bizhub C252P / ineo+ 251P / magicolor 7465CK
全体制御ソフトウェア

セキュリティターゲット

バージョン：1.04

発行日：2007年5月21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

＜更新履歴＞

日付	Ver	担当部署	承認者	確認者	作成者	更新内容
2006/05/08	1.00	**制御第12開発部**	**石田**	**中島**	**吉田**	**初版**
2006/07/05	1.01	**制御第12開発部**	**石田**	**中島**	**吉田**	**・オプション製品の記載誤記など修正** **・セットアップ機能の説明追加** **・FAXユニットが接続可能とした誤植を削除**
20070/3/09	1.02	**制御第12開発部**	**石田**	**中島**	**吉田**	**・bizhub C252/ ineo+ 251 全体制御ソフトウェア セキュリティターゲットの最終フィックス（1.04版発行）に伴う修正** **・誤植修正**
2007/04/25	1.03	**制御第12開発部**	**石田**	**中島**	**吉田**	**・誤植修正**
2007/05/21	1.04	**制御第12開発部**	**石田**	**中島**	**吉田**	**・誤植修正（所見対応）**

―【 目次 】――――――――――――――――――――――――――――――――――――

1. ST 概説 5
1.1. ST **識別** 5
1.2. TOE **識別** 5
1.3. CC **適合主張** 5
1.4. ST **概要** 6
2. TOE 記述 7
2.1. TOE **の種別** 7
2.2. プリンタの利用環境 7
2.3. TOE **の動作環境構成** 8
2.4. TOE **の利用に関係する人物の役割** 9
2.5. TOE **の機能** 10
2.5.1. 基本機能 *10*
2.5.2. ボックス機能 *10*
2.5.3. 管理者機能 *11*
2.5.4. サービスエンジニア機能 *12*
2.5.5. その他の機能 *12*
2.5.6. セキュリティ強化機能 *13*
3. TOE セキュリティ環境 15
3.1. 保護対象資産の考え方 15
3.2. 前提条件 16
3.3. 脅威 16
3.4. 組織のセキュリティ方針 17
4. セキュリティ対策方針 18
4.1. TOE **セキュリティ対策方針** 18
4.2. 環境のセキュリティ対策方針 19
4.2.1.** IT **環境のセキュリティ対策方針 *19*
4.2.2.** Non-IT **環境のセキュリティ対策方針 *19*
5. IT セキュリティ要件 21
5.1. TOE **セキュリティ要件** 21
5.1.1.** TOE **セキュリティ機能要件 *21*
5.1.2. 最小セキュリティ機能強度 *38*
5.1.3.** TOE **のセキュリティ保証要件 *38*
5.2. IT **環境のセキュリティ要件** 39
6. TOE 要約仕様 41
6.1. TOE **セキュリティ機能** 41
6.1.1.** F.ADMIN **(管理者機能) *41*
6.1.2.** F.ADMIN-SNMP **(SNMP 管理者機能) *46*
6.1.3.** F.SERVICE **(サービスモード機能) *47*
6.1.4.** F.BOX **(ボックス機能) *49*
6.1.5.** F.PRINT **(機密文書プリント機能) *50*
6.1.6.** F.OVERWRITE-ALL **(全領域上書き削除機能) *51*
6.1.7.** F.CRYPT **(暗号鍵生成機能) *51*
6.1.8.** F.HDD **(HDD 検証機能) *52*
6.1.9.** F.RESET **(認証失敗回数リセット機能) *52*

6.2. TOE **セキュリティ機能強度** 52
6.3. TOE **セキュリティ機能と機能要件の対応関係** 52
6.4. 保証手段 53
7. PP 主張 **54**
8. 根拠 **55**
8.1. セキュリティ対策方針根拠 55
8.1.1. 必要性 *55*
8.1.2. 前提条件に対する十分性 *55*
8.1.3. 脅威に対する十分性 *56*
8.1.4. 組織のセキュリティ方針に対する十分性 *58*
8.2. IT **セキュリティ要件根拠** 59
8.2.1. IT セキュリティ機能要件根拠 *59*
8.2.2. 最小機能強度根拠 *72*
8.2.3. IT セキュリティ保証要件根拠 *73*
8.2.4. IT セキュリティ機能要件のセット一貫性根拠 *73*
8.3. TOE **要約仕様根拠** 74
8.3.1. TOE セキュリティ機能根拠 *74*
8.3.2. TOE セキュリティ機能強度根拠 *86*
8.3.3. 相互サポートする TOE セキュリティ機能 *86*
8.3.4. 保証手段根拠 *86*
8.4. PP **主張根拠** 86

―【 図目次 】――――――――――――――――――――――――――――――――――――

図 1　**プリンタの利用環境の例** 7
図 2　TOE **に関係するハードウェア構成** 8

―【 表目次 】――――――――――――――――――――――――――――――――――――

表 1　**ボックスアクセス制御　操作リスト** 22
表 2　**機密文書プリントファイルアクセス制御　操作リスト** 22
表 3　**設定管理アクセス制御　操作リスト** 23
表 4　TOE **のセキュリティ保証要件** 38
表 5　TOE **のセキュリティ機能名称と識別子の一覧** 41
表 6　**パスワードに利用されるキャラクタと桁数** 42
表 7　**全領域の上書き削除のタイプと上書きの方法** 43
表 8　TOE **保証要件と保証手段の関係** 53
表 9　**前提条件、脅威に対するセキュリティ対策方針の適合性** 55
表 10　**セキュリティ対策方針に対する** IT **セキュリティ機能要件の適合性** 59
表 11　IT **セキュリティ機能要件コンポーネントの依存関係** 67
表 12　IT **セキュリティ機能要件の相互サポート関係** 68
表 13　TOE **セキュリティ機能要件に対する** TOE **セキュリティ機能の適合性** 74

1. ST 概説

1.1. ST 識別

・ST名称　：　bizhub C252P / ineo+ 251P / magicolor 7465CK全体制御ソフトウェア
セキュリティターゲット
・STバージョン　：　1.04
・CCバージョン　：　2.3
・作成日　：　2007年5月21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　　吉田 英一

1.2. TOE 識別

・TOE名称　：　日本名：
bizhub C252P / ineo+ 251P / magicolor 7465CK　全体制御ソフトウェア
英名　：
bizhub C252P / ineo+ 251P / magicolor 7465CK　Control Software
・TOE識別　：　4038-0100-GN0-03-000
・TOEの種別　：　ソフトウェア
・製造者　：　コニカミノルタビジネステクノロジーズ株式会社

1.3. CC 適合主張

本STが対象とするTOEは、以下に適合する。

- セキュリティ機能要件
パート2拡張。

- セキュリティ保証要件
パート3適合。

- 評価保証レベル
EAL3適合。（追加する保証コンポーネントはない。）

- PP参照
本STは、PP参照を行っていない。

- 補足
補足-0512（Interpratations-0512）を適用する。

- **参考資料**
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model 2005 Version 2.3 CCMB-2005-08-001
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements 2005 Version 2.3 CCMB-2005-08-002
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements　2005 Version 2.3 CCMB-2005-08-003
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-001 （平成17年12月翻訳第1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-002 （平成17年12月翻訳第1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
  - 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 2005年8月 バージョン2.3 CCMB-2005-08-003 （平成17年12月翻訳第1.0版 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）
  - 補足-0512（平成17年12月 独立行政法人情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）

1.4. ST 概要

bizhub C252P、ineo+ 251P / magicolor 7465CK とは、コニカミノルタビジネステクノロジーズ株式会社が提供するネットワークプリンタである。（以下、これらすべての総称としてプリンタと呼称する。）本 ST では、プリンタ本体のパネルやネットワークから受け付ける操作制御処理、画像データの管理等、プリンタの動作全体を制御する“ bizhub C252P、ineo+ 251P / magicolor 7465CK 全体制御ソフトウェア ”を評価対象（以下 TOE とする）として、TOE が提供するセキュリティ機能について説明する。

TOE は、プリンタに保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。またプリンタ内に画像データを保存する媒体である HDD が不正に持ち出される等の危険性に対して、プリンタのオプション部品である暗号化基板を取り付けることによって、HDD に書き込まれる画像データを暗号化することが可能である。他に、TOE は各種上書き削除規格に則った削除方式を有し、HDD のすべてのデータを完全に削除し、プリンタを廃棄・リース返却する際に利用することによってプリンタを利用する組織の情報漏洩の防止に貢献する。

本 ST は、これら TOE のセキュリティ機能の必要・十分性を記述したドキュメントである。

2. TOE 記述

2.1. TOE の種別

TOE である bizhub C252P、ineo+ 251P / magicolor 7465CK 全体制御ソフトウェアとは、プリンタ制御コントローラ上のフラッシュメモリにあって、プリンタ全体の動作を統括制御する組み込み型ソフトウェアである。

2.2. プリンタの利用環境

TOE の搭載されるプリンタの利用が想定される一般的な利用環境を図 1 に示す。また以下に利用環境にて想定される事項について箇条書きで示す。

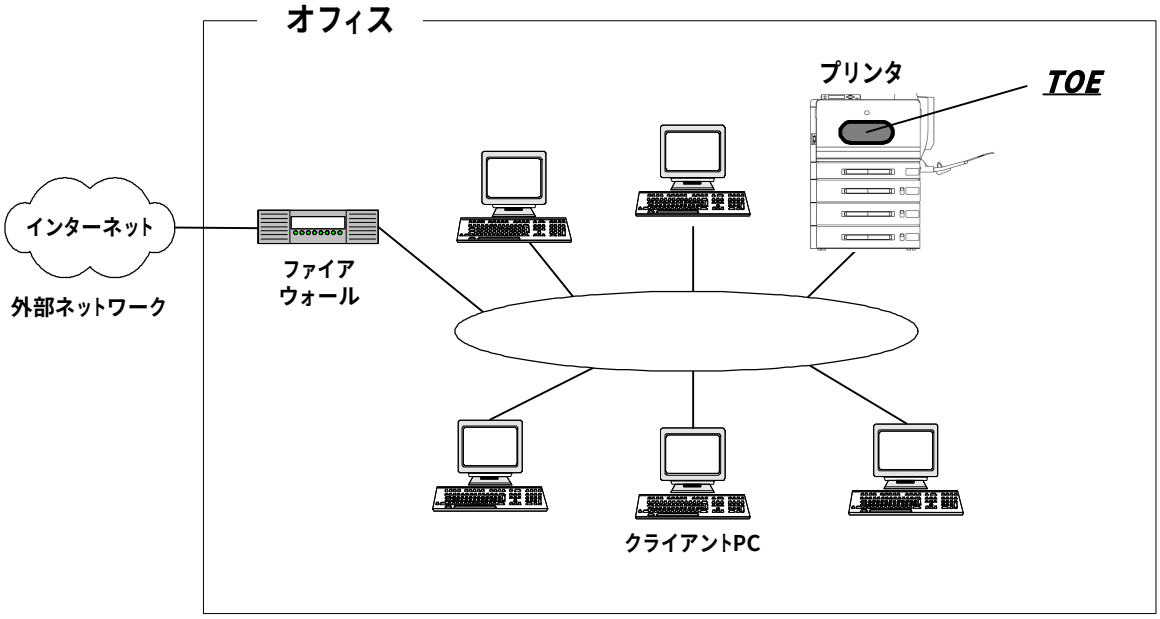

図 1　プリンタの利用環境の例

- オフィス内部のネットワークとしてオフィス内 LAN が存在する。
- プリンタはオフィス内 LAN を介してクライアント PC と接続され、相互にデータ通信を行える。
- オフィス内 LAN が外部ネットワークと接続する場合は、ファイアウォールを介して接続する等の措置が取られ、外部ネットワークからプリンタに対するアクセスを遮断するための適切な設定が行われる。
- オフィス内 LAN は、スイッチングハブ等の利用、盗聴の検知機器の設置などオフィスの運用によって、盗聴されないネットワーク環境が整備されている。

2.3. TOE の動作環境構成

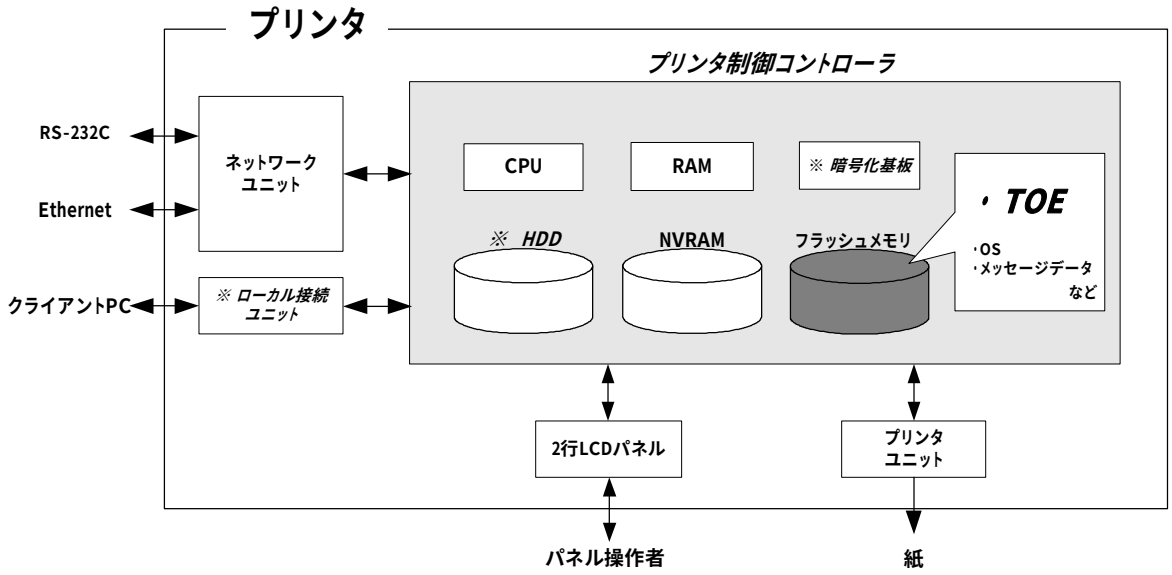

図 2　TOE に関係するハードウェア構成

TOE が動作するために必要なプリンタ上のハードウェア環境の構成を図 2 に示す。プリンタ制御コントローラはプリンタ本体内に据え付けられ、TOE はそのプリンタ制御コントローラ上のフラッシュメモリ上に存在し、ロードされる。

以下には図 2 にて示されるプリンタ制御コントローラ上の特徴的なハードウェア、プリンタ制御コントローラとインターフェースを持つハードウェア、及び RS-232C を用いた接続について説明する。

- **フラッシュメモリ**
  TOE であるプリンタ全体制御ソフトウェアのオブジェクトコードが保管される記憶媒体。TOE の他に、ネットワークからのアクセスに対するレスポンス等などで表示するための各国言語メッセージデータや OS（VxWorks）なども保管される。

- HDD（**※オプションパーツ**）
  容量 40GB のハードディスクドライブ。画像データがファイルとして保管されるほか、伸張変換などで一時的に画像データが保管される領域としても利用される。
  特徴的な機能として、パスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（HDD ロック機能）が搭載されている。なお、パスワード照合に一定回数不成功となるとパスワード照合機能をロックする機能も準備されている。装着されない場合は、HDD が必要となる機能を利用することができない。

- NVRAM
  不揮発性メモリ。TOE の処理に使われるプリンタの動作において必要な様々な設定値等が保管される記憶媒体。

- **暗号化基板（※オプションパーツ）**
  HDD に書き込まれるすべてのデータを暗号化するための暗号機能がハード的に実装されている。暗号化のための集積回路。販売上の都合によりプリンタには標準搭載されず、オプションパーツ

として販売される。

- 2 行 LCD パネル
  2 行 LCD の液晶パネルとテンキーやカーソールキー、メニュー/選択キー、キャンセルキーを備えたプリンタを操作するための専用コントロールデバイス。

- 主電源
  プリンタを動作させるための電源スイッチ。

- ネットワークユニット
  Ethernet 接続インターフェースデバイス。10BASE-T、100BASE-TX をサポート。

- ローカル接続ユニット（※オプションパーツ）
  クライアント PC と USB、またはパラレルポートを使って接続し、ローカル接続でプリント機能を使うためのユニット。販売上の都合によりプリンタには標準搭載されず、オプションパーツとして販売される。

- プリンタユニット
  プリンタ制御コントローラから印刷指示されると、印刷用に変換された画像データを実際に印刷するためのデバイス。

- RS-232C
  D-sub9 ピンを介して、シリアル接続することが可能。初期設定の際のセットアップ機能（後述）や故障時などのメンテナンス機能を使用することができる。また公衆回線と接続されるモデムと接続して、遠隔診断機能（後述）を利用することも可能である。

2.4. TOE の利用に関係する人物の役割

TOE の搭載されるプリンタの利用に関連する人物の役割を以下に定義する。

- ユーザ
  プリンタを使って PC から印刷などを行うプリンタの利用者。（一般には、オフィス内の従業員などが想定される。）

- 管理者
  プリンタの運用管理を行うプリンタの利用者。プリンタの動作管理、ユーザの管理を行う。（一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される。）

- サービスエンジニア
  プリンタの保守管理を行う利用者。プリンタの修理、調整等の保守管理を行う。（一般的には、コニカミノルタビジネステクノロジーズ株式会社と提携し、プリンタの保守サービスを行う販売会社の担当者が想定される。）

- プリンタを利用する組織の責任者
  プリンタが設置されるオフィスを運営する組織の責任者。プリンタの運用管理を行う管理者を任命する。

- **プリンタを保守管理する組織の責任者**
  プリンタを保守管理する組織の責任者。プリンタの保守管理を行うサービスエンジニアを任命する。

この他に、TOE の利用者ではないが TOE にアクセス可能な人物として、オフィス内に出入りする人物などが想定される。

2.5. TOE の機能

利用者は、パネルやクライアント PC からネットワークを介して TOE の各種機能を使用する。以下には、基本機能、保管された画像ファイルを管理するためのボックス機能、利用者であるユーザの識別認証機能、管理者が操作する管理者機能、サービスエンジニアが操作するサービスエンジニア機能、ユーザには意識されずにバックグラウンドで動作する機能といった代表的な機能について説明する。

2.5.1. 基本機能

プリンタには、PC からのプリントを受け付ける機能が存在し、TOE はこれら機能の動作における中核的な制御を行う。プリンタ制御コントローラ外部のデバイスから取得した生データを画像ファイルに圧縮変換し、RAM や HDD に登録する。（PC からのプリント画像ファイルは、複数の変換処理を行なった後に圧縮変換される。）圧縮変換された画像ファイルは、印刷用または送信用のデータとして伸張変換され、目的のプリンタ制御コントローラ外部のデバイスに転送される。
プリントの動作は、ジョブという単位で管理され、パネルからの指示により動作の中止などが行える。以下は基本機能においてセキュリティと関係する機能である。

- **機密文書プリント機能**
  プリントデータと共に機密文書パスワードを受信した場合、画像ファイルを印刷待機状態で保管し、パネルからの印刷指示とパスワード入力により印刷を実行する。
  これより PC からのプリント行為において、機密性の高いプリントデータが、印刷された状態で他の利用者に盗み見られる可能性や、他の印刷物に紛れ込む可能性を排除する。

2.5.2. ボックス機能

画像ファイルを保管するための領域として、HDD にボックスと呼称されるディレクトリを作成できる。ボックスに設定されるパスワードを使って利用ユーザのアクセスを制御する。
TOE は、パネル、またはクライアント PC からネットワークを介したネットワークユニットから伝達される操作要求に対して、ボックス、ボックス内の画像ファイルに対する以下の操作要求を処理する。

- ボックス内の画像ファイルの印刷、他のボックスへの移動、他のボックスへのコピー
- ボックス内の画像ファイルの削除
- ボックス内の画像ファイルの保管期間設定（期間経過後は自動的に削除）
- ボックスの名称変更、パスワードの変更、ボックスの削除など

2.5.3. 管理者機能

TOE は、認証された管理者だけが操作することが可能な管理者モードにてボックスの管理、ネットワークや画質等の各種設定の管理などの機能を提供する。
以下にはセキュリティに関係する機能について例示する。

