認　証　報　告　書

評価対象

申請受付年月日（受付番号）	**平成16年1月26日（IT認証4023）**
認証申請者	**キヤノン株式会社**
TOE**の名称**	EOS-1D Mark II **ファームウェア**
TOE**のバージョン**	Ver.1.0.1
PP**適合**	**なし**
適合する保証要件	EAL2+ ALC_DVS.1
TOE**開発者**	**キヤノン株式会社カメラ開発センター**
評価機関の名称	**株式会社電子商取引安全技術研究所評価センター**

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16年7月21日

独立行政法人情報処理推進機構
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　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology - Security techniques - Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 ― 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法
⑤ Common Methodology for Information Technology Security Evaluation Version 1.0
⑥ CCIMB Interpretation-0210
⑦ 認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「EOS-1D Mark II ファームウェア Ver.1.0.1」は、独立行政法人情報処理推進機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 3
1.2.4 TOEの機能 3
1.3 評価の実施 5
1.4 評価の認証 5
1.5 報告概要 6
1.5.1 PP適合 6
1.5.2 EAL 6
1.5.3 セキュリティ機能強度 6
1.5.4 セキュリティ機能 6
1.5.5 脅威 6
1.5.6 組織のセキュリティ方針 7
1.5.7 構成条件 7
1.5.8 操作環境の前提条件 7
1.5.9 製品添付ドキュメント 8
2 評価機関による評価実施及び結果 9
2.1 評価方法 9
2.2 評価実施概要 9
2.3 製品テスト 9
2.3.1 開発者テスト 9
2.3.2 評価者テスト 11
2.4 評価結果 13
3 認証実施 13
4 結論 13
注意事項 17
5 用語 18
6 参照 19

1 全体要約

1.1 はじめに

この認証報告書は、「EOS-1D Mark II ファームウェア Ver.1.0.1」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所評価センター（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。

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:	EOS-1D Mark II
開発者:	キヤノン株式会社

1.2.2 製品概要

本製品は、TOEであるデジタルカメラのファームウェアが組み込まれたEOS-1D Mark II（以下、EOSデジタルカメラと呼ぶ）である。

デジタルカメラで撮影された画像は、従来の銀塩写真と異なり、現像やプリントの手間が不要、経年劣化がない、保管や検索が容易、通信回線を用いたデータ転送といった様々なメリットがある。一方、画像データのデジタル化により、市販のフォトレタッチツール等により容易に画像データを加工、修正することができてしまうというデメリットが発生する。建設業界で工事の進捗状況や仕様の確認のためにデジタルカメラの画像を使用する場合等、デジタルカメラで撮影した画像データを証拠資料として利用する場合には、画像データのオリジナル性が問題になる。

TOEであるファームウェアは、EOSデジタルカメラで撮影された画像ファイルのオリジナル性を検証するために必要な検証データの生成を行う機能を提供する。

画像データのオリジナル性の検証は、EOSデジタルカメラ、オリジナルデータ確認

キット（オリジナル性検証プログラム、スマートカードリーダ/ライター、スマートカード）及びPCで構成するオリジナル性検証システムで実施される。オリジナル性検証の動作概要を以下に示す。

① EOSデジタルカメラは、検証用の鍵を生成し、撮影した画像ファイルと生成した鍵を使用して検証データを生成する（検証データはTOEであるファームウェアが生成）
② 検証データが付加された画像ファイルをPCに読み込む
③ オリジナル性検証プログラムにおいて、読み込んだ画像ファイルの一覧からオリジナル性を検証する画像ファイルを選択する
④ スマートカードにおいて、③で選択した画像ファイルをもとに検証用の鍵が生成され、生成した鍵と選択した画像ファイルを使用して検証データを生成する
⑤ EOSデジタルカメラが生成した検証データと、スマートカードで生成された検証データを比較することで画像ファイルのオリジナル性を検証する

