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1月23日** (IT**認証**8193)
認証番号	C0186
認証申請者	**キヤノン株式会社**
TOE**の名称**	Canon MFP Security Chip
TOE**のバージョン**	1.50
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	**有限責任中間法人　ITセキュリティセンター 評価部**

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9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 MFP Security Chip バージョン 1.50」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 MFP Security Chip バージョン 1.50」（以下「本TOE」という。）について有限責任中間法人 ITセキュリティセンター 評価部（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 MFP Security Chip
バージョン： 1.50
開発者： キヤノン株式会社

1.2.2 製品概要

TOEはCanon MFP Security Chipであるが、利用者にはTOEを搭載したHDDデータ暗号化キットとして提供される。本TOEにより、キヤノン複合機・プリンタとしての拡張性や汎用性、利便性、パフォーマンスを損ねることなく、キヤノン複合機・プリンタに搭載されたHDDを、盗難による機密情報の暴露から保護することができる。

本TOEはHDDを保護するために、以下のセキュリティ機能を提供する。

- HDDデータ暗号化機能
- 暗号鍵管理機能
- 本体識別認証機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOE の範囲

TOEはCanon MFP Security Chip全体である。その構成を図1-1に示す。

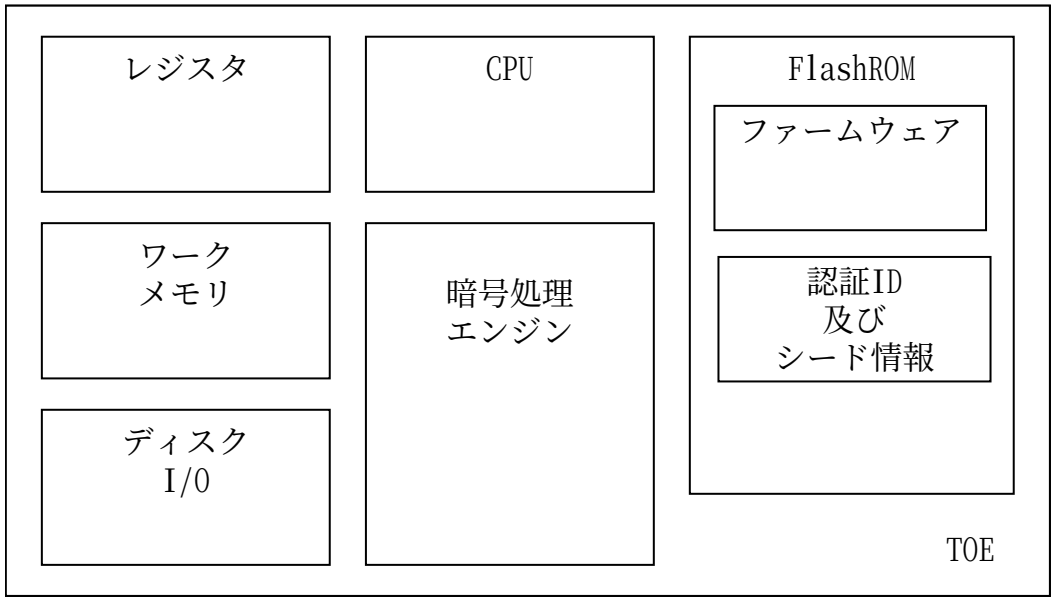

図1-1　TOE物理構成図

TOEを構成する要素の役割は表1-1の通りである。

表1-1　TOE構成要素の役割

名称	役割
レジスタ	プログラム命令や計算結果を一時的に保管する
ワークメモリ	データやプログラムを記憶する揮発性メモリで、暗号鍵が格納される
CPU	メモリに記憶されたプログラムを実行する
Flash ROM	TOEを制御するファームウェアを格納する不揮発性メモリ。認証ID及びシード情報も格納される。
ディスクI/O	TOEに対するI/Oを処理するインタフェース
暗号処理エンジン	データの暗号処理、復号処理を行う

