EXCEED YOUR VISION

EpsonNet ID Print Authentication Print Module
セキュリティターゲット

Ver1.11

2008 年 6 月 24 日

セイコーエプソン株式会社

変更履歴

Ver	変更日	変更内容	変更箇所	作成	承認
1.1	2007/04/06	新規作成	全体	杢屋	-
1.2	2007/05/16	「2.6.3 利用方法」「2.6.4 運用方法」を削除、指摘事項反映	2 章､3 章、4 章、8 章	杢屋	青木
		その他誤字修正等	全体		
		承認欄追加	変更履歴		
1.3	2007/06/18	機能要件 FMT_MOF.1 を削除。その他指摘事項反映。	全体	杢屋	青木
1.4	2007/08/06	海外版の製品名称変更。TOE バージョン変更。	1 章	杢屋	青木
		対応プリンタ機種追加	2 章		
		その他、誤字等指摘事項を修正。	全体		
1.5	2007/09/07	前提条件の表現見直し	3 章､4 章、6 章	杢屋	青木
		保証手段のドキュメント名称修正	6 章		
1.6	2007/09/13	誤記修正	全体	杢屋	青木
1.7	2007/09/26	保証手段修正	6 章	杢屋	青木
		相互サポート表記修正	8 章		
1.8	2007/10/29	誤字修正。指摘事項修正。	全体	杢屋	青木
		機能強度主張修正。	6 章		
1.9	2008/02/06	商標、製品名の表記見直し	1.5, 2.1.3	杢屋	青木
		保証手段にドキュメント追加	6.2		
		最小機能強度、機能強度主張修正	5.1.3, 6.1.2		
		前提条件・対策方針の表現見直し	3.1, 4.2		
		相互サポートに無効化防止を追記	8.2.4		
		その他、誤字などを修正	全体		
1.10	2008/03/18	保証手段にドキュメント追加・修正	6.2	杢屋	青木
		「セキュリティ機能要件のセキュリティ属性」を追記	8.2.5		
		最小機能強度の妥当性の記述を修正	8.2.6		
1.11	2008/06/24	JavaVM に関する記述を追記。その他誤字修正。 2.7 評価構成を追記。	1 章、2 章	杢屋	青木

目次

1. ST 概説

本章では ST 概説として、ST 識別、ST 概要、CC 適合、及び用語について述べる。

1.1. ST 識別

本 ST の識別情報は以下の通りである。

ST 名称		:EpsonNet ID Print Authentication Print Module セキュリティターゲット
ST バージョン		:1.11
作成日		:2008/6/24
作成者		:セイコーエプソン株式会社 ビジネス機器事業部 ビジネス機器事業推進部
TOE 名称	(日本語版)	:EpsonNet ID Print Authentication Print Module
	(英語版)	:EpsonNet ID Print Authentication Print Module
TOE バージョン	(日本語版)	:1.5b
	(英語版)	:1.5bE
評価保証レベル		:EAL2
キーワード		:セイコーエプソン、EPSON、レーザプリンタ、プリンタ、複合機、認証印刷、認証
CC バージョン		:Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 情報技術セキュリティ評価のためのコモンクライテリア パート 1:概説と一般モデル バージョン 2.3 2005 年 8 月 CCMB-2005-08-001 パート 2:セキュリティ機能要件 バージョン 2.3 2005 年 8 月 CCMB-2005-08-002 パート 3:セキュリティ保証要件 バージョン 2.3 2005 年 8 月 CCMB-2005-08-003 補足-0512

1.2. ST 概要

本 ST は、セイコーエプソン株式会社製プリンタおよび複合機のプリンタ部分（以降ではこれらを総称してプリンタと表記する）のオプション製品である認証印刷機能付きネットワーク IF カード（以降ではネットワークカードと表記する）に搭載される Offirio SynergyWare ID Print(海外版：EpsonNet Authentication Print)の認証印刷モジュールのセキュリティ仕様について記述するものである。TOE は、ネットワークカード上の ROM に組み込まれたソフトウェア、および PC 上で動作する附属アプリケーションソフトウェアからなる JavaVM 上で動作するソフトウェア製品である。
本 TOE は、ユーザが印刷を依頼した印刷データを、プリンタに接続された認証装置により印刷者本人を確認してから印刷物として出力する機能を提供する。これにより、印刷を依頼した印刷データを印刷者が印刷物として取得するまでの間に印刷データが不正に暴露されることを防止するものである。

1.3. CC 適合

本 ST は以下の CC に適合している。

- 機能要件：CC Part2 適合
- 保証要件：CC Part3 適合
- 評価保証レベル：EAL2
- 適合している PP はない

1.4. 用語、略語

本 ST の用語及び略語は以下の通りである。

用語	内容
プリンタ設定情報	ネットワークカードに格納されている、認証印刷に関する設定情報。認証装置の種類、認証方法、ユーザ識別情報の作成規則、プリンタパスワードがある。
プリンタパスワード	プリンタ設定情報を変更するためのパスワード。
認証印刷	印刷者の識別・認証をおこなってから印刷物を出力する印刷方法。
印刷依頼	ユーザが、クライアント PC からプリンタに対して認証印刷による印刷を依頼する行為。
印刷出力	ユーザが印刷依頼した印刷データをプリンタが印刷物として出力する動作。
印刷データ	ユーザが印刷出力するデータ。
印刷ジョブ	印刷データに印刷方法やユーザ識別情報を加えたデータ。ユーザが印刷依頼を実行すると、プリンタドライバによって印刷ジョブが作成される。
印刷方法	印刷用紙のサイズ、印刷の向きなど、印刷データを印刷する方法についての情報。
ユーザ識別情報	印刷を依頼したユーザを識別する情報。デフォルトでは、ユーザが利用しているクライアント PC のログインユーザ名が識別情報となる。なお、利用環境に応じて、ユーザ識別情報となる情報は変更できる。
ユーザ識別情報を記録した媒体	認証装置に読み込ませる ID カードや生体情報などの認証媒体。
ネットワーク IF カード	プリンタや複合機にネットワーク接続機能を追加するための、ネットワークインターフェースカード。

略語	内容
CC	コモンクライテリア（Common Criteria)
EAL	評価保証レベル（Evaluation Assurance Level）
IT	情報技術（Information Technology）
PP	プロテクションプロファイル（Protection Profile）
SF	セキュリティ機能（Security Function）
SFP	セキュリティ機能方針（Security Function Policy）
SOF	機能強度（Strength of Function）

ST	セキュリティターゲット（Security Target）
TOE	評価対象（Target of Evaluation）
TSC	TSF 制御範囲（TSF Scope of Control）
TSF	TOE セキュリティ機能（TOE Security Functions）
TSP	TOE セキュリティ方針（TOE Security Policy）

1.5. 商標

本 ST では、下記正式名称の製品を、下記略称で表記している。

正式名称	略称
Microsoft® Windows® 2000 Operating System	Windows 2000
Microsoft® Windows® XP Operating System	Windows XP
Microsoft® Windows Server® 2003 Operating System	Windows Server 2003
Microsoft® Windows Vista® Operating System	Windows Vista
Java™ Platform Standard Edition 6	Java SE6

Microsoft、Windows、Windows Server、Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標である。

なお、本 ST では、上記の製品の特定のエディション、ファミリを指定する場合には、「Windows 2000 Server」、「Windows Vista Business」のように、略称の後ろに追記する形で表記する。また、各製品に対する特定の Service Pack(以下 SP)を指定する場合には、「Windows 2000 SP4」のように、略称の後ろに追記する形で表記する。

Java および Java 関連の商標およびロゴは、米国 Sun Microsystems.Inc. の米国およびその他の国における登録商標である。

その他、記載の商品名、会社名は、各社の登録商標または商標である。

2. TOE 記述

本章では TOE 記述として、TOE 種別、TOE の説明、関係者、保護資産、物理的構成、論理的構成、及び利用方法について記述する。

2.1. TOE の概要

2.1.1.TOE 種別

本 TOE は、社内 LAN などのネットワーク環境に接続されるプリンタ利用時において、ユーザが印刷を依頼した印刷データを、ユーザ本人を識別したうえで、本人の目前で印刷出力する機能を提供するための JavaVM 上で動作するソフトウェア製品である。
本 TOE は、プリンタのオプション製品であるネットワークカードおよびその附属アプリケーションソフトウェアとして提供される。

2.1.2.利用目的

本 TOE は、プリンタに出力された印刷物を、印刷を依頼したユーザ以外の人物が持ち去ることにより、印刷したデータが漏洩することを防止する目的で利用する。
一般的なオフィス内で社内 LAN に接続されたプリンタを利用する場面では、プリンタの出力トレイに出力されたまま印刷物が長時間放置されていたり、複数のユーザが出力した印刷物が重なって残っていたりする場合がある。このような場合、印刷を依頼したユーザ以外の者により出力トレイに放置されている印刷物が持ち去られ、印刷データの内容が漏洩する恐れがある。実際、プリンタからの印刷データの漏洩の多くは、出力トレイに残された印刷物の持ち去りにより発生している。
本 TOE は、上記のような脅威から印刷データを保護する。

2.1.3.利用環境

本 TOE は、一般的なオフィス内の LAN 環境において、ネットワークに接続されたプリンタを複数のユーザで利用する環境を想定している。すなわち、LAN 環境に接続されたプリンタに対し、同じく LAN に接続された各ユーザのクライアント PC から印刷依頼が行われるような環境である。
本 TOE は、ユーザの印刷依頼により作成された印刷ジョブをすぐにプリンタに送信するのではなく、その印刷ジョブに印刷を依頼したユーザを識別するためのユーザ識別情報を付与した上で、一時的に保持しておき、ユーザがプリンタ側の認証装置によりユーザ情報を記録した媒体を読み込ませるなどの操作を行った際に認証装置から送られる情報に基づいてユーザを識別し、保持している印刷ジョブのうち、識別したユーザの印刷ジョブをプリンタに送信するという機能を実現している。ここで利用

されるユーザ識別情報としてどのような情報を利用するかについては、環境に応じて設定が可能である。したがって、TOE を利用するユーザを一意に識別できる情報であれば、社員番号や PC のログイン ID などがそのまま利用できる。また、ディレクトリサービスやデータベースにより、社員番号などを一元管理している環境であれば、そのサーバの情報をそのまま利用することも可能である。

本 TOE では、印刷ジョブを一時保持する機能をどこに持たせるかによって、以下の２つの方式を用意している。

１）サーバ経由方式

ユーザの印刷依頼により作成された印刷ジョブを一時的に保持するためのサーバを設け、印刷ジョブをまとめてこのサーバ上に保持する方式である。この方式を利用する場合の一般的な利用環境の構成図を図 1 に示す。図中の各構成要素については、表 1 に示す通りである。なお、図中の認証印刷サーバが、印刷ジョブを一時的に保持する役割を果たす。

図中に示した通り、TOE は、ネットワークカード、認証印刷サーバに含まれるソフトウェアである。

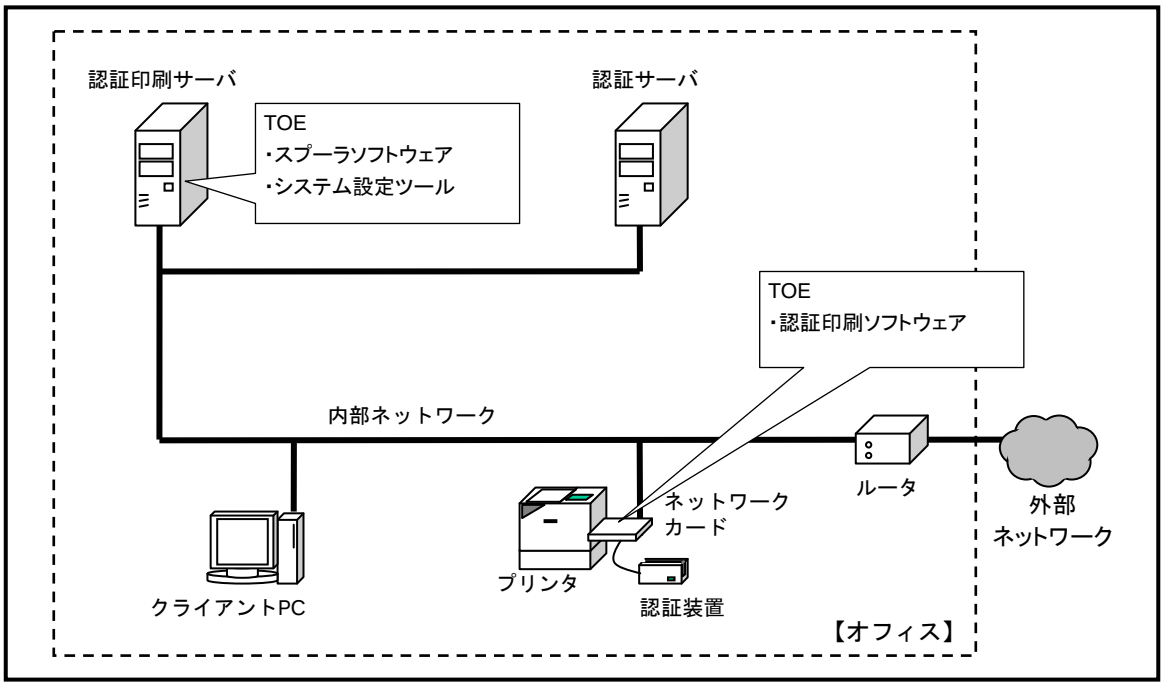

図 1：利用環境（サーバ経由方式）

２）直接印刷方式

ユーザの印刷依頼により作成された印刷ジョブを、各クライアント PC 自身に一時的に保持する方式である。この方式を用いる場合、認証印刷サーバは不要となる。

こちらの方式で利用する場合の構成図を図 2 に示す。なお、こちらの図の構成要素も、表 1 に示した通りである。

図中に示した通り、TOE はネットワークカード、クライアント PC に含まれるソフトウェアである。なお、クライアント PC に含まれる TOE のソフトウェアは、クライアント PC が複数ある場合には、すべてのクライアント PC にインストールされる。

