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6月29日** (IT**認証**9257)
認証番号	C0246
認証申請者	**株式会社リコー**
TOE**の名称**	Ricoh imagio MP 5000SP/4000SP **セキュリティカード タイプ9付き**
TOE**のバージョン**	**・構成ファームウェア（システムバージョン：**V2.16-00） System/Copy :1.11.1　Printer:1.11　Network Support:7.26 MSIS:7.15.02　Network DocBox:1.10C　RPCS Font :1.01 Web Support:1.59　Engine:1.04:05　Web Uapl:1.15 OpePanel:1.01　animation:1.3　LANG0:1.01 Scanner:01.24　LANG1:1.01　RPDL:7.33 ADF:15.000:15 ・ASIC　Ic Key:1100 **・オプション**　Data Erase Opt:1.01m
PP**適合**	2600.1, Protection Profile for Hardcopy Devices, Operational Environment A　1.0, dated June 2009
適合する保証パッケージ	EAL3**及び追加の保証コンポーネント**ALC_FLR.2
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2月25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

「Ricoh imagio MP 5000SP/4000SP セキュリティカード タイプ9付き」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、「Ricoh imagio MP 5000SP/4000SP セキュリティカード タイプ9付き」（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追加である。
追加の保証コンポーネントは、ALC_FLR.2である。

1.1.2 PP適合

本TOEは以下のPPへの論証適合を主張する。

PP名称： 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
バージョン： 1.0, dated June 2009

また、上記PPで定義されたSFRパッケージについては以下のものに適合する。

- 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A, Version 1.0,

dated June 2009

・2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A, Version 1.0, dated June 2009

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

製品名称： Ricoh imagio MP 5000SP/4000SP セキュリティカード タイプ9付き

バージョン：

・構成ファームウェア

システムバージョン：	V2.16-00
System/Copy	1.11.1
Network Support	7.26
Network DocBox	1.10C
Web Support	1.59
Web Uapl	1.15
animation	1.3
Scanner	01.24
RPDL	7.33
Printer	1.11
MSIS	7.15.02
RPCS Font	1.01
Engine	1.04:05
OpePanel	1.01
LANG0	1.01
LANG1	1.01
ADF	15.000:15

・ASIC

Ic Keyバージョン： 1100

・オプション

Data Erase Opt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、紙文書の電子化、文書管理、印刷をするためのコピー機能、スキャナ機能、プリンタ機能等を提供する株式会社リコー製のデジタル複合機（以下「MFP」という。）である。

この製品は、コピー機能にスキャナ、プリンタの各機能を組み合わせて構成される製品であり、一般的にはオフィスのLANに接続され、文書データの入力・蓄積・出力に利用される。この製品は、内部に蓄積された文書データ等の情報を意図しない開示や操作から保護し、またクライアントとの間で送受信する文書データの漏洩に対処するためのセキュリティ機能を装備する。

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は、MFPである「Ricoh imagio MP5000SP/4000SP」に、残存情報消去オプションである「セキュリティカード タイプ9」を取り付けた形で利用者に販売される製品全体である。開発者が利用者のサイトにて「セキュリティカード タイプ9」をMFP本体「Ricoh imagio MP5000SP/4000SP」に取り付け、動作確認を行った上で、TOE「Ricoh imagio MP5000SP/4000SP セキュリティカード タイプ9付き」として利用者に引き渡される。

