



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



評価対象

申請受付日（受付番号）	平成20年3月28日（IT認証8219）
認証番号	C0212
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：bizhub PRO 950 全体制御ソフトウェア 海外：bizhub PRO 950 control software
TOEのバージョン	画像制御プログラム（画像制御 I1）：00I1-G00-10 コントローラ制御プログラム（ICコントローラ P）：00P1-G00-11
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	一般社団法人 ITセキュリティセンター 評価部

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4月21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。

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

評価結果：合格

「日本：bizhub PRO 950 全体制御ソフトウェア（画像制御プログラム（画像制御 I1）：00I1-G00-10、コントローラ制御プログラム（ICコントローラ P）：00P1-G00-11）海外：bizhub PRO 950 control software（Image Control Program（Image Control I1）：00I1-G00-10、Controller Control Program（IC Control P）：00P1-G00-11）」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	2
1.2.3	TOEの範囲と動作概要	3
1.2.4	TOEの機能	4
1.3	評価の実施	6
1.4	評価の認証	7
1.5	報告概要	7
1.5.1	PP適合	7
1.5.2	EAL	7
1.5.3	セキュリティ機能強度	7
1.5.4	セキュリティ機能	8
1.5.5	脅威	10
1.5.6	組織のセキュリティ方針	10
1.5.7	構成条件	10
1.5.8	操作環境の前提条件	11
1.5.9	製品添付ドキュメント	11
2	評価機関による評価実施及び結果	13
2.1	評価方法	13
2.2	評価実施概要	13
2.3	製品テスト	13
2.3.1	開発者テスト	13
2.3.2	評価者テスト	15
2.4	評価結果	16
3	認証実施	17
4	結論	18
4.1	認証結果	18
4.2	注意事項	24
5	用語	25
6	参照	27

1 全体要約

1.1 はじめに

この認証報告書は、「日本：bizhub PRO 950 全体制御ソフトウェア（画像制御プログラム（画像制御 I1）：00I1-G00-10、コントローラ制御プログラム（ICコントローラ P）：00P1-G00-11）、海外：bizhub PRO 950 control software（Image Control Program(Image Control I1）：00I1-G00-10、Controller Control Program(IC Control P）：00P1-G00-11）」（以下「本TOE」という。）について一般社団法人 ITセキュリティセンター 評価部（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ものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

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

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称： 日本：bizhub PRO 950 全体制御ソフトウェア
海外：bizhub PRO 950 control software

バージョン： 日本：画像制御プログラム（画像制御 I1）：00I1-G00-10
コントローラ制御プログラム（ICコントローラ P）：
00P1-G00-11

海外：Image Control Program(Image Control I1）：00I1-G00-10
Controller Control Program(IC Control P）：00P1-G00-11

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

1.2.2 製品概要

本製品（「bizhub PRO 950 全体制御ソフトウェア(*1)」という）は、コニカミノルタビジネステクノロジー株式会社製デジタル複合機（「bizhub PRO 950 シリーズ」という）に搭載され、利用者毎に保存されたドキュメントデータの漏洩に対する危険性を減ずることを目的としたソフトウェア製品である。

bizhub PRO 950 全体制御ソフトウェアは、コピー/プリンタなどを活用した機能において、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機能および各種管理機能を実装し、文書を保管するHDD（ハードディスク装置）には機密性の高いもの（ハードディスクロック機能(*2)付のハードディスク）を採用している。bizhub PRO 950 全体制御ソフトウェアは、bizhub PRO 950シリーズに搭載し提供される。

bizhub PRO 950シリーズの利用環境として図1-1に示すオフィスを想定する。

(*1) 日本：bizhub PRO 950 全体制御ソフトウェア、海外：bizhub PRO 950 control softwareのことを示す。

(*2) ハードディスクを取外し他の機器で読み込みができないように、ハードディスクにパスワードを持たせる機能のことをいう。ハードディスクロック機能で設定するパスワードをHDDロックパスワードという。

