文書 ID:

CANON-Device03-001

Canon iR4570/iR3570/iR2870/iR2270 シリーズ用

iR セキュリティキット・B2
セキュリティターゲット

Version 1.11
2005/01/11

キヤノン株式会社

更新履歴

バージョン	日付	事由	作成者	検査者	承認者
Ver.1.00	2004/06/09	新規作成	関田	浅井／宮原	牧谷
Ver.1.01	2004/07/07	所見報告書 VCE-EOR-0001～0005 による指摘への対応修正 内部レビューによる修正	関田	宮原	牧谷
Ver.1.02	2004/07/12	内部レビューによる修正	関田	宮原	牧谷
Ver.1.03	2004/08/02	所見報告書 VCE-EOR-0006～0009 による指摘への対応修正 内部レビューによる修正	関田	宮原	牧谷
Ver.1.04	2004/08/17	内部レビューによる修正	関田	宮原	牧谷
Ver.1.05	2004/08/26	内部レビューによる修正	関田	宮原	牧谷
Ver.1.06	2004/09/01	内部レビューによる修正	関田	宮原	牧谷
Ver.1.07	2004/11/02	所見報告書 VCE-EOR-0022 による指摘への対応修正 内部レビューによる修正 対応機種追加による修正	関田	宮原	牧谷
Ver.1.08	2004/11/15	内部レビューによる修正	関田	宮原	牧谷
Ver.1.09	2004/12/09	内部レビューによる修正	関田	宮原	牧谷
Ver.1.10	2004/12/10	内部レビューによる修正	関田	宮原	牧谷
Ver.1.11	2005/01/11	所見報告書 VCE-EOR-0025～0026による指摘への対応修正	関田	宮原	牧谷

目 次

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張について記述する。

1.1. ST 識別

タイトル: Canon iR4570/iR3570/iR2870/iR2270 シリーズ用 iR セキュリティキット・B2 セキュリティターゲット

識別名: CANON-Device03-001

日付: 2005/01/11

バージョン: Version 1.11

作成者: キヤノン株式会社

TOE: Canon iR4570/iR3570/iR2870/iR2270 シリーズ用

iR セキュリティキット・B2　Version 1.04（日本国内）

iR Security Kit-B2 Version 1.04（海外）

（注）本 ST では、日本国内／海外向けいずれに対しても、iRセキュリティキット・B2 という記述を用いる。また、評価対象となる表示言語は、日本国内向けは日本語表示、海外向けは英語表示である。

キーワード: Canon、キヤノン、imageRUNNER、iR、iR4570、iR3570、iR2870、iR2270、デジタル複合機、コピー、プリント、ファクス、送信、ファクシミリ、残存情報保護、上書き、完全消去、暗号化、ボックス、セキュリティキット

CC のバージョン: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

CCIMB Interpretations-0210

和訳として、認証機関より提供された以下の文書を使用する。

情報技術セキュリティ評価のためのコモンクライテリア 1999 年 8 月バージョン 2.1（平成 13 年 1 月翻訳第 1.2 版）

補足-0210

評価保証レベル: EAL2

1.2. ST 概要

本ドキュメントは、デジタル複合機上で動作する、デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞のセキュリティ機能を強化するためのソフトウェアである＜iR セキュリティキット・B2＞についてのセキュリティ仕様を定めたセキュリティターゲットである。

TOE は、オプション製品＜iR セキュリティキット・B2＞として利用者に提供される。利用者は担当サービスに依頼し、TOE をデジタル複合機の HDD にインストールして、デジタル複合機の制御ソフトウェア全体を置き換えることにより、セキュリティ機能が強化されたデジタル複合機を使用できるようになる。

本 TOE は、デジタル複合機におけるテンポラリイメージデータやボックスに保存されたイメージデータを保護するために、以下の機能を提供する。

- HDD データ暗号化機能
- HDD データ完全消去機能
- ボックス利用者識別認証機能
- ボックス管理機能
- システム管理者識別認証機能
- システム管理者管理機能

1.3. CC 適合の主張

この TOE は、下記の CC に適合している。

- 機能要件－CC パート2適合
- 保証要件－CC パート3適合
- 保証レベル－EAL2 適合

本 ST が適合している PP はない。

1.4. 略語・用語

本 ST では以下の略語・用語を使用する。

Table 1-1 略語・用語

略語・用語	意味
HDD	デジタル複合機に搭載されるハードディスクのこと。TOE 本体および、保護資産が保存される。
I ファクス	ファクス文書の送受信を行うためのインフラとして、電話回線ではなく、インターネットを使用するインターネットファクスのこと。

MEAP	デジタル複合機上で動作するアプリケーションのプラットフォームのこと。 (Multifunctional Embedded Application Platform)
MEAP 認証アプリケーション	デジタル複合機の一般利用者の個人認証やディレクトリサービスとの連携を行うアプリケーション。部門別 ID 管理によるデジタル複合機の一般利用者の識別認証の代わりに使用することができる。
イメージデータ	読み込み、プリント、受信などによってデジタル複合機内に生成された画像データ。
コントローラー	TOE が動作するプラットフォームであり、CPU やメモリなどが実装されるハードウェアである。
システムボックス	I ファクスメモリ受信／ファクスメモリ受信した文書が保存されるボックスであり、文書のプリントまたは送信が可能である。
システム管理者	デジタル複合機の設定や管理を行う管理者のこと。ボックス利用者に代わって、ボックスの管理を行う場合もある。デジタル複合機上では、システム管理部門 ID を使用する利用者がシステム管理者として識別される。
システム管理モード	デジタル複合機に対しシステム管理者としての権限を維持するモード。このモードが維持されている間の操作は、システム管理者の権限での操作となる。このモードに移行するためには、システム管理者のシステム管理部門 ID とシステム管理暗証番号が必要になる。ID キーの押下により終了する。
スキャンエンジン・ADF	デジタル複合機を構成するハードウェアであり、紙媒体からイメージデータをデジタル複合機に読み込むための機器である。
操作部	デジタル複合機を構成するハードウェアであり、操作キーとタッチパネルから構成され、デジタル複合機を操作するときに使用される。
デジタル複合機	コピー機能、ファクス機能、プリンタ機能、送信（Universal Send）機能などを併せ持つ複写機のこと。それらの機能を使用するため、大容量の HDD を持つ。
ファクスボックス	I ファクス転送／ファクス転送された文書が保存されるボックスであり、保存された文書の再プリントが可能である。
フォーム画像	イメージ合成のためにデジタル複合機に登録された画像のこと。
プリンタエンジン	デジタル複合機を構成するハードウェアであり、デジタル複合機内のイメージデータを紙媒体に印刷するための機器である。
部門 ID	デジタル複合機を使用する部門もしくは個人の ID。部門 ID 管理が実施されている場合には、デジタル複合機を操作する前に、識別認証が必要になる。システム管理者は、部門 ID のうち、システム管理部門 ID として登録された利用者である。
部門別 ID 管理	利用者部門ごとにコピー枚数などを管理するために、利用者部門ごとに部門 ID および暗証番号を設定する機能である。部門別 ID 管理を実施すると、デジタル複合機の使用前に、正しい部門 ID および暗証番号によって識別認証されることが要求される。
文書	デジタル複合機内で取り扱われる利用者データであり、管理情報とイメージデータから構成される。

ボックス	デジタル複合機において読み込みやプリント、ファクス受信した文書を保存する領域。ユーザボックス、ファクスボックス、システムボックスの 3 種類が存在する。
メモリ受信	受信したファクス／ I ファクスを、プリントしないでシステムボックスに保存しておくこと。
ユーザボックス	デジタル複合機で一般利用者が読み込んだ文書や、PC からプリントした文書などが保存されるボックスであり、文書のプリントや送信などが可能である。
リモート UI	Web ブラウザからネットワークを経由してデジタル複合機にアクセスし、デジタル複合機の動作状況の確認やジョブの操作、ボックスに対する操作、各種設定などができるインターフェイスである。

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 範囲、役割、および資産について記述する。

2.1. TOE 種別

TOE は、デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞にセキュリティ機能を追加するオプションソフトウェアである。

TOE がデジタル複合機にインストールされる際には、既存のデジタル複合機の制御ソフトウェアは TOE で置き換えられる。

2.2. TOE 概要

TOE は、デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞にセキュリティ機能を追加するオプションソフトウェアであり、オプション製品＜iR セキュリティキット・B2＞として利用者に提供される。

