RICOH

Remote Communication Gate

Type N/L/BN1/BM1

セキュリティターゲット

株式会社リコー　柿井弘、佐藤淳、船木靖、平林治之

2006-06-07

Version 1.03

Document Revision History

Version	Date	Author	Description
0.10	2005-03-04	柿井、平林	初稿
0.11	2005-03-06	柿井、船木、平林	誤字修正
0.12	2005-04-18	佐藤、平林	2.4 TOE の物理的範囲 ・ 内容修正、物理的構成図追加 2.5 TOE の論理的範囲 ・ 内容修正、図 4に保護資産を追加 3.2 前提条件 ・ 一般的利用者への教育と啓蒙の必要性を追加 4.2.1 IT 環境対策方針 ・ ウィルス対策ソフトが導入されていることを追加 4.2.2 非 IT 環境対策方針 ・ 管理者は一般的利用に対して教育と啓蒙活動を行うことを追加 8.1 セキュリティ対策方針根拠 ・ 表 9に A.LAN_USER 追加 ・ A.LAN_USER とOE.ADMIN の根拠追加
0.13	2005-7-19	柿井、佐藤	・ 製品種別の整理 ・ 保護資産の明確化 ・ 前提条件（A），脅威（T），セキュリティ対策方針（O）の対応関係の改定 ・ 関連用語の統一化 ・ TOE の再定義
0.14	2005-8-11	柿井、佐藤	・ 前提条件（A），脅威（T），セキュリティ対策方針（O）の対応関係の見直し ・ OSP 位置付け見直し
0.15	2005-9-6	柿井、佐藤	・ 暗号アルゴリズムの追記
0.16	2005-9-8	柿井、佐藤	・ 構成図の修正 ・ 製品名称のリスト整理
0.17	2005-9-8	船木	8.2.4 セキュリティ機能要件の依存性根拠 ・ 全面見直し 8.2.5 セキュリティ機能要件の相互サポート ・ 追記 5.1 セキュリティ機能要件 ・ FCS_CKM.4 の依存性の記述を修正
0.18	2005-9-12	佐藤、柿井	保護資産、前提条件の修正 FDP_ACF、FCS_COP の修正 インポート情報の追加 TSF データの整理

			根拠の対応表修正
0.19	2005-9-13	佐藤	FCS_COP の修正
0.20	2005-9-26	柿井、佐藤	TOE 名称の修正追加 バージョンの追加 用語統一（復号、HTTPS 方式、SMTP 方式、RC Gate モニタ）
0.21	2005-10-06	柿井、佐藤	脅威の見直しとOSP の追加 用語の統一（Web、TOE、RC Gate） 前提条件と環境セキュリティの修正追加
0.22	2005-10-21	柿井、佐藤	名称・バージョンの統一 FDP_ACF.1 の表追加、関連記述変更 タイムスタンプ記述変更 O.SIGNATURE の記述修正追加 Web のセキュリティ機能からO.CIPHER を除外
0.23	2005-10-26	柿井、佐藤	CC 識別/適合追記 用語統一：LAN 対応型、モデム対応型 T.FAKE_CS 後半記述削除 OE.CS 記述修正 機能強度主張の根拠追記 利用者データと TSF データの整理（FDP_ACF、FMT_MTD）→8章根拠全般修正
0.24	2005-11-04	柿井、佐藤	組織のセキュリティ方針 修正 セキュリティ機能要件（FTP_ITC.1 など）修正 表紙・ヘッダー・フッターの変更
0.25	2005-11-09	柿井、佐藤	8.1.1 セキュリティ機能要件根拠 修正 8.2.1 TOE セキュリティ機能の根拠 修正
0.26	2005-11-24	柿井、佐藤	5.1 章 FCS_CKM、FCS_COP 修正 6.1 章 セキュリティ機能記述 修正 8.1.1 章 セキュリティ機能要件根拠 修正
0.27	2005-11-30	柿井、佐藤、船木	5.1 章: FDP_ACF、FIA_ATD、FIA_UID、FMT_SMF 変更、FMT_MSA 追加、FMT_MOF 削除 6 章: 8.2.1 章への参照を記述 監査ログに関する修正（A.TIME, O.AUDIT, OE.TIME, FMT_MTD.1Ta, FMT_MTD.1Tb, FMT_MTD.1Tc, FAU_GEN.1, FAU_SAR.1, FAU_STG.2, FPT_STM.1, 及び SF.AUDIT の削除。根拠等の修正）
0.28	2005-12-09	柿井、佐藤、船木	UAU.7 修正、保護資産、前提条件、脅威、組織のセキュリティ方針、TOE 要約仕様の整理
0.29	2005-12-14	柿井、佐藤	TOE 記述、前提条件、対策方針、セキュリティ機能要件、TOE 要約仕様、根拠の修正
0.30	2005-12-20	柿井、佐藤	SF 記述及び用語解説整理
0.31	2006-01-06	柿井、佐藤	5 章 FDP_ACF 表の修正

