Canon iR3225/iR3230/iR3235/iR3245 Series
HDD Data Erase Kit-B2
セキュリティターゲット

Version 1.01
2008/08/08

キヤノン株式会社

更新履歴

Ver. 1.00	2008/05/13	初版
Ver. 1.01	2008/08/08	TOE セキュリティ機能の記述変更

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 iR3225/iR3230/iR3235/iR3245 Series
HDD Data Erase Kit-B2 セキュリティターゲット

日付: 2008/08/08

バージョン: Version 1.01

作成者: キヤノン株式会社

TOE:
Canon iR3225/iR3230/iR3235/iR3245 Series
HDD Data Erase Kit-B2 Version 1.00

キーワード: Canon、キヤノン、imageRUNNER、iR、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、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 2.3
Interpretations-0512
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。
Common Criteria for Information Technology Security Evaluation に係る情報処理推進機構(IPA)翻訳文書 (IPA 翻訳文書)
- 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

評価保証レベル: EAL3

1.2. ST 概要

本ドキュメントは、デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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<HDD Data Erase Kit-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<HDD Data Erase Kit-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、デジタル複合機のシステム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の残存情報を再利用されることから保護するために、以下の機能を提供する。

- HDD データ完全消去機能
- システム管理者識別認証機能
- システム管理機能

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－EAL3 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） Java 言語を使用して開発された専用のアプリケーション『MEAP アプリケーション』を稼動させることができる。
MEAP アプリケーション	デジタル複合機上で動作する Java 言語を使用して開発された専用のアプリケーションであり、プリント、コピー、ファクス、スキャン等、デジタル複合機の機能と組み合わせることにより、ユーザインターフェースのカスタマイズ、ドキュメントフローの簡略化、定型業務の自動化を実現することができる。

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 Active Directory との連携を行う MEAP アプリケーション。
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	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。
操作パネル	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。これらの機能を使用するため、大容量の HDD を持ち、TOE は複合機上で動作する。
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。
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ースである。

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 iR3225/iR3230/iR3235/iR3245 Series>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システムソフトウェアは TOE で置き換えられる。

2.2. TOE 概要

TOE は、デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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<HDD Data Erase Kit-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、デジタル複合機のシステム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。

デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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。一般的なデジタル複合機では、このような一時保存されたイメージデータであるテンポラリイメージデータを、コピーやプリント等の終了時に論理的に削除するだけで、その残存情報を削除しておらず、そのため、残存情報が不正に再利用される可能性が存在していた。

TOE は、テンポラリイメージデータの残存情報を再利用されることから保護する目的で使用される。

デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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。Figure 2-1 に想定する設置使用環境を示す。なお、Figure 2-1 は、デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>のオプションを含む機能を使用する場合の想定設置環境であり、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。