- ボックスの設定管理
  - ボックスパスワードの登録・変更
- ネットワーク設定管理
  - IP アドレス、NetBIOS 名、AppleTalk プリンタ名など
- NVRAM、HDD のバックアップ及びリストア機能
  - クライアント PC に導入される管理用の専用アプリケーションを利用して、ネットワークを介して実行される。
- HDD の完全上書き削除機能
  - 各種軍用規格などに則ったデータ削除方式が存在
  - 起動すると、設定された方式に則り、HDD の全領域に対して上書き削除を実行する。
- HDD のフォーマット機能
  - 論理フォーマットが実行可能。

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- パスワード規約機能の設定
  - 各種パスワードの有効桁数等、パスワード諸条件をチェックする機能の動作、禁止を選択
- 機密文書プリントの認証方式及び認証操作禁止機能の設定
  - 機密文書プリントの認証に対して認証操作禁止機能が動作するモード、しないモードが存在
  - 各認証機能における不成功認証の検出する機能の動作モードも連動
  - 上記の動作モードを選択
- SNMPv1、v2 によるネットワーク設定変更機能の設定
  - SNMPv1、v2 による MIB の変更操作機能を許可、禁止を選択
- HDD ロック機能の設定
  - 動作、停止を選択
  - 動作選択時には、HDD ロックパスワード登録・変更
- 暗号化機能の設定（※暗号化基板を装着時のみ）
  - 動作、停止を選択
  - 動作選択時には、暗号鍵ワードを登録・変更
- ボックス一括管理機能の設定
  - ボックスの一括管理機能を許可、禁止を選択
- プリントキャプチャ機能の設定
  - プリント機能の故障時などにプリンタが受信するプリントデータを確認するための機能
  - 上記機能を動作、停止を選択
- ネットワーク設定管理リセット機能の設定
  - ネットワーク設定管理リセット機能は、一連の項目を工場出荷値にリセットする。
  - 上記機能を許可、禁止を選択

2.5.4. サービスエンジニア機能

TOE は、サービスエンジニアだけが操作することが可能なサービスモードにて、管理者の管理、プリントなどのデバイスの微調整等のメンテナンス機能などを提供する。以下はセキュリティに関係する機能について例示する。

- 管理者モードパスワードの変更機能

以下は、特にセキュリティ機能のふるまいに関係する動作設定機能である。

- 遠隔診断機能（後述）の設定
  - 利用、禁止を選択することが可能。
- インターネット経由 TOE 更新機能の設定
  - 利用、禁止を選択することが可能。
- メンテナンス機能の設定
  - 利用、禁止を選択することが可能。
- HDD のフォーマット機能
  - 論理フォーマット、物理フォーマットが実行可能。
- HDD の装着設定
  - HDD をデータ保管領域として利用するには、明示的な装着設定が必要。
- イニシャライズ機能
  - 管理者、ユーザが設定した各種設定値、ユーザが保管したデータを削除する。

2.5.5. その他の機能

TOE はユーザには意識されないバックグラウンドで処理される機能や TOE の更新機能などを提供する。以下に代表的な機能について説明する。

① **暗号鍵生成機能**
オプション製品である暗号化基板がプリンタ制御コントローラに設置されている場合に、暗号化基板にて HDD のデータ書き込み、読み込みにおいて暗号化・復号処理を実施する。(TOE は、暗復号処理そのものを行わない。)
管理者機能にて本機能の動作設定を行う。動作させる場合は、TOE はパネルにて入力された暗号鍵ワードより暗号鍵を生成する。

② **HDD ロック機能**
HDD は、不正な持ち出し等への対処機能として、パスワードを設定した場合に HDD ロック機能が動作する。
管理者機能にて本機能の動作設定を行う。プリンタの起動動作において、プリンタ側に設定された HDD ロックパスワードと HDD 側に設定される HDD のパスワードロックを照合し、一致した場合に HDD へのアクセスを許可する。(HDD を持ち出されても、当該 HDD が設置されていたプリンタ以外で利用することができない。)

③ **遠隔診断機能**

RS-232C を介したモデム接続、E-mail などいくつかの接続方式を利用して、コニカミノルタビジネステクノロジーズ株式会社が製造するプリンタのサポートセンターと通信し、プリンタの動作状態、印刷数等の機器情報を管理する。また必要に応じて適切なサービス（追加トナーの発送、課金請求、故障診断からサービスエンジニアの派遣など）を提供する。

④ TOE **の更新機能**

TOE は TOE 自身を更新するための機能を有する。更新手段は、遠隔診断機能の項目の 1 つとしても存在する他、Ethernet を介して FTP サーバよりダウンロードする方法（インターネット経由 TOE 更新機能）、コンパクトフラッシュメモリ媒体を接続して行う方法がある。

⑤ **セットアップ機能**

RS-232C 経由でクライアント PC と接続し、PC 上で動作する専用のインストールソフトウェアを使ってセットアップを行う機能を提供する。本セットアップ機能の中で、特にセキュリティ機能のふるまいに関係する動作設定機能を示す。なお専用のインストールソフトウェアは、サービスエンジニアが利用するもので、ユーザには提供されない。

- ✧ 遠隔診断機能（後述）の設定
  - ♦ 利用、禁止を選択することが可能。
- ✧ インターネット経由 TOE 更新機能の設定
  - ♦ 利用、禁止を選択することが可能。
- ✧ メンテナンス機能の設定
  - ♦ 利用、禁止を選択することが可能。
- ✧ HDD のフォーマット機能
  - ♦ 論理フォーマット、物理フォーマットが実行可能。
- ✧ HDD の装着設定
  - ♦ HDD をデータ保管領域として利用するには、明示的な装着設定が必要。
- ✧ イニシャライズ機能
  - ♦ 管理者、ユーザが設定した各種設定値、ユーザが保管したデータを削除する。

2.5.6. セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また個別には動作設定機能を持たない機能として、ネットワーク設定のリセット機能、ネットワーク介した TOE の更新機能が存在するが、これら機能の利用は禁止される。

以下にセキュリティ強化機能有効時の一連の設定状態をまとめる。なお、セキュリティ強化機能を有効にするためには、管理者パスワード、CE パスワードを事前にパスワード規約に違反しない値に設定する等の事前準備が必要である。

- パスワード規約機能の設定　：有効
- 機密文書プリントの認証方式の設定　：認証操作禁止機能有効方式（アカウントロック（失敗回数閾値：1～3 回）状態にもなる。）
- ボックス一括管理機能の設定　：禁止
- SNMPv1、v2 ネットワーク設定変更機能　：禁止

- HDD ロック機能の設定　：有効（暗号化機能が有効の場合、無効も可）
- 暗号化機能の設定　：有効（HDD ロック機能が有効の場合、無効も可）
- プリントキャプチャ機能の設定　：禁止
- メンテナンス機能の設定　：禁止
- 遠隔診断機能　：禁止
- ネットワーク設定管理リセット機能　：禁止
- インターネット経由 TOE の更新機能　：禁止

以下の機能はセキュリティ強化機能が有効になるタイミングで以下に示される設定状態になるが、上記の機能群と異なり、個別に設定を変更することが可能である。ただし設定を有効にした場合は、セキュリティ強化条件を満たしていないとして、2 行 LCD パネルにその状態を知らせる仕組みを持つ。

- セットアップ機能　：禁止

3. TOE セキュリティ環境

本章では、保護対象資産の考え方、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 保護対象資産の考え方

TOE のセキュリティコンセプトは、**“ユーザの意図に反して暴露される可能性のあるデータの保護”**である。プリンタを通常の利用方法で使用している場合、利用可能な状態にある以下の画像ファイルを保護対象とする。（なお以下の画像ファイルは、HDD が装着された場合に扱えるファイルであるため、TOE セキュリティ環境におけるプリンタには、オプションである HDD が装着されていることを想定する。）

- **機密文書プリントファイル**
  - 機密文書プリントによって登録される画像ファイル
- **ボックスファイル**
  - ボックスに保管される画像ファイル

複数のジョブの動作により待機状態として保管されるジョブの画像ファイルや、仕上がりの確認のために残り部数の印刷が待機状態となって保管されるジョブの画像ファイル等、上記の対象とする画像ファイル以外は、プリンタの通常利用において保護されることが意図されないため、保護資産とは扱わない。

なお機密文書プリントファイルの印刷、ボックスファイルの送信においては、万が一不正なプリンタやメールサーバなどが接続された場合に考えられる脅威に備え、プリンタの設定（IP アドレスなど）を不正に変更出来ないようにする必要がある。したがってプリンタの設定（IP アドレスなど）は副次的な保護資産として考慮する。

一方、プリンタをリース返却、廃棄するなど利用が終了した場合や HDD が盗難にあった場合などユーザの管轄から保管されるデータが物理的に離れてしまった場合は、ユーザは HDD に残存するあらゆるデータの漏洩可能性を懸念する。従ってこの場合は以下のデータファイルを保護対象とする。

- **機密文書プリントファイル**
- **ボックスファイル**
- **オンメモリ画像ファイル**
  - 待機状態にあるジョブの画像ファイル
- **保管画像ファイル**
  - 機密文書プリントファイル、ボックスファイル以外の保管される画像ファイル
- **残存画像ファイル**
  - 一般的な削除操作（ファイル管理領域の削除）だけでは削除されない、HDD データ領域に残存するファイル
- **画像関連ファイル**
  - プリント画像ファイル処理において生成されたテンポラリデータファイル

3.2. 前提条件

本節では、TOE の利用環境に関する前提条件を識別し、説明する。

A.ADMIN（管理者の人的条件）
管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。

A.SERVICE（サービスエンジニアの人的条件）
サービスエンジニアは、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。

A.NETWORK（プリンタのネットワーク接続条件）
・TOE が搭載されるプリンタを設置するオフィス内 LAN は、盗聴されない。
・TOE が搭載されるプリンタを設置するオフィス内 LAN 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プリンタへアクセスできない。

A.SECRET（秘密情報に関する運用条件）
TOE の利用において使用される各パスワードや暗号鍵ワードは、各利用者から漏洩しない。

A.SETTING（セキュリティ強化機能の動作設定条件）
セキュリティ強化機能が有効化した上で、TOE が搭載されたプリンタを利用する。

3.3. 脅威

本節では、TOE の利用及び TOE 利用環境において想定される脅威を識別し、説明する。

T.DISCARD-PRINTER（プリンタのリース返却、廃棄）
リース返却、または廃棄となったプリンタが回収された場合、悪意を持った者が、プリンタ内の HDD を取り出して解析することにより、機密文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、設定されていた各種パスワード（管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号鍵ワード、機密文書パスワード、ボックスパスワード）の秘匿情報が漏洩する。

T.BRING-OUT-STORAGE（HDD の不正な持ち出し）
・悪意を持った者や悪意を持ったユーザが、プリンタ内の HDD を不正に持ち出して解析することにより、機密文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、設定されていた各種パスワード（機密文書パスワード、ボックスパスワード）が漏洩する。
・悪意を持った者や悪意を持ったユーザが、プリンタ内の HDD を不正にすりかえる。すりかえられた HDD には新たに機密文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、設定されていた各種パスワード（機密文書パスワード、ボックスパスワード）が蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえた HDD を持ち出して解析することにより、これら画像ファイル等が漏洩する。

T.ACCESS- BOX（ユーザ機能を利用したボックスへの不正なアクセス）
悪意を持った者や悪意を持ったユーザが、利用を許可されないボックスにアクセスし、ボックスファイルを印刷することにより、ボックスファイルが暴露される。

T.ACCESS-SECURE-PRINT（ユーザ機能を利用した機密文書プリントファイルへの不正なアクセス）
悪意を持った者や悪意を持ったユーザが、利用を許可されない機密文書プリントファイルを印刷することにより、機密文書プリントファイルが暴露される。

T.ACCESS-NET-SETTING（ネットワーク設定の不正変更）
悪意を持った者や悪意を持ったユーザが、TOE が導入されるプリンタに設定されるプリンタを識別するためのネットワーク設定を変更し、不正な別のプリンタなどのエンティティにおいて本来 TOE が導入されるプリンタの設定（NetBIOS 名、AppleTalk プリンタ名、IP アドレスなど）を設定することにより、機密文書プリントファイルが暴露される。

T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）
悪意を持った者や悪意を持ったユーザが、セキュリティ強化機能に関係する設定を変更してしまうことにより、ボックスファイル、機密文書プリントファイルが漏洩する可能性が高まる。

T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）
悪意を持った者や悪意を持ったユーザが、バックアップ機能、リストア機能を不正に使用することにより、ボックスファイル、機密文書プリントファイルが漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、各種設定値が改ざんされる。

3.4. 組織のセキュリティ方針

本 TOE に適用することが想定される組織のセキュリティ方針は存在しない。

4. セキュリティ対策方針

本章では、3 章にて識別された前提条件、脅威、組織のセキュリティ方針を受けて、TOE 及び TOE の利用環境にて必要なセキュリティ対策方針について記述する。以下、TOE のセキュリティ対策方針、環境のセキュリティ対策方針に分類して記述する。

4.1. TOE セキュリティ対策方針

本節では、TOE のセキュリティ対策方針について識別し、説明する。

O.BOX（ボックスアクセス制御）
TOE は、そのボックスの利用を許可されたユーザだけに、そのボックス及びそのボックス内のボックスファイルに対するユーザ機能の利用を許可する。

O.SECURE-PRINT（機密文書プリントファルアクセス制御）
TOE は、その機密文書プリントファイルの利用を許可されたユーザだけに、その機密文書プリントファイルの印刷を許可する。

O.CONFIG（管理機能へのアクセス制限）
TOE は、管理者だけに以下に示す機能の操作を許可する。
・プリンタのネットワークアドレスに関係する設定機能
・バックアップ機能
・リストア機能
TOE は、管理者及びサービスエンジニアだけに以下に示す機能の操作を許可する。
・セキュリティ強化機能の設定に関係する機能

O.OVERWRITE-ALL（完全上書き削除）
TOE は、プリンタ内の HDD のすべてのデータ領域に削除用データを上書きし、あらゆる画像データを復旧不可能にする。またユーザ、管理者が設定した秘匿性のある NVRAM 上のパスワード（管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号鍵ワード）の設定値を初期化する機能を提供する。

O.CRYPT-KEY（暗号鍵生成）
TOE は、プリンタ内の HDD に書き込まれる画像ファイルを含むすべてのデータを暗号化して保存するための暗号鍵を生成する。

O.CHECK-HDD（HDD の正当性確認）
TOE は、正しい HDD が設置されていることを検証する。

4.2. 環境のセキュリティ対策方針

本節では、TOE の利用環境における環境のセキュリティ対策方針を IT 環境のセキュリティ対策方針、Non-IT の環境セキュリティ対策方針で識別し、説明する。

4.2.1. IT 環境のセキュリティ対策方針

OE.CRYPT（HDD の暗号化）
プリンタ内に設置される暗号化基板は、プリンタ内の HDD に書き込まれる画像ファイルを含むすべてのデータを暗号化して HDD に保管する。

OE.LOCK-HDD（HDD のアクセス制御）
プリンタ内に設置される HDD は、設置されたプリンタだけのデータの読み出しを受け付ける。

OE.FEED-BACK（パスワードのフィードバック）
クライアント PC にてプリンタにアクセスするために利用されるブラウザなどのアプリケーションは、入力されるボックスパスワード、管理者パスワードに対して保護された適切なフィードバックを提供する。

4.2.2. Non-IT 環境のセキュリティ対策方針

OE-N.ADMIN（信頼できる管理者）
プリンタを利用する組織の責任者は、TOE が搭載されるプリンタの運用において課せられた役割を忠実に実行する人物を管理者に指定する。

OE-N.SERVICE（サービスエンジニアの保証）
・プリンタを保守管理する組織の責任者は、TOE の設置、セットアップ及び TOE が搭載されるプリンタの保守において課せられた役割を忠実に実行するようにサービスエンジニアを教育する。
・管理者は、サービスエンジニアによる TOE が搭載されるプリンタのメンテナンス作業に立会う。

OE-N.NETWORK（プリンタの接続するネットワーク環境）
・プリンタを利用する組織の責任者は、TOE が搭載されるプリンタを設置するオフィス LAN において暗号通信機器や盗聴検知機器を設置するなど、盗聴防止対策を実施する。
・プリンタを利用する組織の責任者は、外部ネットワークから TOE が搭載されるプリンタへのアクセスを遮断するためにファイアウォールなどの機器を設置して、外部からの不正侵入対策を実施する。

OE-N.SECRET（秘密情報の適切な管理）
管理者は、ユーザに対して以下に示す運用を実施させる。
・機密文書パスワードを秘匿する。
・ボックスパスワードは共同で利用するユーザの間で秘匿する。
・機密文書パスワード、ボックスパスワードに推測可能な値を設定しない。
・ボックスパスワードの適宜変更を行う。
・管理者がボックスパスワードを変更した場合は、速やかに変更させる。

管理者は、以下に示す運用を実施する。
・管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号鍵ワードに推測可能な値を設定しない。
・管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号鍵ワードを秘匿する。
・管理者パスワード、SNMP パスワード、HDD ロックパスワード、暗号鍵ワードの適宜変更を行う。
サービスエンジニア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 パスワードの適宜変更を行う。
・サービスエンジニア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。

OE-N.SESSION（操作後のセッションの終了）
管理者は、ユーザに対して以下に示す運用を実施させる。
・機密文書プリントファイルの操作、ボックス及びボックスファイルの操作の終了後にログオフ操作を行う。
管理者は、以下に示す運用を実施する。
・管理者モードの諸機能を操作終了後にログオフ操作を行う。
サービスエンジニアは、以下に示す運用を実施する。
・サービスモードの諸機能を操作終了後にログオフ操作を行う。

OE-N.SETTING-SECURITY（セキュリティ強化機能の動作設定）
管理者は、TOE の運用にあたってセキュリティ強化機能の設定を有効化する。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境セキュリティ要件について記述する。

＜ラベル定義について＞

TOE 及び IT 環境に必要とされるセキュリティ機能要件を記述する。機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用し、ラベルも同一のものを使用する。CC パート 2 に記載されない新しい追加要件は、CC パート 2 と競合しないラベルを新設して識別している。また各要件の対象が TOE、IT 環境のどちらであるか明示するため、IT 環境において必要とされる要件のラベルの後には[E]を付ける。

＜セキュリティ機能要件“操作”の明示方法＞

以下の記述の中において、イタリック且つボールドで示される表記は、“割付”、または“選択”されていることを示す。アンダーラインで示される原文の直後に括弧書きでイタリック且つボールドで示される表記は、アンダーラインされた原文箇所が“詳細化”されていることを示す。ラベルの後に括弧付けで示される番号は、当該機能要件が“繰り返し”されて使用されていることを示す。（なお、繰り返しは TOE 要件、IT 環境要件でそれぞれ分離して付与する。）

＜依存性の明示方法＞

依存性の欄において括弧付け“（　）”された中に示されるラベルは、本 ST にて使用されるセキュリティ機能要件のラベルを示す。また本 ST にて適用する必要性のない依存性である場合は、同括弧内にて“適用しない”と記述している。

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

5.1.1.1. 暗号サポート

FCS_CKM.1　　暗号鍵生成
FCS_CKM.1.1
TSF は、以下の[割付: *標準のリスト*]に合致する、指定された暗号鍵生成アルゴリズム[割付: *暗号鍵生成アルゴリズム*]と指定された暗号鍵長[割付: *暗号鍵長*]に従って、暗号鍵を生成しなければならない。
[割付: *標準のリスト*]： ***コニカミノルタ暗号仕様標準***
[割付: *暗号鍵生成アルゴリズム*]： ***コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）***
[割付: *暗号鍵長*]： ***128bit***
下位階層　：　なし **依存性**　：　FCS_CKM.2 or FCS_COP.1（FCS_COP.1[E]）、FCS_CKM.4（適用しない）、 FMT_MSA.2（適用しない）

5.1.1.2. 利用者データ保護

FDP_ACC.1[1]　　サブセットアクセス制御
FDP_ACC.1.1[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*]： ***「表 1　ボックスアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]： ***ボックスアクセス制御***
下位階層　：　なし **依存性　：**　FDP_ACF.1（FDP_ACF.1[1]）

