発行日：2008/4/07

Canon MFP Security Chip
セキュリティターゲット

Version 1.06

2008/4/07

キヤノン株式会社

- 更新履歴 -

バージョン	日付	事由	作成元	検査者	承認者
1.00	2007/11/30	新規作成	安立 作成日： 2007/11/30	安立 検査日： 2007/11/30	牧谷 承認日： 2007/11/30
1.01	2008/1/25	記載の修正	安立 作成日： 2008/01/25	安立 検査日： 2008/01/25	牧谷 承認日： 2008/01/25
1.02	2008/01/29	記載の修正	安立 作成日： 2008/01/29	安立 検査日： 2008/01/29	牧谷 承認日： 2008/01/29
1.03	2008/02/27	記述の修正	安立 作成日： 2008/02/26	安立 検査日： 2008/02/26	牧谷 承認日： 2007/02/27
1.04	2008/03/07	記述の修正	安立 作成日： 2008/03/05	安立 検査日： 2008/03/05	牧谷 承認日： 2008/3/07
1.05	2008/03/10	記述の修正	安立 作成日： 2008/03/10	安立 検査日： 2008/03/10	牧谷 承認日： 2008/03/10
1.06	2008/04/07	記述の修正	安立 作成日： 2008/04/04	安立 検査日： 2008/04/04	牧谷 承認日： 2008/04/07

～ 目次 ～

～ 図目次 ～

～ 表目次 ～

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語・略語について記述する。

1.1. ST 識別

1.1.1. ST の識別と管理

名称：Canon MFP Security Chip　セキュリティターゲット
バージョン：1.06
作成日：2008 年 4 月 7 日
作成者：キヤノン株式会社

1.1.2. TOE の識別と管理

名称：Canon MFP Security Chip
バージョン：1.50
作成者：キヤノン株式会社

1.1.3. 適用する CC のバージョン

CC v2.3
補足-0512 適用

1.2. ST 概要

本 ST は、キヤノン複合機・プリンタ用オプション製品として提供される HDD データ暗号化キット B シリーズに搭載されるセキュリティチップを対象としている。

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

1.3. CC 適合

本 ST は、以下を満たしている。

パート 2 適合

パート 3 適合

EAL 3 適合

適合する PP は存在しない。

1.4. 参考資料

- 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
- 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
- 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
- Common Criteria for Information Technology Security Evaluation
  Part 1： Introduction and general model
  August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2： Security functional requirements
  August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3： Security assurance requirements

August 2005 Version 2.3 CCMB-2005-08-003

- ISO/IEC 15408:2005 Information Technology – Security Techniques-Evaluation Criteria for IT Security
- 補足-0512

1.5. 表記規則、用語・略語

1.5.1. 表記規則

第 3 章の前提条件、脅威、組織のセキュリティ方針、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 5 章の IT セキュリティ要件では、詳細化の部分に下線を引く。また、IT 環境に対するセキュリティ要件については、[E]を付与する。

1.5.2. 用語・略語

本 ST で使用する用語・略語を表 1.1 に定義する。

表 1-1 用語・略語定義

用語・略語	定義内容
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。
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 ST の以降の記述で「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
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。
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。
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。
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。

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 構成、及び保護対象となる資産について記述する。

2.1. TOE 種別

本 TOE は暗号化用セキュリティチップであり、キヤノン複合機・プリンタのセキュリティを強化する「HDD データ暗号化キット B シリーズ」への搭載を目的に設計された IT 製品である。

2.2. TOE 概要

2.2.1. TOE の利用目的

キヤノン複合機・プリンタを利用することにより、HDD には利用者から入力されたデータが保存される。

本 TOE は、HDD 盗難により 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。

2.2.2. 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。

2.2.3. TOE の利用方法

本 TOE は、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。HDD データ暗号化キットは、キヤノン複合機・プリンタに装着して利用する。HDD データ暗号化キットの装着により、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、TOE を介して行われる。但し、HDD データ暗号化キットを動作させるための設定として、HDD データ暗号化キットに同梱される Flash ボードを、キヤノン複合機・プリンタに装着しておく必要がある。

