認　証　報　告　書

評価対象

申請受付年月日（受付番号）	**平成**16**年**8**月**5**日**(IT**認証**4032)
認証番号	C0027
認証申請者	**キヤノン株式会社**
TOE**の名称**	**（英語版）** Canon iR5570/iR6570 Series Encrypted Printing Software-B1 **（日本語版）**Canon iR5570/iR6570 **シリーズ用 セキュアプリント機能拡張キット（暗号化）**･B1
TOE**のバージョン**	Version 1.01
PP**適合**	**なし**
適合する保証要件	EAL2
TOE**開発者**	**キヤノン株式会社**
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17年6月2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 Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「（英語版）Canon iR5570/iR6570 Series Encrypted Printing Software-B1 Version 1.01 （日本語版）Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット（暗号化）･B1 Version 1.01」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 はじめに

この認証報告書は、「(英語版) Canon iR5570/iR6570 Series Encrypted Printing Software-B1、(日本語版) Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット (暗号化)・B1」(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: (英語版) Canon iR5570/iR6570 Series Encrypted Printing Software-B1
(日本語版) Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット (暗号化)・B1

バージョン:Version 1.01

開発者: キヤノン株式会社

1.2.2 製品概要

一般的なオフィス環境では、PCに搭載されたアプリケーションによって様々なデータが作成され、業務が実施されている。そして、一般的にそれらのデータの印刷は、ネットワークで接続されている共有の複合機、またはプリンタ等の印刷装置を使用して行われる。

本製品は、複合機「Canon iR5570/iR6570シリーズ」と印刷操作を実施するPCで動作するソフトウェアであり、以下に示す機能を提供する。

- PCから複合機までの経路上における印刷ジョブデータの保護
- 複合機においてPCで印刷操作を実施した際に使用したICカードと同じICカードが使用されていることを確認してから該当の印刷ジョブデータを印刷する機能

1.2.3 TOEの範囲と動作概要

TOEは、PCで動作する「Add-inソフトウェア」とMFPで動作する「MFP制御用ソフトウェア」であり、保護資産は「PDLデータ」である。

TOEが持つセキュリティ機能を表1-1に示す。

表1-1　TOEのセキュリティ機能

Add-inソフトウェア	MFP制御用ソフトウェア
・ PDLデータ暗号化機能 ・ 設定機能	・ PDLデータ復号機能 ・ 印刷ジョブデータ確認機能

TOEのセキュリティ機能を利用した印刷操作の動作概要を以下に示す。なお、以下の動作概要は、プリンタ管理者がTOE（Add-inソフトウェア）によりTOEのセキュリティ機能を有効化にした状態の動作を示す。TOEセキュリティ機能の有効化／無効化の設定は、プリンタ管理者が設定を変更するまで継続されるため、印刷の度に有効化設定を行う必要はない。

