認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成27年2月20日 (IT認証5534)
認証番号	C0506
認証申請者	キヤノン株式会社
TOEの名称	HDDデータ暗号化キット Eシリーズ
TOEのバージョン	2.10
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	一般社団法人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28年4月25日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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 バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「HDDデータ暗号化キット Eシリーズ」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、キヤノン株式会社が開発した「HDD データ暗号化キット E シリーズ」（以下「本 TOE」という。）について一般社団法人 IT セキュリティセンター 評価部（以下「評価機関」という。）が平成 28 年 4 月 13 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者であるキヤノン株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者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 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、キヤノン複合機・プリンタに搭載された HDD に保存するデータを暗号化するための、オプションのハードウェア製品である。

本 TOE は、HDD に保存するデータの暗号化機能と、その暗号化機能のテスト機能を提供する。

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である。

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。

本 TOE を装着するキヤノン複合機・プリンタは、管理者が HDD を取り外し可能である。そのため、取り外された HDD からデータが不正に読み出される脅威がある。

本 TOE は、取り外された HDD からデータが不正に読み出されることを防止するために、暗号化機能とそれを補助するセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、以下のキヤノン複合機・プリンタに装着して利用する。

・imagePRESS C10000VP, imagePRESS C8000VP
・imagePRESS C65, imagePRESS C650

本 TOE を搭載したキヤノン複合機・プリンタは、物理的な不正アクセスができないように、管理された環境に設置されることを想定している。

1.1.3 免責事項

本 TOE が提供する以下の機能は、本評価による保証の対象外である。

・TOE が設置時に登録されたキヤノン複合機・プリンタを識別認証する機能

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 4 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	HDDデータ暗号化キット Eシリーズ
バージョン：	2.10
開発者：	キヤノン株式会社

HDD データ暗号化キット E シリーズには、次の 2 つの製品がある。2 つの製品は、名称が異なるだけで構成品は同じである。

・「HDD データ暗号化／ミラーリングキット・E1」
本製品は、imagePRESS C10000VP, imagePRESS C8000VP 用である。

・「HDD データ暗号化／ミラーリングキット・E2」
本製品は、imagePRESS C65, imagePRESS C650 用である。

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

(1) TOE 名称

製品のパッケージ外装に印字された名称が、以下のとおりであることを確認する。なお、「HDD データ暗号化／ミラーリングキット・E1」は、国内向けと海外向けで共通である。

・「HDD データ暗号化／ミラーリングキット・E1」の場合

HDD データ暗号化／ミラーリングキット・E1
HDD Data Encryption & Mirroring Kit-E1
Kit d'encryptage et d'écriture du disque dur-E1

・「HDD データ暗号化／ミラーリングキット・E2」（国内向け）の場合

HDD データ暗号化／ミラーリングキット・E2

・「HDD データ暗号化／ミラーリングキット・E2」（海外向け）の場合

HDD Data Encryption & Mirroring Kit-E2
Kit d'encryptage et d'écriture du disque dur-E2

(2) バージョン

TOE のガイダンスの記載に従って TOE を装着したキヤノン複合機・プリンタの操作パネルにバージョン情報を表示させて、「Canon MFP Security Chip」が「2.10」であることを確認する。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、キヤノン複合機・プリンタから取り外された HDD から、データが不正に読み出されることを防止するために、HDD に格納するデータを暗号化する機能を提供する。

また、TOE は、暗号化機能を補助するために、推測の困難な暗号鍵を生成する機能と、暗号化機能が正常に動作していることを確認する自己テスト機能を提供する。

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。

表3-1 想定する脅威

識別子	脅威
T.HDD_ACCESS	HDDは取り外し可能な構成であるため、キヤノン複合機・プリンタから取り外されたHDDを攻撃者が不正に入手し、ディスク解析ツールを利用して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。

（補足）

4 章の前提条件により、攻撃者は HDD を取り外すことはできない。しかし、管理者が取り外した HDD は前提条件の対象外であり、上記の脅威が存在する。

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。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 脅威「T.HDD_ACCESS」への対抗

