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

プロテクションプロファイル（PP）

申請受付日（受付番号）	平成29年2月9日（IT認証7627）
認証識別	JISEC-C0553
プロテクションプロファイル名称／識別	Protection Profile for Hardcopy Devices
プロテクションプロファイルバージョン	1.0 dated September 10, 2015
プロテクションプロファイル開発者	IPA, NIAP, and the MFP Technical Community
プロテクションプロファイル申請者	独立行政法人情報処理推進機構
要求する保証要件	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	株式会社 ECSEC Laboratory 評価センター

上記のPP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29年5月29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　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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

「Protection Profile for Hardcopy Devices」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、IPA, NIAP and the MFP Technical Community が開発した「Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015」[12]（以下「本 PP」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が平成 29 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独立行政法人情報処理推進機構に報告するとともに、本 PP 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。

本認証報告書は、本 PP に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、本 PP 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。

また、本認証報告書の読者は本 PP を併読されたい。特に本 PP が TOE に対して要求するセキュリティ機能要件、保証要件及びその背景となるセキュリティ課題について詳述されている。

1.1 評価対象製品概要

本 PP 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 PP概要

本 PP はスキャン、コピー、プリント等の基本機能を有するデジタル複合機（Hardcopy Device、以下「HCD」という）に関するセキュリティ要件を規定するものである。

本 PP に適合する HCD（以下、「TOE」という）は、以下に示す基本機能のうち１つ以上の機能を提供し、合わせてローカルエリアネットワーク上で文書データ等を送受信するネットワーク通信機能と各種設定やログ収集等を行う管理機能を提供する。

・プリント：電子文書を紙文書に変換（印刷）する
・スキャン：紙文書を電子文書に変換する
・コピー：紙文書を複製する

また、TOE 構成によっては FAX 通信機能や内部ストレージへの文書蓄積機能等が提供される。

TOE は、これらの基本機能に加えて、TOE で扱う文書データやセキュリティに関する設定データ等を漏えいや改ざんから保護するためのセキュリティ機能を提供する。

本 PP では、TOE 毎に異なる（セキュリティ機能を含む）機能構成を踏まえ、すべての TOE に対する必須セキュリティ要件、特定条件の TOE に必要となるセキュリティ要件（Conditionally Mandatory Requirements、Selection-based Requirements）、その他オプションとして提供されるセキュリティ要件（Optional Requirements）がそれぞれ規定される。各セキュリティ要件については、次項以降に示す。

1.1.1.1 脅威とセキュリティ対策方針

本 PP は、TOE に対して以下の脅威を想定し、それに対抗することを目的としたセキュリティ機能を要求する。

TOE の保護資産である利用者の文書データやセキュリティに影響する設定情報は、TOE の操作や、TOE が設置されているネットワーク上の通信データへのアクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

それらの脅威に対抗するために、TOE は利用者の識別認証、アクセス制御、暗号化などのセキュリティ機能を提供する。

また、TOE 自身の改ざんや、故障によるセキュリティの喪失といった脅威に対抗するため、アップデートソフトウェアの検証機能やセルフテスト機能などのセキュリティ機能を提供する。

1.1.1.2 構成要件と前提条件

本 PP は、TOE が次のような構成及び前提で運用されることを想定する。

TOE は、不正な物理的アクセスが制限され、外部ネットワークから保護された LAN に接続される環境で運用されることを想定している。また、TOE の運用にあたっては、管理者がガイダンス文書に従って適切に設定し、維持管理しなければならない。

1.1.2 免責事項

TOE は 1.1.1.2 に示す環境で運用されることを想定しており、本 PP では TOE に対する物理攻撃やインターネット経由での直接的な攻撃に関する脅威に対しては対抗していない。

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 PP 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 29 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]、所見報告書、及び関連する評価証拠資料を検証し、本 PP 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。本 PP 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 PP識別

本 PP は、以下のとおり識別される。

PP名称：	Protection Profile for Hardcopy Devices
PPバージョン：	1.0 dated September 10, 2015 (Protection Profile for Hardcopy Devices – v1.0 Errata #1)
開発者：	IPA, NIAP, and the MFP Technical Community