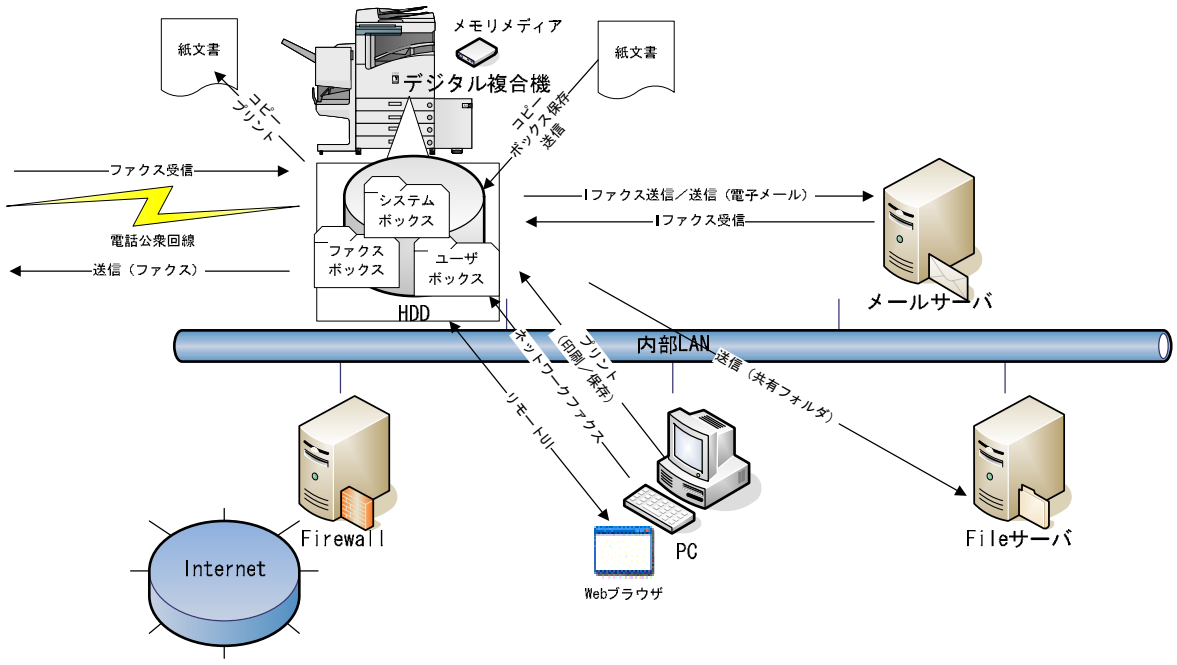

Figure 2-1 デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>の想定設置使用環境

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

  紙文書をスキャナで読み込み、プリントすることにより、紙文書を複写する機能である。紙文書のスキャン時に HDD 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または転送する機能である。ファクスの受信時に HDD にテンポラリイメージデータを生成する。

- 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は、文書結合やフォーム画像のイメージ合成などの編集操作を施した後に出力することが可能である。

- プリンタ機能

  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 ファイル形式で電子メールアドレスや PC の共有フォルダなど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。

  文書の送信時には HDD にテンポラリイメージデータを生成する。

- メモリメディア連携機能

  ユーザによって挿入されたメモリメディアに、スキャナで読み取った原稿画像(ScanToMemory)やBOX 内の文書(BoxToMemory)を PDF 等に変換し、保存する機能である。また、メモリメディア内に保存された文書を印刷(MemoryToPrint)する機能である。

  スキャン時および印刷時に HDD 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以外に、リモート UI を使用して、デジタル複合機の機能を使用することができる。リモート UI は利用者の PC 上の 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。

- MEAP 機能

  利用者は、デジタル複合機にオプションソフトウェアである MEAP アプリケーションをインストールして、デジタル複合機に新たな機能を追加することができる。

TOE をデジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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の消去時に、論理的な削除を実行するだけでなく、削除したテンポラリイメージデータの残存情報を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<Canon iR3225/iR3230/iR3235/iR3245 Series>の HDD 上にあるテンポラリイメージデータの残存情報を、不正な再利用から保護することが可能となる。

2.3. TOE の動作環境

TOE は、デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series> にインストールすることにより動作する。

また、下記のような機能を利用するためには、他のサーバやソフトウェアを必要とする。

リモート UI を使用してデジタル複合機を操作する場合は、Web ブラウザを PC 上にインストールして使用する必要がある。

PC からプリントやファクス送信を行う場合は、適切なプリンタドライバまたは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。

I ファクスや送信（Universal Send）を行う場合は、適切なメールサーバ、FTP サーバ、ファイルサーバが必要となる。

なお、TOE をテストする際に利用した PC の環境は下記である。

OS:	Microsoft Windows XP Professional SP2
Web ブラウザ:	Microsoft Internet Explorer Version 6.0 SP2

2.4. TOE の範囲

TOE の物理的範囲と論理的範囲は以下の通りである。

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の機能を制御するソフトウェア全体、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、および標準装備される MEAP 認証アプリケーションである。

これらはいずれも、デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>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や HDD を含むハードウェア、およびユーザ 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。

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。標準装備される MEAP 認証アプリケーションは TOE の範囲内となるが、オプションでインストールされる MEAP アプリケーションは TOE の範囲外である。デジタル複合機<Canon iR3225/iR3230/iR3235/iR3245 Series>上の TOE の物理的範囲は以下の Figure 2-2 の通りとなる。

<table>
<tr><td rowspan="2">制御ソフトウェア
（TOE:ソフトウェア）</td><td>リモート UI
コンテンツ
（TOE:
ソフトウェア）</td><td>標準装備
MEAP
アプリケーション
（TOE:
ソフトウェア）</td><td>オプション
MEAP
アプリケーション
（TOE 外:
ソフトウェア）</td></tr>
<tr><td colspan="3">コントローラ（TOE 外:ハードウェア）</td></tr>
<tr><td>スキャンエンジン・ADF
（TOE 外:
ハードウェア）</td><td>プリンタエンジン
（TOE 外:
ハードウェア）</td><td colspan="2">操作パネル
（TOE 外:
ハードウェア）</td></tr>
</table>