TOE は、「HDD データ暗号化機能」と「暗号鍵管理機能」で本脅威に対抗する。

TOE の「HDD データ暗号化機能」は、HDD への書き込みデータを暗号化し、HDD から読み出すデータを復号する。暗号アルゴリズムは、128bit または 256bit の AES である。

TOE の「暗号鍵管理機能」は、SP800-90A[14] の Hash_DRBG に準拠した乱数生成アルゴリズムを使用して、暗号鍵を生成する。

それらの機能により、TOE は、HDD への書き込みデータを、乱数性の確保された暗号鍵を使用して暗号化することで、HDD からデータが暴露されることを防止する。

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。

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.TSF_VERIFICATION	HDDデータ暗号化機能の故障や暗号鍵の破損を検出するために、それらの自己テストを実施しなければならない。

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。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 組織のセキュリティ方針「P.TSF_VERIFICATION」への対応

TOE は、「自己テスト機能」で本方針を満足する。

TOE の「自己テスト機能」は、「HDD データ暗号化機能」と「暗号鍵管理機能」で使用する暗号アルゴリズムについて、既知解テストを行う。さらに、TOE 内のソフトウェアコードと暗号鍵生成に使用される鍵シード情報の完全性を検証する。

それらの機能により、TOE は、HDD データ暗号化機能の故障や暗号鍵の破損を検出する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件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.PHYSICAL_ACCESS_MANAGED	TOEを搭載したキヤノン複合機・プリンタは、悪意を持つ者によるTOEへの物理的なアクセスを制限できる、管理された環境に設置されるものとする。

4.2 運用環境と構成

本 TOE は、キヤノン複合機・プリンタのオプション製品であり、キヤノン複合機・プリンタに装着して利用する。

本 TOE を搭載したキヤノン複合機・プリンタ内部の概要を図 4-1 に示す。

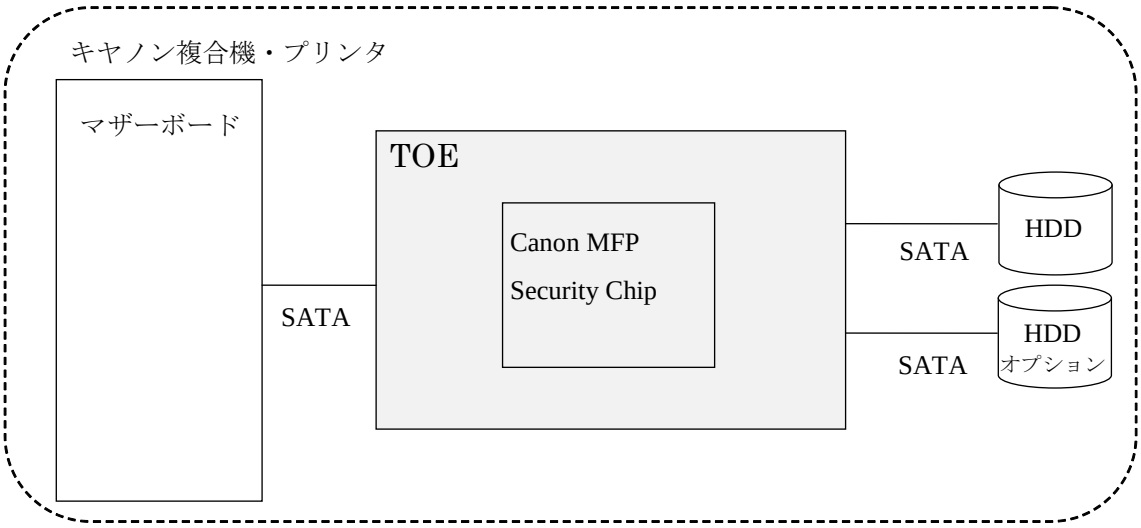

図4-1 TOEの運用環境

図 4-1 で中央が TOE である。TOE は、セキュリティ機能を実現する Canon MFP Security Chip を搭載した基板と、その装着に必要なケーブル類で構成される。TOE は、キヤノン複合機・プリンタの内部で、マザーボードと HDD の間に、SATA インタフェースで接続される。