1.2.3.2 TOE の動作概要

図1-2はTOEの論理構成を示した図である。

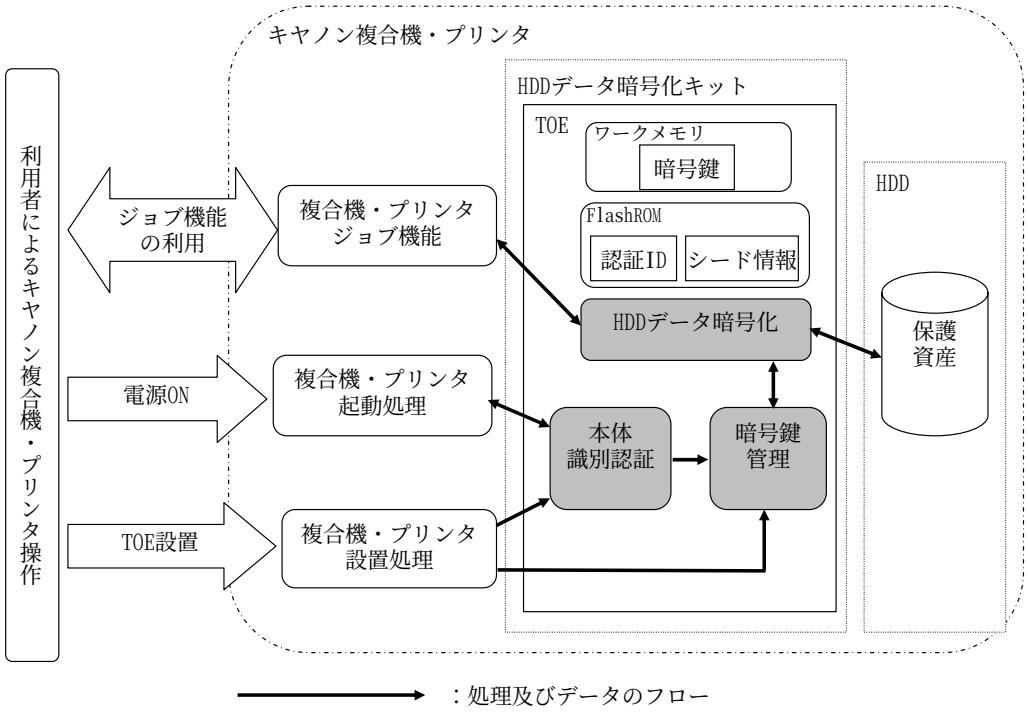

図1-2　TOEの動作概要

図1-2に示すように、利用者はキヤノン複合機・プリンタを操作して、TOEを利用する。

1. 利用者がキヤノン複合機・プリンタにTOEを設置することで、キヤノン複合機・プリンタ設置処理により、キヤノン複合機・プリンタは暗号鍵管理機能で使用するシード情報及び本体識別認証機能にて使用する認証IDをFlashROMに登録する。

   以降、キヤノン複合機・プリンタ設置処理により最初に装着されたキヤノン複合機・プリンタを「登録済み本体デバイス」と称す。なお、認証IDにはHDDデータ暗号化キットが装着されたキヤノン複合機・プリンタを識別できる情報が含まれている。

2. 利用者がキヤノン複合機・プリンタの電源をONにすることで、本体識別認証機能により、使用しているキヤノン複合機・プリンタが「登録済み本体デバイス」であることを確認する。

   「登録済み本体デバイス」であることが確認できた場合、TOEは暗号鍵管理機能により、HDDデータ暗号化機能で使用する暗号鍵をワークメモリに生成する。

3. 利用者がキヤノン複合機・プリンタのコピー、プリンタ等のジョブ機能を利用することで、HDDデータ暗号化機能により、HDDに対して書き込むデータ、HDDから読み出すデータを暗号化／復号する。

