



認証報告書

独立行政法人情報処理推進機構
理事長 藤江 一正

原紙
押印済

評価対象

| | |
|-------------|---|
| 申請受付日（受付番号） | 平成24年1月4日（IT認証2391） |
| 認証番号 | C0368 |
| 認証申請者 | コニカミノルタビジネステクノロジーズ株式会社 |
| TOEの名称 | 日本語名：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア 英語名：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 control software |
| TOEのバージョン | 画像制御プログラム（画像制御 I1）：A4EU0Y0-00I1-G00-15 コントローラ制御プログラム（ICコントローラ P）： A4E-00P1-G00-15 |
| PP適合 | なし |
| 適合する保証パッケージ | EAL3 |
| 開発者 | コニカミノルタビジネステクノロジーズ株式会社 |
| 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24年8月30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3
- 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3

評価結果：合格

日本：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 /

ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア 英語名 : bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 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 | 評価対象製品概要 | 1 |
| 1.1.1 | 保証パッケージ | 1 |
| 1.1.2 | TOEとセキュリティ機能性 | 1 |
| 1.1.2.1 | 脅威とセキュリティ対策方針 | 2 |
| 1.1.2.2 | 構成要件と前提条件 | 2 |
| 1.1.3 | 免責事項 | 3 |
| 1.2 | 評価の実施 | 3 |
| 1.3 | 評価の認証 | 4 |
| 2 | TOE識別 | 4 |
| 3 | セキュリティ方針 | 5 |
| 3.1 | セキュリティ機能方針 | 5 |
| 3.1.1 | 脅威とセキュリティ機能方針 | 5 |
| 3.1.1.1 | 脅威 | 5 |
| 3.1.1.2 | 脅威に対するセキュリティ機能方針 | 6 |
| 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 | 8 |
| 3.1.2.1 | 組織のセキュリティ方針 | 8 |
| 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 | 8 |
| 4 | 前提条件と使用環境 | 10 |
| 4.1 | 使用及び環境に関する前提条件 | 10 |
| 4.2 | 使用環境と構成 | 11 |
| 4.3 | 使用環境におけるTOE範囲 | 12 |
| 5 | アーキテクチャに関する情報 | 13 |
| 5.1 | TOE境界とコンポーネント構成 | 13 |
| 5.2 | IT環境 | 15 |
| 6 | 製品添付ドキュメント | 16 |
| 7 | 評価機関による評価実施及び結果 | 18 |
| 7.1 | 評価方法 | 18 |
| 7.2 | 評価実施概要 | 18 |
| 7.3 | 製品テスト | 19 |
| 7.3.1 | 開発者テスト | 19 |
| 7.3.2 | 評価者独立テスト | 22 |
| 7.3.3 | 評価者侵入テスト | 26 |
| 7.4 | 評価構成について | 30 |
| 7.5 | 評価結果 | 30 |
| 7.6 | 評価者コメント/勧告 | 31 |

| | | |
|-----|-------------------|----|
| 8 | 認証実施 | 32 |
| 8.1 | 認証結果..... | 32 |
| 8.2 | 注意事項..... | 32 |
| 9 | 附属書..... | 33 |
| 10 | セキュリティターゲット | 33 |
| 11 | 用語 | 34 |
| 12 | 参照 | 37 |

1 全体要約

この認証報告書は、コニカミノルタビジネステクノロジーズ株式会社が開発した「日本語名：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア 英語名：bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 control software全体制御ソフトウェア、バージョン 画像制御プログラム（画像制御 I1）：A4EU0Y0-00I1-G00-15 コントローラ制御プログラム(ICコントローラ P)：A4E-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24年8月8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ビジネステクノロジーズ株式会社に報告するとともに、本TOEに関心を持つ消費者や調達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、コニカミノルタビジネステクノロジーズ株式会社製高速印刷用の大型デジタル複合機「bizhub PRESS 1250シリーズ」（以下「MFP」という。）に搭載され、MFPを制御してコピーや印刷、スキャン等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、文書データの入力、蓄積、出力に利用される。

本TOEは、MFPに保存される機密性の高いドキュメントデータの漏洩を防止する。このため、ドキュメントデータを保護するユーザBOX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、MFP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MFP本体の動作を停止する。

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、MFP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、他の一般利用者のユーザBOX内のドキュメントデータを開示することである。本TOEは、MFP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している。

本TOEは、MFP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、MFPの利用を許可された一般利用者、管理者やCEが立ち入ることができる区画へMFPへ搭載された状態で設置され、一般利用者、管理者及びCE以外は立ち入ることができない。本TOEが搭載されたMFP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MFP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MFPに対する通信を遮断するための適切な設定を行う。

TOEの管理者には、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状態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。

- MFP に搭載された HDD へ保存された状態以外の文書データは、保護対象外とする。
 - TOE がドキュメントデータの処理中に MFP 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（揮発性メモリへ一時的に保存されたドキュメントデータを外部へ読み出すには、非常に高度な技術が必要である。また、電源 OFF により揮発性メモリのドキュメントデータは消去されるため、一般利用者がドキュメントデータを読み出す脅威は低いと判断する。
 - MFP から、MFP 外へ送信されたドキュメントデータ（Scan to Email 機能、Scan to FTP 機能、Scan to PC(SMB)機能によって、送信されたドキュメントデータ）
 - プリンタコントローラの HDD へ保存されたドキュメントデータ
（クライアント PC からプリンタコントローラへ送信されたドキュメントデータ、MFP からプリンタコントローラへ送信され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文書データ
 - 紙で所有している文書データ
- 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 MFP に搭載され、MFP 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、MFP 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。