図1-1にTOEの運用環境の一例を示す。

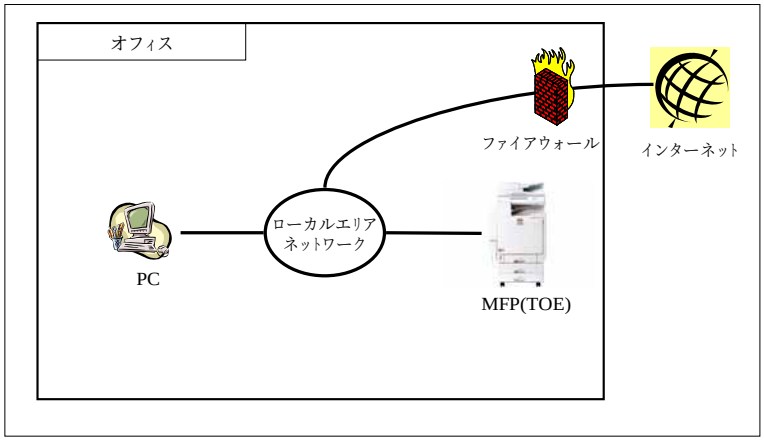

図1-1 TOEの利用環境

図1-1に示すとおり、TOEはオフィス内で利用されることを想定している。

【ローカルエリアネットワーク】

オフィス内で利用されるローカルエリアネットワーク（以降、LAN）を示す。

【PC】

クライアントPCとして動作し、LANを経由しTOEであるMFPと通信し、以下の処理を行う。

・Webブラウザ経由でのMFP本体設定操作、及び利用者文書操作（削除、ダウンロード）

・プリンタドライバ経由での利用者文書操作（蓄積、印刷）

【ファイアウォール】

インターネットからオフィス内へのネットワーク攻撃を防止するための装置。

また、本環境においてTOEを利用するにあたり、関連する利用者を表1-1に示す。

表1-1　TOE利用者

利用者定義		説明
一般利用者		TOEの使用を許可された利用者。ログインユーザー名を付与され通常のMFP機能の利用ができる。
管理者	スーパーバイザー	MFP管理者ログインパスワードの削除とMFP管理者の新規登録をする権限を持つ。
	MFP管理者	TOEの管理を許可された利用者。一般利用者のユーザー情報管理、機器管理、文書管理、ネットワーク管理の管理業務を行う。

表1-1に示すとおり、TOEの利用者は一般利用者と管理者に分類され、さらにその役割によって管理者はスーパーバイザーとMFP管理者とに分類される。TOEを直接利用する利用者としては表1-1に示すとおりであるが、それ以外にMFP管理者及びスーパーバイザーの選任権限を持つMFP管理責任者がTOEの間接的な利用者として存在する。MFP管理責任者は運用環境における組織の責任者等を想定している。

1.2.3.2　TOE 構成と動作概要

図1-2にTOEの内部物理構成を示す。

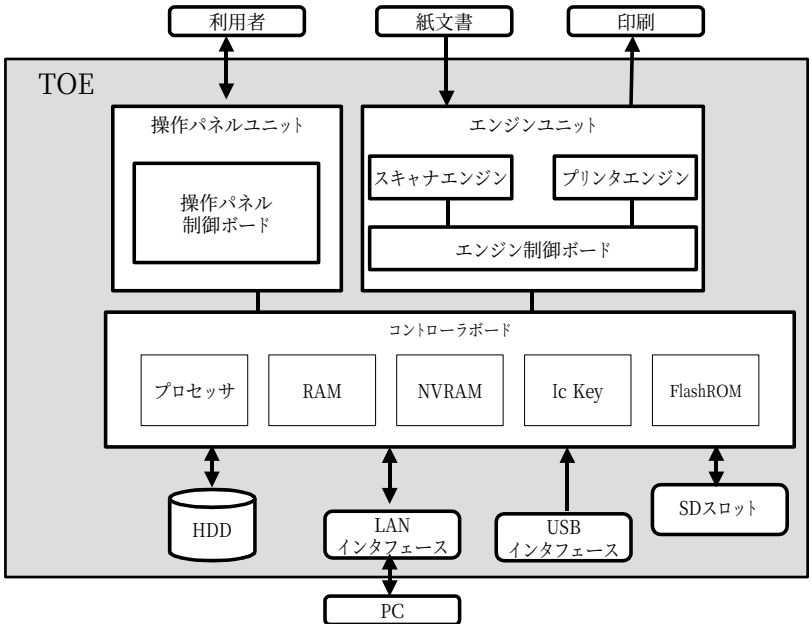

図1-2　TOE内部構成

図1-2に示すとおり、TOEは操作パネルユニット、エンジンユニット、コントローラボード、HDD、LANインタフェース、USBインタフェース、SDスロットのハードウェアから構成される。以下に各構成要素の概要を示す。

【操作パネルユニット（以下、「操作パネル」という。)】

操作パネルは、TOEに組み付けられている、TOEの利用者がTOE操作に使用するインタフェース装置である。ハードキー、LED、タッチパネル付き液晶ディスプレイと操作パネル制御ボードで構成される。

【エンジンユニット】

紙文書を読込むためのデバイスであるスキャナエンジン、紙文書を印刷し排出するデバイスであるプリンタエンジン、各エンジンを制御するエンジン制御ボードから構成される。

【コントローラボード】

コントローラボードはプロセッサ、RAM、NVRAM、Ic Key、FlashROM が載った基板である。各要素の簡潔な説明は以下の通り。

プロセッサ	：ソフトウェアに従い演算等を行うプロセッサ。
RAM	：画像メモリとして利用される揮発性メモリ。
NVRAM	：MFPの動作を決定するMFP制御データが入った不揮発性メモリ。
Ic Key	：乱数発生、暗号鍵生成の機能を持ち、MFP制御ソフトウェアの改ざん検知に利用されるセキュリティチップ。
FlashROM	：MFP制御ソフトウェアがインストールされている不揮発性メモリ。MFP制御ソフトウェアは、TOE を識別する要素のうち、System/Copy 、Network Support 、Scanner 、Printer 、Web Support、Web Uapl、Network Doc Box、animation、RPDL、MSIS、RPCS Fontを含む。

