認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太
原紙押印済

評価対象

申請受付年月日(受付番号)	**平成17年9月30日（IT認証5070）**
認証番号	C0036
認証申請者	**キヤノン株式会社**
TOEの名称	• [**日本国内**] Canon iR4570/iR3570/iR2870/iR2270 **シリーズ** iR **セキュリティキット**-B2 • [**海外**] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2
TOEのバージョン	Version 2.03
PP適合	**なし**
適合する保証要件	EAL3
TOE開発者	**キヤノン株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　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18年1月18日

独立行政法人 情報処理推進機構
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　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「[日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2 Version 2.03 [海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03」は、独立行政法人 情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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

1.1 はじめに

この認証報告書は、「[日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2 Version 2.03 [海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が行った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ものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:　[日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2
　　[海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2
バージョン:Version 2.03
開発者:　キヤノン株式会社

1.2.2 製品概要

本製品は、デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞（以降、「デジタル複合機」という）にインストールして使用するソフトウェアである。

デジタル複合機は、コピー機能、送信（Universal Send）機能、ファクス受信機能、ユーザボックス機能、プリンタ機能、リモートUI機能（Webブラウザからデジタル複合機を操作するインタフェース）などを持つ事務機器である。コピー機能、送信（Universal Send）機能、ファクス受信機能（Iファクス受信／ファクス受信)、プリ

ンタ機能を使用するとデジタル複合機のHDD上にテンポラリイメージデータが生成される。ユーザボックス機能とよばれる文書保存機能、ファクス受信機能（Iファクスメモリ受信／ファクスメモリ受信、Iファクス転送／ファクス転送）を使用するとデジタル複合機が持つボックスにイメージデータが保存される。また、リモートUI機能を使用すると利用者のPC上のWebブラウザとデジタル複合機間のネットワーク上でイメージデータが通信される。

本製品をインストールすることにより、デジタル複合機のセキュリティ機能が強化され、HDD上に生成されたテンポラリイメージデータ、ボックスに保存されたイメージデータ、リモートUI機能で使用するネットワークを流れるイメージデータに対する暴露の脅威に対抗することができる。

