Multi functional printer
(digital copier)
bizhub PRO C6500
セキュリティターゲット
第13版

2007 年 2 月 15 日

コニカミノルタビジネステクノロジーズ株式会社

－ 更新履歴 －

改訂 版数	改訂内容	承認者	審査者	作成者
1	・ 新規作成	2006.8.04 小林 千春	2006.8.04 安田 和夫	2006.8.04 新井 浩之
2	・ 是正要請による修正	2006.10.17 小林 千春	2006.10.17 安田 和夫	2006.10.17 新井 浩之
3	・ 是正要請による修正	2006.11.2 小林 千春	2006.11.2 安田 和夫	2006.11.2 工藤 公生
4	・ 是正要請による修正	2006.11.6 小林 千春	2006.11.6 安田 和夫	2006.11.6 工藤 公生
5	・ 是正要請による修正	2006.11.25 小林 千春	2006.11.25 安田 和夫	2006.11.25 工藤 公生
6	・ 是正要請による修正	2006.11.29 小林 千春	2006.11.29 安田 和夫	2006.11.29 工藤 公生
7	・ バージョンアップ A03U0Y0-00I1-G00-15	2006.12.25 小林 千春	2006.12.25 安田 和夫	2006.12.25 工藤 公生
8	・ TOE 作成日の修正	2006.12.28 小林 千春	2006.12.28 安田 和夫	2006.12.28 工藤 公生
9	・ 是正要請による修正	2007.1.11 小林 千春	2007.1.11 安田 和夫	2007.1.11 工藤 公生
10	・ 是正要請による修正	2007.1.15 小林 千春	2007.1.15 安田 和夫	2007.1.15 工藤 公生
11	・ 是正要請による修正	2007.1.17 小林 千春	2007.1.17 安田 和夫	2007.1.17 工藤 公生
12	・ 是正要請による修正	2007.2.06 小林 千春	2007.2.06 安田 和夫	2007.2.06 工藤 公生
13	・ 是正要請による修正	2007.2.15 小林 千春	2007.2.15 安田 和夫	2007.2.15 工藤 公生

- 目次 -

－ 図目次 －

－ 表目次 －

1. ST 概説

1.1. ST 識別

1.1.1. ST の識別と管理

名称: Multi functional printer(digital copier) bizhub PRO C6500 セキュリティターゲット

バージョン: 第13 版

作成日: 2007 年 2 月 15 日

作成者: コニカミノルタビジネステクノロジーズ株式会社

1.1.2. TOE の識別と管理

名称: 日本 : bizhub PRO C6500　画像制御プログラム

海外 : bizhub PRO C6500　Image Control Program

注 1)Image Control Program は画像制御プログラムの、
英語名称であり、それぞれ名称が異なるだけで、同一物である。

注2)bizhub PRO C6500 操作部での識別は日本語表示の場合
「画像制御 I1」、英語表示の場合「Image Control I1」である。

バージョン: A03U0Y0-00I1-G00-15

作成日: 2006/12/26

作成者: コニカミノルタビジネステクノロジーズ株式会社

1.1.3. 使用する CC のバージョン

CC バージョン 2.3, ISO/IEC 15408:2005
Interpretations-0512

注)日本語訳は以下の資料を利用する。

- 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
- 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-2005-002
- 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-2005-003
- 補足-0512

1.2. ST 概要

本 ST は、コニカミノルタビジネステクノロジーズ株式会社製デジタル複合機「bizhub PRO C6500」(以降 bizhub PRO C6500 シリーズと記述する)に搭載する「bizhub PRO C6500 画像制御プログラム」につ

いて記述している。

bizhub PRO C6500 画像制御プログラムは、コピー/プリンタなどを活用した機能において、bizhub PRO C6500 シリーズ内部の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 1 時保存する媒体である HDD(ハードディスク装置)から不正にデータが読み出される危険性に対して、ロックパスワードによる保護機能を提供し、bizhub PRO C6500 シリーズを利用する組織の情報漏洩の防止に貢献する。

1.3. CC 適合

パート 2 適合

パート 3 適合

EAL3 適合

1.4. 参考資料

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 2005 Version 2.3 CCMB-2005-003-003
- Interpretations-0512
- 補足-0512
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 2005/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 2005/12

2. TOE 記述

2.1. TOE 種別

ネットワーク機能を搭載したデジタル複合機のソフトウェア製品

2.2. 用語説明

No.	用語	説明
1	ドキュメントデータ	ドキュメントデータは、文字や図形などの情報を電子化したデータである。
2	紙文書	紙文書は、文字や図形などの情報を持つ紙媒体の文書である。
3	一時保存	入力されたドキュメントデータは紙文書に印刷されるまでの間に、DRAM/HDD に一時的に保存される。
4	操作パネル	操作パネルは、bizhub PRO C6500 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。
5	内部ネットワーク	内部ネットワークは、bizhub PRO C6500 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。
6	外部ネットワーク	外部ネットワークは、内部ネットワーク(No.5 参照)以外のネットワーク(例えばインターネットなど)である。

2.3. TOE 概要

TOE は、bizhub PRO C6500 画像制御プログラムである。TOE を搭載する bizhub PRO C6500 シリーズは、ネットワーク機能を搭載したデジタル複合機である。TOE はコピー/プリンタなどを活用した機能、bizhub PRO C6500 シリーズを運用管理するための機能及び bizhub PRO C6500 シリーズを保守管理するための機能を提供する。bizhub PRO C6500 シリーズの利用環境として『図 2.1 bizhub PRO C6500 シリーズの利用環境』に示すオフィスを想定する。

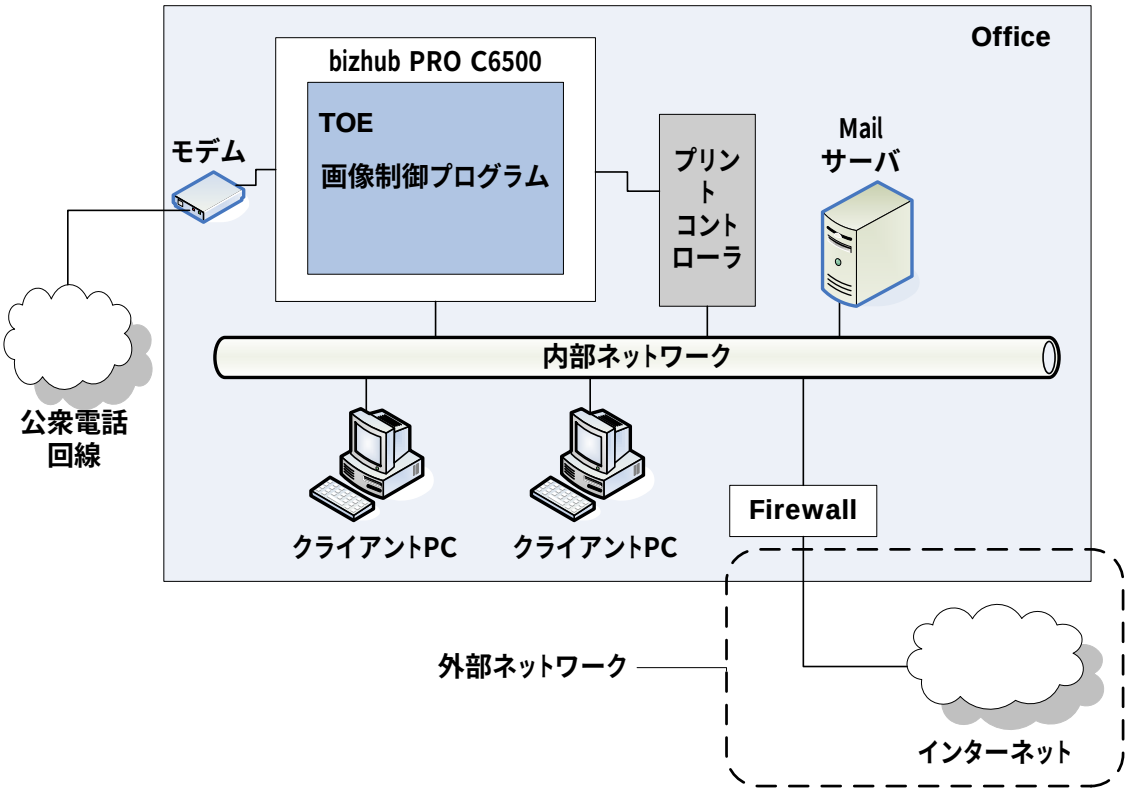

図 2.1 bizhub PRO C6500 シリーズの利用環境

TOE を搭載する bizhub PRO C6500 シリーズは、『図 2.1 bizhub PRO C6500 シリーズの利用環境』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 C6500 シリーズがデータを送信する Mail サーバと接続されている。TOE は、クライアント PC、及び Mail サーバに対してドキュメントデータを送受信する機能は持たない。また、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。