2.2.4. TOE の動作環境

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。

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。

2.3. TOE 構成

2.3.1. TOE の物理的構成

図 2-1 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。

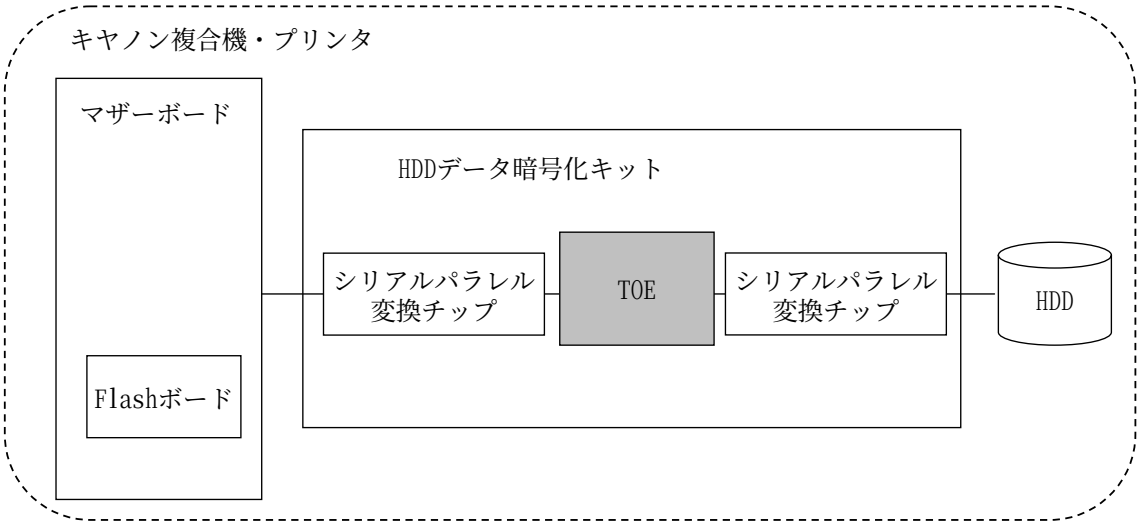

図 2-1 TOE の利用環境

図 2-1 で示した各要素の役割を、表 2-1 に示す。

表 2-1 TOE の利用環境の役割

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及び Flash ボードが装着される。
Flash ボード	マザーボードに装着される基板。

	認証のロジックが格納される。
HDD データ暗号化キット	TOE が搭載される基板。本基板は、HDD 毎の接続形態を取る（つまり、HDD が複数ある場合には、複数必要になる）。
TOE	本 TOE。
シリアルパラレル変換チップ	パラレル ATA とシリアル ATA を変換するチップである。TOE の入出力インタフェースがパラレル ATA で、キヤノン複合機･プリンタがシリアル ATA であるため、本チップが必要となる。 なお、本チップは物理的な入出力インタフェース対応のためであり、セキュリティ機能に影響を与えるものではない。

次に、図 2-2 において、図 2-1 に示した TOE の詳細構成を示す。

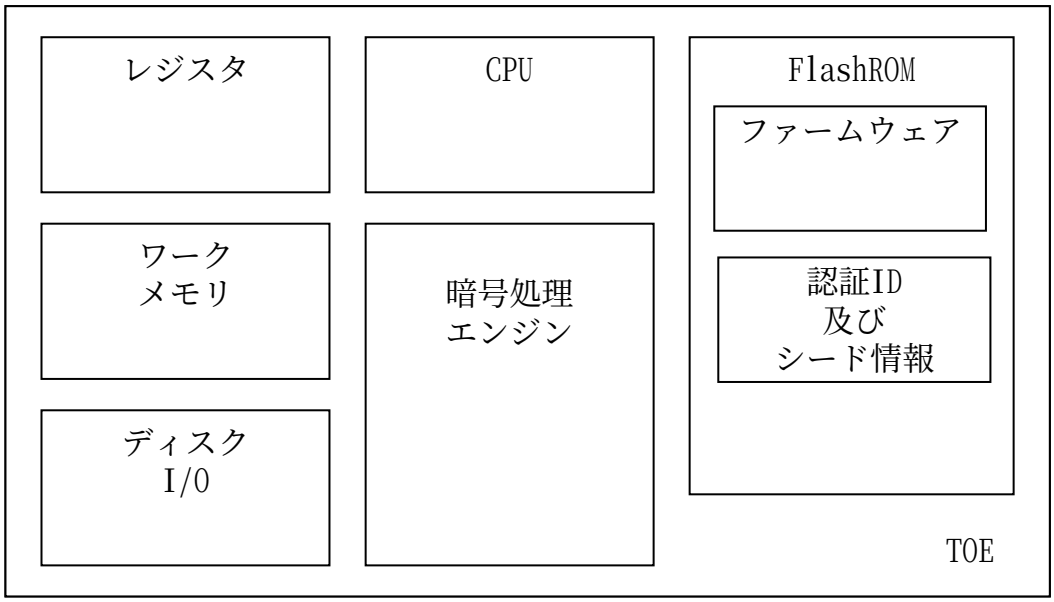

図 2-2 TOE 物理構成図

図 2-2 で示した、TOE を構成する要素の役割を表 2-2 に記載する。

表 2-2 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。

	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。
FlashROM	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、シード情報が格納される。
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。

