JISEC

サーベイランス報告書

発行日　：　2014-7-11

資料番号：　SRP-C0287-01

下記評価対象について、ITセキュリティ認証等に関する要求事項(CCM-02) 8.1に基づき、サーベイランスが実施されたことを報告いたします。認証報告書と合わせて参照願います。

評価対象：

認証番号	C0287
認証申請者	キヤノン株式会社
TOEの名称	Canon imageRUNNER ADVANCE C5000 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	みずほ情報総研株式会社　情報セキュリティ評価室

サーベイランス管理番号：　JISEC-SV14-001

サーベイランス実施報告：

- サーベイランス結果

本TOEは、セキュリティが維持されない可能性が確認され、本TOEに対する認証維持は不可と判断します。

- サーベイランス概要

本TOEに対する保証の根拠となる開発証拠資料と矛盾する情報が公開されていることが判明し、それらの資料に基づく評価結果について保証を満たせない可能性があるため、2014年3月から同年7月にかけてサーベイランスを実施しました。

サーベイランスの結果、本TOEは評価時の保証の根拠となる前提が失われており、厳密な管理下にない運用環境においてはセキュリティが維持できなくなる可能性があることが判りました。制度では、本TOEに対し認証の「一時停止」を行い、申請者に対し是正処置を依頼しました。

現在、当該TOEについては再評価が実施されており、認証製品として購入することはできません。また、すべての購入済み調達者についてはキヤノン株式会社により担当サービスによる

稼働中全認証製品に対する設定の確認と対処がなされていることが報告されています。

本サーベイランスで指摘された問題の詳細については、開発者であるキヤノン株式会社より情報が提供されていますので、そちらに問い合わせください。

参考:「オフィス向け複合機セキュリティキットについてのお知らせ」
http://cweb.canon.jp/e-support/products/office-mfp/ipa-notice.html

以上

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

評価対象

申請受付日（受付番号）	平成22年2月25日 (IT認証0294)
認証番号	C0287
認証申請者	キヤノン株式会社
TOEの名称	Canon imageRUNNER ADVANCE C5000 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	みずほ情報総研株式会社 情報セキュリティ評価室

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23年3月29日

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 3

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 3

評価結果：合格

「Canon imageRUNNER ADVANCE C5000 Series 2600.1 model」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、キヤノン株式会社が開発した「Canon imageRUNNER ADVANCE C5000 Series 2600.1 model、 バージョン 1.0」（以下「本TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」という。）が平成23年3月17日に完了したITセキュリティ評価に対し、その内容の認証結果を申請者であるキヤノン株式会社に報告するとともに、本TOEに関心を持つ消費者や調達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、インターネットファクス機能、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、オプションであるFAXボードを利用することで電話回線を使用したファクス機能を利用することも可能であるが、ファクス機能は本TOEの構成には含まれていない。

本TOEは、デジタル複合機用の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、ファクス機能に対する要件を除いて、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している。

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。

本評価では、TOEを操作するためのWebブラウザとして、Microsoft Internet Explorer 6 SP1だけが対象である。その他のWebブラウザやバージョンは、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セキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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23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]、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、本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 C5000 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 C5000 Series （英文名称） Canon imageRUNNER ADVANCE C5000 Series	デジタル複合機iR-ADV C5051、iR-ADV C5045、iR-ADV C5035、iR-ADV C5030のいずれか。
（和文名称） iR-ADVセキュリティーキット・A1 for IEEE 2600.1 Ver 1.00 （英文名称） iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Ver 1.00	「Canon imageRUNNER ADVANCE C5000 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/ミラーリングキットC （英文名称） HDD Data Encryption & Mirroring Kit-C	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。
（和文名称） IPSec セキュリティーボード・B （英文名称） IPSec Board-B	LANデータのIPパケットを暗号化するためのハードウェア。
（和文名称） データ消去キット C （英文名称） Data Erase Kit-C	制御ソフトウェアに含まれているHDDデータ完全消去機能を有効にするライセンス。