1.2.3 TOEの範囲と動作概要

TOEがインストールされるデジタル複合機の使用環境例を図1-1に示す。

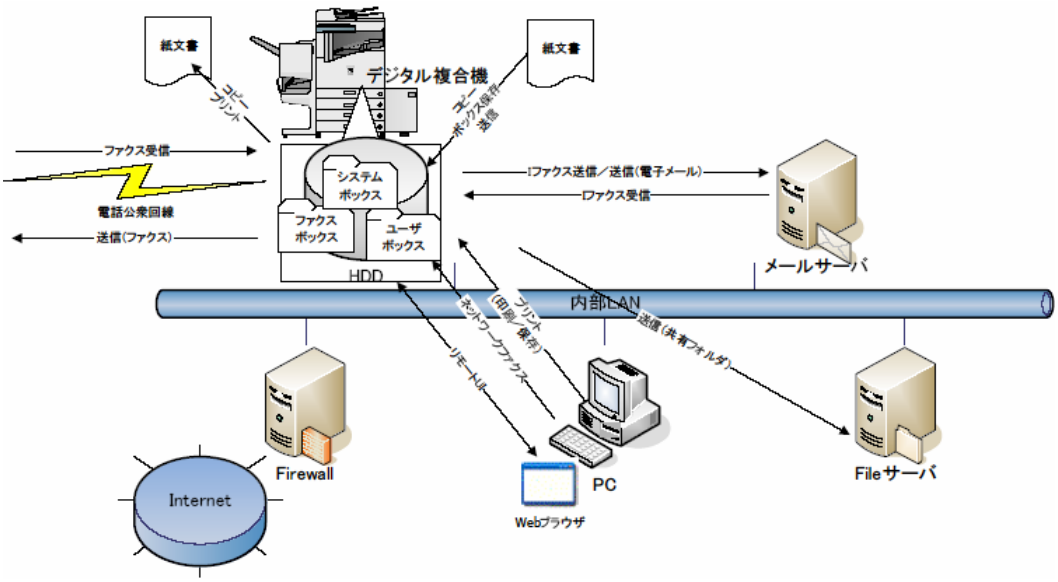

図1-1　TOEを含むデジタル複合機の使用環境例

TOEは、デジタル複合機にインストールされるデジタル複合機のすべての機能を制御するソフトウェア、リモートUIを使用するためのWebブラウザ用のコンテンツ、及び標準添付のMEAPアプリケーションであり、保護資産はデジタル複合機のHDDに生成されるテンポラリイメージデータ、ボックスに保存されるイメージデータ、及びデジタル複合機とリモートUI間を流れるイメージデータである。

デジタル複合機を制御するソフトウェアは、デジタル複合機上のコントローラー部で実行され、リモートUIのコンテンツは、PC側のWebブラウザで実行される。デジタル複合機上のコントローラーやHDDを含むハードウェア、PC側のハードウェア、OS、Webブラウザ、プリンタドライバ、ファクスドライバ、イメージプレビュー用プラグインはTOEに含まれない。

デジタル複合機におけるTOEの範囲を図1-2に示す。

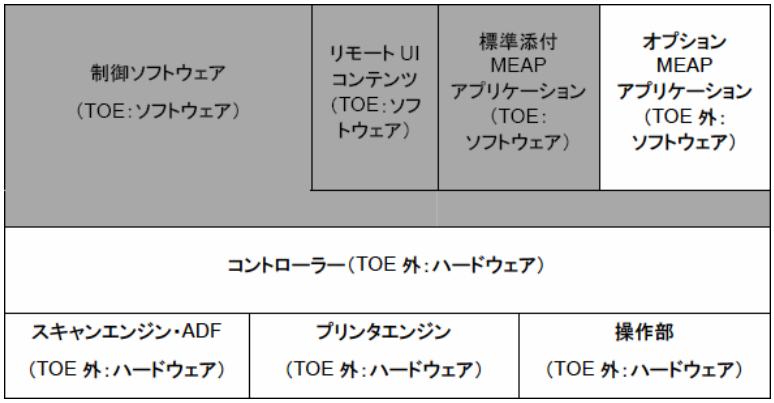

図1-2　デジタル複合機におけるTOE範囲

TOEは、セキュリティ機能として「HDDデータ暗号化機能」、「HDDデータ完全消去機能」、「ボックス利用者識別認証機能」、「ボックス管理機能」、「システム管理者識別認証機能」、「システム管理者管理機能」、「セキュア通信（リモートUI）機能」を持つ。

TOEのセキュリティ機能に関連する動作概要を以下に示す。

・ コピー、送信（Universal Send）、ファクス受信、プリント操作に関する動作概要
一般利用者が、コピー、送信（Universal Send）、ファクス受信（Iファクス受信／ファクス受信）、プリントの各操作を行うことにより、デジタル複合機のHDDに暗号化されたテンポラリイメージデータが生成され、テンポラリイメージデータが読み出される時はテンポラリイメージデータの復号が行われる。各操作が完了した時点で、HDDのテンポラリイメージデータは無意味なデータで上書き消去される。テンポラリイメージデータの暗号化、復号、上書き消去は、一般利用者がTOEの操作を意識することなく自動的に行われる。（関連するセキュリティ機能：HDDデータ暗号化機能、HDDデータ完全消去機能）

・ ユーザボックス機能、ファクス受信操作に関する動作概要
一般利用者が、ユーザボックス機能（スキャナによる文書の読み込み、PCからのボックス指定のプリント）、ファクス受信（Iファクスメモリ受信／ファクスメモリ受信、Iファクス転送／ファクス転送）の各操作を行うことにより、デジタル複合機が持つボックスに暗号化されたイメージデータが保存される。一般利用者は、ボックス一覧から該当のボックスを選択することにより、ボックスに保存したイメージデータを使用することができる。イメージデータが読み出される時、イメージデータの復号が行われる。ボックスからの文書の消去時には、ボックスに保存されているイメージデータは無意味なデータで上書き消去される。イメージデータの暗号化、復号、上書き消去は、一般利用者がTOEの操作を意識することなく自動的に行われる。（関連するセキュリティ機能：HDDデータ暗号化機能、HDDデータ完全消去機能）