2.3.2. TOE の論理的構成

図 2-3 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 の機能である。

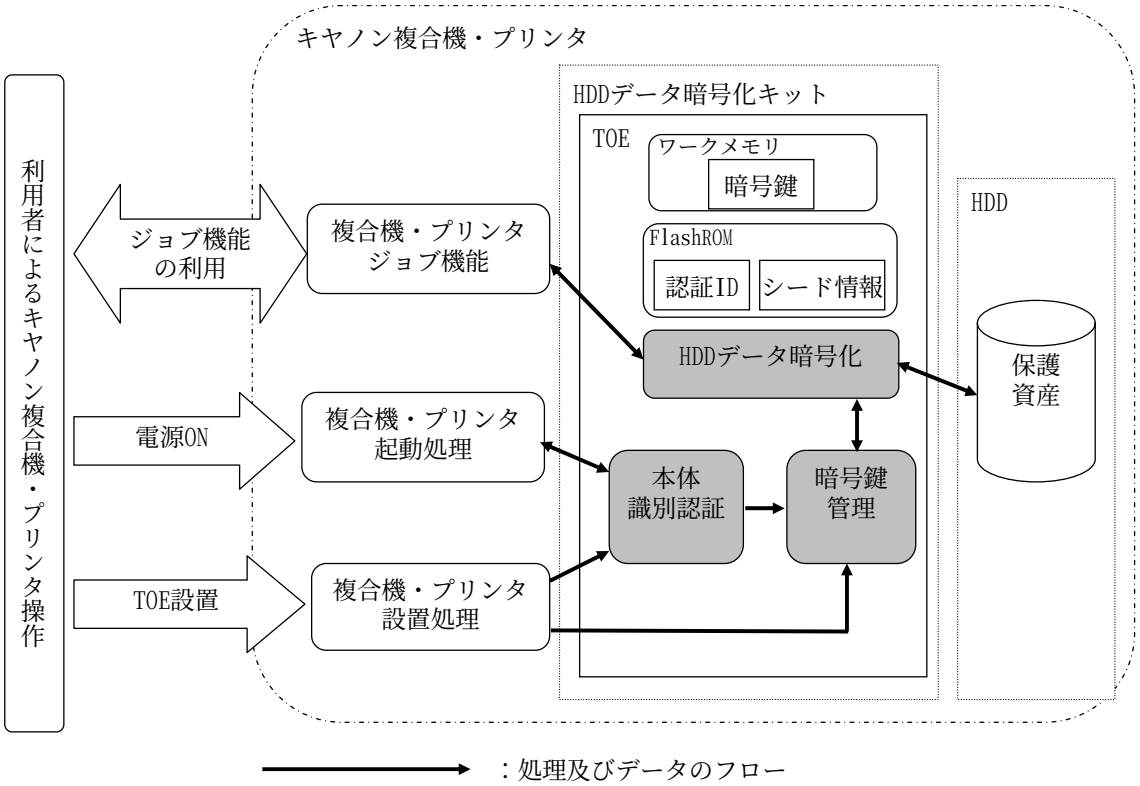

図 2-3 TOE 論理構成図

図 2-3 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、TOE は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、TOE は 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。

TOE が提供するセキュリティ機能は以下である。なお、図 2-3 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であるワーク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。
- 本体識別認証機能
  本体識別認証機能は、TOE 設置時に登録された認証 ID を使用し、TOE が設置されたキヤノン複合機・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。
  本体識別認証機能は、TOE が「登録済み本体デバイス」に取り付けられていることを確認できない限り、HDD アクセスを禁止する。
  すなわち、利用者が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」である場合、利用者による TOE を介した HDD アクセスはすべて許可される。

2.4. 保護対象となる資産

TOE は、キヤノン複合機・プリンタに搭載された HDD が抜き取られ、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。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

TOE が想定する前提条件はない。

3.2. 脅威

以下では、攻撃者の攻撃能力を低レベルと想定する。

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。

3.3. 組織のセキュリティ方針

TOE が従わなければならない組織のセキュリティ方針はない。

4. セキュリティ対策方針

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もしくは他のキヤノン複合機・プリンタを利用して、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.BOARD_AUTH

TOE は、「登録済み本体デバイス」以外から、TOE を介した HDD アクセスを試みても、HDD へアクセス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。

- 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確認する
- 「登録済み本体デバイス」に接続されている場合のみ、TOE を介した HDD へのアクセスを許可する

4.2. 環境のセキュリティ対策方針

OE.UNIQUE_INFO

キヤノン複合機・プリンタは、機器個体ごとに一意となる認証 ID を生成する。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

本節では、TOE が満たさなければならないセキュリティ要件を示す。

5.1.1. TOE セキュリティ機能要件

FCS_CKM.1 暗号鍵生成

下位階層：なし

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]

- FIPS 186-2

[割付：暗号鍵生成アルゴリズム]

- FIPS 186-2 に基づく暗号鍵生成アルゴリズム

[割付：暗号鍵長]

- 256 ビット

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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1　　暗号操作

下位階層：なし

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]
- 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

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 FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FIA_UAU.2　　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

詳細化：「利用者」→登録済み本体デバイス
：「各利用者」→各キヤノン複合機・プリンタ

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.4　　単一使用認証メカニズム

下位階層：なし

FIA_UAU.4.1

TSFは、[割付：識別された認証メカニズム]に関する認証データの再使用を防止しなければならない。

[割付：識別された認証メカニズム]

・　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

依存性：なし

FIA_UID.2　　アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化：「利用者」→登録済み本体デバイス
　　：「各利用者」→各キヤノン複合機・プリンタ

依存性：なし

FPT_RVM.1　　TSP の非バイパス性

下位階層：なし

FPT_RVM.1.1

TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

5.1.2.　TOE 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表 5.1 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。

