EPSON
EXCEED YOUR VISION

S-02

セイコーエプソン

PP-100N セキュリティ制御機構 セキュリティターゲット

Version 2.0

2009 年 7 月 3 日

セイコーエプソン株式会社

目 次

1 ST 概説 5

1.1 ST 識別 5
1.2 ST 概要 5
1.3 CC 適合 6
1.4 用語･略語 6
1.5 商標 8

2 TOE 記述 9

2.1 TOE の概要 9
2.1.1 TOE 種別 9
2.1.2 利用目的 9
2.1.3 利用環境 9
2.2 TOE の関係者 10
2.3 物理的構成 11
2.3.1 ハードウェア構成 11
2.3.2 ハードウェア構成要素 11
2.3.3 ハードウェアの TOE 範囲 13
2.3.4 ソフトウェア構成 13
2.3.5 ソフトウェア構成要素 13
2.3.6 ソフトウェアの TOE 範囲 15
2.4 論理的構成 15
2.4.1 論理構成 15
2.4.2 論理構成要素 16
2.4.3 論理構成の TOE 範囲 17
2.5 保護資産 17
2.6 TOE の機能 18
2.6.1 TOE が提供する機能 18
2.6.2 利用方法 20
2.6.3 運用手順 22
2.7 評価構成 24

3 TOE セキュリティ環境 25

3.1 前提条件 25

3.2 脅威 25
3.3 組織のセキュリティ方針 26

4 セキュリティ対策方針 27

4.1 TOE のセキュリティ対策方針 27
4.2 環境のセキュリティ対策方針 27

5 IT セキュリティ要件 29

5.1 TOE セキュリティ要件 29
5.1.1 TOE セキュリティ機能要件 29
5.1.2 TOE セキュリティ保証要件 42
5.1.3 最小機能強度 43
5.2 IT 環境に対するセキュリティ要件 43

6 TOE 要約仕様 44

6.1 TOE セキュリティ機能 44
6.1.1 TOE セキュリティ機能 44
6.1.2 TOE セキュリティ機能強度 49
6.2 保証手段 50

7 PP 主張 51

8 根拠 52

8.1 セキュリティ対策方針根拠 52
8.1.1 セキュリティ対策方針の必要性 52
8.1.2 セキュリティ対策方針の十分性 52
8.2 セキュリティ要件根拠 54
8.2.1 セキュリティ機能要件の必要性 54
8.2.2 セキュリティ機能要件の十分性 55
8.2.3 セキュリティ機能要件の依存性の妥当性 57
8.2.4 セキュリティ機能要件の相互サポート構造 59
8.2.5 最小機能強度の妥当性 61
8.2.6 評価保証レベルの妥当性 61
8.2.7 セキュリティ保証要件の根拠 61
8.2.8 セキュリティ機能要件の一貫性の根拠 61

8.3 TOE 要約仕様根拠 **61**
8.3.1 TOE セキュリティ機能の必要性 62
8.3.2 TOE セキュリティ機能の十分性 62
8.3.3 機能強度の根拠 65
8.3.4 保証手段の妥当性 65
8.4 PP 主張の根拠 **68**

1 ST 概説

本章では ST 概説として、ST 識別、ST 概要、CC 適合、用語･略語、及び商標について記述する。

1.1 ST 識別

本 ST の識別情報は以下の通りである。

ST 名称	和名 セイコーエプソン PP-100N セキュリティ制御機構 セキュリティターゲット 英名 SEIKO EPSON PP-100N Security control unit Security Target
ST バージョン	2.0
作成日	2009/07/03
作成者	セイコーエプソン株式会社
TOE 名称	和名 PP-100N セキュリティ制御機構 英名 PP-100N Security control unit
TOE バージョン	1.00
評価保証レベル	EAL3
キーワード	セイコーエプソン、エプソン、CD-R、DVD-R、パブリッシャー、 プリンタ、オートローダ、取り出し、電子錠
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 補足-0512 (Interpretations-0512) 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 Part1～3 2005 年 8 月バージョン 2.3 平成 17 年 12 月翻訳第 1.0 版

1.2 ST 概要

本 ST は、TOE である PP-100N セキュリティ制御機構の仕様を記述したものである。PP-100N は、ネットワークを介して電子情報を CD-R や DVD-R などのディスクに記録し、同時にレーベル印刷も行う CD/DVD パブリッシャー製品である。本 TOE は、利用者が自身の作成したディスクを確実に受け取ることができるよう、以下のセキュリティ機能を提供する。

- 識別認証機能
- 取り出し制御機能
- 電子錠開機能

- 警告機能
- 設定情報管理機能

1.3 CC 適合

- 本 ST は、以下に適合している。
- 機能要件 CC Part2 拡張
- 保証要件 CC Part3 適合
- 評価保証レベル EAL3
- 適合している PP なし

1.4 用語･略語

本 ST において使用する用語･略語を「表 1 用語解説」に示す。

表 1 用語解説

用語	内容
ディスク	CD-R、DVD-Rなどのディスク型記録媒体。
記録面	電子情報を記録するディスクの面。
レーベル面	印刷できるディスクの面。
ブランクディスク	電子情報が記録されていないディスク。
作成済みディスク	電子情報が記録され、レーベル面への印刷も完了したディスク。エラーディスクも含まれる。
エラーディスク	電子情報の記録、又はレーベル面への印刷に失敗したディスク。
レーベルデータファイル	レーベル面に印刷する印刷データファイル。
ディスクイメージファイル	記録面に記録するデータファイル。
スプールデータ	レーベルデータファイルをディスクに印刷するまで、及びディスクイメージファイルをディスクに記録するまでPP-100N内のHDD上に一時保管したデータ。
動作ログ	サービスマンに有用となる情報を時間経過と共に記録したもの。
監査ログ	セキュリティ機能の成否、TSFデータへのアクセス記録等を時間経過と共に記録したもの。
ソースデータ	ディスクイメージファイルの元データ。
スタッカ	ディスクを積み重ねて格納する容器。
スタッカ1	ブランクディスクをセットするスタッカ。スタッカは取り外し可能。セキュリティモードでは、ディスクの一時退避用にも使用される。
スタッカ2	作成済みディスクを格納するスタッカ。スタッカは取り外し可能。
スタッカ3	作成済みディスクを格納するスタッカ。スタッカ4の上に装着される。セキュリティモードでは使用されない。
スタッカ4	作成済みディスクを格納するスタッカ。作成済みディスクを利用者に渡すために使用される。
プリンタ	レーベル面を印刷する装置。

プリンタトレイ	レーベル面を印刷するディスクを乗せるトレイ。
ドライブ	ディスクの記録面にディスクイメージファイルを書き込むための装置。PP-100Nには2台搭載されている。
操作パネル	LCD、LED、操作キーから構成されるユーザインターフェース部。
ディスクカバー	PP-100Nの前面にあるカバー。通常はディスクカバー錠により鍵が掛けられ、電子錠、もしくは物理鍵により解錠してから開けることができる。ディスクカバーを開けると、以下の構成要素にアクセスできる。 ・ スタッカ1 ・ スタッカ2 ・ ドライブ ・ プリンタ ・ セキュリティロック切替レバー
JOB	ディスク作成ごとに発生する PP-100N の作業単位。
JOB ID	JOB を識別するために使用される番号。
SMTPサーバ	利用者にPP-100Nの状況を通知するために使用するメールサーバ。
セキュリティモード	PP-100Nにはセキュリティモードと非セキュリティモードがあり、セキュリティモードでは、以下の機能が自動的に必須機能として動作する。 ・ 識別認証機能 ・ 取り出し制御機能 ・ 電子錠開機能 ・ 警告機能 ・ 設定情報管理機能 尚、本STは、セキュリティモード設定時について記述する。
PP-100NWebアプリ	PP-100Nに搭載されたWebサーバ機能により、クライアントPCから呼び出され、ディスクの作成承認依頼、ディスクの作成承認、設定情報･利用者情報の登録/変更などを行うアプリケーション。
Total Disc Maker	クライアントPCにインストールされるアプリケーション。ディスクに書き込むファイルの選択、レーベル面のデザイン作成を行う。
Total Disc Monitor	クライアントPCにインストールされるアプリケーション。JOBの進捗状況確認、一時停止、再開、キャンセルなどを行う。
Total Disc Setup	クライアントPCにインストールされるアプリケーション。Total Disc Makerを使用するための初期設定を行う。
認証発行オプション	セキュリティモードにするために必須のものであり、以下の構成物からなる。 ・ 運用者ガイド（認証発行オプション編） ・ ユーザーズガイド（認証発行オプション編） ・ アクティベーションキー問い合せ先シート

CC Part1 に記載されている略語は省略する。

1.5 商標

商標に関して、本文中の社名や商品名は、各社の登録商標、もしくは商標である。

2 TOE 記述

本章では TOE 記述として、TOE の概要、TOE の関係者、物理的構成、論理的構成、保護資産、及び TOE の機能について記述する。

2.1 TOE の概要

2.1.1 TOE 種別

本 TOE は、CD-R や DVD-R にデータを記録するパブリッシャー製品「PP-100N」に組み込まれたセキュリティ制御機構であり、以下のセキュリティ機能を持つソフトウェアとハードウェアで構成された製品である。

- 識別認証[Web_app]機能：PP-100NWeb アプリから PP-100N へログインする利用者を識別認証する機能
- 識別認証[Cli_app]機能：Total Disc Maker や Total Disc Monitor から PP-100N へログインする利用者を識別認証する機能
- 識別認証[Panel]機能：操作パネルから PP-100N へログインする利用者を識別認証する機能
- 取り出し制御機能：ディスクを作成した利用者にディスクを排出する機能
- 電子錠開機能：ディスクカバーの電子錠の解錠を運用者のみに許可する機能
- 警告機能：セキュリティ侵害の可能性がある場合、運用者に警告を行う機能
- 設定情報管理機能：PP-100N を運用する上で必要になる情報（設定管理情報や JOB 情報など）へのアクセスを権限のある利用者のみに許可する機能

2.1.2 利用目的

本 TOE を利用することにより、ディスクを作成した本人のみが、自身の作成したディスクを受け取ることができる。従って、ディスクが他人の手に渡ることがなくなり、ディスクに記録されているデータの漏洩を防止することができる。

2.1.3 利用環境

本 TOE が利用される典型的な環境を「図 1 利用環境」に示す。

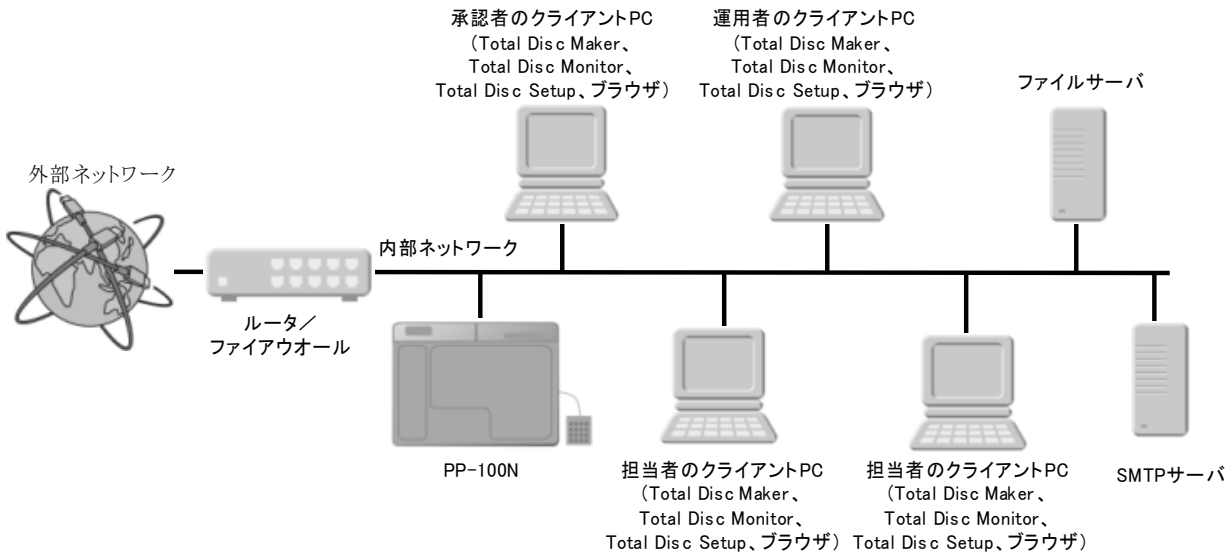

図 1 利用環境

通常、PP-100N はオフィスにおいて顧客情報を取り扱うエリアに設置される。また外部ネットワークとはルータやファイアウォールにより保護された状態にあり、内部ネットワークに接続されている。内部ネットワークにはクライアント PC、SMTP サーバ、ファイルサーバなどが接続されている。ディスクを作成する利用者のクライアント PC には Total Disc Maker、Total Disc Monitor、Total Disc Setup、及びブラウザがインストールされた状態にある。尚、外部ネットワーク、SMTP サーバ、ファイルサーバは、利用環境によっては存在しない場合もあるが TOE に影響はない。

2.2 TOE の関係者

本 TOE の関係者を「表 2 TOE の関係者」に示す。

表 2 TOE の関係者

関係者名	役割・権限	知識・信頼度
組織の責任者	PP-100N が設置されるオフィスの責任者。承認者、運用者を任命する。	信頼できる。TOE に対して悪意を持った行為は行わない。
利用者	PP-100N によるディスク作成の権限を持っている者。オフィスの関係者で運用者、承認者、担当者を含めて利用者と呼ぶ。	
運用者	PP-100N の運用管理を行う者。	信頼できる。TOE に対して悪意を持った行為は行わない。
担当者	運用者、承認者を除く利用者。	必ずしも信頼できるとは限らず、TOE に対して悪意を持った行為を行う可能性がある。高度な情報処理技術を有していない。
承認者	作成者（ディスク作成を行う利用者）が作成しようとするディスクの作成承認依頼を承認する者。	信頼できる。TOE に対して悪意を持った行為は行わない。
サービスマン	セイコーエプソン社員、現地法人社員、サービス委託修理会社社員であり、PP-100N 故障時の修理や保守を行う者。	サービスマンは、必ずしも信頼できるとは限らず、TOE に対して悪意を持った行為を行う可能性がある。修理を行うことができる知識はあるが、高度な情報処理技術を有していない。
第三者	上記以外の者。	TOEに対して悪意を持った行為を行う可能性がある。高度な情報処理技術を有していない。