表 1　ボックスアクセス制御　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	***ボックスファイル***	***・印刷*** ***・他のボックスへの移動*** ***・他のボックスへのコピー*** ***・バックアップ***

FDP_ACC.1[2]　　サブセットアクセス制御
FDP_ACC.1.1[2]
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*]： ***「表 2　機密文書プリントファイルアクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]： ***機密文書プリントファイルアクセス制御***
下位階層　：　なし **依存性　：**　FDP_ACF.1（FDP_ACF.1[2]）

表 2　機密文書プリントファイルアクセス制御　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	***機密文書プリントファイル***	***・印刷*** ***・バックアップ***

FDP_ACC.1[3]　　サブセットアクセス制御
FDP_ACC.1.1[3]
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*]： ***「表 3　設定管理アクセス制御　操作リスト」に記載***
[割付: *アクセス制御 SFP*]： ***設定管理アクセス制御***
下位階層　：　なし **依存性　：**　FDP_ACF.1（FDP_ACF.1[3]）

表 3　設定管理アクセス制御　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* *・暗号鍵ワードオブジェクト*	*・ 設定* *・ バックアップ* *・ リストア*
	・プリンタアドレスグループオブジェクト[1]	*・ 設定* *・ リストア*

FDP_ACF.1[1]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[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　⇒　・ボックス属性（ボックス ID）*** ***・管理者属性*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・ボックスファイル　⇒　・ボックス属性（ボックス ID）***
[割付: *アクセス制御 SFP*]： ***ボックスアクセス制御***
FDP_ACF.1.2[1]
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*]： ***・ボックス属性（ボックス ID）が関連付けられる利用者を代行するタスクは、サブジェクト属性のボックス属性と一致するボックス属性を有するボックスファイルに対して、印刷、他のボックスへの移動、他のボックスへのコピー操作をすることが許可される。*** ***・管理者属性を有する利用者を代行するタスクは、ボックスファイルをバックアップ操作することを許可される。***
FDP_ACF.1.3[1]
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[1]
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。***
下位階層　：　なし **依存性**　：　FDP_ACC.1（FDP_ACC.1[1]）、FMT_MSA.3（適用しない）

[1] プリンタアドレスグループオブジェクトとは、IP アドレス、Appletalk プリンタ名などプリンタ本体のアドレスに関する一連のデータのことである。

FDP_ACF.1[2]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[2]
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　⇒　・ファイル属性（機密文書内部制御 ID）*** ***・管理者属性*** --- ***＜オブジェクト＞　　＜オブジェクト属性＞*** ***・機密文書プリントファイル　⇒　・ファイル属性（機密文書内部制御 ID）***
[割付: *アクセス制御 SFP*]： ***機密文書プリントファイルアクセス制御***
FDP_ACF.1.2[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*]： ***ファイル属性（機密文書内部制御 ID）を持つ利用者を代行するタスクは、ファイル属性（機密文書内部制御 ID）と一致するファイル属性（機密文書内部制御 ID）を持つ機密文書プリントファイルに対して印刷操作を許可される。***
FDP_ACF.1.3[2]
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*]： ***管理者属性を有する利用者を代行するタスクは、機密文書プリントファイルをバックアップ操作することを許可される。***
FDP_ACF.1.4[2]
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。***
下位階層　：　なし **依存性**　：　FDP_ACC.1（FDP_ACC.1[2]）、FMT_MSA.3（FMT_MSA.3）

FDP_ACF.1[3]　　セキュリティ属性によるアクセス制御
FDP_ACF.1.1[3]
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*** ***・CE 属性*** --- ***＜オブジェクト＞*** ***・HDD ロックパスワードオブジェクト*** ***・暗号鍵ワードオブジェクト***

・プリンタアドレスグループオブジェクト
[割付: *アクセス制御 SFP*]： ***設定管理アクセス制御***
FDP_ACF.1.2[3]
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、暗号鍵ワードオブジェクトを設定、バックアップ、リストア操作することが許可される。*** ***・管理者属性を持つ利用者を代行するタスクは、プリンタアドレスグループオブジェクトを設定、リストア操作することが許可される。*** ***・CE 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、暗号鍵ワードオブジェクトを設定することが許可される。***
FDP_ACF.1.3[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[3]
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。***
下位階層　：　なし **依存性**　：　FDP_ACC.1（FDP_ACC.1[3]）、FMT_MSA.3（適用しない）

5.1.1.3. 識別と認証

FIA_AFL.1[1]　　認証失敗時の取り扱い
FIA_AFL.1.1[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*]： ***・サービスモードにアクセスする際の認証*** ***・CE パスワードを改変する際の再認証***
[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]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[1]
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*]： ***＜検出した際のアクション＞*** ***・認証中であれば、サービスモードへの認証状態からログオフし、CE パスワードを利用する認証機能をロックする。*** ***・認証中でなければ、CE パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[1]）

FIA_AFL.1[2]　　認証失敗時の取り扱い
FIA_AFL.1.1[2]
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*]： ***・管理者モードにアクセスする際の認証*** ***・管理者パスワードを改変する際の再認証***
[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]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[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*]： ***＜検出した際のアクション＞*** ***・認証中であれば、管理者モードへの認証状態からログオフし、管理者パスワードを利用する認証機能をロックする。*** ***・認証中でなければ、管理者パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[3]　　認証失敗時の取り扱い
FIA_AFL.1.1[3]
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*]： ***SNMP を利用して MIB オブジェクトへアクセスする際の認証***
[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]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[3]
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*]： ***＜検出した際のアクション＞*** ***MIB オブジェクトへのアクセスを拒否し、SNMP パスワードを利用する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***・管理者モード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[2]）

FIA_AFL.1[4]　　認証失敗時の取り扱い
FIA_AFL.1.1[4]
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*]： ***機密文書プリントファイルにアクセスする際の認証***
[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]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[4]

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*]： ***＜検出した際のアクション＞*** ***当該機密文書プリントファイルへのアクセスを拒否し、当該機密文書プリントファイルに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***・管理者モード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[3]）

FIA_AFL.1[5]　認証失敗時の取り扱い
FIA_AFL.1.1[5]
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*]： ***ボックスにアクセスする際の認証***
[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]」*] ***[割付: 許容可能な値の範囲]：1～3 内における管理者設定可能な正の整数値***
FIA_AFL.1.2[5]
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*]： ***＜検出した際のアクション＞*** ***当該ボックス及び当該ボックス内のボックスファイルへのアクセスを拒否し、当該ボックスに対する認証機能をロックする。*** ***＜通常復帰のための操作＞*** ***・管理者モード内にて提供されるロック解除機能を実行する。*** ***・TOE の起動処理を行う。***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[4]）

FIA_AFL.1[6]　認証失敗時の取り扱い
FIA_AFL.1.1[6]
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*]： ***・サービスモードにアクセスする際の認証*** ***・パネルより管理者モードにアクセスする際の認証*** ***・機密文書プリントファイルにアクセスする際の認証*** ***・パネルよりボックスにアクセスする際の認証***
[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]」*] ***[割付:正の整数値]：1***
FIA_AFL.1.2[6]
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*]： ***＜検出した際のアクション＞*** ***パネルからのすべての入力受付拒否*** ***＜通常復帰のための操作＞*** ***5 秒経過後に自動解除***

下位階層	**：**	**なし**
依存性	**：**	FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]）

FIA_ATD.1　　利用者属性定義
FIA_ATD.1.1
TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:*セキュリティ属性のリスト*]を維持しなければならない。
[割付:*セキュリティ属性のリスト*]： ***・ボックス属性（ボックス ID）*** ***・ファイル属性（機密文書内部制御 ID）***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[1]　　秘密の検証
FIA_SOS.1.1[1]
TSF は、秘密***（管理者パスワード、CE パスワード）***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*]： ***・桁数　：8 桁*** ***・文字種：ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）*** ***・規則　：① 同種の文字列だけで構成されていない。　② 現在設定されている値と合致しない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[2]　　秘密の検証
FIA_SOS.1.1[2]
TSF は、秘密***（SNMP パスワード）***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*]： ***・桁数　：8 桁以上*** ***・文字種：ASCII コード（0x20 ～ 0x7E）***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[3]　　秘密の検証
FIA_SOS.1.1[3]
TSF は、秘密***（HDD ロックパスワード、暗号鍵ワード）***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*]： ***・桁数　：20 桁*** ***・文字種：ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く）*** ***・規則　：同種の文字列だけで構成されていない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[4]　　秘密の検証
FIA_SOS.1.1[4]
TSF は、秘密（***機密文書パスワード、ボックスパスワード***）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*]： ***・桁数　：8 桁*** ***・文字種：ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く）*** ***・規則　：同種の文字列だけで構成されていない。***
下位階層　：　なし
依存性　：　なし

FIA_SOS.1[5]　　秘密の検証
FIA_SOS.1.1[5]
TSF は、秘密（***セッション情報***）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*]： ***10^{10} 以上***
下位階層　：　なし
依存性　：　なし

FIA_SOS.2　　秘密の検証
FIA_SOS.2.1
TSF は、[割付: *定義された品質尺度*]に合致する秘密（***セッション情報***）を生成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*]： ***10^{10} 以上***
FIA_SOS.2.2
TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付: *TSF 機能のリスト*]： ***・管理者認証（ネットワーク経由アクセス）*** ***・ボックス認証（ネットワーク経由アクセス）***
下位階層　：　なし
依存性　：　なし

FIA_UAU.2[1]　　アクション前の利用者認証
FIA_UAU.2.1[1]
TSF は、その利用者（***サービスエンジニア***）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（***サービスエンジニア***）に自分自身を認証することを要求しなければならない。
下位階層　：　FIA_UAU.1
依存性　：　FIA_UID.1（FIA_UID.2[1]）

FIA_UAU.2[2]　　アクション前の利用者認証
FIA_UAU.2.1[2]
TSF は、その利用者*（管理者）*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*（管理者）*に自分自身を認証することを要求しなければならない。
下位階層　：　FIA_UAU.1
依存性　：　FIA_UID.1（FIA_UID.2[2]）

FIA_UAU.2[3]　　アクション前の利用者認証
FIA_UAU.2.1[3]
TSF は、その利用者*（機密文書プリントファイルの利用を許可されたユーザ）*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*（機密文書プリントファイルの利用を許可されたユーザ）*に自分自身を認証することを要求しなければならない。
下位階層　：　FIA_UAU.1
依存性　：　FIA_UID.1（FIA_UID.2[3]）

FIA_UAU.2[4]　　アクション前の利用者認証
FIA_UAU.2.1[4]
TSF は、その利用者*（ボックスの利用を許可されたユーザ）*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*（ボックスの利用を許可されたユーザ）*に自分自身を認証することを要求しなければならない。
下位階層　：　FIA_UAU.1
依存性　：　FIA_UID.1（FIA_UID.2[4]）

FIA_UAU.6　　再認証
FIA_UAU.6.1
TSF は、条件[割付: *再認証が要求される条件のリスト*]のもとで利用者を再認証しなければならない。
[割付: *再認証が要求される条件のリスト*] ***・管理者が管理者パスワードを改変する場合*** ***・サービスエンジニアが CE パスワードを改変する場合*** ***・管理者が HDD ロックの設定を変更する場合*** ***・管理者が暗号化機能の設定を変更する場合***
下位階層　：　なし
依存性　：　なし

FIA_UAU.7　　保護された認証フィードバック
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*]： ***入力された文字データ 1 文字毎に“＊”の表示***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]）

FIA_UID.2[1]　　アクション前の利用者識別
FIA_UID.2.1[1]
TSF は、その利用者（サービスエンジニア）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（サービスエンジニア）に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[2]　　アクション前の利用者識別
FIA_UID.2.1[2]
TSF は、その利用者（管理者）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（管理者）に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[3]　　アクション前の利用者識別
FIA_UID.2.1[3]
TSF は、その利用者（機密文書プリントファイルの利用を許可されたユーザ）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（機密文書プリントファイルの利用を許可されたユーザ）に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_UID.2[4]　　アクション前の利用者識別
FIA_UID.2.1[4]
TSF は、その利用者（ボックスの利用を許可されたユーザ）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（ボックスの利用を許可されたユーザ）に自分自身を識別することを要求しなければならない。
下位階層　：　FIA_UID.1
依存性　：　なし

FIA_USB.1　　利用者・サブジェクト結合
FIA_USB.1.1
TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: *利用者セキュリティ属性のリスト*]
[割付: *利用者セキュリティ属性のリスト*]： ・ボックス属性（ボックス ID） ・ファイル属性（機密文書内部制御 ID）
FIA_USB.1.2
TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: *属性の最初の関連付けに関する規則*]
[割付: *属性の最初の関連付けに関する規則*]： ・ボックス属性の場合、ボックスに対するアクセスにおいて認証された際に、利用者を代行するタスクに当該ボックスのボックス ID を関連付ける。 ・ファイル属性の場合、機密文書プリントファイルに対するアクセスにおいて認証された際に、利用者を代行するタスクに、当該機密文書プリントファイルの機密文書内部制御 ID を関連付ける。

FIA_USB.1.3
TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: *属性の変更に関する規則*]
[割付: *属性の変更に関する規則*]： ***なし***
下位階層　：　なし
依存性　：　FIA_ATD.1

5.1.1.4. セキュリティ管理

FMT_MOF.1[1]　セキュリティ機能のふるまい管理
FMT_MOF.1.1[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*]： ***セキュリティ強化設定***
[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*]： ***を停止する***
[割付: *許可された識別された役割*]： ***・管理者*** ***・サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MOF.1[2]　セキュリティ機能のふるまい管理
FMT_MOF.1.1[2]
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*]： ***SNMP パスワード認証機能***
[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*]： ***のふるまいを改変する***
[割付: *許可された識別された役割*]： ***管理者***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MOF.1[3]　セキュリティ機能のふるまい管理
FMT_MOF.1.1[3]
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*]： ***セットアップ機能***
[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***
[割付: *許可された識別された役割*]： ***サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]）

FMT_MSA.3　　静的属性初期化
FMT_MSA.3.1
TSF は、その SFP を実施するために使われるセキュリティ属性（***機密文書内部制御 ID***）として、[選択: *制限的、許可的：から一つのみ選択、[割付：その他の特性]*]デフォルト値を与える[割付: *アクセス制御 SFP、情報フロー制御 SFP*]を実施しなければならない。
[選択: *制限的、許可的：から一つのみ選択、[割付：その他の特性]*]： ***[割付：その他の特性]：一意に識別される***
[割付: *アクセス制御 SFP、情報フロー制御 SFP*]： ***機密文書プリントファイルアクセス制御***
FMT_MSA.3.2
TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。
[割付: *許可された識別された役割*] ***該当なし***
下位階層　：　なし
依存性　：　FMT_MSA.1（適用しない）、FMT_SMR.1（適用しない）

FMT_MTD.1[1]　　TSF データの管理
FMT_MTD.1.1[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*]： ***・SNMP パスワード*** ***・機密文書パスワード*** ***・認証失敗回数閾値***
[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***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[2]　　TSF データの管理
FMT_MTD.1.1[2]
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*]： ***当該ボックスのボックスパスワード***
[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*]： ***・そのボックスの利用を許可されたユーザ*** ***・管理者***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]、FMT_SMR.1[3]）

FMT_MTD.1[3]　　TSF データの管理
FMT_MTD.1.1[3]
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*** ***・サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MTD.1[4]　　TSF データの管理
FMT_MTD.1.1[4]
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*]： ***・SNMP パスワード*** ***・ボックスパスワード*** ***・機密文書パスワード***
[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]*]： ***問い合わせ***
[割付:*許可された識別された役割*]： ***管理者***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[2]）

FMT_MTD.1[5]　　TSF データの管理
FMT_MTD.1.1[5]
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 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*]： ***サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]）

FMT_MTD.1[6]　　TSF データの管理
FMT_MTD.1.1[6]
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、SNMP 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]*]： ***[割付：その他の操作]：初期化***
[割付:*許可された識別された役割*]： ***管理者、サービスエンジニア***
下位階層　：　なし
依存性　：　FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_SMF.1　　管理機能の特定
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*]： ***・管理者によるセキュリティ強化機能の停止機能*** ***・管理者による SNMP パスワード認証機能の動作設定機能*** ***・管理者による認証操作禁止機能における認証失敗回数閾値の設定機能*** ***・管理者によるバックアップ機能*** [2] ***・管理者によるリストア機能*** [3] ***・管理者による SNMP 不正アクセス検出値の消去機能*** ***・管理者による機密文書不正アクセス検出値の消去機能*** ***・管理者によるボックス不正アクセス検出値の消去機能*** ***・管理者による管理者パスワードの改変機能*** ***・管理者による SNMP パスワードの改変機能*** ***・管理者によるボックスパスワードの改変機能*** ***・管理者による管理者パスワードの初期化機能*** ***・管理者による SNMP パスワードの初期化機能*** ***・サービスエンジニアによる CE パスワードの改変機能*** ***・サービスエンジニアによる管理者パスワードの改変機能*** ***・サービスエンジニアによるセットアップ機能の動作機能*** ***・サービスエンジニアによるセキュリティ強化機能の停止機能*** ***・サービスエンジニアによる管理者パスワードの初期化機能*** ***・サービスエンジニアによる SNMP パスワードの初期化機能*** ***・ボックスの利用を許可されたユーザによる当該ボックスのボックスパスワードの改変機能***
下位階層　：　なし
依存性　：　なし

FMT_SMR.1[1]　　セキュリティ役割
FMT_SMR.1.1[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*]： ***サービスエンジニア***
FMT_SMR.1.2[1]
TSF は、利用者を役割に関連づけなければならない。
下位階層　：　なし
依存性　：　FIA_UID.1（FIA_UID.2[1]）

[2] バックアップ機能の一部は、TSF データの問い合わせ機能に相当する。
[3] リストア機能の一部は、TSF データの改変機能に相当する。

FMT_SMR.1[2]　　セキュリティ役割
FMT_SMR.1.1[2]
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[2]
TSF は、利用者を役割に関連づけなければならない。
下位階層　：　なし
**依存性　：　**FIA_UID.1（FIA_UID.2[2]）

FMT_SMR.1[3]　　セキュリティ役割
FMT_SMR.1.1[3]
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*]： ***そのボックスの利用を許可されたユーザ***
FMT_SMR.1.2[4]
TSF は、利用者を役割に関連づけなければならない。
下位階層　：　なし
**依存性　：　**FIA_UID.1（FIA_UID.2[4]）

5.1.1.5. TSF の保護

FPT_RVM.1　　TSP の非バイパス性
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。
下位階層　：　なし
依存性　：　なし

FPT_SEP.1　　TSF ドメイン分離
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。
下位階層　：　なし
依存性　：　なし

5.1.1.6. 拡張要件：アクセス先の識別と承認

FIA_NEW.1　　TOE からのアクセス対象となる利用者の識別と承認
FIA_NEW.1.1
TSF は、TOE から利用者（*HDD*）に対してアクションする前に、その利用者の識別に成功することを要求しなければならない。
FIA_NEW.1.2
TSF は、利用者の識別に失敗した場合、TOE から利用者（*HDD*）に対するアクションの起動を停止しなければならない。
下位階層　：　なし
依存性　：　なし

監査：FIA_NEW.1
FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである。 a)　最小　提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 b)　基本　提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用
管理：FIA_NEW.1
以下のアクションは FMT における管理機能と考えられる。 a)　利用者識別情報の管理

5.1.1.7. 拡張要件：明示的な消去操作後の残存情報保護

FNEW_RIP.1　　明示的な消去操作後の利用者データと TSF データの残存情報保護
FNEW_RIP.1.1
TSF は、以下のオブジェクト及び TSF データに対する明示的な消去操作において、資源に割り当てられた以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト及び TSF データのリスト*]。
[割付: *オブジェクトのリスト及び TSF データのリスト*]： ***＜オブジェクト＞*** ***・ボックスファイル*** ***・機密文書プリントファイル*** ***・オンメモリ画像ファイル*** ***・保管画像ファイル*** ***・残存画像ファイル*** ***・画像関連ファイル・HDD ロックパスワードオブジェクト*** ***・暗号鍵ワードオブジェクト*** ***＜TSF データ＞*** ***・管理者パスワード*** ***・SNMP パスワード*** ***・ボックスパスワード*** ***・機密文書パスワード*** ***・残存 TSF データ*** [4]
下位階層　：　なし **依存性**　：　なし

