Xerox 4112/4127 Copier/Printer

セキュリティターゲット

Version 1.0.9

FUJI Xerox

― 更新履歴 ―

No.	更新日	バージョン	更新内容
1	2009 年 9 月 15 日	V 1.0.0	初版
2	2009 年 10 月 13 日	V 1.0.1	ROM バージョン更新、誤記修正
3	2009 年 11 月 27 日	V 1.0.2	ROM バージョン変更等
4	2009 年 11 月 30 日	V 1.0.3	指摘事項修正
5	2009 年 12 月 10 日	V 1.0.4	誤記修正
6	2009 年 12 月 15 日	V 1.0.5	誤記修正
7	2009 年 12 月 28 日	V 1.0.6	誤記修正
8	2010 年 01 月 12 日	V 1.0.7	誤記修正
9	2010 年 01 月 13 日	V 1.0.8	誤記修正
10	2010 年 01 月 27 日	V 1.0.9	指摘事項修正

－ 目次 －

－ 図表目次 －

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1. ST 参照

本節では ST の識別情報を記述する。

タイトル:	Xerox 4112/4127 Copier/Printer セキュリティターゲット
バージョン:	V 1.0.9
発行日:	2010 年 01 月 27 日
作成者:	富士ゼロックス株式会社

1.2. TOE 参照

本節では TOE の識別情報を記述する。

TOE は Xerox 4112 Copier/Printer、Xerox 4127 Copier/Printer として動作する。TOE は以下の TOE 名とバージョンで識別する。

TOE 名:	Xerox 4112/4127 Copier/Printer	
TOE のバージョン:	・Controller+PS ROM	Ver. 1.211.8
	・IOT ROM	Ver. 46.18.0
	・IIT ROM	Ver. 15.6.1
	・IIT Option ROM	Ver. 14.0.4
	・ADF ROM	Ver. 12.2.7
開発者:	富士ゼロックス株式会社	

1.3. TOE 概要

1.3.1. TOE 種別および主要セキュリティ機能

1.3.1.1. TOE の種別

本 TOE は IT 製品であり、コピー機能、プリンター機能、スキャナー機能を有するデジタル複合機（Multi Function Device 略称 MFD）である Xerox 4112/4127 Copier/Printer（以降、単に「MFD」と記す）である。

TOE は、MFD 全体の制御および、内部ハードディスク装置に蓄積された文書データ、利用済み文書データおよびセキュリティ監査ログデータ、また TOE とリモート間の内部ネットワーク上に存在する文書データ、TOE 設定データおよびセキュリティ監査ログデータを脅威から保護する製品である。

1.3.1.2. TOE の機能種別

表 1 に TOE が提供する製品の機能種別を記述する。

表 1　TOE が提供する機能と機能種別

機能種別	TOE が提供する機能
基本機能	・操作パネル機能 ・CWIS 機能 ・コピー機能 ・プリンター機能 ・スキャナー機能 ・ネットワークスキャン機能
セキュリティ機能	・ハードディスク蓄積データ上書き消去機能 ・ハードディスク蓄積データ暗号化機能 ・ユーザー認証機能 ・システム管理者セキュリティ管理機能 ・カストマーエンジニア操作制限機能 ・セキュリティ監査ログ機能 ・内部ネットワークデータ保護機能

- 本TOEはセキュリティ機能を利用することを前提としており、これを実現するためにオプションのデータセキュリティキットは必須である。
- プリンター機能、スキャナー機能を使用するためには、TOE 外の一般利用者クライアントおよびシステム管理者クライアントにプリンタードライバ、スキャナードライバ、ネットワークスキャナーユーティリティがインストールされていることが必要である。

1.3.1.3. TOE の使用法と主要セキュリティ機能

TOE の主な使用法を以下に示す。

- コピー機能と操作パネル機能により、操作パネルからの一般利用者の指示に従い、IIT で原稿を読み込み IOT への印刷を行う。またコピー蓄積機能として再出力用データの IOT への印刷と同時保存、および再出力用保存が可能である。
  同一原稿の複数部のコピーが指示された場合、IIT で読み込んだ文書データは、一旦 MFD の内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
- プリンター機能により、一般利用者クライアントから送信された印刷データをデコンポーズして印刷する。
- CWIS機能により、MFDに対してスキャナー機能によりスキャンして、親展ボックスに格納された文書データを一般利用者クライアントから取り出す。
  さらにシステム管理者は、Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う。
- スキャナー機能と操作パネル機能により、操作パネルからの一般利用者の指示に従い、IIT で原稿を読み込み、MFD の内部ハードディスク装置に作られた親展ボックスに蓄積する。
  蓄積された文書データは、一般的な Web ブラウザを使用して CWIS やネットワークスキャナーユーティリティの機能により取り出す

・ ネットワークスキャン機能により、操作パネルからの一般利用者の指示に従い IIT で原稿を読み込み後に MFD に設定されている情報に従って、FTP サーバ、SMB サーバ、Mail サーバへ文書データの送信を行う。

TOE は以下のセキュリティ機能を提供する。

・ハードディスク蓄積データ上書き消去機能
コピー、プリンターおよびスキャナー等の各機能の動作後、ハードディスク装置に蓄積された利用済みの文書データの上書き消去を行う機能である。
・ハードディスク蓄積データ暗号化機能
コピー、プリンターおよびスキャナー等の各機能の動作時や各種機能設定時にハードディスク装置に蓄積される文書データやセキュリティ監査ログデータの暗号化を行う機能である。
・ユーザー認証機能
許可された特定の利用者だけに TOE の機能を使用する権限を持たせるために、操作パネルまたは一般利用者クライアントのプリンタードライバ、ネットワークスキャナーユーティリティ、CWIS からユーザーID とユーザーパスワードを入力させて識別認証する機能である。
・システム管理者セキュリティ管理機能
操作パネルまたはシステム管理者クライアントから、識別および認証されたシステム管理者が、TOE のセキュリティ機能に関する設定の参照および変更をシステム管理者のみが行えるようにする機能である。
・カストマーエンジニア操作制限機能
カストマーエンジニアが TOE のセキュリティ機能に関する設定の参照および変更をできなくするシステム管理者の設定機能である。
・セキュリティ監査ログ機能
いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザー操作など）を、追跡記録するための機能である。
・内部ネットワークデータ保護機能
内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護する機能である。（一般的な暗号化通信プロトコル（SSL/TLS，IPSec，SNMPv3，S/MIME）に対応する）

1.3.2. TOE 利用環境

本 TOE は、IT 製品として一般的な業務オフィスに、ファイアウォールなどで外部ネットワークの脅威から保護された内部ネットワークおよび利用者クライアントと接続されて利用される事を想定している。

TOE の想定する利用環境を図 1 に記述する。

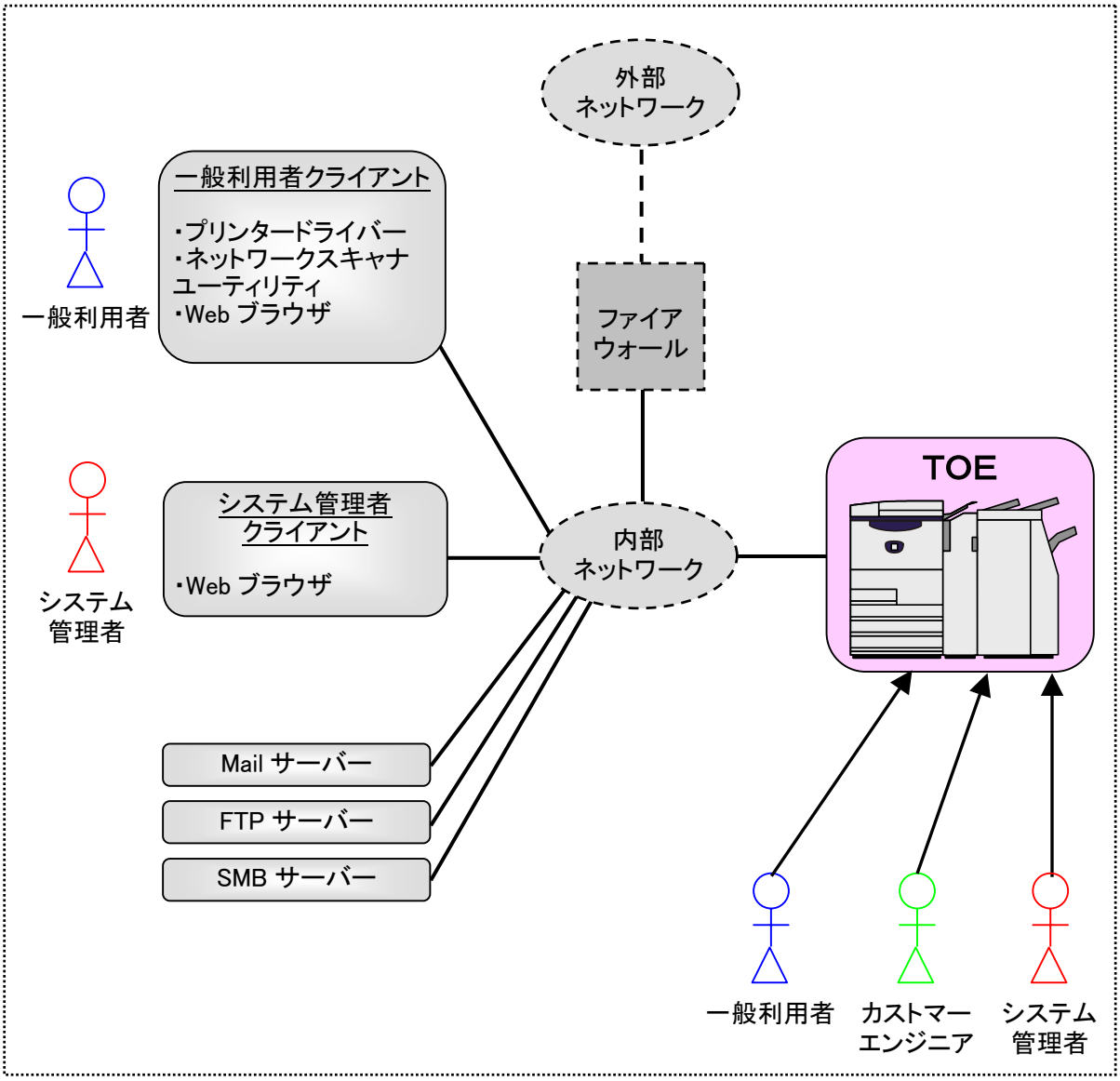

図 1 TOE の想定する利用環境

1.3.3. TOE 以外のハードウェア構成とソフトウェア構成

図-1 に示す利用環境の中で TOE は MFD であり、下記の TOE 以外のハードウェアおよびソフトウェアが存在する。

① 一般利用者クライアント:
ハードウェアは汎用の PC であり、プリンタードライバ、ネットワークスキャナーユーティリティがインストールされており、MFD に対して文書データのプリント要求、文書データの取り出し要求を行うことができる。
また、Web ブラウザを使用して MFD のスキャナー機能によりスキャンした文書データの取り出し要求を行う。
また一般利用者が MFD に登録した親展ボックスのボックス名称、パスワード、アクセス制限、および文書の自動削除指定の設定変更が出来る。

② システム管理者クライアント:
ハードウェアは汎用の PC であり、Web ブラウザを使用して TOE に対して TOE 設定データの参照や変更を行うことができる。

③ Mail サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFD はメールプロトコルを用いて、Mail サーバと文書データの送受信を行う。

④ FTP サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFD は FTP プロトコルを用いて、FTP サーバに文書データの送信を行う。

⑤ SMB サーバ:
ハードウェア/OS は汎用の PC またはサーバであり、MFD は SMB プロトコルを用いて、SMB サーバに文書データの送信を行う。

①、②の一般利用者クライアントとシステム管理者クライアントの OS は Windows 2000、 Windows XP、 Windows Vista とする。

1.4. TOE 記述

本章では、TOE の利用者役割、TOE の論理的範囲、および物理的範囲について記述する。

1.4.1. TOE 関連の利用者役割

本 ST で、TOE に対して想定する利用者役割を表 2 に記述する。

表 2 TOE が想定する利用者役割

関連者	内容説明
組織の管理者	TOE を使用して運用する組織の責任者または管理者。
一般利用者	TOE が提供するコピー機能、プリンター機能等の TOE 機能の利用者。
システム管理者 （機械管理者＋SA）	TOE のシステム管理者モードで機器管理を行うための、特別な権限を持つ利用者で、TOE の操作パネルおよび Web ブラウザを使用して、TOE 機器の動作設定の参照/更新、および TOE セキュリティ機能設定の参照/更新を行う。
カストマー エンジニア	カストマーエンジニアは、カストマーエンジニア専用のインターフェースを使用して、TOE の機器動作設定を行う。

1.4.2. TOE の論理的範囲

TOE の論理的範囲はプログラムの各機能である。
図 2 に TOE の論理的構成を記述する。

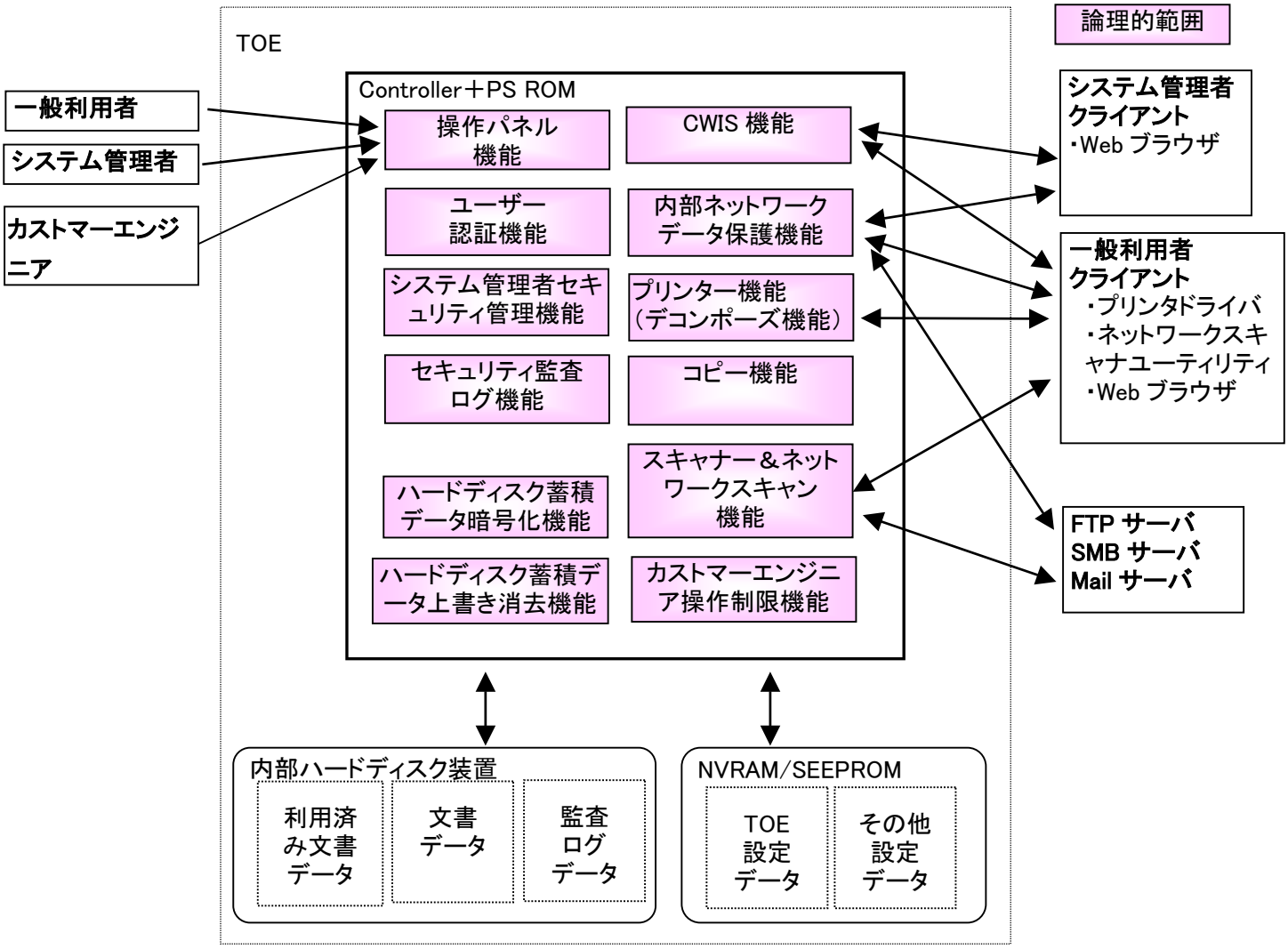

図 2 MFD 内の各ユニットと TOE の論理的範囲

1.4.2.1. TOE が提供する基本機能

TOE は一般利用者に対して、下記 表 3 のように操作パネル機能、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能および CWIS 機能を提供する。

