認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	平成19年4月17日　（IT認証7146)
認証番号	C0177
認証申請者	セイコーエプソン株式会社
TOEの名称	（日本語版）EpsonNet ID Print Authentication Print Module （英語版）　EpsonNet ID Print Authentication Print Module
TOEのバージョン	（日本語版）1.5b （英語版）　1.5bE
PP適合	なし
適合する保証パッケージ	EAL2
開発者	セイコーエプソン株式会社
評価機関の名称	みずほ情報総研株式会社　情報セキュリティ評価室

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20年8月12日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「（日本語版）EpsonNet ID Print Authentication Print Module バージョン：1.5b、（英語版）EpsonNet ID Print Authentication Print Module バージョン：1.5bE」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「(日本語版) EpsonNet ID Print Authentication Print Module バージョン：1.5b、(英語版) EpsonNet ID Print Authentication Print Module バージョン：1.5bE」（以下「本TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（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セイコーエプソ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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

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：	(日本語版) EpsonNet ID Print Authentication Print Module
	(英語版) EpsonNet ID Print Authentication Print Module
バージョン：	(日本語版) 1.5b
	(英語版) 1.5bE
開発者：	セイコーエプソン株式会社

1.2.2 製品概要

本製品は、セイコーエプソン株式会社製プリンタ及び複合機のプリンタ部分のオプション製品（以下合わせて「プリンタ」という。）である認証印刷機能付きネットワークカードに搭載されるOffirio SynergyWare ID Print（海外版：EpsonNet Authentication Print）の認証印刷モジュール、及び印刷要求を処理するコンピュータ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、クライアントPCを利用するユーザが印刷を依頼した印刷データに対してユーザ識別情報等が付与された印刷ジョブを受け取り、本TOE内において一時的に保持し、プリンタのネットワークカード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（以下「認証印刷」という。）を提供する。本TOEが提供するセキュリティ機能を以下に示す。

- ユーザ識別機能
- 印刷ジョブ管理機能
- プリンタ設定機能
- 設定管理機能

なお、以下の機能は本TOEに含まれるが評価対象外である。

- システム設定ツールの起動時のユーザ識別・認証機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの範囲及び動作環境

本TOEは、認証印刷機能付きネットワークカードに搭載されるOffirio SynergyWare ID Print（海外版：EpsonNet Authentication Print）の認証印刷モジュール、及び印刷要求を処理するコンピュータ上で動作する附属アプリケーションソフトウェアであり、認証印刷ソフトウェア、スプーラソフトウェア及びシステム設定ツールの3つから構成される。

本TOEには、印刷ジョブを一時的に保持する機能を持たせる場所により、サーバ経由方式と直接印刷方式の２つの利用形態が存在する。

サーバ経由方式では、クライアントPCの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（認証印刷サーバ）を設け、印刷ジョブをまとめてこのサーバ上に保持し、プリンタからの出力要求に応じて印刷ジョブを受け渡す。

直接印刷方式では、クライアントPCのユーザの印刷依頼により作成された印刷ジョブは各クライアントPC上に一時的に保持し、プリンタからの出力要求に応じて印刷ジョブを受け渡す。

サーバ経由方式を用いた場合の本TOEの動作環境概要を図1-1、物理的範囲を図1-2に、直接印刷方式を用いた場合の本TOEの動作環境概要を図1-3、物理的範囲を図1-4に示す。

