THE DOCUMENT COMPANY
FUJI XEROX

EP 通信集約サーバーソフトウエア
セキュリティーターゲット

バージョン：1.26

発効日：2008/11/14

作成者：富士ゼロックス株式会社

富士ゼロックス株式会社

更新履歴

NO	更新日	バージョン	更新内容
1	2008/02/15	1.0	評価版として新規作成
2	2008/03/19	1.01	レビュー結果を反映
3	2008/04/04	1.02	指摘事項を反映
4	2008/05/16	1.03	指摘事項を反映
5	2008/05/23	1.04	指摘事項を反映
6	2008/05/26	1.05	指摘事項を反映
7	2008/05/27	1.06	指摘事項を反映
8	2008/06/04	1.07	指摘事項を反映
9	2008/06/05	1.08	指摘事項を反映
10	2008/06/18	1.09	指摘事項を反映
11	2008/06/18	1.10	指摘事項を反映
12	2008/07/03	1.11	指摘事項を反映
13	2008/07/14	1.12	指摘事項を反映
14	2008/07/23	1.13	指摘事項を反映
15	2008/07/29	1.14	指摘事項を反映
16	2008/08/01	1.15	指摘事項を反映
17	2008/08/27	1.16	指摘事項を反映
18	2008/08/28	1.17	指摘事項を反映
19	2008/09/01	1.18	指摘事項を反映
20	2008/09/19	1.19	指摘事項を反映
21	2008/09/29	1.20	指摘事項を反映
22	2008/10/15	1.21	拡張セキュリティ機能要件 FTP_ICD を定義。
23	2008/10/16	1.22	指摘事項を反映
24	2008/10/20	1.23	指摘事項を反映
25	2008/10/24	1.24	指摘事項を反映
26	2008/10/31	1.25	指摘事項を反映
27	2008/11/14	1.26	指摘事項を反映

－ 目次 －

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、及び 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 EP 通信集約サーバーソフトウエア セキュリティーターゲット
バージョン 1.26
発行日 2008 年 11 月 14 日
作成者 富士ゼロックス株式会社

1.2. TOE 参照

本節では TOE の識別情報を記述する。

TOE EP 通信集約サーバーソフトウエア
バージョン 1.0.1
キーワード デジタル複合機、遠隔サービス、内部ネットワーク、外部ネットワーク、オフィス
開発者 富士ゼロックス株式会社

1.3. 略語

本 ST で使用する略語について説明する。

略語	説明
FX	富士ゼロックス株式会社
EP	Electronic Partnership
EP-BB	Electronic Partnership-Broad Band

1.4. 用語

本 ST で使用する用語について説明する。

用語	説明
複合機	複写機、プリンター、イメージスキャナ、ファクシミリなどの事務機器の機能を一つの筐体に収めた機器。
メーター値	複合機を使用して出力した印刷物のうち、情報が文字・画像として紙面に定着している面の数を測定した値。
EP サービス	FX の複合機を購入したお客様に対して提供する下記サービスの総称。 1) 事務サービス 定期的にメーター値を EP センターに送信することにより、お客様自身がメーター値を通知する手間をなくす。 2) 物流サービス 複合機の消耗品情報(Near Empty/Near Full など)を自動的に EP センターに送信することにより、お客様が消耗品の追加注文を連絡する手間をなくす。 3) 保守サービス 複合機の障害情報を EP センターに送信することにより、保守員の保守作業を支援する。

用語	説明
EP センター	EP サービスを提供するために、FX が管理運用しているセンター。インターネットを利用して、複合機から EP サービスのための情報を収集する。
Edge サーバー	外部から EP センターに送られてくる情報を受けるフロントエンドの役割をするサーバー。お客様のサイトに設置される TOE の通信先となる。
FX プロダクト認証局	FX が管理運用している認証局。インターネットを介して、TOE 及び EP-BB 機能搭載複合機に発行する、EP 証明書の管理運用を行う。
FX 認証局	FX が管理運用している認証局。FX プロダクト認証局の上位認証局。CA と呼ばれる場合もある。
EP-BB 機能	設置先の内部ネットワークから、外部ネットワーク経由で Edge サーバーと通信する機能。
EP-BB 機能搭載複合機	EP-BB 機能を搭載した複合機を EP-BB 機能搭載複合機と呼ぶ。TOE を中継して、Edge サーバーと通信することもできる。EP-BB 機能搭載複合機は TOE と SSL 通信する。 EP-BB 機能搭載複合機は、EP サービスの適用対象である。
EP 通信データ	EP サービスをお客様に提供するために、EP-BB 機能搭載複合機から、TOE を経由して Edge サーバーに送信されるデータのことである。
通信中継サーバー(PC)	TOE が稼動するための PC であり、内部ネットワークに接続されている。通信中継サーバー(PC)は管理者によって管理される。
管理保守クライアント(PC)	TOE の管理と保守を実施する際に使用される PC であり、内部ネットワークに接続されている。管理保守クライアント(PC)は管理者によって管理されている。
HTTPS	HTTPS は、Web サーバーとクライアントがデータを送受信する際に使用されるプロトコルである HTTP に、SSL ハンドシェイクによる認証機能、データの完全性保証機能、及びデータの暗号化機能を追加している。
SSL ハンドシェイク	Web サーバーとクライアントが、HTTPS でデータの送受信を開始する際に使用されるメッセージ交換の手順。公開鍵技術を使用して、クライアント側で Web サーバーの認証をする。また、必要な場合は、公開鍵技術を使用して、Web サーバー側でのクライアントの認証をすることもできる。
Edge サーバー証明書	Edge サーバーに格納され、TOE と SSL ハンドシェイクによる認証をする際に、TOE に送信される証明書である。
ルート証明書	証明書を発行する認証局が、その正当性を証明するために自ら署名して発行する証明書。TOE が受信した証明書が正当なものかを確認するための信頼の基点となる。
EP 証明書	FX プロダクト認証局により管理運用される証明書。TOE 及び EP-BB 機能搭載複合機に対して発行される。 EP-BB 機能搭載複合機に対して発行された EP 証明書は、EP-BB 機能搭載複合機の内部に格納され、TOE との SSL ハンドシェイクによる認証の際に、クライアント証明書として TOE に対して送られる。 TOE に対して発行された EP 証明書は、TOE に格納され、EP-BB 機能搭載複合機との SSL ハンドシェイクによる認証の際に、サーバー証明書として EP-BB 機能搭載複合機に送られる。また、Edge サーバーとの SSL ハンドシェイクによる認証の際に、クライアント証明書として送られる。
中間 CA 証明書	EP 証明書、及び Edge サーバー証明書とルート証明書との関係を証明する証明

用語	説明
	書。FXプロダクト認証局証明書、FX 認証局証明書がこれに含まれる。FX 認証局証明書は、CA 証明書と呼ばれる場合もある。
O	証明書の内容で、証明書の発行局の組織名(Organization)を示す。
OU	証明書の内容で、証明書のサブジェクト名（公開鍵所有者の識別名）の組織単位(Organization Unit)を示す。
CN	証明書の内容で、証明書のサブジェクト名（公開鍵所有者の識別名）の一般名(Common Name)を示す。
FQDN	Fully Qualified Domain Name の略。インターネットやイントラネットなどのTCP/IPネットワーク上で、ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のこと。

1.5. TOE 概要

1.5.1. TOE の利用者役割

本 ST で想定する利用者役割を表 1に示す。

表1 利用者役割

役割	説明
管理者	TOE を管理するお客様側の管理者。TOE の各種設定を行う特別な権限を持つ。管理者は、管理保守クライアント(PC)にて Web ブラウザを使用して管理を行う。管理者は、TOE が接続される内部ネットワークの管理も行う。
保守員	TOE の障害対応をするFXまたはFX関連会社の従業員。管理者と同じくTOE の各種設定を行う特別な権限を持ち、さらに保守用のログを取得することができる。但し、保守員による管理を許可するかどうかは管理者が設定することができる。保守員は、管理保守クライアント(PC)にて Web ブラウザを使用して管理と保守を行う。

TOE を直接利用する表 1の利用者の他に、TOE に関係するその他の関連者を表 2に示す。

表 2 その他の関連者

関連者	説明
組織の責任者	TOE を利用運用する組織の責任者。管理者及び複合機管理者を任命する。
複合機管理者	EP-BB 機能搭載複合機を管理するお客様側の複合機管理者。複合機の各種設定を行う特別な権限を持つ。

管理者及び複合機管理者が、TOE 及び複合機を管理する際にはパスワードが必要である。また、保守員が、TOE の障害対応をする際にもパスワードが必要である。以降、それぞれのパスワードを、管理者パスワード、複合機管理者パスワード、及び保守員パスワードと記述する。

1.5.2. TOE 種別及び主要セキュリティ機能

TOE は、FX 製の EP-BB 機能搭載複合機を使うお客様に対して提供する EP サービスにおいて、Edge サーバーと、EP-BB 機能搭載複合機との間の通信を中継する PC 上で稼動するアプリケーションソフトウェアであり、基本機能（設定機能、ネットワーク設定チェック機能、ログバックアップ機能、及び、WebUI 制御機能）、及

び、EP 通信データの漏えい、改ざんを防止、または事前に検知するためのセキュリティ機能を提供する。

TOE が提供するセキュリティ機能の概要を以下に示す。

利用者識別認証機能:

TOE は、利用者（管理者、保守員）の識別認証を行い、利用者に応じて TSF データへのアクセスを制限する。管理者は、管理者パスワードを変更できるが、保守員パスワードを変更することはできない。また、保守員は、保守員パスワードを変更できるが、管理者パスワードを変更することはできない。

また TOE は、保守員のアクセスを禁止する機能を管理者に提供する。

ログ生成/ダウンロード機能:

TOE は、Web ブラウザからの操作についてのアクセスログをファイルに記録する。また、Edge サーバーとの通信についての通信ログをファイルに記録する。さらに、EP-BB 機能搭載複合機との通信に失敗した場合、及びログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）となり、古いログファイルの削除により空いた領域にログを記録し、古いログファイルを削除してもログが満杯の場合に、システムログをファイルに記録する。

管理者と保守員が、Web ブラウザからの操作でアクセスログと通信ログを管理保守クライアント(PC)にダウンロードする。また、保守員が、Web ブラウザからの操作でシステムログを管理保守クライアント(PC)にダウンロードする。

HTTPS 通信中継機能:

TOE が、EP-BB 機能搭載複合機と Edge サーバーとの通信を中継する際に、EP-BB 機能搭載複合機と Edge サーバーの識別認証とデータの暗号処理を行う。

また、TOE は、HTTPS 通信中継機能において、EP-BB 機能搭載複合機からの通信を受信するための通信ポート番号を設定する機能を管理者及び保守員に提供する。

1.5.3. TOE 利用環境

1.5.3.1. TOE 運用環境

TOE は、EP-BB 機能搭載複合機がオフィスの内部ネットワークから、外部ネットワークを介して EP センターの窓口である Edge サーバーとデータの送受信を行う際の中継を行う。

TOE の運用環境を図 1に示す。

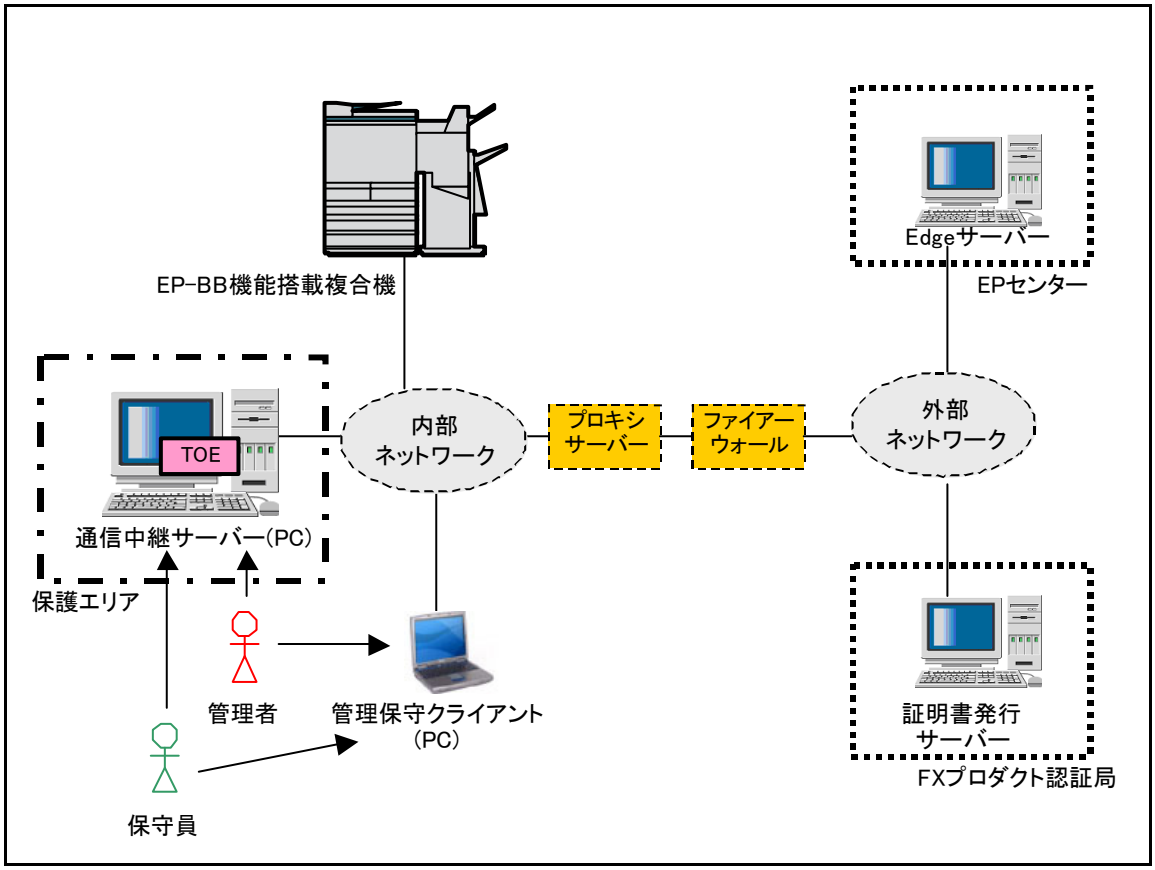


図 1 TOE の運用環境

以下、図 1の各機器の役割を説明する。

1. Edge サーバー

   TOE が、内部ネットワーク経由で通信する外部ネットワーク上にあるサーバー。外部から EP センターに送られてくる情報を受けるフロントエンドの役割をする。TOE と通信する際は、HTTPS サーバーとしてメッセージを受信する。TOE との通信は、鍵長 128 ビットの RC4 アルゴリズムでメッセージが暗号化されている。Edge サーバーをフロントエンドとして持つ EP センターは、FX の責任のもと高い信頼性で管理運用されている。