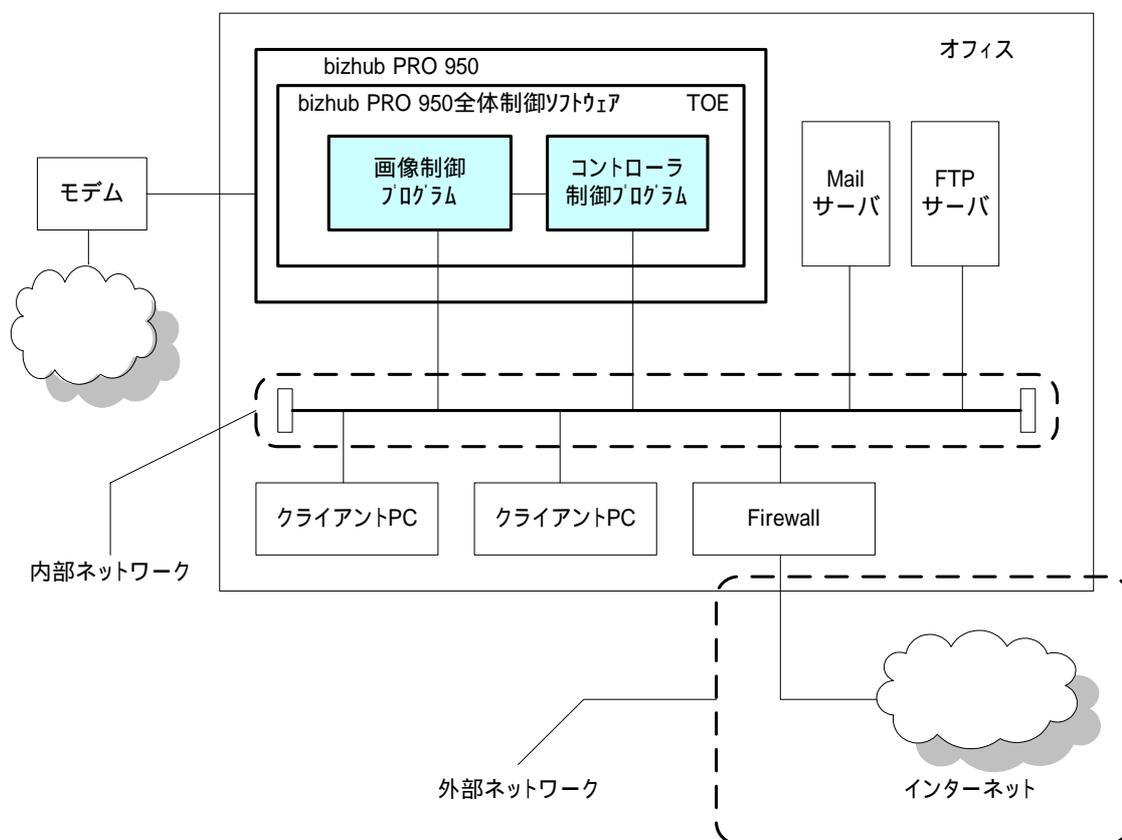


図1-1 bizhub PRO 950 シリーズの利用環境

TOEを搭載するbizhub PRO 950 シリーズは、図1-1に示すように内部ネットワーク及び公衆電話回線網に接続される。内部ネットワークは、一般利用者のクライアントPC、及びbizhub PRO 950がデータを送信するMailサーバやFTPサーバと接続する。本TOEは外部ネットワークとのインタフェースは持たない。内部ネットワークの各機器を保護するため、外部ネットワークとの接続を行う場合はFirewallを介して接続する。

