認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成26年4月25日 (IT認証4505)
認証番号	C0496
認証申請者	コニカミノルタ株式会社
TOEの名称	日本語名：bizhub PRESS 2250P 全体制御ソフトウェア 英語名　：bizhub PRESS 2250P control software
TOEのバージョン	画像制御プログラム（画像制御　I1）： A64F0Y0-00I1-G00-15 コントローラ制御プログラム(ICコントローラ　P)： A64F-00P1-G00-15
PP適合	なし
適合する保証パッケージ	EAL3
開発者	コニカミノルタ株式会社
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28年1月26日

技術本部
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 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 バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「日本語名 ：bizhub PRESS 2250P 全体制御ソフトウェア、英語名 ：bizhub PRESS 2250P control software」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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

この認証報告書は、コニカミノルタ株式会社が開発した

「 日本語名 ：bizhub PRESS 2250P 全体制御ソフトウェア
英語名 ：bizhub PRESS 2250P control software
バージョン
画像制御プログラム（画像制御 I1）：A64F0Y0-00I1-G00-15
コントローラ制御プログラム(IC コントローラ P)：A64F-00P1-G00-15 」

（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。）が平成 27 年 12 月 11 日に完了した 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コニカミノルタ株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を搭載した製品を導入する組織において、これの管理責任を持つ者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL3 である。

1.1.2 TOEとセキュリティ機能性

本TOEは、コニカミノルタ株式会社製高速印刷用の大型プリンタ機「bizhub PRESS 2250P」（以下「プリンタ機」という。）に搭載され、プリンタ機を制御して印刷の機能を提供する組み込み型ソフトウェアである。本製品は、高速処理能力を求める企業のオフィス等の書類を扱う環境において、ドキュメントデータの入力、蓄積、出力に利用される。

本TOEは、プリンタ機に保存される機密性の高いドキュメントデータの漏洩及び削除を防止する。このため、プリンタ機を利用してドキュメントデータに対してア

クセスを行う一般利用者を識別認証する機能、ドキュメントデータを生成した所有者のみに対してドキュメントデータへのアクセスを許可する、アクセス制御機能を提供する。さらには、管理者とサービスエンジニア（以下、「CE」という。）に対して、識別認証を実施し、認証された管理者とCEに、セキュリティ機能のふるまいに関係する各種設定やユーザBOXパスワードの管理を行うためのセキュリティ管理機能の利用を許可する。これにより、一般利用者がセキュリティ管理機能を不正に操作して、プリンタ機に蓄積された他の一般利用者のドキュメントデータを取り出して意図しない開示や削除を行う脅威から保護する。さらに、製品関係者のTOEに対する操作内容は日時と共に監査ログとして格納され、管理者は不正な操作を検出することができる。

また、ドキュメントデータを保存する媒体であるHDD（ハードディスク装置）にはHDDロック機能を持ったものを採用している。TOEはHDDに対して一定のパスワード規約を満たすHDDロックパスワードを設定し、起動時にHDDロックパスワード認証によりHDDの正当性を確認し、正当性が確認されない場合はHDDに保存されたドキュメントデータに対する機能を使用できないようにする。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本TOEが想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

想定する脅威は、一般利用者が、プリンタ機の操作パネルから TOE の基本機能やセキュリティ機能（セキュリティ管理機能を含む）を使用して、他の一般利用者のドキュメントデータを開示や削除することである。本 TOE は、プリンタ機の一般利用者、管理者及び CE に対して識別と認証を実施し、識別認証された者の役割を確認することで、操作できるドキュメントデータや、使用できるセキュリティ管理機能を制限する。また、TOE は、セキュリティ機能の挙動に関する情報を記録し、管理者へ提供する。これにより、一般利用者によって、他の一般利用者の所有するドキュメントデータが、意図せず開示や削除される脅威に対抗する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、プリンタ機へ搭載され、商用事務製品として企業のオフィス等の環境において使用されることを想定している。

TOE は、製品関係者が立ち入ることができる区画へプリンタ機に搭載された状態で設置され、製品関係者以外は立ち入ることができない。本 TOE が搭載されたプ

リンタ機は、内部ネットワークに接続して、同じネットワークに接続されたクライアント PC から、ドキュメントデータの印刷に使用することができる。この内部ネットワークを外部ネットワークと接続する場合は、外部ネットワークからプリンタ機へ通信ができないように、ネットワークの境界にファイアウォールを接続し、外部ネットワークからプリンタ機に対する通信を遮断するための適切な設定を行う。

責任者としては、プリンタ機を利用する組織の責任を持つ者が想定される。責任者は、TOE の管理者に、信頼できる不正な行為を行わない人物を任命する。CE は、管理者の監視のもと、不正な行為を行わない人物である。管理者と CE は、セキュリティ機能を動作させるために必要な管理者と CE の識別認証機能や、TOE をセキュリティ強化モードに設定する機能を必ず有効に設定し、TOE のセキュアな状態を維持管理しなければならない。

1.1.3 免責事項

本 TOE は、以下の場合において、セキュリティを保証していない。

- プリンタ機に搭載された HDD へ保存された状態以外のドキュメントデータ(以下に例を挙げる)は、保護対象外とする。
  - TOE がドキュメントデータの処理中にプリンタ機の揮発性メモリへ一時的に保存したドキュメントデータ
  - クライアント PC 上や内部ネットワーク上に存在するドキュメントデータ
- 本 TOE は、HDD ロック機能をテストするセキュリティ機能を用いて、本 TOE の要求仕様に適合した HDD ロック機能を持つ HDD がプリンタ機に搭載され、プリンタ機の操作パネルからの操作に対して正しく動作していることを保証する。HDD に実装されている HDD ロック機能の安全性は保証の対象外である。したがって、本 TOE は、プリンタ機から HDD が取り出されて、HDD ロック機能を解除するためのパスワードが抜き取られたり、取り出された HDD からドキュメントデータが読み出されたりする脅威には、対抗しない。
- セキュリティ強化モードが有効でない場合は保証対象外とする。有効にした場合、プリンタ機の一部の機能は使えなくなる。ST の「1.4.3.5. セキュリティ強化機能」を参照のこと。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された

内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 27 年 12 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の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。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： 日本語名：bizhub PRESS 2250P 全体制御ソフトウェア
英語名 ：bizhub PRESS 2250P control software
バージョン： 画像制御プログラム（画像制御 I1）：
A64F0Y0-00I1-G00-15
コントローラ制御プログラム(ICコントローラ P)：
A64F-00P1-G00-15
開発者： コニカミノルタ株式会社

製品が評価･認証を受けた本 TOE であることを、管理者は以下の方法によって確認することができる。

管理者は CE に依頼を行い、CE が本 TOE が搭載されたプリンタ機においてパネルを操作することによって、TOE のバージョンが表示される。これにより、管理者は、設置された製品が評価を受けた本 TOE であることを確認できる。(バージョンのみで TOE の完全な識別となる。)