なお、ASE クラスは、保証レベルに関わらず必須となる保証要件として採用する。

表 5-1 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		コンポーネント
構成管理	許可の管理	ACM_CAP.3
	TOE の CM 範囲	ACM_SCP.1
配付と運用	配付手続き	ADO_DEL.1
	設置、生成、及び立上げ手順	ADO_IGS.1
開発	非形式的機能仕様	ADV_FSP.1
	セキュリティ実施上位レベル設計	ADV_HLD.2
	非形式的対応の実証	ADV_RCR.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
ライフサイクルサポート	セキュリティ手段の識別	ALC_DVS.1
テスト	カバレージの分析	ATE_COV.2
	テスト：上位レベル設計	ATE_DPT.1
	機能テスト	ATE_FUN.1
	独立テスト- サンプル	ATE_IND.2
脆弱性評定	ガイダンスの検査	AVA_MSU.1
	TOEセキュリティ機能強度評価	AVA_SOF.1
	開発者脆弱性分析	AVA_VLA.1

5.2. IT 環境に対するセキュリティ要件

本節では、IT 環境が満たさなければならないセキュリティ要件を示す。

5.2.1. IT 環境のセキュリティ機能要件

FIA_SOS.2[E] TSF 秘密生成

下位階層: なし

FIA_SOS.2.1[E]

TSF は、[割付: *定義された品質尺度*]に合致する秘密を生成するメカニズムを提供しなければならない。

詳細化：「TSF」→キヤノン複合機・プリンタ

[割付: *定義された品質尺度*]
・キヤノン複合機・プリンタ毎に一意となる32byteのデータ値

FIA_SOS.2.2[E]

TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。

詳細化：「TSF」→キヤノン複合機・プリンタ

[割付: *TSF 機能のリスト*]
・本体識別認証機能

依存性: なし

5.2.2.　　IT 環境のセキュリティ保証要件

IT 環境のセキュリティ保証要件はない。

5.3.　セキュリティ機能強度

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本である。また、明示された機能強度が適用される TOE セキュリティ機能要件は、FIA_UAU.2、FIA_UAU.4、FIA_UID.2であり、機能強度は SOF-基本である。

なお、採用する暗号アルゴリズムは、TOE セキュリティ機能強度の対象外である。

6. TOE 要約仕様

本章では、TOE の要約仕様を記述する。

6.1. 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、5.1.1.TOE セキュリティ機能要件で記述した TOE セキュリティ機能要件を満たす。

6.1.1. 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群を備える。

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」	FCS_COP.1 FPT_RVM.1

6.1.2. 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群を備える。

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、「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。	FCS_CKM.1 FPT_RVM.1

6.1.3. 本体識別認証機能（F.KIT_CHECK）

本体識別認証機能は、以下のセキュリティ機能群を備える。

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「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。	FIA_UAU.2 FIA_UAU.4 FIA_UID.2 FPT_RVM.1

6.2. セキュリティ機能強度

本 TOE において、機能強度の対象となる順列的・確率的メカニズムを有する IT セキュリティ機能は F.KIT_CHECK であり、機能強度は SOF-基本である。

6.3. 保証手段

本節では、TOE の保証手段を説明する。表 6-1 に示すように、以下のセキュリティ保証手段は、表 5-1 で記述した TOE セキュリティ保証要件を満たすものである。なお、ASE クラスに対する保証手段は、本セキュリティターゲットである。

表 6-1 TOE の保証手段一覧

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	許可の管理	ACM_CAP.3	キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（1） キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（2） Canon MFP Security Chip 評価証拠一覧
	TOE の CM 範囲	ACM_SCP.1	
配付と運用	配付手続き	ADO_DEL.1	キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（1） キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（2）
	設置、生成、及び立上げ手順	ADO_IGS.1	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）
開発	非形式的機能仕様	ADV_FSP.1	キヤノン複合機・プリンタ用セキュリティチップ ファームウェア外部仕様書
	セキュリティ実施上位レベル設計	ADV_HLD.2	キヤノン複合機・プリンタ用セキュリティチップ ファームウェア上位レベル仕様書 HERMIT ハードウェアマニュアル

	非形式的対応の実証	ADV_RCR.1	キヤノン複合機・プリンタ用セキュリティチップ ファームウェア表現対応表
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	HDD データ暗号化キット・B シリーズ ユーザーズガイド HDD Data Encryption Kit-B Series Reference Guide 別紙（注意書き） 別紙（Caution）
	利用者ガイダンス	AGD_USR.1	
ライフサイクルサポート	セキュリティ手段の識別	ALC_DVS.1	キヤノン複合機・プリンタ用セキュリティチップ ファームウェア開発セキュリティ規約
テスト	カバレージの分析	ATE_COV.2	キヤノン複合機・プリンタ用セキュリティチップ テストカバレージ分析書
	テスト：上位レベル設計	ATE_DPT.1	キヤノン複合機・プリンタ用セキュリティチップ テスト深さ分析書
	機能テスト	ATE_FUN.1	キヤノン複合機・プリンタ用セキュリティチップ テスト仕様書 キヤノン複合機・プリンタ用セキュリティチップ テスト手順書 キヤノン複合機・プリンタ用セキュリティチップ テスト結果報告書
	独立テスト - サンプル	ATE_IND.2	Canon MFP Security Chip 1.50
脆弱性評定	ガイダンスの検査	AVA_MSU.1	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） HDD データ暗号化キット・B シリーズ ユーザーズガイド HDD Data Encryption Kit-B Series Reference Guide 別紙（注意書き） 別紙（Caution）