監査：FNEW_RIP.1

[4] ファイル管理領域の削除だけでは削除されない、HDD データ領域に残存している TSF データ

明示的な消去操作を行う利用者識別情報を含む使用
管理：FNEW_RIP.1
予見される管理アクティビティはない。

5.1.2. 最小セキュリティ機能強度

TOE の最小機能強度レベルは、SOF-基本である。確率的・順列的メカニズムを利用する TOE セキュリティ機能要件は、FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]、FIA_UAU.6、FIA_SOS.1[1]、FIA_SOS.1[2]、FIA_SOS.1[3]、FIA_SOS.1[4]、FIA_SOS.1[5]、FIA_SOS.2 である。

なお FMT_CKM.1 の暗号鍵生成アルゴリズムは、最小機能強度主張の対象には含まない。

5.1.3. TOE のセキュリティ保証要件

TOE は、一般的なオフィス環境にて利用される商用事務製品であるため、商用事務製品の保証として十分なレベルである EAL3 適合によって必要な TOE セキュリティ保証要件を適用する。下表に適用される TOE のセキュリティ保証要件をまとめる。

表 4　TOE のセキュリティ保証要件

TOEセキュリティ保証要件		コンポーネント
構成管理	CM 能力	ACM_CAP.3
	CM 範囲	ACM_SCP.1
配付と運用	配付	ADO_DEL.1
	設置・生成・及び立上げ	ADO_IGS.1
開発	機能仕様	ADV_FSP.1
	上位レベル設計	ADV_HLD.2
	表現対応	ADV_RCR.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1
テスト	カバレージ	ATE_COV.2
	深さ	ATE_DPT.1
	機能テスト	ATE_FUN.1
	独立テスト	ATE_IND.2
脆弱性評定	誤使用	AVA_MSU.1
	TOE セキュリティ機能強度	AVA_SOF.1
	脆弱性分析	AVA_VLA.1

5.2. IT 環境のセキュリティ要件

5.2.1.1. 暗号サポート

FCS_COP.1[E]　　暗号操作
FCS_COP.1.1[E]
TSF（***暗号化基板***）は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。
[割付: *標準のリスト*]： ***FIPS PUB 197***
[割付: *暗号アルゴリズム*]： ***AES***
[割付: *暗号鍵長*]： ***128bit***
[割付: *暗号操作のリスト*]： ***・HDD に書き込まれるすべてのデータの暗号化*** ***・HDD から読み出されるすべてのデータの復号***
下位階層　：　なし **依存性**　：　FDP_ITC.1 or FCS_CKM.1（FCS_CKM.1）、FCS_CKM.4（適用しない）、 FMT_MSA.2（適用しない）

5.2.1.2. 識別と認証

FIA_AFL.1[E]　　認証失敗時の取り扱い
FIA_AFL.1.1[E]
TSF（***HDD***）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*]： ***HDD にアクセスする際の HDD ロック機能による認証***
[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]*」] ***[割付:正の整数値]：5***
FIA_AFL.1.2[E]
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*]： ***＜検出した際のアクション＞*** ***HDD へのデータの読み込み及び書き込みを拒否する。*** ***＜通常復帰のための操作＞*** ***HDD への通電 OFF（電源 OFF）***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[E]）

FIA_UAU.2[E]　　アクション前の利用者認証
FIA_UAU.2.1[E]
TSF（***HDD***）は、その利用者（***HDD が設置されたプリンタ本体***）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（***HDD が設置されたプリンタ本体***）に自分自身を認証することを要求しなければならない。

下位階層	：	FIA_UAU.1
依存性	：	FIA_UID.1（適用しない）

FIA_UAU.7[E]　保護された認証フィードバック

FIA_UAU.7.1[E]
TSF（*PC アプリケーション*）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*]： ***入力された文字データ１文字毎に“＊”表示***
下位階層　：　なし
依存性　：　FIA_UAU.1（FIA_UAU.2[2]、FIA_UAU.2[4]）

6. TOE 要約仕様

6.1. TOE セキュリティ機能

TOE のセキュリティ機能要件より導かれる TOE のセキュリティ機能を以下の表 5 にて一覧を示す。仕様詳細は、後述の項にて説明する。

表 5　TOE のセキュリティ機能名称と識別子の一覧

No.	TOE のセキュリティ機能	
1	F.ADMIN	管理者機能
2	F.ADMIN-SNMP	SNMP 管理者機能
3	F.SERVICE	サービスモード機能
4	F.BOX	ボックス機能
5	F.PRINT	機密文書プリント機能
6	F.OVERWRITE-ALL	全領域上書き削除機能
7	F.CRYPT	暗号鍵生成機能
8	F.HDD	HDD 検証機能
9	F.RESET	認証失敗回数リセット機能

6.1.1. F.ADMIN（管理者機能）

F.ADMIN とは、パネルやネットワークからアクセスする管理者モードにおける管理者識別認証機能、管理者パスワードの変更やロックされたボックスのロック解除などのセキュリティ管理機能といった管理者が操作する一連のセキュリティ機能である。（なお、すべての機能がパネル及びネットワークの双方から実行可能な機能ということではない。）

6.1.1.1. 管理者識別認証機能

管理者モードへのアクセス要求に対して、アクセスする利用者を管理者であることを識別及び認証する。

- 表 6 に示されるキャラクタからなる管理者パスワードにより認証する管理者認証メカニズムを提供する。
  - ネットワークからのアクセスに対して管理者認証後は、管理者パスワードとは別のセッション情報を利用した、管理者認証メカニズムを提供する。
  - プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- 管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 管理者パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、管理者パスワードを利用するすべての認証機能をロックする。(管理者モードへのアクセスを拒否する。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET 機能が動作して解除する。

表 6　パスワードに利用されるキャラクタと桁数

対象	桁数	キャラクタ
CE パスワード 管理者パスワード	8 桁	合計 92 文字が選択可能 ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~
ボックスパスワード 機密文書パスワード	8 桁	合計 93 文字が選択可能 ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、*SPACE*
HDD ロックパスワード 暗号鍵ワード	20 桁	合計 83 文字が選択可能 ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、 #、 $、 %、 &、 ’ 、 *、 +、 -、.、 /、 =、 ?、 @、 ^、 _、 `、 {、 |、 }、 ~
SNMP パスワード ・Privacy パスワード ・Authentication パスワード	8 桁以上	合計 95 文字が選択可能 ASCII コード（0x20 ～ 0x7E） ・数字：0 ～ 9 ・英字：大文字、小文字 ・記号：!、#、$、%、&、'、(、)、*、,、-、.、/、:、;、<、=、>、?、@、[、¥、]、^、_、`、{、|、}、~、”、+、*SPACE*

6.1.1.2. 管理者モードにて提供される機能

管理者モードへのアクセス要求において管理者識別認証機能により、管理者として識別認証されると、利用者を代行するタスクに管理者属性が関連づけられ、以下の操作、機能の利用が許可される。

① 管理者パスワードの変更

管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

- 表 6 に示されるキャラクタからなる管理者パスワードにより認証する管理者パスワード認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、パネルからのアクセスの場合、管理者パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 管理者パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、パネルからアクセスする管理者モードをログオフし、管理者パスワードを利用するすべての認証機能をロックする。（管理者モードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET 機能が動作して解除する。

- 新規設定される管理者パスワードは以下の品質を満たしていることを検証する。
  - 表 6 の管理者パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

② ボックスの設定

- ボックスの登録
  - 選択した未登録ボックス ID に対して、ボックスパスワードを設定し、ボックスを登録する。
  - 新しく設定されるボックスパスワードは以下の品質を満たしていることを検証する。
    - ✧ 表 6 のボックスパスワードに示される桁数、キャラクタから構成される。
    - ✧ 1 つのキャラクタで構成されない。
- ボックスパスワードの変更
  - ボックスに設定されるボックスパスワードを変更する。
  - 新しく設定されるボックスパスワードは以下の品質を満たしていることを検証する。
    - ✧ 表 6 のボックスパスワードに示される桁数、キャラクタから構成される。
    - ✧ 1 つのキャラクタで構成されない。

③ ロックの解除

すべての機密文書プリントの認証失敗回数を 0 クリアする。

- アクセスがロックされている機密文書プリントが存在すれば、ロックが解除される。

すべてのボックスの認証失敗回数を 0 クリアする。

- アクセスがロックされているボックスが存在すれば、ロックが解除される。

SNMP パスワードによる認証失敗回数を 0 クリアする。

- MIB オブジェクトへのアクセスがロックされていれば、ロックが解除される。

④ 不正アクセス検出閾値の設定

認証操作禁止機能における不正アクセス検出閾値を 1～3 回間で設定する。

⑤ 全領域上書き削除機能の設定と実行

以下の表に示される消去方式を選択し、HDD のデータ領域の上書き削除を実行する。（F.OVERWRITE-ALL を実行する。）

表 7　全領域の上書き削除のタイプと上書きの方法

方式	上書きされるデータタイプとその順序
Mode:1	0x00
Mode:2	乱数 ⇒ 乱数 ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証
Mode:4	乱数 ⇒ 0x00 ⇒ 0xFF
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証

⑥ ネットワークの設定

以下の設定データの設定操作を行う。

- プリンタアドレスに関係する一連の設定データ（IP アドレス、NetBIOS 名、AppleTalk プリンタ名等）

⑦ バックアップ、リストア機能の実行

管理者パスワード、CE パスワードを除いて、NVRAM 及び HDD に保管されるあらゆる設定データをバックアップ、リストアする。（媒体の単位で設定可能。）セキュリティに関係する対象としては、秘匿性、完全性の関係より以下の分類にて示されるものが対象となっている。

＜タイプ A　バックアップ・リストア制限されるべき対象＞

- HDD ロックパスワード
- 暗号鍵ワード
- SNMP パスワード
- 機密文書パスワード
- ボックスパスワード

＜タイプ B　リストアが制限されるべき対象＞

- プリンタアドレス設定に関係する一連のデータ
- セキュリティ強化機能の設定データ
- 認証操作禁止機能の認証失敗回数閾値

＜タイプ C　バックアップが制限されるべき対象＞

- 機密文書プリントファイル
- ボックスファイル

⑧ HDD ロック機能の動作設定機能

＜動作設定　ON＞

OFF から ON にする場合、新しく設定される HDD ロックパスワードが以下の品質を満たしていることを検証する。

- 表 6 の HDD ロックパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

＜HDD ロックパスワード変更＞

HDD ロックパスワードを変更する。現在設定される HDD ロックパスワードを使い、管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

- 表 6 に示されるキャラクタからなる HDD ロックパスワードを照合する HDD ロックパスワード照合メカニズムを提供する。
- 照合では、HDD ロックパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 新規設定される HDD ロックパスワードは以下の品質を満たしていることを検証する。
  - 表 6 の HDD ロックパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

⑨ 暗号化機能の動作設定

暗号化基板オプションがプリンタに装着されている場合のみ操作可能。

＜動作設定　ON＞

OFF から ON にする場合、新しく設定される暗号鍵ワードが以下の品質を満たしていることを検証し、F.CRYPT が実行される。

- 表 6 の暗号鍵ワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

＜暗号鍵ワード変更＞

暗号鍵ワードを変更する。現在設定される暗号鍵ワードを使い、管理者であることを再認証され、且つ新規設定される暗号鍵ワードが品質を満たしている場合に変更し、F.CRYPT が実行される。

- 表 6 に示されるキャラクタからなる暗号鍵ワードを照合する暗号鍵ワード照合メカニズムを提供する。
- 照合では、暗号鍵ワード入力のフィードバックに 1 文字毎“＊”を返す。
- 新規設定される暗号鍵ワードは以下の品質を満たしていることを検証する。
  - 表 6 の暗号鍵ワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

⑩ セキュリティ強化機能に関連する機能

管理者が操作するセキュリティ強化機能の設定に影響する機能は以下の通り。（※バックアップ・リストア機能の影響については、⑦にて説明済み）

- セキュリティ強化機能の動作設定
  セキュリティ強化機能の有効、無効を設定する機能。
- HDD 論理フォーマット機能
  HDD に OS のシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- 全領域上書き削除機能
  全領域の上書き削除の実行により、セキュリティ強化機能の設定を無効にする。

⑪ SNMP パスワードの変更

SNMP パスワード（Privacy パスワード、Authentication パスワード）を変更する。新しく設定される SNMP パスワードが以下の品質を満たしていることを検証する。

- 表 6 の SNMP パスワードに示される桁数、キャラクタから構成される。

⑫ SNMP パスワード認証機能の設定

SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。

6.1.2. F.ADMIN-SNMP（SNMP 管理者機能）

F.ADMIN-SNMP とは、PC から SNMP を利用してネットワークを介したアクセスにおいて管理者を識別認証し、識別認証された管理者だけにネットワークの設定機能の操作を許可するセキュリティ機能である。

6.1.2.1. SNMP パスワードによる識別認証機能

SNMP を用いてネットワークを介して MIB オブジェクトにアクセスする利用者が管理者であることを SNMP パスワードによって識別認証する。

- 表 6 に示されるキャラクタからなる SNMP パスワードにより認証する SNMP 認証メカニズムを提供する。
  - Authentication パスワードのみ、または Privacy パスワード及び Authentication パスワード双方を利用する。
  - SNMP の場合は、別途セッション情報による管理者認証メカニズムを必要とせず、毎回のセッションに SNMP パスワード利用する。
- 認証に成功すると、認証失敗回数をリセットする。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に成功した場合に認証失敗回数をリセットする。
- SNMP パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、SNMP パスワードを利用するすべての認証機能をロックする。（MIB オブジェクトへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
  - Privacy パスワード、Authentication パスワードの双方を利用している場合は、双方共に認証に失敗した場合でも 1 回の失敗として検知する。
- ロック状態は、F.ADMIN の MIB オブジェクトに対するロック解除機能を実行する、または F.RESET 機能が動作して解除する。

6.1.2.2. SNMP を利用した管理機能

SNMP パスワードにより管理者であることが識別認証されると、MIB オブジェクトへのアクセスが許可され、以下に示す設定データの設定操作を行うことが許可される。

① ネットワークの設定

以下の設定データの設定操作を行う。

- プリンタアドレスに関係する一連の設定データ（IP アドレス、NetBIOS 名、AppleTalk プリンタ名等）

② SNMP パスワードの変更

SNMP パスワード（Privacy パスワード、Authentication パスワード）を変更する。新しく設定される SNMP パスワードが以下の品質を満たしていることを検証する。

- 表 6 の SNMP パスワードに示される桁数、キャラクタから構成される。

③ SNMP パスワード認証機能の設定

SNMP パスワード認証機能における認証方式を「Authentication パスワードのみ」または「Authentication パスワード且つ Privacy パスワード」に設定する。

6.1.3. F.SERVICE（サービスモード機能）

F.SERVICE とは、パネルからアクセスするサービスモードにおけるサービスエンジニア識別認証機能、CE パスワードの変更や管理者パスワードの変更などのセキュリティ管理機能といったサービスエンジニアが操作する一連のセキュリティ機能である。

6.1.3.1. サービスエンジニア識別認証機能

パネルからサービスモードへのアクセス要求に対して、アクセスする利用者をサービスエンジニアであることを識別及び認証する。

- 表 6 に示されるキャラクタからなる CE パスワードにより認証する CE 認証メカニズムを提供する。
  - サービスモードの場合はパネルからのアクセスのみになるため、別途セッション情報による CE 認証メカニズムを必要としない。
- CE パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、CE パスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET 機能が動作して解除する。

6.1.3.2. サービスモードにて提供される機能

サービスモードへのアクセス要求においてサービスエンジニア識別認証機能により、サービスエンジニアとして識別認証されると、以下の機能の利用が許可される。

① CE パスワードの変更

サービスエンジニアであることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

- 表 6 に示されるキャラクタからなる CE パスワードにより再認証する CE パスワード認証メカニズムを提供する。
- 再認証に成功すると、認証失敗回数をリセットする。
- 再認証では、CE パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- CE パスワードを利用する各認証機能において通算 1～3 回目となる認証失敗を検知すると、パネルからアクセスするサービスモードをログオフし、CE パスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.RESET 機能が動作して解除する。
- 新規設定される CE パスワードは以下の品質を満たしていることを検証する。
  - 表 6 の CE パスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。
  - 現在設定される値と一致しない。

② 管理者パスワードの変更

管理者パスワードを変更する。新規設定される管理者パスワードは以下の品質を満たしていることを検証する。

- 表 6 の管理者パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。
- 現在設定される値と一致しない。

③ セキュリティ強化機能に関連する機能

サービスエンジニアが操作するセキュリティ強化機能の設定に影響する機能は以下の通り。

- HDD 論理フォーマット機能
  HDD に OS のシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- HDD 物理フォーマット機能
  HDD にトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。
- HDD 装着設定機能
  搭載された HDD を有効化するための機能。この HDD 装着設定を無効化することにより、セキュリティ強化機能の設定を無効にする。
- イニシャライズ機能
  NVRAM に書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、セキュリティ強化機能の設定を無効にする。

④ セットアップ機能の動作設定機能

セットアップ機能の利用有無（起動）を設定する。

⑤ パスワード初期化機能に関連する機能

サービスエンジニアが操作するパスワードの初期化に関係する機能は以下の通り。

- イニシャライズ機能
  NVRAM に書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、管理者パスワード、SNMP パスワードを工場出荷の初期値に設定する。HDD ロック機能、暗号化機能の動作設定をいずれも OFF にする。（動作設定が OFF されることにより、設定されていた HDD ロックパスワード、暗号鍵ワードを再度利用することができなくなる。）
- HDD 物理フォーマット機能
  HDD にトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、HDD ロック機能を OFF にする。（動作設定が OFF されることにより、設定されていた HDD ロックパスワードを再度利用することができなくなる。）

6.1.4. F.BOX（ボックス機能）

F.BOX とは、ボックスへのアクセスに対してボックスの利用を許可されたユーザであることを認証し、認証後に当該ボックス、ボックスファイルの各種操作を許可するアクセス制御機能などボックスに関係する一連のセキュリティ機能のことである。

6.1.4.1. ボックスの登録

- 選択した未登録ボックス ID に対して、ボックスパスワードを設定し、ボックスを登録する。
- 登録されるボックスパスワードが以下の条件を満たすことを検証する。
  - 表 6 のボックスパスワードに示される桁数、キャラクタから構成される。
  - 1 つのキャラクタで構成されない。

6.1.4.2. ボックスへのアクセスにおける認証機能

ボックスへのアクセス要求に対して、アクセスする利用者をそれぞれ当該ボックスの利用を許可されたユーザであることを認証する。

- 表 6 に示されるキャラクタからなるボックスパスワードにより認証するボックス認証メカニズムを提供する。
  - ネットワークからのアクセスに対してボックス認証後は、ボックスパスワードとは別のセッション情報を利用した、ボックス認証メカニズムを提供する。
- プロトコルに応じて、10^{10} 以上のセッション情報を利用、または 10^{10} 以上のセッション情報を生成して利用する。
- ボックスパスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 当該ボックスに対して、通算 1～3 回目となる認証失敗を検知すると、当該ボックスに対する認証機能をロックする。
- 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- 認証機能のロックは、F.ADMIN のボックスに対するロック解除機能を実行する、または F.RESET 機能が動作して解除する。

6.1.4.3. ボックス内のボックスファイルに対するアクセス制御

ボックスの利用を許可されたユーザを代行するタスクは、そのボックスの「ボックス ID」がボックス属性としてタスクに関連付けられる。このタスクは、タスクのボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

6.1.4.4. ボックスパスワードの変更

ボックスのボックスパスワードを変更する。新しく設定されるボックスパスワードが以下の品質を満たしている場合、変更する。

- 表 6 のボックスパスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

6.1.5. F.PRINT（機密文書プリント機能）

F.PRINT とは、パネルからの機密文書プリントファイルへのアクセスに対して機密文書プリントファイルの利用を許可されたユーザであることを認証し、認証後に当該機密文書プリントファイルの印刷を許可するアクセス制御機能など機密文書プリントに関係する一連のセキュリティ機能である。