2.3 物理的構成

2.3.1 ハードウェア構成

本 TOE が使用されるハードウェア構成を「図 2 ハードウェア構成」に示す。TOE は網掛け部である。

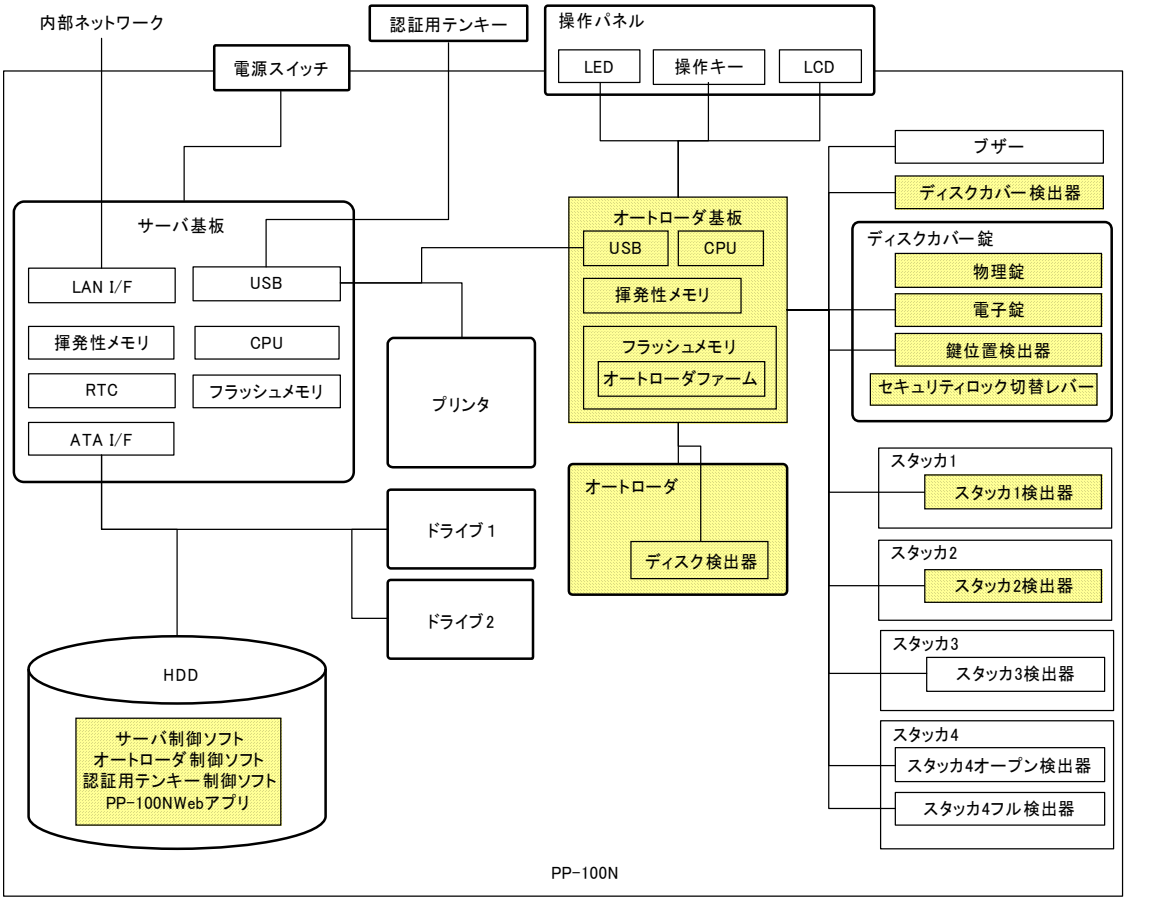

図 2 ハードウェア構成

2.3.2 ハードウェア構成要素

ハードウェア構成要素を「表 3 ハードウェア構成」に示す。

表 3 ハードウェア構成

構成要素	内容
オートローダ基板	オートローダファームが記録されたフラッシュメモリや入出力ポートなどから構成されたCPU基板であり、以下の制御を行う。 ・ オートローダ ・ ディスク検出器 ・ 操作パネル ・ ブザー ・ ディスクカバー検出器 ・ 電子錠 ・ 鍵位置検出器

	・ スタッカ1検出器 ・ スタッカ2検出器 ・ スタッカ3検出器 ・ スタッカ4オープン検出器 ・ スタッカ4フル検出器
オートローダ	ディスクを要求された場所(スタッカ1、スタッカ2、スタッカ4、プリンタトレイ、ドライブ)に搬送する装置。
ディスク検出器	オートローダがディスクを掴んでいるか否かを検出する検出器。また、スタッカ1、スタッカ2のディスク残量を確認する際にも使用される。
サーバ基板	CPU、メモリ、LAN I/F、USB I/F(オートローダ、プリンタ、及び認証用テンキー制御用)、ATA I/F(内蔵HDDやドライブ制御用)、RTC、HDD内のデータを暗号化する暗号化チップが実装されたCPU基板。PP-100Nを統合的に制御する。
HDD	サーバ基板用のHDD。サーバ制御ソフト、PP-100NWebアプリの他、スプールデータ、設定管理情報などのデータも記録する。
ディスクカバー検出器	ディスクカバーの開閉状態を検出する検出器。
ディスクカバー錠	ディスクカバーの錠であり、ソフトウェアから電気的に解錠できる電子錠、もしくは物理鍵により解錠できる物理錠のどちらかで解錠できる。ディスクカバーを閉めるとオートロックされる。
電子錠	ソフトウェアの制御により電気的に解錠できる錠。
物理錠	物理鍵により解錠できる錠。
鍵位置検出器	ディスクカバー錠の開閉状態とセキュリティロック切替レバーのオン/オフ状態を検出する検出器。
セキュリティロック切替レバー	ディスクカバー錠の有効/無効を切り替えるレバー。セキュリティロック切替レバーをオフにするとディスクカバー錠は常に解錠状態となる。オンにするとディスクカバー錠が有効になる。
スタッカ1検出器	スタッカ1にスタッカが着脱されたことを検出する検出器。
スタッカ2検出器	スタッカ2にスタッカが着脱されたことを検出する検出器。
スタッカ3検出器	スタッカ3が着脱されたことを検出する検出器。
スタッカ4オープン検出器	スタッカ4が引き出されたことを検出する検出器。
スタッカ4フル検出器	スタッカ4が収納許容枚数に達したことを検出する検出器。
電源スイッチ	PP-100Nの電源スイッチ。
LCD	操作メニューや警告メッセージを表示するディスプレイ。
LED	PP-100Nの状態を表す発光ダイオード。以下に示す3つのLEDがある。 ・ POWER LED:電源オン/オフ状態、プリンタのクリーニング状態を示す ・ BUSY LED:ディスク作成中であることを示す ・ ERROR LED:エラー状態であることを示す
操作キー	LCDに表示される操作メニューの操作を行う入力ボタン。
ブザー	PP-100Nに異常が発生したことを音で知らせる装置。
認証用テンキー	PP-100Nにおいて識別認証を行うために使用するUSBテンキー。本テンキーはオプシ

	ョンである。製品には同梱されないが、TOEを操作するために必須である。運用者が準備し、PP-100Nに接続する必要がある。

2.3.3 ハードウェアの TOE 範囲

ハードウェアの TOE 範囲を以下に示す。(「図 2 ハードウェア構成」の網掛け部参照)

- オートローダ基板
- オートローダ
- ディスク検出器
- ディスクカバー検出器
- 物理錠
- 電子錠
- 鍵位置検出器
- セキュリティロック切替レバー
- スタッカ 1 検出器
- スタッカ 2 検出器

2.3.4 ソフトウェア構成

TOE が利用されるソフトウェア構成を「図 3 ソフトウェア構成」に示す。TOE は網掛け部である。

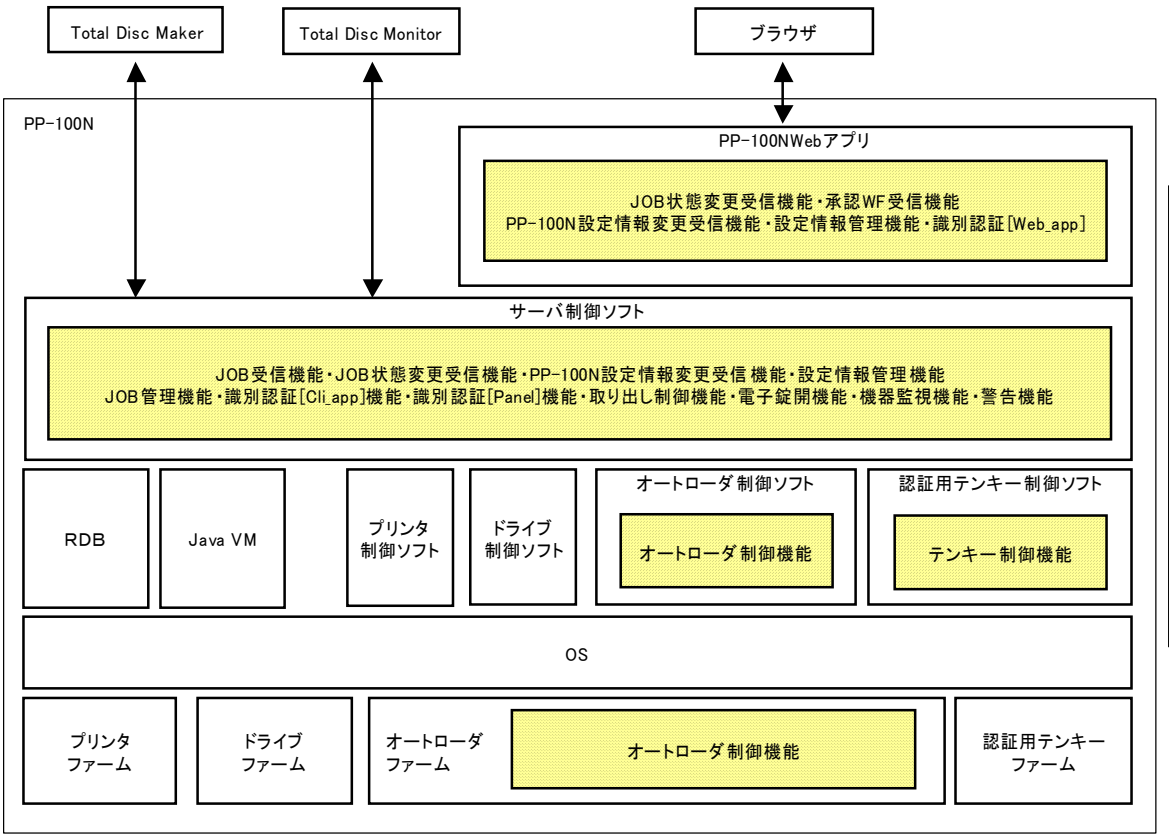

図 3 ソフトウェア構成

2.3.5 ソフトウェア構成要素

ソフトウェア構成要素を「表 4 ソフトウェア構成」に示す。

表 4 ソフトウェア構成

構成要素	内容
PP-100NWebアプリ	PP-100Nに搭載されたWebサーバ機能により、クライアントPCから呼び出され、ディスクの作成承認依頼、ディスクの作成承認、設定情報・利用者情報の登録/変更などを行うアプリケーション。
Total Disc Maker	クライアントPCにインストールされるアプリケーション。ディスクに書き込むファイルの選択、レーベル面のデザイン作成を行う。
Total Disc Monitor	クライアントPCにインストールされるアプリケーション。JOBの進捗状況確認、一時停止、再開、キャンセルなどを行う。
サーバ制御ソフト	PP-100N 本体を制御するソフトウェア。サーバ基板に搭載された OS 上で動作する。
RDB	リレーショナルデータベース。以下の情報を取り扱う。 ・ 設定管理情報 ・ JOB 情報 ・ ディスク位置情報 ・ 監査ログ ・ 動作ログ ・ スプールデータへのパス情報（物理的位置情報）
オートローダ制御ソフト	オートローダを制御するライブラリ。
プリンタ制御ソフト	プリンタを制御するライブラリ。
ドライブ制御ソフト	ドライブを制御するライブラリ。
認証用テンキー制御ソフト	認証用テンキーを制御するライブラリ。
プリンタファーム	プリンタ機構を制御するため、プリンタ基板内に搭載されたファームウェア。
ドライブファーム	ドライブ機構を制御するため、ドライブに搭載されたファームウェア。
オートローダファーム	次の機構を制御するため、オートローダ基板に搭載されたファームウェア。 ・ オートローダ ・ 操作パネル ・ ブザー ・ ディスクカバー検出器 ・ 電子錠 ・ 鍵位置検出器 ・ スタッカ1検出器 ・ スタッカ2検出器 ・ スタッカ3検出器 ・ スタッカ4オープン検出器 ・ スタッカ4フル検出器
認証用テンキーファーム	認証用テンキーを制御するファームウェア。
ブラウザ	Webページを閲覧するためのアプリケーション。
Java VM	Javaバイトコードをそのプラットフォームのネイティブコードに変換して実行するソフトウェア。

2.3.6 ソフトウェアの TOE 範囲

ソフトウェアの TOE 範囲は以下の各要素の一部である。(「図 3 ソフトウェア構成」の網掛け部参照)

- サーバ制御ソフト
- PP-100NWeb アプリ
- オートローダ制御ソフト
- オートローダファーム
- 認証用テンキー制御ソフト

2.4 論理的構成

2.4.1 論理構成

本 TOE の論理構成図を「図 4 論理構成」に示す。TOE は網掛け部である。

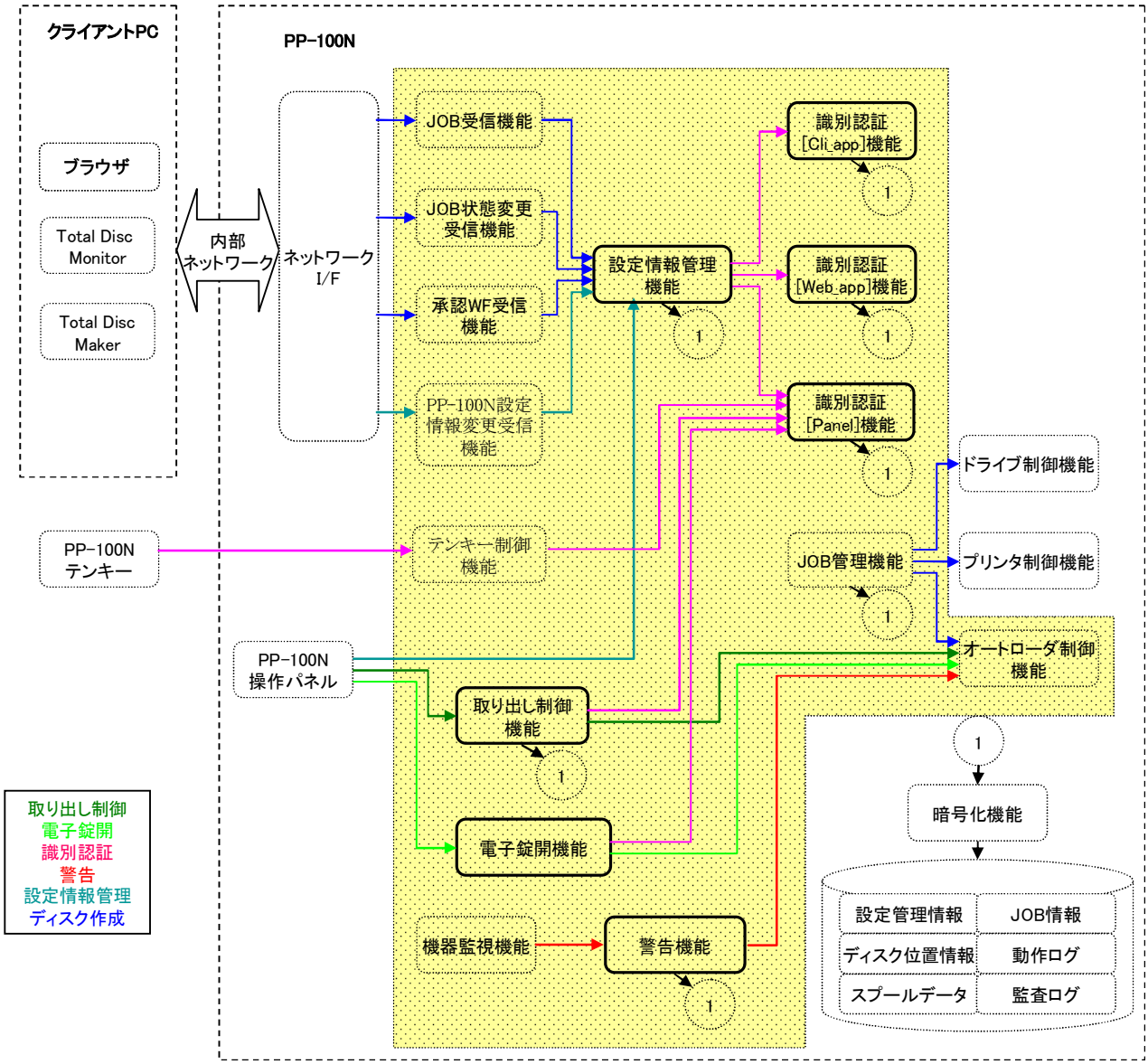

図 4 論理構成

2.4.2 論理構成要素

論理構成要素を「表 5 論理構成要素」に示す。

表 5 論理構成要素

構成要素	内容
識別認証[Panel]機能	ディスク取り出し、電子錠の解錠、PP-100Nの設定変更を行うため、操作パネルからPP-100Nへログインする利用者を識別認証する機能。
識別認証[Web_app]機能	利用者情報や設定情報を操作するため、PP-100NWeb アプリから PP-100N へログインする利用者を識別認証する機能。
識別認証[Cli_app]機能	JOB 登録、JOB 進行状況確認、一時停止、再開、キャンセルを行うため、Total Disc Maker や Total Disc Monitor から PP-100N へログインする利用者を識別認証する機能。
取り出し制御機能	オートローダを制御し、スタッカ 2 に保管された作成済みディスクから、利用者が作成したディスクのみをスタッカ 4 に排出する機能。
電子錠開機能	運用者に電子錠の解錠を許可する機能。
警告機能	PP-100N にセキュリティ侵害の可能性が発生した場合、ブザー、LED、及び LCD により警告する機能。
設定情報管理機能	PP-100N 内の情報（設定管理情報や JOB 情報など）へのアクセスを、権限のある利用者のみに許可する機能
機器監視機能	ディスクカバー検出器、鍵位置検出器、ディスク検出器、スタッカ 1 検出器、スタッカ 2 検出器、スタッカ 3 検出器、スタッカ 4 オープン検出器、及びスタッカ 4 フル検出器からの情報を受け付け、また情報を要求する機能。
ドライブ制御機能	ドライブを制御する機能。
プリンタ制御機能	プリンタを制御する機能。
オートローダ制御機能	オートローダを制御する機能。
JOB 管理機能	JOB 実行を管理する機能。
JOB 受信機能	JOB を受信する機能。
JOB 状態変更受信機能	JOB 情報の変更依頼を受信する機能。
承認 WF 受信機能	承認者からのディスク作成を承認する情報を受信する機能。
PP-100N 設定情報変更受信機能	PP-100N に対する設定情報変更依頼を受信する機能。
テンキー制御機能	テンキーから入力された信号をサーバ制御ソフトへのコマンドとして変換する機能。
暗号化機能	HDD に記録するデータを暗号化し、また復号化する機能。
設定管理情報	PP-100N の設定情報と各利用者の利用者情報の総称。
JOB 情報	JOB に関連付けられた各種の情報。
ディスク位置情報	JOB に対するスタッカ 2 におけるディスクの位置情報。
スプールデータ	レーベルデータファイルをディスクに印刷するまで、及びディスクイメージファイルをディスクに記録するまで PP-100N 内の HDD 上に一時保管したデータ。
動作ログ	サービスマンに有用となる情報を時間経過と共に記録したもの。
監査ログ	セキュリティ機能の成否、TSF データへのアクセス記録等を時間経過と共に記録したもの。