・ ボックスを使用した文書管理に関する動作概要
一般利用者は、デジタル複合機の操作パネルやリモートUIを操作することによりデジタル複合機が持つボックスにボックス暗証番号を設定することができる。暗証番号が設定されたボックスをボックス一覧画面から選択するとボックス暗証番号の入力が要求される。暗証番号による認証に成功した場合、ボックスに保存してあるイメージデータを使用することができる。
また、リモートUIからはボックスに保存したイメージデータをプレビューすることができる。この時、リモートUIとデジタル複合機間で通信されるイメージデータはSSLにより保護される。（関連するセキュリティ機能：ボックス管理機能、ボックス利用者識別認証機能、セキュア通信（リモートUI）機能）

・ ボックス暗証番号の管理に関する動作概要
ボックス利用者は、ボックス暗証番号の認証に成功している状態において、該当ボックスのボックス暗証番号を変更、消去することができる。
システム管理者は、デジタル複合機の操作パネルを操作してシステム管理部門IDとシステム管理暗証番号による識別認証に成功することによりシステム管理モードに移行することができる。システム管理モードでは、すべてのボックスのボックス暗証番号の変更、消去を行うことができる。また、システム管理モードにおいては、システム管理部門IDとシステム管理暗証番号を変更することができる。（関連するセキュリティ機能：ボックス利用者識別認証機能、ボックス管理機能、システム管理者識別認証機能、システム管理者管理機能）

1.2.4 TOEの機能

TOEが持つ機能を以下に示す。

(1) セキュリティ機能
TOEは以下に示すセキュリティ機能を持つ。

・ HDDデータ暗号化機能
すべてのテンポラリイメージデータ及びイメージデータを暗号化してHDDに保存する。

・ HDDデータ完全消去機能
HDD上のすべてのテンポラリイメージデータ及びイメージデータを消去する際に、無意味なデータを上書きして完全消去をする。

・ ボックス利用者識別認証機能
ボックスの文書を操作して該当のボックスに保存されたイメージデータを読み出す前に、暗証番号によって、正規のボックス利用者かどうかを識別認証する。

・ ボックス管理機能
ボックス暗証番号の設定を行う。

・ システム管理者識別認証機能
システム管理モードに移行する際に、システム管理部門IDとシステム管理暗証番号によって、正規のシステム管理者かどうかを識別認証する。

・ システム管理者管理機能
システム管理部門ID及びシステム管理暗証番号の設定、及びセキュア通信（リモートUI）機能の設定・解除を行う。

・ セキュア通信（リモートUI）機能
リモートUIとデジタル複合機間の通信にSSLを使用する。

(2) デジタル複合機の制御
TOEは以下に示す機能の制御を行う。

・ コピー機能
スキャナで紙文書を読み込んでプリントすることにより、紙文書の複写をする機能である。紙文書を読み込んだ際に、HDD内にテンポラリイメージデータを生成する。

・ 送信（Universal Send）機能
スキャンした文書やユーザボックス／システムボックスに保存されている文書を、ファクス送信したり、TIFFやPDFファイル形式に変換して電子メールやPCの共有フォルダなどのあて先に送信したりする機能である。また、PC上からファクスドライバを使用して、デジタル複合機をネットワークファクスとして使用することができる。送信時にはHDD上にテンポラリイメージデータを生成する。

・ ファクス受信機能
ファクス受信／Iファクス受信した文書を紙にプリントしたり、転送したりする機能である。受信時にHDDにテンポラリイメージデータを生成する。
ファクスメモリ受信／Iファクスメモリ受信した文書をシステムボックスにイメージデータとして保存し、送信やプリントすることができる。
Iファクス転送／ファクス転送により、システムボックスに保存する前に、他のあて先やファクスボックスに振り分けることが可能である。ファクスボックスに受信した文書はプリントすることができる。

・ ユーザボックス機能
スキャナから読み込んだ文書や、PCからボックス保存を指定してプリントした文書を、ユーザボックスにイメージデータとして保存する機能である。ユーザボックスに保存されたイメージデータは、文書結合やフォーム画像のイメー

