認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成27年5月27日 (IT認証5552)
認証番号	C0495
認証申請者	キヤノン株式会社
TOEの名称	Canon imageRUNNER ADVANCE C3300 Series 2600.1 model
TOEのバージョン	1.0
PP適合	IEEE Std 2600.1-2009
適合する保証パッケージ	EAL3 及び追加の保証コンポーネントALC_FLR.2
開発者	キヤノン株式会社
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。

平成27年12月21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

「Canon imageRUNNER ADVANCE C3300 Series 2600.1 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　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 6
3.1　セキュリティ機能方針 7
3.1.1　脅威とセキュリティ機能方針 7
3.1.1.1　脅威 7
3.1.1.2　脅威に対するセキュリティ機能方針 7
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 9
3.1.2.1　組織のセキュリティ方針 9
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 10
4　前提条件と評価範囲の明確化 12
4.1　使用及び環境に関する前提条件 12
4.2　運用環境と構成 13
4.3　運用環境におけるTOE範囲 14
5　アーキテクチャに関する情報 16
5.1　TOE境界とコンポーネント構成 16
5.2　IT環境 17
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 29
7.6　評価結果 30

7.7　評価者コメント/勧告 31
8　認証実施 32
8.1　認証結果 32
8.2　注意事項 32
9　附属書 33
10　セキュリティターゲット 33
11　用語 34
12　参照 37

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 C3300 Series 2600.1 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。)が平成 27 年 12 月 14 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、本書の付属書である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 保証パッケージ

本 TOE の保証パッケージは、EAL3 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、MFP 用の Protection Profile である IEEE Std 2600.1-2009[14](以下「PP」という。)で定義されているセキュリティ機能要件について、要求されているすべてのセキュリティ機能要件を満足するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおり。

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、平成 27 年 12 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 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： Canon imageRUNNER ADVANCE C3300 Series 2600.1 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、ハードウェア及びライセンスから構成される。

表2-1 TOEの構成品

名称	説明
(和文名称) Canon imageRUNNER ADVANCE C3300 Series (英文名称) Canon imageRUNNER ADVANCE C3300 Series	以下のいずれかのMFP本体。 ● iR-ADV C3330 ● iR-ADV C3330i ● iR-ADV C3330F ● iR-ADV C3325 ● iR-ADV C3325i ● iR-ADV C3320 ● iR-ADV C3320i ● iR-ADV C3320F 末尾が「F」であるものを「Fモデル」、末尾が「i」であるものを「iモデル」と呼ぶ。
(和文名称) iR-ADVセキュリティーキット・L1 for IEEE 2600.1 Ver 1.00 (英文名称) iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Ver 1.00	「Canon imageRUNNER ADVANCE C3300 Series」用の制御ソフトウェア及びセキュリティーキットライセンスが含まれる。
(和文名称) HDDデータ暗号化キットC (Canon MFP Security Chip 2.01) (英文名称) HDD Data Encryption Kit-C (Canon MFP Security Chip 2.01)	HDDに格納されるデータ全体を暗号化するためのハードウェア。

名称	説明
(和文名称) スーパーG3FAXボード・AR1 (英文名称) Super G3 FAX Board-AR1	MFP本体に装着するファクスボード。 Fモデル(以下のMFP本体)には標準で含まれる。 ● iR-ADV C3330F ● iR-ADV C3320F
(和文名称) Access Management System (英文名称) Access Management System	制御ソフトウェアに含まれているアクセス制御機能を有効にするライセンス。 日本・北米地区ではMFP本体に標準で含まれる。