2.4.3 論理構成の TOE 範囲

論理構成の TOE 範囲を以下に示す。(「図 4 論理構成」の網掛け部参照)

- 識別認証[Web_app]機能
- 識別認証[Cli_app]機能
- 識別認証[Panel]機能
- 取り出し制御機能
- 電子錠開機能
- 警告機能
- 設定情報管理機能
- 機器監視機能
- JOB 管理機能
- オートローダ制御機能
- JOB 受信機能
- JOB 状態変更受信機能
- 承認 WF 受信機能
- PP-100N 設定情報変更受信機能
- テンキー制御機能

2.5 保護資産

本 TOE の保護資産は、PP-100N 内に保管された作成済みディスク内のデータである。作成済みディスクには PP-100N を購入した企業における機密情報が記録されている。ディスクが持ち出されてしまうと、高度な情報処理知識を有しなくともディスクの中身を容易に見ることができてしまう。従って、ディスクは、承認者によって作成を許可された者のみに渡らなければならない。

作成済みディスクが取り出されるまでのデータの流れを以下に示す。

1. 利用者のクライアント PC において、ファイルサーバやクライアント PC 内にあるソースファイルを選択し、ディスクイメージファイルを作成する。ソースファイル、及びディスクイメージファイルは、そのオフィスが管理しているファイルサーバやクライアント PC 内にあるので、本 TOE の保護資産としない。
2. ディスクイメージファイルは、PP-100N に転送され、スプールデータとして HDD に一時保管される。
3. ディスク作成要求により、スプールデータをディスクに記録し、作成済みディスクとして PP-100N 内に保管する。作成済みディスクはディスクカバー錠により施錠された PP-100N 内にあり、容易に取り出すことはできない。
4. ディスクの取り出し要求により、作成済みディスクはスタッカ 4 に排出される。
5. 排出された作成済みディスク内のデータは、ディスクを作成した利用者の管理責任とし、本 TOE の保護資産としない。

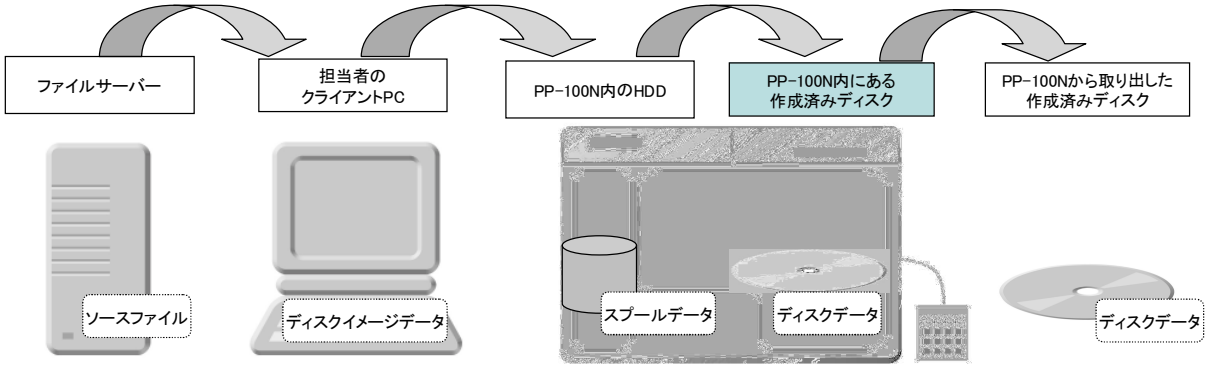

図 5 データの流れ

以上より、スプールデータがディスクへ記録された時点から、そのディスクがスタッカ4に排出されるまでの間のディスク内のデータを、本 TOE の保護資産とする。

2.6 TOE の機能

2.6.1 TOE が提供する機能

TOE が提供するセキュリティ機能

- 識別認証機能
  - 識別認証[Web_app]機能

    クライアント PC のブラウザを介し PP-100NWeb アプリから PP-100N へログインする利用者を識別認証する機能。
  - 識別認証[Cli_app]機能

    クライアント PC の Total Disc Maker や Total Disc Monitor から PP-100N へログインする利用者を識別認証する機能。
  - 識別認証[Panel]機能

    PP-100N の操作パネルから PP-100N へログインする利用者を識別認証する機能。

- 取り出し制御機能

スタッカ 2 に保管された作成済みディスクをスタッカ 4 に排出する機能。PP-100N の操作パネルにある取り出しボタンが押されると、取り出し制御機能は、登録されている利用者であるか否かを確認するため、識別認証[Panel]機能の実行を要求する。次に、取り出し制御機能は識別認証[Panel]機能により識別認証された利用者の作成済みディスクがスタッカ 2 に存在するか否かを確認する。存在するならば、オートローダを制御し、該当するディスクのみをスタッカ 4 に排出する。

- 電子錠開機能

ディスクカバーの電子錠を解錠する機能。操作パネルの操作メニューから電子錠を解錠するメニュー項目が選択されると、電子錠開機能は、操作する利用者が運用者であるか否かを確認するため、識別認証[Panel]機能の実行を要求する。利用者が運用者であると確認されたならば、電子錠開機能は電子錠を解錠する。

■ 警告機能

セキュリティ侵害の可能性を検知し、運用者に対して以下の警告を行う機能。

・ ブザーを鳴らす
・ ERROR LED を点灯する
・ LCD にセキュリティ侵害の可能性の内容を表示する

セキュリティ侵害の可能性のある事象を、以下に示す。

1) 作成済みディスク残留
・ 電源オフ処理時、PP-100N 内に作成済みディスクがある

2) ディスクカバー未施錠
・ ディスクカバーが 60 秒以上開いた状態
・ ディスクカバーを閉めた後、物理錠により 10 秒以上解錠の状態
・ ディスクカバーを閉めた後、10 秒以上セキュリティロック切替レバーがオフの状態

3) ディスク取り落とし
・ オートローダがディスクを取り落とす

4) スタッカ 2 取り外し
・ 「ディスクカバーが開いているときに、スタッカ 2 が取り外され戻された」かつ「ディスクカバーが閉められたときに、スタッカ 2 にディスクがある」

■ 設定情報管理機能

識別認証[Web_app]機能、識別認証[Cli_app]機能、識別認証[Panel]機能により識別認証され、動作進行を許可された者のみに設定管理情報、及び JOB 情報へのアクセスを許可する機能。設定管理情報、及び JOB 情報の閲覧、追加、変更、削除も行う。

TOE が提供する非セキュリティ機能

■ 機器監視機能

ディスクカバー検出器、鍵位置検出器、ディスク検出器、スタッカ 1 検出器、スタッカ 2 検出器、スタッカ 3 検出器、スタッカ 4 オープン検出器、及びスタッカ 4 フル検出器からの情報を受け付け、また情報を要求する機能。

■ JOB 管理機能

JOB の実行を管理する機能。JOB 情報を監視し、状態が変更された JOB が発生次第、順次 JOB を実行する。

■ オートローダ制御機能

オートローダを制御して、ディスクを要求された場所（スタッカ 1、スタッカ 2、スタッカ 4、プリンタトレイ、ドライブ）に搬送する機能。

■ JOB 受信機能

Total Disc Maker において発行した JOB を受信する機能。

■ JOB 状態変更受信機能

Total Disc Monitor からの JOB の進捗状況確認、一時停止、再開、キャンセルなどの要求を受信する機能。更に PP-100NWeb アプリからの JOB 承認申請を受信する機能。

■ 承認 WF 受信機能

承認者からのディスク作成を承認する情報を受信する機能。

■ PP-100N 設定情報変更受信機能

運用者からの PP-100N に対する設定情報変更依頼を受信する機能。

■ テンキー制御機能

テンキーから入力された信号をサーバ制御ソフトへのコマンドとして変換する機能。

2.6.2 利用方法

ディスク作成までのフローを「図 6 ディスク作成」に示す。

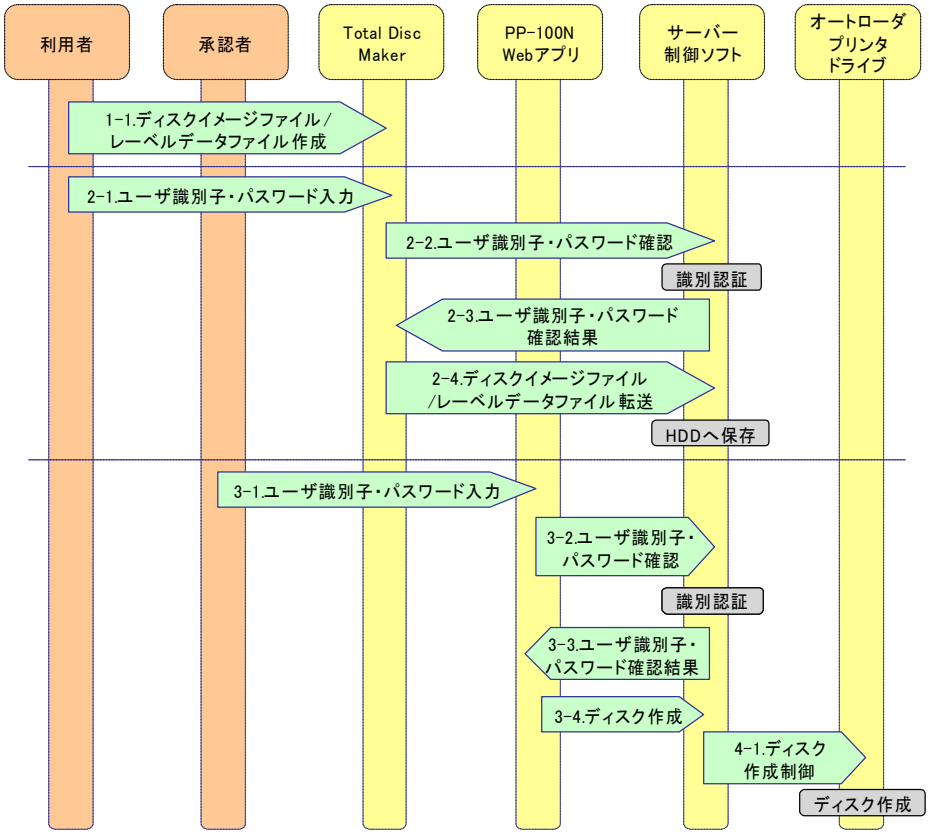

図 6 ディスク作成

1 ディスクイメージファイルの作成

1. 利用者はクライアント PC にインストールされた Total Disc Maker により、ファイルサーバやクライアント PC に保持されたデータからディスクイメージファイルとレーベルデータファイルを作成する。

2 ディスクイメージファイルの転送

1. 利用者は Total Disc Maker のディスク発行を実行し、ユーザ識別子[Appli]とパスワード[Appli]を入力する。
2. Total Disc Maker はサーバ制御ソフトに対して、正しい利用者であるか否かを確認する。

3. サーバ制御ソフトは識別認証を実行し、Total Disc Maker に識別認証の確認結果を通知する。
4. Total Disc Maker はディスクイメージファイルとレーベルデータファイルを PP-100N に転送する。転送されたデータはスプールデータとして HDD に記録される。

3 ディスク承認

1. 承認者は PP-100NWeb アプリを起動し、ユーザ識別子[Appli]とパスワード[Appli]を入力する。
2. PP-100NWeb アプリはサーバ制御ソフトに対して、正しい承認者であるか否かを確認する。
3. サーバ制御ソフトは識別認証を実行し、PP-100NWeb アプリに識別認証の確認結果を通知する。
4. PP-100NWeb アプリはサーバ制御ソフトにディスク作成を指示する。

4 ディスク作成

1. サーバ制御ソフトは JOB 情報を監視し、ディスク作成が実行できる状態になり次第、処理（データ記録、レーベル印刷）を実行する。作成されたディスクはスタッカ 2 に格納される。

JOB 操作とディスク取り出しのフローを「図 7 JOB 操作とディスク取り出し」に示す。

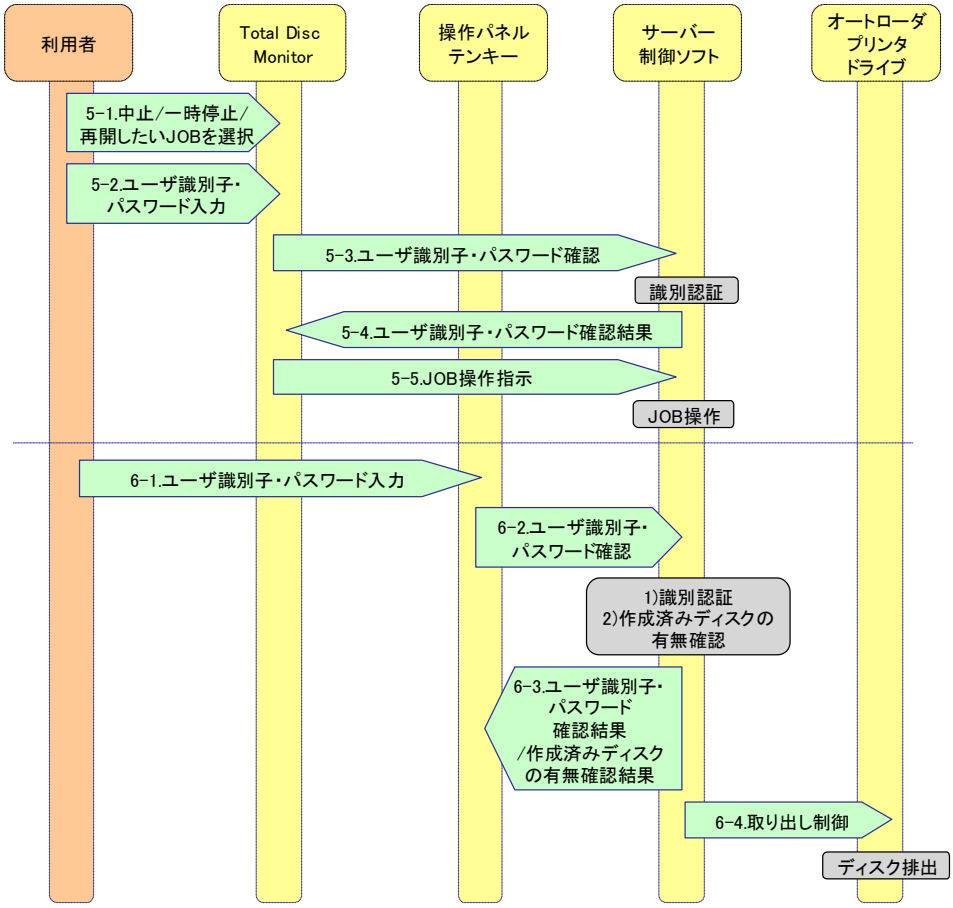

図 7 JOB 操作とディスク取り出し

5 JOB 操作

1. 利用者は Total Disc Monitor より一時停止、再開、キャンセル JOB を選択する。操作対象となる JOB とは、「承認済み」で「ディスク作成待ち」もしくは「ディスク作成中」の JOB のことである。また、操作種別により、対象となる JOB は以下のように区分される。
   - 一時停止

