Panasonic

データセキュリティーキット
DA-SC06
セキュリティーターゲット

第１．０１版　　２００８年　５月２１日

パナソニック コミュニケーションズ株式会社

改訂履歴

版数	年月日	頁	内容	担当
第 1.00 版	2008.1.25	ー	新規作成。	猪原
第 1.01 版	2008.5.21	ー	確認事項 002 の指摘修正。	猪原

目　次

１．　ＳＴ概説

１．１．　ＳＴ識別

１．１．１．　ＳＴの識別と管理

名称：　　データセキュリティーキット　DA-SC06
　　セキュリティーターゲット
バージョン：　第１．０１版
作成日：　　２００８年　５月２１日
作成者：　　パナソニック コミュニケーションズ株式会社

１．１．２．　ＴＯＥの識別と管理

名称：　　日本：データセキュリティーキット　DA-SC06
　　海外：Data Security Kit DA-SC06
バージョン：　V１．０１
作成者：　　パナソニック コミュニケーションズ株式会社

データセキュリティーキット DA-SC06 と Data Security Kit DA-SC06 は、名称が異なるのみで同一物である。

１．１．３．　使用するＣＣのバージョン

Common Criteria for Information Technology Security Evaluation,Version2.3,August 2005
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２．３（翻訳第１．０版）
補足－０５１２

１．２．　ＳＴ概要

１．２．１．　機能概要

本セキュリティーターゲットは、以下に示すパナソニック コミュニケーションズ株式会社製デジタル複合機のオプション製品である「データセキュリティーキット　DA-SC06」のセキュリティー仕様について記述したものである。

・日本国内適用機種（※）：DP-8032P / 8025P、DP-8032V / 8025V、DP-8032VA / 8025VA
・海外適用機種（※）　　：DP-8032 / 8025

（※）すべての適用機種に、別途オプション製品であるハードディスクユニットが必要。

「データセキュリティーキット　DA-SC06」はデジタル複合機の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するためのソフトウェア製品である。

１．２．２．　評価保証レベル

ＥＡＬ２適合

１．２．３．　適合するＰＰ

適合するＰＰはない。

１．２．４．　関連するセキュリティーターゲット

関連するセキュリティーターゲットはない。

１．３．　ＣＣ適合

下記のＣＣに適合している。

- ＣＣバージョン２．３　パート２拡張
- ＣＣバージョン２．３　パート３適合

１．４．　用語説明

本書で用いる用語を表１．で説明する。

表１．用語説明

用語	説明
デジタル複合機 DP-8032 / 8025	コピー／プリンター／スキャナー／ファクス等の機能を１台に集約した周辺機器。 本ＳＴでは、ハードディスクユニットを搭載したパナソニック コミュニケーションズ株式会社製 ・日本国内適用機種：DP-8032P / 8025P、DP-8032V / 8025V、DP-8032VA / 8025VA ・海外適用機種　　：DP-8032 / 8025 を総称してデジタル複合機 DP-8032 / 8025 と記述する。
ハードディスクユニット	パナソニック コミュニケーションズ株式会社が提供するデジタル複合機用のオプション製品であるハードディスク装置のことである。
内部ネットワーク	デジタル複合機 DP-8032 / 8025 を導入する組織の LAN をいう。
外部ネットワーク	内部ネットワーク以外のネットワーク（例えばインターネット）をいう。
USB	周辺機器とパソコンを結ぶデータ伝送路の規格のひとつ。
タンデムコピー	スキャナーユニットから読み込まれたデータのコピー部数の半分を読み込んだデジタル複合機 DP-8032 / 8025 で、残り半分を内部ネットワークに接続された他のデジタル複合機 DP-8032 / 8025 で印刷する機能。
リモートコピー	スキャナーユニットから読み込まれたデータのすべてを内部ネットワークに接続された他のデジタル複合機 DP-8032 / 8025 で印刷する機能。
一般利用者	デジタル複合機 DP-8032 / 8025 のコピー／プリンター／スキャナー／ファクス機能を利用する者。
キーオペレーター	デジタル複合機 DP-8032 / 8025 の機械管理者。
サービス技術者	デジタル複合機 DP-8032 / 8025 の設置／保守／修理を行うサービス実施会社の技術者。
サービスモード	サービス技術者がデジタル複合機 DP-8032 / 8025 の設置／保守／修理を行う時に使用する保守管理機能。
サービスモード設定手順	サービス技術者がサービスモードへ移行するための設定手順。
初期化	保守管理機能の「システム初期化」で実行できる初期設定値に戻す操作。
コントロールパネル	デジタル複合機 DP-8032 / 8025 の操作に必要なキー、ランプ、タッチパネルディスプレイが配置された操作パネル。
ＳＰＣ	スキャナー／プリンターユニットのメカ制御を行う基板。
ＦＲＯＭ	電気的な一括消去および任意部分の再書き込みを可能とした不揮発性メモリー。
文書データ	デジタル複合機 DP-8032 / 8025 のコピー／プリンター／スキャナー／ファクス機能の利用時、デジタル複合機の内部で扱われるすべてのデジタル化された画像情報の総称。 ・スキャナーユニットから読み込まれた画像情報。 ・プリンターユニットで印字できる画像情報。 ・イメージデータを画像処理技術により変換した画像情報。 ・クライアント PC より受信した画像情報、画像情報に変換されるデータ。
利用済み文書データ	デジタル複合機 DP-8032 / 8025 のハードディスク装置に一時蓄積され、利用が終了した文書データ。
ジョブ	デジタル複合機 DP-8032 / 8025 のコピー／プリンター／スキャナー／ファクス機能等における一連の機能の動作単位。
ジョブ削除	デジタル複合機 DP-8032 / 8025 のコピーやプリンター機能利用時、複数の処理（ジョブ）が指示された場合まだプリンターユニットで印字を開始していないジョブを、コントロールパネルからの指示で削除する機能。
受付音	デジタル複合機 DP-8032 / 8025 のコントロールパネルからの入力時入力文字や操作等が正常に受付られた時に通知されるピというパネルタッチ音。
拒否音	デジタル複合機 DP-8032 / 8025 のコントロールパネルからの入力時入力文字や操作等に誤りがあった時に通知されるピ、ピ、ピというパネルタッチ音。

１．５．　参考資料

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

２．　ＴＯＥ記述

２．１．　ＴＯＥ種別

ＴＯＥは、デジタル複合機に搭載されるデータセキュリティーキット　DA-SC06 であり、デジタル複合機の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するためのソフトウェア製品である。

本ＴＯＥは、以下に示すパナソニック コミュニケーションズ株式会社製デジタル複合機のオプション製品として提供され、デジタル複合機の標準ソフトウェアと置き換えることにより、セキュリティー機能を提供する。

・日本国内適用機種（※）：DP-8032P / 8025P、DP-8032V / 8025V、DP-8032VA / 8025VA
・海外適用機種（※）　　：DP-8032 / 8025
（※）すべての適用機種に、別途オプション製品であるハードディスクユニットが必要。

以下、デジタル複合機 DP-8032 / 8025 の説明は、DP-8032 / 8025 に搭載できるオプション製品であるファクス通信ユニットを搭載した DP-8032V / 8025V、DP-8032VA / 8025VA の構成で説明する。（なお、DP-8032P / 8025P はファクス通信ユニットのみ搭載できない構成である。）

２．２．　ＴＯＥの利用環境

デジタル複合機 DP-8032 / 8025 は、ネットワーク機能も搭載したデジタル複合機でありコピー／プリンター／ スキャナー／ファクスを利用した機能、デジタル複合機を運用管理するための機能および保守管理するための機能を提供する。

デジタル複合機 DP-8032 / 8025 は図１．想定される利用環境に示すように、オフィスや公共施設内の内部ネットワーク、公衆電話回線網、あるいはクライアント PC とローカルに接続され利用されることを想定している。

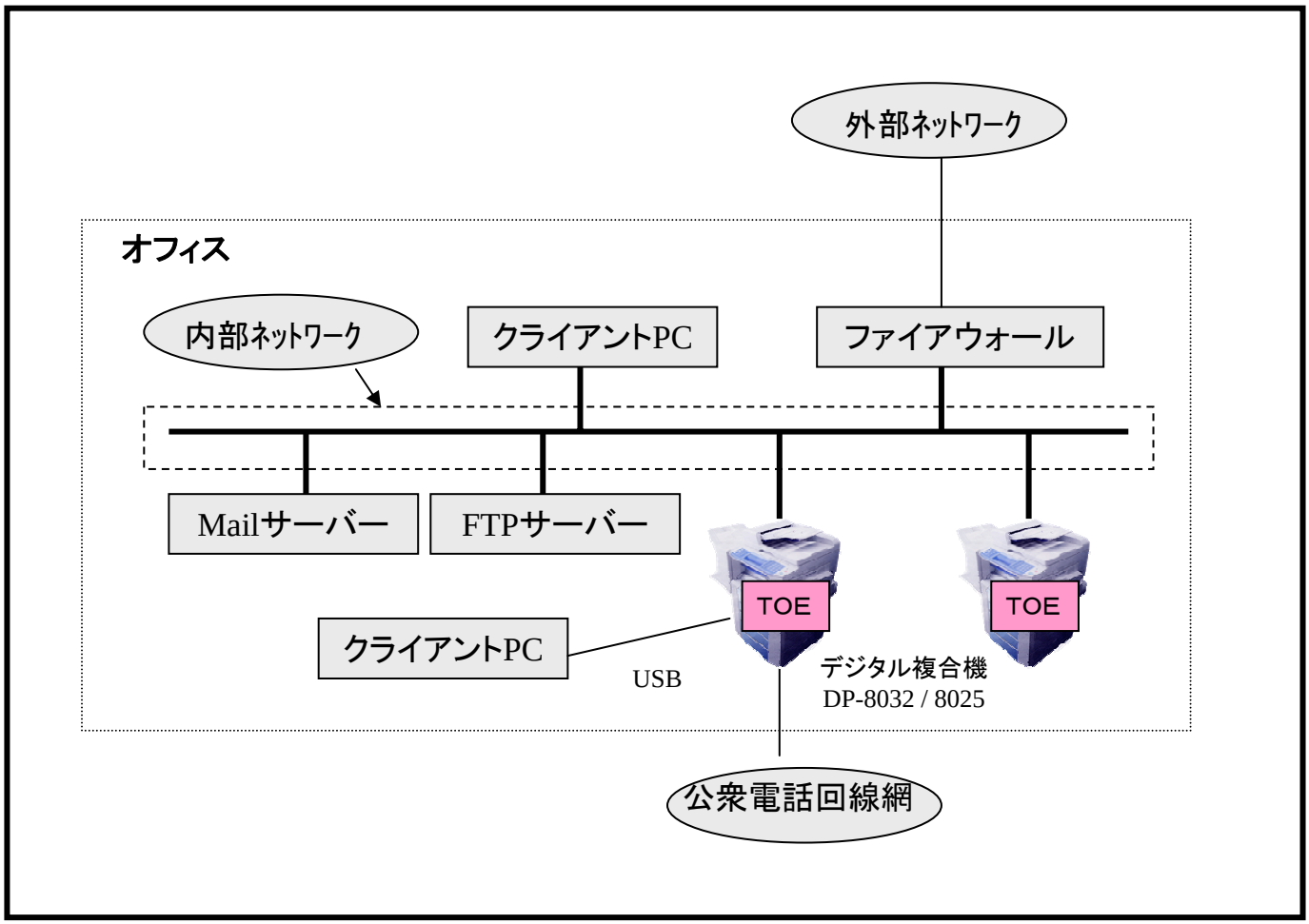

図　１．想定される利用環境

デジタル複合機 DP-8032 / 8025 は内部ネットワークを経由して、一般利用者のクライアント PC や FTP サーバー、Mail サーバーと接続され、クライアント PC や Mail サーバーから受信した文書データを印刷したり、スキャナーから読み込んだ文書データをクライアント PC や FTP サーバー、Mail サーバーへ送信する。

デジタル複合機 DP-8032 / 8025 は内部ネットワークを経由して他のデジタル複合機 DP-8032 / 8025 と接続され、一方の複合機のスキャナーから読み込んだ文書データを他の複合機で印刷するタンデムコピーやリモートコピーに利用される。

また、一般利用者のクライアント PC とローカル接続（USB 接続）されプリンターとして利用される。

外部ネットワークと接続する場合は、内部ネットワークに接続された各機器を保護するために、ファイアウォールを介して接続される。

ＴＯＥは、デジタル複合機 DP-8032 / 8025 に搭載され、デジタル複合機の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護する利用目的のためのソフトウェアである。