（和文名称） Access Management System拡張キット B （英文名称） Access Management System Kit-B	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。

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、デジタル複合機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。

3 セキュリティ方針

本章では、本TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

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ハードディスク装置に蓄積したり、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、ハードディスク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、印刷、プレビュー、ネットワークへの送信、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し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.
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.MAN	To prevent unauthorized use of the external interfaces

AGEMENT	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、プリントジョブとIファクスジョブの投入は、識別認証なしで使用できる。しかし、それらのジョブで投入された文書は、投入時点では印刷や送信はされずTOE内に格納される。TOEに格納された文書の印刷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、取付け時にデジタル複合機本体の認証用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&レスポンス方式でデジタル複合機本体を認証し、正当なデジタル複合機本体の場合のみHDDへのアクセスを許可する。

4 前提条件と使用環境

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使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.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 使用環境と構成

TOEであるデジタル複合機は、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の一般的な使用環境を図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。

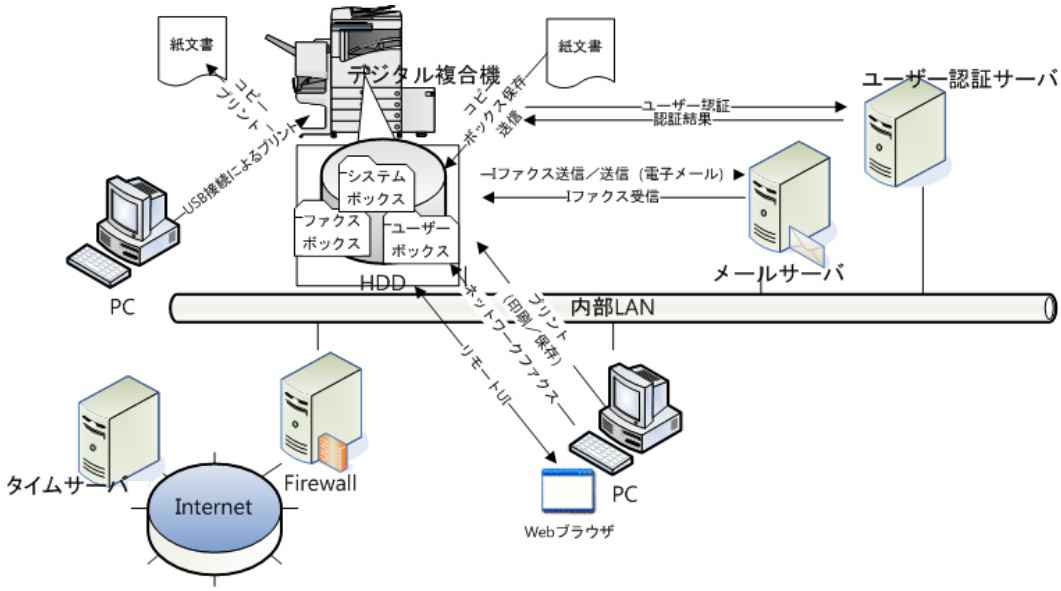

図4-1　TOEの使用環境

TOEの使用環境の構成品について以下に示す。

(1) 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、Canon LIPSLX Printer Driver Version 20.30を使用。
・Webブラウザ：本評価では、Microsoft Internet Explorer 6 SP1を使用。

(2) 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認証方式である。

(3) 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。

(4) 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 使用環境における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印刷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や、FTP印刷でFTPプロトコルが備えている識別認証が該当する。

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印刷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について、目的と関連を説明する。

