メッセージが表示される。TOE は監査データの再送信を試みるが、運用者は警告メッセージに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： SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U セキュリティターゲット
バージョン： 1.02
発行日： 2023 年 9 月 19 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。

MFD	Multifunction Device
PSTN	Public Switched Telephone Network

本報告書で使用された IT 技術に関する略語を以下に示す。

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CTR_DRBG	Counter (CTR) mode block cipher algorithm DRBG
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
FTP	File Transfer Protocol
GCM	Galois/ Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IPP	Internet Printing Protocol
LDAP	Lightweight Directory Access Protocol
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security

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、スキャナ、ファクス装置、デジタルコピー機、デジタル複合機,「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.
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。
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。
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。
ファクス機能	公衆電話回線に接続された G3 規格に準拠した外部のファクス機と文書データの送受信を行う機能である。紙文書をスキャンして外部のファクス機に送信するファクス送信機能と外部のファクス機から受信した文書データを利用者の操作により印刷するファクス受信機能がある。
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。
保証アクティビティ	PP 適合のために評価者が実施しなければならない評価作業。CEM の補足であり、適合 PP [14]では適合 PP の中に記述されている。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和5年12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, 令和5年12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, 令和3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 Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[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5版, 2017年4月, CCMB-2017-04-001 (平成29年7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5版, 2017年4月, CCMB-2017-04-002 (平成29年7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5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[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5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U セキュリティターゲット, バージョン 1.02, 2023年9月19日, シャープ株式会社

[13] シャープ株式会社 SHARP BP-B550WD / B547WD / B540WR / B537WR fax-standard model with BP-FR12U 評価報告書, 第1.2版, 2024年1月17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

[16] 「ハードコピーデバイスのプロテクションプロファイル」適合の申請案件についてのガイドライン, 第1.8版, 2020年11月11日, 独立行政法人情報処理推進機構, JISEC-CERT-2020-A18