認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	平成20年3月27日 (IT認証8218)
認証番号	C0198
認証申請者	キヤノン株式会社
TOEの名称	Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2
TOEのバージョン	Version 1.00
PP適合	なし
適合する保証パッケージ	EAL3
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20年12月24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　鈴木　秀二

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 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 Version 1.00」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証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

1.1 はじめに

この認証報告書は、「Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 Version 1.00」（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：	Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2
バージョン：	Version 1.00
開発者：	キヤノン株式会社

1.2.2 製品概要

本製品（＝TOE）は、デジタル複合機「Canon iR3225/iR3230/iR3235/iR3245 Series」（以下「MFP」という。）にセキュリティ機能を追加するためのオプションソフトウェアである。本TOEがMFPにインストールされることにより、MFPのシステムソフトウェア（制御ソフトウェア等）はTOEで置き換えられる。

本TOEは、基本機能として、MFPのコピー機能、プリンタ機能、ファクス受信機能、ユーザボックス機能等の制御を行い、コピーやプリント等の際にイメージ

データをHDDに一時保存する。一般的なデジタル複合機では、このような一時保存されたイメージデータであるテンポラリイメージデータを、コピーやプリント等の終了時に論理的に削除するだけで、その残存情報を削除しておらず、そのため、残存情報が不正に再利用される可能性が存在していた。

本TOEは、テンポラリイメージデータの残存情報を再利用されることから保護するために、セキュリティ機能としてHDDデータ完全消去機能を有している。また、本TOEは、上記HDDデータ完全消去機能を管理するためのセキュリティ機能として、システム管理者識別認証機能、及びシステム管理機能を有している。

1.2.3 TOEの範囲と動作概要

TOEの物理的範囲を図1-1に示す。

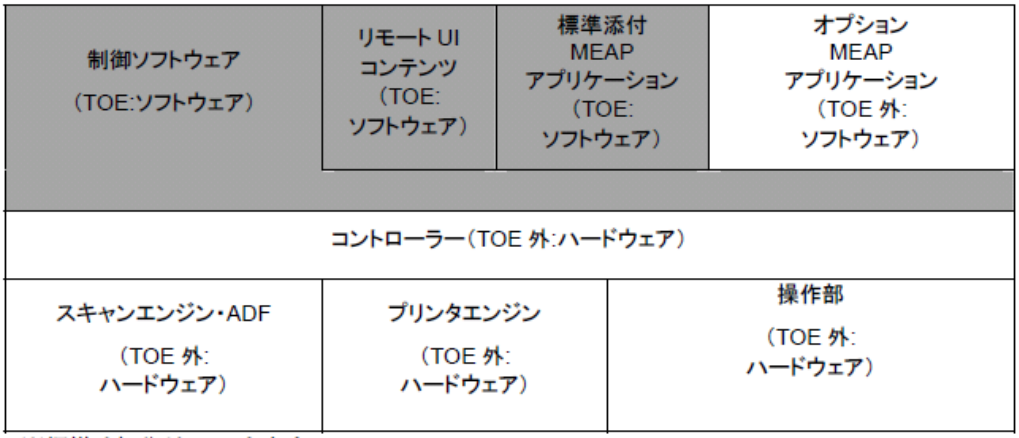

図1-1 TOEの物理的範囲

TOEの物理的範囲は、図1-1に示したように、MFPのすべての機能を制御するソフトウェア全体、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、及び標準装備されるMEAP認証アプリケーションである。これらはいずれも、MFPのHDDにインストールされる。

MFP上のコントローラやHDDを含むハードウェア、及びユーザ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構成に含まれない。

TOE上では、MEAPに対応するアプリケーションを実行することができる。標準装備されるMEAP認証アプリケーションはTOEの範囲内となるが、オプションでインストールされるMEAPアプリケーションはTOEの範囲外である。