２．３．　ＴＯＥの関連者

ＴＯＥを搭載したデジタル複合機 DP-8032 / 8025 の関連者は下記のとおりである。

（１）一般利用者

一般利用者はデジタル複合機 DP-8032 / 8025 のコピー／プリンター／スキャナー／ファクス等の一般利用機能の利用者である。

（２）キーオペレーター

キーオペレーターと呼ばれる機械管理者は、デジタル複合機 DP-8032 / 8025 の提供する運用管理機能を利用して、運用管理を行う。

キーオペレーターはデジタル複合機 DP-8032 / 8025 の責任者から任命される。

（３）責任者

デジタル複合機 DP-8032 / 8025 の導入責任者で、キーオペレーターを選任し、管理・監督する。

（４）サービス技術者

サービス技術者は、デジタル複合機 DP-8032 / 8025 の提供する保守管理機能を利用して、設置／保守／修理等の作業を行う。

サービス技術者はデジタル複合機 DP-8032 / 8025 の保守を委託されている企業に属する。

２．４．　ＴＯＥの構成

２．４．１．　物理的構成

ＴＯＥを搭載したデジタル複合機 DP-8032 / 8025 の物理的構成を図２．に示す。

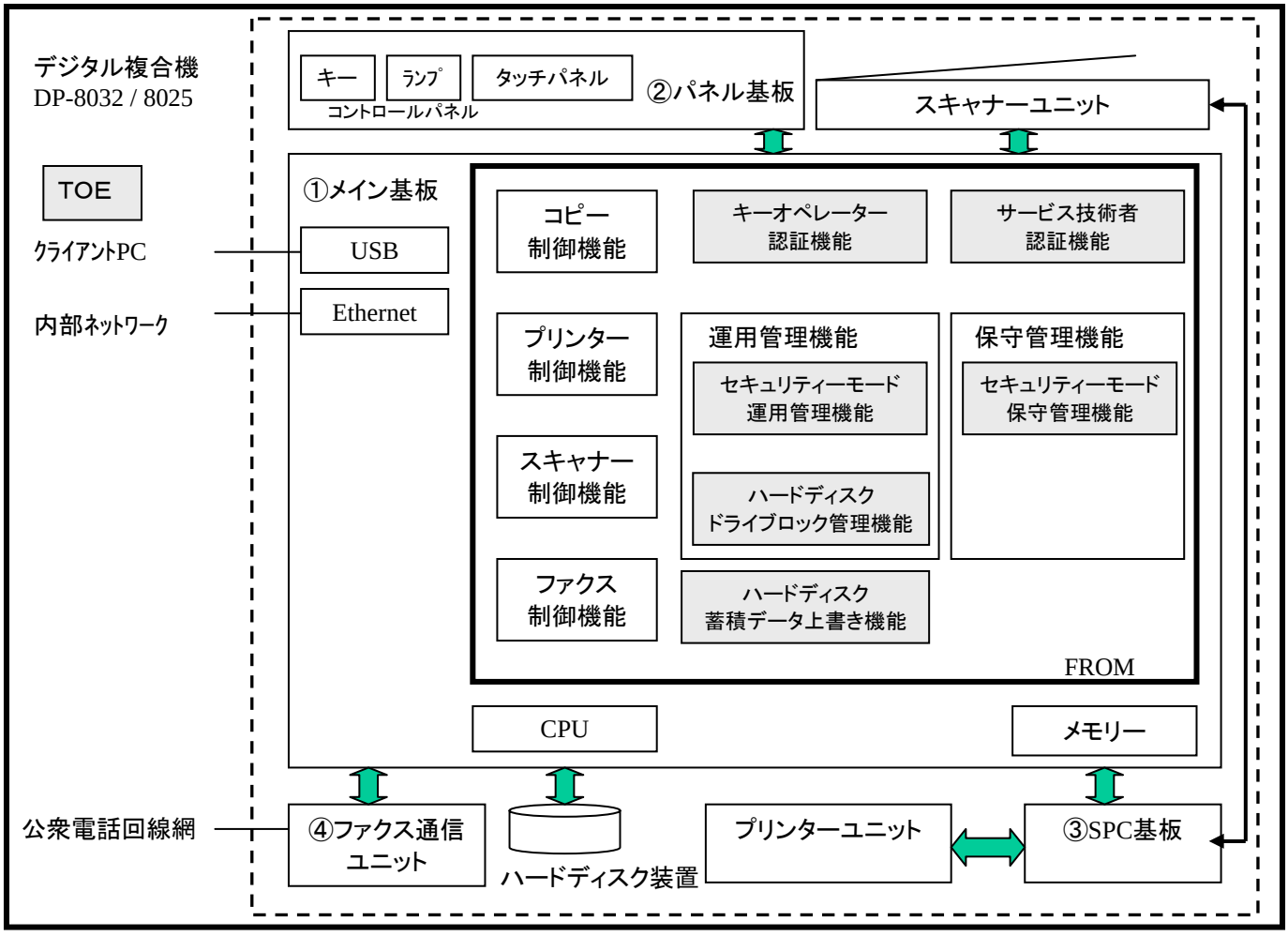

図　２．デジタル複合機 DP-8032 / 8025 の物理的構成とＴＯＥ

デジタル複合機 DP-8032 / 8025 は、
①複合機システム全体の制御を行うメイン基板
②複合機の操作に必要なキー、ランプ、タッチパネルディスプレイが配置されたコントロールパネルの制御を行うパネル基板
③スキャナーユニットやプリンターユニットのメカ制御を行うＳＰＣ基板
④ファクス通信ユニット
の４つの基板から構成される。
①メイン基板と②パネル基板は、制御データの通信を行うために内部インターフェースで接続されている。
①メイン基板と③ＳＰＣ基板は、制御データや文書データの通信を行うために内部インターフェースで接続されている。
③ＳＰＣ基板はスキャナーユニットと制御データの通信をおこないスキャナーのメカ制御を行う。スキャナーから読み込まれた文書データは直接①メイン基板に送信される。また、③ＳＰＣ基板はプリンターユニットと制御データ・文書データの通信をおこない、プリンターのメカ制御を実行しながら文書データの印刷を行う。
①メイン基板と④ファクス通信ユニットは、内部インターフェースで接続され、④ファクス通信ユニットはファクスデータの送受信を行うため、公衆電話回線網に接続されている。
さらに、①メイン基板は、クライアント PC、Mail サーバーや FTP サーバーと接続するために、Ethernet や USB インターフェースを有している。また、文書データを蓄積するためのハードディスク装置も①メイン基板に接続される。
①メイン基板はＣＰＵ、ソフトウェアを格納するＦＲＯＭ、データを格納するメモリー、その他複合機システム全体の制御を行うための電気回路で構成される。

ＴＯＥはメイン基板に実装されているＦＲＯＭに記録されている図２．で網掛けされた部分
・キーオペレーター認証機能
・サービス技術者認証機能
・セキュリティーモード運用管理機能
・セキュリティーモード保守管理機能
・ハードディスクドライブロック管理機能
・ハードディスク蓄積データ上書き機能
のソフトウェアであり、コピー／プリンター／スキャナー機能の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するものである。

２．４．２．　デジタル複合機の機能

デジタル複合機 DP-8032 / 8025 は一般利用者にコピー機能／プリンター機能／スキャナー機能／ファクス機能を提供する。

（１）コピー機能
スキャナーユニットから読み込まれた文書データをプリンターユニットで印刷する機能である。
コピー機能には、ハードディスク装置に文書データを一時蓄積する機能として下記がある。
・ノンソートコピー機能：
例えば３ページ２部の文書データを、Ｐ１，Ｐ１，Ｐ２，Ｐ２，Ｐ３，Ｐ３の印刷順序で出力することをノンソートという。スキャナーユニットから読み込まれた文書データをハードディスク装置に蓄積し、ハードディスク装置から読み出しノンソートの印刷順序で印刷する機能。
・ソートコピー機能：
例えば３ページ２部の文書データを、Ｐ１，Ｐ２，Ｐ３，Ｐ１，Ｐ２，Ｐ３の印刷順序で出力することをソートという。スキャナーユニットから読み込まれた文書データをハードディスク装置に蓄積し、ハードディスク装置から読み出しソートの印刷順序で印刷する機能。
・タンデムコピー機能：
スキャナーユニットから読み込まれた文書データをハードディスク装置に蓄積し、コピー部数の半分を読み込んだデジタル複合機 DP-8032 / 8025 で印刷し、残り半分の文書データを内部ネットワークに接続された他のデジタル複合機 DP-8032 / 8025 で印刷する機能。内部ネットワークから受信した文書データも一時ハードディスク装置に蓄積し、印刷速度にあわせハードディスク装置から読出し印刷する。
・リモートコピー機能：
スキャナーユニットから読み込まれた文書データをハードディスク装置に蓄積し、すべての文書データを内部ネットワークに接続された他のデジタル複合機 DP-8032 / 8025 で印刷する機能。内部ネットワークから受信した文書データも一時ハードディスク装置に蓄積し、印刷速度にあわせハードディスク装置から読出し印刷する。
・合成機能：
1 枚目にスキャナーから読み込まれた文書データをハードディスク装置に蓄積し、2 枚目以降のスキャナーから読みこまれた文書データと重ねてコピーする機能。
・ファイル編集機能：
スキャナーから読み込んだ文書データをハードディスクに蓄積、イメージタイトルと呼ばれる文書名をつけて登録、文書名変更、削除する機能。登録された文書データと、スキャナーから読み込まれた文書データと重ねてコピーする時に利用される。

（２）プリンター機能
一般利用者のクライアント PC から受信した文書データをプリンターユニットで印刷する機能である。
一般利用者のクライアント PC には、デジタル複合機 DP-8032 / 8025 用のプリンタードライバを インストールする。

プリンター機能では、受信した文書データはハードディスク装置に一時蓄積される。通常のプリンター機能では、受信した文書データは、複合機内部での処理が終了すれば印刷されるが、一般利用者のコントロールパネルからの印刷指示による印刷終了までハードディスク装置に文書データが保存される機能として下記がある。

・メールボックス機能：
受信した文書データをハードディスク装置に蓄積し、デジタル複合機 DP-8032 / 8025 のコントロールパネルからの操作によりユーザーID を入力し、文書データを印刷する機能。

・セキュリティーボックス機能：
受信した文書データをハードディスク装置に蓄積し、デジタル複合機 DP-8032 / 8025 のコントロールパネルからの操作によりユーザーID、パスワードを入力し、文書データを印刷する機能。

（３）スキャナー機能

スキャナーユニットから読み込まれた文書データをハードディスク装置に一時蓄積後、クライアントＰＣや FTP サーバーへ送信する機能である。

クライアント PC へ送信するためには、クライアント PC に本体付属ソフトウェアである Panasonic Document Management System の Panasonic コミュニケーションユーティリティがインストールされ、稼動していなければならない。

（４）ファクス機能

ファクス機能は、Ｇ３通信／インターネットＦＡＸ／Ｅメール機能の総称である。

Ｇ３通信は、スキャナーユニットから読み込まれた文書データを公衆電話回線網を介して、電話回線網に接続されているＦＡＸ端末へ送信したり、ＦＡＸ端末から公衆電話回線網を介して受信した文書データをプリンターユニットで印刷する機能である。

インターネットＦＡＸは、スキャナーユニットから読み込まれた文書データを Mail サーバーへ 送信、Mail サーバーからネットワークに接続されているインターネットＦＡＸ端末へ送信したり、インターネットＦＡＸ 端末から Mail サーバーを介して受信した文書データを印刷する機能である。

Ｅメールは、スキャナーユニットから読み込まれた文書データを指定されたＥメールアドレス先へ、メール添付して Mail サーバーを介して送信する機能である。

ファクス機能ではハードディスク装置に一時蓄積される文書データはない。

以上のコピー機能／プリンター機能／スキャナー機能／ファクス機能を実現するためにデジタル複合機を制御する機能を各コピー制御機能／プリンター制御機能／スキャナー制御機能／ファクス制御機能と呼ぶ。

（５）保守管理機能

サービス技術者のみが操作できるサービスモードとも呼ばれる機能で、デジタル複合機 DP-8032 / 8025 の設置／保守／修理等の作業をコントロールパネルから指示できる。主な機能として、コントロールパネルの全ランプ点灯等の自己試験機能、1 枚コピー／連続コピー等の動作試験機能、電源周波数の切り換え等のパラメータの設定、ソフトウェアのアップデート機能がある。

保守管理機能には、ハードディスク装置内に蓄積された文書データにアクセスする機能はないが、「システム初期化」呼ばれる２．４．３．論理的構成（６）セキュリティーモード保守管理機能で記述するＴＯＥの設定データを初期設定値にもどす機能がある。

（６）運用管理機能

キーオペレーターのみが操作できる機能で、デジタル複合機 DP-8032 / 8025 の運用に関する設定をコントロールパネルから指示できる。主な機能として、低電力モードの設定、日付時刻の設定、ネットワークに関する設定等があり、（２）プリンター機能で記述したメールボックスやセキュリティーボックスに対して「メールボックスデータ保持期間」の設定や「メールボックスデータ手動削除」の操作ができる。

運用管理機能には、ハードディスク装置内に蓄積された文書データにアクセスする機能はないが、ハードディスク装置を使用可能にするための管理情報等を作成するフォーマット機能がある。２．４．３．論理的構成で記述する（３）ハードディスクドライブロック管理機能、（４）セキュリティーモード運用管理機能も運用管理機能のひとつである。

（７）ハードディスク装置の機能

デジタル複合機 DP-8032 / 8025 のハードディスク装置は、ハードディスク装置そのものに直接パスワードを設定することにより、そのパスワードを入力しない場合ハードディスク装置が認識できなくなるドライブロック機能付きハードディスク装置を採用している。２．４．３．論理的構成で記述する（３）ハードディスクドライブロック管理機能により「ハードディスクドライブロックパスワード」の設定コマンドを受信したハードディスク装置は、ハードディスク装置内にそのパスワードを保持し、ハードディスク装置は装置内に保持しているパスワードと一致した時のみ、デジタル複合機 DP-8032 / 8025 からのデータのアクセスを許可する。また、ハードディスク装置は、ハードディスクドライブロックパスワードが一致した時にハードディスク装置に設定されていたパスワードを未設定状態にする機能を有する。