【HDD】

イメージデータ、識別認証に利用するユーザー情報が書込まれるハードディスクドライブである。

【LANインタフェース】

Ethernet(100BASE-TX/10BASE-T)をサポートしたLAN用の外部インタフェースである。

【USBインタフェース】

PCから直結して印刷を行う場合に、TOEとPCを接続する外部インタフェースである。なお本TOEでは設置時に利用禁止設定とする。

【SDスロット】

SDカードを挿入するためのスロットであり、残存情報消去機能ソフトウェア（Data Erase Opt）が保持されている。SDスロットは機器内部に存在し、通常運用においてはSDカードが操作されることはない。

また、TOEは図1-2に示したTOE構成で実現される下記の基本機能を、製品のサービス機能として提供する。

(1) コピー機能

コピー機能は、紙文書をスキャンし、読取った画像を、指定する部数、倍率、編集指定に従って印刷する機能である。

(2) プリンタ機能

プリンタ機能は

・ネットワーク経由でPCからの印刷情報を利用者文書として蓄積する機能

・ネットワーク経由でPCからの印刷情報を直接印刷する機能

から構成される。一般利用者はガイダンスに従って最初に指定のプリンタドライバをPCにインストールして利用する。

(3) スキャナ機能

スキャナ機能は、紙文書をスキャンし、

・利用者文書として本体内のHDDに蓄積する機能

・蓄積された利用者文書に対して、PCへのダウンロード操作をする機能

から構成される。

(4) ドキュメントボックス機能

ドキュメントボックス機能は、MFP本体内のHDDに蓄積された利用者文書に対する、印刷、削除等の操作を実施する。

(5) 管理機能

管理機能は、MFP機器の動作全体にかかわる制御機能である。操作パネルあるいはWebブラウザ経由で実施する。

(6) 保守機能（本機能は無効）

保守機能は、機器故障時の保守サービス処理を実行する機能である。本TOEの運用においては、本機能を無効化する保守機能移行禁止設定が行われていることが前提となる。

(7) Web機能

Web機能は、TOEの利用者がPCからTOEの機能（管理機能等）を使用するための機能である。本機能を使用するためには、PCにインストールされたWebブラウザを使用し、TOEとはLAN経由で接続する。

1.2.3.3 TOE のセキュリティ機能

TOEは1.2.3.2に示す基本機能において使用される文書情報等に対する、不正なアクセス（改ざん、漏洩等）を防ぐために、セキュリティ機能を提供する。以下ではセキュリティ機能の保護対象となる資産（保護資産）、及び各セキュリティ機能の概要を示す。

(1) 保護資産

TOEの保護資産を表1-2、表1-3に示す。TOEのセキュリティ機能の保護資産として、下記の利用者情報、及びTSF情報が含まれる。

表1-2 TOE保護資産（利用者情報）

種別	資産内容
文書情報	デジタル化されたTOEの管理下にある利用者文書、削除された文書、一時的な文書あるいはその断片。
機能情報	利用者が指示したジョブ。（以下、「利用者ジョブ」という。）

表1-3 TOE保護資産（TSF情報）

種別	資産内容
保護情報	ログインユーザー名、利用者ジョブのステータス、ログインパスワード入力許容回数、ロックアウト時間、ロックアウト解除タイマー設定、年月日設定、時刻設定、保守機能移行禁止設定。 （以下、「TSF保護情報」という。）
秘密情報	ログインパスワード、監査ログ。（以下、「TSF秘密情報」という。）

(2) セキュリティ機能

TOEが提供するセキュリティ機能を以下に示す。

【監査機能】

監査機能は、TOEの運用状況を確認したり、セキュリティ侵害を検知したりするために事象発生時に監査ログを記録する機能と、記録した監査ログを、MFP管理者だけに読出し、削除の操作を許可する機能で構成される。監査ログの読出し、削除操作はWeb機能を利用して実施する。

【識別認証機能】

識別認証機能は、TOEを利用しようとする者に対して識別認証機能、認証を連続失敗した利用者に対してのロックアウト機能、パネル操作時のログインパスワード入力時認証フィードバック領域の保護機能で構成される。プリンタ機能利用時は、プリンタドライバにログインユーザー名とログインパスワードを入力して識別認証を行う。

【アクセス制御機能】

アクセス制御機能は、識別認証機能で認証されたTOE許可利用者に対して、その利用者の役割に対して与えられた権限、または利用者毎に与えられた利用者文書の操作権限に基づいた制御をする機能である。