1.2.3 TOEの範囲と動作概要

本TOEを含むbizhub PRO 950 シリーズの構成を図1-2に示す。

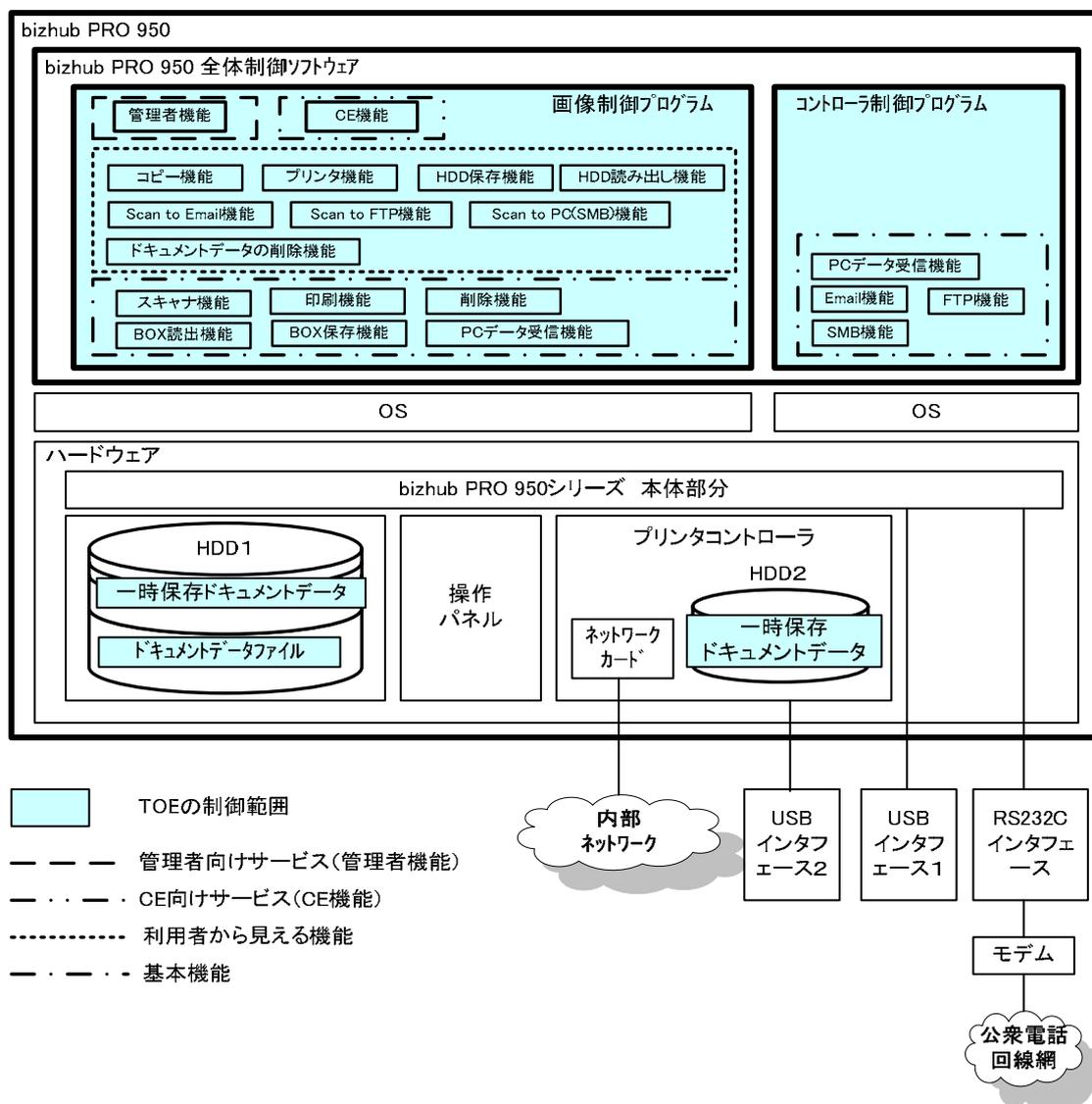


図1-2 bizhub PRO 950 シリーズの構成

bizhub PRO 950 シリーズは、ハードウェア、bizhub PRO 950 全体制御ソフトウェアから構成される。bizhub PRO 950 全体制御ソフトウェアのコンポーネントは、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。ハードウェアは、

bizhub PRO 950 シリーズ本体部分、プリンタコントローラ部分、HDD1部分、HDD2部分、操作パネル及びネットワークカードである。HDD1部分には記憶装置が存在し、ドキュメントの格納と、一時的なドキュメントの格納を行う。HDD2部分にも記憶装置が存在しドキュメントの一時的な格納を行う。本TOEの一部である画像制御プログラムは、画像制御プログラム用のOS上で、コントローラ制御プログラムは、コントローラ制御プログラム用のOS上で動作する。

本TOEの制御範囲であるTOEに含まれる各機能と本TOEが生成するデータ拡張領域を図1-2の網掛けで示す。

1.2.4 TOEの機能

本TOEは、ユーザBOX内のドキュメントデータファイルに格納されたドキュメントデータの操作をする「基本機能」、管理者がTOEの設定を行う「管理機能」及び、CE(*3)がTOEの初期設定(管理者の登録やTOEのインストール)を行う「CE機能」から構成される。

