RISO セキュリティパッケージ

セキュリティターゲット

Version 1.04

29 Jul.2013

理想科学工業株式会社

【 変更履歴 】

更新日	バージョン	変更内容	作成
2012/10/17	V1.00	新規作成	榎本
2013/01/11	V1.01	指摘事項修正	榎本
2013/03/21	V1.02	指摘事項修正	榎本
2013/06/07	V1.03	指摘事項修正	植木
2013/07/29	V1.04	指摘事項修正	植木

【 目次 】

【 用語定義 】

用語・略語	定義
MFP	Multi Function Printer デジタル複合機。プリント機能のほかに、コピー、スキャンなど複数の機能を 1 台に搭載した機器。
利用者	MFP を使う者。操作可能な機能のレベルにより、一般利用者、管理者に分類される。
一般利用者	MFP のプリント機能、コピー機能、スキャン機能などの基本機能を利用する者。
管理者	MFP と一般利用者の運用管理を行う者。
保守員	MFP の設置・保守を行う者。通常は、理想科学工業株式会社もしくは MFP の保守を委託されている企業の技術者。
ジョブ	MFP が実行する仕事（プリント、コピー、スキャン）の処理単位。仕事の開始から終了までの流れ。
ジョブデータ	ジョブの実行中に MFP 内で扱うデジタルデータ。 ジョブデータは、ジョブ情報と画像データで構成される。
ジョブ情報	ジョブの属性や処理方法を示すデータの総称。 例えば、ファイル名、プリント枚数、データ所有者等である。 ジョブ情報は、ジョブデータの一部である。
画像データ	二次元画像データ部分の総称。サムネイル画像や、ボックスに保存されたデータも含む。画像データは、ジョブデータの一部である。 なお、本文中ジョブ（プリント、コピー、スキャン）を特定せずに「画像データ」と記述してある場合は、プリントジョブとコピージョブの画像データを指す。
一時画像データ	コピージョブの実行中に MFP 内部で一時的に生成される二次元画像データ。コピージョブと関連を持つが、コピージョブの画像データの一部ではない。
プリント指示待ちジョブ	利用者が操作パネルでプリント開始を指示するまで、プリント処理を開始しないプリントジョブ
プリンタ出力用ファイル	理想科学工業社製 MFP でプリント可能なデータ形式のファイル。 例えば、プリントジョブデータ、コピージョブデータである。
スキャンファイル	スキャン機能で生成した、PDF・TIFF・JPEG のいずれかの形式のファイル。 スキャンファイルは、MFP で直接プリントしたり、ボックスに保存することは出来ない。
内部フォルダ	スキャンファイルを保管するために、MFP の不揮発性記憶装置に割り当てられた領域。 プリンタ出力用ファイルは保管できない。

用語・略語	定義
ボックス	利用者がプリンタ出力用ファイルをMFP内に保管する際、ファイルを整理・分類するために用いる、仮想的に区分けされた保存場所。 「ボックスに保存する」と、ファイルは、物理的には MFP の不揮発性記憶装置に保存される。
UI	User Interface ユーザインターフェース。
RAW ポート	プリンタドライバからMFPにデータを送信する通信ポートの1つ。プリンタドライバを標準設定でインストールした場合に選択されるポートである。

1. ST 概説(ST introduction)

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

1.1. ST 参照(ST reference)

本節では、ST の識別情報を記述する。

- タイトル　　：RISO セキュリティパッケージ　セキュリティターゲット
- バージョン　：1.04
- 作成者　　：理想科学工業株式会社
- 発行日　　：2013 年 7 月 29 日

1.2. TOE 参照(TOE reference)

本節では、TOE の識別情報を記述する。

- TOE 名　　：【日本】RISO セキュリティパッケージ
  【英語】RISO Security Package
- バージョン　：2.0
- 開発者名　　：理想科学工業株式会社

1.3. TOE 概要(TOE overview)

本節では、TOE の使用方法およびその主要なセキュリティ機能の特徴、TOE 利用環境、TOE の利用者役割、TOE に必要とされる TOE 以外のハードウェア/ソフトウェア/ファームウェアについて記述する。

1.3.1. TOE の使用方法及びその主要なセキュリティ機能の特徴

RISO セキュリティパッケージは、理想科学工業社製 MFP 用のデータ保護オプションソフトウェア製品である。標準ソフトウェアを搭載した MFP に TOE をインストールすると、下記のセキュリティ機能が追加される。これらのセキュリティ機能は、TOE インストール以前と同様の操作でプリント要求、コピー要求、ジョブの削除要求などを行なう事によって利用できる。

なお、TOE をインストールする MFP は、HDD 以外の不揮発性記憶装置に資産を保存しないため、これ以降、不揮発性記憶装置を HDD と表現する。

TOE が提供する、主なセキュリティ機能の概要を以下に示す。
なお、スキャン機能で生成したスキャンファイルは、MFP の製品仕様上、不特定利用者による取得を認めている。そのため、スキャン機能の利用およびスキャンファイル保護は、TOE セキュリティ機能の対象としない。