※網掛け部分が TOE を表す。

Figure 2-2 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<Canon iR3225/iR3230/iR3235/iR3245 Series>を制御するソフトウェア全体を置き換えるため、その論理的範囲は、2.2 章で示したデジタル複合機の機能全体である。TOE が提供するセキュリティ機能は以下のものである。

- HDD データ完全消去機能

  HDD 上のテンポラリ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残存情報を完全消去する機能である。

- 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機能、および「HDD データ完全消去機能」の各種設定機能である。

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であり、システム管理機能を使うことができる。

2.6. 資産

本 ST における TOE の保護資産は以下の通りである。

- テンポラリイメージデータの残存情報

  テンポラリイメージデータとは、コピー、プリント、ファクス受信、送信（Universal Send）などを実行した際に生成される一時的なイメージデータである。また、プリントのために、PC から受信した印刷データ（スプールデータ）もテンポラリイメージデータとして扱われる。

  一般的なデジタル複合機では、このような一時保存されたイメージデータであるテンポラリイメージデータを、コピーやプリント等の終了時に論理的に削除するだけで、その残存情報を削除しておらず、そのため、残存情報が不正に再利用される可能性が存在していた。

  TOE の保護資産は、一般的なデジタル複合機では削除していなかったテンポラリイメージデータの残存情報である。

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. 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.ADMIN_PWD:　　システム管理暗証番号

システム管理者は、システム管理暗証番号として、安易でない 7 桁の数字を設定するものと想定する。

3.1.2. 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。

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、デジタル複合機のテンポラリイメージデータの残存情報を再利用するかもしれない。

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 のセキュリティ対策方針、環境のセキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

O.RESIDUAL:　　イメージデータの残存情報保護

TOE は、テンポラリイメージデータの消去時に、残存情報を完全消去する。

O.ADMIN_AUTH:　　システム管理機能の識別認証

TOE は、システム管理者だけがシステム管理機能を使用できるように、正規の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.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.ADMIN_PWD:　　システム管理暗証番号

システム管理者は、システム管理暗証番号として、安易でない 7 桁の数字を設定するものと想定する。

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。

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。

セキュリティ機能要件はCCパート2で規定されている機能コンポーネント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、詳細化を行った場合には()とイタリック体にて、繰返しを行った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. 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。

5.1.1.1. 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:テンポラリイメージデータ]

依存性: なし

5.1.1.2. 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 TSFは、[割付:システム管理者の認証]に関して、 [選択: [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.1.2 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: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_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.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

5.1.1.3. セキュリティ管理

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1 TSF は、機能[割付: HDD データ完全消去機能][選択: 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: 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.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: システム管理部門 ID、システム管理暗証番号]を[選択: 改変, 削除]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
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	FMT_MOF.1

	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。	
FIA_AFL.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) 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_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.1
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.1
FMT_MOF.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) 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;	なし
FMT_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) 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	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)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: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

5.1.1.4. 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。

本 TOE における確率的、順列的メカニズムとして、システム管理者を識別・認証する必要があり、FIA_UAU.2、FIA_UID.2 の機能要件にて、低レベルの攻撃に対抗できる機能強度を要求している。

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、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そのまま使用する。

Table 5-2 EAL3 の保証要件

保証要件クラス	保証要件コンポーネント
ASE	ASE.1
ACM	ACM_CAP.3, ACM_SCP.1
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	ALC_DVS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_MSU.1, AVA_SOF.1, AVA_VLA.1

5.2. IT 環境に対するセキュリティ要件

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 環境に対するセキュリティ機能要件

IT 環境が満たすべきセキュリティ機能要件は存在しない。

6. TOE 要約仕様

本章では、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.ADM_AUTH における暗証番号（パスワード）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.COMP_ERASE	FDP_RIP.1
SF.ADM_AUTH	FIA_UAU.2, FIA_UID.2, FIA_AFL.1, FMT_SMR.1, FPT_RVM.1
SF.ADM_MANAGE	FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