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、ネットワークまたは USB インタフェースを経由して接続されたクライアント PC からドキュメントデータを受信することにより、TOE が搭載されたプリンタ機内の HDD へドキュメントデータを保管し、印刷による出力を行う。そのため、TOE は、ドキュメントデータの受信と保管、出力の処理に関して、セキュリティ機能を提供する。TOE のセキュリティ機能を以下に説明する。

■ 一般利用者にはそれぞれユーザ BOX が割り当てられる運用が行われることが想定され、TOE は一般利用者をユーザ BOX 識別子とユーザ BOX パスワードにより識別・認証する。その一般利用者へ自分のユーザ BOX 内のドキュメントデータだけを操作する許可を与えることで、一般利用者が、プリンタ機に搭載された HDD へ蓄積された他の一般利用者のユーザ BOX 内のドキュメントデータに対し意図しない開示や削除を行うことを防止する。

一般利用者の識別認証情報（ユーザ BOX 識別子やユーザ BOX パスワード）やセキュリティ機能の使用を安全に管理するために、TOE の管理者と CE に対して識別認証を実施し、認証された管理者には、ユーザ BOX の登録やユーザ BOX パスワードの登録/変更、セキュリティ強化モード等の各種設定の管理が行え、認証された CE には、CE パスワードの登録・変更が行える機能等のセキュリティ管理機能の利用を許可する。これにより、一般利用者がセキュリティ管理機能を不正に操作して、他の一般利用者に成りすましてプリンタ機に蓄積されたドキュメントデータに対し意図しない開示や削除を行う脅威から保護することができる。

■ プリンタ機の一般利用者、管理者及び CE がパスワードを設定する時にパスワード用の文字列の品質を管理する機能を有しており、一般利用者が、識別認証を試行して他の一般利用者、管理者及び CE に成りすます脅威にも対抗している。

■ セキュリティ機能の挙動に関する情報を記録し、管理者へその情報を提供する。これにより、管理者は、不正な操作を検出することができる。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1　想定する脅威

識別子	脅威
T.ACCESS（ユーザBOXへの不正なアクセス）	一般利用者が、操作パネルから、利用者機能を使うことにより、他の一般利用者の所有するユーザBOX内のドキュメントデータに対して権限外の操作（印刷、削除）をされる恐れがある。
T.IMPADMIN（CE、管理者へのなりすまし）	一般利用者が、CE機能インタフェースや管理者機能インタフェースを不正に使用することにより、ドキュメントデータが漏洩及び削除する恐れがある。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.ACCESS」への対抗

一般利用者が、操作パネルから一般利用者向けの機能を使って、他の一般利用者の所有するユーザ BOX 内のドキュメントデータを漏洩させる、または削除する恐れ「T.ACCESS」には、以下の一般利用者の識別認証、利用可能な機能の制限、識別認証情報の管理、監査によって対抗する。

TOE は、TOE の機能を利用しようとする一般利用者に対し、ユーザ BOX 識別子とユーザ BOX パスワードの入力を求める。TOE は、入力されたユーザ BOX 識別子とユーザ BOX パスワードが正当なものであるかどうかを確認する。入力されたユーザBOX識別子とユーザBOXパスワードが事前に登録されたものと一致した一般利用者は、一般利用者が所有するユーザ BOX 内のドキュメントデータに対する操作が許可され、かつ操作パネルから一般利用者向けの機能を使用することが許可されるため、ドキュメントデータの印刷、削除を行うことができる。同様に、識別認証された一般利用者は、所有するユーザ BOX のユーザ BOX パスワードを変更するセキュリティ機能を使用することが許可される。

TOE は、ユーザ BOX パスワードの品質を管理する機能を有しており、パスワード規約に定められた品質（文字数、文字種の構成、パスワードの設定履歴）を満たした文字列だけをパスワードとして設定する。これにより、一般利用者が、識別認証を試行して他の一般利用者が所有するユーザBOXのユーザBOXパスワードを解読し、他の一般利用者に成りすます脅威にも対抗している。

また、TOE は、一般利用者のドキュメントデータの操作のうち、セキュリティ機能に関係する操作を監査情報として監査ログへ記録する。TOE は、この監査ログを管理者へ提供する。したがって、管理者は、監査ログに記録された監査情報を確認することによって、パスワードの総当たり攻撃等の識別認証機能への不正操作や、ドキュメントデータの不正な読み出し、印刷、削除を検出できる。

以上により、TOE の一般利用者は、他の一般利用者の所有するユーザ BOX 内のドキュメントデータを操作できないことから、一般利用者が他の一般利用者の所有するドキュメントデータを漏洩させる、または削除する恐れ「T.ACCESS」は、一般利用者の識別認証、利用可能な機能の制限、監査、識別認証情報の管理によって対抗される。

⑵ 脅威「T.IMPADMIN」への対抗

一般利用者が、管理者や CE へなりすまして、操作パネルから管理者機能や CE 機能を使って、他の一般利用者の所有するユーザ BOX 内のドキュメントデータを漏洩させる、または削除する恐れ「T.IMPADMIN」には、以下の管理者と CE の識別認証、利用可能な機能の制限、識別認証情報の管理、監査によって対抗する。

TOE は、管理者と CE を識別し、管理者と CE に対してパスワードの入力を求める。TOE は、管理者/CE の識別子に対するパスワードが正当なものであるかどうかを確認する。管理者/CE の識別子に対するパスワードが事前に登録されたものと一致した管理者/CE は、操作パネルから各々管理者や CE 向けの管理用の機能や保守用の機能、セキュリティ機能を使用することが許可される。

以下に、管理者と CE の役割と利用が許可されたセキュリティ機能の関係を示す。

1) 管理者向けのセキュリティ機能

管理者は、以下のセキュリティ機能を利用する権限が与えられている。

- セキュリティ強化モードに設定する機能の停止機能
- ユーザ BOX の新規登録、削除機能、ユーザ BOX パスワードの新規登録、変更機能
- 管理者のパスワードの変更機能
- HDD ロック機能用のパスワードの変更機能
- プリンタ機の日時の変更
- 監査ログの出力機能

2) CE 向けのセキュリティ機能

CE には、以下のセキュリティ機能を利用する権限が与えられている。

- CE のパスワードの新規登録、変更機能
- 管理者のパスワードの新規登録、変更機能

TOE は、管理者と CE のパスワードの品質を管理する機能を有しており、パスワード規約に定められた品質（文字数、文字種の構成、パスワードの設定履歴）を満たした文字列だけをパスワードとする。これにより、一般利用者が、識別認証を試行して、管理者や CE のパスワードを解読し、管理者や CE に成りすます脅威にも対抗している。

また、TOE は、管理者と CE 向けのセキュリティ機能が操作されたことを監査情報として監査ログへ記録する。TOE は、この監査ログを管理者へ提供する。したがって、管理者は、監査ログに記録された監査情報を確認することによって、パスワードの総当たり攻撃等の識別認証機能への不正操作や、セキュリティ機能の不正な操作を検出できる。