1) HDD 保存データ暗号化／復号機能

画像データ・一時画像データを、MFP に内蔵された HDD に暗号化して保存する機能。

2) **残存データ上書き消去機能**

ジョブ終了後に削除された画像データや一時画像データ、利用者操作により削除された画像データが保存された HDD の領域を上書きし、情報の再現を防止する機能。

3) **利用者データ一括上書き消去機能**

画像データを保存した HDD の領域を上書きし、情報の再現を防止する機能。

1.3.2. TOE 利用環境

TOE を搭載した MFP の利用環境を、図 1- 1 に示す。

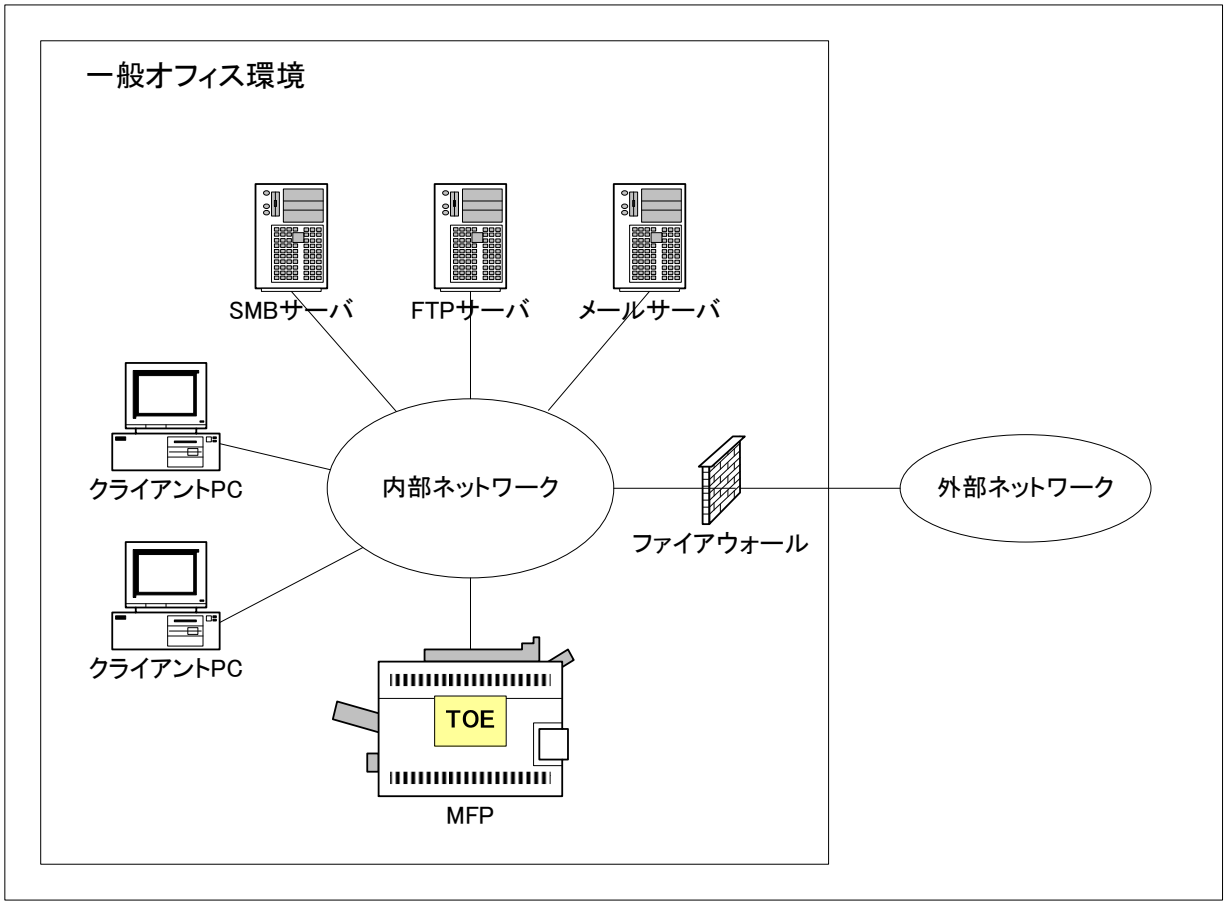

図 1- 1：MFP の利用環境

- TOE を搭載した MFP は、内部ネットワーク（LAN）に接続することで、以下のような機器とデータ通信が可能となる。
  - 利用者のクライアント PC：
    インストールしたプリンタドライバを用いて、MFP へデータのプリントを要求する。また、MFP からスキャンファイルを取得、MFP の稼働状況の確認、ジョブ操作、ボックス操作、MFP の設定を行う。
  - FTP サーバ：
    MFP が送信したスキャンファイルを保存する。
  - SMB サーバ：