「承認済み」で「ディスク作成待ち」もしくは「ディスク作成中」の JOB

- 再開

「一時停止中」の JOB

- キャンセル

「承認済み」で「ディスク作成待ち」もしくは「ディスク作成中」の JOB

「一時停止中」の JOB

2. 利用者は Total Disc Monitor よりユーザ識別子[Appli]とパスワード[Appli]を入力する。
3. Total Disc Monitor はサーバ制御ソフトに対して、利用者に JOB 操作の権限があるか否かを確認する。
4. サーバ制御ソフトは識別認証を実行し、Total Disc Monitor に識別認証の確認結果を通知する。
5. Total Disc Monitor はサーバ制御ソフトに JOB 操作を指示する。

6 ディスク取り出し

1. ディスクを作成した利用者は、ディスクを取り出すため、PP-100N の操作パネルにあるディスク取り出しボタンを押し、認証用テンキーよりユーザ識別子[Panel]とパスワード[Panel]を入力する。
2. サーバ制御ソフトに正しい利用者であるか否か、またその利用者の作成済みディスクが存在するか否かを確認する。
3. サーバ制御ソフトは識別認証と作成済みディスクの有無確認を実行し、その結果を通知する。
4. サーバ制御ソフトは識別認証された利用者の作成済みディスクを、オートローダを制御し、スタッカ 2 からスタッカ 4 へ移動させる。

2.6.3 運用手順

TOE を正しく動作させるため、以下の運用手順に従わなければならない。

＜購入後の対応＞

運用者は、PP-100N 及び認証発行オプションを購入後、運用を開始する前に以下のことを行う必要がある。

1. 認証用テンキー接続

PP-100N 内部にある USB ポートに認証用テンキーを接続する。

2. セキュリティモード設定

電源を投入すると操作パネルに操作メニューが表示される。操作メニューに従い、セキュリティモードに設定する。

3. ネットワーク設定

操作パネルの操作メニューより、IP アドレス等のネットワーク設定を行う。

4. クライアント PC にアプリケーションをインストール

同梱されているインストール CD からクライアント PC に、Total Disc Maker、Total Disc Setup、Total Disc Monitor をインストールする。

5. PP-100N の登録

クライアント PC の Total Disc Setup を起動し、PP-100N を登録する

6. 運用者登録

クライアント PC のブラウザを起動し、PP-100N に直接接続する。その際、運用者を登録する。

7. 利用者情報管理

PP-100N の PP-100NWeb アプリを起動し、（ユーザ識別子[Appli]、パスワード[Appli]による）識別・認証後、利用者の利用者情報を登録する。

8. TOE バージョンの確認

操作パネルの操作メニューより、TOE バージョンを確認する。

＜通常運用時の対応＞

運用者は、PP-100N の通常運用時、以下のことを行う必要がある。

1. 利用者情報管理

PP-100N の PP-100NWeb アプリを起動し、（ユーザ識別子[Appli]、パスワード[Appli]による）識別・認証後、利用者の利用者情報を登録・変更する。

2. ブランクディスクの供給

操作パネルに操作メニューを表示し、認証用テンキーより識別認証後、ディスクカバーを開け、スタッカ 1 にブランクディスクをセットする。

3. 電源オン時の対応

電源オン時、スタッカ 2 に残存するディスクを全て取り除く。

4. スタッカ 2 を取り外した際の対応

スタッカ 2 を取り外した際、スタッカ 2 に残存するディスクを全て取り除く。

5. 警告時の処置

PP-100N にセキュリティ侵害の可能性が発生し、警告が発せられた場合には、早急にその原因を排除する。

利用者は、PP-100N の通常運用時、以下のことを行う必要がある。

1. 本人情報管理

PP-100N の PP-100NWeb アプリを起動し、（ユーザ識別子[Appli]、パスワード[Appli]による）識別・認証後、利用者本人のパスワード[Appli]とパスワード[Panel]を変更する。

＜修理・保守時の対応＞

PP-100N の修理・保守には、PP-100N が設置された場所にサービスマンを派遣するオンサイトサービスと、PP-100N をサービスセンターに送付して修理するオフサイトサービスの 2 通りがある。運用者は、PP-100N の運用・保守時、以下のことを行う必要がある。

1. オンサイトサービスの場合

運用者はサービスマンが PP-100N の修理・保守作業を行っている間、その修理・保守作業に同席する。

2. オフサイトサービスの場合

運用者は PP-100N 内にある作成済みディスクを取り除き、設定管理情報を全て消去してからサービスセンターに送付する。

2.7 評価構成

本 TOE のテストで使用した評価構成を以下に示す。

・ クライアント PC の OS

WindowsXP Professional SP3

WindowsVista Ultimate SP1

・ ブラウザ

Internet Explorer6 SP3

Internet Explorer7

・ クライアントアプリケーション

Total Disc Monitor Ver.2.0

Total Disc Maker Ver.2.0

・ テンキー

サンワサプライ NT-9UBK

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記述する。

3.1 前提条件

前提条件は以下の通りである。

A.承認者

承認者は、TOE に対して悪意を持った行為を行わない。

A.運用者

運用者は、TOE に対して悪意を持った行為を行わない。

A.パスワード

利用者のパスワードは、利用者本人以外に知られることはない。また、パスワードは推測されにくいものが設定され、適切な頻度で変更される。

A.運用状態管理

運用者は、以下に示すことが行われないよう PP-100N の運用状態を管理する。

- PP-100N の破壊
- 運用者以外の者によるディスクカバー解錠

A.セキュリティモード

運用者は、認証発行オプションを購入後、認証用テンキーを接続し、PP-100N をセキュリティモードに設定する。

A.ネットワーク

ネットワーク環境は、以下の条件を満たす。

- TOE は、外部ネットワークからの攻撃を受けることはない。
- TOE が実装される機器に接続する内部ネットワークは、盗聴されることはない。

3.2 脅威

脅威は以下の通りである。

T.ディスク持ち出し

ディスクを作成した担当者以外の者が、ディスクを作成した担当者、もしくは運用者になりすまし、作成済みディスクを持ち出し、ディスクデータを暴露するかもしれない。

T.ディスクカバー未施錠

運用者のミスによりディスクカバーが未施錠の状態となり、ディスクを作成した担当者以外の者が、作成済みディスクを持ち出し、ディスクデータを暴露するかもしれない。

T.ディスク取り落とし

オートローダが作成済みディスクを搬送中に取り落とした場合、作成済みディスクがスタッカ 4 に入る可能性がある。その際、ディスクを作成した担当者以外の者が、オートローダが取り落とした作成済みディスクを持ち出し、そのディスクデータを暴露するかもしれない。

T.ディスク置き間違え

ディスクを作成した担当者以外の者が、運用者、もしくはサービスマンによるスタッカ 2 へのディスクの置き間違えにより誤排出された作成済みディスクを持ち出し、ディスクデータを暴露するかもしれない。

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以下の通りである。

P.作成済みディスク

作成済みディスクが残った状態で PP-100N の運用が停止されることはない。

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記述する。

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.識別認証

TOE は、TOE へアクセスする利用者を識別認証しなければならない。また、TOE は、識別認証において、利用者のパスワード[Panel]を秘匿しなければならない。

O.取り出し制御

TOE は、ディスクを取り出す際、ディスクを作成した利用者本人のディスクを取り出さなければならない。

O.カバー開制御

TOE は、運用者のみがディスクカバーを開けることができるようにしなければならない。

O.登録管理

TOE は、利用者情報の追加、変更、削除、参照(※パスワード[Appli]、パスワード[Panel]の参照を除く。)と設定情報の変更、参照を運用者のみに制限しなければならない。TOE は利用者に対して、本人のパスワード[Appli]、パスワード[Panel]の変更を許可しなければならない。

O.警告

TOE は、以下のセキュリティ侵害の可能性が発生した場合において、その事象を検出し、運用者に警告しなければならない。

- 電源オフ処理時、PP-100N 内に作成済みディスクがある
- ディスクカバーが未施錠となる
- オートローダがディスクを取り落とす
- 電源オン期間中、スタッカ 2 が取り外され戻されたとき、スタッカ 2 内にディスクがある

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。

OE.承認者の信頼

組織の責任者は、信頼できる人物を承認者に任命しなければならない。

OE.運用者の信頼

組織の責任者は、信頼できる複数の人物を運用者に任命し、必要な知識が習得できるよう教育を実施しなければならない。

OE.運用者による対応

PP-100N の運用･保守において、TOE にセキュリティ侵害の可能性が発生した場合、運用者は速やかに対応しなければならない。

OE.パスワード管理

利用者は、自身のパスワードを本人以外の人に知られないよう管理しなければならない。また、TOE のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワードを変更しなければならない。

OE.運用者監視

運用者は、以下に示すことが行われないよう PP-100N の運用状態を監視しなければならない。

- PP-100N の破壊
- 運用者以外の者によるディスクカバー解錠

OE.セキュリティモード設定

運用者は、PP-100N を運用する場合、認証発行オプションを購入し、以下の項目が未設定である場合には対処しなければならない。

- 認証用テンキーの接続
- セキュリティモードへの設定

OE.ネットワーク

運用者は、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データを盗聴から保護しなければならない。

OI.パスワード秘匿

ブラウザ、Total Disc Maker、及び Total Disc Monitor は、識別認証において、利用者のパスワード[Appli]を秘匿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記述する。

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記述する。

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。本 ST では新規に TOE セキュリティ機能要件（FAU_GET.1 イベント情報の取得）を作成し、使用する。

FAU_ARP.1 セキュリティアラーム

下位階層:なし

FAU_ARP.1.1	TSFは、セキュリティ侵害の可能性が検出された場合、[割付: 混乱を最小にするアクションのリスト]を実行しなければならない。 [割付: 混乱を最小にするアクションのリスト] ・ 警告をする（ブザー、LED 点灯、LCD 表示）

依存性: FAU_SAA.1 侵害の可能性の分析

FAU_SAA.1 侵害の可能性の分析

下位階層: なし

FAU_SAA.1.1	TSF は、監査事象のモニタに規則のセットを適用し、これらの規則に基づき TSP 侵害の可能性を示すことができなければならない。
FAU_SAA.1.2	TSFは、監査事象をモニタするための以下の規則を実施しなければならない; a) セキュリティ侵害の可能性を示すものとして知られている[割付: 定義された監査対象事象のサブセット]をすべて合わせた、あるいは組み合わせたもの; b) [割付: その他の規則]。 [割付: 定義された監査対象事象のサブセット] ・ 電源オフ処理時、PP-100N内に作成済みディスクがある ・ ディスクカバーが未施錠となる ・ オートローダがディスクを取り落とす ・ 電源オン期間中、スタッカ2が取り外され戻されたとき、スタッカ2内にディスクがある [割付: その他の規則] なし

依存性: FAU_GEN.1 監査データ生成

FAU_GET.1 イベント情報の取得

FAU_GET.1は監査対象事象に対するイベント情報を取得する。

管理: FAU_GET.1

予見される管理アクティビティはない。

監査: FAU_GET.1

予見される監査対象事象はない。

下位階層: なし

FAU_GET.1.1	TSFは、[割付: 個別に定義した監査対象事象]のイベント情報を取得できなければならない: [割付: 個別に定義した監査対象事象] ・ 電源オフ処理時、PP-100N内に作成済みディスクがある ・ ディスクカバーが未施錠となる ・ オートローダがディスクを取り落とす ・ 電源オン期間中、スタッカ2が取り外され戻されたとき、スタッカ2内にディスクがある

依存性: なし

FIA_UAU.2[Panel] 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。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2[Panel] 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

FIA_UAU.7[Panel] 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] 入力された文字数と同数の"*"の表示

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1[Panel] 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1	TSF は、[割付: 認証事象のリスト]に関して、[選択: [割付:正の整数値], 「[割付:許容可能な値の範囲]内における管理者設定可能な正の整数」]回の不成功認証試行が生じたときを検出しなければならない。 [割付: 認証事象のリスト] 操作パネルからサーバ制御ソフトへの利用者認証 [選択: [割付:正の整数値], 「[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数」] [割付:正の整数値] 3
FIA_AFL.1.2	不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: アクションのリスト]をしなければならない。 [割付: アクションのリスト] ・ 既定時間（運用者：6 時間、運用者以外：1 時間）のアカウントロック

依存性: FIA_UAU.1 認証のタイミング

FIA_SOS.1[Panel] 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] パスワード[Panel]：数字5桁以上

依存性: なし

FIA_UAU.2[Appli] 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。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2[Appli] 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

FIA_AFL.1[Appli] 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1	TSF は、[割付: 認証事象のリスト]に関して、[選択: [割付:正の整数値], 「[割付:許容可能な値の範囲]内における管理者設定可能な正の整数」]回の不成功認証試行が生じたときを検出しなければならない。 [割付: 認証事象のリスト] ・ PP-100NWeb アプリからサーバ制御ソフトへの利用者認証 ・ Total Disc Maker からサーバ制御ソフトへの利用者認証 ・ Total Disc Monitor からサーバ制御ソフトへの利用者認証 [選択: [割付:正の整数値], 「[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数」] [割付:正の整数値] 3
FIA_AFL.1.2	不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: アクションのリスト]をしなければならない。 [割付: アクションのリスト] ・ 既定時間（運用者：6 時間、運用者以外：1 時間）のアカウントロック

依存性: FIA_UAU.1 認証のタイミング

FIA_SOS.1[Appli] 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] パスワード[Appli]：英数字又は特殊文字（「.」「-」「_」）5 桁以上

依存性: なし

FDP_ETC.1 セキュリティ属性なし利用者データのエクスポート

下位階層: なし

FDP_ETC.1.1	TSFは、SFP(s)制御下にある利用者データをTSCの外部にエクスポートするとき、[割付: アクセス制御SFP(s)、及び/または情報フロー制御SFP(s)]を実施しなければならない。 [割付: アクセス制御SFP(s)、及び/または情報フロー制御SFP(s)] 取り出し制御 SFP
FDP_ETC.1.2	TSF は、利用者データに関係したセキュリティ属性なしで利用者データをエクスポートしなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御、あるいは FDP_IFC.1 サブセット情報フロー制御]

FDP_ACC.1[Disk_eject] サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1	TSFは、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。 [割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト] サブジェクト: ・ 担当者プロセス オブジェクト: ・ JOB 情報 ・ ディスク位置情報 SFP で扱われるサブジェクトとオブジェクト間の操作リスト: ・ JOB 情報を参照する、変更する ・ ディスク位置情報を参照する、変更する、削除する [割付: アクセス制御 SFP] 取り出し制御 SFP

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1[Disk_eject] セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1	TSFは、以下の[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御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オブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ] ・ 「表6 サブジェクト及び対応するセキュリティ属性(Disk_eject)」参照 ・ 「表7 オブジェクト及び対応するセキュリティ属性(Disk_eject)」参照 [割付: アクセス制御SFP] 取り出し制御 SFP
FDP_ACF.1.2	TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

	[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則] ・ 以下の場合において、JOB情報、ディスク位置情報の参照を許可する 担当者プロセスに関連付けられたユーザ識別子[Appli]とJOB情報に関連付けられたユーザ識別子[Appli]が一致し、そのJOB情報に関連付けられたJOB IDとディスク位置情報に関連付けられたJOB IDが一致する ・ 以下の場合において、JOB情報の変更、ディスク位置情報の変更、削除を許可する JOB の実行が完了する
FDP_ACF.1.3	TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。 [割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則] なし
FDP_ACF.1.4	TSFは、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則] なし

依存性: FDP_ACC.1 サブセットアクセス制御

依存性: FMT_MSA.3 静的属性初期化

表 6 サブジェクト及び対応するセキュリティ属性(Disk_eject)

