ORPHIS FT2430 / ComColor FT2430 with ORスキャナーHS7000 / Scanner HS7000 and RISOセキュリティパッケージ for FT / RISO Security Package F20

セキュリティターゲット

Version 2.0

2022/9/16

RISO KAGAKU CORPORATION

Revision history

Ver.	Date	Section	Description	Author
1.0	2022/1/28	−	新規作成	中台
1.1	2022/2/9	−	誤記修正	中台
1.2	2022/2/22	−	誤記修正	中台
1.3	2022/3/4	−	誤記修正	中台
1.4	2022/3/15	−	誤記修正	中台
1.5	2022/3/29	−	誤記修正	中台
1.6	2022/4/7	−	誤記修正	中台
1.7	2022/4/21	−	誤記修正	中台
1.8	2022/6/3	−	誤記修正	中台
1.9	2022/6/9	−	誤記修正	中台
2.0	2022/9/16	1.ST 概説	ファームとガイダンスのバージョン、ファームファイル名を変更。	中台

Contents

1. ST 概説

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

本節では、ST の識別情報を記述する。

・タイトル　：ORPHIS FT2430 / ComColor FT2430 with
ORスキャナーHS7000 / Scanner HS7000 and
RISOセキュリティパッケージ for FT / RISO Security Package F20
セキュリティターゲット

・バージョン　：2.0

・作成日　：2022 年 9 月 16 日

・作成者　：理想科学工業株式会社

1.2. TOE 参照

本節では、TOE の識別情報を記述する。

・TOE 名　：【日本語】
ORPHIS FT2430 with ORスキャナーHS7000 and RISOセキュリティパッケージ for FT
【英語】
ComColor FT2430 with Scanner HS7000 and RISO Security Package F20

・バージョン　：SORAALL 1.2.000

・開発者　：【日本語】
理想科学工業株式会社
【英語】
RISO KAGAKU CORPORATION

・構成　：以下の HCD 本体と HCD 接続の必須オプションで構成する。
HCD 本体：
ORPHIS FT2430 / ComColor FT2430
必須オプション：
ORスキャナーHS7000 / Scanner HS7000
FBファームバージョン3.1.009
AFファームバージョン1.5.000

1.3. TOE 概要

本節では、TOE 種別、TOE の主要なセキュリティ機能、TOE の使用方法、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 種別

本 TOE は、ネットワーク環境で使用される HCD である。主な機能に、プリント機能、コピー機能、スキャン機能、及びボックス機能（文書の保存と取り出し）がある。コピー機能、スキャン機能及びボックス機能には、スキャナー（必須オプション）が必要である。

1.3.2. TOE の主要なセキュリティ機能及び TOE の使用方法

本 TOE は、プリント機能、コピー機能、スキャン機能、及びボックス機能（文書の保存と取り出し）を持つ HCD である。本 TOE を使用するにあたっては、ユーザー名とパスワードによる利用者の識別認証が必要であり、外部認証にも対応している。上記の各機能は、利用者に割り振られた役割によって使用を制限することができる。プリント機能やスキャン機能によってデータ化した文書は、暗号化して TOE 内に保存されるが、TOE のセキュリティを維持するための設定情報も同じく TOE 内に暗号化して保存される。TOE のセキュリティを維持するための管理機能は、管理者のみが操作可能である。本 HCD はファイアーウォールで守られた内部ネットワーク環境で使用することを想定しており、クライアント PC のブラウザを使用して TOE を操作したり、スキャンした文書データをメールサーバー経由で送信もしくはファイルサーバーに保存したりすることができる。これらのサーバーやクライアント PC との通信は暗号化通信（IPsec）によって保護される。TOE が使用された履歴は監査ログとして監査サーバーへ送信される。TOE は自己テスト機能を持ち、電源 ON の都度ファームウェアの完全性を確認する。また、ファームウェアのアップデート時には署名検証が実施される。

TOE の利用環境を図 1 に示し、使用方法を説明する。

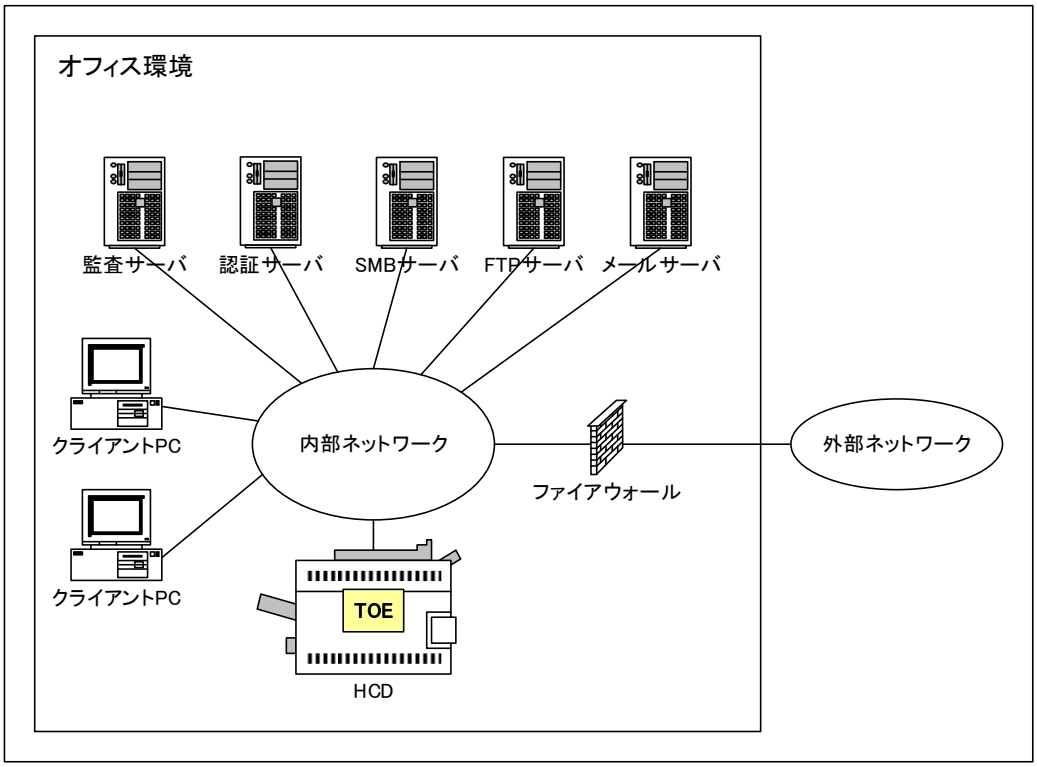


図 1　TOE の利用環境

クライアント PC

内部ネットワーク（LAN）に接続される。ブラウザ（Microsoft Edge）を介して HCD と接続し、HCD をリモート操作できる。プリンタードライバーをインストールすることで、利用者文書を印刷、保存できる。

監査サーバー

内部ネットワーク（LAN）に接続される。HCD が作成した監査ログを保存する。

認証サーバー

内部ネットワーク（LAN）に接続される。HCD の利用者を識別、認証するためのサーバーであり、外部認証システムで運用する場合に Windows Server 2019 が必要となる。アプリケーションプロトコルは、LDAP 及び Kerberos を使用する。

SMB サーバー

内部ネットワーク（LAN）に接続される。HCD でスキャンして送信した文書データを保存する。ファイルを SMB プロトコルで転送する場合に必要となる。

FTP サーバー

内部ネットワーク（LAN）に接続される。HCD でスキャンして送信した文書データを保存する。ファイルを FTP プロトコルで転送する場合に必要となる。

メールサーバー

内部ネットワーク（LAN）に接続される。HCD でスキャンした文書データをメールで送信する。

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

TOE に必要とされる TOE 以外のハードウェア／ソフトウェア／ファームウェアを表 1 に示す。

表 1　TOE の機能利用に必要な環境

機器		評価の構成
認証サーバー		Windows Server 2019 Std.
クライアント PC	OS	Windows10（64-bit）
	ブラウザ	Microsoft Edge 93
	プリンタードライバー	RISO Printer Driver for ORPHIS FT Series 1.20.002 RISO Printer Driver for ComColor FT Series 1.20.002
監査サーバー		Kali Linux-2021.1 rsyslog 8.2102.0 Strongswan 5.9.2（IPsec デーモン）
		Windows10（64-bit） WinSyslog 17.0
メールサーバー		Kali Linux-2021.1 postfix 3.5.6 Strongswan 5.9.2（IPsec デーモン）
SMB サーバー		Kali Linux-2021.1 samba 4.13.5 Strongswan 5.9.2（IPsec デーモン）
FTP サーバー		Kali Linux-2021.1 vsftpd 3.0.3 Strongswan 5.9.2（IPsec デーモン）

1.4. TOE 記述

1.4.1. TOE の物理的範囲及び TOE の配付方法

TOE の物理的範囲を図 2 に示す。

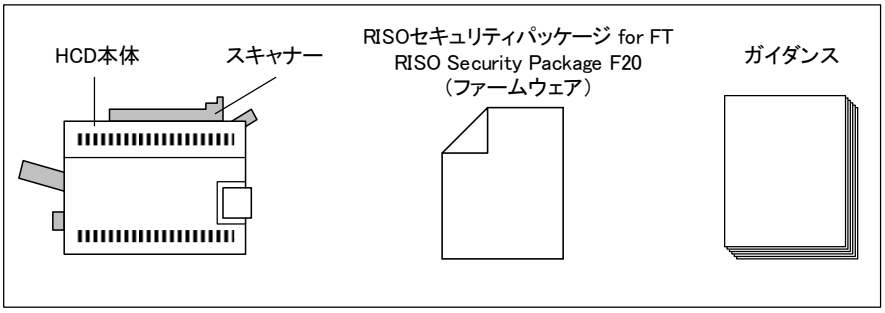


図 2 TOE の物理的範囲

TOEは、表 2のHCD本体機種名に示した機種の何れかとスキャナーとRISOセキュリティパッケージ for FT／RISO Security Package F20とガイダンスで構成される。構成要素について説明する。

表 2 HCD 本体及びスキャナー

仕向け	HCD 本体機種名 （バージョン）	スキャナー機種名 （バージョン）
日本	ORPHIS FT2430 （ファームバージョン 1.21.004）	ORスキャナーHS7000 （FB ファームバージョン 3.1.002※ AF ファームバージョン 1.0.000）
海外	ComColor FT2430 （ファームバージョン 1.21.004）	Scanner HS7000 （FB ファームバージョン 3.1.002※ AF ファームバージョン 1.0.000）

※出荷時点の FB ファームバージョンは 3.1.002、AF ファームバージョンは 1.0.000 であるが、セキュリティパッケージのインストールにより、FB ファームバージョンは 3.1.009、AF ファームバージョンは 1.5.000 にアップされる。

・HCD 本体

表 2 に示す仕向けに応じて、HCD 本体機種名の何れかが、スキャナーとは別梱包で業者により別配送される。

・スキャナー

表 2 に示す仕向けに応じたスキャナーが、HCD 本体とは別梱包で業者により別配送される。TOE の必須オプション。

・RISOセキュリティパッケージ for FT／RISO Security Package F20（ファームウェア）

USB メモリーに保存され（*.tgz）、保守員によりハンドキャリーされる。TOE の必須オプション。

ファームバージョン SORAALL 1.2.000

ファームファイル名「SORAPAC_V001002000.tgz.enc」（バージョンと一意に紐づく数字 9 桁を含む）

・ガイダンス

USB メモリーに保存され（*.pdf）、保守員によりハンドキャリーされる。

「ORPHIS FTシリーズ RISOセキュリティパッケージ for FT セキュリティガイド（067-36067-003）（2022/4） ／ ComColor FT Series ComColor black FT Series RISO SECURITY PACKAGE F20 Security Guide（067-36068-000）（2022/4）」と

「RISOセキュリティパッケージ for FT お客様用手順書 ORPHIS FT5430 / ORPHIS FT5230 / ORPHIS FT5230A / ORPHIS FT5231 / ORPHIS FT2430 / ORPHIS FT1430（067-36070-306） ／ RISO Security Package F20 Installation Procedure (Customer) ComColor FT5430 / ComColor FT5430R / ComColor FT5230 / ComColor FT5230R / ComColor FT5231 / ComColor FT5231R / ComColor FT5000 / ComColor FT5000R / ComColor FT2430 / ComColor black FT1430 / ComColor black FT1430R（067-36079-303）」は紙でも配付される。

「1.4.3.ガイダンス」を参照。

1.4.2. TOE の論理的範囲

1.4.2.1. 基本機能

TOE の基本機能の概要を以下に示す。

1)プリント機能

リモート利用者は、クライアント PC のプリンタードライバーから LAN 上の HCD へ印刷指示と共に文書データを送る。ローカル利用者は操作パネルから文書データの印刷を指示する。

2)コピー機能

ローカル利用者は、スキャナーで紙原稿をスキャンし、文書データを印刷する。

3)スキャン機能

ローカル利用者は、スキャナーで紙原稿をスキャンして SMB サーバー、FTP サーバー及びメールサーバーへ送る。

4)ボックス機能（文書の保存と取り出し）

ローカル利用者またはリモート利用者は、スキャナーで読み込まれた文書データもしくはプリンタードライバーから投入された文書データをボックスに保存する、もしくはボックス内に保存された文書データをプレビュー／印刷する。スキャンして一時保存された文書データを RISO Console からダウンロードする。

1.4.2.2. セキュリティ機能

TOE のセキュリティ機能を以下に示す。

1)識別認証及び権限付与

一般利用者の識別認証はユーザー名とパスワードを操作パネルもしくは RISO Console から入力することによって行われる。識別認証は外部認証にも対応しており、アプリケーションプロトコルは LDAP および Kerberos を使用する。

管理者の認証はセキュリティパスワードを操作パネルもしくは RISO Console から入力することによって行われる。

プリンタードライバーから投入されたジョブ及び文書はユーザー名によって識別される。

識別認証が成功したユーザーには役割が関連付けられ、ログアウトするまで維持される。

ログインした利用者が一定時間操作しない状態が続いた場合は自動的にログアウトされる。

認証画面で入力されるパスワード及びセキュリティパスワードはダミー文字で置き換えられ、認証失敗回数が設定値に達した場合は認証機能をロックする。パスワード及びセキュリティパスワードは最小パスワード長や使用可能文字などの条件を満たす必要がある。

