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7月18日** (IT**認証**7161)
認証番号	C0228
認証申請者	**セイコーエプソン株式会社**
TOE**の名称**	PP-100N**セキュリティ制御機構**
TOE**のバージョン**	1.00
PP**適合**	**なし**
適合する保証パッケージ	EAL3
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21年7月27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　山里　拓己

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

「PP-100Nセキュリティ制御機構」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
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの機能 6
1.3 評価の実施 7
1.4 評価の認証 7
1.5 報告概要 8
1.5.1 PP適合 8
1.5.2 EAL 8
1.5.3 セキュリティ機能強度 8
1.5.4 セキュリティ機能 8
1.5.5 脅威 12
1.5.6 組織のセキュリティ方針 12
1.5.7 構成条件 13
1.5.8 操作環境の前提条件 13
1.5.9 製品添付ドキュメント 14
2 評価機関による評価実施及び結果 15
2.1 評価方法 15
2.2 評価実施概要 15
2.3 製品テスト 15
2.3.1 開発者テスト 15
2.3.2 評価者テスト 18
2.4 評価結果 20
3 認証実施 21
4 結論 22
4.1 認証結果 22
4.2 注意事項 28
5 用語 29
6 参照 32

1 全体要約

1.1 はじめに

この認証報告書は、「PP-100Nセキュリティ制御機構」（以下「本TOE」という。）についてみずほ情報総研株式会社（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： PP-100Nセキュリティ制御機構
バージョン： 1.00
開発者： セイコーエプソン株式会社

1.2.2 製品概要

TOEはCD/DVDパブリッシャー製品であるPP-100Nに実装される、ソフトウェア及びハードウェアから構成されるセキュリティ制御機構である。本製品（以降、PP-100N）はネットワークを介して電子情報をCD-RやDVD-R等のディスクに記録し、同時にレーベル印刷を行うサービスを提供する。

本TOEは、情報が記録済みのディスクに対して、ディスク作成者以外による不正なディスク取り出しを防ぐため、下記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

1.2.3 TOEの範囲と動作概要

(1) TOE動作環境

図1-1にTOEの利用環境の一例を、表1-1にTOE利用環境における関係者を示す。

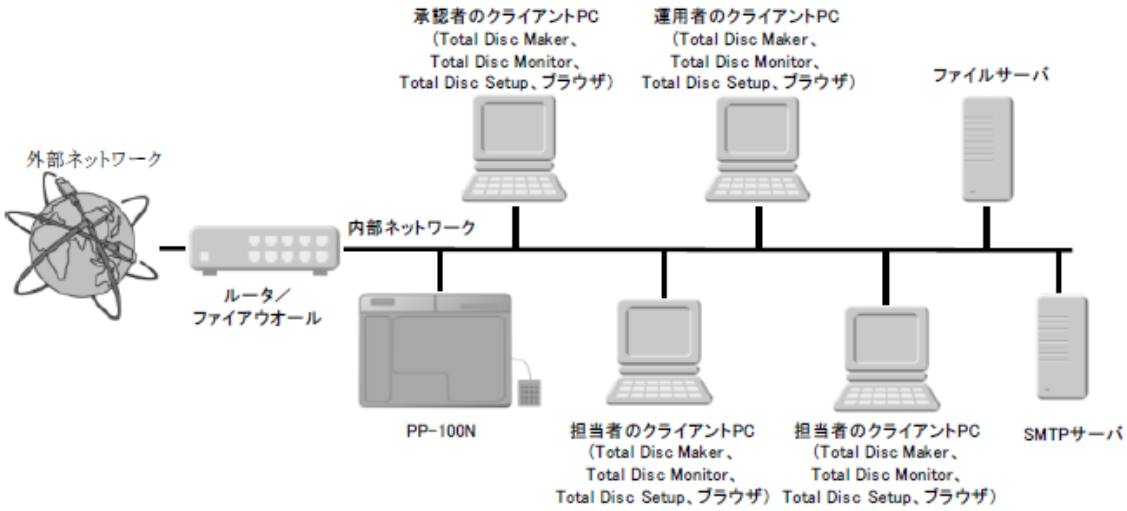

図1-1　TOE利用環境

表1-1　TOE利用環境における関係者

組織の責任者	承認者、運用者の任命責任を持つ。
利用者	PP-100Nによるディスク作成権限を有した者。下記運用者、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。信頼できる人間であり、悪意を持った行為は行わない。
承認者	ディスク作成者からの作成承認依頼に対して承認を行う者。信頼できる人間であり、悪意を持った行為は行わない。
担当者	ディスク作成権限のみ有する利用者。TOEに対して悪意を持った行為を行う可能性がある。
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。TOEに対して悪意を持った行為を行う可能性がある。
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。