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セキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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24年8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、本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 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア
英語名： bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 control software

バージョン： 画像制御プログラム (画像制御 I1) : A4EU0Y0-00I1-G00-15
コントローラ制御プログラム(ICコントローラ P) :
A4E-00P1-G00-15

開発者： コニカミノルタビジネステクノロジー株式会社

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MFPにおいてパネルを操作することによって、TOEの名称、及び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。

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、一般利用者の紙文書を取り込んだり、ネットワークを經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したりして、TOEが搭載されたMFP内のHDDへドキュメントデータを保管し、印刷、配布による出力を行う。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。

- MFPの一般利用者を識別認証し、その利用者へ自分の所有する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、MFP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を取り出して意図しない開示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識別子やパスワード等)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MFPに蓄積されたドキュメントデータを取り出し、意図しない開示を行う脅威から保護することができる。
- MFP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に成りすまず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への不正な操作) | 一般利用者が、操作パネルから利用者向けの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を漏洩させる恐れがある。 |
| T.IMPADMIN (CE、管理者へのなりすまし) | 一般利用者が、CE機能のインタフェースや管理者機能のインタフェースを不正に使用することにより、ユーザBOX内のドキュメントデータが漏洩する恐れがある |

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ドキュメントデータを漏洩させる恐れ「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保管、印刷、配布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、一般利用者自身の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、MFPの一般利用者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のパスワードを解読し、他の一般利用者になりすます脅威にも対抗している。

また、TOEは、一般利用者のユーザBOX内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や印刷を検出できる。

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。

(2) 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ドキュメントデータを漏洩させる恐れ「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。

- セキュリティ強化状態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

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、ユーザBOX内の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の利用にあ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、MFP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MFPには、指定された仕様のHDDロック機能を持つHDDが追加装備される。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、同HDD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MFP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状態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、一般利用者、管理者及びCEが利用可能な区画へMFPへ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MFP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MFPへ通信ができないようにする。 |
| 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、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、管理者から漏えいしない。CEのパスワードはCEから漏えいしない。ユーザBOXパスワードは、一般利用者自身から漏えいしない。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) | <ul style="list-style-type: none"> • 管理者は、HDDロック機能を有効に設定する。 • CEの識別認証機能を有効に設定する。 • 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状態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。

い。

4.2 運用環境と構成

本TOEは、MFP「bizhub PRESS 1250シリーズ」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。

