



## 認 証 報 告 書

東京都文京区本駒込2丁目 ~~原番紙~~  
独立行政法人情報処理推進機構 ~~捺印済~~  
理事長 富田 達夫

### IT製品 (TOE)

申請受付日 (受付番号)	平成31年1月18日 (IT認証8702)
認証識別	JISEC-C0652
製品名称	Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model
バージョン及びリリース番号	1.0
製品製造者	キヤノン株式会社
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	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。

令和元年 9月25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

「Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model」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.....	2
1.3	評価の認証.....	2
2	TOE識別 .....	4
3	セキュリティ方針 .....	5
3.1	セキュリティ機能方針.....	6
3.1.1	脅威とセキュリティ機能方針.....	6
3.1.1.1	脅威 .....	6
3.1.1.2	脅威に対するセキュリティ機能方針 .....	6
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.....	8
3.1.2.1	組織のセキュリティ方針.....	8
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.....	9
4	前提条件と評価範囲の明確化 .....	11
4.1	使用及び環境に関する前提条件 .....	11
4.2	運用環境と構成.....	11
4.3	運用環境におけるTOE範囲 .....	13
5	アーキテクチャに関する情報 .....	15
5.1	TOE境界とコンポーネント構成.....	15
5.2	IT環境 .....	16
6	製品添付ドキュメント .....	18
7	評価機関による評価実施及び結果.....	19
7.1	評価機関.....	19
7.2	評価方法.....	19
7.3	評価実施概要 .....	19
7.4	製品テスト .....	20
7.4.1	開発者テスト .....	20
7.4.2	評価者独立テスト .....	23
7.4.3	評価者侵入テスト .....	26
7.5	評価構成について .....	28
7.6	評価結果.....	29

7.7	評価者コメント/勧告 .....	29
8	認証実施 .....	30
8.1	認証結果 .....	30
8.2	注意事項 .....	30
9	附属書 .....	31
10	セキュリティターゲット .....	31
11	用語 .....	32
12	参照 .....	35

# 1 全体要約

この認証報告書は、キヤノン株式会社が開発した「Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model バージョン 1.0」(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。)が令和元年 8 月 27 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キヤノン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 を購入する調達者及び一般消費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、コピー機能、プリント機能、送信(Universal Send)機能、ファクス機能、インターネットファクス機能、ユーザーボックス機能等を併せ持つデジタル複合機(以下「MFP」という。)である。

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 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。

そのため TOE は、それらの保護資産の不正な読出しや改ざんを防止するために、識別認証、アクセス制御、暗号化等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、次のような構成及び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。

### 1.1.3 免責事項

- ・ 本評価の対象となる識別認証は、プリントジョブの投入時には適用されない。プリントジョブの投入で使用するプロトコル自体が識別認証を備えていても、そのプロトコルの識別認証は本評価の対象外である。

## 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、令和元年 8 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： Canon imageRUNNER ADVANCE C35900KG (III)/C3500  
III Series 2600 model  
バージョン： 1.0  
開発者： キヤノン株式会社

本 TOE は、以下のソフトウェア、ハードウェアから構成される。

表2-1 TOEの構成品

	構成品	識別情報
和文	• iR-ADVセキュリティキット・AC1 for IEEE 2600 Ver 1.00 (制御ソフトウェア)	• [セキュリティキット for IEEE 2600]及び[コントローラーバージョン 1230]
	• Canon imageRUNNER ADVANCE C35900KG (III)/ C3500 III Series ファクス付き	• [iR-ADV C3530 III, iR-ADV C3525 III, iR-ADV C3520 III]のいずれか及び[Super G3 FAX Board-AZ]
	• Canon MFP Security Chip 2.11	• [Canon MFP Security Chip 2.11]
英文	• iR-ADV Security Kit-AC1 for IEEE 2600 Common Criteria Certification Ver 1.00 (system software)	• [Security Kit for IEEE 2600]及び [Controller Version 1230]
	• Canon imageRUNNER ADVANCE C35900KG (III)/ C3500 III Series with Fax	• [iR-ADV C3530 III, iR-ADV C3525 III, iR-ADV C3520 III]のいずれか及び[Super G3 FAX Board-AZ]
	• Canon MFP Security Chip 2.11	• [Canon MFP Security Chip 2.11]

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。

- MFP の操作パネルより、TOE の構成品の識別情報を確認する。

なお、本書では、表 2-1 の「Canon imageRUNNER ADVANCE C35900KG (III)/ C3500 III Series ファクス付き」及び「Canon imageRUNNER ADVANCE C35900KG (III)/ C3500 III Series with Fax」で示される構成品を「MFP 本体」という。

### 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、コピー機能、プリント機能、スキャン機能等の MFP 機能を提供しており、ユーザの文書データを内部の HDD 装置に蓄積したり、ネットワークを介してユーザの端末や各種サーバとやりとりしたりする機能を有している。

本 TOE が適合する PP は、比較的高いレベルのセキュリティ確保や操作の説明責任が求められる環境を想定しており、その環境で必要とされるセキュリティ機能要件を規定している。TOE は、MFP 機能を使用する際に、PP で要求されているセキュリティ機能要件を満たすセキュリティ機能を提供する。

TOE の提供するセキュリティ機能には、ユーザの識別認証とアクセス制御、HDD 装置の蓄積データの暗号化とデータ削除時の上書き消去、暗号通信プロトコル等が含まれており、保護資産であるユーザの文書データ及びセキュリティに影響する設定データを保護する。

