



認 証 報 告 書

独立行政法人 情報処理推進機構
理事長 藤原 武平



評価対象

申請受付年月日(受付番号)	平成17年9月15日 (IT認証5060)
認証番号	C0046
認証申請者	株式会社リコー
TOEの名称	日本版名称 : imagioセキュリティカード タイプC ソフトウェア 海外版名称 : DataOverwriteSecurity Unit Type D Software
TOEのバージョン	V0.03
PP適合	なし
適合する保証要件	EAL2
TOE開発者	株式会社リコー
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18年3月24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 田淵 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。

Common Criteria for Information Technology Security Evaluation Version 2.1
Common Methodology for Information Technology Security Evaluation Version 1.0
CCIMB Interpretations-0407

評価結果 : 合格

「imagioセキュリティカード タイプC ソフトウェア (日本版名称) / DataOverwriteSecurity Unit Type D Software (海外版名称) V0.03」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証手続規程に従い、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	2
1.2.4	TOEの機能	4
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	7
1.5.6	組織のセキュリティ方針	7
1.5.7	構成条件	8
1.5.8	操作環境の前提条件	9
1.5.9	製品添付ドキュメント	9
2	評価機関による評価実施及び結果	10
2.1	評価方法	10
2.2	評価実施概要	10
2.3	製品テスト	10
2.3.1	開発者テスト	10
2.3.2	評価者テスト	12
2.4	評価結果	12
3	認証実施	12
4	結論	13
4.1	認証結果	13
4.2	注意事項	18
5	用語	19
6	参照	21

1 全体要約

1.1 はじめに

この認証報告書は、「imagioセキュリティカード タイプC (日本版名称) ソフトウェア / DataOverwriteSecurity Unit Type D Software (海外版名称) V0.03」(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株式会社リコー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: 日本版名称: imagioセキュリティカード タイプC
海外版名称: DataOverwriteSecurity Unit Type D

バージョン: V0.03

開発者: 株式会社リコー

1.2.2 製品概要

本TOE は、MFPに搭載される「データオーバーライトモジュールのソフトウェア(以降DOMS と記す)」であり、SDメモリーカードに記録された状態で提供される。

本TOE は、MFPをより安全に使用するためのオプションキットであり、MFP から指定されたHDD 上の領域を上書き消去する。

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOE の範囲

TOEはソフトウェアであり、SDメモリーカードに記録された状態でMFPのコントローラボードに取り付けられる。TOE及びその動作環境であるMFPの構成は図1-1の通りである。

