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

Version 1.20
2016/11/28

キヤノン株式会社

目 次

1 ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、表記規則、用語・略語、TOE 記述、TOE 範囲及び保護対象となる資産について記述する。

1.1 ST 参照

本節ではセキュリティターゲットの識別情報を記述する。

ST 名称: 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: 1.20
発行者: キヤノン株式会社
発行日: 2016/11/28

1.2 TOE 参照

本節では TOE の識別情報を記述する。

TOE 名称: HDD データ暗号化キット E シリーズ
バージョン: 2.11
作成者: キヤノン株式会社

尚、本 TOE は以下のいずれかの製品名で識別することができる。
名称: ＨＤＤデータ暗号化／ミラーリングキット・E1
※英名: HDD Data Encryption & Mirroring Kit-E1
仏名: Kit d'encryptage et d'écriture du disque dur-E1
名称: ＨＤＤデータ暗号化／ミラーリングキット・E2
※英名: HDD Data Encryption & Mirroring Kit-E2
仏名: Kit d'encryptage et d'écriture du disque dur-E2

1.3 表記規則、略語・用語

1.3.1 表記規則

第 3 章の組織のセキュリティ方針、前提条件、及び第 4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体**フォントで記述し、続けてその定義を通常フォントで記述する。
第 6 章のセキュリティ要件では、詳細化の部分に下線を引く。

1.3.2 略語・用語

本 ST で使用する用語･略語を Table 1 に定義する。

Table 1 ―略語・用語

略語･用語	説明
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。
HDD	キヤノン複合機・プリンタに搭載されるハードディスク。

略語・用語	説明
HDD データ暗号化/ミラーリングキット	「HDD データ暗号化/ミラーリングキット」とは、TOE である「HDD データ暗号化キット E シリーズ」の製品名称であり、各々対応する複合機・プリンタとの接続形態に合わせてオプション製品として提供される。
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。
鍵シード情報	暗号鍵を生成するための情報。TOE は起動時に TOE 内に保存した鍵シード情報を利用して暗号鍵の再生成を行う。
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/ミラーリングキット E 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/ミラーリング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。
シリアル ATA	HDD 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。

1.4 TOE 概要

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・プリンタに搭載された HDD 内のデータを暗号化することを目的に設計された IT 製品である。

1.4.1 TOE の利用目的

本 TOE は、キヤノン複合機・プリンタに搭載される HDD に保存されたデータが漏洩する問題への対抗を目的として利用される。本 TOE を利用することで、キヤノン複合機・プリンタ本体の拡張性や処理パフォーマンスを劣化させることなく、HDD に書き込まれるデータを暗号化できる。

1.4.2 TOE の動作環境

本節では、TOE を使用するために要求される TOE 以外のハードウェア/ソフトウェアについて説明する。
TOE を使用するためにはキヤノン複合機・プリンタが必要である。キヤノン複合機・プリンタは機種毎に対応オプションのリスト(搭載可能なオプション製品が記載されている製品情報)が用意されており、TOE が装着可能なキヤノン複合機・プリンタは、この対応オプションのリストによって識別される。
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、TOE への対応有無、及び、装着可能な TOE を識別することができる。なお、HDD データ暗号化キット E シリーズには製品として HDD データ暗号化/ミラーリングキット E1 及び HDD データ暗号化/ミラーリングキット E2 があり、対応するキヤノン複合機・プリンタによって異なる。
本 TOE を搭載可能なキヤノン複合機・プリンタを以下に記載する。

Table 2 —TOE を搭載可能なキヤノン複合機・プリンタ

TOE の製品名称	対応するキヤノン複合機・プリンタ
ＨＤＤデータ暗号化／ミラーリングキット・E1 和名：ＨＤＤデータ暗号化／ミラーリングキット・E1 英名：HDD Data Encryption & Mirroring Kit-E1 仏名：Kit d'encryptage et d'écriture du disque dur-E1	imagePRESS C10000VP imagePRESS C8000VP