図1-1に示すように、TOEが実装されるPP-100Nは外部ネットワークからファイアウォール等で保護された内部ネットワークに接続される事を想定している。その他構成要素としては、運用者、承認者、担当者が使用する各クライアントPC、ディスクに書き込むデータが保存されるファイルサーバ、内部ネットワークの運用環境によって設置されるネットワーク関連サーバ(図1-1中SMTPサーバ)等が存在する。各クライアントPCにはTOEの操作、モニタリング等を行うためのPP-100N添付の専用アプリケーションソフトウェア(Total Disc Maker等)がインストールされる。また、利用者は製品の購入に加え別途認証発行オプションを購入し、それによって得られるアクティベーションキーを用いてTOEのセキュリティ機能を活性化（セキュリティモード設定）する必要がある。

下記にPP-100Nにおけるディスク作成処理の概要を示す。PP-100Nにおいて実行される処理としては、利用者がディスク作成処理を開始してからディスクが作成され、PP-100Nの内部に格納されるまで（下記、ディスク作成処理）と、作成されたディスクを利用者がPP-100Nから取り出すまで(下記､ディスク取り出し処理)の、２つのフェーズに分類される。

【ディスク作成処理】

- 利用者はクライアントPC上のアプリケーション（Total Disc Maker）を使用しディスクに書き込むディスクイメージファイル、レーベルデータファイルを作成する。

- 利用者はクライアントPC上のアプリケーション(Total Disc Maker)からディスク作成処理を開始し、作成したディスクイメージファイルとレーベルデータファイルがPP-100Nに転送され、スプールデータとしてPP-100N内のHDDに記録される。
  （ディスク作成処理が開始された時点でTOE内にJOB情報が新規に生成され管理される）

- 利用者からのディスク作成要求が承認者に送信され、承認者はクライアントPCからPP-100Nに接続し、ディスク作成を指示する。

- PP-100Nにおいてディスク作成処理（データ記録、レーベル印刷）が実行され、作成されたディスクがスタッカ2（作成済みディスク格納先）に格納される。

【ディスク取り出し処理】

- ディスクを作成した利用者が、PP-100Nの操作パネル上でディスク取り出し処理を開始し、認証用テンキーよりユーザ識別子とパスワードを入力する。

- 識別認証の成功後に、PP-100N内のオートローダが利用者の作成したディス

クをスタッカ2からスタッカ4に移動させる。
（識別された利用者により作成されたディスクが複数存在する場合は、全てのディスクがスタッカ4に移動され、その際一時的に退避させる必要のあるディスクが存在する場合はスタッカ1を使用する）

- 利用者がスタッカ4を開け、移動されたディスクを取り出す。
（スタッカ4にあるディスクのみ、引き出しを自由に開けて取り出すことができる）

(2) TOE構成及び動作概要

図1-2にPP-100Nの内部構成ブロック図を、図1-3にPP-100Nの内部イメージを示す。また、図1-2において網掛け部がTOEであり、その構成リストを表1-2に示す。