MFP が送信したスキャンファイルを保存する。

- メールサーバ:
  MFP が送信したスキャンファイルを受信する。

1.3.3. TOE に必要とされる TOE 以外のハードウェア/ソフトウェア/ファームウェア

- 国内機: ORPHIS X7200/X7250/X7250A/X9050
  ORPHIS EX7200/EX 7250/EX 7250A/EX 9000/EX 9050/EX7200L
  海外機: ComColor 3010/3010R/7010/7010R/3050/3050R/7050/7050R/9050/9050R
  /3110/3110R/3150/3150R/7110/7110R/7150/7150R/9110/9110R/9150/9150R/2150

1.4. TOE 記述(TOE description)

本節では、TOE の物理的な範囲と境界、TOE の論理的な範囲と境界、TOE を構成するガイダンスについて記述する。

1.4.1. TOE の物理的な範囲と境界

MFP 内の各ユニットと TOE の物理的範囲を、図 1- 2 に示す。

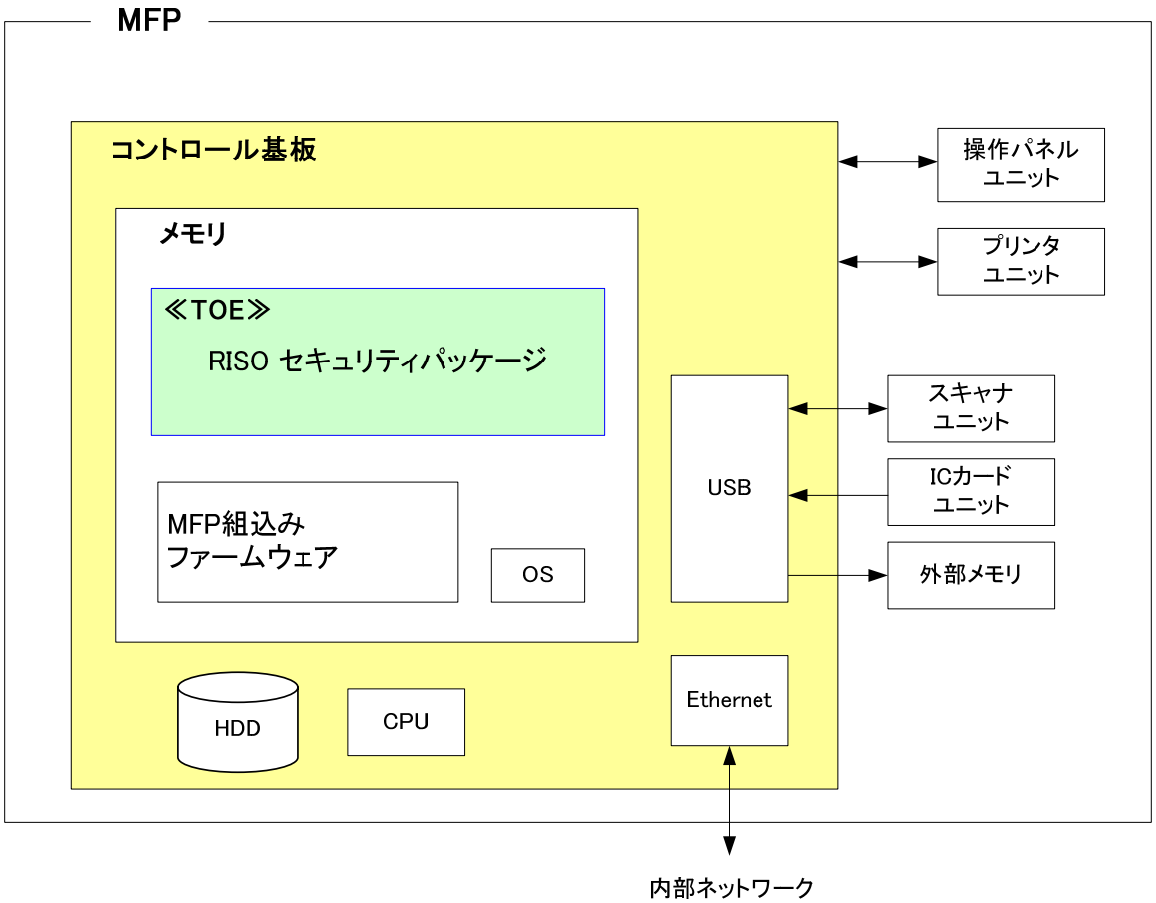

図 1- 2 : TOE の物理的範囲

TOE は、MFP 本体内のコントロール基板上に存在するソフトウェアである。

関連する各ユニットについて説明する。

- **コントロール基板**
  MFP の全体制御を行うための回路基板。
- **操作パネルユニット**
  MFP の操作および設定を行うための、液晶ディスプレイ、LED、テンキー、ボタンなどを備えた、入出力装置。
- **プリンタユニット**
  ジョブデータを紙媒体に印字する装置。
- **スキャナユニット**
  紙原稿を読み取り、デジタルデータに変換する装置。
- **IC カードユニット**
  利用者の識別に用いる IC カードの情報を読み取る装置。
- **外部メモリ**
  MFP に USB インターフェースで接続するメモリ。スキャン機能で生成したスキャンファイルの保存や、ファームウェアのダウンロードに使用する。なお、外部メモリ内のファイルを直接プリントすることや、MFP から外部メモリへプリンタ出力用ファイルを保存することは出来ない。
- HDD