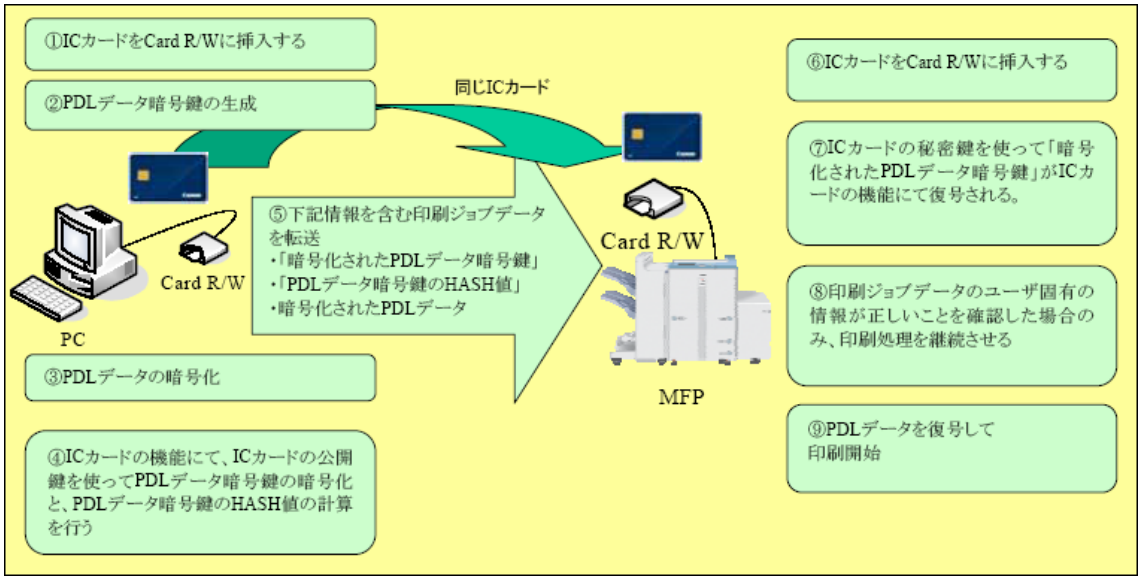

図1-1　TOEの機能を利用した印刷操作のイメージ

① ユーザは、PCに接続されているCard R/WにICカードを挿入する。
② ユーザがPCから印刷操作を行うと、TOE（Add-inソフトウェア）はPDLデータを暗号化するための「PDLデータ暗号鍵」を生成する。
③ TOE（Add-inソフトウェア）は、②で生成した「PDLデータ暗号鍵」を使用してPDLデータを暗号化する。
④ ICカードは、ICカードに格納されている公開鍵を使用して「PDLデータ暗号鍵」を暗号化し、さらに「PDLデータ暗号鍵のHASH値」を計算する。
⑤ TOE（Add-inソフトウェア）は、「暗号化されたPDLデータ」、「暗号化されたPDLデータ暗号鍵」、「PDLデータ暗号鍵のHASH値」を含む印刷ジョブデータをMFP

へ転送する。MFPは、PCから転送された印刷ジョブデータを格納する（印刷は実施されない）。

⑥ ユーザは、MFPに接続されているCard R/Wに①と同じICカードを挿入し、MFPに格納された印刷ジョブデータの印刷操作を行う。

⑦ ICカードは、ICカードに格納されている秘密鍵を使用して印刷ジョブデータに含まれる「暗号化されたPDLデータ暗号鍵」を復号する。

⑧ TOE（MFP制御用ソフトウェア）は、⑦で復号したPDLデータ暗号鍵のHASH値を計算する。TOE（MFP制御用ソフトウェア）は、PCから転送された印刷ジョブデータに含まれる「PDLデータ暗号鍵のHASH値」と計算したHASH値を比較する。

⑨ ⑧におけるHASH値の比較結果が一致した場合、TOE（MFP制御用ソフトウェア）は⑦で復号したPDLデータ暗号鍵を使用して暗号化されたPDLデータを復号し、印刷を開始する。

1.2.4 TOEの機能

TOEは以下に示すセキュリティ機能を持つ。

- PDLデータ暗号化機能
  TOE（Add-inソフトウェア）は、PDLデータを暗号化する。
- 設定機能
  プリンタ管理者以外の利用者がセキュリティ機能を無効化することをできないように、TOE（Add-inソフトウェア）はプリンタ管理者に対してのみセキュリティ機能を有効化／無効化できる機能を提供する。
- 印刷ジョブデータ確認機能
  TOE（MFP制御用ソフトウェア）は、ICカードによって復号された「復号されたPDLデータ暗号鍵」を使用してHASH値を求める機能、印刷ジョブデータに含まれている「PDLデータ暗号鍵のHASH値」と「復号されたPDLデータ暗号鍵」使用した求めたHASH値を比較して、HASH値が一致した場合のみ印刷処理を継続する。
- PDLデータ復号機能
  TOE（MFP制御用ソフトウェア）は、暗号化されたPDLデータを復号する。