6.1.5.1. 機密文書パスワードによる認証機能

パネルから機密文書プリントファイルへのアクセス要求に対して、アクセスする利用者を当該機密文書プリントファイルの利用を許可されたユーザであることを認証する。

- 表 6 に示されるキャラクタからなる機密文書パスワードにより認証する機密文書認証メカニズムを提供する。
  - 機密文書プリントの場合はパネルからのアクセスのみになるため、別途セッション情報による機密文書認証メカニズムを必要としない。
- 機密文書パスワード入力のフィードバックに 1 文字毎“＊”を返す。
- 認証に成功すると、認証失敗回数をリセットする。
- パネルからのアクセスの場合、認証に失敗するとパネルからの入力を 5 秒間受け付けない。
- 当該機密文書プリントファイルに対して、通算 1～3 回目となる認証失敗を検知すると、当該機密分文書プリントファイルに対する認証機能をロックする。
  - 失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。
- ロック状態は、F.ADMIN の機密文書プリントファイルに対するロック解除機能を実行する、または F.RESET 機能が動作して解除する。

6.1.5.2. 機密文書プリントファイルに対するアクセス制御機能

機密文書プリントファイルの利用を許可されたユーザを代行するタスクは、ファイル属性に、認証された機密文書プリントファイルの**機密文書内部制御** ID を持つ。このタスクは、このファイル属性と一致するファイル属性を持つ機密文書プリントファイルに対して印刷を許可される。

6.1.5.3. 機密文書の登録機能

機密文書プリントファイルの登録要求において、以下の処理を行う。

① **機密文書パスワードの登録**

機密文書と共に登録される機密文書パスワードが以下の条件を満たすことを検証する。

- 表 6 の機密文書パスワードに示される桁数、キャラクタから構成される。
- 1 つのキャラクタで構成されない。

② **機密文書内部制御** ID **の付与**

機密文書プリントファイルの登録要求において、機密文書パスワードの検証が完了すると、一意に識別される機密文書内部制御 ID を当該機密文書プリントファイルに設定する。

6.1.6. F.OVERWRITE-ALL（全領域上書き削除機能）

F.OVERWRITE-ALL とは、HDD のデータ領域に上書き削除を実行すると共に NVRAM に設定されているパスワード等の設置値を初期化する。削除、または初期化される対象は以下の通りである。

＜削除される対象：HDD＞
- 機密文書プリントファイル
- ボックスファイル
- オンメモリ画像ファイル
- 保管画像ファイル
- 残存画像ファイル
- 画像関連ファイル
- ボックスパスワード
- 機密文書パスワード
- 残存 TSF データ

＜初期化される対象：NVRAM＞
- 管理者パスワード
- SNMP パスワード
- HDD ロック機能の動作設定（OFF）
- 暗号化機能の動作設定（OFF）

HDD に書き込むデータ、書き込む回数など削除方式は、F.ADMIN において設定される全領域上書き削除機能の消去方式（表 7）に応じて実行される。HDD ロック機能及び暗号化機能は動作設定が OFF されることによって、設定されていた HDD ロックパスワード、暗号鍵ワードが利用できなくなる。なお、本機能の実行においてセキュリティ強化機能の設定は無効になる。（F.ADMIN におけるセキュリティ強化機能の動作設定の記載参照）

6.1.7. F.CRYPT（暗号鍵生成機能）

F.CRYPT とは、コニカミノルタ暗号仕様標準によって規定されるコニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）を利用し、HDD に書き込まれるすべてのデータを暗号化するための暗号鍵を生成する。コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）とは、FIPS 180-1 が規定する SHA-1 を利用して暗号鍵を生成するアルゴリズムである。

F.ADMIN においてアクセス制限される暗号化機能の動作設定において暗号鍵ワードが決定されると、コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）を用いて暗号鍵ワードから 128bit 長の暗号鍵を生成する。

6.1.8. F.HDD（HDD 検証機能）

F.HDD とは、HDD に HDD ロックパスワードを設定している場合において、不正な HDD が設置されていないことを検証し、正当性が確認された場合だけ HDD への読み込み、書き込みを許可するチェック機能である。

HDD に HDD ロックパスワードが設定されている場合、TOE 起動時の HDD 動作確認において、HDD のステータス確認を行う。ステータス確認の結果、HDD ロックパスワードが確かに設定されていることが返された場合は、HDD へのアクセスを許可し、HDD ロックパスワードが設定されていないことが返された場合は、不正な可能性があるため HDD へのアクセスを拒否する。

6.1.9. F.RESET（認証失敗回数リセット機能）

F.RESET とは、管理者認証を始めとした各認証機能においてカウントされる認証失敗回数をリセットする機能である。（ロックの有無と関係しない。）

主電源が ON される、または停電などから復帰した場合など TOE の起動により本機能は動作する。起動すると、以下の認証失敗回数をリセットする。（アカウントロックされていた対象は、ロックが解除される。）

- 管理者の認証に対する失敗回数
- SNMP パスワードを利用した認証に対する失敗回数
- サービスエンジニアの認証に対する失敗回数
- 各ボックスの認証に対する失敗回数
- 各機密文書プリントの認証に対する失敗回数

6.2. TOE セキュリティ機能強度

確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りであり、機能強度はそれぞれ SOF-基本を満たす。

① F.ADMIN が提供する管理者認証メカニズム、HDD ロックパスワード照合メカニズム、暗号鍵ワード照合メカニズム
② F.SERVICE が提供する CE 認証メカニズム
③ F.PRINT が提供する機密文書認証メカニズム
④ F.BOX が提供するボックス認証メカニズム
⑤ F.ADMIN-SNMP が提供する SNMP 認証メカニズム

6.3. TOE セキュリティ機能と機能要件の対応関係

TOE のセキュリティ機能と TOE セキュリティ機能要件との対応関係は 8.3 TOE 要約仕様根拠の表 13 に示す。表 13 は TOE のセキュリティ機能が少なくとも 1 つ以上の TOE セキュリティ機能要件に対応していることが示される。

6.4. 保証手段

表 8 で記述した EAL3 の TOE セキュリティ保証要件のコンポーネントを満たす保証手段を下表に示す。

表 8　TOE 保証要件と保証手段の関係

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	CM 能力	ACM_CAP.3	・構成管理計画書 ・構成リスト ・CM 記録
	CM 範囲	ACM_SCP.1	
配付と運用	配付	ADO_DEL.1	配付説明書
	設置・生成・及び立上げ	ADO_IGS.1	・サービスマニュアル bizhub C252P サービスマニュアル[セキュリティ機能編]（和文）、bizhub C252P / ineo+ 251P / magicolor 7465CK Service Manual [Security Function]（英文） ・ユーザーズガイド bizhub C252P ユーザーズガイド[セキュリティ機能編]（和文）、bizhub C252P User's Guide [Security Operations]（英文）、ineo+ 251P User's Guide [Security Operations]（英文）、magicolor 7465CK User's Guide [Security Operations]（英文）
開発	機能仕様	ADV_FSP.1	セキュリティ機能仕様書
	上位レベル設計	ADV_HLD.2	セキュリティ上位レベル設計書
	表現対応	ADV_RCR.1	表現対応分析書
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	・サービスマニュアル bizhub C252P サービスマニュアル[セキュリティ機能編]（和文）、bizhub C252P / ineo+ 251P / magicolor 7465CK Service Manual [Security Function]（英文） ・ユーザーズガイド bizhub C252P ユーザーズガイド[セキュリティ機能編]（和文）、bizhub C252P User's Guide [Security Operations]（英文）、ineo+ 251P User's Guide [Security Operations]（英文）、magicolor 7465CK User's Guide [Security Operations]（英文）
	利用者ガイダンス	AGD_USR.1	
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1	開発セキュリティ説明書
テスト	カバレージ	ATE_COV.2	カバレージ分析書
	深さ	ATE_DPT.1	深さ分析書
	機能テスト	ATE_FUN.1	テスト仕様・結果報告書
	独立テスト	ATE_IND.2	TOE を含むプリンタ制御ソフトウェア
脆弱性評定	誤使用	AVA_MSU.1	※特にドキュメントはなし （ガイダンス文書証拠に要求事項反映）
	TOE セキュリティ機能強度	AVA_SOF.1	脆弱性分析書
	脆弱性分析	AVA_VLA.1	

7. PP 主張

本 ST には、適合する PP はない。

8. 根拠

8.1. セキュリティ対策方針根拠

8.1.1. 必要性

前提条件、脅威、及び組織のセキュリティ方針とセキュリティ対策方針の対応関係を下表に示す。セキュリティ対策方針が少なくとも 1 つ以上の前提条件、脅威に対応していることを示している。

表 9　前提条件、脅威に対するセキュリティ対策方針の適合性

前提・脅威 / セキュリティ対策方針	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-PRINTER	T.BRING-OUT-STORAGE	T.ACCESS-BOX	T.ACCESS-SECURE-PRINT	T.ACCESS-NET-SETTING	T.ACCESS-SETTING	T.BACKUP-RESTORE
O.BOX								●				
O.SECURE-PRINT									●			
O.CONFIG										●	●	●
O.OVERWRITE-ALL						●						
O.CRYPT-KEY							●					
O.CHECK-HDD							●					
OE.CRYPT							●					
OE.LOCK-HDD							●					
OE.FEED-BACK								●	●	●	●	●
OE-N.ADMIN	●											
OE-N.SERVICE		●										
OE-N.NETWORK			●									
OE-N.SECRET				●								
OE-N.SESSION								●	●	●	●	●
OE-N.SETTING-SECURITY					●							

8.1.2. 前提条件に対する十分性

前提条件に対するセキュリティ対策方針について以下に説明する。

- **A.ADMIN（管理者の人的条件）**
  本条件は、管理者が悪意を持たないことを想定している。
  OE-N.ADMIN は、プリンタを利用する組織がプリンタを利用する組織において信頼のおける人物を管理者に指定するため、管理者の信頼性が実現される。

- **A.SERVICE（サービスエンジニアの人的条件）**
  本条件は、サービスエンジニアが悪意を持たないことを想定している。
  OE-N.SERVICE は、プリンタを保守管理する組織においてサービスエンジニアを教育する。また管理者は、サービスエンジニアの行うメンテナンス作業に立ち会うことが規定されているため、サービスエンジニアの信頼性は確保される

- **A.NETWORK（プリンタのネットワーク接続条件）**
  本条件は、オフィス内 LAN の盗聴行為、外部ネットワークから不特定多数の者による攻撃などが行われないことを想定している。
  OE-N.NETWORK は、オフィス内 LAN に暗号化通信を行うための機器や盗聴検知機器を設置するなどにより、盗聴の防止を規定している。また外部ネットワークからプリンタへのアクセスを遮断するためにファイアウォールなどの機器を設置することにより外部からの不正侵入の防止を規定しており、本条件は実現される。

- **A.SECRET（秘密情報に関する運用条件）**
  本条件は、TOE の利用において使用される各パスワード、暗号鍵ワードが各利用者より漏洩しないことを想定している。
  OE-N.SECRET は、管理者がユーザに対して機密文書パスワード、ボックスパスワードに関する運用規則を実施させることを規定し、管理者が管理者パスワード、HDD ロックパスワード、SNMP パスワード、暗号鍵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、サービスエンジニアが CE パスワードに関する運用規則を実施し、管理者に対して、管理者パスワードに関する運用規則を実施させることを規定しており、本条件は実現される。

- **A.SETTING（セキュリティ強化機能の動作設定条件）**
  本条件は、セキュリティ強化機能の動作設定条件が満たされることを想定している。
  OE-N.SETTING-SECURITY は、管理者がセキュリティ強化機能の設定を有効化した上で利用することを規定しており、本条件は実現される。

8.1.3. 脅威に対する十分性

脅威に対抗するセキュリティ対策方針について以下に説明する。

- **T.DISCARD-PRINTER（プリンタのリース返却、廃棄）**
  本脅威は、ユーザから回収されたプリンタ内の HDD より情報漏洩する可能性を想定している。
  O.OVERWRITE-ALL は、TOE が HDD の全領域に削除用のデータを上書きする機能を提供し、NVRAM の情報を初期化するとしており、プリンタが回収される前にこの機能を実行することによって、脅威の可能性は除去される。
  したがって本脅威は十分対抗されている。

- **T.BRING-OUT-STORAGE（HDD の不正な持ち出し）**
  本脅威は、プリンタを利用している運用環境から HDD が盗み出される、または不正な HDD が取り付けられて、そこにデータが蓄積されたところで持ち出されることにより、HDD 内の画像データ、パスワードが漏洩する可能性を想定している。
  これに対して以下の 2 つの対策の少なくともどちらかの対策が、管理者によって選択されるため、脅威の可能性は除去される。

① O.CRYPT-KEY は、TOE が HDD に書き込まれるデータを暗号化するための暗号鍵を生成し、OE.CRYPT により、暗号化基板がデータを暗号化する。

② OE.LOCK-HDD は、HDD の機能として、プリンタに設置される HDD が設置されたプリンタ以外からはデータを読み出しすることを許可しない。

上記において、②のみが選択された場合は、HDD がすりかえられて、②の機能を持たない HDD が設置されることにより、持ち出されて漏洩する危険性が存在する。これに対しては、O.CHECK-HDD により、TOE によって設置されている HDD の正当性が検証されるため、すりかえられた HDD にはデータを書き込むことはない。したがって脅威の可能性は除去される。
したがって本脅威は十分対抗されている。

- **T.ACCESS-BOX（ユーザ機能を利用したボックスへの不正なアクセス）**

本脅威は、ユーザが共有して利用する画像ファイルの保管場所であるボックスに対して、ユーザ機能を利用して不正な操作が行われる可能性を想定している。
O.BOX によってボックス、ボックス内のボックスファイルの操作が、許可されたユーザだけに制限され、脅威の可能性は除去される。
OE.FEED-BACK は、ボックスの認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE-N.SESSION により操作終了後にはログオフする運用が要求されるため、O.BOX は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-SECURE-PRINT（機密文書プリントファイルへの不正なアクセス）**

本脅威は、機密文書プリントに対して不正な操作が行われてしまう可能性を想定している。
O.SECURE-PRINT によって、機密文書プリントの操作が許可されたユーザだけに制限され、脅威の可能性は除去される。
OE.FEED-BACK は、機密文書プリントへのアクセス認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE-N.SESSION により操作終了後にはログオフする運用が要求されるため、O.SECURE-PRINT は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-NET-SETTING（ネットワーク設定の不正変更）**

本脅威は、プリンタのアドレスに関係するネットワーク設定を不正に変更された場合に、TOE であると思って利用するユーザが、不正なエンティティに PC からプリント機能を利用してしまう可能性を想定している。特にオフィス内の他のユーザに対しても秘匿性が要求される機密文書プリントファイルが不正なエンティティに送信されると問題となる。
これに対して O.CONFIG により、TOE が送信に関係するネットワーク設定を操作する役割を管理者に制限するとしており、本脅威の可能性は除去される。
OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE-N.SESSION により操作終了後にはログオフする運用が要求されるため、O.CONFIG は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.ACCESS-SETTING（セキュリティに関係する機能設定条件の不正変更）**

本脅威はセキュリティに関係する特定の機能設定を変更されることにより、結果的にボックスファイルや機密文書プリントファイルの漏洩に発展する可能性を想定している。
O.CONFIG により、一連のセキュリティに関連する設定機能を統括するセキュリティ強化機能の設定を管理者及びサービスエンジニアだけに許可するとしており、脅威の可能性が除去される。

OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE-N.SESSION により管理者モード、サービスモードの操作終了後にはそれぞれログオフする運用が要求されるため、O.CONFIG は十分サポートされている。
したがって本脅威は十分対抗されている。

- **T.BACKUP-RESTORE（バックアップ機能、リストア機能の不正な使用）**
  本脅威はバックアップ機能、リストア機能が不正に利用されることにより、ボックスファイルや機密文書プリントファイルが漏洩する可能性がある他、パスワード等秘匿性のあるデータが漏洩する、各種設定値等が改ざんされた結果、ボックスファイル、機密文書プリントファイルを想定している。
  O.CONFIG により、バックアップ機能、リストア機能の利用を管理者だけに許可するとしており、脅威の可能性が除去される。
  OE.FEED-BACK は、管理者の認証において入力されるパスワードに対して保護されたフィードバックを返すとしており、また OE-N.SESSION により操作終了後にはログオフする運用が要求されるため、O.CONFIG をサポートしている。
  したがって本脅威は十分対抗されている。

8.1.4. 組織のセキュリティ方針に対する十分性

組織のセキュリティ方針は適用されていない。

8.2. IT セキュリティ要件根拠

8.2.1. IT セキュリティ機能要件根拠

8.2.1.1. 必要性

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関係を下表に示す。IT セキュリティ機能要件が少なくとも 1 つ以上のセキュリティ対策方針に対応していることを示している。

表 10　セキュリティ対策方針に対する IT セキュリティ機能要件の適合性

セキュリティ対策方針 / セキュリティ機能要件	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	OE.CRYPT	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
set.admin	●	●	●								
set.service	●	●	●								
FCS_CKM.1					●						
FDP_ACC.1[1]	●		●								
FDP_ACC.1[2]		●	●								
FDP_ACC.1[3]			●								
FDP_ACF.1[1]	●		●								
FDP_ACF.1[2]		●	●								
FDP_ACF.1[3]			●								
FIA_AFL.1[1]											●
FIA_AFL.1[2]										●	
FIA_AFL.1[3]			●								
FIA_AFL.1[4]		●									
FIA_AFL.1[5]	●										
FIA_AFL.1[6]	●	●								●	●
FIA_ATD.1	●	●									
FIA_SOS.1[1]										●	●
FIA_SOS.1[2]			●								
FIA_SOS.1[3]			●								
FIA_SOS.1[4]	●	●									
FIA_SOS.1[5]	●									●	
FIA_SOS.2	●									●	
FIA_UAU.2[1]											●
FIA_UAU.2[2]			●							●	
FIA_UAU.2[3]		●									
FIA_UAU.2[4]	●										
FIA_UAU.6			●							●	●
FIA_UAU.7	●	●								●	●
FIA_UID.2[1]											●
FIA_UID.2[2]			●							●	
FIA_UID.2[3]		●									
FIA_UID.2[4]	●										
FIA_USB.1	●	●									
FMT_MOF.1[1]			●								

セキュリティ対策方針 / セキュリティ機能要件	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	OE.CRYPT	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
FMT_MOF.1[2]			●								
FMT_MOF.1[3]			●								
FMT_MSA.3		●									
FMT_MTD.1[1]	●	●	●							●	●
FMT_MTD.1[2]	●		●								
FMT_MTD.1[3]										●	
FMT_MTD.1[4]			●								
FMT_MTD.1[5]											●
FMT_MTD.1[6]			●							●	
FMT_SMF.1	●	●	●							●	●
FMT_SMR.1[1]			●							●	●
FMT_SMR.1[2]	●	●	●							●	
FMT_SMR.1[3]	●										
FPT_RVM.1	●	●	●			●					
FPT_SEP.1	●	●	●								
FNEW_RIP.1				●							
FIA_NEW.1						●					
FCS_COP.1[E]							●				
FIA_AFL.1[E]								●			
FIA_UAU.2[E]								●			
FIA_UAU.7[E]									●		

注) ***set.admin***、***set.service*** は、要件のセットを示しており、「●」が記され対応関係があるとされるセキュリティ対策方針は、縦軸の※ set.admin、※ set.service にて対応付けられる一連の要件セットが、当該セキュリティ対策方針にも対応していることを示す。

8.2.1.2. 十分性

各セキュリティ対策方針に対して適用される IT セキュリティ機能要件について以下に説明する。

- **O.BOX（ボックスアクセス制御）**

  本セキュリティ対策方針は、ボックスの設定、ボックス内のボックスファイルの操作をそのボックスの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