２．４．３．　論理的構成

ＴＯＥを搭載したデジタル複合機 DP-8032 / 8025 の論理的構成を図３．に示す。

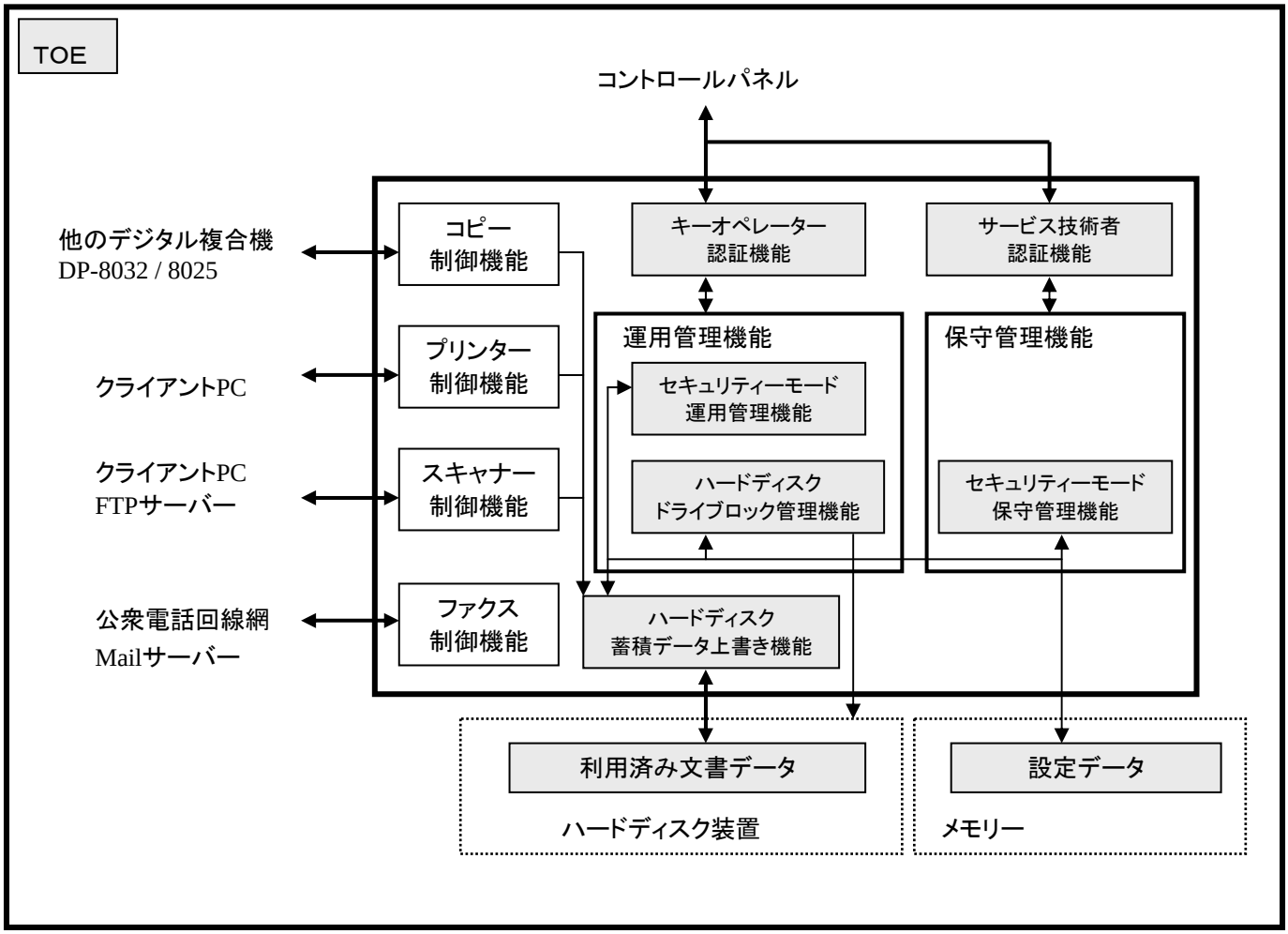

図　３．デジタル複合機 DP-8032 / 8025 の論理的構成とＴＯＥ

ＴＯＥを搭載したデジタル複合機 DP-8032 / 8025 では、コピー機能／プリンター機能／スキャナー機能によりハードディスク装置に一時蓄積された文書データは表２．利用済み文書データの発生するパターンに示すとおり、その利用が終了した時点で利用済み文書データとなり、そのデータの削除を行う。

通常、ハードディスク装置を扱う電子機器においては、ハードディスク装置のデータ削除は、データの管理情報を削除するのみでデータ領域すべてを消去しているわけではない。

したがって、ハードディスク装置の盗難や交換、廃棄時一般利用者の利用済み文書データは残存した状態にあり、PC やツール等によりハードディスク装置内の利用済み文書データを読み出すことが可能である。

これを対策するためにＴＯＥは、ハードディスク装置内に蓄積された利用済みの文書データに対し、下記に示すセキュリティー機能を提供する。

（１）ハードディスク蓄積データ上書き機能

コピー制御機能／プリンター制御機能／スキャナー制御機能の各動作処理後、ハードディスク装置内に蓄積された利用済み文書データをその発生時点で自動的に文書データのデータ領域も上書き消去する機能である。

上書き消去の方法として、下記の３種類がある。

・標準：文書データの管理情報のみを削除する

・レベル１：文書データのデータ領域にすべてＯのデータを 3 回上書き消去する

・レベル２：文書データのデータ領域にランダムな値を 2 回、その後すべてＯのデータを 1 回上書き消去する

（４）セキュリティーモード運用管理機能の「ハードディスクデータ消去レベル」でこの上書き消去の方法を設定する。

標準：文書データの管理情報のみを削除するが初期設定値なので、キーオペレーターはレベル１またはレベル２に設定してデジタル複合機 DP-8032 / 8025 を運用する。

また、（４）セキュリティーモード運用管理機能の「ハードディスク初期化」機能によりキーオペレーターのみが、廃棄時等ハードディスク装置内に蓄積された文書データをレベル１、レベル２の２種類の方法で上書き消去できる。

（２）キーオペレーター認証機能

コントロールパネルへの指示、入力されたキーオペレーター専用のパスワード（以下、キーオペレーターパスワードと記述する）により、キーオペレーターの識別と認証を行う機能である。　キーオペレーターのみ、（３）ハードディ

スクドライブロック管理機能、（４）セキュリティーモード運用管理機能の操作ができる。

（３）ハードディスクドライブロック管理機能

ハードディスク装置として、ハードディスク装置そのものに直接パスワードを設定することにより、そのパスワードを入力しない場合ハードディスク装置が認識できなくなるドライブロック機能付きのハードディスク装置を採用している。キーオペレーターのみ、「ハードディスクドライブロックパスワード」のデジタル複合機内のメモリーおよびハードディスク装置に対するパスワードの設定・変更とパスワードを未設定状態にするドライブロックの解除を行うことができる。デジタル複合機は起動時、複合機内のメモリーに格納されているパスワードをハードディスク装置に対して送信し、ハードディスク装置へのデータアクセスの許可を依頼する。

（４）セキュリティーモード運用管理機能

キーオペレーターのみ、以下のセキュリティーに関する設定データの設定・変更および処理の指示ができる。

・「ハードディスクデータ消去レベル」

コピー制御機能／プリンター制御機能／スキャナー制御機能の各動作処理後の利用済み文書データ発生時点で自動的に実行するハードディスク蓄積データ上書き機能の消去方法を設定する。

標準（初期設定値）、レベル１、レベル２の３種類の上書き消去の方法が設定できる。

・「ハードディスク初期化」

キーオペレーターの指示により、ハードディスク装置内に蓄積された文書データすべてを上書き消去する機能である。上書き消去の方法として、レベル１、レベル２の２種類有する。

・「キーオペレーターパスワード」

キーオペレーターパスワードを設定・変更する機能である。

（５）サービス技術者認証機能

コントロールパネルからのサービスモード設定手順の操作、入力されたサービス技術者パスワードにより、サービス技術者の識別と認証を行う機能である。サービス技術者のみ、（６）セキュリティーモード保守管理機能の操作ができる。

（６）セキュリティーモード保守管理機能

サービス技術者のみ、以下のセキュリティーに関する設定データの設定・変更および初期化（初期設定値に戻す操作）の指示ができる。

・「サービス技術者パスワード」

サービス技術者パスワードを設定・変更する機能である。

・「システム初期化」

サービス技術者の指示により、（３）ハードディスクドライブロック管理機能で記述した「ハードディスクドライブロックパスワード」、（４）セキュリティーモード運用管理機能で記述した「ハードディスクデータ消去レベル」および「キーオペレーターパスワード」、（６）セキュリティーモード保守管理機能で記述した「サービス技術者パスワード」の設定データを初期化（初期設定値に戻す操作）する機能である。

セキュリティーに関する設定データ「ハードディスクドライブロックパスワード」、「ハードディスクデータ消去レベル」、「キーオペレーターパスワード」、「サービス技術者パスワード」は、メモリーに格納される。

「システム初期化」は、デジタル複合機 DP-8032 / 8025 の修理、廃棄時使用できるメイン基盤上のメモリーに設定された内容を初期化すなわち工場からの出荷時の状態に設定データを戻す機能である。「ハードディスクデータ消去レベル」は標準が初期設定値であるため、ハードディスク装置内に蓄積された利用済み文書データのデータ領域は上書き消去されなくなる。「ハードディスクドライブロックパスワード」は、設定データのみ初期化しハードディスク装置への設定コマンドは送信しないので、「システム初期化」だけではハードディスク装置内の既に蓄積されているデータを読みだすことはできない。「キーオペレーターパスワード」、「サービス技術者パスワード」も初期設定値になるので、「システム初期化」実行時は再設定が必要になる。

ＴＯＥを搭載したデジタル複合機 DP-8032 / 8025 の設置時、「システム初期化」実行時は、
サービス技術者は、コントロールパネルより、初期設定値のサービス技術者パスワードを入力し認証された後、

・「サービス技術者パスワード」を変更

キーオペレーターは、コントロールパネルより、初期設定値のキーオペレーターパスワードを入力し認証された後、

・「ハードディスクデータ消去レベル」をレベル１またはレベル２に設定
・　設置時は「ハードディスクドライブロックパスワード」の設定
「システム初期化」実行時は、ハードディスク装置に設定されている「ハードディスクドライブロックパスワード」の再設定
・「キーオペレーターパスワード」を変更

を実施して、ＴＯＥを利用、運用する。

表２．利用済み文書データの発生するパターン

利用機能名	発生パターン
コピー機能利用時（注）	一般利用者がコントロールパネルより指示したノンソートコピー（例えば 3P2 部の文書データを、P1,P1,P2,P2,P3,P3 の印刷順序の出力）時、各ページの印刷が終了した時点で利用済み文書データとなる。
	一般利用者がコントロールパネルより指示したソートコピー（例えば 3P2 部の文書データを、P1,P2,P3,P1,P2,P3 の印刷順序の出力）時、すべての印刷が終了した時点で利用済み文書データとなる。
	一般利用者がコントロールパネルより指示したリモートコピーにおいて、他のデジタル複合機に読み込んだ文書データをすべて転送終了した時点で利用済み文書データとなる。
	上記ノンソートコピー、ソートコピー中に一般利用者がコントロールパネルより印刷中止を指示した時点で利用済み文書データとなる。
	上記ノンソートコピー、ソートコピー中に一般利用者がコントロールパネルよりジョブ削除を指示した時点で利用済み文書データとなる。
	ファイル編集において、登録された文書データを、一般利用者がコントロールパネルより消去を指示した時点で利用済み文書データとなる。
プリンター機能利用時	一般利用者がクライアント PC より指示したプリンター機能で、ノンソート指定時は各ページの、ソート指定時はすべての印刷が終了した時点で利用済み文書データとなる。
	一般利用者がクライアント PC よりメールボックス指示した文書データを、一般利用者がコントロールパネルからユーザーID を入力後指示した印刷がすべて終了した時点で利用済み文書データとなる。
	一般利用者がクライアント PC よりセキュリティーボックス指示した文書データを、一般利用者がコントロールパネルからユーザーID、パスワードを入力後指示した印刷がすべて終了した時点で利用済み文書データとなる。
	プリンター機能を利用した印刷中に、一般利用者がコントロールパネルより印刷中止を指示した時点で利用済み文書データとなる。
	プリンター機能を利用した印刷の開始前に、一般利用者がコントロールパネルよりジョブ削除を指示した時点で利用済み文書データとなる。
	メールボックス、セキュリティーボックスに保存されている文書データで、キーオペレーターが運用管理機能を用いて設定した「メールボックスデータ保持期間」を経過した時点で利用済み文書データとなる。
	メールボックス、セキュリティーボックスに保存されている文書データで、キーオペレーターが運用管理機能の「メールボックスデータ手動削除」を指示した時点で利用済み文書データとなる。
コピープリンター機能利用時	一般利用者がコントロールパネルより指示したコピー、一般利用者がクライアント PC より指示したプリンター機能において、印刷中に紙ジャム等の印刷が中断する事象が発生した場合一時的にハードディスク装置に保存された文書データは、紙ジャム中断事象から復帰後、ノンソート指定時は各ページの、ソート指定時はすべての印刷が終了した時点で利用済み文書データとなる。
スキャナー機能利用時	一般利用者がコントロールパネルより指示したスキャナー機能において、クライアント PC または FTP サーバーへ読み込んだ文書データをすべて転送終了した時点で利用済み文書データとなる。
	一般利用者がコントロールパネルより指示したスキャナー機能において、クライアント PC または FTP サーバーへ読み込んだデータを転送、終了前にエラーにより転送できず利用済み文書データとなる。
	スキャナーユニットから読み込み中に、一般利用者がコントロールパネルより中止を指示した時点で利用済み文書データとなる。