なお、TOE は、使用に関して以下の役割を想定している。

- U.NORMAL

TOE が提供するコピー機能、プリント機能、スキャン機能等の TOE のユーザである。

- U.ADMINISTRATOR

TOE のセキュリティ機能の設定を行うための特別な権限を持つ TOE のユーザである。

- TOE Owner

TOE 資産の保護や、TOE の運用環境のセキュリティ対策方針の実現に責任を持つ人物または組織である。

また、TOE の保護資産は以下のものである。

- User Document Data

ユーザの文書データ。

- User Function Data

TOE によって処理されるユーザの文書データやジョブに関連する情報。プリントの優先度とプリント設定が含まれる。

- TSF Confidential Data

セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められる



るデータ。ユーザのパスワード、ボックス暗証番号、監査ログが含まれる。なお暗号鍵は、ユーザが操作可能なインタフェースが存在しないため、含まれない。

・TSF Protected Data

セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。ユーザの識別情報や権限情報等が含まれる。

### 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 3-1 に示す脅威を想定し、これに対抗する機能を備える。これらの脅威は、PP に記述されているものと同じである。

表3-1 想定する脅威

識別子	脅威
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons.

##### 3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.DOC.DIS」「T.DOC.ALT」「T.FUNC.ALT」への対抗

これらは利用者のデータに対する脅威であり、TOEは、「ユーザ認証機能」、「ジョブ実行アクセス制御機能」、「投入ジョブアクセス制御機能」、「HDDデータ完全消去機能」及び「LANデータ保護機能」で対抗する。

TOEの「ユーザ認証機能」「ジョブ実行アクセス制御機能」は、正当な利用者だけにTOEの利用を許可する。これらの機能の詳細は、3.1.2.2のP.USER\_AUTHORIZATIONの項目を参照。

TOEの「投入ジョブアクセス制御機能」は、識別認証された利用者が、TOEに保存されたプリントジョブとファクス/Iファクスジョブの文書、及びボックスに保存された文書に対して、プリント、プレビュー、ネットワークへの送信、ファクス送信、削除、プリントの優先度の変更、プリント設定の変更の操作をする際にアクセス制御を行い、操作対象の文書の所有者とU.ADMINISTRATORに当該操作を許可する。識別認証された利用者が文書の所有者であるかどうかは、以下のように判定される。

- プリントジョブとして投入された文書の場合には、識別認証された利用者のユーザ名が、プリントジョブ投入時に指定されたユーザ名と一致する場合、所有者であると判定される。
- スキャン機能やファクス/Iファクスなどプリントジョブ以外の手段によって保存された文書の場合には、操作時にボックス暗証番号の入力が求められる。文書を格納するためのボックスは、ユーザ毎に割当てられ事前に7桁のボックス暗証番号が設定されている。利用者が入力したボックス暗証番号と、ユーザ毎のボックスに事前設定されたボックス暗証番号が一致する場合、所有者であると判定される。

TOEの「HDDデータ完全消去機能」は、文書ファイルを削除する際に、文書ファイルが格納されていたHDD領域を上書き消去し、削除した文書ファイルの内容がHDDから読み出されることを防止する。

TOEの「LANデータ保護機能」は、TOEがLANを經由して他のIT機器と通信する際に、暗号通信プロトコルであるIPsecを適用し、通信データが漏えいしたり改ざんされたりすることを防止する。

以上の機能により、TOEは、TOEの権限外使用や、HDDに格納されたデータや通信データへの不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

## (2) 脅威「T.PROT.ALT」「T.CONF.DIS」「T.CONF.ALT」への対抗

これらはセキュリティ機能に影響するTSFデータに対する脅威であり、TOEは、「ユーザ認証機能」、「管理機能」及び「LANデータ保護機能」で対抗する。

TOEの「管理機能」は、利用者情報の管理や、各種設定データの管理を、識別認証されたU.ADMINISTRATORだけに許可する。ただし、U.NORMALは、自身のパスワード及び自身の利用するボックスのボックス暗証番号の変更は許可される。

その他の「ユーザ認証機能」及び「LANデータ保護機能」は、(1)の場合と同じである。

以上の機能により、TOE は、TOE の権限外使用や、HDD に格納されたデータや通信データへの不正アクセスによって、保護対象のデータが漏えいしたり改ざんされたりすることを防止する。

### 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 3-2 に示す。これらの組織のセキュリティ方針は、P.STORAGE.CRYPT を除き PP に記述されているものと同じである。

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.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.STORAGE.CRYPT *1	TOEのHDDに記録するデータは、暗号化されていなければならない。

\*1: 「P.STORAGE.CRYPT」は、顧客が HDD に記録するデータを暗号化する機能を要求することが想定されるため設定された。

### 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 3-2 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

TOEは、「ユーザ認証機能」、「ジョブ実行アクセス制御機能」で本方針を実現する。

TOEの「ユーザ認証機能」は、識別認証の成功した利用者だけにTOEの利用を許可する。さらにTOEは、識別認証機能を補強するために、認証用のパスワードは、規定された長さや文字種を混在した文字列に限定し、規定回数連続して認証失敗した場合には、識別認証を規定時間停止する。

なお、プリントジョブの投入、およびファクス/Iファクスの受信は、識別認証なしで受け付ける。しかし、それらの受け付けた文書は、受け付けた時点ではプリントや送信はされずTOE内に格納される。TOEに格納された文書のプリントや送信を行うためにはTOEの操作パネルでの操作が必要であり、識別認証が要求される。