	TOE セキュリティ機能強度評価	AVA_SOF.1	キヤノン複合機・プリンタ用セキュリティチップ 脆弱性分析書
	開発者脆弱性分析	AVA_VLA.1	

7. PP 主張

本 ST が適合する PP は存在しない。

8. 根拠

8.1. 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『表 8.1 TOE セキュリティ環境とセキュリティ対策方針の対応』に示す。

表 8-1 TOE セキュリティ環境とセキュリティ対策方針の対応

TOE セキュリティ環境 / セキュリティ対策方針	T.HDD_ACCESS	T.WRONG_BOARD
O.CRYPTO	○	
O.BOARD_AUTH		○
OE.UNIQUE_INFO		○

以下に、『表 8.1　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、悪意のある者がHDDを取り外し、ディスク解析ツールや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脅威である。

この脅威に対抗するためには、HDDへ直接アクセスしてもデータを解析できなくすることが必要である。

本TOEでは、O.CRYPTOにより、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しているため、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、TOEを介さずに直接HDDへアクセスしてもデータを解析することはできない。

従って、セキュリティ対策方針O.CRYPTOが満たされることにより本脅威に対抗することができる。

T.WRONG_BOARD

T.WRONG_BOARDは悪意のある者が、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脅威である。

この脅威に対抗するためには、「登録済み本体デバイス」以外から、TOEを介したHDDアク

セスを試みても、HDDへアクセスできないようにすることが必要である。また、「登録済み本体デバイス」とは別のキヤノン複合機・プリンタが、「登録済み本体デバイス」と重複する認証IDを生成した場合、悪意のある者はHDDデータ暗号化キット及びHDDを認証IDが重複する別のキヤノン複合機・プリンタに接続し、HDD上のデータを暴露してしまう。そのため、キヤノン複合機・プリンタは機器個体ごとに一意となる認証IDを生成することが必要である。
本 TOE では、O.BOARD_AUTH により、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確認し、「登録済み本体デバイス」に接続されている場合のみ、TOE を介した HDD へのアクセスを許可しているため、「登録済み本体デバイス」以外から、TOE を介した HDD アクセスを行うことはできない。また、OE.UNIQUE_INFO により、キヤノン複合機・プリンタは、機器個体ごとに一意となる認証 ID を生成する。

従って、セキュリティ対策方針O.BOARD_AUTHが満たされることにより本脅威に対抗することができる。

8.2.　セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

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『表8.2 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。

表 8-2 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.BOARD_AUTH	OE.UNIQUE_INFO
FCS_CKM.1	○		
FCS_COP.1	○		
FIA_UAU.2		○	
FIA_UAU.4		○	
FIA_UID.2		○	
FPT_RVM.1	○	○	
FIA_SOS.2[E]			○

以下に、『表 8.2 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、「FIPS 186-2」に合致する、「FIPS186-2 に基づく暗号鍵生成アルゴリズム」によって「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、「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。

また、FPT_RVM.1 により、FCS_CKM.1 による暗号鍵生成、FCS_COP.1 による暗号操作が確実に実施され、成功することを保証する。

以上により、O.CRYPTO を実現することができる。

O.BOARD_AUTH

本セキュリティ対策方針は、TOE が、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確認し、「登録済み本体デバイス」に接続されている場合のみ、TOE を介した HDD へのアクセスを許可することを規定している。

FIA_UAU.2、FIA_UID.2 により、TOE は登録済み本体デバイスを識別認証し、識別認証の結果、「登録済み本体デバイス」であると判断した場合、HDD へのアクセスを許可する。

登録済み本体デバイスの認証に使用される認証メカニズムは「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」であり、FIA_UAU.4 により、認証データの再使用を防止している。

また、FPT_RVM.1 により、FIA_UAU.2 及び FIA_UID.2 による識別認証、FIA_UAU.4 による認証データの再使用防止が確実に実施され、成功することを保証する。

以上により、O.BOARD_AUTH を実現することができる。

OE.UNIQUE_INFO

本セキュリティ対策方針は、キヤノン複合機・プリンタが、機器個体ごとに一意となる認証 ID を生成することを規定している。

FIA_SOS.2[E]により、HDD データ暗号化キット取り付け時に生成される認証 ID は、キヤノン複合機・プリンタ毎に一意の 32byte のデータ値となる。なお、この認証 ID は、本体識別認証機能にて使用される。

以上により、OE.UNIQUE_INFO を実現することができる。

8.2.2. 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『表 8.3 セキュリティ機能要件間の依存関係』に示す。