2.4. bizhub PRO C6500 シリーズの関連者と役割

bizhub PRO C6500 シリーズの関連者と役割を以下に示す。

- 一般利用者

  一般利用者は、TOE が提供するコピー/プリンタなどに関する利用者機能を利用する。

  一般利用者としては、IT の基礎知識をもっており、公開された情報を使って攻撃はできるが、公開されていない新たな攻撃手法を考案することはできないことを想定する。

- 管理者

  管理者は、bizhub PRO C6500 シリーズを導入する組織に在籍し、bizhub PRO C6500 シリーズの運用管理を行う。TOE が提供する運用管理の機能を利用する。

- 責任者

  責任者は、bizhub PRO C6500 シリーズを導入する組織に在籍し、管理者を選任する。
- CE

  CE は、bizhub PRO C6500 シリーズの保守を委託されている企業に在籍する。CE は TOE が提供する保守管理の機能を利用し、bizhub PRO C6500 シリーズの保守作業を行う。責任者又は管理者と bizhub PRO C6500 シリーズの保守契約を締結している。

なお、一般利用者、管理者及び CE を製品関係者とする。

2.5. TOE の構成

本 TOE の構成を『図 2.2 TOE の構成』に示す。

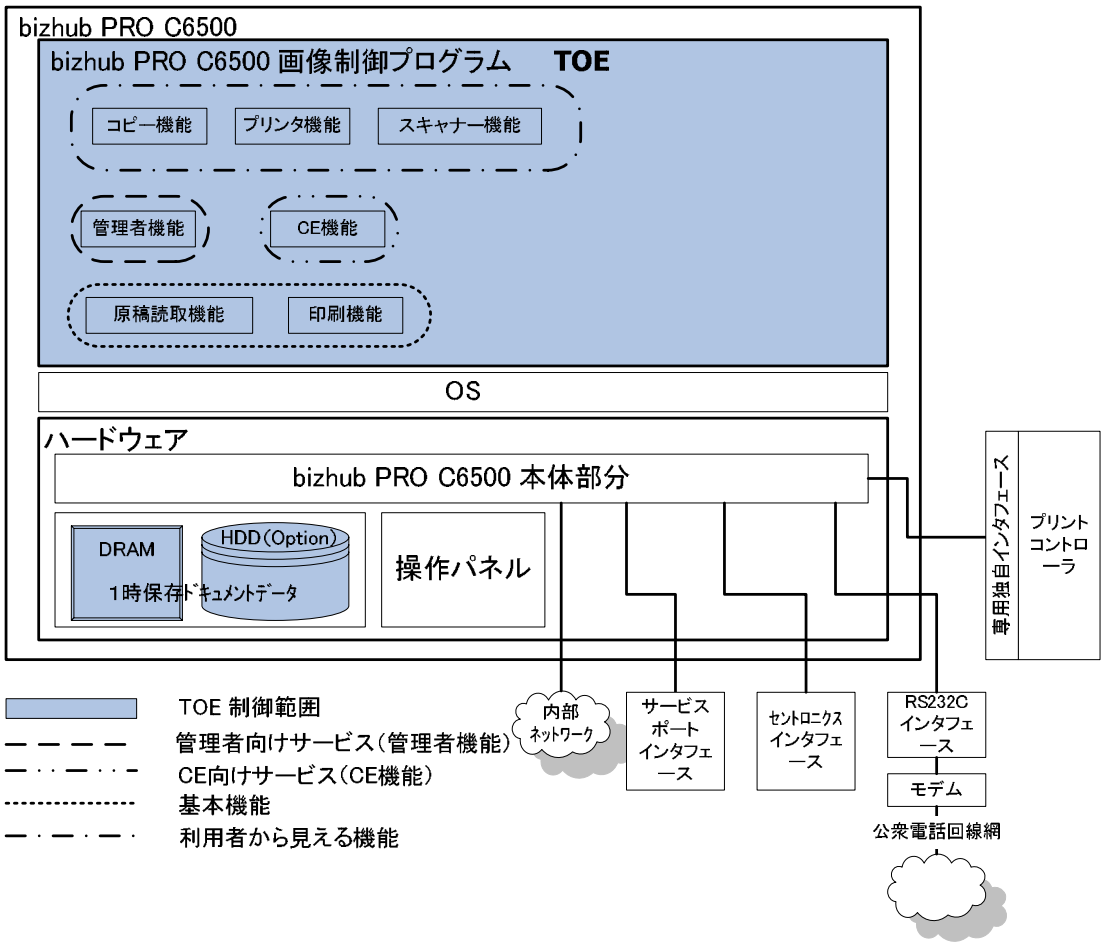

図 2.2 TOE の構成

bizhub PRO C6500 シリーズは、ハードウェア、bizhub PRO C6500 画像制御プログラムから構成される。ハードウェアは、bizhub PRO C6500 シリーズ本体部分、DRAM/HDD 部分、操作パネル及びネットワーク

カード、各種インタフェースである。なお、HDD は、オプションユニットであり標準では搭載されていない。HDD 部分には、4 個の HDD が搭載され、YMCK 各色に1個の HDD を割り当てられている。以下、4 個の HDD をまとめて HDD と呼ぶことにする。bizhub PRO C6500 シリーズ本体部分は、紙文書を電子化するための原稿読取機能と印刷用の紙に文字や図形を印刷する印刷機能を搭載している。プリントコントローラは PC からの受信データを印刷用の紙に文字や図形を印刷するためのデータ変換を行っている。プリントコントローラと本体の間は、専用の独自なインタフェースにて接続されている。サービスポートインタフェースとセントロニクスインタフェースは、TOE の設置生成を行う際に保守用のコンピュータと接続するためのインタフェースであり、このインタフェースからドキュメントデータへのアクセスはできない。DRAM/HDD 部分は、ドキュメントの一時的な格納を行う。bizhub PRO C6500 画像制御プログラムは、OS 上で動作する。OS は、ハードウェア及び bizhub PRO C6500 画像制御プログラムに対するドキュメントデータの入出力を制御する。画像制御プログラムは、管理機能、CE 機能、利用者機能（表 2.1 に記述するように、コピー機能、プリンタ機能、スキャナー機能および基本機能の原稿読取機能、印刷機能）を制御する。

bizhub PRO C6500 シリーズは、製品関係者による操作パネルからの処理要求及び製品関係者によるネットワーク経由の処理要求を受け付け、TOE はその処理要求を実行する。

2.6. bizhub PRO C6500 画像制御プログラムの機能構成

bizhub PRO C6500 画像制御プログラムは以下の機能を有する。

なお、セキュリティ機能は 管理者の識別・認証機能、セキュリティ強化モード、CE の識別・認証機能、サービス設定モードである。

2.6.1. 基本機能

コピー機能時は、紙文書を読み取ったドキュメントデータ（電子データ）は、一旦 DRAM 及び HDD の一時保存領域に格納した後、一時保存領域から読み出し印刷される。プリンタ機能時は、クライアント PC からのドキュメントデータは外部のプリントコントローラにてデータ変換された後に、bizhub PRO C6500 シリーズへと入力され、一旦 DRAM 及び HDD の一時保存領域に格納した後、一時保存領域から読み出し印刷される。なお、一時保存DRAMに一時格納されたデータは、電源の OFF と共に消える。スキャナー機能時は、入力された紙文書を読み取った電子データは一時保存をせずに外部のプリントコントローラへと送信される。