以上により、TOE の一般利用者が管理者や CE へなりすますことができないことから、一般利用者が操作パネルから管理者機能や CE 機能を悪用して、他の一般利用者の所有するユーザ BOX 内のドキュメントデータを漏洩させる、または削除する恐れ「T.IMPADMIN」は、管理者と CE の識別認証、利用可能な機能の制限、監査、識別認証情報の管理によって対抗される。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 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 3-2 に示す。

表3-2 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.CHECK-HDD （HDDの検証）	TOEは、プリンタ機に搭載されたHDDのHDDロック機能が正しく動作していることを検証する。HDDロック機能用のパスワードの管理機能は、管理者のみに許可する。HDDロック機能用のパスワードは、8～32桁の半角英大文字、半角英小文字、半角数字を満たした文字列を採用する。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.CHECK-HDD」への対応

TOE が搭載されたプリンタ機には、指定された仕様の HDD ロック機能を持つ HDD が複数装備される。TOE は、HDD ロック機能をテストするセキュリティ機能を使用して、HDD1 と HDD2(図 5-1 参照)の HDD ロック機能が有効な状態であり、HDD ロック機能用のパスワードが設定されており、HDD に蓄積されたデータを読み出せないようロックされた状態であることをプリンタ機の起動時に確認する。

TOE は、管理者を識別し、管理者に対してパスワードの入力を求める。TOE は、入力された識別子とパスワードが正当なものであるかどうかを確認する。入力した識別子とパスワードが事前に登録されたものと一致した管理者は、操作パネルから HDD ロック機能用のパスワードを変更する機能を使用できる。

また、そのパスワード変更機能は、パスワードの品質を管理する機能を有している。新しく変更するパスワードは、8～32 桁の半角英大文字、半角英小文字、半角数字を満たした文字列が採用される。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 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4-1　前提条件

識別子	前提条件
ASM.SECMOD （セキュリティ強化モードの設定条件）	TOEの運用中は、管理者がTOEをセキュリティ強化モードに設定する機能を有効にしておく。
ASM.PLACE （TOEの設置条件）	TOEは、製品関係者のみが利用可能な区画へプリンタ機に搭載された状態で設置される。
ASM.NET （内部ネットワークの設置条件）	本TOEが搭載されたプリンタ機を内部ネットワークへ接続し、その内部ネットワークを外部ネットワークと接続する場合は、外部ネットワークからプリンタ機へ通信ができないようにする。 また、プリンタ機のメイン機とサブ機との間には盗聴、改ざん防止対策を実施する。
ASM.ADMIN （信頼できる管理者）	管理者は、不正な行為を行わない人物とする。
ASM.CE （CEの条件）	CEは、管理者の監視のもと、不正な行為を行わない人物とする。
ASM.SECRET （秘密情報に関する運用条件）	管理者のパスワード及びHDDロック機能用のパスワードは、管理者から漏洩しない。CEのパスワードはCEから漏洩しない。ユーザBOXパスワードは、一般利用者自身から漏洩しない。また、各パスワードに対して、推測困難なパスワードが設定される。
ASM.SETTING （セキュリティに関する動作設定条件）	① HDDロック機能の設定を有効に設定する。 ② CEの識別認証機能を有効に設定する。 ③ 管理者の識別認証機能を有効に設定する。

また、TOE に、TOE が規定した品質を満たす管理者と CE のパスワードが設定され、かつ管理者と CE の識別認証機能が有効に設定された状態でなければ、TOE

をセキュリティ強化モードに設定する機能が有効にならない。管理者および CE は、上記の条件を満たすよう TOE を管理し、常に TOE を安全な状態に保たなければならない。

4.2 運用環境と構成

本 TOE は、プリンタ機「bizhub PRESS 2250P」へ搭載されてオフィスに設置される。TOE は、内部ネットワークと接続されて、同じく内部ネットワークに接続されたクライアント PC から利用される場合がある。本 TOE の一般的な運用環境を図 4-1 に示す。

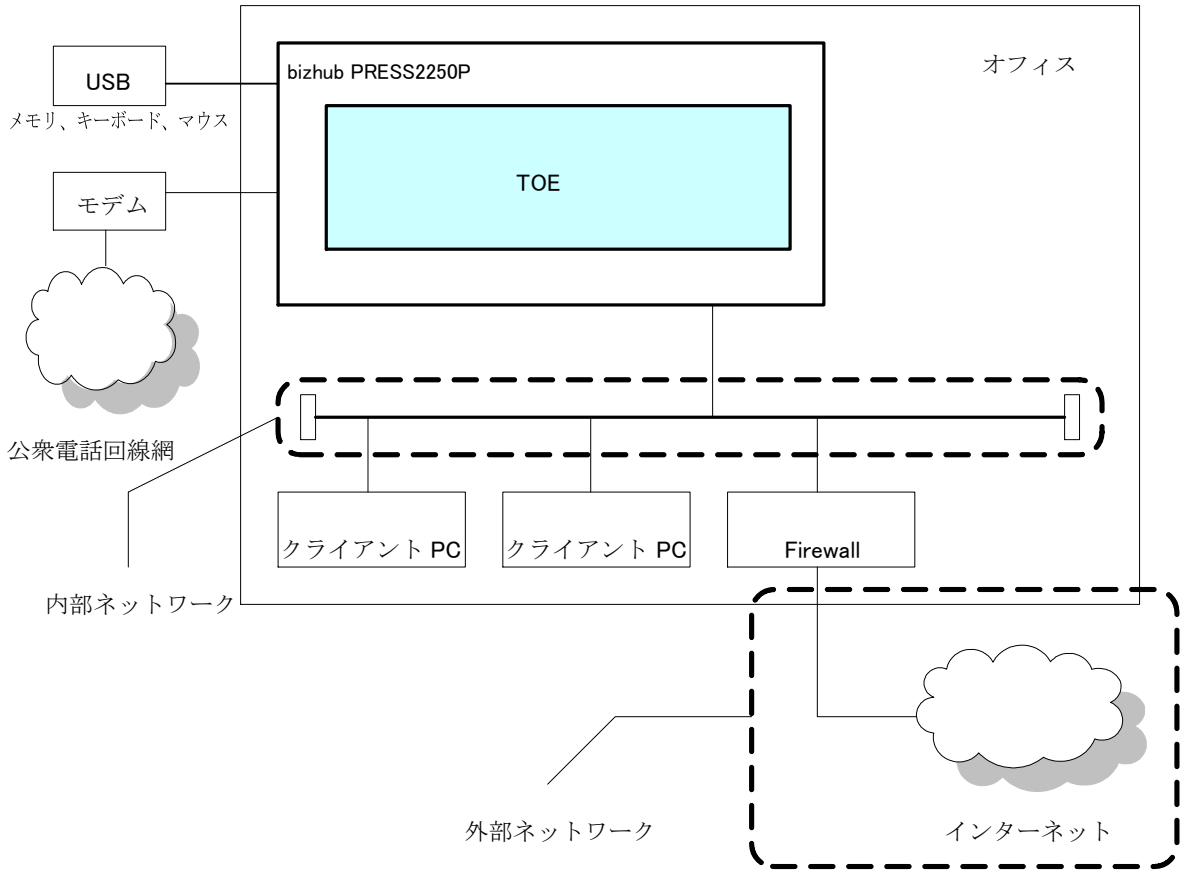

図4-1 TOEの運用環境

本 TOE は、図 4-1 に示すような高速処理能力を求める企業のオフィス等の環境において使用されることを想定している。TOE が搭載されたプリンタ機には、モデムや USB 機器、内部ネットワークが接続される。