表 8-3 セキュリティ機能要件間の依存関係

NO	セキュリティ機能要件	下位階層	依存関係	参照 NO	備考
1	FCS_CKM.1	なし	[FCS_CKM.2 または FCS_COP.1] FCS_CKM.4 FMT_MSA.2	2	暗号鍵は、揮発性メモリであるワーク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伴う電荷消失により消去される。 よって、FCS_CKM.4 は不要である。
					本 TOE では、鍵種別や有効期限など、セキュリティに関する属性は存在しない。よって、FMT_MSA.2 は採用しない。
2	FCS_COP.1	なし	[FDP_ITC.1 または FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1	暗号鍵は、揮発性メモリであるワーク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伴う電荷消失により消去される。 よって、FCS_CKM.4 は不要である。
					本 TOE では、鍵種別や有効期限など、セキュリティに関する属性は存在しない。よって、FMT_MSA.2 は採用しない。
3	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	5	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
4	FIA_UAU.4	なし	なし		

5	FIA_UID.2	FIA_UID.1	なし		
6	FPT_RVM.1	なし	なし		
7	FIA_SOS.2[E]	なし	なし		

8.2.3. TOE セキュリティ機能要件の相互作用

明示的な依存関係は要求されないが、相互支援を目的として選択されたセキュリティ機能要件を『表 8.4 TOE セキュリティ機能要件の相互作用について』に示す。

表 8-4 TOE セキュリティ機能要件の相互作用について

NO	機能要件	相互サポート
1	FCS_CKM.1	FPT_RVM.1
2	FCS_COP.1	FPT_RVM.1
3	FIA_UAU.2	FPT_RVM.1
4	FIA_UAU.4	FPT_RVM.1
5	FIA_UID.2	FPT_RVM.1
6	FPT_RVM.1	なし

FPT_RVM.1<迂回防止>

FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、暗号鍵生成に関するセキュリティ機能要件、暗号操作に関するセキュリティ機能要件、チャレンジ＆レスポンス認証に関するセキュリティ機能要件が呼び出され成功することが保証される。対象となるセキュリティ機能要件は、FCS_CKM.1、FCS_COP.1、FIA_UAU.2、FIA_UAU.4、FIA_UID.2 である。

従って、FPT_RVM.1 によって FCS_CKM.1、FCS_COP.1、FIA_UAU.2、FIA_UAU.4、FIA_UID.2 の迂回防止を支援しているため、セキュリティ対策方針 O.CRYPTO 及び O.BOARD_AUTH が達成される。

<ドメイン分離>

本 TOE には、オブジェクトにアクセスする利用者代行のサブジェクトは存在しないため、アクセス制御や情報フロー制御は実施しない。そのため、信頼できないサブジェクトによる外部の干渉、及び改ざんから TSF を保護する機能要件である FPT_SEP.1 は不要である。

<非活性化>

本 TOE には、セキュリティ機能の起動や停止を含む、セキュリティ管理に関する機能は存在しない。そのため、セキュリティ機能の非活性化から TSF を保護する機能要件は不要である。

8.2.4. 最小機能強度根拠

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、攻撃方法は、公開インタフェース、公開情報、及びディスク解析ツール（市販されたツール）を利用したものとなる。低レベルの攻撃であれば、TOEが実施している対策である暗号化及び「登録済み本体デバイス」確認で対抗できるため、TOEのセキュリティ対策方針は低レベルの攻撃に対抗しているといえる。従って、TOEのセキュリティ対策方針が低レベルの攻撃者に対抗しているため、TOEのセキュリティ対策方針は最小機能強度SOF-基本と一貫している。

また、特定の機能要件(FIA_UAU.2、FIA_UAU.4、FIA_UID.2)の機能強度はSOF-基本であり、最小機能強度のSOF-基本と一貫している。

8.2.5. 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、低レベルの攻撃者による、HDD 盗難を原因としたデータ漏洩の脅威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。

8.3. TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』に示す。

表 8-5 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / セキュリティ機能要件	F.HDD_CRYPTO	F.KEY_MANAGE	F.KIT_CHECK
FCS_CKM.1		○	
FCS_COP.1	○		
FIA_UAU.2			○
FIA_UAU.4			○
FIA_UID.2			○
FPT_RVM.1	○	○	○

以下に、『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』の根拠を示す。

FCS_CKM.1

FCS_CKM.1 は、「FIPS 186-2」に合致する「FIPS186-2 に基づく暗号鍵生成アルゴリズム」により「256 ビット長の暗号鍵」を生成する機能要件である。F.KEY_MANAGE により、FIPS186-2 に基づく暗号鍵生成アルゴリズムを利用して、暗号鍵長 256 ビットの暗号鍵を生成するため、FCS_CKM.1 は実現されている。

FCS_COP.1

FCS_COP.1 は、「256 ビット長の暗号鍵」を使用して「FIPS PUB 197」に合致する「暗号アルゴリズム AES」により、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を行う機能要件である。F.HDD_CRYPTO により、256 ビット長の暗号鍵を使用して、FIPS PUB 197 に合致する AES アルゴリズムによって、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、FCS_COP.1 は実現されている。

FIA_UAU.2

FIA_UAU.2 は、TSF が登録済み本体デバイスを認証することを要求する機能要件である。F.KIT_CHECK により、TOE が、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チャレンジ＆レスポンス認証により確認するため、FIA_UAU.2 は実現されている。