また、TOEがインストールされたMFPは、一般のオフィス等において汎用的に使

用されることを想定している。MFPの使用環境例を図1-2に示す。MFPは、図1-2に示されたTOEの機能をフルに使用する場合以外に、複写機としてスタンドアロンで使用される場合や、ファクス機を目的として電話回線のみに接続される場合も想定される。

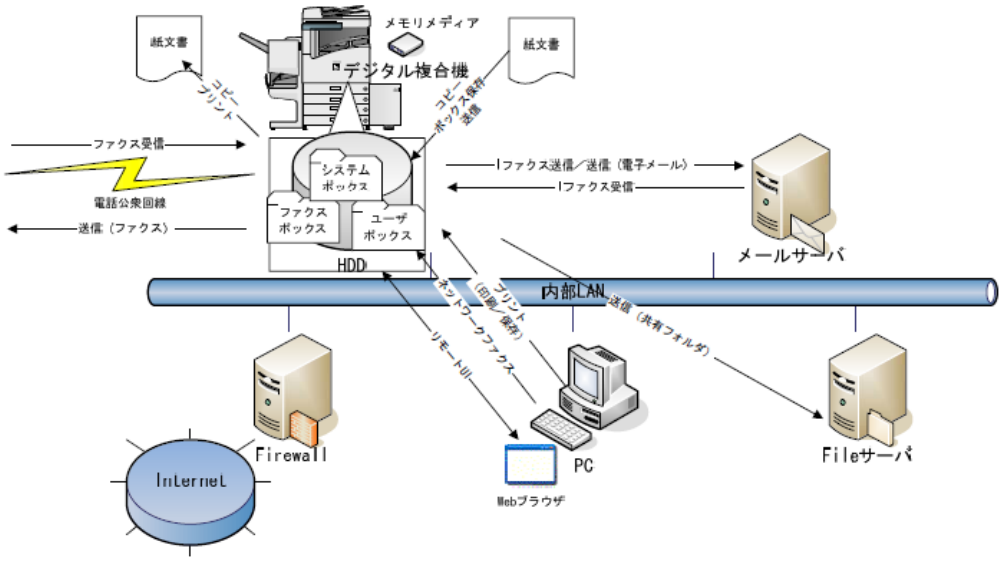

図1-2　MFPの想定設置使用環境

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データ完全消去機能
  HDD上のテンポラリ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残存情報を完全消去する機能である。
- 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機能である。
- システム管理機能
  システム管理部門IDとシステム管理暗証番号の設定、及び「HDDデータ完全消去機能」の各種設定を行う機能である。

(2)　MFPの制御

TOEは以下に示す機能の制御を行う。

・ コピー機能
紙文書をスキャナで読み込み、プリントすることにより、紙文書を複写する機能である。

・ ファクス受信機能
ファクスやIファクスから受信した文書を紙にプリントまたは転送する機能である。

・ 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操作を施した後に出力することが可能である。

・ プリンタ機能
MFP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。

・ 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ファイル形式で電子メールアドレスやPCの共有フォルダ等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、MFPをネットワークファクスとして使用することができる。

・ メモリメディア連携機能
ユーザによって挿入されたメモリメディアに、スキャナで読み取った原稿画像やボックス内の文書をPDF等に変換し、保存する機能である。また、メモリメディア内に保存された文書を印刷する機能である。

・ リモートUI機能
利用者は、MFP本体の操作パネル以外に、リモートUIを使用して、MFPの機能を使用することができる。利用者は、リモートUI機能により、PC上のWebブラウザからネットワークを経由してMFPにアクセスし、MFPの状況の確認やジョブの管理、ボックスの管理、各種設定等を行うことができる。

・ MEAP機能
MEAPに対応するアプリケーションを実行する機能である。利用者は、標準添付のMEAPアプリケーション以外に、オプションソフトウェアであるMEAPアプリケーションをインストールして、MFPに新たな機能を追加することができる。

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セキュリティ認証申請手続等に関する規程」[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」[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 iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 セキュリティターゲット」（以下「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]のいずれか) 附属書B、CCパート2（[6][9][12]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]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、「Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]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、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20年12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

