認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付日（受付番号）	**平成19年8月31日** (IT**認証**7169)
認証番号	C0145
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**7 **ソフトウェア** **海外版名称：**DataOverwriteSecurity Unit Type H Software
TOE**のバージョン**	1.01x
PP**適合**	**なし**
適合する保証パッケージ	EAL3
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20年2月28日

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　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「imagio セキュリティカード タイプ7 ソフトウェア(日本版名称) ／ DataOverwriteSecurity Unit Type H Software(海外版名称) Ver.1.01x」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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 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7 ソフトウェア(日本版名称) ／ DataOverwriteSecurity Unit Type H Software(海外版名称) Ver.1.01x」（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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

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7 ソフトウェア
海外版名称：DataOverwriteSecurity Unit Type H Software

バージョン： 1.01x
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。

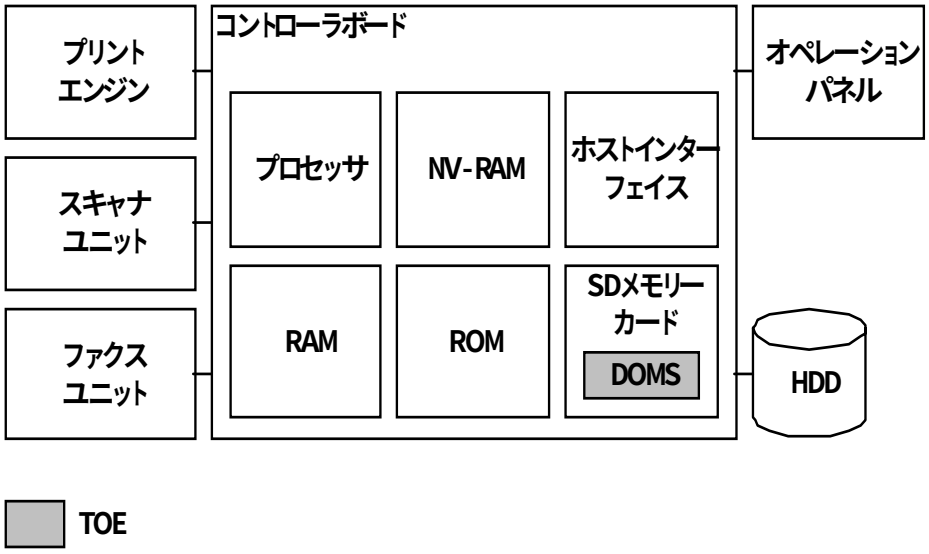

図1-1 TOEとMFPの構成

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及びコピーの受信データを印刷し、同時に給紙及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。コピー及びスキャン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、及びスキャンする際に、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フェースを持つ。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メモリカードを取り付けることができる。TOEはSDメモリ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