2)アクセス制限機能

TOE は保護資産である利用者文書及び利用者データへのアクセスを、ユーザーに割り付けられた役割に応じて制限する。

3)保存データの暗号化

現地交換可能な不揮発性ストレージデバイス上に保存される保護資産（利用者データ及び TSF データ）を保護するため、保存データを暗号化する。暗号化は、国際的に承認された暗号アルゴリズムの使用により保証される。

保護資産は、不揮発性ストレージデバイス上に保存される際に文書単位もしくは入力されたデータ単位で暗号化され、保護資産のみを保存するための特定領域に書き込まれる。特定領域以外に保護資産が書き込まれることはない。

暗号化に使用される鍵は平文で不揮発性ストレージデバイスに保存されない。不要になった平文の鍵及び鍵材料は破棄される。また全ての対称暗号鍵の読出しは防止される。

4)通信の保護

ネットワーク通信を保護するための高信頼な通信パスは、内部ネットワーク（LAN）内で HCD と接続される機器間で行われることを保証するために確立される。

セキュリティプロトコル（IPsec）を使用して、通信相手の識別や通信内容の改変検知や通信データの暗号化を実施し、HCD と各サーバーの間、及び、HCD と各クライアント PC の間の通信を保護することを保証する。IPsec で使用される平文の鍵及び鍵材料は不揮発性ストレージデバイスには保存されない。不要になった平文の鍵及び鍵材料は破棄される。また全ての対称暗号鍵の読出しは防止される。

IPsec で使用される事前共有鍵は 22～32 文字の範囲で使用が許可されている文字のみで構成される。

5)セキュリティ機能の管理

セキュリティ機能に関連する設定は、管理者メニューから実施でき、このメニューへのアクセスは管理者のみに許可されている。また、セキュリティ属性及び TSF データの管理を許可された役割に制限する。

6)監査ログ機能

セキュリティ関連の事象と HCD の利用が権限付与された管理者によりモニターできることを保証するため、監査対象事象が発生するごとに監査ログが HCD により生成される。生成された監査ログには信頼されたタイムスタンプが付与され、HCD の不揮発性ストレージデバイス上には保存されず、外部の監査ログサーバーへ暗号化通信により送信される。

7)自己テスト及びファームウェアの検証

HCD へのファームウェアのアップデートは、アップデートの適用前にファームウェアが正規なものであるかを保証するためにデジタル署名によって検証される。また HCD の運用が検出可能な故障等により中断されないことを保証するため、電源 ON による HCD の起動時にハッシュによる自己テストを実行する。

1.4.3. ガイダンス

TOE を構成するガイダンス文書を表 3 に示す。
ガイダンス文書は日本語版と英語版を用意している。販売地域に応じて適切な言語の文書を配付する。

表 3　ガイダンス文書

言語	名称（バージョン）
日本語	ORPHIS FT シリーズ 5430/5230/5230A/5231/2430/1430 スタートガイド（067-36001-100）
	ORPHIS FT シリーズ 5430/5230/5230A/5231/2430/1430 ユーザーズガイド（067-36002-505）
	ORPHIS FT シリーズ 5430/5230/5230A/5231/2430/1430 こんなときには（067-36003-102）
	ORPHIS FT シリーズ 5430/5230/5230A/5231/2430/1430 管理者ガイド（067-36004-206）
	ORPHIS FT シリーズ RISO セキュリティパッケージ for FT セキュリティガイド（067-36067-003）（2022/4）
	RISO セキュリティパッケージ for FT お客様用手順書 ORPHIS FT5430 / ORPHIS FT5230 / ORPHIS FT5230A / ORPHIS FT5231 / ORPHIS FT2430 / ORPHIS FT1430（067-36070-306）
英語	ComColor FT Series 5430/5430R/5230/5230R/5231/5231R/5000/5000R/2430 ComColor black FT Series 1430/1430R Quick Guide（067-36005-105）
	ComColor FT Series 5430/5430R/5230/5230R/5231/5231R/5000/5000R/2430 ComColor black FT Series 1430/1430R User's Guide（067-36006-500）
	ComColor FT Series 5430/5430R/5230/5230R/5231/5231R/5000/5000R/2430 ComColor black FT Series 1430/1430R Troubleshooting Guide（067-36007-108）
	ComColor FT Series 5430/5430R/5230/5230R/5231/5231R/5000/5000R/2430 ComColor black FT Series 1430/1430R Administrator's Guide（067-36008-201）
	ComColor FT Series ComColor black FT Series RISO SECURITY PACKAGE F20 Security Guide（067-36068-000）（2022/4）
	RISO Security Package F20 Installation Procedure (Customer) ComColor FT5430 / ComColor FT5430R / ComColor FT5230 / ComColor FT5230R / ComColor FT5231 / ComColor FT5231R / ComColor FT5000 / ComColor FT5000R / ComColor FT2430 / ComColor black FT1430 / ComColor black FT1430R（067-36079-303）

2. 適合主張

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

・ST が適合を主張する CC のリビジョン
Part1: Introduction and general model Version 3.1 Revision 5
Part2: Security functional components Version 3.1 Revision 5
Part3: Security assurance components Version 3.1 Revision 5

・CC パート 2（セキュリティ機能要件）への適合
Part 2 (CCMB-2017-04-002) Extended

・CC パート 3（セキュリティ保証要件）への適合
Part 3 (CCMB-2017-04-003) Conformant

2.2. PP 主張

・本 ST 及び TOE が適合する PP は下記の通り。

PP 名称	：Protection Profile for Hardcopy Devices
PP バージョン	：1.0 dated September 10, 2015
Errata	：Protection Profile for Hardcopy Devices -v1.0 Errata #1, June 2017

2.3. パッケージ主張

パッケージへの適合は主張しない

2.4. 適合根拠

PP が要求する以下の条件を満足し、PP の要求通り「Exact Conformance」である。そのため、TOE 種別は PP と一貫している。

・Required Uses

Printing, Copy, Scanning, Network communications, Administration

・Conditionally Mandatory Uses

Storage and retrieval, Field-Replaceable Nonvolatile Storage

・Optional Uses

なし

3. セキュリティ課題定義

本章では、利用者、保護資産、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. 利用者

TOE の利用者を表 4 に定義する。

表 4 利用者分類

名称	分類名	定義
U.NORMAL	一般利用者	識別され、認証された利用者で、管理者役割を持たない利用者
U.ADMIN	管理者	識別され、認証された利用者で管理者役割を持つ利用者

3.2. 保護資産

TOE の保護資産は、利用者データと TSF データの 2 つがある。表 5 に定義する。

表 5 資産分類

名称	資産分類	定義
D.USER	利用者データ	TSF の操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ
D.TSF	TSF データ	TSF の操作に影響を与えるかもしれない TOE のための TOE によって作成されたデータ

3.2.1. 利用者データ

利用者データは、利用者文書データと利用者ジョブデータの 2 つがある。表 6 に定義する。

表 6 利用者データ種別

名称	利用者データ種別	定義
D.USER.DOC	利用者文書データ	電子的またはハードコピーの形式で、利用者文書に含まれる情報
D.USER.JOB	利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報

3.2.2. TSF データ

TSF データは、TSF 保護データと TSF 秘密データの 2 つがある。表 7 に定義する。

表 7　TSF データ種別

名称	TSF データ種別	定義
D.TSF.PROT	保護された TSF データ	データの所有者でもなく、管理者役割も持たない利用者によって、改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないが、暴露については容認できるような TSF データ。 内部認証時のユーザー名・役割（一般利用者／管理者）・パソコンログイン ID・日時・監査サーバーの接続設定・認証サーバーの接続設定・ネットワークの接続設定・IP アドレスの制限設定・IPsec 設定・メールサーバーの接続設定・最小パスワード長・自動ログアウト時間・ログイン失敗制限回数・証明書のインストールの許可設定・証明書・ファームウェアのアップデートの許可設定・ファームウェア
D.TSF.CONF	秘密の TSF データ	データの所有者でもなく、管理者役割も持たない利用者によって、暴露または改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないような TSF データ。 ログインパスワード・セキュリティパスワード・ファイル暗号鍵・IPsec 通信の事前共有鍵・IPsec 通信の RSA 秘密鍵・LDAP サーバー検索用パスワード・SMB サーバーパスワード・FTP サーバーパスワード

3.3. 脅威

TOE に対する脅威を表 8 に示す。

表 8　脅威

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the

	security of the TOE by monitoring or manipulating network communication.

3.4. 組織のセキュリティ方針

組織のセキュリティ方針を表 9 に示す。

表 9 組織のセキュリティ方針

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.

3.5. 前提条件

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 10 に示す。

表 10 前提条件

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

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、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. 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を表 11 に示す。

表 11 運用環境のセキュリティ対策方針

Designation	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer’s guidance to correctly configure the TOE and protect passwords and keys accordingly.

5. 拡張コンポーネント定義

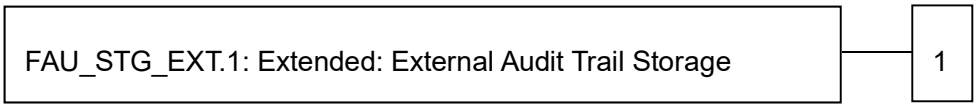
CC パート 2 に定義された、セキュリティ機能コンポーネントの拡張コンポーネントとして、以下の項目を定義する。

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component leveling:



FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:

The following actions could be considered for the management functions in FMT:

• The TSF shall have the ability to configure the cryptographic functionality.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Rationale:

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

5.2. FCS_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

Component leveling:

FCS_CKM_EXT.4: Extended: Cryptographic Key Material Destruction	4

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

Management:

The following actions could be considered for the management functions in FMT:

・There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

Rationale:

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

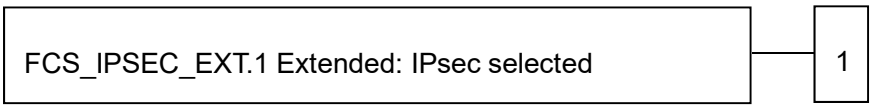
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_IPSEC_EXT Extended: IPsec selected

Family Behavior:

This family addresses requirements for protecting communications using IPsec.

Component leveling:



FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

Rationale: According to the cPP for Network devices v1.0, there is FCS_IPSEC_EXT.1 related SFR with some dependencies. For consistency between other cPPs/PPs and HCD PP v1.0, missing SFRs are appended in its dependencies list.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], *and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996* [selection: *with no*

support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23], *and* [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection*: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]*; IKEv1 SA lifetimes can be established based on* [selection*: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP)),* [assignment: *other DH groups that are implemented by the TOE*]*, no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.

Rationale:

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

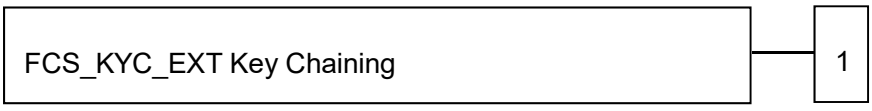
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family Behavior:

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

Component leveling:



FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping), FCS_SMC_EXT.1 Extended: Submask Combining, FCS_COP.1(i) Cryptographic operation (Key Transport), FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation), and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEVor DEK*; *intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)*: [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

Rationale:

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.

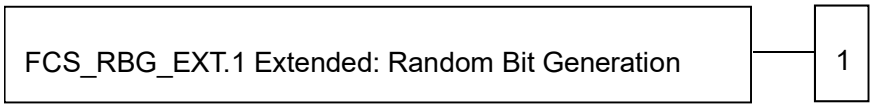
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.5. FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family Behavior:

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component leveling:



FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security strength table for hash functions”, of the keys and hashes that it will generate.

Rationale:

Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.6. FDP_DSK_EXT Extended: Protection of Data on Disk

Family Behavior:

This family is to mandate the encryption of all protected data written to the storage.

Component leveling:

FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

FDP_DSK_EXT.1.1 The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

Rationale:

Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

5.7. FIA_PMG_EXT Extended: Password Management

Family Behavior:

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component leveling:

FIA_PMG _EXT.1 Extended: Password Management	1

FIA_PMG _EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FIA_PMG _EXT.1 Extended: Password management

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG _EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

• Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*, [assignment: *other characters*]];

• Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

Rationale:

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.8. FIA_PSK_EXT Extended: Pre-Shared Key Composition

Family Behavior:

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

Component leveling:

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition	1

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

• 22 characters in length and [selection: [assignment: *other supported lengths*]*, no other lengths*];

• composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

Rationale:

Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

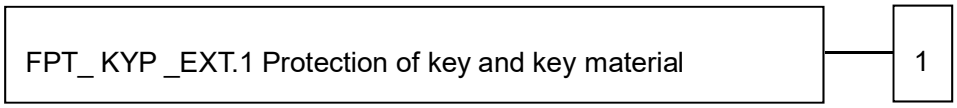
This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

5.9. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

Component leveling:



FPT_ KYP _EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FPT_ KYP _EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ KYP _EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such

plaintext key on a device that uses the key for its encryption.

Rationale:

Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

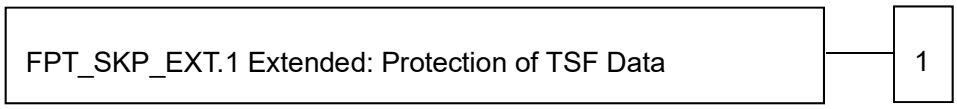
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.10. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

Component leveling:



FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Rationale:

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

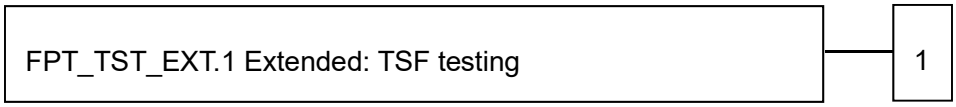
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

5.11. FPT_TST_EXT Extended: TSF testing

Family Behavior:

This family addresses the requirements for self-testing the TSF for selected correct operation.

Component leveling:



FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Rationale:

TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.12. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

Management:

The following actions could be considered for the management functions in FMT:

• There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

• There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

(for O.UPDATE_VERIFICATION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), FCS_COP.1(c) Cryptographic operation (Hash Algorithm).