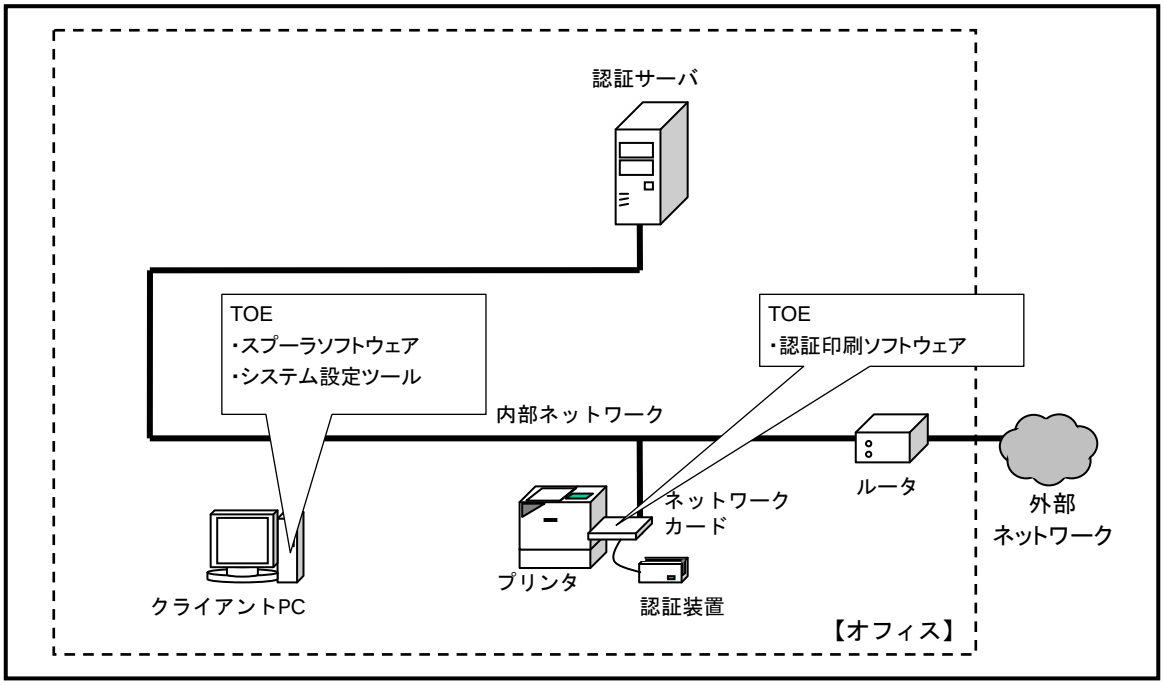

図 2：利用環境（直接印刷方式）

表 1: 利用環境の構成要素

構成要素	内容
クライアント PC	ユーザが業務に利用している PC。ユーザはこの PC から認証印刷の印刷依頼を実行する。認証印刷を利用するために必要な、いくつかのアプリケーションソフトウェアがインストールされる。 下記 JavaVM が動作可能な PC であることが条件となる。 ・ Java SE6 update3 以降 なお、図中にはクライアント PC は 1 台しか接続されていないが、複数台接続される場合も考えられる（認証印刷サーバを利用する場合は最大 50 台）。
プリンタ	TOE を含むネットワークカードが搭載可能なセイコーエプソン製品。TOE を含むネットワークカードが搭載可能なプリンタや複合機などの製品（表 2 に示す）が対象となる。 なお、図中にはプリンタは 1 台しか接続されていないが、複数台接続される場合も考えられる。
ネットワークカード	セイコーエプソン製プリンタ・複合機用オプション製品である認証印刷機能付きネットワーク IF カード。TOE は、このネットワークカードに含まれるソフトウェアとして実装される。 対応ネットワークカードは以下に示す通りである。 ・ PRIFNW7S(日本語版 [仕向け先：日本])に同梱されるネットワークカード ・ C12C824402(英語版 [仕向け先：海外])に同梱されるネットワークカード ※C12C824402 は PRIFNW7S の英語版であり、ハードウェアは同じものである。
認証装置	ネットワークカードに接続される、ユーザを識別・認証する装置。ユーザの認証を行い、識別情報を読み込む。磁気カードリーダや IC カードリーダ、生体認証装置など、認証媒体を利用する認証装置。

認証印刷サーバ (図 1 のみ)	ユーザの印刷依頼により作成された印刷ジョブを、ユーザの識別・認証が行われるまでの間保持するサーバ PC。 下記 JavaVM が動作可能な PC であることが条件となる。 ・ Java SE6 update3 以降 TOE は、この PC にインストールされるアプリケーションソフトウェアである。 なお、直接印刷方式の場合には、各クライアント PC が認証印刷サーバの役割を果たすため、この認証印刷サーバは不要である。
認証サーバ	ユーザ識別情報を管理しているサーバ。ディレクトリサーバなどが利用される。
ルータ	外部ネットワークと内部ネットワークの間のルータ。外部ネットワークからの侵入を防止する。
内部ネットワーク	ルータにより外部ネットワークから遮断されており、外部ネットワークからの攻撃を受けないネットワーク環境。
外部ネットワーク	インターネットなどの不特定多数の人間が利用しているネットワーク環境。さまざまな悪意を持った行為を行う可能性のある人がいる環境。
オフィス	ユーザが TOE による認証印刷を利用するエリア。一般的なオフィス環境が想定される。

※：クライアント PC で認証印刷を利用するために必要なアプリケーションソフトウェアをインストール可能な OS は以下の通りである。なお、以下の OS は、JavaVM がサポートしているものである。

Windows 2000 Server (SP4 以降)
Windows 2000 Professional (SP4 以降)
Windows Server 2003 (SP2 以降)
Windows XP Professional (SP2 以降)
Windows Vista Ultimate (今後リリースされる SP 含む)
Windows Vista Business (今後リリースされる SP 含む)
Windows Vista Enterprise (今後リリースされる SP 含む)
(64 ビット版を除く)

※：認証印刷サーバで認証印刷を利用するために必要なアプリケーションソフトウェアをインストール可能な OS は以下の通りである。なお、以下の OS は、JavaVM がサポートしているものである。

Windows 2000 Server (SP4 以降)
Windows Server 2003 (SP2 以降)
(64 ビット版を除く)

※：認証サーバ、外部ネットワークは、環境によっては無くてもよい。

表 2: 対象機種一覧

国内対象機種	海外対象機種
LP-S6500 シリーズ、LP-S7000 シリーズ、 LP-9800C シリーズ、LP-9200C シリーズ、 LP-9000C シリーズ、LP-8800C シリーズ、 LP-7000C シリーズ、LP-S4500 シリーズ、 LP-9200B シリーズ、LP-9100 シリーズ、 LP-7900 シリーズ、LP-8900 シリーズ、 LP-9000B シリーズ、LP-9400 シリーズ、 LP-2500 シリーズ、LP-M6500 シリーズ、 LP-M9800 シリーズ、LP-S3000 シリーズ、 LP-S4000 シリーズ、LP-M6000 シリーズ(*1) *1: LP-M6000 本体の「ユーザ識別機能」利用時を除く。	AcuLaser C3800 シリーズ、 AcuLaser C2600 シリーズ、 AcuLaser C4200 シリーズ、 AcuLaser C9100 シリーズ、 AcuLaser 2600 シリーズ、 EPL-N2550 シリーズ、 EPL-N3000 シリーズ、 AL-M4000 シリーズ

*: 全シリーズについて、PostScript ドライバなど ESC/Page 以外のドライバは対象外。

本 TOE を利用するときの流れを簡単に説明する。
まず、各ユーザは自分のクライアント PC から、印刷依頼を実行する。印刷依頼により作成された印刷ジョブは、印刷を依頼したユーザ（印刷者）のユーザ識別情報が付与された上で、認証印刷サーバ（サーバ経由方式の場合）あるいは各クライアント PC（直接印刷方式の場合）に一時保持される。
つぎに、印刷者は、TOE 外である、プリンタのネットワークカードに接続されている認証装置により、ユーザ情報を記録した媒体を読み込ませるなどの操作を行う。認証装置は読み込んだ情報を TOE に送信し、TOE は、認証装置から送信された情報に基づき印刷者を識別する。
TOE は、識別された印刷者のユーザ識別情報が付与された印刷ジョブをプリンタから印刷出力させる。

2.2. TOE の関係者

本節では関係者として、TOE の関係者を記述する。

表 3 : TOE の関係者

関係者名	内容
管理者	【役割】 TOE の利用環境構築・設定・管理(※1)を行う人。 【権限】 TOE の設置・初期設定・設定変更、ユーザ識別情報の決定、認証サーバの設定・運用。 【信頼度】 信頼できる。 【知識】 IT に関する知識もあり、プリンタについての知識も有している。

組織の責任者	【役割】	管理者を選定する。
	【権限】	TOE の導入を決定できる。
	【信頼度】	信頼できる。
	【知識】	想定される知識レベルはない(IT に関する知識は必要としない)。
ユーザ	【役割】	TOE による認証印刷を利用する人。
	【権限】	印刷の依頼。
	【信頼度】	必ずしも信頼できるとは言い切れない。 誤って他のユーザの印刷物を持っていく可能性あり。 悪意を持った行為を行う可能性あり。
	【知識】	基本的な IT に関する知識を有する。
サービスマン	【役割】	管理者の依頼により、TOE の利用環境構築・設定(※1)を行う人。
	【権限】	TOE の設置・初期設定・設定変更。
	【信頼度】	ユーザと同じ。
	【知識】	IT に関する知識もあり、プリンタについての知識も有している。
第三者	【役割】	TOE 利用環境のオフィス内で想定される、上記以外の人。 すなわち、認証印刷のユーザではないが、オフィス内に出入りする可能性がある人。例えば、他部署の者、宅配業者、清掃員、アルバイトなど。
	【権限】	なし。
	【信頼度】	ユーザと同じ。
	【知識】	基本的な IT に関する知識を有する。

※1：ガイダンスに従った TOE の設置、初期設定、設定の変更を指す。

2.3. 物理的構成

2.3.1.ハードウェア構成

本 TOE は、ネットワークカードおよび認証印刷サーバ、クライアント PC 上で動作するソフトウェアである。したがって、物理構成上の TOE の範囲は、ネットワークカードの ROM 上に実装されたソフトウェア、及び認証印刷サーバ、クライアント PC のハードディスク上にインストールされたソフトウェアになる。

TOE 利用時のハードウェア構成と実装されるソフトウェアの位置関係を、図 3、図 4 に示す。また、図中の各ソフトウェアの説明を表 4 に示す。

なお、図中の認証印刷サーバ、クライアント PC、プリンタ、ネットワークカード、認証サーバおよび認証装置については、「表 1：利用環境の構成要素」で説明した通りである。