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セキュリティ認証申請等の手引き」[2]、「ITセキュリティ評価機関に対する要求事項」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項」[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「Canon iR5570/iR6570 Series Encrypted Printing Software-B1 Security Target」（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、「（英語版）Canon iR5570/iR6570 Series Encrypted Printing Software-B1、（日本語版）Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット（暗号化）・B1 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17年4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は、一般のオフィスで利用されるPCとMFPで動作するソフトウェアである。従って、最小機能強度として“SOF-基本”を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

- SF.A.ENCRYPT: PDLデータ暗号化機能
  TOEは、PDLデータの暗号化機能にて、<Add-inソフトウェア>と<MFP制御用ソフトウェア>の間のPDLデータの機密性を保護している。TOEは、利用環境に応じて、Triple DESもしくはAESのどちらかの暗号方式を選択する。
  Triple DESの場合は、まず、PDLデータを暗号化するために、擬似乱数生成のアルゴリズムにて168bitのPDLデータ暗号鍵を生成する。生成した168bitのPDLデータ暗号鍵を使って、PDLデータを、FIPS PUB 46-3に規定された共通鍵暗号方式であるTriple DESにて暗号操作を行う。最後に、PDLデータ暗号鍵をNULLクリアのアルゴリズムにて、破棄する。
  AESの場合は、まず、PDLデータを暗号化するために、擬似乱数生成のアルゴリズムにて256bitのPDLデータ暗号鍵を生成する。生成した256bitのPDLデータ暗号鍵を使って、PDLデータを、FIPS PUB 197に規定された共通鍵暗号方式であるAES にて暗号操作を行う。最後に、PDLデータ暗号鍵をNULLクリアのアルゴリズムにて、破棄する。
  また、<MFP制御用ソフトウェア>とのPDLデータ暗号鍵の鍵交換のために、「暗号化されたPDLデータ暗号鍵」を印刷ジョブデータのジョブ情報として追加する。さらに、<MFP制御用ソフトウェア>にてPCで印刷時に使用したICカードと同じICカードがMFPで使用されていることを確認するために、印刷ジョブデータ固有の情報である「PDLデータ暗号鍵のHASH値」を印刷ジョブデータのジョブ情報として追加している。これら「暗号化されたPDLデータ暗号鍵」と「PDLデータ暗号鍵のHASH値」はICカードの暗号機能により得られたものである。これらの印刷ジョブデータを<MFP制御用ソフトウェア>に転送する。
    ・暗号化されたPDLデータ暗号鍵
    ・PDLデータ暗号鍵のHASH値
    ・暗号化されたPDLデータ

- SF.A.SETTING: 設定機能
  プリンタ管理者以外の利用者がセキュリティ機能を無効化することをできないように、TOEはプリンタ管理者に対してのみセキュリティ機能を有効化/無効化できる機能を提供する。TOEに対応したMFPに対する印刷において、PDLデータの暗号化を行う場合は、この機能を初期状態の有効化のまま運用する。

- SF.M.CONFIRM_PRINTJOB: 印刷ジョブデータ確認機能
  あらかじめ、PCで印刷時に使用したICカードと同じICカードがMFPで使用されていることが確認できるように、印刷ジョブデータ固有の情報である「PDLデータ

暗号鍵のHASH値」を印刷ジョブデータのジョブ情報として追加されている。
<MFP制御用ソフトウェア>からの要求により、ICカードの秘密鍵を使って「暗号化されたPDLデータ暗号鍵」がICカードの機能にて復号される。
その「復号されたPDLデータ暗号鍵」からFIPS PUB 180-2に規定されたSHA-1のアルゴリズムにてHASH値を求める。
印刷ジョブデータに含まれている「PDLデータ暗号鍵のHASH値」と、「復号されたPDLデータ暗号鍵」から求めたHASH値が一致した場合のみ、印刷ジョブデータを通過させ印刷処理を継続する、という印刷ジョブデータフロー制御を実施する。

- SF.M.DECRYPT: PDLデータ復号機能
TOEは、SF.A.ENCRYPTによって暗号化されたPDLデータを、このSF.M.DECRYPTのPDL復号機能によって、復号することで<Add-inソフトウェア>と<MFP制御用ソフトウェア>の間のPDLデータの機密性を保護している。
<MFP制御用ソフトウェア>からの要求により、ICカードの秘密鍵を使って「暗号化されたPDLデータ暗号鍵」がICカードの機能にて復号される。その「復号されたPDLデータ暗号鍵」を利用する。
TOEは、印刷ジョブデータの暗号方式に応じて、Triple DESもしくはAESのどちらかの復号方式を選択する。
Triple DESの場合は、168bitの「復号されたPDLデータ暗号鍵」を使って、PDLデータを、FIPS PUB 46-3に規定された共通鍵暗号方式であるTriple DESにて復号操作を行う。復号操作の後に、「復号されたPDLデータ暗号鍵」をNULLクリアのアルゴリズムにて、破棄する。
AESの場合は、256bitの「復号されたPDLデータ暗号鍵」を使って、PDLデータを、FIPS PUB 197に規定された共通鍵暗号方式であるAESにて復号操作を行う。復号操作の後に、「復号されたPDLデータ暗号鍵」をNULLクリアのアルゴリズムにて、破棄する。

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 想定する脅威

識別子	脅 威
T.WIRETAP_DATA: PDLデータの盗聴	攻撃者が、PCと印刷装置間における経路中の印刷ジョブデータ内のPDLデータを盗聴することにより、印刷内容を知りえるかもしれない。
T.PRINTOUT:印刷出力	攻撃者が、＜MFP制御用ソフトウェア＞に格納された印刷ジョブデータを、TOEを操作することにより、印刷出力するかもしれない。
T.MISUSE:誤操作	プリンタ管理者以外の利用者が、誤操作によりTOEのセキュ

	リティ機能を無効化してしまうことにより、PDLデータが暗号化されずに印刷装置に送信されてしまうかもしれない。

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はない。

1.5.7 構成条件

本TOEは、キヤノン株式会社が提供する複合機およびPCで動作するソフトウェア製品である。TOEが動作する環境を以下に示す。

また、TOEの利用者は、公開鍵暗号方式に対応したISO7816準拠のICカードを使用することが必要になる。

表1-3 TOE（Add-inソフトウェア）が動作するために必要なPCの構成

	英語版	日本語版
PC	CPU、メモリ、ハードディスクを有するWindows PC それぞれの仕様は、OSの動作環境に準ずるものとする。	
ICカードリーダライタ	ICカードに対応したICカードリーダライタ	
OS	Windows XP Professional/Home Edition 英語版、または Windows 2000 Professional 英語版 SP4	Windows XP Professional/Home Edition 日本語版、または Windows 2000 Professional 日本語版 SP4
キヤノン製 プリンタドライバ	Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 以降、または Canon UFR II Printer Driver for Microsoft Windows Version 1.20 以降	Canon LIPS4 Printer Driver for Microsoft Windows Version 10.40 以降 、Canon LIPS LX Printer Driver for Microsoft Windows Version 1.20 以降、または Canon UFR Printer Driver for Microsoft Windows Version 1.30 以降
ICカード認証ソフトウェア	ICカードに対応したソフトウェア	

表1-4 TOE（MFP制御用ソフトウェア）が動作するために必要な複合機の構成

	英語版	日本語版
MFP	iR 5570/ iR 6570	
拡張メモリ	―	増設メモリ（本体と合わせ512MB以上）
拡張バス	Expansion Bus-C1	PCIバス拡張キット・C1
拡張ボード	USB Application Interface Board-D1	セキュリティ拡張ボード（USB）・D1
ICカードリーダライタ	ICカードに対応したICカードリーダライタ	
ICカード認証ソフトウェア	SSO IC Card Smart Card（英語版）	SSO IC Card Smart Card（国内版）

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1-6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1-6 TOE使用の前提条件

識別子	前提条件
A.PRODUCTS:TOEに対応した製品	TOEの機能を利用するために、TOEに対応した以下の製品を必要とする。 <Add-inソフトウェア>と<MFP制御用ソフトウェア>に共通 ・ICカード <Add-inソフトウェア> ・PC ・ICカードリーダライタ ・OS ・キヤノン製プリンタドライバ ・ICカード認証ソフトウェア <MFP制御用ソフトウェア> ・MFP ・拡張メモリ（本体と合わせ512MB以上の場合は必要なし） ・拡張バス ・拡張ボード ・ICカードリーダライタ ・ICカード認証ソフトウェア
A.SETTING:プリンタ管理者の設定	<Add-inソフトウェア>において、プリンタ管理者はTOEのセキュリティ機能を有効化に設定する。

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。

- （英語版）Canon iR5570/iR6570 Series Encrypted Printing Software-B1
  Encrypted Printing Software User's Guide, FA7-7516
- （日本語版）Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット（暗号化）・B1
  セキュアプリント機能拡張キット(暗号化)・ユーザーズガイド,FA7-7513

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8月に始まり、平成17年4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。構成管理・配付と運用については、他のTOE評価において開発サイトの訪問が実施済みであったため、改めてサイト訪問は実施せずに実施済みのサイト訪問結果の調査を行った。また、平成17年3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

開発者が実施したテストの構成を表2-1に示す。

表2-1　開発者テストの構成

TOE	バージョン
Add-inソフトウェア側	
PC	DELL Dimension L566cx (Intel Celeron 566MHz、192MB、HDD 37GB)
ICカードリーダライタ	ICカードリーダライタ・A1
OS	日本語版：Windows XP Professional / Home Edition、 Windows 2000 Professional SP4 英語版：　Windows XP Professional / Home Edition Windows 2000 Professional SP4
プリンタドライバ	日本語版： Canon LIPS4 Printer Driver for Microsoft Windows Version 10.62 Canon LIPS LX Printer Driver for Microsoft Windows Version 1.22 Canon UFR Printer Driver for Microsoft Windows Version 1.33 英語版： Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 Canon UFR II Printer Driver for Microsoft Windows Version 1.22
Add-inソフトウェア	日本語版： 暗号化セキュアプリント ドライバAdd-in for Client PC ICカード対応版 Version 1.10c 英語版： Encrypted Secured Print Driver Add-in for Client PC IC Card Support Version 1.10c
ICカード認証ソフトウェア	ICカード認証クライアントソフトウェア(Fujitsu Safety Domain)
MFP側	
MFP	日本語版：iR 5570N(IR 5570 / 6570を包含、仕向地：日本) 英語版：iR 5570N(IR 5570 / 6570を包含、仕向地：米国)
拡張メモリ	本体と合わせ512MB
拡張バス	PCIバス拡張キット・C1
拡張ボード	セキュリティ拡張ボード（USB）・D1
ICカードリーダライタ	ICカードリーダライタ・A1
MFP制御用ソフトウェア	日本語版：System Software（国内版） 英語版：System Software（英語版）
ICカード認証ソフトウェア	SSO IC Card Smart Card
ツール類、その他	
Microsoft Office	日本語版：Microsoft Office 2000 英語版：Microsoft Office 2000
検証用ツールA	Openssl.exe
検証用ツールB	PickupRND.exe
検証用ツールC	TestTool.exe
検証用ツールD	ENCPDL_2K.bat , ENCPDL_XP.bat
検証用ツールE	Ethereal.exe
検証用ツール F	WinDiff.exe
検証用ツール G	UNDUMP.EXE
検証用ツール H	Add-in'
正規のICカード2 枚	ICカード・A1
通信経路データ取得用PC	COMPAQ Evo D500 US (Intel Celeron 1.40 GHz、512 MB、HDD 20 GB)
HUB	NETGEAR EN2005
サンプルデータ	日本語版：SampleST.doc 英語版：W1.doc

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の構成を表2-1に示す。

開発者は、複合機としてSTに記載されている複合機と異なるモデルを使用している（STの記載：iR 5570/ iR6570、評価者テスト環境：iR 5570N）。しかし、iR5570 とiR6570 の相違点は印刷速度の違いであり、Nという識別は複合機のオプション構成の違いを示すものであり、TOEへの影響はない。

開発者は、プリンタドライバとしてSTに記載されているすべてのプリンタドライバのバージョンを使用していない。しかし、プリンタドライバにおいてTOEと関連するする部分の仕様は各バージョンで同じであり、プリンタドライバのバージョンの相違によるTOEへの影響はない。従って、すべてのバージョンのプリンタドライバを使用しなくてもSTに記載されている動作環境を考慮したテストが実施されていると判断できる。

各種ツール類は、テストに必要な情報を取得するための機材、テスト結果の検証を行うために使用するツールであり、TOEのセキュリティ機能に影響を及ぼさないことが確認されている。

b.テスト手法

テストには、以下の手法が使用された。

①デジタル複合機本体の操作パネル、PCを操作して、セキュリティ機能の外部インタフェースを刺激し、外部インタフェースのふるまいを直接観察する。

②外部インタフェースのふるまいを直接観察することができないセキュリティ機能については、ツールを使用してセキュリティ機能のふるまいを確認する。

表2-2にセキュリティ機能ごとのテスト手法を示す。

表2-2　テスト手法

セキュリティ機能	テスト手法
SF.A.SETTING	・ レジストリエディタ[regedit.exe]を使用し、該当するエントリの値を確認する。 ・ 本体操作パネル、及びリモートUIを操作して機能仕様書に記載されるとおりに動作する事を確認する。
SF.A.ENCRYPT SF.M.CONFIRM_PRINTJOB SF.M.DECRYPT	・ ログイン処理もしくは印刷処理を行い、指示された条件の時に正しいメッセージが表示されることを確認する。 ・ TOEにて処理を行っていない印刷ジョブデータとTOEにて処理を行った印刷ジョブデータを実際に印刷し、目視によって相違が無いことを確認する。 ・ Add-inと外部ツールで同様の処理を行い、同じ結果にな

	ることを確認する。 ・ Add-inから、スプーラと印刷装置に同じ印刷ジョブデータを転送し、ツールを用いて2つのデータを比較して同じ結果になることを確認する。

c.実施テストの範囲

テストは開発者によって168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。

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を表2-3に示す。

表2-3 評価者テストの構成

TOE	バージョン
Add-inソフトウェア側	
PC	DELL Dimension L566cx (Intel Celeron 566MHz、194MB、HDD 37GB)
ICカードリーダライタ	ICカードリーダライタ・A1
OS	日本語環境： Windows XP Professional 日本語版 SP1 Windows 2000 Professional 日本語版 SP4 英語環境： Windows XP Home Edition 英語版
プリンタドライバ	日本語環境： Canon LIPS4 Printer Driver for Microsoft Windows Version 10.62、 Canon LIPS LX Printer Driver for Microsoft Windows Version 1.22、 英語環境： Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 Canon UFR II Printer Driver for Microsoft Windows Version 1.22
Add-inソフトウェア	日本語環境： 暗号化セキュアプリント ドライバAdd-in for Client PC IC カード対応版 Version 1.10c 英語環境： Encrypted Secured Print Driver Add-in for Client PC Smart Card Support Version 1.10c
ICカード認証ソフトウェア	ICカード認証クライアントソフトウェア(Fujitsu Safety Domain)
MFP側	
MFP	日本語環境：iR 5570N (IR 5570 / 6570 を包含、仕向地：日本)

	英語環境：iR 5570N (IR 5570 / 6570 を包含、仕向地：米国)
拡張メモリ	本体と合わせ512MB
拡張バス	PCIバス拡張キット・C1
拡張ボード	セキュリティ拡張ボード（USB）・D1
ICカードリーダライタ	ICカードリーダライタ・A1
MFP制御用ソフトウェア	System Software（国内版） System Software（英語版）
ICカード認証ソフトウェア	SSO IC Card Smart Card
ツール類、その他	
Microsoft Office	英語環境： Microsoft Office 2000 日本語環境：Microsoft Office 2000
検証用ツールA	Openssl.exe
検証用ツールB	PickupRND.exe
検証用ツールC	TestTool.exe
検証用ツールD	ENCPDL_2K.bat , ENCPDL_XP.bat
検証用ツールE	Ethereal.exe
検証用ツールF	WinDiff.exe
検証用ツールG	UNDUMP.EXE
検証用ツールH	Add-in'
正規のICカード2枚	ICカード・A1
正規でないICカード1枚	正規のICカードと異なるICカード(VISAクレジットカード)
通信経路データ取得用PC	COMPAQ Evo D500 US (Intel Celeron 1.40 GHz、512 MB、HDD 20 GB)
HUB	NETGEAR EN2005 (Ethernet HUB)
サンプルデータ	英語環境：SampleST.doc 英語環境：W1.doc

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を表2-3に示す。

評価者は、OS及びプリンタドライバに関して、開発者テストと異なる環境でテストを実施しているが、STに記載されている構成に含まれている環境であり、評価者テストを実施するのに問題のないテスト構成である。

b.テスト手法

評価者は、開発者が行ったテスト手法が、セキュリティ機能の期待されたふるまいを検証するのに適していると判断し､開発者テストと同様の手法でテストを実施している。

c.実施テストの範囲

評価者は、評価者が独自に考案したテストを11項目、開発者テストのサンプリングによるテストを36項目、侵入テストを6項目、計53項目のテストを実施している。

評価者が独自に考案したテストは、以下に示す観点を考慮している。

①開発者テストで確認されていないパラメタの組み合わせ
②開発者テストにてテストされていないTSFI
③開発者テストで確認されていない、外部からふるまいを見ることができないセキュリティ機能

サンプリングテストは、開発者が実施した168項目のテストの21%にあたる36項目を選択している。

侵入テストは、開発者の脆弱性分析結果、評価者が評価作業中に得たTOEに関する知識に基づき脆弱性分析を行い、その分析結果に基づいて6項目のテストを実施している。

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

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

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 ([7][10][13][16]のいずれか) 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。
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。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。
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。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_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。
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。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_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。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。
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。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。

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_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。

PDL	Page Description Languageの略であり、プリント出力のフォーマットや描画を定義するためのページ記述言語
PDLデータ	印刷内容を表現するPDLで記述されたデータ
印刷ジョブデータ	PCを利用しているユーザが、アプリケーションやOSを操作して、印刷命令する単位ごとに生成するデータである。ジョブ情報、PDLデータから構成される。
ジョブ情報	印刷の枚数、拡大/縮小、片面印刷/両面印刷などの印刷の属性に関する情報
PDLデータ暗号鍵	PDLデータの暗号化を行う暗号鍵
公開鍵	公開鍵暗号方式で使用されるペアになった秘密鍵と公開鍵のうち、一般に公開される鍵
秘密鍵	公開鍵暗号方式で使用されるペアになった秘密鍵と公開鍵のうち、一般に公開されない鍵
MFP	コピー機能、ファクス機能、プリンタ機能、送信機能などを併せ持つデジタル複合機
印刷装置	印刷ジョブデータを受信して、印刷する装置であり、MFPやプリンタ等の装置を指す
PC	パーソナルコンピュータ
プリンタ管理者	PC上のOSで定義される、「プリンタの管理」権限を有する

	ユーザ
ユーザ	プリンタ管理者を含むTOEの全ての利用者

6 参照

[1] Canon iR5570/iR6570 Series Encrypted Printing Software-B1 Security Target V1.12 2005年3月29日 キヤノン株式会社

[2] ITセキュリティ認証申請等の手引き 平成16年4月 独立行政法人情報処理推進機構 ITQM-23

[3] ITセキュリティ評価機関に対する要求事項 平成16年4月 独立行政法人情報処理推進機構 ITQM-07

[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16年4月 独立行政法人情報処理推進機構 ITQM-08

[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

[21] 補足-0407

[22] （英語版）Canon iR5570/iR6570 Series Encrypted Printing Software-B1、（日本語版）Canon iR5570/iR6570 シリーズ用 セキュアプリント機能拡張キット（暗号化）・B1 評価報告書 第1.0版 2005年4月21日
株式会社電子商取引安全技術研究所　評価センター