TOE の製品名称	対応するキヤノン複合機・プリンタ
ＨＤＤデータ暗号化／ミラーリングキット・E2 和名：ＨＤＤデータ暗号化／ミラーリングキット・E2 英名：HDD Data Encryption & Mirroring Kit-E2 仏名：Kit d'encryptage et d'écriture du disque dur-E2	imagePRESS C65 imagePRESS C650 imagePRESS C750 imagePRESS C850

キヤノン複合機・プリンタは、コピー機能・プリント機能・送信（Universal Send）機能・ファクス機能・I ファクス受信機能、などのジョブ機能を併せ持つ複合機やプリント機能のみを持つプリンタである。キヤノン複合機・プリンタは、各ジョブ機能を実行する際に文書データなどのデータの HDD への書き込み、HDD に格納されている文書データなどのデータの読み出しを行う。TOE により、HDD へ書き込まれるこれらのデータを暗号化により保護できる。

1.4.3 TOE の利用方法

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・プリンタ用 HDD データ暗号化キットとして利用者に提供される。TOE は、キヤノン複合機・プリンタに装着して利用される。TOE の装着により、キヤノン複合機・プリンタの機能を利用した HDD アクセスは、自動的に TOE を介して行われる。

1.4.4 TOE の主要なセキュリティ機能

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
- 自己テスト機能

1.5 TOE 記述

本節では、TOE の関連者、保護対象となる資産、TOE の範囲について記述する。

1.5.1 TOE の関連者

TOE の関連者は以下である。なお、TOE の利用に際して、特別な役割や権限は不要である。

- 利用者
  キヤノン複合機・プリンタを使用する者である。キヤノン複合機・プリンタに HDD データ暗号化キットを装着し、コピー・プリンタ・スキャナといったキヤノン複合機・プリンタの機能を使用することで、TOE の機能を利用する。

1.5.2 保護対象となる資産

資産は、User Data である。

1.5.2.1 User Data

TOE は、キヤノン複合機・プリンタに搭載された HDD に保存されたデータが解析されることから HDD を保護するための機能を提供する。
すなわち、TOE の保護対象となる資産は利用者がキヤノン複合機・プリンタを使用することで HDD に書き込まれるデータである。以降 User Data と呼ぶ。

1.5.3 TOE の範囲

1.5.3.1 TOE の物理的範囲

Figure 1 に TOE を利用するための環境を図示する。図において網掛けしたものが、TOE である。TOE は TOE のセキュリティ機能を実現する Canon MFP Security Chip を搭載した基板及びケーブル類から構成される。TOE はキヤノン複合機・プリンタのマザーボードと HDD との間に位置し、TOE を装着することで、HDD へのアクセスは全て TOE を介して行われる。マザーボードーTOE 間、及び TOEーHDD 間のインタフェースは、シリアル ATA である。