利用者は、担当サービスに依頼し TOE をデジタル複合機の HDD にインストールすることにより、デジタル複合機全体を制御する制御ソフトウェアを TOE で置き換える。それにより、利用者はデジタル複合機に HDD データ暗号化機能と HDD データ完全消去機能を追加し、ボックス利用者識別認証機能およびシステム管理者識別認証機能を強化することができる。

デジタル複合機は、コピー機能、送信（Universal Send）機能、ファクス受信機能、ユーザボックス機能、プリンタ機能、などを併せ持つ複写機であり、大容量の HDD を持ち、コピーやプリント等の際にイメージデータを HDD に一時保存する。また、ユーザボックス機能と呼ばれる文書保存機能を持ち、プリントするイメージデータや読み込んだイメージデータを、デジタル複合機内のユーザボックスに保存しておくことができる。ユーザボックスを含む各ボックスには、ボックス利用者の識別認証のためのボックス暗証番号を設定することができる。

ボックス利用者は、ボックス一覧画面において該当ボックスを選択し、該当ボックス利用者として識別認証された後で、ボックスに保存されたイメージデータに対して、再プリントや、メールアドレスや共有フォルダへの送信などのイメージデータの読み出しを伴う操作を行うことができる。また、システム管理者は、システム管理者として識別認証されたのち、同様の操作を行うことができる。

TOE は、ボックスに保存されたイメージデータの不正な操作（再プリントや送信など）による暴露と、テンポラリイメージデータおよびボックスに保存されたイメージデータの消去時における残存情報の暴露を保護する目的で使用される。

デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞は、一般のオフィスなどにおいて、汎用的に使用されることを想定している、その想定する設置使用環境は以下の Figure 2-1 のとおりである。なお、Figure 2-1 は、デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞のオプションを含む機能を使用する場合の想定設置使用環境であり、使用しない機能がある場合には、設置環境は異なる場合がある。

使用方法によっては、デジタル複合機は、複写機としてスタンドアロンで使用される場合や、ファクス機として電話回線のみに接続される場合もある。

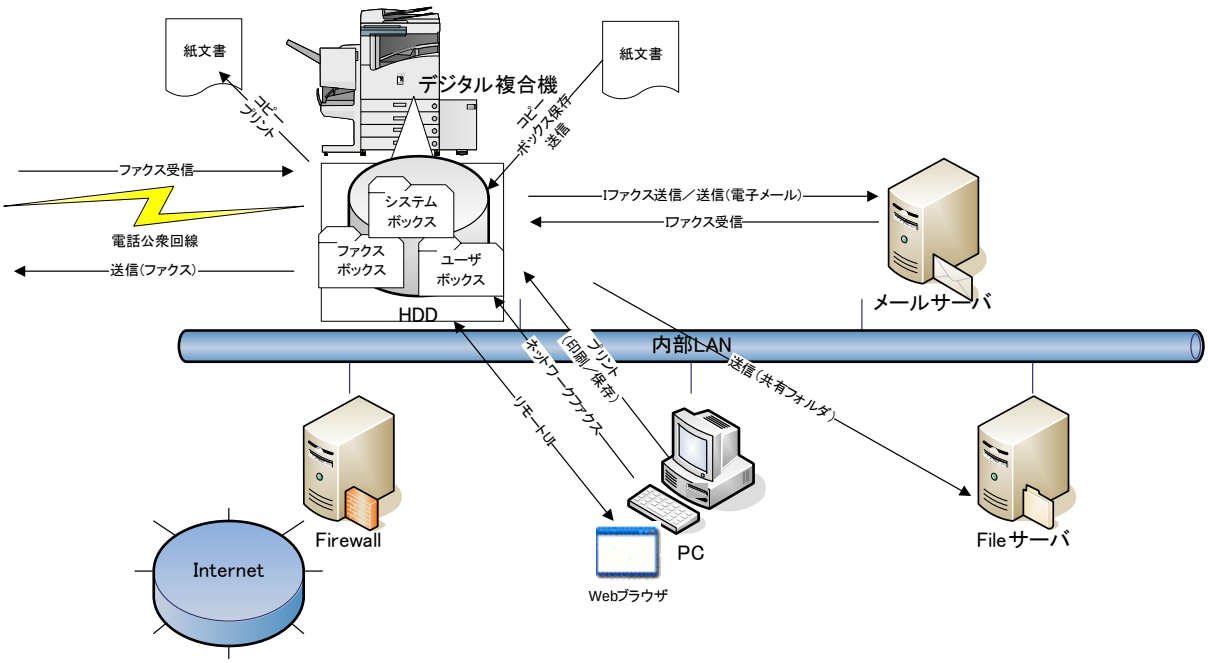


Figure 2-1 デジタル複合機＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞の想定設置使用環境

Figure 2-1 に記述のように、デジタル複合機には以下にあげる機能がある。

- **コピー機能**

  スキャナで紙文書を読み込んでプリントすることにより、紙文書の複写をする機能である。紙文書を読み込んだ際に、HDD 内にテンポラリイメージデータを生成する。

- **ファクス受信機能**

  ファクスや I ファクスから受信した文書を紙にプリントしたり、転送したりする機能である。受信時に HDD にテンポラリイメージデータを生成する。

  転送設定により、システムボックスに保存する前に、他のあて先やファクスボックスに振り分けることが可能である。またシステムボックスにメモリ受信した文書は、送信やプリントを行うことができ、ファクスボックスに受信した文書はプリントすることができる。その際、送信やプリントなどの操作によって、ボックスに保存されたイメージデータを読み出す際には、ボックス利用者として識別認証される必要がある。ファクスや I ファクスの受信時には、システムボックスおよびファクスボックスに保存されたイメージデータの読み出しを伴わないため、ボックス利用者の識別認証は不要となる。

- **ユーザボックス機能**

  スキャナから読み込んだ文書や、PC からボックス保存を指定してプリントした文書を、ユーザボックスにイメージデータとして保存する機能である。

  ユーザボックスに保存されたイメージデータをプリントや送信などの操作を行って読み出す際には、あらかじめボックス利用者として識別認証される必要がある。ユーザボックスにイメージデータを保存する場合には、ボックスに保存されたイメージデータの読み出しを伴わないため、ボックス利用者としての識別認証は行われない。

ユーザボックスに保存されたイメージデータは、文書結合やフォーム画像のイメージ合成などの編集をしてから出力することができる。

- **プリント機能**

  デジタル複合機をネットワークプリンタとして使用し、PC からのプリントデータをプリントする機能である。プリント時に HDD にテンポラリイメージデータを生成する。

- **送信（Universal Send）機能**

  スキャンした文書やユーザボックス／システムボックスに保存されている文書を、ファクス送信したり、TIFF や PDF ファイル形式に変換して電子メールや PC の共有フォルダなどのあて先に送信したりする機能である。

  また、PC 上からファクスドライバを使用して、デジタル複合機をネットワークファクスとして使用することができる。

  送信時には HDD 上にテンポラリイメージデータを生成する。

- **リモート UI 機能**

  利用者は、デジタル複合機本体の操作パネルを使用する以外に、リモート UI を使用することができる。リモート UI は利用者の Web ブラウザからネットワークを経由して、デジタル複合機にアクセスし、デジタル複合機の状況の確認やジョブの管理、ボックスの管理、各種設定などができる機能である。Web サーバ機能はデジタル複合機内に内蔵されているので、Web ブラウザ以外のソフトウェアを用意する必要はない。

TOE を＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞にインストールすることにより、上記の各機能を使用した際に生成されるテンポラリイメージデータと、ファクス受信機能およびユーザボックス機能で使用されるボックスに保存したイメージデータについて、HDD 上にデータ生成時に暗号化して保存し、消去時には完全消去する機能が追加される。これらの機能によりデジタル複合機の HDD 上にあるテンポラリイメージデータの残存情報と、ボックスに保存されたイメージデータを効果的に保護することが可能となる。

2.3. TOE の動作環境

TOE が動作する環境は以下の通りである。

Table 2-1 TOE が動作する対象のデジタル複合機と必須オプション（日本国内モデル）

デジタル複合機モデル名	必須オプション
Canon iR4570	PCI バス拡張キット・B1、セキュリティ拡張ボード（USB）・D1、増設メモリ（本体と合わせ 512MB 以上）
Canon iR4570F	
Canon iR3570	
Canon iR3570F	
Canon iR2870	
Canon iR2870F	