TOE の運用環境は以下のとおりである。

(1) キヤノン複合機・プリンタ

本 TOE を使用可能なキヤノン複合機・プリンタは、以下の機種である。ただし、機種によって対応している暗号鍵長が異なる。

・暗号鍵長 128bit 対応機種
imagePRESS C10000VP, imagePRESS C8000VP

・暗号鍵長 256bit 対応機種
imagePRESS C65, imagePRESS C650

(2) HDD

本 TOE は、ミラーリング機能を提供しており、HDD を 2 台接続可能である。ただし、ミラーリング機能の使用は必須ではなく、HDD 1 台でも運用可能である。

なお、本構成に示されているキヤノン複合機・プリンタの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

暗号鍵長の 128 bit と 256 bit のどちらを使用するかは、キヤノン複合機・プリンタの機種によって一意に決められており、利用者は変更できない。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE を搭載したキヤノン複合機・プリンタの構成を図 5-1 に示す。

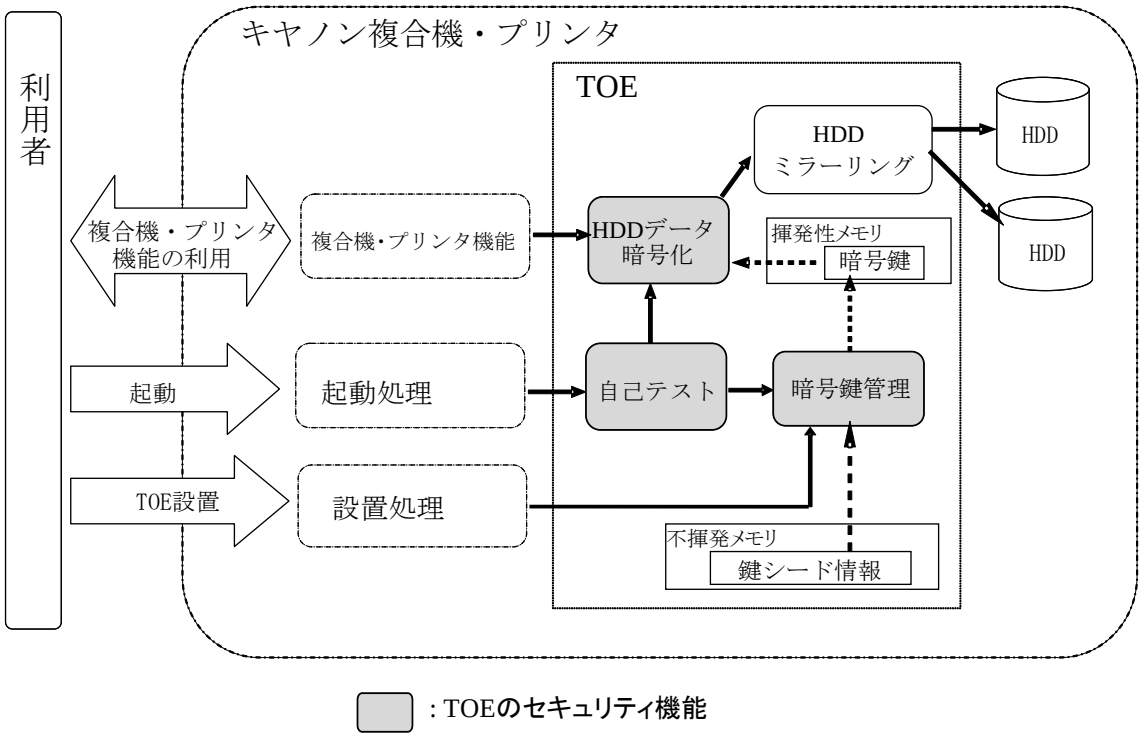

図5-1　TOE境界

TOE は、セキュリティ機能である「HDD データ暗号化機能」「暗号鍵管理機能」「自己テスト機能」と、一般機能である「HDD ミラーリング機能」で構成されており、利用者がキヤノン複合機・プリンタを操作することで自動的に動作する。