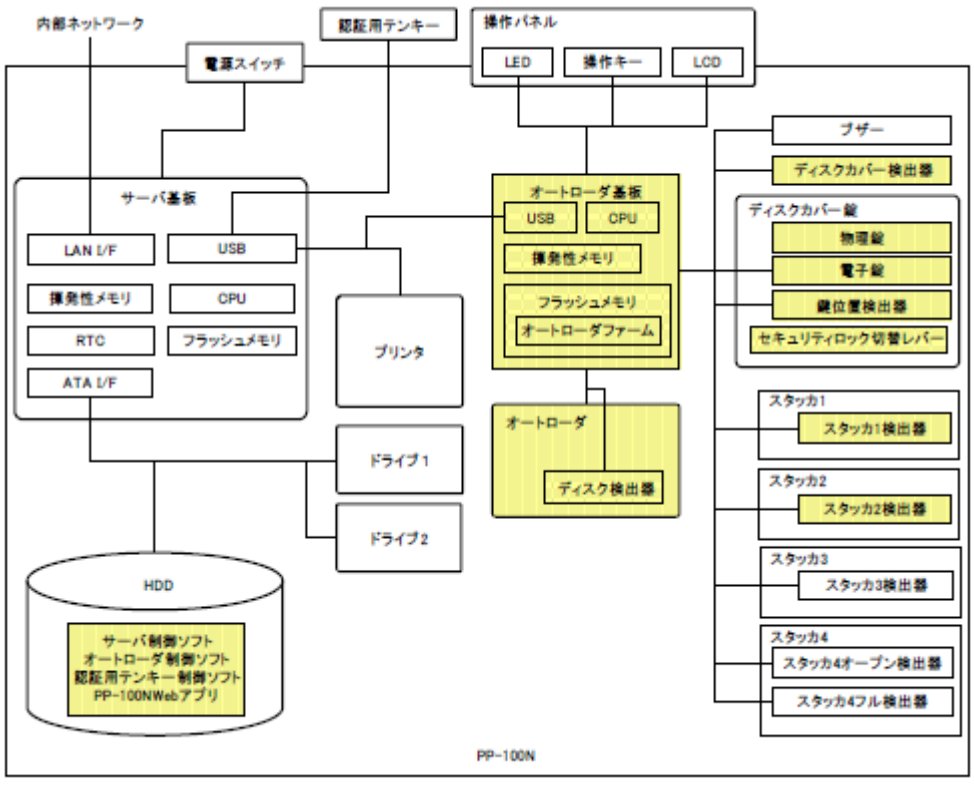

図1-2　PP-100N内部構成（網掛け部がTOE）

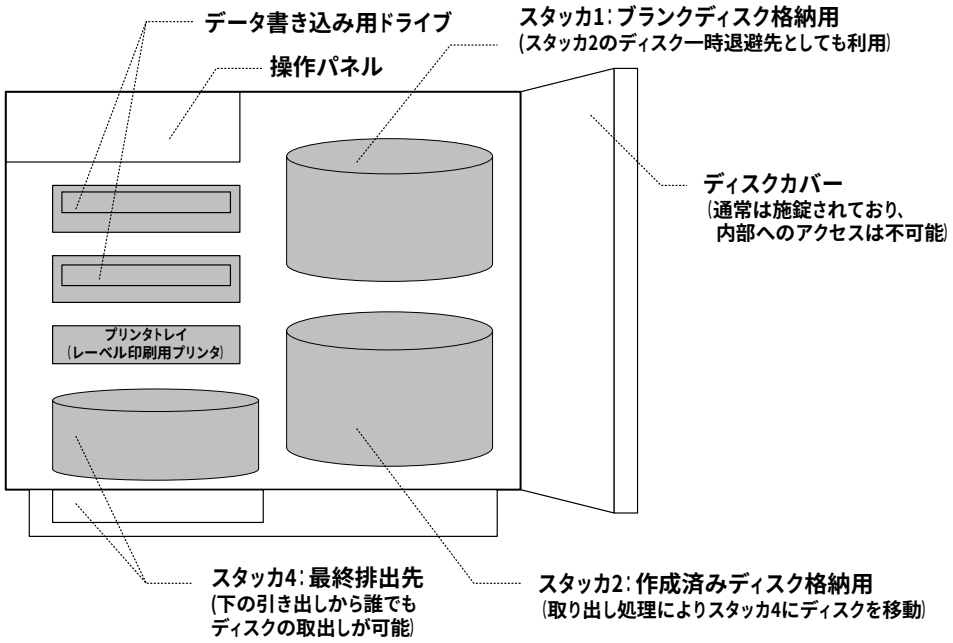

図1-3　PP-100N**内部構成イメージ**

表1-2　TOE**構成リスト**

オートローダ基板	ハードウェア制御用CPU,メモリ等で構成され、TOEハードウェア制御等を行う。
オートローダ	ディスクを1枚ずつ保持し搬送する装置であり、オートローダ基板の制御によりディスクを必要な場所（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）に移動させる。
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。
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。
物理錠	物理的な鍵によりディスクカバーを解錠できる錠。 鍵は運用者により安全に管理される
電子錠	ソフトウェアの制御によりディスクカバーを電気的に解錠できる錠。
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ため、本TOEではオンの状態で運用される。
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。
PP-100NWebアプリ	クライアントPCとの各種通信を行うアプリケーション。
オートローダ制御 ソフト	オートローダ制御を行うためのライブラリ、及びファームウェア
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。
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。