TOE をインターネット等の外部ネットワークに接続された内部ネットワークに接続する場合は、ネットワークを通じて、外部ネットワークから TOE へ攻撃が及

ばないように、外部ネットワークと内部ネットワークの境界にファイアウォールを設置して、内部ネットワーク及び TOE を保護する。内部ネットワークにはクライアント PC が接続され、TOE とドキュメントデータ等の通信を行う。

なお、本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではないが、十分に信頼できるものとする。

4.3 運用環境におけるTOE範囲

TOE 範囲は、bizhub PRESS 2250P の全体制御ソフトウェアであり、これは画像制御プログラムとコントローラ制御プログラムと OS から成る。この画像制御プログラムには、基本機能とセキュリティ機能がある

このセキュリティ機能は、指定された仕様の HDD がプリンタ機に正しく搭載された状態で、一般利用者が TOE の機能を悪用して、HDD 上に蓄積された他の一般利用者のユーザ BOX 内のドキュメントデータに対して意図しない開示または削除をおこなう脅威に対抗する。

本 TOE は、プリンタ機へ装備された HDD に対して特定の命令を送信し、同 HDD が備える HDD ロック機能の動作状況の情報を取得する等、HDD に実装された情報保護機能を使用する。しかし、HDD ロック機能及び関連する HDD の情報保護機能は、TOE のセキュリティ機能ではないため、本評価の対象外である。したがって、プリンタ機から HDD を取り出して、HDD ロック機能を解除し、HDD 上に蓄積された情報を読み出す脅威には、対抗しない。

同じくプリンタコントローラ等のプリンタ機のハードウェアも、TOE の範囲外であるため、プリンタ機のハードウェアに関する脅威にも対抗しない。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