3 セキュリティ方針

本章では、本 PP に適合する TOE が解決すべきセキュリティ課題と実装すべきセキュリティ機能について述べる。

TOE は HCD として必要な基本機能を提供し、さらに一般的に利用者の文書データを内部に蓄積し、ネットワークを介して利用者の端末や各種サーバと通信を行う機能を有する。TOE はこれらの機能を使用する際に利用者の文書データや設定データ等が不正に暴露されたり改ざんされたりすることを防止し、自身を安全に動作させるためにセキュリティ機能を提供する。

また、本 PP はセキュリティ機能によって保護されるべき資産として以下のものを定義すると共に、利用者役割の定義を以下の通り TOE に求める。なお、資産及び利用者役割に関しては、TOE 毎に必要に応じて追加の定義を行ってもよい。

資産

（利用者データ）

D.USER.DOC：利用者文書データ

D.USER.JOB：利用者ジョブデータ

（TSF データ）

D.TSF.PROT：(Protected TSF Data) 全ての利用者の閲覧は可能だが、不正な改ざん、削除から保護されなければならない TSF データ

D.TSF.CONF：(Confidential TSF Data) 権限のある利用者以外は閲覧、改ざん、削除が禁止される TSF データ

利用者役割

U.NORMAL：管理者役割を持たない、識別認証される一般利用者

U.ADMIN：管理者役割を持つ、識別認証される管理者

3.1 脅威

本 PP に適合する TOE は、表 3-1 に示す脅威を想定しこれに対抗する機能を備える。

表3-1　想定する脅威

識別子	脅威
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.

3.2 組織のセキュリティ方針

本 PP に適合する 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 3-2 に示す。

表 3-2　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.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.

識別子	組織のセキュリティ方針
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 (conditionally mandatory)	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 (conditionally mandatory) ＊このセキュリティ方針は、P.STORAGE_ENCRYPTIONと共に適用される	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 (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE (optional)	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 (optional)	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.

3.3 セキュリティ対策

本 PP に適合する TOE は、3.1 及び 3.2 に示したセキュリティ課題への対策として、以下に概要を示すセキュリティ機能を実装する。

3.3.1 利用者の識別認証機能

TOE は、TOE 自身が提供するメカニズムや認証サーバ等の信頼できる外部 IT エンティティを利用した形で、TOE にアクセスしようとする利用者の識別及び認証を行う機能を提供する。識別認証に成功した利用者には役割に対応した権限が与えられ、TOE の利用が許可される。

3.3.2 アクセス制御機能

利用者からの処理要求に対して、その利用者の役割、権限を基に利用者データ及び TSF データに対するアクセス制御を実施する。具体的なアクセス制御規則については TOE 毎に明確に規定されるが、基本的な方針として本 PP は以下を求める。

- TOE 内部で管理される D.USER.DOC については、その所有者と管理者以外の利用者が閲覧、改変、削除等の操作を行うことが禁止される
- TOE 内部で管理される D.USER.JOB については、その所有者と管理者以外の利用者が改変、削除等の操作を行うことが禁止される
- D.TSF.PROT については、その所有者と管理者以外の利用者が改変等の操作を行うことが禁止される
- D.TSF.CONF については、その所有者と管理者以外の利用者が閲覧、改変等の操作を行うことが禁止される

3.3.3 暗号化通信機能

TOE は、利用者端末及び各種サーバ間のネットワーク通信に関して、通信データへの不正なアクセス、リプレイ攻撃、送信元・宛先のなりすまし等に対抗するための保護機能を提供する。具体的な保護手段、通信プロトコル、暗号スイート等は TOE 毎に具体的に規定される。

3.3.4 自己テスト

TOE は、セキュリティ機能が適切に動作していることを自ら検証するためのセルフテストを起動時に実施する。

3.3.5 監査機能

TOE は、監査対象となるセキュリティ事象が発生した際に、事象種別、発生日時、結果等の項目からなる監査ログを生成し、監査サーバ等の外部 IT エンティティに送信する機能を提供する。送信する際の通信路についても他のネットワーク通信と同様に保護される。また、生成した監査ログを TOE 内部で安全に管理し、権限を有する利用者が閲覧できる機能を提供してもよい。

