



認 証 報 告 書

東京都文京区本駒込~~原~~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

IT製品 (TOE)

申請受付日 (受付番号)	令和2年7月31日 (IT認証0766)
認証識別	JISEC-C0719
製品名称	RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S
バージョン及びリリース番号	E-1.00
製品製造者	株式会社リコー
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	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.2
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3年4月14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 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 バージョン3.1 リリース5
- ② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース5

評価結果：合格

「RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro

C5300S/C5310S, infotec Pro C5300S/C5310S バージョン E-1.00」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	1
1.1	評価対象製品概要	1
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	1
1.1.2	TOEとセキュリティ機能性.....	1
1.1.2.1	脅威とセキュリティ対策方針	2
1.1.2.2	構成要件と前提条件.....	2
1.1.3	免責事項	2
1.2	評価の実施.....	3
1.3	評価の認証.....	3
2	TOE識別	4
3	セキュリティ方針	8
3.1	セキュリティ機能方針.....	9
3.1.1	脅威とセキュリティ機能方針.....	9
3.1.1.1	脅威	9
3.1.1.2	脅威に対するセキュリティ機能方針	10
3.1.2	組織のセキュリティ方針とセキュリティ機能方針.....	11
3.1.2.1	組織のセキュリティ方針.....	11
3.1.2.2	組織のセキュリティ方針に対するセキュリティ機能方針.....	12
4	前提条件と評価範囲の明確化	15
4.1	使用及び環境に関する前提条件	15
4.2	運用環境と構成.....	15
4.3	運用環境におけるTOE範囲	18
5	アーキテクチャに関する情報	19
5.1	TOE境界とコンポーネント構成.....	19
5.2	IT環境	20
6	製品添付ドキュメント	21
7	評価機関による評価実施及び結果.....	25
7.1	評価機関.....	25
7.2	評価方法.....	25
7.3	評価実施概要	25
7.4	製品テスト	26
7.4.1	開発者テスト	26
7.4.2	評価者独立テスト	28
7.4.3	評価者侵入テスト	31
7.5	評価構成について	33
7.6	評価結果.....	34

7.7	評価者コメント/勧告	34
8	認証実施	35
8.1	認証結果.....	35
8.2	注意事項.....	35
9	附属書.....	36
10	セキュリティターゲット.....	36
11	用語.....	37
12	参照.....	40

1 全体要約

この認証報告書は、株式会社リコーが開発した「RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S バージョン E-1.00」（以下「本 TOE」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。）が令和 3 年 3 月 30 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株式会社リコー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、市販される本 TOE を購入する一般消費者、及び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。

U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

本 TOE の保証パッケージは、EAL2及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

本TOEは、紙文書の電子化、文書管理、印刷をするためのコピー機能、スキャナー機能、プリンター機能、ファクス機能を提供する株式会社リコー製のデジタル複合機（以下「MFP」という。）である。

MFPは、コピー機能にスキャナー、プリンター、ファクスの各機能を組み合わせて構成される製品であり、一般的にはオフィスのLANに接続され、ドキュメントの入力・蓄積・出力に利用される。

本TOEは、適合PPで要求されるセキュリティ機能、及びTOEが運用される組織が要求するセキュリティ方針を実現するための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おり、それに対抗するセキュリティ機能を提供する。

TOEが扱う文書やセキュリティ機能に関する設定情報等の保護資産に対して、TOEへの不正アクセスやネットワーク上の通信データへの不正アクセスによる、暴露や改ざんの脅威が存在する。

本TOEでは、それら保護資産に対する不正な暴露や改ざんを防止するための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

評価対象製品は、次のような前提で運用することを想定する。

本TOEは、TOEの物理的部分やインタフェースが不正なアクセスから保護されるような環境に設置されることを想定している。また、TOEの運用にあたっては、ガイド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。

1.1.3 免責事項

本TOEでは、以下の機能を無効化して運用することが前提となる。この設定を変更して運用された場合、それ以降は本評価における保証の対象外となる。

- ・保守機能への移行
- ・IP-Fax機能、及びInternet Fax機能の使用
- ・ベーシック認証（本体認証時）以外の認証方式の使用

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 3 年 3 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： RICOH Pro C5300S/C5310S,
 SAVIN Pro C5300S/C5310S,
 LANIER Pro C5300S/C5310S,
 nashuatec Pro C5300S/C5310S,
 Rex Rotary Pro C5300S/C5310S,
 Gestetner Pro C5300S/C5310S,
 infotec Pro C5300S/C5310S

バージョン： E-1.00

開発者： 株式会社リコー

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。

- 製品外装に表示されている名称が「Pro C5300S」または「Pro C5310S」と一致することを確認する。
- ファクスオプションの梱包箱上のラベルシールに記載された名称が「Fax Option Type M42」と一致することを確認する。
- 製品のガイダンスの記載に従って操作し、製品の操作パネルに表示された名称とバージョンと部番(一部の項目には部番がない)が表2-1, 表2-2, 表2-3 に示すものと一致することを確認する。

表2-1 本体のソフトウェアの識別情報

名称	バージョン	部番
System/Copy	1.04	D0CQ5760H
Network Support	19.21	D0CQ5769D
Web Support	1.03	D0CQ5765G
OSS Info	1.00	D0CQ5789A
Fax	01.00.00	D0CQ5762B
RemoteFax	01.00.00	D0CQ5763B
Scanner	01.01	D0CQ5764D
Web Uapl	1.00	D0CQ5766D
NetworkDocBox	1.01.1	D0CQ5770B
animation	1.00	D0CQ5767C

名称	バージョン	部番
Printer	1.01	D0CQ5772D
RPCS	3.24.6	D0CN5774B
Font EXP	1.00	D2415581
PCL	1.00	D0CN5775C
IRIPS PS3	1.00	D0CN5781B
IRIPS PDF	1.02	D0CN5778C
IRIPS Font	1.20	D0CN5783
GraphicData	1.01	D0CQ5784D
MovieData	1.01	D0CQ5785C
MovieData2	1.01	D0CQ5786C
MovieData3	1.01	D0CQ5787C
HelpData	0.03	D0CQ5788A
Data Erase Onb	1.05	D2625244
GWFCU3.8-25(WW)	01.00.00	D0CN5755A
PowerSaving Sys	F.L3.25	D0CN5761
MediaLibrary	0.03	D0CQ5776A
CheetahSystem	1.04	D0CN1537E
appsite	3.02.01	D0CN1576A
bleservice	1.02	D0CN1568A
camelsl	1.00	D0CN1597A
cispluginble	4.0.1	D0CN1548
cispluginkeyst	3.03.02	D0CN1547A
cispluginnfc	3.03.02	D0CN1546A
decolet	3.00.02	D0CN1541A
ecoinfo	1.00	D0CN1564A
faxinfo	1.00	D0CN1562A
helpservice	1.00	D0CN1596A
iccd	3.08.02	D0CN1578A
introductionset	0.41G25	D0CN1584B
iwnnimelanguage	2.8.2	D0BQ1456A
iwnnimelanguage	2.8.2	D0BQ1454A
iwnnimelanguage	2.8.2	D0BQ1455A
iwnnimeml	2.8.201	D0BQ1453C
kerberos	1.07.03	D0CN1595A
langswitcher	1.00	D0CN1560A
mediaappappui	1.00	D0CN1574A
mlpsmartdevicec	4.1.0	D0CN1542