  ＜ボックスアクセス制御（ボックス）＞
  ボックス内のボックスファイルを操作するには、そのボックスの利用を許可されたユーザである必要があるが、FIA_UID.2[4]、FIA_UAU.2[4]により、そのボックスの利用を許可されたユーザであることを識別認証される。
  認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
  FIA_AFL.1[6]により、パネルから試行した不成功認証の場合は、失敗の度、5 秒間パネルからの

すべての入力受付を拒否し、FIA_AFL.1[5]により、不成功認証が 1～3 回に達すると、当該ボックスに対する認証機能をロックする。このロック状態は、TOE の起動、または管理者の解除操作によって解除される。
そのボックスの利用を許可されたユーザであることの認証における不成功認証の試行回数である不正アクセス検出値の閾値の設定は、FMT_MTD.1[1]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクにボックス ID が関連付けられると、FDP_ACC.1[1]、FDP_ACF.1[1]により、サブジェクト属性のボックス ID と一致するオブジェクト属性を持つボックスファイルに対して、印刷、他のボックスへの移動、他のボックスへのコピー操作が許可される。

＜ボックスの管理＞
FMT_MTD.1[2]により、ボックスパスワードの変更は、管理者及びそのボックスの利用を許可されたユーザだけに許可される。この際に FIA_SOS.1[4]により、ボックスパスワードの品質が検証される。また FIA_SOS.1[5]によりネットワークを経由したボックス認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者、FMT_SMR.1[3]によりそのボックスの利用を許可されたユーザとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.SECURE-PRINT（機密文書プリントファルアクセス制御）**

本セキュリティ対策方針は、機密文書プリントファイルの印刷をその機密文書プリントファイルの利用を許可されたユーザだけに制限しており、アクセス制御に関係する諸要件が必要である。

＜機密文書プリントファイルアクセス制御＞
機密文書プリントファイルを印刷するには、その機密文書プリントファイルの利用を許可されたユーザである必要があるが、FIA_UID.2[3]、FIA_UAU.2[3]により、その機密文書プリントファイルの利用を許可されたユーザであることを識別認証される。
認証には、FIA_UAU.7 により、パネルに保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。
FIA_AFL.1[6]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[4]により、不成功認証が 1～3 回に達すると、当該機密文書プリントファイルに対する認証機能をロックする。このロック状態は、TOE の起動、または管理者の解除操作によって解除される。
機密文書プリントファイルの利用を許可されたユーザであることの認証における不成功認証の試行回数である不正アクセス検出値の閾値の設定は、FMT_MTD.1[1]により、管理者だけに許可される。
FIA_ATD.1、FIA_USB.1 により、利用を代行するタスクに機密文書内部制御 ID が関連付けられ

ると、FDP_ACC.1[2]、FDP_ACF.1[2]により、サブジェクト属性の機密文書内部制御 ID と一致するオブジェクト属性を持つ機密文書プリントファイルに対して、印刷操作が許可される。なお機密文書内部制御 ID は、FMT_MSA.3 より機密文書プリントファイルの登録時に一意に識別される値が与えられている。

＜機密文書パスワード＞
FIA_SOS.1[4]により機密文書プリントパスワードの品質は検証される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[2]により管理者として維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.CONFIG（管理機能へのアクセス制限）**

本セキュリティ対策方針は、プリンタの IP アドレスなどの設定、セキュリティ強化機能に関係する設定、バックアップ機能、リストア機能を管理者に制限しており、一連の設定機能や管理機能に対してアクセスを制限するための諸要件が必要である。

＜ネットワークの設定管理＞
利用を代行するタスクに管理者属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、利用者を代行するタスクは、プリンタアドレスグループオブジェクトに対する設定操作が許可される。

＜バックアップ、リストア機能の操作制限＞
利用を代行するタスクに管理者属性が関連づけられると、利用者を代行するタスクは、
- FDP_ACC.1[1]、FDP_ACF.1[1]によりボックスファイル
- FDP_ACC.1[2]、FDP_ACF.1[2]により機密文書プリントファイル
- FDP_ACC.1[3]、FDP_ACF.1[3]により暗号鍵ワードオブジェクト、HDD ロックパスワードオブジェクト

を対象として、バックアップ操作が許可される。また
- FDP_ACC.1[3]、FDP_ACF.1[3]により暗号鍵ワードオブジェクト、HDD ロックパスワードオブジェクト、プリンタアドレスグループオブジェクト

を対象として、リストア操作を許可される。更に
- FMT_MOF.1[1]によりセキュリティ強化設定データ
- FMT_MTD.1[1]により SNMP パスワード、認証失敗回数、機密文書パスワード
- FMT_MTD.1[2]によりボックスパスワード

を対象データとして管理者だけにリストア操作（すなわち改変操作）が許可される。
FMT_MTD.1[4]により SNMP パスワード、ボックスパスワード、機密文書パスワードのバックアップ操作（すなわち問い合わせ操作）が管理者だけに許可される。

＜セキュリティ強化機能の操作制限＞
セキュリティ強化機能の停止設定は、FMT_MOF.1[1]により、管理者及びサービスエンジニアだけに許可される。セットアップ機能の動作設定（起動）は、FMT_MOF.1[3]により、サービスエンジニアだけに許可される。

＜HDD ロックパスワード、暗号鍵ワードの管理＞
利用者を代行するタスクに管理者属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、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、暗号鍵ワードオブジェクトに対する設定操作が許可される。FIA_SOS.1[3]により HDD ロックパスワード及び暗号鍵ワードの品質が検証される。なお HDD ロックパスワードや暗号鍵ワードが変更される際は、FIA_UAU.6 により、それぞれ既登録済み HDD ロックパスワード、暗号鍵ワードと照合することによって管理者であることを再認証し、再認証された場合に変更が許可される。
また利用者を代行するタスクに CE 属性が関連づけられると、FDP_ACC.1[3]、FDP_ACF.1[3]により、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、暗号鍵ワードオブジェクトに対する設定操作が許可される。

＜MIB オブジェクトに対するアクセスに必要な要件＞
プリンタアドレスグループオブジェクトは、MIB オブジェクトとしても存在するため、SNMP によるアクセスにも制限が必要である。
FIA_UID.2[2]、FIA_UAU.2[2]により、MIB オブジェクトにアクセスする利用者が管理者であることを識別認証する。
FIA_AFL.1[3]により、不成功認証が 1～3 回に達すると、MIB オブジェクトにアクセスするための認証機能をロックする。このロック状態は、TOE の起動、または管理者によるロック解除操作によって解除される。
SNMP パスワード利用した管理者認証における不成功認証の試行回数である不正アクセス検出値の閾値の設定は、FMT_MTD.1[1]により、管理者だけに制限される。
FMT_MTD.1[1]により SNMP パスワードの変更は、管理者に制限される。FIA_SOS.1[2]により、SNMP パスワードの品質が検証される。
SNMP パスワードの初期化は、FMT_MTD.1[6]により、管理者、サービスエンジニアだけに制限される。
SNMP パスワード認証機能の方式は、FMT_MOF.1[2]により、管理者だけに制限される。

＜管理者をセキュアに維持するために必要な要件＞
⇒ set.admin 参照

＜サービスエンジニアをセキュアに維持するために必要な要件＞
⇒ set.service 参照

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニア、FMT_SMR.1[2]により管理者として維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

これら複数の機能要件が満たされることにより、本セキュリティ対策方針は満たされる。

- **O.OVERWRITE-ALL（完全上書き削除）**
  本セキュリティ対策方針は、HDD のすべてのデータ領域を抹消し、利用者が設定した NVRAM 上の秘匿情報を初期化するとしており、削除に関係する諸要件が必要である。

FNEW_RIP.1 により、これら対象とする情報が消去操作によって以前のどの情報の内容も利用できなくすることを保証する。
よって本セキュリティ対策方針は満たされる。

- **O.CRYPT-KEY（暗号鍵生成）**
  本セキュリティ対策方針は、暗号化基板が設置されている場合に、HDD に書き込むすべてのデータを暗号化するために必要な暗号鍵を生成するとしており、暗号鍵生成に関係する諸要件が必要である。
  FCS_CKM.1 により、コニカミノルタ暗号仕様標準に従ったコニカミノルタ HDD 暗号鍵生成メカニズム（SHA-1）を利用し、128bit の暗号鍵を生成する。なおコニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）とは、一般標準で認められたアルゴリズムではないが、FIPS 180-1 で指定される SHA-1 を使ったアルゴリズムであるため、128bit のエントロピーを損ねることのない、強度十分なアルゴリズムであり、セキュリティ対策方針が求める強度レベルを損ねることはない。（本アルゴリズムに関する説明は、6 章 TOE 要約仕様参照）
  この機能要件によって本セキュリティ対策方針は満たされる。

- **O.CHECK-HDD（HDD の正当性確認）**
  本セキュリティ対策方針は、不正な HDD が紛れ込んでいないことを確認するため、HDD の正当性を検証するとしており、TOE からの外部エンティティの検証に関係する諸要件が必要である。
  FIA_NEW.1 により、TOE から HDD へのアクションの前に HDD を識別し、識別に失敗した場合は、予定されていたアクションを停止する。
  この機能要件によって本セキュリティ対策方針は満たされる。

- **OE.CRYPT（HDD の暗号化）**
  本セキュリティ対策方針は、TOE のセキュリティ維持に必要な IT 環境のエンティティである暗号化基板により、HDD 内に保管されるデータを暗号化するとしており、暗号に関係する諸要件が必要である。
  FCS_COP.1[E]により、暗号化基板は FIPS PUB 197 に準拠する AES を使って 128bit の暗号鍵より HDD に書き込まれるすべてのデータの暗号化、復号処理を行う。
  この機能要件によって本セキュリティ対策方針は満たされる。

- **OE.LOCK-HDD（HDD のアクセス制御）**
  本セキュリティ対策方針は、TOE のセキュリティ維持に必要な IT 環境のエンティティである HDD により、設置されたプリンタ以外からの不正なアクセスを拒否するとしており、TOE が設置された正当なプリンタであることを検証する諸要件が必要である。
  FIA_UAU.2[E]により HDD は、HDD にアクセスするエンティティを、HDD が設置されたプリンタであることを認証する。
  FIA_AFL.1[E]により、不成功認証が 5 回に達すると、HDD へのデータ読み込み、書き込み関する一切のアクセスを拒否する。
  これら複数の機能要件が組み合わさることにより、本セキュリティ対策方針は満たされる。

- **OE.FEED-BACK（パスワードのフィードバック）**
  本セキュリティ対策方針は、TOE のセキュリティ維持に必要な IT 環境のエンティティであるアプリケーション（クライアント PC にてプリンタにアクセスするために利用される）は、入力されるボックスパスワード、管理者パスワードに対して保護された適切なフィードバックを提供するとしている。
  FIA_UAU.7[E]によりアプリケーションは、入力された文字データ一文字毎に“＊”を表示する。

この機能要件によって本セキュリティ対策方針は満たされる。

以下には、①管理者をセキュアに維持するために必要な要件のセット（set.admin）、②サービスエンジニアをセキュアに維持するために必要な要件のセット（set.service）のセットをまとめる。

- ***set.admin*（管理者をセキュアに維持するために必要な要件のセット）**

  ＜管理者の識別認証＞

  FIA_UID.2[2]、FIA_UAU.2[2]により、アクセスする利用者が管理者であることを識別認証する。

  認証には、FIA_UAU.7 により、保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。

  FIA_AFL.1[6]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[2]により、不成功認証が 1～3 回に達すると、管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除される。

  管理者認証における不成功認証の試行回数である不正アクセス検出値の閾値の設定は、FMT_MTD.1[1]により、管理者だけに許可される。

  ＜管理者の認証情報の管理など＞

  管理者パスワードは、FIA_SOS.1[1]により品質が検証される。また FIA_SOS.[5]によりネットワークを経由した管理者認証において利用されるセッション情報の品質検証、FIA_SOS.2 により生成されて利用されるセッション情報の品質が確保される。管理者パスワードの変更は、FMT_MTD.1[3]により、管理者及びサービスエンジニアに制限される。管理者が管理者パスワードを変更する場合は、FIA_UAU.6 により再認証される。この再認証において、FIA_AFL.1[2]により、不成功認証が 1～3 回に達すると、管理者の認証状態を解除し、管理者パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除される。

  また管理者パスワードの初期化は FMT_MTD.1[6]により管理者、サービスエンジニアに制限される

  ＜各管理のための役割、管理機能＞

  これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアと FMT_SMR.1[2]により管理者にて維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

- ***set.service*（サービスエンジニアをセキュアに維持するために必要な要件のセット）**

  ＜サービスエンジニアの識別認証＞

  FIA_UID.2[1]、FIA_UAU.2[1]により、アクセスする利用者がサービスエンジニアであることを識別認証する。

  認証には、FIA_UAU.7 により、保護されたフィードバックに入力毎 1 文字ごとに“＊”を返し、認証をサポートする。

  FIA_AFL.1[6]により、失敗の度、5 秒間パネルからのすべての入力受付を拒否し、FIA_AFL.1[1]により、不成功認証が 1～3 回に達すると、CE パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除される。

  サービスエンジニア認証における不成功認証の試行回数である不正アクセス検出値の閾値の設定は、FMT_MTD.1[1]により、管理者だけに許可される。

  ＜サービスエンジニアの認証情報の管理など＞

  CE パスワードは、FIA_SOS.1[1]により、品質が検証される。CE パスワードの変更は、FMT_MTD.1[5]により、サービスエンジニアに制限される。また FIA_UAU.6 により再認証され

る。この再認証において、FIA_AFL.1[1]により、不成功認証が 1～3 回に達すると、サービスエンジニアの認証状態を解除して、CE パスワードを利用するすべての認証機能をロックする。このロック状態は、電源 OFF/ON などによる TOE の起動によって解除される。

＜各管理のための役割、管理機能＞
これら管理を行う役割は、FMT_SMR.1[1]によりサービスエンジニアとして維持される。またこれら管理機能は、FMT_SMF.1 により特定される。

なお FPT_RVM.1、FPT_SEP.1 は、直接的にはセキュリティ対策方針と関連付けられないセキュリティ機能要件であるので、上記の十分性の説明に含まれていないが、後述される相互サポートの中で上記の十分性の説明に含まれるセキュリティ機能要件をサポートすることが示されている。この 2 つのセキュリティ機能要件は、2 つのセキュリティ機能要件がそれぞれサポートしているセキュリティ機能要件が対応するセキュリティ対策方針と関連することになるため、結果的にセキュリティ対策方針との対応関係は明らかである。

8.2.1.3. 明示された IT セキュリティ機能要件の必要性

本 ST では、拡張要件として FNEW_RIP.1 と FIA_NEW.1 を挙げている。これら要件を提示する必要性、及びこれら要件を保証する上で適用している保証要件の妥当性について以下に記述する。

- **拡張要件：FNEW_RIP.1 の必要性**

  FNEW_RIP.1 は、残存情報保護という観点では FDP_RIP.1 が最も近い要件に相当するが、要件は利用者データだけでなく、TSF データの保護を規定する必要があるため、利用者データ保護のクラスに存在する当該機能要件では不適切であり、拡張要件が必要である。

  ＜要件識別構造の妥当性＞

  本要件は、該当するクラスが存在しないため、TSF データと利用者データの区分のない統合されたデータ保護クラスということで、FNEW という新しいクラスを設け、残存情報保護を示す FDP クラスの RIP ファミリと同一のファミリ名を付与し、識別を明確化した。

  予見される管理アクティビティはないとしているが、情報の再利用不可とするタイミングは要件において具体的に規定しているなど、特に可変的に扱われるパラメタなどは本要件において推察されない。また予見される監査アクティビティに利用者識別と共に実行の記録が残されていることが示されている。

- **拡張要件：FIA_NEW.1 の必要性**

  FIA_NEW.1 は、識別という観点では FIA_UID.1 や FIA_UID.2 が最も近い要件に相当するが、HDD の検証行為は、TOE が外部エンティティからアクセスされる行為を承認するのではなく、TOE 自らが外部エンティティに対して発動する行為への承認であり、当該機能要件では不適切であり、拡張要件が必要である。

  ＜要件識別構造の妥当性＞

  本要件は、識別要件の 1 つであるため、FIA クラスの中に追加されるファミリとして NEW というファミリを設定し、識別を明確化した。

  管理において予見されるアクティビティとして、FIA_UID 要件と同様の管理項目が想定されている。また監査において予見されるアクティビティにも、FIA_UID 要件と同様の監査項目が想定されている。

8.2.1.4. 明示された IT セキュリティ機能要件の保証妥当性

2 つの明示された機能要件（FNEW_RIP.1、FIA_NEW.1）は、CC パート 2 に規定される機能要件の概念を大幅に拡張したものではなく、新規性の高い内容ではない。つまり本機能要件を正確に評価するにあたり、特別に TSP モデルを提示するといった必要性や、潜在的な隠れチャネルの可能性等を想定するものではない。

従って、EAL3 の保証要件のセットによって十分にこれら機能要件が示す機能の妥当性を保証することが可能であり、特別な保証要件や、EAL4 以上から求められる保証要件を必要としない。

8.2.1.5. IT セキュリティ機能要件の依存性

IT セキュリティ機能要件コンポーネントの依存関係を下表に示す。CC パート 2 で規定される依存性を満たさない場合、「本 ST における依存関係」の欄にその理由を記述する。

表 11　IT セキュリティ機能要件コンポーネントの依存関係

N/A：Not Applicable

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1、 FCS_CKM.4、 FMT_MSA.2	FCS_COP.1[E] ＜①FCS_CKM.4、②FMT_MSA.2 を適用しない理由＞ ① 暗号鍵は、保管されるデータのために定常的に保管される。また保管媒体への任意のアクセスは困難であり、暗号鍵破棄の必要性はない。 ② 本 TOE には、暗号鍵に対して管理されるべきセキュリティ属性をもたないため、セキュアなセキュリティ属性を規定する必要はない。
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[1] ＜FMT_MSA.3 を適用しない理由＞ 生成されるオブジェクトにセキュアな管理が要求されるセキュリティ属性が存在しないため、必要性はない。（ボックス ID は、任意のユーザが登録可能である。）
FDP_ACF.1[2]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3
FDP_ACF.1[3]	FDP_ACC.1、 FMT_MSA.3	FDP_ACC.1[3] ＜FMT_MSA.3 を適用しない理由＞ オブジェクト属性が存在しないため、本要件を適用する必要性はない。
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[1] 、 FIA_UAU.2[2] 、 FIA_UAU.2[3] 、 FIA_UAU.2[4]
FIA_ATD.1	なし	N/A

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FIA_SOS.1[1]	なし	N/A
FIA_SOS.1[2]	なし	N/A
FIA_SOS.1[3]	なし	N/A
FIA_SOS.1[4]	なし	N/A
FIA_SOS.1[5]	なし	N/A
FIA_SOS.2	なし	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.6	なし	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1] 、 FIA_UAU.2[2] 、 FIA_UAU.2[3] 、 FIA_UAU.2[4]
FIA_UID.2[1]	なし	N/A
FIA_UID.2[2]	なし	N/A
FIA_UID.2[3]	なし	N/A
FIA_UID.2[4]	なし	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	両者とも適用しない ＜FMT_MSA.1 を適用しない理由＞ 一意に識別される内部制御 ID であり、一度割り当てられた後に変更、削除といった管理を必要としないため。 ＜FMT_SMR.1＞ FMT_MSA.3.2 の割付は該当なしである。FMT_SMR.1 は、左記に関係して設定されている依存性であり、したがって適用の必要性がない。
FMT_MTD.1[1]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1、 FMT_SMR.1[2]
FMT_MTD.1[5]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[6]	FMT_SMF.1、 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_SMF.1	なし	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[4]
FPT_RVM.1	なし	N/A
FPT_SEP.1	なし	N/A
FNEW_RIP.1	なし	N/A
FIA_NEW.1	なし	N/A
FCS_COP.1[E]	FDP_ITC.1 or FCS_CKM.1、	FCS_CKM.1