  ハードディスクドライブ。ファームウェアおよび、ジョブデータ、利用者情報などを保存する。

TOE の物理的構成要素を。表 1-1 に示す。

表 1- 1：TOE の構成要素

名称		バージョン
【日本】RISO セキュリティパッケージ 【英語】RISO Security Package		2.0
	SNSO	1.0.4
	【日本】RISO セキュリティパッケージ取扱説明書 セキュリティガイド 【英語】RISO Security Package Security Guide	050-36055-300 050-36056-306

SNSO は、MFP 本体内のコントロール基板上に存在するソフトウェアである。

1.4.2. TOE の論理的な範囲と境界

TOE の論理的な範囲と境界を、図 1- 3 に示す。

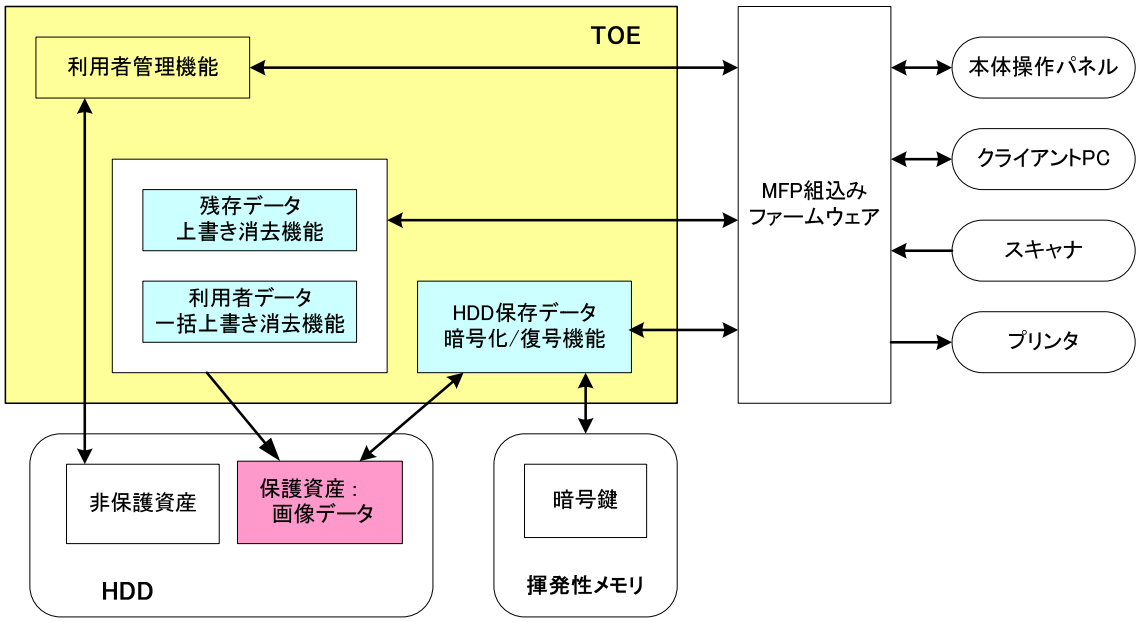

図 1- 3：TOE の論理的範囲

1.4.2.1. MFP の基本機能

MFP の基本機能として、プリント機能、コピー機能、スキャン機能、ボックス保存機能、ログイン機能、ログアウト機能が提供される。

このうちログイン機能・ログアウト機能の一部（図 1- 3 の利用者管理機能）が TOE に含まれるが、評価対象のセキュリティ機能ではない。

1) **プリント機能**

クライアント PC から受信したデータや、ボックスから読み出したデータを、紙媒体にプリントする機能。

2) **コピー機能**

操作パネルからの指示により、紙原稿をスキャナユニットで読み取り、紙媒体にプリントする機能。

3) **スキャン機能**

操作パネルからの指示により、紙原稿をスキャナユニットで読み取り、スキャンファイルを生成する機能。スキャンファイルは、以下のいずれかの方法で、保存または送信する。

- MFP の内部フォルダに保存
- ファイルサーバ（FTP サーバ、SMB サーバ）に保存
- 外部メモリに保存
- メール送信

4) **ボックス保存機能**

クライアント PC から受信したデータ、またはコピー機能で読み取ったデータを、ボックスに保存する機能。

5) **ログイン機能**

ログインが必要と指定されたモードを利用する前に、操作者が MFP に登録された一般利用者であるか、識別認証する機能。識別認証に成功すると、操作者に対して MFP の機能の使用を許可する。