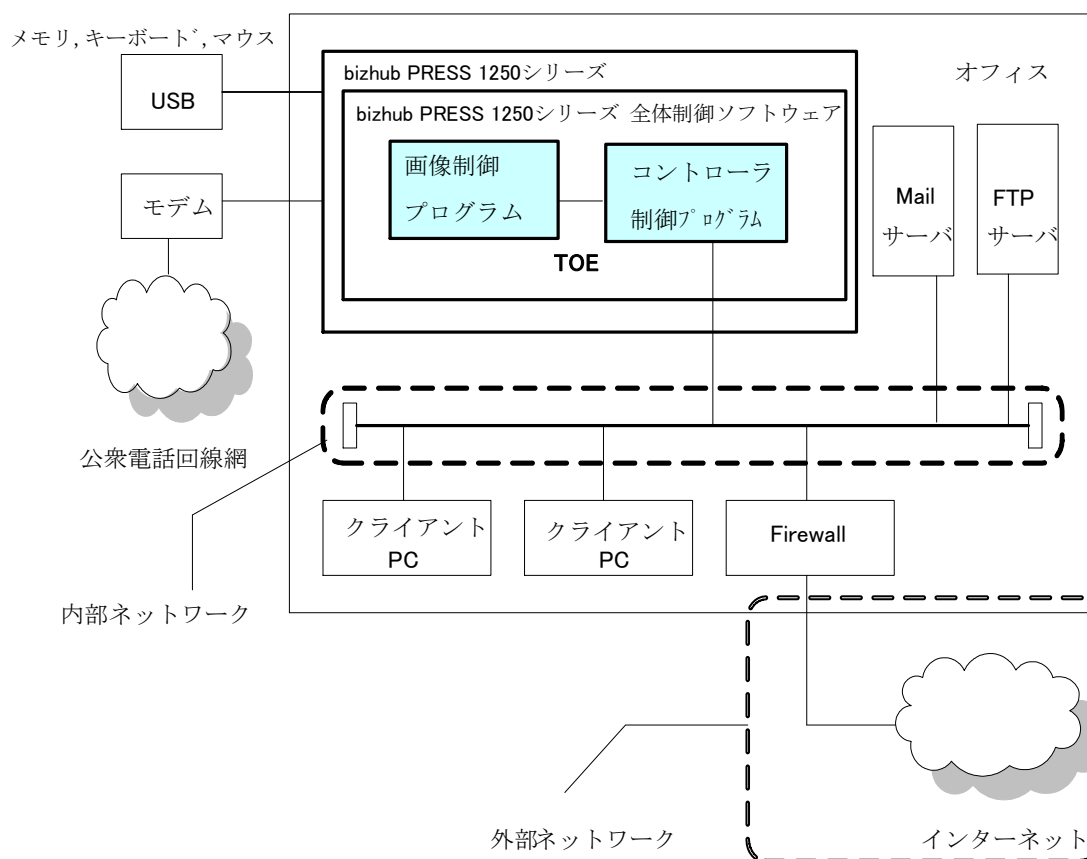


図4-1 TOEの運用環境

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MFP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、FTPサーバ、Mailサーバ等のサーバコンピュータ、及びクライアントPCが接続され、TOEとドキュメントデータ等の通信を行う。

TOEの操作は、MFPの操作パネルを使用する。プリンタ機能を使用して印刷する場合は、クライアントPCから内部ネットワークを経由してプリンタコントローラヘッドキュメントデータを送信し、プリンタコントローラがTOEヘッドキュメントデータを送信する。

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 1250シリーズ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MFP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を取り出して、意図しない開示をおこなう脅威に対抗する。

本TOEは、MFP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、MFP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も、TOEの範囲外であるため、プリンタコントローラ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）について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

TOEを構成する要素、及びTOEが動作するために必要なMFPのハードウェア構成を図5-1に示す。オペレーティングシステム（OS）とMFP本体、プリンタコントローラ等のハードウェアは、TOEの範囲ではない。