表 3 TOE の基本機能

機能	概要
操作パネル機能	操作パネル機能は一般利用者、システム管理者、カストマーエンジニアが MFD の機能を利用するための操作に必要なユーザーインターフェイス機能である。
コピー機能	コピー機能は、一般利用者が MFD の操作パネルから指示をすることにより、IIT で原稿を読み取り IOT から印刷を行う機能である。またコピー蓄積機能として再出力用データの IOT への印刷と同時保存、および再出力用保存が可能である。 同一原稿の複数部のコピーが指示された場合、IIT で読み込んだ文書データは、一旦 MFD の内部ハードディスク装置に蓄積され、指定部数回、内部ハードディスク装置から読み出されて印刷される。
プリンター機能	プリンター機能は、一般利用者が一般利用者クライアントからプリント指示をして、プリンタードライバを介して作成された印刷データが MFD へ送信され、MFD は印刷データを解析し、ビットマップデータに変換（デコンポーズ）して、IOT から印刷を行う機能である。 プリンター機能には、直接 IOT から印刷を行う通常プリントと、ビットマップデータを一時的に内部ハードディスク装置に蓄積して、一般利用者が操作パネルから印刷指示をした時点で IOT から印刷を行う蓄積プリントがある。
スキャナー機能、 ネットワークスキャン 機能	スキャナー機能は、一般利用者が MFD の操作パネルから指示をすることにより、IIT で原稿を読み取り、文書データとして内部ハードディスク装置に蓄積する機能である。 蓄積された文書データは、一般利用者が一般利用者クライアントを使って CWIS 機能やネットワークスキャナーユーティリティにより取り出すことができる。 またネットワークスキャン機能は MFD に設定されている情報に従って、一般利用者が MFD の操作パネルから原稿を読み取り後に自動的に一般利用者クライアント、FTP サーバ、Mail サーバ、SMB サーバへ転送する機能である。
CWIS 機能	CWIS 機能は、一般利用者が一般利用者クライアントの Web ブラウザからの指示により、内部ハードディスク装置に蓄積されている、スキャナから読み取られた文書データの取り出しを行う。 またシステム管理者は、システム管理者クライアントの Web ブラウザからシステム管理者の IDとパスワードを入力して MFD に認証されると、システム管理者セキュリティ管理機能により TOE 設定データにアクセスしてデータを更新することが出来る。

1.4.2.2. TOE が提供するセキュリティ機能

本 TOE は利用者に対して、以下のセキュリティ機能を提供する。

（1）ハードディスク蓄積データ上書き消去機能

内部ハードディスク装置に蓄積される文書データは、利用が終了して削除される際に管理情報だけが削除され、蓄積された文書データ自体は削除されない。 このため内部ハードディスク装置上に利用済み文書データとして残存した状態になる。 この問題を解決するために、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能のジョブ完了後に、内部ハードディスク装置に蓄積された利用済み文書データに対して、上書き

消去を行う。

上記に加えて、システム管理者が設定した時刻に蓄積文書を削除して上書き消去する（時刻指定文書削除機能）機能も提供する。

（2）ハードディスク蓄積データ暗号化機能

内部ハードディスク装置には親展ボックス内の文書データやセキュリティ監査ログデータのように電源がオフされても残り続けるデータがある。この問題を解決するために、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能や各種機能設定時に内部ハードディスク装置に蓄積される文書データやセキュリティ監査ログデータの暗号化を行う。

（3）ユーザー認証機能

TOE は、許可された特定の利用者だけに MFD の機能を使用する権限を持たせるために、操作パネルまたは利用者クライアントのプリンタードライバ、ネットワークスキャナーユーティリティ、CWIS からユーザーID とユーザーパスワードを入力させて識別認証する機能を有する。

認証が成功した利用者のみが下記の機能を使用可能となる。

① 本体操作パネルで制御される機能

コピー機能、スキャン機能、ネットワークスキャン機能、親展ボックス操作機能、プリンター機能（プリンタードライバでのユーザーID とユーザーパスワードの設定が条件であり印刷時に操作パネルで認証する）

②利用者クライアントのネットワークスキャナーユーティリティで制御される機能

親展ボックスからの文書データ取出し機能

③CWIS で制御される機能

機械状態の表示、ジョブ状態・履歴の表示、親展ボックスからの文書データ取出し機能、ファイル指定によるプリント機能

セキュリティ機能としてのユーザー認証機能は、攻撃者が正規の利用者になりすまして内部ハードディスク装置内の文書データを不正に読み出すことを防ぐ機能であり、上記の認証により制御される機能中の

・本体操作パネルから認証する場合の蓄積プリント機能(プライベートプリント機能)および親展ボックス操作機能

・CWIS、ネットワークスキャナーユーティリティから認証する場合の親展ボックスからの文書データ取出し機能（親展ボックス操作機能）、CWIS からのファイル指定による蓄積プリント機能(プライベートプリント機能)がセキュリティ機能に該当する。

これらの機能の認証フローを図 3 に示す。

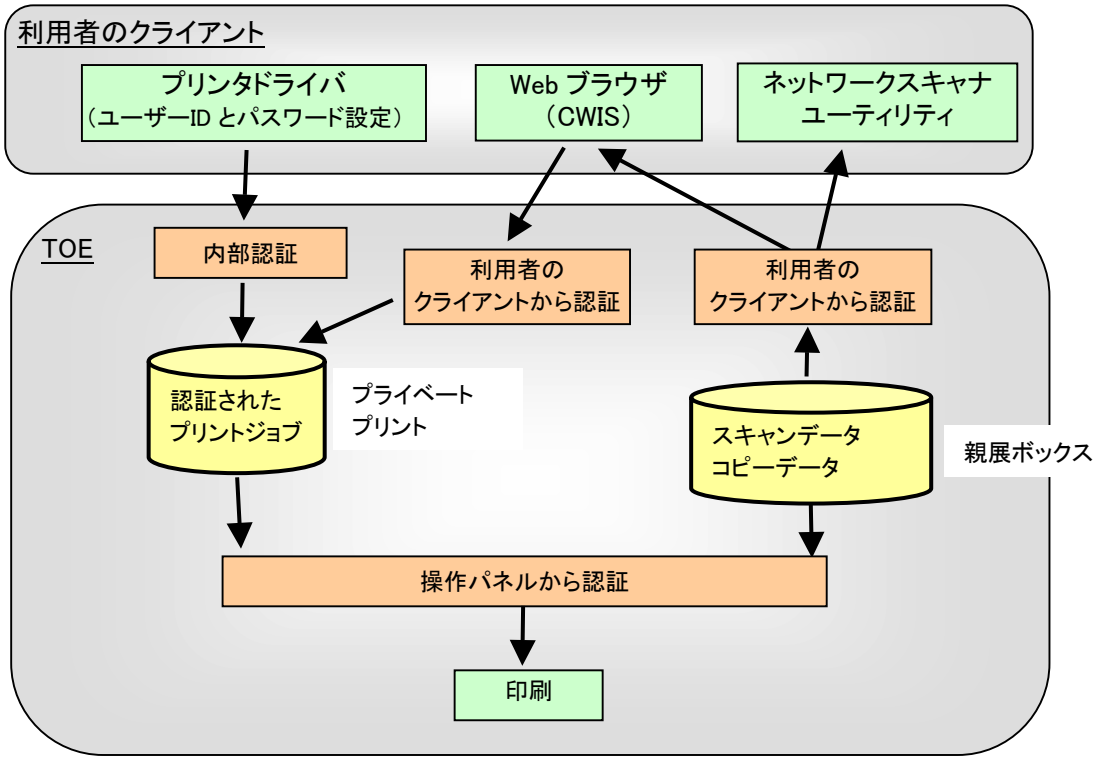

図 3 プライベートプリントと親展ボックスの認証フロー

- プライベートプリント機能（蓄積プリント機能）

MFD で「認証成功のジョブをプライベートプリントに保存」の設定を行うと、利用者が利用者クライアントのプリンタードライバからユーザーID とパスワードを設定した状態でプリント指示をする場合、MFD は内部に登録されたユーザーID とパスワードが一致するかをチェックし、一致した場合のみ印刷データをビットマップデータに変換（デコンポーズ）してプライベートプリントとしてユーザーID ごとに区分して内部ハードディスク装置に一時蓄積する。

また CWIS からユーザーID とパスワードを入力し、認証後に利用者クライアント内のファイル指定によりプリント指示をする場合も同様にユーザーID ごとのプライベートプリントとして内部ハードディスク装置に一時蓄積される。

利用者は一時蓄積されたプリントデータを確認するために、MFD の操作パネルからユーザーID とパスワードを入力し、認証されるとユーザーID に対応したプリント待ちのリストだけが表示される。利用者はこのリストから印刷指示、または削除の指示が可能となる。

- 親展ボックス操作機能

図 3 には図示されていない IIT から親展ボックスにコピーデータおよびスキャンデータを格納することが可能である。

コピーデータおよびスキャンデータを親展ボックスに格納するには、利用者が MFD の操作パネルからユーザーIDとユーザーパスワードを入力させて、認証されるとコピー機能およびスキャン機能の利用が可能になり、操作パネルからコピー蓄積またはスキャン指示をすることにより IIT が原稿を読み取り、内部ハードディスク装置に蓄積する。

登録されたユーザーID ごとの個別親展ボックスは、利用者が操作パネル、CWIS またはネットワークスキャナーユーティリティからユーザーIDとパスワードを入力すると MFD は内部に登録されたユーザーIDとパスワードが一致するかをチェックし、一致した場合のみ認証が成功しボックス内のデータを確認することが可能となり、取出し

（スキャンデータのみ）や印刷、削除の操作が可能となる。

（4）システム管理者セキュリティ管理機能

本 TOE は、ある特定の利用者へ特別な権限を持たせるために、システム管理者モードへのアクセスをシステム管理者にのみに制限して、認証されたシステム管理者のみに、操作パネルから下記のセキュリティ機能の参照と設定を行う権限を許可する。

- ハードディスク蓄積データ上書き消去機能の参照と設定
- ハードディスク蓄積データ暗号化機能の参照と設定
- ハードディスク蓄積データ暗号化キーの設定
- 本体パネルからの認証時のパスワード使用機能の参照と設定
- 機械管理者 ID とパスワード設定（機械管理者のみ可能）
- SA、一般利用者 ID の参照と設定およびとパスワード設定
- システム管理者認証失敗によるアクセス拒否機能の参照と設定
- ユーザーパスワード(一般利用者と SA)の文字数制限機能の参照と設定
- SSL/TLS 通信機能の参照と設定
- IPSec 通信機能の参照と設定
- S/MIME 通信機能の参照と設定
- 時刻指定文書削除機能の参照と設定
- ユーザー認証機能の参照と設定
- 蓄積プリント機能の参照と設定
- 日付、時刻の参照と設定

また本 TOE はシステム管理者クライアントから Web ブラウザを通じて CWIS 機能により、認証されたシステム管理者のみに、CWIS 機能により下記のセキュリティ機能の参照と設定を行う権限を許可する。

- 機械管理者 ID とパスワード設定（機械管理者のみ可能）
- SA、一般利用者 ID の参照と設定およびパスワード設定
- システム管理者認証失敗によるアクセス拒否機能の参照と設定
- ユーザーパスワード(一般利用者と SA)の文字数制限機能の参照と設定
- 監査ログ機能の参照と設定
- SSL/TLS 通信機能の参照と設定
- IPSec 通信機能の参照と設定
- SNMPv3 通信機能の参照と設定
- SNMPv3 認証パスワードの設定
- S/MIME 通信機能の参照と設定
- X.509 証明書の作成/アップロード/ダウンロード
- 時刻指定文書削除機能の参照と設定

- ユーザー認証機能の参照と設定

（5）カストマーエンジニア操作制限機能

本 TOE は、カストマーエンジニアが（4）のシステム管理者セキュリティ管理機能に関する設定の参照および変更が出来ないように、認証されたシステム管理者のみに操作パネルと CWIS から、カストマーエンジニア操作機能制限の有効/無効の参照と設定を行う権限を許可する。

（6）セキュリティ監査ログ機能

本 TOE は、いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザー操作など）を、追跡記録するためのセキュリティ監査ログ機能を提供する。 この機能はシステム管理者のみ利用可能であり、閲覧や解析のために Web ブラウザを通じて CWIS によりタブ区切りのテキストファイルでダウンロードすることが可能である。 システム管理者がセキュリティ監査ログデータをダウンロードするためには、SSL/TLS 通信が有効に設定されていなければならない。

（7）内部ネットワークデータ保護機能

本 TOE は、内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護するための以下の一般的な暗号化通信プロトコルに対応する。

- SSL/TLS プロトコル
- IPSec プロトコル
- SNMPv3 プロトコル
- S/MIME プロトコル

1.4.3. TOE の物理的範囲

本 TOE の物理的範囲は複合機全体である。図 4 に MFD 内の各ユニット構成と、TOE の物理的範囲を記述する。

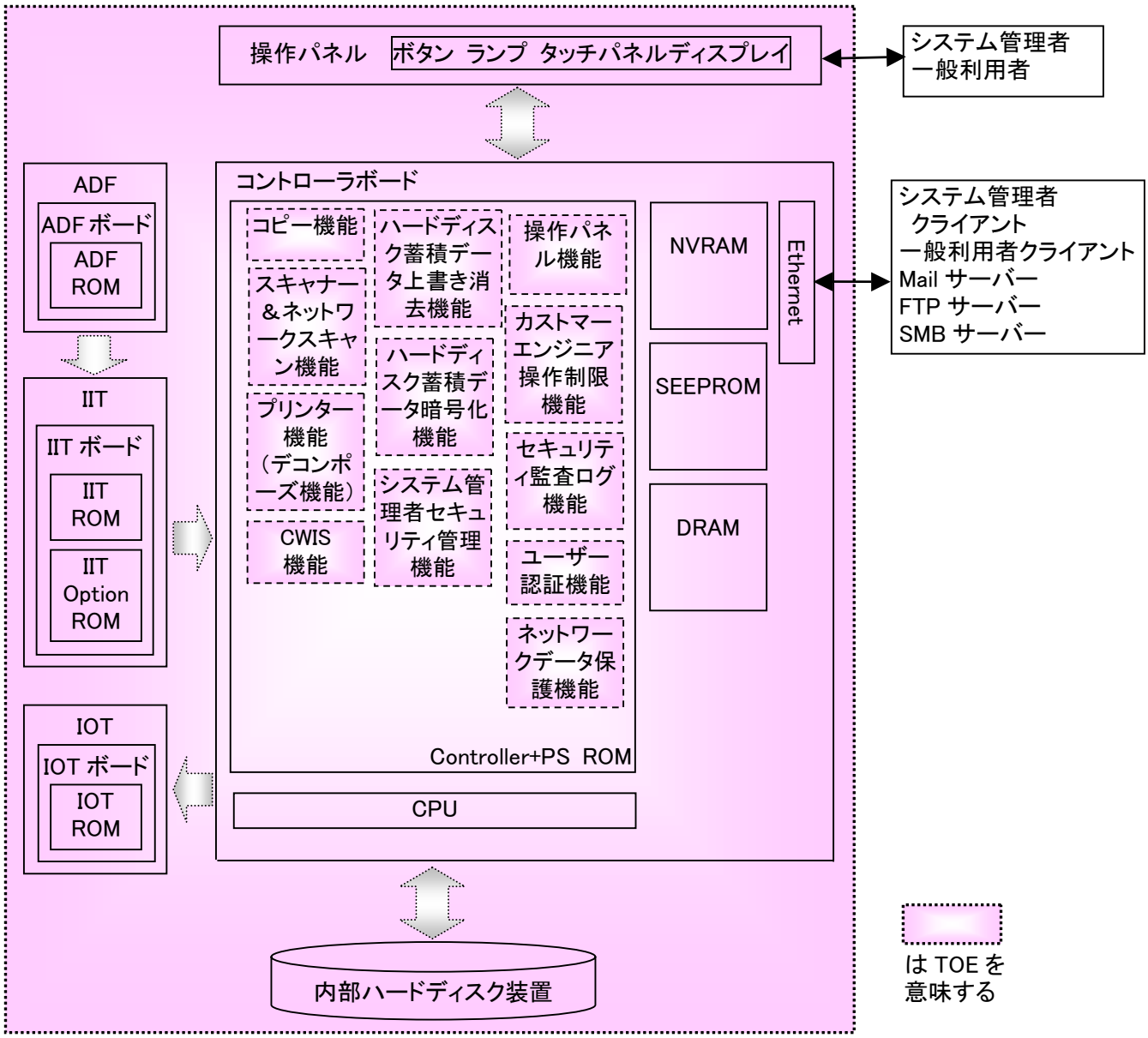

図 4 MFD 内の各ユニットと TOE の物理的範囲

MFD は、コントローラボード、操作パネルの回路基板ユニットおよび IIT、IOT、ADF から構成される。
コントローラボードと操作パネルの間は、制御データの通信を行う内部インターフェースで接続されている。コントローラボードと IIT ボードの間、およびコントローラボードと IOT ボードの間は、文書データおよび制御データの通信を行うための、専用の内部インターフェースで接続されている。
コントローラボードは、MFD のコピー機能、プリンター機能、スキャナー機能の制御を行うための回路基板であり、ネットワークインタフェース（Ethernet）を持ち、IIT ボードや IOT ボードが接続されている。

操作パネルは、MFD のコピー機能、プリンター機能、スキャナー機能の操作および設定に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネルである。
画像入力ターミナル（IIT）は、コピー、スキャナー機能の利用時に、原稿を読み込み、画像情報をコントローラボードへ転送する入力デバイスである。尚、IIT ROM と IIT Option ROM のコントローラソフト全体を含めて論理的に IIT と呼ぶ。
画像出力ターミナル（IOT）は、コントローラボードから転送される画像情報を出力するデバイスである。
自動原稿送り装置（ADF）は、原稿を自動的に IIT に搬送するデバイスである。