図1-2、及び表1-2に示される通り、TOEはハードウェア及びソフトウェアにより構成される。またPP-100NはTOEの他に、図1-3に示すディスクカバー、データ書き込み用ドライブ、レーベル印刷用プリンタ及びプリンタトレイ、ディスクを格納するスタッカ（スタッカ1、スタッカ2、スタッカ4の3台-スタッカ3は使用しない）、操作パネル、その他制御基板等のハードウェア、及びOS、データベース、ハードウェア制御ソフト等のソフトウェアで構成される。

本TOEではデータ書き込み、及びレーベル印刷が終了し、スタッカ2に格納された状態から、スタッカ4に排出されるまでのディスク自体を保護資産とし、セキュリティ機能により不正な利用者によるディスク取り出しを防ぐ（内部HDDに書き込みデータが一時的にスプールデータとして保存されるが、これは本TOEのセキュリティ機能による保護対象ではない）。

1.2.4 TOEの機能

本TOEは、TOEが実装される製品（以降PP-100N）のサービスとして作成されるディスクに対して、ディスク作成者以外による不正なディスク取り出しを防ぐためのセキュリティ機能を主に提供する。セキュリティ機能の詳細については「1.5.4 セキュリティ機能」を参照されたい。

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「PP-100Nセキュリティ制御機構 セキュリティターゲット」（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・製造・出荷の現場を調査し、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、「PP-100Nセキュリティ制御機構 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21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、EAL3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、外部ネットワークからの攻撃から保護された、一般のオフィス環境での利用を想定している。TOEへの直接的なアクセスあるいは内部ネットワークを経由した攻撃は、運用者による監視下にあり複雑な攻撃を想定されない。このため、攻撃者の攻撃力を“ 低レベル ”とすることは妥当であり、最小機能強度は“ 低レベル ”に対抗できる “ 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は、以下のとおりである。

(1) 取り出し制御機能

本機能はディスクを作成した利用者のみが、作成済みディスクをTOEから取り出すことができるように、ディスク排出に関するアクセス制御を実施する機能であり、下記の処理フローにより実行される。

- 利用者によるディスク取り出し指示（PP-100N操作パネルの取り出しボタン押下）により本機能の実行を開始する
- 識別認証[Panel]機能を実行し利用者の識別認証を行う
  （認証失敗の場合は処理終了）
- 識別されたユーザ識別子[Panel]に関連付けられたJOB情報を探索し、利用者本人の作成済みディスクが存在すると判断した場合に、各JOB情報及び対応するディスク位置情報から取り出す作成済みディスクの位置を把握する（JOB情報が存在しない場合には本機能の処理を終了する）
- オートローダを制御し、取り出す作成済みディスクをスタッカ2からスタッカ4に排出する（取り出すディスクの上に他のディスクが存在する場合は、他のディスクを一旦スタッカ1に退避させる）
- TOEが管理するディスク位置情報を、ディスク取り出し後の情報に更新する

(2) 電子錠開機能

ディスクカバーを運用者のみ開けることができるようにディスクカバーの電子錠の開閉を制御する機能である。

- 運用者はディスクカバーを開ける際にPP-100N本体の操作パネルに表示される操作メニューから電子錠を開錠する項目を選択する
- TOEは識別認証[Panel]機能を実行し、運用者の識別認証を行う
- 運用者であることが確認された場合、電子錠を解錠する
- 電子錠の解錠後一定時間（5秒以上）ディスクカバーが開かれなかった場合は電子錠を施錠する

(3) 識別認証機能

TOE利用者の識別、認証を行う機能であり、使用されるインタフェースにより識別認証[Web_app]機能、識別認証[Cli_app]機能、識別認証[Panel]機能の3種類の機能で構成される。

【識別認証[Web_app]機能】

- 利用者がブラウザを介してTOEが提供する各種設定機能（詳細については“ (5) 設定情報管理機能 ”において説明）にアクセスする際に、TOEに登録された正しい利用者である事を確認する機能
- Webアプリ起動時に識別認証画面を表示し、ユーザ識別子[Appli]とパスワード[Appli]を入力させる
- TOEが管理する利用者情報と入力された情報が一致した場合は正しい利用者であると判断し、一致しなかった場合は再度入力を要求する
- 識別認証に3回連続で失敗した場合、運用者は6時間、それ以外の利用者は1時間TOEへのアクセスがロックされる