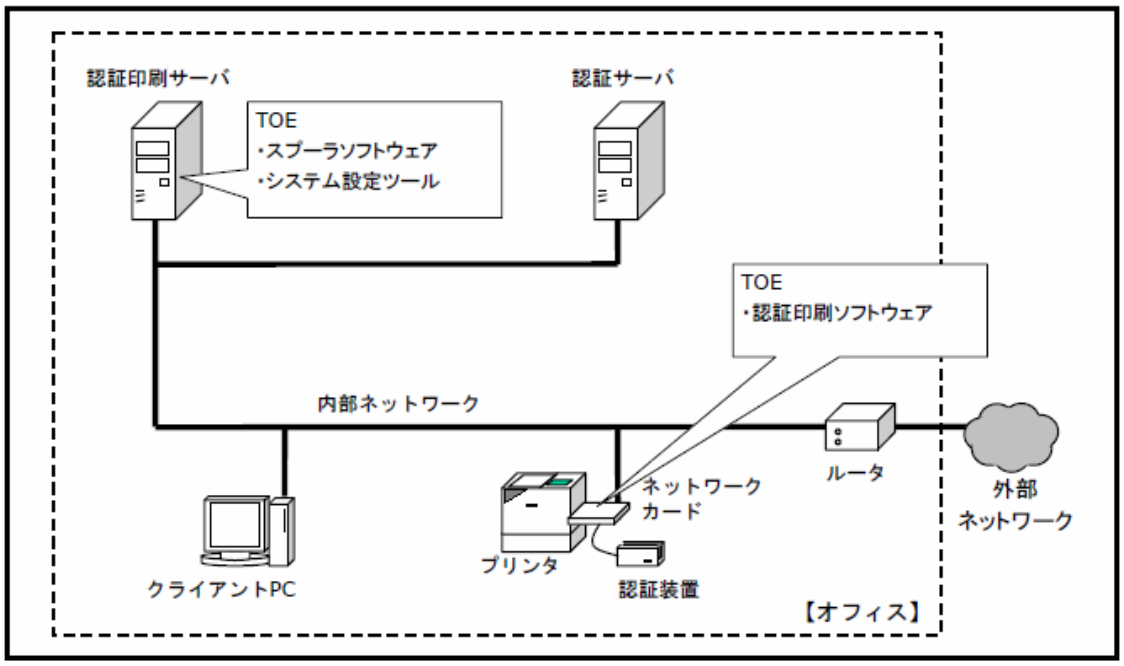

図1-1　TOEの動作環境概要（サーバ経由方式）

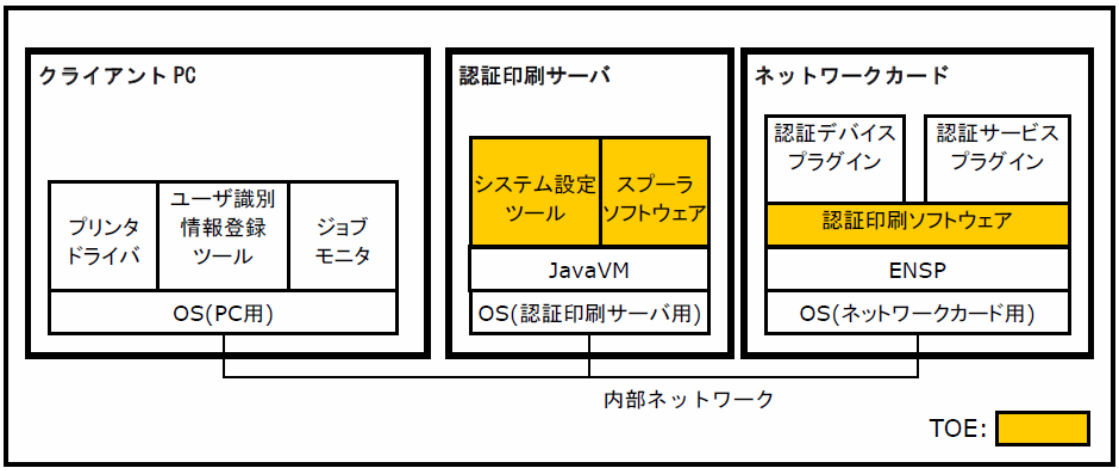

図1-2　TOEの物理的範囲（サーバ経由方式）

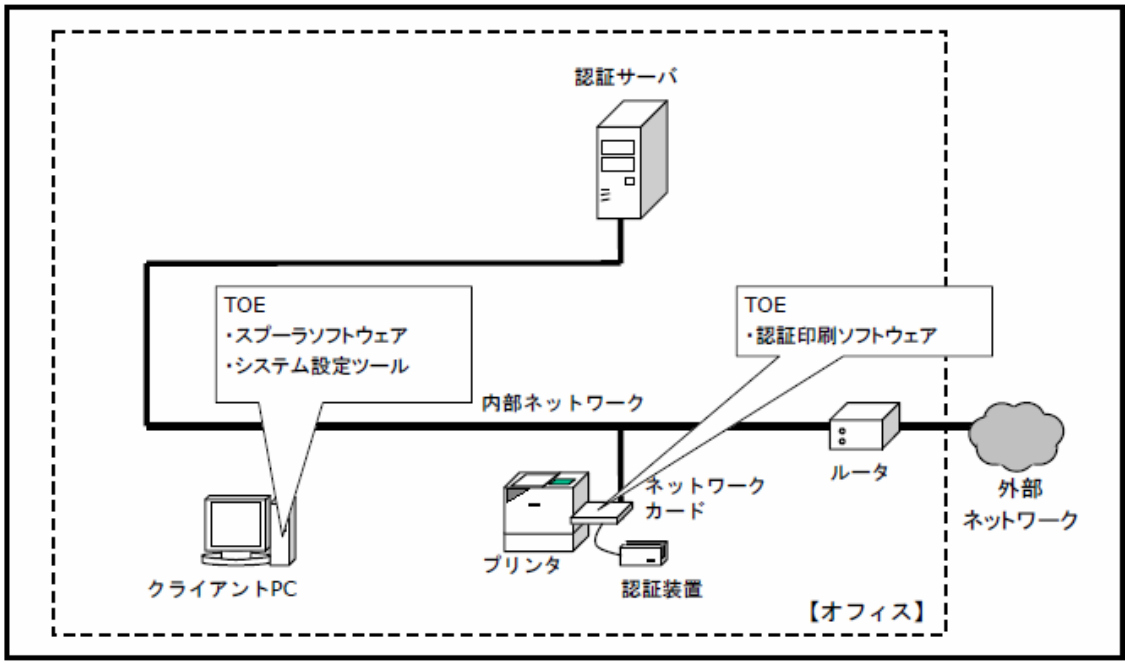

図1-3　TOEの動作環境概要（直接印刷方式）

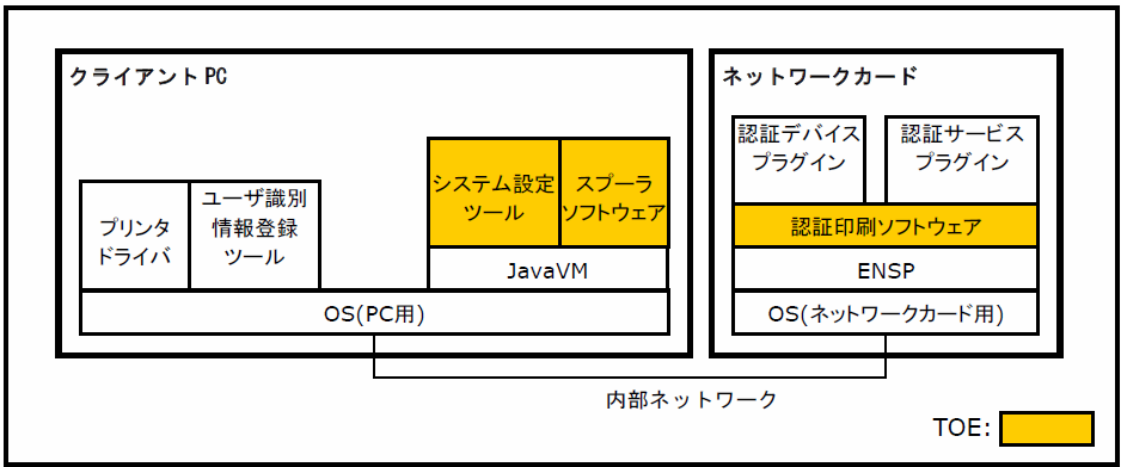

図1-4　TOEの物理的範囲（直接印刷方式）

本TOEの動作に関わる構成要素の役割を以下に示す。

【クライアントPC】（直接印刷方式の場合、TOEを搭載）
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。また、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（サーバ経由方式の場合：プリンタドライバ、ユーザ識別情報登録ツール及びジョブモニタ、直接印刷方式の場合：プリンタドライバ、ユーザ識別情報登録ツール及びJavaVM）がインストールされる。直接印刷方式の場合、印刷ジョブを一時的に保持するために、本TOEの一部である、スプーラソフトウェア及びシステム設定ツールがインストールされる。

ユーザが認証印刷の印刷依頼を実行した際に、印刷データにユーザ識別情報等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印刷ジョブを送信する。
クライアントPC は複数台用いることが可能である。ただし、サーバ経由方式を用いる場合は、認証印刷サーバ1台あたりの接続可能クライアントPCの最大数は50台である。

【ユーザ識別情報登録ツール】（TOE範囲外）
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。

【プリンタドライバ】（TOE範囲外）
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、ユーザ識別情報及び印刷方法の情報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。
認証印刷サーバにインストールし、共有利用することも可能である。

【ジョブモニタ】（TOE範囲外）
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。
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。

【JavaVM】（TOE範囲外）
本TOEを構成する、スプーラソフトウェア、システム設定ツール及び認証印刷ソフトウェアを動作させるためのソフトウェア。

【OS（PC用）】（TOE範囲外）
プリンタドライバ、ユーザ識別情報登録ツール、JavaVMを動作させるためのOS。

【認証印刷サーバ】（サーバ経由方式の場合、TOEを搭載）