1.2.4 TOEの機能

TOEは以下の機能を持つ。

- TOEが最初に装着されたキヤノン複合機・プリンタでのみTOEが動作するように制限する。
- HDDへの書き込みの指示を受け、入力されたデータを暗号化し、暗号化されたデータをHDDへ書き込む。
- HDDからの読み出しの指示を受け、HDDからデータを読み出し、そのデータを復号化して出力する。

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 MFP Security Chip　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、「キヤノン株式会社 Canon MFP Security Chip 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、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20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

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。

TOEが利用される環境での攻撃者の攻撃能力を低レベルと定義しているため、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、次の暗号操作を行う。
  - HDDへ書き込まれるデータを暗号化する
  - HDDから読み出されるデータを復号する

  暗号操作に用いる暗号鍵、暗号アルゴリズムは以下のとおり。
  - 鍵長が「256ビット」の暗号鍵
  - FIPS PUB 197に従った「AESアルゴリズム」

- 暗号鍵管理機能
  TOEは、次の仕様に基づき、HDDデータ暗号化機能で使用する暗号鍵を生成する。
  - 暗号鍵を生成するアルゴリズムは、「FIPS186-2に基づく暗号鍵生成アルゴリズム」
  - 生成される暗号鍵の鍵長は「256ビット」

暗号鍵の管理は以下のように行う。

- 起動時に、TOEはFlashROMに格納されたシード情報を読み出して暗号鍵を再生成する
- TOEは暗号鍵を生成した後、ワークメモリに格納する

なお、シード情報が格納されるFlashROMはTOE外部から読み出すことが不可能である。また、暗号鍵は揮発性メモリであるワークメモリに存在するため、電源断により消失する。

- 本体識別認証機能

TOEは、起動時に「登録済み本体デバイス」に接続されていることを、認証IDを用いて確認する。なお、登録済み本体デバイスを認証するために用いられる認証メカニズムに関する認証データの再使用を防止するために、チャレンジ&レスポンス認証を採用し、TOEの起動の度に、新規のチャレンジ用の擬似乱数を生成する。

【認証IDの登録】

TOEは、HDDデータ暗号化キット取り付け時に、キヤノン複合機・プリンタから認証IDを受取り、FlashROMに保存する。

【識別認証の手順】

TOEは起動時に擬似乱数を生成し、チャレンジ用の乱数としてキヤノン複合機・プリンタへ渡す。キヤノン複合機・プリンタは、認証IDとチャレンジ用の乱数から計算された値をレスポンスとしてTOEへ渡す。TOEは、同様の計算を行い、レスポンスの検証を行う。

TOEが「登録済み本体デバイス」に取り付けられていることが確認できない場合、HDDへのアクセスを禁止する。

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 想定する脅威

識別子	脅 威
T.HDD_ACCESS	悪意のある者がHDDを取り外し、ディスク解析ツールもしくは他のキヤノン複合機・プリンタを利用してHDDに直接アクセスすることにより、HDD上のデータを暴露するかもしれない。
T.WRONG_BOARD	悪意のある者がHDDデータ暗号化キットとHDDを「登録済み本体デバイス」以外に装着し、HDDデータ暗号化キットを介したHDDアクセスを行うことにより、HDD上のデータを暴露するかもしれない。 (以下の補足参照のこと)

脅威T.WRONG_BOARDに関する補足

脅威T.WRONG_BOARDに対抗するためには、本TOEがキヤノン複合機・プリンタの個々の機体を識別できなければならない。そのためには、本TOEに対応したキヤノン複合機・プリンタは、個々の機体ごとに異なる「認証ID」を持たなければならない。

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

TOEは、HDDデータ暗号化キットに搭載されて動作する。HDDデータ暗号化キットは、HDDデータ暗号化キットBシリーズに対応したキヤノン複合機・プリンタに装着されて動作する。装着可能なHDDデータ暗号化キットは、キヤノン複合機・プリンタの対応オプションのリスト（キヤノン複合機・プリンタの機種ごとに装着可能なオプション製品が記載されているリスト）によって識別される。