TOEの「ジョブ実行アクセス制御機能」は、識別認証された利用者がTOEの機能を使用する際にアクセス制御を行い、権限のある利用者だけに実行を許可する。アクセス制御では、利用者に設定された「ロール」と呼ばれる権限情報を参照し、対象機能の実行が許可されているかどうかを判断する。

これらにより、TOEは、正当な利用者だけに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

TOEは、「自己テスト機能」で本方針を実現する。

TOEの「自己テスト機能」は、起動時に、HDDに暗号化されて格納されている実行コードを復号した後、LANデータ保護機能で使用する暗号アルゴリズム及び監査ログの完全性をチェックする。それにより、TOEセキュリティ機能の実行コードの完全性が検査される。

なお、本機能は、TOEセキュリティ機能の実行コードの一部分だけをチェックしているが、その部分の完全性が確認されれば、同じメカニズムで復号された他の実行コードも完全であるという評価がされている。

#### (3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

TOEは、「監査ログ機能」で本方針を実現する。

TOEの「監査ログ機能」は、セキュリティ機能の使用において、セキュリティ事象が発生した際に監査ログを生成しTOEのHDDに格納する。格納された監査ログは、識別認証されたU.ADMINISTRATORだけがWebブラウザを使用して読み出すことができる。

TOEは、格納された監査ログを監査ログ用のサーバに送信することが可能である。

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

TOEは、「ユーザ認証機能」と「受信ジョブ転送機能」で、本方針を実現する。

TOEの「ユーザ認証機能」は、識別認証の成功した利用者だけにTOEの利用を許可する。また、利用者が操作をしない状態が規定時間経過した場合には、セッションを切断する。

また、TOEの「受信ジョブ転送機能」は、TOEの各種インタフェースから受信したデータを、TOEが処理せずにLANに転送することができないしくみになっている。

これらにより、TOEのインタフェースが不正に使用されることを防止する。

(5) 組織のセキュリティ方針「P.STORAGE.CRYPT.」への対応

TOEは、「HDD暗号化機能」で、本方針を実現する。

TOEの「HDD暗号化機能」は、TOEが備えているHDDに格納される全データを暗号化することにより、データの機密性を確保する。なお、暗号アルゴリズムは256bitのAESであり、暗号鍵は起動時にNIST SP800-90Aの決定論的乱数生成メカニズムに従って生成され、電源オフにより消去される。

## 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。これらの前提条件は、PP に記述されているものと同じである。

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	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.  ※ "correctly configure" には、例えば「8.2 注意事項」の(1)のような内容が含まれる。
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

### 4.2 運用環境と構成

TOE である MFP は、一般的な業務オフィスにおいて、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワークに接続されて利用されることを想定している。本 TOE の一般的な運用環境を図 4-1 に示す。

TOE の利用者は、TOE の操作パネル、USB に接続された PC、LAN に接続された PC を操作して、TOE を使用する。

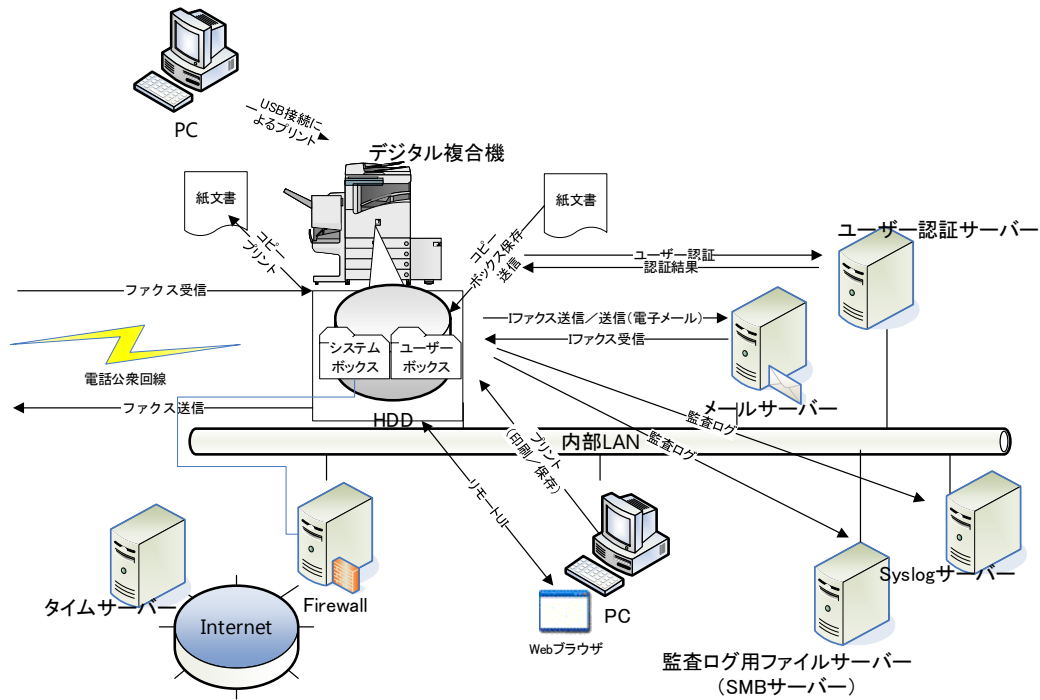


図4-1 TOE の運用環境

TOE の使用環境の構成品について以下に示す。

(1) ファクスボード (2回線目以降のオプション)

