認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司

原紙押印済

評価対象

申請受付日（受付番号）	**平成21年11月16日** (IT**認証**9279)
認証番号	C0253
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**9 **ソフトウェア** **海外版名称：**DataOverwriteSecurity Unit Type I Software
TOE**のバージョン**	1.01m
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22年3月29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　山里　拓己

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 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 バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

評価結果：合格

「imagio セキュリティカード タイプ9 ソフトウェア(日本版名称) ／ DataOverwriteSecurity Unit Type I Software (海外版名称) Ver.1.01m」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
1.1 はじめに 1
1.1.1 評価保証レベル 1
1.1.2 PP適合 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 2
1.2.3 TOE範囲とセキュリティ機能 2
1.3 評価の実施 3
1.4 評価の認証 4
2 TOE概要 5
2.1 セキュリティ課題と前提 5
2.1.1 脅威 5
2.1.2 組織のセキュリティ方針 5
2.1.3 操作環境の前提条件 5
2.1.4 製品添付ドキュメント 6
2.1.5 構成条件 6
2.2 セキュリティ対策 7
2.2.1 P.UNREADABLEの実現 7
3 評価機関による評価実施及び結果 8
3.1 評価方法 8
3.2 評価実施概要 8
3.3 製品テスト 8
3.3.1 開発者テスト 8
3.3.2 評価者独立テスト 10
3.3.3 評価者侵入テスト 10
3.4 評価結果 11
3.4.1 評価結果 12
3.4.2 評価者コメント/勧告 12
4 認証実施 13
5 結論 14
5.1 認証結果 14
5.2 注意事項 14
6 用語 15
7 参照 16

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9 ソフトウェア (日本版名称) ／ DataOverwriteSecurity Unit Type I Software (海外版名称) Ver.1.01m」（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とともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威への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、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販される本TOEを購入する一般消費者、及び本TOEが導入される機器の管理責任を持つ者を読者と想定している。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。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL3適合である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品である。

製品名称：	日本版名称：imagio セキュリティカード タイプ9 海外版名称：DataOverwriteSecurity Unit Type I
バージョン：	1.01m
開発者：	株式会社リコー

1.2.2 製品概要

本認証が対象とする製品は、MFPに搭載される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提供される。

SDメモリカードは評価の対象ではなく、SDメモリカードに記録されたソフトウェアが評価の対象であることを明示するために、TOE名称には「ソフトウェア」「Software」が付加されている。

この製品は、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範囲とセキュリティ機能

1.2.3.1 TOE 範囲と動作環境

TOEの範囲は、「1.2.1 製品名称」に記載した製品と同一である。

図1-1は、TOEと、その動作環境であるMFPの関係である。TOEはSDメモリカードに記録されており、そのSDカードはMFPのSD CARDスロットに挿入される。TOEは、MFP内のコントローラボードにロードされ、コントローラボード上で動作する。