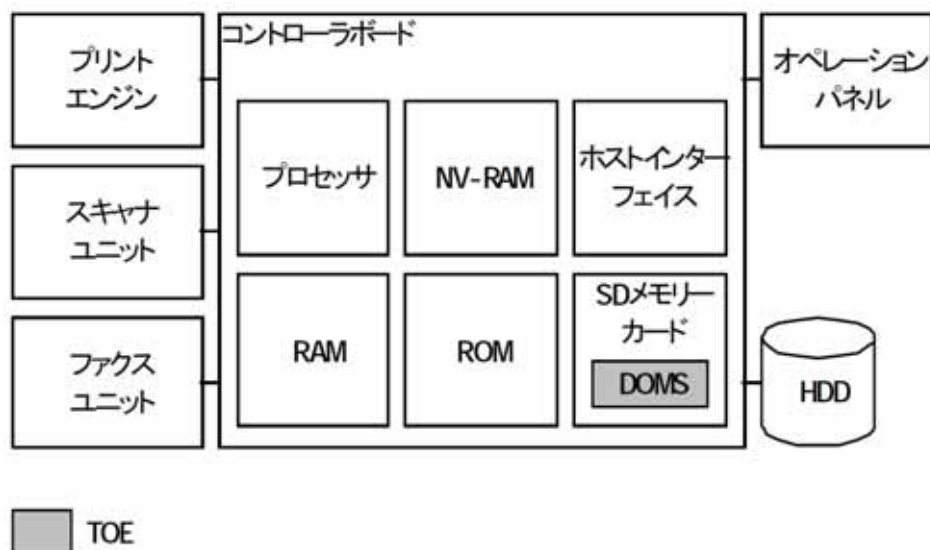


図1-1 TOEとMFPの構成

以降は図1-1における各要素の説明である。

- プリントエンジンはプリント、コピー、およびファクスの受信データを印刷し、同時に給紙および排紙の制御をする。
- スキャナユニットは紙文書からイメージデータを取り込む。コピー、スキャン、およびファクス送信するイメージデータの取り込みに使用する。
- ファクスユニットはファクスの送受信を行なう。
- オペレーションパネルは、MFPの利用者に伝える情報を表示し、また、MFPの利用者からの入力を受け付ける。MFPの利用者はオペレーションパネルを操作してMFPの機能を利用することができる。
- HDDにはイメージデータが保存される。プリント、コピー、スキャン、およびファクスの送受信の際に、MFPが作業用として一時的にイメージデータを保存する。また、MFPの利用者の指示によって蓄積されるイメージデータもここに保存される。
- コントローラボードは、MFP全体を制御する。MFP内のソフトウェアを実行す

るためのプロセッサとRAM、MFPのOSやMFPの制御ソフトウェアが記録されたROM、MFPの設定情報が記録されるNV-RAM、PCや各種サーバと接続するためのインターフェイスを持つ。また、機能を追加するためのソフトウェアが記録されたSDメモリーカードを取り付けることができる。TOEはSDメモリーカードに記録されてコントローラボードに取り付けられる。

1.2.3.2 TOE の動作概要

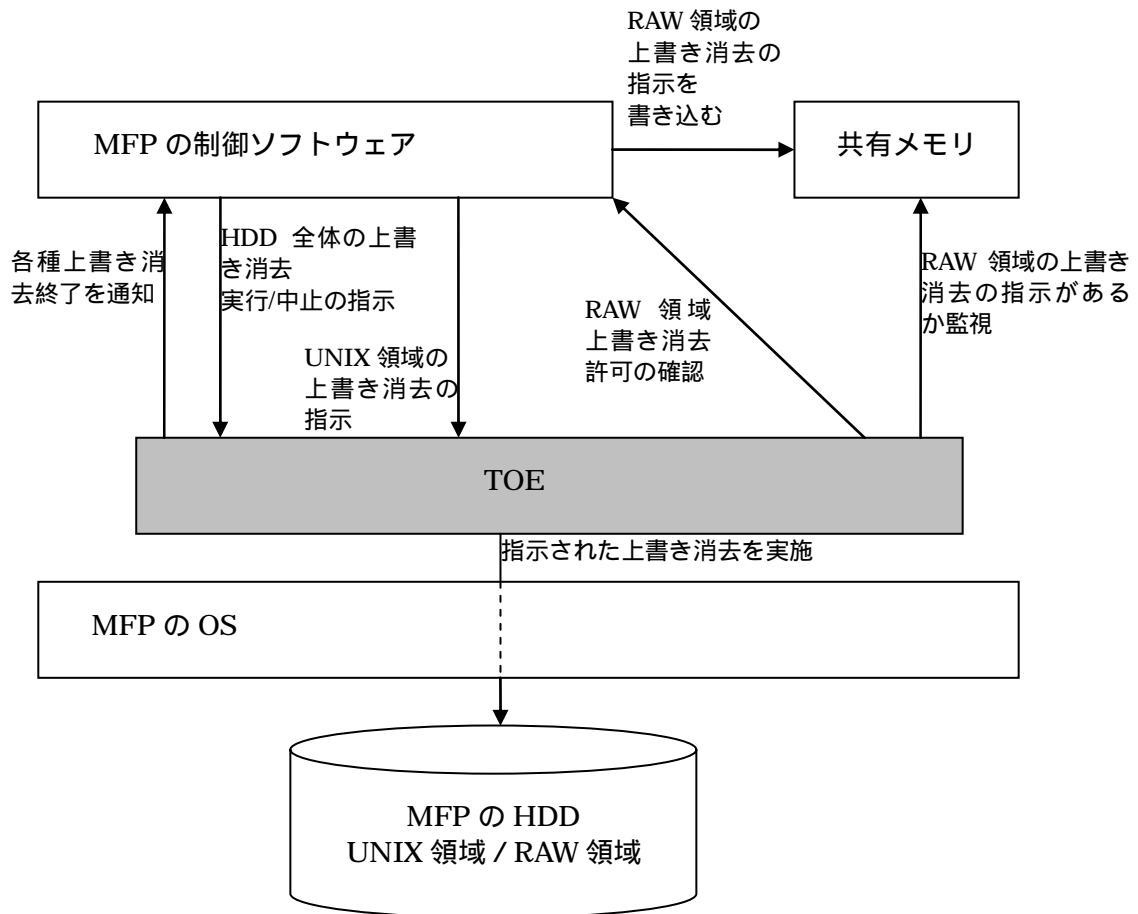


図1-2 TOEの動作概要

図1-2はTOEの動作概要である。

MFPの制御ソフトウェアとMFPのOSは、図1-1のコントローラボード上のROMに存在するソフトウェアである。MFPのHDDは図1-1のHDDであり、UNIX領域とRAW領域に分けられている。共有メモリは、図1-1のコントローラボード上のRAMの中に定義される領域である。