TOE のセキュリティ機能について説明する。

(1) HDD データ暗号化機能

本機能は、HDD へ書き込まれるデータを暗号化し、HDD から読み出されるデータを復号する機能である。暗号アルゴリズムは、128bit または 256bit の AES である。

(2) 暗号鍵管理機能

本機能は、HDD データ暗号化機能で使用する暗号鍵を生成する機能である。暗号鍵の生成には、SP800-90A の Hash_DRBG に準拠した乱数生成アルゴリズムを使用する。使用しているハッシュ関数は SHA-256 である。

TOE は、TOE の設置時に、キヤノン複合機・プリンタから指定された情報と、HDD のアクセス時間のばらつきを利用して、鍵シード情報を生成し保存する。

その後、TOE は、鍵シード情報から暗号鍵を生成する。生成された暗号鍵は揮発性メモリに置かれ、電源 OFF で消失する。次の電源 ON の時に、TOE は保存された鍵シード情報から同じ暗号鍵を生成する。

(3) 自己テスト機能

本機能は、TOE の起動時に以下の自己テストを行う機能である。

・TOE 内のファームウェアと鍵シード情報の CRC の検証
・既知解テスト（AES、Hash_DRBG、SHA-256 の各アルゴリズム）

TOE の起動処理は以下の場合に実行され、自己テストでエラーが発生した場合には動作を停止する。

・電源 ON 時（キヤノン複合機・プリンタは介在しない）
・キヤノン複合機・プリンタによるリセットコマンド発行時

5.2 IT環境

本 TOE はキヤノン複合機・プリンタに搭載されて動作する。

キヤノン複合機・プリンタは、TOE に対して以下の動作を行う。

・TOE の設置時に、暗号鍵長と鍵シード生成に使用される情報を TOE に指示
・キヤノン複合機・プリンタの起動処理中に、TOE にリセットコマンドを発行
・利用者の利用に伴い、TOE を介して HDD への読み書きを実施

キヤノン複合機・プリンタは上記の動作を自動的に実行し、利用者は TOE のための特別な設定や操作をする必要はない。

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。

(1)「HDD データ暗号化／ミラーリングキット・E1」の場合

表 6-1 のすべてのガイダンスが添付される。

表 6-1　ガイダンス一覧

項番	名称	バージョン
1	HDD Data Encryption & Mirroring Kit-E Series Installation Procedure HDD データ暗号化/ ミラーリングキット・E シリーズ設置手順書	FT2-0299(010)
2	HDD データ暗号化キット ユーザーズガイド	FT6-1331(010)
3	HDD ミラーリングキット ユーザーズガイド	FT6-1335(000)
4	本製品のご利用を開始する前にかならずお読みください	FT6-1332(000)
5	HDD Data Encryption & Mirroring Kit-E Series User Documentation	FT6-1333(010)
6	Make sure to read this notice before using this product.	FT6-1334(000)

(2)「HDD データ暗号化／ミラーリングキット・E2」（国内向け）の場合

表 6-1 の項番 1, 2, 3, 4 のガイダンスが添付される。

(3) 「HDD データ暗号化／ミラーリングキット・E2」（海外向け）の場合

表 6-1 の項番 1, 5, 6 のガイダンスが添付される。

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した一般社団法人 IT セキュリティセンター 評価部は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 27 年 2 月に始まり、平成 28 年 4 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 27 年 6 月、7 月、8 月、9 月、平成 28 年 2 月及び 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 27 年 6 月、9 月及び平成 28 年 2 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者は、キヤノン複合機・プリンタを使用せずに本 TOE の動作を詳細に確認するテスト（これを「ファームウェアレベルテスト」という。）と、キヤノン複合機・プリンタを使用して本 TOE の運用環境の動作を確認するテスト（これを「複合機レベルテスト」という。）の 2 種類のテストを実施している。