ジ合成などの編集をしてから出力することができる。

・ プリント機能
デジタル複合機をネットワークプリンタとして使用し、PCからのプリントデータをプリントする機能である。プリント時にHDDにテンポラリイメージデータを生成する。

・ リモートUI機能
利用者は、デジタル複合機本体の操作パネルを使用する以外に、リモートUIを使用することができる。リモートUIは利用者のWebブラウザからネットワークを経由して、デジタル複合機にアクセスし、デジタル複合機の状況の確認やジョブの管理、ボックスの管理、各種設定などができる機能である。Webサーバ機能はデジタル複合機内に内蔵されているので、Webブラウザ以外のソフトウェアを用意する必要はない。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート3及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット･B2 V2 セキュリティターゲット Version 1.03」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「[日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2 Version 2.03 [海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03 評価報告書」

（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]のいずれか）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成17年9月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、商用製品であるデジタル複合機のためのソフトウェアであり、一般のオフィスで使用されることを想定している。従って、最小機能強度として”SOF-基本”を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

- HDDデータ暗号化機能
  TOEはキヤノンiR暗号鍵生成アルゴリズムを用いて、Triple DES用の168bit暗号鍵を生成する。TOEはすべてのイメージデータのHDDへのデータ書き込み時に、FIPS PUB 46-3に準拠する暗号鍵長168bitのTriple DESアルゴリズムを使用して、イメージデータを暗号化する。TOEはすべてのイメージデータのHDDからのデータ読み込み時に、FIPS PUB 46-3に準拠する暗号鍵長168bitのTriple DESアルゴリズムを使用して、イメージデータを復号する。TOEはキヤノンiR暗号鍵破棄方法に基づき、暗号鍵を破棄する。

- HDDデータ完全消去機能
  TOEがテンポラリイメージデータやボックスに保存されたイメージデータをHDDから削除する際、そのハードディスク領域を無意味なデータで上書きすることによりデータの完全消去を実施する。HDDデータ完全消去機能が動作するタイミングを以下に示す。
  - コピー、プリント、ファクス受信、送信（Universal Send）操作時に生成されたテンポラリイメージデータを、コピー等の処理後にHDDから削除する。
  - ボックスに保存されたイメージデータを、ボックスの文書消去の操作時にHDDから削除する。
  - テンポラリイメージデータを、TOEの起動時にHDDから削除する。
  - テンポラリイメージデータおよびボックスに保存されたイメージデータを、システム管理者による『全データ/設定の初期化』の操作後の再起動時にHDDから削除する。

・ ボックス利用者識別認証機能

TOEは、利用者がボックスにアクセスする前に（ボックスへのイメージデータの追加を除く）、既にボックス暗証番号が設定されているボックスであれば、ボックス暗証番号の入力を要求する。ボックスに暗証番号が設定されていない場合には、暗証番号の入力は要求しない。入力したボックスの暗証番号が、選択しているボックスに登録された暗証番号と一致した場合にのみ、操作している利用者を、該当ボックス利用者として識別認証し、該当ボックスの操作画面を表示する。TOEは、該当ボックス利用者として識別認証された利用者を、操作パネルでの操作においては該当ボックスへの操作画面を終了してボックス一覧表示画面に戻るまで該当ボックス利用者として維持し、リモートUIでの操作においては、他のボックスに対する操作を実施する、またはWebブラウザを終了するまでの間、該当ボックス利用者として維持する。操作パネルもしくはリモートUIを使って、入力されたボックス暗証番号が一致しない場合は、TOEは次の入力画面を出すまでに、1秒間の間隔をあける。

・ ボックス管理機能

TOEは、正規のボックス利用者およびシステム管理者に対してのみ、そのボックスの暗証番号を変更、消去する（ボックス暗証番号を付加しない）権限を与える。TOEは、システム管理者に、操作パネルを操作することによってボックスの暗証番号を変更、消去する機能を提供する。TOEは、該当ボックス利用者に、操作パネルまたはリモートUIの操作によって、そのボックスの暗証番号を変更、消去する機能を提供する。TOEは、ボックス暗証番号を7桁の数字に制限する。暗証番号が付加されなかった場合には、そのボックス暗証番号を消去する。