Canon iR2270	
Canon iR2270F	

Table 2-2 TOE が動作する対象のデジタル複合機と必須オプション（海外モデル）

デジタル複合機モデル名	必須オプション
Canon iR4570	Expansion Bus-B1、USB Application Interface Board-D1
Canon iR3570	
Canon iR2870	
Canon iR2270	

PC からプリントやファクス送信を行うためには、プリンタドライバやファクスドライバを PC にインストールして使用する必要がある。TOE に対応した主なプリンタドライバ、ファクスドライバは以下の通りである。

- Canon LIPS IV／LIPS LX Printer Driver（日本国内）
- Canon PCL5e / PCL6 Printer Driver（海外）
- Canon FAX Driver（日本国内／海外）

リモート UI を使用してデジタル複合機を操作するには、以下のソフトウェアを PC 上にインストールして使用する必要がある。

- Web ブラウザ

  動作環境の Web ブラウザは以下の通りである。ただし、評価構成の Web ブラウザは、Windows 上で動作する Microsoft Internet Explorer 6.0 のみである。

Table 2-3 リモート UI が動作する Web ブラウザ環境

動作 OS	ソフトウェア名	バージョン	修正パッチ
Windows	Microsoft Internet Explorer	5.01	SP2 以降
		5.5	SP2 以降
		6.0	－
	Netscape Communicator	4.75	－
		6.2.1	－
		7.1	－
Macintosh	Microsoft Internet Explorer	5.0	－
		5.2	－

- イメージプレビュー用プラグイン（リモート UI からプレビューを行うときのみ必要）

  Canon JBIG Image Viewer プラグインソフトウェア（デジタル複合機に添付）

また、I ファクスや送信（Universal Send）を実施するには、メールサーバや FTP サーバ、ファイルサーバが必要となる。

2.4. TOE の範囲

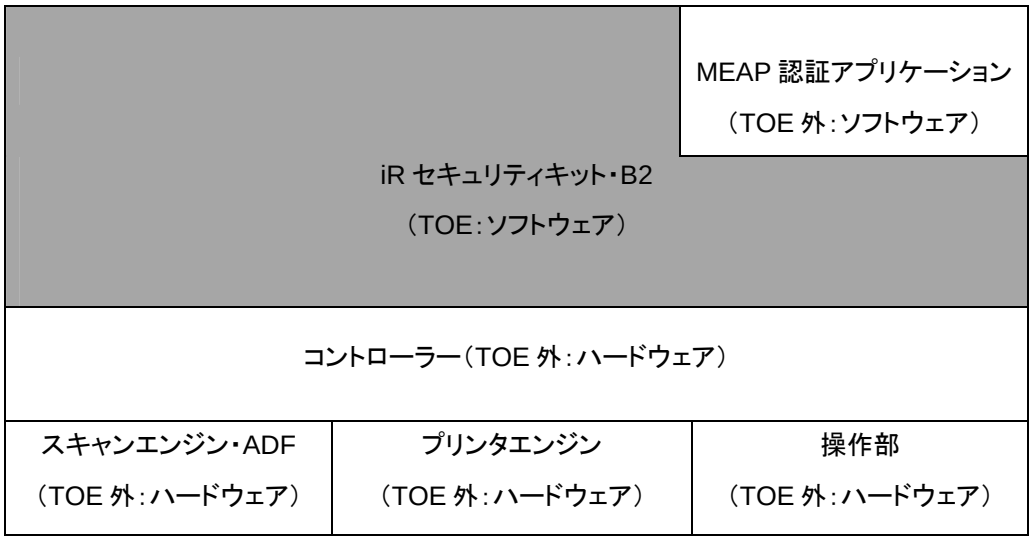
TOE の物理的範囲と論理的範囲は以下に記述のとおりとなる。

2.4.1.TOE の物理的範囲

TOE の物理的範囲は、2.2 章で示したデジタル複合機のすべて機能を制御するソフトウェア全体と、リモート UI を使用するための Web ブラウザ用のコンテンツである。

それらはいずれも、＜Canon iR4570/iR3570/iR2870/iR2270 シリーズ＞の HDD にインストールされる。デジタル複合機上のコントローラーや HDD を含むハードウェア、および PC 側のハードウェア、OS、Web ブラウザ、プリンタドライバ、ファクスドライバ、イメージプレビュー用プラグインは TOE 構成に含まれない。

デジタル複合機上で実行される TOE は単一の実行モジュールと言語ファイルによって構成される。また、TOE 上では MEAP に対応するアプリケーションを実行することができる。標準で＜MEAP 認証アプリケーション＞がインストールされるが、これは TOE の範囲外となる。本 TOE においては、他の MEAP アプリケーションを追加することはできない。デジタル複合機上の TOE の物理的範囲は以下の Figure 2-2 のとおりとなる。



※網掛け部分が TOE を表す。

Figure 2-2 デジタル複合機上の TOE と TOE 外のハードウェア／ソフトウェア

2.4.2.TOE の論理的範囲

本 TOE は、デジタル複合機を制御するソフトウェア全体を置き換えるため、論理的範囲は、2.2 章で示したデジタル複合機の機能全体であり、それに以下にあげるセキュリティ機能を追加したものとなる。

MEAP 認証アプリケーションが持つ、デジタル複合機の一般利用者の個人認証やディレクトリサービスとの連携機能は、本 TOE の論理的範囲に含まない。

- **HDD データ暗号化機能**

  すべてのイメージデータを暗号化して HDD に保存する機能である。

- **HDD データ完全消去機能**

  HDD 上のすべてのイメージデータを消去する際に、無意味なデータを上書きして完全消去をする機能である。

- **ボックス利用者識別認証機能**

  ボックスの文書を操作して該当のボックスに保存されたイメージデータを読み出す前に、暗証番号によって、正規のボックス利用者かどうかを識別認証する機能である。

- **ボックス管理機能**

  ボックス暗証番号の設定を行う機能である。

- **システム管理者識別認証機能**

  システム管理モードに移行する際に、システム管理部門 ID とシステム管理暗証番号によって、正規のシステム管理者かどうかを識別認証する機能である。

- **システム管理者管理機能**

  システム管理部門 ID およびシステム管理暗証番号の設定を行う機能である。

2.5. TOE の利用者

ここでは TOE の利用者について記述する。

- 一般利用者

  デジタル複合機を使用する利用者

- システム管理者

  デジタル複合機の設定・管理を行う利用者であり、ボックス利用者が暗証番号を忘れた場合などに、暗証番号を設定しなおす権限を持つ。

- ボックス利用者

  該当のボックスを使用する一般利用者。そのボックスに暗証番号を設定することにより、他の一般利用者のそのボックスへのアクセスを制限することができる。

2.6. 資産

本 ST における TOE の保護資産とそれ以外の一般データは以下の通りである。

本 ST における保護資産は、TOE が HDD に保存した文書のうち、管理情報を除く、イメージデータ部分である。

- テンポラリイメージデータ

  コピー、プリントなどを実行したときに生成される一時的なイメージデータであり、暴露から保護する必要がある。

- ボックスに保存されたイメージデータ

  読み込み、ファクス受信などによって、ボックスに保存されたイメージデータであり、暴露から保護する必要がある。ボックス暗証番号が設定されていないボックスに保存されたイメージデータは保護対象外である。

本 ST において文書やイメージデータに関連するが、保護資産として扱わない一般データには以下のものがある。

- 文書の管理情報（文書名や作成者、作成日時など、イメージデータ以外の情報）
- ネットワークや電話回線上の送信中および受信中のイメージデータ
- 暗証番号が設定されていないボックスに保存されたイメージデータ
- フォーム画像（イメージ合成のために登録されたイメージデータ）

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

本 ST における前提条件を以下に記述する。

3.1.1. 意図する使用法

A.OUT_OF_TOE: TOE 外のイメージデータ

TOE の利用者は、TOE 外に送信されたイメージデータおよび TOE が受信前のイメージデータは TOE の範囲外であり保護資産外であることに留意するものとする。