0.32	2006-01-23	柿井、佐藤、船木	5.2 最小機能強度宣言　修正 6.3 機能強度の主張　修正 8.2.2 最小機能強度レベルの根拠　修正 8.3.2 機能強度の主張根拠　修正 5.1　セキュリティ機能要件　修正 FDP_ACF.1、FIA_UAU.6、FTA_MCS.2 6.1　TOE 要約仕様 SF.OPE_I&A、SF.OPE_AC
0.33	2006-01-24	柿井、佐藤	FIA_UAU.6 の記述修正
0.34	2006-01-24	柿井、佐藤	FIA_UAU.6　とそれに基づく記述修正、FTA_MCS.2 から1 への変更、8.3.3 章修正
0.35	2006-01-25	佐藤、柿井	FIA_UAU.6 の修正
0.36	2006-01-26	佐藤、柿井	FMT_MTD.1、FMT_SMF.1　に関して表と記述修正、相互サポートI修正
0.37	2006-01-27	佐藤	6.2 章、8.3.1 章　表・記述よりFIA_UAU.7 部分削除 相互サポートI修正
0.38	2006-02-16	柿井、佐藤	TOE バージョン変更 マニュアルバージョン記述修正
0.39	2006-04-07	柿井、佐藤、船木	保護資産の明確化、前提条件 A.NETWORK の見直し、関連用語の統一と再定義、OSP　記述修正、FTA_MCS.1 の削除
1.00	2006-04-11	柿井、佐藤、船木	脅威の明確化、CE 操作権限の記述追加、正式リリースとしてバージョンを 1.00 に変更
1.01	2006-05-02	柿井、佐藤	A.BROWSER と関連部分の削除。P.ACCESS の内容追加と関連部分の変更
1.02	2006-05-09	柿井、佐藤	P.ACCESS と関連部分の修正。最小機能強度レベルの根拠、保証要件の根拠、の修正
1.03	2006-06-07	柿井、佐藤、船木	SF.OPE_I&A　セッション記述削除。関連文書のバージョン統一。

目　次

List of Figures

List of Tables

1 ST 概説

1.1 ST 識別

ST 名称： Remote Communication Gate TypeN/L/BN1/BM1 セキュリティターゲット

ST バージョン： 1.03

ST 作成日付： 2006-06-07

ST 作成者： 株式会社リコー 柿井弘、佐藤淳、船木靖、平林治之

製品名称： 日本：Remote Communication Gate Type N, Remote Communication Gate Type L
海外：Remote Communication Gate Type BN1, Remote Communication Gate Type BM1
(注)これ以降、上記製品を総称して “RC Gate”とする

TOE 名称： (日本語版)Remote Communication Gate アプリケーションソフトウェア
(英語版)Remote Communication Gate Application Software

TOE バージョン：3.34

評価保証レベル：EAL3

CC 識別： CC バージョン 2.1, ISO/IEC 15408:1999, JIS X 5070:2000;
CCIMB Interpretations-0407

キーワード： 遠隔サービス、画像 I/O 機器、内部ネットワーク、外部ネットワーク、オフィス

1.2 ST 概要

本セキュリティターゲットは、RC Gate のソフトウェアモジュールに関するセキュリティ仕様について説明したものである。RC Gate は主にビジネスオフィスに置かれ、画像 I/O 機器と遠隔サービス監視サーバ "Communication Server (以降 CS)"との仲介機器として利用される。RC Gate が収集したデータは、インターネットまたは電話回線 (ダイアルアップ PPP 接続)経由で信頼される CS に送信される。TOE は RC Gate のソフトウェアモジュールであり、下記のセキュリティ機能が搭載されている。

- RC Gate の設定変更を行うオペレータの識別認証
- オペレータごとのアクセスコントロール
- 直接 CS と通信する時の CS 識別認証とデータ暗号処理
- CS へ電子メールで情報を送信するときのデータ暗号処理

本製品は画像 I/O 機器の保守管理を遠隔サービスで行う重要な1要素となっている。大きく分けて以下の3つのサービスが提供されている。

1. 画像 I/O 機器の遠隔診断保守
   遠隔診断保守では、リコーのカスタマーエンジニア（CE）に画像 I/O 機器の故障である SC（保守サービスを要求する“サービスコール”を表す）を自動通報することができる。また、ファームウェアなどのアップグレードもインターネットを介して遠隔でおこなうことができる。人手による煩雑な作業がなくなる。

2. 定期的な自動カウンター通知
   定期的にコピーカウンターなどを CS に通知することにより、お客様自身がカウンター値を報告する必要がなくなる。この製品の導入により、完全な自動支払請求も可能となるのである。煩雑な作業量が減らされ、支払請求のミスや面倒なルーチンワークも減る。

3.不定期のサプライ（トナーなど）の自動通知
   遠隔診断保守ではトナー残量の通知機能も持っているので、もはや追加注文のための電話をすることもなく、トナーのストック忘れや供給遅れについて心配する必要もない。つまり、在庫管理や発注作業の必要がなくなるのである。

これらの特徴から分かるとおり、画像 I/O 装置と CS との間の通信データは正確に伝わらなければならない。なぜなら、間違いのない課金やサービス業務をおこなうためには、正確な情報伝達が必要になるからである。またインターネットを利用することから、情報漏洩、改ざんに対する適切な防御機能が必要である。RC Gate は仲介機器であるため、このサービスを運用していく上でとても重要な製品である。