2. 証明書発行サーバー

   TOE に対して、EP 証明書を新規に作成して発行する。また、EP 証明書の発行の際に、TOE に対して、中間 CA 証明書とルート証明書の送付をする外部ネットワーク上にあるサーバー。FX プロダクト認証局は、FX の責任のもと高い信頼性で管理運用されている。

3. ファイアーウォール

   内部ネットワークと外部ネットワークとの通信を監視し、外部ネットワークからの不正なアクセスや侵入を防止することにより、内部ネットワークの安全を維持することを目的としたソフトウェア、あるいはソフトウェアを搭載したハードウェア。

4. プロキシサーバー

   内部ネットワークと外部ネットワークとの境にあって、内部ネットワークのコンピュータに代わって、「代理」として外部ネットワークとの接続を行うことを目的としたソフトウェア、あるいはソフトウェアを搭載し

たハードウェア。

5. EP-BB 機能搭載複合機

EP-BB 機能搭載複合機は、内部ネットワークに接続され、TOE を中継して、外部ネットワークにある Edge サーバーと通信する機能を搭載している。TOE と通信する際は、HTTPS クライアントとしてメッセージを送信する。EP-BB 機能搭載複合機には、保護資産である EP 通信データが存在し、この EP 通信データが TOE を経由して Edge サーバーに送信される。EP-BB 機能搭載複合機には、複合機管理者以外の利用者が、EP 通信データを変更する機能は搭載されていない。

6. 管理保守クライアント(PC)

管理保守クライアント(PC)は、内部ネットワークに接続され、管理者が管理しているPC である。保守員は、障害対応時に管理者の許可のもとで管理保守クライアント(PC)を使用できる。管理者と保守員は、Web ブラウザを使って、TOE にログインすることができ、TOE の各種設定や、通信ログ・アクセスログの TOE から管理保守クライアント(PC)へのダウンロードをすることができる。

7. 通信中継サーバー(PC)

通信中継サーバー(PC)は、内部ネットワークに接続され、管理者が管理しているPC であり、TOE が稼動するための PC である。EP-BB 機能搭載複合機からの通信を中継して、Edge サーバーと通信する。EP-BB 機能搭載複合機からの通信を受信する際は、HTTPS サーバーとしてメッセージを受信する。また、Edge サーバーと通信する際は、HTTPS クライアントとしてメッセージを送信する。TOE は、管理者または、管理者の許可のもとで保守員により通信中継サーバー(PC)にインストールされる。

1.5.3.2. ハードウェア構成

表 3に、TOE の動作環境としてのハードウェア構成を示す。

表 3 ハードウェア構成

項目	仕様	備考
ハードウェア	PC/AT 互換機	ネットワークポート(10/100/1000Base-T)必要
CPU	1GHz 以上のプロセッサ	
物理メモリ	512MB 以上	
ハードディスク空き容量	1GB 以上	
ディスプレイ	PC/AT 互換機に接続可能な仕様	TOE は WebUI を提供するため通常運用時は不要。但し、TOE のインストール時に必要
外部記憶装置	CD-ROM ドライブ	TOE のインストール時に必要
キーボード・マウス	PC/AT 互換機に接続可能な仕様	

1.5.3.3. ソフトウェア構成

表 4に管理保守クライアント(PC)のソフトウェア構成、及び TOE が動作する通信中継サーバー(PC)のソフトウェア構成と通信プロトコルを示す。

表 4 ソフトウェア構成

No.	管理保守クライアント(PC)		通信中継サーバー(PC)		通信プロトコル
	Web ブラウザ	OS	OS	IIS	
1	Microsoft® Internet Explorer® 6 SP2	Microsoft® Windows® XP Professional 日本語版 SP2	Microsoft® Windows® Server™ 2003, Standard Edition R2 日本語版	IIS6.0	IPv4
2	Windows® Internet Explorer® 7	Microsoft® Windows® XP Professional 日本語版 SP2	Microsoft® Windows® Server™ 2003, Standard Edition R2 日本語版	IIS6.0	IPv4
3	Microsoft® Internet Explorer® 6 SP2	Microsoft® Windows® XP Professional 日本語版 SP2	Microsoft® Windows® XP Professional 日本語版 SP2	IIS5.1	IPv4
4	Windows® Internet Explorer® 7	Microsoft® Windows® XP Professional 日本語版 SP2	Microsoft® Windows® XP Professional 日本語版 SP2	IIS5.1	IPv4
5	Windows® Internet Explorer® 7	Microsoft® Windows® Vista Business 日本語版	Microsoft® Windows® Vista Business 日本語版	IIS7.0	IPv4
6	Windows® Internet Explorer® 7	Microsoft® Windows® Vista Business 日本語版	Microsoft® Windows® Vista Business 日本語版	IIS7.0	IPv6

表 4に示したTOEが動作する通信中継サーバー(PC)のソフトウエア構成に加えて、TOEの動作に必要なソフトウエア構成を表 5に示す。

表 5 TOE の動作に必要なソフトウェア構成

項目	名称	備考
J#再頒布可能パッケージ	Microsoft® Visual J# 2.0 再頒布可能パッケージ	管理者または保守員が、通信ログとアクセスログを管理保守クライアント(PC)にダウンロードする際、または保守員が、システムログを管理保守クライアント(PC)にダウンロードする際にファイルを圧縮するために使用される。 インストールされていない場合、TOE のインストーラーにより、Microsoft® Visual J# 2.0 再頒布可能パッケージがインストールされる。
.NET Framework 再頒布可能パッケージ	Microsoft® .NET Framework 2.0 再頒布可能パッケージまたは Microsoft® .NET Framework 3.0 再頒布可能パッケージ	Edge サーバー及び EP-BB 機能搭載複合機との暗号通信や、排他制御、スレッド処理などを行うために使用する。 Microsoft® Windows® Server™ 2003, Standard Edition R2 日本語版、及び Microsoft® Windows® XP Professional 日本語版 SP2 においてインストールされていない場合、TOE のインストーラーにより、Microsoft® .NET Framework 2.0 再頒布可能パッケージがインストールされる。 Microsoft® Windows® Vista Business 日本語版には既に、Microsoft® .NET Framework3.0 が含まれているため、TOE のインストーラーが、Microsoft® .NET Framework 2.0 再頒布可能パッケージをインストールすることはない。

1.6. TOE 記述

本章では TOE の資産、TOE の論理的範囲、及び TOE の物理的範囲について記述する。

1.6.1. TOE の保護資産

TOE の保護資産は、EP-BB 機能搭載複合機が、TOE を中継して外部ネットワーク経由で Edge サーバーに送信する EP 通信データである。

保護資産である EP 通信データを保護するためのデータとして、Web ブラウザからの TOE に対する操作を記録したアクセスログ、Edge サーバーとの通信を記録した通信ログ、TOE に管理者または保守員が設定する設定データ、そして HTTPS 通信に使用する EP 証明書、中間 CA 証明書、及びルート証明書が、TSF データとしてファイルに格納されている。

TOE の保護資産について、利用者データの内容を表 6に、TSF データの内容を表 7に示す。

表6 利用者データ

利用者データ	内容
R.EP_COMM_DATA	**<EP 通信データ>** EP-BB 機能搭載複合機が、TOE を中継して Edge サーバーに送信するデータであり、以下のデータを含んでいる。 • データ送信元の EP-BB 機能搭載複合機の IP アドレス • EP-BB 機能搭載複合機の機種コードとシリアル番号 • EP-BB 機能搭載複合機のメーター値 • EP-BB 機能搭載複合機の障害情報 • 消耗品の使用状況(トナーの Near Empty、回収ボトルの Near Full) • 保守員の社員番号(複合機の保守作業時に保守員が入力)

表 7 TSF データ

TSF データ	内容
R.LOG	**<アクセスログ、通信ログ、及びシステムログ>** TOE は、Web ブラウザからの操作について、表 8に示すアクセスログの記録情報をファイルに記録する。また TOE は、Edge サーバーとの通信について、表 8に示す通信ログの記録情報をファイルに記録する。さらに TOE は、EP-BB 機能搭載複合機との通信に失敗した場合に、表 8に示すシステムログの記録情報をファイルに記録する。
R.CONF_DATA	**<設定データ>** TOE が動作するために必要な設定データがファイルに格納されている。 • 管理者パスワード • 保守員パスワード • HTTPS 受信ポート番号 上記以外のデータ(バックアップ先フォルダなど)もファイルに格納されているが、それらのデータには、秘密情報が含まれない。
R.CERT	**<証明書>** TOE が、EP-BB 機能搭載デバイス及び Edge サーバーと HTTPS 通信を行う際に、下記の証明書を使う。 • EP 証明書 • 中間 CA 証明書 • ルート証明書 TOE は、以下のタイミングで EP 証明書の有無と有効性を検証する。EP 証明書が無い、もしくは無効である場合に証明書発行サーバーから EP 証明書が発行される。EP 証明書が発行される際に、中間 CA 証明書とルート証明書も証明書発行サーバーから渡される。 • ネットワーク設定チェック機能の実施時 • TOE の起動時

TSF データ	内容
	• 毎日午前 0 時 0 分 TOE は、EP 証明書、中間 CA 証明書、及びルート証明書をファイルに格納する。TOE は、これらの証明書にアクセスする機能を提供しない。

表 8 ログの記録情報

CC(FAU_GEN.1.2)で要求される監査記録情報	アクセスログ	通信ログ	システムログ
事象の日付・時刻	・操作日時	・通信日時	・日時
事象の種別	・実施された操作	・通信種別	・ログレベル（INFORMATION, ERROR, CRITICAL）
サブジェクト識別情報	・利用者種別（管理者または保守員のどちらかが記録される）	・通信元の EP-BB 機能搭載複写機の IP アドレス ・通信先の Edge サーバーの IP アドレス	・モジュール名（ログを出力する内部モジュール名）
事象の結果（成功または失敗）	・操作結果	・通信結果	・内容（エラーコード）
その他の監査関連情報	・管理保守クライアント(PC)の IP アドレス ・社員番号（利用者種別が保守員の場合に、入力された社員番号が記録される） ・操作に伴い入力された値	・通信データ量	・内容（エラーメッセージ）

1.6.2. TOE の論理的範囲

TOE の論理的範囲を図 2に示す。

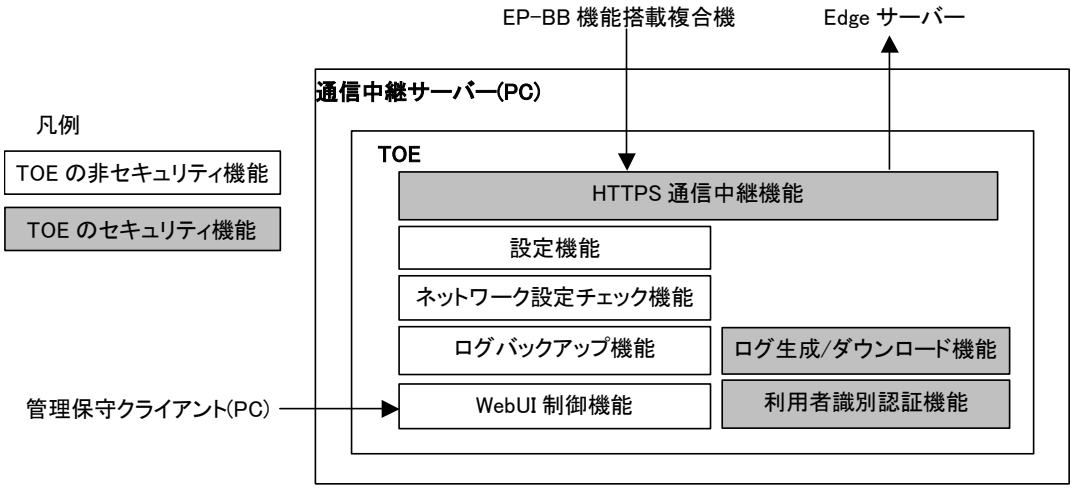


図 2 TOE の論理的範囲

TOE で提供される機能は大別すると以下のように分類される。

(1)基本機能

- 設定機能
- ネットワーク設定チェック機能
- ログバックアップ機能
- WebUI 制御機能

(2)セキュリティ機能

- 利用者識別認証機能
- ログ生成/ダウンロード機能
- HTTPS 通信中継機能

1.6.2.1節、1.6.2.2節に述べる機能はすべて、TOE の範囲である。

1.6.2.1. TOE によって提供される基本機能

表 9に、TOE が提供する基本機能の概要を記す。

表 9 TOE によって提供される基本機能

機能	概要
設定機能	管理者または保守員が使用する機能。Edge サーバーと通信する際に外部ネットワークにアクセスするために経由するプロキシサーバーに関する設定、及び、ログバックアップ機能におけるログバックアップ保存先に関する設定をする機能。 TOE のインストール時にのみ、ログ生成/ダウンロード機能におけるログ生成先に関する設定をすることができる。また、TOE のインストール時には、ログバックアップ機能におけるログバックアップ保存先に関する設定をすることもできる。
ネットワーク設定チェック機能	Edge サーバーとの通信確認により、ネットワークに関する設定が正しくされているかをチェックする機能。
ログバックアップ機能	TOE が、バックアップ先として指定されたフォルダに定期的にログをバックアップする機能。
WebUI 制御機能	管理保守クライアント(PC)の Web ブラウザを使った、管理者または保守員からの入力を、設定機能、ネットワーク設定チェック機能、利用者識別認証機能、及び、ログ生成/ダウンロード機能に伝える。