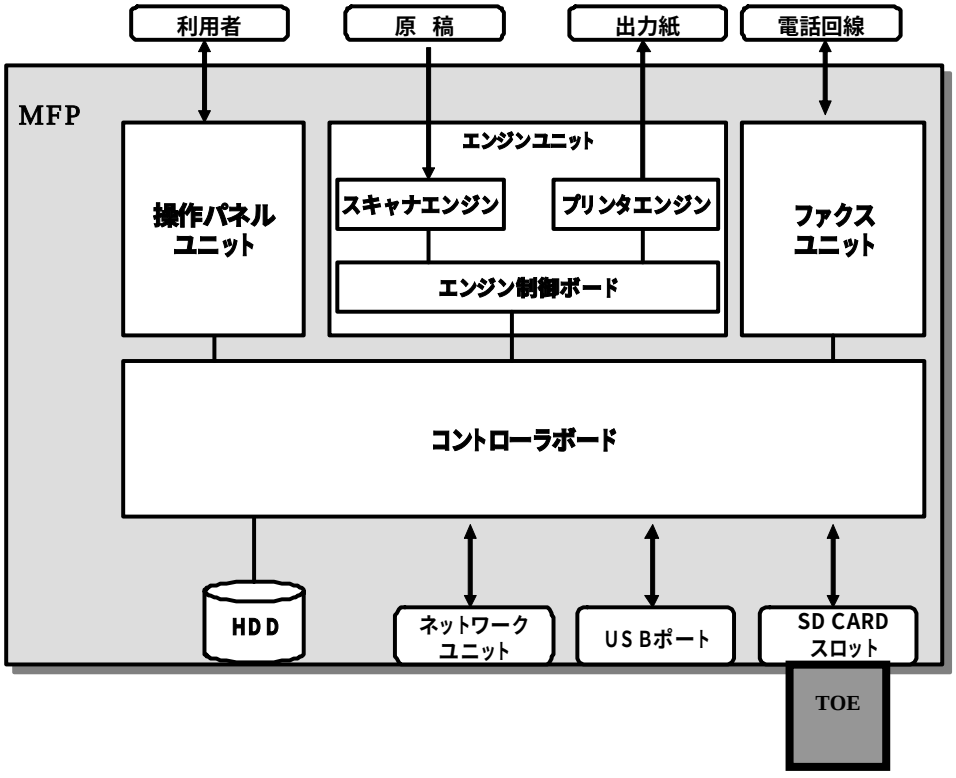

図1-1 TOEと、その動作環境であるMFP

1.2.3.2 TOE のセキュリティ機能

TOEは、MFPから指定されたHDD上の領域を上書き消去する機能を持つ。

MFPが指定するHDD上の領域は、「残存データ」が存在する領域である。「残存データ」が存在する領域をMFPが正しく指定することを仮定すれば、その領域をTOEが上書き消去することで、「残存データ」の漏洩が防がれる。

「残存データ」は、以下のようなデータである。

- MFPはコピー、プリンタ、スキャナ、ファクス、およびドキュメントボックスの機能を提供する。MFPは、これらの機能を実行する際に、ドキュメントの全部あるいは一部の情報を含む一時的な作業用データを、HDD上に作成する。これらの機能が終了し、不要になった一時的な作業用データは、「残存データ」となる。
- MFPはドキュメントボックスの機能によりHDD上にドキュメントを蓄積することができる。利用者がMFPに対して蓄積されたドキュメントを削除することを指示した場合、削除の対象となったドキュメントは「残存データ」となる。

MFPによるHDD上の領域の指定は、以下のように行われることが想定される。

- 利用者がMFPを通常に使用している場合は、「残存データ」が生じる度に、MFPはTOEに「残存データ」が存在する場所を指定する。(逐次消去)
- HDDの交換や廃棄、MFPの返却等の際に、利用者がMFPに対してHDD上の全ての領域を上書きすることを指示することができる。MFPはTOEにHDD上の全ての領域を指定する。(一括消去)

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9, DataOverwriteSecurity Unit Type I 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]のいずれか） 附属書A、CCパート2（[6][9]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]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9 ソフトウェア Ver.1.01m、海外：DataOverwriteSecurity Unit Type I Software Ver.1.01m 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

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、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22年3月の評価機関による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。

2 TOE概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEには、想定される脅威は無い。

2.1.2 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2-1に示す。

表2-1 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上の領域の情報を読み取れないようにしなければならない。

2.1.3 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2-2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2-2 TOE使用の前提条件

識別子	前提条件
A.MODE.AUTOMATIC	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。

2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

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 D377-7250

2.1.5 構成条件

本TOEを搭載可能なMFPは表2-3の通りである。なお、本TOEが搭載されるMFPのハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

表2-3　TOEを搭載可能なMFP

国内製品名称	海外製品名称
リコー imagio MP 4000/5000シリーズ	Ricoh Aficio MP 4000/5000 series Savin 9040/9050 series Lanier LD 040/050 series Lanier MP 4000/5000 series Gestetner MP 4000/5000 series infotec MP 4000/5000 series nashuatec MP 4000/5000 series Rex-Rotary MP 4000/5000 series

2.2 セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.2の組織のセキュリティ方針を満たす。

2.2.1 P.UNREADABLEの実現

TOEは、P.UNREADABLEを実現するために、MFPから指定されたHDD上の領域を指定された方式により上書きする機能を持つ。

TOEがMFPからHDD上の領域の指定を受ける方法として、以下の2通りがある。

- 逐次消去

  TOEは、MFPの残存データ管理機能が管理しているHDD上にある残存データ領域の有無の情報を常に監視し、残存データが存在することを見つけ出したときに、残存データ領域を上書き消去する。