必要に応じて、以下のファクスボードを装着可能である。これらのファクスボードはTOEには含まれない。

- ・ G3回線増設キット (2回線) ・ AU

(2) PC

利用者が使用する汎用のPCであり、USBまたは内部LANを介してTOEと接続する。以下のソフトウェアが必要である。

- ・ プリンタドライバ: 本評価では、以下のプリンタドライバを使用。
  - Canon Generic Plus LIPSLX Printer Driver Version 2.00
  - Canon Generic Plus PS3 Printer Driver Version 2.00
  - Canon Generic Plus PCL Printer Driver Version 2.00
- ・ Webブラウザ: 本評価では、Microsoft Internet Explorer 11 を使用した。

(3) ユーザ認証サーバ

3章で説明したTOEの「ユーザ認証機能」は、TOE内に保存されている利用者情報を使用する「内部認証方式」と、外部のサーバに登録されている利用者

情報を使用する「外部認証方式」をサポートしている。

ユーザ認証サーバは、TOEで「外部認証方式」を使用する場合に必要なサーバである。認証プロトコルは、KerberosまたはLDAP認証方式である。

本評価では、LDAP認証方式を使用する場合、認証サーバソフトウェアとしてeDirectory 8.8 SP8、Kerberos認証方式を使用する場合、Active Directory Domain Serviceを使用した。

#### (4) 監査ログ用ファイルサーバ

SMBサーバであり、TOEから送信される監査ログを保存する。

本評価では、Windows Server 2012 R2 Standard Edition を使用した。

#### (5) syslogサーバ

TOEが、syslogプロトコルを使用して、監査ログを保存するサーバである。

本評価では、psyslog v1.04を使用した。

#### (6) メールサーバ

MFPのIファクス機能を利用する際に、必要に応じて設置する。

本評価では、Microsoft Exchange Server 2013を使用した。

#### (7) タイムサーバ

インターネットで一般に提供されているNTPサービスである。監査ログのタイムスタンプに使用されるMFPの時刻を同期させるために、使用可能な環境の場合にはTOEに設定することが推奨される。設定しない運用も可能であるが、その場合、TOEの管理機能で設定され維持される時刻が使用される。

本評価では、Windows Timeを使用した。

なお、本構成に示されている TOE 以外のソフトウェアやハードウェアの信頼性は本評価の範囲ではない。

### 4.3 運用環境におけるTOE範囲

本評価では、MFPのプリント機能に対して、PPが要求している識別認証のセキュリティ機能要件は、MFPにプリントジョブを投入する操作は適用対象外であり、MFPにプリントジョブとして投入され蓄積された文書に対するプリント等の操作



だけが適用対象であるという解釈がされている。そのため、以下は評価対象のセキュリティ機能ではない。

- ① **TOE**では、プリントジョブの投入で、各種のプリント用のプロトコルをサポートしている。プロトコルによっては、プロトコル自体が識別認証の機能を備えているが、それらは評価対象のセキュリティ機能ではない。例えば、IPPプロトコルが備えている識別認証などが該当する。

## 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（サブシステム）を説明する。

### 5.1 TOE境界とコンポーネント構成

図 5-1 に、TOE である MFP の構成を、MFP 以外の IT 環境と共に示す。図 5-1 で、TOE は中央の TOE と記述した太線で囲まれている部分であり、ユーザ認証サーバ、監査ログ用ファイルサーバ、syslog サーバ、メールサーバ、PC、タイムサーバ、ユーザは含まない。

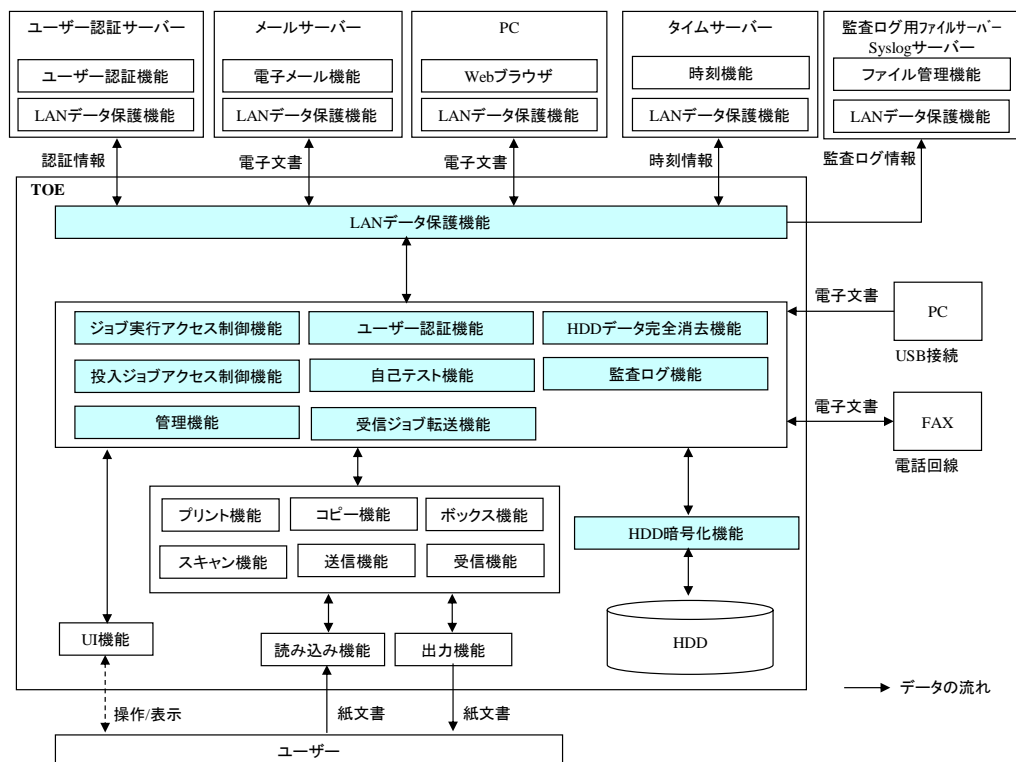


図 5-1 TOE 境界

また、図5-1で、TOE 内の色付の機能は3章で説明したセキュリティ機能であり、それ以外の機能は MFP の基本機能である。MFP の基本機能については、11章の用語説明を参照。