1.3 CC 適合の主張

TOE は、機能要件－CC バージョン 2.1 パート2（ISO/IEC 15408-part2:1999(E)）に適合する。

TOE は、保証要件－CC バージョン 2.1 パート3（ISO/IEC 15408-part3:1999(E)）に適合する。

TOE は、CCIMB Interpretations-0407 を適用する。

評価保証レベルは EAL3 に適合する。

本 ST が適合する PP はない。

2 TOE 記述

2.1 製品種別

この製品の種別は、遠隔サービス用仲介機器である。製品名一覧を表 1 に示す。

表 1: RC Gate の製品種別一覧

製品名	仕向地	タイプ	コード
Remote Communication Gate Type N	日本	LAN 対応型	A768-00
Remote Communication Gate Type L	日本	モデム対応型	A769-00
Remote Communication Gate Type BN1	北米	LAN 対応型	A768-17
Remote Communication Gate Type BM1	北米	モデム対応型	A769-17
Remote Communication Gate Type BN1	欧州	LAN 対応型	A768-27
Remote Communication Gate Type BM1	欧州	モデム対応型	A769-27

RC Gate は、オフィスの内部ネットワークからインターネットや電話回線を介して CS とデータの送受信をおこなう LAN 対応型である RC Gate Type N/BN1 の代表的な接続形態を図 1に示す。

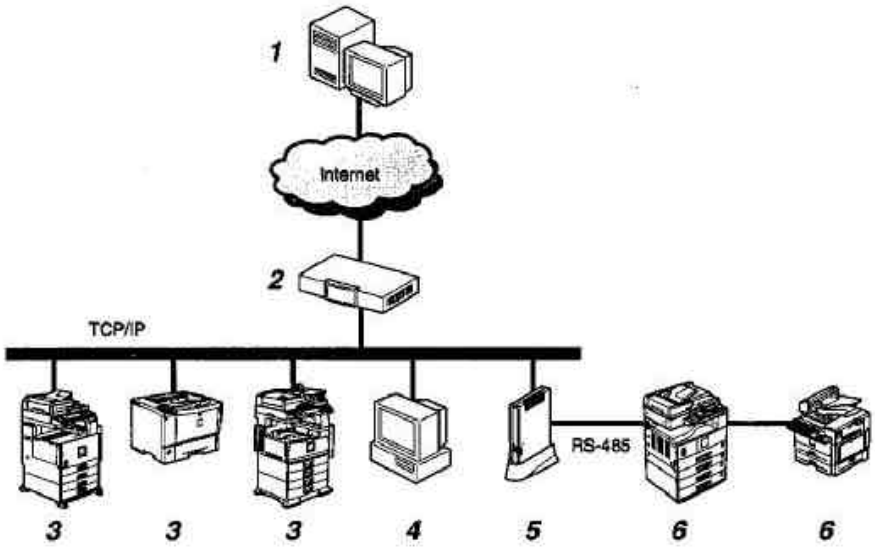


図 1: RC Gate Type N/BN1 の接続形態

以下、図 1の番号にしたがって各機器の役割を説明する。

1. コミュニケーションサーバ
   RC Gate がインターネット経由で通信する監視サーバをこのように呼ぶ。前述のように略称で CS と呼ぶ。
2. プロキシサーバ・ファイアウォール
   オフィスの内部ネットワーク環境を外部ネットワークから保護するためのセキュリティシステム
3. 画像 I/O 機器
   リコーの遠隔サービスをサポートしている画像 I/O 機器、および MIB 機能を有する画像 I/O 機器。
4. RC Gate 用 PC
   Web ブラウザを経由して RC Gate にアクセスするための PC。
5. Remote Communication Gate Type N/BN1
   RC Gate は画像 I/O 機器を管理する仲介機器であり、機器情報を CS に転送したり、CS から機器用のファームウェアをダウンロードしたりする。RC Gate とCS との間の通信方式には 2 通りある。
   1) HTTPS 方式：HTTPS サーバとしての CS と、HTTPS クライアントとしての RC Gate の間でメッセージをやり取りする。
   2) SMTP 方式：SMTP サーバ経由で RC Gate からS/MIME 方式で CS へメッセージを送る。

   * RC Gate Type N は、上記通信方式のうちで HTTPS 方式のみをサポートしているが、RC GateTypeBN1 では上記の通信方式（HTTPS 方式、SMTP 方式）の内どちらか 1 つを利用者が選択して利用する。
6. シリアルバス(RS-485) 経由で管理される画像 I/O 機器
   リコー製の画像 I/O 機器は、シリアルケーブルで RC Gate へ直接接続して管理することも可能である。シリアルでは最大 5 台まで画像 I/O 機器を接続できる。

前述の LAN 対応型のほかに、オフィスの内部ネットワークからインターネットに直接アクセスせず、モデムを利用して電話回線経由で「ダイアルアップ方式」での CS との通信が可能なモデム対応型が RC Gate Type L/BM1 である。ダイアルアップでは、RC Gate 専用の電話回線あるいはファックスとの共用回線を使用する。RC Gate Type L/BM1 の代表的なネットワーク環境を図 2 に示す。