SF.COMP_ERASE:　　HDD データ完全消去機能
TOE がテンポラリイメージデータを HDD から削除する際は、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テンポラリイメージデータの残存情報の完全消去を実施する。

SF.COMP_ERASE が動作するタイミングは下記である。

(1) コピー、プリント、ファクス受信、送信（Universal Send）操作時に生成されたテンポラリイメージデータの残存情報を、コピー等の処理後には HDD から完全消去する。

(2) テンポラリイメージデータの残存情報を、TOE の起動時に HDD から完全消去する。

(3) テンポラリイメージデータの残存情報を、システム管理者による『全データ/設定の初期化』の操作後の再起動時に HDD から完全消去する。

SF.ADM_AUTH:　　システム管理者識別認証機能
TOE は、「システム管理機能」の利用者をシステム管理者に限定するため、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。

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、システム管理者として識別認証せず、応答を 1 秒間遅延させる。

SF.ADM_MANAGE:　　システム管理機能
TOE は、正規のシステム管理者に対してのみ、下記の権限を与える。

(1) システム管理部門 ID、システム管理暗証番号を変更または削除することができる。

(2) 「HDD データ完全消去機能」に関して下記の各種設定ができる。

A) 「HDD データ完全消去機能」の起動・停止
B) 「HDD データ完全消去機能」の消去モードの変更
   ① 0 データ 1 回書き込み
   ② ランダムデータ 1 回書き込み
   ③ ランダムデータ 3 回書き込み

6.2. 保証手段

本章では、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。

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
ASE.1	本 ST
ACM_CAP.3	HDD Data Erase Kit-B2 構成管理計画書
ACM_SCP.1	HDD Data Erase Kit-B2 構成リスト
ADO_DEL.1	HDD Data Erase Kit-B2 配付手順書
ADO_IGS.1	HDD Data Erase Kit-B2 Installation Procedure
ADV_FSP.1	HDD Data Erase Kit-B2 機能仕様書
ADV_HLD.2	HDD Data Erase Kit-B2 上位レベル設計書
ADV_RCR.1	HDD Data Erase Kit-B2 表現対応分析書
AGD_ADM.1 AGD_USR.1	HDD Data Erase Kit-B2 Reference Guide iR Series User Documentation
ALC_DVS.1	HDD Data Erase Kit-B2 開発セキュリティ規程書
ATE_COV.2	HDD Data Erase Kit-B2 セキュリティテスト分析書
ATE_DPT.1	HDD Data Erase Kit-B2 セキュリティテスト分析書
ATE_FUN.1	HDD Data Erase Kit-B2 セキュリティテスト仕様書 HDD Data Erase Kit-B2 セキュリティテスト報告書
ATE_IND.2	TOE
AVA_MSU.1	HDD Data Erase Kit-B2 Reference Guide iR Series User Documentation HDD Data Erase Kit-B2 Installation Procedure
AVA_SOF.1	HDD Data Erase Kit-B2 機能強度分析書
AVA_VLA.1	HDD Data Erase Kit-B2 脆弱性分析書

iR Series User Documentation は、下記 Guide から構成されている。

- imageRUNNER 3225/3230/3235/3245 Reference Guide
- imageRUNNER 3225/3230/3235/3245 Copying and Mail Box Guide
- imageRUNNER 3225/3230/3235/3245 Sending and Facsimile Guide
- imageRUNNER 3225/3230/3235/3245 Remote UI Guide
- imageRUNNER 3225/3230/3235/3245 Network Guide
- MEAP SMS Administrator Guide

7. PP 主張

本章では、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

	T.HDD_ACCESS	A.ADMIN	A.ADMIN_PWD	A.NETWORK
O.RESIDUAL	X			
O.ADMIN_AUTH	X			
OE.ADMIN		X		
OE.ADMIN_PWD			X	
OE.NETWORK				X

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:

TOE は、O.RESIDUAL により、保護資産であるテンポラリイメージデータの残存情報を再利用することができないように完全消去している。そのため、保護資産が HDD から完全消去されて、T.HDD_ACCESS の脅威を除去している。

また、システム管理機能の不正操作により、テンポラリイメージデータの残存情報保護機能を停止されないようにする必要がある。また、システム管理者が理由があってテンポラリイメージデータの残存情報保護機能を停止しているにも関わらず、意図せずテンポラリイメージデータの残存情報保護機能を動作されないようにする必要もある。そのために、O.ADMIN_AUTH により、テンポラリイメージデータの残存情報保護機能を有効化・無効化できる機能の存在するシステム管理機能の操作を正規のシステム管理者に制限している。