3.1.2. 人的前提条件

A.ADMIN: 信頼できる管理者

システム管理者は、信頼でき、不正な行為は行わないものと想定する。

A.PWD_MANAGE: 暗証番号の管理

ボックス暗証番号およびシステム管理暗証番号は、他人に知られず、他人から容易に推測されないものと想定する。

A.PWD_SET: 暗証番号の設定

保護する必要のあるイメージデータが保存されているボックスには、ボックス暗証番号が設定されているものと想定する。

システム管理部門 ID およびシステム管理暗証番号は、設定されていると想定する。

3.1.3. 接続性の前提条件

A.NETWORK: デジタル複合機の接続

TOE が動作するデジタル複合機をネットワークに接続する場合、インターネットなどの外部ネットワークから直接アクセスされない内部ネットワークに接続されるものと想定する。

また、リモート UI 機能を使用する場合には、その内部ネットワークは、送信先以外に不要なデータを送信しないネットワーク機器や、暗号化などの通信方法が使用されるとともに、内部ネットワークの管理者によって不正な機器が接続されないように管理され、ネットワークの盗聴が防止されているものと想定する。

3.2. 脅威

本 ST で想定する脅威を以下に記述する。

T.HDD_ACCESS: HDD データの直接アクセス

悪意のある者が、デジタル複合機の HDD を取り外し、ディスクエディタなどを利用して HDD に直接アクセスすることにより、デジタル複合機の HDD に保存されている、テンポラリイメージデータやボックスに保存されたイメージデータを暴露するかもしれない。

T.UNAUTH: 許可されない利用者の操作

該当のボックス利用者以外の者（システム管理者を除く）がデジタル複合機の操作パネルまたはリモート UI を操作することによって、該当のボックスに保存されたイメージデータを暴露するかもしれない。

3.3. 組織のセキュリティ方針

本 ST で取り上げられる組織のセキュリティ方針はない。

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、環境セキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

O.CRYPTO:　イメージデータの暗号化

TOE は、ボックスに保存されたイメージデータおよびテンポラリイメージデータを暗号化して、HDD に保存する。

O.RESIDUAL:　イメージデータの残存情報保護

TOE は、ボックスに保存されたイメージデータおよびテンポラリイメージデータの消去時に、残存情報が残らないようにする。

O. AUTH:　識別認証

TOE は、正規のボックス利用者およびシステム管理者だけが、ボックスに保存されたイメージデータの読み出しを行えるように、利用者が該当ボックスの操作を行って、ボックスに保存されたイメージデータを読み出す前に、正規のボックス利用者もしくはシステム管理者であることを識別認証する。

4.2. 環境のセキュリティ対策方針

OE.OUT_OF_TOE:　TOE 外のイメージデータ

TOE の利用者は、TOE 外に送信されたイメージデータおよび TOE が受信前のイメージデータは TOE の範囲外であり保護資産外であることに留意する。

OE.ADMIN:　信頼できる管理者

デジタル複合機を利用する組織の責任者は信頼できる者をシステム管理者に任命する。

OE.PWD_MANAGE:　暗証番号の管理

各ボックス利用者およびシステム管理者は、暗証番号が他人に知られないように管理し、他人から容易に推測されないものを設定し、適時変更するようにする。

OE.PWD_SET:　暗証番号の設定

該当ボックスの利用者は、該当ボックスに保護する必要のあるイメージデータを保存するときには、使用開始時に該当ボックスに暗証番号を設定し、ボックス暗証番号が必ず設定されている状態で TOE を使用する。また、ボックスの利用をやめるときには（ボックス暗証番号を消去するときには）保護する必要のあるイメージデータが、該当ボックス内にないことを確認する。

システム管理者は、TOE のインストール直後にシステム管理部門 ID とシステム管理暗証番号を設定し、システム管理部門 ID とシステム管理暗証番号が必ず設定された状態で TOE を使用する。

OE.NETWORK: デジタル複合機の接続

TOE が動作するデジタル複合機をネットワークに接続する際には、ファイアウォール等によって外部ネットワークからは直接アクセスできない内部ネットワークに接続しなければならない。

またリモート UI 機能を使用する場合、内部ネットワークの管理者は盗聴防止を実現するために、その内部ネットワークを送信先以外に不要なデータを送信しないネットワーク機器や、暗号化などの通信方法を使用して構築するとともに、不正な機器が接続されないように管理しなければならない。

5. セキュリティ要件

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

5.1. TOE セキュリティ要件

本章では、TOE が満たすべき TOE セキュリティ要件について記述する。

5.1.1.TOE セキュリティ機能要件

本章では、TOE が提供するセキュリティ機能要件を記述する。機能コンポーネントは、CC パート 2 で規定されているものを引用して、下記の記述規則で、操作を実施した。

選択、割付を行った場合は下線にて、また、詳細化を行った場合には、()とイタリック体にて操作を示す。また、繰返しを行ったコンポーネントの場合はコンポーネント名の後ろに小文字のローマ字を付与して、操作を示す。

5.1.1.1. 暗号サポート

FCS_CKM.1　暗号鍵生成

下位階層: なし

FCS_CKM.1.1 TSFは、以下の[割付：標準なし]に合致する、指定された暗号鍵生成アルゴリズム[割付：キヤノンiR暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付:168bit]に従って、暗号鍵を生成しなければならない。

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
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4　暗号鍵破棄

下位階層: なし

FCS_CKM.4.1 TSFは、以下の[割付 :標準なし]に合致する、指定された暗号鍵破棄方法[割付：キヤノンiR暗号鍵破棄アルゴリズム]に従って、暗号鍵を破棄しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート
または
FCS_CKM.1 暗号鍵生成]
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付 : FIPS PUB 46-3]に合致する、特定された暗号アルゴリズム[割付 : Triple DES]と暗号鍵長[割付 :168bit]に従って、[割付 : ボックスに保存されるイメージデータおよびテンポラリイメージデータの暗号化及び復号]を実行しなければならない。

依存性: [FDP_ITC.1 セキュリティ属性なし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

FMT_MSA.2 セキュアなセキュリティ属性

5.1.1.2. 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 : 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 :ボックスに保存されたイメージデータおよびテンポラリイメージデータ]

依存性: なし

5.1.1.3. 識別と認証

FIA_AFL.1a 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1a TSFは、[割付 : ボックス利用者の認証]に関して、[割付:1]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。

FIA_AFL.1.2a 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 : 再度ボックス利用者の認証試行を可能とするまでに1秒間間隔をあけること]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1b 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1b TSFは、[割付 :システム管理者の認証]に関して、[割付:1]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。

FIA_AFL.1.2b 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：再度システム管理者の認証試行を可能とするまでに1秒間間隔をあけること]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_SOS.1a 秘密の検証

下位階層: なし

FIA_SOS.1.1a TSFは、秘密 *(ボックス暗証番号)*が[割付：7桁の数字]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。

依存性: なし

FIA_SOS.1b 秘密の検証

下位階層: なし

FIA_SOS.1.1b TSFは、秘密 *(システム管理暗証番号)*が[割付：7桁の数字]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。

依存性: なし

FIA_UAU.1 認証のタイミング

下位階層: なし

FIA_UAU.1.1 TSFは、利用者（*ボックス利用者*）が認証される前に利用者を代行して行われる[割付：ボックス一覧の表示]を許可しなければならない。

FIA_UAU.1.2 TSFは、その利用者（*ボックス利用者*）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。

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

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

依存性: FIA_UID.1 識別のタイミング

FIA_UID.1 識別のタイミング

下位階層: なし

FIA_UID.1.1 TSFは、利用者（*ボックス利用者*）が識別される前に利用者を代行して実行される[割付：ボックス一覧の表示]を許可しなければならない。

FIA_UID.1.2 TSFは、その利用者(*ボックス利用者*)を代行する他のTSF調停アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

依存性: なし

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

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

依存性: なし

5.1.1.4. セキュリティ管理

FMT_MTD.1a TSF データの管理

下位階層: なし

FMT_MTD.1.1a TSFは、[割付：該当ボックス暗証番号]を[選択：改変、消去]する能力を[割付：該当ボックス利用者およびシステム管理者]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MTD.1b TSF データの管理

下位階層: なし

FMT_MTD.1.1b TSFは、[割付：システム管理部門IDおよびシステム管理暗証番号]を[選択：改変]する能力を[割付：システム管理者]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付: 下記のTable5-1の「管理対象とすべきアクション」の項目において、下線を引いた管理用セキュリティ機能]

