EOS-1D Mark II ファームウェアセキュリティターゲット

Version 1.8
Date 2004 年 6 月 30 日
Author キヤノン(株) カメラ開発センター

更新履歴

Version	日付	変更内容
1.0	2004/01/26	第 1 版発行.
1.1	2004/02/25	表示機能の追加. 2004/02/20 発行 OR に対応.
1.2	2004/03/10	誤記修正.
1.3	2004/04/01	誤記修正.
1.4	2004/04/04	保証手段の更新. (public 版にバージョンを合わせるため)
1.5	2004/05/20	認証レビュー（CRV-T017-001）に対応. 保証手段の更新. 実情に合わせて 2 章を修正.
1.6	2004/06/07	8.2.4 節の記述を修正. 保証手段の更新. TOE 名称の変更. ヘッダーの変更.
1.7	2004/06/22	保証手段の更新.
1.8	2004/06/30	3 章の表現方法の見直し.

目次

1 ST 概説 1
1.1 ST 識別 1
1.2 ST 概要 1
1.3 CC 適合の主張 2
1.4 略語/用語の定義 2
2 TOE 記述 3
2.1 TOE の種別 3
2.2 TOE の概要 3
2.3 TOE の構成 5
2.3.1 TOE の物理的範囲 5
2.3.2 TOE の論理的範囲 7
2.3.3 TOE の利用者の役割 9
2.3.4 TOE の保護資産 9
3 TOE セキュリティ環境 10
3.1 前提条件 10
3.1.1 A.TAMPER 10
3.2 脅威 10
3.3 組織のセキュリティ方針 10
3.3.1 P.GEN_VD 10
3.3.2 P.SECURE_KEY 10
4 セキュリティ対策方針 11
4.1 TOE セキュリティ対策方針 11
4.1.1 O.GEN_VD 11
4.1.2 O.GEN_KEY 11
4.2 環境セキュリティ対策方針 11
4.2.1 OE.PHS_TAMPER 11
4.2.2 OE.LOG_TAMPER 11
5 IT セキュリティ要件 12
5.1 TOE セキュリティ要件 12
5.1.1 TOE セキュリティ機能要件 12
5.1.2 最小機能強度宣言 12
5.1.3 TOE セキュリティ保証要件 13
5.2 IT 環境のセキュリティ要件 13

6 TOE 要約仕様 14
6.1 IT セキュリティ機能 14
6.1.1 SF.GEN_DV 14
6.2 IT セキュリティ機能と機能要件の対応関係 14
6.3 機能強度主張 14
6.4 保証手段 15
7 PP 主張 16
8 根拠 17
8.1 セキュリティ対策方針の根拠 17
8.2 TOE セキュリティ要件の根拠 18
8.2.1 TOE の機能要件による TOE の対策方針の充足 18
8.2.2 依存性の根拠 19
8.2.3 セキュリティ要件の相互補完 20
8.2.4 最小機能強度主張の適合性の根拠 21
8.2.5 TOE 保証要件の妥当性 21
8.3 TOE 要約仕様の根拠 21
8.3.1 IT セキュリティ機能の根拠 21
8.3.2 IT セキュリティ機能のコンビネーション 22
8.3.3 機能強度の根拠 22
8.3.4 保証手段の根拠 22

1 ST 概説

本章では, ST 識別, ST 概要, CC 適合の主張, 略語/用語について記述する.

1.1 ST 識別

本章では ST の識別情報を記述する.

ST タイトル	EOS-1D Mark II ファームウェアセキュリティターゲット
ST バージョン	1.8
ST 発行日	2004 年 6 月 30 日
ST 発行者	キヤノン(株) カメラ開発センター
TOE タイトル	EOS-1D Mark II ファームウェア
TOE バージョン	1.0.1
キーワード	デジタルカメラ, 改ざん検出, 完全性, MAC, EAL2+.
CC のバージョン	ISO/IEC 15408-1:1999
	ISO/IEC 15408-2:1999
	ISO/IEC 15408-3:1999

(注) 日本語訳は「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 1-3 (平成 13 年 1 月翻訳第 1.2 版 情報処理振興事業協会セキュリティセンター)」を使用した. さらに, 「補足－0210 (独立行政法人製品評価技術基盤機構適合性評価センター)」を適用した.

1.2 ST 概要

本 ST は, EOS-1D Mark II と呼ばれるデジタルカメラ (以下, EOS デジタルカメラと示す) のファームウェアのセキュリティターゲットである. EOS デジタルカメラのファームウェアの提供するセキュリティ機能は以下のとおりである.

- 撮影画像である画像ファイルのオリジナル性を検証するための検証データを生成する機能.

本 ST の構成は以下のとおりである. 1 章は ST 概説として, ST 識別, ST 概要, CC 適合の主張および略語/用語について記述する. 2 章は TOE の種別, TOE の説明, TOE を含む構成について記述する. 3 章は TOE のセキュリティ環境について記述する. 4 章はセキュリティ対策方針について記述する. 5 章はセキュリティ要件を記述する. 6 章は TOE 要約仕様について記述する. 7 章は PP 主張について記述する. 8 章はセキュリティ対策方針根拠, IT セキュ

リティ要件根拠, TOE 要約仕様根拠について記述する.

1.3 CC 適合の主張

本 ST は, 以下の CC に適合する.

CC Part 2 適合.

CC Part 3 適合, EAL2 追加. EAL2 に ALC_DVS.1 を追加する.

補足－0210 適用.

また, 本 ST が適合している PP はない.

1.4 略語/用語の定義

本章では略語/用語を定義する.

CC：コモンクライテリア（Common Criteria）
EAL：評価保証レベル（Evaluation Assurance Level）
PP：プロテクションプロファイル（Protection Profile）
ST：セキュリティターゲット（Security Target）
TOE：評価対象（Target Of Evaluation）
MAC：メッセージ認証コード（Message Authentication Code）
FIPS：商務省連邦情報処理規格（The Federal Information Processing Standards）

2 TOE 記述

本章では, TOE の種別, TOE の説明, TOE を含む構成について記述する.