オリジナル性検証システムのイメージを図1に示す。

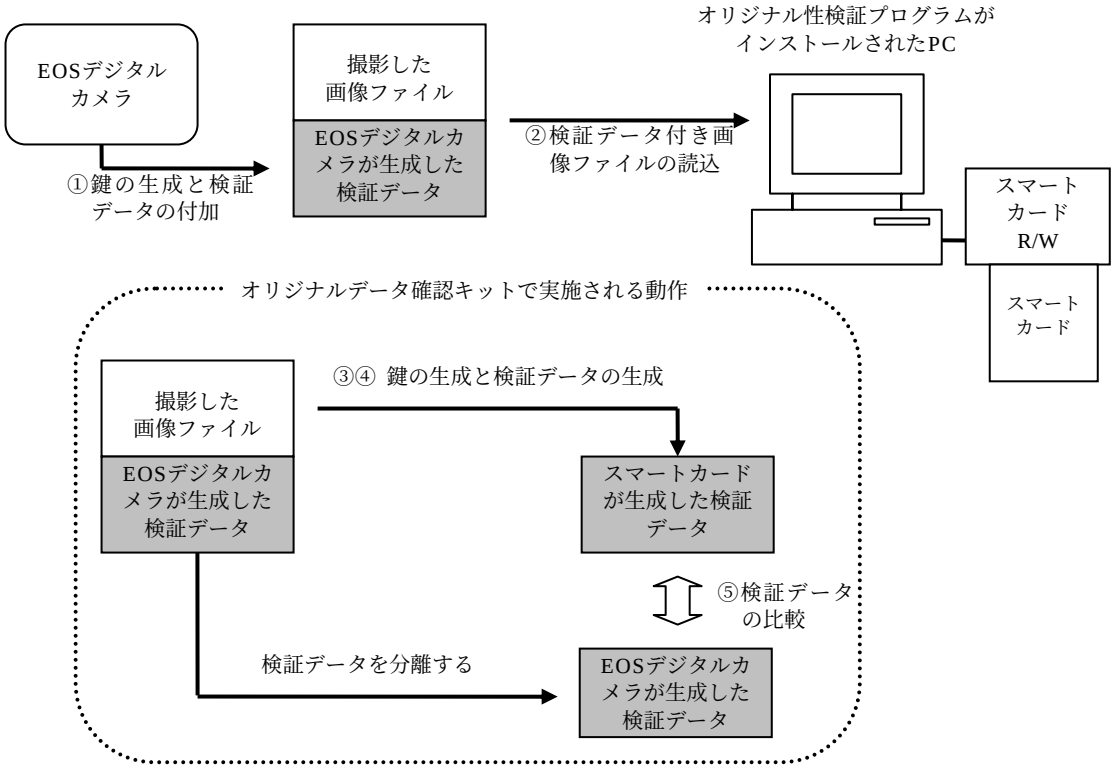

図1　オリジナル性検証システムのイメージ

1.2.3 TOEの範囲と動作概要

TOEの構成イメージを図2に示す。

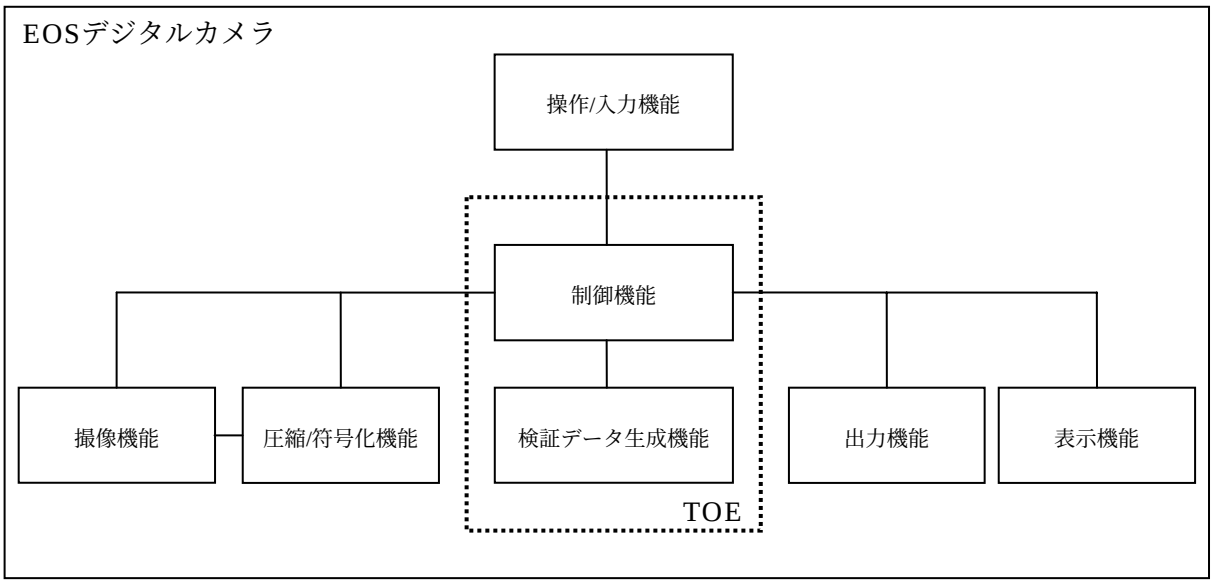

図2　TOEの構成イメージ

TOEは、EOSデジタルカメラに組み込まれた「EOS-1D Mark II ファームウェア Ver.1.0.1」である。

TOEである「EOS-1D Mark II ファームウェア Ver.1.0.1」は、セキュリティ機能として「検証データ生成機能」を持つ。「制御機能」はセキュリティ機能ではない。

検証データを付加した画像を撮影する場合の動作例を以下に示す。

- 利用者は、EOSデジタルカメラにおいて検証データを付加させるための設定を行い、シャッターボタンを押す（表示機能、操作/入力機能、制御機能）
- 入力された光を画像データとして取り込み、圧縮、符号化を行い、画像ファイルを生成する（撮像機能、圧縮/符号化機能、制御機能）
- 生成された画像ファイルをもとに検証データが生成され、検証データ付の画像データが記憶メディアに出力される。（検証データ生成機能、出力機能、制御機能）

1.2.4 TOEの機能

TOEは、「検証データ生成機能」、「制御機能」から構成される。

(1) 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。

(2) 制御機能（セキュリティ機能ではない）

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、及び検証データ生成機能を制御する機能である。制御機能が各機能を制御することにより画像の撮影、検証データの生成等が可能になる。

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セキュリティ認証申請等の手引き (平成15年10月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項 (平成14年4月)」[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「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」(以下「本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][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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、「EOS-1D Mark II ファームウェア ver.1.0.1 評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21]）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、本評価報告書、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16年6月の評価機関による本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