1.4.4. ガイダンス

本 TOE を構成するガイダンス文書は以下のとおりである。
Xerox 4112/4127 Copier/Printer System Administration Guide
Xerox 4112/4127 Copier/Printer User Guide
Xerox 4112/4127 Copier/Printer Security Function Supplementary Guide

2. 適合主張

2.1. CC 適合主張

本 ST および TOE の CC 適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン:

パート 1: 概説と一般モデル 2007 年 3 月 バージョン 3.1 翻訳第 1.2 版
パート 2: セキュリティ機能コンポーネント 2008 年 3 月 バージョン 3.1 翻訳第 2 .0 版
パート 3: セキュリティ保証コンポーネント 2008 年 3 月 バージョン 3.1 翻訳第 2 .0 版

CC パート 2 に対する ST の適合: CC パート 2 適合
CC パート 3 に対する ST の適合: CC パート 3 適合

2.2. PP 主張、パッケージ主張

2.2.1. PP 主張

本 ST が適合している PP はない。

2.2.2. パッケージ主張

EAL3 適合

2.2.3. 適合根拠

本 ST は PP 適合を主張していないので、PP 適合根拠はない。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威

3.1.1. TOE 資産

本 TOE が保護する資産は以下のとおりである(図 5)。

（1） MFD を使用する権利

一般利用者が、TOE の各機能を使用する権利を資産とする。

（2） ジョブ処理のために蓄積する文書データ

一般利用者が MFD をコピー、プリント、スキャン等の目的で利用すると画像処理や通信、蓄積プリントのために内部ハードディスク装置に一時的に文書データが蓄積される。また CWIS 機能やネットワークスキャナーユーティリティにより一般利用者クライアントから MFD 内に蓄積された文書データの取り出しが可能である。これらは一般利用者の機密情報であり、保護資産とする。

（3） ジョブ処理後の利用済み文書データ

一般利用者が MFD をコピー、スキャン等の目的で利用すると画像処理や通信、蓄積プリントのために内部ハードディスク装置に一時的に文書データが蓄積され、ジョブの完了やキャンセル時は管理情報を削除するがデータは残存する。これらは一般利用者の機密情報であり、保護資産とする。

（4） セキュリティ監査ログデータ

MFD に対し、いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザ操作など）を追跡記録するためにセキュリティ監査ログ機能により、内部ハードディスク装置内にログデータが発生した都度、記録保存される。 また CWIS 機能によりシステム管理者クライアントから MFD 内に蓄積されたセキュリティ監査ログデータの取り出しが可能である。この機能はトラブルの予防保全や対応、不正使用の検出に使用され、セキュリティ監査ログデータはシステム管理者のみアクセス可能なデータであり保護資産とする。

（5） TOE 設定データ

システム管理者はシステム管理者セキュリティ管理機能により TOE のセキュリティ機能の設定が、MFD の操作パネルやシステム管理者クライアントから可能であり、設定データは TOE 内に保存される（表 4）。これらは他の保護資産の脅威につながるものであり保護資産とする。

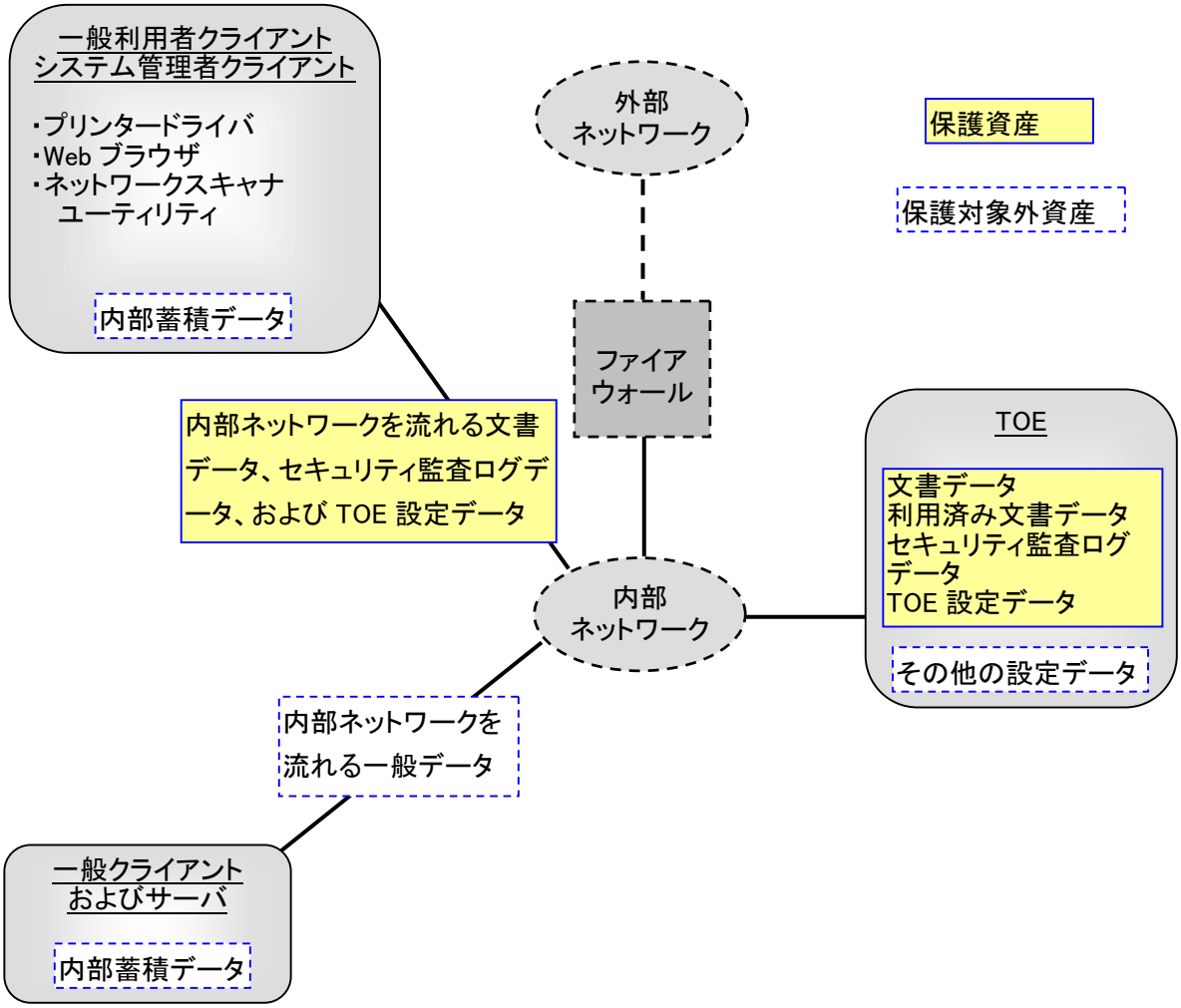

図 5 保護資産と保護対象外資産

注）内部ネットワーク内に存在する一般クライアントおよびサーバ内部の蓄積データや内部ネットワークを流れる一般データは保護対象外の資産である。

表 4 にコントローラボードの NVRAM および SEEPROM に記憶される TOE 設定データを記述する。

表 4 TOE 設定データ項目分類

TOE 設定データ項目分類（注）
ハードディスク蓄積データ上書き消去情報
ハードディスク暗号化情報
本体パネルからの認証時のパスワード使用情報
ユーザーパスワードの最小文字数情報
システム管理者 ID とパスワード情報
システム管理者認証失敗によるアクセス拒否情報
カストマーエンジニア操作制限情報

TOE 設定データ項目分類（注）
内部ネットワークデータ保護情報
セキュリティ監査ログ情報
親展ボックス情報
ユーザー認証情報
蓄積プリント情報
日付、時刻情報

注） 記憶場所の NVRAM と SEEPROM には、TOE 設定データ以外のデータも格納されているが、それらの設定データは TOE のセキュリティ機能に関係しないため保護対象の資産ではない。

3.1.2. 脅威

本 TOE に対する脅威を、表 5 に記述する。攻撃者は低レベルの攻撃能力を持つ者であり TOE の動作について公開されている情報知識を持っていると想定する。

表 5 脅威

脅威 （識別子）	内容説明
T.RECOVER	攻撃者が、内部ハードディスク装置を取り出して、その内容を読み取るために市販のツール等に接続して、内部ハードディスク装置上の利用済み文書データや文書データ、およびセキュリティ監査ログデータを不正に読み出して漏洩するかもしれない。
T.CONFDATA	攻撃者が、操作パネルやシステム管理者クライアントから、システム管理者のみアクセスが許可されている、TOE 設定データにアクセスして設定の変更、または不正な読み出しを行うかもしれない。
T.DATA_SEC	攻撃者が、操作パネルや Web ブラウザから、文書データおよびセキュリティ監査ログデータを不正に読み出すかもしれない。
T.COMM_TAP	攻撃者が、内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴や改ざんをするかもしれない。
T.CONSUME	攻撃者が、TOE にアクセスし TOE の利用を不正に行うかもしれない。

3.2. 組織のセキュリティ方針

本 TOE が順守しなければならない組織のセキュリティ方針はない。

3.3. 前提条件

本 TOE の動作、運用、および利用に関する前提条件を、表 6 に記述する。

表 6 前提条件

前提条件（識別子）	内容説明
人的な信頼	
A.ADMIN	システム管理者は、TOE セキュリティ機能に関する必要な知識を持ち、課せられた役割に従い TOE の維持管理を遂行し、悪意をもった不正を行わないものとする。
保護モード	
A.SECMODE	システム管理者は、TOE を運用するにあたり、下記の通りに設定するものとする。 • 本体パネルからの認証時のパスワード使用設定：有効にする • システム管理者パスワード長：9 文字以上 • システム管理者認証失敗によるアクセス拒否設定：有効にする • システム管理者認証失敗によるアクセス拒否回数設定：5 • カストマーエンジニア操作制限設定：有効にする • ユーザー認証設定：有効にする（ローカル認証を選択） • ユーザーパスワード(一般利用者と SA)文字数制限設定：9 文字以上 • プライベートプリント設定：認証成功のジョブを蓄積にする • 監査ログ設定：有効にする • SNMPv3 通信設定：有効にする • SNMPv1/v2c 通信設定：無効にする • SNMPv3 認証パスワード：8 文字以上 • SSL/TLS 通信設定：有効にする • IPSec 通信設定：有効にする • S/MIME 通信設定：有効にする • SMB 通信設定：NetBEUI を無効にする • ハードディスク蓄積データ上書き消去設定：有効にする • ハードディスク蓄積データ暗号化設定：有効にする • ハードディスク蓄積データ暗号化キー：12 文字 • 時刻指定文書削除設定：有効にする

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 7 に記述する。

表 7 TOE セキュリティ対策方針

セキュリティ対策方針（識別子）	詳細内容
O.AUDITS	本 TOE は、不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供しなければならない。
O.CIPHER	本 TOE は、内部ハードディスク装置に蓄積されている文書データ、利用済み文書データ、セキュリティ監査ログデータを取り出しても解析が出来ないように、ハードディスク上に蓄積されるデータを暗号化する機能を提供しなければならない。
O.COMM_SEC	本 TOE は、TOE とリモート間の内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを、盗聴や改ざんから保護するために暗号化通信機能を提供しなければならない。
O.MANAGE	本 TOE は、セキュリティ機能の設定を行うシステム管理者モードのアクセスを、認証されたシステム管理者のみ許可して、一般利用者による TOE 設定データへのアクセスを不可能にしなければならない。
O.RESIDUAL	本 TOE は、内部ハードディスク装置に蓄積される利用済み文書データの再生および復元を不可能にするために上書き消去機能を提供しなければならない。
O.USER	本 TOE は、正当な TOE の利用者を識別し、正当な利用者のみに文書データの登録、取り出し、削除、パスワードの変更を可能にする権利を提供しなければならない。
O.RESTRICT	本 TOE は、許可されていない者への TOE の機能使用を制限する機能を提供しなければならない。

4.2. 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を表 8 に記述する。

表 8 運用環境のセキュリティ対策方針

セキュリティ対策方針（識別子）	詳細内容
OE.ADMIN	システム管理者は組織の管理者により本 TOE を管理するために信頼できる組織内の適任者として任命され、TOE を管理するために必要な教育を受け、ガイダンスに従い TOE の維持管理を実施する。
OE.AUTH	本 TOE を管理するシステム管理者は、下記の通りに TOE のセキュリティ機能を設定して、TOE を運用しなければならない。 • 本体パネルからの認証時のパスワードの使用設定：有効にする • システム管理者パスワード長：9 文字以上 • システム管理者認証失敗によるアクセス拒否設定：有効にする • システム管理者認証失敗によるアクセス拒否回数設定：5 • カストマーエンジニア操作制限設定：有効にする • ユーザー認証設定：有効にする（ローカル認証を選択） • ユーザーパスワード(一般利用者と SA)文字数制限設定：9 文字以上 • プライベートプリント設定：認証成功のジョブを蓄積にする
OE.COMMS_SEC	本 TOE を管理するシステム管理者は、下記の通りに内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定して、TOE を運用しなければならない。 • SNMPv3 通信設定：有効にする • SNMPv1/v2c 通信設定：無効にする • SNMPv3 認証パスワード：8 文字以上 • SSL/TLS 通信設定：有効にする • IPSec 通信設定：有効にする • S/MIME 通信設定：有効にする • SMB 通信設定：NetBEUI を無効にする
OE.FUNCTION	本 TOE を管理するシステム管理者は、下記の通りに TOE のセキュリティ機能を設定して、TOE を運用しなければならない。 • ハードディスク蓄積データ上書き消去設定：有効にする • ハードディスク蓄積データ暗号化設定：有効にする • ハードディスク蓄積データ暗号化キー：12 文字 • 時刻指定文書削除設定：有効にする • 監査ログ設定：有効にする

4.3. セキュリティ対策方針根拠

セキュリティ対策は、セキュリティ課題定義で規定した前提条件に対応するためのもの、あるいは脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対応する前提条件、対抗する脅威、実現する組織のセキュリティ方針の対応関係を表 9 に示す。また各セキュリティ課題定義がセキュリティ対策方針により保証されていることを表 10 に記述する。

表 9 セキュリティ対策方針と対抗する脅威、組織セキュリティ方針及び前提条件

セキュリティ課題定義 / セキュリティ対策方針	A.ADMIN	A.SECMODE	T.RECOVER	T.CONFDATA	T.COMM_TAP	T.DATA_SEC	T.CONSUME
O.AUDITS				○		○	
O.CIPHER			○				
O.COMM_SEC					○		
O.MANAGE				○		○	
O.RESIDUAL			○				
O.USER				○		○	
O.RESTRICT							○
OE.ADMIN	○						
OE.AUTH		○		○		○	
OE.COMM_SEC		○			○		
OE.FUNCTION		○	○	○		○	

表 10 セキュリティ課題定義に対応するセキュリティ対策方針根拠

セキュリティ課題定義	セキュリティ対策方針根拠
A.ADMIN	運用環境のセキュリティ対策方針である OE.ADMIN により、システム管理者は組織の管理者により本 TOE を管理するために信頼できる組織内の適任者として任命され、TOE を管理するために必要な教育を受け、ガイダンスに従い TOE の維持管理を実施する。 この対策方針により、A.ADMIN を実現できる。
A.SECMODE	運用環境のセキュリティ対策方針である OE.AUTH によりシステム管理者は IDとパスワードを適切に設定し、またカストマーエンジニア操作制限機能を有効にし、またユーザー認証を有効にして運用する。 また OE.COMM_SEC により、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定して運用する。

セキュリティ課題定義	セキュリティ対策方針根拠
	また OE.FUNCTION により、「ハードディスク蓄積データ上書き消去機能」、「ハードディスク蓄積データ暗号化機能」、「セキュリティ監査ログ機能」を有効に設定して、内部ハードディスク装置に蓄積されている利用済み文書データの復元を、不可能にする。 これらの対策方針により、A.SECMODE を実現できる。
T.RECOVER	この脅威に対抗するには、運用環境のセキュリティ対策方針である OE.FUNCTION により、下記の TOE セキュリティ機能を有効に設定して、内部ハードディスク装置に蓄積されている文書データやセキュリティ監査ログデータの読み出しや、利用済み文書データの復元を、不可能にする事が必要であり、具体的にはセキュリティ対策方針である O.RESIDUAL、および O.CIPHER によって対抗する。 「ハードディスク蓄積データ上書き消去機能」、「ハードディスク蓄積データ暗号化機能」 文書データを保護するため、O.CIPHER により、内部ハードディスク装置上に蓄積される文書データやセキュリティ監査ログデータを暗号化することによって、文書データ、利用済み文書データ、セキュリティ監査ログデータの閲覧や読み出しを不可能にする。 また利用済み文書データを保護するため、O.RESIDUAL により、利用が終了した文書データを上書き消去することによって、内部ハードディスク装置上に蓄積された利用済み文書データの再生や復元を不可能にする。 これらの対策方針により、T.RECOVER に対抗できる。
T.CONFDATA	この脅威に対抗するには、運用環境のセキュリティ対策方針である OE.AUTH と OE.FUNCTION により、下記の TOE セキュリティ機能を有効に設定して、認証されたシステム管理者のみに、TOE 設定データの変更を許可する事が必要であり、具体的にはセキュリティ対策方針である O.MANAGE と O.USER 、O.AUDITS によって対抗する。 「パスワード使用」、「システム管理者パスワード」、「システム管理者認証失敗によるアクセス拒否」、「カストマーエンジニア操作制限機能」、「監査ログ機能」 O.MANAGE により、TOE セキュリティ機能の有効/無効化や、TOE 設定データの参照/更新は、認証されたシステム管理者のみに限定される。 また O.USER により、正当な利用者のみにパスワード変更を可能にする権利を提供する。 また O.AUDITS により不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供する。 これらの対策方針により、T.CONFDATA に対抗できる。
T.CONSUME	この脅威に対抗するには、セキュリティ対策方針である O.RESTRICT によって対抗する。 O.RESTRICT により TOE の利用を制限することができる。 この対策方針により、T.CONSUME に対抗できる。
T.COMM_TAP	この脅威に対抗するには、セキュリティ対策方針である O.COMM_SEC により、