ユーザの認証印刷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。
サーバ経由方式の場合、いくつかの印刷ジョブを一時的に保持するために、本TOEの一部であるスプーラソフトウェア及びシステム設定ツール、TOEを動作させるためのJavaVMがインストールされる。
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。

【スプーラソフトウェア】（TOEの一部）
EpsonNet ID Print Spooler Serviceのこと。
ユーザ識別情報等を付与して送信され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】（TOEの一部）
EpsonNet ID Print システム設定のこと。
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。

【OS（認証印刷サーバ用）】（TOE範囲外）
認証印刷サーバで、JavaVMを動作させるためのOS。

【ネットワークカード】（TOEを搭載）
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カード。本TOEの一部である、認証印刷ソフトウェアがネットワークカードに実装されている。

【認証印刷ソフトウェア】（TOEの一部）
EpsonNet ID Print AuthBaseのこと。
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】（TOE範囲外）
EpsonNet Service Platformのこと。
認証印刷ソフトウェアが動作するプラットフォーム。JavaVMも含まれている。

【認証デバイスプラグイン】（TOE範囲外）
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】（TOE範囲外）
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元に、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。

【OS（ネットワークカード用）】（TOE範囲外）
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。

【プリンタ】（TOE範囲外）
本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。
プリンタは複数台用いることが可能である。

【認証装置】（TOE範囲外）
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。
プリンタを利用する単位に配付されている磁気カードリーダ、IC カードリーダ、生体認証装置などの認証媒体を用いて、ユーザの認証を行い、認証媒体から読み込んだ情報を元に、必要に応じて認証サーバを用いてユーザ識別情報を特定する。