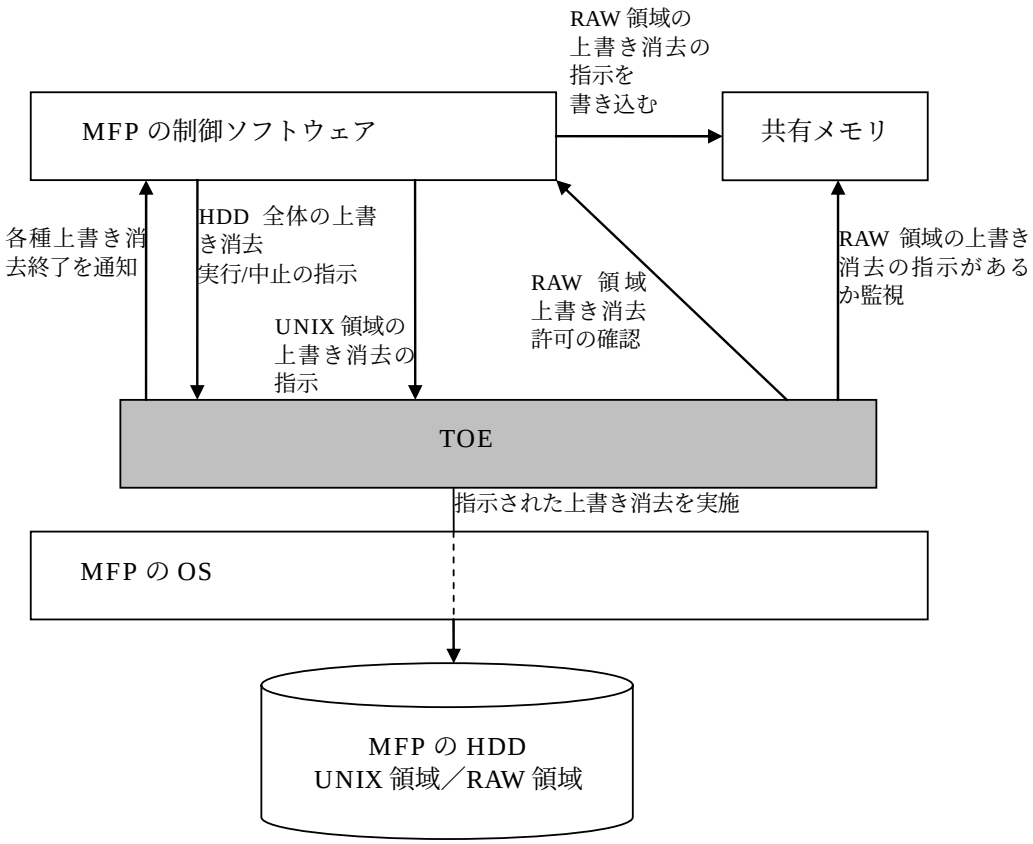

図1-2 TOEの動作概要

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一時停止の指示を受けることができ、上書き消去一時停止の指示を受けた場合は上書き消去を一時停止する。

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セキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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7, DataOverwriteSecurity Unit Type H セキュリティターゲット」（以下「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]のいずれか) 附属書B、CCパート2（[6][9][12]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]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、「日本：imagio セキュリティカード タイプ7 ソフトウェア Ver.1.01x、海外：Data OverwriteSecurity Unit Type H Ver.1.01x 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]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、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。評価は、平成20年1月の評価機関による評価報告書の提出をもって完了し、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

STが規定するTOEの評価保証レベルは、EAL3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
P.UNREADABLE	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
モデル1	リコー imagio MP C6000 シリーズ リコー imagio MP C7500 シリーズ	Ricoh Aficio MP C6000 シリーズ Ricoh Aficio MP C7500 シリーズ Savin C6055/C7570 シリーズ Lanier LD260c/275c シリーズ Lanier MP C6000/C7500 シリーズ Gestetner MP C6000/C7500シリーズ Infotec MP C6000/C7500 シリーズ NRG MP C6000/C7500 シリーズ

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.MODE.AUTOMATIC	**TOEの逐次消去の動作が中断されることはないものとする。** TOEが逐次消去による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.MODE.MANUAL	**TOEの一括消去が一時停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、一時停止ボタン操作やMFPの電源の切断により一括消去が一時停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7
  imagio セキュリティカード タイプ9
  使用説明書
  Version D377-7902

海外向けのドキュメント

- DataOverwriteSecurity Unit Type H
  DataOverwriteSecurity Unit Type I
  Operating Instructions
  Version D377-7940

- Notes for Users
  Version D377-7250

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

評価は、平成19年9月に始まり、平成20年1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19年12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・ライフサイクル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20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。

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 MP C6000 / リコー Aficio MP C6000
  (システムバージョン: 1.02)

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の刺激及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及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51項目実施されている。

カバレージ分析が実施され、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。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステム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

評価者テストは開発者テストと同様の構成で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

- 操作パネルからの操作及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4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15項目のテストを実施した。テスト項目はCEM 2:ATE_IND.2-4と2:ATE_IND.2-9に従った選択基準で考案された。下記はその主要な観点である。

① パラメータの網羅性やインタフェースを使用するタイミングの観点で開発者テストの十分性に懸念がある場合、それを補うためのテストを独自に考案する。

② 開発者テストのサンプリングに関しては、すべてのセキュリティ機能とインタフェースが対象となることを考慮し、十分な量のテストを選択する。

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

評価報告書をもって、評価者は本TOEがCEM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

認証機関は、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評価報告書で示されたように評価されていること。
④ 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 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。

認証機関は、ST及び評価報告書において、所見報告書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EAL3に対する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記述が理路整然とし一貫してい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。
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。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、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、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、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。
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を参照せずに明示された要件が必要であり、CCのモデルに従っていて、TOEがその要件に適合するかどうかが評価可能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の依存性が適切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.3.1E	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。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んで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.2.1E	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.2.2E	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	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。
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。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	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かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.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上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであ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。
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。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。

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_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされてい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、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しい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

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 Function Product)。 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7, DataOverwriteSecurity Unit Type H セキュリティターゲット バージョン 1.00（2007年12月13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19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[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2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[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2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] 日本：imagio セキュリティカード タイプ7 ソフトウェア Ver.1.01x、海外：Data OverwriteSecurity Unit Type H Ver.1.01x 評価報告書 第1.0版 2008年1月30日 株式会社電子商取引安全技術研究所　評価センター