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。

ガイダンスに記載された手順に従って、MFP の操作パネルを操作して画面に表示された TOE の構成品の識別情報を確認する。

一部の構成品は、以下のように表 2-1 に記載した名称とは異なる識別情報が表示される。識別情報の確認方法についてもガイダンスの記載を参照する必要がある。

・ 「Canon imageRUNNER ADVANCE C3300 Series」は、表 2-1 の説明にある「F モデル」の場合は、MFP 本体の製品名としては末尾の F がない名称が表示され、ファクスボードはオプションとして MFP 本体の製品名とは別に表示される。
(例えば iR-ADV C3330F であれば、製品名「iR-ADV C3330」とファクスボードの名称の表示となる。この表示は、「iR-ADV C3330」に「キヤノン　スーパーG3 FAX ボード・AP1」を装着した場合と同じである。)

「i モデル」の場合は、MFP 本体の製品名としては末尾の i がない名称が表示される。加えて、「i モデル」に特有のライセンスの名称が表示される。

・ 「iR-ADV セキュリティーキット・L1 for IEEE 2600.1 Ver 1.00」は、制御ソフトウェアのバージョンと、セキュリティーキットライセンスの表示となる。

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、利用者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利用者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、利用者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、保護資産である利用者の文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。

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の利用者である。

・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の利用者である。

・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
　利用者の文書データ。

・User Function Data
　TOEによって処理される利用者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データ。利用者のパスワード、ボックス暗証番号、監査ログが含まれる。なお暗号鍵は、利用者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。利用者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、「ユーザー認証機能」、「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」、「HDD暗号化機能」及び「LANデータ保護機能」で対抗する。

TOEの「ユーザー認証機能」「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ー名が、プリントジョブ投入時に指定されたユーザー名と一致する場合、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、ユーザー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、ユーザー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「HDD暗号化機能」は、TOEが備えている取り外し可能なHDDに格納される全データを暗号化することにより、TOEから取り外された状態のHDDから、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。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FIPS PUB 186-2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。

TOEの「LANデータ保護機能」は、TOEがLANを経由して他の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、「ユーザー認証機能」、「管理機能」、「HDD暗号化機能」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「ユーザー認証機能」、「HDD暗号化機能」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し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。P.HDD.ACCESS.AUTHORIZATION を除くセキュリティ方針は、PP に記述されているものと同じである。P.HDD.ACCESS.AUTHORIZATION は、PP に対して追加されたものであり､TOEが備えているリムーバブルHDDを利用するにあたり、一般的に要求されることを想定したセキュリティ方針である。

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

識別子	組織のセキュリティ方針
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.HDD.ACCESS.AUTHORIZATION	To prevent access TOE assets in the HDD with connecting the other HCDs, TOE will have authorized access the HDD data.

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、「ユーザー認証機能」、「ジョブ実行アクセス制御機能」で本方針を実現する。

TOEの「ユーザー認証機能」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暗号鍵生成アルゴリズム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。

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

TOEは、「ユーザー認証機能」と「受信ジョブ転送機能」で、本方針を実現する。

TOEの「ユーザー認証機能」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.HDD.ACCESS.AUTHORIZATION」への対応

TOEは、「HDD暗号化機能」に含まれている本体識別認証機能で、本方針

を実現する。

TOE の「HDD 暗号化機能」の本体識別認証機能は、TOE の構成要素である HDD データ暗号化/ミラーリングボードが提供する機能である。当該ボードは、取付け時に MFP 本体の認証用 ID が設定される。それを用いて、当該ボードは、毎回起動時にチャレンジ&レスポンス方式で MFP 本体を認証し、正当な MFP 本体の場合のみ HDD へのアクセスを許可する。