（注）タンデムコピー、リモートコピー、合成コピーにおいてノンソートコピー、ソートコピーと利用済み文書データの発生するパターンが同一のものはノンソートコピー、ソートコピーに含める。

２．５．　ＴＯＥが保護する資産

ＴＯＥが保護する資産は、デジタル複合機 DP-8032 / 8025 のデジタル複合機処理後のハードディスク装置内に蓄積された利用済み文書データである。

３．　ＴＯＥセキュリティー環境

３．１．　前提条件

本ＴＯＥの動作／運用／利用の前提条件を表３．に示す。

表 ３．前提条件

前提条件	内容
A.SETSEC	・セキュリティーモード設定 キーオペレーターは、下記のＴＯＥの機能を有効にして運用する。 「ハードディスクドライブロックパスワード」を設定する。
A.ADMIN	・キーオペレーターの信頼 キーオペレーターは不正な行為を行わない人物である。
A.SE	・サービス技術者の信頼 サービス技術者は不正な行為を行わない人物である。

３．２．　脅威

本ＴＯＥの対抗すべき脅威を表４．に示す。

攻撃者は、複合機やＩＴの一般的な知識を有し、簡単に入手できる情報やツールを利用して、ＴＯＥを攻撃する低レベルの攻撃力をもつ者と想定する。

表 ４．脅威

脅威	内容
T.RECOVER	・利用済み文書データの不正再生 悪意をもった一般利用者やＴＯＥの非関連者がハードディスク装置に、PC やツール等直接接続して利用済み文書データを再生するかもしれない。

３．３．　組織のセキュリティー方針

本ＴＯＥが要求され従わなければならない組織のセキュリティー方針を表５．に示す。

表 ５．組織のセキュリティー方針

組織のセキュリティー方針	内容
P.OWMETHOD	・ハードディスク装置内に蓄積された利用済み文書データを上書き消去する。 ハードディスク装置内に蓄積された利用済み文書データのデータ領域を上書き消去しなければならない。

４．　セキュリティー対策方針

４．１．　ＴＯＥのセキュリティー対策方針

ＴＯＥのセキュリティー対策方針を表６．に示す。

表 ６．ＴＯＥのセキュリティー対策方針

対策方針	説明
O.HDLMNG	ＴＯＥは、認証されたキーオペレーターのみ「ハードディスクドライブロックパスワード」をハードディスク装置に設定することにより、ハードディスク装置内に蓄積された利用済み文書データの再生を不可能にしなければならない。
O.RESIDUAL	ＴＯＥは、上書き消去を行わない標準レベルの他に、「ハードディスクデータ消去レベル」：レベル１、レベル２の２種類のハードディスク蓄積データ上書き機能を提供しなければならない。

４．２．　環境のセキュリティー対策方針

ＴＯＥ環境のセキュリティー対策方針を表７．に示す。

表 ７．環境のセキュリティー対策方針

対策方針	説明
OE.AUTH	キーオペレーターは、保守時以外においてはデジタル複合機 DP-8032 / 8025 の運用管理機能を利用し、「ハードディスクデータ消去レベル」：レベル１またはレベル２、「ハードディスクドライブロックパスワード」を設定して運用しなければならない。
OE.ADMIN	責任者はキーオペレーターが不正な行為を行わないことを保証するために適切なキーオペレーターの人選を行うとともに、課せられたキーオペレーターの業務を遂行できるように管理や、必要な知識が習得できるよう教育を実施しなければならない。
OE.SE	サービス技術者がデジタル複合機 DP-8032 / 8025 の保守作業を行う時には、責任者またはキーオペレーターは、サービス技術者が複合機の保守を委託している企業の社員であることを確認しなければならない。
OE.HDD	ハードディスク装置は、ハードディスクドライブロックパスワードを使用してハードディスク装置内の利用済み文書データに対する不正なアクセスを防止する。

５．　ＩＴセキュリティー要件

５．１．　ＴＯＥセキュリティー機能要件

ＴＯＥが提供するセキュリティー要件を規定する。

５．１．１．　クラスＦＤＰ　：　利用者データ保護

FDP_RIP.1　　サブセット残存情報保護

下位階層：　なし

FDP_RIP.1.1　TSF は、以下のオブジェクト［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］。

［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
［割付：オブジェクトのリスト］
・利用済み文書データが蓄積されたハードディスク

依存性：　なし

５．１．２．　クラスＦＩＡ　：　識別と認証

FIA_AFL.1(1)　　認証失敗時の取り扱い

下位階層：　なし

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。（注）

［割付：認証事象のリスト］
・キーオペレーター認証機能
［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」］（注）
・１

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］
・認証を１秒間以上受付停止

依存性：　FIA_UAU.1　認証のタイミング

FIA_AFL.1(2)　　認証失敗時の取り扱い

下位階層：　なし

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。（注）

［割付：認証事象のリスト］
・サービス技術者認証機能
［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」］（注）
・１

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］
・認証を１秒間以上受付停止

依存性：　FIA_UAU.1　認証のタイミング

（注）［、「、」、］の関係は、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２．３（翻訳第１．０版）と異なる。

FIA_SOS.1(1)　　秘密の検証

下位階層：　なし

FIA_SOS.1.1(1)　TSF は、秘密が［割付：定義された品質尺度］に合致することを検証するメカニズムを提供しなければならない。

詳細化　：　秘密　→　キーオペレーターのパスワード

［割付：定義された品質尺度］

キーオペレーターのパスワードの品質尺度を以下に定義する。

・８文字固定

・英大文字、英小文字、数字、記号

・同一文字の８文字連続は禁止

依存性：　なし

FIA_SOS.1(2)　　秘密の検証

下位階層：　なし

FIA_SOS.1.1(2)　TSF は、秘密が［割付：定義された品質尺度］に合致することを検証するメカニズムを提供しなければならない。

詳細化　：　秘密　→　サービス技術者のパスワード

［割付：定義された品質尺度］

サービス技術者のパスワードの品質尺度を以下に定義する。

・８文字固定

・英大文字、英小文字、数字、記号

・同一文字の８文字連続は禁止

依存性：　なし

FIA_UID.2(1)　　アクション前の利用者識別

下位階層：　FIA_UID.1

FIA_UID.2.1(1)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　：　利用者　→　キーオペレーター

依存性：　なし

FIA_UID.2(2)　　アクション前の利用者識別

下位階層：　FIA_UID.1

FIA_UID.2.1(2)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　：　利用者　→　サービス技術者

依存性：　なし

FIA_UAU.2(1)　　アクション前の利用者認証

下位階層：　FIA_UAU.1

FIA_UAU.2.1(1)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

詳細化　：　利用者　→　キーオペレーター

依存性：　FIA_UID.1　識別のタイミング

FIA_UAU.2(2)　　アクション前の利用者認証

下位階層：　FIA_UAU.1

FIA_UAU.2.1(2)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

詳細化　：　利用者　→　サービス技術者

依存性：　FIA_UID.1　識別のタイミング

FIA_UAU.7(1)　　保護された認証フィードバック

下位階層：　　なし

FIA_UAU.7.1(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］

・キーオペレーターパスワードとして入力された文字データ１字ごとに‘*’を表示

依存性：　　FIA_UAU.1　認証のタイミング

FIA_UAU.7(2)　　保護された認証フィードバック

下位階層：　　なし

FIA_UAU.7.1(2)　　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］

・サービス技術者パスワードとして入力された文字データ１字ごとに‘*’を表示

依存性：　　FIA_UAU.1　認証のタイミング

５．１．３．　クラスＦＭＴ　：　セキュリティー管理

FMT_MOF.1　　セキュリティー機能のふるまいの管理

下位階層：　　なし

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

［割付：機能のリスト］

・ハードディスク蓄積データ上書き機能

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

・のふるまいを決定する

・を停止する

・を動作させる

［割付：許可された識別された役割］

・キーオペレーター、サービス技術者

役割とハードディスク蓄積データ上書き機能の選択できる能力の関係を表８．に示す。

表８．役割とハードディスク蓄積データ上書き機能の選択できる能力の関係

役割 ＼ 能力	ハードディスク蓄積データ上書き機能
キーオペレーター	・のふるまいを決定する ・を停止する ・を動作させる
サービス技術者	・を停止する

依存性：　　FMT_SMF.1　管理機能の特定

FMT_SMR.1　セキュリティー役割

FMT_MTD.1(1)　　TSF データの管理

下位階層：　　なし

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］

・「ハードディスクデータ消去レベル」

標準：文書データの管理情報のみを削除する（初期設定値）

レベル１：文書データのデータ領域にすべて０のデータを３回上書き消去する

レベル２：文書データのデータ領域にランダムな値を２回、その後すべて０のデータ

を１回上書き消去する
[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
[割付：許可された識別された役割]
・キーオペレーター、サービス技術者

役割と「ハードディスクデータ消去レベル」の選択できる能力の関係を表９．に示す。

表９．役割と「ハードディスクデータ消去レベル」の選択できる能力の関係

能力 / 役割	「ハードディスクデータ消去レベル」			
	問い合わせ	改変		
		標準	レベル１	レベル２
キーオペレーター	○	○	○	○
サービス技術者	×	○	×	×

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

FMT_MTD.1(2)　TSF データの管理
下位階層：　なし
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]
・「キーオペレーターパスワード」
[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、その他の操作：初期化（初期設定値に戻す操作）
[割付：許可された識別された役割]
・キーオペレーター、サービス技術者

役割と「キーオペレーターパスワード」の選択できる能力の関係を表 10. に示す。

表 10. 役割と「キーオペレーターパスワード」の選択できる能力の関係

能力 / 役割	「キーオペレーターパスワード」	
	改変	その他の操作：初期化
キーオペレーター	○	×
サービス技術者	×	○

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

FMT_MTD.1(3)　TSF データの管理
下位階層：　なし
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]
・「サービス技術者パスワード」
[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、その他の操作：初期化（初期設定値に戻す操作）
[割付：許可された識別された役割]
・サービス技術者
依存性：　FMT_SMF.1　管理機能の特定
FMT_SMR.1　セキュリティー役割

FMT_SMF.1　　管理機能の特定
下位階層：　　なし
FMT_SMF.1.1　　TSF は、以下のセキュリティー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ー管理機能のリスト］。

［割付：TSF によって提供されるセキュリティー管理機能のリスト］
・表 11. に示す管理項目を管理する機能
依存性：　　なし

表 11. 管理項目を管理する機能

機能要件	管理要件	管理項目と管理機能
FDP_RIP.1	残存情報保護がいつ実施されるかの管理	残存情報保護の実施タイミングは、割当て解除時に固定のため管理項目はない。
FIA_AFL.1(1)	不成功の認証試行に対する閾値の管理、認証失敗の事象においてとられるアクションの管理	閾値は固定、アクションも固定であるため管理項目はない。
FIA_AFL.1(2)	不成功の認証試行に対する閾値の管理、認証失敗の事象においてとられるアクションの管理	閾値は固定、アクションも固定であるため管理項目はない。
FIA_SOS.1(1)	秘密の検証に使用される尺度の管理	尺度は固定のため管理項目はない。
FIA_SOS.1(2)	秘密の検証に使用される尺度の管理	尺度は固定のため管理項目はない。
FIA_UID.2(1)	利用者識別情報の管理	利用者識別情報は固定のため管理項目はない。
FIA_UID.2(2)	利用者識別情報の管理	利用者識別情報は固定のため管理項目はない。
FIA_UAU.2(1)	キーオペレーターによる認証データの管理	キーオペレーターのパスワード。
FIA_UAU.2(2)	サービス技術者による認証データの管理	サービス技術者のパスワード。
FIA_UAU.7(1)	管理要件なし	－
FIA_UAU.7(2)	管理要件なし	－
FMT_MOF.1	TSF の機能と相互に影響を及ぼす役割グループの管理	キーオペレーター、サービス技術者の役割は固定されているため管理項目はない。
FMT_MTD.1(1)	TSF のデータと相互に影響を及ぼす役割グループの管理	キーオペレーター、サービス技術者の役割は固定されているため管理項目はない。
FMT_MTD.1(2)	TSF のデータと相互に影響を及ぼす役割グループの管理	キーオペレーター、サービス技術者の役割は固定されているため管理項目はない。
FMT_MTD.1(3)	TSF のデータと相互に影響を及ぼす役割グループの管理	サービス技術者の役割は一人に固定されているため左記の管理項目はない。
FMT_SMF.1	管理要件なし	－
FMT_SMR.1	役割の一部をなす利用者グループの管理	キーオペレーター、サービス技術者の役割は固定されているため管理項目はない。
FPT_RVM.1	管理要件なし	－
FIT_SOS.1	ＩＴ環境の秘密の検証に使用される尺度の管理	尺度は固定のため管理項目はない。
FIT_MTD.1	管理者データと相互に影響を及ぼす役割グループの管理	キーオペレーター、サービス技術者の役割は固定されているため管理項目はない。