2.1 TOE の種別

TOE を含む製品の種別はデジタルカメラである. また, TOE は EOS デジタルカメラと呼ばれるデジタルカメラのファームウェアであり, TOE の種別は組込ソフトウェアである.

2.2 TOE の概要

銀塩写真は現像やプリントという手間が必要である一方で, デジタルカメラで撮影された画像はこれらの手間が必要ない. また, デジタルカメラで撮影された画像は, デジタルデータであるため, 経年劣化がなく, 保管や検索が容易であり, 通信回線を用いてデータを遠隔地に送信できる. これらの様々なメリットがあるため, デジタルカメラは多くの業務分野で利用されている. その例として, 事故車の破損状況を撮影し, 撮影された画像に基づいて事故査定に用いる損害保険業界, 建設現場での工事の進捗状況や仕様の確認のために建築物を撮影する建設業界が挙げられる. 国土交通省では既に土木工事現場の記録用にデジタルカメラで撮影された画像の使用を認めている.
しかし, デジタル化されることによるデメリットも指摘されている. それは, 市販されているフォトレタッチツール等を使用することで容易に加工や修正が出来るという特徴のために, 画像が証拠として扱われる事故の写真や報告書において, デジタルカメラで撮影した画像の信頼性が銀塩写真の画像と比較して低いという欠点である. 実際に, デジタルデータの加工の容易性を悪用し, 建築物の完成写真を改変することで不正に補助金を受給していた事件が発生している.
銀塩写真でも画像の改変を行うことは不可能ではないが, その改変を行うためのコストが改変で得られるコストよりも非常に大きいか, 画像の改変結果が不自然であることから実際には改変は行われにくく, それが証拠として採用される根拠になっている. したがって損害保険, 建設業界ではこの問題が将来大きな問題になることが懸念されており, このような欠点を克服するための仕組みが必要とされている.

EOS デジタルカメラは, このような背景を踏まえて開発された, 画像ファイルの完全性を検証可能なオリジナル性検証システムで利用されるデジタルカメラである.

初めにデジタルカメラとオリジナル性検証キットからなるオリジナル性検証システムの全体像を説明する. 図 2-1 にオリジナル性検証システムの全体像を示す.

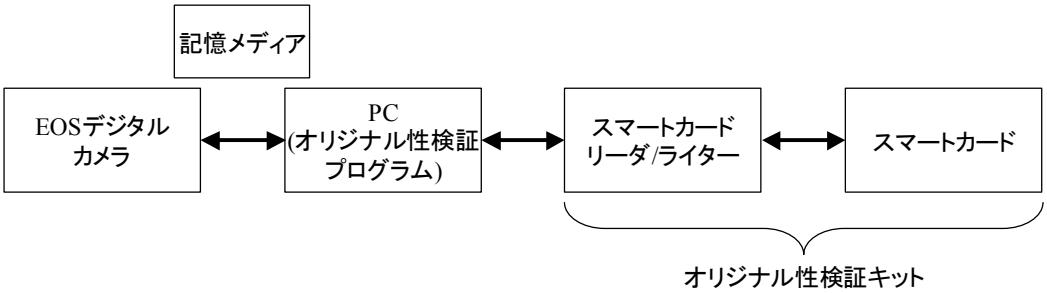

図 2-1 オリジナル性検証システム

オリジナル性検証システムは, EOS デジタルカメラ, PC（オリジナル性検証プログラムがインストールされた） およびオリジナル性検証キットから構成される．オリジナル性検証キットは, 当該 PC に接続されるスマートカードリーダ/ライターおよび当該スマートカードリーダ/ライターと接続されるスマートカードから構成される．なお, スマートカードは, スマートカードと同等の機能を持つ製品を含む．オリジナル性検証システムは, EOS デジタルカメラによって撮影された画像ファイルの完全性を検証することを目的とし, EOS デジタルカメラによって完全性を検証するための検証データを生成し, オリジナル性検証プログラムがインストールされた PC とオリジナル性検証キットを用い検証データに基づいて画像ファイルの完全性を検証する．つまり本システムは, EOS デジタルカメラによって撮影された画像ファイルが改ざんされるかもしれないという脅威に対して, EOS デジタルカメラと PC とオリジナル性検証キットのセットによって対抗している．画像ファイルの生成者が EOS デジタルカメラで検証データ付画像ファイルを生成し, 画像ファイルの検証者が PC およびオリジナル性検証キットで検証データ付画像ファイルの完全性を検証する．画像ファイルの生成者と画像ファイルの検証者は, 同一の場合も想定可能であるし, 異なる場合も想定可能である．本システムの応用によって異なる．
また本システムの対抗する脅威は, 画像ファイルの完全性だけである．本システムは, 画像ファイルの秘匿性や可用性の脅威を想定しておらず, 対抗しない．完全性の検証可能な画像ファイルは EOS デジタルカメラで撮影された画像ファイルだけであるが, EOS デジタルカメラによって撮影された全ての画像ファイルが完全性の検証可能な画像ファイルではない．完全性を検証したい画像ファイルだけが対象となる．つまり EOS デジタルカメラの利用者は, 画像ファイルを撮影するに先立ち, あらかじめ検証データを生成するか否かを選択する．

例として, 損害保険業界におけるオリジナル性検証システムの利用例を以下に示す．まず, 事故調査者は EOS デジタルカメラで事故現場の画像ファイル（事故写真）を撮影する．な

お, 事故調査者は, 検証データの生成することを選択した状態で撮影する. 損害保険会社は PC およびオリジナル性検証キットを保持する. 損害保険会社は前記事故調査者によって撮影された検証データ付画像ファイル（事故写真）を受信し, PC およびオリジナル検証キットによって受信した検証データ付画像ファイル（事故写真）の完全性を検証する. 完全性の検証に成功した場合, 損害保険会社は当該画像ファイル（事故写真）が確かに EOS デジタルカメラで撮影されたと推定する.