【ネットワーク保護機能】

ネットワーク保護機能は、LAN利用時にネットワーク上のモニタリングによる情報漏えいを防ぐための暗号化通信を行う機能である。

【残存情報消去機能】
HDD上の削除された利用者文書、一時的な文書あるいはその断片に対して、指定パターンデータを上書きすることにより残存情報を完全に消去する機能である。
【セキュリティ管理機能】
セキュリティ管理機能は、管理者が行うセキュリティ管理に関連した管理機能全般をさす。
【ソフトウェア検証機能】
ソフトウェア検証機能は、FlashROMにインストールされているMFP制御ソフトウェアの実行コードの完全性、正当性をチェックすることで、MFP制御ソフトウェアが正規のものであることを確認する機能である。

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 MP 5000SP/4000SPセキュリティカード タイプ9付き 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、「Ricoh imagio MP5000SP/4000SP セキュリティカード タイプ9付き 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、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22年2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は、表2-1に示す脅威を想定し、これに対抗する機能を備える。これらの脅威は適合PPに定義されたものと同等であることを前提に、英文から日本語に翻訳し、さらにTOEの実装、及び運用環境を考慮し具体化したものである。なお以下の脅威における攻撃者は、基本レベルの攻撃能力を有し、本TOEの動作に関して公開されている情報を知識として持つ利用者を想定している。

表2-1 想定する脅威

識別子	脅 威
T.DOC.DIS (文書の開示)	TOEが管理している利用者文書、削除された文書、一時的な文書あるいはその断片が、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持っているがそれらの文書へのアクセス権限をもたない者によって閲覧されるかもしれない。
T.DOC.ALT (利用者文書の改変)	TOEが管理している利用者文書が、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持っているがその利用者文書へのアクセス権限をもたない者によって改変されるかもしれない。
T.FUNC.ALT (利用者ジョブの改変)	TOEが管理している利用者ジョブが、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持っているがその利用者ジョブへのアクセス権限をもたない者によって改変されるかもしれない。
T.PROT.ALT (TSF保護情報の改変)	TOEが管理しているTSF保護情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持っているがそのTSF保護情報へのアクセス権限をもたない者によって改変されるかもしれない。
T.CONF.DIS (TSF秘密情報の開示)	TOEが管理しているTSF秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持っているがそのTSF秘密情報へのアクセス権限をもたない者によって閲覧されるかもしれない。
T.CONF.ALT (TSF秘密情報の改変)	TOEが管理しているTSF秘密情報が、ログインユーザー名をもたない者、あるいは、ログインユーザー名は持ってい

	るがそのTSF秘密情報へのアクセス権限をもたない者によって改変されるかもしれない。

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2-2に示す。これらの方針は適合PPに定義されたものと同等であることを前提に、英文から日本語に翻訳し、さらにTOEの実装、及び運用環境を考慮し具体化したものである。

表2-2 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.USER. AUTHORIZATION (利用者の識別認証)	TOE利用のログインユーザー名をもった者だけがTOEを利用することができるようにしなければならない。
P.SOFTWARE. VERIFICATION (ソフトウェア検証)	TOEの実行コードを自己検証できる手段を持たなければならない。
P.AUDIT.LOGGING (監査ログ記録管理)	TOEはTOEの使用及びセキュリティに関連する事象のログを監査ログとして記録維持し、監査ログが権限をもたない者によって開示あるいは改変されないように管理できなければならない。さらに権限を持つものが、そのログを閲覧できるようにしなければならない。
P.INTERFACE. MANAGEMENT (外部インタフェース管理)	TOEの外部インタフェース（操作パネル、LAN、USB）が権限外のものに利用されることを防ぐため、それらのインタフェースはTOEとIT環境により、適切に制御されていなければならない。

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2-3に示す。これらの前提条件は適合PPに定義されたものと同等であることを前提に、英文から日本語に翻訳し、さらにTOEの運用環境を考慮し具体化したものである。

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2-3 TOE使用の前提条件

識別子	前提条件
A.ACCESS.MANAGED	ガイダンスに従ってTOEを安全で監視下における場所

(アクセス管理)	に設置し、権限を持たない者に物理的にアクセスされる機会を制限しているものとする。
A.USER.TRAINING (利用者教育)	MFP管理責任者は、利用者が組織のセキュリティポリシーや手順を認識するようガイダンスに従って教育し、利用者はそれらのポリシーや手順に沿っているものとする。
A.ADMIN.TRAINING (管理者教育)	管理者は組織のセキュリティポリシーやその手順を認識しており、ガイダンスに従ってそれらのポリシーや手順に沿ったTOEの設定や処理ができるものとする。
A.ADMIN.TRUST (信頼できる管理者)	MFP管理責任者は、ガイダンスに従ってその特権を悪用しないような管理者を選任しているものとする。