開発者が実施したテストの構成を図 7-1 と図 7-2 に示す。また、その構成要素を表 7-1 と表 7-2 に示す。

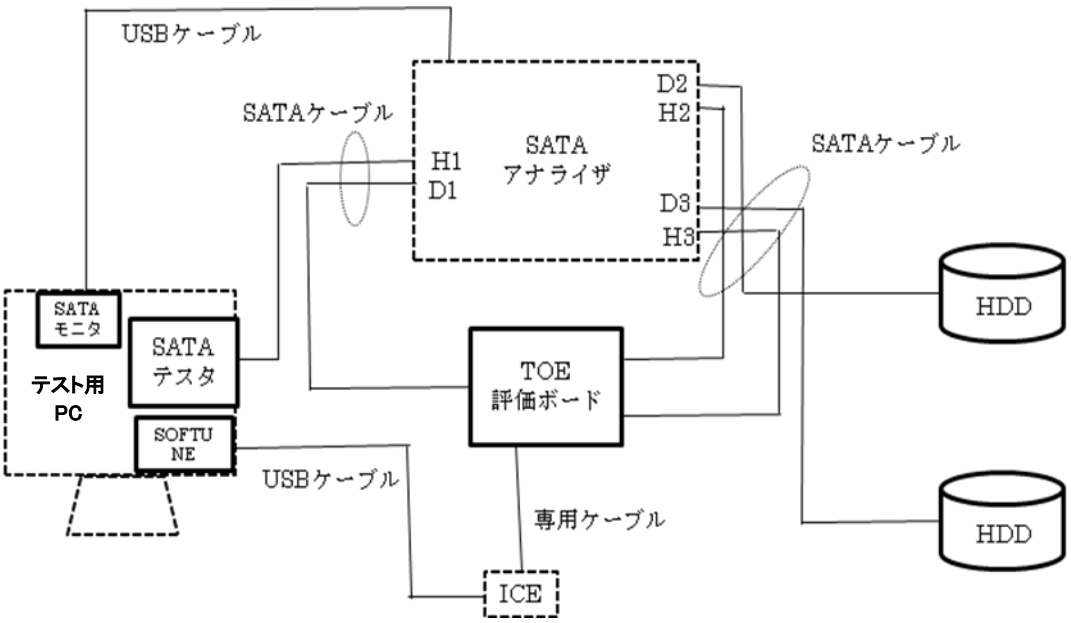

図 7-1　開発者テストの構成図（ファームウェアレベルテスト）

表7-1　開発者テストの構成要素（ファームウェアレベルテスト）

名称		詳細
TOE評価ボード		TOEの代わりに使用。以下の違いを除きTOEと同じ。 ・Canon MFP Security Chipを物理的に保護する覆いがない ・ICE接続用コネクタが存在
テスト用PC		キヤノン複合機・プリンタの代わりにTOEにSATAコマンドを発行したり、SATAアナライザやICEを操作したりするために使用 ・Windows 7 Professional SP1搭載PC ※以下のソフトウェアを搭載。
	SATAテスタ	指定されたスクリプトに従って、SATAコマンドの送受信を行う。 ・東陽テクニカDriveMaster2012Pro
	SATAモニタ	SATAアナライザを制御して、SATAインタフェースのデータを表示する。 ・LeCroy SATA Protocol Suite Software version 4.20
	デバッガ (SOFTUNE)	ICEを制御して、TOEのファームウェアのデバッグを行う。 ・富士通FR統合開発環境 Softune Workbench V60L08
SATAアナライザ		テスト用PCとTOE評価ボードの間、及び、TOE評価ボードとHDDの間のSATAインタフェースのデータを取得する。 ・Catalyst STX-431
ICE		富士通FR用ICE MB2198
HDD		Western Digital WD30EZRX（各種テストで使用） Western Digital WD10EURX（乱数のエントロピー測定で使用）