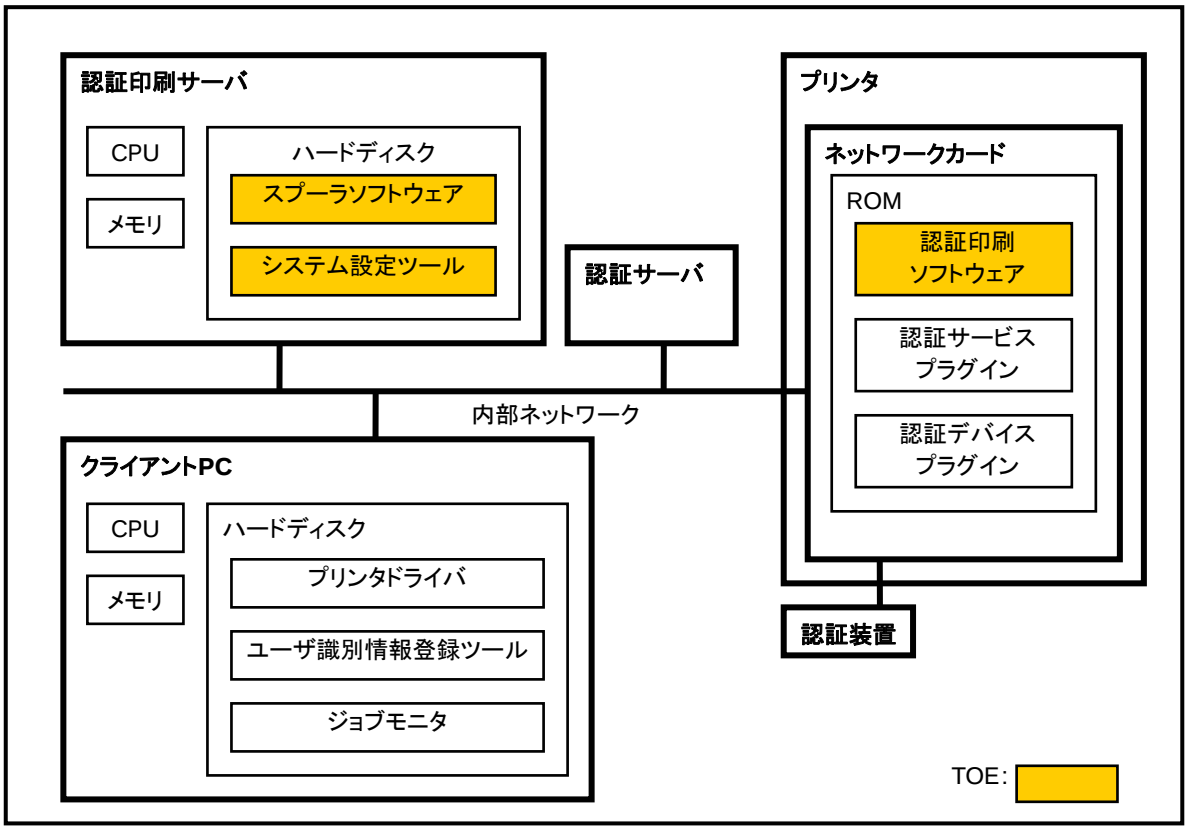

図 3 : TOE のハードウェア構成（サーバ経由方式）

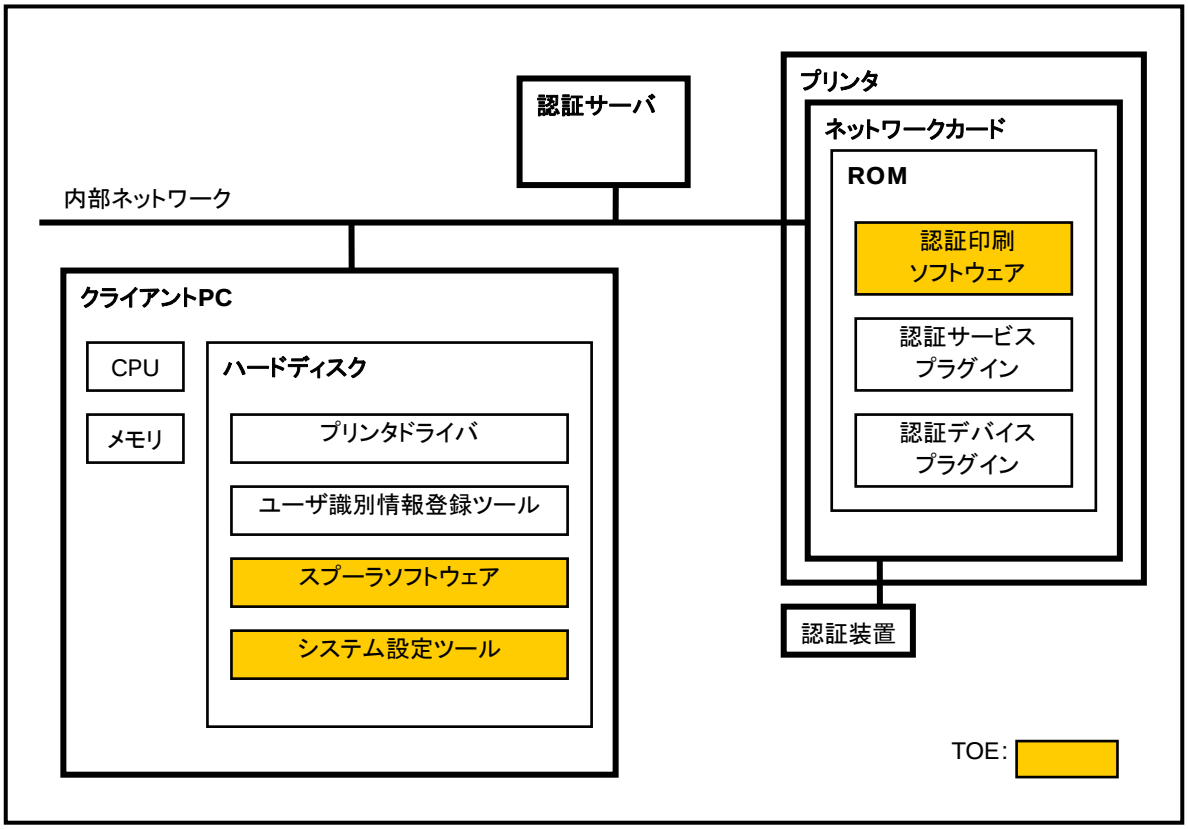

図 4 : TOE のハードウェア構成（直接印刷方式）

2.3.2. ソフトウェア構成

図 3、図 4 に示した各ソフトウェアは、実際には JavaVM や OS、プラットフォーム上で動作する。ソフトウェア構成から見た TOE の範囲を明確にするため、ソフトウェア構成図を図 5、図 6 に示す。

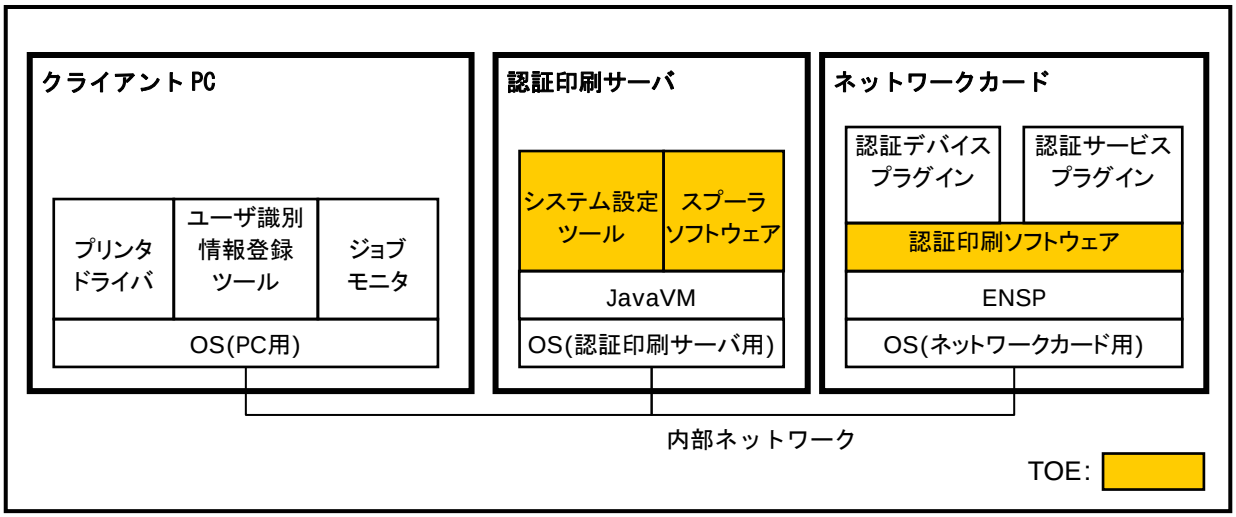

図 5 : TOE のソフトウェア構成（サーバ経由方式）

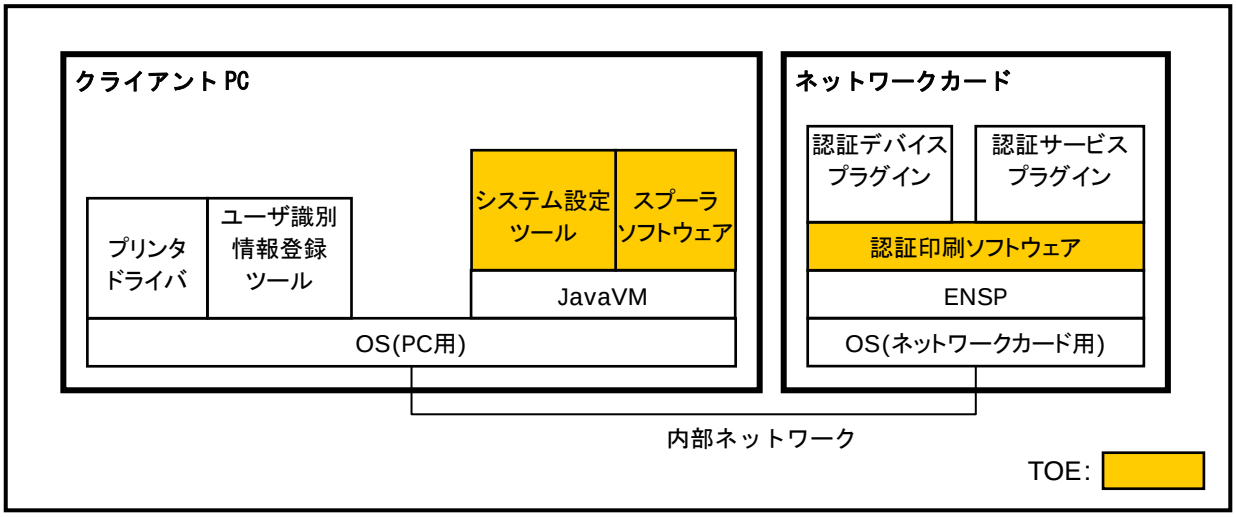

図 6 : TOE のソフトウェア構成（直接印刷方式）

2.3.3. ソフトウェア構成要素

TOE のソフトウェア構成要素の説明を表 4 に示す。

表 4: ソフトウェア構成要素

構成要素	内容
認証デバイスプラグイン	ネットワークカードに接続する認証装置を制御するプラグイン。プリンタ設定情報の設定内容に従い、認証装置から入力されたデータを加工する。認証サーバを利用しない場合は、加工したデータがそのままユーザ識別情報となる。接続する認証装置に対応するものを利用する。
認証サービスプラグイン	認証サーバ利用時に、認証サーバと認証印刷ソフトウェアを中継し、ユーザ識別情報を取得するためのプラグイン。認証デバイスプラグインが加工したデータをもとに、認証サーバにユーザ識別情報を問い合わせる。利用する認証サーバに対応するものを利用する。
認証印刷ソフトウェア	EpsonNet ID Print AuthBase. 認証装置から取得したユーザ識別情報に対応する印刷ジョブの有無をスプーラソフトウェアに問い合わせ、対応する印刷ジョブがあれば取得し、プリンタに転送する。また、印刷終了時には、スプーラソフトウェアに対し該当印刷ジョブの削除を依頼する。
ENSP	EpsonNet Service Platform。認証印刷ソフトウェアが動作するプラットフォーム。
JavaVM	スプーラソフトウェア、システム設定ツールを動作させるためのソフトウェア。
OS(ネットワークカード用)	ネットワークカードに実装される各ソフトウェアを動作させるための組込み機器用 OS。
OS(PC 用)	JavaVM を動作させるための OS。
OS（認証印刷サーバ用）	JavaVM を動作させるための OS。
スプーラソフトウェア	EpsonNet ID Print Spooler Service. ユーザ識別情報を付与した印刷ジョブを保持し、認証印刷ソフトウェアからの印刷ジョブの要求に対し印刷ジョブをプリンタに送るか送らないかを制御する。
システム設定ツール	EpsonNet ID Print システム設定. 認証印刷サーバの設定や、プリンタ設定情報を変更するためのツール。

プリンタドライバ	印刷ジョブの作成やプリンタの制御を行うドライバ。ユーザが印刷依頼した印刷データに対し、ユーザ識別情報などを付与した印刷ジョブを作成し、スプーラソフトウェアに送信する。 使用するプリンタに対応するものを利用する。 なお、図中ではプリンタドライバは「クライアント PC」にあるものとして記述しているが、「認証印刷サーバ」にインストールし共有利用する場合もある。
ジョブモニタ	スプーラソフトウェアに保持されている印刷ジョブを、印刷者自身が削除する際に利用するアプリケーション。なお、直接印刷方式の場合には、このアプリケーションはインストールされず、各クライアント PC のシステム設定ツールにて、印刷ジョブの削除を行う。
ユーザ識別情報登録ツール	印刷ジョブに付与するユーザ識別情報の設定・登録を行う。