【識別認証[Cli_app]機能】

- 利用者がクライアントアプリケーション（Total Disc Maker、Total Disc Monitor）からTOEにアクセスする際、TOEに登録された正しい利用者である事を確認する機能
- クライアントアプリケーション起動時に識別認証画面を表示し、ユーザ識別子[Appli]とパスワード[Appli]を入力させる
- TOEが管理する利用者情報と入力された情報が一致した場合は正しい利用者であると判断し、一致しなかった場合は再度入力を要求する
- 識別認証に3回連続で失敗した場合、運用者は6時間、それ以外の利用者は1時間TOEへのアクセスがロックされる

【識別認証[Panel]機能】

- 利用者がPP-100Nの操作パネルからTOEにアクセスする際、TOEに登録された正しい利用者である事を確認する機能
- 操作パネルに対する利用者の各種操作の中で、必要に応じて本機能が呼び出され実行される

- ユーザ識別子[Panel]とパスワード[Panel]の入力待ち画面を表示し、必要な情報をテンキーから入力させる
- TOEが管理する利用者情報と入力された情報が一致した場合は正しい利用者であると判断し、一致しなかった場合は再度入力を要求する
- 識別認証に3回連続で失敗した場合、運用者は6時間、それ以外の利用者は1時間TOEへのアクセスがロックされる
- パスワードの入力中は入力された文字と同数の"*"をLCDに表示する

(4) 警告機能

セキュリティ侵害の可能性が発生した場合、下記の警告手段を用いて運用者に警告を発生する機能である。

- ブザーを鳴動させる
- ERROR LEDを点灯させる
- LCDに対処方法を表示する

セキュリティ侵害の可能性として検出される事象は下記の通りである。

(a) 電源オフ処理時

電源オフ処理時、JOB情報を検索し、

・作成済みディスクがスタッカ2に残存している

・処理中JOBが存在する

上記の状態が確認された場合、電源オフ処理を中断し警告を発生させる。

(b) ディスクカバーオープン時

ディスクカバーが60秒以上開かれた状態である場合、警告を発生させる。

(c) ディスクカバークローズ時

ディスクカバーが閉じられた際、下記状態が10秒以上続いた場合は警告を発生させる。

・物理鍵が解錠されたままである

・セキュリティロック切替レバーがオフである

(d) ディスク搬送時

ディスク搬送時にオートローダがディスクを取り落とした事を検知した場合、警告を発生させる

(e) スタッカ2取り外し時

作成済みディスクが格納されるスタッカ2がTOE本体より取り外され、また戻された際にTOEはスタッカ2に残存するディスクの有無を確認し、存在している場合は警告を発生させる（これは、外部からスタッカ2に直接ディスクを格納されたりすることで、TOEが内部で管理するディスク位置情報との矛盾が発生し､取り出しディスクの制御が正しく実施されなくなる事を防ぐためである)。

(5) 設定情報管理機能

本機能は設定情報、JOB情報等のTSFデータに対するアクセス制御を行う機能で

あり、予め規定されている利用者種別（運用者、承認者、担当者）と、利用者種別毎に規定された権限に従い、許可された操作のみを実行させる。また、これらの設定処理は、クライアントPC上のブラウザを介してTOEに接続し、識別認証[Web_app]機能の成功後に実行される。なお、利用者種別毎の権限は固定であり、変更は出来ない。以下に利用者種別毎に実施可能な処理を示す（下記ではTSFデータに直接アクセスする事を目的とした操作のみ記載する）。

表1-3 利用者役割毎の実施可能操作

利用者種別	TSFデータ	実施可能な操作
運用者	利用者情報	・利用者情報の参照、追加、削除、改変
	設定情報	・セキュリティモードステータスの改変 ・時刻設定情報の参照、改変 ・ネットワーク設定情報の参照、改変
	JOB情報	・JOB情報の参照、削除、改変
承認者	利用者情報	・本人のパスワード改変
担当者	利用者情報	・本人のパスワード改変