6) **ログアウト機能**

ログイン中の利用者に対する MFP の使用許可を終了する機能。

操作パネルからログインした場合は、操作パネル無操作状態が一定時間経過すると、自動的にログアウトする。

1.4.2.2. セキュリティ機能

TOE は、プリント機能、コピー機能に関する以下の機能を TOE セキュリティ機能として扱う。

なお、スキャン機能で生成したスキャンファイルは、MFP の製品仕様上、不特定利用者による取得を認めている。そのため、スキャン機能の利用およびスキャンファイル保護は、TOE セキュリティ機能の対象としない。

1) **HDD 保存データ暗号化／復号機能**

画像データ・一時画像データを、MFP に内蔵された HDD へ書き込む前に、暗号化を行う機能。また、HDD から読み出した暗号化データを復号する機能。

2) **残存データ上書き消去機能**

プリント機能、コピー機能で使用した画像データ・一時画像データをジョブ終了後に削除する時、あるいは利用者がボックスに保存されたジョブデータやプリント指示待ちジョブデータを削除した時に、画像データ・一時画像データが保存された HDD の領域を上書きし、情報の再現を防止する機能。

3) **利用者データ一括上書き消去機能**

TOE を搭載した MFP に内蔵された HDD から、画像データを一括消去する機能。画像データを保存した HDD の領域を上書きし、情報の再現を防止する。

2. 適合主張(conformance claim)

本章では、CC 適合主張、PP 主張、パッケージ主張、適合根拠について記述する。

2.1. CC 適合主張(CC Conformance claim)

- **ST が適合を主張する CC のバージョン**

  パート 1: 概説と一般モデル バージョン 3.1 改訂第 3 版[翻訳第 1.0 版]

  パート 2: セキュリティ機能コンポーネント バージョン 3.1 改訂第 3 版[翻訳第 1.0 版]

  パート 3: セキュリティ保証コンポーネント バージョン 3.1 改訂第 3 版[翻訳第 1.0 版]

- **CC パート 2(セキュリティ機能要件)への適合**

  CC パート 2 適合(CC Part 2 conformant)

- **CC パート 3(セキュリティ保証要件)への適合**

  CC パート 3 適合(CC Part 3 conformant)

2.2. PP 主張、パッケージ主張(PP claim, Package claim)

- **PP 主張**

  適合する PP はない。

- **パッケージ主張**

  EAL3 パッケージ適合(package-conformant)

2.3. 適合根拠(Conformance Rationale)

なし

3. セキュリティ課題定義(Security problem definition)

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威(Threats)

3.1.1. TOE 資産

本 TOE の資産は、TOE を搭載した MFP を使用することで MFP に内蔵された HDD に保存される、画像データである。

3.1.2. 脅威

TOE に対する脅威を表 3- 2 に示す。

表 3- 2：脅威

No.	脅威	内容
1	T.REMOVE	＜HDD の取り出し＞ 悪意を持つ者が、廃棄された MFP や、リース・レンタル契約終了により返却された MFP から HDD を取り出し、HDD に残る画像データを漏洩する。

3.2. 組織のセキュリティ方針(Organisational security policy)

組織のセキュリティ方針を表 3- 3 示す。

表 3- 3：組織のセキュリティ方針

No.	組織のセキュリティ方針	内容
1	OSP. CRYPTO	暗号化されていない画像データや一時画像データを、HDD に保存してはならない。

3.3. 前提条件(Assumptions)

TOE の利用にあたり必要な条件、運用において想定される前提条件を、表 3- 4 に示す。

表 3- 4：前提条件

No.	前提条件	内容
1	A.ADMIN	＜信頼できる管理者＞ 管理者は、課せられた役割を遂行するための作業において、悪意を持った行為を行わない。
2	A.PORT	＜プリンタのポート＞ プリンタの送信ポートは、RAW ポートが使用される。
3	A.ACCESS.MANAGED	＜設置場所＞ TOE を搭載した MFP は、悪意を持つ者による物理的なアクセスを制限できる、管理された環境に設置される。

4. セキュリティ対策方針(Security objectives)

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

4.1. TOE のセキュリティ対策方針(Security objectives for the TOE)

TOE のセキュリティ対策方針を表 4- 1 に示す。

表 4- 1：TOE のセキュリティ対策方針

No.	TOE の セキュリティ対策方針	内容
1	O.CRYPTO	＜暗号化＞ TOE は、画像データ・一時画像データを暗号化して HDD に書き込む。
2	O.DELETE	＜一括上書き消去＞ TOE は、画像データが残された HDD の領域を一括上書き消去し、再生を不可能にする機能を提供する。
3	O.RESIDUAL	＜残存データの上書き消去＞ TOE は、ジョブ終了後に削除した一時画像データや画像データが保存された HDD の領域を上書き消去し、再生を不可能にする。