1.6.2.2. TOE によって提供されるセキュリティ機能

TOE が提供するセキュリティ機能の概要を記す。

(1)利用者識別認証機能

TOE は、利用者種別により管理者と保守員の識別を行い、パスワードによりこれらの認証を行う。利用者種別とパスワードは、管理者または保守員により、管理保守クライアント(PC)の Web ブラウザを介して入力される。

TOE は、Web ブラウザを介して入力された利用者種別（管理者または保守員）を管理し、利用者種別に応じた TSF データに対するアクセスを制限する。管理者は、TSF データの管理者パスワードを変更できるが、TSF データの保守員パスワードを変更することはできない。また、保守員は、保守員パスワードを変更できるが、管理者パスワードを変更することはできない。

また、TOE は保守員アカウントでの Web ブラウザからのログインを許可するかどうかを、管理者が設定する機能を提供する。

(2)ログ生成/ダウンロード機能

TOE は、Web ブラウザからの操作について以下の内容のアクセスログをファイルに記録する。

・操作日時
・管理保守クライアント(PC)の IP アドレス
・利用者種別（管理者または保守員のどちらかが記録される）
・社員番号（保守員の場合のみ記録される）
・実施された操作
・操作に伴い入力された値
・操作結果

TOE は、Edge サーバーとの通信について以下の内容の通信ログをファイルに記録する。

・通信日時
・通信元の EP-BB 機能搭載複写機の IP アドレス
・通信先の Edge サーバーの IP アドレス
・通信データ量
・通信種別
・通信結果

TOE は、EP-BB 機能搭載複合機との通信に失敗した場合、以下の内容のシステムログをファイルに記録する。また、ログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）となり、古いログファイルの削除によって空いた領域にログを記録し、古いログファイルを削除してもログが満杯の場合に、以下の内容のシステムログをファイルに記録する。

・日時
・モジュール名（ログを出力する内部モジュール名）
・ログレベル（INFORMATION, ERROR, CRITICAL）
・内容（エラーコード、エラーメッセージ）

また、管理者と保守員は、Web ブラウザからの操作により、管理保守クライアント(PC)にアクセスログ及び通信ログをダウンロードする。保守員は、管理保守クライアント(PC)にシステムログをダウンロードする。

(3)HTTPS 通信中継機能

TOE は、EP-BB 機能搭載複合機と Edge サーバーとの通信を中継する際に、EP-BB 機能搭載複合機と Edge サーバーの識別認証を行う。EP-BB 機能搭載複合機と Edge サーバーの識別認証には、HTTPS 技術を使用している。

EP-BB 機能搭載複合機から TOE に送られてくる EP 証明書と TOE に格納されているルート証明書とを

パス検証することによって、TOE は EP 証明書の有効性を検証している。パス検証には、TOE に格納されている中間 CA 証明書が使われる。また、有効であると判定された EP 証明書の内容を確認することにより、正しい EP-BB 機能搭載複合機であることを判断している。識別認証に成功した場合、EP 通信データを受信することを許可する。識別認証に失敗した場合、EP 通信データを受信することを許可しない。
TOE は、EP-BB 機能搭載複合機の識別認証に成功した場合、.NET Framework 再頒布可能パッケージの機能を利用して、EP-BB 機能搭載複合機から受信した EP 通信データを復号する。TOE の運用環境では、暗号アルゴリズムには RC4 が使用される。

Edge サーバーから TOE に送られてくる Edge サーバー証明書と TOE に格納されているルート証明書とをパス検証することによって、TOE は Edge サーバー証明書の有効性を検証している。パス検証には TOE に格納されている中間 CA 証明書が使われる。また、有効であると判定された Edge サーバー証明書の内容を確認することにより、正しい Edge サーバーであることを判断している。識別認証に成功した場合、EP 通信データを Edge サーバーに送信することを許可する。識別認証に失敗した場合、EP 通信データを送信することを許可しない。

TOE は、Edge サーバーの識別認証に成功した場合、.NET Framework 再頒布可能パッケージの機能を利用して暗号化した EP 通信データを、Edge サーバーに送信する。TOE の運用環境では、暗号アルゴリズムには RC4 が使用される。

TOE は、証明書発行サーバーから EP 証明書の発行、及び中間 CA 証明書とルート証明書の配布を受ける際に、HTTPS 技術を使用して配布もとを検証する。

また、TOE は、Web ブラウザを介して、HTTPS 通信中継機能において、EP-BB 機能搭載複合機からの通信を受信するための通信ポート番号を設定する機能を管理者及び保守員に提供する。

1.6.3. TOE の物理的範囲

図 3の破線内に示されるコンポーネントが TOE の物理的範囲である。

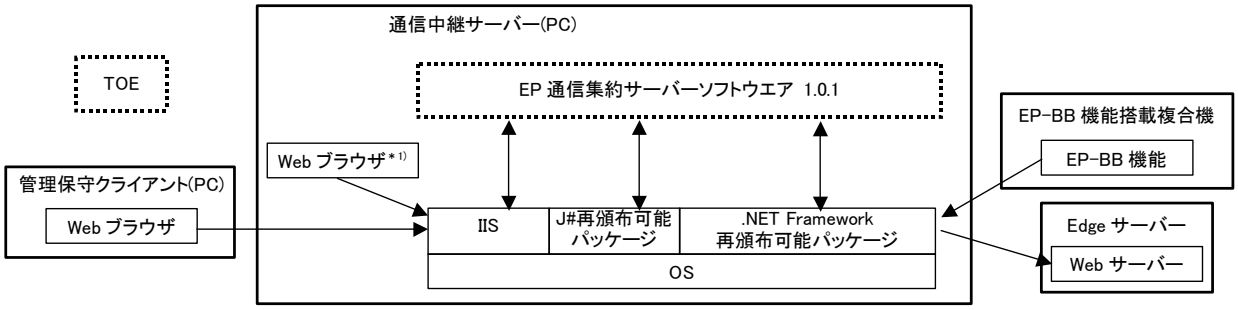


図 3 TOE の物理的範囲

*1)通常、管理者と保守員は、管理保守クライアント(PC)の Web ブラウザを使用して、IIS 経由で TOE にアクセスするが、管理保守クライアント(PC)の代用として通信中継サーバー(PC)の Web ブラウザを通して、TOE にアクセスすることができる。この場合は、通信中継サーバー(PC)と管理保守クライアント(PC)は兼用となる。

本 TOE を構成するガイダンス文書は以下の通りである。

- EP 通信集約サーバーソフトウエア取扱説明書 2008 年 8 月 第 1 版(帳票 No:ME4226J1-2)
- EP 通信集約サーバーソフトウエア取扱説明書(保守員向け補足情報) K1.02

2. 適合主張

2.1. CC 適合主張

本 ST 及び TOE の CC 適合主張は、以下のとおりである。

ST と TOE が適合を主張する CC のバージョン:

パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

パート 2:セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 翻訳 1.2 版

パート 3:セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳 1.2 版

CC パート 2 に対する ST の適合 :CC パート 2 拡張

CC パート 3 に対する ST の適合 :CC パート 3 適合

2.2. PP 主張、パッケージ主張

2.2.1. PP 主張

本 ST が適合している PP はない。

2.2.2. パッケージ主張

EAL2 適合

2.3. 適合根拠

本 ST が適合している PP はない。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。まず始めに、TOE のセキュリティに対する考え方について示す。TOE に対する攻撃を行う者について、以下のとおり想定する。

1.5.1節で識別された人物のうち、TOE を管理する立場にある管理者と複合機を管理する立場にある複合機管理者は、信頼できる人物であり攻撃することは想定されない。また、組織の責任者も、信頼できる人物であり攻撃することは想定されない。攻撃が想定される者（以下、攻撃者と示す。）は、高度な専門知識を持たない者とする。

表10 攻撃者

攻撃者	内容
TA.O	**<組織内攻撃者>** 組織内攻撃者は、EP-BB 機能搭載複合機と管理保守クライアント(PC)が設置された施設に入室可能であり、内部ネットワークにアクセス可能である。TOE に対して内部ネットワークからの不正アクセスなどの攻撃を行う。
TA.I	**<外部ネットワーク攻撃者>** 外部ネットワーク上の攻撃者は、TOE に対して外部ネットワークからの不正アクセスや盗聴/改ざんなどの攻撃を行う。
TA.CE	**<保守員>** 管理者の許可無く、TOE にアクセスする。

3.1. 脅威

TOE に対する特別なアクセス権限を与えられている管理者は信頼できるため、攻撃者には該当しない。本 TOE に対するセキュリティ脅威を表 11に示す。

表11 セキュリティ脅威

脅威	内容	攻撃者	保護資産
T.EP_COM	**<外部ネットワーク上での保護資産の漏洩、改ざん>** 外部ネットワーク攻撃者が、プロトコルアナライザを使用し、TOE と Edge サーバーとの間で送受信される EP 通信データを盗み見るかもしれない。また、EP 通信データを改ざんし、TOE が送信したデータとは異なったデータを Edge サーバーに受信させるかもしれない。	TA.I	R.EP_COMM_DATA
T.FAKE_EDGE_SERVER	**<Edge サーバーになりすまし>** 攻撃者が偽 Edge サーバーを立ち上げ、その偽 Edge サーバーの攻撃者が外部ネットワークを介して、EP 通信データに不正にアクセスするかもしれない。	TA.I	R.EP_COMM_DATA
T.FAKE_EP-BB_DEVICE	**<EP-BB 機能搭載複合機になりすまし>** 攻撃者が偽 EP-BB 機能搭載複合機を内部ネットワークに設置し、EP 通信データに不正にアクセスするかもしれない。	TA.O	R.EP_COMM_DATA
T.ACCESS_TSF_DATA	**<TSF データへの不正アクセス>** 組織内攻撃者が、管理保守クライアント(PC)の Web ブラウザから、管理者または保守員のみアクセス許可されている TOE 設定データにアクセスして設定を変更するかもしれない。また、ログをダウンロードするかもしれない。	TA.O	R.CONF_DATA R.LOG
T.CE_ACCESS	**<CE による不正アクセス>** 保守員、または保守員になりすました者が、管理者の許可なく、管理者または保守員のみアクセス許可されている TSF データにアクセスして設定を変更するかもしれな	TA.CE	R.CONF_DATA R.LOG

脅威	内容	攻撃者	保護資産
	い。また、ログをダウンロードするかもしれない。		

3.2. 組織のセキュリティ方針

組織のセキュリティ方針はない。

3.3. 前提条件

本TOEの動作/運用/利用に関わる前提条件を表12に示す。

表12 前提条件

前提条件	内容
A.PHYSICAL	**<物理的な保護>** 通信中継サーバー(PC)は、許可された利用者のみが入場可能な場所に設置され、入場が許可された利用者だけが物理的にアクセスすると仮定する。
A.ADMIN	**<信頼できる管理者>** 管理者、及び複合機管理者は、課せられた役割を遂行するために必要な知識と情報管理能力を有し、悪意をもった不正を行わないと仮定する。
A.PASSWORD	**<守られたパスワード>** 管理者が、管理保守クライアント(PC)から TOE にアクセスする際には、パスワードが漏洩しないと仮定する。 管理者パスワードと複合機管理者パスワードは、常に厳重に管理され、漏洩しないと仮定する。
A.NET	**<盗聴から守られた内部ネットワーク>** TOE、EP-BB 機能搭載複合機、及び管理保守クライアント(PC)を設置する内部ネットワークは盗聴されない環境を構築すると仮定する。
A.FIREWALL	**<外部から守られた内部ネットワーク>** TOE、EP-BB 機能搭載複合機、及び管理保守クライアント(PC)を設置する内部ネットワークは、ファイアーウォールによって外部ネットワークから隔離され、外部ネットワークからの攻撃から保護されると仮定する。
A.DEVICE	**<守られた複合機>** 複合機管理者だけが、EP-BB 機能搭載複合機の EP 通信データの元となるデータにアクセスできると仮定する。
A.SERVER_PC	**<守られた通信中継サーバー(PC)>** 通信中継サーバー(PC)上の OS には、許可された者だけがアクセスできると仮定する。
A.CLIENT_PC	**<守られた管理保守クライアント(PC)>** 管理保守クライアント(PC)上にあるログ情報が漏洩しないと仮定する。