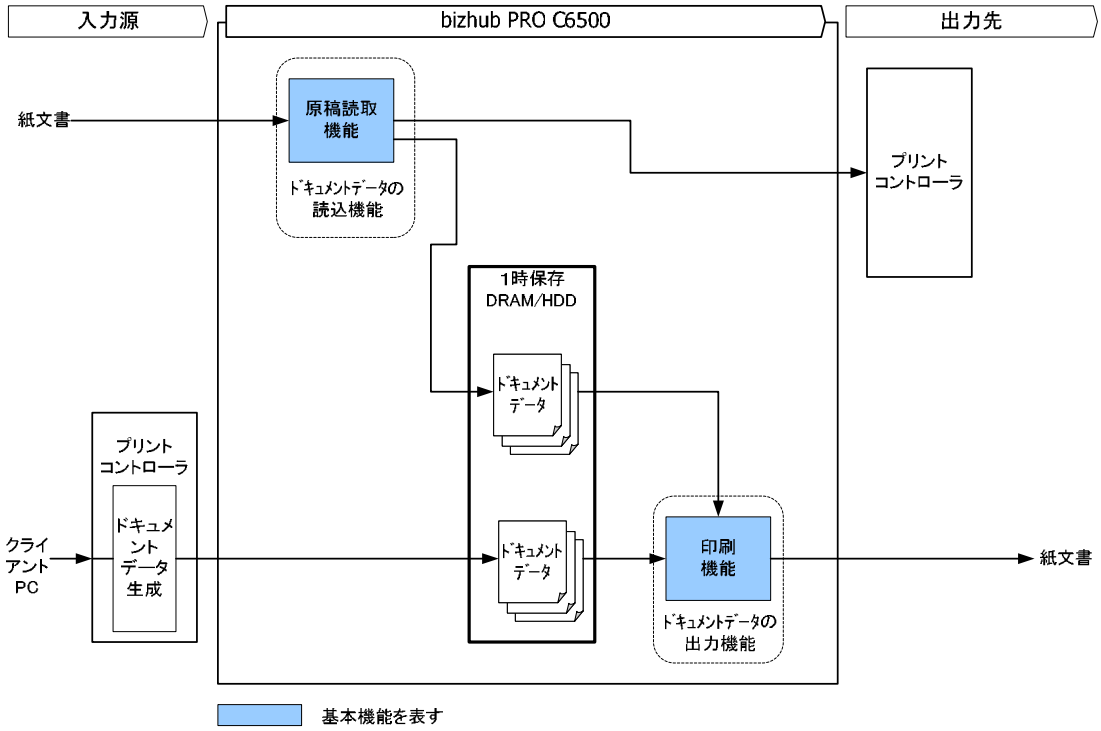

図 2.3 基本機能の処理概念

『表 2.1 利用者機能と基本機能の対応』に示すとおり、利用者機能は基本機能を実施することで実現する。以降、基本機能について説明する。

表 2.1 利用者機能と基本機能の対応

No	利用者機能	基本機能
1	コピー機能	原稿読取機能と印刷機能
2	プリンタ機能	印刷機能
3	スキャナー機能	原稿読取機能

『図 2.3 基本機能の処理概念』に示した機能を以下に述べる。

(1) 原稿読取機能

一般利用者により操作パネルから指示された、紙文書の情報を読取り、電子データに変換する。コピー機能時は、その電子データを一時保存領域に格納する。また、スキャナー機能時は、その電子データをそのまま外部プリントコントローラに送信する機能。

(2) 印刷機能

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

2.6.2. 管理機能

管理機能は、識別と認証が成功した場合のみ管理者に利用を許可する（セキュリティ機能）。本機能は操作パネルからのみ利用できる。管理者は、管理機能を使用して、管理者パスワードの変更、セキュリティ強化モードの設定（セキュリティ機能）、TOE のネットワーク情報の設定、TOE が有する機能の動作設定を行う。また、管理機能は、監査情報の印刷、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。

- セキュリティ強化モード（セキュリティ機能）

  管理者は、セキュリティ強化モードを有効に設定する事によりTOE 提供機能をよりセキュアな状態とする。セキュリティ強化モードの設定は識別・認証された管理者のみに制限される。セキュリティ強化モード有効状態においては、オプションの HDD が装着されているならば、HDD はロックパスワードが設定され、読み書きの出来ないロック状態となる。このことにより bizhub PRO C6500 シリーズが電源 Off 状態にては、HDD はロック状態であり、他からのアクセスを拒否する（読み書きが行えない）。bizhub PRO C6500 シリーズが電源 ON した時点にて TOE はロックパスワードにて HDD に認証及びロック解除の指示を行い、HDD にて正当な TOE であることの確認を行い HDD のロック状態を解除して、HDD の読み書きを可能とする。また、HDD の有無に関わらず内部ネットワークは、後述の CSRC 機能のみを有効とし、他の全ての内部ネットワーク機能は無効となる。さらに、非セキュリティ機能として、セキュリティに関連する設定操作に対し、その日時、操作結果が監査ログとして内部記録され、管理者のみが閲覧可能である。

  設置時においては予め各 bizhub PRO C6500 シリーズ固有の HDD ロックパスワードが bizhub PRO C6500 シリーズに記憶されている（HDD には設定されていない）ので、管理者は HDD ロックパスワードを変更する必要がある。

2.6.3. CE 機能

CE 機能は、識別と認証が成功した場合のみ以下の機能の利用を CE に許可する（セキュリティ機能）。

- サービス設定モード（セキュリティ機能）

  CE は、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。操作パネルから操作し、管理者のパスワード登録を実施する機能を使用できるのは、識別・認証された CE のみであり、管理者のパスワード変更を実施する機能を使用できるのは、識別・認証された CE 及び管理機能での管理者に限定される。

  管理者のみにセキュリティ強化モードの設定を許しているため、その管理者の設定権限を持つ CE の識別と認証を行うことにより管理者の保証を行う。

- CSRC(CS Remote Care)

  CE は公衆回線網に接続したコンピュータから、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 C6500 シリーズにアクセスし、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。CSRC は、RS232C インタフェースまたは E-Mail インタフェースで行われる。RS232C インタフェース、すなわちモデムとの転送規格は独自通信プロトコルを用いている。E-Mail には、独自のメッセージ通信プロトコルを用いており、この CSRC は、ドキュメントデータへのインタフェースを持たない。

2.7. 保護対象となる資産

TOE の保護対象となる資産は一時保存 HDD 内ドキュメントデータである。

なお、DRAM 内ドキュメントデータに関しては、外部からDRAMへのアクセスは行えない、電源Offと共にDRAM内一時保存データは消えるので、データ漏洩の脅威は無い。

2.8. TOEが提供しない機能

ドキュメントデータのオリジナルデータは、利用者がクライアントPCや紙で所有しているので、TOEはドキュメントデータの削除に対する防止は行わない。

3. TOE セキュリティ環境

3.1. 前提条件

ASM.SECMOD　セキュリティ強化モードの動作設定条件

管理者はセキュリティ強化モードを有効化する。

bizhub PRO C6500 シリーズにはオプションの HDD が装着されている。

ASM.NET　内部ネットワークの設置条件

TOE が搭載された bizhub PRO C6500 シリーズを設置する内部ネットワークが外部ネットワークと接続される場合は、外部ネットワークから bizhub PRO C6500 シリーズへアクセスできない。

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.SECRET　秘密情報に関する運用条件

TOE の利用において管理者パスワード及び HDD ロックパスワードは、管理者から漏洩しない。又、CE パスワードは CE から漏洩しない。

3.2. 脅威

T.HDDACCESS　HDD への不正なアクセス

一般利用者がセキュリティ強化モードに関する設定を変更し、HDDに不正な装置を接続してドキュメントデータが読み出される。

3.3. 組織のセキュリティ方針

組織のセキュリティ方針は設けない。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

O.IA 管理機能又はCE機能利用時の識別と認証

TOE は、TOE にアクセスを試みる管理者、および CE を識別認証する。

O.MANAGE 管理機能の提供

TOE は、セキュリティ強化モードを有効化することにより、OE.HDD にて用意される HDD をセキュアに管理する機能（HDD ロックパスワードを管理・設定する機能）を提供する。また、セキュリティ強化モードの管理を管理者に制限する。