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

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、一般のオフィス等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データ完全消去機能

  TOEがテンポラリイメージデータをHDDから削除する際は、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テンポラリイメージデータの残存情報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。

  1）コピー、プリント、ファクス受信、送信（Universal Send）等の操作時に生成されたテンポラリイメージデータの残存情報を、コピー等の処理後にHDDから完全消去する。
  2）テンポラリイメージデータの残存情報を、TOEの起動時にHDDから完全消去する。
  3）テンポラリイメージデータの残存情報を、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から完全消去する。

- システム管理者識別認証機能

  TOEは、「システム管理機能」の利用者をシステム管理者に限定するため、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。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。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、システム管理者として識別認証せず、応答を1秒間遅延させる。

・ システム管理機能

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。

1）システム管理部門ID、システム管理暗証番号を変更または削除することができる。

2）「HDDデータ完全消去機能」に関して、下記の各種設定ができる。

a)「HDDデータ完全消去機能」の起動・停止

b)「HDDデータ完全消去機能」の消去モードの変更

① 0データ1回書き込み

② ランダムデータ1回書き込み

③ ランダムデータ3回書き込み

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、デジタル複合機のテンポラリイメージデータの残存情報を再利用するかもしれない。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって遵守が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

TOEは、MFPにインストールすることにより動作する。また、TOEの下記の機能を利用するためには、下記のサーバやソフトウェアを必要とする。

リモートUIを使用してデジタル複合機を操作する場合は、WebブラウザをPC上にインストールして使用する必要がある。

PCからプリントやファクス送信を行う場合は、適切なプリンタドライバまたはファクスドライバをPCにインストールして使用する必要がある。

Iファクスや送信（Universal Send）を行う場合は、適切なメールサーバ、FTPサーバ、ファイルサーバが必要となる。

なお、本評価においては、TOEをPCから利用する環境として、以下のソフトウェアを評価構成としている。

OS: Microsoft Windows XP Professional SP2

Web ブラウザ: Microsoft Internet Explorer Version 6.0 SP2

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1-2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1-2 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.ADMIN_PWD システム管理暗証番号	システム管理者は、システム管理暗証番号として、安易でない7桁の数字を設定するものと想定する。
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。

・HDD Data Erase Kit-B2 Reference Guide

・HDD Data Erase Kit-B2 Installation Procedure

・iR Series User Documentation

なお、iR Series User Documentationは、下記6種類のGuideから構成される。

・imageRUNNER 3225/3230/3235/3245 Reference Guide

・imageRUNNER 3225/3230/3235/3245 Copying and Mail Box Guide

・imageRUNNER 3225/3230/3235/3245 Sending and Facsimile Guide

・imageRUNNER 3225/3230/3235/3245 Remote UI Guide

・imageRUNNER 3225/3230/3235/3245 Network Guide

・MEAP SMS Administrator Guide

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。

2.2 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20年4月に始まり、平成20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20年8月及び9月に開発・製造現場へ赴き、記録、現物確認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・ライフサイクル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20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。