・ システム管理者識別認証機能

TOEは、システム管理者としてTOEを使用する利用者を、システム管理者として識別認証するため、システム管理者のシステム管理部門IDとシステム管理暗証番号の入力を要求する。システム管理者識別認証機能は、部門別ID管理を行っている場合には、操作パネルやリモートUIにおいてデジタル複合機を操作する前に実施され、部門別ID管理を行っていない場合には、操作パネルやリモートUIにおいてシステム管理設定画面を表示する際に実行される。入力したシステム管理部門IDとシステム管理暗証番号が、登録してあるものと一致した場合にのみ、操作している利用者をシステム管理者として識別認証する。操作パネルもしくはリモートUIを使って、入力されたシステム管理部門IDまたはシステム管理暗証番号が一致しない場合は、TOEは次の入力画面を出すまでに、1秒間の間隔をあける。TOEは、操作パネルを操作して、システム管理者として識別認証された利用者については、システム管理モードを終了するまでシステム管理者として維持し、システム管理設定および、すべてのボックスに対する操作やボックス管理機能の実施を可能とする。システム管理モードは、操作パネルのIDキーの押下によって終了する。TOEは、リモートUIを操作してシステム管理者として識別認証された利用者について、システム管理設定の実施を可能とする。リモートUIを実行しているWebブラウザを終了するまで、

利用者はシステム管理者として維持される。

・ システム管理者管理機能
TOEは、正規のシステム管理者に対してのみ、下記の権限を与える。
システム管理部門IDおよびシステム管理暗証番号を変更することや、システム管理部門IDを削除する（システム管理部門IDを設定しない）ことができる。TOEはシステム管理暗証番号を7桁の数字に制限する。
セキュア通信（リモートUI）機能を設定・解除できる。

・ セキュア通信（リモートUI）機能
TOEは、リモートUIにおける、TOEと利用者PC上のWebブラウザとの間の通信において、その通信データを改変および暴露から保護するためにSSLを用いる。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.HDD_ACCESS: HDDデータの直接アクセス	悪意のある者が、デジタル複合機のHDDを取り外し、ディスクエディタなどを利用してHDDに直接アクセスすることにより、デジタル複合機のHDDに保存されている、テンポラリイメージデータやボックスに保存されたイメージデータを暴露するかもしれない。
T.UNAUTH: 許可されない利用者の操作	該当のボックス利用者以外の者（システム管理者を除く）がデジタル複合機の操作パネルまたはリモートUIを操作することによって、該当のボックスに保存されたイメージデータを暴露するかもしれない。
T.NETWORK_TAP: 通信路上のデータ盗聴	悪意のある者が、リモートUIで使用される通信路上のデータを盗聴して、暗証番号、イメージデータを暴露するかもしれない。

1.5.6 組織のセキュリティ方針

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はない。

1.5.7 構成条件

本TOEは、キヤノン株式会社が提供するデジタル複合機にインストールするソフトウェア製品及びリモートUIを使用するためのWebブラウザ用コンテンツである。TOEが動作する環境を以下に示す。

表1-2　TOEが動作する対象のデジタル複合機と必須オプション（日本国内モデル）

デジタル複合機モデル名	必須オプション
Canon iR4570	PCIバス拡張キット・B1、セキュリティ拡張ボード（USB）・D1、増設メモリ（本体と合わせ512MB以上）
Canon iR4570F	
Canon iR3570	
Canon iR3570F	
Canon iR2870	
Canon iR2870F	
Canon iR2270	
Canon iR2270F	

表1-3　TOEが動作する対象のデジタル複合機と必須オプション（海外モデル）

デジタル複合機モデル名	必須オプション
Canon iR4570	Expansion Bus-B1、USB Application Interface Board-D1
Canon iR3570	
Canon iR2870	
Canon iR2270	