本STが規定するTOEの評価保証レベルは、EAL2追加（ALC_DVS.1を追加）である。

1.5.3 セキュリティ機能強度

検証データの生成メカニズムにより生成される検証データに対して、最小機能強度としてSOF-基本を主張する。

本TOEを含むオリジナル性検証システムが持つ画像ファイルのオリジナル性検証機能は、コマーシャルシステムで利用されることを想定しており、特定の経済的価値の高い情報を扱うことを想定していない。このような背景から、本TOEは高度な専門知識を持たない攻撃者を想定している。従って、TOEとして考慮すべき最小機能強度はSOF-基本で適切と判断された。

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。

(1) SF.GEN_DV

画像ファイルのオリジナル性を保証するための証拠として、鍵を用いて検証データを生成する。検証データの生成アルゴリズムは、FIPS PUB198で規定された鍵長（128bits以上の固定値）のThe Keyed-Hash MessageAuthentication Codeである。検証データ生成に使用する鍵は、開発者独自の暗号鍵生成アルゴリズム（逆難読化アルゴリズム）により、鍵のシードから生成される。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。

1.5.5 脅威

本TOEは、脅威を想定しない。

1.5.6 組織のセキュリティ方針

組織のセキュリティ方針を表に示す。

表1　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.GEN_VD	TOEは、EOSデジタルカメラ及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。
P.SECURE_KEY	鍵は、セキュアに保護されなければならない。

1.5.7 構成条件

本TOEは、EOSデジタルカメラに組み込まれるファームウェアである。

TOEが持つセキュリティ機能により画像データに付加される検証データは、オリジナルデータ確認キット（DVK-E2）及び検証作業を行うPCで構成されるオリジナル性検証システムにおいて利用される。

TOEが持つセキュリティ機能を有効にするためには、EOSデジタルカメラのパーソナルファンクション「P.Fn-31」を「ON」に設定する必要がある。

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有する前提条件を表2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2　TOE使用の前提条件