名称	バージョン	部番
multidevicehub	2.01	D0BM1472A
optimorurcmf	1.1	D0BQ1499B
pptop	1.00	D0CQ1439A
programinfoserv	1.00	D0CN1569A
remotesupport	1.00	D0CN1598A
simpleauth	3.05.03	D0CN1540A
simpledirectcon	1.18	D0CN1549
simpleprinter	1.00	D0CN1570A
smartcopy	1.01	D0CN1571B
smartfax	1.00	D0CN1573A
smartprtstoredj	1.00	D0CN1575A
smartscanner	1.00	D0CN1572A
smartscannerex	2.03	D0CN1593A
stopwidget	1.00	D0CN1543A
tonerstate	1.00	D0CN1561A
voicecontrolser	1.00	D0CN1513A
Engine	1.04:02	D0CN5520G
ADF	01.040:02	D3HA5260C
TDCU	0.07.1:05	D0CN5530

表2-2 本体のハードウェアの識別情報

名称	バージョン	部番
Ic Ctlr	03	(なし)
Ic Key	01024704	(なし)

表2-3 操作パネルユニットのソフトウェアの識別情報

名称	バージョン	部番
Firmware	1.04	D0CN1537E
Keymicon	9.10	(なし)
Application Site	3.02.01	D0CN1576A
Bluetooth Authentication Plugin	4.0.1	D0CN1548
BluetoothService	1.02	D0CN1568A
ChangeLanguages	1.00	D0CN1560A
Copy	1.01	D0CN1571B
CSPF	3.00.02	D0CN1541A
Direct Connection	1.18	D0CN1549

名称	バージョン	部番
Eco-friendly	1.00	D0CN1564A
Fax	1.00	D0CN1573A
FaxRXFile	1.00	D0CN1562A
GraphicData	1.01	D0CQ5784D
ICCardDispatcher	3.08.02	D0CN1578A
Installation Settings	0.41G25	D0CN1584B
iWnn IME	2.8.201	D0BQ1453C
iWnn IME Korean Pack	2.8.2	D0BQ1456A
iWnn IME SimplifiedChinesePack	2.8.2	D0BQ1454A
iWnn IME TraditionalChinesePack	2.8.2	D0BQ1455A
KerberosService	1.07.03	D0CN1595A
LegacyUIData	1.00	D0CQ5767C
MachineStatus	1.00	D0CQ1439A
MultiDevice Hub	2.01	D0BM1472A
Print/Scan(Memory Storage Device)	1.00	D0CN1574A
Printer	1.00	D0CN1570A
ProgramInfoService	1.00	D0CN1569A
Proximity Card Reader Support Plugin	3.03.02	D0CN1547A
Quick Card Authentication Config.	3.05.03	D0CN1540A
Quick PrintRelease	1.00	D0CN1575A
Remote Panel Operation	1.00	D0CN1597A
RemoteConnect Support	1.1	D0BQ1499B
RemoteSupportService	1.00	D0CN1598A
RicohScanGUIService	2.03	D0CN1593A
Scanner	1.00	D0CN1572A
Smart Device Connector	4.1.0	D0CN1542
Standard ICCardPlugin	3.03.02	D0CN1546A
Stop	1.00	D0CN1543A
SupplyInformation	1.00	D0CN1561A
Support Settings	1.00	D0CN1596A
VoiceControlService	1.00	D0CN1513A

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOEはMFPに蓄積された文書に対する不正なアクセスに対抗するためのセキュリティ機能、及びネットワーク上の通信データを保護するためのセキュリティ機能を提供する。

TOEは組織のセキュリティ方針を満たすため、内部の保存データを上書き消去する機能、HDDの記録データを暗号化する機能、及びファクスI/Fを経由した電話回線網からの不正アクセスを防ぐ機能を提供する。

また、上記セキュリティ機能に関する各種設定を管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

本TOEのセキュリティ機能において保護の対象とする資産を表3-1、及び表3-2に示す。

表3-1 TOE保護資産（利用者情報）

種別	資産内容
文書情報	デジタル化されたTOEの管理下にある文書、削除された文書、一時的な文書あるいはその断片。
機能情報	利用者が指示したジョブ。（以下、「利用者ジョブ」という。）

表3-2 TOE保護資産（TSF情報）

種別	資産内容
保護情報	編集権限を持った利用者以外の変更から保護しなければならない情報。 ログインユーザー名、ログインパスワード入力許容回数、年月日、時刻、パスワード最小桁数等が含まれる。 （以下、「TSF保護情報」という。）
秘密情報	編集権限を持った利用者以外の変更から保護し、参照権限を持った利用者以外での読出しから保護しなければならない情報。 ログインパスワード、監査ログ、HDD暗号鍵がある。 （以下、「TSF秘密情報」という。）

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-3 に示す脅威を想定し、これに対抗する機能を備える。表 3-3 の脅威は、適合 PP で定義された脅威を、原文の英文から日本語に翻訳したものであり、両者の同等性については評価の過程において確認されている。

表3-3 想定する脅威

識別子	脅威
T.DOC.DIS (文書の開示)	TOEが管理している文書が、ログインユーザー名を持たない者、あるいはログインユーザー名は持っているがその文書へのアクセス権限を持たない者によって閲覧されるかもしれない。
T.DOC.ALT (文書の改変)	TOEが管理している文書が、ログインユーザー名を持たない者、あるいはログインユーザー名は持っているがその文書へのアクセス権限を持たない者によって改変されるかもしれない。
T.FUNC.ALT (利用者ジョブの改変)	TOEが管理している利用者ジョブが、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがその利用者ジョブへのアクセス権限を持たない者によって改変されるかもしれない。
T.PROT.ALT (TSF保護情報の改変)	TOEが管理しているTSF保護情報が、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF保護情報へのアクセス権限を持たない者によって改変されるかもしれない。
T.CONF.DIS (TSF秘密情報の開示)	TOEが管理しているTSF秘密情報が、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF秘密情報へのアクセス権限を持たない者によって閲覧されるかもしれない。
T.CONF.ALT (TSF秘密情報の改変)	TOEが管理しているTSF秘密情報が、ログインユーザー名を持たない者、あるいは、ログインユーザー名は持っているがそのTSF秘密情報へのアクセス権限を持たない者によって改変されるかもしれない。