- 一括消去

  TOEは、MFPからHDDの一括消去指示を受けたときに、HDDの一括消去をする。一括消去の指示が行われた場合は、HDDの全領域が指定されたことになる。

指定できる上書きの方式には以下のものがある。

- 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。

HDD上の領域はTOEが管理しているのではなく、動作環境であるMFPが管理している。MFPが管理しているものに対して、TOEは保護の手段を提供している。そのことが読者に誤解なく伝わるように、P.UNREADABLEは脅威ではなく組織のセキュリティ方針として定義された。

3 評価機関による評価実施及び結果

3.1 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。

3.2 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21年11月に始まり、平成22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21年12月及び平成22年3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・開発セキュリティ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21年12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。

ただし、構成管理・配付・開発セキュリティの各ワークユニットに関する一部のプロセスの施行状況については、同一の保証レベルの他のTOEに関して実施された平成19年12月、平成21年8月、及び平成21年9月の調査結果が、現時点でも信頼できるとの判断により採用された。

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。

3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

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 4000 / リコー Aficio MP 4000
  (システムバージョン: 2.00)

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

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。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

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。

b. 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、TOE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。

c. 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。

3.3.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

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) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

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 ATE_IND.2-4とATE_IND.2-6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。

b. テスト概要

評価者が実施した独立テストにおいて使用されたツール、テスト手法は開発者テストと同様のものが用いられている。

c. 結果

実施したすべての評価者独立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。

3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルに

おいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

- TOEが記録されたSDメモリカードが取り出された場合に、そのことを利用者が認識できずに使われ続けてしまう可能性がある。
- TOEのインタフェースに想定外の値が入力されて、予期しない動作となる可能性がある。
- TOEが記録されたSDメモリカードの内容が変わってしまった場合に、そのことを利用者が認識できずに使われ続けてしまう可能性がある。
- TOEがデータを削除している途中でMFPの不慮の電源断等により、TOEが削除すべきデータが残ってしまう可能性がある。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

- TOEが記録されたSDメモリカードをMFPから取り出し、そのことを利用者が認識できる状態になるかを確認する。
- 動作環境であるMFPの操作を行い、TOEのインタフェースに容易に想定外の値を入力する手段が存在しないかどうかを確認する。
- 内容を変更したSDメモリカードをMFPに装着し、そのことを利用者が認識できる状態になるかを確認する。
- TOEがデータを削除している途中でMFPの電源を切り、MFPの電源を再度入れる。そのような場合でもTOEによるデータの削除が再開され完了するかどうかを確認する。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

3.4 評価結果

3.4.1 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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告はとくにない。

4 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 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。
② 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。
③ 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及び評価報告書において、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、本認証報告書を発行した。

5 結論

5.1 認証結果

提出された評価報告書、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すものと判断する。

5.2 注意事項

特になし。

6 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義を以下に示す。

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である。
SDメモリカード	SDメモリカードはセキュアデジタルメモリカードである。高い機能を持ったメモリー装置で、切手サイズで、MFPにTOEや他のアプリケーションを供給するために使用される。
ドキュメントボックス機能	MFPの機能。 紙原稿をスキャンしてMFP内のHDDに蓄積することと、コピー、プリンタ、ファクスおよびドキュメントボックスの各機能でMFP内のHDDに蓄積した文書を印刷､削除することができる。

7 参照

[1] imagio セキュリティカード タイプ9, DataOverwriteSecurity Unit Type I セキュリティターゲット バージョン 1.00　2010年3月25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 3.1 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 2 September 2007 CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 2 September 2007 CCMB-2007-09-003

[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3.1 改訂第1版 2006年9月 CCMB-2006-09-001　(平成19年3月翻訳第1.2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: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002　(平成20年3月翻訳第2.0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: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003　(平成20年3月翻訳第2.0版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 2 September 2007 CCMB-2007-09-004

[12] 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3.1 改訂第2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] 日本：imagio セキュリティカード タイプ9 ソフトウェア Ver.1.01m、海外：DataOverwriteSecurity Unit Type I Software Ver.1.01m 評価報告書 第4.0版 2010年3月25日 株式会社電子商取引安全技術研究所 評価センター