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。

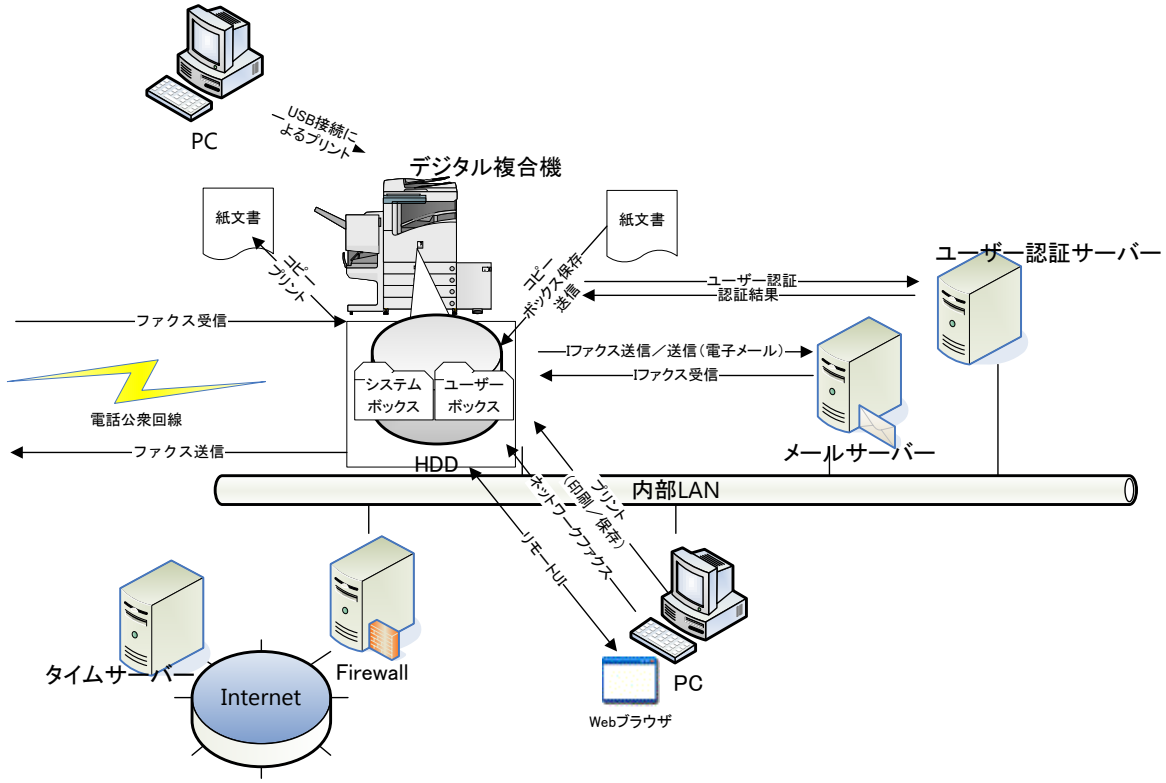

図4-1 TOEの運用環境

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)・AR1

(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 LIPSLX Printer Driver Version 21.45
  - Canon PS3 Printer Driver Ver 21.45
  - Canon PCL Printer Driver Ver 21.45
- Webブラウザ：本評価では、Microsoft Internet Explorer 11 を使用。

(3) ユーザー認証サーバ

3章で説明したTOEの「ユーザー認証機能」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。

ユーザー認証サーバは、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) 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。

(5) 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。

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。

② TOEに、プリンタドライバでプリントジョブを投入する際に、ユーザー名と暗証番号の入力を求められる。それらの入力は、識別認証機能では使用されない。暗証番号は、プリントジョブとして投入された文書に付与され、当該文書を操作パネルからプリント操作する際に照合を求められる(これを「セキュアプリント」という)。そのふるまいは、評価対象のセキュリティ機能ではない。
ユーザー名は、その正当性を認証されることなく、プリントジョブとして投入された文書の属性として付与され、評価対象のアクセス制御機能で使用される。

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、ユーザー認証サーバ、メールサーバ、PC、タイムサーバ、ユーザーは含まない。