4.2. 環境のセキュリティ対策方針

OE.SECMOD セキュリティ強化モード機能の動作設定

管理者は、bizhub PRO C6500 シリーズにオプションの HDD を装着して、セキュリティ強化モードの設定を有効化する。

OE.NET ネットワークの管理

管理者は、ファイアウォールで保護された内部ネットワーク環境にTOEを接続する。

OE.ADMIN 管理者の条件

責任者は、不正を行わない人物を管理者として選任する。

OE.HDD HDD の保護

ロックパスワードを有した HDD を使用する。

OE.CE CE の保証

責任者又は管理者は、CE と保守契約を締結する。保守契約には、不正な行為をしない旨を明記する。

OE.SECRET 秘密情報の適切な管理

管理者は、以下に示す運用を実施する。

・管理者パスワード、HDD ロックパスワードに推測可能な値を設定しない。

・管理者パスワード、HDD ロックパスワードを秘匿する。

CE は以下に示す運用を実施する。

・CE パスワードに推測可能な値を設定しない。

・CE パスワードを秘匿する。

・CE が管理者パスワードを変更した場合は、管理者に速やかに変更させる。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

FIA_UID.2　　アクション前の利用者識別

下位階層:FIA_UID.1

FIA_UID.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　:「利用者」→ 管理者、及びCE

依存性:なし

FIA_UAU.2　　アクション前の利用者認証

下位階層：FIA_UAU.1

FIA_UAU.2.1

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

詳細化　：「利用者」→ 管理者、及びCE

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.7　　保護された認証フィードバック

下位階層：なし

FIA_UAU.7.1

TSFは、認証を行っている間、[割付：フィードバックのリスト]だけを利用者に提供しなければならない。

[割付：フィードバックのリスト]

- 操作者が入力するパスワード文字数分のダミー文字(*)

依存性：FIA_UAU.1　認証のタイミング

FIA_AFL.1　　認証失敗時の取り扱い

下位階層:なし

FIA_AFL.1.1

TSFは、[割付:認証事象のリスト]に関して、[選択: [割付: 正の整数値],「[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値]」]回の不成功認証試行が生じたときを検出しなければならない。

[割付:認証事象のリスト]

- 管理者、及びCEに対する不成功認証

[選択: [割付: 正の整数値],「[割付: 許容可能な値の範囲]内における管理者設定可能な正の整数値]」]

- 1

FIA_AFL.1.2

不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付:アクションのリスト]をしなければならない。

[割付:アクションのリスト]

- 認証不成功となった管理者、又はCEに対して、次の認証試行を5秒間実行しない。

依存性:FIA_UAU.1 認証のタイミング

FIA_SOS.1[1]　　秘密の検証

下位階層:なし

FIA_SOS.1.1

TSF は、秘密が[割付:定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付:定義された品質尺度]

- パスワードの品質尺度を以下のように定義する。
  パスワード長: 8 文字
  構成文字種　:半角英大文字、半角英小文字、半角数字
  許容条件　　:一世代前のパスワードと同一のパスワードを禁止

詳細化 :「秘密」→
「管理者のパスワード」及び「CE のパスワード」

依存性:なし

FIA_SOS.1[2]　　秘密の検証

下位階層:なし

FIA_SOS.1.1

TSF は、秘密が[割付:定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付:定義された品質尺度]

- パスワードの品質尺度を以下のように定義する。

  パスワード長: 8 から 32 文字

  構成文字種　:半角英大文字、半角英小文字、半角数字

  許容条件　　:無し

詳細化 :「秘密」→「HDD ロックパスワード」

依存性:なし

FMT_MTD.1[1]　TSF データの管理

下位階層:なし

FMT_MTD.1.1

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- 管理者のパスワード

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]
その他の操作

[割付:その他の操作]

- 登録

[割付:許可された識別された役割]

- CE

依存性:FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1[2]　TSF データの管理

下位階層:なし

FMT_MTD.1.1

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- CE のパスワード

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]
改変

[割付:許可された識別された役割]

- CE

依存性:FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1[3]　TSF データの管理

下位階層:なし

FMT_MTD.1.1

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- 管理者パスワード

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]

改変

[割付:許可された識別された役割]

- 管理者、CE

依存性:FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMR.1[1]　セキュリティ役割

下位階層:なし

FMT_SMR.1.1

TSFは、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付:許可された識別された役割]

- 管理者

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性:FIA_UID.1 識別のタイミング

FMT_SMR.1[2]　セキュリティ役割

下位階層:なし

FMT_SMR.1.1

TSFは、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付:許可された識別された役割]

- CE

FMT_SMR.1.2

TSFは、利用者を役割に関連づけなければならない。

依存性:FIA_UID.1 識別のタイミング

FMT_MOF.1　　セキュリティ機能のふるまいの管理

下位階層:なし

FMT_MOF.1.1

TSFは、機能[割付:機能のリスト][選択:のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付:許可された識別された役割]に制限しなければならない。

[割付:機能のリスト]

- 機能1
  - 機能1:　セキュリティ強化モード

[選択:のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

を動作させる、を停止する

[割付:許可された識別された役割]

- 管理者

依存性:FMT_SMF.1　管理機能の特定

FMT_SMR.1　セキュリティ役割

FMT_SMF.1　　管理機能の特定

下位階層:なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付:TSF によって提供されるセキュリティ管理機能のリスト]

[割付:TSF によって提供されるセキュリティ管理機能のリスト]

- CE による管理者パスワード登録
- CE による管理者パスワードの変更
- CE による CE パスワードの変更
- 管理者による管理者パスワードの変更
- 管理者によるセキュリティ強化モードの設定

依存性:なし

FPT_RVM.1　　TSP の非バイパス性

下位階層:なし

FPT_RVM.1.1

TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性:なし

FPT_SEP.1　　TSF ドメイン分離

下位階層:なし

FPT_SEP.1.1

TSFは、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性:なし

FDP_ACC.1　　サブセットアクセス制御

下位階層:なし

FDP_ACC.1.1

TSF は、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

管理機能アクセス制御　操作リスト

サブジェクト	オブジェクト	操作
利用者を代行するタスク	HDDロックパスワードオブジェクト	改変

[割付: アクセス制御 SFP]

管理機能アクセス制御

依存性:FDP_ACF.1　セキュリティ属性によるアクセス制御

FDP_ACF.1　　セキュリティ属性によるアクセス制御

下位階層:なし

FDP_ACF.1.1

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

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]

＜サブジェクト＞		＜サブジェクト属性＞
・利用者を代行するタスク	＝＞	・管理者属性

＜オブジェクト＞

・HDD ロックパスワードオブジェクト

[割付: アクセス制御 SFP]

管理機能アクセス制御

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

・管理者属性を持つ利用者を代行するタスクは、HDD ロックパスワードオブジェクトを改変操作することが許可される。

FDP_ACF.1.3

TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない:[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認す

る規則]

なし

FDP_ACF.1.4

TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]

なし

依存性:FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

5.1.2. TOE セキュリティ保証要件

本 TOE は、商用の製品において、十分なレベルの品質保証レベルである EAL3 を主張する。EAL3 に対応する TOE セキュリティ保証要件を『**表 5.1 TOE セキュリティ保証要件一覧**』に示す。

表 5.1 TOE セキュリティ保証要件一覧

保証クラス	保証要件
構成管理	ACM_CAP.3 許可の管理
	ACM_SCP.1 TOE の CM 範囲
配付と運用	ADO_DEL.1 配付手続き
	ADO_IGS.1 設置、生成、及び立ち上げ手順
開発	ADV_FSP.1 非形式的機能仕様
	ADV_HLD.2 セキュリティ実施上位レベル設計
	ADV_RCR.1 非形式的対応の実証
ガイダンス文書	AGD_ADM.1 管理者ガイダンス
	AGD_USR.1 利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1 セキュリティ手段の識別
テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト:上位レベル設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル
脆弱性評定	AVA_MSU.1 ガイダンスの検査
	AVA_SOF.1 TOE セキュリティ機能強度評価
	AVA_VLA.1 開発者脆弱性分析

FIA_UAU.2[E] アクション前の利用者認証

下位階層:FIA_UAU.1

FIA_UAU.2.1[E]

TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を認証することを要求しなければならない。

詳細化 :「TSF」 → 「HDD」

依存性:なし

5.3. セキュリティ機能強度

TOE 機能強度主張が対象とするのは以下の2つのパスワードメカニズムであり、本 ST において対象とする TOE の機能コンポーネントは対応する以下の6つである。