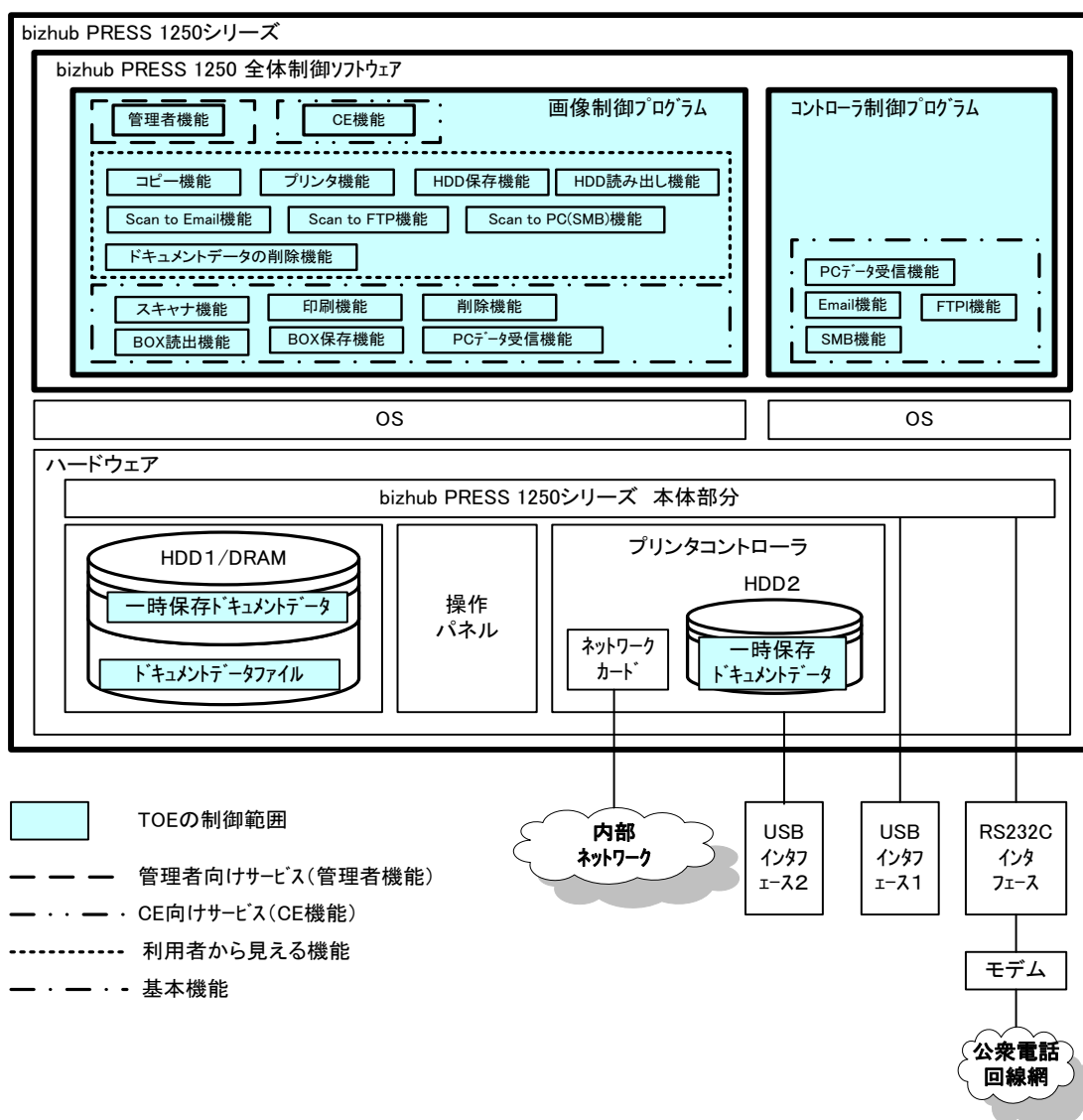


図5-1 TOE境界

以下、TOEを構成する要素について説明する。

■ 基本機能

- 1) スキャナ機能
一般利用者により操作パネルから指示された、紙文書の情報をスキャナから取り込みドキュメントデータに変換する機能。変換されたデータはHDD1または、DRAMに一時保存される。
- 2) PCデータ受信機能
プリンタコントローラから送られてきたドキュメントデータを一時保存HDD2に格納してデータ変換された後に、HDD1、またはDRAMに一時保存する機能。
- 3) BOX保存機能
HDD1に一時保存されたドキュメントデータを、保存する機能。
- 4) BOXデータ読み出し機能
保存されたドキュメントデータを、HDD1から読み出す機能。本機能は、ユーザBOXパスワードで認証された正当なユーザのみに許可される。
- 5) 印刷機能
HDD1または、DRAMに一時保存されたドキュメントデータを印刷する機能。
- 6) 画像データ送信機能
スキャナ機能により読み込まれたドキュメントデータを、一時保存HDD2に格納してFTPサーバなどに送信する機能。
- 7) 削除機能
ユーザBOX識別子に関連付けられたユーザBOX内のドキュメントデータを削除する機能。

■ セキュリティ機能

- 1) 識別認証機能
ユーザBOX識別子、ユーザBOXパスワードを使ってユーザBOXの識別認証を行う。識別認証が成功すると、ユーザに対してユーザBOXパスワードの変更、及び、ユーザBOX内の保存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
ユーザBOX（保存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、ユーザBOXパスワードで認証された正当なユーザのみ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。CE・管理者の識別認証に対する失敗/成功、ユーザBOXの認証に対する成功/失敗、HDDロックパスワードの変更の成功、セキュリティ強化モードの設定（有効化/停止）の成功、ドキュメントデータの読み出し・印刷、監査ログの読み出

し・印刷指示、管理者機能に関する操作が発生した場合に、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。

- ・セキュリティ強化状態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MFPに搭載されていることを検査する。
- ・MFP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MFPは、コントローラ制御プログラムを介して内部ネットワークに接続され、TOEは、FTPサーバ、Mailサーバ等のサーバコンピュータ、及びクライアントPCとドキュメントデータ等を通信する。また、MFPと内部ネットワークは直接接続されているが、TOEのセキュリティ強化状態が有効な場合は、ユーザBOX内のドキュメントデータ等の通信を行えないよう、ネットワークインタフェースが設定される。TOEは、コニカミノルタビジネステクノロジー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。本TOEに添付されるドキュメントは、ユーザーズガイド、インストールマニュアル、サービスマニュアルの3種類から構成される。

TOEの一般利用者、管理者及び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。

表6-1 日本向け bizhub PRESS 1250シリーズ ドキュメント

| No. | 名称 | 識別 |
|-------------|---|------------------|
| ユーザーズガイド | | |
| 1 | bizhub PRESS 1250 / 1052 ユーザーズガイド コピー編 | A4EU9550-CO-00 |
| 2 | bizhub PRESS 1250 / 1052 ユーザーズガイド POD管理者編 | A4EU9550-PA-00 |
| 3 | bizhub PRESS 1250 / 1052 ユーザーズガイド セキュリティー編 | A4EU957200 |
| 4 | bizhub PRESS 1250 / 1052 ユーザーズガイド ネットワークスキャナー編 | A4EU9550-NS-00 |
| 5 | bizhub PRESS 1250 / 1250P / 1052 ユーザーズガイド プリンター編 | A4EU9550-IC-00 |
| 6 | bizhub PRESS 1250P ユーザーズガイド 本体編 | A4EX9550-MB-00 |
| 7 | bizhub PRESS 1250P ユーザーズガイド セキュリティー編 | A4EX957200 |
| 8 | bizhub PRO 951 ユーザーズガイド コピー編 | A4EW9550-CO-00 |
| 9 | bizhub PRO 951 ユーザーズガイド POD管理者編 | A4EW9550-PA-00 |
| 10 | bizhub PRO 951 ユーザーズガイド セキュリティー編 | A4EW957211 |
| 11 | bizhub PRO 951 ユーザーズガイド ネットワークスキャナー編 | A4EW9550-NS-00 |
| 12 | bizhub PRO 951 ユーザーズガイド プリンター編 | A4EW9550-IC-00 |
| インストールマニュアル | | |
| 13 | bizhub PRESS 1250 / 1052 インストールマニュアル | A4EU960000 |
| 14 | bizhub PRESS 1250P インストールマニュアル | A4EX960000 |
| 15 | bizhub PRO 951 インストールマニュアル | A4EW960000 |
| サービスマニュアル | | |
| 16 | bizhub PRESS 1250 / 1250P / 1052 bizhub PRO 951 サービスマニュアル | CCA4EU-M-J2-0950 |