4. セキュリティ対策方針

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 13に示す。

表13 TOE のセキュリティ対策方針

対策方針	説明
O.I&A	**<利用者の識別認証とアクセス制御>** 管理保守クライアント(PC)の Web ブラウザを介して TOE にアクセスする際に、TOE は利用者（管理者、保守員）を識別認証し、また、その利用者に応じて TSF データへのアクセスを制限することを保証する。
O.CE_ACCESS	**<保守員アクセス禁止>** TOE は、保守員のアクセスを禁止する機能を、管理者に提供することを保証する。
O.EDGE_SERVER_ID	**<Edge サーバー識別認証>** 正しい Edge サーバーと通信することを保証する。
O.EP-BB_DEVICE_ID	**<EP-BB 機能搭載複合機識別認証>** 正しい EP-BB 機能搭載複合機と通信することを保証する。
O.CH	**<信頼された通信チャネル>** TOE は、Edge サーバーとの通信において、信頼されるチャネルを確立し、通信データの漏洩防止と、その完全性を保証する。

4.2. 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 14に示す。

表14 運用環境のセキュリティ対策方針

対策方針	説明
OE.PHYSICAL	**<物理的な保護>** 管理者は、許可された利用者以外が通信中継サーバー(PC)に物理的にアクセスできないように、許可された利用者のみが入場可能な場所に通信中継サーバー(PC)を設置しなければならない。
OE.ADMIN	**<信頼できる管理者>** 組織の責任者は、管理者、及び複合機管理者が課せられた役割を遂行するために必要な知識を有し、悪意をもった行為を行わないことを保証するために、適切な人選を行うと共に管理や教育を実施しなければならない。
OE.PASSWORD	**<守られたパスワード>** 管理者は、容易に推測できるパスワードを使用してはならない。また、攻撃者の目に触れる場所にパスワードを格納してはならない。さらに、管理保守クライアント(PC)から TOE にアクセスする際にパスワードが漏洩しないように、キーロガー等の入力を読み取るソフトウェアがインストールされないように、管理保守クライアント(PC)を管理しなければならない。 複合機管理者は、容易に推測できるパスワードを使用してはならない。また、攻撃者の目に触れる場所にパスワードを格納してはならない。
OE.NET	**<盗聴から守られた内部ネットワーク>** 管理者は、盗聴されない環境を維持するために、適切に内部ネットワークの運用管理を行わなければならない。
OE.FIREWALL	**<外部から守られた内部ネットワーク>** TOE が外部ネットワークからの攻撃から保護されるように、ファイアーウォールを設置しなければならない。
OE.DEVICE	**<守られた複合機>** 複合機管理者は、組織内の者からの不正な操作が行われないように、EP-BB 機能搭載複合機を設定、管理しなければならない。
OE.SERVER_PC	**<守られた通信中継サーバー(PC)>** 管理者は、通信中継サーバー（PC）の OS に対して、必要なアカウントのみを登録しなければならない。
OE.CLIENT_PC	**<守られた管理保守クライアント(PC)>** 管理者は、管理保守クライアント(PC)の OS の資産に対して、管理者によって許可された利用者だ

対策方針	説明
	けがアクセスできるように、アクセス権を設定しなければならない。

4.3. セキュリティ対策方針根拠

セキュリティ対策は、セキュリティ課題定義で規定した脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針、及び前提条件の対応関係を表 15示す。

表 15 セキュリティ対策方針と対抗する脅威、組織のセキュリティ方針及び前提条件

脅威・前提条件 / 組織のセキュリティ方針 / セキュリティ対策方針	T.EP_COM	T.FAKE_EDGE_SERVER	T.FAKE_EP-BB_DEVICE	T. ACCESS_TSF_DATA	T.CE_ACCESS	A.PHYSICAL	A.ADMIN	A.PASSWORD	A.NET	A.FIREWALL	A.DEVICE	A.SERVER_PC	A.CLIENTPC
O.I&A				○									
O.CE_ACCESS					○								
O.EDGE_SERVER_ID		○											
O.EP-BB_DEVICE_ID			○										
O.CH	○												
OE.PHYSICAL						○							
OE.ADMIN							○						
OE.PASSWORD								○					
OE.NET									○				
OE.FIREWALL										○			
OE.DEVICE											○		
OE.SERVER_PC												○	
OE.CLIENT_PC													○

○: 対象のセキュリティ対策方針が対応している脅威または前提条件である事を示す。

表 15により、各セキュリティ対策方針は一つ以上の脅威、及び前提条件に対応している。
次に、各脅威がセキュリティ対策方針で対抗できること、各前提条件がセキュリティ対策方針により実現できることを説明する。
説明の中では、各脅威に対して攻撃者を明示し、攻撃者が行う想定される攻撃方法を分析する。次に、攻撃方法に対抗するための有効な対策内容を示し、それがすべて満たされることで脅威に対抗できる十分な対策であることを示す。なお、対策内容は、一つ以上のセキュリティ対策方針がそれを満たし、脅威に対するセキュリティ対策方針として必要であることを示す。

T.EP_COM(外部ネットワーク上での保護資産の漏洩、改ざん)

この脅威は、表 10で識別されるTA.I(外部ネットワーク攻撃者)によって実行される。この攻撃者は、外部ネットワークにてプロトコルアナライザを使用して、TOE と Edge サーバーとの間で送受信される EP 通信データを盗み見る。また、EP 通信データを改ざんし、TOE が送信したデータとは異なるデータを Edge サーバーに受信さ

せる。
この攻撃に対して TOE は、Edge サーバーとの通信時に信頼されるチャネルを作り、EP 通信データが漏洩しないことと、その完全性を保証する。
この対抗策に該当するセキュリティ対策方針は、O.CH である。

T.FAKE_EDGE_SERVER（Edge サーバーになりすまし）
この脅威は、表 10で識別される TA.I（外部ネットワーク攻撃者）によって実行される。攻撃者が偽 Edge サーバーを立ち上げ、その偽 Edge サーバーの攻撃者が外部ネットワークを介して、EP 通信データに不正にアクセスするかもしれない。
この攻撃に対して TOE は、Edge サーバーと通信する際に Edge サーバーから送られてくる Edge サーバー証明書と TOE に格納されているルート証明書とを中間 CA 証明書を用いてパス検証するとともに、Edge サーバー証明書の内容を確認することにより、正しい Edge サーバーと通信することを保証する。この対抗策に該当するセキュリティ対策方針は、O.EDGER_SERVER_ID である。

T.FAKE_EP-BB_DEVICE（EP-BB 機能搭載複合機になりすまし）
この脅威は、表 10で識別される TA.O（組織内攻撃者）によって実行される。攻撃者が偽 EP-BB 機能搭載複合機を内部ネットワークに設置し、EP 通信データに不正にアクセスするかもしれない。
この攻撃に対して TOE は、EP-BB 機能搭載複合機と通信する際に EP-BB 機能搭載複合機から送られてくる EP 証明書と TOE に格納されているルート証明書とを中間 CA 証明書を用いてパス検証するとともに、EP 証明書の内容を確認することにより、正しい EP-BB 機能搭載複合機と通信することを保証する。この対抗策に該当するセキュリティ対策方針は、O.EP-BB_DEVICE_ID である。

T.ACCESS_TSF_DATA（TSF データへの不正アクセス）
この脅威は、表 10で識別される TA.O（組織内攻撃者）によって実行される。この攻撃者は、利用を許可されている者になりすます。
この攻撃に対しては、TOE の利用において識別認証を行い、TOE の利用を正当な者にのみ制限することにより対抗できる。
この対抗策に該当するセキュリティ対策方針は、O.I&A である。

T.CE_ACCESS（CE による不正アクセス）
この脅威は、表 10で識別される TA.CE（保守員）によって実行される。この攻撃者は、管理者の許可なく管理保守クライアント(PC)を使用して、TSF データにアクセスして設定を変更する。また、ログをダウンロードする。
この攻撃に対して、TOE は保守員のアクセスを禁止する機能を管理者に提供することにより対抗できる。
この対抗策に該当するセキュリティ対策方針は、O.CE_ACCESS である。

A.PHYSICAL（物理的な保護）
許可された利用者のみ入場可能な場所に通信中継サーバー(PC)を管理者が設置することにより、表 10で識別される TA.O（組織内攻撃者）及び TA.CE（保守員）が、通信中継サーバー(PC)に物理的にアクセスできないことを保証できる。

この前提条件を実現するセキュリティ対策方針は、OE.PHYSICAL である。

A.ADMIN（信頼できる管理者）

管理者、及び複合機管理者が、課せられた役割を遂行するために必要な知識と情報管理能力を有することにより、管理者、及び複合機管理者が悪意を持った不正を行わないことを保証できる。
この前提条件を実現するセキュリティ対策方針は、OE.ADMIN である。

A.PASSWORD（守られたパスワード）

管理者及び複合機管理者が、容易に推測できるパスワードを使用しない。また、攻撃者の目に触れる場所にパスワードを格納しない。さらに、キーロガー等の入力を読み取るソフトウェアが管理保守クライアント(PC)にインストールされないように、管理者が管理保守クライアント(PC)を管理することにより、パスワードが表 10で識別される TA.O（組織内攻撃者）に対して漏洩しないことが保証される。
この前提条件を実現するセキュリティ対策方針は、OE.PASSWORD である。

A.NET（盗聴から守られた内部ネットワーク）

管理者が、内部ネットワークに盗聴されない環境を実現するために、適切に内部ネットワークの運用管理を行うことにより、表 10で識別される TA.O（組織内攻撃者）に対して盗聴されることが無いことを保証できる。
この前提条件を実現するセキュリティ対策方針は、OE.NET である

A.FIREWALL（外部から守られた内部ネットワーク）

管理者がファイアーウォールを設置することにより、表 10で識別される TA.I（外部ネットワーク攻撃者）から内部ネットワークが保護されることを保証できる。
この前提条件を実現するセキュリティ対策方針は、OE.FIREWALL である。

A.DEVICE（守られた複合機）

複合機管理者が、表 10で識別される TA.O（組織内攻撃者）からの不正な操作が行われないように、EP-BB 機能搭載複合機を設定、管理することにより、EP 通信データの元となるデータが、組織内攻撃者によりアクセスされることが無いことを保証することができる。
この前提条件を実現するセキュリティ対策方針は、OE.DEVICE である。

A.SERVER_PC（守られた通信中継サーバー(PC)）

通信中継サーバー(PC)は、管理者以外が保護資産にアクセスできないように、管理者が使うアカウントのみを OS に登録されることにより、管理者以外の利用者が悪意を持った不正を行わないことを保証できる。
この前提条件を実現するセキュリティ対策方針は、OE.SERVER_PC である。

A.CLIENT_PC（守られた管理保守クライアント(PC)）

管理保守クライアント(PC)は、管理者によって許可された利用者だけが管理保守クライアント(PC)上にあるログ情報にアクセスできるように、OS のアクセス権を設定されることにより、管理者によって許可されていない利用者が悪意を持った不正を行わないことを保証できる。

この前提条件を実現するセキュリティ対策方針は、OE.CLIENT_PC である。

5. 拡張コンポーネントの定義

本章では、FTP クラスの新しいファミリ FTP_ICG（TSF 間高信頼性チャネルの生成と保証）に属する拡張のセキュリティ機能要件 FTP_ICG.1 を定義する。

5.1. クラス FTP： 高信頼パス/チャネル

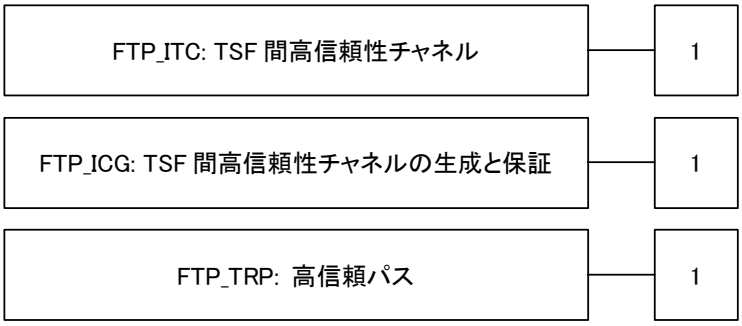


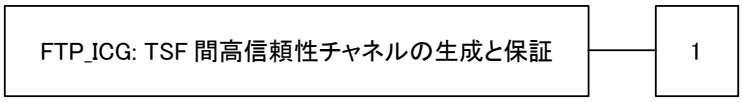
図 4 FTP: 高信頼パス/チャネルクラスのコンポーネント構成

5.1.1. TSF 間高信頼性チャネルの生成と保証（FTP_ICG）

ファミリのふるまい

このファミリは、セキュリティ上の重要な操作のために、TSF と他の高信頼 IT 製品間に高信頼チャネルを生成するための要件を定義する。TSF は高信頼チャネルを提供、または TSF により要請された TOE 外のパーツが提供することを保証する。

コンポーネントのレベル付け



FTP_ICG.1 TSF 間高信頼性チャネルの生成と保証は、TSF が高信頼チャネルを提供、または TSF により要請された TOE 外のパーツが提供することを保証することによって、TSF 自身と他の高信頼 IT 製品間に高信頼通信チャネルを提供することを要求する。

管理: FTP_ICG.1

以下のアクションは FMT における管理機能と考えられる:

a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。

監査: FTP_ICG.1

セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 高信頼チャネル機能の失敗。

b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。

c) 基本: 高信頼チャネル機能のすべての使用の試み。

d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

FTP_ICG.1 TSF 間高信頼チャネルの生成と保証

下位階層: なし

依存性: なし

FTP_ICG.1.1 TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別を提供する通信チャネルを提供しなければならない。