識別子	前提条件
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。

1.5.9 製品添付ドキュメント

本製品に添付されるドキュメントを以下に示す。

- EOS-1D Mark II DIGITAL 使用説明書,CT1-5158-000,2004年2月
- EOS-1D Mark II DIGITAL EOS DIGITAL Solution Disk ソフトウェア使用説明書,CT1-5159-001,2004年2月

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パート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成16年1月に始まり、平成16年6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、セキュリティ機能が仕様どおりに機能することを実証するために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システムの構成を図3に示す。

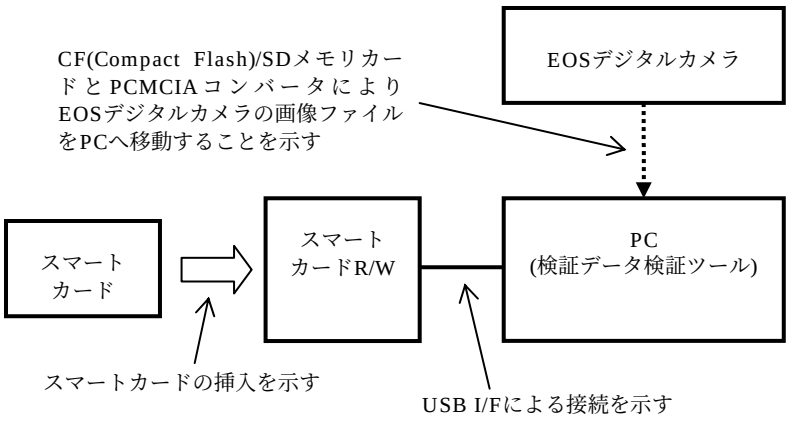

図3　開発者テスト環境

(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構成を図3に示す。

- EOSデジタルカメラ（型番：EOS-1DMK2）
- ファームウェアバージョン1.0.1（EOSデジタルカメラに組み込まれている）
- スマートカード（セキュアモバイルカード、オリジナルデータ確認キットDVK-E2同梱物）
- スマートカード（セキュアモバイルカード、テスト用に不正な鍵を格納したもの）
- スマートカードR/W（オリジナルデータ確認キットDVK-E2同梱物）
- 検証データ検証ツール（オリジナルデータ確認キットDVK-E2同梱物であるオリジナル性検証プログラムと同仕様）
- CF（Compact Flash）、SDメモリカード、PCMCIAコンバータ（デジタルカメラからPCへの画像の取り込みに使用）

開発者テストは、STにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

開発者はテストを実施するにあたり、次のテスト方針／テスト手法を設定している。

① EOSデジタルカメラのシャッターボタンを押下し、検証データ付き画像ファイルを生成させることによりセキュリティ機能の動作を確認する

② テストを実行したときの実際のテスト結果と、期待されるふるまいを比

較して、テストの目標が達成されたか否かを決定する

c.実施テストの範囲

開発者テストは、EOSデジタルカメラのシャッターボタンを押下し検証データ付き画像ファイルを生成させることにより、機能仕様書に記述されているすべてのセキュリティ機能（鍵の生成、検証データの生成）が確認できるようにテスト項目を設定している。開発者の実施したテストを以下に示す。

- EOSデジタルカメラで検証データ付きの画像ファイルを生成し、その画像ファイルを検証データ検証ツールとスマートカード（オリジナルデータ確認キットDVK-E2同梱物、正しい鍵が格納される）を使用してオリジナル性の検証を行う。検証データ検証ツールにおいて、画像ファイルがオリジナルであると判定されることを確認する
- EOSデジタルカメラで検証データ付きの画像ファイルを撮影し、その画像ファイルを検証データ検証ツールとスマートカード（テスト用に不正な鍵を格納したもの）を使用してオリジナル性の検証を行う。検証データ検証ツールにおいて、画像ファイルがオリジナルではないと判定されることを確認する

評価者は、開発者テストがすべてのセキュリティ機能を考慮していることは確認した。しかし、テスト内容が間接的にセキュリティ機能を動作させるテスト内容だけであり、セキュリティ機能の動作を保証するためにはテストが不足していると判断し、評価者テストとして追加のテストを実施している。