4.2. 運用環境のセキュリティ対策方針(Security objectives for the operational environment)

運用環境のセキュリティ対策方針を表 4- 2 に示す。

表 4- 2：運用環境のセキュリティ対策方針

No.	運用環境の セキュリティ対策方針	内容
1	OE.ERASE	＜MFP の廃棄＞ MFP を廃棄または所有者を変更する際、管理者または管理者に依頼された保守員が、画像データを保存した HDD の領域に対して、一括上書き消去を実施する。
2	OE.ADMIN	＜管理者の保証＞ TOE を所有する組織の責任者は、信頼する人物を管理者に任命し、MFP の管理を実施させる。
3	OE.PORT	＜プリンタのポート＞ プリンタの送信ポートは、RAW ポートを使用する。
4	OE.PHYSICAL.MANAGED	＜設置場所＞ ガイダンスに従い、TOE を搭載した MFP を、悪意を持つ者による物理的なアクセスを制限できる、管理された環境に設置する。

4.3. セキュリティ対策方針根拠(Security objectives rationale)

セキュリティ対策方針と脅威および前提条件の対応関係を表 4- 3 に示す。

表 4- 3：セキュリティ対策方針と脅威および前提条件

脅威・前提条件・組織のセキュリティ方針 / セキュリティ対策方針	T.REMOVE	OSP.CRYPTO	A.ADMIN	A.PORT	A.ACCESS.MANAGED
O.CRYPTO		○			
O.DELETE	○				
O.RESIDUAL	○				
OE.ERASE	○				
OE.ADMIN			○		
OE.PORT				○	
OE.PHYSICAL.MANAGED					○

表 4- 3 により、各セキュリティ対策方針は 1 つ以上の脅威または前提条件に対応している。
次に、各脅威、各前提条件が、TOE のセキュリティ対策方針または運用環境のセキュリティ対策方針により満たされることを説明する。

4.3.1. 脅威に対する根拠

脅威に対する根拠を表 4- 4 に示す。

表 4- 4：脅威に対する根拠

No.	脅威	根拠
1	T.REMOVE	O.RESIDUAL により、TOE は、ジョブ終了後に削除した画像データ、一時画像データが保存された HDD の領域を上書き消去する機能を提供する。 また、O.DELETE により、TOE は、画像データが残された HDD の領域を一括上書き消去し再生を不可能にする機能を提供する。OE.ERASE に従い、管理者または保守員が確実に上書き消去を実施することで、これらのデータの漏洩を防ぐことが出来る。 よって、脅威 T. REMOVE は、これらの対策方針により対抗される。

4.3.2. 組織のセキュリティ方針に対する根拠

組織のセキュリティ方針に対する根拠を表 4- 5 に示す。

表 4- 5：組織のセキュリティ方針に対する根拠

No.	組織のセキュリティ方針	根拠
1	OSP.CRYPTO	O.CRYPTO により、TOE は画像データ、一時画像データを暗号化してから HDD に書き込む。 よって、OSP.CRYPTO は、この対策方針により実施される。

4.3.3. 前提条件に対する根拠

前提条件に対する根拠を表 4- 6 に示す。

表 4- 6：前提条件に対する根拠

No.	前提条件	根拠
1	A.ADMIN	OE.ADMIN において、組織の責任者が適切な人物を管理者に任命することを規定している。 よって、前提条件 A.ADMIN は、OE.ADMIN により充足される。
2	A.PORT	OE.PORT において、プリンタの送信ポートは、RAW ポートを使用する事を規定している。 よって、前提条件 A.PORT は、OE.PORT により充足される。
3	A.ACCESS.MANAGED	OE.PHYSICAL.MANAGED において、TOE を搭載した MFP を管理された環境に設置することを規定している。 よって、前提条件 A.ACCESS.MANAGED は、 OE.PHYSICAL.MANAGED により充足される。

5. 拡張コンポーネント定義(Extended components definition)

本 ST では拡張コンポーネントを選択していないため、本章は適用されない。

6. セキュリティ要件(Security requirement)

本章では、セキュリティ要件について記述する。

6.1. TOE セキュリティ機能要件(Security functional requirements for the TOE)

TOE が提供するセキュリティ機能要件を記述する。

■ 暗号サポート(FCS)

FCS_CKM.1　暗号鍵生成

下位階層:　なし

依存性:　[FCS_CKM.2 暗号鍵配付、または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1　TSF は、以下の[割付: 標準のリスト: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: RISO 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 128bit]に従って、暗号鍵を生成しなければならない。

FCS_COP.1　暗号操作

下位階層:　なし

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

FCS_COP.1.1　TSF は、[割付: FIPS PUB 197]に合致する、特定された暗号アルゴリズム[割付: AES]と暗号鍵長[割付: 128bit]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 暗号操作のリスト]