FTP_ICG.1.2 TSF は、TSF により要請された [割付: *TOE 外のパーツ*] が、TSF 自身とリモート高信頼 IT 製品間の通信チャネルのデータを改変や暴露から保護することを保証しなければならない。

FTP_ICG.1.3 TSF は、[選択: *TSF*、*リモート高信頼 IT 製品*] が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ICG.1.4 TSF は、[割付: *高信頼チャネルが要求される機能のリスト*] のために、高信頼チャネルを介して通信を開始しなければならない。

TOE は CC パート 2 の既存のセキュリティ機能要件コンポーネント FTP_ITC.1 が要求する機能の一部を実施しているが、他の一部の機能の実施を TOE 外のパーツに要請しているので、TSF を正確に表現するために拡張のセキュリティ機能要件コンポーネント FTP_ICG.1 を定義する。

6. セキュリティ要件

本章では、セキュリティ要件を記述する。

6.1. セキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。詳細化した部分には、下線を入れて示す。

6.1.1. クラス FAU: セキュリティ監査

FAU_GEN.1　　監査データ生成

下位階層:　　なし

依存性:　　FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1　TSF は、以下の監査対象事象の監査記録を生成できなければならない:

・ 監査機能の起動と終了;

・ 監査の[選択:*最小*、*基本*、*詳細*、*指定なし*:から1つのみ選択]レベルのすべての監査対象事象;

及び

・ [割付:*上記以外の個別に定義した監査対象事象*]。

[選択:最小、基本、詳細、指定なし:から1つのみ選択]

基本

監査対象事象を表 16に示す。

[割付:上記以外の個別に定義した監査対象事象]

なし

監査対象事象の監査レベルは、表 16の CC で要求される監査対象事象欄の太字下線文字で示される。

表 16 監査対象事象

機能要件	CC で要求される監査対象事象	監査対象事象
FAU_GEN.1	予見される監査対象事象はない。	監査対象事象なし。
FAU_SAR.1(1)	**基本**:監査記録からの情報の読み出し。	・アクセスログ及び通信ログのダウンロード。
FAU_SAR.1(2)	**基本**:監査記録からの情報の読み出し。	・システムログのダウンロード。
FAU_STG.4	**基本**:監査格納失敗によってとられるアクション。	・監査格納の失敗。
FIA_AFL.1	**最小**:不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	・ログインの拒絶。 ・ログインの成功。
FIA_SOS.1	最小:TSF による、テストされた秘密の拒否; **基本**:TSF による、テストされた秘密の拒否または受け入れ; 詳細:定義された品質尺度に対する変更の識別。	・管理者パスワード、保守員パスワードの変更。
FIA_UAU.2	最小:認証メカニズムの不成功になった使用;	・ログイン(成功・失敗)。

機能要件	CC で要求される監査対象事象	監査対象事象
	基本:認証メカニズムの全ての使用。	
FIA_UID.2	最小:提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; **基本**:提供される利用者識別情報を含む、利用者識別メカニズムの全ての使用	・ログイン(成功・失敗)。
FMT_MOF.1	**基本**:TSF の機能のふるまいにおける全ての改変。	・保守員アクセス可否の変更。
FMT_MTD.1(1)	**基本**:TSF データのすべての改変。	・管理者パスワードの変更。
FMT_MTD.1(2)	**基本**:TSF データのすべての改変。	・保守員パスワードの変更。
FMT_MTD.1(3)	**基本**:TSF データのすべての改変。	・HTTPS 受信ポート番号の変更。
FMT_MTD.3(1)	最小:TSF データのすべての拒否された値	監査事象なし。*1)
FMT_MTD.3(2)	最小:TSF データのすべての拒否された値	監査事象なし。*1)
FMT_MTD.3(3)	最小:TSF データのすべての拒否された値	監査事象なし。*1)
FMT_SMF.1	**最小**:管理機能の使用	・管理者パスワードの変更。*2) ・保守員パスワードの変更。*2) ・HTTPS 受信ポート番号の変更。*2) ・保守員アクセス可否の変更。*2)
FMT_SMR.1(1)	最小:役割の一部をなす利用者のグループに対する改変; 詳細:役割の権限の使用すべて。	監査事象なし。*3)
FMT_SMR.1(2)	最小:役割の一部をなす利用者のグループに対する改変; 詳細:役割の権限の使用すべて。	監査事象なし。*3)
FPT_STM.1	最小:時間の変更; 詳細:タイムスタンプの提供。	監査事象なし。*4)
FTP_ICG.1(1)	最小:高信頼チャネル機能の失敗。 最小:失敗した高信頼チャネル機能の開始者とターゲットの識別。 基本:高信頼チャネル機能のすべての使用の試み。 **基本**:すべての高信頼チャネル機能の開始者とターゲットの識別。	・Edge サーバーとの接続。 ・EP 通信データの送信(成功・失敗)。
FTP_ICG.1(2)	**最小**:高信頼チャネル機能の失敗。 最小:失敗した高信頼チャネル機能の開始者とターゲットの識別。 基本:高信頼チャネル機能のすべての使用の試み。 基本:すべての高信頼チャネル機能の開始者とターゲットの識別。	・EP-BB 機能搭載複合機との接続(失敗)。*5)

*1) FMT_MTD.3(1)、FMT_MTD.3(2)、及び FMT_MTD.3(3)に関し、FX により適切な管理運用がされている FX プロダクト認証局から、EP 証明書、中間 CA 証明書、及びルート証明書を取得している。また、TOE は EP 証明書、中間 CA 証明書、及びルート証明書にアクセスする機能を提供していない。

*2) FMT_SMF.1 に関し、管理機能である FMT_MOF.1、FMT_MTD.1(1)、FMT_MTD.1(2)、及び FMT_MTD.3(3)にて記録される。

*3)FMT_SMR.1(1)、及び FMT_SMR.1(2)に関し、グループに対する改変は無いため、監査事象はない。

*4)FPT_STM.1 に関し、時間情報の取得は通信中継サーバー(PC)にて稼動する OS から取得する。通信中継サーバー(PC)は、適切な管理のもとで運用されるため、OS から取得する時刻は正確である。

*5) FTP_ICG.1(2)に関し、EP-BB 機能搭載複合機との接続失敗時のみが監査対象であるが、接続成功時に関しては、FTP_ICG.1(1)にて記録されている。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

・ 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);及び

・各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*]

[割付:その他の監査関連情報]

また、事象種別に記録されるその他の監査関連情報を表 17に示す。

表 17 監査対象事象と記録されるその他の監査関連情報

機能要件	監査対象事象	その他の監査関連情報
FAU_GEN.1	監査対象事象なし。	なし
FAU_SAR.1(1)	・アクセスログ及び通信ログのダウンロード。	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される) ・操作に伴い入力された値: ダウンロードしたログの種別(通信ログ、アクセスログ)
FAU_SAR.1(2)	・システムログのダウンロード。	・管理保守クライアント(PC)の IP アドレス ・社員番号 ・操作に伴い入力された値: ダウンロードしたログの種別(システムログ)
FAU_STG.4	・監査格納の失敗。	・内容(エラーメッセージ)
FIA_AFL.1	・ログインの拒絶。 ・ログインの成功。	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される)
FIA_SOS.1	・管理者パスワード、保守員パスワードの変更。	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される)
FIA_UAU.2	・ログイン(成功・失敗)。	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される)
FIA_UID.2	・ログイン(成功・失敗)。	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される)
FMT_MOF.1	・保守員アクセス可否の変更。	・管理保守クライアント(PC)の IP アドレス ・変更種別(有効化、無効化)

機能要件	監査対象事象	その他の監査関連情報
FMT_MTD.1(1)	・管理者パスワードの変更。	・管理保守クライアント(PC)の IP アドレス
FMT_MTD.1(2)	・保守員パスワードの変更。	・管理保守クライアント(PC)の IP アドレス ・社員番号（保守員の場合のみ記録される）
FMT_MTD.1(3)	・HTTPS 受信ポート番号の変更。	・管理保守クライアント(PC)の IP アドレス ・社員番号（保守員の場合のみ記録される） ・操作に伴い入力された値：HTTPS 受信ポート番号
FMT_MTD.3(1)	監査事象なし	なし
FMT_MTD.3(2)	監査事象なし	なし
FMT_MTD.3(3)	監査事象なし	なし
FMT_SMF.1	・管理者パスワードの変更。 ・保守員パスワードの変更。 ・HTTPS 受信ポート番号の変更。 ・保守員アクセス可否の変更。	・FMT_MOF.1 、FMT_MTD.1(1) 、FMT_MTD.1(2) 、及び FMT_MTD.1(3)の「その他の監査関連情報」
FMT_SMR.1(1)	監査事象なし	なし
FMT_SMR.1(2)	監査事象なし	なし
FPT_STM.1	監査事象なし	なし
FTP_ICG.1(1)	・Edge サーバーとの接続 ・EP 通信データの送信（成功・失敗）	・通信データ量
FTP_ICG.1(2)	・EP-BB 機能搭載複合機との接続（失敗）。	・内容（エラーメッセージ）

FAU_SAR.1(1)　監査レビュー

下位階層:　なし

依存性:　FAU_GEN.1 監査データ生成

FAU_SAR.1.1(1)　TSF は、[割付：*許可利用者*]が、[割付：*監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]

管理者、保守員

[割付：監査情報のリスト]

・FAU_GEN1.1 の監査対象事象の監査記録（FAU_STG.4 及び FTP_ICG.1(2)を除く）

・FAU_GEN1.2 の監査記録（FAU_STG.4 及び FTP_ICG.1(2)を除く）

FAU_SAR.1.2(1)　TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_SAR.1(2)　監査レビュー

下位階層:　なし

依存性:　FAU_GEN.1 監査データ生成

FAU_SAR.1.1(2) TSF は、[割付：*許可利用者*]が、[割付：*監査情報のリスト*]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]

保守員

[割付：監査情報のリスト]

・FAU_GEN1.1 の監査対象事象の監査記録（FAU_STG.4 及び FTP_ICG.1(2)）

・FAU_GEN1.2 の監査記録（FAU_STG.4 及び FTP_ICG.1(2)）

FAU_SAR.1.2(2) TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_STG.4 監査データ消失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択：*監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き*: から1つのみ選択]及び[割付：*監査格納失敗時にとられるその他のアクション*]を行わなければならない。

[選択：監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から1つのみ選択]

最も古くに格納された監査記録への上書き

[割付：監査格納失敗時にとられるその他のアクション]

監査格納エラー状態（WebUI にエラーメッセージ「ログフォルダの空き容量が不足しています。」が表示され、EP-BB 機能搭載複合機からの通信を受け付けない状態）への移行

6.1.2. クラス FIA： 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[割付：*認証事象のリスト*]に関して、[選択：*[割付：正の整数値]*、*[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト]

同一 IP アドレスの管理保守クライアント(PC)からの 20 秒以内の間隔での認証

[選択：[割付：正の整数値]、[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値]

[割付：正の整数値]

3

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：*アクションのリスト*]をしなければならない。

[割付：アクションのリスト]

1 分間の認証の拒絶

FIA_SOS.1 秘密の検証

下位階層: なし

依存性: なし

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

[割付：定義された品質尺度]

以下の品質尺度。

・パスワードは、8 文字以上 20 文字以下の、以下の範囲の ASCII 文字が使用できる。

・アルファベットは、半角大文字[A-Z]の 26 文字、半角小文字[a-z]の 26 文字の合計 52 文字（大文字、小文字は区別される。

・数字は、半角で[0-9]の合計 10 文字。

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

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

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.3. クラス FMT： セキュリティ管理

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

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

ればならない。

[割付：機能のリスト]

利用者識別認証機能

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

のふるまいを改変する

[割付：許可された識別された役割]

管理者

FMT_MTD.1(1)　TSF データの管理

下位階層:　なし

依存性:　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(1)　TSF は、[割付：*TSF データのリスト*]を[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]する能力を[割付：*許可された識別された役割*]に制限しなければならない。

[割付：TSF データのリスト]

管理者パスワード

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]

改変

[割付：許可された識別された役割]

管理者

FMT_MTD.1(2)　TSF データの管理

下位階層:　なし

依存性:　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(2)　TSF は、[割付：*TSF データのリスト*]を[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]する能力を[割付：*許可された識別された役割*]に制限しなければならない。

[割付：TSF データのリスト]

保守員パスワード

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]

改変

[割付：許可された識別された役割]

保守員

FMT_MTD.1(3)　TSF データの管理

下位階層:　なし

依存性:　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1(3) TSF は、[割付：*TSF データのリスト*]を[選択：*デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]*]する能力を[割付：*許可された識別された役割*]に制限しなければならない。

[割付：TSF データのリスト]

HTTPS 受信ポート番号

[選択：デフォルト値変更、問い合わせ、改変、削除、消去、[割付：その他の操作]]

改変

[割付：許可された識別された役割]

管理者、保守員

FMT_MTD.3(1) セキュアな TSF データ

下位階層: なし

依存性: FMT_MTD.1 TSF データの管理

FMT_MTD.3.1(1) TSF は、TSF データとしてセキュアな値だけが受け入れられることを保証しなければならない。

[詳細化]

TSF は、EP 証明書としてセキュアな値だけが受け入れられることを保証しなければならない。

FMT_MTD.3(2) セキュアな TSF データ

下位階層: なし

依存性: FMT_MTD.1 TSF データの管理

FMT_MTD.3.1(2) TSF は、TSF データとしてセキュアな値だけが受け入れられることを保証しなければならない。

[詳細化]