パスワードメカニズムおよび、対応する TOE 機能コンポーネント

① 管理者パスワード・CE パスワード認証機能

FIA_UID.2、FIA_UAU.2、FIA_UAU.7、FIA_AFL.1、FIA_SOS.1[1]

② HDD ロックパスワード認証機能

FIA_SOS.1[2]

TOE コンポーネント機能

FIA_UID.2（利用者識別）

FIA_UAU.2（利用者認証）

FIA_UAU.7（保護されたフィードバック）

FIA_SOS.1[1]（秘密の検証）

FIA_SOS.1[2]（秘密の検証）

FIA_AFL.1（認証失敗時の取り扱い）

上記6つの TOE 機能要件に対して、SOF－基本を主張する。また、TOE の最小機能強度に対して、SOF－基本を主張する。

6. TOE 要約仕様

6.1. TOE セキュリティ機能

6.1.1. 識別認証

識別認証機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ機能要件
IA.ADM_ADD 管理者の登録	IA.ADM_ADD は、管理者を TOE に登録する。CE のみが IA.ADM_ADD を操作する。CE は、管理者のパスワードを登録する。 IA.ADM_ADD は、管理者登録のインタフェースを提供する。管理者登録のインタフェースは、登録する管理者に対応するパスワードの入力を要求する。 管理者が入力するパスワードに対して、以下の規則に従い、許容値を検証する。 • パスワードは 8 文字とする • パスワードは半角英大文字、半角英小文字、半角数字で構成する • パスワードは一世代前のパスワードと同一の値を禁止する 許容値の検証において、規則に従っている場合、管理者を登録する。規則に従っていない場合、登録を拒否する。	FIA_SOS.1[1] FMT_MTD.1[1] FMT_SMF.1 FPT_RVM.1 FPT_SEP.1
IA.ADM_AUTH 管理者の識別と認証	IA.ADM_AUTH は、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。 IA.ADM_AUTH は、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。管理者の識別と認証のインタフェースは、IA.ADM_ADD で登録、IA_PASS で変更したパスワードの入力を要求する。IA.ADM_AUTH は、管理者の識別と認証のインタフェースの表示により管理者であることを識別し、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。管理者がパスワードを入力する際は、入力したパスワードの代わりにダミー文字(＊)を表示する。	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1 FPT_SEP.1 FMT_SMR.1[1]

	認証不成功時には、5 秒後に管理者の識別と認証のインタフェースを提供する。	
IA.CE_AUTH CE の識別と認証	IA.CE_AUTH は、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。 IA.CE_AUTH は、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。IA_PASS で変更したパスワードの入力を要求する。IA.CE_AUTH は CE の識別と認証のインタフェースの表示により CE であることを識別し、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。CE がパスワードを入力する際は、入力したパスワードの代わりにダミー文字(＊)を表示する。 認証不成功時には、5 秒後に CE の識別と認証のインタフェースを提供する。	FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FIA_AFL.1 FPT_RVM.1 FPT_SEP.1 FMT_SMR.1[2]
IA.PASS パスワードの変更	IA.PASS は、管理者、及び CE の認証情報である管理者のパスワード、及び CE のパスワードを変更する。 IA.PASS は、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 :管理者のパスワード 製品関係者が入力するパスワードに対して、以下の規則に従い許容値を検証する。 • CE 及び管理者パスワードは 8 文字とする • パスワードは半角英大文字、半角英小文字、半角数字で構成する • パスワードは一世代前のパスワードと同一の値を禁止する 許容値の検証において、規則に従っている場合、パスワードを変更する。	FIA_SOS.1[1] FMT_MTD.1[2] FMT_MTD.1[3] FMT_SMF.1 FPT_RVM.1 FPT_SEP.1

6.1.2. 管理支援

管理支援機能は、以下のセキュリティ機能群を備える。

機能名称	セキュリティ機能の仕様	TOE セキュリティ 機能要件
MNG.MODE セキュリティ強化モードの設定	MNG.MODE は、管理者にのみセキュリティ強化モードを有効化する機能およびそれを停止にする機能を許可し実行する。	FMT_MOF.1 FPT_RVM.1 FPT_SEP.1 FMT_SMF.1
MNG.HDD HDD ロックパスワード機能	MNG.HDD は、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 管理者が入力する HDD ロックパスワードに対して以下の規則に従い、許容値を検証する。 ・ パスワードは 8 文字から 32 文字とする。 ・ パスワードは半角英大文字、半角英小文字、半角数字で構成する。 許容値の検証において、規則に従っている場合、HDD 装置に HDD ロックパスワードを設定／変更する。規則に従っていない場合、変更を拒否する。	FIA_SOS.1[2] FDP_ACC.1 FDP_ACF.1 FPT_RVM.1 FPT_SEP.1

6.2. セキュリティ機能強度

本 TOE は、パスワードメカニズムに対し SOF-基本のセキュリティ機能強度を主張する。該当するパスワードメカニズムは、識別認証機能(IA.ADM_AUTH, IA.CE_AUTH, IA.ADM_ADD 及び IA.PASS)及び管理支援機能(MNG.HDD)である。

6.3. 保証手段

開発者は、セキュリティ保証要件及び開発組織が規定した開発規約に従って開発する。EAL3 を満たすセキュリティ保証要件のコンポーネント及び保証要件に対応する関連文書を『表 6.1 EAL3 の保証要件と関連文書』に示す。

表 6.1 EAL3 の保証要件と関連文書

保証要件項目	コンポーネント	関連文書
構成管理	ACM_CAP.3	bizhub PRO C6500 構成管理書 bizhub PRO C6500 設計文書一覧 bizhub PRO C6500 ソースｺｰﾄﾞ一覧
	ACM_SCP.1	bizhub PRO C6500 構成管理書 bizhub PRO C6500 設計文書一覧 bizhub PRO C6500 ソースｺｰﾄﾞ一覧
配付と運用	ADO_DEL.1	bizhub PRO C6500 配布規定書 bizhub PRO C6500 インストールマニュアル bizhub PRO C6500 ユーザーズガイド コピー編 bizhub PRO C6500 ユーザーズガイド POD管理者編 bizhub PRO C6500 ユーザーズガイド セキュリティ編 bizhub PRO C6500 サービスマニュアルフィールドサービス bizhub PRO C6500 User's Guide Copier bizhub PRO C6500 User's Guide POD Administrator's Reference bizhub PRO C6500 User's Guide Security bizhub PRO C6500 SERVICE MANUAL Field Service bizhub PRO C6500 INSTALLATION MANUAL

	ADO_IGS.1	bizhub PRO C6500 導入・運用規定書 bizhub PRO C6500 インストールマニュアル bizhub PRO C6500 ユーザーズガイド コピー編 bizhub PRO C6500 ユーザーズガイド POD管理者編 bizhub PRO C6500 ユーザーズガイド セキュリティ編 bizhub PRO C6500 サービスマニュアルフィールドサービス bizhub PRO C6500 SERVICE MANUAL Field Service bizhub PRO C6500 INSTALLATION MANUAL bizhub PRO C6500 User's Guide Copier bizhub PRO C6500 User's Guide POD Administrator's Reference bizhub PRO C6500 User's Guide Security
開発	ADV_FSP.1	bizhub PRO C6500 機能仕様書
	ADV_HLD.2	bizhub PRO C6500 機能仕様書
	ADV_RCR.1	bizhub PRO C6500 機能対応書
ガイダンス文書	AGD_ADM.1	bizhub PRO C6500 インストールマニュアル bizhub PRO C6500 ユーザーズガイド コピー編 bizhub PRO C6500 ユーザーズガイド POD管理者編 bizhub PRO C6500 ユーザーズガイド セキュリティ編 bizhub PRO C6500 サービスマニュアルフィールドサービス bizhub PRO C6500 INSTALLATION MANUAL bizhub PRO C6500 User's Guide Copier bizhub PRO C6500 User's Guide POD Administrator's Reference bizhub PRO C6500 User's Guide Security bizhub PRO C6500 SERVICE MANUAL Field Service