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。

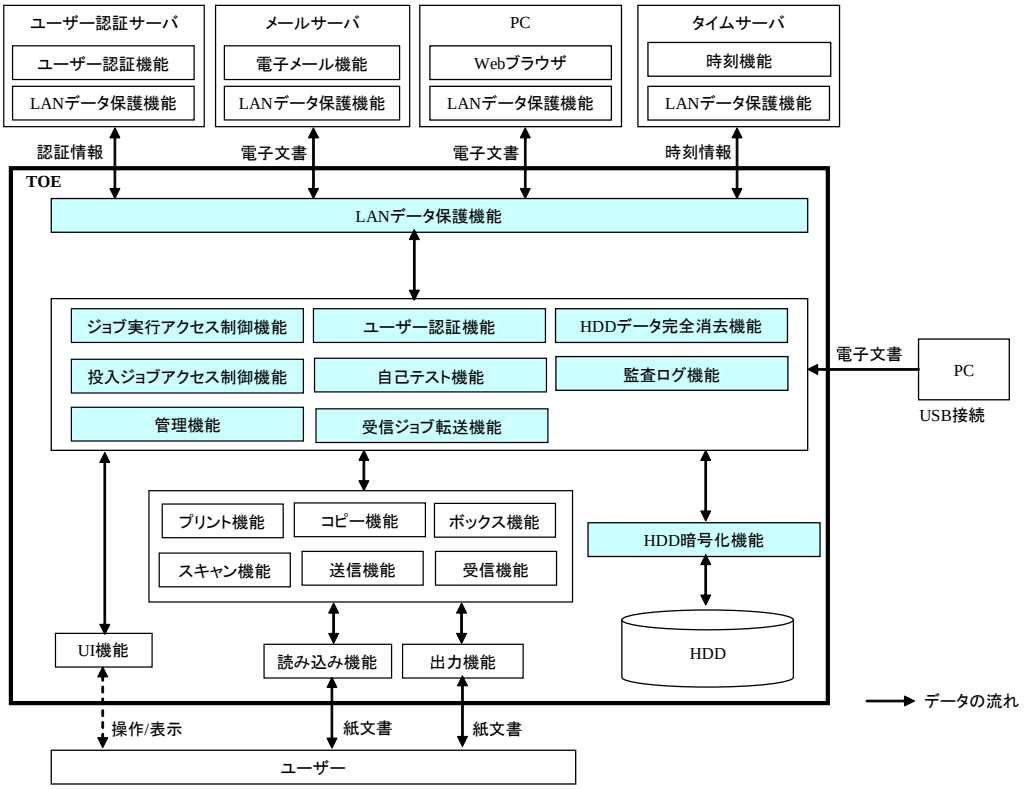

図5-1　TOE境界

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やIファクスジョブの投入する際には、識別認証なしで投入が許可され、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、内蔵ハードディスク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 C5051/C5051F/C5045/C5045F/C5035/C5035F/C5030/C5030F e-マニュアル [FT5-3806-000]
- iR-ADVセキュリティーキット・A1 for IEEE 2600.1アドミニストレーターガイド [FT5-3805-000]
- 『ACCESS MANAGEMENT SYSTEM 拡張キット・B1』Access Management System V3.0個別管理構成アドミニストレーターガイド [FT5-3806-000]
- HDDデータ暗号化キット ユーザーズガイド [FT5-2437]
- iR-ADV セキュリティーキット・A1 for IEEE 2600.1 をお使いになる前にお読みください [FT5-3807-000]

(英文名称)

- imageRUNNER ADVANCE C5051/C5045/ C5035/ C5030 e-Manual [FT5-3809-000 (US)、FT5-3945-000 (AP)]
- iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Certification Administrator Guide [FT5-3808-000]
- ACCESS MANAGEMENT SYSTEM KIT-B1 Access Management System V3.0 Individual Management Configuration Administrator Guide [FT5-3809-000 (US)、FT5-3945-000 (AP)]
- HDD Data Encryption & Mirroring Kit-C Series User Documentation [FT5-2440-010]
- Before Using iR-ADV Security Kit-A1 for IEEE 2600.1 Common Criteria Certification [FT5-3810-000]