FMT_SMR.1　　セキュリティー役割
下位階層：　　なし
FMT_SMR.1.1　　TSF は、役割［割付：許可された識別された役割］を維持しなければならない。

［割付：許可された識別された役割]
・キーオペレーター、サービス技術者

FMT_SMR.1.2　　TSF は、利用者を役割に関連づけなければならない。
依存性：　　FIA_UID.1　識別のタイミング

５．１．４．　クラスＦＰＴ　：　ＴＳＦの保護

FPT_RVM.1　　TSP の非バイパス性
下位階層：　　なし
FPT_RVM.1.1　　TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。
依存性：　　なし

５．１．５．　新規セキュリティー機能要件

本ＳＴでは、新規にＴＯＥセキュリティー機能要件（FIT_SOS.1　ＩＴ環境の秘密の検証、FIT_MTD.1　管理者データの管理）を作成し、使用している。

管理者データとは、キーオペレーター、サービス技術者のみがアクセスできるＩＴ環境のセキュリティー機能の制御データである。

FIT_SOS.1　ＩＴ環境の秘密の検証は、ＩＴ環境の秘密が定義された品質尺度にあっていることをＴＳＦが検証することを要求する。

管理：FIT_SOS.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）ＩＴ環境の秘密の検証に使用される尺度の管理

監査：FIT_SOS.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：TSFによる、テストされたIT環境の秘密の拒否；
ｂ）基本：TSFによる、テストされたIT環境の秘密の拒否または受け入れ；
ｃ）詳細：定義された品質尺度に対する変更の識別。

FIT_SOS.1　　ＩＴ環境の秘密の検証
下位階層：　なし
FIT_SOS.1.1　TSFは、ＩＴ環境の秘密が［割付：定義された品質尺度］に合致することを検証するメカニズムを提供しなければならない。

詳細化　：　ＩＴ環境の秘密　→　「ハードディスクドライブロックパスワード」
［割付：定義された品質尺度］
「ハードディスクドライブロックパスワード」の品質尺度を以下に定義する。
・８文字以上３２文字以下
・英大文字、英小文字、数字、記号
依存性：　なし

FIT_MTD.1　管理者データの管理は、許可利用者が管理者データを管理することを許可する。

管理：FIT_MTD.1
以下のアクションはFMT管理における管理機能と考えられる：
ａ）管理者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。

監査：FIT_MTD.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）基本：基本：管理者データの値のすべての改変。

FIT_MTD.1　　管理者データの管理
下位階層：　なし
FIT_MTD.1.1　TSFは、［割付：管理者データのリスト］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：管理者データのリスト］
・「ハードディスクドライブロックパスワード」
［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、消去、その他の操作：初期化（初期設定値に戻す操作）
［割付：許可された識別された役割］
・キーオペレーター、サービス技術者

役割と「ハードディスクドライブロックパスワード」の選択できる能力の関係を表12.に示す。

表12. 役割と「ハードディスクドライブロックパスワード」の選択できる能力の関係

役割 ＼ 能力	「ハードディスクドライブロックパスワード」
キーオペレーター	改変、消去

サービス技術者	その他の操作：初期化

消去は「ハードディスクドライブロックパスワード」の解除のことである。

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

５．２．　ＴＯＥセキュリティー保証要件

ＴＯＥの評価保証レベルはＥＡＬ２である。
ＥＡＬ２保証要件を表 13. に示す。

表 13. ＥＡＬ２保証要件

保証クラス	保証コンポーネント ID	保証コンポーネント	依存性
構成管理	ACM_CAP.2	構成要素	なし
配付と運用	ADO_DEL.1	配付手続き	なし
	ADO_IGS.1	設置、生成、及び立上げ手順	AGD_ADM.1
開発	ADV_FSP.1	非形式的機能仕様	ADV_RCR.1
	ADV_HLD.1	記述的上位レベル設計	ADV_FSP.1　ADV_RCR.1
	ADV_RCR.1	非形式的対応の実証	なし
ガイダンス文書	AGD_ADM.1	管理者ガイダンス	ADV_FSP.1
	AGD_USR.1	利用者ガイダンス	ADV_FSP.1
テスト	ATE_COV.1	カバレージの証拠	ADV_FSP.1　ATE_FUN.1
	ATE_FUN.1	機能テスト	なし
	ATE_IND.2	独立試験・サンプル	ADV_FSP.1　AGD_ADM.1 AGD_USR.1　ATE_FUN.1
脆弱性評定	AVA_SOF.1	ＴＯＥセキュリティー機能強度評価	ADV_FSP.1　ADV_HLD.1
	AVA_VLA.1	開発者脆弱性分析	ADV_FSP.1　ADV_HLD.1 AGD_ADM.1　AGD_USR.1

５．３．　ＩＴ環境に対するセキュリティー機能要件

FIA_UID.2(IT)　アクション前の利用者識別
下位階層：　FIA_UID.1
FIA_UID.2.1(IT)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

詳細化　：　TSF　→　ハードディスク装置
依存性：　なし

FIA_UAU.2(IT)　アクション前の利用者認証
下位階層：　FIA_UAU.1
FIA_UAU.2.1(IT)　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

詳細化　：　TSF　→　ハードディスク装置
依存性：　FIA_UID.1　識別のタイミング

５．４．　ＴＯＥセキュリティー機能強度

本ＴＯＥのセキュリティー最小機能強度は、ＳＯＦ－基本である。
確率的または順列的メカニズムを利用する機能要件は、
・FIA_UID.2(1)、FIA_UAU.2(1)、FIA_UAU.7(1)、FIA_AFL.1(1)、FIA_SOS.1(1)
・FIA_UID.2(2)、FIA_UAU.2(2)、FIA_UAU.7(2)、FIA_AFL.1(2)、FIA_SOS.1(2)
であり、明示された機能強度はＳＯＦ－基本である。

６．　ＴＯＥ要約仕様

６．１．　ＴＯＥセキュリティー機能

ＴＯＥは以下のセキュリティー機能を有する。

- ハードディスク蓄積データ上書き機能（SF.OVWRT）
- キーオペレーター認証機能（SF.ADM_IA）
- ハードディスクドライブロック管理機能（SF.HDMNG）
- セキュリティーモード運用管理機能（SF.ADMMNG）
- サービス技術者認証機能（SF.SE_IA）
- セキュリティーモード保守管理機能（SF.SEMNG）

表 14. に各ＴＯＥセキュリティー機能とセキュリティー機能要件の関係を示す。

表 14. ＴＯＥセキュリティー機能とセキュリティー機能要件の関係

※	SF.OVWRT	SF.ADM_IA	SF.HDMNG	SF.ADMMNG	SF.SE_IA	SF.SEMNG
FDP_RIP.1	○					
FIA_AFL.1(1)		○				
FIA_AFL.1(2)					○	
FIA_SOS.1(1)				○		
FIA_SOS.1(2)						○
FIA_UID.2(1)		○				
FIA_UID.2(2)					○	
FIA_UAU.2(1)		○				
FIA_UAU.2(2)					○	
FIA_UAU.7(1)		○				
FIA_UAU.7(2)					○	
FMT_MOF.1				○		○
FMT_MTD.1(1)				○		○
FMT_MTD.1(2)				○		○
FMT_MTD.1(3)						○
FMT_SMF.1				○		○
FMT_SMR.1				○		○
FPT_RVM.1	○	○	○	○	○	○
FIT_SOS.1			○			
FIT_MTD.1			○			○

※横にＴＯＥセキュリティー機能を、縦にセキュリティー機能要件を示す。

６．１．１．　ハードディスク蓄積データ上書き機能（SF.OVWRT）

この機能は、ハードディスク装置内に蓄積された利用済み文書データのデータ領域を上書き消去する機能である。

上書き消去の方法は、

・標準：文書データの管理情報のみを削除する

・レベル１：文書データのデータ領域にすべて０のデータを３回上書き消去する

・レベル２：文書データのデータ領域にランダムな値を２回、その後すべて０のデータを１回上書き消去する

である。本機能は、下記の時実行される。

・一般利用者が意識する必要なく、表２．に示した時点で発生する利用済み文書データをキーオペレーターがセキュリティーモード運用管理機能により設定した「ハードディスクデータ消去レベル」標準、レベル１またはレベル２に従い、上書き消去を実行する。

・キーオペレーターがコントロールパネルより、セキュリティーモード運用管理機能「ハードディスク初期化」で指示したレベル１またはレベル２の方法で、文書データの上書き消去を実行する。

６．１．２．　キーオペレーター認証機能（SF.ADM_IA）

この機能は、ハードディスクドライブロック管理機能(SF.HDMNG)およびセキュリティーモード運用管理機能(SF.ADMMNG)で提供される「ハードディスクドライブロックパスワード」、「キーオペレーターパスワード」、「ハードディスクデータ消去レベル」の設定データの操作および「ハードディスク初期化」の指示を認証されたキーオペレーターのみが行えるように制御する。

操作や指示を許可する前に、コントロールパネルから入力されたキーオペレーターのパスワードにより、操作者がキーオペレーターであることを識別・認証する。

SF.ADM_IA は、キーオペレーターの識別・認証の前に上述した運用管理機能の操作や指示を一切許可しない。

キーオペレーターがパスワードを入力する時は、入力された文字データ１字ごとにダミー文字‘*’を表示する。

キーオペレーターのパスワードが正しく入力、キーオペレーターの認証に成功した時には、設定データの操作や指示を許可する。

入力されたキーオペレーターのパスワードが不正であり、キーオペレーターの認証に失敗した時には、拒否音により通知する。
１回認証に失敗すると１秒間認証を拒否し、１秒後に次の認証のインターフェースを与える。

６．１．３．　ハードディスクドライブロック管理機能（SF.HDMNG）

この機能は、キーオペレーターがハードディスクドライブロックの管理を行うための機能であり、SF.ADM_IA によりキーオペレーターと識別・認証された時のみ「ハードディスクドライブロックパスワード」の設定・変更およびドライブロックの解除ができるよう許可し、実行する。

「ハードディスクドライブロックパスワード」の設定・変更は、キーオペレーターが入力する「ハードディスクドライブロックのパスワード」に対して、以下の規則に従い、許容値を検証する。

・８文字以上３２文字以下

・英大文字、英小文字、数字、記号

許容値の検証において、規則に従っている時には、デジタル複合機内のメモリーおよびハードディスク装置のドライブロックパスワードを設定・変更する。

規則に従っていない時には、拒否音により通知し、設定・変更を拒否する。

「ハードディスクドライブロックパスワード」のドライブロックの解除は、既にハードディスク装置に「ハードディスクドライブロックパスワード」が設定されている時、キーオペレーターがコントロールパネルよりロック解除を選択・指示すると、デジタル複合機内のメモリーおよびハードディスク装置に設定されていたパスワードを未設定状態にする。

デジタル複合機起動時は検証された「ハードディスクドライブロックパスワード」を用いてハードディスク装置に対して識別・認証を依頼する。

６．１．４．　セキュリティーモード運用管理機能（SF.ADMMNG）

この機能は、キーオペレーターが運用を行うための管理機能であり、SF.ADM_IA によりキーオペレーターと識別・認証された時のみ、「キーオペレーターパスワード」の設定・変更、「ハードディスクデータ消去レベル」の設定・変更、「ハードディスク初期化」の指示をできるよう許可し、実行する。

「キーオペレーターパスワード」の設定・変更は、キーオペレーターが入力するキーオペレーターパスワードに対して、以下の規則に従い、許容値を検証する。

・８文字固定

・英大文字、英小文字、数字、記号

・同一文字の８文字連続は禁止

許容値の検証において、規則に従っている時には、キーオペレーターのパスワードを設定・変更する。

規則に従っていない時には拒否音により通知し、設定・変更を拒否する。

「ハードディスクデータ消去レベル」の設定・変更は、現在選択されている上書き消去の方法をパネルに明示、コントロールパネルより方法を選択、その選択された上書き消去の方法を再明示することにより設定・変更する。

「ハードディスクデータ消去レベル」の設定・変更では、以下の方法が選択できる。

・標準：文書データの管理情報のみを削除する

・レベル１：文書データのデータ領域にすべてＯのデータを 3 回上書き消去する

・レベル２：文書データのデータ領域にランダムな値を 2 回、その後すべてＯのデータを 1 回上書き消去する

キーオペレーターは、上述のようにハードディスク蓄積データ上書き機能のふるまいを決定したり、「ハードディスクデータ消去レベル」を標準にすることによりハードディスク蓄積データ上書き機能を停止させることができる。

「ハードディスク初期化」は、コントロールパネルより上書き消去の方法を選択・指示することにより、その選択された方法を明示し、ハードディスク蓄積データ上書き機能を動作させ、上書き消去を実行する。