	AGD_USR.1	bizhub PRO C6500 ユーザーズガイド コピー編 bizhub PRO C6500 ユーザーズガイド POD管理者編 bizhub PRO C6500 ユーザーズガイド セキュリティ編 bizhub PRO C6500 User's Guide Copier bizhub PRO C6500 User's Guide POD Administrator's Reference bizhub PRO C6500 User's Guide Security
ライフサイクルサポート	ALC_DVS.1	bizhub PRO C6500 開発セキュリティ規定書
テスト	ATE_COV.2	bizhub PRO C6500 機能分析書
	ATE_DPT.1	bizhub PRO C6500 機能分析書
	ATE_FUN.1	bizhub PRO C6500 機能テスト書
	ATE_IND.2	無し(bizhub PRO C6500 テストセット)
脆弱性評定	AVA_MSU.1	bizhub PRO C6500 導入・運用規定書 bizhub PRO C6500 インストールマニュアル bizhub PRO C6500 ユーザーズガイド コピー編 bizhub PRO C6500 ユーザーズガイド POD管理者編 bizhub PRO C6500 ユーザーズガイド セキュリティ編 bizhub PRO C6500 サービスマニュアルフィールドサービス bizhub PRO C6500 INSTALLATION MANUAL bizhub PRO C6500 User's Guide Copier bizhub PRO C6500 User's Guide POD Administrator's Reference bizhub PRO C6500 User's Guide Security bizhub PRO C6500 SERVICE MANUAL Field Service
	AVA_SOF.1	bizhub PRO C6500 脆弱性分析書
	AVA_VLA.1	bizhub PRO C6500 脆弱性分析書

7. PP 主張

本 ST が準拠する PP はない。

8. 根拠

8.1. セキュリティ対策方針根拠

脅威に対応するセキュリティ対策方針の関係を『表 8.1 脅威及び前提条件とセキュリティ対策方針の対応』に示す。

表 8.1 脅威及び前提条件とセキュリティ対策方針の対応

脅威/前提条件 ＼ セキュリティ対策方針	T.HDDACCESS	ASM.SECMOD	ASM.NET	ASM.ADMIN	ASM.CE	ASM.SECRET
O.IA(利用時の識別と認証)	✔					
O.MANAGE(管理機能の提供)	✔					
OE.SECMOD(セキュリティ強化モードの動作設定)		✔				
OE.NET(ネットワークの管理)			✔			
OE.ADMIN(管理者の条件)				✔		
OE.CE(CE の保証)					✔	
OE.HDD(HDD の保護)		✔				
OE.SECRET(秘密情報の適切な管理)						✔

以下に、『表 8.1 脅威及び前提条件とセキュリティ対策方針の対応』の根拠を示す。

T.HDDACCESS:HDD への不正なアクセス

TSF は O.IA で識別された正当な管理者により、O.MANAGE の管理機能で、HDD のロックパスワードの設定、変更を行う。管理者のみにセキュリティ強化モードの設定を許しているため、O.IA でその管理者の設定権限を持つ CE の識別と認証を行うことにより管理者の保証を行う。これらにより、識別・認証された管理者にのみセキュリティ強化モードに関する設定する機能を許可していることで、HDD のロックパスワー

ドが攻撃者により変更されることを防止する。

以上に示すように、脅威 T.HDDACCESS は対策方針 O.IA、O.MANAGE によって対抗できる。

ASM.SECMOD：セキュリティ強化モードの動作設定条件

TOE は OE.SECMOD によって、管理者が bizhub PRO C6500 シリーズにオプションの HDD を装着して、セキュリティ強化モードの設定を有効化するので、一般利用者は HDD が装着された状態で、そしてセキュリティ強化モードが有効化された状態で、TOE が搭載された bizhub PRO C6500 シリーズを使用できる。

また、OE.HDD によって、bizhub PRO C6500 シリーズに装着されたオプションの HDD はロックパスワード機能を有している。

以上に示すように、前提条件 ASM.SECMOD は対策方針 OE.SECMOD、OE.HDD によって実現できる。

ASM.NET：内部ネットワークの設置条件

OE.NET では、管理者はファイアウォールで保護された内部ネットワークに TOE を設置するので、内部ネットワークが外部ネットワークと接続されていても TOE へのアクセスは外部ネットワークからは出来ない。

以上に示すように、前提条件 ASM.NET は対策方針 OE.NET によって実現できる。

ASM.ADMIN：信頼できる管理者

OE.ADMIN では、管理者の条件を規定している。責任者は、不正を行わない人物を管理者に選任する。

以上に示すように、前提条件 ASM.ADMIN は対策方針 OE.ADMIN によって実現できる。

ASM.CE：保守契約

OE.CE では、TOE を導入する組織は、TOE の保守を担当する組織と CE は不正な行為を行わない旨を明記した保守契約を締結することを規定している。以上に示すように、前提条件 ASM.CE は対策方針 OE.CE によって実現できる。

ASM.SECRET　秘密情報に関する運用条件

OE.SECRET は、管理者が管理者パスワード、HDD ロックパスワードに関する運用規則を実施することを規定している。また、CE が CE パスワードに関する運用規則を実施することを規定しており、本条件は実現される。

8.2.　セキュリティ要件根拠

8.2.1.　セキュリティ機能要件根拠

セキュリティ対策方針に対する TOE セキュリティ機能要件の対応を

『**表 8.2 セキュリティ対策方針と IT セキュリティ機能要件の対応**』に示す。

表 8.2 セキュリティ対策方針と IT セキュリティ機能要件の対応

セキュリティ対策方針 / IT セキュリティ機能要件		O・IA	O・MANAGE	OE・HDD
TOE セキュリティ機能要件	FIA_UID.2	✔		
	FIA_UAU.2	✔		
	FIA_UAU.7	✔		
	FIA_AFL.1	✔		
	FIA_SOS.1[1]	✔		
	FIA_SOS.1[2]		✔	
	FMT_MTD.1[1]	✔		
	FMT_MTD.1[2]	✔		
	FMT_MTD.1[3]	✔		
	FMT_SMR.1[1]	✔	✔	
	FMT_SMR.1[2]	✔		
	FMT_MOF.1		✔	
	FPT_RVM.1	✔	✔	
	FPT_SEP.1	✔	✔	
	FMT_SMF.1	✔	✔	
	FDP_ACC.1		✔	
	FDP_ACF.1		✔	
IT 環境のセキュリティ機能要件	FIA.UAU.2[E]			✔

以下に、『**表 8.2 セキュリティ対策方針と IT セキュリティ機能要件の対応**』の根拠を示す。

O.IA：管理機能又はCE機能利用時の識別と認証

CE であることを FIA_UID.2 で識別し、CE 本人であることを FIA_UAU.2 で認証することで、正当な CE の操作であることが確認できる。

管理者であることを FIA_UID.2 で識別し、管理者本人であることを FIA_UAU.2 で認証することで、正当な管理者の操作であることが確認できる。

管理者、及び CE の認証が不成功となった場合、FIA_AFL.1 で管理者、及び CE に対して次の認証の試行を 5 秒間待たせ、不正な利用者が CE、及び管理者として識別認証成功するまでの時間を長くする。パスワードを秘匿するため、FIA_UAU.7 によりパスワード入力域に入力した字数分のダミー文字(*)を表示する。

CE は管理者のパスワードを FMT_MTD.1[1]で登録出来る。管理者のパスワードを登録することで管理者は TOE に登録され、管理者としての作業が開始できる。CE は CE 自身のパスワードを FMT_MTD.1[2]で変更することが出来るため、CE は適当な期間毎に CE のパスワードを変更することが可能となる。また、FMT_MTD.1[3]は管理者及び CE に管理者自身のパスワードを変更することを許可するため、適当な期間毎に管理者のパスワードを変更することが可能となる。CE が管理者のパスワードを登録する際、及び管理者または CE が管理者パスワードを変更する際、及び CE が CE パスワードを変更する際、パスワードは、FIA_SOS.1[1]で指定されたパスワード規則に従っているか検証されている。パスワードが変更されることで、一般利用者から入力した管理者パスワードもしくは CE パスワードが一致する可能性を低くする。

FPT_SEP.1 により CE 機能制御で想定されている認証された CE を代行するサブジェクトだけが、CE パスワード変更、管理者パスワード登録/変更制御にて規定されるオブジェクトの操作が可能であり、また管理機能制御で想定されている認証された管理者を代行するサブジェクトだけが、管理者パスワード変更制御にて規定されるオブジェクトの操作が可能である。