リモートUIを使用してデジタル複合機を操作するには、以下のソフトウェアをPC上にインストールして使用する必要がある。

・ Webブラウザ

表1-4　リモートUIが動作するWebブラウザ環境

動作OS	ソフトウェア名	バージョン
Windows	Microsoft Internet Explorer	5.01 SP2 以降
	Netscape Communicator	4.6 以降
Macintosh	Microsoft Internet Explorer	5.0 以降

Netscape Communicator 5.x 、Netscape 6.xを除く。

・ イメージプレビュー用プラグイン（リモートUIからプレビューを行うときのみ必要）
Canon JBIG Image Viewer プラグインソフトウェア（デジタル複合機に添付）

1.5.8　操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-5に示す。

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1-5　TOE使用の前提条件

識別子	前提条件
A.ADMIN： 信頼できる管理者	システム管理者は、信頼でき、不正な行為は行わないものと想定する。
A.PWD_MANAGE: 暗証番号の管理	ボックス暗証番号及びシステム管理暗証番号は、他人に知られず、他人から容易に推測されないものと想定する。
A.PWD_SET: 暗証番号の設定	保護する必要のあるイメージデータが保存されているボックスには、ボックス暗証番号が設定されているものと想定する。 システム管理部門ID及びシステム管理暗証番号は、設定されていると想定する。
A.NETWORK： デジタル複合機の接続	TOEが動作するデジタル複合機をネットワークに接続する場合、インターネットなどの外部ネットワークから直接アクセスされない内部ネットワークに接続されるものと想定する。

1.5.9　製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

(1) [日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2 Version 2.03に添付されるドキュメント

- iR セキュリティキット・B2 V2 ユーザーズガイド, FA7-9025
- iR4570/iR4570F/iR3570/iR3570F/iR2870/iR2870F/iR2270/iR2270F ユーザーズガイド, FA7-9029
- iR4570/iR4570F/iR3570/iR3570F/iR2870/iR2870F/iR2270/iR2270F コピー/ ボックスガイド, FA7-9030
- iR4570/iR4570F/iR3570/iR3570F/iR2870/iR2870F/iR2270/iR2270F 送信/ ファクスガイド,FA7-9031
- iR4570/iR4570F/iR3570/iR3570F/iR2870/iR2870F/iR2270/iR2270F リモートUI ガイド, FA7-9032
- iR4570/iR4570F/iR3570/iR3570F/iR2870/iR2870F/iR2270/iR2270F ネットワークガイド, FA7-9033
- MEAP アプリケーション管理機能ガイド, FA7-9034
- MEAP 認証システム設定ガイド, FA7-9035

(2) [海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03に添付されるドキュメント

- iR Security Kit-B2 V2 Reference Guide, FA7-9036
- 4570/3570/2870/2270 Reference Guide, FA7-9041
- 4570/3570/2870/2270 Copying Guide, FA7-9042

- 4570/3570/2870/2270 Mail Box Guide, FA7-9043
- 4570/3570/2870/2270 Sending and Facsimile Guide, FA7-9044
- 4570/3570/2870/2270 Remote UI Guide, FA7-9045
- 4570/3570/2870/2270 Network Guide, FA7-9046
- MEAP SMS Administrator Guide, FA7-9047

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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。

2.2 評価実施概要

以下、本評価報告書による評価実施の履歴を示す。

評価は、平成17年10月に始まり、平成17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17年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・配付と運用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17年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。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を表2-1に示す。

表2-1　開発者テストの構成

TOE	バージョン
TOE	日本国内向け：Ver 2.03　　海外向け：Ver 2.03
機器	主な仕様
デジタル複合機	iR2270F (日本国内向け)、iR2270 (海外向け)
デジタル複合機のオプション	・iR 256MB 拡張RAM・B1　　・セキュリティ拡張ボード(USB)・D1 ・PCIバス拡張キット・B1　　・Send拡張キット ・スーパーG3 FAXボード・R1　　・Webブラウザ
PC	Windowsが動作するPC3台。
HUB	100MbpsスイッチングHUB
ネットワークケーブル2本	UTPケーブル（カテゴリ5）
FAX	デジタル複合機の通信相手となるFAX
擬似交換機	デジタル複合機とFAXを擬似の電話回線で接続するために使用する機器
ソフトウェア	主な仕様
OS	Microsoft Windows2000 Professional Service Pack 4
通信ソフトウェア	シリアル通信用ソフトウェア
印刷ソフトウェア	Windows OSに対応し、Windowsの標準的なプリンタ設定による印刷の実行が可能なソフトウェア
Webブラウザ	Microsoft Internet Explorer Version 6.0 Service Pack 1
プリンタドライバ	Windows LIPS IV または LIPS LXプリンタドライバ(日本国内) PCL6またはPCL5eプリンタドライバ、PSプリンタドライバ(海外向け)