(*3)Customer Engineer : bizhub PRO950 シリーズの保守を委託されている企業に在籍し、bizhub PRO 950 シリーズの保守をする者

1.2.4.1 TOEの基本機能

基本機能は、ドキュメントデータの操作をする機能である。ユーザBOXはユーザBOX識別子で識別され、さらに各ユーザBOXの所有者(一般利用者)の正当性を確認するためにユーザBOX毎にユーザBOXパスワードが設定される。正当なユーザBOXの所有者はそのユーザBOX内のすべてのドキュメントデータをアクセスできる。基本機能の概念を図1-3に示す。

サブBOXはユーザBOX内に作成され、サブBOXの中にドキュメントデータをまとめて格納する。

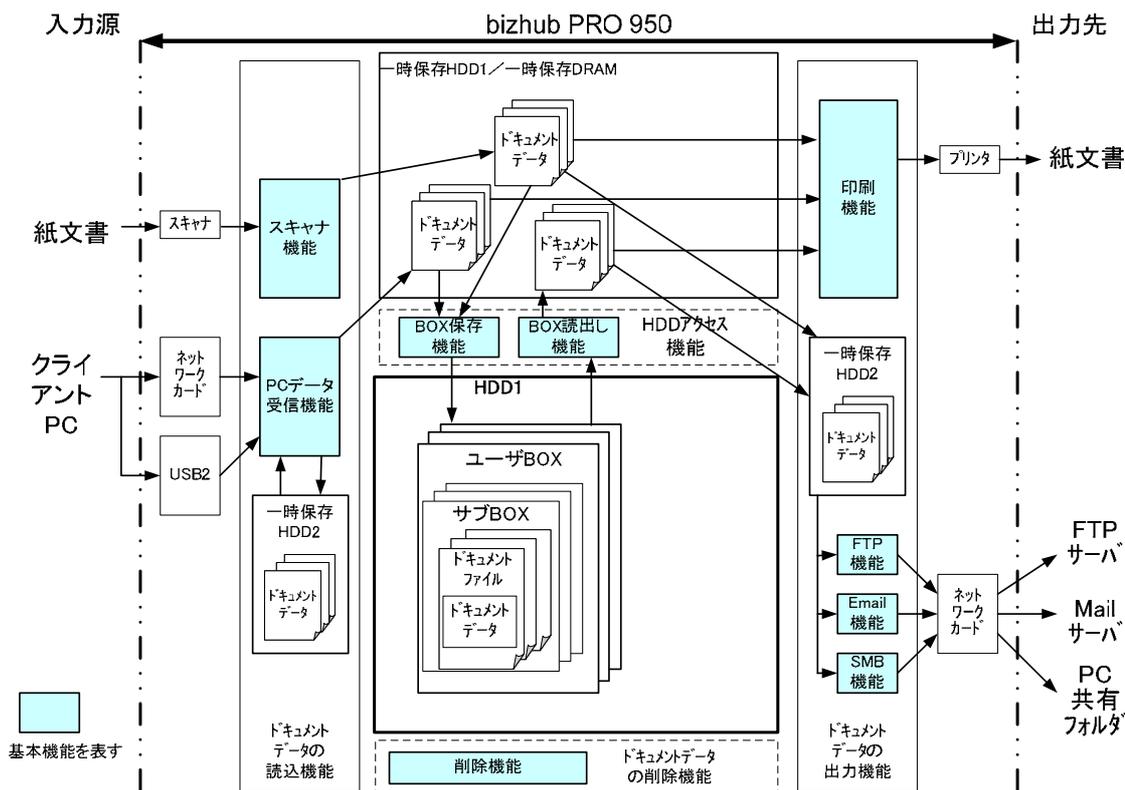


図1-3 基本機能の処理概念

各機能の詳細は以下のとおりである。

(1) スキャナ機能

操作パネルから操作し、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して、一時保存HDD1、または一時保存DRAMに格納する。

(2) PCデータ受信機能

クライアントPCから内部ネットワーク経由で指示されたドキュメントデータを、一時保存HDD2に格納し、データ変換した後、一時保存HDD1、または一時保存DRAMに格納する。