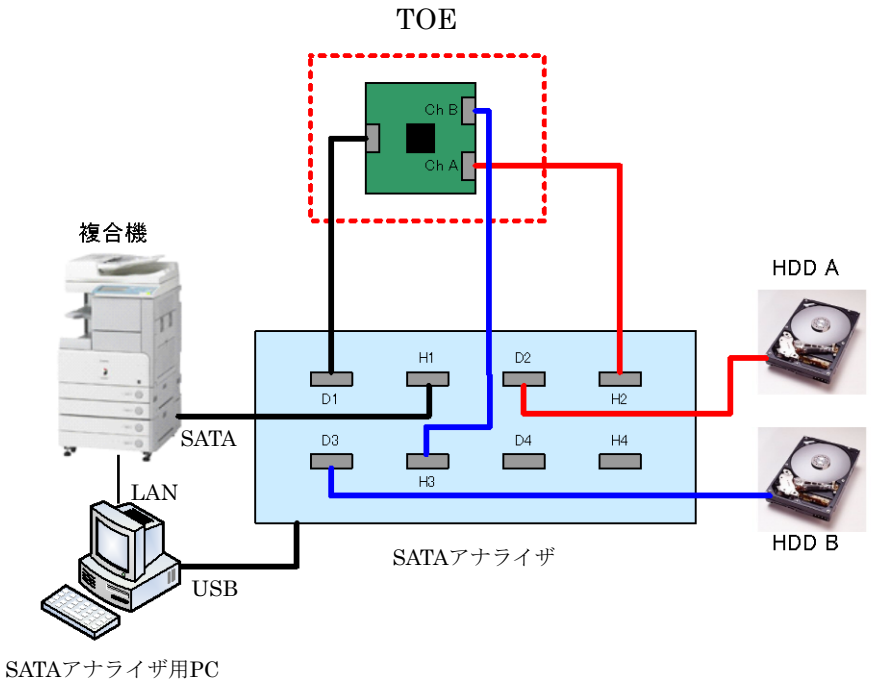

図7-2　開発者テストの構成図（複合機レベルテスト）

表7-2　開発者テストの構成要素（複合機レベルテスト）

名称	詳細
TOE	・HDDデータ暗号化／ミラーリングキット・E1, バージョン2.10 ・HDDデータ暗号化／ミラーリングキット・E2, バージョン2.10 ※ただし、自己テストが失敗する場合のテストでは、表7-1のTOE評価ボードにテスト用に変更したファームウェアを搭載して使用。
複合機 HDD A HDD B	TOEを搭載する複合機。以下の2機種を使用。 a) imagePRESS C10000VP, バージョン 10.02 ・必須オプションのimagePRESS Server B5000装着 ・HDD A(標準搭載)：Western Digital WD2500HHTZ ・HDD B(オプション)：Western Digital WD2500HHTZ b) imagePRESS C650, バージョン 30.52 ・HDD A(標準搭載)：Western Digital WD10EURX ・HDD B(オプション)：Western Digital WD10EURX

SATAアナライザ		複合機とTOEの間、及び、TOEとHDDの間のSATAインタフェースのデータを取得する。 ・Catalyst STX-431
SATAアナライザ用PC		SATAアナライザの操作（USB経由）と、複合機のインストール（LAN経由）に使用。 ・Windows 7 Professional SP1搭載PC ※以下のソフトウェアを搭載。
	SATAモニタ	SATAアナライザを制御して、SATAインタフェースのデータを表示する。 ・LeCroy SATA Protocol Suite Software version 4.00
	保守用ツール	暗号化対象のHDDに、複合機用のソフトウェアやデータをインストールするために使用する。 ・SST version 4.72J