2.3.4.物理構成の TOE 範囲

物理構成の TOE 範囲は、以下の表に示すソフトウェアである。

表 5 : TOE の物理的範囲と名称

TOE	提供されるソフトウェア名称	
	日本語版	英語版
認証印刷ソフトウェア	EpsonNet ID Print AuthBase	EpsonNet ID Print AuthBase
スプーラソフトウェア	EpsonNet ID Print Spooler Service	EpsonNet ID Print Spooler Service
システム設定ツール	EpsonNet ID Print システム設定	EpsonNet ID Print System Configuration

2.4. 論理的構成

2.4.1.論理構成

TOE の論理構成を図 7 に示す。なお、TOE は図中で指定した各機能である。

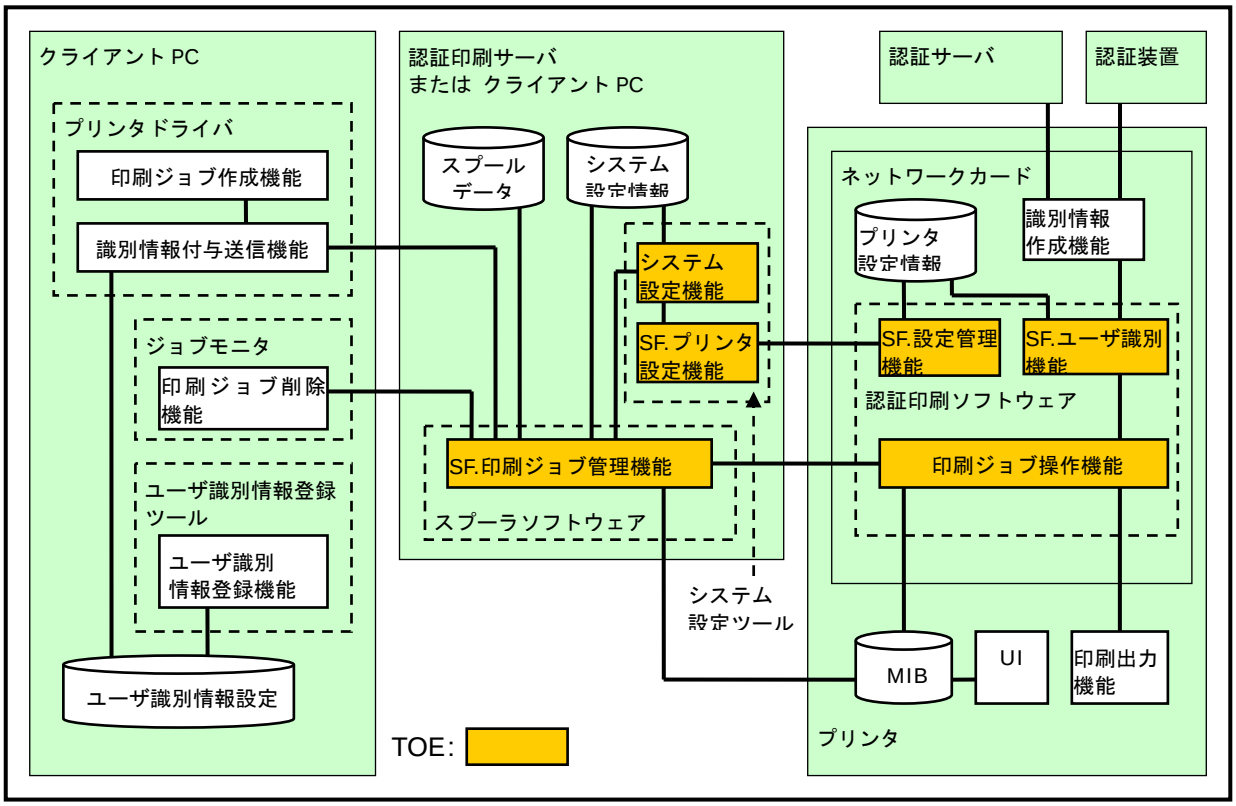

図 7 : TOE の論理的構成

2.4.2. 論理構成要素

TOE の論理構成要素の説明を、表 6 に示す。

表 6 : 論理構成要素一覧

構成要素	内容
印刷ジョブ作成機能	ユーザが印刷依頼した印刷データから、プリンタで印刷するための印刷方法などの情報をもつ印刷ジョブを作成する。
識別情報付与送信機能	ユーザ識別情報設定の内容により、印刷ジョブにユーザの識別情報を付与し、SF.印刷ジョブ管理機能に送信する。
ユーザ識別情報登録機能	ユーザ識別情報設定に、ユーザ識別情報として用いる情報を登録・変更する。
印刷ジョブ削除機能	サーバ経由方式利用時、認証印刷サーバのスプールデータにスプールされる印刷ジョブを削除する。他のクライアント PC から送信された印刷ジョブを削除することは出来ない。
ユーザ識別情報設定	印刷ジョブに付与するユーザ識別情報についての設定。
SF.印刷ジョブ管理機能	スプールデータの管理を行う。

システム設定機能	システム設定情報の設定・変更を行う。また、SF.印刷ジョブ管理機能に対して、指定した印刷ジョブの削除を依頼する。 プリンタ設定情報の設定変更時には、SF.プリンタ設定機能を呼び出す。 本機能は、システム設定ツールによって実装される。なお、システム設定ツールの起動時に識別認証が実施されるが、その識別認証機能はセキュリティ機能ではない。
SF.プリンタ設定機能	ネットワークカードの設定管理機能と連携し、プリンタ設定情報の設定・変更を行う。プリンタ設定情報を変更する画面に移行する前に、管理者の認証のためプリンタパスワードの入力を要求する。
スプールデータ	SF.印刷ジョブ管理機能により、一時的に保持されている印刷ジョブ。
システム設定情報	SF.印刷ジョブ管理機能の動作を決定する設定情報。以下の項目についての情報が含まれる。 ・ 印刷ジョブのタイムアウト時間（スプールデータに保持されてからここに設定された時間経過すると、印刷ジョブは自動的に削除される）。 ・ ウォームアップの ON/OFF（ON に設定されていると、識別情報付与送信機能から印刷ジョブを受け取った時点でプリンタのウォームアップを行う）。
識別情報作成機能	認証装置から読み込まれた情報から、プリンタ設定情報の設定内容に従い、ユーザ識別情報を作成する。設定内容によって、以下のいずれかの処理を行う。 ・ 認証装置から読み込まれた情報を加工し、ユーザ識別情報とする。 ・ 認証装置から読み込まれた情報を加工し、加工された情報を元に認証サーバに対してユーザ識別情報を要求・取得する。
SF.ユーザ識別機能	プリンタ設定情報の認証装置の設定、認証方法の設定により、識別情報作成機能に対してユーザ識別情報の作成を依頼し、得られたユーザ識別情報を印刷ジョブ操作機能に送信する。
SF.設定管理機能	プリンタ設定情報を管理する。
印刷ジョブ操作機能	SF.印刷ジョブ管理機能と連携し、識別されたユーザの印刷ジョブをプリンタの印刷出力機能に転送する。

プリンタ設定情報	認証印刷に関する以下の項目についての設定情報。 ・ 認証装置設定(認証装置の指定、認証装置固有の設定) ・ 認証方法設定(認証サーバ利用の有無) ・ ユーザ識別情報の作成規則 ・ プリンタパスワード
印刷出力機能	印刷ジョブ操作機能から送信された印刷ジョブに含まれる印刷データを、印刷物として出力する。
UI	印刷処理の状況について表示する。
MIB	Management Information Base. 機器の状態を管理するデータベース。

2.4.3.論理構成の TOE 範囲

論理構成の TOE 範囲は、以下にあげる各機能である。

表 7 : TOE の論理的範囲

機能を提供するソフトウェア	機能
認証印刷ソフトウェア	SF.ユーザ識別機能
	SF.設定管理機能
	印刷ジョブ操作機能
スプーラソフトウェア	SF.印刷ジョブ管理機能
システム設定ツール	SF.プリンタ設定機能
	システム設定機能

2.5. 保護資産

オフィス内におけるプリンタ利用時の情報漏えいの多くは、プリンタに出力されたまま、印刷者に取得されることなく放置された印刷物を、印刷者以外の人物によって故意または誤って持ち去られることにより発生している。
これは、多数のユーザが少数のプリンタを利用している状況で、ユーザが自分のクライアント PC から印刷を依頼すると、その後の印刷データの流れを制御できず、そのままプリンタに出力されてしまうことに起因する。

本 TOE は、ユーザの印刷依頼により作成された印刷ジョブにユーザ識別情報を付与した上で一度保持し、同じユーザ識別情報を持つプリンタ側からの出力要求に対してのみ応答する機能により、同じユーザ識別情報を持たない問い合わせから印刷データを保護する。

サーバ経由方式、直接印刷方式それぞれの場合の印刷データの流れを図に示す。保護対象となるのは、いずれの方式の場合も、スプーラに保持されてから印刷物として印刷者の手に渡るまでの間の印刷データである。

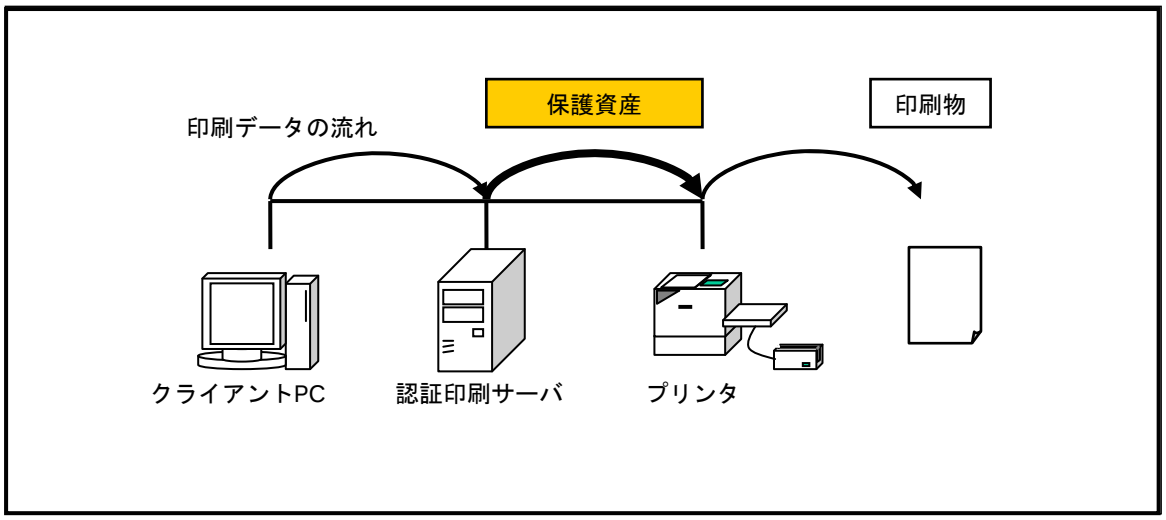

図 8：保護資産（サーバ経由方式）

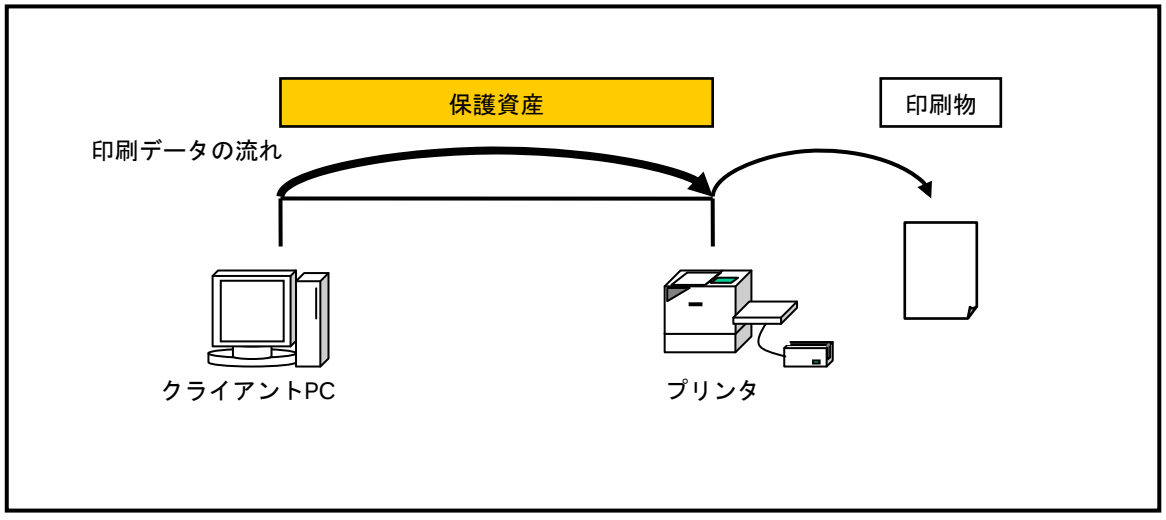

図 9：保護資産（直接印刷方式）

印刷データとは、ユーザが印刷出力を依頼したデータ自体を指す。印刷実行時に内部ネットワークを通過するのは印刷の処理単位である印刷ジョブであり、印刷データはこの中に含まれている。図 10 に、保護対象となる印刷データの範囲を示す。