【認証サーバ】（TOE範囲外）
ユーザ識別情報を管理しているサーバ。
認証装置により読み込まれた認証媒体の情報とユーザ識別情報の対応を管理している。認証装置により読み込まれた認証媒体上にユーザ識別情報がそのまま格納されている場合には設置は不要である。

【内部ネットワーク】（TOE範囲外）
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。

【ルータ】（TOE範囲外）
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。

【外部ネットワーク】（TOE範囲外）
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。

1.2.3.2 TOEの動作概要

本TOEは、図1-1及び図1-2に示すサーバ経由方式の動作環境、図1-3及び図1-4に示す直接印刷方式の動作環境において、以下のとおりTOE以外のソフトウェア等と連動する。

【サーバ経由方式の場合】

① 本TOEの管理者は、本TOEの一部であるシステム設定ツールを用いて、パスワードによる認証を経た上で、認証印刷サーバやネットワークカードの設定を行う。また、クライアントPCから認証印刷を行うために、TOE外であるユーザ識別情報登録ツール、プリンタドライバ、ジョブモニタの設定を行う。
② 各ユーザは、自分のクライアントPC から認証印刷の印刷依頼を実行する。印刷依頼を行うことで、クライアントPCのプリンタドライバが、印刷データに対してユーザ識別情報登録ツールで設定したユーザ識別情報及び指定された印刷方法の情報を付与した印刷ジョブを作成し、認証印刷サーバのスプーラソフトウェアへ送信する。
③ 認証印刷サーバのスプーラソフトウェアは、クライアントPCのプリンタドライバから受信した印刷ジョブにジョブIDを付与した上で保持する。
④ 各ユーザは、プリンタのネットワークカードに接続された認証装置に、各ユーザに対して事前に配付された認証媒体を読み取らせる。
⑤ ネットワークカードは、認証媒体から、TOE外の認証デバイスプラグインを用いてユーザ識別情報を特定するための情報を読み出し、事前に設定された内容に従ってユーザ識別情報を特定する。ユーザ識別情報の特定の際には、TOE外の認証サーバを利用することが可能である。その際にはTOE外の認証サービスプラグインを用いて、TOEの一部である認証印刷ソフトウェアを経由して認証サーバを利用する。
その後、ネットワークカードの認証印刷ソフトウェアは、特定したユーザ識別情報を認証印刷サーバのスプーラソフトウェアに送信する。
⑥ 認証印刷サーバのスプーラソフトウェアは、受信したユーザ識別情報を持つ印刷ジョブを洗い出し、それらの印刷ジョブをネットワークカードの認証印刷ソフトウェアへ送信する。
⑦ ネットワークカードの認証印刷ソフトウェアは、受信した印刷ジョブをプリンタに対して送信し、印刷が開始される。印刷が完了した印刷ジョブについては、ネットワークカードの認証印刷ソフトウェアから認証印刷サーバのスプーラソフトウェアへ削除要求が送信される。
⑧ 認証印刷サーバのスプーラソフトウェアは、削除要求のあった印刷ジョブを削除し、一連の動作を完了する。

【直接印刷方式の場合】

① 本TOEの管理者は、本TOEの一部であるシステム設定ツールを用いて、パスワードによる認証を経た上で、クライアントPCやネットワークカードの設定を行う。また、クライアントPCから認証印刷を行うために、TOE外であるユーザ識別情報登録ツール、プリンタドライバの設定を行う。

② 各ユーザは、自分のクライアントPC から認証印刷の印刷依頼を実行する。印刷依頼を行うことで、クライアントPCのプリンタドライバが、印刷データに対してユーザ識別情報登録ツールで設定したユーザ識別情報及び指定された印刷方法の情報を付与した印刷ジョブを作成し、同じクライアントPCのスプーラソフトウェアへ送信する。

③ クライアントPCのスプーラソフトウェアは、クライアントPCのプリンタドライバから受信した印刷ジョブにジョブIDを付与した上で保持する。

④ 各ユーザは、プリンタのネットワークカードに接続された認証装置に、各ユーザに対して事前に配付された認証媒体を読み取らせる。

⑤ ネットワークカードは、認証媒体から、TOE外の認証デバイスプラグインを用いてユーザ識別情報を特定するための情報を読み出し、事前に設定された内容に従ってユーザ識別情報を特定する。ユーザ識別情報の特定の際には、TOE外の認証サーバを利用することが可能である。その際にはTOE外の認証サービスプラグインを用いて、TOEの一部である認証印刷ソフトウェアを経由して認証サーバを利用する。

その後、ネットワークカードの認証印刷ソフトウェアは、特定したユーザ識別情報をクライアントPCのスプーラソフトウェアに送信する。

⑥ クライアントPCのスプーラソフトウェアは、受信したユーザ識別情報を持つ印刷ジョブを洗い出し、それらの印刷ジョブをネットワークカードの認証印刷ソフトウェアへ送信する。

⑦ ネットワークカードの認証印刷ソフトウェアは、受信した印刷ジョブをプリンタに対して送信し、印刷が開始される。印刷が完了した印刷ジョブについては、ネットワークカードの認証印刷ソフトウェアからクライアントPCのスプーラソフトウェアへ削除要求が送信される。