(3) BOX保存機能

一時保存HDD1、または一時保存DRAMに一時格納されたドキュメントデータを、ユーザBOX内に追加格納する。

(4) BOX読出し機能

ユーザBOX内のドキュメントデータを、一時保存HDD1または、一時保存DRAMに一時読み出しする。

(5) 印刷機能

一時保存HDD1、または一時保存DRAMに一時格納されたドキュメントデータを印刷する。

(6) Email機能

一時保存HDD1、または一時保存DRAMに一時格納された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を経由してメールに添付しMailサーバに送信する。

(7) FTP機能

一時保存HDD1、または一時保存DRAMに一時格納された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を経由してFTPサーバに送信する。

(8) SMB機能

一時保存HDD1または、一時保存DRAMに一時格納された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を経由して内部ネットワークに接続されているPCの共有フォルダに送信する

(9) 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。

1.2.4.2 管理機能

管理者は、管理機能を使用して、本TOEが有する機能の動作設定を行う。また、管理機能は、ユーザBOXの作成/属性変更/削除、監査情報の印刷、HDD1、HDD2の初期化处理（HDDロックパスワードの設定）、プリンタ枚数の管理、トラブルシューティング及びトナーの管理など、デジタル複合機の運用に関わる情報を管理する。

1.2.4.3 CE 機能

CEが本TOEの初期設定および保守を行うため、以下の機能が用意されている。

・サービス設定モード

操作パネルから操作しサービス設定モードの機能を利用し管理者のパスワード登録と変更を実施する。

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」[1]、「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。

本TOEのセキュリティ設計が適切であること。

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。

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。

上記 、 、 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「Multi functional printer(digital copier) bizhub PRO 950 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、「bizhub PRO 950 全体制御ソフトウェア評価報告書」(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4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、一般利用者の攻撃能力について、低レベルであることを想定している。

また、物理的な面と人的な面で十分なセキュリティを確保した条件下で運用されることを想定している。このため、セキュリティ強度は、低レベルの攻撃能力を要する脅威エージェントからの攻撃に対して、十分に対抗できるSOF-基本で妥当である。

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) 識別認証

機能名称	セキュリティ機能
IA.ADM_ADD 管理者の登録	CEのみが操作でき、管理者のパスワードを登録することで、管理者をTOEに登録する。パスワードが仕様に従っている場合登録し、仕様に従っていない場合登録を拒否する。
IA.ADM_AUTH 管理者の識別と認証	操作者がTOEを利用する前に、TOEに登録した管理者であることを識別し、操作者が管理者本人であることを認証する。管理者の識別と認証の前に管理機能の一切の操作を許可しない。操作者が管理者認証インタフェースにアクセスすることで、管理者であることが識別され、入力するパスワードを用いて管理者本人であることを認証する。 認証不成功時には、5秒間アクセスを禁止する。
IA.CE_AUTH CEの識別と認証	操作者がTOEを利用する前に、TOEに登録しているCEであることを識別し、操作者がCE本人であることを認証する。CEの識別と認証の前にCE機能の一切の操作を許可しない。操作者がCE認証インタフェース、入力するパスワードを用いてCE本人であることを認証する。 認証不成功時には、5秒間アクセスを禁止する。
IA.PASS パスワードの変更	管理者のパスワード、CEのパスワード及びユーザBOXパスワードを変更する。 パスワード変更のインタフェースを提供し、新しいパスワードの入力を要求する。 利用者により以下のパスワードの変更が可能である。 CE : CEのパスワード、管理者のパスワード 管理者 : ユーザBOXパスワード、管理者パスワード ユーザBOXを所有している一般利用者 : 自分自身のユーザBOXのユーザBOXパスワード パスワードが仕様に従っている場合変更し、仕様に従っていない場合変更を拒否する。

(2) アクセス制御

機能名称	セキュリティ機能
ACL.USR 一般利用者への アクセスルール と制御	<p>ユーザBOXを所有している一般利用者を識別認証し、本人であることが認証できると、以下のアクセスルールに従い一般利用者が操作可能な範囲を制限する。</p> <p>ユーザBOXを所有している一般利用者をユーザBOX識別子、ユーザBOXパスワードで識別認証を行い、ユーザBOXを所有する一般利用者のユーザBOX識別子と合致するユーザBOXに対してのみ以下の操作を許可する。</p> <ul style="list-style-type: none"> ・ドキュメントデータの読み出しと印刷 <p>識別と認証不成功時には、5秒間の識別と認証の試行を禁止する。</p>