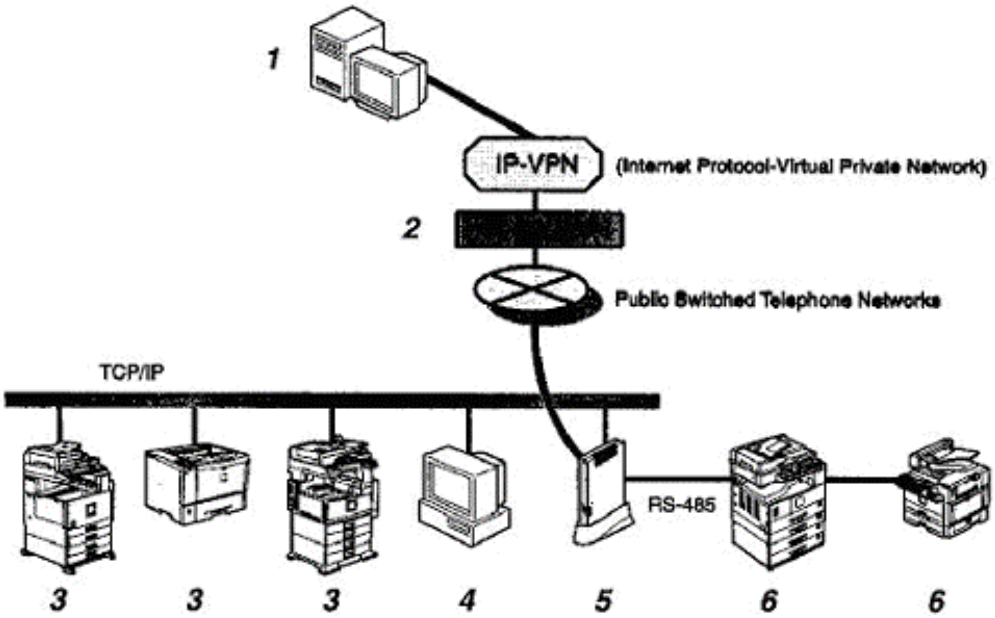


図 2: RC Gate Type L/BM1 の接続形態

1. コミュニケーションサーバ
   RC Gate が通信する監視サーバをこのように呼ぶ。インターネット経由の CS と物理的にも同一である。
2. アクセスポイント
   電話回線でダイアルアップする場合のアクセスポイントである。RC Gate 用のアクセスポイントはプリインストールされて、地域ごとに近いアクセスポイントにアクセスする。
3. 画像 I/O 機器
   リコーの遠隔サービスをサポートしている画像 I/O 機器、および MIB 機能を有する画像 I/O 機器。
4. RC Gate 用 PC
   Web ブラウザを経由して RC Gate にアクセスするための PC。
5. Remote Communication Gate Type L/BM1
   RC Gate は画像 I/O 機器を管理する仲介機器であり、機器情報を CS に転送するが、CS から機器用のファームウェアをダウンロードはしない。RC Gate と CS との間の通信方式は次の 1 通りである。
   1) HTTPS 方式 :HTTPS サーバとしての CS と、HTTPS クライアントとしての RC Gate 間のメッセージをやり取りする。

   RC Gate Type L/BM1 では HTTPS 方式のみサポートされる。
6. シリアルバス(RS-485) 経由で管理される画像 I/O 機器
   リコー製の画像 I/O 機器は、シリアルケーブルで RC Gate へ直接接続して管理することが可能である。シリアルでは最大 5台まで画像 I/O 機器を接続できる。

2.2 RC Gate のオペレータ

本章では TOE のオペレータを示す。オペレータは下記の通りの権限に分かれ、それぞれの権限は明確に分離されている。

1) RC Gate 管理者
RC Gate 管理者は、RC Gate を管理するお客様側の管理者を指す（これ以降、“管理者”という）。管理者は、入力インターフェースを介して RC Gate の各種設定情報に対してアクセスすることができ、プロキシ設定など各種設定が可能である。

2) RC Gate 登録者
RC Gate 登録者は、RC Gate を管理するお客様側の登録者を指す（これ以降、“登録者”という）。登録者は入力インターフェースを介して RC Gate 登録・機器登録をおこない、RC Gate を CS に登録することができる。

3)CE
CE（カスタマーエンジニア）は、RC Gate を取り扱うための教育を受け、RC Gate の設置および障害対応ができることをリコーが認めた、信頼されたカスタマーエンジニアを指す。CE は、お客様の現場で入力インターフェースを介して RC Gate のほとんどの各種設定情報に対してアクセスすることができる。ただし、CE アクセス権限を付与する決定権は、管理者の権限として保有されている。

本書では、管理者、登録者および CE の権限は明確に区別される。RC Gate の権限は、Web 入力インターフェースを介して、TOE の機能であるオペレータの識別及び認証によって区別される。

2.3 その他の関係者

本章では RC Gate に対するその他の関係者を示す。

1) ネットワーク管理者
ネットワーク管理者とは、RC Gate が設置されているお客様の内部ネットワークを管理する IT マネージャなどを指す。

2) RC Gate 責任者
RC Gate 責任者とは、リコー側とお客様側で交わす RC Gate 設置の契約におけるお客様側の責任者を指す。

2.4 RC Gate でのセキュリティの重要性

複写機、ファクシミリまたはプリンタのような画像 I/O 機器は、今日オフィス内 LAN 環境に接続され、多くの IT インフラ情報を保持している。RC Gate が収集する情報には内部ネットワークにどのような機器が接続されているかという情報や RC Gate 管理者メールアドレスといった個人情報が含まれており、このような企業の重要な IT インフラ情報が、インターネットなどの外部ネットワークにおいて不特定多数の目に留まる可能性があることは望ましくない。もちろん外部ネットワークに置かれた偽 CS によってその情報を横取りされることも同様に望ましくない。