TSF は、中間 CA 証明書としてセキュアな値だけが受け入れられることを保証しなければならない。

FMT_MTD.3(3) セキュアな TSF データ

下位階層: なし

依存性: FMT_MTD.1 TSF データの管理

FMT_MTD.3.1(3) TSF は、TSF データとしてセキュアな値だけが受け入れられることを保証しなければならない。

[詳細化]

TSF は、ルート証明書としてセキュアな値だけが受け入れられることを保証しなければならない。

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。[割付: *TSF によって提供される管理機能のリスト*]

[割付:TSF によって提供される管理機能のリスト]

表 18に示す TSF によって提供される管理機能

表 18 TSF によって提供される管理機能

機能要件	CC で要求される管理機能	TSF によって提供される管理機能
FAU_GEN.1	予見される管理アクティビティはない。	無し
FAU_SAR.1(1)	a) 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	a) 無し(管理者及び保守員固定)
FAU_SAR.1(2)	a) 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	a) 無し(保守員固定)
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	a) 無し(アクションは固定)
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理; b) 認証失敗の事象においてとられるアクションの管理。	a) 無し(閾値は固定) b) 無し(アクションは固定)
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	a) 無し(固定)
FIA_UAU.2	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	管理者、保守員のパスワードの管理機能
FIA_UID.2	a) 利用者識別情報の管理。	a) 無し(利用者識別情報は固定)
FMT_MOF.1	a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること。	a) 保守員のアクセスを禁止する機能(管理者固定)
FMT_MTD.1(1)	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) 無し(管理者固定)
FMT_MTD.1(2)	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) 無し(保守員固定)
FMT_MTD.1(3)	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) 無し(管理者及び保守員固定)
FMT_MTD.3(1)	予見される管理アクティビティはない。	無し
FMT_MTD.3(2)	予見される管理アクティビティはない。	無し
FMT_MTD.3(3)	予見される管理アクティビティはない。	無し
FMT_SMR.1(1)	a) 役割の一部をなす利用者のグループの管理。	a) 無し(管理者固定:管理者パスワードを知るものだけが、管理者となれる。)
FMT_SMR.1(2)	a) 役割の一部をなす利用者のグループの管理。	a) 無し(保守員固定:保守員パスワードを知るものだけが、保守員となれる。)
FPT_STM.1	a) 時間の管理。	a) 無し(時刻固定)
FTP_ICG.1(1)	a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。	HTTPS 受信ポート番号変更機能 ※本機能は、FMT_MTD.1(3)の HTTPS 受信ポート番号の変更機能
FTP_ICG.1(2)	a) もしサポートされていれば、高信頼チャネルを要求するアクションの構成。	a) 無し(アクションの構成は固定)

FMT_MOF.1、FMT_MTD.1(1)、FMT_SMR.1(1)に関し、唯一、管理者パスワードにより認証された管理者だけが管理されており、グループの管理は行っていない。また、FAU_SAR(2)、FMT_MTD.1(2)、FMT_SMR.1(2)に関しても、唯一、保守員パスワードにより認証された保守員だけが管理されており、グループの管理は行っていない。さらに、FAU_SAR.1(1)、及び FMT_MTD.1(3)に関し、管理者パスワードにより認証された管理者、及び保守員パスワードにより認証された保守員だけが管理されており、グループの管理は行っていない。

FMT_SMR.1(1)　セキュリティの役割

下位階層:　なし

依存性:　FIA_UID.1 識別のタイミング

FMT_SMR.1.1(1)　TSF は、役割[割付：*許可された識別された役割*]を維持しなければならない。

[割付：許可された識別された役割]

管理者

FMT_SMR.1.2(1)　TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.1(2)　セキュリティの役割

下位階層:　なし

依存性:　FIA_UID.1 識別のタイミング

FMT_SMR.1.1(2)　TSF は、役割[割付：*許可された識別された役割*]を維持しなければならない。

[割付：許可された識別された役割]

保守員

FMT_SMR.1.2(2)　TSF は、利用者を役割に関連付けなければならない。

6.1.4. クラス FPT： TSF の保護

FPT_STM.1　高信頼タイムスタンプ

下位階層:　なし

依存性:　なし

FPT_STM.1.1　TSF は、高信頼タイムスタンプを提供できなければならない。

6.1.5. クラス FTP： 高信頼パス/チャネル

FTP_ICG.1(1)　TSF 間高信頼チャネルの生成と保証

下位階層:　なし

依存性:　なし

FTP_ICG.1.1(1)　TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別を提供する通信チャネルを提供しなければならない。

[詳細化]

TSF は、それ自身と EP-BB 機能搭載複合機間に、他の通信チャネルと論理的に区別され、ルート証明書及び中間 CA 証明書によるその端点の保証された識別を提供する HTTPS 受信ポートを提供しなければならない。

FTP_ICG.1.2(1)　TSF は、TSF により要請された［割付：*TOE 外のパーツ*］が、TSF 自身とリモート高信頼 IT 製品間の通信チャネルのデータを改変や暴露から保護することを保証しなければ

ならない。

[詳細化]

TSF は、TSF により要請された［割付：*TOE 外のパーツ*］が、TSF 自身と EP-BB 機能搭載複合機間の通信チャネルのデータを改変や暴露から保護することを保証しなければならない。

[割付：TOE 外のパーツ]

.NET Framework 再頒布可能パッケージ

FTP_ICG.1.3(1) TSF は、[選択：*TSF*、*リモート高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択：TSF、リモート高信頼 IT 製品]

リモート高信頼 IT 製品

FTP_ICG.1.4(1) TSF は、[割付：*高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付：高信頼チャネルが要求される機能のリスト]

・HTTPS 通信中継機能

EP 通信データが扱われる。

FTP_ICG.1(2) TSF 間高信頼チャネルの生成と要請

下位階層: なし

依存性: なし

FTP_ICG.1.1(2) TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別を提供する通信チャネルを提供しなければならない。

[詳細化]

TSF は、それ自身と Edge サーバー間に、他の通信チャネルと論理的に区別され、ルート証明書及び中間 CA 証明書によるその端点の保証された識別を提供する HTTPS 送信ポートを提供しなければならない。

FTP_ICG.1.2(2) TSF は、TSF により要請された［割付：*TOE 外のパーツ*］が、TSF 自身とリモート高信頼 IT 製品間の通信チャネルのデータを改変や暴露から保護することを保証しなければならない。

[詳細化]

TSF は、TSF により要請された［割付：*TOE 外のパーツ*］が、TSF 自身と Edge サーバー間の通信チャネルのデータを改変や暴露から保護することを保証しなければならない。

[割付：TOE 外のパーツ]

.NET Framework 再頒布可能パッケージ

FTP_ICG.1.3(2) TSF は、[選択：*TSF*、*リモート高信頼 IT 製品*]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択：TSF、リモート高信頼 IT 製品]

TSF

FTP_ICG.1.4(2) TSF は、[割付：*高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付：高信頼チャネルが要求される機能のリスト]

・HTTPS 通信中継機能

EP 通信データが扱われる。

6.2. セキュリティ保証要件

TOE の評価保証レベルは、EAL2 である。[CC パート 3]に規定されている EAL2 保証パッケージのコンポーネントを以下に示す。

表19 EAL2 保証要件

保証クラス	保証コンポーネント ID	保証コンポーネント	依存性
ADV : 開発	ADV_ARC.1	セキュリティアーキテクチャ記述	ADV_FSP.1 ADV_TDS.1
	ADV_FSP.2	セキュリティ実施機能仕様	ADV_TDS.1
	ADV_TDS.1	基本設計	ADV_FSP.2
AGD : ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス	ADV_FSP.1
	AGD_PRE.1	準備手続き	なし
ALC : ライフサイクルサポート	ALC_CMC.2	CM システムの使用	ALC_CMS.1
	ALC_CMS.2	TOE の一部の CM 範囲	なし
	ALC_DEL.1	配付手続き	なし
ASE : セキュリティターゲット評価	ASE_CCL.1	適合主張	ASE_INT.1 ASE_ECD.1 ASE_REQ.1
	ASE_ECD.1	拡張コンポーネント定義	なし
	ASE_INT.1	ST 概説	なし
	ASE_OBJ.2	セキュリティ対策方針	ASE_SPD.1
	ASE_REQ.2	導き出されたセキュリティ要件	ASE_OBJ.2 ASE_ECD.1
	ASE_SPD.1	セキュリティ課題定義	なし
	ASE_TSS.1	TOE 要約仕様	ASE_INT.1 ASE_REQ.1
ATE : テスト	ATE_COV.1	カバレージの証拠	ADV_FSP.2 ATE_FUN.1
	ATE_FUN.1	機能テスト	ATE_COV.1
	ATE_IND.2	独立テスト・サンプル	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1
AVA : 脆弱性評定	AVA_VAN.2	脆弱性分析	ADV_ARC.1 ADV_FSP.1 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件と TOE セキュリティ対策方針の対応関係をに表 20示す。この表で示す通り、各セ

キュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対抗している。

表 20 セキュリティ機能要件とセキュリティ対策方針の対応関係

TOE セキュリティ対策方針 / セキュリティ機能要件	O.I&A	O.CE_ACCESS	O.EDGE_SERVER_ID	O.EP-BB_DEVICE_ID	O.CH
FAU_GEN.1	○	○	○	○	○
FAU_SAR.1(1)	○	○	○		○
FAU_SAR.1(2)	○	○	○	○	○
FAU_STG.4	○	○	○	○	○
FIA_AFL.1	○				
FIA_SOS.1	○				
FIA_UAU.2	○				
FIA_UID.2	○				
FMT_MOF.1		○			
FMT_MTD.1(1)	○				
FMT_MTD.1(2)	○				
FMT_MTD.1(3)	○				
FMT_MTD.3(1)			○	○	
FMT_MTD.3(2)			○	○	
FMT_MTD.3(3)			○	○	
FMT_SMF.1	○	○			
FMT_SMR.1(1)	○	○			
FMT_SMR.1(2)	○				
FPT_STM.1	○	○	○	○	○
FTP_ICG.1(1)				○	
FTP_ICG.1(2)			○		○

○： 対象のセキュリティ機能要件が対応しているセキュリティ対策方針である事を示す。

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

各セキュリティ対策方針に対し、必要な対策の詳細を分析する。次に、それぞれの対策に対し、要求される機能を示し、それがすべて満たされることでセキュリティ対策方針を実現できることを示す。なお、要求される機能については、一つ以上のセキュリティ機能要件がそれを満たし、セキュリティ対策方針に対する機能要件として必要であることを示す。

O.I&A（利用者の識別認証とアクセス制御）

この TOE セキュリティ対策方針は、正しい利用者が TOE を利用するための、利用者の制限を求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. TOE 利用前に、利用者を識別する。

利用者が TOE を利用する前には、利用を許可されている者であることが識別されなければならない。よって、利用者が識別される前に実行が許可される TSF は、利用者を識別する TSF のみである。

この要件に該当するセキュリティ機能要件は、FIA_UID.2 である。

b. TOE 利用前に、利用者を認証する。
利用者が TOE を利用する前には、利用を許可されている者であることが認証されなければならない。よって、利用者が認証される前に実行が許可されるTSF は、利用者を認証するTSF のみである。この要件に該当するセキュリティ機能要件は、FIA_UAU.2 である。

c. 認証情報の品質を検証する。
識別認証の機能強度を確保するためには、利用者認証情報が、利用者本人以外に予測されることが困難でなければならない。予測されることが困難であるためには、利用者認証情報に対し、必要なレベルの品質を明確に定義し、その品質が満たされていることを検証しなければならない。この要件に該当するセキュリティ機能要件は、FIA_SOS.1 である。

d. 指定回数以内に識別認証に成功しない場合、TOE の利用を拒絶する。
識別認証に失敗した利用者は、TOE の正しい利用者ではないとみなす必要がある。TOE は指定した回数識別認証に失敗した利用者に対し、あらかじめ定義されたアクション（一定期間の拒絶）を実施しなければならない。この要件に該当するセキュリティ機能要件は、FIA_AFL.1 である。

e. 管理者パスワードを改変する機能を管理者に提供する。
管理者だけが、TSF データの管理者パスワードを改変できるように制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD.1(1) 、FMT_SMF.1、及び FMT_SMR.1(1)である。

f. 保守員パスワードを改変する機能を保守員に提供する。
保守員だけが、TSF データの保守員パスワードを改変できるように制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD.1(2)、FMT_SMF.1、及び FMT_SMR.1(2)である。

g. HTTPS 受信ポート番号を改変する機能を管理者及び保守員に提供する。
管理者及び保守員だけが、TSF データの HTTPS 受信ポート番号を改変できるように制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD.1(3)、FMT_SMF.1、FMT_SMR.1(1)、及び FMT_SMR.1(2)である。

h. 利用者の操作を記録し、記録を読み出す機能を管理者と保守員に提供する。
機能を確実に実施する上で侵害事象を検出して責任追跡が行えるように、利用者の識別認証に関する操作、TSF データの改変に関する操作をアクセスログファイルに記録しなければならない。また、管理者と保守員が操作の記録を読み出せなければならない。さらに、操作日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_SAR.1(1)、及び FPT_STM.1 である。

i. ログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。古いログファイルを削除してもログが満杯の場合、監査格納エラー状態（6.1.1の FAU_STG.4 を参照）に移行しシステムログにエラーメッセージを記録しなければならない。また、保守員がシステムログを読み出せなければならない。さらに、日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_STG.4、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

j. 監査レベルとして基本を採用している。TOE では、機能要件 FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FMT_MTD.1(1) 、FMT_MTD.1(2) 、FMT_MTD.1(3)、FMT_SMF.1、FMT_SMR.1(1)、FMT_SMR.1(2)、FPT_STM.1、及び FAU_STG.4 に関し、