※「US」はUS向けガイダンスの型番であり、「AP」はAsia Pacific向けガイダンスの型番である。

7 評価機関による評価実施及び結果

7.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

7.2 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22年3月に始まり、平成23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。また、平成22年9月、同年10月及び平成23年3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22年12月に開発者サイトで開発者のテスト環境を使用し、開発者が実施した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、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

7.3 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。

7.3.1 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。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成は、図4-1に示したTOE使用環境と同じである。開発者がテストしたTOEは、2章のTOE識別に該当する機種の中の、iR-ADV C5030である。他機種は、スキャンやプリント等のハードウェア処理速度が異なるだけで、セキュリティ機能の振る舞いに違いはなく、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。なお、評価者は、機種依存性がないことを検証するために、開発者がテストしていない他機種でもテストを実施している。詳細は「7.3.2 評価者独立テスト」を参照。

テスト環境のTOE以外の構成要素を表7-1に示す。

表7-1 開発者テストの使用機器

名称	詳細
PC	利用者用PC。 ・Windows 2000 SP4搭載PC ・Webブラウザ：Internet Explorer 6.0 sp1 ・プリンタドライバ： Canon LIPSLX Printer Driver Version 20.30
ユーザー認証サーバ兼タイムサーバ	外部認証使用時の認証サーバ及びインターネットのタイムサーバの代用として使用。 ・Windows Server 2008 Enterprise SP1搭載PC ・認証サーバソフトウェア： Active Directory Domain Services (OS附属) ・タイムサーバソフトウェア： Windows TIME (OS附属)
メールサーバ	Iファクスの送受信用サーバとして使用。 ・Windows Server 2003 Standerd Edition SP1搭載PC ・メールサーバソフトウェア：

	Microsoft POP3 Service (OS附属) Simple Mail Transfer Protocol (OS附属)

開発者テストは本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。

なお、開発者テスト環境は、STとは異なり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、Firewallは存在せず、また、インターネット上のタイムサーバは、ユーザー認証サーバ兼タイムサーバ上のソフトウェアで代用されている。これらの構成でも本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。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

＜開発者テスト手法＞

① 操作パネル、Webブラウザ、プリンタドライバなどの利用者インタフェースを操作して、その表示、TOEのふるまい、監査ログの内容を確認する。

② HDDデータ完全消去機能の確認のために、HDD用プロトコルアナライザを使用して消去後のHDD内容を読み出して、所定のデータで上書きされていることを確認する。

③ HDD暗号化機能の確認のために、HDDに暗号化して書き込まれたデータと別ツールで暗号化した結果を比較し、仕様どおりの暗号アルゴリズムであることを確認する。また、暗号鍵生成で、様々なシードで乱数を生成してその結果を既知のデータと比較し、仕様どおりの暗号鍵生成アルゴリズムであることを確認する。

④ IPSec機能の確認のために、PCとの間でIPSecの通信を行い、IPSecの通信が正常に行われることを確認する。さらに、ネットワークアナライザにより仕様通りの暗号通信プロトコルが適用されていることを確認する。

⑤ HDDデータ暗号化/ミラーリングキットの本体識別認証機能の確認のために、正当な本体に接続した場合と、識別の異なる別本体に接続した場合のふるまいを確認する。

＜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　開発者テストツール

ツール名称	概要・利用目的
HDD用プロトコルアナライザ Catalyst Enterprises社 ST4-31-0186	HDDの接続されたバスをモニタし、入出力データを解析するツール。
ネットワークアナライザ Wireshark Version 1.2.1	LAN上の通信データをモニタし、解析するツール。
暗号ライブラリ 富士通 AESライブラリ for FR 第1.0版	暗号アルゴリズムの実装の妥当性を確認するために、比較のために使用する。