なお、表1-3のTSFデータ（利用者情報、JOB情報）は主に下記情報により構成される。

【利用者情報】

利用者識別子[Appli]、パスワード[Appli]：

クライアントアプリケーション等からの識別認証に使用されるユーザ識別子、パスワード

利用者識別子[Panel]、パスワード[Panel]：

PP-100N本体操作パネル上での識別認証に使用されるユーザ識別子、パスワード

権限：利用者の役割（運用者、承認者、担当者）

【JOB情報】

JOB ID：各JOBの識別子

利用者識別子：JOBに関連付けられた利用者の識別子

ステータス：JOBの現在のステータス情報

ディスク位置情報：JOBが関連付けられているディスクのスタッカ内の位置

1.5.5 脅威

本TOEは、表1-4に示す脅威を想定し、これに対抗する機能を備える。

表1-4 想定する脅威

識別子	脅 威
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。 ＊本脅威はスタッカ2に実際に積まれているディスクの情報と、TOEが内部で管理するディスク位置情報との間で矛盾が発生する事により生じるディスクの誤排出を懸念している。

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を表1-5に示す。

表1-5 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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。

1.5.7 構成条件

本TOEの動作環境として、下記ブラウザが動作するクライアントPCが必要となる。また製品添付のクライアントアプリケーション（Total Disc Maker、Total Disc Monitor）をクライアントPCにインストールする事が必要となる。

ブラウザ（下記のいずれか）：

Microsoft Internet Explorer 6

Microsoft Internet Explorer 7

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.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。

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の識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

【日本語版】

ドキュメント名	識別子
PP-100N 運用者ガイド【認証発行オプション編】	411650900
PP-100Nユーザーズガイド【認証発行オプション編】	411650800

【英語版】

ドキュメント名	識別子
PP-100N Security Administrator's Guide	M00012700
PP-100N Security User's Guide	M00012000

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8月に始まり、平成21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21年1月、3月、6月に開発・製造現場へ赴き、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・ライフサイクル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21年4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図2-1に示す。