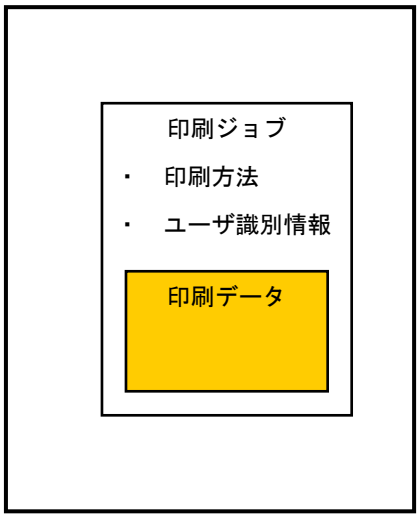

図 10：印刷データの範囲

2.6. TOE の機能

2.6.1. TOE が提供する機能

以下に、TOE が提供する各機能の説明を記述する。

2.6.1.1. セキュリティ機能

SF.ユーザ識別機能

ユーザの識別を行う機能。

- プリンタ設定情報の認証装置の設定、認証方法の設定により、識別情報作成機能に対してユーザ識別情報の作成を依頼。
- 取得したユーザ識別情報を、印刷ジョブ操作機能に送信。

SF.印刷ジョブ管理機能

スプールデータの管理を行う機能。スプールデータに対して以下の処理を行う。

- TOE 外である識別情報付与送信機能からユーザ識別情報を付与して送信された印刷ジョブにジョブ ID をつけてスプールデータに保持。
- 印刷ジョブ操作機能から指定されたユーザ識別情報を含む印刷ジョブのジョブ ID 一覧を印刷ジョブ操作機能に送信。
- 印刷ジョブ操作機能から指定されたジョブ ID に対応する印刷ジョブを印刷ジョブ操作機能を介してプリンタに転送。

SF.プリンタ設定機能

プリンタ設定情報にアクセスするための UI を提供する機能。

- プリンタ設定情報へのアクセスの前に管理者の認証を実施。
- プリンタ設定情報の設定変更画面を表示。

SF.設定管理機能

プリンタ設定情報を管理する機能。

- プリンタ設定情報へのアクセスを、認証された管理者に制限。

2.6.1.2. 非セキュリティ機能

印刷ジョブ操作機能

SF.印刷ジョブ管理機能と連携し、識別されたユーザの印刷ジョブをプリンタに転送する機能。

- SF.ユーザ識別機能からユーザ識別情報を受信。
- SF.印刷ジョブ管理機能にユーザ識別情報に対応する印刷ジョブのジョブ ID 一覧を問い合わせ。
- SF.印刷ジョブ管理機能から受信したジョブ ID 一覧に含まれる印刷ジョブを SF.印刷ジョブ管理機能に問い合わせ。
- SF.印刷ジョブ管理機能から受信した印刷ジョブをプリンタの印刷出力機能に転送。
- MIB を監視し、プリンタの状態や印刷出力の進捗状況を取得。
- MIB を介して、プリンタの UI に識別の成功・失敗、印刷の状況を表示。
- SF.印刷ジョブ管理機能に対し、印刷が終了した印刷ジョブの削除を依頼。

システム設定機能

システム設定情報の設定変更を行う機能。本機能は TSF ではない。

2.6.2.TOE が提供しない機能

本 TOE は、以下にあげる機能を提供しない。

- 印刷ジョブにユーザ識別情報を付与する機能。

2.7. 評価構成

TOEは、図１：利用環境（サーバ経由方式）及び、図２：利用環境（直接印刷方式）において、表１：利用環境の構成要素及び、表２：対象機種一覧に示す、複数のプリンタ、認証装置等の構成要素から任意に選択した環境で使用することができる。

TOEは、これら構成要素の違いによる影響を受けないため、評価構成は、各方式における代表的な以

下の構成とする。

(1) サーバ経由方式の評価構成

プリンタ	AL-C4200	
ネットワークカード	カード	C12C824402
	認証印刷ソフトウェア	EpsonNet ID Print AuthBase
	認証サービスプラグイン	EpsonNet Auth Proxy Plugin
	認証デバイスプラグイン	ENSP Device Control Libraries
	ENSP	ENSP Framework
認証装置	PcProx	
認証メディア	PcProx カード	
認証サーバ	認証サーバ	LDAP(Active Directory)
	認証プロキシサーバ	EpsonNet Authentication Server
認証印刷サーバ	システム設定ツール	EpsonNet ID Print System Configuration
	スプーラソフトウェア	EpsonNet ID Print Spooler Service
	JavaVM	JavaSE6 update3
	OS	Windows Server 2003 Enterprise Edition SP2(32bit)
クライアント PC	プリンタドライバ	AL-C4200 Printer Driver
	ユーザ識別情報登録ツール	EpsonNet ID Print User ID Register
	ジョブモニタ	EpsonNet ID Print Job Monitor
	OS	Windows XP Professional SP2(32bit)

(2) 直接印刷方式の評価構成

プリンタ	LP-S6500	
ネットワークカード	カード	PRIFNW7S
	認証印刷ソフトウェア	EpsonNet ID Print AuthBase
	認証印刷プラグイン	EpsonNet Auth Proxy Plugin
	認証デバイスプラグイン	ENSP Device Control Libraries
	ENSP	ENSP Framework
認証装置	PaSoRi / 磁気カードリーダ	
認証メディア	FeliCa カード/ 磁気カード	
認証サーバ	認証サーバ	LDAP(Active Directory)
	認証プロキシサーバ	EpsonNet 認証プロキシ for LDAP

クライアント PC	システム設定ツール	EpsonNet ID Print システム設定
	スプーラソフトウェア	EpsonNet ID Print Spooler Service
	JavaVM	JavaSE6 update3
	プリンタドライバ	LP-S6500 Printer Driver
	ユーザ識別情報登録ツール	EpsonNet ID Print ユーザ識別情報登録
	OS	Windows XP Professional SP2(32bit)

3. TOE セキュリティ環境

本章では、TOE セキュリティ環境として、前提条件、脅威、組織のセキュリティ方針について述べる。

3.1. 前提条件

想定する前提条件は以下の通りである。なお、サーバ経由方式、直接印刷方式の指定がないものは、両方式に共通する前提条件である。

A.管理者

管理者は、悪意を持った行為を行なうことはない。

A.サービスマン

管理者は、サービスマンが TOE の設置・初期設定およびこれら設定の変更を行なう際に、悪意を持った行為を行えない環境で実施させる。

A.ユーザ識別情報

ユーザ識別情報を記録した媒体は、他のユーザ、サービスマン、および第三者に利用されることはない。また、ユーザのクライアント PC に設定されたユーザ識別情報は、他のユーザ、サービスマン、および第三者に不正に変更されることはない。

A.スプールデータ

スプールデータは、不正アクセスやハードディスクの持ち去り、修理時の持ち出しにより暴露されることはない。

A.ネットワーク

TOE を利用するネットワーク環境は、以下の条件を満たす。

- 外部ネットワークからの攻撃を受けることはない。
- 内部ネットワークを流れるデータは、盗聴、改ざんされることはない。
- 管理者の管理下にない認証印刷機能付きネットワークカードが接続されることはない。
- 認証印刷サーバ利用時、管理者が設定した認証印刷サーバの IP アドレスを不正に利用され、認証印刷サーバになりすまされることはない。
- 認証サーバ利用時、管理者が設定した認証サーバの IP アドレスを不正に利用され、認証サーバになりすまされることはない。

3.2. 脅威

想定する脅威は以下の通りである。

T.印刷物の暴露

印刷者以外のユーザ、サービスマン、および第三者が、印刷物として出力された印刷者の印刷データを持ち出し、印刷データを暴露する。

T.設定情報の改ざん

ユーザ、サービスマン、および第三者が、管理者になりすましプリンタ設定情報を変更することで、印刷データを暴露するかもしれない。

なお、変更されることにより本脅威につながるプリンタ設定情報の設定項目、及び TOE 設置の際に管理者により設定される値または内容を、表 8 に示す。

表 8: プリンタ設定情報の項目と内容

プリンタ設定情報の設定項目	値または内容
認証装置の指定	使用する認証装置を指定
ユーザ識別情報の作成規則	ユーザを一意に識別できる設定値
認証方法の設定（認証サーバ利用の有無）	利用環境に合わせた設定値
プリンタパスワード	推測されにくい値に設定

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ない。

4. セキュリティ対策方針

本章では、セキュリティ対策方針として、TOE のセキュリティ対策方針、及び環境のセキュリティ対策方針について述べる。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針は以下の通りである。

O.印刷前のユーザ識別

TOE は、印刷物を出力する前に、ユーザを識別しなければならない。

O.印刷ジョブの制御

TOE は、印刷者に対してのみ、その印刷者が依頼した印刷物を出力しなければならない。

O.管理者の認証

TOE は、管理者がプリンタ設定情報を設定する前に、管理者を認証しなければならない。

O.プリンタ設定情報

TOE は、プリンタ設定情報の設定を、管理者のみに許可しなければならない。

4.2. 環境のセキュリティ対策方針

環境のセキュリティ対策方針は以下の通りである。なお、サーバ経由方式、直接印刷方式の指定がないものは、両方式に共通する対策方針である。

OE.管理者

TOE を導入する組織の責任者は、管理者として悪意を持った行為を行わない信頼できる者を選出しなければならない。

OE.サービスマンの作業

管理者は、サービスマンが TOE の設置・初期設定およびこれら設定の変更を行なう際には、悪意を持った行為を行わないよう作業に立ち会わなければならない。

OE.ユーザ識別情報管理

管理者は、ユーザ識別情報の管理として、以下のことを実施しなければならない。

- ユーザ識別情報を記録した媒体が、ユーザ本人以外に使用されないよう管理する。
- ユーザ識別情報を記録した媒体が、ユーザ本人以外に使用されないよう、ユーザに指示する。

ユーザは、ユーザ識別情報の管理として、以下のことを実施しなければならない。

- 管理者の指示に従い、ユーザ識別情報を記録した媒体が、ユーザ本人以外に使用されないように管理する。
- クライアント PC に設定されたユーザ識別情報が不正に変更されないよう、クライアント PC の OS のアカウントを管理する。

OE.認証印刷サーバ

サーバ経由方式利用時、管理者は、以下に示す運用を実施し、認証印刷サーバ内のスプールデータを不正アクセスやハードディスクの持ち出しによる暴露から保護しなければならない。

- 認証印刷サーバ内のハードディスクを不正に持ち出され、内部に保持されているスプールデータが暴露することのないよう、ハードディスクを保護する。
- 認証印刷サーバの修理時など、認証印刷サーバが管理者以外のものに渡る場合には、残っている印刷ジョブをすべて削除する。
- 認証印刷サーバの OS の Administrator 権限を持つアカウントが不正に利用され、スプールデータを読み出されることのないよう、認証印刷サーバの OS の Administrator 権限を持つアカウントがユーザ、サービスマン、及び第三者に漏洩しないよう管理する。

OE.クライアント PC

直接印刷方式利用時、ユーザは、以下に示す運用を実施し、自分のクライアント PC 内のスプールデータを不正アクセスやハードディスクの持ち出しによる暴露から保護しなければならない。

- クライアント PC 内のハードディスクを不正に持ち出され、内部に保持されているスプールデータが暴露することのないよう、ハードディスクを保護する。
- クライアント PC の修理時など､クライアント PC がユーザ以外のものに渡る場合には、残っている印刷ジョブをすべて削除する。
- ユーザの、クライアント PC の OS のアカウントを不正に利用され、ユーザになりすまされてスプールデータを読み出されることのないよう、クライアント PC の OS のアカウントが他のユーザ、サービスマン、及び第三者に漏洩しないよう管理する。

OE.ネットワーク

管理者は、TOE に対する外部ネットワークからの攻撃を遮断し、かつ内部ネットワークを流れる通信内容を暴露・改ざんから保護しなければならない。

管理者は、自分の管理下にない認証印刷機能付きネットワークカードが内部ネットワークに

接続されることのないよう、内部ネットワークに接続されている認証印刷機能付きネットワークカードを管理しなければならない。

認証印刷サーバ利用時、管理者は、内部ネットワークに接続した認証印刷サーバの IP アドレスが不正に利用され、認証印刷サーバに成りすまされることがないよう、IP アドレスを管理しなければならない。

認証サーバ利用時、管理者は、内部ネットワークに接続された認証サーバの IP アドレスが不正に利用され、認証サーバに成りすまされることがないよう、IP アドレスを管理しなければならない。