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。

- imagio MP 5000/4000 シリーズ 使用説明書<セキュリティ編>（D012-7950）
- セキュリティ機能をお使いの方へ（D011-7750A）
- IEEE Std. 2600.1-2009 準拠でお使いになる管理者の方へ（D011-7755）
- 使用説明書記載内容の変更（D012-7954）
- 本機をお使いのお客さまへ（D015-7103）
- imagio MP5000/4000 シリーズ 同梱されている使用説明書（D012-7501）
- imagio MP5000/4000 シリーズ 使用説明書<コピー機能/ドキュメントボックス機能編>（D012-7650）
- imagio MP5000/4000 シリーズ クイックガイド（D012-7658）
- imagio MP5000/4000 シリーズ 使用説明書<本機のご利用にあたって>（D012-7750/D012-7751）
- imagio MP5000/4000 シリーズ 使用説明書<初期設定編>（D012-7900）
- imagio MP5000/4000 シリーズ 使用説明書<プリンター機能編>（D381-7000）
- imagio MP5000/4000 シリーズ 使用説明書<スキャナー機能編>（D381-7100）
- imagio MP5000/4000 シリーズ 使用説明書<ネットワークガイド>（D381-7200）
- imagio MP5000/4000 シリーズ 使用説明書<こんなときには>（D012-7800/D012-7801）
- 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（D377-7902）

2.1.5 構成条件

クライアントPCからTOEのプリンタ機能を使用するためには、専用のプリンタドライバをクライアントPCにインストールする必要がある。評価においては下記のプリンタドライバでの動作が確認されている。

・imagio MP5000/4000 Windows XP用 RPCSドライバVer.7.69
・imagio MP5000/4000 Windows Vista用 RPCSドライバVer.7.69

また、クライアントPCで使用されるWebブラウザに関しては、評価環境において下記ブラウザでの動作が確認されている。

・Internet Explorer6.0/7.0

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2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

2.2.1 脅威への対抗

STで定義された全ての脅威は、TOEの正当な利用者以外の者、もしくは正当な権限を有さない者による利用者情報、TSF情報への侵害（閲覧、改ざん）に関するものである。
これら脅威に対しては下記のセキュリティ機能により対抗する。

(1) 利用者の識別認証
TOEを利用しようとする者に対して、ログインユーザー名、ログインパスワードの入力要求を行い、TOE内部で管理されている利用者情報に一致することを確認する。入力手段としては、TOE本体操作パネルからの入力、クライアントPCのWebブラウザ上からの入力、プリンタ機能使用時のドライバ経由での入力がある。
必要な機能強度を確保する手段として下記の機能を有する。

・MFP管理者により設定された規定回数連続して認証に失敗すると、そのユーザーアカウントはロックアウトされる（解除されるまでそのユーザーアカウントは使用できなくなる）
・ログインパスワードについてはその長さ（桁数）、文字種別に関して一定品質以上のものが設定時に要求される（品質の詳細についてはMFP管理者の設定に依存するが、桁数については8桁以上が必須となる）

ログインユーザー名、パスワードが正当であると確認されると、その利用者の役割毎に予め規定されたTOEの利用権限が与えられ、TOEの利用が許可される。
TOEが特定する役割は以下の通りである。

・一般利用者
・MFP管理者
・スーパーバイザー

また、識別認証機能をサポートする手段として下記の機能を有する。

・入力画面に入力されたログインパスワードに対して、ダミー文字を表示する
・ログイン後一定時間TOEに対する操作が行われない場合には自動的にログアウトする

(2) アクセス制御（利用者情報に対するアクセス制御）

利用者からの処理要求に対して、その利用者のログインユーザー名、役割毎の権限を元に文書情報、及び利用者ジョブへの操作に対してアクセス制御を実施する。TOEに蓄積された利用者文書には、どの利用者に対して操作（削除、印刷、ダウンロード）を許可するかを規定する情報（文書利用者リスト）が関連付けられており、一般利用者からの操作要求に対してそのログインユーザー名と文書利用者リストの情報から、許可もしくは拒否の制御を行う。MFP管理者の利用者文書に対する操作としては、全ての利用者文書に対して削除権限のみが与えられる。

利用者ジョブに対しても、そのジョブを作成したログインユーザー名が関連付けられており、ログインユーザー名が一致する一般利用者には該当ジョブの削除操作が許可される。MFP管理者に対しては全ての利用者ジョブに対して削除権限が与えられる。スーパーバイザーに対しては、利用者情報に関して全ての操作が禁止される。