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を表2-1に示す。

開発者は、TOEをインストールするデジタル複合機としてSTに記載されているすべてのデジタル複合機のモデルを使用していない（4種類のモデルのうち1種類を使用）。しかし、TOEが動作するコントローラーは各モデルで同じであり、スキャナエンジンとプリンタエンジンの相違によるTOEへの影響はない。従って、すべてのデジタル複合機のモデルを使用しなくても動作環境を考慮したテストが実施されていると判断できる。

通信ソフトウェア、印刷ソフトウェアなどは、テストに必要な情報を取得す

るための機材であり、TOEのセキュリティ機能に影響を及ぼさないことが確認されている。ファクスとのデータ授受については、擬似交換機を用いてファクス機器を接続しているが、実回線と擬似交換機の差異がTOEのセキュリティ機能に与える影響はない。

その他の構成要素は、STで記載されているTOEの動作環境と一致している。

b.テスト手法

①デジタル複合機本体の操作パネルまたはリモートUIを操作して、セキュリティ機能の外部インタフェースを刺激し、外部インタフェースのふるまいを直接観察する。

②外部インタフェースにより直接セキュリティ機能の動作を観察できない機能については、プログラム動作状態のモニタリング、ハードディスクのダンプ取得、LAN上パケットのモニタリングを行いセキュリティ機能のふるまいを確認する。

c.実施テストの範囲

テストは開発者によって107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、上位レベル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。

d.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。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストの構成に侵入テストに使用するツールを加えた構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト手法

評価者は、開発者が行ったテスト手法が、セキュリティ機能の期待されたふるまいを検証するのに適していると判断し、開発者テストと同様の手法でテストを実施している。

b.実施テストの範囲

評価者は、評価者が独自に考案したテストを10項目、開発者テストのサンプリングによるテストを24項目、侵入テストを14項目、48項目のテストを実施している。

評価者が独自に考案したテストは、以下に示す観点を考慮している。

①外部からふるまいを確認できないセキュリティ機能
②パラメタを変更することができるセキュリティ機能

サンプリングテストは、開発者が実施した107項目のテストの23%にあたる24項目をすべての機能が含まれるように選択している。

侵入テストは、公知になっている脆弱性情報、デジタル複合機特有の脆弱性、評価者が評価作業中に得たTOEに関する知識に基づき脆弱性分析を行い、その分析結果に基づいて14項目のテストを実施している。

d.結果

実施したすべての評価者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。また、悪用される可能性のある明白な脆弱性がないことを確認した。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

3 認証実施

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 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

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本評価報告書で示されたように評価されていること。

④ 本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 本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。

4 結論

4.1 認証結果

提出された本評価報告書、当該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保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。

ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別､概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ､ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が明記され、それらが脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ､PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ､PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が理路整然とし、完結しており、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ､CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ､CCを参照せずに明示された要件はないため非適用であることを確認している。

ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完結しており、理路整然とし、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.3.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完

	全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していることを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**

ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果が含まれておりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判

	断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法が記述されていることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

HDD	デジタル複合機に搭載されるハードディスクのこと。TOE本体及び保護資産が保存される。
Iファクス	ファクス文書の送受信を行うためのインフラとして、電話回線ではなく、インターネットを使用するインターネットファクスのこと。
MEAP	デジタル複合機上で動作するアプリケーションのプラットフォームのこと。（Multifunctional Embedded Application Platform） Java言語を使用して開発された専用のアプリケーション『MEAPアプリケーション』を稼動させることができる。
MEAPアプリケーション	デジタル複合機上で動作するJava言語を使用して開発された専用のアプリケーションであり、プリント、コピー、ファクス、スキャン等、デジタル複合機の機能と組み合わせることにより、ユーザインターフェースのカスタマイズ、ドキュメントフローの簡略化、定型業務の自動化を実現することができる。
イメージデータ	読み込み、プリント、受信などによってデジタル複合機内に