プリンタ機はメイン機とサブ機がネットワークインタフェースで接続された構成であり、TOE である全体制御ソフトウェアはメイン機とサブ機それぞれに分散して存在する。

TOE を構成する要素は、図 5-1 と図 5-2 の基本機能と状態管理機能に該当する部分である。それ以外の要素(プリンタ等)は、TOE の範囲ではない。

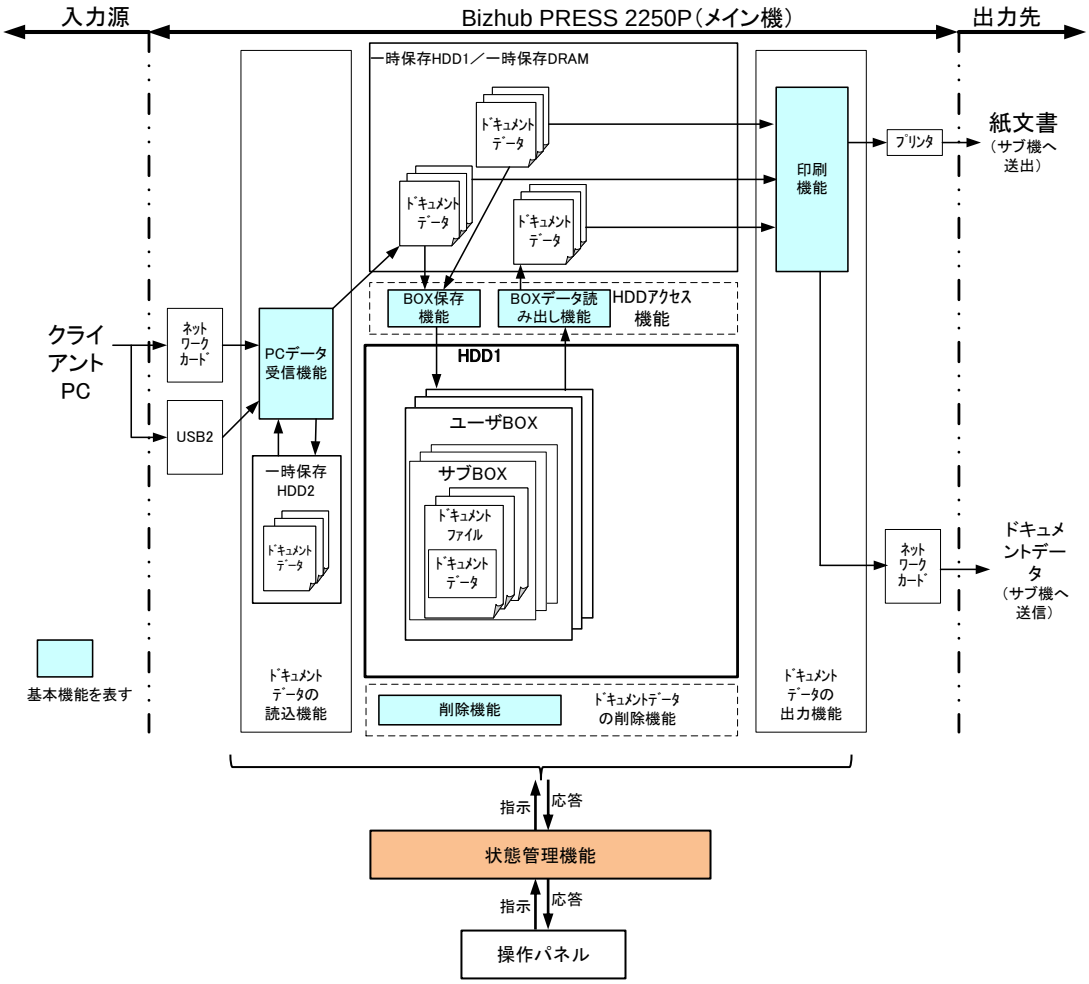

図5-1　TOE境界（メイン機）

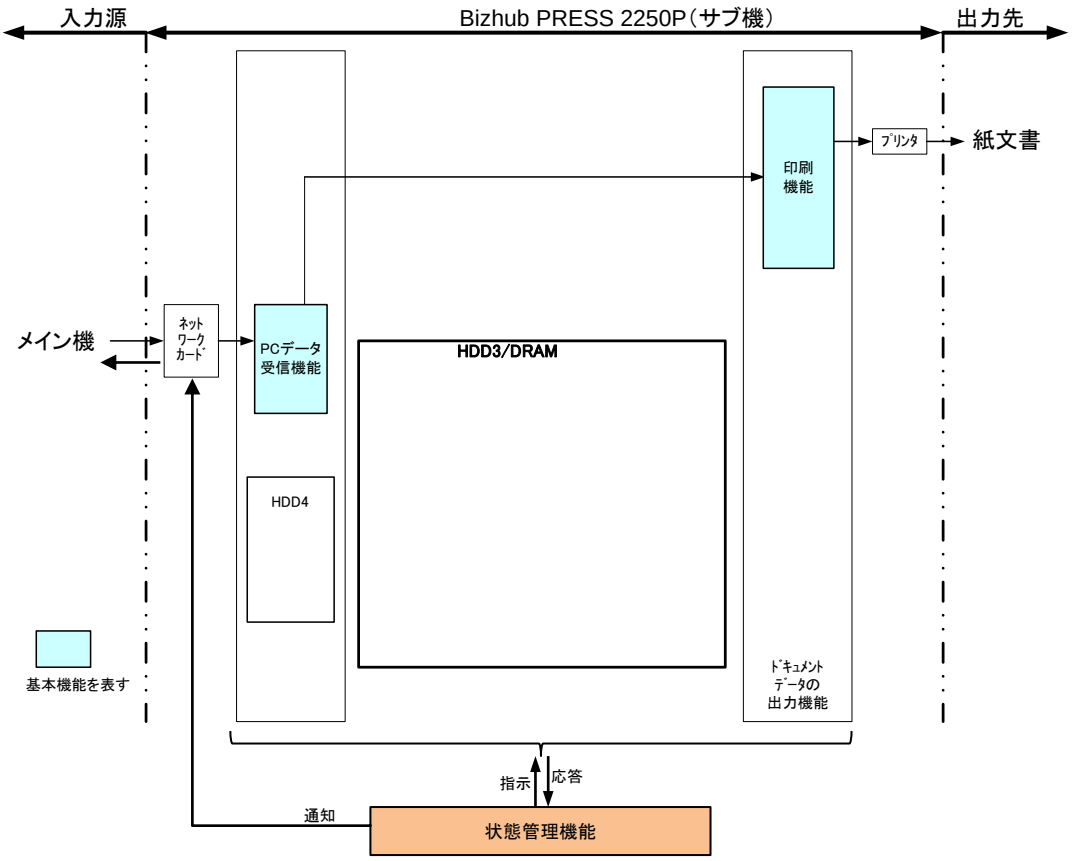

図5-2　TOE境界 (サブ機)

以下、TOE を構成する要素について説明する。

基本機能（メイン機）

1) PCデータ受信機能
クライアントPCから送られてきたドキュメントデータをHDD、またはDRAMに一時保存する機能。

2) BOX保存機能
HDDに一時保存されたドキュメントデータを、ユーザBOXに保存する機能。

3) BOXデータ読み出し機能
ユーザBOXに保存されたドキュメントデータを読み出す機能。

4) 印刷機能
HDDまたは、DRAMに一時保存されたドキュメントデータを、メイン機で印刷、またはサブ機に印刷指示する機能。

5) 削除機能
ユーザBOXに保存されたドキュメントデータを削除する機能。

基本機能（サブ機）

1) PCデータ受信機能
メイン機から送られてきたデータを印刷機能に送る機能。

2) 印刷機能
PCデータ受信機能から送られたデータを印刷する機能。

3) 状態管理機能
サブ機の状態を監視しメイン機へ通知や印刷機能への指示をする機能。

セキュリティ機能（セキュリティ機能は主にメイン機の状態管理機能が実施する）

1) 識別認証機能
ユーザBOX識別子とユーザBOXパスワードを使って一般利用者の識別認証を行う。識別認証が成功すると、一般利用者に対してユーザBOXパスワードの変更、及び、保存されたドキュメントデータへのアクセスを許可する。

2) アクセス制御機能
保存されたドキュメントデータへアクセス可能な利用者を制限することができる。アクセス制御機能により、認証された正当な一般利用者のみ自身のユーザBOX内のドキュメントデータの読み出しが可能である。

3) 監査機能
セキュリティ機能の挙動に関する監査証跡を1000件記録することができる。監査対象事象が発生した場合に、操作が発生した日時（年月日時分秒）、操作の内容を監査ログとして生成する。

4) 管理者機能
識別認証された管理者へ、以下の管理用の機能を提供する。
- セキュリティ強化モードに設定する機能の停止機能
- ユーザBOXの登録、ユーザBOXパスワードの登録/変更機能
- 管理者のパスワードの変更機能
- HDDロック機能用のパスワードの変更機能
- 監査ログの出力機能

5) CE機能
識別認証されたCEへ、以下の管理用の機能を提供する。
- CEのパスワードの新規登録、変更機能
- 管理者のパスワードの新規登録、変更機能

6) HDDロック機能をテストするセキュリティ機能
   - TOEの要求仕様に適合したHDDロック機能を持つHDDがプリンタ機に搭載されていることを検査する。
   - プリンタ機起動時にHDDがロックされていること検査する。
   - HDDロック機能用のパスワードを送信し、HDDロック機能が解除されたことを確認する。

5.2 IT環境

TOE が搭載されたプリンタ機は内部ネットワークに接続され、TOE はクライアント PC とドキュメントデータ等を通信する。TOE は、コニカミノルタ株式会社が指定した装置と、RS232C インタフェースによって接続されたモデムを介して、印刷枚数、ジャム回数、トナー切れ等のハードウェア保守に関する情報を通信する。

6 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。

(日本向けドキュメント)

- bizhub PRESS 2250P ユーザーズガイド セキュリティー機能編 Ver.1.2

(海外向けドキュメント)

- bizhub PRESS 2250P User's Guide Security Operations Ver.1.2

(補足) 本 TOE に添付されるドキュメントではないが、CE 向けのドキュメントとしてサービスマニュアルがある。CE 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。

(日本向けドキュメント)

- bizhub PRESS 2250P サービスマニュアル セキュリティー機能編 Ver.1.4

(海外向けドキュメント)

- bizhub PRESS 2250P SERVICE MANUAL SECURITY FUNCTION Ver.1.4

■ 日本語版と英語版の違いについて

本章に記載したドキュメントには、日本向けの日本語版と、海外向けの英語版の 2 種類が存在する。ただし、英語版は、日本語版の正確な翻訳として作成されており、日本語版と英語版の内容は同一である。

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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た。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 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 26 年 4 月に始まり、平成 27 年 12 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 26 年 10 月、平成 27 年 1 月、2 月、及び 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・開発セキュリティ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 27 年 6 月及び 9 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、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(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 7-1 に示す。