セキュリティ課題定義	セキュリティ対策方針根拠
	暗号化通信プロトコルが持つクライアント/サーバ認証機能により、正規の利用者のみに通信データの送受が許可される。 また暗号化通信機能により通信データを暗号化することによって、内部ネットワーク上の文書データ、セキュリティ監査ログデータおよび TOE 設定データの盗聴や改ざんを不可能にする。 さらに運用環境のセキュリティ対策方針である OE.COMM_SEC により、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを盗聴より保護するように設定することで、これらのデータが保護対象となる。 これらの対策方針により、T.COMM_TAP に対抗できる。
T.DATA_SEC	この脅威に対抗するには、運用環境のセキュリティ対策方針である OE.AUTH と OE.FUNCTION により、下記のパスワードとユーザー認証機能、セキュリティ監査ログ機能を設定して、認証された正当な利用者のみに、セキュリティ監査ログデータと文書データへのアクセスを許可する必要があり、具体的にはセキュリティ対策方針である O.USER と O.MANAGE と O.AUDITS によって対抗する。 ・「ユーザーパスワード」、「システム管理者パスワード」「ローカル認証」、「セキュリティ監査ログ機能」 O.USER により、内部ハードディスク装置上に蓄積された文書データやセキュリティ監査ログデータの読み出しは、認証された正当な利用者のみに限定される。 また O.MANAGE により TOE セキュリティ機能の設定を認証されたシステム管理者のみに限定する。 また O.AUDITS により不正アクセス監視に必要な監査イベントの記録機能とセキュリティ監査ログデータを提供する。 これらの対策方針により、T.DATA_SEC に対抗できる。

5. 拡張コンポーネント定義

5.1. 拡張コンポーネント

本 ST は CC パート 2 及び CC パート 3 に適合しており、拡張コンポーネントは定義しない。

6. セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件およびセキュリティ要件根拠について記述する。
なお、本章で使用する用語の定義は以下のとおりである。

・ サブジェクト

名称	定義
機械管理者プロセス	機械管理者のユーザー認証が成功した状態での親展ボックス、蓄積プリントに対する操作
SA プロセス	SA のユーザー認証が成功した状態での親展ボックス、蓄積プリントに対する操作
一般利用者プロセス	一般利用者のユーザー認証が成功した状態での親展ボックス、蓄積プリントに対する操作
内部ネットワーク送信	内部ネットワーク内でネットワークスキャンのデータを宛先のクライアント PC へ送信する。
内部ネットワーク受信	内部ネットワーク内でクライアント PC からのプリントデータを受信する。

・ オブジェクト

名称	定義
親展ボックス	MFD の内部ハードディスク装置に作成される論理的なボックス。コピー機能およびスキャナー機能により読み込まれた文書データをユーザー別や送信元別に蓄積することが出来る。
個別親展ボックス	一般利用者が個別に使用できる親展ボックス。各一般利用者が作成する。
共用親展ボックス	すべての利用者が共有して使える親展ボックス。機械管理者が作成できる。
蓄積プリント	プリンター機能において、印刷データをデコンポーズして作成したビットマップデータを、MFD の内部ハードディスク装置に一旦蓄積し、認証された一般利用者が操作パネルより指示する事で印刷を開始するプリント方法。
内部ハードディスク装置に蓄積される利用済み文書データ	MFD の内部ハードディスク装置に蓄積された後、利用が終了しファイルは削除されるが、内部ハードディスク装置内にはデータ部は残存している状態の文書データ。
文書データ	一般利用者が MFD のコピー機能、プリンター機能、スキャナー機能を利用する際に、MFD 内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。
セキュリティ監査ログ	いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザ操作など）を、追跡記録されたデータ。

・ 操作

名称	定義
ふるまいを改変する	ユーザー認証機能（ローカル、外部）、蓄積プリント機能（認証失敗時の蓄積、削除）、内部ネットワークデータ保護機能（認証方式、暗号化方式）、ハードディスク蓄積データ上書き消去機能（上書き回数、上書き情報、時刻指定文書削除）のふるまいの変更
改変	TOE 設定データの設定変更およびセキュリティ属性（利用者識別情報）の変更

・ セキュリティ属性

名称	定義
一般利用者役割	一般利用者が TOE を利用する際に必要な権限を表す
SA 役割	SA が TOE を利用する際に必要な権限を表す
機械管理者役割	機械管理者が TOE を利用する際に必要な権限を表す
一般利用者識別情報	一般利用者を認証識別するためのユーザーID とパスワード情報
SA 識別情報	SA を認証識別するためのユーザーID とパスワード情報
機械管理者識別情報	機械管理者を認証識別するためのユーザーID とパスワード情報
親展ボックスに対応する所有者識別情報（個別、共用）	各親展ボックスに対応したアクセス可能なユーザー、親展ボックス名、パスワード、文書削除条件等の情報
蓄積プリントに対応する所有者識別情報	プライベートプリントに対応させたユーザーID、パスワード、認証不成功時の処理方法等の情報

・ 外部のエンティティ

名称	定義
システム管理者	機械管理者と SA の総称。
機械管理者	MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。
SA （System Administrator）	機械管理者あるいは既に作成された SA が作成することができ、MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。
一般利用者	MFD のコピー機能、スキャナー機能およびプリンター機能を利用する者。

・ その他の用語

名称	定義
富士ゼロックス標準の FXOSENC 方式	富士ゼロックス標準の暗号鍵生成アルゴリズムで、起動時に使用される。
AES	FIPS 標準規格の暗号化アルゴリズムで、ハードディスクデータの暗号化と復号化に使用される。

認証失敗によるアクセス拒否	システム管理者 ID 認証失敗が所定回数に達した時に、操作パネルでは電源切断/投入以外の操作は受け付けなくなり、また Web ブラウザでは本体の電源の切断/投入まで認証操作を受け付けなくなる動作。
本体パネルからの認証時のパスワード使用情報	TOE 設定データであり、本体パネルからの認証時のパスワード使用機能の有効/無効の情報。
機械管理者の ID 情報	TOE 設定データであり、機械管理者認証のための ID 情報。
機械管理者のパスワード情報	TOE 設定データであり、機械管理者認証のためのパスワード情報
SA の ID 情報	TOE 設定データであり、SA 認証のための ID 情報。
SA のパスワード情報	TOE 設定データであり、SA 認証のためのパスワード情報
一般利用者の ID 情報	TOE 設定データであり、一般利用者認証のための ID 情報。
一般利用者のパスワード情報	TOE 設定データであり、一般利用者認証のためのパスワード情報
システム管理者認証失敗によるアクセス拒否情報	TOE 設定データであり、システム管理者 ID 認証失敗に関係する機能の有効/無効の情報と失敗回数情報
セキュリティ監査ログ設定情報	いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザ操作など）を、追跡記録する機能の有効/無効の情報。
ユーザー認証方法の情報	MFD のコピー機能、スキャナー機能およびプリンター機能を利用する際に、ユーザー認証情報にて認証する機能の有効/無効および認証方法の情報。
内部ネットワークデータ保護情報	内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データといった通信データを保護するために対応する一般的な暗号化通信プロトコルの有効/無効および設定の情報。
カストマーエンジニア操作制限情報	TOE 設定データであり、カストマーエンジニア操作制限機能の有効/無効の情報。
ハードディスク蓄積データ暗号化情報	TOE 設定データであり、ハードディスク蓄積データ暗号化機能に関係する機能の有効/無効の情報と暗号化キー情報。
ハードディスク蓄積データ上書き情報	TOE 設定データであり、ハードディスク蓄積データ上書き消去機能に関係する機能の有効/無効の情報と上書き回数情報、および時刻指定文書削除機能の有効/無効の情報と日時指定情報。
日付、時刻情報	TOE 設定データであり、ログを管理するための時計情報
システム管理者モード	一般利用者が MFD の機能を利用する動作モードとは別に、システム管理者が TOE の使用環境に合わせて、TOE 機器の動作設定や TOE セキュリティ機能の参照/更新といった設定の変更を行う動作モード。

証明書	ITU-T勧告のX.509に定義されており、本人情報（所属組織、識別名、名前等）、公開鍵、有効期限、シリアルナンバ、シグネチャ等が含まれている情報。
プリンタードライバ	一般利用者クライアント上のデータを、MFDが解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウエアで、利用者クライアントで使用する。
ネットワークスキャナユーティリティ	MFD 内の親展ボックスに保存されている文書データを一般利用者クライアントから取り出すためのソフトウェア。

6.1. セキュリティ機能要件

本TOEが提供するセキュリティ機能要件を以下に記述する。 セキュリティ機能要件は[CCパート2]で規定されているクラスおよびコンポーネントに準拠している。

6.1.1. クラス FAU: セキュリティ監査

① FAU_GEN.1 監査データ生成
下位階層: なし
依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:
a)監査機能の起動と終了;
b)監査の[選択:最小、基本、詳細、指定なし] レベルのすべての監査対象事象; 及び
c)[割付:上記以外の個別に定義した監査対象事象]

[選択:最小、基本、詳細、*指定なし*]
・*指定なし*
[割付:上記以外の個別に定義した監査対象事象]
・*表 11 のリストに示された各機能要件を選択した場合に監査対象とすべきアクション(規約)と、それに関連するTOEの監査対象事象（実行ログとして記録を残す事象）*

表 11 TOEの監査対象事象と個別に定義した監査対象事象

機能要件	CCで定義された監査対象とすべきアクション	TOEの監査対象事象
FAU_GEN.1	なし	ー
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	*基本:監査ログデータのダウンロード成功を監査する。*
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	*基本:監査ログデータのダウンロード失敗を監査する。*

FAU_STG.1	なし	ー
FAU_STG.4	a) 基本:監査格納失敗によってとられるアクション。	*監査事象は採取しない*
FCS_CKM.1	a) 最小: 動作の成功と失敗。 b) 基本: オブジェクト属性及び機密情報(例えば共通あるいは秘密鍵)を除くオブジェクトの値。	*監査事象は採取しない*
FCS_COP.1	a) 最小: 成功と失敗及び暗号操作の種別。 b) 基本: すべての適用可能な暗号操作のモード、サブジェクト属性、オブジェクト属性。	*監査事象は採取しない*
FDP_ACC.1	なし	ー
FDP_ACF.1	a) 最小: SFPで扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFPで扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	*基本:* *親展ボックスの作成、削除が監査される。* *親展ボックスアクセス、蓄積プリントの実行に関しユーザー名、ジョブ情報、成功可否が監査される。*
FDP_RIP.1	なし	ー
FIA_AFL.1	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	*＜最小＞* *連続認証エラーを監査する。*
FIA_ATD.1	なし	ー
FIA_UAU.2	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	*＜最小＞* *連続認証エラーを監査する。*
FIA_UAU.7	なし	ー
FIA_UID.2	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。	*＜最小＞* *連続認証エラーを監査する*

FIA_USB.1	a）最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b）基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)。	*＜最小＞* *連続認証エラーを監査する*
FMT_MOF.1	a) 基本: TSFの機能のふるまいにおけるすべての改変。	*＜基本＞* *セキュリティ機能の設定変更を監査する。*
FMT_MSA.1	a) 基本:セキュリティ属性の値の改変すべて。	*＜基本＞* *親展ボックスの作成、削除が監査される。* *親展ボックスアクセス、蓄積プリントの実行に関しユーザー名、ジョブ情報、成功可否が監査される。*
FMT_MSA.3	a) 基本:許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本:セキュリティ属性の初期値の改変すべて。	*＜個別に定義した監査対象事象＞* *システム管理者の認証成功／認証失敗を監査する。*
FMT_MTD.1.	a) 基本:TSF データの値のすべての改変。	*＜個別に定義した監査対象事象＞* *セキュリティ機能の設定変更を監査する。*
FMT_SMF.1	a) 最小:管理機能の使用。	*＜個別に定義した監査対象事象＞* *システム管理者の認証成功／認証失敗を監査する。*
FMT_SMR.1	a) 最小:役割の一部をなす利用者のグループに対する改変; b) 詳細:役割の権限の使用すべて。	*＜個別に定義した監査対象事象＞* *システム管理者の認証成功／認証失敗を監査する。*
FPT_STM.1	a) 最小:時間の変更; b) 詳細:タイムスタンプの提供。	*＜最小＞* *時刻設定の変更を監査する*
FTP_TRP.1	a) 最小: 高信頼パス機能の失敗。 b) 最小: もし得られれば、すべての高信頼パス失敗に関係する利用者の識別情報。 c) 基本: 高信頼パス機能のすべての使用の試み。 d) 基本: もし得られれば、すべての高信頼パス呼出に関係する利用者の識別情報。	*＜個別に定義した監査対象事象＞* *証明書の登録と抹消を監査する。*

FAU_GEN.1.2　TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:
a)事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗); 及び
b)各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、［割付:その他の監査関連情報］。

[割付:その他の監査関連情報]
・*その他の監査関連情報はない*

② FAU_SAR.1　監査レビュー
下位階層:　なし
依存性:　FAU_GEN.1　監査データ生成

FAU_SAR.1.1　TSF は、［割付:許可利用者］が、［割付:監査情報のリスト］を監査記録から読み出せるようにしなければならない。

[割付:許可利用者]
・*システム管理者*
[割付:監査情報のリスト]
・*すべてのログ情報*

FAU_SAR.1.2　TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

③ FAU_SAR.2　限定監査レビュー
下位階層:　なし
依存性:　FAU_SAR.1　監査レビュー

FAU_SAR.2.1　TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

④ FAU_STG.1　保護された監査証跡格納
下位階層:　なし
依存性:　FAU_GEN.1　監査データ生成

FAU_STG.1.1　TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2　TSF は、監査証跡に格納された監査記録への不正な改変を［選択:防止、検出: から1つのみ選択］できなければならない。

[選択:防止、検出: から1つのみ選択]
・*防止*

⑤ FAU_STG.4 監査データ損失の防止
下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション
依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、［選択:監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から１つのみ選択］及び［割付:監査格納失敗時にとられるその他のアクション］を行わねばならない。

[選択:監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から 1 つのみ選択]
・*最も古くに格納された監査記録への上書き*
[割付:監査格納失敗時にとられるその他のアクション]
・*実施するその他のアクションは無い*

6.1.2. クラス FCS: 暗号サポート

① FCS_CKM.1 暗号鍵生成
下位階層: なし
依存性: [FCS_CKM.2 暗号鍵配付、または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

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]
・*指定なし*
[割付: 暗号鍵生成アルゴリズム]
・*富士ゼロックス標準の FXOSENC 方式*
[割付: 暗号鍵長]
・*128 ビット*

② FCS_COP.1 暗号操作
下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または

FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、
または FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1　TSF 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]
・*128 ビット*
[割付：暗号操作のリスト]
・*内部ハードディスク装置に蓄積される文書データおよびセキュリティ監査ログデータの暗号化、内部ハードディスク装置から取り出される文書データおよびセキュリティ監査ログデータの復号化*

6.1.3. クラス FDP：　利用者データ保護

① FDP_ACC.1　サブセットアクセス制御
下位階層：　なし
依存性：　FDP_ACF.1　セキュリティ属性によるアクセス制御

FDP_ACC.1.1　TSF は、［割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト］に対して［割付：アクセス制御 SFP］を実施しなければならない。

[割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]
・*表 12 に示すサブジェクトとオブジェクトのリストおよびオブジェクトの操作のリスト*
[割付：アクセス制御 SFP]
・*MFD アクセス制御 SFP*

表 12 サブジェクトとオブジェクトのリストおよびオブジェクトの操作のリスト

サブジェクト	オブジェクト	操作
機械管理者 *プロセス*	*親展ボックス*	*個別親展ボックスの削除* *共用親展ボックスの作成* *共用親展ボックスの削除* *文書データの登録* *すべての文書データの削除* *すべての文書データの取り出し*
	蓄積プリント	*文書データの登録* *すべての文書データの削除* *すべての文書データの取り出し*
SA *プロセス*	*親展ボックス*	*個別親展ボックスの作成* *個別親展ボックスの削除* *文書データの登録* *文書データの取り出し* *文書データの削除*
	蓄積プリント	*文書データの登録* *すべての文書データの削除* *すべての文書データの取り出し*
一般利用者プロセス	*親展ボックス*	*個別親展ボックスの作成* *個別親展ボックスの削除* *文書データの登録* *文書データの取り出し* *文書データの削除*
	蓄積プリント	*文書データの登録* *文書データの削除* *文書データの取り出し*