TOE が搭載されたHDDデータ暗号化キットBシリーズは、図1-3のように、キヤノン複合機･プリンタの中のマザーボードとHDDの間の通信がそれを介して行われるように装着される。マザーボードには、TOEがキヤノン複合機･プリンタを識別･認証するために必要なロジックを提供するFlashボードが装着される。

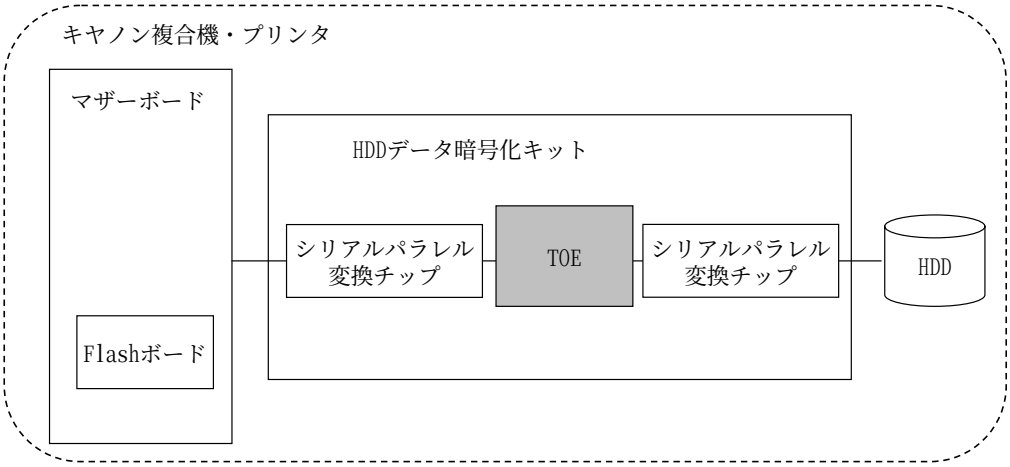

図1-3　TOE、HDDデータ暗号化キット、キヤノン複合機・プリンタの構成

なお、TOEとHDDデータ暗号化キットBシリーズの間のインタフェースはパラレルATAであり、HDDデータ暗号化キットBシリーズとキヤノン複合機・プリンタ及びHDDの間のインタフェースはシリアルATAとなる。

利用者は、対応オプションのリストを参照することで、キヤノン複合機・プリンタの各機種に対して、HDDデータ暗号化キットBシリーズへの対応有無、及び、装着可能なHDDデータ暗号化キットを識別することができる。なお、HDDデータ暗号化キットBシリーズに対応していないキヤノン複合機・プリンタでは、HDDデータ暗号化キットは動作しない。

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必要な前提条件はない。

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 Encryption Kit-B Series Installation Procedure　HDDデータ暗号化キット・Bシリーズ 設置手順書（英日合冊）（FT1-0218-000）
- HDDデータ暗号化キット・Bシリーズ ユーザーズガイド（FT5-1905-000）
- HDD Data Encryption Kit-B Series　Reference Guide（USRM1-3593-00）
- 注意書き (FT5-1904-000)
- Caution (FT5-1906-000)

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1月に始まり、平成20年9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3月、4月及び7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・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3月及び7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。