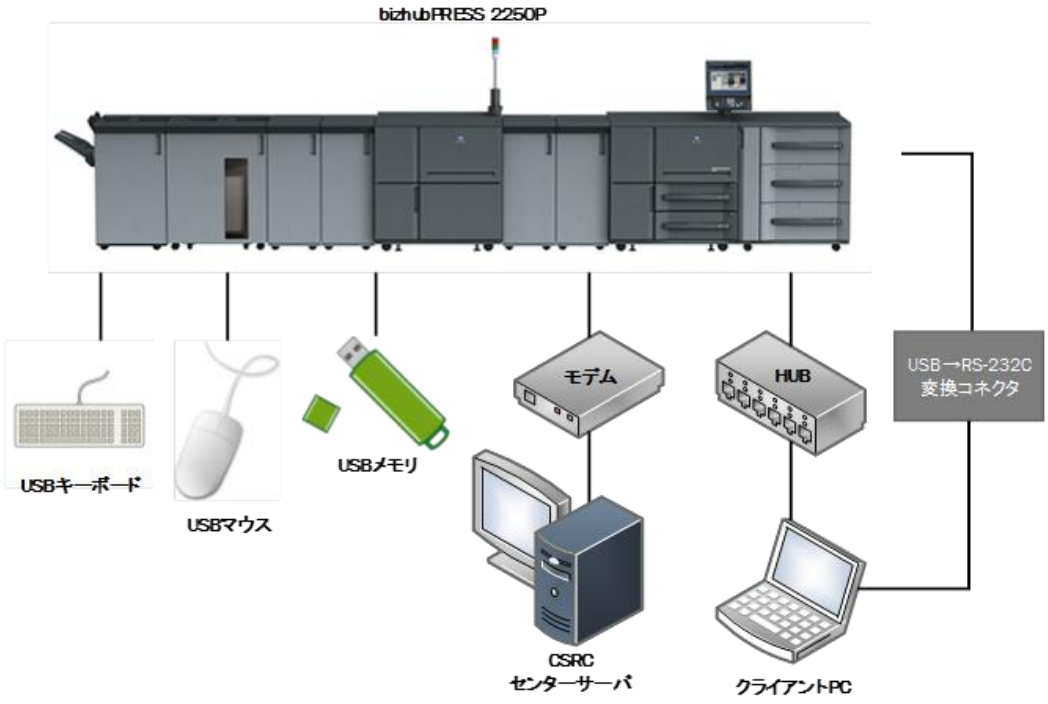

図7-1　開発者テストの構成図

開発者テストの構成における TOE 以外の構成要素について、表 7-1 に説明する。

表7-1　開発者テストの構成要素

構成要素	詳細
bizhub PRESS 2250P 本体	テスト対象となるプリンタ機である。 また、搭載するファームウェアのバージョンが、評価対象の以下の通りであることが明記されている。 ・画像制御プログラム： A64F0Y0-00I1-G00-15 ・コントローラ制御プログラム： A64F-00P1-G00-15
クライアントPC	OS： Windows7 Professional SP1 (64ビット)
ネットワーク	100BASE-T 規格
プリンタドライバ	プリンタコントローラへの印刷用にKONICA MINOLTA bizhub PRESS 2250P PSドライバVersion 1.0.319 を利用することが示されている。
モデム	電話回線用のモデム。プリンタ機の電話回線経由でのCSRCセンターテスト時の、CSRCセンターサーバとの接続に使用する。
CSRCセンターサーバ	CSRCのセンターソフトウェア Ver. 2.8.1が動作するPC。
USBメモリ	TOE更新機能のテストに利用する。
USBキーボード	操作パネルの代わりにプリンタ機を操作する手段として利用する。
USBマウス	操作パネルによる操作の補助としてプリンタ機を操作する手段として利用する。

図7-1と表7-1に示すこの構成は、TOEを搭載するプリンタ機へすべての装置を装着、接続した構成であり、TOEのすべての機能をテストできる。

したがって、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。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

開発者テストは、想定されるTOEの利用方法（操作パネルの操作、内部ネットワークで接続されたクライアントPCの操作）に基づいて、TOEの外部インタフェースを刺激し、その結果をパネル上から目視観察する方法が採られた。ただし、想定されるTOEの利用方法ではインタフェースの刺激が困難な場合や、テスト結果を操作パネル上から目視観察できない場合は、以下の手法が採られた。

- 監査ログ機能は、監査情報を記録する事象が発生する操作を実施した後、監査ログを出力し、その監査ログの記録内容を確認した。
- netcatやostinatoを利用して異常な通信データを生成し、TOEに送信した。Wiresharkを利用して、TOEの応答を確認した。
- 印刷のためにTOEに送信するデータをStirlingを使用して改変し、TOEに送信してふるまいを観察した。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-2 に示す。

表7-2　開発テストツール

ツール名称	概要・利用目的
USB→RS232C 変換コネクタ	クライアントPCからTOEの内部的なふるまいを観察するために使用。
Wireshark (Version 1.6.7)	LAN上の通信データをモニタし、解析するツール。 LAN上でTOEの応答を観察するために使用。
netcat (Version 1.11)	TCP,UDPパケットを読み書きするためのツール。 異常な通信データを送信するために使用。
ostinato (Version 0.7.1)	TCP,UDPパケットを送信するためのツール。 異常な通信データを送信するために使用。
Stirling (Version 1.31)	バイナリエディタ。 印刷のために送信するデータを改変するために使用。

＜開発者テストの実施＞

開発者が提供したテスト証拠資料に記載されたあらかじめ期待されたテスト計画書の値と開発者テストの結果の値を比較した。その結果、期待されるテスト結果とテスト証拠資料の実際のテスト結果が一貫していることが確認できた。

b) **開発者テストの実施範囲**

開発者テストは開発者によって66項目実施された。カバレージ分析によって、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た。深さ分析によって、TOE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た。

c) **結果**

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価の対象としたTOEは、「bizhub PRESS 2250P 全体制御ソフトウェア」である。TOEが搭載されるプリンタ機は「bizhub PRESS 2250P」であり、テスト環境は開発者テストと同じ構成とした。 この構成は、TOEを搭載するプリンタ機へすべての装置を装着、接続した構成であり、TOEのすべての機能をテストでき、TOEのセキュリティ機能のふるまいに影響がないことから、評価者独立テストの構成として問題ないと判断した。

テスト環境やテストツールは、開発者テストに用いられたものを利用しているが、これらの仕様確認及び動作試験と校正は評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) **独立テストの観点**

＜評価者が考案したテスト＞

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点に

基づいてテスト8項目を考案した。

(観点1) 複数の機能から操作できる設定(特にセキュリティ強化モードに関係するもの)において、矛盾が生じるような操作ができないかどうかについて開発者テストに対して厳密さを補完する。
(観点2) 特に確率的・順列的メカニズムに関係するものを対象とすることを考慮し、文字桁数及び文字種類の観点で、開発者テストに対して厳密さを補完する。
(観点3) 役割の違い(一般利用者、管理者、CE)、パラメタや動作の状況の違いの観点で、開発者テストに対して厳密さを補完する。

＜サンプリングテスト＞

開発者テストからのサンプリングテストは、テスト対象のセキュリティ機能とインタフェースのテストをカバーし、かつ以下の観点も考慮し、26項目を選択した。

・ セキュリティ機能の網羅性
すべてのセキュリティ機能をテストの対象とする。
特に、シリーズ機種と異なる、プリンタ機がメイン機とサブ機から構成されることに関連する機能、及び、HDDロックパスワードの機能に関しても、テスト対象として考慮する。
・ 入力デバイスの網羅性
操作パネル、電源、コントローラ経由など、各種の外部インタフェースの起動先をテストの対象とする。
・ テスト手法の網羅性
パネル操作、HDD脱着、出力監査ログの確認などのすべてのテスト手法を対象とする。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