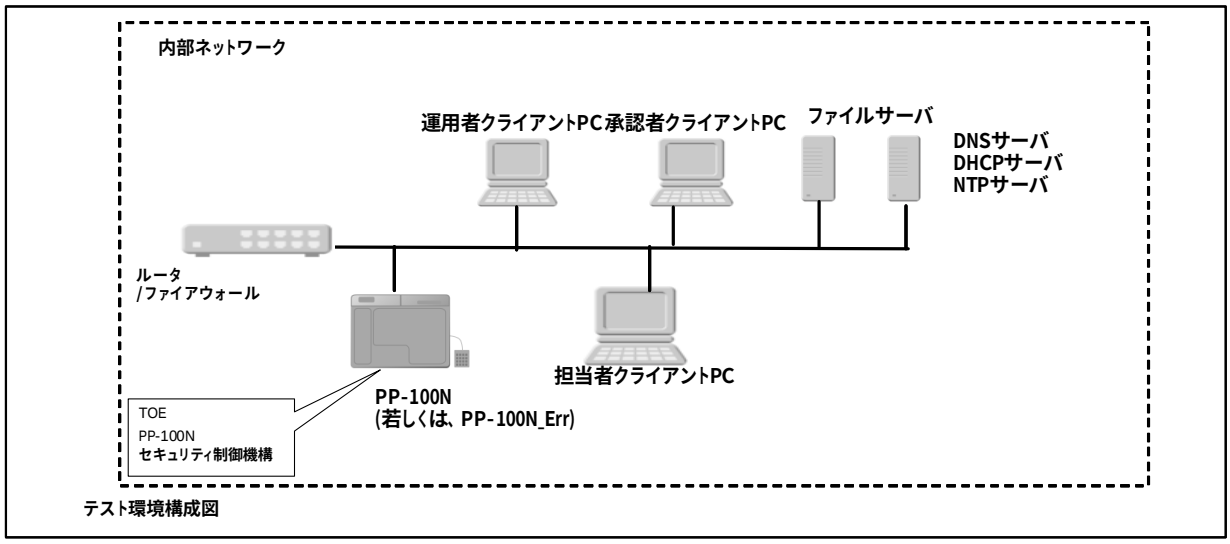

図2-1　開発者テストの構成図

表2-1　開発者テスト構成

構成要素	概要説明
PP-100N	TOEであるセキュリティ制御機構が実装された製品。 TOEバージョン：1.00
PP-100N_Err	PP-100Nのディスクカバー前面をくりぬいた、エラー系テスト専用機。 TOEバージョン：1.00
クライアントPC	運用者、承認者、担当者が使用するクライアントPC。各PCでは下記OS、ブラウザと共に、Total Disc Maker等のクライアントアプリケーションがインストールされる。 OS： Windows XP Professional SP3 Windows Vista Ultimate SP1 ブラウザ： Internet Explorer6,7
ファイルサーバ	ディスクに書き込むためのデータが格納されるサーバマシンで、必要に応じて設置される。本テスト環境では下記OSが搭載されたPCをファイルサーバとして使用している。 OS： Windows Server 2003

DNSサーバ DHCPサーバ NTPサーバ	使用するネットワーク環境において必要に応じて設置されるサーバ群。本テスト環境では下記OSが搭載されたPCをサーバとして使用している。 OS： Windows Server 2003
ルータ/ ファイアウォール	内部ネットワーク内の通信制御のためのルータ/ファイアウォール。本テスト環境においては外部ネットワークと接続しないため、ファイアウォール機能は利用していない。

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

開発者テストは図2-1、表2-1に示すとおり、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。

b. テスト手法

テストには、以下の手法が使用された。

①実際の運用で使用されるユーザインタフェース（本体パネル、クライアントアプリ）を刺激し、セキュリティ機能の振る舞いを以下手段により確認する。

・TOEによる作成ディスク排出、ディスクカバー施錠動作等の物理的な動作確認

・操作画面上（本体液晶画面、クライアントPC上の画面表示）での動作確認、メッセージ出力等の確認

・ブザー音、警告LEDの発光、エラーメッセージ表示確認等によるエラー発生確認

②製品前面のディスクカバーをくりぬいたテスト専用機（表中PP-100N_Err）を使用し、製品内部への直接的な操作（オートローダの動作中に手で押さえる、搬送中のディスクを手で叩き落す等）を行う事により、セキュリティ機能の振る舞いを以下手段により確認する。

・操作画面上（本体液晶画面、クライアントPC上の画面表示）での動作確認、メッセージ出力等の確認

・ブザー音、警告LEDの発光、エラーメッセージ表示確認等によるエラー発生確認

c. 実施テストの範囲

テストは開発者によって1,071項目実施されている。また、各項目は正常系、異常系、実施パラメータ等によりさらに細分類される。

このテスト項目に対して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。また、深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステム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図2-2、表2-2に示す（表2-2は開発者テスト環境と異なる要素のみ）。