※ 「ログインユーザー名を持つ者」とはTOEの利用を許可された者を表す。

3.1.1.2 脅威に対するセキュリティ機能方針

表 3-3 に示す全ての脅威は、TOE の正当な利用者以外の者、もしくは正当な権限を有さない者による利用者情報、TSF 情報への侵害（閲覧、改ざん）に関するものである。

これら脅威に対しては下記のセキュリティ機能により対抗する。

(1) 利用者の識別認証

利用者に対してログインユーザー名、ログインパスワードの入力要求を行い、入力された情報がTOE内部で管理されている利用者の認証情報に一致することを確認することで、TOEを利用しようとする者が許可利用者であるかを検証する。入力手段としては、TOE本体操作パネルからの入力、クライアントPCのWebブラウザ上からの入力、プリンター機能使用時及びPCファクス機能使用時のドライバー経由での入力がある。

必要な機能強度を確保する手段として下記の機能を提供する。

- ・ MFP管理者により設定された規定回数連続して認証に失敗すると、そのユーザーアカウントはロックアウトされる（ロックアウト時間が経過、または解除されるまでそのユーザーアカウントは使用できなくなる）
- ・ ログインパスワードについてはその長さ（桁数）、文字種別に関して一定品質以上のものが設定時に要求される

ログインパスワードの正当性が確認され許可利用者と判断された場合、その利用者の役割毎に予め規定されたTOEの利用権限が与えられ、TOEの利用が許可される。TOEが特定する役割は「表4-2 TOE利用者」に示すとおり、一般利用者、MFP管理者、スーパーバイザーである。

また、識別認証機能をサポートする手段として下記の機能を有する。

- ・ 入力画面に入力されたログインパスワードに対して、ダミー文字を表示する
- ・ ログイン後一定時間TOEに対する操作が行われない場合には自動的にログアウトする

(2) アクセス制御（利用者情報に対するアクセス制御）

利用者からの処理要求に対して、その利用者のログインユーザー名、役割毎の権限を元に文書情報、及び利用者ジョブへの操作に対してアクセス制御を実施する。蓄積文書には、どの利用者に対して操作（削除、印刷、ダウンロード等）を許可するかを規定する情報（文書利用者リスト）が関連付けられており、一般利用者から

の操作要求に対してそのログインユーザー名と文書利用者リストの情報から、許可もしくは拒否の制御を行う。MFP管理者の蓄積文書に対する操作としては、全ての蓄積文書に対して削除権限のみが与えられる。

利用者ジョブに対しても、そのジョブを作成したログインユーザー名が関連付けられており、ログインユーザー名が一致する一般利用者には該当ジョブの削除操作が許可される。MFP管理者に対しては全ての利用者ジョブに対して削除権限が与えられる。スーパーバイザーに対しては、利用者情報に関して全ての操作が禁止される。

(3) 残存情報削除

HDDに残存する削除済みの文書、一時的に利用された文書、その断片に対する不正なアクセスを防ぐため、文書が削除される際に指定データを上書きし残存情報が残らないようにする。

(4) ネットワーク保護

通信経路のモニタリングによる情報漏えいを防ぐため、TOEとクライアント間のWebブラウザ経由での操作に関する通信、プリンター機能及びPCファクス機能を使用した通信についてTLS暗号化通信を使用する。また、TOEと相手先との通信にはIPsec通信、及びS/MIME通信を使用する。

(5) セキュリティ管理

TSF情報に対する、利用者の権限を超えた不正なアクセスを防ぐためTOE利用者の役割によってTOE設定情報の参照・改変、利用者情報の新規登録、改変等に対するアクセス制御を行う。情報の改変（変更）に関する権限のポリシーとしては、一般利用者は自身のログインパスワード改変のみ権限を有し、スーパーバイザーは自身、及びMFP管理者のログインパスワード改変のみ権限を有している。それ以外の改変はMFP管理者にのみ許可される。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 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 3-4 に示す。P.STORAGE.ENCRYPTION を除くセキュリティ方針は、適合 PP に記載されているものと同様であることが評価の過程で確認されている。

P.STORAGE.ENCRYPTION は HDD へのデータ書き込みを、直接読み取れない形式で行なうことを想定したセキュリティ方針である。

表3-4 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.USER. AUTHORIZATION (利用者の識別認証)	TOE利用の許可を受けた利用者だけがTOEを利用することができるようにしなければならない。
P.SOFTWARE. VERIFICATION (ソフトウェア検証)	TSFの実行コードを自己検証できる手段を持たなければならない。
P.AUDIT.LOGGING (監査ログ記録管理)	TOEはTOEの使用及びセキュリティに関連する事象のログを監査ログとして記録維持し、監査ログが権限を持たない者によって開示あるいは改変されないように管理できなければならない。さらに権限を持つものが、そのログを閲覧できるようにしなければならない。
P.INTERFACE. MANAGEMENT (外部インタフェース管理)	TOEの外部インタフェースが権限外のものに利用されることを防ぐため、それらのインタフェースはTOEとIT環境により、適切に制御されていなければならない。
P.STORAGE. ENCRYPTION (記憶装置暗号化)	TOEのHDDに記録しているデータは、暗号化されていなければならない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-4 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.USER.AUTHORIZATION」への対応

このセキュリティ方針は、TOEに正式に登録されたユーザーのみにTOEを使用させることを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a) 利用者の識別認証

3.1.1.2に記載の識別認証により、TOEを利用しようとする者が許可利用者であるかを、利用者から取得した識別認証情報を使って検証し、許可利用者と判断された場合にのみ、その利用者の役割毎に予め規定されたTOEの利用権限を与えTOEの利用を許可する。

(2) 組織のセキュリティ方針「P.SOFTWARE.VERIFICATION」への対応

このセキュリティ方針は、TOEの実行コードの正当性について、自己検証できる

ことを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a) 自己テスト

TOE (FCU以外の構成要素) は、電源投入後の初期立ち上げ中に自己テストを実行し、MFP制御ソフトウェア及び操作パネル制御ソフトウェアの実行コードの完全性、正当性の確認を行う。自己テストではファームウェアのハッシュ値を検証し実行コードの完全性を確認し、各アプリケーションに対して、署名鍵ベースでの検証を行い実行コードの正当性を確認する。

自己テスト中にMFP制御ソフトウェアに何らかの異常が認められた場合は、操作パネルにエラー表示を行い、一般利用者がTOEを利用できない状態で動作停止する。また、操作パネル制御ソフトウェアの異常が認められた場合は、一般利用者が操作パネルからTOEを利用できない状態になる。自己テストで異常が認められなかった場合は、立上げ処理を続行し利用者がTOEを利用できる状態にする。

FCUについては、完全性検証を行うための検証情報を利用者が確認できる形で提供し、利用者がこの情報を基に確認を行い、問題がない場合にTOEを使用する。

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

このセキュリティ方針は、TOEのセキュリティ事象に関する監査ログを取得し、適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(a) セキュリティ監査