TOE はオリジナル性検証システムで利用される EOS デジタルカメラのファームウェアである. つまり, TOE は, オリジナル性検証システムにおける検証データの生成だけを担うデジタルカメラのファームウェアである. 本システム全体は第三者による画像ファイルの改ざんという脅威に対抗するが, 本 TOE だけでは画像ファイルの改ざんという脅威に対抗しない. つまり, 本 TOE は, 本システムで必要となる機能の一部, つまり画像ファイルの改ざんを検証するための検証データ生成という一部の機能だけを担う.

本システムで用いられている技術は次の特徴を持つ. 画像ファイルの検証データは鍵を用いて生成する. なお, 鍵は EOS デジタルカメラにそのまま保持されているのでなく, 鍵に関連する情報（以下, 鍵のシードと示す）という形式で EOS デジタルカメラに保持されている.

2.3 TOE の構成

2.3.1 TOE の物理的範囲

TOE と TOE のプラットフォームの物理的構成を図 2-2 に示す.

図 2-2 TOE を含む物理的構成

図 2-2 に示すように TOE を含む物理的構成はデジタルカメラである. TOE のプラットフォームはデジタルカメラを構成するハードウェアであって, デジタルカメラに挿入される記憶メディアやデジタルカメラに装着されるレンズを含まない. なお, 記憶メディアは外部

記憶メディアの総称であって，本デジタルカメラは CF（Compact Flash）カード，SD (Secure Digital）カードおよび PC へのダイレクト転送の 3 種類の記憶メディアを持つ．デジタルカメラの利用方法は，デジタルカメラのシャッターボタンや設定ダイヤル等から直接操作する方法と，デジタルカメラに接続した PC から操作する方法がある．図 2-3 にさらに詳細なデジタルカメラの構成を示す．

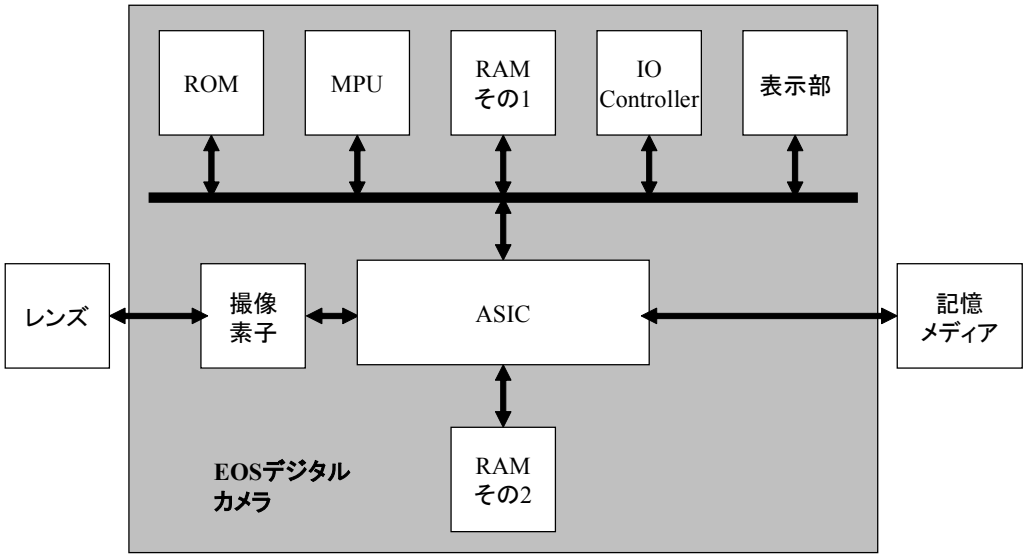

図 2-3 デジタルカメラの物理的構成

以下に各構成要素を説明する．

MPU	デジタルカメラ各部を制御する機能を担う演算処理チップである．
ROM	デジタルカメラを駆動するために必要なデータが記憶される読み出し専用メモリである．なお, ROM は上記 MPU 上で動作する基本ソフトウェア (Operating System）を含む．
RAM その 1	上記 MPU が使用する読み書き可能なメモリである．
IO Controller	デジタルカメラと PC 等の外部装置とが通信するための接続インタフェース，および利用者からの指示をカメラに伝えるためのシャッターボタンや設定ダイヤル等で構成される．
表示部	画像ファイル，各種設定値および状態を表示するための液晶モニタ，複数の表示パネルおよびビデオ出力端子である．
撮像素子	入力された光電荷量を電圧に変換するセンサである．
ASIC	撮像素子からの信号を基にしてノイズ除去し，画像ファイルを生成するための IC である．

RAM その 2　　上記 ASIC がデータ生成を行う時に用いる，読み書き可能なメモリである．

TOE の物理的境界は図 2-3 で示された MPU で実行するソフトウェア，つまりファームウェアである．表 2-1 に TOE を含む，つまりデジタルカメラの物理的構成要素の詳細を示す．