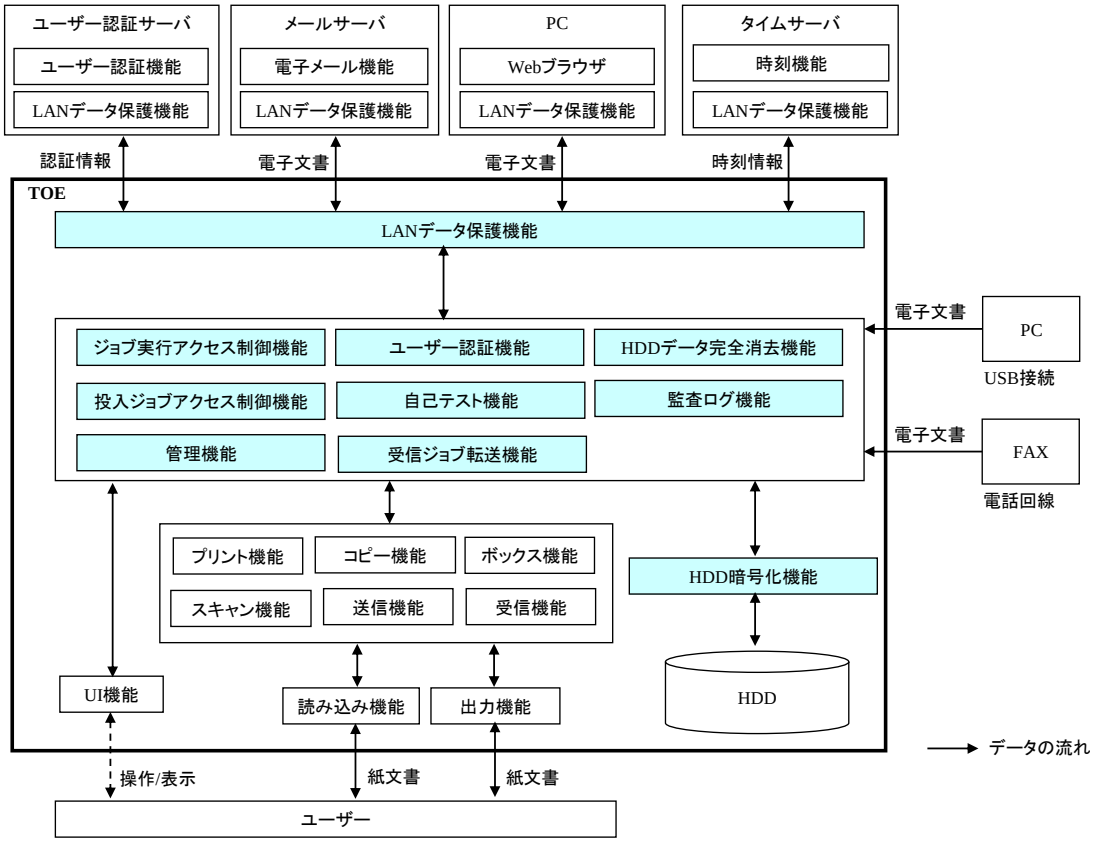

図5-1　TOE境界

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「ユーザー認証機能」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、「ユーザー認証機能」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。

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「ユーザー認証機能」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ー認証サーバが参照され識別認証が実施される。ユーザー認証サーバへの利用者情報の登録は、ユーザー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。したがって、TOE と通信する外部の IT 機器も IPsec プロトコルの設定が必要である。

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)

- imageRUNNER ADVANCE C3300 Series 2600.1 model eマニュアルCD [FT6-1433 (000)]
- iR-ADV セキュリティーキット・L1 for IEEE 2600.1アドミニストレーターガイド [FT6-1400(000)]
- iR-ADV セキュリティーキット・L1 for IEEE 2600.1 をお使いになる前にお読みください [FT6-1401(000)]
- HDDデータ暗号化キット　ユーザーズガイド [FT5-2437 (020)]

(英文名称)