TOEはMFPの制御ソフトウェアからの指示により、MFPのHDD上の指定された部分を指定された方法で上書き消去する。

TOEの上書き消去の動作には以下の3通りがある。

- RAW領域上書き消去の動作概要
TOEへのRAW領域上書き消去の指示は、共有メモリを介して、上書きする領域を指定し、TOEからのRAW領域上書き消去許可の確認に対して返答することによって行う。この際上書き消去の方法も指定される。
TOEは共有メモリにRAW領域上書き消去の指示があるかどうかを監視し、上書き消去の指示を見付けると、RAW領域上書き消去許可の確認を行い、許可の返答の場合はOSを通してRAW領域の指定された部分を上書き消去する。
上書き消去が終了すると、TOEは終了したことを通知する。
- UNIX領域上書き消去の動作概要
TOEへのUNIX領域上書き消去の指示は、UNIX領域のファイルと上書き消去の方法を指定して指示することで行われる。
TOEは、UNIX領域のファイルに対する上書き消去の指示を受けると、OSを通してそのファイルを上書き消去する。
上書き消去が終了すると、TOEは終了したことを通知する。
- HDD全体上書き消去の動作概要
TOEはHDD全体の上書き消去の指示を受けると、OSを通してHDD上の全ての領域を上書き消去する。上書き消去の方法は、HDD全体の上書き消去の指示とともに指定する。
上書き消去が終了すると、TOEは終了したことを通知する。
TOEはHDD全体上書き消去の動作中に上書き消去中止の指示を受けることができ、上書き消去中止の指示を受けた場合は上書き消去を中止する。

1.2.4 TOEの機能

TOEは、HDD上の以下の各領域に対する上書き消去の機能を持つ。

- RAW領域中の指定された領域
- UNIX領域中の指定されたファイル
- HDD全体

上書き消去の方法としては以下の方法のいずれかの指定が可能である。

- NSA 方式
NSA 方式は以下の手順でデータを上書きする。
 - 乱数2 回上書き
 - Null(0) 1 回上書き
- DoD 方式
DoD 方式は以下の手順でデータを上書きする。
 - 固定値1 回上書き
 - 上記の固定値の2 の補数1 回上書き
 - 乱数1 回上書き

- 最後に検証を実行
- 乱数書込み方式
乱数を指定された回数(1~9 回)上書きする。

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セキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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「imagio セキュリティカード タイプC, DataOverwriteSecurity Unit Type D セキュリティターゲット」(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、「imagio セキュリティカード タイプC, DataOverwriteSecurity Unit Type D 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]のいずれか)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18年3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適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、“SOF-基本”を主張する。

本TOE の動作環境であるMFPは一般的なオフィスで使用されることを想定しているため、本TOE の最小機能強度はSOF-基本が妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、HDD上の以下の各領域に対する上書き消去の機能である。

- RAW領域中の指定された領域
- UNIX領域中の指定されたファイル
- HDD全体

上書き消去の手段としては以下の方法のいずれかの指定が可能である。

- NSA 方式
NSA 方式は以下の手順でデータを上書きする。
 - 乱数2 回上書き
 - Null(0) 1 回上書き
- DoD 方式
DoD 方式は以下の手順でデータを上書きする。
 - 固定値1 回上書き
 - 上記の固定値の2 の補数1 回上書き
 - 乱数1 回上書き
 - 最後に検証を実行
- 乱数書込み方式
乱数を指定された回数(1~9 回)上書きする。

1.5.5 脅威

本TOEには、想定される脅威は無い。

1.5.6 組織のセキュリティ方針

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1-1に示す。

表1-1 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
OSP.RESIDUAL	TOEはMFPから指示されたHDD上の領域から情報を読み出せないようにしなければならない。