表6-2 海外向け bizhub PRESS 1250シリーズ ドキュメント

| No. | 名称 | 識別 |
|----------|--|----------------|
| ユーザーズガイド | | |
| 1 | bizhub PRESS 1250 / 1052 User's Guide Copier | A4EU9551-CO-00 |

| | | |
|-------------|---|------------------|
| 2 | bizhub PRESS 1250 / 1052 User's Guide POD Administrator's Reference | A4EU9551-PA-00 |
| 3 | bizhub PRESS 1250 / 1052 User's Guide Security | A4EU957300 |
| 4 | bizhub PRESS 1250 / 1052 User's Guide Network Scanner | A4EU9551-NS-00 |
| 5 | bizhub PRESS 1250 / 1250P / 1052 User's Guide Printer | A4EU9551-IC-00 |
| 6 | bizhub PRESS 1250P User's Guide Main body | A4EX9551-MB-00 |
| 7 | bizhub PRESS 1250P User's Guide Security | A4EX957300 |
| 8 | bizhub PRO 951 User's Guide Copier | A4EW9551-CO-11 |
| 9 | bizhub PRO 951 User's Guide POD Administrator's Reference | A4EW9551-PA-11 |
| 10 | bizhub PRO 951 User's Guide Security | A4EW957311 |
| 11 | bizhub PRO 951 User's Guide Network Scanner | A4EW9551-NS-11 |
| 12 | bizhub PRO 951 User's Guide Printer | A4EW9551-IC-11 |
| 13 | ineo 1250 / 1052 User's Guide Copier | A4EU9555-CO-00 |
| 14 | ineo 1250 / 1052 User's Guide POD Administrator's Reference | A4EU9555-PA-00 |
| 15 | ineo 1250 / 1052 User's Guide Security | A4EU957600 |
| 16 | ineo 1250 / 1052 User's Guide Network Scanner | A4EU9555-NS-00 |
| 17 | ineo 1250 / 1250 User's Guide Printer | A4EU9555-IC-00 |
| 18 | ineo 951 User's Guide Copier | A4EW9555-CO-00 |
| 19 | ineo 951 User's Guide POD Administrator's Reference | A4EW9555-PA-00 |
| 20 | ineo 951 User's Guide Security | A4EW957600 |
| 21 | ineo 951 User's Guide Network Scanner | A4EW9555-NS-00 |
| 22 | ineo 951 User's Guide Printer | A4EW9555-IC-00 |
| インストールマニュアル | | |
| 23 | bizhub PRESS 1250 / 1052 INSTALLATION MANUAL | A4EU960100 |
| 24 | bizhub PRESS 1250P INSTALLATION MANUAL | A4EX960100 |
| 25 | bizhub PRO 951 INSTALLATION MANUAL | A4EW960100 |
| 26 | Press 125ppm / Press 105ppm INSTALLATION MANUAL | A4EU960500 |
| 27 | Pro 95ppm INSTALLATION MANUAL | A4EW960500 |
| サービスマニュアル | | |
| 28 | bizhub PRESS 1250 / 1250P / 1052 bizhub PRO 951 SERVICE MANUAL | CCA4EU-M-E2-0000 |

■ 日本語版と英語版の違いについて

本 TOE に添付されるドキュメントには、日本国内向けの機種用の日本語版と、海外向けの機種用の英語版の 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。

7.2 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24年1月に始まり、平成24年8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24年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24年5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。