Figure 1 TOE の利用環境

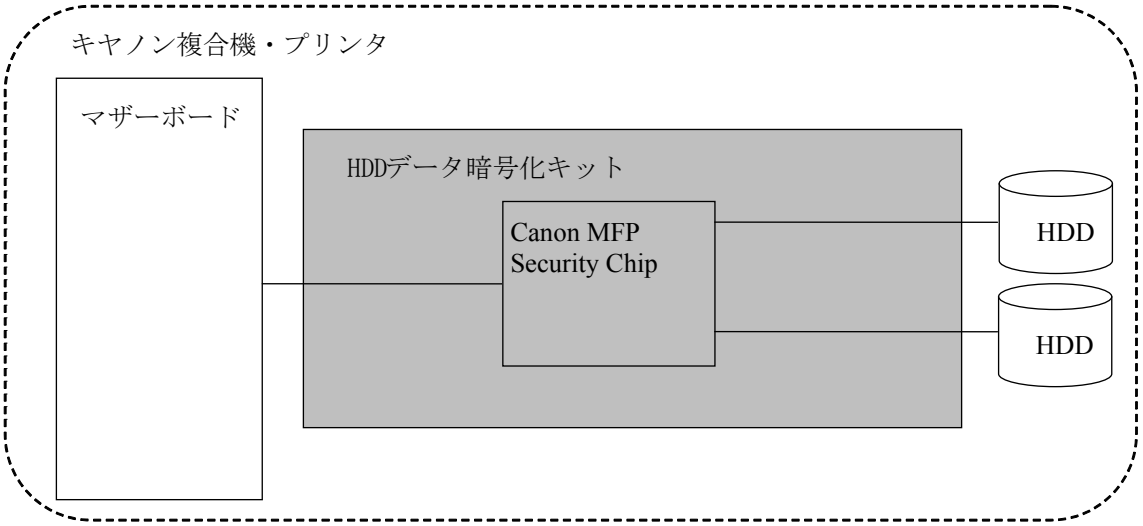


Figure 1 に示した各要素の役割を、以下に示す。

Table 3 ―各要素の一覧

名称	役割
マザーボード	キヤノン複合機・プリンタ内の基板。本基板に、HDD データ暗号化キットが装着される。
HDD データ暗号化キット	本 TOE
Canon MFP Security Chip	本 TOE のセキュリティ機能を実現する ASIC。
HDD	データが格納されるディスク。本 TOE はミラーリング機能を有しているため、2 台の HDD を接続できるが、2 台の HDD は必須ではなく 1 台の HDD でも運用できる。 HDD は利用者が簡単に取り外し可能な構成となっている。

TOE に含まれるガイダンスは以下の通りである。日本向けと海外向けでそれぞれ対応したガイダンスが同梱される。日本向けと海外向けの違いは、言語のみであり記載内容は同じである。尚、ＨＤＤデータ暗号化／ミラーリングキット・E1 は共通のため、以下 6 つのガイダンスが全て同梱される。

(日本向け)
- HDD データ暗号化キット ユーザーズガイド FT6-1331(020)
- HDD ミラーリングキット ユーザーズガイド FT6-1335(000)
- 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)

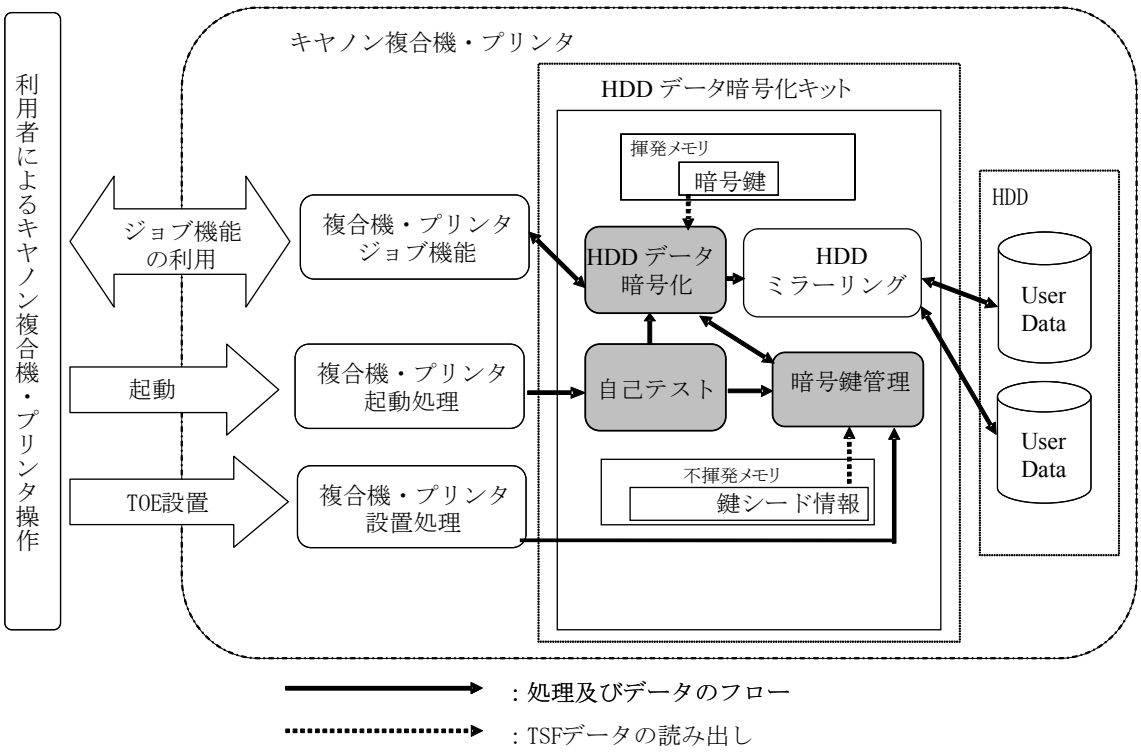
(海外向け)
- HDD Data Encryption & Mirroring Kit-E Series User Documentation FT6-1333(020)
- Make sure to read this notice before using this product. FT6-1334(000)