ファームウェアレベルテスト及び一部の複合機レベルテストでは、TOE の代わりに TOE 評価ボードが使用されている。評価者は、TOE と TOE 評価ボードの違いは物理的な覆いやコネクタの有無だけであり、開発者のテストで問題はないと判断している。また、評価者は、ICE や SATA アナライザの追加は、テストに影響を与えないと判断している。

開発者がテストしたキヤノン複合機・プリンタは、TOE の動作対象機種の内、imagePRESS C10000VP と imagePRESS C650 のみである。評価者は、他の機種は、開発者がテストした機種と同一のソフトウェアを搭載しているため、開発者のテストで十分であると判断している。

したがって、開発者テストは、本 ST において識別されている TOE 構成と同じ TOE テスト環境で実施されているとみなすことができる。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

① TOEが提供している外部インタフェースで確認可能なふるまい

TOE の外部インタフェースについて、テスト用 PC や複合機を操作して入力を行い、その応答や複合機の動作を確認する。また、SATA モニタを使用して、SATA インタフェースのデータを確認する。

② TOE が提供している外部インタフェースでは確認できないふるまい

TOE が提供しているインタフェースでは確認できない TOE 内部のデータについては、デバッガを使用して確認する。

また、自己テストや暗号アルゴリズムについては、以下のように、当該モジュールのテスト用に変更したファームウェアを使用して確認する。

- 自己テストは、自己テストが必ず失敗するように変更したファームウェアを使用して、①の場合と同じ手法で確認する。
- 各種暗号アルゴリズムは、当該モジュールへの入出力を SATA インタフェースの拡張コマンドで実行できるように変更したファームウェアを使用して、SATA テスタを用いて実行結果を取得する。取得したデータを、既知解と比較したり、分析したりすることで、仕様どおりの暗号アルゴリズムが実装されていることを確認する。

＜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 7-3 に示す。

表7-3　開発テストツール

ツール名称	概要・利用目的
SATAモニタ＋SATAアナライザ ※表7-1と表7-2参照	テスト用PCや複合機とTOEの間、TOEとHDDの間のSATAインタフェースのデータを表示する。
SATAテスタ ※表7-1参照	指定されたスクリプトに従って、SATAコマンドの送受信を行う。
デバッガ＋ICE ※表7-1参照	TOEの処理にブレークポイントを設定し、処理途中のデータを表示する。
開発者テスト用ファームウェア	開発者のテスト用に変更したファームウェア。テスト対象のモジュールはTOEと同じである。 ・自己テスト確認用（7種類） ・暗号アルゴリズム確認用（3種類） ・乱数のエントロピー測定用（1種類）

＜開発者テストの実施内容＞

TOE に対して様々な入力を行い、セキュリティ機能が仕様どおりに動作することを確認した。

暗号アルゴリズム AES、Hash_DRBG、SHA-256 について、既知解と一致することを確認した。また、鍵シード情報の生成に使用される情報のエントロピーの測定を行い、SP800-90A の要求を満足することを確認した。

b) **開発者テストの実施範囲**

開発者テストは開発者によって、ファームウェアレベルテストは206項目、複合機レベルテストは7項目実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証された。深さ分析によって、TOE設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証された。

c) **結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、前述の開発者テストの構成と同じである。独立テストは、本 ST において識別されている TOE の構成と同じ環境で実施されたとみなすことができる。

なお、独立テスト環境の構成品やテストツールは、開発者テストに用いられたものを利用しているが、それらの妥当性確認及び動作試験は、評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) **独立テストの観点**

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① 開発者とは異なる入力のバリエーションや組合せを確認する。

② 開発者がテストしていないふるまいや構成を確認する。

③ サンプリングテストでは、以下の観点で開発者テストの項目を抽出する。

・セキュリティ機能に関係するインタフェースを確認する。
・テスト手法の異なるテストを確認する。

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である。

＜独立テスト手法＞

独立テストは、開発者テストと同じテスト手法で実施された。

＜独立テストツール＞

独立テストツールは､開発者テストと同じツールに､独立テスト用のツールを追加した。独立テストで追加したツールを表 7-4 に示す。

表7-4 独立テストで追加したツール

ツール名称	概要・利用目的
独立テスト用ファームウェア	独立テスト用に変更したファームウェア｡テスト対象のモジュールはTOEと同じである。 ・自己テスト確認用（4種類） ・暗号アルゴリズム確認用（3種類）