⑧ クライアントPCのスプーラソフトウェアは、削除要求のあった印刷ジョブを削除し、一連の動作を完了する。

1.2.3.3 TOEに関係する利用者役割

本TOEに関係する利用者とその役割を以下に示す。

【管理者】

役割　：TOEの利用環境構築・設定・管理（ガイダンスに従ったTOEの設置、初期設定、設定の変更）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。

【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（ガイダンスに従ったTOEの設置、初期設定、設定の変更）を行う人。

権限　：TOEの設置・初期設定・設定変更。

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　：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。

【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。

【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）。

1.2.4　TOEの機能

本TOEが保持する機能は、セキュリティ機能と非セキュリティ機能に分類される。TOE及びTOEと連動する機能の関係を図1-5に、本TOEが保持するセキュリティ機能を表1-1に、本TOEが保持する非セキュリティ機能（評価対象外の機能を含む）を表1-2に示す。

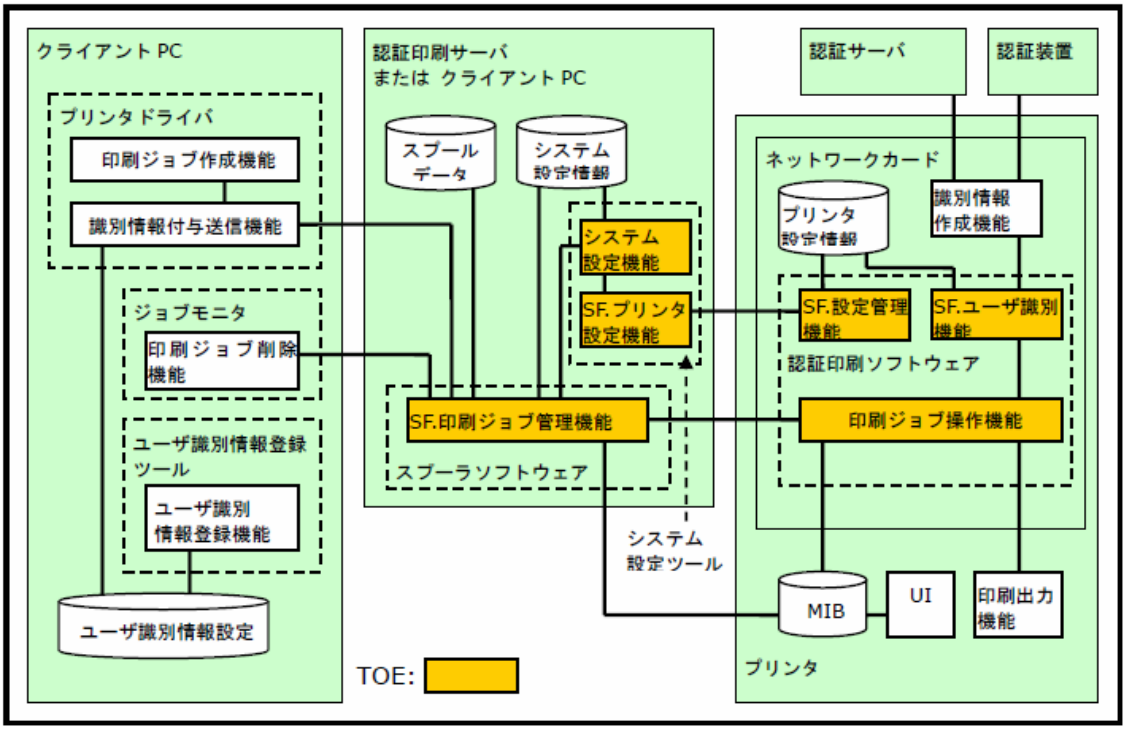

図1-5　TOEの論理的範囲

表1-1　TOEのセキュリティ機能

セキュリティ機能	概要
ユーザ識別機能（認証印刷ソフトウェアが保持）	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、TOE外である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する。 ・取得したユーザ識別情報を、印刷ジョブ操作機能に送信する。
印刷ジョブ管理機能（スプーラソフトウェアが保持）	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等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として保持する。 ・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する。 ・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する。
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ユーザインタ

（システム設定ツールが保持）	フェースを提供する機能。 ・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する。 ・プリンタ設定情報の設定変更画面を表示する。
設定管理機能 （認証印刷ソフトウェアが保持）	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する。

表1-2　TOEの非セキュリティ機能（評価対象外の機能を含む）

非セキュリティ機能	概要
システム設定機能 （システム設定ツールが保持）	システム設定機能を利用する前には識別・認証が行われ、システム設定情報の設定･変更を行う。また、TOEのセキュリティ機能である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、TOEのセキュリティ機能である、プリンタ設定機能を呼び出す。 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。
印刷ジョブ操作機能 （認証印刷ソフトウェアが保持）	TOEのセキュリティ機能である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、TOE外であるプリンタの印刷出力機能に転送し、印刷を行う。