② FDP_ACF.1 セキュリティ属性によるアクセス制御
下位階層: なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 TSF は、以下の［割付:示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ］に基づいて、オブジェクトに対して、［割付:アクセス制御 SFP］を実施しなければならない。

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

性の名前付けされたグループ]
・*一般利用者プロセスと対応する一般利用者識別情報、SA プロセスと対応する SA 識別情報、機械管理者プロセスと対応する機械管理者識別情報、*
・*親展ボックスと対応する所有者識別情報、・蓄積プリントと対応する所有者識別情報*
[割付：アクセス制御 SFP]
・*MFD アクセス制御 SFP*

FDP_ACF.1.2　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、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]
・*表 13 に示す、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*

表 13 アクセスを管理する規則

一般利用者プロセス、SA プロセスでの親展ボックスの操作の規則
・*個別親展ボックスの作成* *個別親展ボックスの作成操作を行うと、個別親展ボックスの所有者識別情報に、個別親展ボックスを作成した一般利用者、SA プロセスの一般利用者識別情報、SA 識別情報が設定された個別親展ボックスが作成される。* ・*個別親展ボックスの削除* *個別親展ボックスの所有者識別情報と、一般利用者、SA プロセスの一般利用者識別情報、SA 識別情報が一致した場合、その個別親展ボックスに関する、個別親展ボックスの削除の操作が許可される。* ・*個別親展ボックスの文書データの登録、文書データの取り出し、文書データの削除* *個別親展ボックスの所有者識別情報と、一般利用者、SA プロセスの一般利用者識別情報、SA 識別情報が一致した場合、その個別親展ボックスに関する文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。* ・*共用親展ボックスの文書データの登録、文書データの取り出し、文書データの削除* *親展ボックスが共用親展ボックスの場合、その共用親展ボックスに関する文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。*
一般利用者プロセス、SA プロセスでの蓄積プリントの操作の規則
・*文書データの登録* *文書データの登録の操作を行うと、一般利用者、SAプロセスが持つ一般利用者識別情報、SA識別情報をその蓄積プリントの所有者識別情報に設定した蓄積プリントが作成さ*

れ、その蓄積プリントに文書データが登録される。 *・文書データの削除、文書データの取り出し* *蓄積プリントの所有者識別情報と、一般利用者、SAプロセスの一般利用者識別情報、SA識別情報が一致した場合、一般利用者、SAプロセスに対して、その蓄積プリントに関する文書データの取り出し、文書データの削除の操作が許可される。文書データの削除の操作が行われると、その蓄積プリントも削除される。*
機械管理者プロセスでの親展ボックスの操作の規則
・機械管理者プロセスの場合、機械管理者識別情報が設定された共用親展ボックスの作成操作、共用親展ボックスの削除操作および個別親展ボックスの削除操作が許可される。

FDP_ACF.1.3　TSF は、次の追加規則、[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許可する規則]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許可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許可する規則]
・表14 に示す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許可する規則

表 14 アクセスを明示的に管理する規則

機械管理者プロセスでの親展ボックスの操作の規則
・機械管理者プロセスの場合、すべての親展ボックスに対し親展ボックスの削除、文書データの登録、文書データの削除、文書データの取り出しの操作を許可する。
機械管理者プロセス、SA プロセスでの蓄積プリントの操作の規則
・機械管理者プロセスおよびSA プロセスの場合、すべての蓄積プリントに対し文書データの削除、文書データの取り出しを許可する。

FDP_ACF.1.4　TSF は、［割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則］ に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

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

⑤ FDP_RIP.1　サブセット情報保護
下位階層：　なし
依存性：　なし

FDP_RIP.1.1　TSF は、[割付： オブジェクトのリスト]のオブジェクト[選択： への資源の割当て、

からの資源の割当て解除]において、資源の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]
・*内部ハードディスク装置に蓄積される利用済み文書データ*
[選択：への資源の割当て、からの資源の割当て解除]
・*からの資源の割当て解除*

6.1.4. クラス FIA： 識別と認証

① FIA_AFL.1 (1) 認証失敗時の取り扱い
下位階層： なし
依存性： FIA_UAU.1 認証のタイミング

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]
・*システム管理者の認証*
[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]*
[割付：正の整数値]
・*5*

FIA_AFL.1.2 (1) 不成功の認証試行が定義した回数[選択：に達する、を上回った]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。

[選択：に達する、を上回った]
・*に達する*
[割付：アクションのリスト]
・*操作パネルでは電源切断/投入以外の操作は受け付けない。またWebブラウザでも本体の電源の切断/投入まで認証操作は受け付けない*

① FIA_AFL.1 (2) 認証失敗時の取り扱い
下位階層： なし
依存性： FIA_UAU.1 認証のタイミング

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]
・*一般利用者の認証*
[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]*
[割付：正の整数値]
・*1*

FIA_AFL.1.2 (2) 不成功の認証試行が定義した回数[選択：に達する、を上回った]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。

[選択：に達する、を上回った]
・*に達する*
[割付：アクションのリスト]
・*操作パネルでは"認証が不成功の"旨のメッセージを表示してユーザー情報の再入力を要求する。Web ブラウザ、ネットワークスキャナーユーティリティではユーザー情報の再入力を要求する*

② FIA_ATD.1 利用者属性定義
下位階層： なし
依存性： なし

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]

[割付：セキュリティ属性のリスト]
・*機械管理者役割*
・*SA 役割*
・*一般利用者役割*

③ FIA_UAU.2 アクション前の利用者認証
下位階層： FIA_UAU.1 認証のタイミング
依存性： FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

④ FIA_UAU.7 保護された認証フィードバック
下位階層： なし

依存性: FIA_UAU.1 認証のタイミング

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]
・*パスワードとして入力した文字を隠すための'*'文字の表示*

⑤ FIA_UID.2 アクション前の利用者識別
下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

⑥ FIA_USB.1 利用者・サブジェクト結合
下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

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:以下の利用者セキュリティ属性のリスト]
・*機械管理者役割*
・*SA 役割*
・*一般利用者役割*

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の規則]

[割付:属性の最初の関連付けの規則]
・*なし*

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:属性の変更の規則]

[割付:属性の変更の規則]
・*なし*

6.1.5. クラス FMT: セキュリティ管理

① FMT_MOF.1 セキュリティ機能のふるまいの管理
下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MOF.1.1 TSF は、機能［割付:機能のリスト］［選択:のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する］能力を［割付:許可された識別された役割］に制限しなければならない。

［割付:機能のリスト］
・*表 15 のセキュリティ機能のリスト*
［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］
・*のふるまいを停止する、を動作させる、のふるまいを改変する*
［割付:許可された識別された役割］
・*表 15 のセキュリティ機能のリストで示された役割*

表 15 セキュリティ機能のリスト

セキュリティ機能	を停止する、を動作させる、のふるまいを改変する	役割
本体パネルからの認証時のパスワード使用	*動作、停止*	*機械管理者、SA*
システム管理者認証失敗によるアクセス拒否	*動作、停止*	*機械管理者、SA*
ユーザー認証機能	*動作、停止、改変*	*機械管理者、SA*
セキュリティ監査ログ機能	*動作、停止*	*機械管理者、SA*
蓄積プリント機能	*動作、停止、改変*	*機械管理者、SA*
内部ネットワークデータ保護機能	*動作、停止、改変*	*機械管理者、SA*
カストマーエンジニア操作制限機能	*動作、停止*	*機械管理者、SA*
ハードディスク暗号化機能	*動作、停止*	*機械管理者、SA*
ハードディスク蓄積データ上書き消去機能	*動作、停止、改変*	*機械管理者、SA*

② FMT_MSA.1 セキュリティ属性の管理
下位階層: なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1 TSF は、セキュリティ属性[割付:セキュリティ属性のリスト]に対し[選択: デフォ

ルト値変更、問い合わせ、改変、削除、[割付:その他の操作]]をする能力を[割付: 許可された識別された役割]に制限する[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。

[割付:セキュリティ属性のリスト]
・*利用者識別情報、親展ボックスに対応する所有者識別情報、蓄積プリントに対応する識別情報*
[選択:デフォルト値変更、問い合わせ、改変、削除、[割付:その他の操作]]
・*問い合わせ、削除、[割付:その他の操作]*
[割付:その他の操作]
・*作成*
[割付:許可された識別された役割]
・*表 16 の操作、役割*
[割付:アクセス制御 SFP、情報フロー制御 SFP]
・*MFD アクセス制御 SFP*

表 16 セキュリティ属性の管理役割

セキュリティ属性	問い合わせ、改変、削除、作成	役割
機械管理者識別情報	*改変*	*機械管理者*
SA識別情報	*問い合わせ、改変、削除、作成*	*機械管理者、SA*
一般利用者識別情報	*問い合わせ、改変、削除、作成*	*機械管理者、SA*
個別親展ボックスに対応する所有者識別情報	*問い合わせ、削除、作成*	*一般利用者、SA*
すべての個別親展ボックスに対応する所有者識別情報	*問い合わせ、削除、作成*	*機械管理者*
共用親展ボックスに対応する所有者識別情報	*問い合わせ、削除、作成*	*機械管理者*
蓄積プリントに対応する識別情報	*問い合わせ、削除*	*機械管理者、SA、一般利用者*
すべての蓄積プリントに対応する識別情報	*問い合わせ、削除*	*機械管理者、SA*

③ FMT_MSA.3 静的属性初期化
下位階層: なし
依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

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に対して、[選択:制限的、許可的、[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、[割付:その他の特性]]
・*許可的、[割付:その他の特性]*
[割付:その他の特性]
・*なし*
[割付:アクセス制御 SFP、情報フロー制御 SFP]
・*MFD アクセス制御 SFP*

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特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]
・*なし*

④ FMT_MTD.1　TSF データの管理
下位階層:　なし
依存性:　FMT_SMR.1　セキュリティの役割
FMT_SMF.1　管理機能の特定

FMT_MTD.1.1　TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト]
・*表 17 の TSF データの操作リスト*
[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、改変、削除*
[割付: 許可された識別された役割]
・*表 17 の TSF データの操作リストで示された役割*

表 17　TSF データの操作リスト

TSF データ	問い合わせ、改変、削除、作成	役割
機械管理者 ID 情報	*改変*	*機械管理者*
機械管理者パスワード情報	*改変*	*機械管理者*

SA のID 情報	*問い合わせ、改変、削除、作成*	*機械管理者、SA*
SA のパスワード情報	*改変*	*機械管理者、SA*
一般利用者のID 情報	*問い合わせ、改変、削除、作成*	*機械管理者、SA*
一般利用者のパスワード情報	*改変*	*機械管理者、SA、一般利用者*
ユーザー認証方法の情報	*問い合わせ、改変*	*機械管理者、SA*
本体パネルからの認証時のパスワード使用情報	*問い合わせ、改変*	*機械管理者、SA*
ユーザーパスワードの最小文字数情報	*問い合わせ、改変*	*機械管理者、SA*
蓄積プリントの情報	*問い合わせ、改変*	*機械管理者、SA*
システム管理者認証失敗によるアクセス拒否情報	*問い合わせ、改変*	*機械管理者、SA*
セキュリティ監査ログ設定情報	*問い合わせ、改変*	*機械管理者、SA*
内部ネットワークデータ保護情報	*問い合わせ、改変、削除*	*機械管理者、SA*
カストマーエンジニア操作制限情報	*問い合わせ、改変*	*機械管理者、SA*
ハードディスク暗号化情報	*問い合わせ、改変*	*機械管理者、SA*
ハードディスク蓄積データ上書き情報	*問い合わせ、改変*	*機械管理者、SA*
日付、時刻情報	*問い合わせ、改変*	*機械管理者、SA*

⑤ FMT_SMF.1　　管理機能の特定

下位階層:　　なし

依存性:　　なし

FMT_SMF.1.1　　TSF は、以下の管理機能を実行することができなければならない。:
[割付: TSF によって提供される管理機能のリスト]

[割付: TSF によって提供される管理機能のリスト]

・*表 18 に示すTSF によって提供されるセキュリティ管理機能のリスト*

表 18 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	CC で定義された管理対象	TOE の管理機能
FAU_GEN.1	なし	*セキュリティー監査ログ設定情報の管理*
FAU_SAR.1	a) 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	*機械管理者および SA のIDとパスワード情報の管理）*
FAU_SAR.2	なし	-
FAU_STG.1	なし	-
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維	*なし*

	持(削除、改変、追加)。	*理由: 監査記録の制御パラメータは固定であり管理対象にならない*
FCS_CKM.1	なし	-
FCS_COP.1	なし	*・ハードディスク蓄積データ暗号化情報の管理*
FDP_ACC.1	なし	-
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	*なし* *理由: アクセスはユーザ認証情報(ID とパスワード)により管理される*
FDP_RIP.1	a) いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOE において設定可能にされる。	*・ハードディスク蓄積データ上書き情報の管理*
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	*・認証失敗によるアクセス拒否と認証失敗回数の管理*
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	*なし* *理由: 追加のセキュリティ属性はないため管理対象にならない*
FIA_UAU.2	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	*・本体パネルからの認証時のパスワード使用情報* *・機械管理者、SA および一般利用者の ID とパスワード情報の管理*
FIA_UAU.7	なし	-
FIA_UID.2	a) 利用者識別情報の管理。	*・機械管理者、SA および一般利用者の ID とパスワード情報の管理*
FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、サブジェクトのセキュリティ属性を変更できる。	*なし* *理由: アクション、セキュリティ属性は固定であり管理対象にならない*
FMT_MOF.1	a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること	*・カストマーエンジニア操作制限情報の管理*
FMT_MSA.1	a)セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	*なし* *理由: 役割グループは固定であり管理対象にならない*
FMT_MSA.3	a)初期値を特定し得る役割のグループを管理すること; b)所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること; c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	*なし* *理由: 役割グループはシステム管理者だけであり管理対象にならない*
FMT_MTD.1.	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	*・カストマーエンジニア操作制限情報の管理*

FMT_SMF.1	なし	-
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	*なし* *理由: 役割グループは固定であり管理対象にならない*
FPT_STM.1	a) 時間の管理。	*日付、時刻情報の管理*
FTP_TRP.1	a) もしサポートされていれば、高信頼パスを要求するアクションの構成。	*内部ネットワークデータ保護情報の管理*

⑥ FMT_SMR.1 セキュリティの役割
下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割［割付:許可された識別された役割］を維持しなければならない。
[割付: 許可された識別された役割]
・*機械管理者*、*SA*、*一般利用者*

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

6.1.6. クラス FPT: TSF の保護

① FPT_STM.1 高信頼タイムスタンプ
下位階層: なし
依存性: なし

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

6.1.7. クラス FTP: 高信頼パス/チャネル

① FTP_TRP.1 高信頼パス
下位階層: なし
依存性: なし

FTP_TRP.1.1 TSF は、それ自身と［選択:リモート、ローカル］利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、[選択:改変、暴露、[割付:ほかのタイプの完全性、または機密性侵害]]からの通信データの保護を提供する通信パスを提供しなければならない。

[選択:リモート、ローカル]
・*リモート*
[選択:改変、暴露、[割付:ほかのタイプの完全性、または機密性侵害]]
・*改変*、*暴露*、*[割付:ほかのタイプの完全性、または機密性侵害]*
・[割付:ほかのタイプの完全性、または機密性侵害]

・*なし*

FTP_TRP.1.2　TSF は、［選択：TSF、ローカル利用者、リモート利用者］が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択：TSF、ローカル利用者、リモート利用者]
・*リモート利用者*

FTP_TRP.1.3　TSF は、［選択： 最初の利用者認証、[割付：高信頼パスが要求される他のサービス]］に対して、高信頼パスの使用を要求しなければならない。

[選択：最初の利用者認証、[割付：高信頼パスが要求される他のサービス]]
・*TOE の Web による通信サービス、プリンタードライバ用通信サービス、ネットワークユーティリティ用通信サービスおよび高信頼性パスが要求される他のサービス*

6.2. セキュリティ保証要件

表 19 にセキュリティ保証要件を記述する。

本 TOE の評価保証レベルは EAL3 である。 すべての保証要件コンポーネントは、[CC パート 3]で規定されている、EAL3 のコンポーネントを直接引用している。

表 19 EAL3 保証要件

保証要件	セキュリティ保証要件名称	依存性
クラス ADV: 開発		
ADV_ARC.1	セキュリティアーキテクチャ記述	ADV_FSP.1, ADV_TDS.1
ADV_FSP.3	完全な要約を伴う機能仕様	ADV_TDS.1
ADV_TDS.2	アーキテクチャ設計	ADV_FSP.3
クラス AGD: ガイダンス文書		
AGD_OPE.1	利用者操作ガイダンス	ADV_FSP.1
AGD_PRE.1	準備手続き	なし
クラス ALC: ライフサイクルサポート		
ALC_CMC.3	許可の管理	ALC_CMS.1, ALC_DVS.1
ALC_CMS.3	実装表現の CM カバレージ	なし
ALC_DEL.1	配布手続き	なし
ALC_DVS.1	セキュリティ手段の識別	なし
ALC_LCD.1	開発者によるライフサイクルモデルの定義	なし
クラス ASE: セキュリティターゲット評価		
ASE_CCL.1	適合主張	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
ASE_ECD.1	拡張コンポーネント定義	なし