FIA_UAU.4

FIA_UAU.4 は、TSF が「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機能要件である。F.KIT_CHECK により、「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」が、チャレンジ＆レスポンス認証処理として具体化して実現され、また、「認証データの再使用を防止する」に関しては、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ことにより実現されている。そのため、FIA_UAU.4 は実現されている。

FIA_UID.2

FIA_UID.2 は、TSF が利用される前に、TSF が登録済み本体デバイスを識別することを要求する機能要件である。F.KIT_CHECK により、HDD データ暗号化キット取り付け時にキヤノン複合機・プリンタから受け取った認証 ID を基に、チャレンジ＆レスポンス認証を行い、登録済み本体デバイスを識別している。そのため、FIA_UID.2 は実現されている。

FPT_RVM.1

FPT_RVM.1 は、TSP 実施機能がバイパスされずに必ず呼び出されることを保証する機能要件である。

F.HDD_CRYPTO により、HDD へのデータの書き込み、及び HDD からのデータの読み出しの経路を単一化し、データは必ず TOE である暗号化チップを介して暗号化/復号されるため、F.HDD_CRYPTO での TSP の非バイパス性が保証できる。

F.KEY_MANAGE により、物理的なスイッチである電源ボタンを押下したタイミングで、F.HDD_CRYPTO にて使用する暗号鍵を生成する。F.KEY_MANAGE に対して電源ボタン以外のインタフェースは存在せず、また、電源ボタンの使用方法は ON/OFF のみであるため、電源 ON の際に F.KEY_MANAGE を迂回することはできない。従って、F.KEY_MANAGE での TSP の非バイパス性が保証できる。

F.KIT_CHECK により、物理的なスイッチである電源ボタンを押下したタイミングで、チャレンジ＆レスポンス認証を実施する。なお、F.KIT_CHECK に対して電源ボタン以外のインタフェースは存在せず、また、電源ボタンの使用方法は ON/OFF のみであるため、電源 ON の際に F.KIT_CHECK を迂回することはできない。従って、F.KIT_CHECK での TSP の非バイパス性が保証できる。

8.3.2.　セキュリティ機能強度根拠

特定の TOE セキュリティ機能要件に対する機能強度は、FIA_UAU.2、FIA_UAU.4、FIA_UID.2 に対する機能強度である SOF-基本である。また、IT セキュリティ機能に対する機能強度は、F.KIT_CHECK に対する機能強度である SOF-基本である。そのため、特定の TOE セキュリティ機能要件に対する機能強度と、IT セキュリティ機能に対する機能強度は一貫している。

8.3.3.　保証手段根拠

表 6-1 に示した通り、全ての TOE セキュリティ保証要件は保証手段により示されたドキュメントのセットによって対応付けられる。

以下に、EAL3 の保証要件セットが各保証手段により満たされる根拠を示す。

ACM_CAP.3　許可の管理

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（１）
- キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（２）
- Canon MFP Security Chip 評価証拠一覧

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（１）」、「キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（２）」及び「Canon MFP Security Chip 評価証拠一覧」には、TOE のバージョンを識別するための命名規則、構成要素の一覧表、構成要素の一意の識別方法を規定する。そのため、保証要件 ACM_CAP.3 は満たされる。

ACM_SCP.1　TOE の CM 範囲

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（１）
- キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（２）
- Canon MFP Security Chip 評価証拠一覧

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（１）」、「キヤノン複合機・プリンタ用セキュリティチップ 構成管理計画・手順書（２）」及び「Canon MFP Security Chip 評価証拠一覧」には、TOE の構成要素の管理対象範囲を規定する。そのため、保証要件 ACM_SCP.1 は満たされる。

ADO_DEL.1　　配付手続き

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（１）
- キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（２）

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（１）」及び「キヤノン複合機・プリンタ用セキュリティチップ 配送手順書（２）」には、TOE をユーザサイトに配付する際に採用される、TOE の完全性を維持するための手続きを規定する。そのため、保証要件 ADO_DEL.1 は満たされる。

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

- 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）

【保証要件根拠】

保証手段である「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）」には、TOE をセキュアな構成にするために採用される、設置手順及び起動の確認方法を規定する。そのため、保証要件 ADO_IGS.1 は満たされる。

ADV_FSP.1　　非形式的機能仕様

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ ファームウェア外部仕様書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ ファームウェア外部仕様書」には、TOE のセキュリティ機能に対する全ての外部インタフェースの仕様を規定する。そのため、保証要件 ADV_FSP.1 は満たされる。

ADV_HLD.2　　セキュリティ実施上位レベル設計

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ ファームウェア上位レベル仕様書
- HERMIT ハードウェアマニュアル

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ ファームウェア上位

レベル仕様書」には、TSF をサブシステム単位に分割し、各サブシステムの仕様及び、サブシステム間インタフェースの仕様を規定する。また、「HERMIT ハードウェアマニュアル」には、ファームウェア開発のために必要なハードウェア情報を記載する。そのため、保証要件 ADV_HLD.2 は満たされる。