表 2-1 デジタルカメラの構成要素

識別情報	型番/バージョン
EOS デジタルカメラ本体ハードウェア	EOS-1DMK2
EOS-1D Mark II ファームウェア（TOE）	1.0.1

なお，EOS デジタルカメラ本体ハードウェアのバージョンを識別すると図 2-3 で示したデジタルカメラの詳細な構成要素は全て一意に特定可能である．

2.3.2 TOE の論理的範囲

TOE を含むデジタルカメラの論理的構成を図 2-4 に示す．

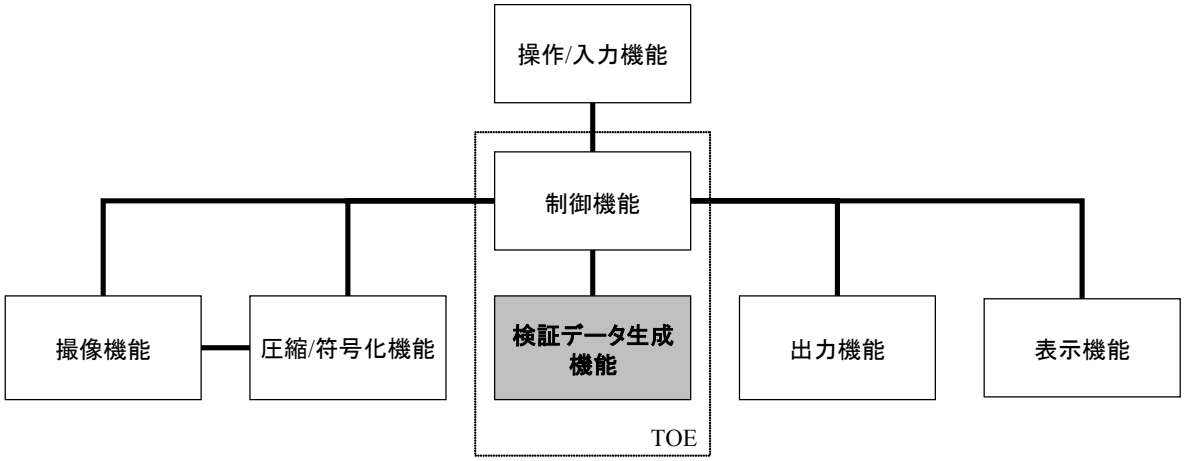

図 2-4 デジタルカメラの論理的構成

以下に各機能を説明する．

撮像機能　　撮像機能は，デジタルデータを生成する機能である．撮像素子で入力された光を画像データとしてデジタルカメラに取り込む機能である．さらに詳しく記述すると撮像素子の他に，不要な光を削除するためのフィルタ部や

撮像素子からの出力をデジタル化する変換部等に分類し記述することも可能である．しかし， 本TOEのセキュリティ機能とは無関係であるので，詳細は記述しない．

圧縮/符号化機能　圧縮/符号化機能は，撮像機能により EOS デジタルカメラに取り込まれたデジタルデータを圧縮アルゴリズムにより圧縮，さらには符号化することにより画像ファイルを生成する機能である．

操作/入力機能　操作/入力機能は，シャッターボタンや設定ダイヤル等を用いることで利用者が EOS デジタルカメラに指示を入力するための機能である．また，PC 等の外部装置とデジタルカメラとの間で行う通信機能も有する．操作/入力のために記憶メディアの画像ファイルを入力する場合があるが，検証データ生成のために画像ファイルを入力する機能は存在しない．

表示機能　表示機能は，表示部に EOS デジタルカメラで取り扱う画像ファイル，各種設定値および状態を表示する機能である．

出力機能　出力機能は，画像ファイルを特定の記憶メディアに記憶する機能である．検証データを付加する場合は，検証データ付画像ファイルを特定の記憶メディアに記憶し，検証データを付加しない場合は，検証データなし画像ファイルを特定の記憶メディアに記憶する．

検証データ生成機能
検証データ生成機能は，鍵を用いて画像ファイルの検証データを生成する機能である．本機能は，被検証データ（検証データなし画像ファイル）を入力し，検証データを出力する．また，検証データ生成機能は，鍵のシードから検証データ生成時に利用する鍵を生成する．

制御機能　制御機能は，撮像機能，圧縮/符号化機能，操作/入力機能，表示機能，出力機能および検証データ生成機能を制御する機能である．例えば，制御機能は，操作/入力機能によって撮影を指定した場合（例えば，シャッターボタンを押された場合）に，これらの機能を利用して，EOS デジタルカメラの利用者に，画像ファイルを提供する機能である．

なお，画像データは，撮影されたデジタルデータまたは当該デジタルデータが圧縮/符号化されたデジタルデータを示す．画像ファイルは，画像データに画像データの付属情報が付

加されたデジタルデータを示す.

次に, 図 2-4 に示されて論理的構成要素とそれらを実現している物理的構成要素の対応を表 2-2 に示す.

表 2-2 論理的構成要素と実現している物理的構成要素の対応

論理的構成要素	実現している物理的構成要素
撮像機能	撮像素子
圧縮/符号化機能	ASIC, RAM その 2
操作/入力機能	IO Controller
表示機能	表示部
出力機能	ASIC
検証データ生成機能	ファームウェア (TOE)
制御機能	ファームウェア (TOE)

図 2-4 および表 2-2 に示したとおり TOE であるファームウェアの機能は, 検証データ生成機能および制御機能である. また, 図 2-4 において影付きで示した検証データ生成機能はセキュリティ機能である.

2.3.3 TOE の利用者の役割

本 TOE を含む製品は EOS デジタルカメラである. したがって, EOS デジタルカメラの所有者は TOE の利用者である. さらに, 通常 EOS デジタルカメラの所有者は当該 EOS デジタルカメラの唯一の利用者であるため, EOS デジタルカメラの所有者を TOE の管理者とみなす. つまり, EOS デジタルカメラの所有者は TOE の利用者であり, TOE の管理者でもある. 以下, EOS デジタルカメラの所有者を利用者と呼ぶ.

2.3.4 TOE の保護資産

本 TOE の保護資産は, 以下の通りである.

鍵　　鍵は検証データの生成に用いる情報である. なお, 本 TOE は鍵をそのまま保持することはなく, 変換後の情報から変換前の情報を得ることを困難にするための難読化操作により変換された鍵のシードとして保持する.

3 TOE セキュリティ環境

本章では, TOE のセキュリティ環境について記述する.

3.1 前提条件

3.1.1 A.TAMPER

TOE の利用者は, 動作中におけるハードウェア的な直接攻撃から保護されており, かつ専用ソフトウェアだけインストール可能な EOS デジタルカメラを利用しなければならない.

3.2 脅威

本 ST は脅威を想定しない.

3.3 組織のセキュリティ方針

3.3.1 P.GEN_VD

TOE は, EOS デジタルカメラおよびオリジナル性検証キット等からなるオリジナル性検証システムにおいて画像ファイルの完全性を検証可能にするために, 画像ファイルの完全性を検証するための検証データを生成しなければならない. 特に, TOE は, 当該 EOS デジタルカメラで撮影した画像ファイルに対してだけ, 鍵を用いて検証データを生成しなければならない. さらに, 検証データは, 高度な専門知識を持たない悪意のある攻撃者によって不正に生成できないデータでなければならない.

3.3.2 P.SECURE_KEY

鍵はセキュアに保護されなければならない.