管理者を FMT_SMR.1[1]で、及び CE を FMT_SMR.1[2]で維持する。

パスワードの管理を FMT_SMF.1 で特定する。以上の機能は FPT_RVM.1 によりバイパスされることはない。

従って、対応するセキュリティ機能要件により対策方針 O.IA は実現可能である。

O.MANAGE：管理機能の提供

FDP_ACC.1、FDP_ACF.1 は管理者に、HDD の HDD ロックパスワードを変更し、管理する機能を提供する。これにより、HDD の不正アクセスを防ぐことができる。このパスワードは、FIA_SOS.1[2]により指定された規則に従っているか検証されている。

管理者を FMT_SMR.1[1]で維持する。以上の機能は FPT_RVM.1 によりバイパスされることはない。また、FMT_MOF.1 で管理者に、セキュリティ強化モードの起動／停止を許可する。セキュリティ強化モードの起動/停止により HDD の認証機能が起動/停止する。

FPT_SEP.1 により管理機能制御で想定されている認証された管理者を代行するサブジェクトだけが、HDD ロックパスワード変更制御及びセキュリティ強化モード起動/停止制御にて規定されるオブジェクトの操作が可能である。セキュリティ強化モードの管理を FMT_SMF.1 で特定する。

従って、対応するセキュリティ機能要件により O.MANAGE は実現可能である。

OE.HDD：HDD の保護

FIA_UAU.2[E]は、HDD の認証に成功した TOE にのみアクセスを許可する。

従って対応するセキュリティ機能要件により、OE.HDD は実現可能である。

上記に示した通りに、選択されている要件は、管理者、CE の識別認証及びそれに基づくアクセス制御（TOE セキュリティ機能要件）、アクション前の利用者認証要件（IT 環境のセキュリティ要件）であり、競合する可能性のある要件は存在しない。したがって、IT セキュリティ要件セットは内部的に一貫している。

8.2.2. TOE セキュリティ機能要件間の依存関係

TOE セキュリティ機能要件間の依存関係は『表 8.3 TOE セキュリティ機能要件間の依存関係』に示すように、No.17 を除き、必要な依存関係を満たしている。

表 8.3 TOE セキュリティ機能要件間の依存関係

No	TOE セキュリティ機能要件	下位階層	CC 規定の依存関係	ST での依存関係参照 No	備考
1	FIA_UID.2	FIA_UID.1	なし		
2	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	1	
3	FIA_UAU.7	なし	FIA_UAU.1	2	
4	FIA_AFL.1	なし	FIA_UAU.1	2	
5	FIA_SOS.1[1]	なし	なし		
6	FIA_SOS.1[2]	なし	なし		
7	FMT_MTD.1[1]	なし	FMT_SMR.1 FMT_SMF.1	12 11	
8	FMT_MTD.1[2]	なし	FMT_SMR.1 FMT_SMF.1	13 11	
9	FMT_MTD.1[3]	なし	FMT_SMR.1 FMT_SMF.1	12 11	
10	FMT_MOF.1	なし	FMT_SMR.1 FMT_SMF.1	12 11	

11	FMT_SMF.1	なし	なし		
12	FMT_SMR.1[1]	なし	FIA_UID.1	1	
13	FMT_SMR.1[2]	なし	FIA_UID.1	1	
14	FPT_RVM.1	なし	なし		
15	FPT_SEP.1	なし	なし		
16	FDP_ACC.1	なし	FDP_ACF.1	17	
17	FDP_ACF.1	なし	FDP_ACC.1 FMT_MSA.3	16 （注）	
18	FIA_UAU.2[E]	FIA_UAU.1	FIA_UID.1	1	

(注)FMT_MSA.3 を適用しない理由:オブジェクトの生成に相当する事象がないため、必要性はない。

8.2.3. TOE セキュリティ機能要件の相互作用

No	TOE セキュリティ機能要件	防御を提供している機能		
		迂回	非活性化	改ざん
1	FIA_UID.2	FPT_RVM.1	FMT_MOF.1	
2	FIA_UAU.2	FPT_RVM.1	FMT_MOF.1	
3	FIA_UAU.7	FPT_RVM.1	FMT_MOF.1	
4	FIA_AFL.1	FPT_RVM.1	FMT_MOF.1	
5	FIA_SOS.1[1]	なし	FMT_MOF.1	
6	FIA_SOS.1[2]	なし	FMT_MOF.1	
7	FMT_MTD.1[1]	なし	FMT_MOF.1	
8	FMT_MTD.1[2]	なし	FMT_MOF.1	
9	FMT_MTD.1[3]	なし	FMT_MOF.1	
10	FMT_MOF.1	FPT_RVM.1		
11	FMT_SMF.1	なし	FMT_MOF.1	
12	FMT_SMR.1[1]	なし	FMT_MOF.1	
13	FMT_SMR.1[2]	なし	FMT_MOF.1	
14	FPT_RVM.1		FMT_MOF.1	
15	FPT_SEP.1		FMT_MOF.1	
16	FDP_ACC.1	なし	FMT_MOF.1	
17	FDP_ACF.1	FIA_UAU.2	FMT_MOF.1	FPT_SEP.1

【迂回】　FPT_RVM.1

TOE の管理機能及び CE 機能を使用するにあたり、管理者及び CE は識別認証(FIA_UID.2、FIA_UAU.2、FIA_UAU.7、FIA_AFL.1)を実施する。

セキュリティ強化モードの設定操作は管理者にのみ可能である。(FMT_MOF.1)

FPT_RVM.1 により、以上が確実に実行されるため、迂回を防止する。

【迂回】　FIA_UAU.2

管理機能アクセス制御を規定する FDP_ACF.1 は、管理者の識別認証を規定する FIA_UAU.2 によって迂回の防止がサポートされる。さらに FIA_UAU.2 は FPT_RVM.1 によって必ず呼び出されるため、迂回の防止がサポートされる。

【非活性化】　FMT_MOF.1

FMT_MOF.1 により、セキュリティ強化モードの動作設定が管理者だけに許可されている。セキュリティ強化モードは、TOE のセキュリティ構造すべてに影響するものであるため、TOE のセキュリティ要件によって実現されるすべてのセキュリティ機能の非活性化防止がサポートされる。

【改ざん】

FPT_SEP.1 により管理機能アクセス制御で想定されている認証された管理者を代行するサブジェクトだけが、管理機能アクセス制御にて規定されるオブジェクトの操作が可能であり、又、CE 機能アクセス制御で想定されている認証された CE を代行するサブジェクトだけが、CE 機能アクセス制御にて規定されるオブジェクトの操作が可能である。FDP_ACF.1 は他の不正なサブジェクトによる不正な干渉・破壊防止がサポートされる。

8.2.4.　セキュリティ対策方針に対するセキュリティ機能強度の一貫性

本 TOE は、「2.TOE 記述」で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おり、「3.TOE セキュリティ環境」で、「一般利用者がセキュリティ強化モードに関する設定を変更し、HDD に不正な装置を接続してドキュメントデータが読み出される。」と記述しており、特にスキルの高い攻撃者を想定していない。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-基本を 『5.3. セキュリティ強度』で主張している。

以下に、本 TOE を安全に動作させるための運用対策を示す。

- 管理者は、セキュリティ強化モードの設定を有効化する。
- 管理者は、ファイアウォールで保護された内部ネットワーク環境にTOEを接続する。
- 責任者は、不正を行わない人物を管理者として選任する。
- 責任者又は管理者は、CE と保守契約を締結する。保守契約には、不正な行為をしない旨を明

記する。

- 管理者パスワード、HDD ロックパスワードに推測可能な値を設定しない。
- 管理者パスワード、HDD ロックパスワードを秘匿する。
- CE パスワードに推測可能な値を設定しない。
- CE パスワードを秘匿する。
- CE が管理者パスワードを変更した場合は、管理者に速やかに変更させる。

よって、脅威エージェントを以下の人物に特定できる。

攻撃能力　：　低レベル

以上により、上記の攻撃能力を有した脅威エージェントに対して十分な対抗性があることからセキュリティ対策方針に対する最小機能強度として SOF-基本が適切であり、一貫している。