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、利用者識別、発生日時、結果等の項目から成る監査ログを生成し、監査ログファイルに追加保存する。生成した監査ログファイルは識別認証に成功したMFP管理者のみに読出し、削除を許可する。監査ログファイルの読出しはクライアントPCのWebブラウザを介してテキスト形式で行う。

また、監査ログの事象発生日時を記録するため、日付、時間情報をTOEのシステム時計から取得する。

(4) 組織のセキュリティ方針「P.INTERFACE.MANAGEMENT」への対応

このセキュリティ方針は、TOEが提供する外部インタフェース（操作パネル、LANインタフェース、USBインタフェース、電話回線）が不正な利用者に使用されないように適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する

(a) 利用者の識別認証

3.1.1.2に記載の識別認証により、TOEを利用しようとする者が許可利用者であるかを、利用者から取得した識別認証情報を使って検証し、許可利用者と判断された場合にのみ、その利用者の役割毎に予め規定されたTOEの利用権限を与えTOEの利用を許可する。

(b) 外部インタフェース間の情報転送制御

本機能は能動的なメカニズムの実装ではなく、外部インタフェースのアーキテクチャ設計として対応するもので、外部から入力された情報に対する処理、及び外部インタフェースから送信される情報の制御についてはかならずTOEが関与することにより、外部インタフェース間で不正な情報転送が実施されることを防ぐ。

USBインタフェースについては、使用を無効化する設定で運用することにより、このインタフェースを使用した不正な情報転送を防ぐ。

(5) 組織のセキュリティ方針「P.STORAGE. ENCRYPTION」への対応

このセキュリティ方針は、TOEに内蔵するHDDの記録内容を暗号化することを求めている。TOEではこの方針を下記のセキュリティ機能で実現する。

(a) 蓄積データ保護機能

HDDに対して書き込み、読み出しを行う全てのデータを対象にAESによる暗号化、復号処理を行う。暗号化、復号処理の際には管理者操作により初期設置時に作成されTOE内に格納される256ビット長の鍵が使用される。

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。表 4-1 の前提条件は、適合 PP で定義された前提条件を、原文の英文から日本語に翻訳したものであり、両者の同等性については評価の過程において確認されている。

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

識別子	前提条件
A.ACCESS.MANAGED (アクセス管理)	ガイダンスに従ってTOE を安全で監視下における場所に設置し、権限を持たない者に物理的にアクセスされる機会を制限しているものとする。
A.USER.TRAINING (利用者教育)	MFP 管理責任者は、利用者が組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っているものとする。
A.ADMIN.TRAINING (管理者教育)	管理者は組織のセキュリティポリシーやその手順を認識しており、ガイダンスに従ってそれらのポリシーや手順に沿ったTOE の設定や処理ができるものとする。
A.ADMIN.TRUST (信頼できる管理者)	MFP 管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任しているものとする。

4.2 運用環境と構成

本 TOE はオフィスに設置され、ローカルエリアネットワーク（以下、「LAN」という。）で接続され、TOE 本体の操作パネル及び同様に LAN に接続されたクライアント PC から利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

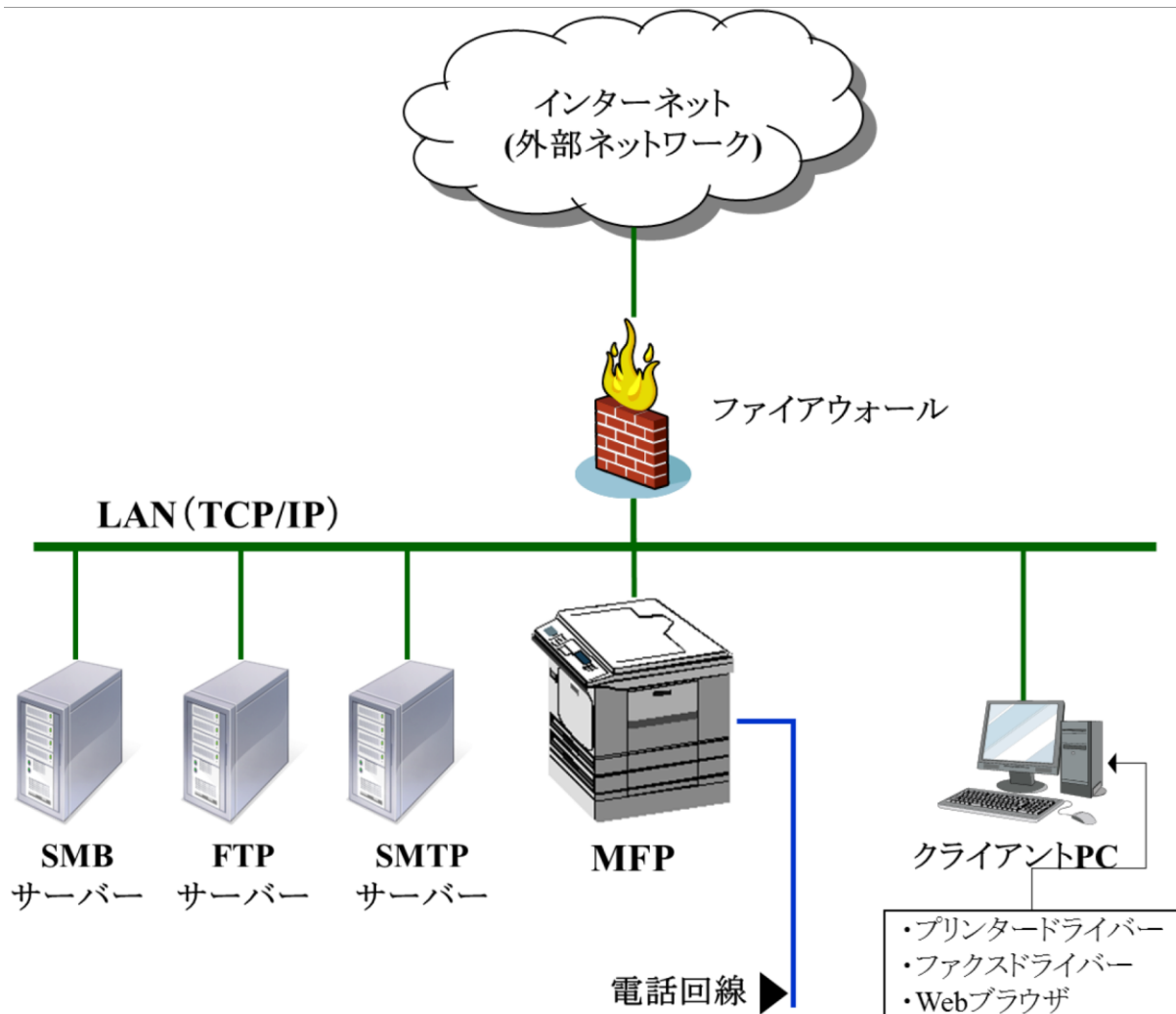


図4-1 TOEの運用環境

本TOEは、図4-1に示すような一般的な企業のオフィス等の書類を扱う環境において使用されることを想定している。TOEには、LAN、及び電話回線が接続される。

TOEをインターネット等の外部ネットワークに接続されたLANに接続する場合は、ネットワークを通じて、外部ネットワークからTOEへ攻撃が及ばないように、外部ネットワークとLANの境界にファイアウォールを設置して、LAN及びTOEを保護する。LANには、FTPサーバー、SMBサーバー、SMTPサーバー等のサーバーコンピュータ、及びクライアントPCが接続され、TOEと文書、各種情報収集等の通信を行う。