各ワークユニットの評価作業中に発見された問題点は存在せず、所見報告書の発行は行われなかった。

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。

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図2-1に示す。

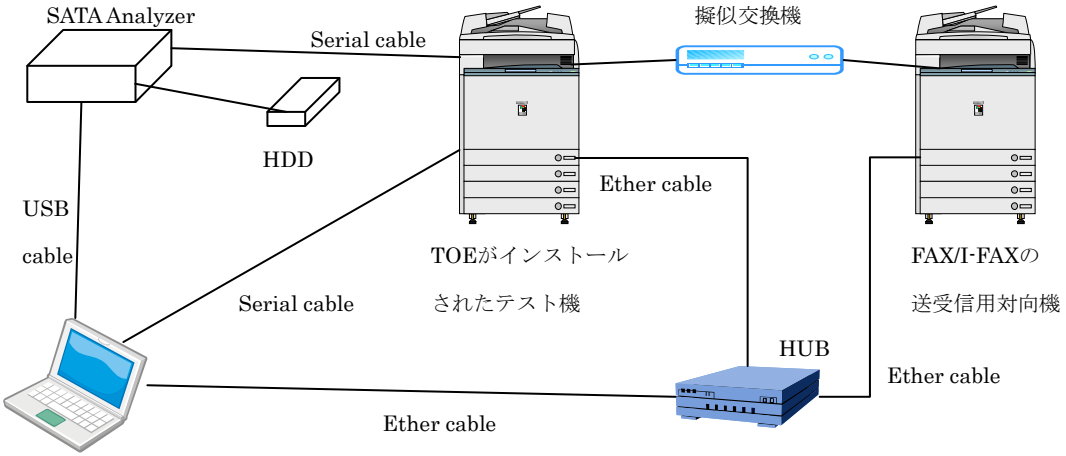

図2-1　開発者テストの構成図

開発者テストは、図2-1に示したテスト環境・構成において、以下の表2-1に示した構成要素（ハードウェア、ハードウェア・ツール、ソフトウェア）を利用することにより実施された。

表2-1　構成要素一覧

構成要素	概要説明
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。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。本テストにおいては、iR3245を使用。 ※ TOEが動作する対象のデジタル複合機(Canon iR3225/iR3230/iR3235/iR3245 Series)において、TOEの動作するコントローラはすべて同一であるため、上記の1機種のみを使用したテストで問題ない。テストでは2台使用(FAX通信機能利用のため、iR3245とは別に同一機種iR3245を使用)する。
TOE	Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 Version 1.00。
デジタル複合機のオプションソフトウェア（TOE外）	Send機能を利用可能にするUniversal Send（ソフトウェア）、本体UIでウェブブラウザ機能を利用可能にするWeb Access Software（ソフトウェア）、メモリメディア機能を利用可能にするUSB Memory Connectivity（ソフトウェア）、ページ記述言語「PostScript」を利用するPS（ソフトウェア）、ページ記述言語「Printer Control Language」を利用可能にするPCL（ソフトウェア）、ページ記述言語「Ultra Fast Rendering II」を利用可能にするUFR Ⅱ（ソフトウェア）、ダイレクトプリント機能、ウェブブラウザからの印刷機能を可能にするDirect Printing（ソフトウェア）をインストール。 ※ 上記のオプションソフトウェア（「1.5.7 構成条件」には記載されていない）は、サービスエンジニアによって行われるTOEのインストールを含むデジタル複合機

構成要素	概要説明
	の設置・立ち上げにおいて、インストールされる（消費者ごとのデジタル複合機の使用方法に応じて、カスタマイズしてインストールされる可能性がある)。
SATA Analyzer	ATA Write Commandのパケットをキャプチャして分析することが可能な機器。
PC	OSとしてWindowsをインストールし、シリアルケーブルでの接続及びネットワーク接続が可能なコンピューター一台。
RS232c ボード	デジタル複合機本体内部のコントローラ部に接続するシリアル通信用基板。
シリアルケーブル	PCとデジタル複合機本体を接続するためのDSUB 9ピンのコネクタを有するクロスケーブル。
シリアルATAケーブル	HDDコントローラとHDDをつなぐケーブル。
HUB	LANを構築するための接続機器。TCP/IP接続可能な100Mbps スイッチングHUBを使用する。
ネットワークケーブル	デジタル複合機本体とHUB、及びPCが接続されたネットワーク線とHUBを接続するUTPケーブル（カテゴリ5)。3本使用。
擬似交換機	デジタル複合機とFAX（もう1 台のデジタル複合機 : iR3245）を擬似の電話回線で接続するために使用する機器。
OS	Microsoft Windows XP Professional Service Pack 2。
ターミナルソフトウェア	PCで動作させるWindows標準搭載のターミナルソフトウェア。デジタル複合機本体と接続して、TOEの状態をモニタするために使用する。Tera Term Proを使用。
Web ブラウザ	汎用のブラウザソフトウェア。操作補助PC上でリモートUIを動作させるのに用いる。Microsoft Internet Explorer Version 6.0 SP2を使用。
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。
プリンタドライバ	ir3245の同梱CDに内蔵されている専用プリンタドライバーソフトウェアであるPCL5eを使用。
SATA Analyzer ソフトウェア	SATA AnalyzerでキャプチャしたデータをPCで分析するための専用ソフトウェア。
MEAP テストプログラム	MEAP_APIのテストに使用する開発者作成のテストプログラム。テストプログラムが提供するUIからの操作により、製品版のMEAPアプリケーションと同様に、MEAP_APIをコールすることで、TSFの動作を確認することができる。 MEAP_SDKのマニュアル、SMSのマニュアルに従いデジタル複合機本体にインストールして使用する。本テストで使用するテストプログラムは下記のものである。 ・ SC040SimplePDLPrint2.jar ・ SC049CopyJobManage.jar ・ SC029DepartmentManage3.jar