	生成された画像データ。
一般利用者	デジタル複合機を使用する利用者。
コントローラー	TOEが動作するプラットフォームであり、CPUやメモリなどが実装されるハードウェアである。
システムボックス	Iファクスメモリ受信／ファクスメモリ受信した文書が保存されるボックスであり、文書のプリントまたは送信が可能である。
システム管理者	デジタル複合機の設定や管理を行う管理者のこと。ボックス利用者に代わって、ボックスの管理を行う場合もある。デジタル複合機上では、システム管理部門IDを使用する利用者がシステム管理者として識別される。
システム管理モード	デジタル複合機に対しシステム管理者としての権限を維持するモード。このモードが維持されている間の操作は、システム管理者の権限での操作となる。このモードに移行するためには、システム管理者のシステム管理部門IDとシステム管理暗証番号が必要になる。IDキーの押下により終了する。
スキャンエンジン・ADF	デジタル複合機を構成するハードウェアであり、紙媒体からイメージデータをデジタル複合機に読み込むための機器である。
操作部	デジタル複合機を構成するハードウェアであり、操作キーとタッチパネルから構成され、デジタル複合機を操作するときに使用される。
デジタル複合機	コピー機能、ファクス機能、プリンタ機能、送信（Universal Send）機能などを併せ持つ複写機<Canon iR4570/iR3570/iR2870/iR2270 シリーズ>のこと。これらの機能を使用するため、大容量のHDDを持ち、TOEはこの複合機上で動作する。
ファクスボックス	Iファクス転送／ファクス転送された文書が保存されるボックスであり、保存された文書の再プリントが可能である。
フォーム画像	イメージ合成のためにデジタル複合機に登録された画像のこと。
プリンタエンジン	デジタル複合機を構成するハードウェアであり、デジタル複合機内のイメージデータを紙媒体に印刷するための機器である。

部門ID	デジタル複合機を使用する部門もしくは個人のID。部門ID管理が実施されている場合には、デジタル複合機を操作する前に、識別認証が必要になる。システム管理者は、部門IDのうち、システム管理部門IDとして登録された利用者である。
部門別ID管理	利用者部門ごとにコピー枚数などを管理するために、利用者部門ごとに部門ID及び暗証番号を設定する機能である。部門別ID管理を実施すると、デジタル複合機の使用前に、正しい部門ID及び暗証番号によって識別認証されることが要求される。
文書	デジタル複合機内で取り扱われる利用者データであり、管理情報とイメージデータから構成される。
ボックス	デジタル複合機において読み込みやプリント、ファクス受信した文書を保存する領域。ユーザボックス、ファクスボックス、システムボックスの3種類が存在する。
ボックス利用者	該当のボックスを利用する一般利用者。そのボックスに暗証番号を設定することにより、他の一般利用者のそのボックスへのアクセスを制限することができる。
メモリ受信	受信したファクス／Iファクスを、プリントしないでシステムボックスに保存しておくこと。
ユーザボックス	デジタル複合機で一般利用者が読み込んだ文書や、PCからプリントした文書などが保存されるボックスであり、文書のプリントや送信などが可能である。
リモートUI	Web ブラウザからネットワークを経由してデジタル複合機にアクセスし、デジタル複合機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である。

6 参照

[1] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット･B2 V2 セキュリティターゲット Version 1.03 2005年11月17日 キヤノン株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構 EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031

[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2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032

[10] 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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論

バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版、補足-0407

[22] [日本国内] Canon iR4570/iR3570/iR2870/iR2270 シリーズ iR セキュリティキット・B2 Version 2.03 [海外] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03 評価報告書 VAA-ETR-0001-01 第1.1版 2005年12月26日 株式会社電子商取引安全技術研究所 評価センター