OE.プリンタパスワードの管理

管理者は、プリンタパスワードをデフォルトのパスワードから推測されにくいパスワードに変更し、管理者以外に漏洩しないよう、管理しなければならない。

OI.ユーザ識別情報付与

プリンタドライバは、ユーザが印刷依頼した印刷ジョブに対して、そのユーザのユーザ識別情報を付与しなければならない。

5. IT セキュリティ要件

本章では、IT セキュリティ要件として、TOE セキュリティ要件、及び環境に対するセキュリティ要件について述べる。

5.1. TOE セキュリティ要件

本節では、TOE セキュリティ要件として、TOE セキュリティ機能要件、TOE セキュリティ保証要件、及び最小機能強度について述べる。

5.1.1.TOE セキュリティ機能要件

TOE セキュリティ機能要件は以下の通りである。

FDP_IFC.1 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:サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]に対して[割付:情報フロー制御 SFP]を実施しなければならない。

[割付:サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]

サブジェクト：ユーザプロセス

情報：印刷ジョブ

操作：送信または保留

[割付:情報フロー制御 SFP]

印刷ジョブ制御

依存性: FDP_IFF.1 単純セキュリティ属性

FDP_IFF.1 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:情報フロー制御 SFP]を実施しなければならない:[割付:示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性]。

[割付:情報フロー制御 SFP]

印刷ジョブ制御

[割付:示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性]

サブジェクト：ユーザプロセス

セキュリティ属性：ユーザ識別情報

情報：印刷ジョブ

セキュリティ属性：ジョブ ID、ユーザ識別情報

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: 各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]。

[割付:各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]

ユーザプロセスのユーザ識別情報に一致するユーザ識別情報をもつ印刷ジョブのジョブ ID リストを作成し、ジョブ ID リストの中のジョブ ID と一致するジョブ ID をもつ印刷ジョブをプリンタの印刷出力機能に送信する。

一致するユーザ識別情報を持つ印刷ジョブがない場合、印刷ジョブの送信を保留する。

FDP_IFF.1.3 TSF は、[割付: 追加の情報フロー制御 SFP 規則]を実施しなければならない。

[割付:追加の情報フロー制御 SFP 規則]

なし

FDP_IFF.1.4 TSF は、以下の[割付: 追加の SFP 能力のリスト]を提供しなければならない。

[割付:追加の SFP 能力のリスト]

なし

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: セキュリティ属性に基づいて、明示的に情報フローを承認する規則]

[割付: セキュリティ属性に基づいて、明示的に情報フローを承認する規則]

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: セキュリティ属性に基づいて、明示的に情報フローを拒否する規則]

[割付: セキュリティ属性に基づいて、明示的に情報フローを拒否する規則]
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

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:セキュリティ属性のリスト]を維持しなければならない。

[割付:セキュリティ属性のリスト]
ユーザ識別情報

依存性: なし

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付: 定義された品質尺度]
5 文字以上 10 文字以内の英数混在

依存性: なし

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.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、各利用者に認証が成功することを要求しなければならない。

[詳細化] （※下線部について詳細化を行っている）
利用者：管理者

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1 TSF は、認証を行っている間、[割付: フィードバックのリスト]だけを利用者に提供しなければならない。

[割付: フィードバックのリスト]

入力された文字数分の”*”等の文字

依存性: FIA_UAU.1 認証のタイミング

FIA_UID.2 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。

[詳細化] （※下線部について詳細化を行っている）

利用者：ユーザ

依存性: なし

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1 TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]

ユーザ識別情報

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: 属性の最初の関連付けに関する規則]

[割付: 属性の最初の関連付けに関する規則]

なし

FIA_USB.1.3　TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: 属性の変更に関する規則]

[割付: 属性の変更に関する規則]

なし

依存性:　FIA_ATD.1 利用者属性定義

FMT_MSA.3(1) 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 : から一つのみ選択、[割付 : その他の特性]]デフォルト値を与える[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]

[割付 : その他の特性]

その他の特性：自動的に割り当てられる一意の整数値

[割付: アクセス制御 SFP、情報フロー制御 SFP]

印刷ジョブ制御

[詳細化]

セキュリティ属性：ジョブ ID（※下線部について詳細化を行っている）

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: 許可された識別された役割]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。

[割付: 許可された識別された役割]

なし

依存性　FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティの役割

FMT_MTD.1 TSF データの管理

下位階層:　なし

FMT_MTD.1.1　TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト]

認証装置の指定

ユーザ識別情報の作成規則

認証方法（認証サーバ利用の有無）

プリンタパスワード

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]

改変

[割付:許可された識別された役割]

管理者

依存性:　FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層:　なし

FMT_SMF.1.1　TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付:TSF によって提供されるセキュリティ管理機能のリスト]。

[割付:TSF によって提供されるセキュリティ管理機能のリスト]

表 9 に示す管理項目を管理する機能

依存性:　なし

表 9: セキュリティ管理機能一覧

機能要件	FMT における管理要件	管理項目
FDP_IFC.1	予見される管理アクティビティはない。	なし
FDP_IFF.1	明示的なアクセスに基づく決定に使われる属性の管理。	なし
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし
FIA_SOS.1	秘密の検証に使用される尺度の管理。	なし

FIA_UAU.2	管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	プリンタパスワードの管理機能(FMT_MTD.1)
FIA_UAU.7	予見される管理アクティビティはない。	なし
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	なし
FIA_UID.2	利用者識別情報の管理。	なし
FMT_MSA.3(1)	a) 初期値を特定できる役割のグループを管理すること; 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。	なし
FMT_MTD.1	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし
FMT_SMF.1	予見される管理アクティビティはない。	なし
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	なし
FPT_RVM.1	予見される管理アクティビティはない。	なし
FPT_SEP.1	予見される管理アクティビティはない。	なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSFは、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]

管理者

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

FPT_RVM.1 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

FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性: なし

5.1.2. TOE セキュリティ保証要件

TOE セキュリティ保証要件は以下の通りである。

表 10 : TOE セキュリティ保証要件

保証クラス	保証コンポーネント	
構成管理	ACM_CAP.2	構成要素
配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.1	記述的上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
テスト	ATE_COV.1	カバレージの証拠

	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.1.3.最小機能強度

本 TOE の最小機能強度は SOF-基本である。尚、対象となる TOE セキュリティ機能要件を以下に示す。

・ FIA_UAU.2

5.2. IT 環境に対するセキュリティ要件

IT 環境に対するセキュリティ要件は以下の通りである。

FMT_MSA.3(2) 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 : から一つのみ選択、[割付 : その他の特性]]デフォルト値を与える[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]

[割付 : その他の特性] : ユーザ識別情報

[割付: アクセス制御 SFP、情報フロー制御 SFP]

印刷ジョブ制御

[詳細化] （※下線部について詳細化を行っている）

セキュリティ属性：ユーザ識別情報

TSF:プリンタドライバ

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: 許可された識別された役割]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。

[割付: 許可された識別された役割]

なし

[詳細化] （※下線部について詳細化を行っている）

TSF:プリンタドライバ

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

6. TOE 要約仕様

本章では、TOE 要約仕様として、TOE セキュリティ機能、及び保証手段について述べる。

6.1. TOE セキュリティ機能

本節では、TOE セキュリティ機能として、TOE セキュリティ機能、セキュリティメカニズム、及び機能強度主張について述べる。

6.1.1. TOE セキュリティ機能

TOE セキュリティ機能は以下の通りである。

表 11 : TOE セキュリティ機能とセキュリティ機能要件の対応

	FDP_IFC.1	FDP_IFF.1	FIA_SOS.1	FIA_ATD.1	FIA_UAU.2	FIA_UAU.7	FIA_UID.2	FIA_USB.1	FMT_MSA.3(1)	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1
SF.ユーザ識別機能				○			○	○					○	○
SF.印刷ジョブ管理機能	○	○							○				○	○
SF.設定管理機能					○					○	○	○	○	○
SF.プリンタ設定機能			○			○							○	○

SF.ユーザ識別機能

本機能は、ユーザを識別する機能である。

TOE は、印刷物を出力する前に、識別情報作成機能に印刷者のユーザ識別情報を要求する[FIA_UID.2]。また、TOE は、印刷者を代行して動くサブジェクトに対してユーザ識別情報を関連付け、それを維持する[FIA_USB.1, FIA_ATD.1]。
この機能は、SF.印刷ジョブ管理機能によるフロー制御が行われる前に必ず実行される[FPT_RVM.1]。またこの機能は、他のプロセスから分離されたメモリ空間で実行される[FPT_SEP.1]。

SF.印刷ジョブ管理機能

本機能は、ユーザ識別情報に対応する印刷ジョブのみを、プリンタの印刷出力機能に転送する機能である。

TOE は、プリンタドライバによりユーザ識別情報が付与された印刷ジョブを受信する。
TOE は、受信した印刷ジョブに対し、ジョブ ID を割り当て保持する。ここで割り当てられるジョブ ID は、TOE により自動的に割り当てられる一意の整数値である[FMT_MSA.3(1)]。
TOE は、SF.ユーザ識別機能によりユーザ識別情報を受信したら、印刷ジョブ制御 SFP に従い、保持している印刷ジョブに対して以下のフロー制御を実施する[FDP_IFC.1, FDP_IFF.1]。

- 保持している印刷ジョブのうち、受信したユーザ識別情報と一致するユーザ識別情報を持つ印刷ジョブのジョブ ID 一覧を作成する。(印刷ジョブは複数あることが考えられるためリスト（一覧）になる。)
- 作成したリスト中のジョブ ID に対応する印刷ジョブをプリンタの印刷出力機能に転送する。
- 受信したユーザ識別情報と一致するユーザ識別情報を持つ印刷ジョブがない場合、印刷ジョブの送信を保留する。

これらの機能は、TSF 機能動作進行中に必ず実行される[FPT_RVM.1]。またこの機能は、他のプロセスから分離されたメモリ空間で実行される[FPT_SEP.1]。

SF.設定管理機能

本機能は、TOE のセキュリティ機能のふるまいの変更や、プリンタ設定情報の改変を行う能力を、認証された管理者に制限する機能である。

TOE は、プリンタ設定情報にアクセスする前に、プリンタパスワードを要求し、管理者を認証する[FIA_UAU.2]。
TOE は、管理者の役割を維持する。また、プリンタ設定情報を編集する画面を表示中、認証されたサブジェクトを管理者という役割に関連付ける。[FMT_SMR.1, FMT_SMF.1]
これにより、管理者のみが、下記の設定情報、内容を変更できるようになる。

- 認証装置の設定[FMT_MTD.1]
- 認証方法の設定(認証サーバ使用の有無)[FMT_MTD.1]
- プリンタパスワードの変更[FMT_MTD.1]
- ユーザ識別情報の作成規則[FMT_MTD.1]

これらの機能は、TSF 機能動作進行中に必ず実行される[FPT_RVM.1]。またこの機能は、他のプロセスから分離されたメモリ空間で実行される[FPT_SEP.1]。

SF.プリンタ設定機能

本機能は、プリンタ設定情報へのアクセスの際の、管理者を認証するためのプリンタパスワード入力画面を表示、プリンタ設定情報の編集画面を表示する機能である。

TOE は、プリンタパスワード入力画面では、入力されたパスワードを”*”等の文字で表示し、覗き見によるパスワードの漏洩を防止する[FIA_UAU.7]。
また、TOE は、プリンタパスワード変更時、推測されやすいパスワードへの設定を避けるた

めに、文字数を 5 文字以上 10 文字以内の英数混在という条件を満たさないパスワードには設定できないようにしている[FIA_SOS.1]。
これらの機能は、プリンタパスワード入力時、プリンタパスワード変更時に必ず実行される[FPT_RVM.1] またこの機能は、他のプロセスから分離されたメモリ空間で実行される[FPT_SEP.1]。

6.1.2.機能強度主張

TOE セキュリティ機能の内、非暗号で且つ確率的或いは順列的メカニズムに基づく物と、そのセキュリティ強度主張の対応を表 12 に示す。

表 12 : 機能強度

TOE セキュリティ機能	強度主張
SF.設定管理機能（パスワードによる認証メカニズム）	SOF-基本

6.2. 保証手段

保証手段として提供される文書は以下の通りである。

表 13 : 保証手段一覧

保証クラス	保証 コンポーネント	ドキュメント名称、及び TOE
ACM (構成管理)	ACM_CAP.2	・ EpsonNet ID Print 構成管理計画 ・ EpsonNet ID Print 構成リスト ・ EpsonNet ID Print バージョン管理表 ・ EpsonNet ID Print Install 構成
ADO (配付と運用)	ADO_DEL.1	・ PRIFNW7S/C12C824402 配付手順書 ・ EpsonNet ID Print Web 配付手順書