4 セキュリティ対策方針

本章では，セキュリティ対策方針について記述する．

4.1 TOE セキュリティ対策方針

4.1.1 O.GEN_VD

TOE は，当該 EOS デジタルカメラで撮影した画像ファイルに対してだけ，撮影した画像ファイルの完全性を検証するための，かつ高度な専門知識を持たない悪意のある攻撃者によって不正に生成できない検証データを生成する．なお，本 TOE は，検証データを生成するために記憶メディアから画像ファイルを読み取る機能を有さない．

4.1.2 O.GEN_KEY

TOE は，難読化操作の逆変換であって，手順の推測が困難な逆難読化操作により，鍵のシードから鍵を生成する．

4.2 環境セキュリティ対策方針

4.2.1 OE.PHS_TAMPER

TOE の利用者は，以下のハードウェア的特徴をもつ EOS デジタルカメラを利用しなければならない. EOS デジタルカメラのハードウェアは，専用ハードウェアであって, TOE の動作中におけるハードウェア的な直接攻撃から保護されなければならない．つまり，デジタルカメラのハードウェアは，専用回路構成および専用筐体構造を持ち，TOE の動作中において，ハードウェア的な直接攻撃によるデジタルカメラ内部の鍵へのアクセスから保護されなければならない．

4.2.2 OE.LOG_TAMPER

TOE の利用者は，以下のソフトウェア的特徴をもつ EOS デジタルカメラを利用しなければならない．EOS デジタルカメラのソフトウェアは，専用ハードウェア上の専用ソフトウェアであって，開発者が提供したソフトウェアだけインストール可能としなければならない．

5 IT セキュリティ要件

本章では, セキュリティ要件を記述する.

5.1 TOE セキュリティ要件

5.1.1 TOE セキュリティ機能要件

本章では, TOE セキュリティ機能要件について記述する. なお, 全てのセキュリティ機能要件は, CC Part 2 に規定のセキュリティ機能要件である.

5.1.1.1 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: 部門の独自標準]に合致する, 指定された暗号鍵生成アルゴリズム[割付: 部門の独自暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 128bits 以上の固定値]に従って, 暗号鍵を生成しなければならない.

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

5.1.1.2 FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 TSF は, [割付: FIPS PUB 198]に合致する, 特定された暗号アルゴリズム[割付: The Keyed-Hash Message Authentication Code]と暗号鍵長[割付: 128bits 以上の固定値]に従って, [割付: 画像ファイルに対する検証データの生成]を実行しなければならない.

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

5.1.2 最小機能強度宣言

本 TOE の最小機能強度レベルは SOF-基本とする.

なお, FCS_COP.1 は暗号アルゴリズムを利用したセキュリティ機能要件である. 暗号アルゴリズムの評価は CC 評価の対象ではない.

5.1.3 TOE セキュリティ保証要件

本章では, TOE セキュリティ保証要件について記述する. 本 TOE の評価保証レベルは EAL2 追加であり, EAL2 に ALC_DVS.1 のセキュリティ保証要件コンポーネントを追加する. 本 TOE のセキュリティ保証要件を表 5-1 に示す. なお, 全てのセキュリティ保証要件は, CC Part 3 に規定のセキュリティ保証要件である.

表 5-1 TOE セキュリティ保証要件コンポーネントの一覧

保証クラス	保証要件コンポーネント	
構成管理	ACM_CAP.2	構成要素
配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置, 生成, 及び立上げ手順
開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.1	記述的上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
テスト	ATE_COV.1	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト- サンプル
脆弱性評定	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.2 IT 環境のセキュリティ要件

本章では, IT 環境が提供するセキュリティ要件を記述する. 本 ST では IT 環境が提供するセキュリティ要件はない.

6 TOE 要約仕様

本章では, TOE 要約仕様について記述する.

6.1 IT セキュリティ機能

本章では, TOE の提供するセキュリティ機能を記述する.

6.1.1 SF.GEN_DV

本 SF は, 画像ファイルの有効性を保証として利用できる証拠として, 後述の鍵を用いて検証データを生成する. ただし, 本 TOE は, 検証データを生成する機能だけを保持しており, 有効性の証拠を検証する機能は保持しない. 検証データの生成アルゴリズムは, FIPS PUB 198 で規定された鍵長 (128bits 以上の固定値) の The Keyed-Hash Message Authentication Code である.
また, 本 SF は, 部門の独自の暗号鍵生成アルゴリズム, つまり逆難読化アルゴリズムを実行し, 鍵のシードから検証データを生成するための鍵を生成する. 鍵長は 128bits 以上の固定値である. 生成した鍵は揮発性の RAM に保持される.

6.2 IT セキュリティ機能と機能要件の対応関係

IT セキュリティ機能と TOE セキュリティ機能要件との対応関係を表 6-1 に示す.

表 6-1 IT セキュリティ機能とセキュリティ機能要件との対応

	FCS_CKM.1	FCS_COP.1
SF.GEN_DV	×	×

6.3 機能強度主張

確率的または順列的メカニズムによって実現される IT セキュリティ機能は, SF.GEN_DV である. SF.GEN_DV は機能強度レベル SOF-基本である.
なお, SF.GEN_DV は暗号アルゴリズムであるセキュアハッシュ関数を利用した IT セキュリティ機能である. 暗号アルゴリズムであるセキュアハッシュ関数のアルゴリズムは本機

能強度の対象としない.

6.4 保証手段

本章では, TOE セキュリティ保証手段を記述する. 表 6-2 に TOE セキュリティ保証手段を示す. これらの TOE セキュリティ保証手段は, 5.1.3 節で記述した TOE セキュリティ保証要件を満たす.