保証要件	セキュリティ保証要件名称	依存性
ASE_INT.1	ST 概説	なし
ASE_OBJ.2	セキュリティ対策方針	ASE_SPD.1
ASE_REQ.2	導き出されたセキュリティ要件	ASE_OBJ.2, ASE_ECD.1
ASE_SPD.1	セキュリティ課題定義	なし
ASE_TSS.1	TOE 要約仕様	ASE_INT.1, ASE_REQ.1
クラス ATE: テスト		
ATE_COV.2	カバレージの分析	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	テスト:基本設計	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
ATE_FUN.1	機能テスト	ATE_COV.1
ATE_IND.2	独立テスト – サンプル	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
クラス AVA: 脆弱性評定		
AVA_VAN.2	脆弱性分析	ADV_ARC.1,ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応を、表 20 に記述する。 この表で示す通り、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対応している。また各セキュリティ対策方針が、セキュリティ機能要件により保証されている根拠を、表 21 に記述する。

表 20 セキュリティ機能要件とセキュリティ対策方針の対応関係

セキュリティ対策方針 / セキュリティ機能要件	O.AUDITS	O.CIPHER	O.COMM_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FAU_GEN.1	○						
FAU_SAR.1	○						
FAU_SAR.2	○						

セキュリティ対策方針 / セキュリティ機能要件	O.AUDITS	O.CIPHER	O.COMM_SEC	O.MANAGE	O.RESIDUAL	O.RESTRICT	O.USER
FAU_STG.1	○						
FAU_STG.4	○						
FCS_CKM.1		○					
FCS_COP.1		○					
FDP_ACC.1							○
FDP_ACF.1							○
FDP_RIP.1					○		
FIA_AFL.1 (1)				○		○	○
FIA_AFL.1 (2)						○	○
FIA_ATD.1							○
FIA_UAU.2				○		○	○
FIA_UAU.7				○		○	○
FIA_UID.2				○		○	○
FIA_USB.1							○
FMT_MOF.1				○			
FMT_MSA.1							○
FMT_MSA.3							○
FMT_MTD.1				○			○
FMT_SMF.1				○			
FMT_SMR.1				○			○
FPT_STM.1	○						
FTP_TRP.1			○				

表 21 セキュリティ対策方針によるセキュリティ機能要件根拠

セキュリティ対策方針	セキュリティ機能要件根拠
O.AUDITS	O.AUDITS は監査イベントの記録機能とセキュリティ監査ログデータを提供する対策方針である。 本セキュリティ対策方針を実現するためには、 FAU_GEN.1 により監査対象イベントに対してセキュリティ監査ログデータが生成される。 （ただし下記の機能要件は示す理由により監査は不要である。

セキュリティ対策方針	セキュリティ機能要件根拠
	・FAU_STG.4：監査ログデータの総件数は固定であり格納、更新は自動的に処理される。 ・FCS_CKM.1,FCS_COP.1：暗号化の失敗はジョブステータスとして監査される FAU_SAR.1 により許可されているシステム管理者は、監査ログファイルからのセキュリティ監査ログデータの読み出し機能を提供する。 FAU_SAR.2 により許可されているシステム管理者以外の監査ログへのアクセスを禁止する。 FAU_STG.1 により監査ログファイルに格納されているセキュリティ監査ログデータを、不正な削除や改変から保護する。 FAU_STG.4 により監査ログが満杯になった時に、最も古いタイムスタンプで格納された監査ログを上書き削除して、新しい監査イベントを、監査ログファイルへ格納する。 FPT_STM.1 により TOE の持つ高信頼なクロックを用いて、監査対象イベントと共にタイムスタンプが監査ログに記録される。 以上のセキュリティ機能要件により O.AUDITS を満たすことができる。
O.CIPHER	O.CIPHER は内部ハードディスク装置に蓄積されている文書データやセキュリティ監査ログデータを取り出しても解析が出来ないように、内部ハードディスク装置上に蓄積されるデータを暗号化する対策方針である。 本セキュリティ対策方針を実現するためには、 FCS_CKM.1 により指定された 128 ビットの暗号鍵長に従って、暗号鍵が生成される。 FCS_COP.1 により決められた暗号アルゴリズムと暗号鍵長で、文書データやセキュリティ監査ログデータを内部ハードディスク装置へ蓄積する時に暗号化され、読み出し時に復合化される。 以上のセキュリティ機能要件により O.CIPHER を満たすことができる。
O.COMM_SEC	O.COMM_SEC は内部ネットワーク上に存在する文書データ、セキュリティ監査ログデータおよび TOE 設定データを、盗聴や改ざんから保護する機能を提供する対策方針である。 本セキュリティ対策方針を実現するためには、 FTP_TRP.1 により TOE とリモート間の内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータおよび TOE 設定データを脅威から保護するために、通信データ暗号化プロトコルに対応することで、高信頼パスを提供することが出来る。 以上のセキュリティ機能要件により O.COMM_SEC を満たすことができる。
O.MANAGE	O.MANAGE はセキュリティ機能の設定を行うシステム管理者モードのアクセスを、認証されたシステム管理者のみ許可して、一般利用者による TOE 設定データへのアクセスを、不可能にする対策方針である。 本セキュリティ対策方針を実現するためには、 FIA_AFL.1（1）によりシステム管理者認証の認証失敗時に、認証失敗によるアクセス拒否回数分の認証に失敗した場合、電源 OFF/ON が必要になり、連続した攻撃を防ぐ。

セキュリティ対策方針	セキュリティ機能要件根拠
	FIA_UAU.2、FIA_UID.2 により正当なシステム管理者と一般利用者を識別するために、ユーザー認証が行われる。 FIA_UAU.7 によりユーザー認証に関して認証フィードバックは保護されるので、パスワードの漏洩は防げる。 FMT_MOF.1 によりセキュリティ機能の動作や停止、および機能の設定は、システム管理者だけに限定しているので、システム管理者だけに制限される。 FMT_MTD.1 によりセキュリティ機能の機能設定は、システム管理者だけに限定しているので、TSF データの問い合わせ、改変、作成は、システム管理者だけに制限される。 FMT_SMF.1 により TOE セキュリティ機能の管理機能の設定を、システム管理者へ提供する。 FMT_SMR.1 により特権を持つ利用者として、システム管理者の役割を維持することで、セキュリティに関する役割をシステム管理者に特定する。 以上のセキュリティ機能要件により O.MANAGE を満たすことができる。
O.RESIDUAL	O.RESIDUAL は内部ハードディスク装置に蓄積される利用済み文書データの再生および復元を、不可能にする対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_RIP.1 により内部ハードディスク装置に蓄積された利用済み文書データの、以前の情報の内容を利用できなくする。 以上のセキュリティ機能要件により O.RESIDUAL を満たすことができる。
O.RESTRICT	O.RESTRICT は許可されていない者への TOE の利用を制限する機能を持つ対策方針である。 本セキュリティ対策方針を実現するためには、 FIA_AFL.1（1）によりシステム管理者認証の認証失敗時に、認証失敗によるアクセス拒否回数分の認証に失敗した場合、電源 OFF/ON が必要になり、連続した攻撃を防ぐ。 FIA_AFL.1 (2)によりユーザー認証時の認証失敗時に、“パスワードが正しくない”旨のメッセージを表示して、パスワードの再入力を要求する。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者およびシステム管理者を識別するために、ユーザー認証が行われる。 FIA_UAU.7 によりユーザー認証に関して認証フィードバックは保護されるので、パスワードの漏洩は防げる。 以上のセキュリティ機能要件により O.RESTRICT を満たすことができる。
O.USER	O.USER は正当な TOE の利用者を識別し、正当な利用者に文書データの登録、取り出し、削除、パスワードの変更機能を利用者へ提供する対策方針である。 本セキュリティ対策方針を実現するためには、 FDP_ACC.1 FDP_ACF.1 によりユーザー認証を実施することで、許可された利用者のみに、オブジェクトの操作を許可する。 FIA_AFL.1（1）によりシステム管理者認証の認証失敗時に、認証失敗によるア

セキュリティ対策方針	セキュリティ機能要件根拠
	クセス拒否回数分の認証に失敗した場合、電源 OFF/ON が必要になり、連続した攻撃を防ぐ。 FIA_AFL.1 (2)によりユーザー認証時の認証失敗時に、“パスワードが正しくない”旨のメッセージを表示して、パスワードの再入力を要求する。 FIA_ATD.1、 FIA_USB.1 により機械管理者役割、SA 役割、一般利用者役割を維持することにより、許可された利用者のみにサブジェクトを割り当てる。 FIA_UAU.2、FIA_UID.2 により正当な一般利用者およびシステム管理者を識別するために、ユーザー認証が行われる。 FIA_UAU.7 によりユーザー認証に関して認証フィードバックは保護されるので、パスワードの漏洩は防げる。 FMT_MSA.1 によりセキュリティ属性の問い合わせ、改変、削除、作成を管理する。 FMT_MSA.3 により適切なデフォルト値を管理する。 FMT_MTD.1 により機械管理者のパスワード設定は機械管理者に、SA のパスワード設定は機械管理者と SA に、一般利用者のパスワード設定は、システム管理者と一般利用者本人に制限される。 FMT_SMR.1 によりシステム管理者、一般利用者の役割は維持されて、その役割が関連付けられる。 以上のセキュリティ機能要件により O.USER を満たすことができる。

6.3.2. 依存性の検証

セキュリティ機能要件が依存している機能要件、および依存関係を満足しない機能要件と、依存関係が満たされなくても問題がない根拠を、表 22 に記述する。

表 22 セキュリティ機能要件コンポーネントの依存性

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FAU_GEN.1 監査データ生成	FPT_STM.1	—
FAU_SAR.1 監査レビュー	FAU_GEN.1	—
FAU_SAR.2 限定監査レビュー	FAU_SAR.1	—
FAU_STG.1 保護された監査証跡格納	FAU_GEN.1	—
FAU_STG.4 監査データ損失の防止	FAU_STG.1	—

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FCS_CKM.1 暗号鍵生成 （HDD 蓄積データ）	FCS_COP.1	FCS_CKM.4: 暗号鍵は MFD の起動時に生成され、DRAM（揮発性メモリ）に格納される。 この暗号鍵は MFD 本体の電源を切断すると消滅するので、暗号鍵を破棄する必要性がない。
FCS_COP.1 暗号操作 （HDD 蓄積データ）	FCS_CKM.1	FCS_CKM.4: 暗号鍵は MFD の起動時に生成され、DRAM（揮発性メモリ）に格納される。 この暗号鍵は MFD 本体の電源を切断すると消滅するので、暗号鍵を破棄する必要性がない。
FDP_ACC.1 サブセットアクセス制御	FDP_ACF.1	—
FDP_ACF.1 セキュリティ属性によるアクセス制御	FDP_ACC.1 FMT_MSA.3	—:
FDP_RIP.1 サブセット残存情報保護	なし	
FIA_AFL.1（1） 認証失敗時の取り扱い （システム管理者）	FIA_UAU.2	FIA_UAU.1: FIA_UAU.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FIA_AFL.1 (2) 認証失敗時の取り扱い （一般利用者）	FIA_UAU.2	FIA_UAU.1: FIA_UAU.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FIA_ATD.1 利用者属性定義	なし	
FIA_UAU.2 アクション前の利用者認証	FIA_UID.2	FIA_UID.1: FIA_UID.2 は FIA_UID.1 の上位階層の機能要件のため、FIA_UID.1 への依存性は満たされる。
FIA_UAU.7 保護されたフィードバック	FIA_UAU.2	FIA_UAU.1: FIA_UAU.2 は FIA_UAU.1 の上位階層の機能要件のため、FIA_UAU.1 への依存性は満たされる。
FIA_UID.2 アクション前の利用者識別	なし	
FIA_USB.1 利用者・サブジェクト結合	FIA_ATD.1	—
FMT_MOF.1 セキュリティ機能のふるまいの管理	FMT_SMF.1 FMT_SMR.1	—

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件および要件名称	満足している要件	依存性を満足していない要件とその正当性
FMT_MSA.1 セキュリティ属性の管理	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	—
FMT_MSA.3 静的属性初期化	FMT_MSA.1 FMT_SMR.1	—
FMT_MTD.1 TSF データの管理	FMT_SMF.1 FMT_SMR.1	—
FMT_SMF.1 管理機能の特定	なし	
FMT_SMR.1 セキュリティ役割	FIA_UID.2	FIA_UID.1: FIA_UID.2 は FIA_UID.1 の上位階層の機能要件のため、FIA_UID.1 への依存性は満たされる。
FPT_STM.1 高信頼タイムスタンプ	なし	
FTP_TRP.1 高信頼パス	なし	

6.3.3. セキュリティ保証要件根拠

本 TOE はデジタル複合機である、商用の製品である。 低レベルの攻撃力を持つ攻撃者による、操作パネルおよびシステム管理者クライアントの Web ブラウザから TOE の外部インタフェースを使用した攻撃、または内部ネットワーク上に存在するデータの盗聴や改ざん、市販ツール等の接続による内部ハードディスク装置の情報を読み出そうとすることが想定される。

これらに対して本 TOE は安全性を確保するためのセキュリティ機能を提供する必要がある。

EAL3 は TOE における開発段階のセキュリティ対策の分析(系統だったテストの実施と分析、及び開発環境や開発生産物の管理状況の評価)を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報が含まれていることの分析が含まれるので妥当な選択であるといえる。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。

7.1. セキュリティ機能

表 23 に TOE セキュリティ機能とセキュリティ機能要件の対応を示す。
本節で説明する TOE セキュリティ機能は 6.1 節に記述されるセキュリティ機能要件を満たすものである。

表 23 TOE セキュリティ機能とセキュリティ機能要件の対応関係

セキュリティ機能 / セキュリティ機能要件	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT
FAU_GEN.1						○	
FAU_SAR.1						○	
FAU_SAR.2						○	
FAU_STG.1						○	
FAU_STG.4						○	
FCS_CKM.1		○					
FCS_COP.1		○					
FDP_ACC.1			○				
FDP_ACF.1			○				
FDP_RIP.1	○						
FIA_AFL.1 (1)			○				
FIA_AFL.1 (2)			○				
FIA_ATD.1			○				
FIA_UAU.2			○				
FIA_UAU.7			○				
FIA_UID.2			○				
FIA_USB.1			○				
FMT_MOF.1				○	○		
FMT_MSA.1			○	○			
FMT_MSA.3				○			
FMT_MTD.1			○	○	○		
FMT_SMF.1				○	○		
FMT_SMR.1			○	○	○		
FPT_STM.1						○	

セキュリティ機能 / セキュリティ機能要件	TSF_IOW	TSF_CIPHER	TSF_USER_AUTH	TSF_FMT	TSF_CE_LIMIT	TSF_FAU	TSF_NET_PROT
FTP_TRP.1							O

以下では各 TOE セキュリティ機能に関して概要と対応するセキュリティ機能要件について説明する。

7.1.1. ハードディスク蓄積データ上書き消去機能（TSF_IOW）

ハードディスク蓄積データ上書き消去機能は、システム管理者によりシステム管理者モードで設定された「ハードディスク蓄積データ上書き消去機能設定」に従い、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能の各ジョブの完了後に、内部ハードディスク装置に蓄積された利用済み文書データに対して、内部ハードディスク装置の文書データ領域を、1 回または 3 回の上書きにより消去する。これは複合機の使用環境に応じて、処理の効率性を優先する場合と、セキュリティ強度を優先する場合を考慮しているためである。

処理の効率性を優先する場合は、上書き消去の回数を1回とし、セキュリティ強度を優先する場合は、上書き消去の回数を 3 回とする。 3 回の上書き消去回数は、1回に比べて処理速度は低下するが、より強固な上書き消去回数（推奨値）である。

さらに、システム管理者が設定した時刻に蓄積文書を削除して上書き消去する（時刻指定文書削除機能）。

（1） FDP_RIP.1 サブセット残存情報保護

TOE は各ジョブ完了後の上書き消去機能の制御として、上書き回数 1 回（”0（ゼロ）”による上書き）と、3 回（乱数・乱数・”0（ゼロ）”による上書き）の選択が出来る。

また内部ハードディスク装置上に、上書き消去予定の利用済み文書データの一覧を持ち、TOE 起動時に一覧をチェックして、消去未了の利用済み文書データが存在する場合は、上書き消去処理を実行する。

7.1.2. ハードディスク蓄積データ暗号化機能（TSF_CIPHER）

ハードディスク蓄積データ暗号化機能は、システム管理者によりシステム管理者モードで設定された「ハードディスク蓄積データ暗号化機能設定」に従い、コピー機能、プリンター機能、スキャナー機能、ネットワークスキャン機能動作時や各種機能設定時に内部ハードディスク装置に蓄積される文書データやセキュリティ監査ログデータの暗号化を行う。

(1) FCS_CKM.1 暗号鍵生成

TOE はシステム管理者により設定された「ハードディスク蓄積データ暗号化キー」を使用し、起動時に富士ゼロックス標準の FXOSENC 方式アルゴリズムによって 128 ビットの暗号鍵生成を行う（「ハードディスク蓄積データ暗号化キー」が同じであれば、同じ暗号鍵が生成される）。なお FXOSENC 方式アルゴリズムは、十分