TOE の利用者は、TOE の操作パネル（図5-1では UI 機能に相当）、LAN 接続された PC の Web ブラウザ（図5-1では PC の Web ブラウザに相当）、LAN または USB 接続された PC のプリンタドライバ（図5-1では PC は図示されているがプリンタドライバは省略されている。）を操作して、TOE を使用する。

TOE のセキュリティ機能は、利用者が MFP の基本機能を使用する際に適用される。以下、セキュリティ機能と MFP の基本機能の関係について説明する。

- ① 利用者が LAN または USB 接続された PC からプリントジョブを投入した場合、およびファクス/Iファクスを受信した場合には、識別認証なしで文書を受け付け、TOE 内に格納される。TOE 内に格納された文書は、操作パネルや Web ブラウザを操作して利用する。

利用者が、操作パネルや Web ブラウザを操作して、TOE の基本機能を使用する際には、まず「ユーザ認証機能」と「ジョブ実行アクセス制御機能」が適用され、正当な利用者だけに TOE の操作が許可される。さらに当該利用者が TOE に格納されている文書を操作する際には「投入ジョブアクセス制御機能」が適用され、操作対象の文書の所有者と管理者の操作だけが許可される。

利用者が、操作パネルや Web ブラウザを操作して、セキュリティ機能の「管理機能」や「監査ログ機能」の中の監査ログを参照する機能を使用する際には、「ユーザ認証機能」が適用され、識別認証された管理者権限を持つ利用者だけに TOE の操作が許可される。

なお、これらのセキュリティ機能を使用する際に、「監査ログ機能」によって、監査ログが生成される。監査ログは HDD に格納される。また、監査ログを監査ログ用ファイルサーバ及び syslog サーバに出力することが可能である。

- ② ①の利用時に、内蔵 HDD 装置に格納されるデータ全体に対して、「HDD 暗号化機能」が適用される。文書データを削除する際には、「HDD データ完全消去機能」が適用される。
- ③ ①の利用時に、TOE と、その他の IT 機器が LAN を経由して通信する場合には、「LAN データ保護機能」が適用される。また、「受信ジョブ転送機能」により、各種インタフェースから入力されたデータに対して、TOE のセキュリティ機能が介在しない不正な中継が防止される。

## 5.2 IT 環境

TOE の「ユーザ認証機能」で外部認証方式を使用する場合は、Kerberos または LDAP のプロトコルでユーザ認証サーバが参照され識別認証が実施される。ユーザ認証サーバへの利用者情報の登録は、ユーザ認証サーバの管理機能で行う。

TOE の監査ログに記録される時刻情報は、TOE が保持している時刻が使用される。TOE の時刻は TOE の管理機能で設定され維持されると共に、外部のタイムサーバと NTP プロトコルで同期することも可能である。

TOE が監査ログを監査ログ用ファイルサーバに出力する際には SMB プロトコル、syslog サーバに出力する際には syslog プロトコルを使用する。

TOE がネットワークを介して外部の IT 機器と通信する際には、IPsec プロトコルを使用する。

## 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。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。

(和文名称)

- ・ iR-ADV セキュリティーキット・AC1 for IEEE 2600 アドミニストレーターガイド [FT6-2324 (000)]
- ・ iR-ADV セキュリティーキット・AC1 for IEEE 2600 をお使いになる前にお読みください [FT6-2325 (000)]
- ・ imageRUNNER ADVANCE C3500 III Series 2600 model ユーザーズガイドCD [FT6-2326 (000)]

(英文名称)

- ・ iR-ADV Security Kit-AC1 for IEEE 2600 Common Criteria Certification Administrator Guide [FT6-2327 (000)]
- ・ Before Using the iR-ADV Security Kit-AC1 for IEEE 2600 Common Criteria Certification [FT6-2328(000)]
- ・ imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model User's Guide CD (USE Version) [FT6-2329 (000)]
- ・ imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model User's Guide CD (APE Version) [FT6-2330(000)]

(補足) 上記の識別に含まれている「APE」はアジア・太平洋向けであることを表す。「USE」は米国向けであることを表す。

## 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、平成 31 年 1 月に始まり、令和元年 8 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 31 年 4 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査を行った。一部のプロセスの施行状況については、現地訪問は省略され、過去の認証案件での調査内容の再利用が可能であると、評価機関の責において判断されている。

また、平成 31 年 4 月に開発者サイトで開発者のテスト環境を使用し、開発者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

開発者がテストした TOE は、2章の TOE 識別で示した構成のうちの、MFP 本体が iR-ADV C3530 III の場合の構成である。

以下の理由により、テストの構成は十分であることが評価者によって評価されている。

- 本 TOE を構成する MFP 本体間の相違は、印字速度などのハードウェア処理の違いである。印字速度などのハードウェア処理はセキュリティ機能に影響しないため、iR-ADV C3530III をテストの対象とした。