3.3.6 アップデート検証機能

TOE は自身をアップデートする際に、不正なソフトウェアによって自分自身を改ざんされることを防ぐためにアップデートソフトウェアの真正性を検証する機能を提供する。この検証が成功した場合のみソフトウェアアップデートが実行される。

3.3.7 ストレージ暗号化機能

ストレージ暗号化機能は、TOE が D.USER.DOC または D.TSF.CONF を現地交換可能なストレージデバイス上に格納する場合に提供される機能であり、TOE 毎に具体的に規定される国際的に承認された暗号メカニズムによって、これら格納データを暗号化する機能である。本機能で使用される暗号鍵、鍵生成時に使用される鍵材料等は、不正なアクセスから保護されると共に、上記ストレージデバイスとは異なる領域に格納される。

3.3.8 FAX回線-ネットワーク分離機能

FAX 回線-ネットワーク分離機能は、TOE が FAX 通信をサポートする場合に提供される機能であり、FAX 通信で使用する PSTN 経由で LAN へのアクセスを禁止する機能である。本機能では、TOE が接続される LAN に対する不正アクセスを防ぐため、FAX プロトコルを用いた D.USER.DOC の送受信以外の PSTN を使用する通信が禁止される。

3.3.9 上書き消去及び完全消去機能

本機能は、TOE が処理終了及び中断後に内部に残存する不要な情報を、規定のデータで上書き消去する機能と、管理者の操作により TOE に蓄積された全ての利用者データ、TSF データを完全に消去し、利用できなくする機能とにより構成される。これらの機能は本 PP においてオプショナル要件として定義され、機能提供の有無については TOE 毎に規定される。

4 前提条件と評価範囲の明確化

本章では、本 PP に適合する 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、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

識別子	前提条件
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.

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した「株式会社 ECSEC Laboratory 評価センター」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。

5.2 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た。評価報告書では、本 PP の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 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 2 月に始まり、平成 29 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。

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。

5.4 評価結果

評価者は、評価報告書をもって本 PP 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。

評価では以下について確認された。

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。

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1

5.5 評価者コメント/勧告

本評価は、本 PP に「Protection Profile for Hardcopy Devices – v1.0　Errata #1」[13]（以下「Errata」という。）を適用して実施している。Errata を適用しない本 PP の総合判定結果は合格にはならないので注意が必要である。

6 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 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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。

6.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 PP が CC パート 3 の保証コンポーネント APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1 に対する保証要件を満たすものと判断する。

6.2 注意事項

・「1.1.1 PP 概要」に記載されている通り、本 PP では TOE 構成によって要求されるセキュリティ要件が異なる場合があるため、本 PP に適合した TOE を調達する調達者は、購入する製品の機能構成を踏まえ必要なセキュリティ機能が実装されていることを確認する必要があることに注意されたい。

・「5.5 評価者コメント/勧告」にも記載されている通り、本 PP を認証済み PP として使用するためには、誤記訂正である Errata[13]を適用する必要があることに注意されたい。

7 附属書

特になし。

8 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

LAN	Local Area Network ローカルエリアネットワーク
MFP	Multifunction Printer, Multifunction Peripheral デジタル複合機
PSTN	Public Switched Telephone Network 公衆交換電話網

本報告書で使用された用語の定義を以下に示す。

Document Processing	文書をプリント、スキャン、コピーすること。
Field-Replaceable (unit)	故障修理のために現地で交換可能である（部品の最小単位）

9 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] Protection Profile for Hardcopy Devices, 1.0 dated September 10, 2015, MFP Technical Community

[13] Protection Profile for Hardcopy Devices – v1.0 Errata #1

[14] PP評価報告書, 第2.0版, 2017年4月26日, 株式会社 ECSEC Laboratory 評価センター