表 6-2 TOE セキュリティ保証手段と TOE セキュリティ保証要件の対応

TOE セキュリティ 保証手段	TOE セキュリティ 保証要件
EOS デジタルカメラ構成管理文書, ver 1.3, 2004/06/18	ACM_CAP.2
EOS デジタルカメラ配付手続文書, ver 1.4, 2004/06/18	ADO_DEL.1 ADO_IGS.1
EOS デジタルカメラファームウエア機能仕様書, ver 1.7, 2004/06/30	ADV_FSP.1
EOS デジタルカメラ上位レベル設計書, ver 1.5, 2004/06/30	ADV_HLD.1
EOS デジタルカメラ対応分析書, ver 1.6, 2004/06/30	ADV_RCR.1
EOS デジタルカメラ利用者ガイダンス, ver 1.2, 2004/04/26	AGD_ADM.1 AGD_USR.1
EOS デジタルカメラ開発セキュリティ文書, ver 1.2, 2004/05/20	ALC_DVS.1
EOS デジタルカメラテストドキュメント, ver 1.3, 2004/06/30	ATE_COV.1 ATE_FUN.1
EOS デジタルカメラ (TOE)	ATE_IND.2
EOS デジタルカメラ脆弱性ドキュメント, ver 1.2, 2004/06/30	AVA_SOF.1 AVA_VLA.1

7 PP 主張

本章では, PP 主張について記述する. 本 ST は, PP への適合を主張しない.

8 根拠

本章では，セキュリティ対策方針根拠, IT セキュリティ要件根拠, TOE 要約仕様根拠について記述する.

8.1 セキュリティ対策方針の根拠

セキュリティ対策方針と前提条件，または脅威，または組織のセキュリティ方針で記述された TOE セキュリティ環境の対応関係を表 8-1 に示す.

表 8-1 セキュリティ対策方針と前提条件，脅威，組織のセキュリティ方針の対応

	A.TAMPER	P.GEN_VD	P.SECURE_KEY
O.GEN_VD		×	
O.GEN_KEY			×
OE.PHS_TAMPER	×		×
OE.LOG_TAMPER	×		×

表 8-1 により，各セキュリティ対策方針は 1 つ以上の TOE セキュリティ環境に対応していることが分かる.

次に，各 TOE セキュリティ環境に対して，セキュリティ対策方針が当該 TOE セキュリティ環境を満たしていることを示す.

A.TAMPER は，OE.PHS_TAMPER および OE.LOG_TAMPER によって対抗される. OE.PHS_TAMPER によって, EOS デジタルカメラのハードウェアは，専用ハードウェアであって，TOE の動作中におけるハードウェア的な直接攻撃から保護されることを実現する. OE.LOG_TAMPER によって，EOS デジタルカメラのソフトウェアは，専用ハードウェア上の専用ソフトウェアであって，開発者が提供したソフトウェアだけインストール可能とすることによって，開発者が提供したソフトウェア以外のソフトウェアから保護されていることを実現する. さらに, OE.PHS_TAMPER および OE.LOG_TAMPER によって, TOE

の利用者は，上記ハードウェア的特徴およびソフトウェア的特徴をもつ EOS デジタルカメラを使用しなければならない．したがって, OE.PHS_TAMPER および OE.LOG_TAMPER は A.TAMPER を満たしている．

P.GEN_VD は, O.GEN_VD によって対抗される. O.GEN_VD によって, TOE は，当該 EOS デジタルカメラで撮影した画像ファイルに対してだけ，撮影した画像ファイルの完全性を検証するための，かつ高度な専門知識を持たない悪意のある攻撃者によって不正に生成できない検証データを生成することを実現する．したがって, O.GEN_VD は P.GEN_VD を満たしている．なお，本 TOE は，検証データを生成するために記憶メディアから画像ファイルを読み取る機能を有さない．したがって，被検証データを撮影した画像ファイルに限定している．

P.SECURE_KEY は, O.GEN_KEY, OE.PHS_TAMPER および OE.LOG_TAMPER によって対抗される. O.GEN_KEY によって, TOE は，鍵のシードから逆難読化操作により鍵を生成している．さらに，OE.PHS_TAMPER によって，デジタルカメラのハードウェアは，TOE の動作中において，ハードウェア的な直接攻撃によって，デジタルカメラ内部の鍵へのアクセスから保護されなければならない. OE.LOG_TAMPER によって，デジタルカメラのソフトウェアは，開発者が提供したソフトウェア以外のソフトウェアによるデジタルカメラ内部の鍵へのアクセスから保護されなければならない．したがって，O.GEN_KEY, OE.PHS_TAMPER および OE.LOG_TAMPER は P.SECURE_KEY を満たしている．

8.2 TOE セキュリティ要件の根拠

8.2.1 TOE の機能要件による TOE の対策方針の充足

TOE セキュリティ機能要件は, TOE セキュリティ対策方針に対抗するための機能要件である. TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 8-2 に示す．

表 8-2 TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応

	O.GEN_VD	O.GEN_KEY
FCS_CKM.1		×
FCS_COP.1	×	

表 8-2 により，各 TOE セキュリティ機能要件は 1 つ以上の TOE セキュリティ対策方針に対応していることが分かる．

次に，各 TOE セキュリティ対策方針に対して，TOE セキュリティ機能要件が当該 TOE セキュリティ対策方針を満たしていることを示す.

O.GEN_VD は，FCS_COP.1 によって対抗される．FCS_COP.1 によって，TSF は，FIPS PUB 198 で規定された The Keyed-Hash Message Authentication Code にしたがって検証データを生成する機能を実現する．また，The Keyed-Hash Message Authentication Code で用いられる鍵長は 128bits 以上の固定値である．したがって，FCS_COP.1 は O.GEN_VD を満たしている.

O.GEN_KEY は，FCS_CKM.1 によって対抗される．FCS_CKM.1 によって，TSF は，部門の独自標準に合致する，部門の独自暗号鍵生成アルゴリズムによって鍵のシードから鍵を生成する機能を実現する．したがって，FCS_CKM.1 は O.GEN_KEY を満たしている.

8.2.2 依存性の根拠

TOE のセキュリティ要件の依存性を表 8-3 に示す．表中の「*」は除去された依存のあるセキュリティ要件を表し，「!」は選択可能なセキュリティ要件の中から選択したセキュリティ要件を表す.