Rationale: Dependency FCS_COP.1(c) is mandatory for signature verification.

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.

Rationale:

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

6. セキュリティ要件

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

TOE セキュリティ機能要件記載に関する表記法を表 12 に示す。

表 12 表記法

書体	表記内容
ボールド書体	PP で完成または詳細化した部分を示す。
イタリック書体	本 ST において選択または割付した部分を示す。選択または割付した値は [ ] 内に記載する。
ボールドイタリック書体	PP で完成または詳細化した部分、かつ、本 ST において選択または割付した部分を示す。選択または割付した値は [ ] 内に記載する。
括弧内に文字（例えば、(a)、(b)、・・・）	PP による繰返しを示す。

6.1.1. Class FAU: Security Audit

FAU_GEN.1 Audit data generation

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **All auditable events specified in 表 13**, [*なし*]。

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in 表 13**, [*と以下の*

監査関連情報。

・プリンター識別情報

・出力するログの文字コード

]

表 13　監査対象事象リスト

Auditable event	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	操作された管理機能、操作内容
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

FAU_GEN.2 User identity association

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_STG_EXT.1 Extended: External Audit Trail Storage

(for O.AUDIT)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation,

FTP_ITC.1 Inter-TSF trusted channel.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

6.1.2. Class FCS: Cryptographic Support

FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [**

• *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*

• *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes*

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b) Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: No Standard.**

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

FCS_CKM.4 Cryptographic key destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

For volatile memory, the destruction shall be executed by* [*powering off a device*]*. For nonvolatile storage, the destruction shall be executed by a* [*single*] *overwrite of key data storage location consisting of* [*a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1)*]*, followed by a* [*none*]*. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: [***no standard***].

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)] FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(a) Refinement: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in** [***暗号利用モード：CBC***] and cryptographic key sizes **128-bits and 256-bits** that meets the following:

• FIPS PUB 197, "Advanced Encryption Standard (AES)"

• **[*NIST SP 800-38A*]**

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1: The TSF shall perform all deterministic random bit generation services in accordance with [*NIST SP 800-90A*] using [*Hash_DRBG (SHA256)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1つの*] *hardware-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.

Dependencies: FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(i) Cryptographic operation (Key Transport),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [*intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)*: [*key encryption as specified in FCS_COP.1(f)*]] while maintaining an effective strength of [*128 bits*].

FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

(for O. STORAGE_ENCRYPTION)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [*CBC*] mode** and cryptographic key sizes **[*128 bits*]**

that meet the following: **AES as specified in ISO/IEC 18033-3, [*CBC as specified in ISO/IEC 10116*].**

FCS_COP.1(f) Cryptographic operation (Key Encryption)

(selected from FCS_KYC_EXT.1.1)

Hierarchical to: No other components.

Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(f) Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [*CBC*] mode** and cryptographic key sizes **[*128 bits*]** that meet the following: **AES as specified in ISO /IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

FCS_IPSEC_EXT.1 Extended: IPsec selected

Hierarchical to: No other components.

Dependencies: FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [*transport mode*].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [*the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [*IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [*no other RFCs for extended sequence numbers*], *and* [*RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [*IKEv1*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [*no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [*IKEv1 SA lifetimes can be established based on* [*length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [*no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [*RSA*] algorithm and Pre-shared Keys.

FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-**[***SHA-1, SHA-256, SHA-384, SHA-512***], **key size** [***160ビット、256ビット、384ビット、512ビット***], **and message digest sizes [*160, 256, 384, 512*] bits** that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.
Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) Refinement: The TSF shall perform **cryptographic signature services** in accordance with a **[*RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of* [*2048 ビット*]]**
that meets the following **[*FIPS PUB 186-4,* "*Digital Signature Standard*"].**

FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.1.1(c) Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

6.1.3. Class FDP: User Data Protection

FDP_ACC.1 Subset access control
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **表 14 and 表 15.**

FDP_ACF.1 Security attribute based access control
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on

the following: subjects, objects, and attributes specified in **表 14 and 表 15.**

FDP_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in 表 14 and 表 15**.

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*なし*].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*なし*].

表 14 D.USER.DOC Access Control SFP

		"Create"	**"Read"**	**"Modify"**	**"Delete"**
Print	**Operation:**	**Submit a document to be printed**	**View image or Release printed output**	**Modify stored document**	**Delete stored document**
	Job owner	(note 1)		*拒否*	
	U.ADMIN			*拒否*	
	U.NORMAL		denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	**Operation:**	**Submit a document for scanning**	**View scanned image**	**Modify stored image**	**Delete stored image**
	Job owner	(note 2)		*拒否*	
	U.ADMIN		*拒否*	*拒否*	*拒否*
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	**Operation:**	**Submit a document for copying**	**View scanned image or Release printed copy output**	**Modify stored image**	**Delete stored image**
	Job owner	(note 2)		*拒否*	

	U.ADMIN		*拒否*	*拒否*	
	U.NORMAL		denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Storage / retrieval	**Operation:**	**Store document**	**Retrieve stored document**	**Modify stored document**	**Delete stored document**
	Job owner	(note 1)		*拒否*	
	U.ADMIN		*拒否*	*拒否*	
	U.NORMAL		denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied

表 15　D.USER.JOB Access Control SFP

		"Create"	**"Read"**	**"Modify"**	**"Delete"**
Print	**Operation:**	**Create print job**	**View print queue / log**	**Modify print job**	**Cancel print job**
	Job owner	(note 1)			
	U.ADMIN			*拒否*	
	U.NORMAL		*拒否*	denied	denied
	Unauthenticated	*(condition 1)*	*拒否*	denied	denied
Scan	**Operation:**	**Create scan job**	**View scan status / log**	**Modify scan job**	**Cancel scan job**
	Job owner	(note 2)		*拒否*	
	U.ADMIN			*拒否*	*拒否*
	U.NORMAL		*拒否*	denied	denied
	Unauthenticated	denied	*拒否*	denied	denied
Copy	**Operation:**	**Create copy job**	**View copy status / log**	**Modify copy job**	**Cancel copy job**
	Job owner	(note 2)			
	U.ADMIN			*拒否*	*拒否*
	U.NORMAL		*拒否*	denied	denied
	Unauthenticated	denied	*拒否*	denied	denied
Storage / retrieval	**Operation:**	**Create storage / retrieval job**	**View storage / retrieval log**	**Modify storage / retrieval job**	**Cancel storage / retrieval job**
	Job owner	(note 1)			
	U.ADMIN			*拒否*	*拒否*
	U.NORMAL		*拒否*	denied	denied

	Unauthenticated	(condition 1)	*拒否*	denied	denied

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.

Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.

Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

FDP_DSK_EXT.1.1 The TSF shall [*perform encryption in accordance with FCS_COP.1(d)*] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

6.1.4. Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* [*1～5*]] *unsuccessful authentication attempts occur related to* [*認証事象リスト（表 16）*].

表 16　認証事象リスト

認証事象
操作パネルでの一般利用者ログイン
クライアント PC のブラウザ上から RISO Console を利用する際の一般利用者ログイン
操作パネルで「管理者メニュー」へアクセスするための管理者への役割昇格
クライアント PC のブラウザ上から RISO Console を利用する際に「管理者メニュー」へアクセスするため

の管理者への役割昇格

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*認証失敗時のアクションリスト(表 17)の実行*].

表 17　認証失敗時のアクションリスト

認証事象	アクション
一般利用者ログイン	・該当する一般利用者に対する次回認証受付を、5 分間停止する(ロック状態)。5 分経過後、ロック状態を解除し、自動的に認証受付を再開する。 ・管理者が、ロック解除の操作をすることで、認証受付停止から 5 分以内であっても認証受付を再開する。
管理者への役割昇格	・該当する管理者に対する次回認証受付を、5 分間停止する(ロック状態)。5 分経過後、ロック状態を解除し、自動的に認証受付を再開する。

FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*セキュリティ属性リスト(表 18)*]

表 18　セキュリティ属性リスト

セキュリティ属性
ユーザー名
役割（一般利用者／管理者）

FIA_PMG_EXT.1 Extended: Password Management

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

• Passwords shall be able to be composed of any combination of upper and lower case

letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“ ”, “-”, “.”, “_”, “~”, “{”, “}”, “;”, “:”, “,”, “?”, “/”, “\”, “+”, “=”, “<”, “>”, “[”, “]”]];
• Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

FIA_UAU.1 Timing of authentication

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 Refinement: The TSF shall allow [***利用者データアクセス制御SFPと矛盾しない、D.TSF.CONFへのアクセスを提供しない、かつ任意のTSFデータを変更しない****TSF仲介アクションのリスト（表 **19**）*] on behalf of the user to be performed before the user is authenticated.

表 19　認証前の仲介アクションのリスト

TSF 仲介アクションのリスト
ユーザー名の問い合わせ（内部認証時のみ）
TOE のシステム時計の日付・時刻の問い合わせ
ネットワーク設定の問い合わせ
ファームウェアバージョンの問い合わせ
システム情報プリントのプリント
サンプル画像プリントのプリント
詳細カウントのプリント
チャージカウントのプリント
プリントジョブの投入
ボックス保存ジョブの投入

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*フィードバックのリスト(表 20)*] to the user while the authentication is in progress.

表 20　フィードバックのリスト

フィードバックのリスト
パスワードとして入力された文字数分の隠蔽文字「＊（アスタリスク）」

FIA_UID.1 Timing of identification

(for O.USER_I&A and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 Refinement: The TSF shall allow [***The User Data Access Control SFPと矛盾しない、D.TSF.CONFへのアクセスを提供しない、かつ任意のD.TSFデータを変更しないことを条件とするTSF****仲介アクションのリスト(表 21)*] on behalf of the user to be performed before the user is identified.

表 21　識別前の仲介アクションのリスト

TSF 仲介アクションのリスト
ユーザー名の問い合わせ（内部認証時のみ）
TOE のシステム時計の日付・時刻の問い合わせ
ネットワーク設定の問い合わせ
ファームウェアバージョンの問い合わせ
システム情報プリントのプリント
サンプル画像プリントのプリント
詳細カウントのプリント
チャージカウントのプリント

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*FIA_ATD.1に記載のセキュリティ属性(表 18　セキュリティ属性リスト)*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*属性の最初の関連付けの規則(表 22)*].

表 22　属性の最初の関連付けの規則

属性の最初の関連付けの規則
認証成功時にユーザー名と一般利用者を関連付ける

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*属性の変更に関する規則(表 23)*].

表 23　属性の変更に関する規則

属性の変更に関する規則
セキュリティパスワード照合成功時に管理者役割を追加で関連付ける
「管理者メニュー」から抜けた時に管理者役割の関連付けを削除する

FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [[*23～32文字*]];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [*SHA-256, SHA-512*, [*SHA-384*]] and be able to [*use no other pre-shared keys*].

6.1.5. Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

(for O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*セキュリティ機能のリスト(表 24)*] to **U.ADMIN**.

表 24　セキュリティ機能のリスト

セキュリティ機能のリスト
認証サーバー設定（内部認証／外部認証の切り替え）

FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [*query, modify, delete,* [*新規作成*]] the security attributes [*セキュリティ属性リスト(表 18)*] to [*利用者セキュリティ属性の管理(表 25)の「許可された利用者役割」*].

表 25　利用者セキュリティ属性の管理

セキュリティ属性	操作	許可された利用者役割
ユーザー名	問い合わせ	一般利用者、管理者
	新規作成、削除、改変	管理者
役割	問い合わせ、改変	管理者

FMT_MSA.3 Static attribute initialization

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 Refinement: The TSF shall allow the **[*no role*]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

(for O.ACCESS CONTROL)

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in 表 26.**

表 26 Management of TSF Data

Data	Operation	Authorised role(s)
[*パソコンログイン ID*]	[*modify, delete*, [*新規作成*]]	U.ADMIN
[*ログインパスワード*]	[*modify, delete*, [*新規作成*]]	U.ADMIN
	[*modify,* [*その他の操作なし*]]	the owning U.NORMAL.
[*セキュリティパスワード*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*日時*]	[*modify*, [*その他の操作なし*]]	U.ADMIN
[*監査サーバーの接続設定*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*認証サーバーの接続設定*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*ネットワークの接続設定*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*IP アドレスの制限設定*]	[*modify*, [*その他の操作なし*]]	U.ADMIN
[*IPsec 設定*]	[*modify, delete,* [*新規作成*]]	U.ADMIN
[*メールサーバーの接続設定*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*最小パスワード長*]	[*modify,* [*その他の操作なし*]]	U.ADMIN
[*自動ログアウト時間*]	[*modify,* [*その他の操作なし*]]	U.ADMIN

[*ログイン失敗制限回数*]	[***modify,*** [*その他の操作なし*]]	U.ADMIN
[*証明書のインストールの許可設定*]	[***modify,*** [*その他の操作なし*]]	U.ADMIN
[*証明書*]	[***modify, delete,*** [*新規作成*]]	U.ADMIN
[*ファームウェアのアップデートの許可設定*]	[***modify,*** [*その他の操作なし*]]	U.ADMIN
[*ファームウェア*]	[***modify,*** [*その他の操作なし*]]	U.ADMIN

FMT_SMF.1 Specification of Management Functions

(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*TSFにより提供される管理機能のリスト(表 27)*].

表 27　管理機能

管理機能	管理できる項目	許可された役割
認証サーバー設定	内部認証／外部認証の切り替え	管理者
	認証サーバーの接続設定	管理者
ユーザー設定	内部認証時のユーザー名	管理者
	役割（一般利用者／管理者）	管理者
	基本機能の使用許可設定（各基本機能の使用許可／不許可をユーザーごとに切り替え）	管理者
	パソコンログイン ID	管理者
	ログインパスワード	管理者
パスワード変更	ログインパスワード	所有する一般利用者管理者
セキュリティパスワード変更	セキュリティパスワード	管理者
日時設定	日時	管理者
監査サーバー設定	監査サーバーの接続設定	管理者
ネットワーク設定	ネットワークの接続設定	管理者
IP アドレス制限設定	IP アドレスの制限設定	管理者
IPsec 設定	IPsec 設定	管理者

メール送信設定	メールサーバーの接続設定	管理者
最小パスワード長設定	最小パスワード長	管理者
ログイン設定	自動ログアウト時間	管理者
	ログイン失敗制限回数	管理者
証明書関連ファイル管理	証明書	管理者
保守操作許可切替	証明書のインストールの許可設定	管理者
	ファームウェアのアップデートの許可設定	管理者
ファームウェアのアップデート	ファームウェア	管理者

FMT_SMR.1 Security roles

(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 Refinement: The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6. Class FPT: Protection of the TSF

FPT_SKP_EXT.1 Extended: Protection of TSF Data

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_STM.1 Reliable time stamps

(for.O.AUDIT)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST_EXT.1 Extended: TSF testing

(for O.TSF_SELF_TEST)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

FPT_TUD_EXT.1 Trusted Update

(for O.UPDATE_VERIFICATION)

Hierarchical to: No other components.

Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), FCS_COP.1(c) Cryptographic operation (Hash Algorithm).

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [*no other functions*] prior to installing those updates.

FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

(for O.KEY_MATERIAL)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KYP_EXT.1.1 Refinement: The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

6.1.7. Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*利用者が非アクティブである経過時間リスト(表 28)*].

表 28　非アクティブ状態での経過時間リスト

非アクティブ状態での経過時間
管理者が設定した自動ログアウト時間（10～300 秒の範囲）

6.1.8. Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF trusted channel

(for O.COMMS_PROTECTION, O.AUDIT)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1 Refinement: The TSF shall **use [*IPsec*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities:** [*authentication server,* [*監査サーバー、SMB サーバー、FTP サーバー、メールサーバー*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 Refinement: The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for [***TSF が通信を開始できるサービスのリスト(表 29)***].

表 29　通信を開始できるサービス

通信先	通信を開始できるサービス
監査サーバー	監査サーバーへ監査ログを送信するサービス
認証サーバー	ユーザー名/ログインパスワードを送信して外部認証サーバーへユーザーの認証を依頼するサービス
SMB サーバー	保存先へスキャナー保存を実施するサービス
FTP サーバー	保存先へスキャナー保存を実施するサービス
メールサーバー	宛先へメール送信を実施するサービス

FTP_TRP.1(a) Trusted path (for Administrators)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) Refinement: The TSF shall **use [*IPsec*] to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(a) Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path

FTP_TRP.1.3(a) Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

FTP_TRP.1(b) Trusted path (for Non-administrators)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) Refinement : The TSF shall **use [*IPsec*] to** provide **a trusted** communication path between

itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(b) Refinement: The TSF shall permit [***remote users***] to initiate communication via the trusted path

FTP_TRP.1.3(b) Refinement: The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

6.2. TOE セキュリティ保証要件

TOE セキュリティ保証要件を表 30 に示す。
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 30 TOE セキュリティ保証要件

Assurance Class	Assurance Components	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.3. セキュリティ要件根拠

セキュリティ要件の根拠を示す。

6.3.1. セキュリティ機能要件根拠

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。

6.3.2. セキュリティ機能要件間の依存関係

セキュリティ機能要件のコンポーネントの依存性を、表 31 に示す。

表 31 セキュリティ機能要件間の依存関係

セキュリティ機能要件	PP 規定の依存関係	本 ST での依存関係
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1
FCS_CKM.1(a)	[FCS_COP.1(b), or FCS_COP.1(i)], FCS_CKM_EXT.4	FCS_COP.1(b), FCS_CKM_EXT.4
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)], FCS_CKM_EXT.4, FCS_RBG_EXT.1	FCS_COP.1(a), FCS_COP.1(d), FCS_COP.1(f), FCS_COP.1(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1
FCS_CKM_EXT.4	[FCS_CKM.1(a), or FCS_CKM.1(b)], FCS_CKM.4	FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4
FCS_CKM.4	[FCS_CKM.1(a), or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)
FCS_COP.1(a)	[FCS_CKM.1(b)],	FCS_CKM.1(b),

	FCS_CKM_EXT.4	FCS_CKM_EXT.4
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a), ※1
FCS_COP.1(c)	-	-
FCS_COP.1(d)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4
FCS_COP.1(f)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4
FCS_IPSEC_EXT.1	FIA_PSK_EXT.1, FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1	FIA_PSK_EXT.1, FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, and/or FCS_COP.1(i)]	FCS_COP.1(f)
FCS_RBG_EXT.1	-	-
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	-	-
FIA_PMG_EXT.1	-	-
FIA_PSK_EXT.1	FCS_RBG_EXT.1	※2
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1

FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_KYP_EXT.1	-	-
FPT_SKP_EXT.1	-	-
FPT_STM.1	-	-
FPT_TST_EXT.1	-	-
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b) , FCS_COP.1(c)
FTA_SSL.3	-	-
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_IPSEC_EXT.1

※1 IPsec 通信で使用する RSA 秘密鍵は、不揮発ストレージに暗号化されて保存される。
　ファームウェアの完全性確認は、予め用意されている公開鍵で署名検証する。
※2 事前共有鍵の生成にランダムビット生成器で生成したランダムビットを使用しない。

7. TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について記述する。

7.1. 識別認証及び権限付与

利用者を識別認証し、識別認証された利用者に、その役割に応じて権限を付与する。
対応する SFR の実現方法を以下に示す。

FIA_UID.1、FIA_UAU.1

・識別認証方式には、内部認証と外部認証の 2 種類があり、「管理者メニュー」で設定されたものを使用する。外部認証を設定する操作は以下。
- 操作パネルもしくは RISO Console 画面の［管理者メニュー］の［認証サーバー設定］で［ON］を選択。

・内部認証は、HCD が HCD 内部に登録された情報を基に識別認証する。
・外部認証は、HCD 内部に登録された管理者の役割を持つ 1 名を除き、認証サーバーに登録された情報を基に識別認証する。外部認証には Windows server 2019 が必要で、アプリケーションプロトコルは LDAP および Kerberos を使用する。

・識別認証前の利用者が HCD にログインを試みると、HCD は識別認証を実施する。
・ログイン手段は、ローカルログインとリモートログインの 2 種類がある。
・ローカルログインは HCD を物理的に操作してログインする。操作パネルからユーザー名とログインパスワードを入力させる。操作は以下。
- 操作パネルの［ログイン］キーを押してユーザー名を選択／ログイン名を入力して、ログインパスワードを入力して、ログインを実行。

・リモートログインはクライアント PC 上のウェブインターフェースから RISO Console にアクセスしてログインする。クライアント PC に接続されたキーボード等の入力手段から、ユーザー名とログインパスワードを入力させる。操作は以下。
- RISO Console 画面でユーザー名とログインパスワードを入力して、ログインを実行。

・利用者により入力されたユーザー名を登録情報と照合し、一致した場合（照合成功）を識別成功とする。
・識別成功後、利用者により入力されたログインパスワードを登録情報と照合し、一致した場合（照合成功）を一般利用者の認証成功とする。

・管理者になることができる一般利用者がログイン中のときにのみ、「管理者メニュー」へアクセスするた

めのインターフェースを提供する。
・「管理者メニュー」へのアクセスを許可する前に、セキュリティパスワードを入力させる。操作は以下。
- 操作パネルもしくは RISO Console 画面で［管理者メニュー］を選択して、セキュリティパスワードを入力して、ログインを実行。
・ローカルログインでは、操作パネルからセキュリティパスワードを入力させる。
・リモートログインでは、クライアント PC に接続されたキーボード等の入力手段から、セキュリティパスワードを入力させる。
・セキュリティパスワードは全ての管理者で同一である。
・入力されたセキュリティパスワードを HCD に登録されたセキュリティパスワードと照合し、一致した場合（照合成功）を管理者の認証成功とする。これにより、管理者役割をもつ一般利用者は管理者に役割昇格する。

・プリンタードライバーからプリントジョブ／ボックスジョブ（保存）が投入されたら、HCD は識別を実施する。ジョブに付随しているパソコンログイン ID を登録情報と照合し、一致した場合（照合成功）を識別成功とする。

・識別前の利用者に表 21　識別前の仲介アクションのリストに記載された機能の利用を許可する。
・認証前の利用者に表 19　認証前の仲介アクションのリストに記載された機能の利用を許可する。
ユーザー名の問い合わせ（内部認証時のみ）
- 操作パネルで［ログイン／ログアウト］キーを押す。
TOE のシステム時計の日付・時刻の問い合わせ
- 操作パネルに表示（操作なし）
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］を選択。
ネットワーク設定の問い合わせ／ファームウェアバージョンの問い合わせ
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］を選択。
システム情報プリントのプリント
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］から［情報プリント］の［システム情報プリント］を実行。
サンプル情報プリントのプリント
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］から［情報プリント］の［サンプル情報プリント］を実行。
詳細カウントのプリント
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］の［カウント表示］を選択して、［詳細］タブの［このリストを印刷］を実行。
チャージカウントのプリント
- 操作パネルもしくは RISO Console 画面で［システム情報］の［機種情報］の［カウント表示］を選択して、［チャージ］タブの［このリストを印刷］を実行。

FIA_AFL.1

・操作パネルもしくは RISO Console における一般利用者ログイン、及び、管理者への役割昇格のそれぞれについて、認証失敗回数をカウントする。

・認証失敗回数と比較する値は、「管理者メニュー」で［1～5］の範囲で設定できる。操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ログイン設定］を選択して、［ログイン失敗制限回数］を入力。

・操作パネルもしくは RISO Console における一般利用者ログイン、及び、管理者への役割昇格のそれぞれについて、認証に失敗した回数が「管理者メニュー」で設定された値に達した場合、その利用者の認証受付を 5 分間停止する（ロック状態を保つ)。

・5 分経過後、自動的に認証受付を再開する。

・一般利用者ログインの認証受付を停止中の一般利用者に対し、当該利用者以外の管理者がロック解除を行うと、認証受付停止から 5 分経過していなくても認証受付を再開する。ロック解除の操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、［ロック解除］でログインパスワードの仮パスワードを入力。

FIA_ATD.1

・HCD は表 18　セキュリティ属性リストに記載された属性を定義し、維持することができる。

・ユーザー名を設定する操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、ユーザー名を入力。

・ユーザーに役割を設定する操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、［管理者権限］の［OFF／ON］を選択。

FIA_USB.1

・操作パネルもしくは RISO Console 画面での認証成功時にユーザー名と一般利用者役割を関連付ける（表 22　属性の最初の関連付けの規則)。

・操作パネルもしくは RISO Console 画面でのセキュリティパスワード照合成功時に管理者役割を追加で関連付ける（表 23　属性の変更に関する規則)。

・「管理者メニュー」から抜けた時に管理者役割の関連付けを削除する（表 23　属性の変更に関する規則)。

・操作は FIA_UID.1 と FIA_UAU.1 を参照。

FMT_SMR.1

・一般利用者の役割はログイン時に割り当てられ、ログアウトするまで維持する。

・一般利用者のログイン操作は FIA_UID.1 を参照。
・管理者への役割昇格中は、一般利用者役割と管理者役割を持つ。管理者の役割は役割昇格したとき（セキュリティパスワード照合成功時）に割り当てられ、役割降格するまで維持する。
・管理者の役割昇格の操作は FIA_UID.1 と FIA_UAU.1 を参照。
・管理者の役割降格の操作は以下。
- 操作パネルの［ホーム］キーを押す。(「管理者メニュー」から抜ける。)
- RISO Console 画面で管理者メニュー以外の操作領域を選択する。(「管理者メニュー」から抜ける。)
- 一般利用者のログアウト操作を参照。

FIA_PMG_EXT.1

・パスワードはログインパスワードとセキュリティパスワードの 2 種類がある。
・ログインパスワードもセキュリティパスワードもアルファベットの大文字［A-Z］(26 文字) と小文字［a-z］（26 文字)、数字［0-9］（10 文字)、及び特殊文字（29 文字）を組み合わせることができる。表 32 に使用できる特殊文字の一覧を示す。
・操作パネルもしくは RISO Console 画面でパスワードの入力内容を確定した時に、入力内容に上記以外の文字が含まれていた場合はパスワードを再入力させる。パスワード入力の操作は以下。
- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、ログインパスワードを入力。
- 操作パネルもしくは RISO Console 画面で［システム情報］の［ユーザー情報］を選択して、ログインパスワードを入力。
- 操作パネルもしくは RISO Console 画面で［管理者メニュー］を選択して、セキュリティパスワードを入力。
・最小パスワード長は「管理者メニュー」で変更可能であり、15 文字以上を選択できる（[7～16］文字の範囲で設定できる)。操作は以下。
- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［最小パスワード長設定］を選択して、数字（[7～16］の何れか）を入力。

表 32　パスワードで使用できる特殊文字

特殊文字	Unicode スカラ値	名称
!	U+0021	EXCLAMATION MARK
@	U+0040	COMMERCIAL AT
#	U+0023	NUMBER SIGN
$	U+0024	DOLLAR SIGN
%	U+0025	PERCENT SIGN
^	U+005E	CIRCUMFLEX ACCENT
&	U+0026	AMPERSAND

*	U+002A	ASTERISK
(	U+0028	LEFT PARENTHESIS
)	U+0029	RIGHT PARENTHESIS
	U+0020	SPACE
-	U+002D	HYPHEN-MINUS
.	U+002E	FULL STOP
_	U+005F	LOW LINE
~	U+007E	TILDE
{	U+007B	LEFT CURLY BRACKET
}	U+007D	RIGHT CURLY BRACKET
;	U+003B	SEMICOLON
:	U+003A	COLON
,	U+002C	COMMA
?	U+003F	QUESTION MARK
/	U+002F	SOLIDUS
|	U+007C	VERTICAL LINE
+	U+002B	PLUS SIGN
=	U+003D	EQUALS SIGN
<	U+003C	LESS-THAN SIGN
>	U+003E	GREATER-THAN SIGN
[	U+005B	LEFT SQUARE BRACKET
]	U+005D	RIGHT SQUARE BRACKET

FIA_UAU.7

・操作パネルまたは RISO Console でログインパスワードまたセキュリティパスワードを入力した時は、表 20　フィードバックのリストに記載の通り、入力された文字数と同じ文字数の「＊（アスタリスク）」を表示する。

FTA_SSL.3

・管理機能で設定された自動ログアウト時間の間、ログイン中の利用者が操作パネルの操作または RISO Console の操作を行わなかった場合は、自動的に当該利用者をログアウトさせる。