依存性: なし

Table 5-1 機能要件から参照された管理用セキュリティ機能

機能要件	管理対象とすべきアクション	実現する機能要件
FCS_CKM.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) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし
FCS_CKM.4	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) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	なし
FCS_COP.1	これらのコンポーネントについて予見される管理アクティビティはない。	なし
FDP_RIP.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) 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。	なし
FIA_AFL.1a	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) 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	なし
FIA_AFL.1b	以下のアクションは FMT における管理機能と考えられる: c) 不成功の認証試行に対する閾値の管理 d) 認証失敗の事象においてとられるアクションの管理	なし
FIA_SOS.1a	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) 秘密の検証に使用される尺度の管理。	なし
FIA_SOS.1b	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) 秘密の検証に使用される尺度の管理。	なし
FIA_UAU.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: 管理者による認証データの管理; 関係する利用者による認証データの管理; 利用者が認証される前にとられるアクションのリストを管理すること。	FMT_MTD.1a
FIA_UAU.2	以下のアクションは FMT における管理機能と考えられる。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	FMT_MTD.1b
FIA_UID.1	以下のアクションは FMT における管理機能と考えられる: a) 利用者識別情報の管理;	なし

機能要件	管理対象とすべきアクション	実現する機能要件
	b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	
FIA_UID.2	以下のアクションは FMT における管理機能と考えられる: a) 利用者識別情報の管理。	FMT_MTD.1b
FMT_MTD.1a	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) 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。	なし
FMT_MTD.1b	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) 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。	なし
FMT_SMF.1	このコンポーネントに関して予見される管理アクティビティはない。	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
FPT_RVM.1	予見される管理アクティビティはない。	なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSFは、役割[割付:ボックス利用者およびシステム管理者]を維持しなければならない。

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

5.1.1.5. 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

5.1.2.最小機能強度レベル

本 TOE の最小機能強度レベルは、SOF-基本 である。

5.1.3.TOE セキュリティ保証要件

本章では、TOE のセキュリティ保証要件を記述する。
この TOE の保証要件は、EAL2 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 EAL2 のコンポーネントをそのまま使用する。

なお、ASE クラスは、表中に記載されていないが、TOE 評価において必須となる保証要件である。

Table 5-2 EAL2 の保証要件

保証要件クラス	保証要件コンポーネント
ACM	ACM_CAP.2
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.1, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ATE	ATE_COV.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_SOF.1, AVA_VLA.1

5.2. IT 環境のセキュリティ要件

本章では、IT 環境が満たすべきセキュリティ要件について記述する。

5.2.1. IT 環境のセキュリティ機能要件

本 TOE では、IT 環境のセキュリティ機能要件を必要としない。

6. TOE 要約仕様

この章では、TOE の要約仕様を記述する。

6.1. TOE セキュリティ機能

ここでは、TOE セキュリティ機能について記述する。

6.1.1.TOE セキュリティ機能の記述

SF.BOX_AUTH、SF.BOX_MANAGE および、SF.ADM_AUTH、SF.ADM_MANAGE における暗証番号メカニズムが本 ST における確率的、順列的メカニズムであり、その機能強度レベルは、SOF-基本である。

Table 6-1 セキュリティ機能と対応するコンポーネント

セキュリティ機能	機能要件コンポーネント
SF.CRYPTO	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
SF.COMP_ERASE	FDP_RIP.1
SF.BOX_AUTH	FIA_UAU.1, FIA_UID.1, FIA_AFL.1a, FMT_SMR.1, FPT_RVM.1
SF.BOX_MANAGE	FIA_SOS.1a, FMT_MTD.1a, FMT_SMF.1, FPT_RVM.1
SF.ADM_AUTH	FIA_UAU.2, FIA_UID.2, FIA_AFL.1b, FMT_SMR.1, FPT_RVM.1
SF.ADM_MANAGE	FIA_SOS.1b, FMT_MTD.1b, FMT_SMF.1, FPT_RVM.1

SF.CRYPTO: HDD データ暗号化機能
TOE はキヤノン iR 暗号鍵生成アルゴリズムを用いて、Triple DES 用の 168bit 暗号鍵を生成する。

TOE はすべてのイメージデータの HDD へのデータ書き込み時に、FIPS PUB 46-3 に準拠する暗号鍵長 168bit の Triple DES アルゴリズムを使用して、イメージデータを暗号化する。
TOE はすべてのイメージデータの HDD からのデータ読み込み時に、FIPS PUB 46-3 に準拠する暗号鍵長 168bit の Triple DES アルゴリズムを使用して、イメージデータを復号する。

TOE はキヤノン iR 暗号鍵破棄アルゴリズムに基づき、暗号鍵を破棄する。

SF.COMP_ERASE: HDD データ完全消去機能
TOE は、ボックスの文書消去時に、ボックスに保存されたイメージデータを HDD から削除する。また、TOE は、コピーやプリント、ファクス受信、送信（Universal Send）操作において、操作完了後に、生成されたテンポラリイメージデータを HDD から削除する。

TOE は、すべてのイメージデータを HDD から削除する際に、そのハードディスク領域を、無意味なデータで、上書きすることによりデータの完全消去を実施する。

また TOE は、TOE の起動時（デジタル複合機の起動時）に、テンポラリイメージデータに対して削除を実施する。その際には、無意味なデータで、そのハードディスク領域を上書きすることによりデータの完全消去を実施する。

SF.BOX_AUTH: ボックス利用者識別認証機能

TOE は、利用者がボックスにアクセスする前に（ボックスへのイメージデータの追加を除く）、既にボックス暗証番号が設定されているボックスであれば、ボックス暗証番号の入力を要求する。ボックスに暗証番号が設定されていない場合には、暗証番号の入力は要求しない。

入力したボックスの暗証番号が、選択しているボックスに登録された暗証番号と一致した場合にのみ、操作している利用者を、該当ボックス利用者として識別認証し、該当ボックスの操作画面を表示する。
TOE は、該当ボックス利用者として識別認証された利用者を、操作パネルでの操作においては該当ボックスへの操作画面を終了してボックス一覧表示画面に戻るまで該当ボックス利用者として維持し、リモート UI での操作においては、他のボックスに対する操作を実施する、または Web ブラウザを終了するまでの間、該当ボックス利用者として維持する。

入力されたボックス暗証番号が一致しない場合は、TOE は次の入力画面を出すまでに、1 秒間の間隔をあける。

SF.BOX_MANAGE: ボックス管理機能

TOE は、正規のボックス利用者およびシステム管理者に対してのみ、そのボックスの暗証番号を変更、消去する（ボックス暗証番号を付加しない）権限を与える。

TOE は、システム管理者に、操作パネルを操作することによってボックスの暗証番号を変更、消去する機能を提供する。TOE は、該当ボックス利用者に、操作パネルまたはリモート UI の操作によって、そのボックスの暗証番号を変更、消去する機能を提供する。

TOE は、ボックス暗証番号を 7 桁の数字に制限する。 暗証番号が付加されなかった場合には、そのボックス暗証番号を消去する。

SF.ADM_AUTH: システム管理者識別認証機能

TOE は、システム管理者として TOE を使用する利用者を、システム管理者として識別認証するため、システム管理者のシステム管理部門 ID とシステム管理暗証番号の入力を要求する。

システム管理者識別認証機能は、部門別 ID 管理を行っている場合には、操作パネルやリモート UI においてデジタル複合機を操作する前に実施され、部門別 ID 管理を行っていない場合には、操作パネルやリモート UI においてシステム管理設定画面を表示する際に実行される。
入力したシステム管理部門 ID とシステム管理暗証番号が、登録してあるものと一致した場合にのみ、操作している利用者をシステム管理者として識別認証する。

入力されたシステム管理部門 ID またはシステム管理暗証番号が一致しない場合は、TOE は次の入力画面を出すまでに、1 秒間の間隔をあける。

TOE は、操作パネルを操作して、システム管理者として識別認証された利用者については、システム管理モードを終了するまでシステム管理者として維持し、システム管理設定および、すべてのボックスに対する操作やボックス管理機能の実施を可能とする。システム管理モードは、操作パネルの ID キーの押下によって終了する。

TOE は、リモート UI を操作してシステム管理者として識別認証された利用者について、システム管理設定の実施を可能とする。リモート UI を実行している Web ブラウザを終了するまで、利用者はシステム管理者として維持される。