	ADO_IGS.1	・ PRIFNW7S はじめにお読みください ・ PRIFNW7S/U セットアップガイド ・ Offirio SynergyWare ID Print 管理者ガイド ・ Online Guide Supplement ・ EpsonNet Authentication Print Network Interface Card User's Guide ・ EpsonNet Authentication Print Software Administrator's Guide ・ Offirio SynergyWare ID Print アップデータ適用手順. ・ How to use EpsonNet Authentication Print Software Updater ・ PRIFNW7S ファームウェア アップデート手順 ・ How to use EpsonNet Authentication Print Network Interface Card Firmware Updater
ADV (開発)	ADV_FSP.1	・ EpsonNet ID Print 機能仕様書
	ADV_HLD.1	・ EpsonNet ID Print 上位レベル設計書
	ADV_RCR.1	・ EpsonNet ID Print 表現対応分析書
AGD (ガイダンス文書)	AGD_ADM.1	・ Offirio SynergyWare ID Print 管理者ガイド ・ EpsonNet Authentication Print Software Administrator's Guide
	AGD_USR.1	・ Offirio SynergyWare ID Print 利用者ガイド ・ EpsonNet Authentication Print Software User's Guide
ATE (テスト)	ATE_COV.1	・ EpsonNet ID Print テスト仕様書兼成績書 ・ EpsonNet ID Print テストカバレージ
	ATE_FUN.1	・ EpsonNet ID Print テスト仕様書兼成績書
	ATE_IND.2	・ EpsonNet ID Print テスト仕様書兼成績書
AVA (脆弱性評定)	AVA_SOF.1	・ EpsonNet ID Print 機能強度分析書
	AVA_VLA.1	・ EpsonNet ID Print 脆弱性分析書

7. PP 主張

本 ST は PP への適合を主張しない。

8. 根拠

本章では、根拠として、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、及び PP 主張根拠について述べる。

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根拠として、セキュリティ対策方針の必要性、及びセキュリティ対策方針の十分性について述べる。

8.1.1. セキュリティ対策方針の必要性

セキュリティ対策方針と TOE セキュリティ環境との対応を表 14 に示す。
表の通り、すべてのセキュリティ対策方針は少なくとも一つの TOE セキュリティ環境と対応している。従って、すべてのセキュリティ対策方針の必要性は満たされている。

表 14 : TOE セキュリティ環境とセキュリティ対策方針の対応

	A. 管理者	A.サービスマン	A.ユーザ識別情報	A.スプールデータ	A.ネットワーク	T.印刷物の暴露	T.設定情報の改ざん
O.印刷前のユーザ識別						○	
O.印刷ジョブの制御						○	
O.管理者の認証							○
O.プリンタ設定情報							○
OE.管理者	○						
OE.サービスマンの作業		○					
OE.ユーザ識別情報管理			○				
OE.認証印刷サーバ				○			
OE.ネットワーク					○		
OE.プリンタパスワードの管理							○
OE.クライアント PC				○			
OI.ユーザ識別情報付与						○	

8.1.2.セキュリティ対策方針の十分性

A.管理者

本条件は、管理者が悪意を持った行為を行なわないことを想定している。

OE.管理者により、組織の責任者は、悪意を持った行為を行なわない信頼できる者を管理者として選出する。

これにより A.管理者は実現できる。

A.サービスマン

本条件は、管理者が、サービスマンが TOE の設置・初期設定・およびこれら設定の変更を行う際に悪意を持った行為を行えない環境で実施させることを想定している。

OE.サービスマンの作業により、管理者は、サービスマンがこれらの作業を行う際には悪意を持った行為を行わないよう立ち会う。

これにより、A.サービスマンは実現できる。

A.ユーザ識別情報

本条件は、ユーザ識別情報を記録した媒体を、他のユーザ、サービスマン、第三者に利用されることがないこと､ユーザのクライアント PC に設定されたユーザ識別情報が他のユーザ、サービスマン、第三者に不正に変更されないことを想定している。

OE.ユーザ識別情報管理により、管理者は、ユーザ識別情報を記録した媒体がユーザ本人以外に利用されないよう厳重に管理し、ユーザ識別情報を記録した媒体の管理についてユーザに指導する。また、ユーザは、管理者の指示に従い、ユーザ識別情報を記録した媒体がユーザ本人以外に利用されないよう管理し、クライアント PC に設定されたユーザ識別情報が不正に変更されないよう、クライアント PC の OS のアカウントを管理する。

これにより、他のユーザ、サービスマン、および第三者が、ユーザ識別情報を記録した媒体を利用することは出来ず、また、ユーザのクライアント PC に設定されたユーザ識別情報を不正に変更することは出来ないため、A.ユーザ識別情報は実現できる。

A.スプールデータ

本条件は，スプールデータが不正アクセスやハードディスクの持ち去り、修理時の持ち出しにより暴露されないことを想定している。

サーバ経由方式利用時には、OE.認証印刷サーバにより、以下のことが行われる。

- 管理者は、認証印刷サーバ内のハードディスクを不正に持ち出され、内部に保持されているスプールデータが暴露されることのないよう、ハードディスクを保護する。
- 管理者は、認証印刷サーバの修理時などに認証印刷サーバが管理者以外のものにわたる場合には、認証印刷サーバ内の印刷ジョブをすべて削除する。
- 管理者は、管理者の「認証印刷サーバにインストールされた OS のアカウント」をユーザ、サービスマン、及び第三者に漏洩しないよう管理する。

また、直接印刷方式利用時には、OE.クライアント PC により、以下のことが行われる。

- ユーザは、クライアント PC 内のハードディスクを不正に持ち去られ、内部に保持されているスプールデータが暴露されることのないよう、ハードディスクを保護する。
- ユーザは、クライアント PC の修理時などにクライアント PC がユーザ本人以外のものにわたる場合には、クライアント PC 内の印刷ジョブをすべて削除する。
- ユーザは、ユーザの「クライアント PC にインストールされた OS のアカウント」が、他のユーザ、サービスマン、及び第三者に漏洩しないよう管理する。

以上によって、A.スプールデータは実現できる。

A.ネットワーク

本条件は、TOE を利用するネットワーク環境について、以下のことを想定している。

- 外部ネットワークからの攻撃を受けることはない。
- 内部ネットワークを流れるデータは、盗聴、改ざんされることはない。
- 管理者の管理下に無い認証印刷機能付きネットワークカードが接続されることはない。
- 認証印刷サーバ利用時、管理者が設定した認証印刷サーバの IP アドレスを不正に利用され、認証印刷サーバになりすまされることはない。
- 認証サーバ利用時、管理者が設定した認証サーバの IP アドレスを不正に利用され、認証サーバに成りすまされることはない。

OE.ネットワークにより、以下のことが実施される。

- 管理者は、TOE に対する外部ネットワークからの攻撃を遮断し、内部ネットワークの通信内容を暴露・改ざんから保護する。
- 管理者は、自分の管理下にない認証印刷機能付きネットワークカードが内部ネットワークに接続されることのないよう、内部ネットワークに接続されている認証印刷機能付きネットワークカードを管理する。
- 認証印刷サーバ利用時、管理者は、内部ネットワークに接続された認証印刷サーバの IP アドレスが不正に利用され、認証印刷サーバになりすまされることがないよう、IP アドレスを管理する。
- 認証サーバ利用時、管理者は、内部ネットワークに接続された認証サーバの IP アドレスが不正に利用され、認証サーバになりすまされることがないよう、IP アドレスを管理する。

これにより、A.ネットワークは実現できる。

T.印刷物の暴露

本脅威は、印刷者以外のユーザ、サービスマン、および第三者が、印刷物として出力された印刷者の印刷データを持ち出し、印刷データを暴露することを想定している。

この脅威に対抗するためには、印刷者以外に印刷データを印刷物として出力しない必要がある。本 TOE は、印刷者が暴露から保護したいデータを印刷する際に利用されるため、印刷者

の目前で印刷出力されれば本脅威が発生しないのは自明である。
OI.ユーザ識別情報付与により、プリンタドライバは、印刷者のユーザ識別情報を印刷ジョブに付与する。
O.印刷前のユーザ識別により、TOE は、ユーザを識別する。
また、O.印刷ジョブの制御により、TOE は印刷者に対してのみ、その印刷者が依頼した印刷物を出力する。印刷者が、出力された印刷物を直ちに回収するのは自明である。
したがって、印刷者以外のユーザ、サービスマン、および第三者によって印刷物を持ち出されることはなく、この脅威には対抗できる。

T.設定情報の改ざん

本脅威は、ユーザ、サービスマン、および第三者が、管理者になりすましプリンタ設定情報を変更することで、印刷データを暴露することを想定している。
この脅威に対抗するためには、プリンタ設定情報へのアクセスを管理者にのみ許可する必要がある。
TOE は、O.管理者の認証により、管理者を認証した後、O.プリンタ設定情報により、プリンタ設定情報へのアクセスを認証された管理者のみに許可する。
さらに、管理者は、OE.プリンタパスワードの管理により、プリンタパスワードをデフォルトのパスワードから推測されにくいパスワードに変更し、管理者以外に漏洩しないよう、管理する。
したがって、ユーザ、サービスマン、および第三者により、プリンタ設定情報を変更されることはないため、この脅威には対抗できる。

8.2. セキュリティ要件根拠

本節では、セキュリティ要件根拠として、セキュリティ機能要件の必要性、セキュリティ機能要件の十分性、セキュリティ機能要件の依存性の妥当性、セキュリティ機能要件の相互サポート構造、最小機能強度の妥当性、評価保証レベルの妥当性、及びセキュリティ保証要件の必要性について述べる。

8.2.1.セキュリティ機能要件の必要性

TOE セキュリティ機能要件と TOE セキュリティ対策方針との対応を以下の表に示す。

表の通り、すべての TOE セキュリティ機能要件は少なくとも一つの TOE セキュリティ対策方針と対応している。従って、すべての TOE セキュリティ機能要件の必要性は満たされている。

表 15 : セキュリティ対策方針とセキュリティ機能要件の対応

	O.印刷前のユーザ識別	O.印刷ジョブの制御	O.管理者の認証	O.プリンタ設定情報
FDP_IFC.1		○		
FDP_IFF.1		○		
FIA_ATD.1		○		
FIA_SOS.1			○	
FIA_UAU.2			○	
FIA_UAU.7			○	
FIA_UID.2	○			
FIA_USB.1		○		
FMT_MSA.3(1)		○		
FMT_MTD.1				○
FMT_SMF.1				○
FMT_SMR.1				○
FPT_RVM.1	○	○	○	○
FPT_SEP.1	○	○	○	○

またIT環境に対するセキュリティ機能要件とIT環境のセキュリティ対策方針との対応を以下の表に示す。

表 16 : IT 環境のセキュリティ対策方針とセキュリティ機能要件の対応

	OI.ユーザ識別情報付与
FMT_MSA.3(2)	○

表の通り、すべてのIT環境に対するセキュリティ機能要件は少なくとも一つのIT環境のセキュリティ対策方針と対応している。従って、すべてのIT環境に対するセキュリティ機能要件の必要性は満たされている。

8.2.2.セキュリティ機能要件の十分性

O.印刷前のユーザ識別

本セキュリティ対策方針は、TOE が印刷ジョブをプリンタの印刷出力機能に転送する前に、ユーザを識別することを求めている。

FIA_UID.2 により、TOE は印刷ジョブをプリンタの印刷出力機能に転送する前に、ユーザに自分自身を識別することを要求する。なお、これらの処理は FPT_RVM.1 により迂回されず、FPT_SEP.1 によりその他のサブジェクトからの干渉や改ざんから保護されたセキュリティドメインで実行される。

したがって、本対策方針は実現できる。

O.印刷ジョブの制御

本セキュリティ対策方針は、印刷者に対してのみ、その印刷者が依頼した印刷物を出力することを求めている。

FIA_ATD.1,FIA_USB.1 により、TOE は、ユーザプロセスに対してユーザ識別情報を関連付け、それを維持する。

FDP_IFC.1,FDP_IFF.1 により、TOE は、「識別されたユーザ識別情報に対応するジョブ ID」と「印刷ジョブに付随するジョブ ID」とが一致する印刷ジョブをプリンタの印刷出力機能に転送する。

また、印刷ジョブに付随するジョブ ID については、FMT_MSA.3(1)によって初期値が与えられている。なお、これらの処理は FPT_RVM.1 により迂回されず、FPT_SEP.1 によりその他のサブジェクトからの干渉や改ざんから保護されたセキュリティドメインで実行される。

したがって、本対策方針は実現できる。

O.管理者の認証

本セキュリティ対策方針は、管理者がプリンタ設定情報へアクセスする前に、TOE が管理者を認証することを求めている。

FIA_UAU.2 により、TOE は管理者に対してプリンタパスワードによる認証が成功することを要求する。このとき、FIA_UAU.7 により、認証フィードバックは保護される。また、FIA_SOS.1 により、プリンタパスワードとしては 5 文字以上 10 文字以内の英数混在のものが必ず用いられる。

なお、これらの処理は FPT_RVM.1 により迂回されず、FPT_SEP.1 によりその他のサブジェクトからの干渉や改ざんから保護されたセキュリティドメインで実行される。