＜開発者テストの実施＞

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。また、内部認証と外部認証の場合など、評価構成で許容されているすべての設定値が仕様通りに動作することを確認した。

b. 実施テストの範囲

テストは開発者によって275項目実施されている。

カバレージ分析が実施され、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ている。深さ分析が実施され、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ている。

c. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

7.3.2　評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、開発者テストと同等の構成である。

評価者がテストしたTOEは、2章のTOE識別に該当する機種の中の、iR-ADV

C5035とiR-ADV C5051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) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

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 開発者と異なる機種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。

② 開発者テストのサンプリングの観点で、開発者が実施したテストから、すべてのTSFIとセキュリティ機能が含まれるようにテスト項目を抽出し、開発者と同じテストを実施する。

③ 開発者テストにおいて､セキュリティ機能のふるまいについて厳密なテストが実施されていないインタフェースが存在するため､テストされていないパラメタのふるまいを確認する。

b. 独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜独立テスト手法＞

開発者テストと同じ手法を使用して、開発者と同じテスト及び入力パラメタを変更したテストを実施する。

＜独立テストツール＞

開発者テストと同じツールを用いた。

＜独立テストの実施＞

評価者が実施した独立テストの観点とその対応したテスト内容を表7-3に示す。なお、開発者がすべての設定値をテストしているのに対し、評価者は、設置手順を終えた後の初期設定状態の設定値をテストしている。

表7-3 実施した独立テスト

独立テストの観点	テスト概要
①②	開発者が実施したテスト項目から、テストの観点に基づいてテスト項目を抽出して開発者と同じテストを実施し、開発者と同じ結果が得られることを確認する。実施したテストは275項目中、107項目である。
③	利用者のパスワードやボックス暗証番号の長さ制限の限界値のふるまいが、仕様どおりであることを確認する。
③	TOEは、U.NORMALとして複数のロールを提供している。U.NORMALに該当するロールを付与された利用者は、どのロールの場合であっても、仕様どおりにU.ADMINISTRATOR用の管理機能は使用できないことを確認する。
③	TOEに登録されていないユーザー名で、セキュアプリントを送付した時のふるまいを確認する。 （管理者は、全てのセキュアプリントのジョブの確認や削除ができる。管理者以外は、ユーザー名が一致しないため操作できない。）
③	ボックスに格納した文書をネットワークに送信する最中にLANケーブルを抜き、仕様どおり送信エラーのログが作成されることを確認する。

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

7.3.3 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の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

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。なお、暗号鍵については、TOEの起動時に行われる暗号鍵の生成メカニズムとその開発者テ

ストの分析から、想定している攻撃者の攻撃能力では暗号鍵の入手や推測ができないことが評価されている。

① 公知の脆弱性情報であるネットワークサービスの不正利用、Webの各種脆弱性について、本TOEにも該当する懸念がある。
② Webのインタフェースについて、制限値を超えた長さの入力に対して、TOEが予期しない動作をする懸念がある。
③ Webのインタフェースについて、URLを直接指定したりセッション管理情報を推定したりすることにより、識別認証やアクセス制御がバイパスされる可能性がある。
④ スタートアップやクローズダウンの途中に電源OFF/ONを行うと、TOEが予期しない動作をする懸念がある。
⑤ 操作パネルとWebブラウザのインタフェースから、同時に同じ文書データを操作すると、TOEが予期しない動作をする懸念がある。
⑥ ディスク領域などTOE内のリソースが枯渇すると、TOEが予期しない動作をする懸念がある。