開発者が実施したテストの環境における構成要素は、表7-1の通りである。テストの構成は図4-1に示した TOE 使用環境に準ずるが、以下の点で相違がある。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 の機能の確認には問題ないことが評価者により評価されている。

- インターネットとは接続されていない環境を使用している。そのため、ST に記載されている環境の内、ファイアウォールは存在しない。
- 電話公衆回線の代わりに、電話公衆回線と同じファクス通信プロトコルをエミュレートすることができる電話回線擬似交換機を使用している。
- 2回線目以降のオプションのファクスボードが装着されている。

表7-1 開発者テストの構成要素

要素	詳細
TOE	<ul style="list-style-type: none"> <li>・セキュリティキット： iR-ADVセキュリティキット・AC1 for IEEE 2600 Ver 1.00</li> <li>・MFP本体： iR-ADV C3530 III Super G3 FAX Board-AZ</li> <li>・セキュリティチップ： Canon MFP Security Chip 2.11</li> </ul>
ファクスボード	<ul style="list-style-type: none"> <li>・増設ファクスボード： G3回線増設キット（2回線）・AU</li> </ul>
サーバ1	<p>ユーザー認証サーバ (Kerberos)、メールサーバ、タイムサーバ、監査ログ用ファイルサーバ、syslogサーバとして使用</p> <ul style="list-style-type: none"> <li>・OS： Windows Server 2012 R2 Standard Edition</li> <li>・ユーザー認証サーバ(Kerberos)： Active Directory Domain Services</li> <li>・メールサーバ： Microsoft Exchange Server 2013</li> <li>・タイムサーバ： Windows Time</li> <li>・監査ログ用ファイルサーバ： OSのSMBサーバ機能</li> <li>・syslogサーバ： psyslog v1.04</li> </ul>
サーバ2	<p>ユーザ認証サーバ(LDAP)として使用</p> <ul style="list-style-type: none"> <li>・OS： Windows Server 2012 R2 Standard Edition</li> <li>・ユーザ認証サーバ(LDAP)： eDirectory 8.8 SP8</li> </ul>
テスト用PC	<ul style="list-style-type: none"> <li>・OS： Microsoft Windows 7 Professional</li> <li>・Webブラウザ： Microsoft Internet Explorer 11</li> </ul>

## (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>

- ① 操作パネル、電源ボタンなどのハードキー、リモート UI などのユーザインタフェースなどを操作して、操作結果(正常終了または異常終了、エラーメッセージなど)や監査ログを確認した。



- ② HDD データ完全消去機能の確認のために、SATA アナライザを使用して HDD への入出力データをキャプチャし確認した。
- ③ HDD 暗号化機能の確認のために、暗号機能を実装するチップのファームウェアを、テストのためのコマンドを追加したものに置き換える。追加したコマンドを使用して既知解テストを実施した。
- ④ IPsec 通信機能の確認のため、通信データをパケットキャプチャソフトウェアにてキャプチャして IPsec 機能のふるまいを確認した。また、IPsec 通信に使用される暗号鍵が規定されたアルゴリズムにて生成されていることを、暗号鍵の生成部分呼び出すためのテスト用のプログラムを使用して、特定の入力に対して想定する疑似乱数が出力されることを確認することで検証した。

<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

ツール名称	概要・利用目的
・ Wireshark Ver.1.12.5, Ver. 3.0.0	LAN上の通信データをモニタし、解析するツール
・ SierraM6-2 SAS-M006-802-X (LeCroy)	SATAケーブル間に接続してSATAインタフェースの信号をキャプチャするためのツール
・ SATA Protocol Suite Ver.4.00	SATAインタフェースからキャプチャしたデータを解析するツール
・ 疑似乱数テストツール	IPsecで利用する疑似乱数生成器の動作を確認するために開発者により開発されたツール
・ 電話回線疑似交換機	電話回線の交換動作を疑似的に行う装置
・ Canon Generic Plus LIPSLX Printer Driver Version 2.00 ・ Canon Generic Plus PS3 Printer Driver Version 2.00 ・ Canon Generic Plus PCL Printer Driver Version 2.00	プリンタドライバ

<開発者テストの実施内容>

各種インタフェースより、MFPの基本機能とセキュリティ管理機能进行操作し、様々な入力パラメタに対して、適用されるセキュリティ機能が仕様通りに動作することを確認した。

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418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セキュリティ機能と外部インタフェースに対するテストのカバレッジが確認された。一部の外部インタフェースに対してはカバレッジが不十分と判断され、評価者独立テストで補足された。

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行され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行されることをより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

評価者が実施した独立テストの構成は、開発者テストに使用したテスト環境をそのまま使用して実施した。利用された機器やテストツールの仕様確認及び動作試験と校正は評価者によって実施されている。

評価者がテストした TOE は、2章の TOE 識別で示した構成のうちの、MFP 本体が iR-ADV C3530III の場合の構成と iR-ADV C3520III の場合の構成である。

評価者テストは本 ST において識別されている TOE 構成と同等の TOE テスト環境で実施されている。

### (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

評価者は、TOEのセキュリティ機能が仕様どおりに機能することを評価者自らが実証するために、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