評価者は、開発者テストと同様のテスト手法に基づいて独立テスト手順書を作成し、評価者が考案したテストを以下のような方法で実施した。

・ 操作パネルのみを用いたテスト
例えば、操作パネルから、定められていない文字種を入力した場合の開発者テストは、操作パネルから開発者テストで実施されなかった文字列を入力し、テスト結果を操作パネルの表示から確認する。

・操作パネル以外からテスト結果を確認するテスト
例えば、操作パネルから監査情報を記録する事象が発生する操作を実施し、監査情報が記録された監査ログを印刷し、その記録内容を確認する。また、ネットワークアクセスの制限を確認するため、クライアントPCからのアクセスに対する応答を確認する。

サンプリングテストは、開発者テストと同様のテスト手法により実施された。

＜独立テストツール＞

開発者テストと同じツールを用いた。

＜独立テストの実施内容＞

独立テストの観点とそれに対応したテスト内容を表 7-3 に示す。

表7-3 実施した独立テスト

名称	テスト内容
CEのパスワードの変更機能テスト(観点2)	CEのみがCEのパスワードを変更できること。定められた品質を満たした文字列だけをパスワードとして設定すること。
CEによる管理者のパスワードの変更機能テスト(観点2)	CEのみが管理者のパスワードを変更できること。
管理者による管理者のパスワードの変更機能テスト(観点2)	管理者のみが管理者自身のパスワードを変更できること。定められた品質を満たした文字列だけをパスワードとして設定すること。
管理者によるユーザBOXパスワードの変更機能テスト(観点2)	管理者のみがユーザBOXのパスワードを変更できること。定められた品質を満たした文字列だけをパスワードとして設定すること。
HDDロック機能用のパスワードの変更機能テスト(観点2)	管理者のみがHDDロック機能用のパスワードを変更できること。定められた品質を満たした文字列だけをパスワードとして設定すること。
監査ログ出力機能テスト(観点3)	日時を戻した後も監査ログは、事象発生順に記録され確認できること。
ドキュメントデータ保存テスト(観点3)	ドキュメントデータの保存機能が正しく動作すること。

名称	テスト内容
セキュリティ強化モード時の強化機能の設定確認テスト(観点1)	TOEがセキュリティ強化モードに設定された状態において、CE認証機能等のTOEのセキュリティを強化する設定が変更できないこと。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。（脆弱性情報（CVN、JVN等）の調査により発見されたOS、ライブラリ等に関する公知の脆弱性は、想定する攻撃能力を持つ攻撃者が悪用可能ではないことが評価者の分析により確認されたため、以下には含まれていない。）

表7-4　懸念される脆弱性

項番	懸念される脆弱性の内容	脆弱性の観点
VLA-T1	TOEのネットワークインタフェースに使用しないネットワークポートが存在する。	侵入検査
VLA-T2	telnet等の命令が手入力可能なインタフェースを持つ通信サービスのネットワークポートがTOEのネットワークインタフェースに存在し、命令が実行できる。	侵入検査
VLA-T3	使用しないネットワークポートがTOEのネットワークインタフェースに存在し、TOE以外からの通信を受信して、その通信内容に応じた処理が行われる場合、その通信の処理に関する脆弱性が悪用される。	侵入検査 公知の脆弱性

項番	懸念される脆弱性の内容	脆弱性の観点
VLA-T4	パスワード用の文字列として定められた文字種以外のパスワードが設定できる。	バイパス 直接攻撃
VLA-T5	セキュリティ機能の動作中に意図しない操作を行うことによって、セキュリティ機能がバイパスされたり、改ざんされたりして、TOEのセキュリティ機能が正しく動作しない状態になる。	バイパス 改ざん 誤使用
VLA-T6	USBを使用したTOEの更新機能が悪用される。	改ざん
VLA-T7	プリンタコントローラ経由で不正なデータを受信したときに、TOE が意図しない動作を行い、TOE のセキュリティ機能が損なわれる。	改ざん
VLA-T8	監査ログ領域は有限であり、不正アクセス行為を隠蔽するために、意味の無いジョブ等で容易に監査ログを満杯にできる。	改ざん

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者が実施した侵入テストの構成を図 7-2 に示す。

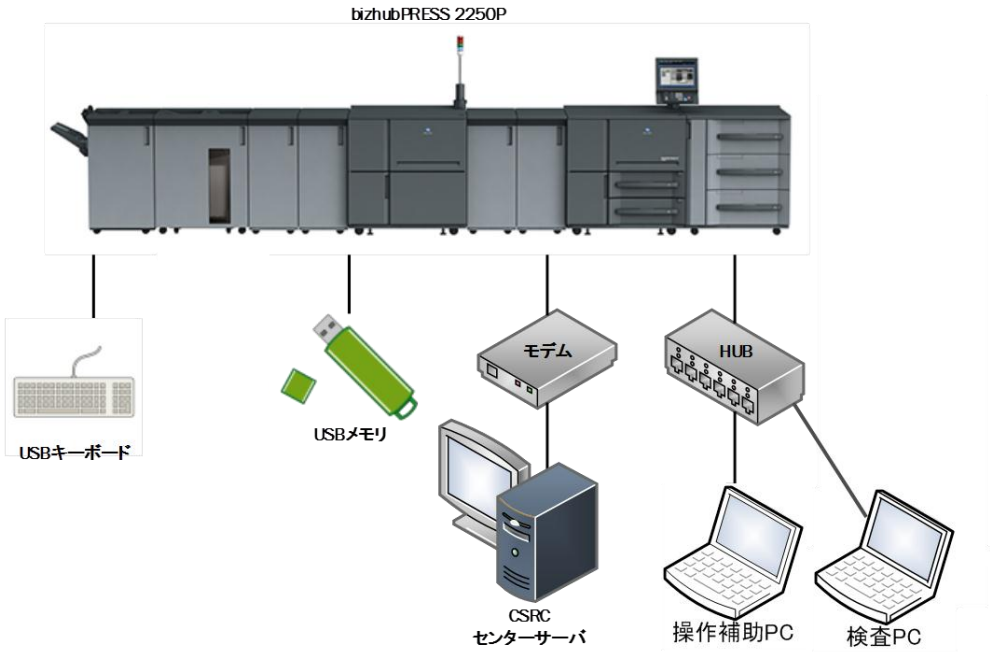

図7-2　侵入テスト環境

評価者侵入テストの構成（図7-2）は、以下の点で開発者テストの構成（図7-1）と異なる。(操作補助PCは、開発者テストのクライアントPCと同じソフトウェアを導入している。)

- USBマウス、USB-RS232Cコネクタは、TOEの動作に必須ではなく、侵入テストでは利用しないため接続していない。
- 侵入テストのためのツールを動作させるために検査PCを接続している。