・ログアウトさせた利用者が役割昇格中であった場合は、役割降格と同時にログアウトさせる。

・自動ログアウト時間は、「管理者メニュー」で［10～300］秒の範囲で設定できる。操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ログイン設定］を選択して、［自動ログアウト時間］を入力。

・操作パネルでは、利用者をログアウトさせたら、ホーム画面に戻り、表示していたユーザー名を消す。
・RISO Console では、利用者をログアウトさせたら、ログアウト以降に RISO Console の画面更新があったときに、［管理者メニュー］の［コンソール起動画面］で設定した画面に戻り、表示していたユーザー名を消す。

7.2. アクセス制限機能

利用者の役割に応じた権限に基づき、文書、及び文書処理に関連する情報の操作を制限する。
対応する SFR の実現方法を以下に示す。

FDP_ACC.1、FDP_ACF.1

1. 利用者文書データのアクセス制御

・利用者文書データに対するアクセスを、表 14　D.USER.DOC Access Control SFP の通りに制限する。
・利用者が HCD へ一般利用者ログインし、プリント機能もしくはボックス機能を選択すると、HCD は当該一般利用者が所有する文書の一覧を表示する。その後、文書が選択されると、HCD は当該文書に対し許可された操作のみインターフェースを提供する。
・利用者が HCD へ一般利用者ログインし、コピー機能もしくはスキャン機能を選択すると、HCD は許可された操作のみインターフェースを提供する。
・利用者が HCD へ管理者ログインし、プリント機能もしくはボックス機能を選択すると、HCD は全利用者が所有する文書の一覧を表示する。その後、文書が選択されると、HCD は当該文書に対し許可された操作のみインターフェースを提供する。
・利用者が HCD へ管理者ログインし、コピー機能もしくはスキャン機能を選択すると、HCD は許可された操作のみインターフェースを提供する。
・HCD が許可する操作を表 33 に示す。

表 33　HCD が許可する操作（D.USER.DOC）

Print		
操作	利用者	HCD が許可する操作
Create	Job owner	クライアント PC にインストールしたプリンタードライバーで、出力方法［プリント］もしくは［プリント＆ボックス］を選択して、文書を送信する。 （プリンタードライバーから送信されたプリントジョブは、利用者識別のための情報を持っている。）
	U.ADMIN	
	U.NORMAL	
	Unauthenticated	
	Job owner	RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、印刷を実行する。

		RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、印刷を実行する。
Read	Job owner	操作パネルのホーム画面もしくは RISO Console 画面で［プリント］を選択し、プリント画面でサムネイル表示する。
		操作パネルのホーム画面もしくは RISO Console 画面で［プリント］を選択し、プリント画面で文書を選択して、詳細確認を実行する。
		操作パネルのホーム画面で［プリント］を選択し、プリント画面で文書を選択して、印刷を実行する。(管理者の設定によっては、操作パネルからログインしただけで印刷が実行される。)
	U.ADMIN	操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［保留ジョブ］タブで文書を選択して、詳細確認を実行する。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	なし（操作インターフェースがない）	
Delete	Job owner	印刷途中で、操作パネルのストップキーを押して一時停止し、中止を実行する。
		操作パネルのホーム画面もしくは RISO Console 画面で［プリント］を選択し、プリント画面で文書を選択して、削除を実行する。
		RISO Console 画面で［プリント］を選択し、プリント画面で文書を選択して、［詳細表示］を選択し、削除を実行する。
		操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブで文書を選択して、削除を実行する。
		操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴)］タブで文書を選択して、削除を実行する。
		RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴)］タブで文書を選択して、［詳細表示］を選択し、削除を実行する。
	U.ADMIN	操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［終了（履歴)］タブで文書を選択して、削除を実行する。
		RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［終了（履歴)］タブで文書を選択して、［詳細表示］を選択し、削除を実行する。
		操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［保留ジョブ］タブで文書を選択して、削除を実行する。
		RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［保留ジョブ］タブで文書を選択して、［詳細表示］を選択し、削除を実行する。
		操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、［ユーザー設定］でユーザーを選択して、削除を実行する。

		操作パネルのホーム画面で［管理者メニュー］を選択し、［管理者設定初期化］で全ユーザーの削除を実行する。
		操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、［認証サーバー設定］の［OFF］［ON］を切り替える。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Scan		
操作	利用者	HCD が許可する操作
Create	Job owner	操作パネルのホーム画面で［スキャン］を選択し、スキャン画面でスキャンを実行する。
	U.ADMIN	
	U.NORMAL	
	Job owner	操作パネルのホーム画面で［スキャン］を選択し、スキャン画面で送信プレビューを実行し、送信プレビュー画面でスキャンを実行する。
	U.ADMIN	
	U.NORMAL	
	Unauthenticated	なし（ログインできないので操作できない）
Read	Job owner	操作パネルのホーム画面で［スキャン］を選択し、スキャン画面で送信プレビューを実行する。
		RISO Console 画面で［スキャン］を選択し、スキャン画面でサムネイル表示する。
		RISO Console 画面で［スキャン］を選択し、スキャン画面で文書を選択して、詳細表示を実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	なし（操作インターフェースがない）	
Delete	Job owner	RISO Console 画面で［スキャン］を選択し、スキャン画面で文書を選択して、削除を実行する。
		RISO Console 画面で［スキャン］を選択し、スキャン画面で文書を選択して、［詳細表示］を選択し、削除を実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Copy		
操作	利用者	HCD が許可する操作
Create	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面でコピーを実行する。
	U.ADMIN	
	U.NORMAL	
	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面で試しコピーを実行し、

	U.ADMIN	試しコピー画面で印刷を実行する。
	U.NORMAL	
	Unauthenticated	なし（ログインできないので操作できない）
Read	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面で試しコピーを実行する。
		操作パネルのホーム画面で［コピー］を選択し、コピー画面でコピーを実行する。
		操作パネルのホーム画面で［コピー］を選択し、コピー画面で試しコピーを実行し、試しコピー画面で印刷を実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	なし（操作インターフェースがない）	
Delete	Job owner	操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブで文書を選択して、削除を実行する。
		操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴)］タブで文書を選択して、削除を実行する。
		RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴)］タブで文書を選択して、［詳細表示］を選択し、削除を実行する。
	U.ADMIN	操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［終了（履歴)］タブで文書を選択して、削除を実行する。
		RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［終了（履歴)］タブで文書を選択して、［詳細表示］を選択し、削除を実行する。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Storage / retrieval		
操作	利用者	HCD が許可する操作
Create	Job owner	保存：
	U.ADMIN	操作パネルのホーム画面で［ボックス］－［保存］を選択し、ボックス保存画面で保存を実行する。
	U.NORMAL	
	Job owner	保存：
	U.ADMIN	操作パネルのホーム画面で［ボックス］－［保存］を選択し、ボックス保存画面で保存プレビューを実行し、保存プレビュー画面で保存を実行する。
	U.NORMAL	
	Job owner	保存：
	U.ADMIN	クライアント PC にインストールしたプリンタードライバーで、出力方法［ボックス］もしくは［プリント＆ボックス］を選択して、文書を送信する。 （プリンタードライバーから送信されたボックスジョブ（保存）は、利用者識別の
	U.NORMAL	
	Unauthenticated	

		ための情報を持っている。）
Read	Job owner	取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面でサムネイル表示する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、詳細確認を実行する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面でサムネイル表示する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、［詳細確認］を実行する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、印刷を実行する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、印刷を実行する。
		RISO Console 画面で［スキャン］を選択し、スキャン画面で文書を選択して、ダウンロードを実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	なし（操作インターフェースがない）	
Delete	Job owner	保存： 操作パネルのホーム画面で［ボックス］－［保存］を選択し、ボックス保存画面で文書を選択して、削除を実行する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、削除を実行する。
		取り出し： RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、［詳細表示］を選択し、削除を実行する。
		取り出し：

		操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、削除を実行する。
		取り出し： RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、［詳細表示］を選択し、削除を実行する。
	U.ADMIN	保存／取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、［ユーザー設定］でユーザーを選択して、削除を実行する。
		保存／取り出し： 操作パネルのホーム画面で［管理者メニュー］を選択し、［管理者設定初期化］で全ユーザーの削除を実行する。
		保存／取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、［認証サーバー設定］の［OFF］［ON］を切り替える。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）

2. 利用者データのアクセス制御

・利用者ジョブデータに対するアクセスを、表 15　D.USER.JOB Access Control SFP の通りに制限する。

・利用者が HCD へ一般利用者ログインし、プリント機能もしくはボックス機能を選択すると、HCD は当該一般利用者が所有するジョブの一覧を表示する。その後、ジョブが選択されると、HCD は当該ジョブに対し許可された操作のみインターフェースを提供する。

・利用者が HCD へ一般利用者ログインし、コピー機能もしくはスキャン機能を選択すると、HCD は許可された操作のみインターフェースを提供する。

・利用者が HCD へ管理者ログインし、プリント機能もしくはボックス機能を選択すると、HCD は全利用者が所有するジョブの一覧を表示する。その後、ジョブが選択されると、HCD は当該ジョブに対し許可された操作のみインターフェースを提供する。

・利用者が HCD へ管理者ログインし、コピー機能もしくはスキャン機能を選択すると、HCD は許可された操作のみインターフェースを提供する。

・HCD が許可する操作を表 34 に示す。

表 34　HCD が許可する操作（D.USER.JOB）

Print		
操作	利用者	HCD が許可する操作
Create	Job owner	クライアント PC にインストールしたプリンタードライバーで、出力方法［プリント］

	U.ADMIN U.NORMAL Unauthenticated	もしくは［プリント＆ボックス］を選択して文書を送信する。 （プリンタードライバーから送信されたプリントジョブは、利用者識別のための情報を持っている。）
	Job owner	操作パネルもしくはRISO Console画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴）］タブで文書を選択して、印刷を実行する。
		RISO Console画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、［詳細確認］を選択し、印刷を実行する。
		RISO Console画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、印刷を実行する。
Read	Job owner	操作パネルのホーム画面もしくはRISO Console画面で［プリント］を選択し、プリント画面を表示する。
		操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブを表示する。
		操作パネルもしくはRISO Console画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴）］タブを表示する。
	U.ADMIN	操作パネルのホーム画面もしくはRISO Console画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［終了（履歴）］タブを表示する。
		操作パネルのホーム画面もしくはRISO Console画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［保留ジョブ］タブを表示する。
	U.NORMAL	なし（Job owner及びU.ADMINのみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	Job owner	プリント途中で、操作パネルのストップキーを押して一時停止し、設定変更を実行する。
		操作パネルのホーム画面で［プリント］を選択し、プリント画面で文書を選択して、設定変更を実行する。
	U.ADMIN	なし（Job ownerのみに操作を制限している）
	U.NORMAL	なし（Job ownerのみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Delete	Job owner	プリント途中で、操作パネルのストップキーを押して一時停止し、ジョブを取り消す。
		操作パネルのホーム画面もしくはRISO Console画面で［プリント］を選択し、プリント画面で文書を選択して、ジョブを取り消す。
		RISO Console画面で［プリント］を選択し、プリント画面で文書を選択して、［詳細表示］を選択し、ジョブを取り消す。
		操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブで文書を選択して、ジョブを取り消す。
	U.ADMIN	操作パネルのホーム画面もしくはRISO Console画面で［管理者メニュー］を選択し、ジョブ/文書管理画面の［保留ジョブ］タブで文書を選択して、ジョブを取り消す。

		操作パネルのホーム画面もしくは RISO Console 画面で[管理者メニュー]を選択し、［ユーザー設定］でユーザーを選択して、削除を実行する。
		操作パネルのホーム画面で［管理者メニュー］を選択し、［管理者設定初期化］で全ユーザーの削除を実行する。
		操作パネルのホーム画面もしくは RISO Console 画面で[管理者メニュー]を選択し、［認証サーバー設定］の［OFF］［ON］を切り替える。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Scan		
操作	利用者	HCD が許可する操作
Create	Job owner	操作パネルのホーム画面で［スキャン］を選択し、スキャン画面でスキャンを実行する。
	U.ADMIN	
	U.NORMAL	
	Job owner	操作パネルのホーム画面で［スキャン］を選択し、スキャン画面で送信プレビューを実行し、送信プレビュー画面でスキャンを実行する。
	U.ADMIN	
	U.NORMAL	
	Unauthenticated	なし（ログインできないので操作できない）
Read	Job owner	操作パネルのホーム画面もしくは RISO Console 画面で［スキャン］を選択し、スキャン画面を表示する。
		操作パネルのホーム画面で［スキャン］を選択し、スキャン画面で送信プレビューを実行する。
		操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の[終了（履歴)］タブを表示する。
	U.ADMIN	操作パネルのホーム画面もしくは RISO Console 画面で[管理者メニュー]を選択し、ジョブ/文書管理画面の［終了（履歴)］タブを表示する。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	なし（操作インターフェースがない）	
Delete	Job owner	スキャン途中で、操作パネルのストップキーを押して、ジョブを取り消す。
		送信プレビュー実行後、操作パネルで取り消しを実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Copy		
操作	利用者	HCD が許可する操作
Create	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面でコピーを実行する。
	U.ADMIN	

	U.NORMAL	
	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面で試しコピーを実行し、試しコピー画面で印刷を実行する。
	U.ADMIN	
	U.NORMAL	
	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面でコピー実行後、ログイン状態を維持したまま追加コピーを実行する。
		操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面の［終了（履歴）］タブでコピージョブを選択して、印刷を実行する。
	Unauthenticated	なし（ログインできないので操作できない）
Read	Job owner	操作パネルのホーム画面で［コピー］を選択し、コピー画面を表示する。
		操作パネルでジョブ確認を選択し、ジョブ確認画面で［処理中/待機中］タブを表示する。
		操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面で［終了（履歴）］タブを表示する。
		操作パネルのホーム画面で［コピー］を選択し、コピー画面で試しコピー実行中に、ジョブ確認を選択する。
	U.ADMIN	操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面で［終了（履歴）］タブを表示する。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	Job owner	コピー途中で、操作パネルのストップキーを押して一時停止し、設定変更を実行する。
		操作パネルで試しコピー実行中に、設定変更を実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Delete	Job owner	コピーの印刷途中で、操作パネルのストップキーを押して一時停止し、ジョブを取り消す。
		スキャナーによるコピー文書の読み込み途中で、操作パネルのストップキーを押して、ジョブを取り消す。
		試しコピー実行後、操作パネルで取り消しを実行する。
		操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブで文書を選択して、ジョブを取り消す。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Storage / retrieval		
操作	利用者	HCD が許可する操作