TOEの操作は、TOEの操作パネルを使用する場合と、クライアントPCを使用する場合とがある。クライアントPCにプリンタードライバーあるいはファクスドライバーをインストールすることによって、クライアントPCからローカルエリアネットワーク経由した印刷等を行うことができる。

運用環境の各機器の想定は以下のとおりである。

- クライアントPC
 - OS : Windows 8.1/10
 - Webブラウザ : Internet Explorer11, Microsoft Edge 44
 - プリンタードライバー(北米仕向け、アジア太平洋仕向けの場合) :
PCL6 Driver 1.0.0.0
 - プリンタードライバー(欧州仕向けの場合) :
PCL6 Driver 1.4.0.0
 - ファクスドライバー : LAN Fax Driver 9.5.0.0
- SMTPサーバー : Windows Server2012 P-Mail Server Manager
- FTPサーバー : Windows Server2012 (IIS8), Linux (Fedora20) vsftpd
- SMBサーバー : Windows Server2012

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が、十分に信頼できるものとする。

また、本環境においてTOEを利用するにあたり、関連する利用者を表4-2に示す。

表4-2 TOE利用者

利用者定義		説明
一般利用者		TOEの使用を許可された利用者。ログインユーザー名を付与され通常のMFP機能の利用ができる。
管理者	スーパーバイザー	MFP管理者のログインパスワードを改変する権限を持つ。
	MFP管理者	TOEの管理を許可された利用者。一般利用者の管理、機器管理、文書管理、ネットワーク管理の管理業務を行う。

表4-2に示すとおり、TOEの利用者は一般利用者、管理者に分類され、さらにその役割によって管理者はスーパーバイザーとMFP管理者とに分類される。TOEを直接利用する利用者としては表4-2に示すとおりであるが、それ以外にMFP管理者及びスーパーバイザーの選任権限を持つMFP管理責任者がTOEの間接的な利用者として存在する。MFP管理責任者は運用環境における組織の責任者等を想定している。

4.3 運用環境におけるTOE範囲

TOE とクライアント PC、TOE と各種サーバーの通信経路上のデータの保護のためには、クライアント PC や各種サーバーにおいても通信プロトコルが正しく動作するようにセキュアに運用されることが必要である。

クライアント PC や各種サーバーが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。TOE は MFP 製品全体である。

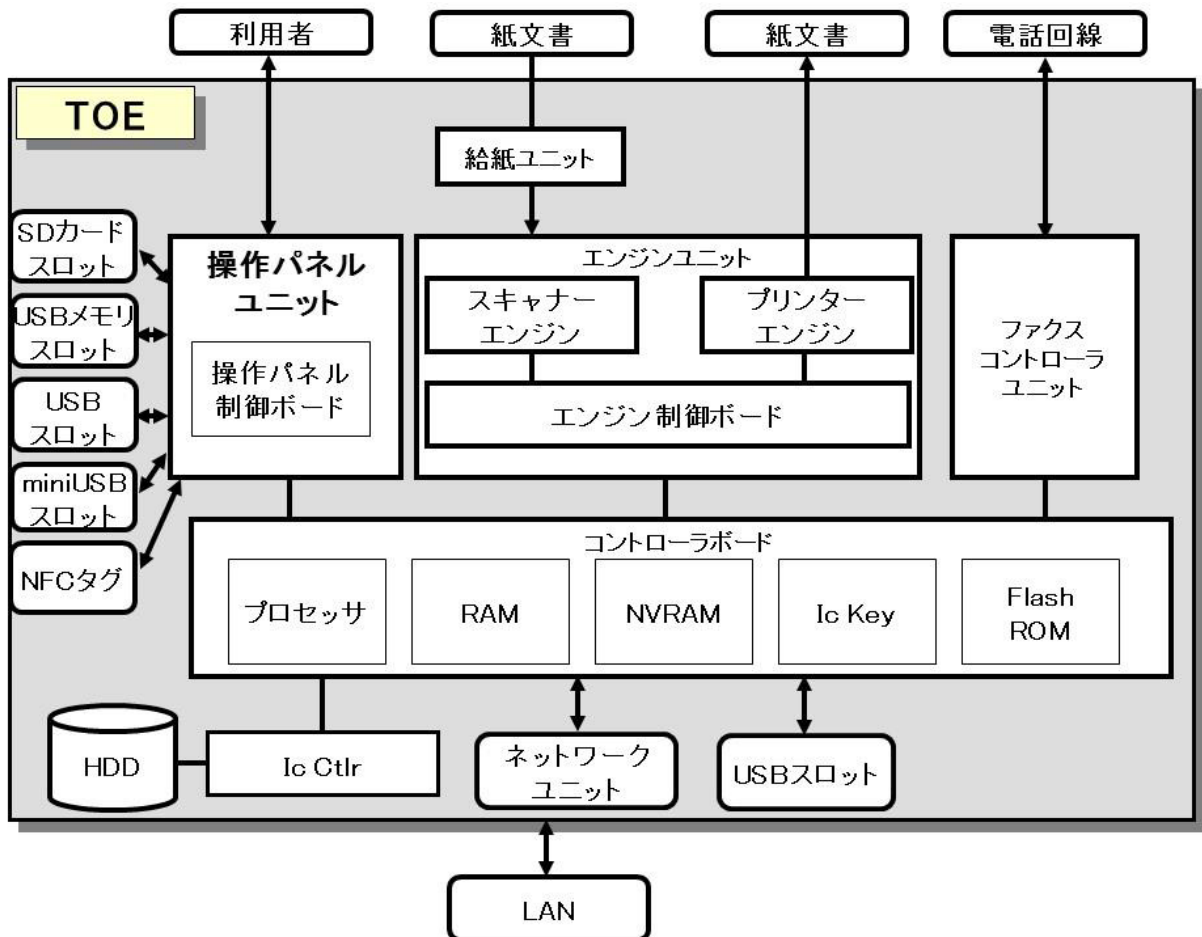


図5-1 TOE境界

以下に各構成要素の概要を示す。

【操作パネルユニット（以下、「操作パネル」という。）】

操作パネルは、TOEに取り付けられている、TOEの利用者がTOE操作に使用するインタフェース装置である。ハードキー、LED、タッチパネル式液晶ディスプレイと操作パネル制御ボードで構成される。操作パネル制御ボードには、操作パネル制御ソフトウェアがインストールされる。