1.3　評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート3及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「EpsonNet ID Print Authentication Print Module セキュリティターゲット Ver1.11」（以下「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の開発の現場を調査し、本TOEがCCパート1 （[5][8][11]のいずれか）附属書B、CCパート2 ([6][9][12]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]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、「EpsonNet ID Print Authentication Print Module 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]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、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20年7月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

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

ST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行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、ユーザ及び第三者であり、これらの攻撃力は低レベルである。よってSOF-基本

で十分である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能については、「1.2.4TOEの機能」を参照。

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅 威
T.印刷物の暴露	印刷者以外のユーザ、サービスマン、及び第三者が、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、及び第三者が、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

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

TOEが動作するために必要なIT製品の中で、本評価にて検証した環境を表1-4及び表1-5に示す。

表1-4 サーバ経由方式の場合の構成（英語版のTOEの利用を想定した環境）

プリンタ	AL-C4200（海外プリンタ、英語表示）	
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)

表1-5　直接印刷方式の場合の構成（日本語版のTOEの利用を想定した環境）

プリンタ	LP-S6500（国内プリンタ、漢字表示）	
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	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
	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

	JavaVM	JavaSE6 update3
	OS	Windows XP Professional SP2(32bit)

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.管理者	管理者は、悪意を持った行為を行うことはない。
A.サービスマン	管理者は、サービスマンがTOEの設置・初期設定及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。
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、及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、及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。

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。

【日本語版】

・Offirio SynergyWare ID Print 管理者ガイド　NPD3196-00
・Offirio SynergyWare ID Print 利用者ガイド　NPD3197-00
・PRIFNW7S はじめにお読みください　411139800
・PRIFNW7S/U セットアップガイド　411139701
・Offirio SynergyWare ID Print アップデータ適用手順　NPD3702-00
・PRIFNW7S ファームウェア アップデート手順　NPD3857-00

【英語版】

・EpsonNet Authentication Print Software Administrator's Guide NPD3647-00
・EpsonNet Authentication Print Software User's Guide　NPD3648-00
・Online Guide Supplement　411200400
・EpsonNet Authentication Print Network Interface Card User's Guide NPD3731-00
・How to use EpsonNet Authentication Print Software Updater　NPD3754-00
・How to use EpsonNet Authentication Print Network Interface Card Firmware Updater　NPD3753-00

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に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成19年4月に始まり、平成20年7月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年3月に開発現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20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1-4及び表1-5に示す。表1-4はサーバ経由方式、表1-5は直接印刷方式のテストを実施した環境である。なお、サーバ経由方式及び直接印刷方式共に認証サーバが構成要素に含まれているが、認証サーバはTOEの動作に必須の要素ではないため、TOEと連動する動作についてのみテストを実施している。

これに加え、プリンタのハードウェアに依存するメッセージ表示ついては、表2-1に示す環境でテストを実施している。

表2-1　プリンタ表示の確認のための開発者テストの構成
（日本語版のTOEを利用した直接印刷方式を使用）

プリンタ	LP-9400（国内プリンタ、英語表示） LP-2500（国内プリンタ、液晶なし） LP-M6000（国内プリンタ、本体メッセージ表示）	
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	PaSoRi	
認証メディア	FeliCa 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
	プリンタドライバ	LP-9400 Printer Driver LP-2500 Printer Driver LP-M6000 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
	JavaVM	JavaSE6 update3
	OS	Windows XP Professional SP2(32bit)

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

開発者テストは表1-4、表1-5及び表2-1の構成で実施されている。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施

されている。

テスト構成の選択の妥当性については評価者により確認されている。

b.テスト手法

テストには、以下の手法が使用された。

①クライアントPCからの印刷要求に始まり、プリンタに接続された認証装置による本人確認後の印刷出力の流れにおいてユーザが介在する操作、ユーザが介在しない動作、画面・メッセージ・送受信されるデータの取得による確認。

②システム設定ツールを利用した管理者による操作、画面・メッセージ・送受信されるデータの取得による確認。

c.実施テストの範囲

テストは開発者によって75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2-2、表2-3、表2-4及び表2-5に示す。表2-2は評価者による開発者テストのサンプリングテスト、表2-3は評価者により追加の確認が必要と判断された状況のテスト、表2-4及び表2-5は評価者による侵入テストを実施した環境である。

表2-2　評価者による独立テストの構成
（日本語版のTOEを利用したサーバ経由方式を使用）

プリンタ	LP-M6000シリーズ（国内プリンタ、本体メッセージ表示）	
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	PaSoRi	
認証メディア	FeliCa カード	
認証サーバ	なし	
認証印刷サーバ	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
	OS	Windows 2000 Server SP4(32bit)
クライアントPC	プリンタドライバ	LP-M6000 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
	ジョブモニタ	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition(32bit) Windows Vista Ultimate Edition(32bit) Windows Vista Enterprise Edition(32bit) Windows 2000 Professional SP4(32bit)

表2-3　評価者による追加テストの構成
（日本語版のTOEを利用したサーバ経由方式を使用）

プリンタ	LP-M6000シリーズ（国内プリンタ、本体メッセージ表示）2台	
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	PaSoRi 2台	
認証メディア	FeliCa カード	
認証サーバ	なし	