(3) 残存情報削除

HDDに残存する削除済みの利用者文書、一時的に利用された文書、その断片に対する不正なアクセスを防ぐため、文書データが削除される際に指定データを上書きし残存情報が残らないようにする。

(4) ネットワーク保護

通信経路のモニタリングによる情報漏えいを防ぐため、TOEとクライアント間のWebブラウザ経由での操作に関する通信、プリンタ機能を使用した通信についてSSL暗号化通信を使用する。

(5) セキュリティ管理

TSF情報に対する、利用者の権限を超えた不正なアクセスを防ぐためTOE利用者の役割によってTOE設定情報の参照・改変、利用者情報の新規登録、改変等に対するアクセス制御を行う。情報の改変（変更）に関する権限のポリシーとしては、一般利用者は自身のログインパスワード改変のみ権限を有し、スーパーバイザーは自

身、及びMFP管理者のログインパスワード改変のみ権限を有している。それ以外の改変はMFP管理者にのみ許可される。

2.2.2 組織のセキュリティ方針の実現

2.2.2.1 P.USER.AUTHORIZATION(利用者の識別認証)の実現

このセキュリティ方針は、TOEに正式に登録されたユーザーのみにTOEを使用させることを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(1) 利用者の識別認証

2.2.1に記載の識別認証により、TOEを利用しようとする者に対してログインユーザー名、ログインパスワードの入力を要求し、TOEに登録された正当な利用者であることを確認し、そのログインユーザー名に対応した役割を関連付ける。

TOEは正当な利用者であると確認された利用者にのみ、TOEが提供する機能の使用を許可する。

(2) セキュリティ管理

TSF情報に対する、利用者の権限を超えた不正なアクセスを防ぐため、TOE利用者の役割によってTOE設定情報の参照・改変に対するアクセス制御を行う。

利用機能リストの改変はMFP管理者のみに許可される。

2.2.2.2 P.SOFTWARE.VERIFICATION(ソフトウェア検証)の実現

このセキュリティ方針は、TOEの実行コードの正当性について、自己検証できることを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(1) 自己テスト

TOEは、電源投入後の初期立ち上げ中に自己テストを実行し、MFP制御ソフトウェアの実行コードの完全性、正当性の確認を行う。自己テストではファームウェアのハッシュ値を検証し実行コードの完全性を確認し、各アプリケーションに対して、署名鍵ベースでの検証を行い実行コードの正当性を確認する。

自己テスト中に何らかの異常が認められた場合には、操作パネルにエラー表示を行い、一般利用者がTOEを利用できない状態で動作停止する。自己テストで異常が認められなかった場合は、立上げ処理を続行し利用者がTOEを利用できる状態にする。

2.2.2.3 P.AUDIT.LOGGING(監査ログ記録管理)

このセキュリティ方針は、TOEのセキュリティ事象に関する監査ログを取得し、適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する。

(1) セキュリティ監査

TOEは、監査対象となるセキュリティ事象が発生した際に、事象種別、利用者識別、発生日時、結果等の項目から成る監査ログを生成し、監査ログファイルに追加保存する。生成した監査ログファイルは識別認証に成功したMFP管理者のみに読出し、削除を許可する。監査ログファイルの読出しはクライアントPCのWebブラウザを介してテキスト形式で行う。

また、監査ログの事象発生日時を記録するため、日付、時間情報をTOEのシステム時計から取得する。

2.2.2.4 P.INTERFACE.MANAGEMENT(外部インタフェース管理)

このセキュリティ方針は、TOEが提供する外部インタフェース（操作パネル、LANインタフェース、USBインタフェース）が不正な利用者に使用されないように適切に管理することを求めている。

TOEではこの方針を下記のセキュリティ機能で実現する

(1)利用者の識別認証

2.2.1に記載の識別認証により、TOEを利用しようとする者に対してログインユーザー名、ログインパスワードの入力を要求し、TOEに登録された正当な利用者であることを確認し、TOEの利用を許可する。

(2)外部インタフェース間の情報転送制御

本機能は能動的なメカニズムの実装ではなく、外部インタフェースのアーキテクチャ設計として対応するもので、外部から入力された情報に対する処理、及び外部インタフェース（特にLANインタフェース）から送信される情報の制御についてはかならずTOEが関与することにより、外部インタフェース間で不正な情報転送が実施されることを防ぐ。

USBインタフェースについては、使用を無効化する設定で運用することにより、このインタフェースを使用した不正な情報転送を防ぐ。

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7月に始まり、平成22年2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8月、平成21年9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10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。