【エンジンユニット】

紙文書を読込むためのデバイスであるスキャナーエンジン、紙文書を印刷し排出するデバイスであるプリンターエンジン、各エンジンを制御するエンジン制御ボードから構成される。

【給紙ユニット】

給紙ユニットは自動原稿送り装置(ADF)(両面同時読み取り)である。

【ファクスコントローラユニット(FCU)】

モデム機能を持ち電話回線と接続し、G3規格で他のファクス装置とファクスの送受信をするユニット。

【コントローラボード】

コントローラボードはプロセッサ、RAM、NVRAM、Ic Key、FlashROM が載った基板である。各要素の簡潔な説明は以下のとおり。

- プロセッサ : MFP動作における基本的な演算処理を行う半導体チップ。
- RAM : 画像メモリとして利用される揮発性メモリ。
- NVRAM : MFPの動作を決定するMFP制御データが入った不揮発性メモリ。
- Ic Key : 乱数発生、暗号鍵生成の機能を持ち、MFP制御ソフトウェアの改ざん検知に利用されるセキュリティチップ。
- FlashROM : MFP制御ソフトウェアがインストールされている不揮発性メモリ。

【HDD】

イメージデータ、識別認証に利用するログインユーザー名とログインパスワードが書込まれるハードディスクドライブである。

【Ic Ctlr】

HDDに保存する情報を暗号化し、HDDから読み出す情報を復号する機能を持ったセキュリティチップである。

【ネットワークユニット】

EthernetをサポートしたLAN用の外部インタフェースである。

以下の構成要素は、通常運用においては使用されない。

- ・ USBスロット (コントローラボード)
- ・ SDカードスロット (操作パネルユニット)
- ・ USBメモリスロット (操作パネルユニット)
- ・ USBスロット (操作パネルユニット)
- ・ miniUSBスロット (操作パネルユニット)
- ・ NFCタグ

5.2 IT環境

TOEは、LANに接続され、FTPサーバー、SMBサーバー、SMTPサーバー等のサーバーコンピュータ及びクライアントPCと通信を行う。またTOEは、電話回線で接続された送信先のファクス装置とも通信を行う。

LANを經由して接続されたクライアントPCは、プリンタードライバーや、ファクスタドドライバー、Webブラウザを介してTOEを利用する。クライアントPCは、文書情報の送受信だけでなく、Webブラウザを介して管理機能の一部の操作やTOEの状態確認を行うことができる。

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以下に示す。本 TOE に添付されるドキュメントは販売地域により 3 種類のセットが存在する。各ドキュメントセット間の差異としては、英語表記の違い、ドキュメント構成の違い、国・地域によるレギュレーションの違い等があるが、内容の同一性については評価の過程で確認されている。

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。

[英語版] 北米向け製品添付ドキュメント

ドキュメント名	バージョン
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7066
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
For Users of This Product	D181-2597
Notes to Users in the United States of America	D219-7457
Note to users in Canada	D219-7460
Safety Information	D0CP-7475
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

[英語版] 欧州向け製品添付ドキュメント

ドキュメント名	バージョン
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7064
Notes for Users	D0CM-7065
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
Note to users EU Countries	D150-1468A
Safety Information	D0CP-7474
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

[英語版] アジア太平洋向け製品添付ドキュメント

ドキュメント名	バージョン
Safe Use of This Machine	D0CM-7062
Notes for Users	D0CM-7067
For Users of This Product	D0CM-7068
SOFTWARE LICENSE AGREEMENT	D0CM-7070
Safety Information	D0CP-7476
Operating Instructions Paper Fundamentals	D0CP-7477
Operator's Guide	D0CP-7478
Security Reference	D0CP-7493
Introduction and Basic Operations	D0CP-7479
Setup/System Settings	D0CP-7480
Copy	D0CP-7481
Document Server	D0CP-7482
Fax	D0CP-7483
Scan	D0CP-7484
Printer	D0CP-7485
Maintenance	D0CP-7486
Troubleshooting	D0CP-7487
Application Settings	D0CP-7488
Paper Settings	D0CP-7489
Specifications	D0CP-7490
Security	D0CP-7491
Copy (Classic)	D0CP-7494
Fax (Classic)	D0CP-7495
Scan (Classic)	D0CP-7496
Printer (Classic)	D0CP-7497
Driver Installation Guide	D0CP-7492
Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D0CP-7087
Notes on Security Functions	D0CP-7085
Help	83NHELENZ 1.00 v251

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。

7.2 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 TOE 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。

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 2 年 7 月に始まり、令和 3 年 3 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。開発現場への現地訪問については省略され、過去の認証案件での調査内容の再利用が可能であると評価機関の責任において判断されている。

また、令和 3 年 1 月に評価機関内または開発者サイトで開発者のテスト環境を使用し、開発者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、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、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評価に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(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7-1に、主な構成要素を表7-1に示す。