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システムの構成を図3に示す。

(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は、開発者テストと同様のテスト構成である。

評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

評価者は以下のテスト手法により評価者テストを実施した。

① EOSデジタルカメラのシャッターボタンを押下し、検証データ付き画像ファイルを生成することによりセキュリティ機能の動作を確認する

② 開発者テストの結果が正しいことを､開発者テストを再実施することで確認する

③ EOSデジタルカメラのシャッターボタンを押下し、検証データ付き画像ファイルを生成させることだけでは確認できないセキュリティ機能の動作について､開発者が実施した機能モジュールのテスト結果を確認することで動作の保証を行う

c.実施テストの範囲

評価者テストは、以下に示すテストが実施された。これらのテストによりすべてのセキュリティ機能（鍵の生成、検証データの生成）を確認するテストが実施されている。

① 評価者の実施した追加テスト

- 検証データ付加に関するパラメタ「P.Fn-31」の変更に伴うセキュリティ機能の動作確認。EOSデジタルカメラのパラメタ「P.Fn-31」をOFFにして撮影し（検証データが付加されない)、生成された画像ファイルについて検証データ検証ツールでオリジナル性の確認を行う
- パラメタ「出力画像フォーマット、画質」を変更しても正しくセキュリティ機能が動作することの確認。EOSデジタルカメラのパラメタ「出力画像フォーマット、画質」を変更して撮影し、生成された画像ファイルについて検証データ検証ツールでオリジナル性の確認を行う
- パラメタ「出力先（CFとSDメモリカード)」を変更しても正しくセキュリティ機能が動作することの確認。EOSデジタルカメラで撮影した検証データ付き画像ファイルをCFとSDメモリカードにそれぞれ出力する。CFとSDメモリカードに出力された画像ファイルについて検証データ検証ツールでオリジナル性の確認を行う

② 開発者が実施したテストの検証

- 正しい鍵が格納されたスマートカードを使用した場合のセキュリティ機能の動作確認
- 不正な鍵が格納されたスマートカードを使用した場合のセキュリティ機能の動作確認

③ 開発者の実施した機能モジュールテスト結果の確認

- 検証データの生成アルゴリズム「128bits以上の固定値の鍵長のThe Keyed Hash Message Authentication Code」の実装確認
- 検証データの生成アルゴリズムにより生成された検証データが正しく画像データに付加されていることの確認
- 逆難読化アルゴリズムにより、鍵のシードから鍵が正しく生成されていることとの確認

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

本評価報告書をもって、評価者は本TOEがCEMパート2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

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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本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

提出された本評価報告書、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 ([7][10][13][16]のいずれか) のEAL2保証要件及びALC_DVS.1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3にまとめる。

表3　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識別、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記述が理路整然と一貫性のあ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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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明記され、それらが脅威、組織のセキュリティ、前提条件へ遡れ、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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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理路整然とし、完結しており、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理路整然とし、完結しており、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結しており、理路整然とし、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.2.1E	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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

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.1.1E	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、ソフトウェア、ファーム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.1.2E	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り、下位レベル設計が上位レベル設計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。
テスト	**適切な評価が実施された**
ATE_COV.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機能仕様に正確に対応してい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が含まれて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。
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_SOF.1.1E	評価はワークユニットに沿って行われ、確率的または順列的メカニズムが存在しないため非適用であ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、確率的または順列的メカニズムが存在しないため非適用である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。
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。

注意事項

検証データを作成するために必要な鍵の作成において、開発者独自の暗号鍵生成アルゴリズム（逆難読化アルゴリズム）が使用されている。評価者は、開発者が提示した暗号鍵生成アルゴリズム（逆難読化アルゴリズム）に関する証拠資料を確認することで、現実的な時間内にアルゴリズムを解析し、同じ鍵を生成することが困難であることを確認している。しかし、本アルゴリズムの強度は評価の対象になっていないことを注意すべきである。

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
CM	Configuration Management
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

6 参照

[1] 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（2004年6月30日） キヤノン株式会社カメラ開発センター

[2] ITセキュリティ認証申請等の手引き 平成15年10月 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

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 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 適合－部門－IT機関要求－02

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成14年4月 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 適合－部門－IT申請要求－02

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0210

[21] 補足-0210

[22] EOS-1D Mark II ファームウェア ver.1.0.1 評価報告書 第2.2版 2004年6月30日 電子商取引安全技術研究組合研究所