な複雑性を持ったセキュアなアルゴリズムである。

(2) FCS_COP.1 暗号操作

TOE は内部ハードディスク装置に文書データおよびセキュリティ監査ログデータを蓄積する際に、起動時に暗号鍵生成(FCS_CKM.1)により生成した 128 ビット長の暗号鍵と FIPS PUB 197 に基づく AES アルゴリズムとにより文書データおよびセキュリティ監査ログデータの暗号化を行う。 また蓄積した文書データおよびセキュリティ監査ログデータを読み出す場合も同様に、起動時に生成した 128 ビット長の暗号鍵と AES アルゴリズムにより復号化を行う。

7.1.3. ユーザー認証機能（TSF_USER_AUTH）

ユーザー認証機能は、許可された特定の利用者だけに MFD の機能を使用する権限を持たせるために、操作パネルまたは利用者クライアントのプリンタードライバ、ネットワークスキャナーユーティリティ、CWIS からユーザーID とユーザーパスワードを入力させて識別認証する機能である。

認証が成功した利用者のみが下記の機能を使用可能となる。

① 本体操作パネルで制御される機能

コピー機能、スキャン機能、ネットワークスキャン機能、親展ボックス操作機能、プリンター機能（プリンタードライバでのユーザーID とユーザーパスワードの設定が条件であり印刷時に操作パネルで認証する）

②利用者クライアントのネットワークスキャナーユーティリティで制御される機能

親展ボックスからの文書データ取出し機能

③CWIS で制御される機能

機械状態の表示、ジョブ状態・履歴の表示、親展ボックスからの文書データ取出し機能、ファイル指定によるプリント機能

また本機能は操作パネルおよびシステム管理者クライアントから TOE セキュリティ機能の参照と設定変更を行う権限を持たせるためにシステム管理者 ID とパスワードを入力させて識別認証するものでもある。

（1） FIA_AFL.1（1） 認証失敗時の取り扱い

TOE はシステム管理者モードへアクセスする前に、システム管理者の認証を行うが、認証時の認証失敗対応機能を提供している。システム管理者 ID 認証失敗を検出し、アクセス拒否回数で設定されている 5 回の連続失敗に達すると、操作パネルでは電源切断/投入以外の操作は受け付けなくなり、Web ブラウザでも MFD 本体の電源の切断/投入まで認証操作は受け付けなくなる。

（2） FIA_AFL.1（2） 認証失敗時の取り扱い

TOE は MFD の機能を使用する前に、一般利用者のユーザー認証を行うが、正当な一般利用者が設定したパスワードと一致しない場合、操作パネルでは”認証が不成功の”旨のメッセージを表示してユーザー情報の再入力を要求する。

また Web ブラウザやネットワークスキャナーユーティリティではユーザー情報の再入力を要求する。

（3） FIA_ATD.1 利用者属性定義

TOE は機械管理者、SA および一般利用者の役割を定義し維持する。

（4） FIA_UAU.2 アクション前の利用者認証

TOE は操作パネルおよび利用者クライアントの Web ブラウザを通じて CWIS 機能の操作を許可する前に、パスワードを入力させて、入力されたパスワードが、TOE 設定データに登録されているパスワード情報と一致することを検証する。 本認証と識別（FIA_UID.2）は、同時に実行され識別・認証の両方が成功した時のみ操作が許可される。

（5） FIA_UAU.7 保護されたフィードバック

TOE はユーザー認証時に、パスワードを隠すために、パスワードとして入力された文字数と同数の`*`文字を、操作パネルや Web ブラウザに表示する機能を提供する。

（6） FIA_UID.2 アクション前の利用者識別

TOE は操作パネルおよび利用者クライアントの Web ブラウザを通じて CWIS 機能の操作を許可する前に、ユーザーID を入力させて、入力されたユーザーID が、TOE 設定に登録されているユーザーID 情報と一致することを検証する。 本識別と認証（FIA_UAU.2）は、同時に実行され識別・認証の両方が成功した時のみ操作が許可される。

（7） FIA_USB.1 利用者・サブジェクト結合

TOE は認証された ID から機械管理者、SA および一般利用者の役割をサブジェクトに割り当てる。

（8） FMT_MSA.1 セキュリティ属性の管理

TOE は表 24 の通り個別親展ボックス、蓄積プリントに対応する識別情報の操作をユーザー認証機能により認証された利用者に制限する。

表 24 セキュリティ属性の管理

セキュリティ属性	問い合わせ、改変、削除、作成	役割
機械管理者識別情報	改変	機械管理者
SA識別情報	問い合わせ、改変、削除、作成	機械管理者、SA
一般利用者識別情報	問い合わせ、改変、削除、作成	機械管理者、SA
個別親展ボックスに対応する所有者識別情報	問い合わせ、削除、作成	一般利用者、SA
すべての個別親展ボックスに対応する所有者識別情報	問い合わせ、削除	機械管理者
共用親展ボックスに対応する所有者識別情報	問い合わせ、削除、作成	機械管理者
蓄積プリントに対応する識別情報	問い合わせ、削除	機械管理者、SA、一般利用者
すべての蓄積プリントに対応する識別情報	問い合わせ、削除	機械管理者、SA

（9） FMT_MTD.1 TSF データの管理

TOE は認証された正当な利用者のみに、パスワードを設定するユーザーインタフェースを提供する。機械管理者のパスワード設定は機械管理者に、SA のパスワード設定は機械管理者と SA に、一般利用者のパスワード設定は、システム管理者と一般利用者本人に制限される。

（10） FMT_SMR.1 セキュリティ役割

TOE はシステム管理者および一般利用者の役割を維持し、その役割を正当な利用者に関連付けている。

（11） FDP_ACC.1 サブセットアクセス制御
FDP_ACF.1セキュリティ属性によるアクセス制御

TOE は表 25 に示すとおり、ユーザー認証機能により親展ボックス、蓄積プリント（プライベートプリント）の操作を認証された利用者に制限する。

表 25 アクセス制御

	個別親展ボックス	共用親展ボックス	蓄積プリント
ボックスの作成	一般利用者、SA が可能	機械管理者が可能	-
ボックスの削除	登録した一般利用者、SA と機械管理者が可能	機械管理者が可能	-
文書の登録、取り出し、削除	登録した一般利用者、SA と機械管理者が可能	一般利用者、SA と機械管理者が可能	一般利用者、SA と機械管理者が可能
すべての文書の取り出し、削除	機械管理者が可能	機械管理者が可能	SA と機械管理者が可能

親展ボックスや蓄積プリントへアクセスする前に、ユーザー認証を実施する。

- 蓄積プリント機能

MFD で「認証成功のジョブをプライベートプリントに保存」の設定を行うと、利用者が利用者クライアントのプリンタードライバからユーザーID とパスワードを設定した状態でプリント指示をする場合、MFD は内部に登録されたユーザーID とパスワードが一致するかをチェックし、一致した場合のみ印刷データをビットマップデータに変換（デコンポーズ）してプライベートプリントとしてユーザーID ごとに区分して内部ハードディスク装置に一時蓄積する。

またCWIS からユーザーID とパスワードを入力し、認証後に利用者クライアント内のファイル指定によりプリント指示をする場合も同様にユーザーID ごとのプライベートプリントとして内部ハードディスク装置に一時蓄積される。

利用者は一時蓄積されたプリントデータを確認するために、MFD の操作パネルからユーザーID とパスワードを入力し、認証されるとユーザーID に対応したプリント待ちのリストだけが表示される。利用者はこのリストから印刷指示、または削除の指示が可能となる。

- 親展ボックス操作機能

図 3 には図示されていない IIT から親展ボックスにコピーデータおよびスキャンデータを格納することが可能である。

コピーデータおよびスキャンデータを親展ボックスに格納するには、利用者が MFD の操作パネルからユーザーIDとユーザーパスワードを入力させて、認証されるとコピー機能およびスキャン機能の利用が可能になり、操作パネルからコピー蓄積またはスキャン指示をすることにより IIT が原稿を読み取り、内部ハードディスク装置に蓄積する。

登録されたユーザーID ごとの個別親展ボックスは、利用者が操作パネル、CWIS またはネットワークスキャナーユーティリティからユーザーIDとパスワードを入力するとMFDは内部に登録されたユーザーIDとパスワードが一致するかをチェックし、一致した場合のみ認証が成功しボックス内のデータを確認することが可能となり、取出し（スキャンデータのみ）や印刷、削除の操作が可能となる。

①一般利用者、SA による親展ボックスの操作

・個別親展ボックスの作成

一般利用者、SA が、個別親展ボックスの作成操作を行うと、個別親展ボックスの所有者識別情報に、個別親展ボックスを作成した一般利用者識別情報、SA 識別情報が設定された個別親展ボックスが作成される。

・個別親展ボックスの削除

個別親展ボックスの所有者識別情報と、一般利用者識別情報、SA 識別情報が一致した場合、その個別親展ボックスに関する、個別親展ボックスの削除の操作が許可される。

・個別親展ボックスの文書データの登録、文書データの取り出し、文書データの削除

個別親展ボックスの所有者識別情報と、一般利用者識別情報、SA 識別情報が一致した場合、その個別親展ボックスに関する、文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。

・共用親展ボックスの文書データの登録、文書データの取り出し、文書データの削除

親展ボックスが、共用親展ボックスの場合、その共用親展ボックスに関する、文書データの登録、文書データの取り出し、文書データの削除の操作が許可される。

②一般利用者、SA による蓄積プリントの操作

・文書データの登録

文書データの登録の操作を行うと、一般利用者、SA が持つ一般利用者識別情報を、その蓄積プリントの所有者識別情報に設定した蓄積プリントが作成され、その蓄積プリントに文書データが登録される。

・文書データの削除、文書データの取り出し

蓄積プリントの所有者識別情報と、一般利用者識別情報、SA 識別情報が一致した場合、一般利用者プロセス、SA プロセスに対して、その蓄積プリントに関する、文書データの取り出し、文書データの削除の操作が許可される。文書データの削除の操作が行われると、その蓄積プリントも削除される。

③機械管理者による親展ボックスの操作

機械管理者の場合、共用親展ボックスの作成操作、すべての親展ボックスに対する親展ボックスの削除、文書データの登録、文書データの削除、文書データの取り出しの操作を許可する。

④機械管理者、SA による蓄積プリントの操作

・機械管理者および SA の場合、すべての蓄積プリントに対し文書データの削除、文書データの取り出しを許可する。

7.1.4. システム管理者セキュリティ管理機能（TSF_FMT）

システム管理者セキュリティ管理機能は、ある特定の利用者へ特別な権限を持たせるために、システム管理者モードへのアクセスをシステム管理者のみに制限して、許可されたシステム管理者のみに操作パネルおよびシステム管理者クライアントから TOE セキュリティ機能の参照と設定変更を行う権限を許可する。

（1）FMT_MOF.1 セキュリティ機能のふるまいの管理
FMT_MTD.1 TSF データの管理
FMT_SMF.1 管理機能の特定

TOE は認証されたシステム管理者のみに、下記の TOE セキュリティ機能に関係する TOE 設定データの参照と設定変更、および各機能の有効/無効を設定するユーザーインタフェースを提供する。
またこれらの機能により、要求されるセキュリティ管理機能を提供する。

操作パネルからは下記の TOE セキュリティ機能の設定を参照し、設定変更を行うことが可能である。

- ハードディスク蓄積データ上書き消去機能の設定を参照し、有効/無効、上書き回数の設定を行う
- ハードディスク蓄積データ暗号化機能の設定を参照し、有効/無効の設定を行う
- ハードディスク蓄積データ暗号化キーの設定を行う
- 本体パネルからの認証時のパスワード使用の設定を参照し、有効/無効の設定を行う
- システム管理者認証失敗によるアクセス拒否設定を参照し、有効/無効、拒否回数の設定を行う
- 機械管理者 ID とパスワードの設定を行う（機械管理者のみ可能）
- SA、一般利用者 ID の設定を参照し ID とパスワードの設定を行う
- システム管理者認証失敗によるアクセス拒否設定を参照し有効/無効、拒否回数の設定を行う
- ユーザーパスワード（一般利用者と SA）の最小文字数制限を参照し設定を行う
- 内部ネットワークデータ保護機能の SSL/TLS 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能の IPSec 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能の S/MIME 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 時刻指定文書削除機能の設定を参照し、有効/無効および削除時刻の設定を行う
- ユーザー認証機能の設定を参照し、ローカル認証/無効の設定を行う
- 蓄積プリント機能の設定を参照し、蓄積/印刷の設定を行う
- 日付、時刻を参照し設定を行う

またシステム管理者クライアントから Web ブラウザを通じて CWIS 機能により、下記の TOE セキュリティ機能の設定を参照し、設定変更を行うことが可能である

- 機械管理者 ID とパスワードの設定を行う（機械管理者のみ可能）
- SA、一般利用者の ID 設定を参照し、ID とパスワードの設定を行う
- システム管理者認証失敗によるアクセス拒否設定を参照し、有効/無効、拒否回数の設定を行う
- ユーザーパスワード（一般利用者と SA）の最小文字数制限を参照し設定を行う
- セキュリティ監査ログ機能の設定を参照し有効/無効の設定を行う

（有効時は、監査ログをタブ区切りのテキストファイルで、システム管理者クライアント PC 上にダウンロードすること

が可能。）

- 内部ネットワークデータ保護機能の SSL/TLS 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能の IPSec 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- 内部ネットワークデータ保護機能の SNMPv3 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- SNMPv3 認証パスワードの設定を行う
- 内部ネットワークデータ保護機能の S/MIME 通信の設定を参照し、有効/無効および詳細情報の設定を行う
- X.509 証明書を作成/アップロード/ダウンロードする
- 時刻指定文書削除機能の設定を参照し、有効/無効および削除時刻の設定を行う
- ユーザー認証機能の設定を参照し、ローカル認証/無効の設定を行う

（2） FMT_MSA.1 セキュリティ属性の管理
TOE はシステム管理者のみに一般利用者識別情報の操作を限定する。

（3） FMT_MSA.3 静的属性初期化
TOE は適切なデフォルト値を提供する。

（4） FMT_SMR.1 セキュリティ役割
TOE はシステム管理者の役割を維持し、その役割をシステム管理者に関連付けている。

7.1.5. カストマーエンジニア操作制限機能（TSF_CE_LIMIT）

カストマーエンジニア操作制限機能は、カストマーエンジニアがシステム管理者セキュリティ管理機能（TSF_FMT）に関する設定の参照および変更が出来ないようにカストマーエンジニアのシステム管理者モードへの操作を制限する機能である。
この機能により、カストマーエンジニアのなりすましによる設定変更が出来なくなる。

（1）FMT_MOF.1 セキュリティ機能のふるまいの管理
FMT_MTD.1 TSF データの管理
FMT_SMF.1 管理機能の特定
TOE は認証されたシステム管理者のみに、操作パネルと CWIS からカストマーエンジニア操作制限機能に関する TOE 設定データの参照と設定変更（機能の有効/無効）のためのユーザーインタフェースを提供する。
またこの機能により要求されるセキュリティ管理機能を提供する。

（2） FMT_SMR.1 セキュリティ役割
TOE はシステム管理者の役割を維持し、その役割をシステム管理者に関連付けている。

7.1.6. セキュリティ監査ログ機能（TSF_FAU）

セキュリティ監査ログ機能は、システム管理者によりシステム管理者モードで設定された「監査ログ設定」に従い、すべての TOE 利用者に対して、いつ、誰が、どのような作業を行ったかという事象や重要なイベント（例えば障害や構成変更、ユーザ操作など）を、追跡記録するためのセキュリティ監査ログ機能を提供する。

（1） FAU_GEN.1 監査データ生成
監査データの生成は、定義された監査対象イベントが、監査ログに記録されることを保証する。
表 26 に監査ログデータの詳細を示す

表 26 監査ログのデータ詳細

監査ログ対象イベントは、以下の固定長データと共に記録される。:
- Log ID：監査ログ識別子としての通し番号（1～60000）
- Date：日付データ（yyyy/mm/dd, mm/dd/yyyy, dd/mm/yyyy のいずれか）
- Time：時刻データ（hh:mm:ss）
- Logged Events：イベント名称（最大 32 桁の任意文字列）
- User Name：利用者名（最大 32 桁の任意文字列）
- Description：イベントに関する内容の説明（最大 32 桁の任意文字列で詳細は下記参照のこと）
- Status：イベントの処理結果もしくは状態（最大 32 桁の任意文字列で詳細は下記参照のこと）
- Optionally Logged Items：共通保存項目以外に監査ログへ保存される追加情報

Logged Events	Description	Status
デバイスの状態変化		
System Status	Started normally(cold boot)	-
	Started normally(warm boot)	
	Shutdown requested	
	User operation(Local)	Start/End
	Scheduled Image Overwriting started	Successful/Failed
	Scheduled Image Overwriting finished	Successful/Failed
ユーザー認証		
Login/Logout	Login(Local Access)	Successful, Failed(Invalid UserID), Failed(Invalid Password), Failed
	Logout	
	Locked System Administrator Authentication	-
	Detected continuous Auhtentication Fail	（失敗回数も保存）
監査ポリシー変更		