1.5.7 構成条件

本TOEを搭載可能なMFPは表1-2の通りである。

表1-2 TOEを搭載可能なMFP

国内製品名称	海外製品名称
リコー imagio Neo W7050 リコー imagio Neo W7050 モデル75TR リコー imagio Neo W7050 モデル75R	Ricoh Aficio 480W Lanier LW411 Savin 4800WD Nashuatec A080 RexRotary A080 Gestetner A080
リコー imagio Neo C355it リコー imagio Neo C455it リコー imagio Neo C285 リコー imagio Neo C285 モデル75 リコー imagio Neo C246 リコー imagio Neo C246 モデル75 リコー imagio Neo C355 リコー imagio Neo C355 モデル75 リコー imagio Neo C455 リコー imagio Neo C455 モデル75	Ricoh Aficio 3228C/3235C/3245C Lanier LD328c/LD335c/LD345c Savin C2824/C3528/C4535 Nashuatec DSc428/DSc435/DSc445 RexRotary DSc428/DSc435/DSc445 Gestetner DSc428/DSc435/DSc445 infotec ISC 2428/2835/3545
リコー imagio Neo C200 リコー imagio Neo C200 モデル6 リコー imagio Neo C200 モデル765	Ricoh Aficio 3224C/3232C Lanier LD124c/LD132c Savin C2410/C3210e Nashuatec DSc424/DSc432 RexRotary DSc424/DSc432 Gestetner DSc424/DSc432 infotec ISC 1024c/1032c
リコー imagio Neo 250 リコー imagio Neo 250 モデル6 リコー imagio Neo 250 モデル75 リコー imagio Neo 250 モデル765 リコー imagio Neo 300 リコー imagio Neo 300 モデル6 リコー imagio Neo 300 モデル75 リコー imagio Neo 300 モデル765	Ricoh Aficio 3025/3030 Lanier LD225/LD230 Savin 8025/8030 Nashuatec DSm725/DSm730 RexRotary DSm725/DSm730 Gestetner DSm725/DSm730 infotec IS 2225/2230
リコー imagio Neo 353 リコー imagio Neo 353 モデルD リコー imagio Neo 353 モデル6 リコー imagio Neo 353 モデル75D リコー imagio Neo 353 モデル765D リコー imagio Neo 453 リコー imagio Neo 453 モデル765	Ricoh Aficio 3035/3045/3035G/3045G Lanier LD235/LD245 Savin 8035/8045 Nashuatec DSm735/DSm745 RexRotary DSm735/DSm745 Gestetner DSm735/DSm745 infotec IS 2235/2245
リコー imagio MP C2500 リコー imagio MP C2500 SP リコー imagio MP C3000 リコー imagio MP C3000 SP	Ricoh Aficio MP C2500/C3000 Lanier LD325c/LD330c Savin C2525/C3030 Nashuatec MP C2500/C3000 RexRotary MP C2500/C3000 Gestetner DSc525/DSc530 infotec ISC 2525/3030

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1-3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1-3 TOE使用の前提条件

識別子	前提条件
A.BREAK	TOE の動作が中断されることはないものとする。 TOE が上書き消去を完了する前に、MFP の電源の切断によりTOE の動作が中断されることはないものとする。
A.CANCEL	TOEの一括消去が中止されることはないものとする。 TOE の一括消去が完了する前に利用者の意図に反して一括消去が中止されることはないものとする。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

国内向けのドキュメント

- imagioセキュリティカード タイプC imagioセキュリティカード タイプD
使用説明書
Version B735-8501A
- imagioセキュリティカード タイプC imagioセキュリティカード タイプD
をお買い上げのお客様へ
Version B735-8510

海外向けのドキュメント

- DataOverwriteSecurity Unit Type C/Unit Type D Operating Instructions
Version B735-8600
- To users of machines with Hold Print and Stored Print functions
Version B735-8801
- Depending on your machine
Version B735-8519

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17年10月に始まり、平成18年3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18年1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・配付と運用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18年1月に開発者サイトで開発者のテスト環境を使用し、開発者が実施した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、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

開発者テストは、以下のMFPにTOEを設置して実施された。

- リコー imagio Neo C355it (システムバージョン1.30)
- リコー imagio Neo 353 (システムバージョン 1.31)

また、テストの操作や結果の観察のために以下の機器が用いられた。

- テスト用PC
RS232C またはイーサネット経由にてMFP と接続されるターミナルソフトウェアを使用
- IDEバスアナライザ
東洋テクニカ IDE-Pocket Ultra DMA/100 supported
- その他
MFP をブートモードで起動するためのブートサーバ、メール送信機能使用時のメールサーバ