したがって、本対策方針は実現できる。

O.プリンタ設定情報

本セキュリティ対策方針は、プリンタ設定情報へのアクセスを管理者のみに制限することを求めている。

FMT_MTD.1 と FMT_SMF.1 により、認証装置の設定、ユーザ識別情報の作成規則、認証方法の設定、プリンタパスワードの改変を管理者に制限している。さらに、FMT_SMR.1 により、管理者の役割が維持されている。

なお、これらの処理は FPT_RVM.1 により迂回されず、FPT_SEP.1 によりその他のサブジェクトからの干渉や改ざんから保護されたセキュリティドメインで実行される。

したがって、本対策方針は実現できる。

OI.ユーザ識別情報付与

本セキュリティ対策方針は、印刷者のユーザ識別情報を印刷ジョブに付与することを求めている。

FMT_MSA.3(2)により、プリンタドライバは、印刷者のユーザ識別情報を印刷ジョブに付与する。

したがって、本対策方針は実現できる。

8.2.3.セキュリティ機能要件の依存性の妥当性

セキュリティ機能要件とその依存先との対応を以下の表に示す。

表 17：セキュリティ機能要件依存性

機能要件	CC の依存性	本 ST の依存性	満たさない依存性	満たさなくてよい根拠
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	-	-
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3(1) FMT_MSA.3(2)		
FIA_ATD.1	-	-	-	-
FIA_SOS.1	-	-	-	-
FIA_UAU.2	FIA_UID.1		FIA_UID.1	(1)
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2		
FIA_UID.2	-	-	-	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	-	-
FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1		FMT_MSA.1 FMT_SMR.1	(2)
FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1		FMT_MSA.1 FMT_SMR.1	(3)

FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1		
FMT_SMF.1	-	-	-	-
FMT_SMR.1	FIA_UID.1		FIA_UID.1	(1)
FPT_RVM.1	-	-	-	-
FPT_SEP.1	-	-	-	-

(1) FIA_UAU.2 および FMT_SMR.1 が依存性 FIA_UID.1 を満たさなくてよい根拠
FIA_UID.1 は、利用者が識別されるときの要件である。
本 TOE の FIA_UAU.2、FMT_SMR.1 で識別が必要とされるのは管理者のみである。前提条件より、管理者は信頼できる人物であり、管理者が複数人いる場合でも、管理者であるかを認証できればよく、管理者一人一人を識別する必要は無い。
したがって、識別は不要となり、FIA_UID.1 を満たす必要はない。

(2) FMT_MSA.3(1)が、依存性 FMT_MSA.1 および FMT_SMR.1 を満たさなくてよい根拠
FMT_MSA.1 は、特定の役割をもつ利用者に対して、セキュリティ属性の管理を認める要件である。
FMT_MSA.3(1)では、セキュリティ属性であるジョブ ID は TOE の内部で初期化され、その後変更することはできない。
したがって、FMT_MSA.1 を満たす必要はない。
また、これに伴い、許可された役割の維持についての要件である FMT_SMR.1 を満たす必要もない。

(3) FMT_MSA.3(2)が、依存性 FMT_MSA.1 および FMT_SMR.1 を満たさなくてよい根拠
FMT_MSA.1 は、特定の役割をもつ利用者に対して、セキュリティ属性の管理を認める要件である。
FMT_MSA.3(2)では、セキュリティ属性であるユーザ識別情報について、プリンタドライバにより初期値が与えられた後、変更することはできない。
したがって、FMT_MSA.1 を満たす必要はない。
また、これに伴い、許可された役割の維持についての要件である FMT_SMR.1 を満たす必要もない。

以上により、セキュリティ機能要件の依存性は妥当である。

8.2.4.セキュリティ機能要件の相互サポート構造

セキュリティ機能要件の相互サポート構造を以下の表 18 に示す。

表 18：セキュリティ機能要件の相互サポート構造

機能要件	迂回防止	改ざん防止	非活性化防止	無効化防止
FDP_IFC.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FDP_IFF.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_ATD.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_SOS.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_UAU.2	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_UID.2	FPT_RVM.1	FPT_SEP.1	なし	なし
FIA_USB.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FMT_MSA.3(1)	FPT_RVM.1	FPT_SEP.1	なし	なし
FMT_MTD.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FMT_SMF.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	なし	なし
FPT_RVM.1	なし	FPT_SEP.1	なし	なし
FPT_SEP.1	FPT_RVM.1	なし	なし	なし

迂回防止

FPT_RVM.1 により、SF.ユーザ識別機能、SF.印刷ジョブ管理機能、SF.設定管理機能、SF.プリンタ設定機能に実装される以下の機能要件は、動作進行中に必ず呼び出され、迂回されない。
FDP_IFC.1, FDP_IFF.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1, FMT_MSA.3(1), FMT_MTD.1,FMT_SMF.1, FMT_SMR.1, FPT_SEP.1

改ざん防止

FPT_SEP.1 により、TSF が実行されるメモリ空間は、その他の不正なサブジェクトから干渉されない。

非活性化防止

本 TOE は、セキュリティ機能を非活性化する機能を持たないため、非活性化防止について対応する必要はない。

無効化防止

本 TOE は、セキュリティ機能を無効化されることはないため、無効化を狙った攻撃の検出を可能にする必要はない。よって無効化防止について対応する必要はない。

以上により、すべての TOE セキュリティ機能要件の相互サポート構造は妥当である。

8.2.5.セキュリティ機能要件の一貫性

本 ST で選択しているセキュリティ機能要件の一貫性について述べる。

セキュリティ機能要件の操作

本 ST では、FMT_MSA.3 を繰り返し用いているが、FMT_MSA.3(1)、FMT_MSA.3(2)は、目的と対象が異なっており、これらの間に重複、競合はない。
また機能要件の割付及び詳細化として、同一のセキュリティ属性（ジョブ ID、ユーザ識別情報）を複数の機能要件（FIA_USB.1、FDP_IFF.1、FMT_MAS.3 など）で使用しているが、それぞれの機能要件は異なる機能を実現するものであり、これらの間で重複、競合するものはない。

セキュリティ機能要件の拡張

本 ST では、セキュリティ機能の拡張は行っていない。

セキュリティ機能要件の依存性

8.2.3 に示すとおり、セキュリティ機能要件の依存性に関して、競合や矛盾はない。

セキュリティ機能要件の相互サポート

8.2.4 に示すとおり、セキュリティ機能要件の相互サポートに関して、競合や矛盾はない。

以上より、本 ST で選択しているセキュリティ機能要件は、競合しているものもなく、また、内部的にも一貫している。

8.2.6.最小機能強度の妥当性

本 TOE では、最小機能強度として SOF-基本を主張する。
本 TOE は、一般的なオフィス環境での利用を想定している。すなわち、オフィス内への出入りを許可された比較的限られた人物が出入りする空間であり、そこで扱われる情報は一般企業の機密情報レベルのものである。また、TOE に関して信頼できない関係者としては、ユーザ、サービスマン、第三者を想定している。このうち、サービスマンについては、前提条件 A.サービスマンによって、悪意を持った行為をおこなうことができない環境の構築を要求していることから、想定される攻撃者は、ユーザおよび第三者であり、これらの攻撃力は低レベルである。
したがって、最小機能強度レベルを SOF-基本とするのは妥当である。

8.2.7.評価保証レベルの妥当性

本 TOE では、評価保証レベルとして EAL2 を主張する。

本 TOE は、一般的なオフィス環境での利用を想定している。すなわち、オフィス内への出入りを許可された比較的限られた人物が出入りする空間であり、そこで扱われる情報は一般企業の機密情報レベルのものである。また、ネットワークはインターネットなどの不特定多数の人物がアクセスする外部ネットワークから保護された環境である。このような環境で使用されるため、TOE に対する脆弱性の分析や、機能仕様に対するテストの実施などについても評価の対象とすべきである。
したがって、評価保証レベルを EAL2 とするのは妥当である。

8.2.8.セキュリティ保証要件の根拠

本 TOE が主張する評価保証レベルは EAL2 である。表 10 で示した通り、本 TOE では、EAL2 のパッケージである保証コンポーネントを、依存性を含めすべて選択している。
したがって、本 TOE が主張するセキュリティ保証要件は妥当である。

8.3. TOE 要約仕様根拠

本節では、TOE 要約仕様根拠として、TOE セキュリティ機能の必要性、TOE セキュリティ機能の十分性、保証手段の妥当性、及び機能強度の根拠について述べる。

8.3.1.TOE セキュリティ機能の必要性

TOE セキュリティ機能と TOE セキュリティ機能要件との対応を表 11 に示した。表の通り、すべての TOE セキュリティ機能は少なくとも一つの TOE セキュリティ機能要件と対応している。
従って、すべての TOE セキュリティ機能の必要性は満たされている。

8.3.2.TOE セキュリティ機能の十分性

FDP_IFC.1, FDP_IFF.1

SF.印刷ジョブ管理機能は、SF.ユーザ識別機能によりユーザ識別情報を受信したら、印刷ジョブ制御 SFP に従い、保持している印刷ジョブに対して以下のフロー制御を実施する。

- 保持している印刷ジョブのうち、受信したユーザ識別情報と一致するユーザ識別情報を持つ印刷ジョブのジョブ ID 一覧を作成する。(印刷ジョブは複数あることが考えられるためリスト（一覧）になる。)
- 作成したリスト中のジョブ ID に対応する印刷ジョブをプリンタの印刷出力機能に転送する。
- 受信したユーザ識別情報と一致するユーザ識別情報を持つ印刷ジョブがない場合、印刷

ジョブの送信を保留する。

したがって、FDP_IFC.1,FDP_IFF.1 の要件は満たされる。

FIA_ATD.1

SF.ユーザ識別機能は、印刷者を代行して動くサブジェクトに対して関連付けられたユーザ識別情報を維持する。

したがって、FIA_ATD.1 の要件は満たされる。

FIA_SOS.1

SF.プリンタ設定機能は、プリンタパスワードを改変する際、5 文字以上 10 文字以内の英数混在のパスワードに設定されていることを検証し、条件を満たさないものには設定できないようにしている。

したがって、FIA_SOS.1 の要件は満たされる。

FIA_UAU.2

SF.設定管理機能は、プリンタ設定情報へのアクセスを許可する前に、パスワードによる認証を要求する。

したがって、FIA_UAU.2 の要件は満たされる。

FIA_UAU.7

SF.プリンタ設定機能は、管理者にプリンタパスワードの入力を要求する際、入力した文字を”*”等の文字で表示する。

したがって、FIA_UAU.7 の要件は満たされる。

FIA_UID.2

SF.ユーザ識別機能は、印刷ジョブをプリンタの印刷出力機能に転送する前に印刷者の識別を要求する。

したがって、FIA_UID.2 の要件は満たされる。

FIA_USB.1

SF.ユーザ識別機能は、印刷者を代行して動くサブジェクトに対してユーザ識別情報を関連付ける。

したがって、FIA_USB.1 の要件は満たされる。

FMT_MSA.3(1)

SF.印刷ジョブ管理機能は、受信した印刷ジョブに対して自動的に一意の整数値を割り当てる。

したがって、FMT_MSA.3(1)の要件は満たされる。

FMT_MTD.1

SF.設定管理機能は、認証装置の設定、認証方法の設定、プリンタパスワードの変更、ユーザ識別情報の作成規則の変更を、認証された管理者に制限している。
したがって、FMT_MTD.1 の要件は満たされる。

FMT_SMF.1

SF.設定管理機能は、プリンタパスワードを管理する機能を提供している。
したがって、FMT_SMF.1 の要件は満たされる。

FMT_SMR.1

SF.設定管理機能は、管理者の役割を維持し、認証されたサブジェクトに対して管理者という役割を関連付けている。
したがって、FMT_SMR.1 の要件は満たされる。

FPT_RVM.1

SF.ユーザ識別機能、SF.印刷ジョブ管理機能、SF.設定管理機能、SF.プリンタ設定機能は、迂回できないよう実装されている。
したがって、FPT_RVM.1 の要件は満たされる。

FPT_SEP.1

不正なサブジェクトからの干渉を防止するため、SF.ユーザ識別機能、SF.印刷ジョブ管理機能、SF.設定管理機能、SF.プリンタ設定機能は、独立したメモリ空間で実行される。
したがって、FPT_SEP.1 の要件は満たされる。

8.3.3.機能強度の根拠

本 TOE において、確率的或いは順列的メカニズムを持つセキュリティ機能と、そのセキュリティ強度主張を表 12 に示した。一方、5.1.3 で示した通り、本 TOE の最小機能強度は、SOF-基本である。
従って、これらは矛盾していない。

8.3.4.保証手段の妥当性

保証手段とセキュリティ保証要件の対応を表 13 に示す。
表の通り、EAL2 で求められるすべての保証コンポーネントを満たしている。
従って、すべての保証手段は満たされている。

8.4. PP 主張の根拠

PP 適合は主張しない。