##### <独立テストの観点>

- ① パラメタが多く複雑なインタフェースにおけるパラメタ、文字列の入力パターン、例外処理やキャンセル時の処理に対し、バリエーションを追加したテストにより開発者テストを補足する。
- ② 関連する複数の機能が同時に使用される場合のテスト、開発者テストを補足する。
- ③ 開発者とは異なる方法によるテストで、開発者テストを補足する。
- ④ 保護資産への影響が疑われる機能に対して開発者テストが不足している場合、そのテストを実施する。
- ⑤ 開発者テストの対象となっていない TOE の構成に対するテストを追加し、構成の相違がセキュリティ機能の振る舞いに影響しないことを確認する。
- ⑥ パスワードに関する想定(試行に要する時間など)の正しさを独立に検証する。

#### b) 独立テスト概要

評価者は、開発者テスト及び提供された評価証拠資料から、60項目のサンプリングテストを実施した。評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点で9項目の追加の独立テストを考案した。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>

操作者が Web ブラウザや操作パネルを操作することで動作する機能は、そのエラーメッセージや画面の状態などからその結果を観察することが可能であるため、応答を確認するテスト手法を用いた。

外部インタフェースに関しては、TOE と接続する機器経由で TOE を刺激することにより TOE の状態や監査ログが変化するため、その結果を観察するテスト手法を用いた。

IPsec 通信や SNMP による通信機能などに関する機能は人が外部から観察することができない機能性であるため、代替手段としてパケットキャプ

チャソフトウェア (Wireshark) や SNMP 関連ツール (Net-snmp) によりそのふるまいを確認する手法を用いた。

セッション ID の管理については Proxy 型脆弱性検査ツール (Burp Suite) を使用してそのふるまいを確認する手法を用いた。

<独立テストツール>

独立テストは、開発者テストに表 7-3 に示すテストツールを追加し実施された。

表7-3 独立テストで使用したツール

ツール名称	概要・利用目的
・ Net-SNMP Ver. 5.6.1.1	SNMPの各バージョンを実装するアプリケーションソフトウェア。 本テストでは、MIBブラウザ機能などのコマンド機能 (snmpwalk、snmpsetなど) のみ使用する。
・ BurpSuite Pro Ver 1.7.37, Ver 2.0.18	Proxy型脆弱性検査ツール。 ブラウザでは確認できないセッションIDを確認するため。
・ Canon Generic Fax Driver Ver 10.20	使用不可としている機能が実際に使用できないことを確認するため。
・ USBメモリ	使用不可としている機能が実際に使用できないことを確認するため。

<独立テストの実施内容>

独立テストの観点とそれに対応したテスト内容を表 7-4 に示す。

表7-4 実施した独立テスト

テスト概要	観点
管理機能、ジョブ実行アクセス制御に関する機能テスト (一般ユーザロールに属するユーザがSTに規定された管理機能にアクセスできないことの確認等)	①
ユーザ認証画面に関する機能テスト (ユーザ名・パスワードの文字長チェックの動作確認等)	①
ユーザ情報編集に関する機能テスト (パスワードに使用できる文字のバリエーションの確認等)	①

テスト概要	観点
リモートUIのセッション管理機能に関する機能テスト (セッションIDの観察や改変による認証機能の確認)	③
投入ジョブアクセス制御に関する機能テスト (PCからのジョブの投入のバリエーション (プロトコル、ドライバ) により投入ジョブのふるまいが変更されないこと、使用が禁止されている機能 (PCからのドライバ経由のファクス送信)が使用できないことの確認等)	①
ユーザ権限の同時利用に関する機能テスト (管理者は同時ログインできないことの確認等)	②
外部インタフェースに関する機能テスト (SNMPにて取得可能な情報が機能仕様に記述された情報のみであること、USBメモリを使用できないことの確認等)	④
ボックス機能に関する機能テスト (リモートUIのアクセスについては管理者のみアクセス可能であることの確認、ボックス暗証番号の試行に要する時間の確認等)	① ⑥
MFP本体が開発者テストとは異なる構成に対し、開発者テストと同様のテストの一部(ハードウェア依存する可能性が高いテストを多く選択)を実施し、MFP本体が異なっても同様の結果となることの確認	⑤

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 設計資料にTOEが運用状態に提供していると記述されている機能以外の

ネットワークサービスが起動している場合、セキュリティ機能をバイパスしてTOEの保護資産を侵害する可能性がある。

- ② 稼働しているネットワークサービスに公知の脆弱性の理由により、本来意図された操作以外の操作が実行可能であることにより、TOEのセキュリティ機能をバイパスして保護資産にアクセスされる可能性がある。
- ③ リモートUIにおいて、セッション情報を確認しないページ（機能）が存在することにより、識別認証やアクセス制御をバイパスできる可能性がある。
- ④ リモートUIにて提供されるチェックをバイパスして入力値に不正な値が指定されることによりTOEが想定しない動作を起こし、結果的にTOEのセキュリティ機能をバイパスすることによりTOEのセキュアな利用に影響を与える可能性がある。

**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>

評価者独立テストの環境に、以下の表 7-5 に示すテストツールを追加して実施した。これらのツールの仕様確認及び動作試験と校正は評価者によって実施されている。

**表7-5 侵入テストに使用したツール**

ツール名称	概要
・ Nmap Ver 7.7	ポートスキャンツール
・ Nessus Ver 7.1.3	脆弱性スキャナ
・ Netcat v1.12	汎用TCP・UDP通信ツール
・ PRET V0.40	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 7-6 に示す。

**表7-6 侵入テスト概要**

脆弱性	テスト概要
①	TOEに対して、ポートスキャンツール（Nmap）を利用してポートスキャンを行った。想定外のネットワークサービスは確認されなかった。コマンドの実行を試みる際、必要に応じてNetcatを使用した。