(3) 監査

機能名称	セキュリティ機能の仕様
AUD.LOG 監査情報の記録	<p>セキュリティ機能の動作に関する監査情報を記録する。</p> <p>監査対象となるイベントを以下に示す。</p> <ul style="list-style-type: none"> ・監査機能の起動と終了 ・管理者、CE、ユーザ BOX を所有している一般利用者の識別と認証に関する成功不成功 ・管理者、ユーザ BOX を所有している一般利用者のパスワード登録時の成功 ・管理者、CE、ユーザ BOX を所有している一般利用者のパスワード変更時の成功 ・ドキュメントデータ読み出しの成功
AUD.MNG 監査領域の管理	監査情報を生成し保存するためにリングバッファ形式により監査格納領域を管理する。

(4) 管理支援

機能名称	セキュリティ機能の仕様
MNG.MODE セキュリティ強化モードの設定	管理者にのみセキュリティ強化モードを停止にする機能を許可する。
MNG.ADM 管理支援機能(管理者)	<p>管理者にのみ以下の処理を許可し実行する。</p> <ul style="list-style-type: none"> ・ユーザ BOX 作成、ユーザ BOX 識別子の登録とユーザ BOX パスワードの設定 ・監査情報の問い合わせ <p>ユーザBOXパスワードが仕様に従っている場合登録し、仕様</p>

	従っていない場合登録を拒否する。
MNG.HDD HDDロックパス ワード機能	管理者にのみ以下の処理を許可し実行する。 ・HDDロックパスワードの変更 HDDロックパスワードが仕様に従っている場合HDD装置にHDDロックパスワードを設定/変更し、仕様に従っていない場合登録/変更を拒否する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅威
T.ACCESS(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を漏洩させる恐れがある。
T.HDDACCESS (HDDへの不正なアクセス)	<ul style="list-style-type: none"> 一般利用者が不正な装置をHDD1に接続することにより、HDD1内のドキュメントデータを漏洩させる恐れがある。 一般利用者が不正な装置をHDD2に接続することにより、HDD2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してドキュメントデータを漏洩する恐れがある。

1.5.6 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はない。

1.5.7 構成条件

本TOEは、bizhub PRO 950 シリーズに搭載されるソフトウェア製品である。

本TOEは、bizhub PRO 950 シリーズ出荷時にセキュリティ機能付製品としてインストールして出荷する形態と、CEのWebダウンロードによるユーザーサイトでの組み込み形態をとる。

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1-2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1-2 TOE使用の前提条件

識別子	前提条件
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に設置される。
ASM.NET(内部ネットワークの設置条件)	TOEは、ドキュメントデータの漏洩が発生しない内部ネットワークに接続される。
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である。
ASM.CE(CEの条件)	CEは、不正な行為を行わない人物である。
ASM.USR(一般利用者の管理)	一般利用者は利用者自身のユーザBOXパスワードを漏らさない。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

国内向け

<CE向けマニュアル>

- ・ bizhub PRO 950 インストールマニュアル A0Y5961011
- ・ bizhub PRO 950 サービスマニュアルフィールドサービス
CCA0Y5-M-FJ1-0550

<管理者・一般利用者向けマニュアル>

- ・ bizhub PRO 950 ユーザーズガイド コピー編 A0Y5955600
- ・ bizhub PRO 950 ユーザーズガイド ネットワークスキャナ編 A0Y5960000
- ・ bizhub PRO 950 ユーザーズガイド POD管理者編 A0Y5956100
- ・ bizhub PRO 950 ユーザーズガイド セキュリティ編 A0Y5956600

海外向け

<CE向けマニュアル>

- ・ bizhub PRO 950 INSTALLATION MANUAL A0Y5961111
- ・ bizhub PRO 950 SERVICE MANUAL Field Service
CCA0Y5-M-FE1-0510

< 管理者・一般利用者向けマニュアル >

- bizhub PRO 950 User's Guide Copier A0Y5955700
- bizhub PRO 950 User's Guide Network Scanner A0Y5960100
- bizhub PRO 950 User's Guide POD Administrator's Reference
A0Y5956200
- bizhub PRO 950 User's Guide Security A0Y5956700