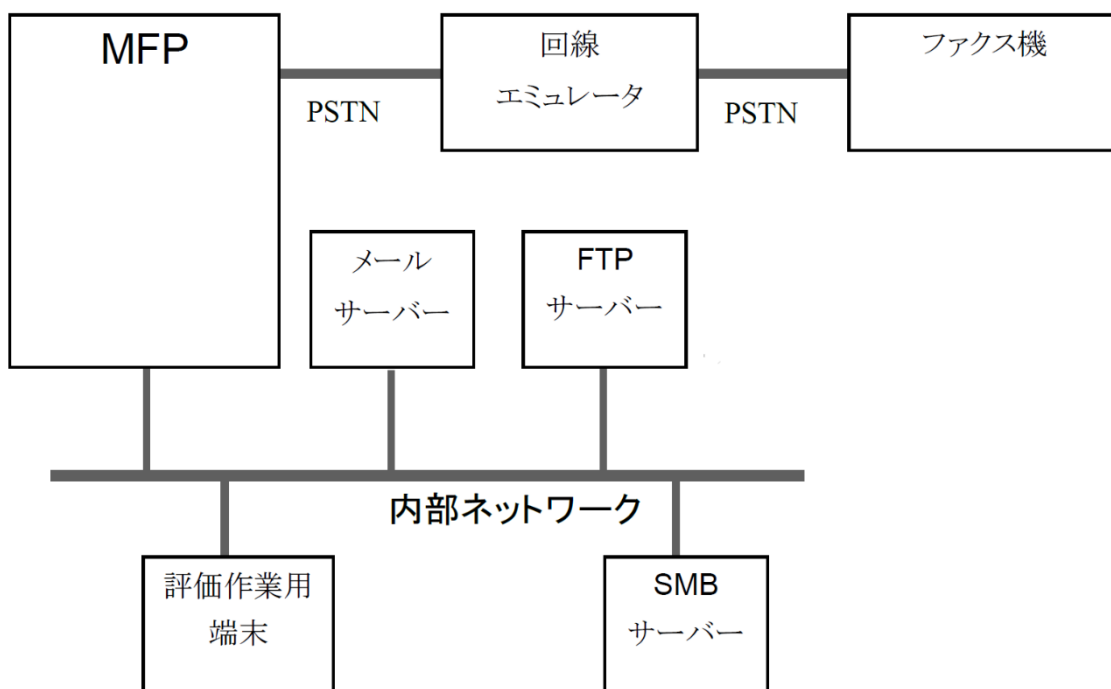


図7-1 開発者テスト構成図

表7-1 テスト構成要素

構成要素	詳細
TOE	MFP本体の名称がPro C5300Sの場合の構成(欧州仕向け) MFP本体の名称がPro C5300Sの場合の構成(北米仕向け) MFP本体の名称がPro C5310Sの場合の構成(アジア太平洋仕向け) (構成の具体的な内容は2章参照)
クライアントPC	OS : Windows 8.1/10 Webブラウザ : Internet Explorer11, Microsoft Edge 44 プリンタードライバー(北米仕向け、アジア太平洋仕向けの場合) : PCL6 Driver 1.0.0.0 プリンタードライバー(欧州仕向けの場合) : PCL6 Driver 1.4.0.0 ファクスドライバー : LAN Fax Driver 9.5.0.0
メールサーバー (SMTPサーバー)	Windows Server 2012 P-Mail Server Manager version 1.91
FTPサーバー	Windows Server 2012 IIS8 V8.0.9200.16384 Linux(Fedora20) vsftpd 3.0.2
SMBサーバー	Windows Server 2012
回線エミュレータ	XF-A150 (パナソニック社)
ファクス機	MP C6503

STではTOEとして複数のMFPの機種が識別されており、機種ごとの相違は印刷速度と仕向けによる表示の違いである。

開発者テストで使用されたTOEはそのうちの一部の機種であるが、印刷速度と仕向けによる表示の違いをそれぞれカバーする。

このことから、開発者テストは、本STにおいて識別されているTOE構成と一貫する環境で実施されたことが評価者により判断された。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

<開発者テスト手法>

開発者テストは通常のTOEの使用において想定される外部インタフェース（操作パネル、Webブラウザ等）を刺激し、結果を目視観察する方法の他、生成された監査ログ、及びデバッグ用ログデータの解析、パケットキャプチャによるクライアントPC、及び各種サーバーとTOE間の通信プロトコルの確認、TSF実装の一部を改造して異常なイベントを発生させる異常系テスト等も行われている。

<開発者テストツール>

開発者テストにおいて利用したツールを表 7-2 に示す。

表7-2 開発テストツール

名称（バージョン）	概要
Wireshark (2.2.5, 3.0.6, 3.0.11)	パケットキャプチャツール

<開発者テストの実施>

開発者が提供したテスト仕様書に記載された期待されるテスト結果の値と、同じく開発者が提供したテスト結果報告書に記載された開発者テストの結果の値を比較した。その結果、期待されるテスト結果の値と実際のテスト結果の値が一致していることが確認された。

b) 開発者テストの実施範囲

開発者テストは開発者によって約500項目実施された。カバレッジ分析によって、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テストされたことが検証された。

c) 結果

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実現されていることを再確認するサンプルテストを実施するとともに、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

をより確信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

評価者が実施した独立テストの構成は、図 7-1 に示した開発者テストと同様の構成である。

(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、開発者テスト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 入力パラメタの種類が多く、網羅性の観点で開発者テストが不足していると思われる TSFI に関して、パラメタの組み合わせ、境界値、異常値等のテスト項目を追加する。
- ② 複数の TSF の実行タイミング、実行の組み合わせに関して条件を追加したテスト項目を実施する。
- ③ 例外処理、キャンセル処理に関して開発者テストと異なるバリエーションを追加したテスト項目を実施する。
- ④ サンプルテストにおいては下記観点からテスト項目を選択する。
 - 網羅性の観点から、全ての TSF、TSFI が含まれるように項目を選択する。
 - 異なるテスト手法、テスト環境を網羅するように項目を選択する。
 - 多くの SFR が対応付けられ、効率よくテストが実施できる TSFI に関する項目を重点的に選択する。

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>

独立テストは、開発者テストとは異なる初期条件の設定や異なるパラメタを使用した上で、通常の TOE の使用において想定される外部インターフェー

ス(操作パネル、Web ブラウザ等)を刺激し、結果を目視観察する方法の他、生成された監査ログの解析、パケットキャプチャによるクライアント PC、及び各種サーバーと TOE 間の通信プロトコルの確認等が行われている。

<独立テストの実施内容>

独立テストの観点に基づき、独立テスト 23 件、サンプリングテスト 19 件のテストが実施された。

実施された主な独立テスト概要と、対応する独立テストの観点を表 7-3 に示す。

表7-3 実施した主な独立テスト

独立テストの観点	テスト概要
①	<ul style="list-style-type: none"> ・ユーザーアカウントロックに関する挙動が仕様どおりであることを条件等を変更しながら確認する。 ・蓄積文書のアクセス制御が仕様どおりであることを、アクセスの手段との組み合わせに関して確認する。 ・蓄積文書のアクセス制御が仕様どおりであることを、蓄積文書の編集との組み合わせに関して確認する。 ・操作パネルの表示のカスタマイズがセキュリティ機能に影響しないことを確認する。
②	<ul style="list-style-type: none"> ・同一の利用者が同時にログインしている状態でオートログアウト処理が仕様どおりに動作することを確認する。 ・ログイン中にオートログアウト時間を変更する場合のふるまいが仕様どおりであることを確認する。 ・異なるインターフェースから内部蓄積文書に対するアクセス権限の変更と内部蓄積文書の操作をした場合、仕様どおりのアクセス制御が行われることを確認する。 ・セキュリティに関する設定を一般利用者が変更できないことを、複数のインターフェースから確認する。

独立テストの観点	テスト概要
③	<ul style="list-style-type: none"> ・有効期限切れの証明書を用いた場合のIPsecの処理が仕様どおりであることを確認する。 ・プリンタードライバーからの不正な入力に対しても仕様どおりの例外処理が実施されることを確認する。 ・ファクス機能のエラー発生時、送信待機がフルの状態において、ファクス機能の動作が仕様どおりであることを確認する。 ・操作パネルに対して想定外の画面操作、パラメタ入力が行われても仕様どおりの処理が実施されることを確認する。 ・蓄積文書の編集において異常なパラメタ指定や中断等があっても、仕様どおりのアクセス制御が維持されることを確認する。 ・無効に設定した機能について、実際に無効になっ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 想定しないインタフェースが存在し、そこからTOEにアクセスできる可能性がある。
- ② インタフェースに対してTOEが意図しない値、形式のデータ入力が行われた場合、セキュリティ機能がバイパスされる可能性がある。
- ③ セキュアチャネルの実装に脆弱性が存在し、結果としてTOEのセキュリ