制御されるサブジェクト	対応するSFP関連セキュリティ属性
担当者プロセス	ユーザ識別子[Appli]

表 7 オブジェクト及び対応するセキュリティ属性(Disk_eject)

制御されるオブジェクト	対応するSFP関連セキュリティ属性
JOB 情報	ユーザ識別子[Appli]、JOB ID
ディスク位置情報	JOB ID

FMT_MSA.3 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] 一意な識別子 [割付: アクセス制御SFP、情報フロー制御SFP] 取り出し制御SFP
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

依存性: FMT_SMR.1 セキュリティの役割

FDP_ACC.1[Cover_open] サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1	TSFは、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。 [割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト] サブジェクト: ・ 運用者プロセス オブジェクト: ・ 電子錠 SFPで扱われるサブジェクトとオブジェクト間の操作リスト: ・ 電子錠を解錠する [割付: アクセス制御SFP] カバー開制御SFP

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1[Cover_open] セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1	TSFは、以下の[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御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オブジェクトのリスト、及び各々に対応

	する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ] ・ 「表 8 サブジェクト及び対応するセキュリティ属性（Cover_open）」参照 ・ 「表 9 オブジェクト及び対応するセキュリティ属性（Cover_open）」参照 [割付: アクセス制御SFP] カバー開制御SFP
FDP_ACF.1.2	TSFは、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。 [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則] ・ 以下の場合において、電子錠の解錠を許可する 運用者プロセスに運用者権限があることが確認された
FDP_ACF.1.3	TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。 [割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則] なし
FDP_ACF.1.4	TSFは、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則] なし

依存性: FDP_ACC.1 サブセットアクセス制御

依存性: FMT_MSA.3 静的属性初期化

表 8 サブジェクト及び対応するセキュリティ属性（Cover_open）

制御されるサブジェクト	対応するSFP関連セキュリティ属性
運用者プロセス	運用者権限

表 9 オブジェクト及び対応するセキュリティ属性（Cover_open）

制御されるオブジェクト	対応するSFP関連セキュリティ属性
電子錠	なし

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1	TSFは、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限するために[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。 [割付: セキュリティ属性のリスト] 「表10 セキュリティ属性に対する操作一覧」の「セキュリティ属性」参照 [選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]] 「表10 セキュリティ属性に対する操作一覧」の「操作」参照 [割付: 許可された識別された役割] 「表10 セキュリティ属性に対する操作一覧」の「役割」参照 [割付: アクセス制御SFP、情報フロー制御SFP] 設定情報管理制御SFP

依存性: [FDP_ACC.1 サブセットアクセス制御またはFDP_IFC.1 サブセット情報フロー制御]

依存性: FMT_SMF.1 管理機能の特定

依存性: FMT_SMR.1 セキュリティ役割

表 10 セキュリティ属性に対する操作一覧

セキュリティ属性	操作	役割
ユーザ識別子[Appli]	問い合わせ	運用者
JOB ID	なし	なし
運用者権限	問い合わせ、改変	運用者

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] ・ 運用者 ・ 担当者 ・ 承認者
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

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11 セキュリティ管理機能リスト」参照

依存性: なし

表 11 セキュリティ管理機能リスト

機能要件	管理要件	セキュリティ管理機能
FAU_ARP.1	a)アクションの管理(追加、除去、改変)	a)アクションは変更できないので管理機能はない
FAU_SAA.1	a)規則のセットから規則を(追加、改変、削除)することによる規則の維持	a)規則のセットは変更できないので管理機能はない
FAU_GET.1	なし	ー
FIA_UAU.2[Panel]	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	パスワード[Panel]の追加、改変、及び削除機能
FIA_UID.2[Panel]	a)利用者識別情報の管理	a)ユーザ識別子[Panel]の問い合わせ、追加、及び削除機能
FIA_UAU.7[Panel]	なし	ー
FIA_AFL.1[Panel]	a)不成功の認証試行に対する閾値の管理 b)認証失敗の事象においてとられるアクションの管理	a)閾値は固定値であるので管理機能はない b)アクションは変更できないので管理機能はない
FIA_SOS.1[Panel]	a)秘密の検証に使用される尺度の管理	a)尺度は固定値であるので管理機能はない
FIA_UAU.2[Appli]	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	パスワード[Appli]の追加、改変、及び削除機能
FIA_UID.2[Appli]	a)利用者識別情報の管理	a)ユーザ識別子[Appli]の問い合わせ、追加、及び削除機能
FIA_AFL.1[Appli]	a)不成功の認証試行に対する閾値の管理 b)認証失敗の事象においてとられるアクションの管理	a)閾値は固定値であるので管理機能はない b)アクションは変更できないので管理機能はない
FIA_SOS.1[Appli]	a)秘密の検証に使用される尺度の管理	a)尺度は固定値であるので管理機能はない
FDP_ETC.1	なし	ー
FDP_ACC.1[Disk_eject]	なし	ー
FDP_ACF.1[Disk_eject]	a)明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	a)ユーザ識別子[Appli]の問い合わせ、追加、及び削除機能
FMT_MSA.3	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	a)初期値を特定できる役割のグループは変更できないので管理機能はない b)デフォルト値は変更できないので管理機能

	オルト値の許可的あるいは制限的設定を管理すること	はない
FDP_ACC.1[Cover_open]	なし	ー
FDP_ACF.1[Cover_open]	a)明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	a)運用者権限の問い合わせ、及び改変機能
FMT_MSA.1	a)セキュリティ属性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	a)セキュリティ属性と相互に影響を及ぼし得る役割のグループは変更できないので管理機能はない
FMT_SMR.1	a)役割の一部をなす利用者のグループの管理	a)役割の一部をなす利用者のグループは変更できないので管理機能はない
FMT_SMF.1	なし	ー
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。	a)デフォルトのセキュリティ属性は定義できないので管理機能はない b)セキュリティ属性の問い合わせ、及び改変機能
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	a)セキュリティ属性を追加することはないので管理機能はない
FMT_MTD.1	a)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	a)TSFデータと相互に影響を及ぼし得る役割のグループは変更できないので管理機能はない
FMT_MOF.1	a)TSFの機能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	a)TSFの機能と相互に影響を及ぼし得る役割のグループは変更できないので管理機能はない
FPT_RVM.1	なし	ー
FPT_SEP.1	なし	ー

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] ・ 運用者権限 ・ ユーザ識別子[Appli]
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]

	操作パネルからサーバ制御ソフトへのアクセス権限を確認する識別認証により、利用者を代行して動作するサブジェクトとユーザ識別子[Appli]を関連付ける。更に、利用者が運用者である場合、利用者を代行して動作するサブジェクトと運用者権限を関連付ける。
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

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] ・ 運用者権限 ・ ユーザ識別子[Appli]

依存性: なし

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] 「表12 TSFデータに対する操作一覧」の「TSFデータ」 参照 [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]] 「表12 TSFデータに対する操作一覧」の「操作」 参照 [割付: 許可された識別された役割] 「表12 TSFデータに対する操作一覧」の「役割」 参照

依存性: FMT_SMF.1 管理機能の特定

依存性: FMT_SMR.1 セキュリティの役割

表 12 TSF データに対する操作一覧

TSF データ	操作	役割
利用者情報	削除 その他の操作:追加	運用者

	ユーザ識別子[Appli] ユーザ識別子[Panel]	問い合わせ	
	パスワード[Appli] パスワード[Panel]	改変	
	権限	問い合わせ、改変	
	アカウントロックステータス	問い合わせ、改変	
設定情報	セキュリティモードステータス	問い合わせ、改変	
	時刻設定情報	問い合わせ、改変	
	ネットワーク設定情報	問い合わせ、改変	
JOB 情報	JOB 情報	問い合わせ、改変、削除	
利用者情報	本人のパスワード[Appli] 本人のパスワード[Panel]	改変	担当者
利用者情報	本人のパスワード[Appli] 本人のパスワード[Panel]	改変	承認者
JOB 情報	JOB 情報	改変	
JOB 情報	JOB 情報	問い合わせ、改変 その他の操作:追加	運用者 担当者
ディスク位置情報	ディスク位置情報	問い合わせ、改変、削除 その他の操作:追加	承認者

FMT_MOF.1 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: 機能のリスト][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: 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: 機能のリスト] ・ セキュリティモード [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] ・ を停止する ・ を動作させる [割付: 許可された識別された役割] 運用者

依存性: FMT_SMF.1 管理機能の特定

依存性: FMT_SMR.1 セキュリティ役割

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と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を「表 13 TOE セキュリティ保証要件」に示す。

表 13 TOE セキュリティ保証要件

クラス	コンポーネント名(ファミリ含む)
構成管理	ACM_CAP.3 許可の管理
	ACM_SCP.1 TOE の CM 範囲
配付と運用	ADO_DEL.1 配付手続き
	ADO_IGS.1 設置、生成、及び立ち上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_HLD.2 セキュリティ実施上位レベル設計
	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
ライフサイクルサポート	ALC_DVS.1 セキュリティ手段の識別
テスト	ATE_COV.2 ガバレージの分析
	ATE_DPT.1 テスト: 上位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テストーサンプル
脆弱性評定	AVA_MSU.1 ガイダンスの検査
	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とその機能強度を「表 14 TOE セキュリティ機能要件と機能強度」に示す。

表 14 TOE セキュリティ機能要件と機能強度

TOE セキュリティ機能要件	強度主張
FIA_UAU.2[Panel]	SOF-基本
FIA_AFL.1[Panel]	SOF-基本
FIA_SOS.1[Panel]	SOF-基本
FIA_UAU.2[Appli]	SOF-基本
FIA_AFL.1[Appli]	SOF-基本
FIA_SOS.1[Appli]	SOF-基本

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。

FIA_UAU.7[Appli] 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] 入力された文字数と同数のダミー文字(″*″等)の表示 [詳細化] (※下線部に関して詳細化を行っている) TSF: ブラウザ、Total Disc Maker、及びTotal Disc Monitor

依存性: FIA_UAU.1 認証のタイミング

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記述する。

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記述する。

6.1.1 TOE セキュリティ機能

TOE が提供するセキュリティ機能を「表 15 セキュリティ機能とセキュリティ要件」に示す。

表 15 セキュリティ機能とセキュリティ要件

	SF.取り出し制御機能	SF.電子錠開制御機能	SF.識別認証 [Panel] 機能	SF.識別認証 [Web_app] 機能	SF.識別認証 [Cli_app] 機能	SF.警告機能	SF.設定情報管理機能
FAU_ARP.1						○	
FAU_SAA.1						○	
FAU_GET.1						○	
FIA_UAU.2[Panel]			○				
FIA_UID.2[Panel]			○				
FIA_UAU.7[Panel]			○				
FIA_AFL.1[Panel]			○				
FIA_SOS.1[Panel]							○
FIA_UAU.2[Appli]				○	○		
FIA_UID.2[Appli]				○	○		
FIA_AFL.1[Appli]				○	○		
FIA_SOS.1[Appli]							○
FDP_ETC.1	○						
FDP_ACC.1[Disk_eject]	○						
FDP_ACF.1[Disk_eject]	○						
FMT_MSA.3	○						
FDP_ACC.1[Cover_open]		○					
FDP_ACF.1[Cover_open]		○					
FMT_MSA.1							○
FMT_SMR.1							○
FMT_SMF.1							○

FIA_USB.1							○
FIA_ATD.1							○
FMT_MTD.1	○						○
FMT_MOF.1							○
FPT_RVM.1	○	○	○	○	○		○
FPT_SEP.1	○	○	○	○	○	○	○

SF.取り出し制御機能

SF.取り出し制御機能は、ディスクを作成した利用者が自身の作成済みディスクを取り出す機能である。

- 利用者は、PP-100N の操作パネルにあるディスク取り出しボタンを押す。
- TOE は、識別認証のため SF.識別認証[Panel]機能を実行する。
- SF.識別認証[Panel]機能により利用者登録されていないと判断された場合、TOE は、処理を終了する。
- SF.識別認証[Panel]機能により利用者登録されていると判断された場合、TOE は、JOB 情報を参照する。取り出し制御 SFP のオブジェクトである JOB 情報には、TOE が一意なユーザ識別子[Appli]と JOB ID を関連付けており、その関連付けは変更されない。【FDP_ACC.1[Disk_eject]、FDP_ACF.1[Disk_eject]、FMT_MTD.1、FMT_MSA.3】
- JOB 情報より利用者本人の作成済みディスクが存在すると TOE が判断した場合、TOE は、ディスク位置情報を参照する。取り出し制御 SFP のオブジェクトであるディスク位置情報には、TOE が一意な JOB ID を関連付けており、その関連付けは変更されない。【FDP_ACC.1[Disk_eject]、FDP_ACF.1[Disk_eject]、FMT_MTD.1、FMT_MSA.3】
- JOB 情報より利用者本人の作成済みディスクが存在しないと TOE が判断した場合、TOE は、処理を終了する。
- TOE は、作成済みディスクのディスク位置情報よりオートローダを制御し、作成済みディスクをスタッカ 4 に搬送する。【FDP_ETC.1】
- スタッカ 4 へのディスク搬送が完了すると、TOE は、ディスク位置情報の変更、削除を実施する。【FMT_MTD.1】
- TOE は、ディスクを作成した利用者が自身の作成済みディスクを取り出す際、SF.取り出し制御機能を呼び出すことにより、アクセス制御が実施され、成功することを保証する。【FPT_RVM.1】
- SF.取り出し制御機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.電子錠開制御機能

SF.電子錠開制御機能は、運用者がディスクカバーを開ける際、電子錠を制御する機能である。

- 運用者は、PP-100N の操作パネルに表示される操作メニューより電子錠を解錠するメニュー項目を選択する。
- TOE は、識別認証のため SF.識別認証[Panel]機能を実行する。
- SF.識別認証[Panel]機能により運用者ではないと判断された場合、TOE は、処理を終了する。
- SF.識別認証[Panel]機能により運用者であると判断された場合、TOE は、電子錠を解錠する。【FDP_ACC.1[Cover_open]、FDP_ACF.1[Cover_open]】
- TOE は、電子錠の解錠後、ディスクカバーが 5 秒以上、開かれないと電子錠を施錠する。
- TOE は、運用者がディスクカバーを開けるための一連の操作を行う際、SF.電子錠開制御機能を呼び出すことにより、アクセス制御が実施され、成功することを保証する。【FPT_RVM.1】
- SF.電子錠開制御機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.識別認証[Panel]機能

SF.識別認証[Panel]機能は、PP-100N の操作パネルより TOE にアクセスする際、登録された正しい利用者であること

を確認する機能である。

- SF.識別認証[Panel]機能は、操作パネルからの操作に対し、識別認証が必要な際に呼び出される。
- TOE は、識別認証が実行されるまで他の操作を受け付けない。【FIA_UAU.2[Panel]、FIA_UID.2[Panel]】
- 利用者はユーザ識別子[Panel]とパスワード[Panel]を入力する。
- TOE は、パスワード入力中、入力された文字と同数の"*"を LCD に表示させる。【FIA_UAU.7[Panel]】
- TOE は、ユーザ識別子[Panel]とパスワード[Panel]を利用者情報と比較し、一致した利用者情報が存在するならば、正しい利用者であると判断する。一致した利用者情報が存在しないならば、再度、ユーザ識別子[Panel]とパスワード[Panel]の入力を促す。
- TOE は、識別認証に一定時間内において 3 回連続で失敗した場合、運用者は 6 時間、その他 1 時間、操作パネルからのログインに対し、アカウントロックを実行する。【FIA_AFL.1[Panel]】
- TOE は、TSC 内の各機能の動作が許可される前に、SF.識別認証[Panel]機能を呼び出すことにより、識別認証が実施され、成功することを保証する。【FPT_RVM.1】
- SF.識別認証[Panel]機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.識別認証[Web_app]機能