7.3 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価に基づく侵入テストを実行した。

7.3.1 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。評価した開発者テストの概要を以下に示す。

(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。

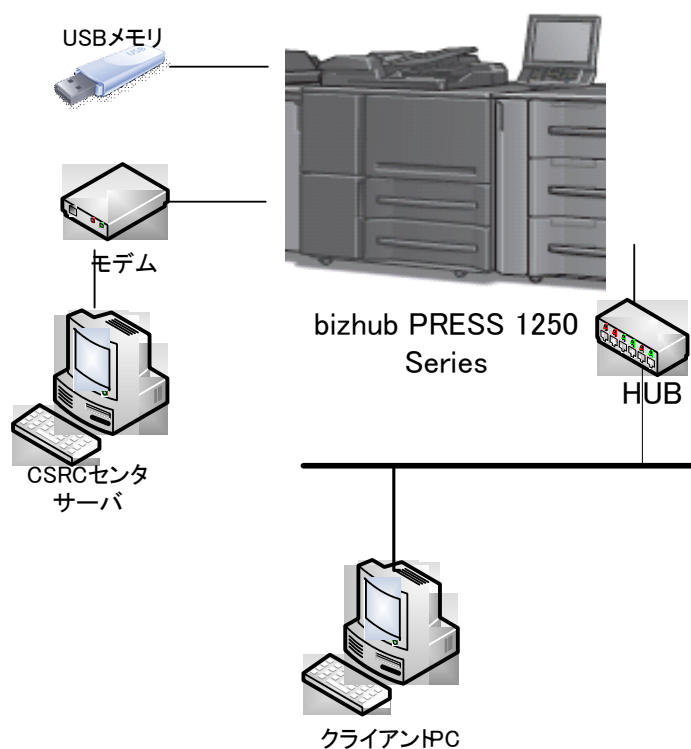


図7-1 開発者テストの構成図

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 1250 Series MFP 本体 | テスト対象となるMFP2台の機種(*)を準備しておくことが明記されている。 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： A4EU0Y0-00I1-G00-15 ・コントローラ制御プログラム： A4E-00P1-G00-15 (*)bizhub PRESS 1250、bizhub PRO 951 |
| クライアントPC | OS： Windows XP |
| 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 1250/1052 PCLドライバVersion 1.1.1.0、PSドライバVersion 1.0.112 および、bizhub PRO 951 PCLドライバVersion 1.1.0.0、PSドライバVersion 1.0.63 (bizhub PRESS 1250/1052、およびbizhub PRO 951互換)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。MFPの電話回線経由でのCSRCセンターテスト時のサーバ側に使用する。 |
| CSRCセンター サーバ | CSRCのセンターソフトウェア Ver. 2.7.0が動作するPC。 |
| USBメモリ | TOE更新機能のテストに利用する。 |

開発者テストで使用されたTOEはSTで識別されている複数のMFPの一部の機種であるが、差異は印刷速度の違い、スキャナ機能なしモデル(bizhub PRESS 1250 P)、OEM製品、仕向地の違いであり、セキュリティ機能は同一でテスト対象としたTOEと同一である。

図7-1と表7-1に示すこの構成は、TOEを搭載するMFP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

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

<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、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。

<開発者テストツール>

図7-1に示した開発者テスト環境の構成以外に、利用されたツールはない。

<開発者テストの実施>

開発者が提供した証拠資料「bizhub PRESS 1250 Series 機能テスト書」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. 実施テストの範囲

開発者によって、35項目（118件）のテストが実施された。

カバレッジ分析が実施され、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。深さ分析が実施され、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ている。

c. 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。

7.3.2 評価者独立テスト

評価者は、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の再確認のための独立テストを実施した。評価者が実施した評価者独立テストの概要を以下に示す。

(1) 評価者独立テスト環境

評価の対象としたTOEは、「bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア」である。TOEが搭載されるMFPは、「bizhub PRESS 1250」と「bizhub PRO 951」を選択し、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MFP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。

(2) 評価者独立テスト概説

評価者の実施した評価者独立テストは以下のとおり。

a. 評価者独立テストの観点

<独自テスト>

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評価者独自テスト10項目を考案した。

- セキュリティ機能の観点
 - 独立テストと重複するテストは除外する。
 - 開発者テストにおいて十分にふるまいを確認できた機能は、除外する。
 - 操作パネルからしか操作できず、パラメタも固定である機能は、除外する。

以上から、独自テストにおいてふるまいを追加確認すべきと判断した「パスワードの変更機能」、「ユーザへのアクセスルールと制御機能」、「監査情報の記録機能」、「監査領域の管理機能」、「管理支援機能(管理者)」、「HDDロックパスワード機能」をテスト対象とし、「管理者の登録・CEの登録機能」、「CEの識別と認証機能」、「管理者の識別と認証機能」、「HDDロック機能のテスト機能」、「セキュリティ強化モードの設定機能」は、テスト対象から除外した。

- 評価者の着目した観点
 - (観点1) セキュリティに重大な影響を与える機能を対象とする。

- (観点2) 確率的・順列的メカニズムを用いたセキュリティ機能(認証メカニズム、HDDロックパスワード照合メカニズム)を対象とする。
- (観点3) ドメイン(一般利用者、管理者及びCE)の違いによってセキュリティ機能に違いがある可能性を考慮し、関係するセキュリティ機能を対象とする。

以上から、セキュリティに重大な影響を与える識別認証からパスワード変更までの機能の異常系テストと、開発者テストとは異なる観点であるドメインの違いに基づいたテストを実施した。

<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、15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ユーザBOX機能、コントローラ制御プログラムに関連する機能に関しても、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TSFI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. 評価者独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

<評価者独立テスト手法>

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、以下のような方法で独自テストを実施した。

- 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>

開発者テスト環境と同様に、評価者独立テストの構成以外に、利用されたツールはない。

<独立テストの実施>

評価者独立テストのうち独自テスト10項目とサンプリングテスト15項目について、その内容を表7-2と表7-3に示す。

表7-2 実施した独自テスト

| 項番 | 名称 | テスト内容 |
|-----|--------------------------------|--|
| E-1 | 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。 |
| E-2 | 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。 |
| E-3 | 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。 |
| E-4 | 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。 |
| E-5 | ユーザによるユーザBOXパスワードの変更機能テスト（観点2） | ユーザによるユーザBOXパスワード変更できること。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。 |

| 項番 | 名称 | テスト内容 |
|------|---|--|
| E-6 | 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。 |
| E-7 | 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。 |
| E-8 | プリンタJOB保存テスト (観点3) | プリンタJOBの保存機能が正しく動作すること。 |
| E-9 | 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状態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。 |
| E-10 | コントローラ制御プログラムに関わる初期化時のふるまいの確認テスト (観点1) | 画像制御プログラム側のOSが起動していない場合には、コントローラ制御プログラム側のネットワークポートもオープンしないこと。 コントローラ制御プログラム側HDDのロックパスワードが一致しない場合にエラー画面を表示し初期化を中断すること。 |