また、RC Gate が収集する情報であるコピーやプリントの印刷枚数であるカウンター値は課金処理に使われるため、外部ネットワークで悪意ある者にカウンター値を改ざんされるかもしれないという脅威が存在する。一方、RC Gate は CS から画像 I/O 機器用ファームウェアを受信し、それを該当する画像 I/O 機器に転送することができるが、このファームウェアが外部ネットワーク内で改ざんされ、不正なプログラムを送り込まれる可能性さえある。RC Gate は、これらの外部ネットワークにおいて想定されるセキュリティ脅威を防がなくてはならないのである。

2.5 TOE の物理的範囲

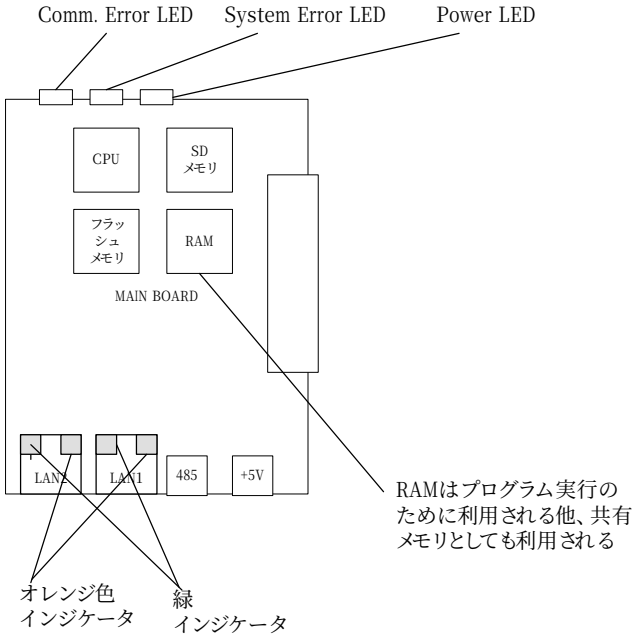
RC Gate は専用筐体で提供される製品で、TOE はその製品にインストールされたアプリケーションソフトウェアである。

RC Gate は、画像 I/O 機器との内部ネットワーク通信、CS との外部ネットワーク通信の仲介機器として動作する。RC Gate は主に一般的な LAN が構築されているオフィスで使用されることを想定している。
RC Gate のハードウェアとしての主要機能はメインボードに集約されている（図 3）。メインボード上には、CPU、フラッシュメモリ、イーサネット回路、RS485、電源ユニットがある。RC Gate Type L/BM1 ではメインボードの他にモデムボードが接続されている。モデムボードは、電話回線インターフェースを持つ。RC Gate のハードウェア詳細は以下の通り。

- CPU :TX4925XB-200
- ROM: 4MB
- RAM: 64MB
- SD メモリ：32MB
- NIC :10Base-T/100Base-TX
- フロント･インジケータ:Power LED(緑)、System Error LED(赤)、Comm. Error LED(オレンジ)
- LAN インジケータ:オレンジ色インジケータ(通信速度 100Mbps の時点灯　10Mbps、未接続のとき消灯)、緑インジケータ(データ送受信時に点灯)

RC Gate Type N/L/BN1/BM1 のソフトウェアは、大きくはアプリケーションソフトとオペレーティングシステム(以降 OS)で構成されている。TOE は、アプリケーションソフトであり、OS は含まない。なお、Type N/L/BN1/BM1 のソフトウェアはすべて共通である。TOE は、ソフトウェア実行プログラムとして SD メモリに格納されている。RC Gate に電源が入れられると、TOE は SD メモリから RAM へとロードされ自動的に起動される。

RC Gate Type N/BN1 (A768-00/17/27)



RC Gate Type L/BM1 (A769-00/17/27)

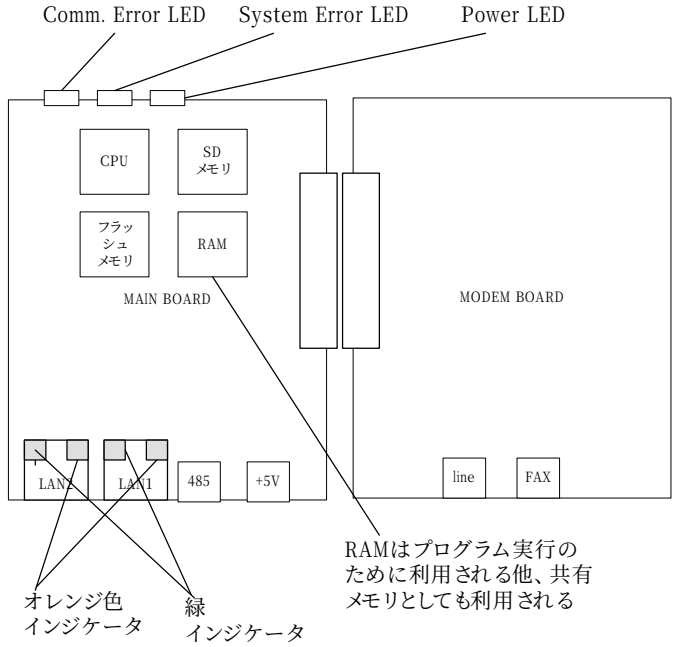


図 3: RC Gate Type N/L/BN1/BM1 の物理構成

2.6 TOE の論理的範囲

RC Gate はハードウェアとソフトウェアで構成されている。ソフトウェア部分は、OS とアプリケーションソフトウェアで構成されている。OS はMontaVista Linux をRC Gate 用にポーティングした組込み Linux であり、RC Gate OS と呼んでいる。OS は TOE の範囲外になる。RC Gate には、オプションで無線 LAN カードが装着できるが、無線 LAN オプション接続時もTOE の範囲外である。