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図2-1に示す。開発者テストは、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。

b.テスト手法

テスト手法としては、利用者が操作可能な外部インタフェースを持つ機能については､開発者の手動操作で機能を実行して動作を観察する方法を用い、利用者が操作可能な外部インタフェースを持たない機能（HDDデータ完全消去機能）については、SATA Analyzerでパケットデータをキャプチャして、解析する方法を用いた。

c.実施テストの範囲

開発者テストは、44項目実施された。

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及び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。また、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、開発者テストと同一の構成である。

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.テスト構成

評価者が実施したテストの構成を図2-1に示す。評価者テストは、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。

b.テスト手法

テスト手法としては、開発者テストのテスト手法と同じく、利用者が操作可能な外部インタフェースを持つ機能については、評価者が手動操作で機能

を実行して動作を観察する方法を用い、利用者が操作可能な外部インタフェースを持たない機能（HDDデータ完全消去機能）については、SATA Analyzerでパケットデータをキャプチャして、解析する方法を用いた。

c.実施テストの範囲

評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを10項目（サンプリング率：約23%）、計15項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① すべてのセキュリティ機能を網羅すること
② 利用者が操作可能なインタフェース（操作パネル、リモートUI、MEAP、ネットワーク）を網羅すること
③ サブシステムを網羅すること
④ 同時操作による影響を確認すること
⑤ パラメタの影響の確認
⑥ 追加された機能（「HDD完全消去機能」の消去モードの変更機能、メモリメディア利用時の「HDD完全消去機能」実行）の確認

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。

2.4 評価結果

評価報告書をもって、評価者は本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。

3 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 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、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た。なお、評価機関による所見報告書の発行は行われなかった。

4 結論

4.1 認証結果

提出された評価報告書、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に対する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記述が理路整然とし一貫してい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、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、

	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完全で、理路整然としていて、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完全で、理路整然としていて、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全で、理路整然としていて、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、実地検査により確認している。
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、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。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
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を含んで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を記述し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主張が正しい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	「キヤノン」の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。
MEAP認証アプ	デジタル複合機の一般利用者の個人認証やActive Directoryとの

リケーション	連携を行うMEAPアプリケーション。
イメージデータ	読み込み、プリント、受信等によってデジタル複合機内に生成された画像データ。
コントローラ	TOEが動作するプラットフォームであり、CPUやメモリ等が実装されるハードウェアである。
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。
操作パネル	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。
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。
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。
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、各種設定等ができるインタフェースである。
Universal Send	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ファイル形式で電子メールアドレスやPCの共有フォルダなどに送信したりする機能（送信機能）である。

6 参照

[1] Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 セキュリティターゲット バージョン 1.01（2008年8月8日）

[2] 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

[3] 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

[4] 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

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[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2.3 2005年8月 CCMB-2005-08-001 (平成17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2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002 (平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-003 (平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 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2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 評価報告書 第3版 2008年12月9日　みずほ情報総研株式会社　情報セキュリティ評価室