認証印刷サーバ	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
	OS	Windows 2000 Server SP4(32bit)
クライアントPC	プリンタドライバ	LP-M6000 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
	ジョブモニタ	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition(32bit) Windows Vista Ultimate Edition(32bit)

表2-4　評価者による侵入テストの構成その１
（日本語版のTOEを利用したサーバ経由方式を使用）

プリンタ	LP-M6000シリーズ（国内プリンタ、本体メッセージ表示）	
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	PaSoRi	
認証メディア	FeliCa カード	
認証サーバ	なし	
認証印刷サーバ	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
	OS	Windows Server 2003 SP2(32bit) Windows 2000 Server

		SP4(32bit)
クライアントPC	プリンタドライバ	LP-M6000 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
	ジョブモニタ	EpsonNet ID Print Job Monitor
	OS	Windows Vista Business Edition(32bit)

表2-5　評価者による侵入テストの構成その2
（日本語版のTOEを利用した直接印刷方式を使用）

プリンタ	LP-S4000（国内プリンタ、英語メッセージ表示）	
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	PaSoRi　2台	
認証メディア	FeliCa カード	
認証サーバ	なし	
クライアントPC	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
	プリンタドライバ	LP-S4000 Printer Driver
	ユーザ識別情報登録ツール	EpsonNet ID Print User ID Register
	JavaVM	JavaSE6 update3
	OS	Windows Vista Ultimate Edition(32bit) Windows Vista Enterprise Edition(32bit)

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

評価者テストは表2-2、表2-3、表2-4及び表2-5の構成で実施されている。評価者テストはSTにおいて識別されているTOE構成から以下の要素を取り除いたTOEテスト環境で実施されている。

・認証サーバ

取り除かれた要素及びテスト構成の選択の妥当性については評価者により確認されている。

b.テスト手法

テストには、以下の手法が使用された。

① クライアントPCからの印刷要求に始まり、プリンタに接続された認証装置による本人確認後の印刷出力の流れにおいてユーザが介在する操作、ユーザが介在しない動作、画面・メッセージ・送受信されるデータの取得による確認。

② システム設定ツールを利用した管理者による操作、画面・メッセージ・送受信されるデータの取得による確認。

③ 脆弱性検査のためのツール（Nessus）による確認。

c.実施テストの範囲

評価者が独自に考案したテストを20項目、開発者テストのサンプリングによるテストを21項目、評価者が独自に考案した侵入テストを24項目、計65項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

【独自に考案したテストの選択基準】

① １つのテストでなるべく多くのTOEセキュリティ機能を含んだテストとすること。

② 一連のテストを行うことによって、ユーザが利用するすべてのTSFIがテストできるようにすること。

③ 一連のテストを順番に沿って実施することにより、すべてのTSFが使用されること。

④ TOEの特徴的な機能である認証操作による印刷ジョブの印刷について直接的なテストを含むこと。

⑤ SOF主張に対するSF.設定管理機能（TSF.管理者認証）のテストを含め、開発者テストに含まれていないバリエーションのプリンタパスワードを使うこと。

⑥ 開発者テストでは単独の競合状態がない状況での機能テストが提供されているため、印刷が競合する場合のテストを行うこと。

【サンプリングテストの選択基準】

① すべてのTSF及びすべてのTSFIを網羅すること。

② パスワード入力のように入力されるパラメタが人間である利用者の操作の影響を受けやすい部分を中心にすること。

【侵入テストの選択基準】

① TOEの脅威（T.設定情報の改ざん、T.印刷物の暴露）に関係する攻撃。

② STの前提条件から内部ネットワーク上で盗聴、改ざんができないためTOEを構成要素であるシステム設定ツール、スプーラソフトウェア、認証装置のインタフェースなどへの直接的な攻撃。

③ 開発者によるテストのうち、脆弱性テストとして確認する必要があると考えられるもの。

④ 開発者による脆弱性分析で与えられた脆弱性テストのうち､評価者が、別な視点からさらに検査する必要があると考えたもの。

⑤ 開発者による機能強度分析で提示された強度分析を裏付けるもの。

⑥ 悪意を持った者がガイダンスの情報を参照して試みると思われるもの。

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

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料を元に、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評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び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のEAL2に対する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記述が理路整然とし一貫していることを確認している。
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。
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、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、

	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。
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完全で、理路整然としていて、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。
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完全で、理路整然としていて、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全で、理路整然としていて、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ることを、類似製品の状況及びインタビュー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実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、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。

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。
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を含んで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。

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主張が正しい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共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

クライアントPC上のプリンタドライバにより印刷データに対して付与されるユーザ識別情報は、製品の利用者全体において一意となるものを付与する必要がある。

認証サーバを利用する場合、TOEは、認証サーバに登録された情報及び認証サーバからの応答が正当であるものとして取り扱う。

クライアントPCまたは認証印刷サーバに搭載されたスプーラソフトウェアに対して印刷データの送信要求を行うことができるのは認証装置付きのネットワークカードを搭載したプリンタに制限されているが、スプーラソフトウェアではプリンタからの印刷データの送信要求を正当なものとして受け入れて動作するため、印刷データの不正な送信要求が行われないようにネットワークを管理する必要がある。