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
	FCS_CKM.4、FMT_MSA.2	＜①FCS_CKM.4、②FMT_MSA.2 を適用しない理由＞ ① 暗号鍵は、保管されるデータのために定常的に保管される。また保管媒体への任意のアクセスは困難であり、暗号鍵破棄の必要性はない。 ② 本 TOE には、暗号鍵に対して管理されるべきセキュリティ属性をもたないため、セキュアなセキュリティ属性を規定する必要はない。
FIA_AFL.1[E]	FIA_UAU.1	FIA_UAU.2[E]
FIA_UAU.2[E]	FIA_UID.1	適用しない ＜FIA_UID.1 を適用しない理由＞ プリンタ内に設置される HDD へのアクセスを規定するものである。HDD へのアクセスは一般的な IDE インターフェースを介してなされるものであるため、複数のアクセスルートはない。 つまり複数の利用者がアクセスする場合に必要となる利用者に応じた認証情報は本処理には不要であり、アクセスするエンティティの識別の必要性はない。
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[2]、FIA_UAU.2[4]

8.2.1.6. IT セキュリティ機能要件の相互サポート関係

機能要件の依存性には明示されない他のセキュリティ機能要件を有効に動作させるための IT セキュリティ機能要件を下表に示す。

表 12　IT セキュリティ機能要件の相互サポート関係

N/A：Not Applicable

IT セキュリティ機能要件	他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント			
	①迂回防止	②干渉、破壊防止	③非活性化防止	④無効化検出
FCS_CKM.1	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACF.1[1]	FIA_UAU.2[2] FIA_UAU.2[4]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[2]	FIA_UAU.2[2] FIA_UAU.2[3]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[3]	FIA_UAU.2[2] FIA_UAU.2[1]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FIA_AFL.1[1]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[2]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[3]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[4]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[5]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_ATD.1	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A

IT セキュリティ機能要件	他のセキュリティ機能要件を有効に動作させる機能要件コンポーネント			
	①迂回防止	②干渉、破壊防止	③非活性化防止	④無効化検出
FIA_SOS.1[5]	N/A	N/A	N/A	N/A
FIA_SOS.2	N/A	N/A	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FMT_MTD.1[5]	FMT_MOF.1[1]	N/A
FIA_UAU.2[2]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[3] FMT_MTD.1[4] FMT_MTD.1[6]	FMT_MOF.1[1]	N/A
FIA_UAU.2[3]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[4]	FMT_MOF.1[1]	N/A
FIA_UAU.2[4]	FPT_RVM.1	FMT_MTD.1[2] FMT_MTD.1[4]	FMT_MOF.1[1]	N/A
FIA_UAU.6	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UAU.7	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_USB.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[1]	N/A	N/A	N/A	N/A
FMT_MOF.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[3]	N/A	N/A	N/A	N/A
FMT_MSA.3	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[6]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMF.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FPT_RVM.1	N/A	N/A	FMT_MOF.1[1]	N/A
FPT_SEP.1	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_NEW.1	FPT_RVM.1	N/A	FMT_MOF.1[1]	N/A
FNEW_RIP.1	N/A	N/A	N/A	N/A
FCS_COP.1[E]	N/A	N/A	N/A	N/A
FIA_AFL.1[E]	N/A	N/A	N/A	N/A
FIA_UAU.2[E]	N/A	N/A	N/A	N/A
FIA_UAU.7[E]	N/A	N/A	N/A	N/A

① 迂回防止

＜管理者に関係する機能要件のバイパス防止＞

ボックスアクセス制御を規定する FDP_ACF.1[1]**、機密文書プリントファイルアクセス制御を規定する** FDP_ACF.1[2]**、管理者モードアクセス制御を規定する** FDP_ACF.1[3]**は、管理者の識別認証を規定する** FIA_UAU.2[2]**によってバイパス防止がサポートされる。**

さらに FIA_UAU.2[2]**は** FPT_RVM.1 **によって必ず呼び出されるため、バイパス防止がサポートされる。**

＜サービスエンジニアに関係する機能要件のバイパス防止＞

設定管理アクセス制御を規定する FDP_ACF.1[3]**は、サービスエンジニアの識別認証を規定する** FIA_UAU.2[1]**によってバイパス防止がサポートされる。**

さらに FIA_UAU.2[1]は FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜ボックスに関係する機能要件のバイパス防止＞
ボックスアクセス制御を規定する FDP_ACF.1[1]は、ボックスの利用を許可されたユーザであることを認証する FIA_UAU.2[4]によってバイパス防止がサポートされる。
さらにボックスの利用を許可されたユーザであることの認証を規定する FIA_UAU.2[4]は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜機密文書プリントに関係する機能要件のバイパス防止＞
機密文書プリントファイルアクセス制御を規定する FDP_ACF.1[2]は、機密文書プリントファイルの利用を許可されたユーザであることを認証する FIA_UAU.2[3]によってバイパス防止がサポートされる。
さらに機密文書プリントファイルの利用を許可されたユーザであることの認証を規定する FIA_UAU.2[3]は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

＜HDD の正当性検証のバイパス防止＞
HDD の正当性を検証する FIA_NEW.1 は、FPT_RVM.1 によって必ず呼び出されるため、バイパス防止がサポートされる。

② 干渉・破壊防止
＜ボックスアクセス制御の維持＞
FPT_SEP.1 により、ボックスアクセス制御で想定されている認証された管理者、認証されたボックスの利用を許可されたユーザの 2 つのタイプのサブジェクトだけがボックス、ボックスファイルの操作が可能であり、FDP_ACF.1[1]は他の不正なサブジェクトによる干渉・破壊防止がサポートされる。

＜機密文書プリントファイルアクセス制御の維持＞
FPT_SEP.1 により機密文書プリントファイルアクセス制御で想定されている認証された管理者、認証された機密文書プリントファイルの利用を許可されたユーザの 2 つのタイプのサブジェクトだけが機密文書プリントファイルの操作が可能であり、FDP_ACF.1[2]は他の不正なサブジェクトによる干渉・破壊防止がサポートされる。

＜設定管理アクセス制御の維持＞
FPT_SEP.1 により設定管理アクセス制御で想定されている認証された管理者、認証されたサービスエンジニアを代行するサブジェクトだけが、設定管理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、FDP_ACF.1[3]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。

＜CE パスワードの管理＞
CE パスワードの改変操作は FMT_MTD.1[5]によりサービスエンジニアだけに許可している。これより FIA_UAU.2[1]の不正な干渉・破壊防止がサポートされる。

＜管理者パスワードの管理＞
管理者パスワードの改変操作は FMT_MTD.1[3]により管理者及びサービスエンジニアだけに許可している。管理者パスワードの初期化は、FMT_MTD.1[6]により管理者、サービスエンジニ

アだけに許可している。これより FIA_UAU.2[2]の不正な干渉・破壊防止がサポートされる。

＜SNMP パスワードの管理＞
SNMP パスワードの改変操作は FMT_MTD.1[1]により管理者、問い合わせ操作は FMT_MTD.1[4]により管理者、初期化操作は FMT_MTD.1[6]により管理者、サービスエンジニアだけに許可している。これより FIA_UAU.2[2]の不正な干渉・破壊防止がサポートされる。

＜機密文書パスワードの管理＞
機密文書パスワードの問い合わせ操作は FMT_MTD.1[4]により管理者だけに許可、改変は FMT_MTD.1[1]により管理者だけに許可している。これより FIA_UAU.2[3]の不正な干渉・破壊防止がサポートされる。

＜ボックスパスワードの管理＞
ボックスパスワードの改変操作は FMT_MTD.1[2]によりボックスの利用を許可されたユーザ及び管理者、問い合わせ操作は FMT_MTD.1[4]により管理者だけに許可している。これより FIA_UAU.2[4]の不正な干渉・破壊防止がサポートされる。

＜認証失敗回数閾値の管理＞
サービスエンジニア認証、管理者認証、機密文書プリント認証、ボックス認証、MIB オブジェクトアクセスにおける認証といったすべての認証行為において設定される認証回数失敗閾値の改変操作は、FMT_MTD.1[1]により管理者だけに許可している。これより FIA_AFL.1[1]、FIA_AFL.1[2]、FIA_AFL.1[3]、FIA_AFL.1[4]、FIA_AFL.1[5]の不正な干渉・破壊防止がサポートされる。

③ 非活性化防止
＜セキュリティ強化機能の維持＞
FMT_MOF.1[1]により、セキュリティ強化機能の動作設定が管理者及びサービスエンジニアだけに許可されている。セキュリティ強化機能は、管理者の明示的な操作によって実行される全領域上書き削除機能、セッション情報の品質以外の TOE のセキュリティ構造すべてに影響するものであり、FNEW_RIP.1、FIA_SOS.1[5]、FIA_SOS.2、FMT_MOF.1[1]を除く 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。

④ 無効化検出
特に無効化検出をサポートする要件は存在しない。[5]

8.2.2. 最小機能強度根拠

本 TOE の搭載されるプリンタは、外部とのネットワーク接続において適切な管理が実施されているオフィス内部 LAN に接続される。よってインターネットを介して不特定多数の者に直接攻撃されるような可能性はなく、3.3 節にて明確化されている TOE の利用者であるユーザ及び TOE の利用者ではないオフィス内に入ることが可能な人物をエージェントとした脅威に対抗する強度レベルを有すれば良い。従って本 TOE は、攻撃者のレベルとして低レベルを想定したセキュリティ対策方針を規定しており、最小機能強度として SOF-基本の選択は妥当である。

[5] 相互サポート分析の中で示されないが、各認証機能の無効化を狙った攻撃に対しては、それぞれ対応する FIA_AFL.1 要件がサポートしており、本 TOE のセキュリティ対策方針を維持するにあたって十分である。（なお、依存性分析にて本内容は明示されている。）

8.2.3. IT セキュリティ保証要件根拠

本 TOE は、物理的・人的・接続的に十分なセキュリティを確保した環境に設置され利用されるが、本 TOE を利用する環境において十分な実効性を保証する必要がある。一般的な商用事務製品として機能仕様、上位レベル設計書に基づくテスト、機能強度分析、脆弱性の探索が実施されている必要があり、また開発環境の制御、TOE の構成管理、セキュアな配付手続きが取られていることが望まれる。従って十分な保証レベルが提供される EAL3 の選択は妥当である。

なお、保証要件依存性分析は、パッケージである EAL が選択されているため、妥当であるとして詳細は論じない。

8.2.4. IT セキュリティ機能要件のセット一貫性根拠

以下に競合可能性のある IT セキュリティ要件が存在しない論拠を示す。

＜IT セキュリティ機能要件＞

- アクセス制御要件（FDP_ACC.1 など）の繰り返しにより、複数のアクセス制御方針を立てているが、①ボックス、②機密文書プリント、③プリンタアドレスなどに関するアクセス制御を規定している。つまりこれらは同一の制御対象を複数のポリシーでカバーし合うものではないため、競合するものではない。
- 保護資産の削除を規定した拡張要件として FNEW_RIP.1 を適用しているが、不正削除の可能性に関する脅威は、機密性重視のコンセプトより、本件では対象としておらず、したがって競合するデータ削除保護に関する要件は全く選択されていない。
- 依存性による要件間の関係、相互サポートによる相関関係、TOE セキュリティ対策方針に対するセキュリティ機能要件妥当性の各種分析より、競合可能性が示唆される構造は存在しない。

＜IT セキュリティ保証要件＞

- 保証パッケージである EAL を利用している。すなわちセキュリティ保証要件が競合する可能性は、本 ST とは関係なく、存在しないことが確認されている。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

8.3.1.1. 必要性

TOE のセキュリティ機能と TOE セキュリティ機能要件との適合性を下表に示す。TOE のセキュリティ機能が少なくとも 1 つ以上の TOE セキュリティ機能要件に対応していることを示している。

表 13　TOE セキュリティ機能要件に対する TOE セキュリティ機能の適合性

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPT	F.HDD	F.RESET
FCS_CKM.1							●		
FDP_ACC.1[1]	●			●					
FDP_ACC.1[2]	●				●				
FDP_ACC.1[3]	●	●	●						
FDP_ACF.1[1]	●			●					
FDP_ACF.1[2]	●				●				
FDP_ACF.1[3]	●	●	●						
FIA_AFL.1[1]			●						●
FIA_AFL.1[2]	●								●
FIA_AFL.1[3]	●	●							●
FIA_AFL.1[4]	●				●				●
FIA_AFL.1[5]	●			●					●
FIA_AFL.1[6]	●		●	●	●				
FIA_ATD.1				●	●				
FIA_SOS.1[1]	●		●						
FIA_SOS.1[2]	●	●							
FIA_SOS.1[3]	●								
FIA_SOS.1[4]	●			●	●				
FIA_SOS.1[5]	●			●					
FIA_SOS.2	●			●					
FIA_UAU.2[1]			●						
FIA_UAU.2[2]	●	●							
FIA_UAU.2[3]					●				
FIA_UAU.2[4]				●					
FIA_UAU.6	●		●						
FIA_UAU.7	●		●	●	●				
FIA_UID.2[1]			●						
FIA_UID.2[2]	●	●							
FIA_UID.2[3]					●				
FIA_UID.2[4]				●					
FIA_USB.1				●	●				
FMT_MOF.1[1]	●		●						
FMT_MOF.1[2]	●	●							

TOE セキュリティ機能 / TOE セキュリティ機能要件	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPT	F.HDD	F.RESET
FMT_MOF.1[3]			●						
FMT_MSA.3					●				
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●			●					
FMT_MTD.1[3]	●		●						
FMT_MTD.1[4]	●								
FMT_MTD.1[5]			●						
FMT_MTD.1[6]	●		●						
FMT_SMF.1	●	●	●	●					
FMT_SMR.1[1]			●						
FMT_SMR.1[2]	●	●							
FMT_SMR.1[3]				●					
FPT_RVM.1	●	●	●	●	●			●	
FPT_SEP.1	●	●	●	●	●				
FNEW_RIP.1						●			
FIA_NEW.1								●	

8.3.1.2. 十分性

各 TOE セキュリティ機能要件に対して適用される TOE セキュリティ機能について以下に説明する。

- **FCS_CKM.1**

  FCS_CKM.1 は、HDD の暗号化に伴い生成される暗号鍵の諸条件を規定している。
  F.CRYPT は、コニカミノルタ HDD 暗号鍵生成アルゴリズム（SHA-1）を利用して 128bit の暗号鍵を生成する。
  従って本機能要件は満たされる。

- **FDP_ACC.1[1]**

  FDP_ACC.1[1]は、オブジェクトであるボックス、ボックスファイル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。
  F.ADMIN は、利用者を代行するタスクが、ボックスファイルをバックアップするためのボックスアクセス制御を実施する。
  F.BOX は、利用者を代行するタスクが、ボックスファイルを印刷、他のボックスへの移動、他のボックスへのコピーするためのボックス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_ACC.1[2]**

  FDP_ACC.1[2]は、オブジェクトである機密文書プリントファイル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。
  F.ADMIN は、利用者を代行するタスクが、機密文書プリントファイルをバックアップするための

機密文書プリントファイルアクセス制御を実施する。
F.PRINT は、利用者を代行するタスクが、機密文書プリントファイルを印刷するための機密文書プリントファイル制御を実施する。
従って本機能要件は満たされる。

- **FDP_ACC.1[3]**

FDP_ACC.1[3]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、暗号鍵ワードオブジェクト、プリンタアドレスグループ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。
F.ADMIN 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、暗号鍵ワードオブジェクトを設定、バックアップ、リストアする設定管理アクセス制御を実施する。またプリンタアドレスグループオブジェクトに対しては、設定、リストアする設定管理アクセス制御を実施する。
F.ADMIN-SNMP は、利用者を代行するタスクが、プリンタアドレスグループオブジェクトを設定する設定管理アクセス制御を実施する。
F.SERVICE 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、暗号鍵ワードオブジェクトを設定する設定管理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[1]**

FDP_ACF.1[1]は、オブジェクトであるボックスファイル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。
F.ADMIN は、以下の規則が適用されるボックスアクセス制御を実施する。
  - 管理者に対してボックスファイルのバックアップ操作を許可する。

F.BOX は、以下の規則が適用されるボックスアクセス制御を実施する。
  - ボックスの利用が許可されたユーザに対して、選択したボックス内のボックスファイルの印刷、他のボックスへの移動、他のボックスへのコピー操作を許可する。

従って本機能要件は満たされる。

- **FDP_ACF.1[2]**

FDP_ACF.1[2]は、オブジェクトである機密文書プリントファイル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。
F.ADMIN は、以下の規則が適用される機密文書プリントファイルアクセス制御を実施する。
  - 管理者に対して機密文書プリントファイルのバックアップ操作を許可する。

F.PRINT は、以下の規則が適用される機密文書プリントファイルアクセス制御を実施する。
  - 機密文書プリントファイルの利用を許可されたユーザに対して、選択した機密文書プリントファイルの印刷操作を許可する。

従って本機能要件は満たされる。

- **FDP_ACF.1[3]**

FDP_ACF.1[3]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、暗号鍵ワードオブジェクト、プリンタアドレスグループ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。
F.ADMIN は、以下の規則が適用される設定管理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、暗号鍵ワードオブジェクトの設定、バックアップ、リストア操作を許可する。
  - 管理者に対してプリンタアドレスグループオブジェクトの設定、リストア操作を許可する。

F.ADMIN-SNMP は、以下の規則が適用される機密文書プリントファイルアクセス制御を実施する。

- 管理者に対してプリンタアドレスグループオブジェクトの設定操作を許可する。

F.SERVICE は、以下の規則が適用される設定管理アクセス制御を実施する。

- サービスエンジニアに対して HDD ロックパスワードオブジェクト、暗号鍵ワードオブジェクトの設定操作（初期化操作）を許可する。

従って本機能要件は満たされる。

- **FIA_AFL.1[1]**

FIA_AFL.1[1]は、サービスエンジニアの認証に対する不成功認証時アクションを規定している。
F.SERVICE は、サービスモードへのアクセス、CE パスワードの変更の際に行うサービスエンジニアの認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知するとサービスモード認証状態であればログオフし、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。
従って本機能要件は満たされる。

- **FIA_AFL.1[2]**

FIA_AFL.1[2]は、管理者の認証に対する不成功認証時アクションを規定している。
F.ADMIN は、管理者モードへのアクセス、管理者パスワードの変更の際に行う管理者の認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると、管理者モード認証状態であればログオフし、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。
従って本機能要件は満たされる。

- **FIA_AFL.1[3]**

FIA_AFL.1[3]は、SNMP を利用して MIB オブジェクトへアクセスする際の管理者認証に対する不成功認証時アクションを規定している。
F.ADMIN-SNMP は、MIB オブジェクトへのアクセスの際に行う SNMP パスワードを利用した認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると MIB オブジェクトへのアクセスを拒否して、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。また F.ADMIN は、管理者モード内にて提供するロック解除機能によりこのロック状態を解除する。
従って本機能要件は満たされる。

- **FIA_AFL.1[4]**

FIA_AFL.1[4]は、機密文書プリントファイルの利用を許可されたユーザであることの認証に対する不成功認証時アクションを規定している。
F.PRINT は、機密文書プリントファイルの利用を許可されたユーザであることの認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると当該機密文書プリントファイルへのアクセスを拒否して、認証機能をロックする。
F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。また F.ADMIN は、管理者モード内にて提供するロック解除機能によりこのロック状態を解除する。
従って本機能要件は満たされる。

- **FIA_AFL.1[5]**

  FIA_AFL.1[5]は、ボックスの利用を許可されたユーザであることの認証に対する不成功認証時アクションを規定している。
  F.BOX は、ボックスへのアクセス、ボックスのパスワード変更の際に行う認証において、管理者が設定する失敗回数閾値（1～3 回）の認証失敗を検知すると当該ボックスへのアクセスを拒否して、認証機能をロックする。
  F.RESET は、電源 OFF/ON などによる TOE の起動において、各認証機能における失敗回数をクリアするためロック状態を解除する。また F.ADMIN は、管理者モード内にて提供するロック解除機能によりこのロック状態を解除する。
  従って本機能要件は満たされる。