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と図2-2に示す。

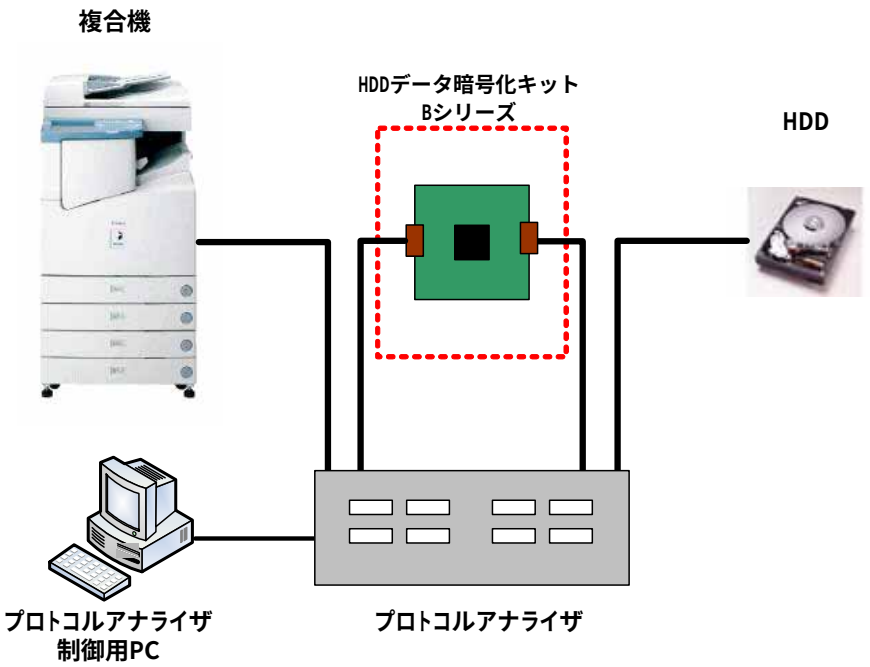

図2-1　開発者テストの構成図(複合機レベルテスト)

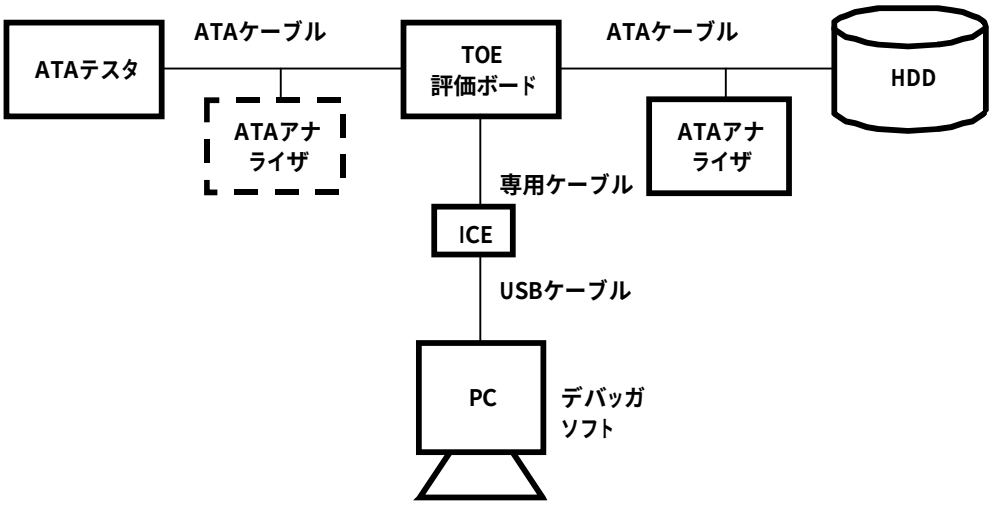

図2-2　開発者テストの構成図(ファームウェアレベルテスト)

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と図2-2に示す。図2-1はSTにおいて識別されているTOE構成と同一のTOEテスト環境である。図2-2における

TOEの動作は、STにおいて識別されているTOE構成の場合のTOEの動作と一貫することが評価者により確認されている。

b.テスト手法

テストには、以下の手法が使用された。

①複合機レベルテストにおいて、人間の利用者として想定される通常の操作と観察を行う。

②複合機レベルテストにおいて、テスト用中継ボードを介して、プロトコルアナライザによりインタフェース信号を確認する。

③ファームウェアレベルテストにおいて、ATAテスタを模擬ホストとしてTOEに対し直接コマンドやデータを送信する。また、ICEを使って、TOEの内部メモリの情報を読み書きし、ATAアナライザを使ってATAのインタフェース信号を確認する。

c.実施テストの範囲

テストは開発者によって90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、開発者テストと同様の構成である。