(共通)
- 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(020)

1.5.3.2 TOE の論理的範囲

Figure 2 は TOE の論理構成を示した図である。なお、図において網掛けしたものが、TOE のセキュリティ機能である。

Figure 2 TOE の論理構成図



TOE が提供するセキュリティ機能は以下である。なお、Figure 2 にて示したように、利用者にはキヤノン複合機・プリンタの機能操作以外に、TOE のセキュリティ機能へ影響を与える方法はない。

■ HDD データ暗号化機能

HDD データ暗号化機能は、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。

■ 暗号鍵管理機能

暗号鍵管理機能は、HDD データ暗号化機能において使用する暗号鍵を生成し、管理する機能である。暗号鍵管理機能は、TOE 設置時に登録された鍵シード情報を使用し、暗号鍵を生成する。暗号鍵は揮発性メモリに格納されるため、キヤノン複合機・プリンタの電源断により消失する。

■ 自己テスト機能

自己テスト機能は、HDD データ暗号化機能による暗号化/復号が正しく動作することを確認する機能である。キヤノン複合機・プリンタを起動することで、TOE は自動的に本機能を動作させる。自己テストに失敗した場合、TOE はそれ以降の動作を停止する。

また、TOE が提供する一般機能は以下である。

■ HDD ミラーリング機能

HDD ミラーリング機能は、2 台の HDD が保持するデータの同一性を保ち、一方の HDD をエラー発生時のバックアップとして使用する機能である。

但し、本機能は、HDD が 2 台の構成、かつ、キヤノン複合機・プリンタにおいて HDD ミラーリング機能を「利用する」の設定をしている場合にのみ動作する。

2 適合主張

本章では、CC 適合主張、PP 適合主張、パッケージ主張について記述する。

2.1 CC 適合主張

本 ST は、以下の Common Criteria（以下、CC と略す）に適合する。

- 適合する CC のバージョン:

  パート 1: 概説と一般モデル バージョン 3.1 改訂第 4 版［翻訳第 1.0 版］

  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［翻訳第 1.0 版］

  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［翻訳第 1.0 版］
- 適合する CC:

  パート 2 及びパート 3

2.2 PP 適合主張

本 ST が適合を主張する PP は存在しない。

2.3 パッケージ主張

本 ST は以下のパッケージ適合を主張する。

- 適合する機能要件のパッケージ主張: なし
- 適合する保証要件のパッケージ主張: EAL3 適合

3 セキュリティ課題定義

本章では、脅威、脅威エージェント、組織のセキュリティ方針、前提条件について記述する。

3.1 脅威

以下の脅威について記述する。

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 User Data を暴露するかもしれない。

3.2 脅威エージェント

攻撃者を以下と定義する。
取り外された HDD を入手し、ディスク解析ツール等を利用して、HDD 上の User Data への不正アクセスを試みる悪意ある者
尚、攻撃者の攻撃能力を低レベルで基本的な攻撃能力と想定する。

3.3 組織のセキュリティ方針

以下に TOE が従わなければならない組織のセキュリティ方針を記述する。

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。

3.4 前提条件

以下に TOE が想定する前提条件について記載する。

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 セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針について記述する。

4.1 TOE のセキュリティ対策方針

本節は、脅威に対抗し、組織のセキュリティ方針を実現するための TOE のセキュリティ対策方針を示す。

O.CRYPTO
TOE は、ディスク解析ツールを利用して直接 HDD へアクセスしてもデータを解析できないようにする。すなわち、TOE は以下の処理を実施する。