「ハードディスク初期化」の指示では以下の方法が選択できる。

・レベル１：文書データのデータ領域にすべてＯのデータを 3 回上書き消去する

・レベル２：文書データのデータ領域にランダムな値を 2 回、その後すべてＯのデータを 1 回上書き消去する

６．１．５．　サービス技術者認証機能（SF.SE_IA）

この機能は、セキュリティーモード保守管理機能(SF.SEMNG)で提供される「サービス技術者パスワード」の設定データの操作および「システム初期化」の指示を認証されたサービス技術者のみが行えるように制御する。

操作や指示を許可する前に、コントロールパネルから入力されたサービスモード設定手順、サービス技術者のパスワードにより、操作者がサービス技術者であることを識別・認証する。

SF.SE_IA は、サービス技術者の識別・認証の前にセキュリティーモード保守管理機能(SF.SEMNG)の操作や指示を一切許可しない。

サービス技術者がパスワードを入力する時は、入力された文字データ１字ごとにダミー文字‘*’を表示する。

サービス技術者のパスワードが正しく入力、サービス技術者の認証に成功した時には、設定データの操作や指示を許可する。

入力されたサービス技術者のパスワードが不正であり、サービス技術者の認証に失敗した時には、拒否音により通知する。

１回認証に失敗すると１秒間認証を拒否し、１秒後に次の認証のインターフェースを与える。

６．１．６．　セキュリティーモード保守管理機能（SF.SEMNG）

この機能は、サービス技術者が保守作業を行うための管理機能であり、SF.SE_IA によりサービス技術者と識別・認証された

時のみ、「サービス技術者パスワード」の設定・変更、「システム初期化」の指示をできるよう許可し、実行する。
「サービス技術者パスワード」の設定・変更は、サービス技術者が入力するサービス技術者パスワードに対して、以下の規則に従い、許容値を検証する。
・８文字固定
・英大文字、英小文字、数字、記号
・同一文字の８文字連続は禁止
許容値の検証において、規則に従っている時には、サービス技術者のパスワードを設定・変更する。
規則に従っていない時には拒否音により通知し、設定・変更を拒否する。
「システム初期化」は、コントロールパネル上に表示されている「システム初期化」を指示することにより実行され「ハードディスクドライブロックパスワード」、「ハードディスクデータ消去レベル」、「キーオペレーターパスワード」、「サービス技術者パスワード」の設定データを初期化（初期設定値に戻す操作）する。
「システム初期化」により「ハードディスクデータ消去レベル」は標準になり、ハードディスク蓄積データ上書き機能は停止する。

６．２．　セキュリティー機能強度

確率的または順列的メカニズムは、キーオペレーター認証機能（SF.ADM_IA）、サービス技術者認証機能（SF.SE_IA）で利用している。
本ＴＯＥのセキュリティー機能強度はＳＯＦ－基本を主張する。

６．３．　保証手段

本ＳＴにおけるセキュリティー保証要件の各コンポーネントに対する保証手段となるドキュメントを表 15. に示す。

表 15. 保証手段

保証ｺﾝﾎﾟｰﾈﾝﾄ ID	保証ｺﾝﾎﾟｰﾈﾝﾄ	保証手段
ACM_CAP.2	構成要素	データセキュリティーキット　DA-SC06　構成管理計画書
		データセキュリティーキット　DA-SC06　構成表
ADO_DEL.1	配付手続き	データセキュリティーキット　DA-SC06　配付手順書
ADO_IGS.1	設置、生成、及び立上げ手順	・取扱説明書　データセキュリティーキット　DA-SC06 ・サービス技術者用　設置工事手順書 データセキュリティーキット　DA-SC06 ・Service Manual　デジタル複合機　DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06 ・Installation Instructions for Service Technicians Data Security Kit DA-SC06 ・Service Manual Digital Imaging Systems DP-8032 / 8025
ADV_FSP.1	非形式的機能仕様	データセキュリティーキット　DA-SC06　　機能仕様書
ADV_HLD.1	記述的上位レベル設計	データセキュリティーキット　DA-SC06　　設計仕様書
ADV_RCR.1	非形式的対応の実証	データセキュリティーキット　DA-SC06　　機能対応書
AGD_ADM.1	管理者ガイダンス	・取扱説明書（基本編）デジタル複合機　DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA ・取扱説明書　データセキュリティーキット　DA-SC06 ・サービス技術者用　設置工事手順書 データセキュリティーキット　DA-SC06 ・Service Manual　デジタル複合機　DP-8032 / 8025 ・Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06 ・Installation Instructions for Service Technicians Data Security Kit DA-SC06 ・Service Manual Digital Imaging Systems DP-8032 / 8025
AGD_USR.1	利用者ガイダンス	・取扱説明書（基本編）デジタル複合機　DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA ・取扱説明書　データセキュリティーキット　DA-SC06 ・Operating Instructions(For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06
ATE_COV.1	カバレージの証拠	データセキュリティーキット　DA-SC06　テスト計画書／成績書
ATE_FUN.1	機能テスト	
ATE_IND.2	独立試験・サンプル	ＴＯＥ
AVA_SOF.1	ＴＯＥセキュリティー機能強度評価	データセキュリティーキット　DA-SC06　セキュリティー機能強度分析書
AVA_VLA.1	開発者脆弱性分析	データセキュリティーキット　DA-SC06　脆弱性分析書

７．　ＰＰ主張

本ＴＯＥはＰＰには準拠していない。

８．　根拠

８．１．　セキュリティー対策方針根拠

表 16. にセキュリティー対策方針と脅威、組織のセキュリティー方針および前提条件の対応を示す。

表 16. セキュリティー対策方針と脅威、組織のセキュリティー方針および前提条件の対応

※	T.RECOVER	P.OWMETHOD	A.SETSEC	A.ADMIN	A.SE
O.HDLMNG	○				
O.RESIDUAL		○			
OE.AUTH		○	○		
OE.ADMIN				○	
OE.SE					○
OE.HDD	○				

※横に脅威、組織のセキュリティー方針および前提条件を、縦にセキュリティー対策方針を示す。
○：対象のセキュリティー対策方針が対応している脅威または前提条件を示す。

表 16. に示すようにすべてのセキュリティー対策方針は、ひとつ以上の脅威、組織のセキュリティー方針または前提条件に対応している。また、すべての脅威、組織のセキュリティー方針または前提条件は表 16. に示すようにいずれかのセキュリティー対策方針が対応している。

対応するセキュリティー対策方針が満足されることにより、脅威に対抗すること、組織のセキュリティー方針を実現できること、前提条件を保証することができる。

以下に、脅威、組織のセキュリティー方針および前提条件が対策されている根拠を示す。

T.RECOVER

脅威 T.RECOVER に対抗するには、ハードディスク装置内に蓄積された利用済み文書データの再生を不可能にしなければならない。そのために、認証されたキーオペレーターのみ、ハードディスク装置に「ハードディスクドライブロックパスワード」の設定を可能とし、ＴＯＥを運用することで対抗する。

OE.HDD により正しい「ハードディスクドライブロックパスワード」を入力しないとハードディスク装置内の文書データにアクセスできない機能をもつハードディスク装置を採用し、O.HDLMNG で認証されたキーオペレーターのみ、ハードディスク装置に「ハードディスクドライブロックパスワード」を設定することにより、利用済み文書データへのアクセスは不可能となる。

従って、ＰＣやツールを接続して利用済み文書データへアクセスを試みても、ハードディスク装置に設定されているハードディスクドライブロックパスワードと同一のパスワードを入力できない限り利用済み文書データの再生はできない。

以上の対策方針により、ハードディスク装置内に蓄積された利用済み文書データの不正な再生防止を図れる。

P.OWMETHOD

組織のセキュリティー方針 P.OWMETHOD を実現するには、「ハードディスクデータ消去レベル」を上書き消去を行うレベルであるレベル１またはレベル２に設定し、ハードディスク装置内に蓄積された利用済み文書データのデータ領域を上書き消去して、ＴＯＥを運用することが必要になる。O.RESIDUAL により、上書き消去を行わない標準レベルの他に「ハードディスクデータ消去レベル」：レベル１、レベル２の２種類のハードディスク蓄積データ上書き機能が提供され、そして、これらのレベルに対して OE.AUTH により保守時以外はキーオペレーターが「ハードディスクデータ消去レベル」を必ずレベル１またはレベル２に設定して運用することにより、運用時にはハードディスク装置内 に蓄積された利用済み文書データのデータ領域を上書き消去する。

以上の対策方針により、P.OWMETHOD を実現できる。

A.SETSEC

前提条件 A.SETSEC は、キーオペレーターがＴＯＥのセキュリティー機能を有効にして、「ハードディスクドライブロックパスワード」を設定して運用することを求めている。そのために、OE.AUTH によりキーオペレーターは、保守時以外においては運用管理機能を利用し、「ハードディスクドライブロックパスワード」を設定して運用する。これにより、A.SETSEC を実現できる。

A.ADMIN

前提条件 A.ADMIN は、キーオペレーターが信頼できることを求めている。そのために、OE.ADMIN により、責任者はキーオペレーターの役割を理解した上でキーオペレーターの人選を厳重に行うとともに、課せられたキーオペレーターの業務を遂行できるように管理や、必要な知識が習得できるよう教育を実施する。これにより、A.ADMIN を実現できる。

A.SE

前提条件 A.SE は、サービス技術者（デジタル複合機 DP-8032 / 8025 の保守を委託している企業の社員）が信頼できることを求めている。そのために、サービス技術者がデジタル複合機 DP-8032 / 8025 の保守作業を行う時には、OE.SE により責任者またはキーオペレーターは、サービス技術者がデジタル複合機 DP-8032 / 8025 の保守を委託している企業の社員であることを確認しなければならない。これにより、A.SE は実現できる。

８．２．　セキュリティー要件根拠

８．２．１．　セキュリティー機能要件根拠

８．２．１．１．　セキュリティー機能要件 FIT_SOS.1、FIT_MTD.1 導入理由

FIT_SOS.1：ＩＴ環境の秘密の検証、FIT_MTD.1：管理者データの管理の導入理由を下記に示す。

管理者データとは、キーオペレーター、サービス技術者のみがアクセスできるＩＴ環境のセキュリティー機能の制御データである。

ＩＴ環境の秘密の検証およびＩＴ環境のセキュリティー機能の制御を、ＴＯＥセキュリティー機能要件でおこなう。

OE.HDD が正しく認証を実行できるようにするためには、ハードディスクドライブロックパスワードを改変、消去より保護する必要があるので、ＴＯＥセキュリティー機能要件が必要である。

ハードディスクドライブロックパスワードは、ＩＴ環境のハードディスク装置の TSF データであるとともにＩＴ環境の秘密であり、ＴＯＥから見れば利用者データである。しかし、キーオペレーター、サービス技術者のみが操作できる TSF データの特性を有する。

このようなデータをＴＯＥの FIA/FMT クラスでは扱えず、一般利用者のアクセス制御の対象でもない。

また、FDP_ACC/FDP_ACF でも、常に許可されるため扱うことができない。

このため、新たな管理的特性を有する機能要件を定義する必要がある。

FIT_SOS.1 は FIA_SOS.1、FIT_MTD.1 は FMT_MTD.1 を参考に導入した。

８．２．１．２．　セキュリティー機能要件とセキュリティー対策方針の関係

表 17. にセキュリティー機能要件とセキュリティー対策方針の関係を示す。

表 17. セキュリティー機能要件とセキュリティー対策方針の関係

※１	O.HDLMNG	O.RESIDUAL	OE.HDD
FDP_RIP.1		○	
FIA_AFL.1(1)	○	○	
FIA_AFL.1(2)	○	○	
FIA_SOS.1(1)	○	○	
FIA_SOS.1(2)	○	○	
FIA_UID.2(1)	○	○	
FIA_UID.2(2)	○	○	
FIA_UAU.2(1)	○	○	
FIA_UAU.2(2)	○	○	
FIA_UAU.7(1)	○	○	
FIA_UAU.7(2)	○	○	
FMT_MOF.1		○	
FMT_MTD.1(1)		○	
FMT_MTD.1(2)	○	○	
FMT_MTD.1(3)	○	○	
FMT_SMF.1	○	○	
FMT_SMR.1	○	○	
FPT_RVM.1	○	○	
FIT_SOS.1	○		
FIT_MTD.1	○		
FIA_UID.2(IT)※２			○
FIA_UAU.2(IT)※２			○

※１：横にセキュリティー対策方針、縦にセキュリティー機能要件を示す。
※２：ＩＴ環境のセキュリティー機能要件、それ以外はＴＯＥセキュリティー機能要件を示す。
○：対象のセキュリティー機能要件が対応しているセキュリティー対策方針を示す。

表 17. に示すようにすべてのセキュリティー機能要件は、セキュリティー対策方針に対応している。
また、すべてのセキュリティー対策方針は表 17. に示すようにいずれかのセキュリティー機能要件に対応している。
以下に、すべてのセキュリティー対策方針が機能要件により対策が保証されている根拠を示す。