- imageRUNNER ADVANCE C3300 Series 2600.1 model e-Manual CD (USE Version) [FT6-1436(000)]
- imageRUNNER ADVANCE C3300 Series 2600.1 model e-Manual CD (APE Version) [FT6-1437(000)]
- iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Certification Administrator Guide [FT6-1402(000)]
- Before Using the iR-ADV Security Kit-L1 for IEEE 2600.1 Common Criteria Certification [FT6-1403 (000)]
- HDD Data Encryption Kit Reference Guide [FT5-3328(010)]

(補足) 上記の識別に含まれている「APE」はオーストラリア、シンガポール、香港向けであることを表す。「USE」はそれ以外の地域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）と相互承認している認定機関（独立行政法人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 27 年 5 月に始まり、平成 27 年 12 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 27 年 7 月、8 月及び 11 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・開発セキュリティ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。また、平成 27 年 7 月、8 月及び 11 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。

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。

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定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 C3330 の場合の構成である。他機種は、印字速度などのハードウェア処理が異なるだけで、セキュリティ機能には影響を与えないため、代表機種によるテストで十分であることが評価者によって評価されている。

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	iR-ADV C3330 (MFP本体) HDDデータ暗号化キット・C iR-ADVセキュリティーキット・L1 for IEEE 2600.1 Ver 1.00 スーパーG3 FAX ボード・AR1
増設ファクスボード	G3回線増設キット(2回線)・AR1
メールサーバ	Windows Server 2012 R2 Standard Edition -Microsoft Exchange Server 2013

要素	詳細
ユーザー認証(Kerberos) サーバ1 兼タイムサーバ	Windows Server 2012 R2 Standard Edition -Active Directory Domain Services -Windows Time
ユーザー認証(LDAP) サーバ2	Windows Server 2012 R2 Standard Edition -eDirectory 8.8 SP8
テスト用PC（3台）	Microsoft Windows 7 Professional -Microsoft Internet Explorer 11 (Web ブラウザ)

(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 などの利用者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、指定した暗号アルゴリズムが実装されているソフトウェアで暗号化した結果と、TOE にて暗号化されたデータが一致することを確認した。また、暗号鍵生成については、モジュールレベルで規定された暗号鍵生成アルゴリズムを実装していること確認した。

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、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。

⑤ MFP 本体が「i モデル」(表 2-1 参照)である場合の動作確認のために、「i モデル」に特有のライセンスを有効にした状態でのテストを実施した。

＜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（バージョン）	概要・利用目的
Wireshark （Ver.1.2.11 Rev.34007）	パケットキャプチャソフトウェア
SATA Protocol Suite （Ver.4.00）	アナライザソフト
SATAテスタ	HDDの標準インタフェースであるSATAに準拠したコマンドやデータの送受信等をするツール
SATAアナライザ	SATAケーブル間に接続してSATAインタフェースの信号を確認するためのツール
ICE	In-Circuit Emulatorの略。CPUの動作をエミュレートすることによりデバッグの支援をする
AESライブラリ for FR	暗号ライブラリ（HDD暗号化ボードテスト用）
擬似乱数テストツール	IPsecで利用する擬似乱数生成器がFIPS186-2 のアルゴリズムで動作することを確認するために開発者により開発されたツール
電話回線擬似交換機	電話回線の交換動作を疑似的に行う装置
プリンタドライバ	Canon LIPSLX Printer Driver Version 21.45 Canon PS3 Printer Driver Ver 21.45 Canon PCL Printer Driver Ver 21.45

＜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を操作し、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482項目実施された。カバレージ分析によって、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十分にテストされたことが検証された。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分に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 C3330またはiR-ADV C3320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 開発者テストでは、複数のセキュリティ機能性が同時に動作するケースが扱われていないため、独立テストで確認する。

② セキュリティ以外の機能とセキュリティ機能との関連性に関するテストを追加する。

③ 例外処理やキャンセル時の処理にバリエーションがあり、開発者テストで実施されていないものについては独立テストで確認する。

④ リモートUIや操作パネルにおける、入力可能桁数の制限や文字数チェック機能が正しく動作することを確認するため、入力値のバリエーションをふやしたテストを実施する。