- **FIA_AFL.1[6]**

  FIA_AFL.1[6]は、パネルにおける各種の認証に対する不成功認証時アクションを規定している。
  F.SERVICE は、サービスモードへのアクセスの際に行うサービスエンジニアの認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
  F.ADMIN は、管理者モードへのアクセスの際に行う管理者の認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
  F.BOX は、パネルからのボックスへのアクセスの際に行う認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
  F.PRINT は、機密文書プリントファイルの利用を許可されたユーザであることの認証において、認証失敗を検知するとパネルからのすべての入力受付を拒否する。
  これら一連の動作解除は、5 秒後に自動的に解除する。
  従って本機能要件は満たされる。

- **FIA_ATD.1**

  FIA_ATD.1 は、利用者に関係付けられるセキュリティ属性を規定している。
  F.BOX は、利用者を代行するタスクに対してボックス ID を関係付ける。
  F.PRINT は、利用者を代行するタスクに対して機密文書内部制御 ID を関係付ける。
  従って本機能要件は満たされる。

- **FIA_SOS.1[1]**

  FIA_SOS.1[1]は、管理者パスワード、CE パスワードの品質を規定している。
  F.ADMIN は､管理者パスワードの品質として 8 桁の合計 92 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されない、且つ現下で設定されている値と一致しないことを検証する。
  F.SERVICE は、CE パスワード、管理者パスワードの品質として 8 桁の合計 92 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されない、且つ現下で設定されている値と一致しないことを検証する。
  従って本機能要件は満たされる。

- **FIA_SOS.1[2]**

  FIA_SOS.1[2]は、SNMP パスワードの品質を規定している。
  F.ADMIN は、SNMP パスワード（Privacy パスワード、Authentication パスワード）の品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）であることを検証する。
  同様にして F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication パスワード）の品質として 8 桁以上の合計 95 文種の ASCII コード（0x20 ～ 0x7E）であることを検

証する。
従って本機能要件は満たされる。

- **FIA_SOS.1[3]**

FIA_SOS.1[3]は、HDD ロックパスワード、暗号鍵ワードの品質を規定している。
F.ADMIN は、HDD ロックパスワード、暗号鍵ワードの品質として 20 桁の合計 83 文種の ASCII コード（0x21 ～ 0x7E、ただし 0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5D を除く）で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

FIA_SOS.1[4]

FIA_SOS.1[4]は、機密文書パスワード、ボックスパスワードの品質を規定している。
F.ADMIN は、ボックスパスワードの品質として 8 桁の合計 93 文種の ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されないことを検証する。
F.BOX は、ボックスパスワードの品質として 8 桁の合計 93 文種の ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されないことを検証する。
F.PRINT は、機密文書パスワードの品質として 8 桁の合計 93 文種の ASCII コード（0x20 ～ 0x7E、ただし 0x22 と 0x2B を除く）で、同一キャラクタから構成されないことを検証する。
従って本機能要件は満たされる。

- **FIA_SOS.1[5]**

FIA_SOS.1[5]は、セッション情報の品質を規定している。
F.ADMIN は、セッション情報の品質として、10^{10} 以上の空間品質であることを検証する。
F.BOX は、セッション情報の品質として、10^{10} 以上の空間品質であることを検証する。従って本機能要件は満たされる。

- **FIA_SOS.2**

FIA_SOS.2 は、セッション情報の生成とその品質を規定している。
F.ADMIN は、管理者認証のセッション情報に 10^{10} 以上の空間品質である秘密を生成する。
F.BOX は、ボックス認証のセッション情報に 10^{10} 以上の空間品質である秘密を生成する。従って本機能要件は満たされる。

- **FIA_UAU.2[1]**

FIA_UAU.2[1]は、サービスエンジニアの認証を規定している。
F.SERVICE は、CE パスワードを使ってサービスモードへアクセスする利用者がサービスエンジニアであることを認証する。
従って本機能要件は満たされる。

- **FIA_UAU.2[2]**

FIA_UAU.2[2]は、管理者の認証を規定している。
F.ADMIN は、管理者パスワードを使って管理者モードへアクセスする利用者が管理者であることを認証する。
F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication パスワード）を使って MIB オブジェクトにアクセスする利用者が管理者であることを認証する。
従って本機能要件は満たされる。

- **FIA_UAU.2[3]**

  FIA_UAU.2[3]は、機密文書プリントファイルの利用を許可されたユーザの認証を規定している。
  F.PRINT は、各機密文書プリントファイルに対して設定される機密文書パスワードを使って機密文書プリントファイルの利用を許可されたユーザであることを認証する。
  従って本機能要件は満たされる。

- **FIA_UAU.2[4]**

  FIA_UAU.2[4]は、ボックスの利用を許可されたユーザの認証を規定している。
  F.BOX は、各ボックスに対して設定されるボックスパスワードを使ってボックスの利用を許可されたユーザであることを認証する。
  従って本機能要件は満たされる。

- **FIA_UAU.6**

  FIA_UAU.6 は、パスワードの変更といった重要な操作の際の再認証を規定している。
  F.ADMIN は、管理者パスワードの変更操作において管理者を再認証する。また HDD ロックパスワードの変更、暗号鍵ワードの変更操作に伴い、既登録済みの HDD ロックパスワード、暗号鍵ワードの照合によって各秘密情報を知り得る管理者であることを再認証する。
  F.SERVICE は、CE パスワードの変更操作においてサービスエンジニアを再認証する。
  従って本機能要件は満たされる。

- **FIA_UAU.7**

  FIA_UAU.7 は、認証中のフィードバックに“＊”を返すことを規定している。
  F.ADMIN は、管理者の認証、再認証においてパネルにて入力される管理者パスワードに対して 1 文字毎に“＊”返し、管理者パスワードのダイレクト表示を防止する。
  F.SERVICE は、サービスエンジニアの認証、再認証においてパネルにて入力される CE パスワードに対して 1 文字毎に“＊”返し、CE パスワードのダイレクト表示を防止する。
  F.PRINT は、機密文書プリントファイルの利用を許可されたユーザのであることの認証においてパネルにて入力される機密文書パスワードに対して 1 文字毎に“＊”返し、機密文書パスワードのダイレクト表示を防止する。
  F.BOX は、ボックスの利用を許可されたユーザであることの認証においてパネル入力されるボックスパスワードに対して 1 文字毎に“＊”返し、ボックスパスワードのダイレクト表示を防止する。
  従って本機能要件は満たされる。

- **FIA_UID.2[1]**

  FIA_UID.2[1]は、サービスエンジニアの識別を規定している。
  F.SERVICE は、サービスモードへアクセスする利用者がサービスエンジニアであると識別する。
  従って本機能要件は満たされる。

- **FIA_UID.2[2]**

  FIA_UID.2[2]は、管理者の認証を規定している。
  F.ADMIN は、管理者モードへアクセスする利用者が管理者であると識別する。
  F.ADMIN-SNMP は、MIB オブジェクトにアクセスする利用者が管理者であると識別する。
  従って本機能要件は満たされる。

- **FIA_UID.2[3]**

  FIA_UID.2[3]は、機密文書プリントファイルの利用を許可されたユーザの識別を規定している。
  F.PRINT は、操作対象として機密文書プリントファイルを選択することにより、機密文書プリントファイルの利用を許可されたユーザであると識別する。
  従って本機能要件は満たされる。

- **FIA_UID.2[4]**

  FIA_UID.2[4]は、ボックスの利用を許可されたユーザの識別を規定している。
  F.BOX は、操作対象としてボックスを選択することにより、ボックスの利用を許可されたユーザであると識別する。
  従って本機能要件は満たされる。

- **FIA_USB.1**

  FIA_USB.1 は、利用者を代行するサブジェクトへのセキュリティ属性関連付けを規定している。
  F.PRINT は、利用者を代行するタスクに機密文書プリントファイルへのアクセスに対して認証された際に、当該機密文書プリントファイルの“機密文書内部制御 ID”を関連付ける。
  F.BOX は、利用者を代行するタスクにボックスのボックスファイルへのアクセスに対して認証された際に、当該ボックスの“ボックス ID”を関連付ける。
  従って本機能要件は満たされる。

- **FMT_MOF.1[1]**

  FMT_MOF.1[1]は、セキュリティ強化機能のふるまい管理を規定している。
  F.ADMIN は、管理者モードにおいてセキュリティ強化機能の設定機能を提供しており、当該機能の停止操作が管理されている。またバックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にセキュリティ強化機能を停止設定させることが可能であるが、F.ADMIN は管理者だけにバックアップ、リストア操作を許可している。HDD 論理フォーマット、全領域の上書き削除機能も実行に伴いセキュリティ強化設定を無効とするが、F.ADMIN により管理者だけに操作が許可される。
  F.SERVICE は、サービスモードにおいて実行に伴いセキュリティ強化機能を無効とする HDD 論理フォーマット機能、HDD 物理フォーマット機能、HDD 装着設定機能、イニシャライズ機能を提供しており、セキュリティ強化機能の停止操作が管理されている。
  従って本機能要件は満たされる。

- **FMT_MOF.1[2]**

  FMT_MOF.1[2]は、SNMP パスワード認証機能のふるまい管理を規定している。
  F.ADMIN は、管理者モードにおいて SNMP パスワード認証機能の設定機能の操作を許可している。
  F.ADMIN-SNMP は、SNMP パスワードによって認証された管理者に SNMP パスワード認証機能の設定機能の操作を許可している。
  従って本機能要件は満たされる。

- **FMT_MOF.1[3]**

  FMT_MOF.1[3]は、セットアップ機能のふるまい管理を規定している。
  F.SERVICE は、サービスモードにおいてセットアップ機能の動作設定（動作禁止）機能を提供しており、セットアップ機能の動作機能が管理されている。
  従って本機能要件は満たされる。

- **FMT_MSA.3**

  FMT_MSA.3 は、機密文書プリントファイルの登録時に設定される機密文書内部制御 ID を規定している。
  F.PRINT は、機密文書プリントファイルの登録時に、一意に識別される機密文書内部制御 ID を当該機密文書プリントファイルに付与する。
  従って本機能要件は満たされる。

- **FMT_MTD.1[1]**

  FMT_MTD.1[1]は、SNMP パスワード、認証失敗回数閾値、機密文書パスワードの管理を規定している。
  F.ADMIN は、管理者モードにて、SNMP パスワードの変更、認証失敗回数閾値の変更操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的に SNMP パスワード、認証失敗回数閾値、機密文書パスワードを改変させることが可能である。
  F.SNMP-ADMIN は、SNMP パスワードの変更を許可している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[2]**

  FMT_MTD.1[2]は、ボックスパスワードの管理を規定している。
  F.ADMIN は、管理者モードにてボックスに設定されるボックスパスワードの変更操作を許可している。また F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータを改変、リストア操作を行うことによって結果的にボックスパスワードを改変させることが可能である。
  F.BOX は、ボックスの利用を許可されたユーザとして認証されたユーザに対して、当該ボックスのボックスパスワードの変更操作を許可している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[3]**

  FMT_MTD.1[3]は、管理者パスワードの管理を規定している。
  F.ADMIN は、管理者モードにて管理者パスワードの変更操作を許可している。
  F.SERVICE は、サービスモードにて管理者パスワードの変更操作を許可している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[4]**

  FMT_MTD.1[4]は、SNMP パスワード、ボックスパスワード、機密文書パスワードの管理を規定している。
  F.ADMIN は、管理者にバックアップ、リストア操作を許可しており、バックアップ操作によって取得されるバックアップデータから、SNMP パスワード、ボックスパスワード、機密文書パスワードを閲覧することが可能である。
  従って本機能要件は満たされる。

- **FMT_MTD.1[5]**

  FMT_MTD.1[5]は、CE パスワードの管理を規定している。
  F.SERVICE は、サービスモードにて CE パスワードの変更操作を許可している。
  従って本機能要件は満たされる。

- **FMT_MTD.1[6]**

  FMT_MTD.1[6]は、管理者パスワード及び SNMP パスワードの管理を規定している。
  F.ADMIN は、管理者モードにて全領域上書削除機能の実行に伴って実行される管理者パスワード及び SNMP パスワードの初期化操作を許可する。
  F.SERVICE は、サービスモードにてイニシャライズ機能の実行に伴って実行される管理者パスワード、SNMP パスワードの初期化操作を許可する。
  従って本機能要件は満たされる。

- **FMT_SMF.1**

  FMT_SMF.1 は、セキュリティ管理機能を特定している。
  F.ADMIN は、以下のセキュリティ管理機能を提供する。
  - 認証失敗回数閾値の設定機能
  - バックアップ、リストア機能
    結果的に以下に示す TSF データの問い合わせ機能に相当する。
    ・SNMP パスワード
    ・ボックスパスワード
    ・機密文書パスワード
    また以下に示す TSF データの改変機能に相当する。
    ・SNMP パスワード
    ・ボックスパスワード
    ・機密文書パスワード
    ・セキュリティ強化機能の動作設定データ
    ・認証操作禁止機能の認証失敗回数閾値
  - セキュリティ強化機能の停止機能
    ・セキュリティ強化機能の動作設定機能
    ・HDD 論理フォーマット機能
  - 管理者パスワードの変更機能
  - ボックスパスワードの変更機能
  - SNMP パスワード（Privacy パスワード、Authentication パスワード）の変更機能
  - ロック解除機能
    以下の認証機能に対して提供する。
    ・MIB オブジェクトへのアクセスにおける認証機能
    ・ボックスへのアクセスにおける認証機能
    ・機密文書プリントへのアクセスにおける認証機能

  F.ADMIN-SNMP は、以下のセキュリティ管理機能を提供する。
  - SNMP パスワード（Privacy パスワード、Authentication パスワード）の変更機能
  - SNMP パスワード認証機能の動作設定機能

  F.SERVICE は、以下のセキュリティ管理機能を提供する。
  - CE パスワードの変更機能
  - 管理者パスワードの変更機能
  - セットアップ機能の動作設定機能
  - 管理者パスワードの初期化機能
    ・イニシャライズ機能
  - SNMP パスワード（Privacy パスワード、Authentication パスワード）の初期化機能
    ・イニシャライズ機能
  - セキュリティ強化機能の停止機能

・HDD 論理フォーマット機能
・HDD 物理フォーマット機能
・HDD 装着設定機能
・イニシャライズ機能

F.BOX は、以下のセキュリティ管理機能を提供する。

- ボックスパスワードの変更機能

F.ADMIN により、以下のセキュリティ管理機能を提供する。

- セキュリティ強化機能の停止機能
  ・全領域上書き削除機能
- 管理者パスワードの初期化機能
  ・全領域上書き削除機能
- SNMP パスワード（Privacy パスワード、Authentication パスワード）の初期化機能
  ・全領域上書き削除機能

従って本機能要件は満たされる。

- **FMT_SMR.1[1]**

FMT_SMR.1[1]は、役割：サービスエンジニアを規定している。
F.SERVICE は、CE パスワードにより認証された利用者をサービスエンジニアとして認識する。
従って本機能要件は満たされる。

- **FMT_SMR.1[2]**

FMT_SMR.1[2]は、役割：管理者を規定している。
F.ADMIN は、管理者パスワードにより認証された利用者を管理者として認識する。
F.ADMIN-SNMP は、SNMP パスワード（Privacy パスワード、Authentication パスワード）により認証された利用者を管理者として認識する。
従って本機能要件は満たされる。

- **FMT_SMR.1[3]**

FMT_SMR.1[3]は、役割：そのボックスの利用を許可されたユーザを規定している。
F.BOX は、ボックスパスワードにより認証された利用者をそのボックスの利用を許可されたユーザとして認識する。
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 実施機能が必ず呼び出されることをサポートすることを規定している。
F.ADMIN は、管理者だけが扱える諸機能の利用が許可される前に、動作することが必須である“管理者認証機能”を必ず起動する。
F.ADMIN-SNMP は、管理者だけが扱えるネットワーク設定機能などの利用が許可される前に、動作することが必須である“管理者認証機能”を必ず起動する。
F.SERVICE は、サービスエンジニアだけが扱える諸機能の利用が許可される前に、動作することが必須である“サービスエンジニア認証機能”を必ず起動する。
F.BOX は、ボックスの利用を許可されたユーザだけが扱える諸機能の利用が許可される前に、動作することが必須である“ボックスパスワードによる認証機能”を必ず起動する。
F.PRINT は、機密文書の利用を許可されたユーザだけが扱える諸機能の利用が許可される前に、動作することが必須である“機密文書パスワードによる認証機能”を必ず起動する。
F.HDD は、HDD ロック機能の動作時において HDD の書き込みが許可される前に、動作するこ

とが必須である“ HDD の正当性検証機能 ”を必ず起動する。
従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。
  F.ADMIN は、管理者だけが操作することを許可される諸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。
  F.ADMIN-SNMP は、SNMP パスワードより認証された管理者だけが操作することを許可される諸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。
  F.BOX は、ボックスパスワードによる認証により、ボックスの利用を許可されたユーザだけが操作することを許可される諸機能が提供されるボックス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。
  F.PRINT は、機密文書パスワードによる認証により、機密文書プリントファイルの利用を許可されたユーザだけが操作することを許可される諸機能が提供される機密文書プリントファイル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。
  F.SERVICE は、サービスエンジニアだけが操作することを許可される諸機能が提供されるサービスエンジニア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。
  従って本機能要件は満たされる。

- **FNEW_RIP.1**

  FNEW_RIP.1 は、明示的な消去操作において対象となるオブジェクト及び TSF データが復旧できないことを規定している。
  F.OVERWRITE-ALL は、指定された上書き削除方式に則り、HDD の全領域に対して上書き削除を行うことによって、ボックスファイル、機密文書プリントファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、ボックスパスワード、機密文書パスワード、残存 TSF データを削除する。
  また NVRAM の管理者パスワード、SNMP パスワードを初期化し、HDD ロック機能、暗号化機能の動作設定を OFF にする。
  従って本機能要件は満たされる。

- **FIA_NEW.1**

  FIA_NEW.1 は、TSF から利用者に対してアクションする前に利用者の識別を規定している。
  F.HDD は、HDD ロックパスワードを設定している場合に、HDD のステータスをチェックし HDD ロックパスワードが設定されていなければ、HDD への書き込み、読み込み処理を行なわない。
  従って本機能要件は満たされる。

8.3.2. TOE セキュリティ機能強度根拠

確率的・順列的メカニズムを有する TOE セキュリティ機能は、以下の通りである。

① F.ADMIN が提供する管理者認証メカニズム
② F.SERVICE が提供する CE 認証メカニズム
③ F.PRINT が提供する機密文書認証メカニズム
④ F.BOX が提供するボックス認証メカニズム
⑤ F.ADMIN-SNMP が提供する SNMP 認証メカニズム
⑥ F.ADMIN が提供する HDD ロックパスワード照合メカニズム
⑦ F.ADMIN が提供する暗号鍵ワード照合メカニズム

①、②は 8 桁 92 種のキャラクタ、③、④は 8 桁 93 種のキャラクタ、⑤8 桁以上 95 種のキャラクタ、⑥、⑦は 20 桁 83 種のキャラクタから構成されるパスワードを利用する。このうち①～⑤は、認証操作禁止機能の動作によって、最大でも連続 3 回の不成功認証により認証機能はロックする。

なお①、④については、ネットワークからのアクセスにおいてセッション情報を秘密に利用する。これら秘密は 10^{10} 以上の値を TOE が生成して利用する。また外部より与えられた 10^{10} 以上の値のセッション情報を利用する。

従って 6.2 節にて主張される通り、これらメカニズムの機能強度は SOF-基本を十分満たしており、5.1.2 項にてセキュリティ機能強度主張される TOE セキュリティ機能要件に対して主張される最小機能強度：SOF-基本と一貫している。

8.3.3. 相互サポートする TOE セキュリティ機能

TOE 要約仕様で識別される IT セキュリティ機能が組み合わさることにより満たされる TOE セキュリティ機能要件は、8.3.1 項に記述される各根拠記述にて述べられる通りである。

8.3.4. 保証手段根拠

評価保証レベル EAL3 において必要なドキュメントは 6.4 節において説明される保証手段に示されたドキュメント資料により網羅されている。これら保証手段として提示されているドキュメントに従った開発、テストの実施、脆弱性の分析、開発環境の管理、構成管理、ライフサイクル管理、配付手続きが実施され、適切なガイダンス文書が作成されることにより、TOE セキュリティ保証要件が満たされる。

8.4. PP 主張根拠

本 ST が参照する PP はない。