SF.識別認証[Web_app]機能は、PP-100NWeb アプリより TOE にアクセスする際、登録された正しい利用者であることを確認する機能である。

- PP-100NWeb アプリが起動すると識別認証画面が表示される。
- TOE は、識別認証が実行されるまで他の操作を受け付けない。【FIA_UAU.2[Appli]、FIA_UID.2[Appli]】
- 利用者は、ユーザ識別子[Appli]とパスワード[Appli]を入力する。
- TOE は、ユーザ識別子[Appli]とパスワード[Appli]を利用者情報と比較し、一致した利用者情報が存在するならば、正しい利用者であると判断する。一致した利用者情報が存在しないならば、再度、ユーザ識別子[Appli]とパスワード[Appli]の入力を促す。
- TOE は、一定時間内において識別認証に 3 回連続で失敗した場合、運用者は 6 時間、その他 1 時間、PP-100N Web アプリからのログインに対し、アカウントロック実行する。【FIA_AFL.1[Appli]】
- TOE は、TSC 内の各機能の動作が許可される前に、SF.識別認証[Web_app]機能を呼び出すことにより、識別認証が実施され、成功することを保証する。【FPT_RVM.1】
- SF.識別認証[Web_app]機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.識別認証[Cli_app]機能

SF.識別認証[Cli_app]機能は、Total Disc Maker や Total Disc Monitor より TOE にアクセスする際、登録された正しい利用者であることを確認する機能である。

- Total Disc Maker や Total Disc Monitor より TOE にアクセスする際、識別認証画面が表示される。
- TOE は、識別認証が実行されるまで他の操作を受け付けない。【FIA_UAU.2[Appli]、FIA_UID.2[Appli]】
- 利用者は、ユーザ識別子[Appli]とパスワード[Appli]を入力する。
- TOE は、ユーザ識別子[Appli]とパスワード[Appli]を利用者情報と比較し、一致した利用者情報が存在するならば、正しい利用者であると判断する。一致した利用者情報が存在しないならば、再度、ユーザ識別子[Appli]とパスワード[Appli]の入力を促す。
- TOE は、一定時間内において識別認証に 3 回連続で失敗した場合、運用者は 6 時間、その他 1 時間、Total Disc Maker や Total Disc Monitor からのログインに対し、アカウントロック実行する。【FIA_AFL.1[Appli]】

- TOE は、TSC 内の各機能の動作が許可される前に、SF.識別認証[Cli_app]機能を呼び出すことにより、識別認証が実施され、成功することを保証する。【FPT_RVM.1】
- SF.識別認証[Cli_app]機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.警告機能

SF.警告機能は、セキュリティ侵害の可能性が発生した場合、運用者に警告を発する機能である。

- TOE は、以下の(1)～(6)の状態が発生し、セキュリティ侵害の可能性があると判断した場合、次の警告を行う。【FAU_ARP.1】
  - ブザーを鳴らす
  - ERROR LED を点灯する
  - LCD に対処方法を表示する

(1) 電源オフ処理時

電源オフ処理時、PP-100N 内に作成済みディスクがあることを警告する。

- TOE は、JOB 情報から「作成済みディスクの有無」と「処理中 JOB の有無」を確認する。【FAU_GET.1】
- TOE は、「作成済みディスクが存在しない」、かつ「処理中 JOB が存在しない」場合、電源オフ処理を継続する。
- TOE は、「作成済みディスクが存在する」、もしくは「処理中 JOB が存在する」場合、セキュリティ侵害の可能性があると判断する。【FAU_SAA.1】

(2) ディスクカバーオープン時

ディスクカバーが開き続けていることを警告する。

- ディスクカバーを開けた際、TOE は、ディスクカバー検出器より、ディスクカバーが開いたことを検知する。【FAU_GET.1】
- ディスクカバーが 60 秒以上開いていた場合、TOE は、セキュリティ侵害の可能性があると判断する。【FAU_SAA.1】

(3) ディスクカバークローズ時

「物理鍵によりディスクカバー錠が解錠のままである」、もしくは「セキュリティロック切替レバーがオフである」ことを警告する。

- ディスクカバーが閉められた際、TOE は、ディスクカバー検出器、鍵位置検出器より、ディスクカバーが閉められたのにも関わらず「物理鍵によりディスクカバー錠が解錠のままである」、もしくは「セキュリティロック切替レバーがオフである」ことを検知する。【FAU_GET.1】
- TOE は上記状態が 10 秒以上継続した場合、セキュリティ侵害の可能性があると判断する。【FAU_SAA.1】

(4) ディスク搬送時

ディスク搬送時、オートローダがディスクを取り落したことを警告する。

- TOE は、ディスク検出器より、オートローダがディスクを取り落としたことを検知する。【FAU_GET.1】
- TOE は、オートローダがディスクを取り落とした場合、セキュリティ侵害の可能性があると判断する。【FAU_SAA.1】

(5) スタッカ 2 取り外し時

電源オン期間中、スタッカ 2 が取り外され戻されたとき、スタッカ 2 内にディスクがあることを警告する。

- TOE は、ディスクカバー検出器、スタッカ 2 検出器より、ディスクカバーが開いている間に、スタッカ 2 が着脱されたことを検知する。【FAU_GET.1】
- TOE は、ディスクカバー検出器、ディスク検出器より、ディスクカバーが閉じられた後、スタッカ 2 内にディスクが存在することを検知する。【FAU_GET.1】
- TOE は、スタッカ 2 が取り外され戻されたとき、スタッカ 2 内にディスクが存在する場合、セキュリティ侵害の可能性

があると判断する。【FAU_SAA.1】

(1)～(5) 共通

・ SF.警告機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

SF.設定情報管理機能

SF.設定情報管理機能は、「クライアント PC からの設定管理情報、JOB 情報、ディスク位置情報へのアクセス」、「操作パネルからの設定管理情報へのアクセス」を権限のある利用者のみに制限する機能である。

(1) アクセス管理

・ TOE は、以下のセキュリティ属性を定義し、維持する。【FIA_ATD.1】
  ・ ユーザ識別子[Appli]
  ・ 運用者権限
・ TOE は、SF.識別認証[Panel]機能により識別認証された利用者を代行して動作するサブジェクトとユーザ識別子[Appli]を関連付ける。更に、利用者が運用者である場合、利用者を代行して動作するサブジェクトと運用者権限を関連付ける。【FIA_USB.1】
・ TOE は、SF.識別認証[Panel]機能、SF.識別認証[Web_app]機能、もしくは SF.識別認証[Cli_app]機能により識別認証された利用者を以下の役割に関連付け、それを維持する。【FMT_SMR.1】
  ・ 運用者
  ・ 承認者
  ・ 担当者
・ TOE は、セキュリティ機能の設定を運用者のみに許可する。【FMT_MOF.1】
・ 「表 16 役割ごとの利用可能機能一覧」の通り、TOE は、識別認証された利用者の役割に対して、利用可能な操作のみを提供する。【FMT_MSA.1、FMT_MTD.1、FMT_SMF.1】

表 16 役割ごとの利用可能機能一覧

役割	TSF データ		操作
運用者	利用者情報		削除 その他の操作:追加
		ユーザ識別子[Appli] ユーザ識別子[Panel]	問い合わせ
		パスワード[Appli] パスワード[Panel]	改変
		権限	問い合わせ、改変
		アカウントロックステータス	問い合わせ、改変
	設定情報	セキュリティモードステータス	問い合わせ、改変
		時刻設定情報	問い合わせ、改変
		ネットワーク設定情報	問い合わせ、改変
	JOB 情報	JOB 情報	問い合わせ、改変、削除
担当者	利用者情報	本人のパスワード[Appli] 本人のパスワード[Panel]	改変

承認者	利用者情報	本人のパスワード[Appli] 本人のパスワード[Panel]	改変
	JOB 情報	JOB 情報	改変
利用者	JOB 情報	JOB 情報	問い合わせ、改変 その他の操作:追加
	ディスク位置情報	ディスク位置情報	その他の操作:追加

(2) パスワード変更機能

- TOE は、パスワード変更時、入力された文字を別の文字に置き換えて表示をする。置き換える文字は IT 環境である OS の設定に従う。
- TOE は、パスワード変更時、次の規則に従っていることを確認する。【FIA_SOS.1[Panel]、FIA_SOS.1[Appli]】
  - パスワード[Panel]:数字 5 桁以上
  - パスワード[Appli]:英数字又は特殊文字(「.」「-」「_」)5 桁以上

(3) その他

- TOE は、設定管理情報、JOB 情報、ディスク位置情報にアクセスする際、SF.設定情報管理機能を呼び出すことにより、アクセス制御が実施され、成功することを保証する。【FPT_RVM.1】
- SF.設定情報管理機能に関する TSF は、自身を保護し、干渉・改ざんから保護される。【FPT_SEP.1】

6.1.2 TOE セキュリティ機能強度

TOE セキュリティ機能のうち、非暗号で且つ確率的或いは順列的メカニズムに基づくものと、そのセキュリティ強度主張の対応を「表 17 TOE セキュリティ機能と機能強度主張」に示す。

表 17 TOE セキュリティ機能と機能強度主張

TOE セキュリティ機能	強度主張
SF.識別認証[Panel]機能	SOF-基本
SF.識別認証[Web_app]機能	SOF-基本
SF.識別認証[Cli_app]機能	SOF-基本
SF.設定情報管理機能	SOF-基本

6.2 保証手段

保証手段として提供される文書は「表 18 保証手段として提供される文書」の通りである。

表 18 保証手段として提供される文書

保証要件クラス	保証要件コンポーネント	ドキュメント名称及び TOE
ACM（構成管理）	ACM_CAP.3	・KP-01 PP-100N 構成管理計画書（製品全体） ・KP-02 PP-100N 構成管理計画書（メカ部） ・KP-03 PP-100N 構成管理計画書（オートローダ基板） ・KP-04 PP-100N 構成管理計画書（サーバシステムソフト） ・KP-05 PP-100N 構成管理計画書（オートローダファームウェア） ・KL-01 PP-100N 構成リスト（製品全体） ・KL-02 PP-100N 構成リスト（メカ部） ・KL-03 PP-100N 構成リスト（オートローダ基板） ・KL-04 PP-100N 構成リスト（サーバシステムソフト） ・KL-05 PP-100N 構成リスト（オートローダファームウェア）
	ACM_SCP.1	・KL-01 PP-100N 構成リスト（製品全体） ・KL-02 PP-100N 構成リスト（メカ部） ・KL-03 PP-100N 構成リスト（オートローダ基板） ・KL-04 PP-100N 構成リスト（サーバシステムソフト） ・KL-05 PP-100N 構成リスト（オートローダファームウェア）
ADO（配付と運用）	ADO_DEL.1	・PP-100N 配付手順書 ・PP-100N Web 配付手順書
	ADO_IGS.1	・PP-100N 運用者ガイド【認証発行オプション編】 ・PP-100N Security Administrator's Guide ・PP-100N ソフトウェアインストール手順書 ・Install Manual for PP-100N ・Sheet, Security, PP100N

ADV（開発）	ADV_FSP.1	・セイコーエプソン PP-100N セキュリティ制御機構 機能仕様書 ・セイコーエプソン PP-100N セキュリティ制御機構 TOE 機能構成図
	ADV_HLD.2	・セイコーエプソン PP-100N セキュリティ制御機構 上位レベル設計書 ・セイコーエプソン PP-100N セキュリティ制御機構 TOE サブシステム構成図
	ADV_RCR.1	・セイコーエプソン PP-100N セキュリティ制御機構 表現対応分析書
AGD（ガイダンス文書）	AGD_ADM.1	・PP-100N 運用者ガイド【認証発行オプション編】 ・PP-100N Security Administrator's Guide ・Sheet, Security, PP100N
	AGD_USR.1	・PP-100N ユーザーズガイド【認証発行オプション編】 ・PP-100N Security User's Guide
ALC（ライフサイクルサポート）	ALC_DVS.1	・PP-100N セキュリティ制御機構 開発セキュリティ業務処理基準
ATE（テスト）	ATE_COV.2	・PP-100N セキュリティ制御機構 機能テスト仕様書 ・PP-100N セキュリティ制御機構 上位レベルテスト仕様書
	ATE_DPT.1	
	ATE_FUN.1	
	ATE_IND.2	
AVA（脆弱性分析）	AVA_MSU.1	・PP-100N セキュリティ制御機構 誤使用に関する分析書
	AVA_SOF.1	・PP-100N セキュリティ制御機構 機能強度分析書
	AVA_VLA.1	・PP-100N セキュリティ制御機構 脆弱性分析書

7 PP 主張

PP への適合は主張しない。

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、及び PP 主張の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記述する。

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 19 TOE セキュリティ環境との対応」に示す。

表 19 TOE セキュリティ環境との対応

	A.承認者	A.運用者	A.パスワード	A.運用状態管理	A.セキュリティモード	A.ネットワーク	T.ディスク持ち出し	T.ディスクカバー未施錠	T.ディスク取り落とし	T.ディスク置き間違え	P.作成済みディスク
O.識別認証							○				
O.取り出し制御							○				
O.カバー開制御							○				
O.登録管理							○				
O.警告								○	○	○	○
OE.承認者の信頼	○										
OE.運用者の信頼		○									
OE.パスワード管理			○								
OE.運用者による対応								○	○	○	○
OE.運用者監視				○							
OE.セキュリティモード設定					○						
OE.ネットワーク						○					
OI.パスワード秘匿							○				

「表 19 TOE セキュリティ環境との対応」の通り、全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、全てのセキュリティ対策方針の必要性は満たされている。

8.1.2 セキュリティ対策方針の十分性

A.承認者

OE.承認者の信頼により、組織の責任者が信頼できる人物を承認者に任命する。以上より、A.承認者は実現できる。

A.運用者

OE.運用者の信頼により、組織の責任者が信頼できる複数の人物を運用者に任命し、必要な知識の教育を実施する。以上より、A.運用者は実現できる。

A.パスワード

OE.パスワード管理により、利用者が自身のパスワードを本人以外に知られないよう管理することと、TOE のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワード変更を行う。以上より、A.パスワードは実現できる。

A.運用状態管理

OE.運用者監視により、運用者は以下に示すことが行われないよう PP-100N の運用状態を監視する。

- PP-100N の破壊
- 運用者以外の者によるディスクカバー解錠

以上より、A.運用状態管理は実現できる。

A.セキュリティモード

OE.セキュリティモード設定により、運用者は認証発行オプションを購入後、PP-100Nに認証用テンキーを接続し、PP-100N をセキュリティモードに設定する。以上より、A.セキュリティモードは実現できる。

A.ネットワーク

OE.ネットワークにより、運用者は、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データを盗聴から保護する。以上より、A.ネットワークは実現できる。

T.ディスク持ち出し

PP-100N を運用する場合において、利用者情報（ユーザ識別子、パスワードなど）を登録、管理し、利用者を識別認証する必要がある。O.登録管理により、運用者は PP-100N を利用する者の情報を管理することができ、利用者本人のみが自身のパスワード[Panel]、パスワード[Appli]を変更することができる。従って、利用者が利用者本人であることを識別認証することができる。また、識別認証の際のパスワード入力において、O.識別認証により、パスワード[Panel]は秘匿され、OI.パスワード秘匿により、パスワード[Appli]は秘匿される。ディスクを作成した利用者が自身のディスクを取り出す場合、O.識別認証により、ディスクを作成した利用者本人であることを識別認証することができ、O.取り出し制御により、ディスクを作成した利用者本人のディスクを取り出すことができる。運用者がディスクカバーを開ける場合、O.識別認証により、運用者本人であることを識別認証することができ、O.カバー開制御により、運用者のみがディスクカバーを開けることができる。よって、ディスクを作成した利用者以外がディスクを作成した利用者、もしくは運用者になりすますことはできなくなり、T.ディスク持ち出しの脅威を防止することができる。

T.ディスクカバー未施錠

O.警告により、ディスクカバーが未施錠となった場合、運用者に警告することができる。OE.運用者による対応により、運用者は速やかにディスクカバーを施錠することができる。よって、ディスクカバーが未施錠となることはなくなり、T.ディスクカバー未施錠の脅威を防止することができる。

T.ディスク取り落とし

O.警告により、オートローダがディスクを取り落とした場合、運用者に警告することができる。OE.運用者による対応により、運用者は速やかにディスクを取り除くことができる。よって、オートローダがディスクを取り落とした場合、そのディスクに関して、ディスクを作成した担当者以外の者による持ち出しがなくなり、T.ディスク取り落としの脅威を防止することができる。

T.ディスク置き間違え

「電源オン期間中、スタッカ 2 が取り外され戻されたとき、スタッカ 2 内にディスクがある」場合を、運用者、もしくはサービスマンがスタッカ 2 へディスクを置き間違えたと判断し、O.警告により、運用者に警告することができる。OE.運用者による対応により、運用者は速やかにスタッカ 2 内にあるディスクを取り除くことができる。よって、ディスクの置き間違えによる誤排出がなくなり、T.ディスク置き間違えの脅威を防止することができる。