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20年3月に始まり、平成21年4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3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3月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

bizhub PRO 950 シリーズ

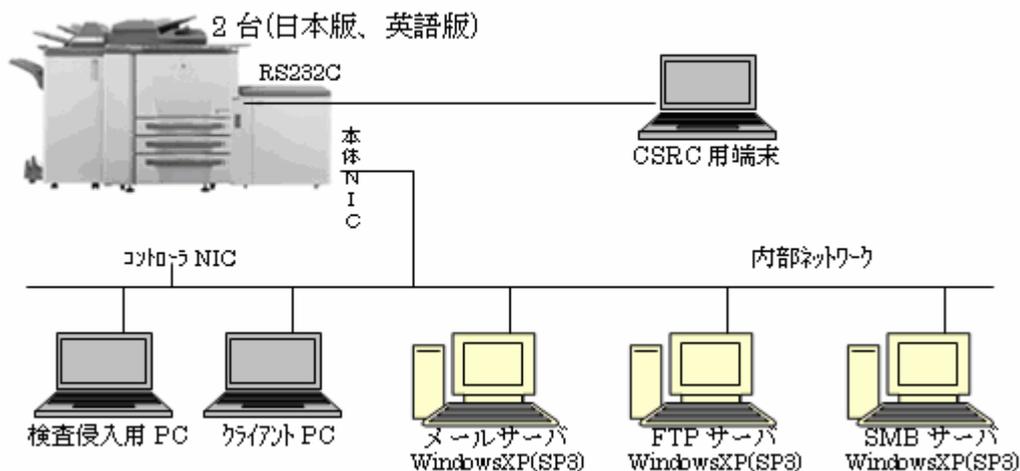


図2-1 開発者テストの構成図

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

開発者が実施したテストの構成を図2-1に示す。

- ・ TOE (bizhub PRO 950 全体制御ソフトウェア (画像制御プログラム (画像制御 I1) 00I1-G00-10、コントローラ制御プログラム (ICコントローラ P) 00P1-G00-11)) を bizhub PRO 950 シリーズに搭載。
- ・ bizhub PRO 950を内部ネットワーク(100baseT)に接続
- ・ 内部ネットワークを介してクライアントPC、メールサーバ、FTPサーバ、SMBサーバ、CSRC端末と接続

テスト構成では、CSRCは、LAN接続の構成のみとしているが、CSRCは、非セキュリティ機能であるため、セキュリティ機能のテスト結果に影響を与えることはない。また、STで記述されている構成のうちひとつ (STでは次のように記述されている。CSRC端末は、RS232CインタフェースまたはLAN接続のE-Mailインタフェースのうちいずれかを選択できる。) のみをテスト構成として選択してもSTで識別されている構成と矛盾しない。

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と評価者により判断されている。

b. テスト手法

テストには、以下の手法が使用された。

TSFIの操作によりセキュリティ機能の動作を確認する。

TSFI、サブシステムインタフェースを、直接bizhub PRO 950 の外部イ

インタフェース経由の操作でテストできない場合は、間接的にそのインタフェースを刺激する手法でテストを行う。

テストの振る舞いの観測について、外部TSFIにて確認できるものは、直接確認し、テスト結果の振る舞いを観測できないものについては、同タイプの別の機器（bizhub PRO 950）を使用して、テスト結果を確認する。

テストを実行したときの実際のテスト結果と、期待される振る舞いを比較して、テストの目標が達成されたか否かを決定する。

c. 実施テストの範囲

テストは開発者によって26項目実施されている。

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、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は、開発者テストと同様の構成である。

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

評価者が実施したテストの構成を図2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同等のテスト環境で実施されている。

評価者による侵入テストにおいては、図2-1のテストの構成に加え、TOEを搭載したbizhub PRO 950へUSBケーブルによりISW端末を接続し、一部の試験を実施しているが、STにおいて識別されているTOEの構成と同等のテスト環境であることが評価者により判断されている。