Create	Job owner	保存： 操作パネルのホーム画面で［ボックス］－［保存］を選択し、ボックス保存画面で保存を実行する。
	U.ADMIN	
	U.NORMAL	
	Job owner	保存： クライアント PC にインストールしたプリンタードライバーで、出力方法［ボックス］もしくは［プリント＆ボックス］を選択して、文書を送信する。 （プリンタードライバーから送信されたボックスジョブ（保存）は、利用者識別のための情報を持っている。）
	U.ADMIN	
	U.NORMAL	
	Unauthenticated	
	Job owner	取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、印刷を実行する。
		取り出し： RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、［詳細表示］を選択し、印刷を実行する。
		取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、印刷を実行する。
		取り出し： RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で検索を実行し、検索結果画面で文書を選択して、［詳細確認］を選択し、印刷を実行する。
Read	Job owner	保存： 操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面で［終了（履歴）］タブを表示する。
		取り出し： 操作パネルでジョブ確認を選択し、ジョブ確認画面で［処理中/待機中］タブを表示する。
		取り出し： 操作パネルもしくは RISO Console 画面でジョブ確認を選択し、ジョブ確認画面で［終了（履歴）］タブを表示する。
	U.ADMIN	保存／取り出し： 操作パネルのホーム画面もしくは RISO Console 画面で［管理者メニュー］を選択し、ジョブ/文書管理画面で［終了（履歴）］タブを表示する。
	U.NORMAL	なし（Job owner 及び U.ADMIN のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Modify	Job owner	保存／取り出し： 操作パネルのホーム画面で［ボックス］－［利用］を選択し、ボックス利用画面で文

		書を選択して、設定変更を実行する。
		保存／取り出し： RISO Console 画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、［詳細表示］を選択し、設定変更を実行する。
		取り出し： 印刷途中で、操作パネルでストップキーを押して一時停止し、設定変更を実行する。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）
Delete	Job owner	保存： 操作パネルのホーム画面で［ボックス］－［保存］を選択し、スキャナーによる読み込み途中で、操作パネルでストップキーを押して、ジョブを取り消す。
		保存： 保存プレビュー実行後、操作パネルで取り消しを実行する。
		取り出し： 操作パネルのホーム画面で［ボックス］－［利用］を選択し、ボックス利用画面で文書を選択して、印刷途中に、操作パネルでストップキーを押して一時停止し、ジョブを取り消す。
		取り出し： 操作パネルでジョブ確認を選択し、ジョブ確認画面の［処理中/待機中］タブで文書を選択して、ジョブを取り消す。
	U.ADMIN	なし（Job owner のみに操作を制限している）
	U.NORMAL	なし（Job owner のみに操作を制限している）
	Unauthenticated	なし（ログインできないので操作できない）

FMT_MSA.3

・ジョブ生成時に、各ジョブへ設定されるセキュリティ属性のデフォルト値を表 35 に記載された通りに実施する。操作は FDP_ACC.1、FDP_ACF.1 を参照。セキュリティ属性のデフォルト値は変更できない。

表 35　利用者データアクセス制御 SFP のセキュリティ属性の初期化

ジョブ	セキュリティ属性	デフォルト値
プリントジョブ	ユーザー名	プリントジョブとして生成されたジョブに含まれているオーナー名と同じパソコンログイン ID が紐付いている利用者のユーザー名
		プリントジョブ生成時にリモートログインしている利用者のユーザー名

スキャンジョブ	ユーザー名	スキャンジョブ生成時にローカルログインしている利用者のユーザー名
コピージョブ	ユーザー名	コピージョブ生成時にローカルログインしている利用者のユーザー名
ボックスジョブ（保存）	ユーザー名	ボックスジョブ生成時にローカルログインしている利用者のユーザー名
		ボックスジョブとして生成されたジョブに含まれているオーナー名と同じパソコンログイン ID が紐付いている利用者のユーザー名
ボックスジョブ（取り出し）	ユーザー名	ボックスジョブ生成時にローカルログインしている利用者のユーザー名
		ボックスジョブ生成時にリモートログインしている利用者のユーザー名

・文書データには、ログインしている利用者のユーザー名もしくはパソコンログイン ID が紐付いている利用者のユーザー名が、文書データ作成時にデフォルト値として付与される。セキュリティ属性のデフォルト値は変更できない。

7.3. 保存データの暗号化

HCD が持つ不揮発性ストレージへ保存されたデータを保護するため、データを暗号化する。
対応する SFR の実現方法を以下に示す。

FDP_DSK_EXT.1、FCS_COP.1(d)、FCS_COP.1(f)、FCS_KYC_EXT.1、FCS_CKM.1(b)

・利用者文書データ及び秘密の TSF データを不揮発性ストレージデバイスに保存する際に暗号化する。TOE 設置手続き時に暗号化が有効になる。
・暗号化した利用者文書データ及び秘密の TSF データは、特定の領域（パーティション）に保存する。それ以外のパーティションやブートローダーの領域には、暗号化したデータは保存しない。スワップ領域は無い。

・鍵暗号鍵は、NIST SP 800-90A に従い、Hash_DRBG (SHA256)を使用するランダムビット生成器で生成したランダムビットを使用して、暗号鍵長 128 ビットで生成する。（FCS_CKM.1(b)）
・鍵暗号鍵は、TOE 設置手続き時に生成し、不揮発性メモリーに保存する。また、電源投入時に不揮発性メモリーから読み出し、揮発性メモリーに一時保存する。

・ファイル暗号鍵は、NIST SP 800-90A に従い、Hash_DRBG (SHA256)を使用するランダムビット生成器で生成したランダムビットを使用して、暗号鍵長 128 ビットで生成する。（FCS_CKM.1(b)）

・ファイル暗号鍵は、TOE 設置手続き時に生成し、鍵暗号鍵で暗号化して不揮発性ストレージデバイスに保存する。また、電源投入時に不揮発性ストレージデバイスから読み出し、鍵暗号鍵で復号して揮発性メモリーに一時保存する。
・ファイル暗号鍵は、暗号鍵長 128 ビットで生成し、暗号鍵長 128 ビットの鍵暗号鍵を使用して暗号化及び復号されるので、強度 128 ビットを維持できている。
・ファイル暗号鍵の暗号化及び復号は、暗号鍵長 128 ビットの鍵暗号鍵を使用し、CBC モード（ISO/IEC10116 で規定）を使用した暗号アルゴリズム AES（ISO/IEC 18033-3 で規定）で実施する。（FCS_COP.1(f)）

・データの暗号化及び復号は、暗号鍵長 128 ビットのファイル暗号鍵を使用し、CBC モード（ISO/IEC10116 で規定）を使用した暗号アルゴリズム AES（ISO/IEC 18033-3 で規定）で実施する。（FCS_COP.1(d)）
・データの暗号化及び復号は、利用者の指示なしに自動的に実行する。利用者文書データは、作成され不揮発性ストレージデバイスに保存するタイミング、もしくはジョブ中に一時保存するタイミングで、文書単位で暗号化及び復号する。秘密の TSF データは、入力され不揮発性ストレージデバイスに保存するタイミングで、データ単位で暗号化及び復号する。操作は FMT_SMF.1 及び FDP_ACC.1、FDP_ACF.1 を参照。

FPT_KYP_EXT.1

・鍵暗号鍵は不揮発性メモリー（基板に半田付けされている部品）に保存するが、不揮発性ストレージデバイスに保存しない。
・ファイル暗号鍵は、TOE 設置手続き時に生成され不揮発性ストレージデバイスに保存されるが、保存する際に鍵暗号鍵で暗号化することで保護する。

FCS_CKM.4、FCS_CKM_EXT.4

・鍵暗号鍵とファイル暗号鍵は不要となった時に破棄する。

・不揮発性メモリーに保存した平文の鍵暗号鍵は、TOE 廃棄手続き時や使用済み TOE の回収依頼時や他所への移設時に不要となる。
・不揮発性メモリーの鍵暗号鍵の保存領域を、NIST SP 800-90A に従い、Hash_DRBG (SHA256)を使用するランダムビット生成器で生成したランダムパターンで 1 回上書きすることで破棄する。操作は、操作パネルから［HDD 初期化］を実行。

・電源投入時に揮発性メモリーに一時保存した鍵暗号鍵は、電源遮断により不要となる。
・電源遮断による揮発によって破棄する。

・不揮発性ストレージデバイスに保存したファイル暗号鍵は、TOE 廃棄手続き時や使用済み TOE の回収依頼時や他所への移設時に不要となる。操作は、操作パネルから［HDD 初期化］を実行。

・電源投入時に揮発性メモリーに一時保存したファイル暗号鍵は、電源遮断により不要となる。
・電源遮断による揮発によって破棄する。

FPT_SKP_EXT.1

・対称鍵の読み出しを防止するための機能を提供する。

・ファイル暗号鍵の暗号化及び復号で使用する鍵暗号鍵は、不揮発性メモリーに保存、揮発性メモリーに一時保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。不揮発性メモリーは基板に半田付けされているので、現地交換できない。

・データ暗号化で使用するファイル暗号鍵は、不揮発性ストレージデバイスに保存、揮発性メモリーに一時保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。不揮発性ストレージデバイスに保存したファイル暗号鍵は鍵暗号鍵で暗号化されている。

FCS_RBG_EXT.1、FCS_COP.1(c)

・256 ビットのエントロピーを最小限持つために、ハードウェアによる 1 つのノイズ源から生成した 384 ビットのエントロピーを持つ乱数をランダムビット生成器にシードとして供給する。
・ランダムビットは、NIST SP 800-90A に従い、Hash_DRBG (SHA256)を使用して生成する。ハッシュアルゴリズムは ISO/IEC 10118-3:2004 に従い実施する。
・384 ビットのエントロピーは以下のように確保する。
ハードウェアによるノイズ源として、Intel Atom®プロセッサ x7-E3950 が内蔵する Intel® Secure Key のハードウェア乱数発生器を使用する。
[Rambus DRNG]の 4.2 節の記述から、最小エントロピー率は 50%より大きいものと推定できるので、エントロピー源における最小エントロピー率は 50%とする。
[Intel DRNG]の 4.2.5 節に従い、10 マイクロ秒以上の間隔で 32 回の RDRAND 命令を実行するという方法で、新たなエントロピーを含む 32 ビット乱数を得る。この方法でエントロピー源の最小エントロピー率が減少することはないので、この 32 ビット乱数には少なくとも 16 ビットのエントロピーが含まれている。
上記を 24 回繰り返すことで 768 ビット乱数を得る。この 768 ビット乱数には少なくとも 384 ビットのエントロピーが含まれる。
・鍵暗号鍵の生成（FCS_CKM.1(b)）と、鍵材料と鍵の破棄（FCS_CKM_EXT.4、FCS_CKM.4）で使用する。

7.4. 通信の保護

TOE と内部ネットワーク（LAN）に接続された機器間の通信を高信頼なものとし、送信元/宛先のなりすまし、及び通信内容の改変から保護する。

対応する SFR の実現方法を以下に示す。

FTP_ITC.1

・HCD と接続されるサーバーには、監査サーバー、認証サーバー、SMB サーバー、FTP サーバー、メールサーバーがある。サーバーとの通信データ保護と通信データの改変を検知するために、IPsec 通信を使用する。各サーバーで使用するプロトコルを表 36 に示す。

表 36　HCD と各サーバーとの通信詳細

通信先	アプリケーションプロトコル
監査サーバー	Syslog
認証サーバー	LDAP
	Kerberos
SMB サーバー	SMB
FTP サーバー	FTP
メールサーバー	SMTP

・各サーバーとの通信を表 29　通信を開始できるサービスに記載のサービスにより開始する。操作は以下。

監査サーバー

- 表 44　監査対象事象の発生タイミングを参照。

認証サーバー

- 外部認証を設定した状態で、ローカルログインもしくはリモートログインを実行。操作は「7.1.識別認証及び権限付与」を参照。

SMB サーバー

- 操作パネルのホーム画面で［スキャン］－［PC］を選択し、スキャン画面でスキャンを実行。

FTP サーバー

- 操作パネルのホーム画面で［スキャン］－［PC］を選択し、スキャン画面でスキャンを実行。

メールサーバー

- 操作パネルのホーム画面で［スキャン］－［メール］を選択し、スキャン画面でスキャンを実行。

FTP_TRP.1(a)、FTP_TRP.1(b)

・HCD とリモート利用者の通信詳細を表 37 に示す。通信データ保護と通信データの改変を検知するために、IPsec 通信を使用する。

表 37　HCD と各利用者との通信詳細

リモート利用者	操作手段
管理者、 一般利用者	RISO Console
一般利用者	プリンタードライバー

・リモート利用者による通信をリモート操作により開始する。操作は以下。

RISO Console

- クライアント PC のブラウザで RISO Console 画面を表示。
- クライアント PC のブラウザ上で RISO Console 画面を操作。

プリンタードライバー

- クライアント PC にインストールしたプリンタードライバーから文書を送信。

FIA_PSK_EXT.1

・IPsec 通信では事前共有鍵を使用できる。事前共有鍵を設定する操作は以下。

- 操作パネルもしくは RISO Console 画面の［管理者メニュー］の［IPsec 設定］の［セキュリティポリシー設定］で、事前共有キーの［使用する］を選択し、［事前共有キー］を入力。

・IPsec 通信の事前共有鍵に、以下のようなテキストベースの事前共有鍵のみを許容する。

長さ：22～32 文字

文字組み合わせ：アルファベットの大文字と小文字、数字、及び特殊文字を使用できる。表 38 に使用できる特殊文字の一覧を示す。

表 38　IPsec の事前共有鍵で使用できる特殊文字

特殊文字	Unicode スカラ値	名称
!	U+0021	EXCLAMATION MARK
@	U+0040	COMMERCIAL AT
#	U+0023	NUMBER SIGN
$	U+0024	DOLLAR SIGN
%	U+0025	PERCENT SIGN
^	U+005E	CIRCUMFLEX ACCENT
&	U+0026	AMPERSAND
*	U+002A	ASTERISK
(	U+0028	LEFT PARENTHESIS
)	U+0029	RIGHT PARENTHESIS
	U+0020	SPACE
-	U+002D	HYPHEN-MINUS
.	U+002E	FULL STOP