＜独立テストの実施内容＞

評価者は、独立テストの観点に基づいて、21 項目のサンプリングテスト（ファームウェアレベル 19 項目、複合機レベル 2 項目）と、19 項目の追加の独立テスト（ファームウェアレベル 14 項目、複合機レベル 5 項目）を実施した。

独立テストの観点とそれに対応した主なテスト内容を表 7-5 に示す。

表7-5 実施した主な独立テスト

観点	テスト概要
観点① （ファームウェアレベル）	・開発者と異なる箇所を変更したファームウェアを用いて、自己テスト機能が仕様どおりに動作することを確認する。 ・各種暗号アルゴリズムについて、開発者が確認していない既知解を確認する。 ・複合機の使用を想定して、複数のSATAコマンドを組み合わせて実行し、一連の動作を確認する。
観点① （複合機レベル）	・開発者が電源ONの操作で確認した暗号鍵生成のテストを、複合機のスリープからの復帰操作で確認する。
観点② （ファームウェアレベル）	・自己テスト失敗後は、HDDへの書き込みがエラーとなり、HDDへの書き込みができないことを確認する。
観点② （複合機レベル）	・開発者がHDDのミラーリング構成で実施したテストを、シングル構成で確認する。 ・ミラーリング設定のために2つのHDD間でデータをコピーしている間に、複合機からHDDの読み書きを行い、暗号化機能が正常に動作することを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① キヤノン複合機･プリンタの管理者及び保守用のインタフェースを使用して、暗号化機能を無効化される懸念がある。

なお、暗号鍵については、暗号鍵の生成メカニズムとその開発者テスト及び評価者独立テストの分析から、前提条件を満足する運用環境において、想定している攻撃者の攻撃能力では､暗号鍵や鍵シード情報の入手や推測ができないことが評価されている。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは、独立テストと同じ環境で実施した。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-6 に示す。

表7-6　侵入テスト概要

脆弱性	テスト概要
脆弱性①	複合機で、管理者用のメニュー及び保守用の操作モードを調査し、保守用の操作モードにミラーリングの有効・無効の操作が存在するだけで、それ以外にTOEに関する操作が存在しないことを確認した。

c) **結果**

評価者が実施した侵入テストでは､想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5 評価構成について

本 TOE は、動作対象のキヤノン複合機・プリンタに装着することで動作し、それ以外に設定値等の構成条件はない。

7.6 評価結果

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

評価では以下について確認された。

セキュリティ機能要件：　コモンクライテリア　パート２　適合
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

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

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

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法が CEM に適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL3 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 TOE は暗号鍵長 128bit と 256bit の両方に対応している。しかし、どちらの暗号鍵長を使用するかは、TOE を装着するキヤノン複合機・プリンタによって一意に決められており、暗号鍵長の変更はできない。本 TOE に関心のある調達者は、購入前に、利用可能な暗号鍵長の確認が必要である。

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。

HDD データ暗号化キット E シリーズ　セキュリティターゲット, バージョン 1.18, 2016 年 4 月 8 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。

ICE	In-Circuit Emulator（インサーキットエミュレータ）
SATA	Serial ATA（シリアルATA）

本報告書で使用された用語の定義を以下に示す。

Canon MFP Security Chip	TOEのセキュリティ機能を実現するASIC

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] HDDデータ暗号化キット Eシリーズ セキュリティターゲット, バージョン 1.18, 2016年4月8日, キヤノン株式会社

[13] CANON HDDデータ暗号化キット Eシリーズ評価報告書, 第1.23版, 2016年4月13日, 一般社団法人ITセキュリティセンター 評価部

[14] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, National Institute of Standards and Technology