以下、図 4 を参照しながらTOE について機能を説明する。

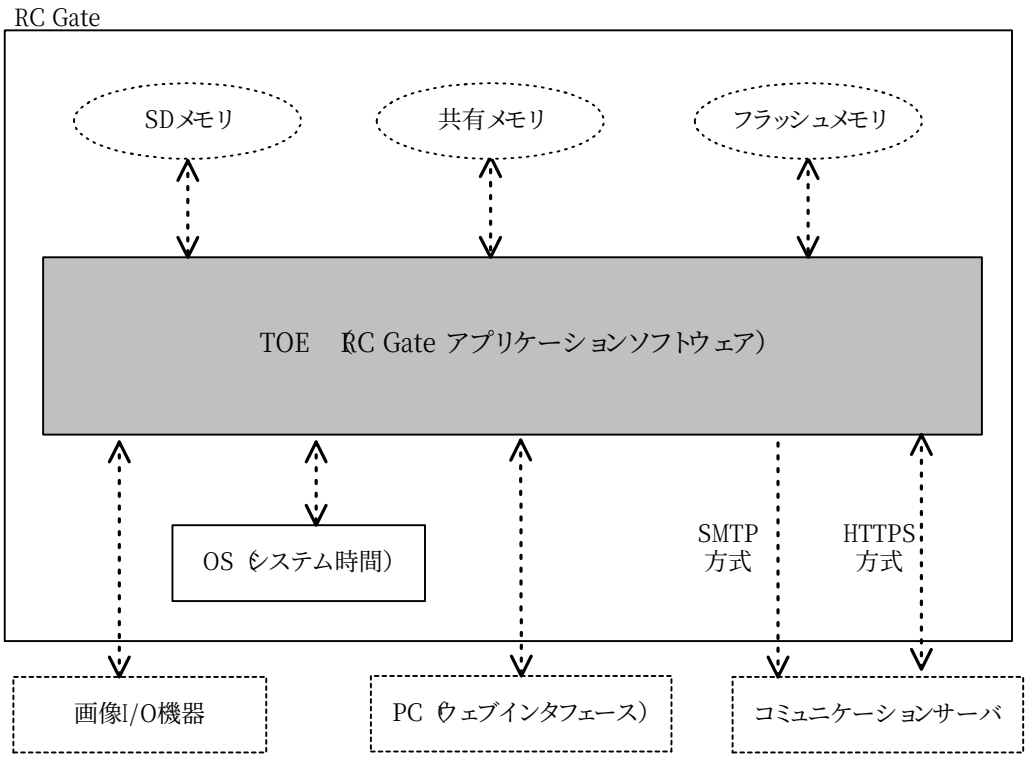
セキュリティ機能としては、アプリケーションソフトウェアが提供しているオペレータ識別認証機能、アクセス制御機能、HTTPS 時の CS 識別認証機能、S/MIME メール送信機能がある。

TOE はオペレータの識別認証及びアクセス制御をウェブインターフェースを介して行う。オペレータの識別認証はオペレータ種別とパスワードの組合せによって実現される。パスワードはTOE 内部の暗号化ライブラリを使用してハッシュ化しSD メモリに保存されている。TOE は識別認証したオペレータ情報を内部メモリに保存し、セッションが継続している間は、保存しているオペレータ情報に基づいて、そのオペレータに割り当てられているアクセス項目にしたがったアクセス制御を行っている。

CS 識別認証は HTTPS 技術を使用して実現している。CS から RC Gate に送られてくる公開鍵証明書と RC Gate が保持するCS ルート証明書を検証することによりTOE は公開鍵証明書の正当性を判断している。また正当であると判断された公開鍵証明書の内容を検証することにより唯一の CS であることも判断している。CS ルート証明書は RC Gate 出荷前に工場で RC Gate のフラッシュメモリに書き込まれており、TOE は RC Gate 起動時にCSルート証明書を共有メモリに展開している。CS への通信開始は、TOE 内部の定期通知スケジューリングあるいは画像 I/O 機器からの故障通報がトリガーとなって行われる。TOE は CS と情報交換する時には、暗号化ライブラリを使用してデータの暗号化と復号を行う。

SMTP 方式による通信では、RC Gate からCS へのメールは S/MIME 形式で転送されるが、このとき必要な CS 公開鍵証明書はアプリケーションソフトウェアに直に書き込まれている。CS への転送開始は、TOE 内部の定期通知スケジューリングがトリガーとなって行われる。送信情報の S/MIME 形式への変換には暗号化ライブラリが使用される。なお、S/MIME メール送信機能は、RC Gate の製品タイプが Type BN1 かつ通信方式が SMTP 方式の場合にのみ有効になる。

非セキュリティ機能であるログの管理機能で、OS のシステム時間をログの時刻情報として利用している。ログファイルは SD メモリに書き込まれ、保存されるログは、アクセスログ、通信ログ、システムログである。