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と図2-2に示す。評価者テストは開発者テストと同等のTOEテスト環境で実施されている。

b.テスト手法

テストには、開発者テストと同様の手法が使用された。

c.実施テストの範囲

評価者が独自に考案したテストを12項目、開発者テストのサンプリングによるテストを28項目、計40項目のテストを実施した。

評価者は、以下を考慮してテストを独自に考案した。

① 重要なセキュリティ機能(HDDデータ暗号化機能、暗号鍵管理機能、本体識別認証機能)に関して、開発者テストを補足すること

② すべてのセキュリティ機能を対象とすること

評価者は、以下を考慮して開発者テストのサンプリングを行った。

① 全てのセキュリティ機能に対して、通常使用する操作と悪意のあるものが実施すると想定される操作を含めること

② 全てのTSFIを刺激するテストを含めること

また、評価者は、潜在的脆弱性、異常系、想定外操作、メンテナンスモードの使用の観点から6項目の侵入テストを考案し、実施した。

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 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、ST及び評価報告書において、所見報告書及び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。

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実現に必要なIT環境としてのハードウェア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。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

読者は、TOEが対抗する脅威T.WRONG_BOARDについて、補足を理解すること。詳細は「1.5.5 脅威」参照。

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。

ATAテスタ	HDD の標準インタフェースであるATA に準拠したコマンドやデータの送受信等をするツール。
ATAアナライザ	ATA ケーブル間に接続してATA インタフェースの信号を確認するためのツール。
HDD	本報告書の記述では、特に断りのない限りキヤノン複合機・プリンタに搭載されるハードディスクを指す。
HDDデータ暗号化キット	セキュリティ強化を目的とし、セキュリティチップが搭載された基板。キヤノン複合機・プリンタ及びHDDへの物理的なインタフェースを持つ。また、本基板上には、シリアルATAとパラレルATAを変換するチップが搭載される。

HDDデータ暗号化キットBシリーズ	HDDデータ暗号化キットのうち、搭載されたセキュリティチップがTOEである基板の総称とする。HDDデータ暗号化キットBシリーズ内の各HDDデータ暗号化キットの違いは、製品名称や各々対応する複合機・プリンタとの接続形態に合わせた物理的な基板形状のみであり、機能やセキュリティチップに違いはない。 本報告書の記述で「HDDデータ暗号化キット」との表記は、「HDDデータ暗号化キットBシリーズ」を指す。 HDDデータ暗号化キットBシリーズには、以下の製品が含まれる。 和名 : HDDデータ暗号化キット・Bシリーズ 英名 : HDD Data Encryption Kit-B Series 仏名 : Kit d'encryptage des données disque dur-Série B
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。
キヤノン複合機・プリンタ	キヤノン製複合機、キヤノン製プリンタの総称。
シリアルATA	記憶装置を接続する規格の一つであり、転送方式にシリアル転送を用いている。従来から使用されているパラレルATAに比べて、転送速度が高速である。
対応オプションのリスト	キヤノン複合機・プリンタの各機種に対して、HDDデータ暗号化キットBシリーズの対応有無、及び、装着可能なHDDデータ暗号化キットが記載されたリスト。 消費者には、キヤノン複合機・プリンタの販売用の製品カタログの位置づけで配布される。
ディスク解析ツール	HDDのセクタ内容を参照できるツールの総称。
パラレルATA	記憶装置を接続する規格の一つであり、転送方式にパラレル転送を用いている。
プロトコルアナライザ	Host(本報告書ではキヤノン複合機・プリンタを指す)とTOE間、TOEとHDD間に取り付けて、インタフェースを流れるデータを収集するツール。

6 参照

[1] Canon MFP Security Chip セキュリティターゲット バージョン1.06（2008年4月7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] キヤノン株式会社 Canon MFP Security Chip 評価報告書 第3.7版 (2008年9月19日) 有限責任中間法人 ITセキュリティセンター 評価部