⑤ パスワードに関する順列的・確率的メカニズムが 機能仕様通りであることを確認するテストを追加する。

⑥ 使用が禁止されている機能が、確かに使用できないことを確認する。

⑦ 開発者テストとは MFP 本体の機種が異なる構成をテストすることで、機種の違いはハードウェアの処理速度の違いだけであり、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。

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、50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11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＞

独立テストでは、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（バージョン）	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。
Burp Suite （Ver. 1.6.22）	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。
AMS Printer Driver Add-in Ver 3.1.3	プリンタドライバからの機能の利用を制限する。 外部インタフェースに関するパラメタを増やしてテストを実施するため。
Canon Generic FAX Driver Ver 10.06	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
ユーザー管理機能、ジョブ実行アクセス制御に関する機能テスト （一般ユーザーロールに属するユーザーが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）	③
ユーザー認証画面に関する機能テスト （ユーザー名・パスワードの文字長チェックの動作確認等）	④
ローカル認証におけるパスワード変更に関する機能テスト （一般ユーザーの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）	③ ④ ⑤
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の付与方法が機能仕様通りであることの確認等）	② ⑤

テスト概要	観点
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 ③ ⑥
ユーザー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ができないこと、それ以外のユーザーは同時ログインが可能であることの確認等）	① ③ ④
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）	① ⑤ ⑥
HDDやジョブが限界に達した状態で不正な動作をしないこと（適切にエラー処理されること）のテスト	③ ⑤
ボックス機能に関する機能テスト(1) （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等）	③
ボックス機能に関する機能テスト(2) （ボックスに関する設定が管理者またはそのボックスの所有者のみであることの確認等）	③ ⑤
開発者テストとはMFP本体の機種が異なる構成に対し、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、機種が異なっていても同様の結果となることの確認	⑦

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（バージョン）	概要
Nmap (Ver 6.25)	ポートスキャンツール
Nessus (Ver 6.4.2)	脆弱性スキャナ
Netcat (Ver1.11)	汎用TCP･UDP通信ツール

＜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い、②の結果を含めて分析した。設計資料に記述されていないサービスが起動していることを確認したが、サービスの種類を特定した後、それがセキュリティ機能に影響しないものであることを確認した。 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。コマンドの実行を試みる際、必要に応じてNetcatを使用した。
②	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公知の脆弱性が存在しないことを確認した。
③	認証後にアクセス可能となる画面のURLをBurp suiteを使用して調査した。 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。 （セッション情報のチェック機能の動作を確認した。）
④	Burp Suite（Proxy型脆弱性検査ツール）を使用し、以下の点を確認した。 ➢ TOEの利用が許可されていないものまたは一般ユーザーが操作可能な画面(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。 ➢ 管理者が操作可能な画面(ユーザー管理機能、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。

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 の構成条件はガイダンスに記述されているとおりであり、各種設定値をガイダ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ダ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：
  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  （IEEE Std 2600.1-2009）

  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。
  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A 適合
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A 適合
  - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A 適合
  - 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A 適合
  - 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A 適合
  - 2600.1-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment A 追加
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A 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。

- EAL3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のみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 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。

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、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 TOE が CC パート 3 の EAL3 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ので、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本認証報告書とともに提供される。

Canon imageRUNNER ADVANCE C3300 Series 2600.1 model Security Target
バージョン 1.03　2015 年 7 月 23 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。
セキュアプリント	暗証番号が付与された文書のプリント。
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] Canon imageRUNNER ADVANCE C3300 Series 2600.1 model Security Target バージョン 1.03　2015年7月23日　キヤノン株式会社

[13] Canon imageRUNNER ADVANCE C3300 Series 2600.1 model 評価報告書, 第1.1版, 2015年12月14日, 株式会社 ECSEC Laboratory 評価センター

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009