※矢印は、データの流れを示す

図 4: RC Gate Type N/L/BN1/BM1 と TOE

2.7 用語解説

本 ST を明確に理解するため、表 2 で用語の意味を定義する。

表 2: RC Gate 関連用語

用語	定義
管理者	管理者は、RC Gate の管理操作をする権限を与えられている。
登録者	登録者は、RC Gate を CS へ登録する権限が与えられている。
CE	CE（Customer Engineer）は RC Gate の故障時などに点検保守操作する権限が与えられている。CE はリコーまたはリコー関連会社の従業員である。
オペレータ	ここでは管理者、登録者、CE をさす。
ファイアウォール	外部ネットワークから内部ネットワーク資産を保護するためのネットワークサーバのことである。
フラッシュメモリ	ボード上に固定されている不揮発性メモリである。
SD メモリ	セキュアデジタルメモリ(Secure Digital memory)の略。画像 I/O 機器用の情報や RC Gate アプリケーションそのものを保存するために使用されている。

用語	定義
共有メモリ	アプリケーションソフトウェアが利用するボード上に固定されている揮発性メモリである。
画像 I/O 機器	複写機、プリンタ、ファクシミリやそれらの機能をあわせ持つ複合機のなどの総称である。
Linux	フリーウェアで高いポータビリティがある UNIX 互換 OS である。RC Gate では MontaVista Software 社から提供される Linux をもとにポーティングされた RC Gate OS が組込まれている。
MIB	MIB（Management Information Base）は管理情報ベースのことである。RC Gate は MIB をサポートする内部ネットワーク機器から情報を取得することができる。RC Gate は、RFC1156 として規定されている MIB1 を扱う。
外部ネットワーク	RC Gate と CS の通信経路として利用されるインターネットや公衆回線によるネットワークをさす。
内部ネットワーク	RC Gate が設置されているオフィス内のネットワークをさす。通常はイントラネットとして構築されているオフィス内 LAN 環境のこと。
共通鍵	暗号化と復号に同じ鍵を用いる暗号方式の鍵。
PKI	PKI（Public Key Infrastructure）は公開鍵暗号方式のことで、安全な通信のために使用されるデジタルキーテクノロジーのことである。
秘密鍵	秘密鍵は公開鍵と組になっている公開されない鍵のことで、情報を暗号化、解読するために使用する。
公開鍵	公開鍵は通信相手に公開するために使用する。PKI の認証に利用する鍵。
RC Gate	Remote Communication Gate の短縮形。RC Gate は画像 I/O 機器と CS 間の通信仲介機器である。
RS-485	米国電子工業会(EIA)によって標準化された、シリアル通信の規格の一つで、RS-422 の上位規格。 RS-422 が一対複数のマルチドロップ接続に対応した通信規格なのに対し、バス型のマルチポイント接続に対応し、最大で 32 台までの複数対複数接続に対応している。本製品においては、最大 5 台まで画像 I/O 機器を接続できる。
HTTPS	HTTPS は、Web サーバとクライアントがデータを送受信するのに使われるプロトコルである HTTP に、SSL による認証機能、データの完全性保証機能それにデータの暗号化機能を付加している。
S/MIME	S/MIME は、電子メールでのセキュリティを実現するための標準のひとつである。共通鍵暗号方式と公開鍵暗号方式およびハッシュ関数を利用して、電子メールの暗号化と改ざん検知を実現する。

3 TOE セキュリティ環境

3.1 保護資産

TOE が守るべき資産（Asset）は、RC Gate 内の設定情報（RC Gate ネットワーク設定、RC Gate 管理者メールアドレス、RC Gate 通信方式、画像 I/O 機器設定情報）、収集された画像 I/O 機器情報（カウンター値、トナー残量、など）、および画像 I/O 機器用データ（画像 I/O 機器用ファームウェア、画像 I/O 機器用鍵セット）のユーザーデータである。これらには内部ネットワークにどのような機器が接続されているかという情報や RC Gate 管理者メールアドレスといった個人情報が含まれており、このような企業の重要な IT インフラ情報が、インターネットなどの外部ネットワークにおいて漏えいすることは望ましくない。

保護資産に関連して、CS ルート証明書、CS 公開鍵証明書（S/MIME 用）およびオペレータパスワードは TSF データとして RC Gate 内に存在する。

表 3 は上記保護資産とその存在箇所をまとめてある。表 4 は上記 TSF データとその存在箇所をまとめてある。

表 3: 保護資産と RC Gate 内の存在箇所

No.	保護資産	SDメモリ	フラッシュメモリ
1	RC Gate内の設定情報	○	×
2	収集された画像I/O機器情報	○	×
3	画像I/O機器用データ	○	×

○：存在する、×：存在しない

表 4: TSF データと RC Gate 内の存在箇所

No.	TSFデータ	SDメモリ	フラッシュメモリ
1	CSルート証明書	×	○
2	CS公開鍵証明書（S/MIME用）	○	×
3	オペレータパスワード	○	×

○：存在する、×：存在しない

3.2 前提条件

この章では、TOE の前提条件を記述する。

A.PHYSICAL　TOE と保護資産は物理的に保護されていることを想定する。

悪意を持った人間が、そのTOE と保護資産、TSF データに物理的にアクセスすることはないことを想定する。要するに、物理的に TOE や保護資産あるいは TSF データを破壊したり、改ざんしたりできないものとする。また、そのような人が筐体をあけて中のメモリを取り出したりもできないものとする。