検査PCで侵入テストのためのツールを動作させてTOEのふるまいを確認するための環境としてこの構成が適切であることが、評価者により判断されている。

評価者侵入テストの環境において使用したツールを表7-5に示す。これらのツールが侵入テストに適した動作をすることは評価者により検証されている。

表7-5　評価者侵入テストツール

ツール名称	概要・利用目的
Nessus	バージョン：6.3.7 ネットワークポートの調査に使用する。
BZ	バージョン：1.62 バイナリエディタ。侵入テスト用の正規版とは異なるTOE を作成するために使用する。
Nmap	バージョン：6.47 システム上のポートを検査するセキュリティスキャナ
extrstr	バージョン：0.2 みずほ情報総研が開発したバイナリ解析ツール。GNU binutils を活用して、バイナリから印刷可能な文字列を抽出して、集計する。
OpenSSL	バージョン：0.9.8zg ハッシュ関数や暗号化・復号ソフトウェアツール。 ネットワークサービスのうち、SSL のポートへの接続を試みるために使用する。
pjlftp	PJL(印刷のジョブに使われる言語)のコマンドを送信するソフトウェア。 不正なデータを含むドキュメントデータを送信するために使用する。

＜侵入テストの実施＞

潜在的な脆弱性の探索において識別された表7-4の懸念される脆弱性について、これと対応する評価者侵入テストを表7-6に示す。評価者は、潜在的な脆弱性が悪用される可能性の有無を決定するため、以下の評価者侵入テストを実施した。

表7-6　侵入テスト概要

項番	テスト概要	懸念される脆弱性の項番
1	検査PCからNessusを使用して、TOEが使用しているネットワークポートを調査する。	VLA-T1
2	検査PCから、ネットワークサービスの一般的なコマンドを実行して、ドキュメントデータを取り出せないことを調査する。	VLA-T2
3	検査PCからNessusを使用して公知の脆弱性を調査する。	VLA-T3
4	パスワードを変更する時に、パスワード用の文字列の品質を満たさない文字列が設定できないことを確認する。	VLA-T4
5	セキュリティ機能の動作中に意図しない操作を行っても、再びTOEが動作した時にTOEのセキュリティ機能が正常に機能することを確認する。	VLA-T5
6	侵入テスト用に作成したTOEをUSBメモリ経由で更新する。	VLA-T6
7	操作補助PCから、不正なデータを含むドキュメントデータを印刷する。	VLA-T7
8	監査ログ領域満杯に要する時間を確認する。	VLA-T8

c) 結果

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本評価では、「7.4.2 評価者独立テスト」及び図7-2に示す構成において、評価を行った。本TOEは、上記と構成要素が大きく異なる構成において、運用される場合はない。

ただし、TOEは、必ずセキュリティ強化モードに設定する機能を有効にした状態で運用しなければならない。そのため、本評価では、以下に示す設定を有効にした状態において、テストを実施した。

- CE の識別認証、管理者の識別認証に使用するパスワードは、定められた品質を満たした文字を設定する。
- CE の識別認証機能を有効にする。
- 管理者の識別認証機能を有効にする。
- TOE をセキュリティ強化モードに設定する機能を有効にする。

よって、評価者は、上記の評価構成は、適切であると判断した。

7.6 評価結果

評価者は、評価報告書をもって本 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。

評価では以下について確認された。

- PP 適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート 2 適合
- セキュリティ保証要件：　コモンクライテリア　パート 3 適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL3 パッケージのすべての保証コンポーネント

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

HDD ロック機能に関しては、専用機器や解読サービスにより破ることが容易になってきていることが評価者によりコメントされている。

プリンタ機の廃棄後や返却後に HDD から情報が漏洩するリスクを検討する場合は、このコメントも考慮した注意が必要である。

8 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 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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、本 ST 及び評価報告書において、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、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、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すものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価対象範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

bizhub PRESS 2250P セキュリティターゲット バージョン 1.14　2015 年 10 月 13 日　コニカミノルタ株式会社

このセキュリティターゲットの名称はプリンタ機全体のセキュリティターゲットであるような名称となっているが、TOE はプリンタ機全体ではなくプリンタ機の一部の制御ソフトウェアである。

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

CE	サービスエンジニアのことで、プリンタ機の保守作業を行う者。
HDD	ハードディスクドライブの略称。TOE内に取り付けられたHDDを指す。
USB	Universal Serial Busの略で、コンピュータにさまざまな周辺機器を接続するためのシリアルバス規格の1つである。

本報告書で使用された用語の定義を以下に示す。

CSRC	CS Remote Care機能を実現するアプリケーションである。プリンタ機でトラブルなどが発生した際に、サービス拠点に存在するセンタターミナルPCへ通知するとともに、センタターミナルPCからの要求に応じてカウンタ情報などを通知する。 セキュリティ強化モードが有効化されている場合はRS232Cインタフェース（モデム）経由での利用のみ許可される。
HDDロック機能	ATA規格で定められたHDDのセキュリティ機能の一つ
Nessus	調査対象のネットワークインタフェースに存在するネットワークポートを調査し、そのポートを利用して、調査対象上に存在する脆弱性を検査する脆弱性スキャナと呼ばれるツール
外部ネットワーク	プリンタ機が設置されている組織が管理できないネットワーク。一般的には汎用インターネットのことを指す。
監査ログ	監査情報を記録したもの

初期化 (TSFのセキュアな初期化)	製品を起動してから製品が運用状態になるまでの初期化処理を対象として、その間にもセキュリティの侵害を防止して、セキュリティ機能が完全な状態で初期化され運用状態に至ることを保証するしくみ
製品関係者	一般利用者、管理者、責任者、及びCEのことを指す。
セキュリティ強化モード	TOEのセキュリティを強化した状態。TOEをセキュリティ強化モードに設定する機能を用いて設定する。
操作パネル	タッチパネル付き液晶ディスプレイ、物理的なキー／ボタン、表示ランプ等で構成され、利用者がプリンタ機の操作に利用する表示入力装置。
ドキュメントデータ	紙文書をスキャナ装置から取り込んでプリンタ機内に保存するために変換したデータや、クライアントPCから送信された文書のデータ
内部ネットワーク	プリンタ機が設置されている組織が管理するネットワーク。通常はイントラネットとして構築されているオフィス内LAN環境のこと。
ネットワークサービス	Webサービスや電子メール、遠隔ログインサービスなど、離れた所からネットワークを経由して利用できるサービス
ネットワークポート	ネットワーク通信を行うときに、送信先や送信元のサービスやプログラムを特定するために使用する番号
プリンタコントローラ	PCからの受信データを紙に印刷するためのデータ変換を行う処理部

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[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2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11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3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] bizhub PRESS 2250P セキュリティターゲット バージョン 1.14　2015年10月13日　コニカミノルタ株式会社

[13] bizhub PRESS 2250P 全体制御ソフトウェア 評価報告書, 第2版 (131200-01-R003-02), 2015年12月11日, みずほ情報総研株式会社 情報セキュリティ評価室