- 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

O.CORRECT_TSF_OPERATION
TOE は、運用環境において HDD データ暗号化機能が正しく動作すること及び暗号鍵に破損がないことを確認するために、HDD データ暗号化機能の自己テストを実施する。

4.2 運用環境のセキュリティ対策方針

本節は、運用環境のセキュリティ対策方針に関して記述する。

OE.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に対して保護された環境に設置されなければならない。

4.3 セキュリティ対策方針根拠

TOE セキュリティ環境に対応するセキュリティ対策方針の関係を Table 4 に示す。

Table 4 —TOE セキュリティ環境とセキュリティ対策方針の対応

脅威、ポリシー、前提条件 / セキュリティ対策方針	T.HDD_ACCESS	P.TSF_VERIFICATION	A.PHYSICAL_ACCESS_MANAGED
O.CRYPTO	✓		
O.CORRECT_TSF_OPERATION		✓	
OE.PHYSICAL_ACCESS_MANAGED			✓

以下に、『Table 4 TOE セキュリティ環境とセキュリティ対策方針の対応』の根拠を示す。

T.HDD_ACCESS
T.HDD_ACCESS は O.CRYPTO によって対抗される。なぜなら、O.CRYPTO によって 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ため、TOE を介さずに直接 HDD へアクセスしデータ解析ツールを利用することにより HDD 上の User Data が漏洩することを防ぐことができる。

P.TSF_VERIFICATION
P.TSF_VERIFICATION は O.CORRECT_TSF_OPETATION によって実施される。なぜなら、O.CORRECT_TSF_OPETATION により、TOE は HDD データ暗号化機能が正しく動作するか、また暗号鍵に破損がないかを確認するための自己テストを実施するためである。

A.PHYSICAL_ACCESS_MANAGED
A.PHYSICAL_ACCESS_MANAGED は OE.PHYSICAL_ACCESS_MANAGED により実現できる。なぜなら、OE.PHYSICAL_ACCESS_MANAGED によって、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に対して保護された環境に設置されるからである。

5　拡張コンポーネント定義

本 ST では、拡張セキュリティ機能要件を定義しない。

6 セキュリティ要件

本章では、TOE のセキュリティ機能要件、セキュリティ保証要件、セキュリティ要件根拠に関して記述する。

6.1 TOE のセキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。

FCS_CKM.1 暗号鍵生成

下位階層: なし

依存性: [FCS_CKM.2 暗号鍵配付 または FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付：標準のリスト]
- 指定なし

[割付：暗号鍵生成アルゴリズム]
- Hash_DRBG を利用した SP800-90A に基づく乱数生成アルゴリズム

[割付：暗号鍵長]
- 128 ビットもしくは 256 ビット

FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート、
または FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、
または FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1 TSF は、[割付：標準のリスト]に合致する、特定された暗号アルゴリズム[割付：暗号アルゴリズム]と暗号鍵長[割付：暗号鍵長]に従って、[割付：暗号操作のリスト]を実行しなければならない。

[割付：標準のリスト]
- FIPS PUB 197

[割付：暗号アルゴリズム]
- AES

[割付：暗号鍵長]
- 128 ビットもしくは 256 ビット

[割付：暗号操作のリスト]
- HDD へ書き込まれるデータの暗号化操作
- HDD から読み出されるデータの復号操作

FPT_TST.1　TSF テスト

下位階層: なし

依存性: なし

FPT_TST.1.1 TSF は、[選択: TSF、[割付: TSF の一部]]の正常動作を実証するために、[選択: 初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件[割付: 自己テストが作動すべき条件]下で]自己テストのスイートを実行しなければならない。

[選択: TSF、[割付: TSF の一部]]
- [割付: TSF の一部]

[割付: TSF の一部]
- HDD データ暗号化及び暗号鍵生成で利用する暗号アルゴリズム

[選択: 初期立ち上げ中、通常運用中定期的に、許可利用者の要求時に、条件[割付: 自己テストが作動すべき条件]下で]
- 初期立ち上げ中

FPT_TST.1.2 TSF は、許可利用者に、[選択: [割付: TSF データの一部]、TSF データ]の完全性を検証する能力を提供しなければならない。

[選択: [割付: TSF データの一部]、TSF データ]
- [割付: TSF データの一部]