表7-3 実施したサンプリングテスト

| 項番 | テスト項目の名称 |
|----|--|
| 1 | CE認証機能インタフェースのテスト |
| 2 | CEによる管理者パスワードの設定インタフェースのテスト |
| 3 | 管理者認証機能インタフェースのテスト |
| 4 | ユーザによるユーザBOXパスワード変更インタフェースのテスト |
| 5 | プリンタ以外のユーザ認証機能インタフェースのテスト |
| 6 | HDDロックパスワードの認証成功の確認インタフェースのテスト |
| 7 | HDDロックパスワードの変更インタフェースのテスト |
| 8 | セキュリティ強化モードの設定変更 (ONからOFFに変更) インタフェースのテスト |
| 9 | 管理者による監査ログデータの出力インタフェースのテスト |
| 10 | TOEがセキュリティ強化状態に設定された状態において、Web接続用のネットワークポートが閉じていることを確認するテスト。 |
| 11 | コントローラNICのポート制御のテスト |
| 12 | プリンタJOB保存方法インタフェースのテスト |
| 13 | スキャナJOB保存インタフェースのテスト |
| 14 | JOB 読出し機能テスト |
| 15 | CSRCインタフェースのテスト |

c. 結果

実施したすべての評価者独立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。

7.3.3 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の可能性について、必要と思われる侵入テストを考案し、実施した。評価者侵入テストの概要を以下に示す。

(1) 評価者侵入テスト概説

評価者の実施した侵入のテストは以下のとおり。

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、評価者侵入テストを必要とする以下の懸念される脆弱性を識別した。

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 |
| VLA-T4 | 脆弱性情報（CVN、JVN等）を調査した結果、発見された公知の脆弱性。（OS、ライブラリ等も含む） | 公知の脆弱性 |
| VLA-T5 | 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 |

| 項番 | 懸念される脆弱性の内容 | 脆弱性の観点 |
|--------|---|--------------------|
| VLA-T6 | 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-T7 | USBを使用したTOEの更新機能が悪用される。 | 改ざん |
| VLA-T8 | 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-T9 | 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. 評価者侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の評価者侵入テストを実施した。

<評価者侵入テスト環境>

評価者が実施した侵入テストの構成を図7-2に示す。

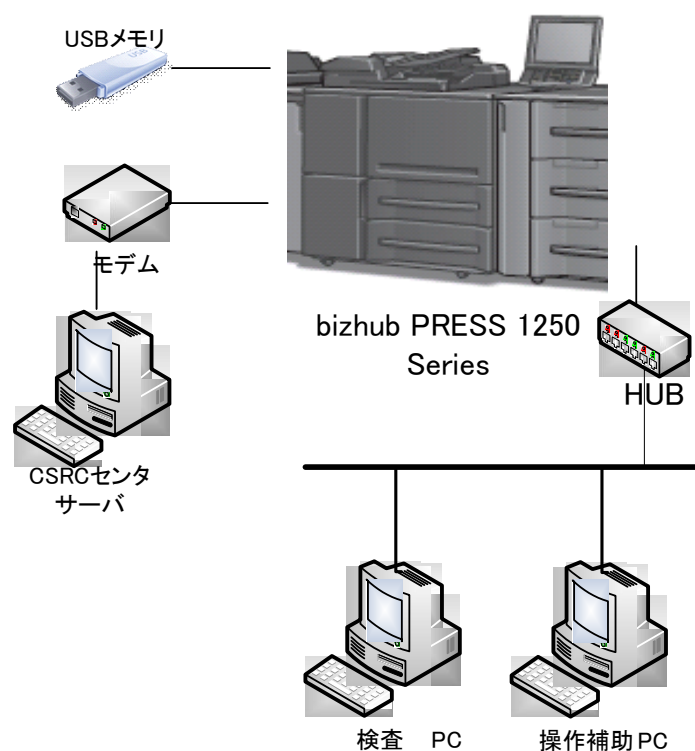


図7-2 評価者侵入テストの構成図

評価者侵入テストの構成（図7-2）は、MFPの機種と検査PCに関係する部分が、開発者テストの構成（図7-1）と異なる。検査PCは、脆弱性テストにおいて、検査ツールを使用するためのものであり、開発者テストの構成におけるTOEの動作と評価者独立テストの構成におけるTOEの動作に違いはない。

評価者侵入テストの構成は、評価者独立テストの構成と同様に、TOEを搭載するMFPへすべての装置やオプションを装着、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、評価者侵入テストの構成として問題ないと判断した。

評価者侵入テストの構成要素のうち、開発者テストの構成要素と異なる部分を表7-5に示す。

表7-5 評価者侵入テストの構成要素

| 構成要素 | 詳細 |
|--------|--|
| 操作補助PC | OS： Windows XP プリンタドライバ： KONICA MINOLTA bizhub PRESS 1250/1052 PCLドライバVersion 1.1.1.0、PSドライバVersion 1.0.112 および、bizhub PRO 951 PCLドライバVersion 1.1.0.0、PSドライバVersion 1.0.63 (bizhub PRESS 1250/1052、およびbizhub PRO 951互換) ※ 表 7-1 のクライアント PC と同等 |
| 検査PC | OS： Windows XP 検査ツール： Nessus、BZ、Nmap、extrstr |