SF.ADM_MANAGE:システム管理者管理機能

TOE は、正規のシステム管理者に対してのみ、そのシステム管理部門 ID およびシステム管理暗証番号を変更し、システム管理部門 ID を削除する(システム管理部門 ID を設定しない)権限を与える。

TOE はシステム管理暗証番号を 7 桁の数字に制限する。

6.2. 保証手段

この章では、TOE のセキュリティ保証手段を記述する。以下のセキュリティ保証手段は、5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

なお ASE クラスに対する保証手段は、本 ST である。

Table 6-2 保証手段と対応するコンポーネント

保証要件コンポーネント	保証手段
ACM_CAP.2	iR セキュリティキット・B2 構成管理計画 iR セキュリティキット・B2 構成リスト
ADO_DEL.1	iR セキュリティキット・B2 配付手順
ADO_IGS.1	iR セキュリティキット・B2 設置手順書(日本国内) iR Security Kit-B2 Installation Procedure(海外)
ADV_FSP.1	iR セキュリティキット・B2 機能仕様書
ADV_HLD.1	iR セキュリティキット・B2 上位レベル設計書
ADV_RCR.1	iR セキュリティキット・B2 表現対応分析書
AGD_ADM.1	iR セキュリティキット・B2 ユーザーズガイド(日本国内) iR Security Kit-B2 Reference Guide(海外)
AGD_USR.1	iR セキュリティキット B2 ユーザーズガイド(日本国内) iR Security Kit-B2 Reference Guide(海外)
ATE_COV.1	iR セキュリティキット・B2 テスト仕様書
ATE_FUN.1	iR セキュリティキット・B2 テスト仕様書 iR セキュリティキット・B2 テスト結果
ATE_IND.2	TOE
AVA_SOF.1	iR セキュリティキット・B2 機能強度分析書
AVA_VLA.1	iR セキュリティキット・B2 脆弱性分析書

7. PP 主張

この章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修正

修正した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

本節では、セキュリティ対策方針が、TOE セキュリティ環境で規定した脅威、前提条件に対抗していることを示す。

Table 8-1 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針および前提条件の対応表

	A.OUT_OF_TOE	A.ADMIN	A.PWD_MANAGE	A.PWD_SET	A.NETWORK	T.HDD_ACCESS	T.UNAUTH
O.CRYPTO						×	
O.RESIDUAL						×	
O.AUTH							×
OE.OUT_OF_TOE	×						
OE.ADMIN		×					
OE.PWD_MANAGE			×				
OE.PWD_SET				×			
OE.NETWORK					×		

8.1.1. 組織のセキュリティ方針に関する根拠

本 ST で取り上げられる組織のセキュリティ方針はない。

8.1.2. 脅威に関する根拠

T.HDD_ACCESS: O.CRYPTO にて、ボックスに保存されるイメージデータおよびテンポラリイメージデータは暗号化して保存される。それにより、保護資産が HDD 内に保存されている時点での T.HDD_ACCESS の脅威は軽減する。

さらに、テンポラリイメージデータおよびボックスに保存されるイメージデータの消去時には、O.RESIDUAL により、保護資産が消去された後の残存情報は保護されることになる。それにより、保護資産が HDD から消去された時点では、T.HDD_ACCESS の脅威は除去される。

これらの対策方針両方によって、HDD に直接アクセスされることによって保護資産が暴露される脅威は大きく減少する。

T.UNAUTH: TOE は、O. AUTH により該当のボックスに対して、正規のボックス利用者以外の者（システム管理者を除く）がアクセスできないように、正規のボックス利用者およびシステム管理者を識別認証する。そのため、正規の利用者でないものが、操作パネルまたはリモート UI を使用して、ボックスに対する操作を行うことにより、ボックスに保存されたイメージデータが暴露される脅威は軽減される。

8.1.3. 前提条件に関する根拠

A.OUT_OF_TOE: OE.OUT_OF_TOE によって、TOE の利用者は、TOE から送信されたイメージデータおよび TOE が受信する前のイメージデータは TOE の範囲外であり、保護対象資産外であることに留意する。そのため、A.OUT_OF_TOE は満たされる。

A.ADMIN: OE.ADMIN によって、デジタル複合機を利用する組織の責任者により信頼できる者がシステム管理者に任命される。そのため、A.ADMIN は満たされる。

A.PWD_MANAGE: OE.PWD_MANAGE により各ボックス利用者およびシステム管理者は、暗証番号が他人に知られないように管理し、他人から容易に推測されないものを設定し、適時変更する。そのため、A.PWD_MANAGE は満たされる。

A.PWD_SET: OE.PWD_SET により各ボックス利用者は、該当ボックスに保護する必要のあるイメージデータを保存するときには、ボックス暗証番号を必ず設定する。そして、ボックスの利用をやめるときには（暗証番号を消去するときには）保護する必要があるイメージデータが該当ボックス内にないことを確認する。また、システム管理部門 ID およびシステム管理暗証番号も必ず設定される。そのため、A.PWD_SET は満たされる。

A.NETWORK: OE.NETWORK により TOE が動作するデジタル複合機は外部ネットワークから直接アクセスできない内部ネットワークに接続される。また、リモート UI 機能を使用する場合には、内部ネットワークはその管理者によって、送信先以外に不要なデータを送信しないネットワーク機器や暗号化などの通信方法を使用して構築されるとともに、不正な機器が接続されず、盗聴が防止されていることが保証される。したがって、A.NETWORK は満たされる。

8.2. セキュリティ要件根拠

8.2.1. TOE セキュリティ機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を Table 8-2 に示す。

Table 8-2 TOE セキュリティ要件と TOE セキュリティ対策方針の対応表

	O.CRYPTO	O.RESIDUAL	O. AUTH
FCS_CKM.1	×		
FCS_CKM.4	×		
FCS_COP.1	×		
FDP_RIP.1		×	
FIA_AFL.1a			×
FIA_AFL.1b			×
FIA_SOS.1a			×
FIA_SOS.1b			×
FIA_UAU.1			×
FIA_UAU.2			×
FIA_UID.1			×
FIA_UID.2			×
FMT_MTD.1a			×
FMT_MTD.1b			×
FMT_SMF.1			×
FMT_SMR.1			×
FPT_RVM.1			×

O.CRYPTO: FCS_CKM.1 で鍵を生成し、その鍵を用いて、FCS_COP.1 において、HDD に保存されるボックスに保存されたイメージデータおよび、テンポラリイメージデータの暗号化が実施される。FCS_CKM.4 において作成した鍵の破棄が可能となっている。したがって、O.CRYPTO は実現される。

O.RESIDUAL: FDP_RIP.1 において、ボックスに保存されたイメージデータおよびテンポラリイメージデータからハードディスク領域から割り当て解除される際に、残存情報を保護している。したがって O.RESIDUAL は満たされる。

O.AUTH: FIA_UID.1 および FIA_UAU.1 によってボックスを操作してボックスに保存されたイメージデータを読み出す前には、必ずボックス利用者の識別認証機能が動作する。また、FIA_UID.2 および FIA_UAU.2 によってシステム管理者としてボックス操作する前

には、必ずシステム管理者の識別認証機能が動作する。識別認証に成功した場合には、FMT_SMR.1 によって、ボックス利用者またはシステム管理者として維持される。識別認証に失敗した場合には、FIA_AFL.1a、FIA_AFL.1b により、次の認証試行まで 1 秒間の間隔が置かれ、一定期間内に実施される認証試行の回数を確実に制限することによって、それらの識別認証機能に対する攻撃に成功する確率は低減し、それらの識別認証機能は効果的に機能する。

以上の機能要件により、正規のボックス利用者およびシステム管理者だけがボックスを操作して、ボックスに保存されたイメージデータを読み出すことが可能となる。

FMT_MTD.1a、FMT_SMF.1 によって、ボックス暗証番号の変更が該当ボックス利用者とシステム管理者に制限され、FIA_SOS.1a によって、ボックス暗証番号の桁数制限が実現される。

FMT_MTD.1b 、FMT_SMF.1 によって、システム管理部門 ID、システム管理暗証番号の変更はシステム管理者に制限され、FIA_SOS.1b によって、システム管理暗証番号の桁数制限が実現される。

以上の機能要件により、正規のボックス利用者やシステム管理者になりすますことを防止する。

また、FPT_RVM.1 によって、ボックスに保存されたイメージデータを読み出す前に、必ずボックス利用者の識別認証、システム管理者の識別認証が実施され、ボックス利用者の識別認証機能、システム管理者の識別認証機能がバイパスされないことが保証される。