O.HDLMNG

キーオペレーターであることをFIA_UID.2(1)、FIA_UAU.2(1)で識別・認証することにより、正当なキーオペレーターの操作であることを確認できる。FIA_AFL.1(1)により、キーオペレーターが１回認証に失敗した場合１秒間以上次の認証が受け付けられないため、連続した攻撃回数を削減する。FIA_UAU.7(1)により、パスワードを入力した文字データ１字ごとに‘*’を表示して、パスワードを秘匿する。FMT_MTD.1(2)により、キーオペレーターのみ「キーオペレーターパスワード」の改変を許可し、不正な攻撃におけるパスワード一致の可能性を低くできる。また、FIA_SOS.1(1)により、キーオペレーターパスワードを設定・変更する時には、定義されたパスワードの規則に合致しているか検証する。

FMT_SMF.1は上記のキーオペレーターパスワードを管理するためのセキュリティー管理機能を提供する。

FIT_MTD.1により、ハードディスクドライブロックパスワードの改変、消去をキーオペレーターのみに制限し、FIT_SOS.1により、ハードディスクドライブロックパスワードを設定・変更する時には、定義されたパスワードの規則に合致しているか検証する。

キーオペレーターパスワード、サービス技術者パスワード、ハードディスクドライブロックパスワードの初期化（初期設定値に戻す操作）を不正に実行されないよう、FMT_MTD.1(2)により「キーオペレーターパスワード」の初期化、FMT_MTD.1(3)により「サービス技術者パスワード」の初期化、FIT_MTD.1により「ハードディスクドライブロックパスワード」の初期化をサービス技術者のみに制限する。

上記の初期化をセキュアに行うために、サービス技術者の識別・認証を行う。サービス技術者であることをFIA_UID.2(2)、FIA_UAU.2(2)で識別・認証することにより、正当なサービス技術者の操作であることを確認できる。FIA_AFL.1(2)により、サービス技術者が１回認証に失敗した場合１秒間以上次の認証が受け付けられないため、連続した攻撃回数を削減する。

FIA_UAU.7(2)により、パスワードを入力した文字データ１字ごとに‘*’を表示して、パスワードを秘匿する。

FMT_MTD.1(3)により、サービス技術者のみ「サービス技術者パスワード」の改変、初期化を許可し、不正な攻撃におけるパスワード一致の可能性を低くできる。また、FIA_SOS.1(2)により、サービス技術者パスワードを設定・変更する時には、定義されたパスワードの規則に合致しているか検証する。

FMT_SMF.1は上記のサービス技術者パスワードを管理するためのセキュリティー管理機能を提供する。

FMT_SMR.1により、キーオペレーター、サービス技術者の役割を維持する。

FPT_RVM.1により、ＴＯＥセキュリティー機能が確実に呼び出されバイパスされることはない。

以上のセキュリティー機能要件により、ＴＯＥは認証されたキーオペレーターのみ「ハードディスクドライブロックパスワード」をハードディスク装置に設定することにより、ハードディスク装置内に蓄積された利用済み文書データの再生を不可能にするセキュリティー対策方針 O.HDLMNG を実現できる。

O.RESIDUAL

FMT_MTD.1(1)により、「ハードディスクデータ消去レベル」の問い合わせ、改変をキーオペレーター のみに制限し、「ハードディスクデータ消去レベル」の標準、レベル１、レベル２の設定を可能としている。

（但し「システム初期化」機能による「ハードディスクデータ消去レベル」の標準への改変のみサービス技術者も可能である）

上記改変をセキュアに行うために、キーオペレーターの識別・認証を行う。キーオペレーターであることを FIA_UID.2(1)、FIA_UAU.2(1)で識別・認証することにより、正当なキーオペレーターの操作であることを確認できる。FIA_AFL.1(1)により、キーオペレーターが１回認証に失敗した場合１秒間以上次の認証が受け付けられないため、連続した攻撃回数を削減する。FIA_UAU.7(1)により、パスワードを入力した文字データ１字ごとに‘*’を表示して、パスワードを秘匿する。

FMT_MTD.1(2)により、キーオペレーターのみ「キーオペレーターパスワード」の改変を許可し、不正な攻撃におけるパスワード一致の可能性を低くできる。また、FIA_SOS.1(1)により、キーオペレーターパスワードを設定・変更する時には、定義されたパスワードの規則に合致しているか検証する。

FMT_SMF.1 は上記のキーオペレーターパスワードを管理するためのセキュリティー管理機能を提供する。

「キーオペレーターパスワード」、「サービス技術者パスワード」、「ハードディスクデータ消去レベル」が不正に初期化されないよう、FMT_MTD.1(2)により「キーオペレーターパスワード」の初期化、FMT_MTD.1(3)により「サービス技術者パスワード」の初期化、FMT_MTD.1(1)により「ハードディスクデータ消去レベル」の初期化（「システム初期化」による標準レベルへの改変）をサービス技術者のみに制限する。

上記の初期化をセキュアに行うために、サービス技術者の識別・認証を行う。サービス技術者であることを FIA_UID.2(2)、FIA_UAU.2(2)で識別・認証することにより、正当なサービス技術者の操作であることを確認できる。FIA_AFL.1(2)により、サービス技術者が１回認証に失敗した場合１秒間以上次の認証が受け付けられないため、連続した攻撃回数を削減する。

FIA_UAU.7(2)により、パスワードを入力した文字データ１字ごとに‘*’を表示して、パスワードを秘匿する。

FMT_MTD.1(3)により、サービス技術者のみ「サービス技術者パスワード」の改変、初期化を許可し、不正な攻撃におけるパスワード一致の可能性を低くできる。また、FIA_SOS.1(2)により、サービス技術者パスワードを設定・変更する時には、定義されたパスワードの規則に合致しているか検証する。

FMT_SMF.1 は上記のサービス技術者パスワードを管理するためのセキュリティー管理機能を提供する。

FMT_MOF.1 により、セキュリティー機能であるハードディスク蓄積データ上書き機能の動作をキーオペレーター、サービス技術者のみに限定しているので、ハードディスク蓄積データ上書き機能はキーオペレーター、サービス技術者しか設定、指示できない。FMT_SMR.1 により、キーオペレーター、サービス技術者の役割を維持する。

FDP_RIP.1 により、ハードディスク装置内に蓄積された利用済み文書データの以前のどの情報の内容も利用できなくする。

FPT_RVM.1 により、ＴＯＥセキュリティー機能が確実に呼び出されバイパスされることはない。

以上のセキュリティー機能要件により、ＴＯＥは、上書き消去を行わない標準レベルの他に、「ハードディスクデータ消去レベル」レベル１､レベル２の２種類のハードディスク蓄積データ上書き機能を提供でき、セキュリティー対策方針 O.RESIDUAL を実現できる。

OE.HDD

ハードディスク装置は、FIA_UID.2(IT)、FIA_UAU.2(IT)により識別・認証に成功したＴＯＥにのみアクセスを許可する。

これによりハードディスク装置の不正なアクセスを防止する OE.HDD を実現できる。

８．２．１．３．　セキュリティー機能要件 FIT_SOS.1、FIT_MTD.1 の追加による保証要件の適切性

FIT_SOS.1 は、FIA_SOS.1 の「秘密」を「ＩＴ環境の秘密」に変更するだけで意味的には FIA_SOS.1 と同じであり、FIT_MTD.1 は、FMT_MTD.1 の「TSF データ」を「管理者データ」に変更するだけで意味的には FMT_MTD.1 と同じである。よって、FIT_SOS.1、FIT_MTD.1 の追加によって特別な保証要件は必要なく、FIA_SOS.1、FMT_MTD.1 同じ保証要件で対応できる。

８．２．２．　セキュリティー機能要件間の依存性

表 18. にセキュリティー機能要件の依存関係を示す。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 18. 機能要件の依存性

機能要件	CC が要求する依存性	本ＳＴにおける依存関係
FDP_RIP.1	なし	なし
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1) 説明:FIA_UAU.2 は FIA_UAU.1 の上位階層のセキュリティー機能要件であるため、FIA_UAU.1 への依存性は満足される。
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2) 説明:FIA_UAU.2 は FIA_UAU.1 の上位階層のセキュリティー機能要件であるため、FIA_UAU.1 への依存性は満足される。
FIA_SOS.1(1)	なし	なし
FIA_SOS.1(2)	なし	なし
FIA_UID.2(1)	なし	なし
FIA_UID.2(2)	なし	なし
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1) 説明:FIA_UID.2 は FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満足される。
FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2) 説明:FIA_UID.2 は FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満足される。
FIA_UAU.7(1)	FIA_UAU.1	FIA_UAU.2(1) 説明:FIA_UAU.2 は FIA_UAU.1 の上位階層のセキュリティー機能要件であるため、FIA_UAU.1 への依存性は満足される。
FIA_UAU.7(2)	FIA_UAU.1	FIA_UAU.2(2) 説明:FIA_UAU.2 は FIA_UAU.1 の上位階層のセキュリティー機能要件であるため、FIA_UAU.1 への依存性は満足される。
FMT_MOF.1	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1
FMT_MTD.1(2)	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1
FMT_MTD.1(3)	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1
FMT_SMF.1	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.2(1)、FIA_UID.2(2) 説明:FIA_UID.2 は FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満足される。
FPT_RVM.1	なし	なし
FIT_SOS.1	なし	なし
FIT_MTD.1	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1
FIA_UID.2(IT) ※	なし	なし
FIA_UAU.2(IT)※	FIA_UID.1(IT)	FIA_UID.2(IT) 説明:FIA_UID.2 は FIA_UID.1 の上位階層のセキュリティー機能要件であるため、FIA_UID.1 への依存性は満足される。

※：ＩＴ環境のセキュリティー機能要件、それ以外はＴＯＥセキュリティー機能要件を示す。

８．２．３．　セキュリティー機能要件の相互作用

表 19. にセキュリティー機能要件の相互作用の関係を示す。

表 19. セキュリティー機能要件の相互作用

セキュリティー機能要件	迂回	非活性化
FDP_RIP.1	FPT_RVM.1	FMT_MOF.1
FIA_AFL.1(1)	FPT_RVM.1	－
FIA_AFL.1(2)	FPT_RVM.1	－
FIA_SOS.1(1)	FPT_RVM.1	－
FIA_SOS.1(2)	FPT_RVM.1	－
FIA_UID.2(1)	FPT_RVM.1	－
FIA_UID.2(2)	FPT_RVM.1	－
FIA_UAU.2(1)	FPT_RVM.1	－
FIA_UAU.2(2)	FPT_RVM.1	－
FIA_UAU.7(1)	FPT_RVM.1	－
FIA_UAU.7(2)	FPT_RVM.1	－
FMT_MOF.1	FPT_RVM.1	－
FMT_MTD.1(1)	FPT_RVM.1	－
FMT_MTD.1(2)	FPT_RVM.1	－
FMT_MTD.1(3)	FPT_RVM.1	－
FMT_SMF.1	－	－
FMT_SMR.1	－	－
FPT_RVM.1	－	－
FIT_SOS.1	FPT_RVM.1	－
FIT_MTD.1	FPT_RVM.1	－

８．２．３．１．　迂回

FPT_RVM.1

キーオペレーターの識別・認証に関するFIA_UID.2(1)、FIA_UAU.2(1)、FIA_UAU.7(1)は、キーオペレーターがセキュリティーに関する運用管理機能を使用するにあたり、キーオペレーターの識別・認証が必ず実行されるため、アクション前の利用者識別、アクション前の利用者認証、保護された認証フィードバックを迂回することはできない。認証失敗時の取り扱い関するFIA_AFL.1(1)も認証失敗時に必ず呼び出されるため迂回することはできない。

サービス技術者の識別・認証に関するFIA_UID.2(2)、FIA_UAU.2(2)、FIA_UAU.7(2)は、サービス技術者がセキュリティーに関する保守管理機能を使用するにあたり、サービス技術者の識別・認証が必ず実行されるため、アクション前の利用者識別、アクション前の利用者認証、保護された認証フィードバックを迂回することはできない。認証失敗時の取り扱い関するFIA_AFL.1(2)も認証失敗時に必ず呼び出されるため迂回することはできない。

残存情報保護に関するFDP_RIP.1は、利用済み文書データ発生時点およびキーオペレーター指示による「ハードディスク初期化」が実行された時に必ず呼び出されるため迂回することはできない。

秘密の検証に関するFIA_SOS.1(1)は、「キーオペレーターパスワード」の設定・変更時、FIA_SOS.1(2)は、「サービス技術者パスワード」の設定・変更時、必ず呼び出されるため迂回することはできない。ＴＳＦデータの管理に関するFMT_MTD.1(1)、FMT_MTD.1(2)は「ハードディスクデータ消去レベル」および「キーオペレーターパスワード」の改変、初期化時に必ず呼び出されるため迂回することはできない。

同様にＴＳＦデータの管理に関するFMT_MTD.1(3)も「サービス技術者パスワード」の改変・初期化時に必ず呼び出されるため迂回することはできない。

セキュリティー機能のふるまいに関するFMT_MOF.1は、キーオペレーターの識別・認証後の「ハードディスクデータ消去レベル」の設定・変更時、「ハードディスク初期化」指示時、サービス技術者の「ハードディスクデータ消去レベル」初期化時必ず呼び出されるため迂回することはできない。

ＩＴ環境の秘密の検証に関するFIT_SOS.1は、キーオペレーターの識別・認証後の「ハードディスクドライブロックパスワード」の設定・変更時必ず呼び出されるため迂回することはできない