8.2.5. 保証要件根拠

本 TOE は、商用利用される製品であり、低レベルの攻撃能力を有する脅威に対抗するために、TOE の機能と外部インタフェースの仕様、開発者テストの結果、明らかな脆弱性に対する開発者の分析及び機能強度分析などが必要となる。したがって、評価保証レベルは EAL3 が妥当である。

8.3. TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応』に示す。

表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応

IT セキュリティ機能 / TOE セキュリティ機能要件	IA・ADM_ADDD	IA・ADM_AUTH	IA・CE_AUTH	IA・PASS	MNG・MODE	MNG・HDDD
FIA_UID.2		✔	✔			
FIA_UAU.2		✔	✔			
FIA_UAU.7		✔	✔			
FIA_AFL.1		✔	✔			
FIA_SOS.1[1]	✔			✔		
FIA_SOS.1[2]						✔
FMT_MTD.1[1]	✔					
FMT_MTD.1[2]				✔		
FMT_MTD.1[3]				✔		
FMT_MOF.1					✔	
FMT_SMF.1	✔			✔	✔	
FMT_SMR.1[1]		✔				
FMT_SMR.1[2]			✔			
FPT_RVM.1	✔	✔	✔	✔	✔	✔
FPT_SEP.1	✔	✔	✔	✔	✔	✔
FDP_ACC.1						✔
FDP_ACF.1						✔

以下に、『**表 8.4 IT セキュリティ機能とセキュリティ機能要件の対応**』の根拠を示す。

FIA_UID.2

管理者に対しては IA.ADM_AUTH で管理者の識別を実施する。CE に対しては IA.CE_AUTH で CE の識別を実施する。

以上により、IA.ADM_AUTH、及び IA.CE_AUTH を実装することで FIA_UID.2 を実現できる。

FIA_UAU.2

管理者に対しては IA.ADM_AUTH で、管理者の認証を実施する。CE に対しては IA.CE_AUTH で、CE の認証を実施する。

以上により、IA.ADM_AUTH、IA.CE_AUTH を実装することで FIA_UAU.2 を実現する。

FIA_UAU.7

管理者の認証のためのパスワード入力時は IA.ADM_AUTH、CE の認証のためのパスワード入力時は IA.CE_AUTH で、入力したパスワードを入力文字数分のダミー文字(*)で表示する。

以上により、IA.ADM_AUTH、IA.CE_AUTH を実装することで FIA_UAU.7 を実現できる。

FIA_SOS.1[1]

管理者のパスワード登録に対しては IA.ADM_ADD で、管理者パスワード及び CE のパスワード変更に対しては IA.PASS で、パスワード規則に従った許容値の範囲であるか判断する。

以上により、IA.ADM_ADD および IA.PASS を実装することで FIA_SOS.1[1]を実現できる。

FIA_SOS.1[2]

FIA_SOS.1[2]は、HDD のロックパスワード設定/変更に対して MNG_HDD で、パスワード規則に従った許容値の範囲であるか判定を行い、規則にしたがっている場合のみ、HDD 装置内の HDD ロックパスワードを設定/変更している。

以上により、MNG_HDD を実装することで、FIA_SOS.1[2]を実現できる。

FIA_AFL.1

管理者に対しては IA.ADM_AUTH で、CE に対しては IA.CE_AUTH で、認証の不成功時に、管理者、CE に対して、次の認証試行を 5 秒間実行しない。

以上により、IA.ADM_AUTH、IA.CE_AUTH を実装することで、FIA_AFL.1 を実現できる。

FMT_MTD.1[1]

管理者のパスワードの登録を IA.ADM_ADD で、CE にのみ許可し実行する。

以上により、IA.ADM_ADD を実装することで FMT_MTD.1[1]を実現できる。

FMT_MTD.1[2]

CE のパスワードの変更を IA.PASS で CE にのみ許可し実行する。

以上により、IA.PASS を実装することで FMT_MTD.1[2]を実現できる。

FMT_MTD.1[3]

管理者パスワードの変更を IA.PASS で管理者及び CE に許可し実行する。

以上により、IA.PASS を実装することで FMT_MTD.1[3]を実現できる。

FMT_MOF.1

本 ST で規定したセキュリティ機能の有効の設定を MNG.MODE で管理者に許可し実行する。以上により、MNG.MODE を実装することで FMT_MOF.1 を実現できる。

FMT_SMF.1

CE による管理者パスワード登録を IA.ADM_ADD で実装する。CE による管理者パスワードの変更、CE による CE パスワードの変更、管理者による管理者パスワードの変更を IA.PASS で実装する。管理者によるセキュリティ強化モードの設定を MNG.MODE で実装する。以上により、IA.ADM_ADD、IA.PASS、MNG.MODE を実装することで FMT_SMF.1 を実現できる。

FMT_SMR.1[1]

IA.ADM_AUTH によって管理者の認証を行い、その役割を維持することから、FMT_SMR.1[1]を実現できる。

FMT_SMR.1[2]

IA.CE_AUTH によって CE の認証を行い、その役割を維持することから、FMT_SMR.1[2]を実現できる。

FDP_ACC.1

FDP_ACC.1 は、オブジェクトである HDD ロックパスワードオブジェクトに対して制御されるサブジェクト、操作の関係を規定している。

MNG_HDD は、利用者を代行するタスクが、HDD ロックパスワードオブジェクトを改変する管理機能アクセス制御を実施する。

従って本機能要件は満たされる。

FDP_ACF.1

FDP_ACF.1 は、オブジェクトである HDD ロックパスワードオブジェクトに対して制御されるサブジェクト、操作の関係の規則を規定している。

MNG.HDD は、以下の規則が適用される管理機能アクセス制御を実施する。

- 管理者に対して HDD ロックパスワードオブジェクトの改変操作を許可する。

従って本機能要件は満たされる。

FPT_RVM.1

FPT_RVM.1 は、TOE の各セキュリティ機能の動作進行が許可される前に、必ず TSP 実施機能が呼び出されることをサポートすることを規定している。

IA.ADM_ADD は、CE が管理者を登録する前に、動作することが必須である IA.CE_AUTH を必ず起動する。

IA.PASS は CE が CE パスワードまたは管理者パスワードを変更する前に、動作することが必須である IA.CE_AUTH を必ず起動し、また管理者が管理者パスワードを変更する前に、動作することが必須である IA.ADM_AUTH を必ず起動する。

MNG.MODE は管理者がセキュリティ強化モードの設定を行う前に、動作することが必須である IA.ADM_AUTH を必ず起動する。

MNG.HDD は管理者が HDD ロックパスワードの変更を行う前に、動作することが必須である IA.ADM_AUTH を必ず起動する。

したがって、本機能要件は満たされる。

FPT_SEP.1

FPT_SEP.1 は、信頼されないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間を分離することを規定している。

IA.ADM_ADD は IA.CE_AUTH により認証された CE だけが管理者を登録する機能が提供される CE 認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。

IA.PASS は IA.CE_AUTH により認証された CE だけが CE パスワードまたは管理者パスワードを変更する機能が提供される CE 認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。また、IA.ADM_AUTH により認証された管理者だけが管理者パスワードを変更する機能が提供される管理者認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。

MNG.MODE は IA.ADM_AUTH により認証された管理者だけがセキュリティ強化モードの設定を行う機能が提供される管理者認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。

MNG.HDD は IA.ADM_AUTH により認証された管理者だけが HDD ロックパスワードの変更を行う機能が提供される管理者認証ドメインを保持し、許可されないサブジェクトによる干渉行為を許可しない。

8.3.2. セキュリティ機能強度根拠

『6.2 セキュリティ機能強度』で述べたように、識別認証機能(IA.ADM_AUTH、IA_CE_AUTH、IA_ADM_ADD及び IA.PASS) 及び管理支援機能(MNG_HDD)のパスワードメカニズムにおいて、SOF-基本を

主張する。『5.3. セキュリティ強度』で述べたようにセキュリティ機能要件に対して最小機能強度は SOF-基本を主張しており、『6.2 セキュリティ機能強度』で主張する SOF-基本と一貫している。

8.3.3. 保証手段根拠

『6.3 保証手段』において、EAL3 で必要とするすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段に示す関連規約によって、本 ST が規定した TOE セキュリティ保証要件が要求する証拠を網羅している。

したがって、EAL3 における TOE セキュリティ保証要件を実現できる。

8.4. PP 主張根拠

本 ST が準拠する PP はない。