したがって、O.AUTH は実現されている。

8.2.2. セキュリティ保証要件根拠

セキュリティ保証要件として EAL2 の保証要件パッケージを選択している。

TOE は、一般の商用製品であるデジタル複合機全体を制御するためのソフトウェアであり、TOE が動作する環境であるデジタル複合機は、一般のオフィスなどにおいて使用される。 そのため、低レベルの攻撃者に対するセキュリティの保証が必要となる。

また、A.NETWORK により、TOE はインターネットなどの外部ネットワークから直接攻撃を受けることはないため、評価期間や評価コストを考慮すると、EAL2 の選択は妥当なものである。

8.2.3. セキュリティ要件依存性

セキュリティ要件のコンポーネントの依存性を、Table 8-3 に示す。表の左側が選択されたコンポーネント、右側が依存するコンポーネントである。除去されたコンポーネントは( )で示す。

Table 8-3 セキュリティ機能要件依存性の対応表

機能要件	依存性
FCS_CKM.1	(FCS_CKM.2)または FCS_COP.1, FCS_CKM.4, (FMT_MSA.2)

FCS_CKM.4	(FDP_ITC.1)または FCS_CKM.1, (FMT_MSA.2)
FCS_COP.1	(FDP_ITC.1)または FCS_CKM.1, FCS_CKM.4, (FMT_MSA.2)
FDP_RIP.1	なし
FIA_AFL.1a	FIA_UAU.1
FIA_AFL.1b	FIA_UAU.1:FIA_UAU.2 によって満たされている。
FIA_SOS.1a	なし
FIA_SOS.1b	なし
FIA_UAU.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1:FIA_UID.2 よって満たされている。
FIA_UID.1	なし
FIA_UID.2	なし
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	なし
FMT_SMR.1	FIA_UID.1
FPT_RVM.1	なし

セキュリティ保証要件に関しては、EAL2 のパッケージに適合しているため、依存性はすべて満たされている。

依存性除去の理由:

FCS_CKM.1 に対する FCS_CKM.2 の除去理由:

FCS_COP.1 が使用されているので、不要である。

FCS_CKM.4 および FCS_COP.1 に対する FDP_ITC.1 の除去理由:

FCS_CKM.1 が使用されているので、不要である。

FCS_CKM.1 に対する FMT_MSA.2 の除去理由:

本 TOE では、HDD データの暗号化に対して、暗号鍵は共通鍵を1つのみ使用しており、鍵タイプや有効期限など、鍵生成時の属性はない。したがって、セキュリティ属性の管理の機能要件は不要である。

FCS_CKM.4 に対する FMT_MSA.2 の除去理由:

本 TOE では、HDD データの暗号化に対して、暗号鍵は共通鍵を1つのみ使用しており、鍵タイプや有効期限など、鍵破棄時の属性はない。したがって、セキュリティ属性の管理の機能要件は不要である。

FCS_COP.1 に対する FMT_MSA.2 の除去理由:

本 TOE では、HDD データの暗号化に対して、暗号鍵は共通鍵を1つのみ使用しており、鍵タイプや有効期限など、暗号操作時の属性はない。したがって、セキュリティ属性の管理の機能要件は不要である。

8.2.4. セキュリティ機能要件の相互サポート

以下の様に、本 ST で選択した機能要件は、相互サポートを行っている。

本 TOE では、ボックスへの不正なアクセスを防ぐため、識別認証機能（FIA）を持つ。識別認証データは改変および消去が可能となるように、セキュリティ管理（FMT）にて管理している。セキュリティ管理（FMT）の機能要件によって、正規の利用者に成りすますことを防ぐことにより、相互サポートの構造をとっている。

また、TOE を介さずに直接 HDD を読み込むことによる、ボックスに保存されたイメージデータおよびテンポラリイメージデータに対する不正アクセスに対しては、FDP_RIP.1 による残存情報保護と FCS_COP.1 による暗号化とを組み合わせることによって保護している。

バイパス防止に関しては、FIA_UID.1、FIA_UID.2、FIA_UAU.1、FIA_UAU.2 による識別認証に成功しない限り、該当ボックス利用者およびシステム管理者が、ボックスの操作によるイメージデータの読み出しを行うことができないようにするため、FPT_RVM.1 によって、ボックス利用者の識別認証機能、およびシステム管理者の識別認証機能に対するバイパス防止を実施している。

また、FMT_MTD.1a、FMT_MTD.1b において、識別認証データを改変または消去できる利用者を限定している。この際にも、FPT_RVM.1 は、FIA_UID.1、FIA_UID.2、FIA_UAU.1、FIA_UAU.2 のボックス利用者の識別認証機能、およびシステム管理者の識別認証機能がバイパスされるのを防止している。

このように FPT_RVM.1 は、正規のボックス利用者およびシステム管理者だけがボックスに保存されたイメージデータを読み出せることを実現するのをサポートする。

8.2.5. 最小機能強度レベル根拠

最小機能強度レベルは、SOF-基本である。

TOE は、商用製品であるデジタル複合機全体を制御するためのソフトウェアであり、TOE が動作する環境であるデジタル複合機は、一般のオフィスなどにおいて使用される。 そのため、低レベルの攻撃者に対する機能強度レベルが必要となる。したがって、最小機能強度レベルは SOF-基本である。

8.3. TOE 要約仕様根拠

8.3.1. セキュリティ機能根拠

TOE のセキュリティ機能と、TOE の機能要件コンポーネントの対応を Table 8-4 に示す。

Table 8-4　TOE のセキュリティ機能と TOE の機能要件コンポーネントの対応表

	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_RIP.1	FIA_AFL.1a	FIA_AFL.1b	FIA_SOS.1a	FIA_SOS.1b	FIA_UAU.1	FIA_UAU.2	FIA_UID.1	FIA_UID.2	FMT_MTD.1a	FMT_MTD.1b	FMT_SMF.1	FMT_SMR..1	FPT_RVM.1
SF.CRYPTO	×	×	×														
SF.COMP_ERASE				×													
SF.BOX_AUTH					×				×		×					×	×
SF.BOX_MANAGE							×						×		×		×
SF.ADM_AUTH						×				×		×				×	×
SF.ADM_MANAGE								×						×	×		×

FCS_CKM.1:

SF.CRYPTO において暗号鍵が生成されることにより実現される。

FCS_CKM.4:

SF.CRYPTO において暗号鍵が破棄されることにより実現される。

FCS_COP.1:

SF.CRYPTO においてすべてのイメージデータの暗号化／復号処理が実施されることにより実現される。

FDP_RIP.1:

SF.COMP_ERASE において、すべてのイメージデータの完全消去が実施されることにより実現される。

FIA_AFL.1a:

SF.BOX_AUTH において、ボックス暗証番号が一致しない場合に、入力画面の再表示までに 1 秒間の間隔があくことにより実現される。

FIA_AFL.1b:

SF.ADM_AUTH において、システム管理暗証番号が一致しない場合に、入力画面の再表示までに 1 秒間の間隔があくことにより実現される。

FIA_SOS.1a:

SF.BOX_MANAGE にて、ボックス暗証番号が 7 桁の数字に制限されていることによって実現される。

FIA_SOS.1b:

SF.ADM_MANAGE にて、システム管理暗証番号が 7 桁の数字に制限されていることによって実現される。

FIA_UAU.1:

SF.BOX_AUTH によって、ボックスに保存されたイメージデータを読み出す前に、ボックス暗証番号によってボックス利用者が認証されることによって実現される。

FIA_UAU.2:

SF.ADM_AUTH によって、部門別 ID 管理実施時のデジタル複合機の初期画面において、および部門別 ID 管理非実施時のシステム管理設定画面表示時において、システム管理暗証番号によってシステム管理者が認証されることによって実現される。

FIA_UID.1:

SF.BOX_AUTH により、ボックス利用者の識別認証において、ボックス暗証番号入力時に自動的に利用者がボックス利用者かどうか識別されることによって実現される。

FIA_UID.2:

SF.ADM_AUTH により、部門別 ID 管理実施時のデジタル複合機の初期画面において、および部門別 ID 管理非実施時のシステム管理設定画面表示時において、システム管理部門 ID によってシステム管理者が識別されることによって実現される。

FMT_MTD.1a:

SF.BOX_MANAGE によって、ボックス暗証番号の変更／消去前に、ボックス利用者の識別認証もしくは操作パネルによるシステム管理者の識別認証が実施されることにより、該当ボックス利用者およびシステム管理者だけが該当ボックス暗証番号の変更／消去できることが実現される。

FMT_MTD.1b:

SF.ADM_MANAGE によって、システム管理部門 ID およびシステム管理暗証番号の変更前にシステム管理者の識別認証が実施されることにより実現される。

FMT_SMF.1:

SF.BOX_MANAGE によって、ボックス利用者だけが、自分が利用するボックスのボックス暗証番号を管理できるため、FIA_UAU.1 の管理項目である、関係する利用者による認証データの管理が実現される。また、SF.ADM_MANAGE によって、システム管理者だけが、自身のシステム管理部門 ID とシステム管理暗証番号を管理できるため、FIA_UAU.2 の管理項目である、管理者による認証データの管理が実現され、FIA_UID.2 の管理項目である、利用者識別情報の管理は実現される。また、以下に管理対象とすべきアクションはあるが、TOE が管理機能を持たない機能要件について、その根拠を示す。

FCS_CKM.1	:a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。 ただ1つの共通鍵を使用するため、暗号鍵に属性は持っていない。
FCS_CKM.4	:a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。 ただ1つの共通鍵を使用するため、暗号鍵に属性は持っていない。
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。

完全消去は資源の割り当て解除後、速やかに実施する必要があるため、設定値は存在しない。

FIA_AFL.1a :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

閾値は固定であり、また、アクションは 1 つしかないため、管理項目はない。

FIA_AFL.1b :a) 不成功の認証試行に対する閾値の管理

c) 認証失敗の事象においてとられるアクションの管理

閾値は固定であり、また、アクションは 1 つしかないため、管理項目はない。

FIA_SOS.1a :a) 秘密の検証に使用される尺度の管理。

秘密の検証尺度は、固定であり管理する必要はない。

FIA_SOS.1b :a) 秘密の検証に使用される尺度の管理。

秘密の検証尺度は、固定であり管理する必要はない。

FIA_UID.1 :a) 利用者識別情報の管理

;b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。

識別は認証とともに行われるため、識別情報の管理の必要はない。また識別前のアクションは固定であり、管理不要である。

FMT_MTD.1a :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。
役割は認証終了時に自動的に維持されるため、管理する項目はない。

FMT_MTD.1b :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。
役割は認証終了時に自動的に維持されるため、管理する項目はない。

FMT_SMR.1 a) 役割の一部をなす利用者のグループの管理

役割は、認証終了時に自動的に維持されるため、管理する項目はない。

FMT_SMR.1:

SF.BOX_AUTH によって、操作パネルでの操作においてはボックスに対する識別認証が成功した利用者がそのボックスに対する操作画面を開いている間、ボックス利用者として維持され、リモート UI での操作においては、他のボックスに対する操作を実施するまで、または Web ブラウザを終了するまでの間、ボックス利用者として維持される。また SF.ADM_AUTH により、システム管理者として識別認証された後、操作パネルでの操作においてはシステム管理モードを終了するまでの間、リモート UI での操作においては Web ブラウザを終了するまでの間、システム管理者として維持されることで実現される。

FPT_RVM.1:

SF.BOX_AUTH と SF.ADM_AUTH、および SF.BOX_MANAGE と SF.ADM_MANAGE によって実現される。詳細は、8.3.3 章を参照。

8.3.2. 機能強度根拠

本 ST における確率的・順列的メカニズムである、SF.BOX_AUTH、SF.BOX_MANAGE および SF.ADM_AUTH、SF.ADM_MANAGE における機能強度レベルは、いずれも SOF-基本である。また本 ST における最小機能強度レベルは、SOF-基本であり、これらは一貫している。したがって、SF.BOX_AUTH、SF.BOX_MANAGE および SF.ADM_AUTH、SF.ADM_MANAGE における機能強度レベル、SOF-基本は適切である。

8.3.3. セキュリティ機能のコンビネーション

直接 HDD に対するアクセスから保護資産を守るため SF.CRYPTO によってボックスに保存されたイメージデータおよびテンポラリイメージデータは暗号化され、また、SF.COMP_ERASE によって、ボックスに保存されたイメージデータおよび、テンポラリイメージの消去時に完全消去が実施される。

ボックスに保存されたイメージデータの保護のため、ボックスに保存されたイメージデータの読み出し前には SF.BOX_AUTH と SF.ADM_AUTH のどちらかが必ず実施されて、正規のボックス利用者とシステム管理者を識別認証することによって、ボックスに保存されたイメージデータに対する不正な読み出しが防止されている。

また SF.BOX_MANAGE によって、該当ボックス暗証番号の管理がなされる。また同様に、SF.ADM_MANAGE によってシステム管理者のシステム管理部門 ID、システム管理暗証番号の管理がなされる。これらの SF.BOX_MANAGE および SF.ADM_MANAGE によるボックス暗証番号の管理および、システム管理部門 ID、システム管理暗証番号の管理は利用者を該当ボックス利用者およびシステム管理者に制限しているため、SF.BOX_AUTH または SF.ADM_AUTH は必ず実施される。これにより、SF.BOX_AUTH または SF.ADM_AUTH が迂回されずに動作することを実現している。

8.3.4. 保証手段の根拠

各保証手段と、EAL2 の保証要件コンポーネントの対応関係を Table 8-5 に示す。

Table 8-5 保証手段と TOE の保証要件コンポーネントの対応表

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.1	AVA_SOF.1	AVA_VLA.1
iR セキュリティキット・B2 構成管理計画	×												
iR セキュリティキット・B2 構成リスト	×												
iR セキュリティキット・B2 配付手順		×											
iR セキュリティキット B2 設置手順書（日本国内） iR Security Kit-B2 Installation Procedure（海外）			×										
iR セキュリティキット・B2 機能仕様書				×									
iR セキュリティキット・B2 上位レベル設計書					×								
iR セキュリティキット・B2 表現対応分析書						×							
iR セキュリティキット B2 ユーザーズガイド（日本国内） iR Secuirty Kit-B2 Reference Guide（海外）							×	×					
iR セキュリティキット・B2 テスト仕様書									×	×			
iR セキュリティキット・B2 テスト結果										×			
TOE											×		
iR セキュリティキット・B2 機能強度分析書												×	
iR セキュリティキット・B2 脆弱性分析書													×

ACM_CAP.2:

iR セキュリティキット・B2 構成管理計画および iR セキュリティキット・B2 構成リストによって、TOE の構成が管理される。

ADO_DEL.1:

iR セキュリティキット・B2 配付手順によって、TOE の配付途中の改ざんなどが行われないことが保証される。

ADO_IGS.1:

iR セキュリティキット B2 設置手順書（日本国内）、iR Security Kit-B2 Installation Procedure（海外）によって、正確にインストールが実施される。

ADV_FSP.1：

iR セキュリティキット・B2 機能仕様書により TOE の機能仕様が提供される。

ADV_HLD.1：

iR セキュリティキット・B2 上位レベル設計書により TOE の上位レベル設計が提供される。

ADV_RCR.1：

iR セキュリティキット・B2 表現対応分析書によって、本 ST の TOE 要約仕様と、機能仕様間、および機能仕様と、上レベル設計間の対応が説明される。

AGD_ADM.1：

iR セキュリティキット・B2 ユーザーズガイド（日本国内）および、iR Security Kit-B2 Reference Guide（海外）によって、管理者および一般利用者に対するガイダンスが提供される。

AGD_USR.1：

iR セキュリティキット・B2 ユーザーズガイド（日本国内）および、iR Security Kit-B2 Reference Guide（海外）によって、管理者および一般利用者に対するガイダンスが提供される。

ATE_COV.1：

iR セキュリティキット・B2 テスト仕様書によって、カバレージの分析が提供される。

ATE_FUN.1：

iR セキュリティキット・B2 テスト仕様書、iR セキュリティキット・B2 テスト結果によって、開発者のテスト計画、テスト結果が提供される。

ATE_IND.2：

TOE が提供される。

AVA_SOF.1：

iR セキュリティキット・B2 機能強度分析書によって、確率的・順列的メカニズムに対する機能強度主張の根拠が示される。

AVA_VLA.1：

iR セキュリティキット・B2 脆弱性分析書によって、開発時点における TOE の脆弱性が分析される。