[割付: TSF データの一部]
- 鍵シード情報

FPT_TST.1.3 TSF は、許可利用者に、[選択: [割付: TSF の一部]、TSF]の完全性を検証する能力を提供しなければならない。

[選択: [割付: TSF の一部]、TSF]
- [割付: TSF の一部]

[割付: TSF の一部]
- TSF 実行コード

6.2　セキュリティ保証要件

本 ST にて要求する、TOE に対する保証レベルは EAL3 である。保証コンポーネント構成を Table 5 に示す。要求する各保証コンポーネントの保証エレメントは、CC Part3 の要求通りである。

Table 5 — TOE の保証要件コンポーネント一覧

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述

保証クラス	保証コンポーネント
	ADV_FSP.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.3 許可の管理
	ALC_CMS.3 実装表現の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト：基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト-サンプル
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

6.3 セキュリティ要件根拠

6.3.1 セキュリティ対策方針とセキュリティ機能要件の対応

セキュリティ対策方針に対するセキュリティ機能要件の対応を『Table 6 セキュリティ対策方針とセキュリティ機能要件の対応』に示す。

Table 6 ―セキュリティ対策方針とセキュリティ機能要件の対応

セキュリティ対策方針 / セキュリティ機能要件	O.CRYPTO	O.CORRECT_TSF_OPERATION
FCS_CKM.1	✓	
FCS_COP.1	✓	
FPT_TST.1		✓

6.3.2 セキュリティ機能要件根拠

以下に、『Table 6 セキュリティ対策方針とセキュリティ機能要件の対応』の根拠を示す。

O.CRYPTO
本セキュリティ対策方針は、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ことを規定している。
暗号化または復号に使用される暗号鍵に関しては、FCS_CKM.1 により、「Hash_DRBG を利用した SP800-90A に基づく乱数生成アルゴリズム」によって「128 ビットもしくは 256 ビット長の暗号鍵」が生成される。
実際の暗号化、復号操作に関しては、FCS_COP.1 により、「128 ビットもしくは 256 ビット長の暗号鍵」を使用した「FIPS PUB197」に合致する「暗号アルゴリズム AES」によって、HDD へ書き込まれるデータの暗号化操作、HDD から読み出されるデータの復号操作が実行される。

以上により、O.CRYPTO を実現することができる。

O.CORRECT_TSF_OPERATION
本セキュリティ対策方針は、運用環境において HDD データ暗号化機能が正しく動作すること及び暗号鍵に破損がないことを確認するために、自己テストを実施することを規定している。
FPT_TST.1 により、TOE は起動時に HDD データ暗号化及び暗号鍵生成で利用する暗号アルゴリズムが正しく動作することの確認と、実行コードの検証のための自己テストを実行し、HDD データ暗号化機能の完全性を検証する。また、暗号鍵は TOE 内に保存された鍵シード情報から再生成されるため、鍵シード情報の完全性を検証することで暗号鍵に破損がないことを確認する。

以上により、O.CORRECT_TSF_OPERATION を実現することができる。

6.3.3 セキュリティ機能要件間の依存関係

セキュリティ機能要件間の依存関係を『Table 7 セキュリティ機能要件間の依存関係』に示す。

Table 7 ―セキュリティ機能要件間の依存関係

機能要件	CC で要求している依存性	ST で満たしている依存性	依存性を満たしていない理由
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4	FCS_COP.1	FCS_CKM.4 を主張していない理由：OE.PHYSICAL_ACCESS_MANAGED により TOE は物理的なアクセスに対して保護されており、暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FCS_COP.1	[FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	FCS_CKM.4 を主張していない理由：OE.PHYSICAL_ACCESS_MANAGED により TOE は物理的なアクセスに対して保護されており、暗号鍵を取り出すことは不可能な構造となっている。従って機能的に暗号鍵破棄をしなくとも暗号鍵は安全に管理されている。
FPT_TST.1	なし	なし	N/A（依存性の要求なし）