P.作成済みディスク

電源オフ処理時、作成済みディスクがある場合、O.警告により、運用者に警告することができる。OE.運用者による対応により、運用者は速やかに作成済みディスクを取り除くことができる。以上より、P.作成済みディスクは実現できる。

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記述する。

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「表 20 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」に示す。

表 20 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

	O.識別認証	O.取り出し制御	O.カバー開制御	O.登録管理	O.警告
FAU_ARP.1					○
FAU_SAA.1					○
FAU_GET.1					○
FIA_UAU.2[Panel]	○				
FIA_UID.2[Panel]	○				
FIA_UAU.7[Panel]	○				
FIA_AFL.1[Panel]	○				
FIA_SOS.1[Panel]				○	
FIA_UAU.2[Appli]	○				
FIA_UID.2[Appli]	○				

FIA_AFL.1[Appli]	○				
FIA_SOS.1[Appli]				○	
FDP_ETC.1		○			
FDP_ACC.1[Disk_eject]		○			
FDP_ACF.1[Disk_eject]		○			
FMT_MSA.3		○			
FDP_ACC.1[Cover_open]			○		
FDP_ACF.1[Cover_open]			○		
FMT_MSA.1				○	
FMT_SMR.1				○	
FMT_SMF.1				○	
FIA_USB.1				○	
FIA_ATD.1				○	
FMT_MTD.1		○		○	
FMT_MOF.1				○	
FPT_RVM.1	○	○	○	○	
FPT_SEP.1	○	○	○	○	○

「表 20 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」の通り、全ての 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、全ての TOE セキュリティ機能要件の必要性は満たされている。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「表 21 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」に示す

表 21 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

	OI.パスワード秘匿
FIA_UAU.7[Appli]	○

「表 21 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」の通り、全ての 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、全ての 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.識別認証

O.識別認証は、FIA_UAU.2[Panel]、 FIA_UID.2[Panel]、FIA_UAU.7[Panel]、FIA_AFL.1[Panel]、FIA_UAU.2[Appli]、 FIA_UID.2[Appli]、FIA_AFL.1[Appli]、FPT_RVM.1、FPT_SEP.1 により実現できる。

<操作パネルからのログイン>

- FIA_UID.2[Panel]、FIA_UAU.2[Panel]により、TSF は、識別認証する。識別認証するまでは他の TOE 操作は受け付けない。
- FIA_UAU.7[Panel]により、TSF は、入力された文字数と同じ"*"を表示させることでパスワードを秘匿する。

- FIA_AFL.1[Panel]により、TSF は、一定時間内において 3 回連続で識別認証に失敗した場合、運用者は 6 時間、その他 1 時間、操作パネルからのログインに対し、アカウントロックを実行する。

〈PP-100NWeb アプリからのログイン〉

- FIA_UID.2[Appli]、FIA_UAU.2[Appli]により、TSF は、識別認証する。識別認証するまでは他の TOE 操作は受け付けない。
- FIA_AFL.1[Appli]により、TSF は、一定時間内において 3 回連続で識別認証に失敗した場合、運用者は 6 時間、その他 1 時間、PP-100NWeb アプリからのログインに対し、アカウントロックを実行する。

〈Total Disc Maker、もしくは Total Disc Monitor からのログイン〉

- FIA_UID.2[Appli]、FIA_UAU.2[Appli]により、TSF は、識別認証する。識別認証するまでは他の TOE 操作は受け付けない。
- FIA_AFL.1[Appli]により、TSF は、一定時間内において 3 回連続で識別認証に失敗した場合、運用者は 6 時間、その他 1 時間、Total Disc Maker や Total Disc Monitor からのログインに対し、アカウントロックを実行する。

〈共通〉

- FPT_RVM.1 により、TSF は、アクセス制御を動作させる前に、必ず呼び出される構造にする。
- FPT_SEP.1 により、TSF は、各機能要件を不正な干渉から保護するために TSF とサブジェクトのドメインを分離･維持する。

O.取り出し制御

O.取り出し制御は、FDP_ETC.1、FDP_ACC.1[Disk_eject]、FDP_ACF.1[Disk_eject]、FMT_MSA.3、FMT_MTD.1、FPT_RVM.1、FPT_SEP.1 により実現できる。

- FDP_ETC.1 により、TSF は、作成済みディスクを取り出す。
- FDP_ACC.1[Disk_eject]により、TSF は、ディスクを作成した利用者本人の作成済みディスクを取り出す際のアクセス制御を実施する。
- FDP_ACF.1[Disk_eject]により、TSF は、ユーザ識別子[Appli]に基づくアクセス制御を実施する。
- FMT_MSA.3 により、TSF は、デフォルト値として、一意な識別子（ユーザ識別子[Appli]）を設定する。
- FMT_MTD.1 により、TSF データであるディスク位置情報に対して、TSF は、ディスクを作成した利用者が指定した操作（変更、削除）のみを実施できるよう管理する。
- FPT_RVM.1 により、TSF は、取り出し制御を動作させる際、必ず呼び出される構造にする。
- FPT_SEP.1 により、TSF は、各機能要件を不正な干渉から保護するために TSF とサブジェクトのドメインを分離･維持する。

O.カバー開制御

O.カバー開制御は、FDP_ACC.1[Cover_open]、FDP_ACF.1[Cover_open]、FPT_RVM.1、FPT_SEP.1 により実現できる。

- FDP_ACC.1[Cover_open]により、TSF は、ディスクカバーを開ける際のアクセス制御を実施する。
- FDP_ACF.1[Cover_open]により、TSF は、運用者権限に基づくアクセス制御を実施する。
- FPT_RVM.1 により、TSF は、カバー開制御を動作させる際、必ず呼び出される構造にする。
- FPT_SEP.1 により、TSF は、各機能要件を不正な干渉から保護するために TSF とサブジェクトのドメインを分離･維持する。

O.登録管理

O.登録管理は、FIA_SOS.1[Panel]、FIA_SOS.1[Appli]、FMT_MSA.1、FMT_SMR.1、FMT_SMF.1、FIA_USB.1、FIA_ATD.1、FMT_MTD.1、FMT_MOF.1、FPT_RVM.1、FPT_SEP.1 により実現できる。

- FIA_SOS.1[Panel]により、TSF は、設定したパスワード[Panel]が一定品質以上であることを検証する。
- FIA_SOS.1[Appli]により、TSF は、設定したパスワード[Appli]が一定品質以上であることを検証する。
- FMT_MSA.1 により、TSF は、利用者のセキュリティ属性を管理する。
- FMT_SMR.1 により、TSF は、利用者の役割について定義し、維持する。
- FMT_SMF.1 により、TSF は、各機能要件の管理要件に対する管理機能を特定する。
- FIA_USB.1 により、TSF は、利用者と利用者を代行して動作するサブジェクトとを関係付ける。
- FIA_ATD.1 により、TSF は、利用者のセキュリティ属性について定義し、維持する。
- FMT_MTD.1 により、TSF データに対して、TSF は、指定された役割が指定された操作のみ実施するよう管理する。
- FMT_MOF.1 により、TSF は、セキュリティ機能の設定を運用者のみに許可する。
- FPT_RVM.1 により、TSF は、登録管理を動作させる際、必ず呼び出される構造にする。
- FPT_SEP.1 により、TSF は、各機能要件を不正な干渉から保護するために TSF とサブジェクトのドメインを分離･維持する。

O.警告

セキュリティ侵害の発生した可能性が高いと判断する事象を以下に示す。

- 電源オフ処理時、PP-100N 内に作成済みディスクがある
- ディスクカバーが未施錠となる
- オートローダがディスクを取り落とす
- 電源オン期間中、スタッカ 2 が取り外され戻されたとき、スタッカ 2 内にディスクがある

O.警告は、FAU_GET.1、FAU_SAA.1、FAU_ARP.1、FPT_SEP.1 により実現できる。

- FAU_GET.1 により、TSF は、上記セキュリティ侵害の可能性を検出するためのイベント情報を取得する。
- FAU_SAA.1 により、TSF は、取得したイベント情報よりセキュリティ侵害の可能性を検出するための分析を行う。
- FAU_ARP.1 により、分析の結果、セキュリティ侵害の可能性が検出された場合、TSF は、運用者に警告する。
- FPT_SEP.1 により、TSF は、各機能要件を不正な干渉から保護するために TSF とサブジェクトのドメインを分離･維持する。

OI.パスワード秘匿

OI.パスワード秘匿は、FIA_UAU.7[Appli]により実現できる。

<PP-100NWeb アプリからのログイン>

- FIA_UAU.7[Appli]により、ブラウザは、入力された文字数と同じダミー文字（"*"等）を表示させることでパスワードを秘匿する。

<Total Disc Maker、もしくは Total Disc Monitor からのログイン>

- FIA_UAU.7[Appli]により、Total Disc Maker、もしくは Total Disc Monitor は、入力された文字数と同じダミー文字（"*"等）を表示させることでパスワードを秘匿する。

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「表 22 TOE セキュリティ機能要件の依存性」に示す。これにより、TOE

セキュリティ機能要件の依存性が満たされている範囲を明確にする。更に、満たされていない依存性については、それが正当である根拠を別途示す。

表 22 TOE セキュリティ機能要件の依存性

No	TOE セキュリティ機能要件	下位階層	依存関係	参照 No	備考
1	FAU_ARP.1	—	FAU_SAA.1	2	
2	FAU_SAA.1	—	FAU_GEN.1	不要	下記(※1)参照
3	FAU_GET.1	—	—	—	
4	FIA_UAU.2[Panel]	FIA_UAU.1	FIA_UID.2[Panel]	5	FIA_UID.2 は FIA_UID.1 の上位コンポーネントであるため依存性は満たされている
5	FIA_UID.2[Panel]	FIA_UID.1	—	—	
6	FIA_UAU.7[Panel]	—	FIA_UAU.2[Panel]	4	FIA_UAU.2 は FIA_UAU.1 の上位コンポーネントであるため依存性は満たされている
7	FIA_AFL.1[Panel]	—	FIA_UAU.2[Panel]	4	FIA_UAU.2 は FIA_UAU.1 の上位コンポーネントであるため依存性は満たされている
8	FIA_SOS.1[Panel]	—	—	—	
9	FIA_UAU.2[Appli]	FIA_UAU.1	FIA_UID.2[Appli]	10	FIA_UID.2 は FIA_UID.1 の上位コンポーネントであるため依存性は満たされている
10	FIA_UID.2[Appli]	FIA_UID.1	—	—	
11	FIA_AFL.1[Appli]	—	FIA_UAU.2[Appli]	9	FIA_UAU.2 は FIA_UAU.1 の上位コンポーネントであるため依存性は満たされている
12	FIA_SOS.1[Appli]	—	—	—	
13	FDP_ETC.1	—	FDP_ACC.1[Disk_eject]	14	
14	FDP_ACC.1[Disk_eject]	—	FDP_ACF.1[Disk_eject]	15	
15	FDP_ACF.1[Disk_eject]	—	FDP_ACC.1[Disk_eject]	14	
			FMT_MSA.3	16	
16	FMT_MSA.3	—	FMT_MSA.1	19	
			FMT_SMR.1	20	
17	FDP_ACC.1[Cover_open]	—	FDP_ACF.1[Cover_open]	18	
18	FDP_ACF.1[Cover_open]	—	FDP_ACC.1[Cover_open]	17	
			FMT_MSA.3	不要	下記(※2)参照
19	FMT_MSA.1	—	FDP_ACC.1[Disk_eject] FDP_ACC.1[Cover_open]	14 17	
			FMT_SMF.1	21	

			FMT_SMR.1	20	
20	FMT_SMR.1	—	FIA_UID.2[Panel] FIA_UID.2[Appli]	5 10	FIA_UID.2 は FIA_UID.1 の上位コンポーネントであるため依存性は満たされている
21	FMT_SMF.1	—	—	—	
22	FIA_USB.1	—	FIA_ATD.1	23	
23	FIA_ATD.1	—	—	—	
24	FMT_MTD.1	—	FMT_SMF.1	21	
			FMT_SMR.1	20	
25	FMT_MOF.1	—	FMT_SMF.1	21	
			FMT_SMR.1	20	
26	FPT_RVM.1	—	—	—	
27	FPT_SEP.1	—	—	—	
28	FIA_UAU.7[Appli]	—	FIA_UAU.2[Appli]	4	FIA_UAU.2 は FIA_UAU.1 の上位コンポーネントであるため依存性は満たされている

(※1) FAU_GEN.1 の依存性を必要としない根拠

本 TOE において FAU_GEN.1 は採用しない。本 TOE においてセキュリティ侵害の可能性があると判断した場合、直後に警告を発し、運用者により、そのセキュリティ侵害の可能性を除去する方針としている。そのため FAU_GEN.1 において要求される時刻情報などの監査事象の情報は不要である。従って、FAU_GEN.1 は採用しない。但し、セキュリティ侵害の可能性を分析するために必要なイベント情報を収集する必要がある。そのため、本 TOE では、セキュリティ侵害の可能性を示すイベント情報を取得する FAU_GET.1 を採用する。

(※2) FMT_MSA.3 の依存性を必要としない根拠

本 TOE において FMT_MSA.3 は採用しない。本 TOE では、サブジェクトのセキュリティ属性をもとに制御を行うため、オブジェクトのセキュリティ属性は必要ない。従って、オブジェクトにおけるセキュリティ属性の初期値を定義する必要もない。ゆえに、FMT_MSA.3 は採用しない。

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「表 23 セキュリティ機能要件の相互サポート構造」に示す。この相互サポート構造は、非活性化防止、迂回防止、及び改ざん防止の観点から構成されている。

表 23 セキュリティ機能要件の相互サポート構造

機能要件	防御を提供している機能要件		
	非活性化	迂回	改ざん
FAU_ARP.1	なし	FPT_RVM.1	FPT_SEP.1
FAU_SAA.1	なし	FPT_RVM.1	FPT_SEP.1
FAU_GET.1	なし	FPT_RVM.1	FPT_SEP.1

FIA_UAU.2[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UID.2[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UAU.7[Panel]	なし	FPT_RVM.1	FPT_SEP.1
FIA_AFL.1[Panel]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_SOS.1[Panel]	なし	FPT_RVM.1	FPT_SEP.1
FIA_UAU.2[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_UID.2[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_AFL.1[Appli]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_SOS.1[Appli]	なし	FPT_RVM.1	FPT_SEP.1
FDP_ETC.1	なし	FPT_RVM.1	FPT_SEP.1
FDP_ACC.1[Disk_eject]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FDP_ACF.1[Disk_eject]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MSA.3	なし	FPT_RVM.1	FPT_SEP.1
FDP_ACC.1[Cover_open]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FDP_ACF.1[Cover_open]	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MSA.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_SMR.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_SMF.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_USB.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FIA_ATD.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MTD.1	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1
FMT_MOF.1	—	FPT_RVM.1	FPT_SEP.1
FPT_RVM.1	FMT_MOF.1	—	FPT_SEP.1
FPT_SEP.1	FMT_MOF.1	FPT_RVM.1	—

非活性化防止

「表 23 セキュリティ機能要件の相互サポート構造」の通り FMT_MOF.1 により、機能要件（FIA_UAU.2[Panel]、FIA_UID.2[Panel]、FIA_AFL.1[Panel]、FIA_UAU.2[Appli]、FIA_UID.2[Appli]、FIA_AFL.1[Appli]、FDP_ACC.1[Disk_eject]、FDP_ACF.1[Disk_eject]、FDP_ACC.1[Cover_open]、FDP_ACF.1[Cover_open]、FMT_MSA.1、FMT_SMR.1、FMT_SMF.1、FIA_USB.1、FIA_ATD.1、FMT_MTD.1、FPT_RVM.1、FPT_SEP.1）を非活性化する能力は運用者に制限される。従って、運用者以外の者による非活性化行為から保護される。

迂回防止

「表 23 セキュリティ機能要件の相互サポート構造」に示す全ての機能要件は、自身がバイパスされることにより、セキュリティ機能が正常に動作しないため、自身がバイパスされることを防止しなければならない。これに関し、FRT_RVM.1により、セキュリティ機能が呼び出され、成功することが保証される。迂回防止を考慮する必要のない機能要件は、本 ST には存在しない。