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

開発者が実施したテストの構成を図3-1に、主な構成要素を表3-1に示す。

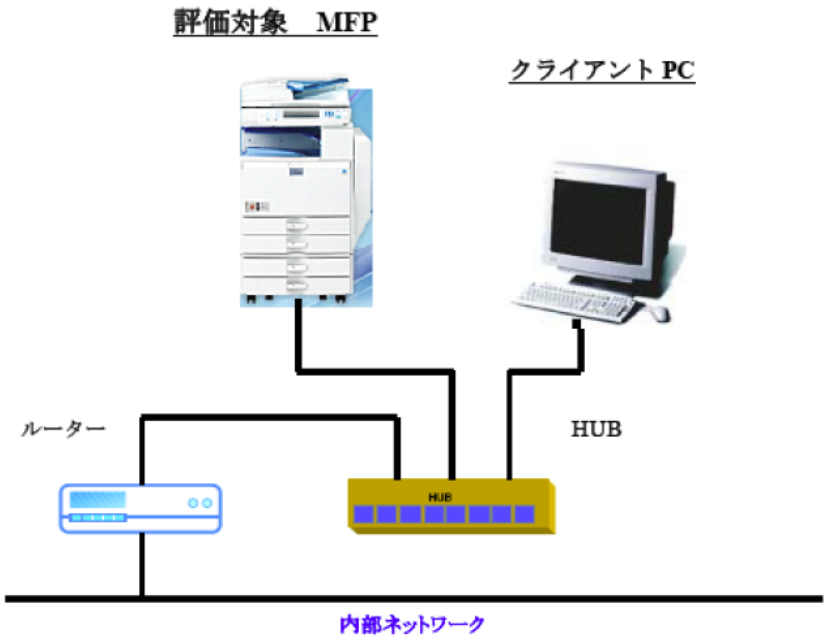

図3-1　開発者テストの構成図

表3-1　テスト構成要素

TOE	imagio MP 5000SP/4000SP セキュリティカードタイプ9付き ・構成ファームウェア システムバージョン：　V2.16-00 System/Copy　1.11.1 Network Support 7.26 Network DocBox　1.10C Web Support　1.59 Web Uapl　1.15 animation　1.3 Scanner　01.24 RPDL　7.33 Printer　1.11 MSIS　7.15.02 RPCS Font　1.01 Engine　1.04:05 OpePanel　1.01 LANG0　1.01 LANG1　1.01 ADF　15.000:15 ・ASIC Ic Keyバージョン　：　1100 ・オプション Data Erase Optバージョン：1.01m
クライアント PC	OS：　Windows XP Pro SP2　/ Windows Vista Business SP1 Webブラウザ：　Internet Explorer6.0/7.0 プリンタドライバ：

	imagio MP5000/4000 Windows XP用 RPCSドライバVer.7.69 imagio MP5000/4000 Windows Vista用 RPCSドライバVer.7.69

開発者テストは本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。

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

開発者が実施したテストの構成を図3-1に、主な構成要素を表3-1に示す。開発者テストは本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。

テストは通常のTOEの使用において想定される外部インタフェース（パネル、Webブラウザ等）を刺激し、結果を目視観察する方法の他、生成された監査ログ、及びデバッグ用ログデータの解析、パケットキャプチャによるクライアントPC間通信プロトコルの確認、不正なTSF実装を使用した異常系テスト等も行われている。

b. 実施テストの範囲

テストは開発者によって339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。

評価者が実施したテストの構成を図3-1に示す。評価者テストは本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。

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

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

・入力パラメタの種類が多く、網羅性の観点で開発者テストが不足していると思われるTSFIに関して、パラメタの組み合わせ、境界値、異常値等のテスト項目を追加する
・複数のTSFの実行タイミング、実行の組み合わせに関して条件を追加したテスト項目を実施する
・サンプリングテストにおいては下記の観点からテスト項目を選択する
  - 網羅性の観点から、全てのTSF,TSFIが含まれるように項目を選択する
  - 入力パラメタの種類が多いTSFIに関するテスト項目を重点的に選択する
  - 多くのSFRが対応付けられ、効率よくテストが実施できるTSFIに関する項目を重点的に選択する

b. テスト概要

上記観点を考慮し、サンプリングテスト36件、独立テスト18件の評価者テストが実施された。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。

・意図しないネットワークポートインタフェースが存在し、そこからTOEにアクセスできる可能性がある
・クライアントPCからの操作で使用するWebアプリケーションに公知の脆弱性が存在する可能性がある
・TOEの外部インタフェースに不正にアクセスすることにより、セキュリティ機能をバイパスできる可能性がある
・過負荷状態でTOEを運用することにより、セキュリティ機能がバイパスされる可能性がある