- 画像データ、一時画像データを暗号化して HDD に書き込む
- HDD から読み出した、画像データ、一時画像データを復号する

■ 利用者データ保護(FDP)

FDP_RIP.1　サブセット情報保護

下位階層:　なし

依存性:　なし

FDP_RIP.1.1　TSF は、[割付: オブジェクトのリスト]のオブジェクト[選択: 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]:

- 画像データを保存したファイル
- 一時画像データを保存したファイル

6.2. TOE セキュリティ保証要件(Security assurance requirements for the TOE)

TOE セキュリティ保証要件を表 6- 1 に示す。

本 TOE の評価保証レベルは、EAL3 である。全てのセキュリティ保証要件は CC パート 3 に規定されているセキュリティ保証コンポーネントを直接使用する。

表 6- 1：保証要件

保証クラス	*保証コンポーネント*	
開発	ADV_ARC.1	*セキュリティアーキテクチャ記述*
	ADV_FSP.3	*完全な要約を伴う機能仕様*
	ADV_TDS.2	*アーキテクチャ設計*
ガイダンス文書	AGD_OPE.1	*利用者操作ガイダンス*
	AGD_PRE.1	*準備手続き*
ライフサイクル サポート	ALC_CMC.3	*許可の管理*
	ALC_CMS.3	*実装表現の CM 範囲*
	ALC_DEL.1	*配付手続き*
	ALC_DVS.1	*セキュリティ手段の識別*
	ALC_LCD.1	*開発者によるライフサイクルモデルの定義*
セキュリティ ターゲット評価	ASE_CCL.1	*適合主張*
	ASE_ECD.1	*拡張コンポーネント定義*
	ASE_INT.1	*ST 概説*
	ASE_OBJ.2	*セキュリティ対策方針*
	ASE_REQ.2	*派生したセキュリティ要件*
	ASE_SPD.1	*セキュリティ課題定義*
	ASE_TSS.1	*TOE 要約仕様*
テスト	ATE_COV.2	*カバレージの分析*
	ATE_DPT.1	*テスト: 基本設計*
	ATE_FUN.1	*機能テスト*
	ATE_IND.2	*独立テスト – サンプル*
脆弱性評定	*AVA_VAN.2*	*脆弱性分析*

6.3. セキュリティ要件根拠(Security requirements rationale)

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件とTOEセキュリティ対策方針の対応関係を表6-2に示す。この表で示す通り、各セキュリティ機能要件が、少なくとも1つの TOE セキュリティ対策方針に対応している。

表 6-2：セキュリティ機能要件とセキュリティ対策方針の対応関係

セキュリティ機能要件 ＼ セキュリティ対策方針	O.CRYPTO	O.DELETE	O.RESIDUAL
FCS_CKM.1	○		
FCS_COP.1	○		
FDP_RIP.1		○	○

次に、各 TOE セキュリティ対策方針が、セキュリティ機能要件によって実現できることを説明する。

・ O.CRYPTO

FCS_CKM.1 により、AES 暗号アルゴリズムで規定された 128bit の暗号鍵を、RISO 暗号鍵生成アルゴリズムにより生成する。

FCS_COP.1 により、AES 暗号アルゴリズムと生成した 128bit の暗号鍵を用いて、画像データを暗号化して HDD に書き込む。HDD から読み出した暗号化されたデータは、同じ AES 暗号アルゴリズムと 128bit の暗号鍵を用いて復号する。

以上の機能要件が実装されれば、データは暗号化されてからHDDに書き込まれ、HDDから読み出した暗号化データは読み出し後に復号されるため、不正な装置やツールの接続によるデータの暴露から保護される。よって、O.CRYPTO は実現される。

・ O.DELETE

FDP_RIP.1 により、HDD に保存した画像データの資源開放後は、資源の以前のどの情報の内容も利用できなくする。

この機能要件が実装されれば、資源開放後にデータの再生を不可能にするという O.DELETE は実現される。

・ O.RESIDUAL

FDP_RIP.1 により、HDD に保存した画像データや一時画像データの資源開放後は、資源の以前のどの情報の内容も利用できなくする。

この機能要件が実装されれば、資源開放後にデータの再生を不可能にするという O.RESIDUAL は実現

される。

6.3.2. セキュリティ機能要件間の依存関係

セキュリティ要件のコンポーネントの依存性を、表 6- 3 に示す。

表 6- 3：セキュリティ機能要件間の依存性

機能要件	CC 規定の依存関係	本 ST での依存関係	依存性除去の理由
FCS_CKM.1	FCS_CKM.2 または FCS_COP.1, FCS_CKM.4	FCS_COP.1	暗号鍵は、揮発性メモリ内に保持するため、MFP の電源オフにより、揮発性メモリ内のデータは消失する。よって、暗号鍵の破棄を行う必要が無いため、FCS_CKM.4 は不要となる。
FCS_COP.1	FDP_ITC.1 または FDP_ITC.2 または FCS_CKM.1, FCS_CKM.4	FCS_CKM.1	暗号鍵は、揮発性メモリ内に保持するため、MFP の電源オフにより、揮発性メモリ内のデータは消失する。よって、暗号鍵の破棄を行う必要が無いため、FCS_CKM.4 は不要となる。
FDP_RIP.1	なし	なし	