ティ機能がバイパスされる可能性がある。

- ④ 過負荷状態でTOEを運用することにより、セキュリティ機能がバイパスされる可能性がある。

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>

侵入テストは、図 7-1 に示した開発者テスト、及び評価者独立テストと同様の環境で実施された。

侵入テストで使用した主なツールを表 7-4 に示す。

表7-4 侵入テスト使用ツール

名称 (バージョン)	概要
ZAP (2.7.0)	プロキシ型のWeb脆弱性検査ツール
nmap (7.70)	ポートスキャンツール
Netcat (1.12)	パケット通信ツール
Nessus (8.8.0) Plugin 202101132029	脆弱性スキャンツール
Burp Suite Professional (1.7.37)	プロキシ型のWeb脆弱性検査ツール
Wireshark (2.2.5, 3.0.6, 3.0.11)	パケットキャプチャツール
OpenSSL 1.0.1j	SSL/TLSプロトコルを提供するソフトウェアライブラリ
PRET (0.40)	PJL、Postscriptテストツール
Android Debug Bridge (1.0.41)	Android OSを搭載したデバイス用のデバッグツール (TOEにAndroid OSが動作する部分があるため使用された)

<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概要を表 7-5 に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、15 件の侵入テストを実施した。

表7-5 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、脆弱性スキャンツール、デバッグツールを使用し、想定外の利用可能なインタフェースが存在しないことを確認する。
②	TOEへのアクセスを行う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。 Webブラウザ経由でのTOEへの接続時に指定するURLによりセキュリティ機能がバイパスされないことを確認する。 PjL、PostScript、SQLに関して実装上の脆弱性がないことを確認する。
③	TLS、IPsecを使用した暗号通信に関して実装上の脆弱性がないことを確認する。 Webインタフェースで使用されるパラメタの乱数性検証を行い、容易に推測されないことを確認する。
④	リソース枯渇状態においてTOEが非セキュアな状態になら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 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：
 - U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

また、上記PPで定義された以下のSFRパッケージに適合する。

- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
- 2600.2-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment B
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

- 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。

- EAL2パッケージのすべての保証コンポーネント
- 追加の保証コンポーネント ALC_FLR.2

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。
- 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で示されている方法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 CC パート 3 の EAL2 及び保証コンポーネント ALC_FLR.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

保守機能を有効化した場合、それ以降の運用での本 TOE のセキュリティ機能への影響については本評価の保証の範囲外となるため、保守の受け入れについては管理者の責任において判断されたい。

また本 TOE の利用者は、「4.3 運用環境における TOE 範囲」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実際の TOE 運用環境において対応可能かどうかについて注意する必要がある。

2 章で説明したように TOE 識別の確認には、TOE の表示等に加えて、梱包箱上のラベルシールの確認が必要である。TOE 識別を確認できるようにするために、ラベルシールに記載されている情報を保持する必要があるため、注意が必要である。

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。

RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S
セキュリティターゲット, バージョン 1.00, 2021 年 3 月 16 日, 株式会社リコー

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)
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。

FCU	ファクスコントローラユニットの略称。
HDD	ハードディスクドライブの略称。本書で、単にHDDと記載した場合はTOE内に取り付けられたHDDを指す。
IPsec	Security Architecture for Internet Protocol 暗号技術を用いて、IPパケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルである。
MFP	デジタル複合機の略称。
PSTN	Public Switched Telephone Networksの略で、公衆交換電話網の意味。
S/MIME	Secure / Multipurpose Internet Mail Extensions 公開鍵方式による電子メールの暗号化とデジタル署名に関する標準規格である。

本報告書で使用された用語の定義を以下に示す。

Internet Fax	メール送受信の仕組みを使ってファクス通信を行う機能。 インターネット回線を利用する。
IP-Fax	国際標準ITU-T T.38勧告に準拠したリコーのリアルタイム型インターネットファクスの総称。 ファクス番号の代わりに相手機のIPアドレスを指定する。

PCファクス機能	ファクス機能の1つ。クライアントPC上のファクスドライバーを利用して、ファクス送信、文書蓄積を行う機能。
管理者役割	<p>MFP管理者に割り当てることができる予め定義された役割。</p> <p>以下の4種類の管理者役割が定義され、それぞれ別の管理者に割り当てることが可能であるが、本TOEにおいては全ての役割が割り当てられたMFP管理者を想定している。</p> <p>(細分類された管理者役割毎のアクセス制御は本TOEの評価対象外となる)</p> <ul style="list-style-type: none"> ・ 機器管理者 (機器管理、監査の実施を行う) ・ ユーザー管理者 (一般利用者の管理を行う) ・ ネットワーク管理者 (TOEのネットワーク接続管理を行う) ・ 文書管理者 (蓄積文書、及び文書利用者リストの管理を行う)
蓄積文書	ドキュメントボックス機能、プリンター機能、スキャナー機能、及びファクス機能で利用するためにTOE内に蓄積されている文書。
文書	TOEが扱う紙文書、電子文書の総称。
保守機能	保守機能は機器故障時の保守サービス処理を実行する機能である。本TOEの運用においては、本機能が無効化する保守機能移行禁止設定が行われていることが前提となる。
利用者ジョブ	TOEのコピー、ドキュメントボックス、スキャナー、プリンター、ファクスの各機能の開始から終了までの作業。利用者ジョブは、開始から終了の間に利用者によって一時停止、キャンセルされることがある。利用者ジョブがキャンセルされた場合、利用者ジョブは終了となる。
ログインパスワード	各ログインユーザー名に対応したパスワード。
ログインパスワード入力許容回数	<p>識別認証時にユーザーアカウントがロックアウトされるまでに許容される、認証連続失敗回数。</p> <p>1～5回の設定値をMFP管理者が設定する。</p>
ログインユーザー名	一般利用者、MFP管理者、及びスーパーバイザーに与えられている識別子。TOEはその識別子により利用者を特定する。
ロックアウト	ユーザーアカウントが使用できなくなる状態。

ロックアウト 時間	ユーザーアカウントがロックアウト状態から自動的に解除されるまでの時間。
--------------	-------------------------------------

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30年7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30年9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30年9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] RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S セキュリティターゲット, バージョン 1.00, 2021年3月16日, 株式会社リコー

- [13] RICOH Pro C5300S/C5310S, SAVIN Pro C5300S/C5310S, LANIER Pro C5300S/C5310S, nashuatec Pro C5300S/C5310S, Rex Rotary Pro C5300S/C5310S, Gestetner Pro C5300S/C5310S, infotec Pro C5300S/C5310S 評価報告書, 第2.0版, 2021年3月31日, 株式会社 ECSEC Laboratory 評価センター
- [14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
- [15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership