# Canon iR5570/iR6570 Series Encrypted Printing Software-B1 Security Target

**V1.12**

**2005/3/29**

キヤノン株式会社

更新履歴

| No | 日付 | バージョン | 事由 | 更新者 | 検査者 | 承認者 |
|---|---|---|---|---|---|---|
| 1 | 2004/08/02 | V1.00 | 初版作成 | 広田 | 桜井 | 川本 |
| 2 | 2004/09/10 | V1.01 | 評価者のORの指摘事項を反映<br>BLQ-EOR-0001-00～BLQ-EOR-0005-00 | 広田 | 桜井 | 川本 |
| 3 | 2004/09/16 | V1.02 | 評価者の OR の指摘事項を反映<br>BLQ-EOR-0006-00 | 広田 | 桜井 | 川本 |
| 4 | 2004/10/29 | V1.03 | 認証レビューの指摘事項を反映<br>CRV-T026-001 | 広田 | 桜井 | 川本 |
| 5 | 2004/11/05 | V1.04 | 表 6-1 の対応するコンポーネントの修正 | 広田 | 桜井 | 川本 |
| 6 | 2004/12/10 | V1.05 | TOE の範囲拡大による全面変更 | 広田 | 桜井、土樋 | 牧谷 |
| 7 | 2005/1/7 | V1.06 | セキュリティ機能の見直しによる変更 | 広田 | 桜井、土樋 | 牧谷 |
| 8 | 2005/1/17 | V1.07 | 評価者の OR の指摘事項を反映<br>BLQ-EOR-0007-00～BLQ-EOR-0009-00 | 広田 | 桜井、土樋 | 牧谷 |
| 9 | 2005/1/19 | V1.08 | 誤記修正 | 広田 | 桜井、土樋 | 牧谷 |
| 10 | 2005/2/15 | V1.09 | 8 章「根拠」の記述変更 | 広田 | 桜井、土樋 | 牧谷 |
| 11 | 2005/2/28 | V1.10 | 誤記修正 | 広田 | 桜井、土樋 | 牧谷 |
| 12 | 2005/3/22 | V1.11 | 認証レビューCRV-T026-005 の指摘事項を反映 | 広田 | 桜井、土樋 | 牧谷 |
| 12 | 2005/3/29 | V1.12 | 誤記修正 | 広田 | 桜井、土樋 | 牧谷 |

# 目 次

# 1. ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張について記述する。

## 1.1. ST 識別

| | |
|---|---|
| タイトル: | Canon iR5570/iR6570 Series Encrypted Printing Software-B1 Security Target |
| 日付: | 2005/3/29 |
| バージョン: | V1.12 |
| 作成者: | キヤノン株式会社 |
| TOE: | |
| (英語版) | Canon iR5570/iR6570 Series<br>Encrypted Printing Software-B1 Version 1.01 |
| (日本語版) | Canon iR5570/iR6570 シリーズ用<br>セキュアプリント機能拡張キット(暗号化)・B1 Version 1.01 |
| キーワード: | キヤノン、CANON、iR、image RUNNER、印刷、暗号、PDL、複合機、MFP、プリンタ、ドライバ、プリンタドライバ、IC カード、LIPS、UFR、PCL |
| CC のバージョン: | Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999<br>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 1999 年 8 月バージョン 2.1 (平成 13 年 1 月翻訳第 1.2 版)<br>補足-0210 第 2 版<br>補足-0407<br>CCIMB Interpretations – 0407 |
| 評価保証レベル: | EAL2 |

## 1.2. ST 概要

本 ST は、TOE のセキュリティ仕様を定めた Security Target である。
TOE は、Canon iR5570/iR6570 Series Encrypted Printing Software-B1 というソフトウェアであり、印刷内容の機密を保護する機能と、印刷ジョブデータの正当な所有者を確認してから印刷を行う機能を提供する。

## 1.3. CC 適合

この TOE は、下記の CC に適合している。
- 機能要件－CC パート2適合
- 保証要件－CC パート3適合
- 保証レベル－EAL2 適合

本 ST が適合している PP はない。

## 1.4. 略語・用語

表 1-1 に略語・用語の説明を記述する。

**表 1-1：略語・用語の説明**

| 略語・用語 | 説明 |
|---|---|
| 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。<br>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 |
| プリンタプロパティの設定 | プリンタドライバの設定、および TOE のセキュリティ機能を有効化/無効化する設定 |

| 略語･用語 | 説明 |
|---|---|
| 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 |
| | |

# 2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 範囲、および資産について記述する。

## 2.1. TOE 種別

TOE は、次の2つから構成されるソフトウェアである。

- <Add-in ソフトウェア>
  Windows 用のキヤノン製プリンタドライバに対して、セキュリティ機能を追加する PC 上で動作するソフトウェア
- <MFP 制御用ソフトウェア>
  MFP<Canon iR 5570/iR 6570 シリーズ>にセキュリティ機能を追加する制御用ソフトウェア

## 2.2. TOE 概要

最近の会社内において、従業員は、PC のアプリケーションを使って種々のデータを作成して、業務を行っている。一般に、そのデータを印刷する際には、ネットワークで接続されている共有の複合機（以下、MFP と略す）もしくはプリンタ等の印刷装置を使って印刷している。
ところが印刷内容は、社内に対して公開して構わない情報とは限らず、社内とはいえ機密にしておくべき情報は多々存在する。
一般的には、PC やサーバ内の情報に関しては、ログインのような識別認証の機能や、情報に対するアクセス制御によって保護されている。また、PC とサーバ間の経路中の情報に対しては、SSL、SSH のような手段を利用して保護されていることが多い。
しかしながら、PC 上のアプリケーションからの印刷命令によって印刷装置に送信される印刷ジョブデータの保護は、PC と印刷装置間の経路中において、もしくは印刷装置自体において怠っている場合が多く、以下のような攻撃を受ける可能性がある。

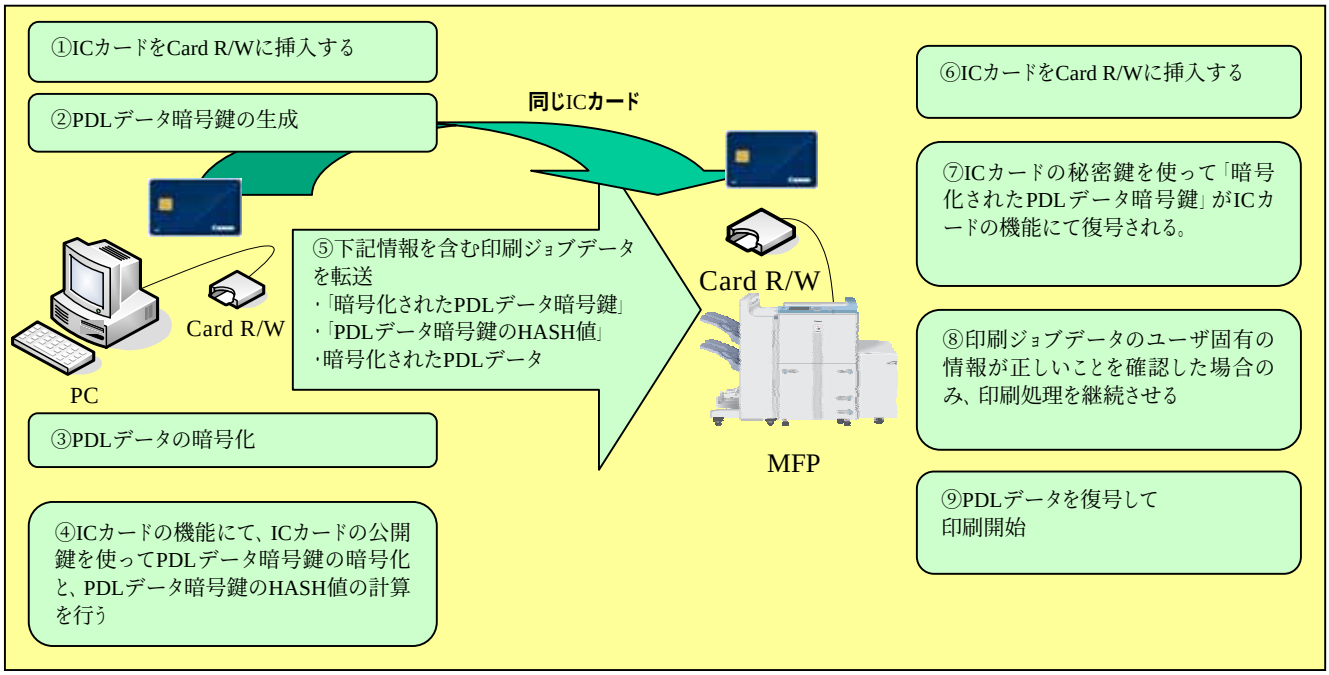
- PC から印刷装置までの経路上の印刷ジョブデータを盗聴する。
- 不正に印刷装置を操作して印刷出力させ、その印刷内容を知りうることができる。

TOE は、上記のような攻撃から印刷内容を保護するために次の2つの機能を提供する。

- 印刷内容の機密を保護する機能
- 印刷ジョブデータの正当な所有者を確認してから印刷を行う機能

まず、印刷内容の機密を保護する機能について説明する。
TOE は、印刷ジョブデータの中の PDL データを<Add-in ソフトウェア>によって暗号化して、<MFP 制御用ソフトウェア>によって復号することで、印刷内容の機密性を保護している。
その暗号化の際に利用した PDL データ暗号鍵を<Add-in ソフトウェア>と<MFP 制御用ソフトウェア>との間で交換する必要がある。その PDL データ暗号鍵の保護のために、IC カードによる公開鍵暗号方式の暗号機能を採用している。従って、本 TOE を使用するために IC カードに各々固有の公開鍵･秘密鍵ペアが登録されており、公開鍵暗号方式の暗号機能を有しているような特定の IC カードを必要としている。
次に、印刷ジョブデータの正当な所有者を確認してから印刷を行う機能について説明する。
<Add-in ソフトウェア>にて印刷ジョブデータに追加されたユーザ固有の情報である「PDL データ暗号鍵の HASH 値」を、<MFP 制御用ソフトウェア>において正しいことを確認した場合のみ、印刷処理を継続させる。このユーザ固有の情報である「PDL データ暗号鍵の HASH 値」は、IC カードの機能を利用して HASH 値の計算を行っている。
2.3.2. 章の「印刷ジョブデータ確認機能」にて、その確認方法を記述する。

図 1 に、<Add-in ソフトウェア>で行う処理と<MFP 制御用ソフトウェア>で行う暗号化印刷における主要な機能の流れを図示する。




凡例：Card R/W は、IC カードリーダライタを示す。

**図 1:暗号化印刷のフロー**

TOE の<Add-in ソフトウェア>は、IT 環境の一部である IC カードと共に①から⑤の機能を提供する。プリンタ管理者は TOE を利用して、あらかじめプリンタプロパティの設定にセキュリティ機能が有効になるよう設定をしておく。
TOE の<MFP 制御用ソフトウェア>は印刷ジョブデータを受信後、IT 環境である IC カードと共に上記⑥から⑨の処理を行い、印刷を完了する。
また⑤において、PC から MFP までの経路は、Ethernet を使った LAN での接続が一般的であるが、USB を使った経路でも可能であり、経路に関して物理的な接続方法は規定していない。

TOE は、以下のセキュリティ機能を持つ。それぞれの機能に関しては 2.3.2. 章で述べる。
<Add-in ソフトウェア>でのセキュリティ機能
- PDL データ暗号化機能
- 設定機能

<MFP 制御用ソフトウェア>でのセキュリティ機能
- PDL データ復号機能
- 印刷ジョブデータ確認機能

# 2.3. TOE 範囲

TOE の範囲に関して、物理的範囲と論理的範囲の観点から記述する。

## 2.3.1. TOE の物理的範囲

TOE に関する構成に関して記述する。
TOE は、<Add-in ソフトウェア>と<MFP 制御用ソフトウェア>から構成される。

まず、<Add-in ソフトウェア>と<MFP 制御用ソフトウェア>に共通に必要なハードウェア構成に関して、表 2-1 に記述する。

**表 2-1:共通に必要なハードウェア構成**

| | |
|---|---|
| IC カード | 公開鍵暗号方式に対応した ISO7816 準拠の IC カード |

次に、<Add-in ソフトウェア>に必要なハードウェア構成とソフトウェア構成に関して、それぞれ表 2-2 および表 2-3 に記述する。

**表 2-2:<Add-in ソフトウェア>に必要なハードウェア構成**

| | |
|---|---|
| PC | CPU、メモリ、ハードディスクを有する Windows PC<br>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 |

**表 2-3:<Add-in ソフトウェア>に必要なソフトウェア構成**

| | 英語版 | 日本語版 |
|---|---|---|
| OS | Windows XP Professional/Home Edition 英語版<br>または<br>Windows 2000 Professional 英語版 SP4 | Windows XP Professional/Home Edition 日本語版<br>または<br>Windows 2000 Professional 日本語版 SP4 |
| キヤノン製<br>プリンタドライバ | Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 以降<br>または<br>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 、<br>Canon LIPS LX Printer Driver for Microsoft Windows Version 1.20 以降<br>または<br>Canon UFR Printer Driver for Microsoft Windows Version 1.30 以降 |
| <Add-in ソフトウェア> | Encrypted Secured Print Driver Add-in for Client PC Smart Card Support Version 1.10c | 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 |
| 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 | |

次に、<MFP 制御用ソフトウェア>のハードウェア構成とソフトウェア構成に関して、それぞれ表 2-4 および表 2-5 に記述する。

表 2-4：<MFP 制御用ソフトウェア>に必要なハードウェア構成

| | 英語版 | 日本語版 |
|---|---|---|
| MFP | iR 5570/ iR 6570 | 同左 |
| 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 | |

表 2-5：<MFP 制御用ソフトウェア>に必要なソフトウェア構成

| | 英語版 | 日本語版 |
|---|---|---|
| <MFP 制御用ソフトウェア> | System Software（英語版） | System Software（国内版） |
| 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） |

また、<MFP 制御用ソフトウェア>は、キヤノン製プリンタドライバの下記に対応する。

| | 英語版 | 日本語版 |
|---|---|---|
| キヤノン製<br>プリンタドライバ | Canon PCL5e/5c Printer Driver for Microsoft Windows Version 6.60 以降<br>または<br>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<br>または<br>Canon LIPS LX Printer Driver for Microsoft Windows Version 1.20 以降 |

本 TOE の物理的範囲は、<Add-in ソフトウェア>および<MFP 制御用ソフトウェア>である。

## 2.3.2. TOE の論理的範囲

本 TOE は、<Add-in ソフトウェア>および<MFP 制御用ソフトウェア>において、以下のセキュリティ機能を持つ。

<Add-in ソフトウェア>
PDL データ暗号化機能
　TOE は、PDL データの暗号化を行う。

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している。
　本 ST での運用状態は、この設定機能を初期状態である有効化の状態に設定して運用していることを想定している。

<MFP 制御用ソフトウェア>
印刷ジョブデータ確認機能
　<Add-in ソフトウェア>にて印刷ジョブデータに追加されたユーザ固有の情報である「PDL データ暗号鍵の HASH 値」を、<MFP 制御用ソフトウェア>において正しいことを確認した場合のみ、印刷処理を継続させる。
　<MFP 制御用ソフトウェア>における確認方法は、以下のように行う。
　まず、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て、得られた PDL データ暗号鍵（以下、「復号された PDL データ暗号鍵」と略す）を利用する。

「復号された PDL データ暗号鍵」から HASH 値を求める。
この HASH 値と、<Add-in ソフトウェア>にてジョブ情報として追加した「PDL データ暗号鍵の HASH 値」の一致により、印刷ジョブデータの正当な所有者を確認している。

PDL データ復号機能
TOE は、暗号化された PDL データの復号を行う。

## 2.4. 資産

本 TOE の資産は下記である。
PDL データ

# 3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

## 3.1. 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.IC_CARD:　　IC カードの管理**
各ユーザは、IC カードを他人に利用されないように管理する。

**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。

## 3.2. 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。

## 3.3. 組織のセキュリティ方針

組織のセキュリティ方針は存在しない。

# 4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

## 4.1. TOE のセキュリティ対策方針

**O.CONFIRM_PRINTJOB: 印刷ジョブデータの確認**
TOE は<MFP 制御用ソフトウェア>において、印刷ジョブデータの正当な所有者の確認を行ってから印刷を行う。

**O.ENCRYPT_SEND: PDL 暗号化転送**
TOE は<Add-in ソフトウェア>において、印刷内容が盗聴されないように PDL データを暗号化して、<MFP 制御用ソフトウェア>に転送する。

**O.SETTING: セキュリティ機能の設定機能**
TOE は<Add-in ソフトウェア>において、プリンタ管理者に対して、TOE のセキュリティ機能を有効化/無効化できる設定機能を提供する。

## 4.2. 環境のセキュリティ対策方針

### 4.2.1. IT 環境のセキュリティ対策方針

**OE.ENCRYPT_KEY: PDL データ暗号鍵の暗号化**
IC カードは、PDL データ暗号鍵の暗号化を行い、および「PDL データ暗号鍵の HASH 値」を求める。

**OE.ROLE: 対応する MFP の設定**
OS は、プリンタプロパティの設定のできるプリンタ管理者の役割を維持管理する。

**OE.DECRYPT_KEY: PDL データ暗号鍵の復号**
IC カードは、「暗号化された PDL データ暗号鍵」を復号する。

### 4.2.2. non-IT 環境のセキュリティ対策方針

**OE.PRODUCTS: TOE に対応した製品**
ユーザは、TOE の機能を利用するために、TOE に対応した以下の製品を用いる。
<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

**OE.SETTING：　　セキュリティ機能の有効化**
プリンタ管理者は、<Add-in ソフトウェア>において、TOE セキュリティ機能を有効化する。

**OE.IC_CARD：　　IC カードの管理**
各ユーザは、IC カードを他人に利用されないように管理する。

# 5. セキュリティ要件

本章では、TOE のセキュリティ要件、IT 環境のセキュリティ要件について記述する。
機能コンポーネントは、CC パート 2 で規定されているコンポーネントを引用して、下記の操作を施した。
選択の場合は、[選択: 暴露、改変、使用不可]のように、選択した内容に下線にて操作を行った。
割付の場合は、[割付:プリンタ管理者]のように、割付した内容に下線にて操作を行った。
繰返しの場合は、コンポーネント名の後ろに a,b,c のアルファベットを付与して、操作を行った。
また、セキュリティ機能要件を理解しやすいように、<Add-in ソフトウェア>、<MFP 制御用ソフトウェア>に関連するセキュリティ機能要件に分類して、<Add-in ソフトウェア>に関連するセキュリティ機能要件には末尾に A を、<MFP 制御用ソフトウェア>に関連するセキュリティ機能要件には末尾に M を付与した。
表 5-1 に、TOE および IT 環境で要求しているセキュリティ機能要件一覧を示す。

**表 5-1:セキュリティ機能要件の一覧**

| | | | セキュリティ機能要件 |
|---|---|---|---|
| TOE | <Add-in ソフトウェア> | | FCS_CKM.1A<br>FCS_CKM.4A<br>FCS_COP.1Aa<br>FMT_MOF.1A |
| | <MFP 制御用ソフトウェア> | | FCS_CKM.4M<br>FCS_COP.1Ma<br>FCS_COP.1Mb<br>FDP_IFC.1M<br>FDP_IFF.1M<br>FMT_MSA.3M<br>FPT_RVM.1M |
| IT 環境 | <Add-in ソフトウェア> | IC カード | FCS_COP.1Ab<br>FCS_COP.1Ac |
| | | OS | FIA_UID.2A<br>FMT_SMR.1A |
| | <MFP 制御用ソフトウェア> | IC カード | FCS_COP.1Mc |

# 5.1. TOE セキュリティ要件

本章では、TOE のセキュリティ要件について記述する。

## 5.1.1. TOE セキュリティ機能要件

本章では、TOE のセキュリティ機能要件を記述する。
なお、すべての TOE のセキュリティ機能要件は、CC パート 2 に規定のセキュリティ機能要件である。

### 5.1.1.1. <Add-in ソフトウェア>のセキュリティ機能要件

#### 5.1.1.1.1. FCS (暗号サポート)

**FCS_CKM.1A 暗号鍵生成**

下位階層: なし

FCS_CKM.1.1 TSFは、以下の[割付: 以下の暗号鍵生成リストの〈標準〉]に合致する、指定された暗号鍵生成アルゴリズム[割付: 以下の暗号鍵生成リストの〈暗号鍵生成アルゴリズム〉]と指定された暗号鍵長[割付: 以下の暗号鍵生成リストの〈鍵長〉]に従って、暗号鍵を生成しなければならない。

表 5-2:暗号鍵生成リスト

| 暗号鍵生成 | 標準 | 暗号鍵生成アルゴリズム | 鍵長 |
|---|---|---|---|
| Triple DES 用<br>PDL データ暗号鍵の生成 | 指定無し | 擬似乱数生成 | 168bit |
| AES 用<br>PDL データ暗号鍵の生成 | 指定無し | 擬似乱数生成 | 256bit |

依存性: [FCS_CKM.2 暗号鍵配付
または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

**FCS_CKM.4A 暗号鍵破棄**

下位階層: なし

FCS_CKM.4.1 TSFは、以下の[割付:指定無し]に合致する、指定された暗号鍵破棄方法[割付: NULL クリア]に従って、暗号鍵を破棄しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

### FCS_COP.1Aa 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

表 5-3：暗号操作リスト

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| PDL データの Triple DES 暗号化 | FIPS PUB 46-3 | Triple DES | 168bit |
| PDL データの AES 暗号化 | FIPS PUB 197 | AES | 256bit |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

#### 5.1.1.1.2. FMT (セキュリティ管理)

### FMT_MOF.1A セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1 TSFは、機能[割付: TOEのセキュリティ機能][選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付:プリンタ管理者]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

## 5.1.1.2. <MFP 制御用ソフトウェア>のセキュリティ機能要件

#### 5.1.1.2.1. FCS (暗号サポート)

### FCS_CKM.4M 暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 TSFは、以下の[割付: 指定無し]に合致する、指定された暗号鍵破棄方法[割付: NULL クリア]に従って、暗号鍵を破棄しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または

FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

### FCS_COP.1Ma 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

**表 5-4：暗号操作リスト**

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| PDL データの Triple DES 復号 | FIPS PUB 46-3 | Triple DES | 168bit |
| PDL データの AES 復号 | FIPS PUB 197 | AES | 256bit |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

### FCS_COP.1Mb 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

**表 5-5：暗号操作リスト**

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| 「復号された PDL データ暗号鍵」の HASH | FIPS PUB 180-2 | SHA-1 | ― |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

## 5.1.1.2.2. FDP (利用者データ保護)

### FDP_IFC.1M サブセット情報フロー制御

下位階層: なし

FDP_IFC.1.1 TSFは、[割付: 以下の情報フロー要因のサブジェクト、情報、及び、操作のリスト]に対して[割付: 印刷ジョブデータフロー制御]を実施しなければならない。

表 5-6:情報フロー要因

| サブジェクト | 情報 | 操作 |
|---|---|---|
| ユーザサブジェクト | 印刷ジョブデータ | 遮断、通過 |

依存性: FDP_IFF.1 単純セキュリティ属性

### FDP_IFF.1M 単純セキュリティ属性

下位階層: なし

FDP_IFF.1.1 TSFは、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: 印刷ジョブデータフロー制御 ]を実施しなければならない: [割付: 下記の印刷ジョブデータフロー制御のセキュリティ属性 ]。

表 5-7:印刷ジョブデータフロー制御のセキュリティ属性

| サブジェクト | サブジェクトのセキュリティ属性 |
|---|---|
| ユーザサブジェクト | <MFP 制御用ソフトウェア>において「復号された PDL データ暗号鍵」から求めた HASH 値 |
| **情報** | **情報のセキュリティ属性** |
| 印刷ジョブデータ | 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」 |

FDP_IFF.1.2 TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付:下記の情報フローの規則 ]。

表 5-8:情報フローの規則

| 規則内容 |
|---|
| <MFP 制御用ソフトウェア>において「復号された PDL データ暗号鍵」から求めた HASH 値と、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」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させる |

FDP_IFF.1.3 TSFは、[割付: なし ]を実施しなければならない。

FDP_IFF.1.4 TSFは、以下の[割付: なし ]を提供しなければならない。

FDP_IFF.1.5 TSFは、以下の規則に基づいて、情報フローを明示的に承認しなければならない: [割付: なし ]

FDP_IFF.1.6 TSFは、次の規則に基づいて、情報フローを明示的に拒否しなければならない: [割付: なし ]

依存性: FDP_IFC.1 サブセット情報フロー制御
FMT_MSA.3 静的属性初期化

#### 5.1.1.2.3. FMT (セキュリティ管理)

**FMT_MSA.3M 静的属性初期化**

下位階層: なし

FMT_MSA.3.1 TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択: 制限的、許可的、[割付:なし]]デフォルト値を与える[割付: 印刷ジョブデータフロー制御 ]を実施しなければならない。

FMT_MSA.3.2 TSFは、オブジェクトや情報が生成されるとき、[割付: なし ]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

#### 5.1.1.2.4. FPT (TSF の保護)

**FPT_RVM.1M TSP の非バイパス性**

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

## 5.1.2. 最小機能強度レベル

本 ST では、最小機能強度は SOF-基本を主張する。
また、TOE では暗号アルゴリズムを利用しているが、暗号アルゴリズムの機能強度は CC の適用範囲外である。

## 5.1.3. TOE セキュリティ保証要件

本章では、TOE のセキュリティ保証要件を記述する。
この TOE の保証要件は、EAL2 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている EAL2 のコンポーネントをそのまま使用する。

表 5-9:評価保証レベル: EAL2

| 保証要件クラス | 保証要件コンポーネント |
|---|---|
| ACM | ACM_CAP.2 |

| 保証要件クラス | 保証要件コンポーネント |
|---|---|
| ADO | ADO_DEL.1, ADO_IGS.1 |
| ADV | ADV_FSP.1, ADV_HLD.1, ADV_RCR.1 |
| AGD | AGD_ADM.1, AGD_USR.1 |
| ATE | ATE_COV.1, ATE_FUN.1, ATE_IND.2 |
| AVA | AVA_SOF.1, AVA_VLA.1 |

# 5.2. IT 環境のセキュリティ要件

本章では、IT 環境セキュリティ要件について記述する。

## 5.2.1. IT 環境のセキュリティ機能要件

本章では、IT 環境のセキュリティ機能要件を記述する。
なお、すべての IT 環境のセキュリティ機能要件は、CC パート 2 に規定のセキュリティ機能要件である。

### 5.2.1.1. <Add-in ソフトウェア>関連の IT 環境のセキュリティ機能要件

#### 5.2.1.1.1. FCS (暗号サポート)

**FCS_COP.1Ab 暗号操作**

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

表 5-10：暗号操作リスト

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| PDL データ暗号鍵の暗号化 | PKCS#1 | RSA | 1024bit |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

**FCS_COP.1Ac 暗号操作**

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

表 5-11：暗号操作リスト

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| PDL データ暗号鍵の HASH | FIPS PUB 180-2 | SHA-1 | — |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

#### 5.2.1.1.2. FIA (識別と認証)

**FIA_UID.2A アクション前の利用者識別**

下位階層: FIA_UID.1

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

#### 5.2.1.1.3. FMT (セキュリティ管理)

**FMT_SMR.1A セキュリティ役割**

下位階層: なし

FMT_SMR.1.1 TSFは、役割[割付: プリンタ管理者 ]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

### 5.2.1.2. <MFP 制御用ソフトウェア>関連の IT 環境のセキュリティ機能要件

#### 5.2.1.2.1. FCS (暗号サポート)

**FCS_COP.1Mc 暗号操作**

下位階層: なし

FCS_COP.1.1 TSFは、[割付：以下の暗号操作リストの〈標準〉]に合致する、特定された暗号アルゴリズム[割付：以下の暗号操作リストの〈暗号アルゴリズム〉]と暗号鍵長[割付：以下の暗号操作リストの〈鍵長〉]に従って、[割付：以下の暗号操作リストの〈暗号操作〉]を実行しなければならない。

表 5-12：暗号操作リスト

| 暗号操作 | 標準 | 暗号アルゴリズム | 鍵長 |
|---|---|---|---|
| 「暗号化された PDL データ暗号鍵」の復号 | PKCS#1 | RSA | 1024bit |

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

## 5.2.2. IT 環境のセキュリティ保証要件

本 TOE では、IT 環境のセキュリティ保証要件を必要としない。

# 6. TOE 要約仕様

この章では、TOE の要約仕様を記述する。

## 6.1. TOE セキュリティ機能の記述

表 6-1 に TOE セキュリティ機能を<Add-in ソフトウェア>と<MFP 制御用ソフトウェア>に分類した。

表 6-1:セキュリティ機能と対応するコンポーネント

| | セキュリティ機能 | 機能要件コンポーネント |
|---|---|---|
| <Add-in ソフトウェア> | SF.A.ENCRYPT | FCS_CKM.1A, FCS_CKM.4A, FCS_COP.1Aa |
| | SF.A.SETTING | FMT_MOF.1A |
| <MFP 制御用ソフトウェア> | SF.M.CONFIRM_PRINTJOB | FDP_IFC.1M, FDP_IFF.1M, FMT_MSA.3M, FPT_RVM.1M, FCS_COP.1Mb |
| | SF.M.DECRYPT | FCS_CKM.4M, FCS_COP.1Ma |

SF.M.CONFIRM_PRINTJOBにおけるHASHメカニズムが本STにおける確率的、順列的メカニズムであり、その機能強度レベルは、SOF-基本である。

### 6.1.1. <Add-in ソフトウェア>のセキュリティ機能

**SF.A.ENCRYPT:　　PDL データ暗号化機能**
FCS_CKM.1A, FCS_CKM.4A, FCS_COP.1Aa
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。(FCS_CKM.1A)
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。(FCS_COP.1Aa)
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。(FCS_CKM.4A)
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。(FCS_CKM.1A)
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。(FCS_COP.1Aa)
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。(FCS_CKM.4A)

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>にて印刷ジョブデータの正当な所有者を確認できるように、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**
FMT_MOF.1A
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。(FMT_MOF.1A)
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。

## 6.1.2. <MFP 制御用ソフトウェア>のセキュリティ機能

**SF.M.CONFIRM_PRINTJOB:　　印刷ジョブデータ確認機能**
FCS_COP.1Mb, FDP_IFC.1M, FDP_IFF.1M, FMT_MSA.3M, FPT_RVM.1M
あらかじめ、印刷ジョブデータの正当な所有者を確認できるように、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。(FCS_COP.1Mb)
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。(FDP_IFC.1M, FDP_IFF.1M, FMT_MSA.3M, FPT_RVM.1M)

**SF.M.DECRYPT:　　PDL データ復号機能**
FCS_CKM.4M, FCS_COP.1Ma
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。(FCS_COP.1Ma)
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。(FCS_CKM.4M)
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。(FCS_COP.1Ma)
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。(FCS_CKM.4M)

# 6.2. 保証手段

この章では、TOE のセキュリティ保証手段を記述する。以下のセキュリティ保証手段は、5.1.3. 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-2:保証手段と対応するコンポーネント

| 保証要件コンポーネント | 保証手段 |
|---|---|
| ASE | 本 Security Target |
| ACM_CAP.2 | Encrypted Printing Software-B1 Configuration Management |
| ADO_DEL.1 | Encrypted Printing Software-B1 Delivery Procedures |
| ADO_IGS.1 | <Add-in ソフトウェア> Readme.txt<br><MFP 制御用ソフトウェア> セキュアプリント機能拡張キット（暗号化）・B1 設置手順書<br><MFP 制御用ソフトウェア> Encrypted Printing Software-B1 Installation Procedure |
| ADV_FSP.1 | Encrypted Printing Software-B1 Security Development |
| ADV_HLD.1 | |
| ADV_RCR.1 | |
| AGD_ADM.1 | <Add-in ソフトウェア>Help ファイル<br><Add-in ソフトウェア>Readme.txt<br><MFP 制御用ソフトウェア> 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<br><MFP 制御用ソフトウェア> Encrypted Printing Software User's Guide |
| AGD_USR.1 | |
| ATE_COV.1 | Encrypted Printing Software-B1 Test Plan<br>Encrypted Printing Software-B1 Test Report |
| ATE_FUN.1 | |
| ATE_IND.2 | TOE |
| AVA_VLA.1 | Encrypted Printing Software-B1 Vulnerability Analysis |
| AVA_SOF.1 | |

# 7. PP 主張

この章では、PP 主張について記述する。

## 7.1. PP 参照

参照した PP はない。

## 7.2. PP 修正

修正した PP はない。

## 7.3. PP 追加

PP への追加はない。

# 8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

## 8.1. セキュリティ対策方針根拠

本節では、セキュリティ対策方針が、TOE セキュリティ環境で規定した脅威、前提条件に対抗していることを示す。

**表 8-1:セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針および前提条件の対応表**

| | A.PRODUCTS | A.IC_CARD | A.SETTING | T.WIRETAP_DATA | T.PRINTOUT | T.MISUSE |
|---|---|---|---|---|---|---|
| O.CONFIRM_PRINTJOB | | | | | X | |
| O.ENCRYPT_SEND | | | | X | | |
| O.SETTING | | | | | | X |
| OE.ROLE | | | X | | | |
| OE.ENCRYPT_KEY | | | | X | | |
| OE.DECRYPT_KEY | | | | | X | |
| OE.PRODUCTS | X | | | | | |
| OE.SETTING | | | X | | | |
| OE.IC_CARD | | X | | | | |

### 8.1.1. 脅威に関する根拠

T.WIRETAP_DATA は、以下の対策方針によって対抗される。
O.ENCRYPT_SEND、OE.ENCRYPT_KEY
なぜならば、

O.ENCRYPT_SEND によって、TOE 内部の通信において、印刷内容が盗聴されないように、PDL データを暗号化して転送する。
この PDL データを暗号化するための、PDL データ暗号鍵は、OE.ENCRYPT_KEY によって、IC カードの機能にて暗号化を行われる。

T.PRINTOUT は、以下の対策方針によって実現される。
O.CONFIRM_PRINTJOB、OE.DECRYPT_KEY
なぜならば、
O.CONFIRM_PRINTJOB によって、TOE は、<Add-in ソフトウェア>にて印刷ジョブデータに追加されたユーザ固有の情報である「PDL データ暗号鍵の HASH 値」を、<MFP 制御用ソフトウェア>において正しいことを確認した場合のみ、印刷処理を継続させる、
ことが実現できる。
そのユーザ固有の情報は、OE.DECRYPT_KEY によって得られた「復号された PDL データ暗号鍵」、から求めた HASH 値である、
からである。

T.MISUSE は、以下の対策方針によって実現される。
O.SETTING
なぜならば、
O.SETTING によって、<Add-in ソフトウェア>において、プリンタ管理者に対して、TOE のセキュリティ機能を有効化/無効化できる設定機能を提供することで、プリンタ管理者以外の利用者はセキュリティ機能を無効化できなくなって誤操作を防いでいる、
からである。

## 8.1.2. 前提条件に関する根拠

A.PRODUCTS は、以下の対策方針によって対抗される。
OE.PRODUCTS
なぜならば、
ユーザは、TOE の機能を利用するために、TOE に対応した製品を用いる、
からである。

A. IC_CARD は、以下の対策方針によって対抗される。
OE.IC_CARD
なぜならば、
各ユーザは、IC カードを他人に利用されないように管理する、
からである。

A. SETTING は、以下の対策方針によって対抗される。
OE. SETTING、OE.ROLE
なぜならば、
OE.ROLE で維持されているプリンタ管理者は、OE.SETTING によって、セキュリティ機能を有効化に設定する、
からである。

# 8.2. セキュリティ要件根拠

## 8.2.1. セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応関係を表 8-2 に示す。

表 8-2:セキュリティ要件とセキュリティ対策方針の対応表

| | | TOE | | | | IT 環境 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | O.CONFIRM_PRINTJOB | O.ENCRYPT_SEND | O.SETTING | | OE.ROLE | OE.ENCRYPT_KEY | OE.DECRYPT_KEY | |
| TOE 機能要件 | FCS_CKM.1A | | X | | | | | | |
| | FCS_CKM.4A | | X | | | | | | |
| | FCS_COP.1Aa | | X | | | | | | |
| | FMT_MOF.1A | | | X | | | | | |
| | FCS_CKM.4M | X | | | | | | | |
| | FCS_COP.1Ma | X | | | | | | | |
| | FCS_COP.1Mb | X | | | | | | | |
| | FDP_IFC.1M | X | | | | | | | |
| | FDP_IFF.1M | X | | | | | | | |
| | FMT_MSA.3M | X | | | | | | | |
| | FPT_RVM.1M | X | | | | | | | |
| IT 環境 | FCS_COP.1Ab | | | | | | X | | |
| | FCS_COP.1Ac | | | | | | X | | |
| | FIA_UID.2A | | | | | X | | | |
| | FMT_SMR.1A | | | | | X | | | |
| | FCS_COP.1Mc | | | | | | | X | |

O.CONFIRM_PRINTJOB は、以下のセキュリティ要件によって実現される。
FCS_COP.1Ma、FCS_CKM.4M、FDP_IFC.1M、FDP_IFF.1M、FMT_MSA.3M、FPT_RVM.1M、FCS_COP.1Mb
なぜならば、

<MFP 制御用ソフトウェア>において、
FCS_COP.1Mb によって「復号された PDL データ暗号鍵」から求めた HASH 値を計算する。
FDP_IFC.1M、FDP_IFF.1M によって、
「復号された PDL データ暗号鍵」から求めた HASH 値と、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」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させる、という印刷ジョブデータフロー制御を実施している。
FCS_COP.1Ma によって、「復号された PDL データ暗号鍵」を利用して PDL データの復号が行われ、印刷を行う。また、FCS_CKM.4M によって、「復号された PDL データ暗号鍵」を破棄している。
FMT_MSA.3M によって、印刷ジョブデータフロー制御のデフォルト値は制限的になっている。
さらに、FPT_RVM.1M によって印刷ジョブデータフロー制御のバイパスが防止されている、
からである。

O.ENCRYPT_SEND は、以下のセキュリティ要件によって実現される。
FCS_CKM.1A、FCS_CKM.4A、FCS_COP.1Aa
なぜならば、
PDL データの<Add-in ソフトウェア>の PDL データ暗号化機能と<MFP 制御用ソフトウェア>の PDL データ復号機能を利用して、PDL データの機密性を保護している、
その、PDL データの<Add-in ソフトウェア>の暗号化機能は、
FCS_CKM.1A によって、TOE は、PDL データを暗号化するために必要な PDL データ暗号鍵の生成を行い、
FCS_COP.1Aa によって、生成した暗号鍵を使って PDL データの暗号化を行い、
FCS_CKM.4A によって、PDL データ暗号鍵を破棄する、
によって成立する、

からである。

O.SETTING は、以下のセキュリティ要件によって実現される。
FMT_MOF.1A
なぜならば、
FMT_MOF.1A によって、TOE のセキュリティ機能が有効化/無効化する機能はプリンタ管理者のみに限定される、
からである。

OE.ENCRYPT_KEY は、以下のセキュリティ要件によって実現される。
FCS_COP.1Ab、FCS_COP.1Ac
なぜならば、
FCS_COP.1Ab によって、IC カードにおいて PDL データ暗号鍵の暗号化を行い、
FCS_COP.1Ac によって、IC カードにおいて「PDL データ暗号鍵の HASH 値」を求める、
からである。

OE.ROLE は、以下のセキュリティ要件によって実現される。
FIA_UID.2A、FMT_SMR.1A
なぜならば、
FMT_SMR.1A によって、OS において、プリンタ管理者の役割は維持管理され、
FIA_UID.2A によって、OS において、そのプリンタ管理者の OS における識別を必要とする、
からである。

OE.DECRYPT_KEY は、以下のセキュリティ要件によって実現される。
FCS_COP.1Mc
なぜならば、
FCS_COP.1Mc によって、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」を復号する、
からである。

## 8.2.2. セキュリティ保証要件根拠

TOE への脅威は、「PC から印刷装置までの経路中の印刷ジョブデータの盗聴により印刷内容を知られること」と「不正に印刷装置を操作して印刷出力させ、その印刷内容を知りうることができる。」である。前者の脅威に対抗するべく、印刷内容の機密を保護する機能を、後者の脅威に対抗するべく、印刷ジョブデータの正当な所有者を確認してから印刷を行う機能を提供している。本 TOE は、一般のオフィスで利用される PC 上で動作するソフトウェアと MFP で動作するソフトウェアである。そのため、一般のユーザによる低レベルの攻撃に対抗する。
従って、TOE の保証としては、TOE の機能と、インタフェースの仕様の確認と、その内容の正確性をインタフェースからのテストによって確認できる EAL2 が妥当である。

## 8.2.3. セキュリティ要件依存性

セキュリティ要件のコンポーネントの依存性を、表 8-3 に示す。
CC が要求する依存性に対して、ST での依存性の項では、ST 内で依存しているセキュリティ要件を下線で示し、除去したコンポーネントは (*) で示す。

表 8-3:セキュリティ要件依存性の対応表

| | セキュリティ要件 | CC が要求する依存性 | ST での依存性 |
|---|---|---|---|
| TOE 機能要件 | FCS_CKM.1A | FCS_CKM.2 またはFCS_COP.1<br>FCS_CKM.4<br>FMT_MSA.2 | FCS_COP.1A<br>FCS_CKM.4A<br>FMT_MSA.2 (*) |
| | FCS_CKM.4A | FDP_ITC.1 またはFCS_CKM.1<br>FMT_MSA.2 | FCS_CKM.1A<br>FMT_MSA.2 (*) |
| | FCS_COP.1Aa | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FCS_CKM.1A<br>FCS_CKM.4A<br>FMT_MSA.2 (*) |
| | FMT_MOF.1A | FMT_SMF.1<br>FMT_SMR.1 | FMT_SMF.1 (*)<br>FMT_SMR.1A |
| | FCS_CKM.4M | FDP_ITC.1 またはFCS_CKM.1<br>FMT_MSA.2 | FCS_CKM.1A<br>FMT_MSA.2 (*) |
| | FCS_COP.1Ma | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FCS_CKM.1A<br>FCS_CKM.4M<br>FMT_MSA.2 (*) |
| | FCS_COP.1Mb | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FDP_ITC.1 (*) または<br>FCS_CKM.1 (*)<br>FCS_CKM.4 (*)<br>FMT_MSA.2 (*) |
| | FDP_IFC.1M | FDP_IFF.1 | FDP_IFF.1M |
| | FDP_IFF.1M | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1M<br>FMT_MSA.3M |
| | FMT_MSA.3M | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1 (*)<br>FMT_SMR.1A (*) |
| | FPT_RVM.1M | — | — |

| | セキュリティ要件 | CC が要求する依存性 | ST での依存性 |
|---|---|---|---|
| IT 環境の機能要件 | FCS_COP.1Ab | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FDP_ITC.1 (*) または<br>FCS_CKM.1A (*)<br>FCS_CKM.4A (*)<br>FMT_MSA.2 (*) |
| | FCS_COP.1Ac | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FDP_ITC.1 (*) または<br>FCS_CKM.1A (*)<br>FCS_CKM.4A (*)<br>FMT_MSA.2 (*) |
| | FIA_UID.2A | ― | ― |
| | FMT_SMR.1A | FIA_UID.1 | FIA_UID.2A |
| | FCS_COP.1Mc | FDP_ITC.1 または FCS_CKM.1<br>FCS_CKM.4<br>FMT_MSA.2 | FDP_ITC.1 (*) または<br>FCS_CKM.1A (*)<br>FCS_CKM.4A (*)<br>FMT_MSA.2 (*) |

**依存性除去の理由**:
FMT_MSA.3M から、FMT_MSA.1、FMT_SMR.1 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FMT_MSA.3M では、印刷ジョブデータフロー制御で利用されるセキュリティ属性は、<MFP 制御用ソフトウェア>における、「復号された PDL データ暗号鍵」から求めた HASH 値、および、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」であるが、FMT_MSA.3.2 によって、その値の上書きをユーザにはできないようになっている。
したがって、セキュリティ属性の上書き機能をある役割に制限する FMT_MSA.1 の機能や、その役割を規定する FMT_SMR.1 の機能は必要なく、この依存関係を除去してもセキュリティ上問題はない。

FCS_CKM.1A、FCS_CKM.4A、FCS_COP.1Aa から、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_CKM.1A、FCS_CKM.4A、FCS_COP.1Aa にて要求している暗号鍵は同一の鍵であり、PDL データを暗号化するために鍵生成、暗号操作、鍵破棄される。この暗号鍵は PDL データを暗号化する際に動的に生成され、暗号化を行い、その後破棄という短いライフサイクルを持ち、TOE の中で永続的に維持管理される暗号鍵ではなく、特にセキュリティ属性を必要としない。従って、この依存関係を除去してもセキュリティ上問題はない。

FMT_MOF.1A から、FMT_SMF.1 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
本 TOE で選択している機能要件、その管理対象、実現するセキュリティ機能の表を示す。

**表 8-4: 管理機能のリスト**

| 機能要件 | CC にて要求されている管理 | TOE での管理機能 |
|---|---|---|
| FCS_CKM.1A | a) 暗号鍵属性の変更の管理 | なし (暗号鍵の属性変更を行っていない) |
| FCS_CKM.4A | a) 暗号鍵属性の変更の管理 | なし (暗号鍵の属性変更を行っていない) |
| FCS_COP.1Aa | 予見される管理アクティビティはない。 | N/A |
| FMT_MOF.1A | a) 役割グループの管理 | OS |
| FCS_CKM.4M | a) 暗号鍵属性の変更の管理 | なし (暗号鍵の属性変更を行っていない) |

| 機能要件 | CC にて要求されている管理 | TOE での管理機能 |
|---|---|---|
| FCS_COP.1Ma | 予見される管理アクティビティはない。 | N/A |
| FCS_COP.1Mb | 予見される管理アクティビティはない。 | N/A |
| FDP_IFC.1M | 予見される管理アクティビティはない。 | N/A |
| FDP_IFF.1M | a) 明示的なアクセスに基づく決定に使われる属性の管理。 | a) なし（明示的なアクセスに基づく決定に使われる属性が存在しない） |
| FMT_MSA.3M | a) 初期値を特定できる役割のグループを管理すること;<br>b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。 | a) なし（初期値を特定できない）<br>b) なし（デフォルト値を変更できない） |
| FPT_RVM.1M | 予見される管理アクティビティはない。 | N/A |

以上により、FMT_SMF.1 で列挙された管理機能の中で、TOE にて必要としている機能は、ひとつも存在せず、この依存関係を除去してもセキュリティ上問題はない。

FCS_CKM.4M、FCS_COP.1Ma から、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_CKM.4M、FCS_COP.1Ma にて要求している暗号鍵は同一の鍵であり、PDL データを復号するために暗号操作、鍵破棄される。この暗号鍵は、PDL データを復号するために IC カードの秘密鍵を使って「復号された PDL データ暗号鍵」を求め、その暗号鍵にて復号を行い、その後破棄という短いライフサイクルを持ち、TOE の中で永続的に維持管理される暗号鍵ではなく、特にセキュリティ属性を必要としない。従って、この依存関係を除去してもセキュリティ上問題はない。

FCS_COP.1Mb から、FDP_ITC.1 または FCS_CKM.1、FCS_CKM.4 、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_COP. 1Mb では、PDL データ暗号鍵の IC カードによる HASH 値を求めている。HASH 値を求めるという暗号化方式は、暗号鍵の使用を必要としないので、鍵のインポートや鍵生成、鍵破棄、鍵のセキュリティ属性チェックのような鍵管理の機能は必要なく、この依存関係を除去してもセキュリティ上問題はない。

FCS_COP.1Ab から、FDP_ITC.1 または FCS_CKM.1、FCS_CKM.4、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_COP.1Ab では、IT 環境の IC カードの公開鍵による PDL データ暗号鍵の暗号化を行っている。
PDL データ暗号鍵は IC カードの公開鍵にて暗号化される。ユーザが IC カードの公開鍵を利用する際には既に生成されている鍵であり、鍵のインポートや鍵生成、鍵破棄、鍵のセキュリティ属性チェックのような鍵管理の機能は TOE には必要なく、この依存関係を除去してもセキュリティ上問題はない。

FCS_COP.1Ac から、FDP_ITC.1 または FCS_CKM.1、FCS_CKM.4 、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_COP.1Ac では、PDL データ暗号鍵の IC カードによる HASH 値を求めている。HASH 値を求めるという暗号化方式は、暗号鍵の使用を必要としないので、鍵のインポートや鍵生成、鍵破棄、鍵のセキュリティ属性チェックのような鍵管理の機能は必要なく、この依存関係を除去してもセキュリティ上問題はない。

FCS_COP.1Mc から、FDP_ITC.1 または FCS_CKM.1、FCS_CKM.4、FMT_MSA.2 への依存性が満たされていないことについて、問題がない根拠を以下に示す。
FCS_COP.1 Mc では、IT 環境の IC カードの秘密鍵による「暗号化された PDL データ暗号鍵」の復号を行っている。

「暗号化された PDL データ暗号鍵」は IC カードの秘密鍵にて復号される。ユーザが IC カードの秘密鍵を利用する際には既に生成されている鍵であり、鍵のインポートや鍵生成、鍵破棄、鍵のセキュリティ属性チェックのような鍵管理の機能は TOE には必要なく、この依存関係を除去してもセキュリティ上問題はない。

また、<Add-in ソフトウェア>と<MFP 制御用ソフトウェア>において、相互サポートに関して記述する。
<Add-in ソフトウェア>において、動作している PC は一般の会社内での管理･運用されていることを想定しているので、セキュリティ機能の迂回やＴＯＥの改ざんについての特定の機能要件を必要としない。
非活性化に関しては、セキュリティ機能を非活性にする設定機能は有しているが、FMT_MOF.1A によってプリンタ管理者にのみ制限されている設定機能なので、セキュリティ上問題はない。
<MFP 制御用ソフトウェア>において、
バイパス防止に関しては FPT_RVM.1M により、FDP_IFC.1M、FDP_IFF.1M、FMT_MSA.3M による印刷ジョブデータフロー制御が迂回されないことが保証されている。
改ざん防止に関しては、MFP 側のインタフェースが印刷ジョブデータの印刷操作に限られており、TOE が改ざんされる事は無い。またセキュリティ機能を非活性化するインタフェースも存在しないため FMT_MOF.1 や FAU クラスも不要である。

### 8.2.4. 最小機能強度レベル根拠

本 ST では、最小機能強度は SOF-基本を主張する。
なぜならば、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。そのため、一般のユーザによる低レベルの攻撃に対抗する。したがって、最小機能強度レベルとして SOF-基本を主張するのは適切である。

## 8.3. TOE 要約仕様根拠

### 8.3.1. セキュリティ機能根拠

TOE のセキュリティ機能と、TOE の機能要件コンポーネントの対応を表 8-5 に示す。

表 8-5:TOE のセキュリティ機能と TOE の機能要件コンポーネントの対応表

| | FCS_CKM.1A | FCS_CKM.4A | FCS_COP.1Aa | FMT_MOF.1A | FCS_CKM.4M | FCS_COP.1Ma | FCS_COP.1Mb | FDP_IFC.1M | FDP_IFF.1M | FMT_MSA.3M | FPT_RVM.1M |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SF.A.ENCRYPT | X | X | X | | | | | | | | |
| SF.A.SETTING | | | | X | | | | | | | |
| SF.M.CONFIRM_PRINTJOB | | | | | | | X | X | X | X | X |
| SF.M.DECRYPT | | | | | X | X | | | | | |

FDP_IFC.1M、 FDP_IFF.1M、 FMT_MSA.3M、FPT_RVM.1M は、以下のセキュリティ機能によって実現される。
SF.M.CONFIRM_PRINTJOB

なぜならば、
SF.M.CONFIRM_PRINTJOB によって、<MFP 制御用ソフトウェア>において、IC カードにより「復号された PDL データ暗号鍵」から求めた HASH 値と、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」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させる、
という印刷ジョブデータフロー制御を実施し、
印刷ジョブデータフロー制御のデフォルト値は制限的になっている。
この印刷ジョブデータフローはバイパスができなくなっている、
からである。

FCS_CKM.1A は、以下のセキュリティ機能によって実現される。
SF.A.ENCRYPT
なぜならば、
SF.A.ENCRYPT は、Triple DES もしくは AES のどちらかを選択して、
Triple DES の場合は、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。
AES の場合は、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。
からである。

FCS_CKM.4A は、以下のセキュリティ機能によって実現される。
SF.A.ENCRYPT
なぜならば、
SF.A.ENCRYPT は、Triple DES もしくは AES のどちらかを選択して、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。
からである。

FCS_COP.1Aa は、以下のセキュリティ機能によって実現される。
SF.A.ENCRYPT
なぜならば、
SF.A.ENCRYPT は、Triple DES もしくは AES のどちらかを選択して、
Triple DES の場合は、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。
AES の場合は、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。
からである。

FMT_MOF.1A は、以下のセキュリティ機能によって実現される。
SF.A.SETTING
なぜならば、
SF.A.SETTING は、TOE のセキュリティ機能を、有効化もしくは無効化できる能力を、プリンタ管理者のみに提供する。
からである。

FCS_CKM.4M は、以下のセキュリティ機能によって実現される。
SF.M.DECRYPT
なぜならば、
SF.M.DECRYPT は、Triple DES もしくは AES のどちらかを選択して、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。
からである。

FCS_COP.1Ma は、以下のセキュリティ機能によって実現される。
SF.M.DECRYPT
なぜならば、

<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。
SF.M.DECRYPT 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。
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。
からである。

FCS_COP.1Mb は、以下のセキュリティ機能によって実現される。
SF.M.CONFIRM_PRINTJOB
なぜならば、
SF.M.CONFIRM_PRINTJOB は、<MFP 制御用ソフトウェア>において一連の下記の機能を行う。
<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 HASH 値を求める。
からである。

## 8.3.2. 機能強度根拠

本 ST における確率的・順列的メカニズムである SF.M.CONFIRM_PRINTJOB における機能強度レベルは、SOF-基本である。また本 ST における最小機能強度レベルは、SOF-基本であり、これらは一貫している。したがって、SF.M.CONFIRM_PRINTJOB における機能強度レベル、SOF-基本は適切である。

## 8.3.3. セキュリティ機能のコンビネーション

本 TOE では、まず、<Add-in ソフトウェア>のセキュリティ機能を利用するために、SF.A.SETTING によりセキュリティ機能を有効化にするように設定している必要がある。
「PC から印刷装置までの経路中の印刷ジョブデータの盗聴により印刷内容を知られること」という脅威に対しては
SF.A.ENCRYPT によって、<Add-in ソフトウェア>において PDL データの暗号化機能が実現され、
SF.M.DECRYPT によって、<MFP 制御用ソフトウェア>において PDL データの復号機能が実現され、この暗号化機能と復号機能によるチャネルを利用して、PDL データの機密性を保護している、
この SF.A.ENCRYPT と SF.M.DECRYPT の機能にて、印刷内容の機密を保護する機能を提供している。
次に、「不正に印刷装置を操作して印刷出力させ、その印刷内容を知りうることができる。」という脅威に対しては、
SF.M.CONFIRM_PRINTJOB によって、<MFP 制御用ソフトウェア>において、IC カードにより「復号された PDL データ暗号鍵」から求めた HASH 値と、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」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させる、
という印刷ジョブデータフロー制御を実施し、この印刷ジョブデータフローはバイパスができなくなっている、

以上のように、セキュリティ機能は、脅威に対して全体として相互サポートの構造をとっている。

## 8.3.4. 保証手段の根拠

各保証手段と、EAL2 の保証要件コンポーネントの対応関係を表 8-6 に示す。

**表 8-6:保証手段と TOE の保証要件コンポーネントの対応表**

| | ASE | ACM_CAP.2 | ADO_DEL.1 | ADO_IGS.1 | ADV_FSP.1 | ADV_HLD.1 | ADV_RCR.1 | AGD_ADM.1 | AGD_USR.1 | ATE_COV.1 | ATE_FUN.1 | ATE_IND.2 | AVA_VLA.1 | AVA_SOF.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 本 Security Target | X | | | | | | | | | | | | | |
| Encrypted Printing Software-B1 Configuration Management | | X | | | | | | | | | | | | |
| Encrypted Printing Software-B1 Delivery Procedures | | | X | | | | | | | | | | | |
| <Add-in ソフトウェア> Readme.txt | | | | X | | | | X | X | | | | | |
| <MFP 制御用ソフトウェア> セキュアプリント機能拡張キット(暗号化)・B1 設置手順書<br><MFP 制御用ソフトウェア> Encrypted Printing Software-B1 Installation Procedure | | | | X | | | | | | | | | | |
| Encrypted Printing Software-B1 Security Development | | | | | X | X | X | | | | | | | |
| <Add-in ソフトウェア> Help ファイル | | | | | | | | X | X | | | | | |
| <MFP 制御用ソフトウェア> 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<br><MFP 制御用ソフトウェア> Encrypted Printing Software User's Guide | | | | | | | | X | X | | | | | |
| Encrypted Printing Software-B1 Test Plan | | | | | | | | | | X | X | | | |
| Encrypted Printing Software-B1 Test Report | | | | | | | | | | X | X | | | |
| TOE | | | | | | | | | | | | X | | |
| Encrypted Printing Software-B1 Vulnerability Analysis | | | | | | | | | | | | | X | X |

上記の各保証手段は、以下の内容を記述している。

保証手段「Encrypted Printing Software-B1 Configuration Management」は、TOE の構成要素を明確に識別しているので、ACM_CAP.2 を満たしている。

保証手段「Encrypted Printing Software-B1 Delivery Procedures」は、TOE の配送時に、セキュリティを維持するために必要な手続きを記述しているので、ADO_DEL.1 を満たしている。

保証手段「<Add-in ソフトウェア>Readme.txt」は、TOE の<Add-in ソフトウェア>のセキュアな設置、生成、及び立上げ手順について記述しているので、ADO_IGS.1 を満たしている。

保証手段「<MFP 制御用ソフトウェア> セキュアプリント機能拡張キット(暗号化)・B1 設置手順書」
「<MFP 制御用ソフトウェア> Encrypted Printing Software-B1 Installation Procedure」は、TOE の<MFP 制御用ソフトウェア>のセキュアな設置、生成、及び立上げ手順について記述しているので、ADO_IGS.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Security Development」は、TOE の非形式的機能仕様を記述しているので、ADV_FSP.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Security Development」は、TOE の記述的上位レベル設計を記述しているので、ADV_HLD.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Security Development」は、TOE の非形式的対応の実証を記述しているので、ADV_RCR.1 を満たしている。

保証手段「<Add-in ソフトウェア>Help ファイル」および「<Add-in ソフトウェア>Readme.txt」は、TOE の<Add-in ソフトウェア>の管理者向けのガイダンスを記述しているので、AGD_ADM.1 を満たしている。

保証手段「<Add-in ソフトウェア>Help ファイル」および「<Add-in ソフトウェア>Readme.txt」は、TOE の<Add-in ソフトウェア>のユーザ向けのガイダンスを記述しているので、AGD_USR.1 を満たしている。

保証手段「<MFP 制御用ソフトウェア> 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」「<MFP 制御用ソフトウェア> Encrypted Printing Software User's Guide」は、TOE の<MFP 制御用ソフトウェア>の管理者向けのガイダンスを記述しているので、AGD_ADM.1 を満たしている。

保証手段「<MFP 制御用ソフトウェア> 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」「<MFP 制御用ソフトウェア> Encrypted Printing Software User's Guide」は、TOE の<MFP 制御用ソフトウェア>のユーザ向けのガイダンスを記述しているので、AGD_USR.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Test Plan」および「Encrypted Printing Software-B1 Test Report」は、識別されたテストと TSF の対応を記述しているので、ATE_COV.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Test Plan」および「Encrypted Printing Software-B1 Test Report」は、TSF のテスト結果を示す証跡資料であるので、ATE_FUN.1 を満たしている。

保証手段「TOE」は、評価者が独立テストを行うために必要であるので ATE_IND.2 を満たしている。

保証手段「Encrypted Printing Software-B1 Vulnerability Analysis」は、明白な脆弱性、識別された脆弱性について記述しているので、AVA_VLA.1 を満たしている。

保証手段「Encrypted Printing Software-B1 Vulnerability Analysis」は、TOE のセキュリティ機能強度分析を記述しているので、AVA_SOF.1 を満たしている。

従って、提供する保証手段によって、EAL2 に必要な保証要件を満たしている。

以上