改ざん防止

「表 23 セキュリティ機能要件の相互サポート構造」に示す全ての機能要件は、自身が干渉・改ざんされることにより、セキュリティ機能が正常に動作しないため、自身が干渉・改ざんされることを防止しなければならない。これに関し、FPT_SEP.1 により、信頼できないサブジェクトによる干渉と改ざんから自身を保護するためにセキュリティドメインを維持し、セキュリティドメイン間の分離を実施することが保証される。改ざん防止を考慮する必要のない機能要件は、本 ST には存在しない。

以上により、全ての 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 最小機能強度の妥当性

本 TOE は、一般的なオフィス環境に設置され、外部ネットワークとはルータやファイアウォールにより保護された状態にある。従って、不特定多数の者に直接攻撃される可能性は低い。また、「表 2 TOE の関係者」において、脅威エージェントとなり得る者は、高度な情報処理技術を有していないことを想定している。従って、セキュリティ機能は低レベルの攻撃に対応する機能を備えればよく、最小機能強度レベルは SOF-基本が妥当と言える。

8.2.6 評価保証レベルの妥当性

本 TOE は、不特定多数の利用者が TOE に対して攻撃する可能性は低いものの、病院のカルテやオフィスの顧客情報など機密情報を扱うことから、開発段階での分析、構成管理、開発セキュリティ、テストを考慮した EAL3 のセキュリティ保証要件が適切な保証レベルと考える。

8.2.7 セキュリティ保証要件の根拠

本 TOE は、一般的なオフィス環境で使用されるため、攻撃の機会は制限される。従って、本 TOE は、低レベルの攻撃能力を有する攻撃者を想定することができる。これに対抗するため TOE 開発のセキュリティ対策の分析（設計の系統だった分析とテスト、及び開発環境が安全であること）でカバーされる範囲を評価することとした。よって、評価保証レベル 3 が妥当である。

8.2.8 セキュリティ機能要件の一貫性の根拠

以下に、競合する可能性のあるセキュリティ機能要件が存在しない根拠を示す。

- 識別認証要件の繰り返しを使用しているが、それらは、①操作パネルから TOE にアクセスする際の識別認証、②アプリケーション（Total Disc Maker、Total Disc Monitor、PP-100NWeb アプリ）から TOE にアクセスする際の識別認証を規定している。「表 15 セキュリティ機能とセキュリティ要件」の通り、各識別認証機能は機能的に分離したものであり、競合するものではない。
- アクセス制御要件の繰り返しにより、複数のアクセス制御方針を立てているが、それらは、①ディスクの取り出し、②電子錠の解錠、③設定管理情報の操作に関するアクセス制御を規定している。つまり、それらは同一の制御対象を複数のポリシーでカバーし合うものではないため、競合するものではない。

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記述する。

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は「表 15 セキュリティ機能とセキュリティ要件」に示した。「表 15 セキュリティ機能とセキュリティ要件」の通り、全ての 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、全ての 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

FAU_ARP.1 セキュリティアラーム

SF.警告機能は、セキュリティ侵害の可能性を検知した際、以下の警告を発する。

- ブザーを鳴らす
- ERROR LEDを点灯する
- LCDに対処方法を表示する

よって、FAU_ARP.1は満たされる。

FAU_SAA.1 侵害の可能性の分析

SF.警告機能は、以下のセキュリティ侵害の可能性を分析する。

- 電源オフ処理時、PP-100N内に作成済みディスクがある
- ディスクカバーが未施錠となる
- オートローダがディスクを取り落とす
- 電源オン期間中、スタッカ2が取り外され戻されたとき、スタッカ2内にディスクがある

よって、FAU_SAA.1は満たされる。

FAU_GET.1 イベント情報の取得

SF.警告機能は、以下の事象についてイベント情報を取得する。

- 電源オフ処理時、PP-100N内に作成済みディスクがある
- ディスクカバーが未施錠となる
- オートローダがディスクを取り落とす
- 電源オン期間中、スタッカ2が取り外され戻されたとき、スタッカ2内にディスクがある

よって、FAU_GET.1は満たされる。

FIA_UAU.2[Panel] アクション前の利用者認証

SF.識別認証[Panel]機能は、操作パネルからTOEへアクセスする際、パスワード[Panel]の入力を要求し、認証が完了することを要求する。よって、FIA_UAU.2[Panel]は満たされる。

FIA_UID.2[Panel] アクション前の利用者識別

SF.識別認証[Panel]機能は、操作パネルからTOEへアクセスする際、ユーザ識別子[Panel]の入力を要求する。よって、FIA_UID.2[Panel]は満たされる。

FIA_UAU.7[Panel] 保護された認証フィードバック

SF.識別認証[Panel]機能は、パスワード入力中、入力された文字と同数の"*"を LCD に表示させる。よって、FIA_UAU.7[Panel]は満たされる。

FIA_AFL.1[Panel] 認証失敗時の取り扱い

SF.識別認証[Panel]機能は、認証に対して一定時間内に 3 回連続で失敗した場合、設定された時間（運用者 6 時間、その他 1 時間）認証を拒否する。よって、FIA_AFL.1[Panel]は満たされる。

FIA_SOS.1[Panel] 秘密の検証

SF.設定情報管理機能は、パスワードの入力規則を次の通り検証する。

- パスワード[Panel]：数字 5 桁以上

よって、FIA_SOS.1[Panel]は満たされる。

FIA_UAU.2[Appli] アクション前の利用者認証

SF.識別認証[Web_app]機能は、PP-100NWebアプリから、SF.識別認証[Cli_app]機能は、Total Disc Maker、もしくはTotal Disc MonitorからTOEへアクセスする際、パスワード[Appli]の入力を要求し、認証が完了することを要求する。よって、FIA_UID.2[Appli]は満たされる。

FIA_UID.2[Appli] アクション前の利用者識別

SF.識別認証[Web_app]機能は、PP-100NWeb アプリから、SF.識別認証[Cli_app]機能は、Total Disc Maker、もしくは Total Disc Monitor から TOE へアクセスする際、ユーザ識別子[Appli]の入力を要求する。よって、FIA_UID.2[Appli]は満たされる。

FIA_AFL.1[Appli] 認証失敗時の取り扱い

SF.識別認証[Web_app]機能、SF.識別認証[Cli_app]機能は、認証に対して一定時間内に 3 回連続で失敗した場合、設定された時間（運用者 6 時間、その他 1 時間）認証を拒否する。よって、FIA_AFL.1[Appli]は満たされる。

FIA_SOS.1[Appli] 秘密の検証

SF.設定情報管理機能は、パスワードの入力規則を次の通り検証する。

- パスワード[Appli]：英数字又は特殊文字（「.」「-」「_」）5 桁以上

よって、FIA_SOS.1[Appli]は満たされる。

FDP_ETC.1 セキュリティ属性なし利用者データのエクスポート

SF.取り出し制御機能は、利用者データである作成済みディスクをアクセス制御SFPに従い、TSF制御範囲外であるスタッカ4へ排出する。よって、FDP_ETC.1は満たされる。

FDP_ACC.1[Disk_eject] サブセットアクセス制御、FDP_ACF.1[Disk_eject] セキュリティ属性によるアクセス制御

SF.取り出し制御機能は、取り出し制御SFPにおいて制御されるセキュリティ属性（ユーザ識別子[Appli]、JOB ID）に基づき、作成済みディスクのディスク位置情報の参照を許可する。よって、FDP_ACC.1[Disk_eject]、FDP_ACF.1[Disk_eject]は満たされる。

FMT_MSA.3 静的属性初期化

SF.取り出し制御機能は、取り出し制御SFPのオブジェクトであるJOB情報に一意なユーザ識別子[Appli]とJOB IDを関連付け、更にディスク位置情報に一意なJOB IDを関連付ける。また、これらセキュリティ属性（ユーザ識別子[Appli]及

びJOB ID）のデフォルト値は変更できない。よって、FMT_MSA.3は満たされる。

FDP_ACC.1[Cover_open] サブセットアクセス制御、FDP_ACF.1[Cover_open] セキュリティ属性によるアクセス制御

SF.電子錠開制御機能は、カバー開制御SFPにおいて制御されるセキュリティ属性（運用者権限）に基づき、電子錠の解錠を許可する。よって、FDP_ACC.1[Cover_open]、FDP_ACF.1[Cover_open]は満たされる。

FMT_MSA.1 セキュリティ属性の管理

SF.設定情報管理機能は、セキュリティ属性の管理を運用者に制限している。よって、FMT_MSA.1は満たされる。

FMT_SMR.1 セキュリティ役割

SF.設定情報管理機能は、利用者の役割を定義し、その役割を各利用者に関連付け、その役割を維持している。よって、FMT_SMR.1は満たされる。

FMT_SMF.1 管理機能の特定

SF.設定情報管理機能は、識別認証された運用者に各機能要件の管理要件の管理を許可する。よって、FMT_SMF.1は満たされる。

FIA_USB.1 利用者・サブジェクト結合

SF.設定情報管理機能は、利用者とその役割の関連付けを行う。よって、FIA_USB.1 は満たされる。

FIA_ATD.1 利用者属性定義

SF.設定情報管理機能は、運用者権限、ユーザ識別子[Appli]を定義し、維持する。よって、FIA_ATD.1 は満たされる。

FMT_MTD.1 TSFデータの管理

SF.取り出し制御機能は、ディスクを作成した利用者のみがディスク位置情報の変更、削除を行うことができることを管理している。SF.設定情報管理機能は、運用者、承認者、担当者、利用者ごとに操作できるTSFデータを管理している。よって、FMT_MTD.1は満たされる。

FMT_MOF.1 セキュリティ機能のふるまいの管理

SF.設定情報管理機能はセキュリティ機能の設定を運用者のみに制限している。よって、FMT_MOF.1は満たされる。

FPT_RVM.1 TSP の非バイパス性

SF.取り出し制御機能は、ディスクを作成した利用者が自身の作成済みディスクを取り出す際、TOE により呼び出され、アクセス制御が実施され、成功することを保証する。SF.電子錠開制御機能は、運用者がディスクカバーを開けるための一連の操作を行う際、TOE により呼び出され、アクセス制御が実施され、成功することを保証する。SF.識別認証[Panel]機能、SF.識別認証[Web_app]機能、及び SF.識別認証[Cli_app]機能は、TSC 内の各機能の動作が許可される前に、TOE により呼び出され、識別認証が実施され、成功することを保証する。SF.設定情報管理機能は、設定管理情報、JOB 情報、ディスク位置情報にアクセスする際、TOE により呼び出され、アクセス制御が実施され、成功することを保証する。よって、FPT_RVM.1 は満たされる。

FPT_SEP.1 TSFドメイン分離

SF.取り出し制御機能、SF.電子錠開制御機能、SF.識別認証[Panel]機能、SF.識別認証[Web_app]機能、SF.識別認証[Cli_app]機能、SF.警告機能、及び SF.設定情報管理機能は、各機能要件を不正な干渉・改ざんから保護するため、TSF とサブジェクトのドメインを分離・維持する。従って、FPT_SEP.1 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は、SF.識別認証[Panel]機能、SF.識別認証[Web_app]機能、SF.識別認証[Cli_app]機能、SF.設定情報管理機能である。これらセキュリティ機能は SOF-基本を示している。一方、本 TOE の最小機能強度は、SOF-基本ある。 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要件の対応を「表 24 TOE セキュリティ保証要件として示されたドキュメント」に示す。

表 24 TOE セキュリティ保証要件として示されたドキュメント

保証要件クラス	保証要件 コンポーネント	ドキュメント名称 及び TOE	内容
ACM（構成管理）	ACM_CAP.3	・KP-01 PP-100N 構成管理計画書（全体編） ・KP-02 PP-100N 構成管理計画書（メカ部） ・KP-03 PP-100N 構成管理計画書（オートローダ基板） ・KP-04 PP-100N 構成管理計画書（サーバシステムソフト） ・KP-05 PP-100N 構成管理計画書（オートローダファームウェア） ・KL-01 PP-100N 構成リスト（全体編） ・KL-02 PP-100N 構成リスト（メカ部） ・KL-03 PP-100N 構成リスト（オートローダ基板） ・KL-04 PP-100N 構成リスト（サーバシステムソフト） ・KL-05 PP-100N 構成リスト（オートローダファームウェア）	TOE 構成要素の完全性を保証するために必要な規定、手順が記述されている。

	ACM_SCP.1	・KL-01 PP-100N 構成リスト(全体編) ・KL-02 PP-100N 構成リスト(メカ部) ・KL-03 PP-100N 構成リスト(オートローダ基板) ・KL-04 PP-100N 構成リスト(サーバシステムソフト) ・KL-05 PP-100N 構成リスト(オートローダファームウェア)	
ADO (配付と運用)	ADO_DEL.1	・PP-100N 配付手順書 ・PP-100N Web 配付手順書	開発元からユーザまでの配付手続きが記述されている。
	ADO_IGS.1	・PP-100N 運用者ガイド【認証発行オプション編】 ・PP-100N Security Administrator's Guide ・PP-100N ソフトウェアインストール手順書 ・Install Manual for PP-100N ・Sheet, Security, PP100N	TOE の安全な設置、運用のために必要な全ての手順が記述されている。
ADV (開発)	ADV_FSP.1	・セイコーエプソン PP-100N セキュリティ制御機構 機能仕様書 ・セイコーエプソン PP-100N セキュリティ制御機構 TOE 機能構成図	TSF のふるまいと TSF インターフェース、TSF 以外の機能についての外部インターフェースが記述されている。
	ADV_HLD.2	・セイコーエプソン PP-100N セキュリティ制御機構 上位レベル設計書 ・セイコーエプソン PP-100N セキュリティ制御機構 TOE サブシステム構成図	サブシステムの観点から TSF を記述したものであり、TSF の構造、サブシステムのインターフェースについて記述されている。

	ADV_RCR.1	・セイコーエプソン PP-100N セキュリティ制御機構 表現対応分析書	ST における要約仕様のセキュリティ機能と機能仕様書、上位レベル設計書におけるサブシステムの関係について分析した結果について記述されている。
AGD（ガイダンス文書）	AGD_ADM.1	・PP-100N 運用者ガイド【認証発行オプション編】 ・PP-100N Security Administrator's Guide ・Sheet, Security, PP100N	TOE の安全な設置、運用のために必要な全ての手順が記述されている。
	AGD_USR.1	・PP-100N ユーザーズガイド【認証発行オプション編】 ・PP-100N Security User's Guide	
ALC（ライフサイクルサポート）	ALC_DVS.1	・PP-100N セキュリティ制御機構 開発セキュリティ業務処理基準	開発環境の中で TOE の設計や実装の機密性と完全性を保証するための手段について記述されている。
ATE（テスト）	ATE_COV.2	・PP-100N セキュリティ制御機構 機能テスト仕様書 ・PP-100N セキュリティ制御機構 上位レベルテスト仕様書	TSF が仕様通りに実行されることを実証するための機能テスト項目、テスト手順、期待されるテスト結果、及びそれらに基づいてテストを行った結果について記述されている。
	ATE_DPT.1		
	ATE_FUN.1		
	ATE_IND.2		
AVA（脆弱性分析）	AVA_MSU.1	・PP-100N セキュリティ制御機構 誤使用に関する分析書	TOE が安全でない場合、TOE 管理者がそれに気付かないリスクを最小にすることを保証するために誤使用分析を実施し、その結果について記述されている。

	AVA_SOF.1	・PP-100N セキュリティ制御機構 機能強度分析書	TOE における暗号化メカニズムを除く確率的または順列的セキュリティメカニズムを有するセキュリティ機能に対して、機能強度分析を実施した結果について記述されている。
	AVA_VLA.1	・PP-100N セキュリティ制御機構 脆弱性分析書	明らかなセキュリティ脆弱性の存在を探索しTOEの意図する環境において、それらの脆弱性が悪用され得ないことを確認する脆弱性分析を実施した結果について記述されている。

「表 24 TOE セキュリティ保証要件として示されたドキュメント」の通り、TOE セキュリティ保証要件は、保証手段として示されたドキュメントのセットによって対応付けられる。また保証手段として示されたドキュメントによって、本 ST が規定した TOE セキュリティ保証要件が要求する証拠を網羅している。

8.4 PP 主張の根拠

参照 PP はない。