表 16に示す監査対象事象について監査記録されることにより、監査レベルとして基本を満たしている。

以上、a、b、c、d、e、f、g、h、i、及びjのすべての対策を満たすことは、O_I&Aを満たすことである。従って、それぞれの対策に必要な機能要件として該当する、FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FMT_MTD.1(1) 、FMT_MTD.1(2) 、FMT_MTD.1(3)、FMT_SMF.1、FMT_SMR.1(1)、FMT_SMR.1(2)、FPT_STM.1、及び FAU_STG.4 の達成により、O.I&A を実現できる。

O.CE_ACCESS（保守員アクセス禁止）

この TOE セキュリティ対策方針は、保守員のアクセスを禁止する機能を、管理者に提供することを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 保守員のアクセスを禁止する機能を管理者に提供する。
管理者だけが、利用者識別認証機能を以下のように改変できなければならない。
保守員ログイン許可：管理者及び保守員を識別認証する。
保守員ログイン不許可：管理者だけを識別認証する。
この要件に該当するセキュリティ機能要件は、FMT_MOF.1、FMT_SMF.1、及び FMT_SMR.1(1)である。

b. 利用者の操作を記録し、記録を読み出す機能を管理者と保守員に提供する。
機能を確実に実施する上で侵害事象を検出して責任追跡が行えるように、利用者識別認証機能の改変操作をしたことをアクセスログファイルに記録しなければならない。また、管理者と保守員が操作の記録を読み出せなければならない。さらに、操作日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_SAR.1(1)、及び FPT_STM.1 である。

c. ログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。また、古いログファイルを削除してもログが満杯の場合、監査格納エラー状態（6.1.1の FAU_STG.4 を参照）に移行しシステムログにエラーメッセージを記録しなければならない。また、保守員がシステムログを読み出せなければならない。さらに、日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_STG.4、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

d. 監査レベルとして基本を採用している。TOE では、機能要件 FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FMT_MOF.1、FMT_SMF.1、FMT_SMR.1(1)、 FPT_STM.1、及び FAU_STG.4 に関し、表 16に示す監査対象事象について監査記録されることにより、監査レベルとして基本を満たしている。

以上、a、b、c、及び d の対策を満たすことは、O.CE_ACCESS を満たすことである。従って、その対策に必要な機能要件として該当する、FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FMT_MOF.1、FMT_SMF.1、FMT_SMR.1(1)、 FPT_STM.1、及び FAU_STG.4 の達成により、O.CE_ACCESS を実現できる。

O.EDGE_SERVER_ID （Edge サーバー識別認証）

この TOE セキュリティ対策方針は、TOE と Edge サーバーとの通信において、TOE が偽 Edge サーバーに EP 通信データを送信しないことを求めている。この要求に対し、必要な対策の詳細と、求められる機能

は以下のとおりである。

a. Edge サーバーとの通信において、保証された識別がされた通信チャネルを提供する。
TOE と Edge サーバーとの通信の際には、通信先の保証された識別が保証されなければならない。また、保証された識別の際に使用される TSF データがセキュアであることを保証しなければならない。これらの要件に該当するセキュリティ機能要件は、FTP_ICG.1(2)、FMT_MTD.3(1) 、FMT_MTD.3(2) 、及び FMT_MTD.3(3)である。

b. Edge サーバーとの通信を記録し、記録を読み出す機能を管理者と保守員に提供する。
機能を確実に実施する上で侵害事象を検出して責任追跡が行えるように、Edge サーバーとの通信において、Edge サーバーの識別認証の結果を通信ログファイルに記録しなければならない。また、管理者と保守員が通信の記録を読み出せなければならない。さらに、通信日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_SAR.1(1)、及び FPT_STM.1 である。

c. ログが満杯(ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下)の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。また、古いログファイルを削除してもログが満杯の場合、監査格納エラー状態(6.1.1の FAU_STG.4 を参照)に移行しシステムログにエラーメッセージを記録しなければならない。また、保守員がシステムログを読み出せなければならない。さらに、日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_STG.4、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

d. 監査レベルとして基本を採用している。TOE では、機能要件 FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FAU_STG.4、FMT_MTD.3(1) 、FMT_MTD.3(2) 、FMT_MTD.3(3)、FPT_STM.1、及び FTP_ICG.1(2)に関し、表 16に示す監査対象事象について監査記録されることにより、監査レベルとして基本を満たしている。

以上、a、b、c、及び d の対策を満たすことは、O.EDGE_SERVER_ID を満たすことである。従って、その対策に必要な機能要件として該当する、FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FAU_STG.4、FMT_MTD.3(1) 、FMT_MTD.3(2) 、FMT_MTD.3(3)、FPT_STM.1、及び FTP_ICG.1(2)の達成により、O.EDGE_SERVER_ID を実現できる。

O.EP-BB_DEVICE_ID (EP-BB 機能搭載複合機識別認証)

この TOE セキュリティ対策方針は、TOE とEP-BB 機能搭載複合機との通信において、TOE が偽 EP-BB 機能搭載複合機から EP 通信データを受信しないことを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. EP-BB 機能搭載複合機との通信において、保証された識別がされた通信チャネルを提供する。
TOE とEP-BB 機能搭載複合機との通信の際には、通信もとの保証された識別が、保証されなければならない。また、保証された識別の際に使用される TSF データがセキュアであることを保証しなければならない。これらの要件に該当するセキュリティ機能要件は、FTP_ICG.1(1)、FMT_MTD.3(1) 、FMT_MTD.3(2) 、及び FMT_MTD.3(3)である。

b. EP-BB 機能搭載複合機との通信を記録し、記録を読み出す機能を保守員に提供する。
機能を確実に実施する上で侵害事象を検出できるように、EP-BB 機能搭載複合機との通信において、EP-BB 機能搭載複合機の識別認証の失敗または通信要求の失敗をシステムログファイルに記

録しなければならない。また、保守員が通信失敗の記録を読み出せなければならない。さらに、通信日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

c. ログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。また、古いログファイルを削除してもログが満杯の場合、監査格納エラー状態（6.1.1の FAU_STG.4 を参照）に移行しシステムログにエラーメッセージを記録しなければならない。また、保守員がシステムログを読み出せなければならない。さらに、日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_STG.4、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

d. 監査レベルとして基本を採用している。TOE では、機能要件 FAU_GEN.1、FAU_SAR.1(2)、FAU_STG.4、FMT_MTD.3(1) 、FMT_MTD.3(2) 、FMT_MTD.3(3)、FPT_STM.1、及び FTP_ICG.1(1)に関し、表 16に示す監査対象事象について監査記録されることにより、監査レベルとして基本を満たしている。

以上、a、b、c、及び d の対策を満たすことは、O.EP-BB_DEVICE_ID を満たすことである。従って、その対策に必要な機能要件として該当する、FAU_GEN.1、FAU_SAR.1(2)、FAU_STG.4、FMT_MTD.3(1) 、FMT_MTD.3(2) 、FMT_MTD.3(3)、FPT_STM.1、及び FTP_ICG.1(1)の達成により、O.EP-BB_DEVICE_ID を実現できる。

O.CH （信頼された通信チャネル）

この TOE セキュリティ対策方針は、TOE と Edge サーバーとの通信において、EP 通信データが漏洩と改ざんから保護されることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 漏洩と改ざんから保護された通信チャネルを提供する。
TOE と Edge サーバーとの通信の際には、EP 通信データが暗号化され、また EP 通信データが改ざんされたことを検知しなければならない。この要件に該当するセキュリティ機能要件は、FTP_ICG.1(2)である。

b. Edge サーバーとの通信に関する情報を記録し、記録を読み出す機能を管理者と保守員に提供する。機能を確実に実施する上で侵害事象を検出して責任追跡が行えるように、Edge サーバーとの通信において、通信に関する情報を通信ログファイルに記録しなければならない。また、管理者と保守員が通信の記録を読み出せなければならない。さらに、通信日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_SAR.1(1)、及び FPT_STM.1 である。

c. ログが満杯（ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下）の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。また、古いログファイルを削除してもログが満杯の場合、監査格納エラー状態（6.1.1の FAU_STG.4 を参照）に移行しシステムログにエラーメッセージを記録しなければならない。また、保守員がシステムログを読み出せなければならない。さらに、日時を正確に記録しなければならない。この要件に該当するセキュリティ機能要件は、FAU_STG.4、FAU_GEN.1、FAU_SAR.1(2)、及び FPT_STM.1 である。

d. 監査レベルとして基本を採用している。TOE では、機能要件 FAU_GEN.1、FAU_SAR.1(1)、

FPT_STM.1、FTP_ICG.1(2)、及び FAU_STG.4 に関し、表 16に示す監査対象事象について監査記録されることにより、監査レベルとして基本を満たしている。

以上、a、b、及び c の対策を満たすことは、O.CH を満たすことである。従って、その対策に必要な機能要件として該当する、FAU_GEN.1、FAU_SAR.1(1)、FAU_SAR.1(2)、FPT_STM.1、FTP_ICG.1(2)、及び FAU_STG.4 の達成により、O.CH を実現できる。

6.3.2. 依存性の検証

セキュリティ機能要件のコンポーネントの依存性を表 21に示す。

表 21 セキュリティ機能要件のコンポーネントの依存性

項番	セキュリティ要件	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされないコンポーネント	妥当性
1	FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし	
2	FAU_SAR.1(1)	FAU_GEN.1	FAU_GEN.1	なし	
3	FAU_SAR.1(2)	FAU_GEN.1	FAU_GEN.1	なし	
4	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 （左記の上位階層）	なし	
5	FAU_STG.4	FAU_STG.1	なし	FAU_STG.1	*1)
6	FIA_SOS.1	なし	なし	なし	
7	FIA_UAU.2	FIA_UID.1	FIA_UID.2 （左記の上位階層）	なし	
8	FIA_UID.2	なし	なし	なし	
9	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.1(1)	なし	
10	FMT_MTD.1(1)	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.1(1)	なし	
11	FMT_MTD.1(2)	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.1(2)	なし	
12	FMT_MTD.1(3)	FMT_SMF.1	FMT_SMF.1	なし	
		FMT_SMR.1	FMT_SMR.1(1) FMT_SMR.1(2)	なし	
13	FMT_MTD.3(1)	FMT_MTD.1	なし	FMT_MTD.1	*2)
14	FMT_MTD.3(2)	FMT_MTD.1	なし	FMT_MTD.1	*2)
15	FMT_MTD.3(3)	FMT_MTD.1	なし	FMT_MTD.1	*2)
16	FMT_SMF.1	なし	なし	なし	
17	FMT_SMR.1(1)	FIA_UID.1	FIA_UID.2 （左記の上位階層）	なし	
18	FMT_SMR.1(2)	FIA_UID.1	FIA_UID.2 （左記の上位階層）	なし	
19	FPT_STM.1	なし	なし	なし	
20	FTP_ICG.1(1)	なし	なし	なし	
21	FTP_ICG.1(2)	なし	なし	なし	

*1)

①通信中継サーバー(PC)の OS からのアクセスについて、OE.SERVER_PC により管理者が使うアカウントのみ OS に登録される。OS のアカウントを制限することにより、通信中継サーバー(PC)への不正ア

クセスが防止されるため、監査記録の不正削除から保護し、不正な改変を防止されているため、FAU_STG.1 への依存は不要である。

②TOE からのアクセスについて、TOE は監査記録の削除、改変のためのインタフェースは提供していないため、監査記録の不正削除から保護及び、不正な改変が防止されているため、FAU_STG.1 への依存は不要である。

*2)TOE が、EP 証明書、中間 CA 証明書、及びルート証明書に対する操作を許可する役割がないため、FMT_MTD.1 への依存は不要である。

セキュリティ保証要件のパッケージの依存性は、EAL2 適合のため依存性を満たす。

6.3.3. セキュリティ保証要件根拠

攻撃者は、高度な専門知識を持たず、管理保守クライアント(PC)の Web ブラウザから TOE の外部インタフェースを使用した攻撃を行う。このため、TOE は、不特定者からの低レベルの攻撃に対抗する必要があり、評価保証レベル EAL2 が妥当といえる。

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述べる。

7.1. TOE セキュリティ機能

表 22に TOE セキュリティ機能とセキュリティ機能要件(SFR)との対応関係について示す。ここで示されるとおり、本節で説明するセキュリティ機能は、表 22に記述される全ての SFR を満たすものである。

表 22 TOE セキュリティ機能とセキュリティ機能要件の対応関係

TOE セキュリティ機能 / セキュリティ機能要件	SF.I&A	SF.LOG	SF.HTTPS
FAU_GEN.1		○	
FAU_SAR.1(1)		○	
FAU_SAR.1(2)		○	
FAU_STG.4		○	
FIA_AFL.1	○		
FIA_SOS.1	○		
FIA_UAU.2	○		
FIA_UID.2	○		
FMT_MOF.1	○		
FMT_MTD.1(1)	○		
FMT_MTD.1(2)	○		
FMT_MTD.1(3)			○
FMT_MTD.3(1)			○
FMT_MTD.3(2)			○
FMT_MTD.3(3)			○
FMT_SMF.1	○		○
FMT_SMR.1(1)	○		○
FMT_SMR.1(2)	○		○
FPT_STM.1		○	
FTP_ICG.1(1)			○
FTP_ICG.1(2)			○