6.4　セキュリティ保証要件根拠

本 TOE は、キヤノン複合機・プリンタにセキュリティ機能を提供する商用の IT 製品であり、低レベルで基本的な攻撃能力の攻撃者による HDD のデータ解析を原因としたデータ漏洩に対抗することを目的としている。従って、TOE には不特定者による低レベルで基本的な攻撃能力の攻撃への対抗性の保証が必要となる。そのため、外部インタフェースの識別、機能の内部構造の特定、テストによるセキュリティ機能の確認、脆弱性分析といった開発プロセスにおけるセキュリティ確保への取組みに加え、開発環境や誤使用の防止といった側面からのセキュリティ確保の取組みが必要であり、評価保証レベルとして EAL3 が求められる。
なお、EAL3 で要求されるすべてのセキュリティ保証要件のセットを採用する。そのため、TOE のセキュリティ保証要件間の依存関係はすべて満たされる。

7　TOE 要約仕様

本章では、TOE 要約仕様を記述する。

7.1　TOE セキュリティ機能

本節では、TOE のセキュリティ機能を説明する。各機能に対応する TOE セキュリティ機能要件が示されているように、本節で説明するセキュリティ機能は、6.1 章で記述した TOE セキュリティ機能要件を満たす。

7.1.1　HDD データ暗号化機能（F.HDD_CRYPTO）

HDD データ暗号化機能は、以下のセキュリティ機能を備える。

セキュリティ機能の仕様	セキュリティ機能要件
TOE は、次の暗号操作を行う。 ■　HDD へ書き込むデータを暗号化する ■　HDD から読み出すデータを復号する 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「128 ビット」もしくは「256 ビット」の暗号鍵 ■　FIPS PUB 197 に従った「AES アルゴリズム」	FCS_COP.1

7.1.2　暗号鍵管理機能（F.KEY_MANAGE）

暗号鍵管理機能は、以下のセキュリティ機能を備える。

セキュリティ機能の仕様	セキュリティ機能要件
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、「Hash_DRBG を利用した SP800-90A に基づく乱数生成アルゴリズム」 ■　生成される暗号鍵の鍵長は「128 ビット」もしくは「256 ビット」 暗号鍵の管理を以下のように行う。 ■　起動時に、TOE は TOE 内に格納された鍵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、TOE 内の揮発性メモリに保持する また、暗号鍵は揮発性メモリにのみ存在するため、電源断により消失する。	FCS_CKM.1

生成される暗号鍵の鍵長は、Table 8 に示す通り TOE が搭載されるキヤノン複合機・プリンタにより一意に定められる。

Table 8 —鍵長とキヤノン複合機・プリンタの関係

鍵長	対応するキヤノン複合機･プリンタ
128 ビット	imagePRESS C10000VP imagePRESS C8000VP
256 ビット	imagePRESS C65 imagePRESS C650 imagePRESS C750 imagePRESS C850

7.1.3 自己テスト機能（F.SELF_TEST）

自己テスト機能は、以下のセキュリティ機能を備える。

セキュリティ機能の仕様	セキュリティ機能要件
TOE は、起動時に自動的に自己テスト機能を実施し、HDD データ暗号化機能の完全性を検証する。自己テストで検証される内容を次に示す。 ■ 実行コードの完全性検証 TOE 内に格納されたファームウェアを読み込む際に、32bit CRC チェックにより完全性を検証する ■ 暗号アルゴリズムの完全性検証 HDD データ暗号化機能により実行される AES アルゴリズムが正しく動作するかを既知解テストにより検証する ファームウェアにより算出される乱数生成が正しく動作するかを既知解テストにより検証する 乱数生成で利用するハッシュ関数が正しく動作するかを既知解テストにより検証する ■ TSF データの完全性検証 TOE 内に格納された鍵シード情報を読み込む際に、32bit CRC チェックにより完全性を検証する また、自己テストに失敗した場合、TOE はエラー状態に移行し、その後の TOE を介した HDD へのアクセスはできない。	FPT_TST.1

以上