脆弱性	テスト概要
②	<p>脆弱性スキャナ（Nessus）によるスキャンを行い、TOEが提供するネットワークサービスに悪用可能な公知の脆弱性が存在しないことを確認した。</p> <p>TOEが提供するネットワークサービスのうち、ファイルを公開する機能やコマンドを実行する機能を持つ可能性のあるインタフェース（FTPなど）において、許可されないコマンド（OSまたはプロトコル）が実行できないことを確認した。</p> <p>PRETを使用して不正な処理を含む印刷ジョブコマンドや印刷ファイルをTOEに入力し、不正な処理が実行されないことを確認した。</p>
③	<p>認証後にアクセス可能となる画面のURLをBurpSuite Proを使用して調査した。</p> <p>認証されていない状態でこれらのURLを指定してアクセスし、認証後でないと該当画面にアクセスできないことを確認した。</p> <p>（セッション情報のチェック機能の動作を確認した。）</p>
④	<p>BurpSuite Proを使用し、以下の点を確認した。</p> <ul style="list-style-type: none"> <li>▶ TOEの利用が許可されていないものまたは一般ユーザが操作可能な画面（ログイン画面、パスワード変更画面、アドレス帳など）の入力項目に対して、ツールを使用して、許可されない文字や長い文字列を入力し問題が発生しないことを確認した。</li> <li>▶ 管理者が操作可能な画面（ユーザ管理機能、各種設定機能）の入力項目に対して、ツールを使用して、許可されない文字や長い文字列を入力し問題が発生しないことを確認した。</li> </ul>

#### 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 の構成条件はガイドンスに記述されているとおりであり、各種設定値をガイドンスに従って設定する必要がある。TOE の設定値の中には、セキュリティ機能の ON/OFF などが含まれており、本評価では値が固定されているものが存在する。それらのセキュリティに影響する設定値をガイドンスで禁止されている値に変更した場合、本評価の対象の構成ではない。

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

- 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

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 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

- (1) 本評価は、ファクスボックスは利用できない設定で実施された。つまり、ファクスボックスを利用する設定とした場合は、本評価による保証の対象とはならない。
- (2) 本評価では、PP で要求されているセキュリティ機能要件について、PC からのプリントジョブの投入時には、識別認証の要件は存在しないという解釈がされている。そのため、プリントジョブの投入時にも識別認証を期待する消費者にとっては、ニーズに合致しない可能性があるため、注意が必要である。
- (3) TOE で「外部認証方式」を使用する場合、認証方式は Kerberos 認証もしくは LDAP 認証を用いることができる。その場合、Kerberos 認証では Active Directory Domain Services を使用する場合、LDAP 認証では eDirectory 8.8 SP8を使用する場合のみが本評価により保証された。

## 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。

Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model Security Target バージョン 1.09, 2019 年 08 月 07 日, キヤノン株式会社

## 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)
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。

MFP	Multifunction Product (デジタル複合機)
HCD	Hardcopy Device

本報告書で使用された用語の定義を以下に示す。

Hardcopy Device (HCD)	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.
Iファクス	電話回線の代わりにインターネットを使用してファクス文書の送受信を行う、インターネットファクスのこと。
TOE Owner	A person or organizational entity responsible for protecting TOE assets and establishing related security policies.
TSF Confidential Data	Assets for which either disclosure or alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE.

TSF Protected Data	Assets for which alteration by a User who is not an Administrator or the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
U. ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.
UI機能	利用者が操作パネルを用いてTOEを操作したり、TOEが操作パネルに表示したりする機能。
U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
User Document Data	The asset that consists of the information contained in a user's document.
User Function Data	The asset that consists of the information about a user's document or job to be processed by the TOE.
外部インタフェース	プリントやファクス (Iファクス) などのジョブの送受信、タイムサーバからのデータを受信するためのインタフェース
コピー機能	紙文書を読み込み、プリントすることにより、紙文書を複写する機能。
スキャン機能	紙文書を読み込み、電子文書を生成する機能。
送信(Universal Send)機能	紙文書をスキャンして生成された電子文書やボックスに保存されている電子文書を、電子メールアドレス、PCの共有フォルダ、Iファクスなどに送信する機能。
ファクスボックス	ファクス/Iファクス転送された電子文書が保存されるボックスであり、保存された電子文書のプリントが可能である。
プリント機能	TOE内に格納された電子文書を紙文書にプリントする機能。
プリント設定	プリント機能に関する各種設定。カラーと白黒の選択、用紙選択、両面印刷などの設定が含まれる。
ボックス	TOEにおいて、読み込みやプリント、ファクス受信した電子文書を保存する領域。

ボックス暗証番号	電子文書が格納されているボックス毎の暗証番号。電子文書に対するアクセス制御に用いられる。
ボックス機能	紙文書をスキャンして読み込んだ電子文書、PCから保存指定した電子文書、ファクス受信した電子文書を、ボックスに保存する機能。及び、ボックスに保存された文書に対して、プリント、送信、削除の操作を提供する機能。
リモートUI	WebブラウザからLANを経由してMFPにアクセスし、MFPの動作状況の確認やジョブの操作、ボックスに対する操作、各種設定などができるインターフェース。

## 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] Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model Security Target バージョン 1.09, 2019年08月07日, キヤノン株式会社
- [13] Canon imageRUNNER ADVANCE C35900KG (III)/C3500 III Series 2600 model 評価報告書 第2.0版, 2019年08月30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