6.3.3. セキュリティ保証要件根拠

本 TOE は、商用製品である MFP に対するファームウェア アップグレード キットである。商用製品に対する一般的な攻撃に対抗するためには、機能仕様および TOE 設計に基づくテストや脆弱性分析による保証が必要であり、また、開発環境管理、TOE 構成管理、セキュアな配布手続きの保証を提供することが望まれる。

従って、それらの保証レベルを満たす EAL3 を選択した。

7. TOE 要約仕様(TOE summary specification)

本章では、TOE が提供するセキュリティ機能の要約仕様について述べる。

7.1. TOE セキュリティ機能

以下では、各 TOE セキュリティ機能に関して、その概要および対応する SFR の具体的な実現方法について説明する。

7.1.1. HDD 保存データ暗号化／復号機能

画像データ・一時画像データを、MFP に内蔵された HDD へ書き込む前に、暗号化を行う機能。また、その HDD から読み出した暗号化データを復号する機能。対応する SFR の実現方法を以下に示す。

1) FCS_CKM.1（暗号鍵生成）

TOE は、暗号鍵の生成において、以下の機能を提供する。これらの機能の実装により、FCS_CKM.1 を実現する。

- 暗号鍵長は 128bit とする。
- 暗号鍵生成アルゴリズムは、RISO 暗号鍵生成アルゴリズムを使用する。
- 暗号鍵の生成には、TOE 内のシード情報を用いる。なお、シード情報を TOE 外から読み出すことは出来ない。
- MFP の電源投入後、任意のタイミングで暗号鍵を生成する。
- 生成した暗号鍵は、揮発性メモリに保存する。

2) FCS_COP.1（暗号操作）

TOE は、暗号操作において、以下の機能を提供する。これらの機能の実装により、FCS_COP.1 を実現する。

- 暗号化および復号には、生成した暗号鍵長 128bit の暗号鍵を使用する。
- 暗号アルゴリズムは、AES 暗号アルゴリズムを使用する。
- 画像データ、一時画像データを HDD へ書き込む前に、暗号操作を行う。
- HDD から画像データ、一時画像データを読み出すときに、復号操作を行う。
- 復号後のデータは、揮発性メモリに保存する。

7.1.2. 残存データ上書き消去機能

プリント機能、コピー機能で使用した画像データ、一時画像データをジョブ終了後に削除する時、あるいは利用者がボックスに保存されたジョブデータやプリント指示待ちジョブデータを削除した時に、画像データ・一時画像データが保存された HDD の領域を上書きし、情報の再現を防止する機能。対応する SFR の実現方法を以下に示す。

1) FDP_RIP.1（サブセット情報保護）

TOE は、残存データの上書き消去において、以下の機能を提供する。これらの機能の実装により、FDP_RIP.1 を実現する。

- HDD に保存した画像データ、一時画像データを用いる処理が終了または中止し、以降の処理に使用しないことが確定すると、その画像データ、一時画像データを保存したファイルに対して上書き消去を行う。
- HDD に保存した画像データに対して、利用者が削除指示を行った場合も、その画像データを保存したファイルに対して上書き消去を行う。
- 上書き消去方法は、対象ファイルの保存領域に、0x00、0xFF、ランダム値を順に上書きし、最後にベリファイを取った後、ファイルを削除して終了とする。
- 上書き消去中に MFP の電源が切れた場合は、次の電源投入時に自動的に上書き処理を再開する。

7.1.3. 利用者データ一括上書き消去機能

TOE を搭載した MFP に内蔵された HDD から、画像データを一括消去する機能。画像データを保存した HDD の領域を上書きし、情報の再現を防止する。対応する SFR の実現方法を以下に示す。

1) FDP_RIP.1（サブセット情報保護）

TOE は、利用者データの一括消去において、以下の機能を提供する。これらの機能の実装により、FDP_RIP.1 を実現する。

- 本機能を実行すると、利用者がボックスに保存したジョブデータやプリント指示待ちジョブデータの画像データを保存したファイルに対し、一括上書き消去を開始する。
- 上書き消去方法は、対象データの保存領域に、0x00、0xFF、ランダム値を順に上書きし、最後にベリファイを取った後、ファイルを削除して終了とする。
- 上書き消去開始後は、本機能の中断を受け付けない。
- 上書き消去中に MFP の電源が切れた場合は、次の電源投入時に自動的に上書き処理を再開する。