表 8-3 TOE セキュリティ要件の依存性

TOE セキュリティ要件	依存性のあるセキュリティ要件
FCS_CKM.1	[FCS_CKM.2 or !FCS_COP.1], *FCS_CKM.4, *FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 or !FCS_CKM.1], *FCS_CKM.4, *FMT_MSA.2
ACM_CAP.2	なし
ADO_DEL.1	なし
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	なし
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_DVS.1	なし
ATE_COV.1	ADV_FSP.1, ATE_FUN.1
ATE_FUN.1	なし
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1

TOE セキュリティ要件	依存性のあるセキュリティ要件
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

表 8-3 より, TOE セキュリティ要件は, 後述する例外を除き, 必要な依存性を満たしている. 依存性を満たしていない根拠を以下に記述する.

FCS_CKM.1 は, FCS_CKM.4 および FMT_MSA.2 へのいずれの依存関係も満たしていない. しかし, 本 TOE は FCS_CKM.1 で生成した鍵を揮発性の RAM 上だけに保持する. また, 鍵は TOE が動作中は保持し続けており, TOE が非動作時だけ鍵を破棄する. TOE 非動作時の鍵破棄は, 揮発性の RAM の物理的な性質を利用した手段であって, IT 機能ではない. また, 本 TOE は鍵のセキュリティ属性を保持していない. したがって, 本 TOE において FCS_CKM.4 および FMT_MSA.2 への依存性は必要ない.

FCS_COP.1 は, FCS_CKM.4 および FMT_MSA.2 へのいずれの依存関係も満たしていない. FCS_CKM.1 から FCS_CKM.4 への依存性の除去で示したように, 鍵破棄は揮発性の RAM の物理的な性質を利用した手段であって, IT 機能で実現していない. また, TOE は鍵のセキュリティ属性を保持していない. したがって, 本 TOE において FCS_CKM.4 および FMT_MSA.2 への依存性は必要ない.

8.2.3 セキュリティ要件の相互補完

8.2.2 節より, TOE セキュリティ機能要件は, 一部の例外を除き, それぞれと依存関係のあるセキュリティ機能要件と相互補完している.

また, 明示的な依存性はないが, 以下の観点からセキュリティ機能要件の相互補完を記述する.
本 TOE は, ユーザデータのアクセス制御またはフロー制御をセキュリティ機能とせず, FDP_ACC.1 または FDP_IFC.1, いずれのセキュリティ機能要件も選択していない. つまり, 本 TOE は TOE 内部に不正なサブジェクトを想定しない. したがって, FPT_RVM.1 および FPT_SEP.1 などのセキュリティ機能要件のバイパスや改ざん防止のセキュリティ機能要件を選択する必要はない.
本 TOE の FCS_CKM.1 で生成する鍵はセキュリティ属性を保持しない. したがって, FCS_CKM.1 に関して, 本 TOE は鍵のセキュリティ属性変更等の管理機能を持たない. また, FCS_COP.1 に関しても, 本 TOE は管理機能を持たない. したがって, FMT_MOF.1 などのセキュリティ機能要件の非活性化を防止するセキュリティ機能要件を選択する必要はない.
さらに FAU クラスなど, 他のセキュリティ機能要件の無効化を狙った検出を可能にする必

要はない.

8.2.4 最小機能強度主張の適合性の根拠

本 TOE を含む検証データの生成と検証というトータルなセキュリティ機能は，コマーシャルシステムで利用されることを想定している．当該トータルなセキュリティ機能は，画像ファイルの完全性を検証可能にする機能であり，経済的価値のある情報を直接取り扱う機能でない.

上記の背景から，本 TOE は，4.1.1 節に示したように，高度な専門知識を持たない攻撃者を想定している．また，4.2 節に示したように，ハードウェア的な直接攻撃や他のソフトウェアからの攻撃は環境でカバーされている.

以上のように，本 TOE が対抗すべきなのは低レベルな攻撃者である．したがって，最小機能強度レベルは SOF-基本が妥当である.

8.2.5 TOE 保証要件の妥当性

本 TOE は，8.2.4 節で述べたように，低レベルな攻撃者を想定している．当該低レベルな攻撃者の想定と，コスト的または時間的な投資の観点から EAL2 が妥当である．ただし，本 TOE では，運用時に必要となる鍵を開発段階で安全に生成し，鍵および鍵の生成に関する情報を安全に管理する必要がある．したがって，EAL2 に開発セキュリティ（ALC_DVS.1）を追加することが妥当である.

8.3 TOE 要約仕様の根拠

8.3.1 IT セキュリティ機能の根拠

IT セキュリティ機能と TOE セキュリティ機能要件との対応関係を表 8-4 に示す.

表 8-4 IT セキュリティ機能とセキュリティ機能要件との対応その 2

	FCS_CKM.1	FCS_COP.1
SF.GEN_DV	×	×

表 8-4 により, IT セキュリティ機能は 1 つ以上の TOE セキュリティ機能要件に対応していることが分かる.

次に，各 TOE セキュリティ機能要件に対して，IT セキュリティ機能が当該 TOE セキュリティ機能要件を満たしていることを示す．

FCS_CKM.1 は，SF.GEN_DV によって対抗される．SF.GEN_DV は，部門の独自の暗号鍵生成アルゴリズム，つまり逆難読化アルゴリズムを実行し，鍵のシードから検証データを生成するための鍵を生成する．なお，鍵長は 128bits 以上の固定値である．したがって，SF.GEN_DV は FCS_CKM.1 を満たしている．

FCS_COP.1 は，SF.GEN_DV によって対抗される．SF.GEN_DV は，検証データを FIPS PUB 198 で規定された The Keyed-Hash Message Authentication Code にしたがって生成する．また，The Keyed-Hash Message Authentication Code で用いる鍵は 128bits 以上の固定値長の鍵である．したがって，SF.GEN_DV は FCS_COP.1 を満たしている．

8.3.2 IT セキュリティ機能のコンビネーション

表 8-4 から，本 TOE は唯一の IT セキュリティ機能を持つ．したがって，IT セキュリティ機能のコンビネーションに関する考察は必要ない．

8.3.3 機能強度の根拠

本 TOE において，確率的または順列的メカニズムによって実現される IT セキュリティ機能は，SF.GEN_DV である．この IT セキュリティ機能の機能強度は，6.3 節において，SOF-基本と記述している．また，本 TOE の最小機能強度は，5.1.2 節において，SOF-基本と記述している．これらの記述は一貫している．