_	U+005F	LOW LINE
~	U+007E	TILDE
{	U+007B	LEFT CURLY BRACKET
}	U+007D	RIGHT CURLY BRACKET
`	U+0060	GRAVE ACCENT

・事前共有鍵は、ファイル暗号鍵で暗号化して不揮発性ストレージデバイスに保存する。また、電源投入時に不揮発性ストレージデバイスから読み出し、ファイル暗号鍵で復号して揮発性メモリーに一時保存する。
・IPsec 通信の IKE のフェーズ 1 で、SHA-256／SHA-512／SHA-384 を使用して事前共有鍵をハッシュ化する。

FCS_IPSEC_EXT.1、FCS_COP.1(g)、FCS_COP.1(c)、FCS_COP.1(b)、FCS_COP.1(a)、FCS_CKM.1(a)、FCS_CKM.1(b)、FCS_RBG_EXT.1

・IPsec 通信では事前共有鍵の他に証明書も使用できる。証明書の使用を設定する操作は以下。
  - 操作パネルもしくは RISO Console 画面の［管理者メニュー］の［IPsec 設定］の［セキュリティポリシー設定］で、証明書の［使用する］を選択。
・IPsec 通信の RSA 秘密鍵と CSR を生成する操作は以下。
  - 操作パネルの［管理者メニュー］の［証明書関連ファイル管理］の［鍵と CSR の作成］を実行。
・CSR をエクスポートする操作は以下。
  - 操作パネルの操作パネルもしくは RISO Console 画面の［管理者メニュー］の［保守操作許可切替］で ON を選択し、所定のフォルダーを作成した USB メモリーを HCD に接続して、再起動する。
・IPsec 証明書とルート CA 証明書をインポートする操作は以下。
  - 操作パネルもしくは RISO Console 画面の［管理者メニュー］の［保守操作許可切替］で ON を選択し、所定のフォルダーを作成した USB メモリーを HCD に接続して、再起動する。
・IPsec 通信の RSA 秘密鍵は、FCS_RBG_EXT.1 で指定されたランダムビット生成器で生成したランダムビットを使用して、FCS_CKM.1(a)の NIST Special Publication 800-56B, Revision 2 の 6.3.1.2 章に記載の rsakpg1-prime-factor 方式に従って生成する。生成する鍵の鍵強度は 112 ビットである。
・IPsec 通信の RSA 秘密鍵は、ファイル暗号鍵で暗号化して不揮発性ストレージデバイスに保存する。また、電源投入時に不揮発性ストレージデバイスから読み出し、ファイル暗号鍵で復号して揮発性メモリーに一時保存する。
・CSR は不揮発性ストレージデバイスに保存する。エクスポート時に不揮発性ストレージデバイスから読み出す。
・IPsec 証明書とルート CA 証明書は不揮発性ストレージデバイスに保存する。証明書を使用した IPsec 通信開始時に不揮発性ストレージデバイスから読み出す。

・IPsec 通信の IPsec アーキテクチャを RFC4301 で定義された通りに実施する。
・IPsec 通信をトランスポートモードで実施する。

・IPsec 設定のセキュリティポリシーは 10 個まで設定でき、優先順位も設定できる。セキュリティポリシーはパケットの保護についての規則を設定でき、廃棄及びバイパスについての規則は設定できない。送受信するパケットに対して、セキュリティポリシーの優先順位に従って保護もしくは破棄を行う。セキュリティポリシーが一致する場合は、パケットを保護する。一致するものがない場合は、パケットを破棄する。各セキュリティポリシーには、通信を許可する IP アドレスを設定できる。IP アドレスが一致しない場合も、送受信するパケットを破棄する。

・IPsec 通信の IPsec プロトコル ESP を RFC4303 で定義された通りに実施する。鍵付ハッシュメッセージ認証を表 39 に従い実施する（FCS_COP.1(g)）。ハッシュアルゴリズムは ISO/IEC 10118-3:2004 に従い実施する。パケットの暗号化に AES-CBC-128（RFC 3602 で規定）もしくは AES-CBC-256（RFC 3602 で規定）を使用する。

表 39　鍵付ハッシュメッセージ認証

暗号アルゴリズム	詳細			
	メッセージダイジェスト長	鍵長	ハッシュアルゴリズム	仕様書
HMAC	160／256／384／512 ビット	160／256／384／512 ビット	SHA-1／SHA-256／SHA-384／SHA-512	FIPS Pub 198-1「The Keyed-Hash Message Authentication Code」、FIPS Pub 180-3「Secure Hash Standard」

・IPsec 通信の IKEv1 プロトコルを RFC 2407、2408、2409、 RFC 4109 で定義された通りに実施する。ハッシュアルゴリズムは RFC4868 で定義された通りに、ISO/IEC 10118-3:2004 に従い実施する。

・IPsec 通信の IKEv1 のデータ暗号化を、RFC3602 で定義された暗号化アルゴリズム AES-CBC-128、AES-CBC-256 を使用して実施する。

・IPsec 通信の IKEv1 フェーズ 1 の鍵交換を FCS_COP.1(c)に含まれる SHA256、SHA384、SHA512 に従ったハッシュアルゴリズムを使用して、メインモードでのみ実施する。

・IPsec 通信の SA ライフタイム時間（確立）をフェーズ 1 では 24 時間固定、フェーズ 2 では 8 時間以内に制限する。

・IPsec 通信の鍵交換で使用する非対称鍵を、FCS_RBG_EXT.1 で指定されたランダムビット生成器で生成したランダムビットを使用し、NIST SP 800-56A Revision 3 の Appendix D Table 25 に記載の DH グループ 14 で生成する。

・IPsec 通信の IKE のフェーズ 1 で生成する非対称鍵は、対称鍵強度で 112bits 以上の強度がある。生成した非対称鍵は揮発性メモリーに保存する。

・IPsec 通信の IKE プロトコルは DH グループ 14（2048 ビット MODP）と FCS_COP.1(c)に含まれる SHA256、SHA384、SHA512 に従ったハッシュアルゴリズムを使用した PRF 関数を使用して、鍵交換及び鍵確立を実施する。

・IPsec 通信の IKE プロトコルは、FCS_COP.1(c)に含まれる SHA256、SHA384、SHA512 に従ったハッ

シュアルゴリズムを使用した PRF 関数と、暗号署名サービスまたは事前共有鍵を使用して、ピア認証を実施する。

・IPsec 通信の暗号署名サービス（鍵長 2048 ビットの FCS_COP.1(c)に含まれる SHA256 を使用した RSA デジタル署名アルゴリズム（rDSA））を、FIPS PUB 186-4 Digital Signature Standard で定義された通りに実施する。（FCS_COP.1(b)）

・IPsec 通信のデータの暗号化及び復号を表 40 に従い実施する。（FCS_COP.1(a)）

表 40　通信データの暗号化と復号

暗号アルゴリズム	詳細		
	暗号鍵長	モード	仕様書
AES	128 ビット及び 256 ビット	CBC モード	FIPS PUB 197「Advanced Encryption Standard (AES)」、NIST SP 800-38A

・IPsec 通信のデータ暗号化で使用する対称鍵（FCS_CKM.1(b)）は、FCS_RBG_EXT.1 で指定されたランダムビット生成器で生成したランダムビットを使用して、暗号鍵長 128 ビットまたは 256 ビットで生成する。

・IPsec 通信の ISAKMP SA 用の暗号鍵は、IKE のフェーズ 1 で生成し、揮発性メモリーに保存する。

・IPsec 通信の IPsec SA 用の暗号鍵は、IKE のフェーズ 2 で生成し、揮発性メモリーに保存する。

・FCS_CKM.1(a)に従う非対称鍵の生成に関して、上記した以外の許可された実装はない。

FCS_CKM.4、FCS_CKM_EXT.4

・通信で使用する暗号鍵は不要となった時に破棄する。

・不揮発性ストレージデバイスに保存した事前共有鍵は以下のタイミングで不要となる。

- TOE 廃棄手続き時や使用済み TOE の回収依頼時や他所への移設時（操作は、操作パネルから［HDD 初期化］を実行。）

・揮発性メモリーに一時保存した事前共有鍵は、電源遮断により不要となる。

・電源遮断による揮発によって破棄する。

・不揮発性ストレージデバイスに保存した RSA 秘密鍵は以下のタイミングで不要となる。

- TOE 廃棄手続き時や使用済み TOE の回収依頼時や他所への移設時（操作は、操作パネルから［HDD 初期化］を実行。）

・揮発性メモリーに一時保存した RSA 秘密鍵は、電源遮断により不要となる。

・電源遮断による揮発によって破棄する。

・揮発性メモリーに保存した IPsec 通信の鍵交換で使用する非対称鍵は以下のタイミングで、同じ鍵が使用

されることがなくなるので、不要となる。
  - 電源遮断
・電源遮断による揮発によって破棄する。

・揮発性メモリーに保存した IPsec 通信の ISAKMP SA 用の暗号鍵は以下のタイミングで、同じ鍵が使用されることがなくなるので、不要となる。
  - 電源遮断
・電源遮断による揮発によって破棄する。

・揮発性メモリーに保存した IPsec 通信の IPsec SA 用の暗号鍵は以下のタイミングで、同じ鍵が使用されることがなくなるので、不要となる。
  - 電源遮断
・電源遮断による揮発によって破棄する。

FPT_SKP_EXT.1

・事前共有鍵、対称鍵、非対称鍵の読み出しを防止するための機能を提供する。

・IPsec 通信で使用する事前共有鍵は、操作パネルもしくは RISO Console 画面の［管理者メニュー］の［IPsec 設定］の［セキュリティポリシー設定］で入力する。読み出しを防止するために、事前共有鍵が確定された後は「＊＊＊＊＊（5 個のアスタリスク）」で表示する。事前共有鍵は不揮発性ストレージデバイスに保存、揮発性メモリーに一時保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。不揮発性ストレージデバイスに保存した事前共有鍵はファイル暗号鍵で暗号化されている。揮発性メモリーに一時保存した事前共有鍵は電源遮断による揮発によって破棄される。

・IPsec 通信で使用する RSA 秘密鍵は、不揮発性ストレージデバイスに保存、揮発性メモリーに一時保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。不揮発性ストレージデバイスに保存した RSA 秘密鍵はファイル暗号鍵で暗号化されている。揮発性メモリーに一時保存した RSA 秘密鍵は電源遮断による揮発によって破棄される。

・IPsec 通信の鍵交換で使用する非対称鍵は、揮発性メモリーに保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。揮発性メモリーに一時保存した非対称鍵は電源遮断による揮発によって破棄される。

・IPsec 通信のデータ暗号で使用する対称鍵は、揮発性メモリーに保存するが、読み出すための機能を管理者にも一般利用者にも提供しないことにより、読み出しを防止する。揮発性メモリーに一時保存した対称鍵は電源遮断による揮発によって破棄される。

7.5. セキュリティ機能の管理

管理者として認証成功した利用者が、管理者の役割としてセキュリティ管理機能を実行する。
対応する SFR の実現方法を以下に示す。

FMT_MOF.1

・管理者は表 24　セキュリティ機能のリストに記載したふるまいに関連する管理機能の改変を実行できる。
・表 24　セキュリティ機能のリストは、「管理者メニュー」に表示する。
・操作は以下。
- 操作パネルもしくは RISO Console 画面の［管理者メニュー］の［認証サーバー設定］で認証サーバーの［OFF］［ON］を切り替える。

FMT_SMF.1

・管理者は表 27　管理機能に記載された通りに管理機能を実行できる。「管理者メニュー」にのみ表示することで実行を管理者のみに制限する。
・表 27　管理機能に記載された機能で、管理者に許可された機能は、「管理者メニュー」に表示する。
・表 27　管理機能に記載された機能の操作を表 41 に示す。操作パネルと RISO Console 画面の両方で操作できない管理機能は、操作に操作場所を記載する。

表 41　管理機能の操作

管理機能	役割	操作
認証サーバー設定	管理者	［管理者メニュー］の［認証サーバー設定］で認証サーバーの［OFF］［ON］を切り替える。 ［管理者メニュー］の［認証サーバー設定］で認証サーバーの接続設定を入力して、確定する。
ユーザー設定	管理者	［管理者メニュー］の［ユーザー設定］－［追加］または［編集］でユーザー設定（内部認証時のユーザー名・役割（一般利用者／管理者）・基本機能の使用許可設定（各基本機能の使用許可／不許可をユーザーごとに切り替え）・パソコンログイン ID・ログインパスワード）を入力して、確定する。 ［管理者メニュー］の［ユーザー設定］－［削除］でユーザー名を選択して、確定する。　※1
パスワード変更	所有する一	［システム情報］の［ユーザー情報］の［パスワード変

	般利用者	更］でパスワードを入力して、確定する。
セキュリティパスワード変更	管理者	［管理者メニュー］の［セキュリティパスワード変更］でセキュリティパスワードを入力して、確定する。
日時設定	管理者	［管理者メニュー］の［日時設定］で日時を入力して、確定する。
監査サーバー設定	管理者	［管理者メニュー］の［監査サーバー設定］で監査サーバーの接続設定を入力して、確定する。
ネットワーク設定	管理者	［管理者メニュー］の［ネットワーク設定（IPv4）］でネットワークの接続設定を入力して、確定する。 ［管理者メニュー］の［ネットワーク設定（IPv6）］でネットワークの接続設定を入力して、確定する。
IP アドレス制限設定	管理者	［管理者メニュー］の［IP アドレス制限設定（IPv4）］で IP アドレスの制限設定を入力して、確定する。 ［管理者メニュー］の［IP アドレス制限設定（IPv6）］で IP アドレスの制限設定を入力して、確定する。
IPsec 設定	管理者	［管理者メニュー］の［IPsec 設定］で IPsec の設定（証明書の設定を含む）を入力して、確定する。
メール送信設定	管理者	［管理者メニュー］の［メール送信設定］でメールサーバーの接続設定を入力して、確定する。
最小パスワード長設定	管理者	［管理者メニュー］の［最小パスワード長］で最小パスワード長を入力して、確定する。
ログイン設定	管理者	［管理者メニュー］の［ログイン設定］で自動ログアウト時間とログイン失敗制限回数を入力して、確定する。
証明書関連ファイル管理	管理者	［管理者メニュー］の［証明書関連ファイル管理］で証明書を選択して、［作成］／［有効化］／［削除］を選択する。
保守操作許可切替	管理者	［管理者メニュー］の［保守操作許可切替］で OFF／ON を選択して、確定する。 電源投入（自動的に OFF が設定される　※2）。
ファームウェアのアップデート	管理者	操作パネルで操作。「7.7. 自己テスト及びファームウェアの検証」を参照。