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

TOEの動作環境であるMFPとしては、STにおいて識別されているMFPのうちの一部の機種が用いられた。STにおいて識別されているMFPの機種間の差異を調査することにより、テストで用いられた一部の機種はSTにおいて識別されているMFPの機種間の差異をカバーしていることが評価者により確認された。

したがって、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たとみなせる。

b. テスト手法

テストにおけるTSFIの刺激および観察には以下の手法が用いられた。

- 操作パネルからの操作およびパネルへの表示の確認。
- MFPに接続されたテスト用PCに出力されたログ表示内容の確認。
- IDEバスアナライザによるHDDとのインタフェースをモニタ。

c. 実施テストの範囲

テストは開発者によって48項目実施されている。

カバレッジ分析が実施され、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の構成は、開発者テストと同様の構成である。

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

テストにおけるTSFIの刺激および観察には以下の手法が用いられた。

- 操作パネルからの操作およびパネルへの表示の確認。
- MFPに接続されたテスト用PCに出力されたログ表示内容の確認。
- IDEバスアナライザによるHDDとのインタフェースをモニタ。

c. 実施テストの範囲

評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを11項目、計16項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

TSFに指示を与えるタイミングの観点で開発者テストを補足すること
すべてのセキュリティ機能とインタフェースを含むこと

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。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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

4.1 認証結果

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のEAL2保証要件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4-1にまとめる。

表4-1 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種別、境界の記述が明瞭であ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_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_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。
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。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.1.2E	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。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.1.3E	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、脅威、組織のセキュリティ方針、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完全で、理路整然としていて、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完全で、理路整然としていて、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を参照しない要件の明示が必要である根拠が示されていること、それらの要件はCCの要件と同様のスタイルと詳細度で記述されていること、それらの要件は明確に曖昧さなく表現されていること、それらの要件は評価可能であること、それらの要件に対して保証要件が適切にサポートする根拠が示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。
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の依存性の識別が不要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全で、理路整然としていて、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。
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。
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環境がないこと、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	<p>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おり、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。</p>
テスト	適切な評価が実施された
ATE_COV.1.1E	<p>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。</p>
ATE_FUN.1.1E	<p>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を含んで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。</p>
ATE_IND.2.1E	<p>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。</p>
ATE_IND.2.2E	<p>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。また、本評価時に行われたテスト実施方法も適切と判断される。</p>
ATE_IND.2.3E	<p>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。</p>
脆弱性評価	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、SOF分析の対象となるセキュリティメカニズムが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、SOF分析の対象となるセキュリティメカニズムが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。

4.2 注意事項

特になし。

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
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
OS	Operating System
RAM	Random Access Memory
ROM	Read Only Memory
HDD	Hard Disk Drive

本報告書で使用された用語を以下に示す。

MFP	デジタル複合機(Multi-Functional Printer)。 1台でコピー、プリンタ等、2種類以上の機能を持ったプリンタのこと。
NV-RAM	不揮発性メモリ。 電源の供給無しに記憶内容を保持できる半導体メモリのこと。
UNIX領域	OSのファイルシステムによって管理されているHDD上の領域。この領域にあるデータは通常のファイル操作によってアクセスできる。
RAW領域	OSのファイルシステムによって管理されていないHDD上の領域。

SDメモリカード セキュアデジタルメモリカード。
著作権保護機能を持った切手サイズのメモリ装置である。

6 参照

- [1] imagio セキュリティカード タイプC, DataOverwriteSecurity Unit Type D セキュリティターゲット バージョン 0.25 (2006年2月28日) 株式会社リコー
- [2] ITセキュリティ評価及び認証制度の基本規程 平成17年7月 独立行政法人 情報処理推進機構 EC-01
- [3] ITセキュリティ認証手続規程 平成17年7月 独立行政法人 情報処理推進機構 EC-03
- [4] 評価機関承認手続規程 平成17年7月 独立行政法人 情報処理推進機構 EC-05
- [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-0407 平成16年8月
- [21] 補足-0210 第2版、補足-0407 平成16年8月
- [22] imagio セキュリティカード タイプC, DataOverwriteSecurity Unit Type D 評価報告書 第1.4版 2006年3月1日
株式会社電子商取引安全技術研究所 評価センター