8.3.4 保証手段の根拠

TOE セキュリティ保証手段と TOE セキュリティ保証要件との対応関係を表 8-5 に示す．

表 8-5 TOE セキュリティ保証手段と TOE セキュリティ保証要件の対応その 2

TOE セキュリティ 保証手段	TOE セキュリティ 保証要件
EOS デジタルカメラ構成管理文書, ver 1.3, 2004/06/18	ACM_CAP.2
EOS デジタルカメラ配付手続文書, ver 1.4, 2004/06/18	ADO_DEL.1 ADO_IGS.1
EOS デジタルカメラファームウエア機能仕様書，ver 1.7, 2004/06/30	ADV_FSP.1
EOS デジタルカメラ上位レベル設計書, ver 1.5, 2004/06/30	ADV_HLD.1

TOE セキュリティ 保証手段	TOE セキュリティ 保証要件
EOS デジタルカメラ対応分析書, ver 1.6, 2004/06/30	ADV_RCR.1
EOS デジタルカメラ利用者ガイダンス, ver 1.2, 2004/04/26	AGD_ADM.1 AGD_USR.1
EOS デジタルカメラ開発セキュリティ文書, ver 1.2, 2004/05/20	ALC_DVS.1
EOS デジタルカメラテストドキュメント, ver 1.3, 2004/06/30	ATE_COV.1 ATE_FUN.1
EOS デジタルカメラ（TOE）	ATE_IND.2
EOS デジタルカメラ脆弱性ドキュメント, ver 1.2, 2004/06/30	AVA_SOF.1 AVA_VLA.1

表 8-5 により, TOE セキュリティ保証手段は 1 つ以上の TOE セキュリティ保証要件に対応していることが分かる.

次に, 各 TOE セキュリティ保証要件に対して, TOE セキュリティ保証手段が当該 TOE セキュリティ保証要件を満たしていることを示す.

ACM_CAP.2 は, 以下の文書によって対抗される.

- EOS デジタルカメラ構成管理文書, ver 1.3, 2004/06/18

本文書は, TOE のバージョン, TOE の構成要素を記述した構成リスト, 構成要素の一意に識別する方法を記述している. したがって, 上記文書は ACM.CAP.2 を満たしている.

ADO_DEL.1 および ADO_IGS.1 は, 以下の文書によって対抗される.

- EOS デジタルカメラ配付手続文書, ver 1.4, 2004/06/18

本文書は, TOE を利用者サイトへ配送するときにセキュリティを維持するために必要なすべての手続き, および TOE のセキュアな設置, 生成, 及び立上げのために必要な手順を記述している. したがって, 上記文書は ADO_DEL.1 および ADO_IGS.1 を満たしている.

ADV_FSP.1 は, 以下の文書によって対抗される.

- EOS デジタルカメラファームウエア機能仕様書, ver 1.7, 2004/06/30

本文書は, TSF およびその外部インタフェースを記述している. したがって, 上記文書は ADV_FSP.1 を満たしている.

ADV_HLD.1 は, 以下の文書によって対抗される.

- EOS デジタルカメラ上位レベル設計書, ver 1.5, 2004/06/30

本文書は，サブシステムの観点から TSF の構造を記述し，当該サブシステムによって提供されるセキュリティ機能性を記述している．本文書は，当該サブシステムのインタフェースを識別している．さらに，TSF が必要とするすべての下層ハードウェアおよびソフトウェアなどの補助的な機能を記述している．したがって，上記文書は ADV_HLD.1 を満たしている．

ADV_RCR.1 は，以下の文書によって対抗される．

- EOS デジタルカメラ対応分析書, ver 1.6, 2004/06/30

本文書は，提供する TSF 表現の隣接するすべての組間の対応分析を記述している．したがって，上記文書は ADV_RCR.1 を満たしている．

AGD_ADM.1 および AGD_USR.1 は，以下の文書によって対抗される．

- EOS デジタルカメラ利用者ガイダンス, ver 1.2, 2004/04/26

EOS デジタルカメラにおいては，EOS デジタルカメラの所有者を，TOE の利用者および TOE の管理者とみなす．したがって，EOS デジタルカメラの所有者向けの本文書は，TOE の利用者の観点からおよび TOE の管理者の観点から機能とインタフェースを記述している．したがって，上記文書は AGD_ADM.1 および AGD_USR.1 を満たしている．

ALC_DVS.1 は，以下の文書によって対抗される．

- EOS デジタルカメラ開発セキュリティ文書, ver 1.2, 2004/05/20

本文書は，開発環境のなかで TOE の設計及び実装の機密性や完全性を保護するために必要となる，物理的，手続き的，人的，及びその他の手段を記述している．したがって，上記文書は ALC_DVS.1 を満たしている．

ATE_COV.1 および ATE_FUN.1 は，以下の文書によって対抗される．

- EOS デジタルカメラテストドキュメント, ver 1.3, 2004/06/30

本文書は，テスト証拠資料で識別されたテストと機能仕様に記述された TSF との対応を記述している．さらに本文書は，テスト計画，テスト手順記述，期待されるテスト結果，実際のテスト結果を記述している．したがって，上記文書は ATE_COV.1 および ATE_FUN.1 を満たしている．

ATE_IND.2 は，以下によって対抗される．

- EOS デジタルカメラ（TOE）

上記は，テストに適した TOE である．したがって，上記は ATE_IND.2 を満たしている．

AVA_SOF.1 および AVA_VLA.1 は，以下の文書によって対抗される．

- EOS デジタルカメラ脆弱性ドキュメント, ver 1.2, 2004/06/30

本文書は，機能強度主張を有するものとして識別された各メカニズムに対し，TOE セキュリティ機能強度分析を記述している．また，本文書は，脆弱性分析を記述している．したがって，上記文書は AVA_SOF.1 および AVA_VLA.1 を満たしている．