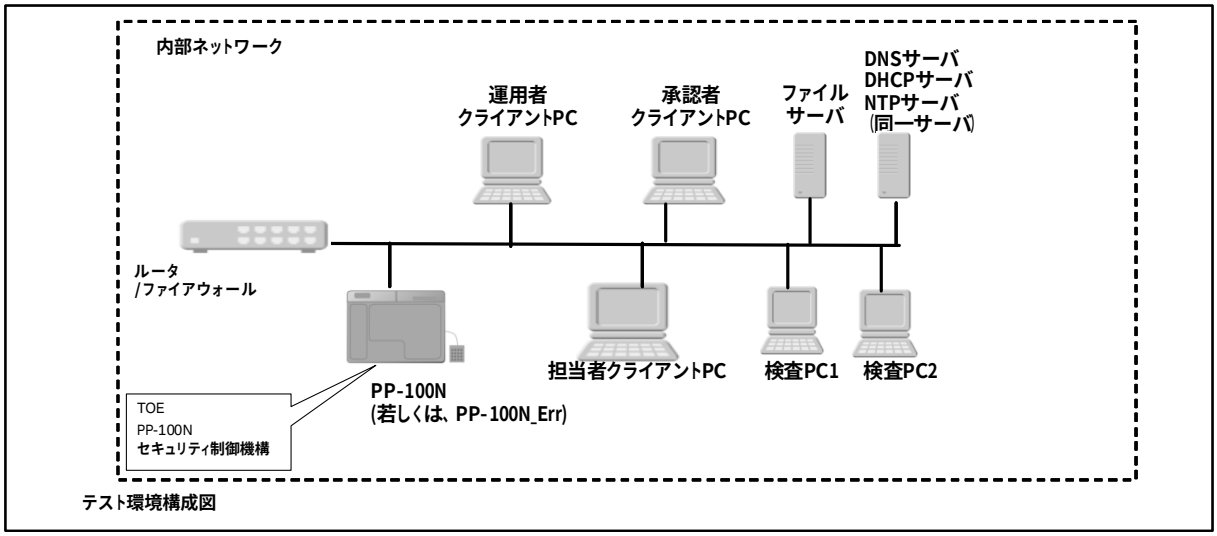

図2-2　評価者テストの構成図

表2-2　評価者テスト構成

構成要素	概要説明
検査PC1、検査PC2	検査PCは共にWindows XP SP2が搭載されたネットワーク端子付きのPCであり、脆弱性テストに利用される。また、本PCにはセキュリティスキャナソフトや各種ツール類がインストールされる。

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

評価者テストは図2-2、表2-2に示すとおり、図2-1に示した開発者テスト環境に、検査PCが追加された構成で実施されている。この検査PCはネットワーク上のパケットデータ観測、TOEへのデータ送信等に使用されるのみであり、STにおいて識別されているTOE構成と同一の環境であると考えられる事が評価者により検証されている。

b. テスト手法

テストには、以下の手法が使用された。

①開発者テストにおいて使用されたテスト手法と同等の手法。

②TSFIに対して検査PCからHTTP等のプロトコルを使用して直接アクセスし、TOEから送信される情報の内容を確認する事によりセキュリティ機能の振る舞いを確認する。

c. 実施テストの範囲

評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを309項目、侵入テストを7項目、計321項目のテストを実施した。また、各項目は開発者テストと同様に正常系、異常系、実施パラメータ等によりさらに細分類される。

テスト項目の選択基準として、下記を考慮している。

①TOEの各セキュリティ機能を網羅する。

②開発者テストにおいて不足していると判断される項目。

・複数ユーザの同時接続、同時操作を意識したテスト手法による検査

・電源断タイミングの想定パターン等の各種パラメータの組み合わせ等

③脆弱性分析において懸念される事項に関するテスト。

・TSFIの想定外の使用（クライアントアプリ以外からの直接アクセス等）によるセキュリティ機能のバイパスの可否

・ネットワークインタフェースに関する公知の脆弱性の残存の有無

・ハードウェアの故障等によるセキュリティ機能への影響等

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。 また、本TOEに含まれるハードウェア故障等によるセキュリティ機能への影響については、開発者により使用部品の故障率、耐用年数等を基にした分析が成され、製品寿命として想定する期間は十分な保証が得られる事が確認されており、評価者がその妥当性について確認している。

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もとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが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EAL3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すべてのTOEのセキュリティ要件の記述が、正当であること、客観的に、明確に、曖昧さなく表現されていること、及び保証要件でサポートされるのに適切で妥当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あらゆるITセキュリティ要件の依存性のすべてが識別されてい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.3.1E	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。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。

ADV_HLD.2.1E	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.2.2E	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。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。

ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	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かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.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上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであ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_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
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ともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

本TOEのセキュリティ機能（特に警告機能）がその役割を適切に果たすためには、運用者が常にTOEの状態を監視できる環境で運用する事と、エラー発生時には運用者が迅速に必要な対処を行う事が前提となる事に読者は注意されたい。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

JOB	ディスク作成ごとに発生するPP-100N の作業単位。
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
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、キャンセル等を行う。
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。
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で、スタッカ2の予備として使用される。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。スタッカ4に格納されたディスクは、PP-100N下部の引き出しを開けることで利用者は自由にディスクを取り出すことができる。
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。
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 なお、本STは、セキュリティモード設定時について記述する。
操作パネル	LCD,LED,操作キーから構成されるユーザインタフェース。
ディスク	CD-R,DVD-R等のディスク型記録媒体。
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。
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 （ディスクカバーを施錠、開錠、どちらの状態で運用するか切り替えるためのレバー）
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。
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。
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
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。
ブザー	PP-100Nに異常が発生したことを音で知らせる装置。
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。
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。
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。

6 参照

[1] PP-100Nセキュリティ制御機構 セキュリティターゲット バージョン 2.0（2009年7月3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] PP-100N セキュリティ制御機構 評価報告書 第1版 2009年7月9日 みずほ情報総研株式会社 情報セキュリティ評価室