ADV_RCR.1　　非形式的対応の実証

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ ファームウェア表現対応表

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ ファームウェア表現対応表」には、TOE のセキュリティ機能の各レベル（要約仕様－機能仕様－上位レベル設計）での完全な対応を記述する。そのため、保証要件 ADV_RCR.1 は満たされる。

AGD_ADM.1　　管理者ガイダンス

【保証手段】

- HDD データ暗号化キット・B シリーズ　ユーザーズガイド
- HDD Data Encryption Kit-B Series　Reference Guide
- 別紙（注意書き）
- 別紙（Caution）

【保証要件根拠】

保証手段である「HDD データ暗号化キット・B シリーズ　ユーザーズガイド」、「HDD Data Encryption Kit-B Series　Reference Guide」、「別紙（注意書き）」、「別紙(Caution)」には、TOE の利用者が使用するインタフェース、TOE をセキュアに運用するための警告を含む使用方法、及び TOE の障害時に利用者が採るべきアクションについて規定する。そのため、保証要件 AGD_ADM.1 は満たされる。

AGD_USR.1　　利用者ガイダンス

【保証手段】

- HDD データ暗号化キット・B シリーズ　ユーザーズガイド
- HDD Data Encryption Kit-B Series　Reference Guide
- 別紙（注意書き）
- 別紙（Caution）

【保証要件根拠】

保証手段である「HDD データ暗号化キット・B シリーズ　ユーザーズガイド」、「HDD Data Encryption Kit-B Series　Reference Guide」、「別紙（注意書き）」、「別紙(Caution)」には、TOE の利用者が使用するインタフェース、及び TOE のセキュアな運用のための警

告を含む使用方法を規定する。そのため、保証要件 AGD_USR.1 は満たされる。

ALC_DVS.1　　セキュリティ手段の識別

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ ファームウェア開発セキュリティ規約

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ ファームウェア開発セキュリティ規約」には、TOE を保護するために開発環境で使用される、物理的、手続き的、人的、及びその他のセキュリティ手段を規定する。そのため、保証要件 ALC_DVS.1 は満たされる。

ATE_COV.2　　カバレージの分析

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ テストカバレージ分析書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ テストカバレージ分析書」には、TOE のセキュリティ機能及び外部インタフェースに対するテストの十分性及び完全性について記述する。そのため、保証要件 ATE_COV.2 は満たされる。

ATE_DPT.1　　テスト：上位レベル設計

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ テスト深さ分析書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ テスト深さ分析書」には、TOE のサブシステム及びサブシステム間インタフェースに対するテストの十分性及び完全性について記述する。そのため、保証要件 ATE_DPT.1 は満たされる。

ATE_FUN.1　　機能テスト

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ テスト仕様書
- キヤノン複合機・プリンタ用セキュリティチップ テスト手順書
- キヤノン複合機・プリンタ用セキュリティチップ テスト結果報告書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ テスト仕様書」、「キヤノン複合機・プリンタ用セキュリティチップ テスト手順書」及び「キヤノン複合機・

プリンタ用セキュリティチップ テスト結果報告書」には、TSF に対するテストの全体計画、テストを実施するための手順、及びテスト結果を記述する。そのため、保証要件 ATE_FUN.1 は満たされる。

ATE_IND.2　　独立テスト - サンプル

【保証手段】

- Canon MFP Security Chip 1.50

【保証要件根拠】

保証手段である「Canon MFP Security Chip 1.50」は、TOE のセキュリティ機能のテスト環境再現及びテスト資材を提供する。そのため、保証要件 ATE_IND.2 は満たされる。

AVA_MSU.1　　ガイダンスの検査

【保証手段】

- 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）
- HDD データ暗号化キット・B シリーズ　ユーザーズガイド
- HDD Data Encryption Kit-B Series　Reference Guide
- 別紙（注意書き）
- 別紙（Caution）

【保証要件根拠】

保証手段である「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)」、「HDD データ暗号化キット・B シリーズ　ユーザーズガイド」、「HDD Data Encryption Kit-B Series　Reference Guide」、「別紙（注意書き)」、「別紙(Caution)」には、TOE の利用者が、誤使用により TOE のセキュリティ機能を非セキュアな状態にしてしまう危険性の無いように TOE の使用方法を記述する。そのため、保証要件 AVA_MSU.1 は満たされる。

AVA_SOF.1　　TOE セキュリティ機能強度評価

【保証手段】

- キヤノン複合機・プリンタ用セキュリティチップ 脆弱性分析書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ 脆弱性分析書」には、TOE のセキュリティ機能のセキュリティメカニズムに対しての TOE セキュリティ機能強度分析について記述する。そのため、保証要件 AVA_SOF.1 は満たされる。

AVA_VLA.1　　開発者脆弱性分析

【保証手段】

・　キヤノン複合機・プリンタ用セキュリティチップ 脆弱性分析書

【保証要件根拠】

保証手段である「キヤノン複合機・プリンタ用セキュリティチップ 脆弱性分析書」には、TOE の意図する環境において、セキュリティ機能の脆弱性が悪用され得ないことについて記述する。そのため、保証要件 AVA_VLA.1 は満たされる。

8.4.　PP 主張根拠

本 ST が参照する PP はない。

（　最終ページ　）