Logged Events	Description	Status
Audit Policy	Audit Log	Enable/Disable
ジョブステータス		
Job Status	Print	Completed, Completed with Warnings, Canceled by User, Canceled by Shutdown, Aborted, Unknown
	Copy	
	Scan	
	Mailbox	
	Print Reports	
	Job Flow Service	
デバイス設定変更		
Device Settings	Adjust Time	Successful/Failed
	Create Mailbox	
	Delete Mailbox	
	Switch Authentication Mode	Successful (設定項目も保存)
	Change Security Setting	
デバイス格納データへのアクセス		
Device Data	Import Certificate	Successful/Failed
	Delete Certificate	
	Add Address Entry	
	Delete Address Entry	
	Edit Address Entry	
	Export Audit Log	

（2）FAU_SAR.1 監査レビュー
監査ログに記録されたすべての情報を、読み出せることを保証する。

また”テキストファイルとして保存する”という名称のボタンがあり、この機能によりセキュリティ監査ログデータを、タブ区切りのテキストファイルとして、ダウンロードすることが出来る。 セキュリティ監査ログデータをダウンロードする時は、Web ブラウザを利用する前に、SSL/TLS 通信を有効に設定されていなければならない。

（3）FAU_SAR.2 限定監査レビュー
監査ログの読み出しを、認証されたシステム管理者のみに限定する。
監査ログへのアクセスは、システム管理者が Web ブラウザのみ使用可能で、操作パネルからアクセスすることは出来ない。 システム管理者が Web ブラウザを通して TOE へログインしていなければ、システム管理者の認証（ログイン）後に使用可能になる。

（4）FAU_STG.1 保護された監査証跡格納
監査ログの削除機能は存在しなく、不正な改ざんや改変から保護されている。

（5）FAU_STG.4 監査データ損失の防止

監査ログが満杯になった時、最も古いタイムスタンプで記録された監査データに上書きして、新しい監査データが損失することなく記録される。
監査ログ対象のイベントは、タイムスタンプと共に NVRAM に保存され 50 件に達した場合、NVRAM 上のログを 50 件単位で一つのファイル（以下、「監査ログファイル」と呼ぶ）として、内部ハードディスク装置へ保存をして、最大 15,000 件のイベントを保存することが出来る。 15,000 件を超える場合は、一番古いタイムスタンプで記録された監査ログファイルから順次消去して、繰り返してイベントが記録される。

（6）FPT_STM.1 高信頼タイムスタンプ
定義された監査対象イベントを監査ログファイルへ記録する時に、TOE が持っているクロック機能によるタイムスタンプを発行する機能を提供する。
時計の設定変更は TSF_FMT によりシステム管理者のみが可能である。

7.1.7. 内部ネットワークデータ保護機能（TSF_NET_PROT）

内部ネットワークデータ保護機能は、システム管理者によりシステム管理者モードで設定された下記 4 つのプロトコル設定の定義により、内部ネットワークデータ保護機能が提供される。

（1）FTP_TRP.1 高信頼パス
TOE とリモート間（Web による通信サービス、プリンタードライバ用通信サービス、ネットワークユーティリティ用通信サービスおよび高信頼性パスが要求される他のサービス）でセキュアなデータ通信が保証される暗号化通信プロトコルによる、文書データ、セキュリティ監査ログデータおよび TOE 設定データを保護する機能を提供する。 この高信頼パスは、他の通信パスと論理的に区別され、その端点の保証された識別および改変や暴露から、通信データを保護する能力を持っている。

① SSL/TLS プロトコル
システム管理者によりシステム管理者モードで設定された「SSL/TLS 通信」に従い、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータや TOE 設定データを保護する一つとして、セキュアなデータ通信が保証される、SSL/TLS プロトコルに対応している。
TOE が対応する機能により、SSL/TLS サーバまたは SSL/TLS クライアントとして動作することが出来る。また SSL/TLS プロトコルに対応することにより、本 TOE とリモート間のデータ通信は、盗聴や改ざんの両方から保護することが出来る。 盗聴からの保護は、下記の機能により通信データを暗号化することによって実現する。 なお暗号鍵はセションの開始時に生成され、MFD 本体の電源を切断するか、またはセションの終了と同時に消滅する。

・ SSLv3/TLSv1 プロトコルとして生成される接続毎の暗号鍵
具体的には、下記の暗号化スイートの何れかが選択される。

SSL/TLS の暗号化スイート	共通鍵暗号方式/鍵サイズ	ハッシュ方式
SSL_RSA_WITH_RC4_128_SHA	RC4/128 ビット	SHA1
SSL_RSA_WITH_3DES_EDE_CBC_SHA	3Key Triple-DES/168 ビット	SHA1
TLS_RSA_WITH_AES_128_CBC_SHA	AES/128 ビット	SHA1
TLS_RSA_WITH_AES_256_CBC_SHA	AES/256 ビット	SHA1

また改ざんからの保護は、SSL/TLS 記録転送プロトコルの HMAC（Hashed Message Authentication Code － IETF RFC2104）機能を使用する事によって実現する。

Web クライアント上で SSL/TLS 通信を有効にすると、クライアントからの要求は HTTPS を通して、受信しなければならない。 SSL/TLS 通信は、IPsec、SNMPv3 、S/MIME をセットアップする前、またはシステム管理者がセキュリティ監査ログデータをダウンロードする前に有効に設定されていなければならない。

② IPSec プロトコル

システム管理者によりシステム管理者モードで設定された「IPSec 通信」に従い、内部ネットワーク上を流れる文書データ、セキュリティ監査ログデータや TOE 設定データを保護する一つとして、セキュアなデータ通信が保証される、IPSec プロトコルに対応している。

IPSec プロトコルは、TOE とリモート間でどのような IPSec 通信を行うかといった、秘密鍵や暗号アルゴリズムなどのパラメータを定義するための、セキュリティアソシエーションの確立をする。 アソシエーションの確立後、指定された特定の IP アドレス間の全ての通信データは、TOE の電源 OFF またはリセットされるまで IPSec のトランスポートモードにより暗号化される。 なお暗号鍵はセションの開始時に生成され、MFD 本体の電源を切断するか、またはセションの終了と同時に消滅する。

・IPSec プロトコル（ESP:Encapsulating Security Payload）として生成される接続毎の暗号鍵
具体的には、下記の共通鍵暗号方式とハッシュ方式の組み合わせの何れかが選択される。

共通鍵暗号方式/鍵サイズ	ハッシュ方式
AES/128 ビット	SHA1
3Key Triple-DES/168 ビット	SHA1

③ SNMPv3 プロトコル

システム管理者によりシステム管理者モードで設定された「SNMPv3 通信」に従い、ネットワーク管理プロトコルの SNMP を利用する時の、セキュリティソリューションの一つとして、SNMPv3 プロトコルに対応している。SNMPv3 プロトコルは IETF RFC3414 で規定されているように、データの暗号化のみならず、各 SNMP メッセージを認証するために使用される。

この機能を使用する時は、認証パスワードとプライバシー（暗号化）パスワードの両方を、TOE とリモートサーバの両方にセットアップしなければならない。 またパスワードは共に 8 文字以上で運用しなければならない。SNMPv3 の認証は SHA-1 ハッシュ関数を使用し、また暗号化は CBC -DES を使用する。 なお暗号鍵はセションの開始時に生成され、MFD 本体の電源を切断するか、またはセションの終了と同時に消滅する。

・SNMPv3 プロトコルとして生成される接続毎の暗号鍵

共通鍵暗号方式/鍵サイズ	ハッシュ方式
DES/56 ビット	SHA1

④ S/MIME プロトコル

システム管理者によりシステム管理者モードで設定された「S/MIME 通信」に従い、内部ネットワークおよび外部ネットワーク上を流れる文書データを保護する一つとして、セキュアなメール通信が保証される、S/MIME プロトコルに対応している。

S/MIME 暗号メールの送受信機能により、外部と電子メールで通信する場合のメール転送経路上での文書データの盗聴を、またS/MIME 署名メールの送受信機能により、文書データの盗聴や改竄を防止する。
なお暗号鍵はメールの暗号化開始時に生成され、MFD 本体の電源を切断するか、またはメールの暗号化完了と同時に消滅する。

・S/MIME プロトコルとして生成されるメール毎の暗号鍵

具体的には、下記の共通鍵暗号方式とハッシュ方式の組み合わせの何れかを選択する。

共通鍵暗号方式/鍵サイズ	ハッシュ方式
RC2/128 ビット	SHA1
3Key Triple-DES/168 ビット	SHA1

8. ST 略語・用語

8.1. 略語

本 ST における略語を以下に説明する。

略語	定義内容
ADF	自動原稿送り装置（Auto Document Feeder）
CC	コモンクライテリア（Common Criteria）
CE	カストマーエンジニア(Customer Engineer)
CWIS	センターウェアインターネットサービス(Centre Ware Internet Service)
DC	デジタルコピー（Digital Copire）
DRAM	ダイナミックランダムアクセスメモリ(Dynamic Randam Access Memory)
EAL	評価保証レベル（Evaluation Assurance Level）
FIPS PUB	米国の連邦情報処理標準の出版物（Federal Information Processing Standard publication）
IIT	画像入力ターミナル（Image Input Terminal）
IOT	画像出力ターミナル（Image Output Terminal）
IT	情報技術（Information Technology）
IP	インターネットプロトコル(Internet Protocol)
MFD	デジタル複合機(Multi Function Device)
NVRAM	不揮発性ランダムアクセスメモリ（Non Volatile Random Access Memory）
PDL	ページ記述言語(Page Description Language)
PP	プロテクションプロファイル（Protection Profile）
SAR	セキュリティ保証要件(Security Assurance Requirement)
SEEPROM	シリアルバスに接続された電気的に書き換え可能な ROM (Serial Electronically Erasable and Programmable Read Only Memory)
SFP	セキュリティ機能方針(Security Function Policy)
SFR	セキュリティ機能要件(Security Functional Requirement)
SMTP	電子メール送信プロトコル(Simple Mail Transfer Protocol)
SOF	機能強度（Strength of Function）
ST	セキュリティターゲット（Security Target）
TOE	評価対象（Target of Evaluation）
TSF	TOE セキュリティ機能（TOE Security Function）

8.2. 用語

本 ST における用語を以下に説明する。

用語	定義内容
利用者	TOE の外部にあって TOEと対話する任意のエンティティ。具体的には一般利用者、システム管理者、およびカストマーエンジニア。
SA(System Administrator)	機械管理者から、MFP の機械管理や TOE セキュリティ機能の設定を許可された者。
システム管理者	MFD の機械管理や TOE セキュリティ機能の設定を行う管理者。 機械管理者と、SA の総称
カストマーエンジニア	MFD の保守/修理を行うエンジニア。
攻撃者	悪意を持って TOE を利用する者。
操作パネル	MFD の操作に必要なボタン、ランプ、タッチパネルディスプレイが配置されたパネル。
一般利用者クライアント	一般利用者が利用するクライアント。
システム管理者クライアント	システム管理者が利用するクライアント。 システム管理者は Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う。
センターウェア インターネットサービス（CWIS）	MFD に対してスキャナー機能によりスキャンして、親展ボックスに格納された文書データを取り出す機能を提供する。 さらにシステム管理者は、Web ブラウザを使い MFD に対して、TOE 設定データの確認や書き換えを行う機能を提供する。
システム管理者モード	一般利用者が MFD の機能を利用する動作モードとは別に、システム管理者が TOE の使用環境に合わせて、TOE 機器の動作設定や TOE セキュリティ機能設定の参照/更新といった、設定値の変更を行う動作モード。
ネットワークスキャナーユーティリティ	MFD 内の親展ボックスに保存されている文書データを一般利用者クライアントから取り出すためのソフトウェア。
プリンタードライバ	一般利用者クライアント上のデータを、MFD が解釈可能なページ記述言語(PDL)で構成された印刷データに変換するソフトウエアで、利用者クライアントで使用する。
印刷データ	MFD が解釈可能なページ記述言語(PDL)で構成されたデータ。 印刷データは、TOE のデコンポーズ機能でビットマップデータに変換される。
制御データ	MFD を構成するハードウエアユニット間で行われる通信のうち、コマンドとそのレスポンスとして通信されるデータ。
ビットマップデータ	コピー機能により読み込まれたデータ、およびプリンター機能により利用者クライアントから送信された印刷データをデコンポーズ機能で変換したデータ。 ビットマップデータは独自方式で画像圧縮して内部ハードディスク装置に格納される。
デコンポーズ機能	ページ記述言語(PDL)で構成された印刷データを解析し、ビットマップデータに変換する機能。
デコンポーズ	デコンポーズ機能により、ページ記述言語(PDL)で構成されたデータを解析し、ビットマップデータに変換する事。
プリンター機能	利用者クライアントから送信された印刷データをデコンポーズして印刷する機能。
原稿	コピー機能で IIT からの読み込みの対象となる文章や絵画、写真などを示す。
文書データ	一般利用者が MFD のコピー機能、プリンター機能、スキャナー機能を利用する際

用語	定義内容
	に、MFD 内部を通過する全ての画像情報を含むデータを、総称して文書データと表記する。 文書データには以下の様な物が含まれる。 • コピー機能を使用する際に、IIT で読み込まれ、IOT で印刷されるビットマップデータ。 • プリンター機能を利用する際に、一般利用者クライアントから送信される印刷データおよび、それをデコンポーズした結果作成されるビットマップデータ。 • スキャナー機能を利用する際に、IIT から読み込まれ内部ハードディスク装置に蓄積されるビットマップデータ。
利用済み文書データ	MFD の内部ハードディスク装置に蓄積された後、利用が終了しファイルは削除したが、内部ハードディスク装置内には、データ部は残存している状態の文書データ。
セキュリティ監査ログデータ	障害や構成変更、ユーザ操作など、デバイス内で発生した重要な事象を、「いつ」「何(誰)が」、「どうした」、「その結果」という形式で時系列に記録したもの。
内部蓄積データ	一般クライアントおよびサーバまたは一般利用者クライアント内に蓄積されている、TOE の機能に係わる以外のデータ。
一般データ	内部ネットワークを流れる TOE の機能に係わる以外のデータ。
TOE 設定データ	TOE によって作成された及び TOE に関して作成されたデータであり、TOE の動作に影響を与える可能性のあるもの。具体的には、内部ハードディスク蓄積データ上書き情報、ハードディスク暗号化情報、システム管理者情報、カストマーエンジニア操作制限情報、本体パネルからの認証時のパスワード使用情報、システム管理者 ID とパスワード情報、システム管理者認証失敗によるアクセス拒否情報、内部ネットワークデータ保護情報、セキュリティ監査ログ情報、親展ボックス情報、ユーザー認証情報。
一般クライアントおよびサーバ	TOE の動作に関与しないクライアントやサーバを示す。
内部ハードディスク装置からの削除	内部ハードディスク装置からの削除と記載した場合、管理情報の削除の事を示す。すなわち、文書データが内部ハードディスク装置から削除された場合、対応する管理情報が削除されるため、論理的に削除された文書データに対してアクセスする事は出来なくなる。 しかし文書データ自体はクリアーされていない状態となり、文書データ自体は、新たなデータが同じ領域に書き込まれるまで利用済み文書データとして内部ハードディスク装置に残る。
上書き消去	内部ハードディスク装置上に蓄積された文書データを削除する際に、そのデータ領域を特定データで上書きする事を示す。
暗号化キー	ユーザーが入力する 12 桁の英数字。 内部ハードディスク装置へ暗号化有効時に、このデータをもとに暗号鍵を生成する。
暗号鍵	暗号化キーをもとに自動生成される 128 ビットのデータ。 内部ハードディスク装置へ暗号化有効時の文書データの保存時に、この鍵データを使用して暗号化を行う。
ネットワーク	外部ネットワークと内部ネットワークを包含する一般的に使用する場合の表現。
外部ネットワーク	TOE を管理する組織では管理が出来ない、内部ネットワーク以外のネットワークを指す。
内部ネットワーク	TOE が設置される組織の内部にあり、外部ネットワークからのセキュリティの脅威に対

用語	定義内容
	して保護されているネットワーク内の、MFD と MFD へアクセスが必要なリモートの高信頼なサーバやクライアント PC 間のチャネルを指す。
ユーザー認証	TOE の各機能を使用する前に、利用者の識別を行って TOE の利用範囲に制限をかけるための機能である。
ローカル認証	TOE のユーザー認証を MFD で登録したユーザー情報を使用して認証管理を行うモード。

9. 参考資料

本 ST 作成時の参考資料を以下に記述する。

略称	ドキュメント名
[CC パート 1]	情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 1: 概説と一般モデル 2006 年 9 月 CCMB-2006-09-001 (平成 19 年 3 月翻訳第 1.2 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)
[CC パート 2]	情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 2: セキュリティ機能要件 2007 年 9 月 CCMB-2007-09-002 (平成 20 年 3 月翻訳第 2 .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)
[CC パート 3]	情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1 パート 3: セキュリティ保証要件 2007 年 9 月 CCMB-2007-09-003 (平成 20 年 3 月翻訳第 2 .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)
[CEM]	情報技術セキュリティ評価のための共通方法 バージョン 3.1 評価方法 2007 年 9 月 CCMB-2007-09-004 (平成 20 年 3 月翻訳第 2 .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)