管理者データの管理に関するFIT_MTD.1もキーオペレーターの識別・認証後の「ハードディスクドライブロックパスワード」の改変・消去時、サービス技術者の識別・認証後の「ハードディスクドライブロックパスワード」の初期化時に必ず呼び出されるため迂回することはできない。

８．２．３．２．　非活性化

FMT_MOF.1

ハードディスク蓄積データ上書き機能（FDP_RIP.1）は、FMT_MOF.1により非活性化する役割はキーオペレーター、サービス技術者に制限される。

８．２．３．３．　　破壊

本ＴＯＥは、セキュリティー機能のふるまいの管理をキーオペレーター、サービス技術者のみに許可している。このため、不正なサブジェクトが存在せずアクセス制御を実施する必要もない。従って、不正なサブジェクトによりＴＳＦが破壊されることはない。

８．２．３．４．　　無効化を狙った攻撃の検出

本ＴＯＥでは、FPT_RVM.1 により運用管理機能の使用を正当なキーオペレーターのみに限定するとともに、保守管理機能の使用を正当なサービス技術者のみに限定しているため、監査に関する FAU クラスの要件は必要ない。

８．２．４．　セキュリティー機能強度レベルの妥当性

本ＴＯＥは、攻撃能力については、低レベルであることを想定している。従って、セキュリティー機能強度レベルがＳＯＦ－基本であることは妥当である。

すべての確率的または順列的メカニズムがＳＯＦ－基本であるので、セキュリティー機能強度を満足している。

８．２．５．　保証要件根拠

本ＴＯＥはオフィスや公共施設内で利用され、その利用者は限定されている。また、攻撃能力については低レベルであることを想定しているため、評価保証レベルＥＡＬ２は妥当である。

８．３．　ＴＯＥ要約仕様根拠

８．３．１．　機能要約仕様根拠

表 20. にＴＯＥセキュリティー機能とセキュリティー機能要件の対応を示す。

表 20. ＴＯＥセキュリティー機能とセキュリティー機能要件の対応

※	SF.OVWRT	SF.ADM_IA	SF.HDMNG	SF.ADMMNG	SF.SE_IA	SF.SEMNG
FDP_RIP.1	○					
FIA_AFL.1(1)		○				
FIA_AFL.1(2)					○	
FIA_SOS.1(1)				○		
FIA_SOS.1(2)						○
FIA_UID.2(1)		○				
FIA_UID.2(2)					○	
FIA_UAU.2(1)		○				
FIA_UAU.2(2)					○	
FIA_UAU.7(1)		○				
FIA_UAU.7(2)					○	
FMT_MOF.1				○		○
FMT_MTD.1(1)				○		○
FMT_MTD.1(2)				○		○
FMT_MTD.1(3)						○
FMT_SMF.1				○		○
FMT_SMR.1				○		○
FPT_RVM.1	○	○	○	○	○	○
FIT_SOS.1			○			
FIT_MTD.1			○			○

※横にＴＯＥセキュリティー機能を、縦にセキュリティー機能要件を示す。
○：対象のセキュリティー機能要件が対応しているＴＯＥセキュリティー機能を示す。

以下に、ＴＯＥセキュリティー機能とセキュリティー機能要件の対応の根拠を示す。

FDP_RIP.1

SF.OVWRT は、表２．で示した利用済み文書データ発生時点で、ハードディスク装置内に蓄積されていた利用済み文書データのデータ領域に対し自動的に３回上書き消去し、また、キーオペレーターの指示による「ハードディスク初期化」の実行により、文書データのデータ領域に対し３回上書き消去する。

以上により、FDP_RIP.1は満足される。

FIA_AFL.1(1)
SF.ADM_IAは、キーオペレーターの認証が1回不成功時に、キーオペレーターの次の認証を1秒間受け付けないことにより、FIA_AFL.1(1)は満足される。

FIA_AFL.1(2)
SF.SE_IAは、サービス技術者の認証が1回不成功時に、サービス技術者の次の認証を1秒間受け付けないことにより、FIA_AFL.1(2)は満足される。

FIA_SOS.1(1)
SF.ADMMNGは、キーオペレーターのパスワードの設定・変更時、定められたパスワード規則に従っているか判定していることにより、FIA_SOS.1(1)は満足される。

FIA_SOS.1(2)
SF.SEMNGは、サービス技術者のパスワードの設定・変更時、定められたパスワード規則に従っているか判定していることにより、FIA_SOS.1(2)は満足される。

FIA_UID.2(1)
SF. ADM _IAは、キーオペレーターの識別を実施していることにより、FIA_UID.2(1)は満足される。

FIA_UID.2(2)
SF.SE_IAは、サービス技術者の識別を実施していることにより、FIA_UID.2(2)は満足される。

FIA_UAU.2(1)
SF.ADM_IAは、キーオペレーターの認証を実施していることにより、FIA_UAU.2(1)は満足される。

FIA_UAU.2(2)
SF.SE_IAは、サービス技術者の認証を実施していることにより、FIA_UAU.2(2)は満足される。

FIA_UAU.7(1)
SF.ADM_IAは、キーオペレーターの認証時、パスワードの入力された文字データ1字ごとに‘*’を表示していることにより、FIA_UAU.7(1)は満足される。

FIA_UAU.7(2)
SF.SE_IAは、サービス技術者の認証時、パスワードの入力された文字データ1字ごとに‘*’を表示していることにより、FIA_UAU.7(2)は満足される。

FMT_MOF.1
SF.ADMMNGはハードディスク蓄積データ上書き機能のふるまいを決定する、停止する、動作させることを識別・認証されたキーオペレーターに、SF.SEMNGはハードディスク蓄積データ上書き機能の停止を識別・認証されたサービス技術者に許可していることにより、FMT_MOF.1は満足される。

FMT_MTD.1(1)
SF. ADMMNGは「ハードディスクデータ消去レベル」の問い合わせ、改変を識別・認証されたキーオペレーターに、SF. SEMNGは「ハードディスクデータ消去レベル」の初期化を識別・認証されたサービス技術者に許可していることにより、FMT_MTD.1(1)は満足される。

FMT_MTD.1(2)
SF. ADMMNGは「キーオペレーターパスワード」の改変を識別・認証されたキーオペレーターに、SF. SEMNGは「キーオペレーターパスワード」の初期化を識別・認証されたサービス技術者に許可していることにより、FMT_MTD.1(2)は満足される。

FMT_MTD.1(3)
SF. SEMNGは、識別・認証されたサービス技術者にのみ「サービス技術者パスワード」の改変、初期化を許可していることにより、FMT_MTD.1(3)は満足される。

FMT_SMF.1
SF.ADMMNGは「キーオペレーターパスワード」を管理するためのセキュリティー管理機能を、SF.SEMNGは「サービス技術者パスワード」を管理するためのセキュリティー管理機能を提供していることにより、FMT_SMF.1は満足される。

FMT_SMR.1
SF. ADMMNGはキーオペレーター、SF. SEMNGはサービス技術者の役割を維持していることにより、FMT_SMR.1は満足される。

FPT_RVM.1

SF.OVWRT、SF.ADM_IA、SF.HDMNG、SF.ADMMNG、SF.SE_IA、SF.SEMNGは、迂回されずに必ず実行されることにより、FPT_RVM.1は満足される。

FIT_SOS.1

SF.HDMNGは、「ハードディスクドライブロックパスワード」の設定・変更時、定められたパスワード規則に従っているか判定していることにより、FIT_SOS.1は満足される。

FIT_MTD.1

SF. HDMNGは「ハードディスクドライブロックパスワード」の改変、消去を識別・認証されたキーオペレーターに、SF. SEMNGは、「ハードディスクドライブロックパスワード」の初期化を識別・認証されたサービス技術者に許可していることによりFIT_MTD.1は満足される。

８．３．２．　セキュリティー機能強度根拠

６．２．　セキュリティー機能強度で記述したように、確率的または順列的メカニズムは、キーオペレーター認証機能（SF.ADM_IA）、サービス技術者認証機能（SF.SE_IA）で利用している。

本ＴＯＥのセキュリティー機能強度はＳＯＦ－基本であり、これは５．４．ＴＯＥセキュリティー機能強度で主張したＳＯＦ－基本を満足している。

８．３．３．　保証手段根拠

表21.に保証手段とＥＡＬ２の保証コンポーネントの対応を示す。

表21. 保証手段とＥＡＬ２の保証コンポーネントの対応

保証手段	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
データセキュリティーキット　DA-SC06　構成管理計画書	○												
データセキュリティーキット　DA-SC06　構成表	○												
データセキュリティーキット　DA-SC06　配付手順書		○											
・取扱説明書　データセキュリティーキット　DA-SC06 ・サービス技術者用　設置工事手順書 データセキュリティーキット　DA-SC06 ・Service Manual　デジタル複合機　DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06 ・Installation Instructions for Service Technicians Data Security Kit DA-SC06 ・Service Manual Digital Imaging Systems DP-8032 / 8025			○										
データセキュリティーキット　DA-SC06　機能仕様書				○									
データセキュリティーキット　DA-SC06　設計仕様書					○								
データセキュリティーキット　DA-SC06　機能対応書						○							

・取扱説明書（基本編）デジタル複合機 DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA ・取扱説明書　データセキュリティーキット　DA-SC06 ・サービス技術者用　設置工事手順書 データセキュリティーキット　DA-SC06 ・Service Manual　デジタル複合機　DP-8032 / 8025 ・Operating Instructions (For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06 ・Installation Instructions for Service Technicians Data Security Kit DA-SC06 ・Service Manual Digital Imaging Systems DP-8032 / 8025							○						
・取扱説明書（基本編）デジタル複合機 DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA ・取扱説明書　データセキュリティーキット　DA-SC06 ・Operating Instructions (For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025 ・Operating Instructions Data Security Kit DA-SC06								○					
データセキュリティーキット　DA-SC06 テスト計画書／成績書									○	○			
ＴＯＥ											○		
データセキュリティーキット　DA-SC06 セキュリティー機能強度分析書												○	
データセキュリティーキット　DA-SC06　脆弱性分析書													○

ACM_CAP.2

データセキュリティーキット　DA-SC06　構成管理計画書および構成表は、ＴＯＥの構成要素を明確に識別しているので要件を満足する。

ADO_DEL.1

データセキュリティーキット　DA-SC06　配付手順書は、ＴＯＥを配送する時、セキュリティーを維持するために必要な手続きを記述しているので要件を満足する。

ADO_IGS.1

・取扱説明書　データセキュリティーキット　DA-SC06
・サービス技術者用　設置工事手順書　データセキュリティーキット　DA-SC06
・Service Manual　デジタル複合機　DP-8032 / 8025
・Operating Instructions Data Security Kit DA-SC06
・Installation Instructions for Service Technicians Data Security Kit DA-SC06
・Service Manual Digital Imaging Systems DP-8032 / 8025

は、ＴＯＥのセキュアな設置、生成　および立上げの手順を記述しているので要件を満足する。

ADV_FSP.1

データセキュリティーキット　DA-SC06　機能仕様書は、ＴＯＥの非形式的機能仕様を記述しているので要件を満足する。

ADV_HLD.1

データセキュリティーキット　DA-SC06　設計仕様書は、ＴＯＥの記述的上位レベル設計を記述しているので要件を満足する。

ADV_RCR.1

データセキュリティーキット　DA-SC06　機能対応書は、ＴＯＥの非形式的対応の実証を記述しているので要件を満足する。

AGD_ADM.1

・取扱説明書（基本編）デジタル複合機　DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA
・取扱説明書　データセキュリティーキット　DA-SC06
・サービス技術者用　設置工事手順書　データセキュリティーキット　DA-SC06
・Service Manual　デジタル複合機　DP-8032 / 8025
・Operating Instructions (For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025
・Operating Instructions Data Security Kit DA-SC06

・Installation Instructions for Service Technicians Data Security Kit DA-SC06
・Service Manual Digital Imaging Systems DP-8032 / 8025
はＴＯＥの管理者向けのガイダンスを記述しているので要件を満足する。

AGD_USR.1
・取扱説明書（基本編）デジタル複合機　DP-8032P / 8025P DP-8032V / 8025V DP-8032VA / 8025VA
・取扱説明書　データセキュリティーキット　DA-SC06
・Operating Instructions (For Copy & Network Scan Functions) Digital Imaging Systems DP-8032 / 8025
・Operating Instructions Data Security Kit DA-SC06
は、ＴＯＥの利用者向けのガイダンスを記述しているので要件を満足する。

ATE_COV
データセキュリティーキット　DA-SC06　テスト計画書／成績書は、識別されたテストと機能仕様に記述されたＴＳＦとの対応を記述しているので要件を満足する。

ATE_FUN.1
データセキュリティーキット　DA-SC06　テスト計画書／成績書は、テスト計画、テスト手順、期待されるテスト結果、実際のテスト結果を記述しているので要件を満足する。

ATE_IND.2
保証手段ＴＯＥは、評価者が独立テストを実施するのに必要なので要件を満足する。

AVA_SOF.1
データセキュリティーキット　DA-SC06　セキュリティー機能強度分析書は、ＴＯＥのセキュリティー機能強度を記述しているので要件を満足する。

AVA_VLA.1
データセキュリティーキット　DA-SC06　脆弱性分析書は、明白な脆弱性、識別された脆弱性について記述しているので要件を満足する。

８．４．　ＰＰ主張根拠
適合を主張するＰＰはない。