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があるかを決定するため、以下の侵入テストを実施した。

＜侵入テスト環境＞

図7-2の評価者独立テスト環境と同じ環境で実施した。ただし、侵入テスト用のツールを搭載したPCを追加して使用した。使用したツールの詳細を表7-4に示す。

表7-4　侵入テスト構成

名称		概要・利用目的
侵入テスト用PC		Windows XPを搭載したPCであり、以下の侵入テスト用ツールを動作させる。
	①Nessus 4.4.0	ネットワークサービスの脆弱性を検出するツール。脆弱性データは、2010年12月3日時点で最新のもの。
	②Nikto 2.03	Webサーバの脆弱性を検出するツール。脆弱性データは、2010年12月3日時点で最新のもの。
	②Tamper IE	Webブラウザ（PC）とWebサーバ（TOE）間の通信を仲介し、その間の通信データの参照と変更を行うツール。 Tamper IEにより、Webブラウザの制約を受け

		ずに、通信データを任意のデータに変更してWebサーバに送信することができる。

＜脆弱性テストの実施＞

懸念される脆弱性と対応する侵入テスト内容を表7-5に示す。

表7-5　侵入テスト概要

脆弱性	テスト概要
①	・TOEに対して、Nessusを使用してオープンポートと脆弱性の探索を行い、想定外のポートがオープンされていないこと、オープンポートに公知の脆弱性が存在しないことを確認した。 ・また、NiktoをTOEのWebサーバ機能の脆弱性の探索を行い、公知の脆弱性が存在しないことを確認した。
②	・パスワード変更画面で、TamperIEを使用してWebブラウザからTOEへの通信データを変更し、上限値を超えるパスワードを送信してもエラーとなり、異常な動作はしないことを確認した。
③	・Webブラウザのログイン画面で、ログインせずにログイン後のURLを直接指定してもログイン画面が表示され、ログインをバイパスすることができないことを確認した。 ・WebブラウザからTOEにログインしている間のセッション情報をTamperIEで複数取得し、それらが想定している攻撃者の攻撃能力では推測できない乱数となっていることを確認した。
④	・TOE起動途中に電源ボタンをOFFにすると、起動途中であってもシャットダウンが実行され、異常な動作はしないことを確認した。 ・TOEシャットダウン途中に電源ボタンをONにすると、シャットダウン完了後に起動され、異常な動作はしないことを確認した。
⑤	・操作パネルとWebブラウザから、同時に同じ文書を削除、文書の結合の結果を同じファイル名に格納するなど、同時アクセスを行う。その結果、最初の削除が有効、後から完了した格納が有効などの動作となり、異常な動作はしないことを確認した。
⑥	・HDDの保存領域が一杯になった状態で、さらにデータの保存を試みてもエラーとなり、異常な動作はしないことを確認した。 ・同様に、登録ユーザー数やセキュアプリントのジョブ数の上限についてもテストを行い、異常な動作はしないことを確認した。

c.　結果

実施した評価者侵入テストでは、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。

7.4 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。

7.5 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-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章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

消費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及び追加の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

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。

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 C5000 Series 2600.1 model Security Target Version 1.17　2011年3月17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.
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.
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.
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.
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。
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。
受信機能	Iファクスで受信した電子文書を紙文書にプリントまたは電子文書として転送する機能。
出力機能	TOEが紙文書を出力する機能。
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。
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、I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。
読み込み機能	TOEが紙文書を入力する機能。

ロール	アクセス制御機能で使用されるユーザーの権限情報。ロールにはMFPの提供機能毎に実行の許可・禁止の情報が含まれており、複数のロールを定義することができる。ユーザー登録の際には、ユーザーがどのロールに該当するかを設定する。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[2] ITセキュリティ認証申請手続等に関する規程　平成19年5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申請手続等に関する規程　平成19年5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 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[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3版 2009年7月 CCMB-2009-07-001 (平成21年12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3版 2009年7月 CCMB-2009-07-002 (平成21年12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3版 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[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3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] Canon imageRUNNER ADVANCE C5000 Series 2600.1 model Security Target Version 1.17　2011年3月17日　キヤノン株式会社

[13] Canon imageRUNNER ADVANCE C5000 Series 2600.1 model 評価報告書 第3版 2011年3月17日　みずほ情報総研株式会社 情報セキュリティ評価室

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