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。

・ポートスキャン用のツールを使用し、必要としないネットワークポートが開いていないことを確認する
・プロキシツール等を使用し、Webアプリケーションに公知の脆弱性が存在しないことを確認する
・不正なUSBデバイス、SDカード等を使用し、TOEのセキュリティ機能がバイパスされないことを確認する
・CPU過負荷状態、リソース枯渇状態においてTOEがアンセキュアな状態にならないことを確認する

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

評価者により、利用者に対する以下の勧告が評価報告書にてなされている。

・本TOEのガイダンス（使用説明書＜セキュリティ編＞）に記載された下記機能については、本評価の範囲外となる。

- 不正コピーガード機能
- 機密印刷
- 管理者役割毎のアクセス制御

（機器管理者、ユーザー管理者、ネットワーク管理者、文書管理者）

また、本TOEでは無効される保守機能に関連する下記機能については、TOEに含まれるガイダンスに従った設置生成手順により無効化される。

- @Remote
- RFU（リモートファームウェア更新）

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 所見報告書でなされた指摘内容が妥当であること。
② 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。

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、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及び保証コンポーネントALC_FLR.2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

TOE廃棄時においては、HDD内データの漏洩防止のため、MFP管理者によりHDD内データの消去機能を明示的に実行する必要がある。

1.2.3.2にも示したとおり、本TOEの評価環境として、基本機能である保守機能についてはその使用が無効化されていることが前提となる。保守機能が有効化され使用された場合、それ以降はTOEではなくなる可能性がある。利用者は使用に際して期待する機能が無効の対象となっていないかを確認すべきである。

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。

HDD	ハードディスクドライブの略称。本書で、単にHDDと記載した場合はTOE内に取り付けられたHDDを指す。
RFU	リモートファームウェア更新の略称。 TOEにリモート接続し、ファームウェアを更新する機能。 （本機能は評価の範囲外となる）
@Remote	インターネット経由でTOEをリモート操作する機能。遠隔故障診断、カウンター情報収集、トナー情報収集等がリモート操作の対象となる。 （本機能は評価の範囲外となる）
不正コピーガード機能	文書の背景に印刷された特殊な地紋をコピー時に検出し、それに対応した処理を行うことにより、文書コピーによる情報漏えいを防ぐ機能。（本機能は評価の範囲外となる）
機密印刷	蓄積した文書を印刷する際に予め設定されたパスワード入力を要求する機能。 （本機能は評価の範囲外となる）
管理者役割	MFP管理者に割り当てることが出来る予め定義された役割。 以下の4種類の管理者役割が定義され、それぞれ別の管理者に割り当てることが可能であるが、本TOEにおいては全ての役割が割り当てられたMFP管理者を想定している。 （細分類された管理者役割毎のアクセス制御は本TOEの評価対象外となる） ・機器管理者（機器管理、監査の実施を行う） ・ユーザー管理者（一般利用者の管理を行う）

	・ネットワーク管理者 （TOEのネットワーク接続管理を行う） ・文書管理者 （利用者文書、及び文書利用者リストの管理を行う）
文書	コピー機能、プリンタ機能、スキャナ機能を利用して生成されるTOE管理下のデジタル画像情報。 本体内のHDDに蓄積されている文書を本STでは明示的に利用者文書と呼ぶ。 単に文書と記述する場合はコピー時や印刷時の削除された文書、一時的な文書あるいはその断片も含む。
利用者ジョブ	利用者がTOEに対して操作を要求する作業。開始と終了をもつひと続きの作業を１ジョブとする。対象となる操作は、利用者文書の蓄積操作、印刷操作、ダウンロード操作、削除操作である。
ログイン パスワード	各ログインユーザー名に対応したパスワード。
ログインパスワード 入力許容回数	識別認証時にユーザーアカウントがロックアウトされるまでに許容される、認証連続失敗回数。 1～5回の設定値をMFP管理者がTOEの初期設定時に設定し、設定後は変更されない。
ログイン ユーザー名	利用者に与えられている識別子。TOEはその識別子により利用者を特定する。
ロックアウト	ユーザーアカウントが使用できなくなる状態
ロックアウト 時間	ユーザーアカウントがロックアウト状態から自動的に解除されるまでの時間。 本TOEではMFP管理者により60分が設定され運用される。

7 参照

[1] imagio MP 5000SP/4000SPセキュリティカード タイプ9付き セキュリティターゲット バージョン 1.00 2010年2月18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] Ricoh imagio MP 5000SP/4000SPセキュリティカード タイプ9付き 評価報告書 第3.0版 2010年2月18日 株式会社電子商取引安全技術研究所 評価センター