※1 ［管理者メニュー］の［ユーザー設定］でも操作が可能。操作は以下。

- RISO Console 画面で［管理者メニュー］の［ユーザー設定］からユーザー設定のインポートを実行する。

※2 電源投入後、証明書インストールまたはファームウェアアップデートが実行される場合は、その処理が終了した時に、自動的に OFF が設定される。

FMT_MSA.1

・各セキュリティ属性に対する操作を、利用者の役割に応じて、表 25　利用者セキュリティ属性の管理に記載された通りに制限する。

・管理者は表 25　利用者セキュリティ属性の管理に記載の「ユーザー名」を問い合わせ／新規作成／削除／改変できる。操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、［追加］／［削除］／［編集］を選択。

・管理者は表 25　利用者セキュリティ属性の管理に記載の「役割」を問い合わせ／改変できる。操作は以下。

- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［ユーザー設定］を選択して、［管理者権限］の［OFF／ON］を選択。

・一般利用者は表 25　利用者セキュリティ属性の管理に記載の「ユーザー名」を問い合わせできる。操作は以下。

- 操作パネルの［ログイン／ログアウト］キーを押す。

FMT_MTD.1

・各 TSF データに対する操作を、利用者の役割に応じて、表 26　Management of TSF Data に記載した通りに制限する。管理者にのみ許可された操作は、操作パネルもしくは RISO Console 画面の「管理者メニュー」にのみ表示することで制限する。操作は FMT_SMF.1 を参照。

・所有する一般利用者にのみ許可された操作は、ログインパスワードの改変のみで、所有する一般利用者がログインしているときにのみ表示することで制限する。ログインパスワードを改変する操作は以下。

- 操作パネルもしくは RISO Console 画面でシステム情報の［ユーザー情報］を選択して、［パスワード変更］を実行。

7.6.　監査ログ機能

監査ログを生成し、生成した監査ログを、高信頼チャネルを用いて監査サーバーに送信する。
対応する SFR の実現方法を以下に示す。

FAU_GEN.1、FAU_GEN.2

・表 42 に示す監査対象事象発生時に、表 42 及び表 43 に示す内容の監査ログを生成する。

表 42　監査対象事象に対する監査ログ内容

○：記録対象　×：記録対象外

監査対象事象	監査ログ内容									
	A	B	C	D	E	F	G	H	I	J
監査機能の起動	○	○	○	○	×	○	×	×	×	×
監査機能の終了	○	○	○	○	×	○	×	×	×	×
ジョブの終了	○	○	○	○	○	○	○	×	×	×
利用者認証失敗	○	○	○	○	○	○	×	×	×	×
利用者識別失敗	○	○	○	○	○	○	×	×	×	×
管理機能(※1)の利用 ※1 表 27　管理機能に記載の機能	○	○	○	○	○	○	×	×	○	○
IPsec SA 確立の失敗	○	○	○	○	×	○	×	○ ※2	×	×
役割の一部である利用者グループの改変	○	○	○	○	○	○	×	×	×	×
時刻の変更	○	○	○	○	○	○	×	×	×	×
管理者認証失敗	○	○	○	○	○	○	×	×	×	×

※2 RFC2408 の Notify Message Types で定義の番号が出力される。

表 43　表 42 の記号と監査ログ内容の対応

記号	監査ログ内容
A	出力するログの文字コード
B	事象の日付及び時刻
C	プリンター識別情報
D	事象の種別（監査対象事象）
E	ユーザー名
F	事象の結果
G	ジョブ種別
H	失敗の理由
I	操作された管理機能
J	操作内容

・監査対象事象の発生タイミングを表 44 に示す。

表 44　監査対象事象の発生タイミング

監査対象事象	発生タイミング
監査機能の起動	電源投入／スリープ（消費電力が少ない）状態からの復帰
監査機能の終了	電源遮断／スリープ（消費電力が少ない）状態への移行
ジョブの終了	表 33　HCD が許可する操作（D.USER.DOC）と表 34　HCD が許可する操作（D.USER.JOB）の Delete に記載の操作（※）

	※ユーザー削除にともなう Delete は含まない（「管理機能の利用」が発生する）。
	プリントジョブ／コピージョブ／ボックスジョブ（取り出し）の印刷の終了
	スキャンジョブ／ボックスジョブ（保存）の文書データ保存の終了
	スキャンジョブの文書データ送信の終了
	スキャンした文書データのダウンロード
	プリントジョブ／スキャンジョブ／コピージョブ／ボックスジョブ（保存）／ボックスジョブ（取り出し）の終了ジョブ保存数が上限に達した状態で終了ジョブを保存
	スキャンジョブ保存数が上限に達した状態でスキャンジョブを保存
	プリントジョブの保留ジョブの保存期間超過
	プリントジョブ／スキャンジョブ／コピージョブ／ボックスジョブ（保存）／ボックスジョブ（取り出し）の終了ジョブの保存期間超過
	スキャンジョブの保存期間超過
	プリントジョブ／スキャンジョブ／コピージョブ／ボックスジョブ（保存）／ボックスジョブ（取り出し）実行中の電源遮断
	受信したプリントジョブ／ボックスジョブ（保存）のパソコンログイン ID が未登録
	非表示に設定された基本機能を使用するジョブを受信
	基本機能の使用禁止が設定されたユーザーの当該基本機能を使用するジョブを受信
	2 色プリントの使用禁止が設定されたユーザーの 2 色プリントするジョブを受信
	ボックスジョブ（保存）保存時にボックス保存文書数が上限に達している
	ボックスジョブ（保存）保存時に指定されたボックスにアクセスできない
	HCD 要因の途中終了（印刷失敗、スキャン失敗、保存失敗、送信失敗、等。）
利用者認証失敗	一般利用者ログイン実行時にログインパスワードが不一致
	ロック状態の利用者が一般利用者ログインを実行
	ローカルログイン中の一般利用者がリモートログインを実行
利用者識別失敗	ログイン実行時にユーザー名が未登録
	プリントジョブ／ボックスジョブ（保存）投入時にジョブに付随しているパソコンログイン ID と登録情報が不一致
管理機能（※）の利用	表 41　管理機能の操作を参照

※表 27　管理機能に記載の機能	
IPsec SA 確立の失敗	監査サーバー／認証サーバー／SMB サーバー／FTP サーバー／メールサーバー／クライアント PC との IPsec SA 確立に失敗
役割の一部である利用者グループの改変	［管理者メニュー］の［ユーザー設定］で管理者権限の設定を変更
時刻の変更	［管理者メニュー］の［日時設定］を設定
管理者認証失敗	管理者ログイン実行時にセキュリティパスワードが不一致
	ロック状態の、管理者になることができる一般利用者が、管理者ログインを実行

FAU_STG_EXT.1

・FAU_GEN.1、FAU_GEN.2 の操作で生成された監査ログを揮発性メモリーに一時保存し、監査サーバーへ送信する。一時保存するデータは暗号化しない。揮発性メモリーに対するインターフェースはない。
・監査サーバーへの監査ログの送信が成功したら、送信された監査ログを削除する。
・監査サーバーへの監査ログの送信が失敗したら、容量 20M バイトになるまで監査ログを一時保存する。新たな監査ログを一時保存しようとしたときに、容量（20M バイト）が不足していた場合は、一時保存しようとしていた監査ログを削除する。
・揮発性メモリーに一時保存した監査ログを、以下の何れかの条件で再送信する。
- FAU_GEN.1、FAU_GEN.2 の操作で新たな監査ログが生成されたときに、一時保存した全ての監査ログと新たに生成された監査ログを監査サーバーへ再送信。
- 一時保存した監査ログが存在する状態で、新たな監査対象事象が発生せずに 5 秒経過したときに、一時保存した全ての監査ログを監査サーバーへ再送信。
・再送信が成功した監査ログは、HCD 内から消去する。
・一時保存した監査ログは電源遮断による揮発によって破棄される。
・監査サーバーへの監査ログの送信が失敗した後で、設定された時間が経過する度に、送信失敗したログがあるかどうかを確認し、送信失敗したログがあれば、操作パネルにエラーメッセージを表示する。
・送信失敗したログがあるかどうかを確認する時間間隔は、「管理者メニュー」で［5～120］分の範囲で設定できる。操作は以下。
- 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［監査サーバー設定］を選択して、［ログ送信エラー通知間隔］を入力。
・「7.4.通信の保護」に記載した通信を使用して、監査サーバーと通信する。
・監査サーバーと通信を開始するタイミングは以下。
- 監査ログを生成。
- 一時保存した監査ログが存在する状態で、新たな監査対象事象が発生せずに 5 秒経過。

FPT_STM.1

・日付と時刻は TOE のシステム時計から取得する。
・TOE のシステム時計は、管理者が変更できる。操作は以下。
  - 操作パネルもしくは RISO Console 画面で［管理者メニュー］の［日時設定］を設定。
・表 43　表 42 の記号と監査ログ内容の対応の B（事象の日付及び時刻）に使用する。

7.7.　自己テスト及びファームウェアの検証

不正なファームウェアにアップデートされるのを防ぐ。自己テストを実施し、TSF が正常動作することを検証する。

対応する SFR の実現方法を以下に示す。

FPT_TUD_EXT.1、FCS_COP.1(b)、FCS_COP.1(c)

・HCD にインストールされているファームウェアのバージョンは、利用者が操作パネル及び RISO Console から確認できる。操作は以下
  - 操作パネルもしくは RISO Console 画面で［機種情報］を表示。
  - 操作パネルもしくは RISO Console 画面で［機種情報］の［システム情報プリント］を実行。
・TOE のファームウェアのアップデートは管理者が実施する。操作は以下
  - 操作パネルの［管理者メニュー］の［保守操作許可切替］で ON を選択し、ファームウェアを保存した USB メモリーを HCD に接続して、再起動する。
・ファームウェアをアップデートする前に、デジタル署名メカニズムを用いて、ファームウェアの完全性を検証する。完全性が検証できた場合のみ、インストールを開始する。
・ファームウェアの完全性の検証は、FIPS PUB 186-4 Digital Signature Standard に従った鍵長 2048 ビットの RSA デジタル署名アルゴリズム(rDSA)を ISO/IEC 10118-3:2004 に従った SHA-256 と組み合わせた、暗号署名サービスで実施する。（FCS_COP.1(b)）（FCS_COP.1(c)）
・管理者が操作パネルからファームウェアのアップデートを開始したときに、デジタル署名メカニズムを起動する。
・完全性が検証できなかった場合は、操作パネルにエラーメッセージを表示して、ファームウェアのアップデートを中止する。

FPT_TST_EXT.1、FCS_COP.1(c)

・TSF はコントロール基板ファームウェアとエントロピー源と DRBG で実現する。
・TOE 起動時にコントロール基板ファームウェアとエントロピー源と DRBG の自己テストを実施する。TSF を実現する全てのものについて自己テストを実施するので、TSF 全体の検証になっており、正常動作の検証として十分である。

・コントロール基板ファームウェアに毀損が無いことを保証するために、電源投入時に FCS_COP.1(c)に含まれる SHA-256 を使用してハッシュ値を計算し、ファームウェア生成時に計算済みの値と比較する。
・エントロピー源が故障していないことを保証するために、[Intel DRNG]の 5.2 節の記述に従い、RDRAND 命令実行後に、CF をチェックすることで、出力が有効かどうか検査する。CF=1 であれば有効、CF=0 であれば有効でないと判断する。CF=0 の場合は、RDRAND 命令の実行をリトライし、10 回のリトライでも CF=1 とならない場合はエントロピー源の故障と判断する。
・DRBG に毀損が無いことを保証するために、Instantiate 機能と Generate 機能と Reseed 機能の既知解テストを NIST SP 800-90A に基づいて実施する。
・自己テストに失敗した場合は、操作パネルにエラーメッセージを表示して、電源遮断以外の操作を受け付けない状態にする。
・自己テストを実施するタイミングは以下。
  - 電源投入

8. 付録

8.1. 参照文献

[Intel DRNG]
“Intel® Digital Random Number Generator (DRNG) Software Implementation Guide”,
Revision 2.1, October 17, 2018, Intel Corporation
https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide

[Rambus DRNG]
“Analysis of Intel's Ivy Bridge Digital Random Number Generator”,
March 2012, Cryptography Research a division of Rambus
http://www.rambus.com/wp-content/uploads/2015/08/Intel_TRNG_Report_20120312.pdf

8.2. 用語説明

表 45 用語説明

用語・略語	定義
パソコンログイン ID	利用者がプリントジョブを送信するパソコンにログインする際に使用している名称。パソコンログイン名称。
RISO Console	クライアント PC 上のブラウザから HCD へアクセスし、HCD の状態確認やジョブの削除などを行うための手段。
プリンタードライバー	HCD のプリント機能を使用する場合にクライアント PC から HCD へジョブを送信するために使用するソフトウェア。クライアント PC へインストールされる。
役割昇格	一般利用者が管理者の役割を持つ（一般利用者に一般利用者の役割の他に管理者の役割を追加する）こと。
役割降格	一般利用者が管理者の役割を失う（一般利用者から管理者の役割を削除する）こと。
不揮発性ストレージデバイス	コントロール基板に接続された HDD（Hard Disk Drive）。
不揮発性メモリー	操作パネルユニットの基板上の CPU 内蔵 Flash。操作パネルユニットの基板に半田付けされている。
揮発性メモリー	コントロール基板上の RAM（Random Access Memory）。

8.3. 図番号

8.4. 表番号