b. テスト手法

評価者によるサンプリングテストには、以下の手法が使用された。

開発者の実施したテストの50%以上を選択する。

評価者が考え出したテストと合わせて、機能仕様書に記述された個々の機能仕様(TSFI)に対してひとつ以上の項目を選択する。

評価者が考え出したテストと合わせて、総ての操作者インタフェースが関係する項目を少なくともひとつ選択する。

評価者が考え出したテストと合わせて、運用に関係する一連の完結した作業が実施できるよう、選択する。

評価者の独立テストには、以下の手法が使用された。

TSFIの操作によりセキュリティ機能を刺激（操作）し、TSFIでテストの振る舞いを観測する。

サブシステムインタフェースは、bizhub PRO 950 の外部インタフェース経由の操作でテストする。

テストの振る舞いを、TSFIで観測できない場合、治具を使用して、テスト結果を確認する。

テストを実行したときの実際のテスト結果と、期待される振る舞いを比較して、テストの目標が達成されたか否かを決定する。

評価者の侵入テストには、以下の手法が使用された。

TOEに低レベルの攻撃者に悪用可能な脆弱性の無いこと確認する。

STで規定される使用環境で残存脆弱性があるかどうか確認する。

c. 実施テストの範囲

開発者テストのサンプリングによるテストを18項目、評価者が独自に考案した独立テストを10項目、評価者が考案した侵入テストを6項目、計34項目のテストを実施した。

d. 結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

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

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

当該所見報告書でなされた指摘内容が妥当であること。

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。

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。

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。

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逸れ、

	その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件が、既存の機能コンポーネントを使用することができない根拠が示されていることと、CCパート2と同じスタイル、同等の詳細レベルで表現されていることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件が、依存性のすべてを識別し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、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.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ータ、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。
脆弱性評価	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、提供されたガイドランスが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、ガイドラ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、提供されたガイドラ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、提供されたガイドランスが、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やガイドラ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をセキュアに利用するための環境のセキュリティ対策方針であるOE.WATCH（管理者は一般利用者が不正を行わないようにTOEを監視する。又、管理者不在時には施錠することにより一般利用者が設置場所には入れないようにする。）には、攻撃者がHDDを盗難した上で、一般に存在するHDDのロックパスワードの解析サービス等を利用してHDDロックパスワードを解析し、保護資産を暴露することを防ぐ目的もある。

5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用された用語を以下に示す。

ユーザBOX	ドキュメントデータを格納するディレクトリである。
ドキュメント データ	文字や図形などの情報を電子化したデータである。
紙文書	文字や図形などの情報を持つ紙媒体の文書である。
操作パネル	bizhub PRO 950 シリーズの筐体に付属するタッチパネル式ディスプレイ及び操作ボタンの名称である。
内部ネットワー ク	bizhub PRO 950 シリーズを導入する組織のLANである。クライアントPCや各種サーバ(例えばMailサーバやFTPサーバなど)が接続されている。
外部ネットワー ク	内部ネットワーク以外のネットワーク(例えばインターネットなど)である。
SMB	Microsoft系OSにおいて、ネットワーク上でコンピュータ同士が通信を行うためのアプリケーションプロトコルである。
CSRC	公衆回線網に接続したコンピュータまたはインターネットに接続したコンピュータから、bizhub PRO 950 にアクセスし、ハードウェア保守のため印刷枚数、ジャム回数、トナー切れなどに関する情報の取得を行う。
ハードディスク ロック機能	ハードディスクを取外し他の機器で読み込みができないように、ハードディスクにパスワードを持たせる機能のことをいう。
HDDロックパ	ハードディスクロック機能でハードディスクに設定するパス

スワード	ワードのことをいう。
一般利用者	bizhub PRO 950 シリーズを導入する組織に在籍し、bizhub PRO 950 シリーズのコピー/プリンタ/FAXなどに関する利用者機能を利用する。
管理者	bizhub PRO 950 シリーズを導入する組織に在籍し、bizhub PRO 950 シリーズの運用管理を行う。bizhub PRO 950 シリーズが提供する運用管理の機能を利用する。
CE	bizhub PRO 950 シリーズの保守を委託されている企業に在籍する。CEはbizhub PRO 950 シリーズが提供する保守管理の機能を利用し、bizhub PRO 950 シリーズの保守作業を行う。責任者又は管理者とbizhub PRO 950 シリーズの保守契約を締結している。
責任者	bizhub PRO 950 シリーズを導入する組織に在籍し、管理者を選任する。
製品関係者	一般利用者、管理者及びCEを示す。

6 参照

- [1] Multi functional printer(digital copier) bizhub PRO 950 セキュリティターゲット 第5版 (2009年3月16日) コニカミノルタビジネステクノロジー株式会社
- [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] bizhub PRO 950 全体制御ソフトウェア 評価報告書 第1.4版 2009年4月15日 一般社団法人 ITセキュリティセンター 評価部