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TOE特有の略語を以下に示す。

ENSP	EpsonNet Service Platform
MIB	Management Information Base
OS	Operating System
UI	User Interface

本報告書で使用された用語を以下に示す。

ENSP	EpsonNet Service Platformの略語。 認証印刷ソフトウェアが動作するプラットフォーム。JavaVMも含まれている。
JavaVM	本TOEを構成する、スプーラソフトウェア、システム設定ツール及び認証印刷ソフトウェアを動作させるためのソフトウェア。
MIB	Management Information Baseの略語。 機器の状態を管理するデータベース。
UI	User Interfaceの略語。 印刷処理の状況について表示する。

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。
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。
印刷ジョブ管理機能	スプールデータの管理を行う機能。TOEの一部であるスプーラソフトウェアが保持している。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等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として保持する。 ・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する。 ・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できない。
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持つ印刷ジョブを作成する。
印刷ジョブ操作機能	TOEのセキュリティ機能である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、TOE外であるプリンタの印刷出力機能に転送し、印刷を行う。
印刷データ	ユーザが印刷出力するデータ。
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。
管理者	役割　：TOEの利用環境構築・設定・管理（ガイダンスに従ったTOEの設置、初期設定、設定の変更）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。

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。また、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（サーバ経由方式の場合：プリンタドライバ、ユーザ識別情報登録ツール及びジョブモニタ、直接印刷方式の場合：プリンタドライバ、ユーザ識別情報登録ツール及びJavaVM）がインストールされる。直接印刷方式の場合、印刷ジョブを一時的に保持するために、本TOEの一部である、スプーラソフトウェア及びシステム設定ツールがインストールされる。
サーバ経由方式	クライアントPCの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（認証印刷サーバ）を設け、印刷ジョブをまとめてこのサーバ上に保持し、プリンタからの出力要求に応じて印刷ジョブを受け渡す方式。
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（ガイダンスに従ったTOEの設置、初期設定、設定の変更）を行う人。 権限　：TOEの設置・初期設定・設定変更。 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　：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。
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。
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、印刷ジョブ管理機能に送信する。
システム設定機能	システム設定機能を利用する前には識別・認証が行われ、システム設定情報の設定・変更を行う。また、TOEのセキュリティ機能である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、TOEのセキュリティ機能である、プリンタ設定機能を呼び出す。

システム設定情報	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）。
システム設定ツール	EpsonNet ID Print システム設定のこと。 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。
ジョブID	ジョブを管理するために、TOEにより自動的に割り当てられる一意の整数値。
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。 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。
スプーラソフトウェア	EpsonNet ID Print Spooler Serviceのこと。 ユーザ識別情報等を付与して送信され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。
スプールデータ	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。
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する。
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）。
第三者	役割　：TOE 利用環境のオフィス内で想定される、組織の責任者、管理者、ユーザ、サービスマン以外の人。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。

直接印刷方式　クライアントPCのユーザの印刷依頼により作成された印刷ジョブは、各クライアントPC上に一時的に保持し、プリンタからの出力要求に応じて印刷ジョブを受け渡す方式。

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。

認証印刷　印刷者の識別・認証を行ってから印刷物を出力する印刷方法。

認証印刷サーバ　ユーザの認証印刷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。
サーバ経由方式の場合、いくつかの印刷ジョブを一時的に保持するために、本TOEの一部であるスプーラソフトウェア及びシステム設定ツール、TOEを動作させるためのJavaVMがインストールされる。
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。

認証印刷ソフトウェア　EpsonNet ID Print AuthBaseのこと。
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。

認証サーバ　ユーザ識別情報を管理しているサーバ。
認証装置により読み込まれた認証媒体の情報とユーザ識別情報の対応を管理している。認証装置により読み込まれた認証媒体上にユーザ識別情報がそのまま格納されている場合には設置は不要である。

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元に、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。
プリンタを利用する単位に配付されている磁気カードリーダ、ICカードリーダ、生体認証装置などの認証媒体を用いて、ユーザの

認証を行い、認証媒体から読み込んだ情報を元に、必要に応じて認証サーバを用いてユーザ識別情報を特定する。

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。

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カード。本TOEの一部である、認証印刷ソフトウェアがネットワークカードに実装されている。

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ユーザインタフェースを提供する機能。
・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する。
・プリンタ設定情報の設定変更画面を表示する。

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、ユーザ識別情報及び印刷方法の情報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。
認証印刷サーバにインストールし共有利用することも可能である。

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。

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。

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、TOE外である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する。

・取得したユーザ識別情報を、印刷ジョブ操作機能に送信する。

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。
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。
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。
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。

6 参照

[1] 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

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　（平成17年12月翻訳第1.0版）

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　（平成17年12月翻訳第1.0版）

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　（平成17年12月翻訳第1.0版）

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月（平成17年12月翻訳第1.0版）

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] EpsonNet ID Print Authentication Print Module 評価報告書 第3版 2008年7月7日 みずほ情報総研株式会社 情報セキュリティ評価室