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

7.1.1. 利用者識別認証機能(SF.I&A)

利用者識別認証機能は、TOE にアクセスする利用者(管理者、保守員)を識別認証するための機能を提供する。また、その利用者に応じて TSF データへのアクセスを制限する機能を提供する。さらに、保守員のアクセスを禁止する機能を管理者に提供する。

7.1.1.1. 対応する SFR の実現方法

(1) FIA_UAU.2 アクション前の利用者認証、FIA_UID.2 アクション前の利用者識別

TOE は、利用者の識別認証をWebブラウザからのログイン時に行う。利用者は、あらかじめ定義されている利用者種別(管理者と保守員)を選択し、パスワードを入力する。TOE は、利用者種別(管理者と保守員)とパスワードの組み合わせから、その利用者が正しいと判断した場合にだけ識別認証を成功とする。

上記機能の実装により、FIA_UAU.2 及び FAI_UID.2 を実現する。

(2) FIA_SOS.1 秘密の検証

TOE は、利用者識別認証機能において以下の機能を提供する。

①TOE は、利用者のパスワードが以下の条件を満たしていることを検証する。

・パスワードは、8 文字以上 20 文字以下の、以下の範囲の ASCII 文字が使用できる。

・アルファベットは、半角大文字[A-Z]の 26 文字、半角小文字[a-z]の 26 文字の合計 52 文字(大文字、小文字は区別される。

・数字は、半角で[0-9]の合計 10 文字。

②TOE は、利用者のパスワード変更時において、新たなパスワードとして入力された文字列が上記①の基準を満たさない場合には、新たなパスワードの再入力を要求する。

上記機能の実装により、FIA_SOS.1 を実現する。

(3) FIA_AFL.1 認証失敗時の取り扱い

TOE は、利用者識別認証機能において以下の機能を提供する。

①利用者が入力したパスワードが異なる場合、利用者種別と管理保守クライアント(PC)の IP アドレスの組み合わせ毎に、パスワード誤り回数をカウントする。

②20 秒以内の間隔で連続 3 回認証に失敗すると、1 分間識別認証が拒絶される。

上記機能の実装により、FIA_AFL.1 を実現する。

(4) FMT_MOF.1 セキュリティ機能のふるまいの管理

TOE は、利用者識別認証機能において、識別認証された管理者にだけ、利用者識別認証機能の改変を制限している。管理者は、以下のように、利用者識別認証機能を改変することができる。

保守員ログイン許可:管理者及び保守員を識別認証する。

保守員ログイン不許可:管理者だけを識別認証する。

この機能の実装により、FMT_MOF.1 を実現している。

(5) FMT_MTD.1(1) TSF データの管理

TOE は、利用者識別認証機能において、識別認証された管理者にだけ、管理者パスワードの変更機能を提供する。この機能の実装により、FMT_MTD.1(1)を実現している。

(6) FMT_MTD.1(2) TSF データの管理

TOE は、利用者識別認証機能において、識別認証された保守員にだけ、保守員パスワードの変更機能を提供する。この機能の実装により、FMT_MTD.1(2) を実現している。

(7) FMT_SMF.1 管理機能の特定

TOE は、識別認証された管理者のみが実行できる以下の管理機能を提供する。

①管理者パスワード変更機能

②保守員アクセス可否の変更

TOE は、識別認証された保守員のみが実行できる以下の管理機能を提供する。

①保守員パスワード変更機能

(8) FMT_SMR.1(1) セキュリティの役割

TOE は、利用者識別認証機能において、管理者と識別された利用者に対して、管理者の役割を割り当てている。この機能の実装により、FMT_SMR.1(1)を実現している。

(9) FMT_SMR.1(2) セキュリティの役割

TOE は、利用者識別認証機能において、保守員と識別された利用者に対して、保守員の役割を割り当てている。この機能の実装により、FMT_SMR.1(2)を実現している。

7.1.2. ログ生成/ダウンロード機能(SF.LOG)

ログ生成/ダウンロード機能は、管理者と保守員が管理保守クライアント(PC)の Web ブラウザから TOE を操作する際のアクセスログをファイルに記録する。また、TOE と Edge サーバーとの通信についての通信ログをファイルに記録する。さらに、障害解析用にシステムログをファイルに記録する。

ログ生成/ダウンロード機能はまた、管理保守クライアント(PC)の Web ブラウザからアクセスログと通信ログを管理保守クライアント(PC)にダウンロードする機能を管理者と保守員に提供する。また、システムログを管理保守クライアント(PC)にダウンロードする機能を保守員のみに提供する。

7.1.2.1. 対応する SFR の実現方法

(1) FAU_GEN.1 監査データ生成

TOE は、TOE の起動時に、アクセスログ及び通信ログに、監査機能の起動を示すログを記録する。また、TOE の終了時に、アクセスログ及び通信ログに、監査機能の終了を示すログを記録する。

各監査対象事象が記録される監査記録種別(アクセスログ、通信ログ、システムログ)を表 23に示す。

表 23監査対象事象と監査記録種別との対応

監査対象事象	監査記録種別
・アクセスログ及び通信ログのダウンロード。	アクセスログ
・システムログのダウンロード。	アクセスログ
・監査格納の失敗。	システムログ
・ログインの拒絶。 ・ログインの成功。	アクセスログ
・ログイン(成功・失敗)。	アクセスログ
・保守員アクセス可否の変更。	アクセスログ
・管理者パスワードの変更。	アクセスログ
・保守員パスワードの変更。	アクセスログ
・HTTPS 受信ポート番号の変更。	アクセスログ
・Edge サーバーとの接続。 ・EP 通信データの送信(成功・失敗)。	通信ログ
・EP-BB 機能搭載複合機との接続(失敗)	システムログ

アクセスログ、通信ログ、及びシステムログが記録する監査記録情報を表 24に示す。

表 24 監査記録情報

CC(FAU_GEN.1.2)で要求される監査記録情報	アクセスログ	通信ログ	システムログ
事象の日付・時刻	・操作日時	・通信日時	・日時
事象の種別	・実施された操作	・通信種別	・ログレベル (INFORMATION, ERROR, CRITICAL)

CC(FAU_GEN.1.2)で要求される監査記録情報	アクセスログ	通信ログ	システムログ
サブジェクト識別情報	・利用者種別	・通信元の EP-BB 機能搭載複写機の IP アドレス ・通信先の Edge サーバーの IP アドレス	・モジュール名(ログを出力する内部モジュール名)
事象の結果(成功または失敗)	・操作結果	・通信結果	・内容(エラーコード)
その他の監査関連情報	・管理保守クライアント(PC)の IP アドレス ・社員番号(保守員の場合のみ記録される) ・操作に伴い入力された値	・通信データ量	・内容(エラーメッセージ)

この機能の実装により、FAU_GEN.1 を実現している。

(2) FAU_SAR.1(1)監査レビュー

TOE は、管理者及び保守員だけが、アクセスログ及び通信ログを読み出す機能を提供する。この機能の実装により、FAU_SAR.1(1)を実現している。

(3) FAU_SAR.1(2)監査レビュー

TOE は、保守員だけが、システムログを読み出す機能を提供する。この機能の実装により、FAU_SAR.1(2)を実現している。

(4) FAU_STG.4 監査データ消失の防止

TOE は、ログが満杯(ログを管理しているディレクトリが存在するパーティションの残り容量が 10MB 以下)の場合、古いログファイルを削除し、削除によって空いた領域にログを記録する。また、古いログファイルを削除してもログが満杯の場合、監査格納エラー状態(6.1.1の FAU_STG.4 を参照)に移行しシステムログにエラーメッセージを記録しなければならない。この機能の実装により、FAU_STG.4 を実現している。

(5) FPT_STM.1 高信頼タイムスタンプ

TOE は、ログ生成/ダウンロード機能において、OS から取得した時刻を用いて、アクセスログ、通信ログ、及びシステムログを記録している。この機能の実装により、FPT_STM.1 を実現している。

7.1.3. HTTPS 通信中継機能(SF. HTTPS)

HTTPS 通信中継機能は、TOE が EP-BB 機能搭載複合機と Edge サーバーとの通信を中継する際に、EP-BB 機能搭載複合機と Edge サーバーの識別認証を行う。TOE は、EP-BB 機能搭載複合機の識別認証に成功した場合、EP 通信データを TOE に受信することを許可する。EP 通信データを受信する際は、データを復号する。識別認証に失敗した場合、EP 通信データの受信を許可しない。

TOE は、Edge サーバーの識別認証に成功した場合、EP 通信データを Edge サーバーに送信することを許可する。EP 通信データを送信する際は、データを暗号化する。識別認証に失敗した場合、EP 通信データの送信を許可しない。

また、TOE は、Web ブラウザを介して、HTTPS 通信中継機能において、EP-BB 機能搭載複合機からの通信を受信するための通信ポート番号を設定する機能を管理者及び保守員に提供する。

7.1.3.1. 対応する SFR の実現方法

(1) FTP_ICG.1(1) TSF 間高信頼チャネルの生成と保証、FTP_ICG.1(2) TSF 間高信頼チャネルの生成と保証
TOE は、HTTPS 通信中継機能において、HTTPS 技術を使用して、以下の機能を提供する。

①EP-BB 機能搭載複合機からの SSL ハンドシェイク時に EP-BB 機能搭載複合機から TOE に送られてくる EP 証明書と、TOE に格納されているルート証明書とのパス検証によって、EP-BB 機能搭載複合機から送られてくる EP 証明書の有効性を検証する機能。TOE に格納されている中間 CA 証明書を用いてルート証明書までのパス検証を行うことにより、EP 証明書の有効性の検証を行っている。
②EP-BB 機能搭載複合機から TOE に送られてくる EP 証明書の内容を確認する機能。TOE は、EP 証明書に記載された発行者の組織名を示す項目である O の内容と、サブジェクト名の組織単位を示す項目である OU の内容が既定の値と一致するか確認する。
③EP-BB 機能搭載複合機から TOE に送られてくる EP 証明書が有効ではない場合、通信を許可しない。
④Edge サーバーとの SSL ハンドシェイク時に Edge サーバーから TOE に送られてくる Edge サーバー証明書と、TOE に格納されているルート証明書とのパス検証によって、Edge サーバー証明書の有効性を検証する機能。TOE に格納されている中間 CA 証明書を用いてルート証明書までのパス検証を行うことにより、Edge サーバー証明書の有効性の検証を行っている。
⑤Edge サーバーから TOE に送られてくる Edge サーバー証明書の内容を確認する機能。TOE は、TOE が保持している Edge サーバーの FQDN と、Edge サーバー証明書に記載されたサブジェクト名の CN が一致しているか確認する。
⑥Edge サーバーから TOE に送られてくる Edge サーバー証明書が有効ではない場合、通信を許可しない。
また、TOE は、.NET Framework 再頒布可能パッケージの機能を利用し、チャネルデータを改変や暴露から保護するためにデータを暗号化する機能を提供する。
①、②、及び③の機能の実装により、FTP_ICG.1(1)を実現している。また、④、⑤、及び⑥の機能の実装により、FTP_ICG.1(2)を実現している。

(2) FMT_MTD.3(1)、FMT_MTD.3(2)、及び FMT_MTD.3(3) セキュアな TSF データ
証明書発行サーバーから EP 証明書の発行及び中間 CA 証明書とルート証明書の配布を受ける際に、TOE は HTTPS 技術（サーバー認証）を使用して配布もとを検証する。
①SSL ハンドシェイク時に証明書発行サーバーから TOE に送られる FX プロダクト認証局証明書と、FX 認証局証明書との署名の検証により、FX プロダクト認証局証明書の有効性を検証する。
②TOE は、TOE に格納されている FX 認証局証明書のハッシュ値と、SSL ハンドシェイク時に TOE に送られる FX 認証局証明書のハッシュ値との比較により、TOE に送られてくる FX 認証局証明書の有効性を検証する。
③TOE は、TOE があらかじめ保持している証明書発行サーバーの FQDN と、TOE に送られてくる FX プロダクト認証局証明書に記載されたサブジェクト名の CN が一致しているか確認する。
④FX プロダクト認証局証明書、及び FX 認証局証明書の有効期間が切れていないことを確認する。
TOE は、証明書発行サーバーから発行された EP 証明書について、以下のタイミングで、証明書が存在するか、また現在保持している証明書の有効期間（3 年間）が残り 30 日を切っていないかを検証する。

a) TOE 起動時
b) 毎日 0 時 0 分

c) ネットワーク設定チェックの実行時

これらの機能の実装により、FMT_MTD.3(1)、FMT_MTD.3(2)、及び FMT_MTD.3(3)を実現している。

(3) FMT_MTD.1(3) TSF データの管理

TOE は、利用者識別認証機能において、識別認証された管理者及び保守員にだけ、HTTPS 受信ポート番号設定の変更機能を提供する。この機能の実装により、FMT_MTD.1(3)を実現している。

(4) FMT_SMF.1 管理機能の特定

TOE は、識別認証された管理者及び保守員のみが実行できる以下の管理機能を提供する。

①HTTPS 受信ポート番号変更機能

(5) FMT_SMR.1(1) セキュリティの役割

TOE は、利用者識別認証機能において、管理者と識別された利用者に対して、管理者の役割を割り当てている。この機能の実装により、FMT_SMR.1(1)を実現している。

(6) FMT_SMR.1(2) セキュリティの役割

TOE は、利用者識別認証機能において、保守員と識別された利用者に対して、保守員の役割を割り当てている。この機能の実装により、FMT_SMR.1(2)を実現している。