8.1.3. 前提条件に関する根拠

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。従って、A.ADMIN は満たされる。

A.ADMIN_PWD:

OE.ADMIN_PWD によって、システム管理者は、システム管理暗証番号として、安易でない 7 桁の数字を設定するものと想定する。従って、A.ADMIN_PWD は満たされる。

A.NETWORK:

OE.NETWORK によって、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。従って、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.RESIDUAL	O.ADMIN_AUTH
FDP_RIP.1	X	
FIA_AFL.1		X
FIA_UAU.2		X
FIA_UID.2		X
FMT_MOF.1		X
FMT_MTD.1		X
FMT_SMF.1		X
FMT_SMR.1		X
FPT_RVM.1		X

O.RESIDUAL:

FDP_RIP.1 において、テンポラリイメージデータの残存情報を再利用できないように、完全消去している。従って、O.RESIDUAL は満たされる。

O.ADMIN_AUTH:

FIA_UID.2 および FIA_UAU.2 によってシステム管理機能を操作する前には、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、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.1 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。また、FPT_RVM.1 によって、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。

以上の機能要件により、正規のシステム管理者だけがシステム管理機能を操作することが可能となる。

FMT_MTD.1、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または削除はシステム管理者に制限される。

さらに、FMT_MOF.1、FMT_SMF.1 によって、「HDD データ完全消去機能」の各種設定はシステム管理者に制限される。

以上の機能要件により、正規のシステム管理者になりすますことを防止する。

従って、O.ADMIN_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 EAL3 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 が動作するデジタル複合機は、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り、評価期間や評価コストを考慮すると EAL3 は妥当な選択である。

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

TOE /IT 環境	機能要件	CC にて要求している依存性	本 ST での依存性
TOE	FDP_RIP.1	なし	なし
	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
	FIA_UAU.2	FIA_UID.1	FIA_UID.2

	FIA_UID.2	なし	なし
	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
	FMT_MTD.1	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
	FPT_RVM.1	なし	なし
IT 環境	なし	N/A	N/A

Table 8-3 から「本 ST での依存性」の機能要件は、「CC にて要求している依存性」の機能要件をすべて満たしている。

セキュリティ保証要件に関しては、EAL3 のパッケージに適合しているため、依存性はすべて満たしている。

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、テンポラリイメージデータの残存情報の再利用の脅威に対しては、FDP_RIP.1 による「HDD データ完全消去機能」によって保護している。

バイパス防止に関しては、攻撃者が、「システム管理機能」を不正操作しないように、FIA_UID.2、FIA_UAU.2 による「システム管理者識別認証機能」を有していて、FPT_RVM.1 によって、この「システム管理者識別認証機能」に対するバイパス防止を実施している。

また、FMT_MTD.1 において、システム管理部門 ID、識別認証データを変更または削除できる利用者を限定している。さらに、FMT_MOF.1 において、「HDD データ完全消去機能」の各種設定をシステム管理者に限定している。

以上のように、それぞれの機能要件は競合する機能要件や矛盾する機能要件を選択しておらず、相互サポートを行っている。

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、低レベルの攻撃者がシステム管理者になりすまし不正操作することに対処する対策方針 O.ADMIN_AUTH が必要となる。機能強度レベルとして、低レベルの攻撃を想定することは適切であるので、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

	FDP_RIP.1	FIA_AFL.1	FIA_UAU.2	FIA_UID.2	FMT_MOF.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
SF.COMP_ERASE	X								
SF.ADM_AUTH		X	X	X				X	X
SF.ADM_MANAGE					X	X	X		

FDP_RIP.1:

SF.COMP_ERASE において、すべてのテンポラリイメージデータの残存情報の完全消去が実施されることにより実現される。

FIA_AFL.1:

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_UAU.2:

SF.ADM_AUTH において、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.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_MOF.1:

SF.ADM_MANAGE により、システム管理者のみが「HDD データ完全消去機能」の起動・停止、消去モードの変更ができる。

FMT_MTD.1:

SF.ADM_MANAGE により、システム管理者のみが、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または削除を実施できる。

FMT_SMF.1:

SF.ADM_MANAGE により、システム管理者のみが、システム管理部門 ID および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。SF.ADM_MANAGE において、システム管理者のみが「HDD データ完全消去機能」を各種設定できる。

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。

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 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。
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; TSF の機能と相互に影響を及ぼし得る役割のグループは、存在しない。
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。 TSF の機能と相互に影響を及ぼし得る役割のグループは、存在しない。
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理 TSF の機能と相互に影響を及ぼし得る役割のグループは、存在しない。

FMT_SMR.1:

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.ADM_AUTH 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 TOE における確率的・順列的メカニズムである、SF.ADM_AUTH における機能強度レベルは、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。従って、SF.ADM_AUTH 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.COMP_ERASE によって、テンポラリイメージデータの消去時に残存情報の完全消去が実施される。

また、 SF.ADM_MANAGE によって「HDD データ完全消去機能」を各種設定できたり、システム管理者のシステム管理部門 ID およびシステム管理暗証番号の変更または削除ができたりするが、利用者をシステム管理者に制限する SF.ADM_AUTH は事前に必ず実施される。これにより、SF.ADM_MANAGE が動作するためには SF.ADM_AUTH は迂回できないことを示している。

8.3.4. 保証手段の根拠

各保証手段と、EAL3 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	ASE.1	ACM_CAP.3	ACM_SCP.1	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.2	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_DVS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_MSU.1	AVA_SOF.1	AVA_VLA.1
本 ST	X																	
HDD Data Erase Kit-B2 構成管理計画書		X																
HDD Data Erase Kit-B2 構成リスト			X															
HDD Data Erase Kit-B2 配付手順書				X														
HDD Data Erase Kit-B2 Installation Procedure					X											X		
HDD Data Erase Kit-B2 機能仕様書						X												
HDD Data Erase Kit-B2 上位レベル設計書							X											
HDD Data Erase Kit-B2 表現対応分析書								X										
HDD Data Erase Kit-B2 Reference Guide および、iR Series User Documentation									X	X						X		
HDD Data Erase Kit-B2 開発セキュリティ規程書											X							
HDD Data Erase Kit-B2 テスト仕様書														X				
HDD Data Erase Kit-B2 テスト分析書												X	X					
HDD Data Erase Kit-B2 テスト結果														X				
TOE															X			
HDD Data Erase Kit-B2 機能強度分析書																	X	
HDD Data Erase Kit-B2 脆弱性分析書																		X

ASE.1:

本 ST によって、ASE に必要な情報が提供される。

ACM_CAP.3:

HDD Data Erase Kit-B2 構成管理計画書によって、TOE の構成が管理される。

ACM_SCP.1:

HDD Data Erase Kit-B2 構成リストによって、TOE の構成が管理される。

ADO_DEL.1:

HDD Data Erase Kit-B2 配付手順書によって、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:

HDD Data Erase Kit-B2 Installation Procedure によって、正確にインストールが実施される。

ADV_FSP.1:

HDD Data Erase Kit-B2 機能仕様書により TOE の機能仕様が提供される。

ADV_HLD.2:

HDD Data Erase Kit-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:

HDD Data Erase Kit-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、上位レベル設計間の対応が説明される。

AGD_ADM.1:

HDD Data Erase Kit-B2 Reference Guide、iR Series User Documentation によって、管理者に対するガイダンスが提供される。

AGD_USR.1:

HDD Data Erase Kit-B2 Reference Guide、iR Series User Documentation によって、一般利用者に対するガイダンスが提供される。

ALC_DVS.1:

HDD Data Erase Kit-B2 開発セキュリティ規程書によって、TOE の開発中のセキュリティが維持される。

ATE_COV.2:

HDD Data Erase Kit-B2 テスト分析書によって、カバレージの分析が提供される。

ATE_DPT.1:

HDD Data Erase Kit-B2 テスト分析書によって、深さの分析が提供される。

ATE_FUN.1:

HDD Data Erase Kit-B2 テスト仕様書、HDD Data Erase Kit-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_MSU.1:

HDD Data Erase Kit-B2 Reference Guide、iR Series User Documentation、HDD Data Erase Kit-B2 Installation Procedure によって、TOE の誤使用を防止する。

AVA_SOF.1:

HDD Data Erase Kit-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:

HDD Data Erase Kit-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。

以上