評価者侵入テストの環境において使用したツールを表7-6に示す。

表7-6 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：4.4.1 build 15078 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：6.0.0 システム上のポートを検査するセキュリティスキャナ |

| ツール名称 | 概要・利用目的 |
|---------|--|
| extrstr | 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。 |

<脆弱性テストの実施>

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7-7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7-7 評価者侵入テスト概要

| 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-T5 |
| 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-T6 |
| 6 | 侵入テスト用に作成したTOEをUSB経由で更新する。 | VLA-T7 |
| 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-T8 |
| 8 | 監査ログ領域満杯に要する時間を確認する。 | VLA-T9 |

■ 「表7-4 懸念される脆弱性」の「VLA-T4」について

OS、ライブラリ等に関する公知の脆弱性は、2012年4月12日時点の調査において、本TOE及び本TOEの動作に必要なOSに含まれていないことを確認したため、テスト項目から除外した。

c. 結果

実施した評価者侵入テストでは、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。

7.4 評価構成について

本評価では、「7.3.2 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状態に設定する機能（セキュリティ強化モード）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状態に設定する機能（セキュリティ強化モード）を有効にする。
- HDD ロック機能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。
- HDD ロック機能を有効にする。

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。

7.5 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章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

消費者に喚起すべき評価者勧告は、特にない。

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

- TOEの設置手続きにおけるHDDロック機能用のパスワードの設定タイミングについて

ガイダンスのTOEの設置手続きには、一般利用者の登録作業を行った後に、HDDロック機能用のパスワードの設定を行うよう記述されている。TOEの設置手続きにおいて、多数の一般利用者の登録作業を行わなければならない場合、その登録作業に時間がかかるため、MFPの電源を遮断する等の誤操作や不正な操作が介入する危険性がある。その場合、HDDロック機能用のパスワードの設定やHDDロック機能が有効化される前であるため、TOEは、評価において保証された安全な状態に至っていない。

したがって、TOEの設置手続きにおいては、登録する一般利用者は最小限にとどめる等して一般利用者の登録作業を短時間にとどめて、TOEの設置手続きを終了し、MFPを再起動すること。MFPの再起動後、TOEがセキュリティ強化状態に設定された状態において、一般利用者の登録作業を行うこと。

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、公表のため、本報告書とは別文書として、以下のとおり提供される。

bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub
PRO 951 / ineo 1250 / ineo 1052 / ineo 951 セキュリティターゲット バージョン 1.12 2012年7月27日 コニカミノルタビジネステクノロジーズ株式会社

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、MFPの保守作業を行う者。 |
| FTP | File Transfer Protocol (ファイル転送プロトコル) |
| 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。 |
| MFP | デジタル複合機の略称 |
| 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。MFP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。 |
| FTPサーバ | File Transfer Protocol (ファイル転送プロトコル) を用いて、クライアントとファイルを送受信するためのサーバ |
| 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 |

| | |
|-----------------------|---|
| Scan to Email機能 | スキャナ装置から紙文書の情報を取り込み、ドキュメントデータに変換した後、Emailを使って送信するTOEの機能 |
| Scan to FTP機能 | スキャナ装置から紙文書の情報を取り込み、ドキュメントデータに変換した後、FTPを使って送信するTOEの機能 |
| Scan to PC(SMB)機能 | スキャナ装置から紙文書の情報を取り込み、ドキュメントデータに変換した後、SMBを使ってクライアントPCへ送信するTOEの機能 |
| SMBサーバ | Server Message Block（サーバメッセージブロック）プロトコルを用いて、クライアントとファイルを共有するためのサーバ |
| SMTPサーバ | Simple Mail Transfer Protocol（簡易メール転送プロトコル）を用いて、電子メールを送信するためのサーバ |
| 外部ネットワーク | MFP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 |
| コピー機能 | スキャナ装置から紙文書の情報を取り込み、ドキュメントデータに変換した後に印刷するTOEの機能 |
| 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 |
| スキャナ機能 | スキャナ装置から紙文書の情報を取り込み、ドキュメントデータに変換する機能 |
| 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状態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MFP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MFP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 | MFP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 |
| ユーザ BOX | ユーザ BOX は、ドキュメントデータを格納する個人用のディレ クトリである。 |
| ユーザBOX識別 子 | ユーザBOX識別子は、ユーザ名である。 |

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24年3月, 独立行政法人情報処理推進機構, CCS-01
- [2] ITセキュリティ認証申請手続等に関する規程, 平成24年3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申請手続等に関する規程, 平成24年3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 Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001
- [5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002
- [6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003
- [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3版, 2009年7月, CCMB-2009-07-001, (平成21年12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3版, 2009年7月, CCMB-2009-07-002, (平成21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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)
- [10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004
- [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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)
- [12] bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 セキュリティターゲット バージョン 1.12 2012年7月27日 コニカミノルタビジネステクノロジーズ株式会社
- [13] bizhub PRESS 1250 / bizhub PRESS 1250P / bizhub PRESS 1052 / bizhub PRO 951 / ineo 1250 / ineo 1052 / ineo 951 全体制御ソフトウェア 評価報告書 第3版 2012年8月8日 みずほ情報総研株式会社 情報セキュリティ評価室