A.NETWORK　内部ネットワークは外部ネットワークから守られていることを想定する。

RC Gate と画像I/O機器が動作している内部ネットワークは、インターネットを通して攻撃する外部者から守られているものとする。

A.CE　信頼されたカスタマーエンジニア(CE)は与えられた権限に対する責務を果すことを想定する。

CE は必要な教育を受け、信頼されている。CE はユーザー管理者の許可なしに RC Gate の構成を変更したり、RC Gate を持ち出したり、RC Gate に不必要なプログラムをインストールしないものとする。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用する。また容易に推測できるパスワードは使用しないものとする。

A.ADMIN　信頼された管理者と登録者は与えられた権限に対する責務を果すことを想定する。

管理者と登録者は信頼されている人が担当していることを想定する。管理者と登録者は同じ人であってもよいが、管理者と登録者は RC Gate の構成を設定、変更することができ、RC Gate が正常に動作するように保守するものとする。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用し、すくなくとも6ヶ月に1回は変更するものとする。また容易に推測できるパスワードは使用しないものとする。

A.CS　CS は信頼された会社によって正しく運用されていることを想定する。

CS は信頼された会社によって運営され、その会社は CS を正しく運用保守しているものとする。

3.3 脅威

この章では、TOE またはその環境によって対抗される脅威を記述する。

T.CS_COMM **RC Gate がCS と直接通信するとき、保護資産の情報漏れや不当な変更がインターネットまたは電話回線を介して起こるかもしれない。**

外部ネットワーク上の悪意のある攻撃者はインターネットまたは電話回線に対してプロトコルアナライザを使用し、直接 RC Gate とCS の間で送受信される通信データ（保護資産：RC Gate 内の設定情報、収集された画像 I/O 機器情報、画像 I/O 機器用データ）を盗み見るかもしれない。あるいは、その通信データに変更を加え、送信者が送信したデータとは異なったデータを受信者に受信させるかもしれない。

T.CS_MAIL **RC Gate が CS への通信に電子メールを使用するとき、保護資産の情報漏れや不当な変更がインターネットを介して起こるかもしれない。**

外部ネットワーク上の悪意のある攻撃者はインターネットにおいてプロトコルアナライザを使用し、RC Gate からCS へ送信するメール情報（保護資産：RC Gate 内の設定情報、収集された画像 I/O 機器情報）を盗み見るかもしれない。あるいは、そのメールに変更を加え、送信者が送信したデータとは異なったメールを受信者に受信させるかもしれない。

T.FAKE_CS **偽 CS が立ち上げられて CS になりすまし、RC Gate と通信をし、不正な情報を送りこんだり、あるいは保護資産を盗んだりするかもしれない。**

悪意のある攻撃者は偽 CS を立ち上げ、その偽 CS の管理者はインターネットまたは電話回線を介して、収集された画像 I/O 機器情報などの保護資産を取得するかもしれない。

3.4 組織のセキュリティ方針

この章では、TOE にかかわる組織のセキュリティ方針を記述する。

P.ACCESS **セキュリティ関連機器にアクセスして操作できる人は、その機器を管理する役割を持っているオペレータに制限しなければならない。**

機器を管理する役割をもっている特定のオペレータだけが、TOE にアクセスできるようにしなければならない。CE のアクセスを禁止する機能を、管理者に提供しなければならない。アクセス管理にパスワードを利用し、パスワードポリシーとして SOF-基本を満たす機能強度を持たなければならない。

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

この章では、脅威と組織のセキュリティ方針に対するセキュリティ対策方針を記述する。

O.OPE_I&A **TOE は識別、認証をして TOE データにアクセスできるオペレータを管理することと、CE 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。**

WEB インターフェースを通して TOE にアクセスするとき、TOE はオペレータ (管理者、登録者、CE)を識別し、そのオペレータの役割に応じた RC Gate 内の設定情報にアクセスできることを保証する。TOE は、CE 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。アクセス管理にパスワードを利用し、パスワードポリシーとして SOF-基本を満たす機能強度を持つことを保証する。

O.CS_ID **TOE は、通信相手が正しい CS であることを保証する。**

TOE は CS から送られてくる公開鍵証明書と対応するルート証明書の検証によるその正当性及びその公開鍵証明書の内容チェックにより、正しい CS と通信することを保証する。

O.T_CH **TOE は CS との直接通信時に信頼されるチャネルを作り、データが漏洩しないことと、その完全性を保証する。**

TOE が CS と通信するとき、通信用に信頼されるチャネルを確立する。

O.CIPHER **TOE は CS へのメール送信時に、流れるデータが漏洩しないことを保証する。**

TOE が CS へメールを送るとき、そのメール情報を暗号化し、そのデータが漏洩しないことを保証する。

O.SIGNATURE **TOE は CS への通信時に、データの完全性を保証する。**

TOE が CS へメールを送るとき、メールが改ざんされたことを検出（完全性を保証）するために、ハッシュ値をつけることを保証する。

4.2 環境セキュリティ対策方針

4.2.1 環境セキュリティ対策方針

この章では、3 章で記述した前提あるいは脅威に対する環境のセキュリティ対策方針を記述する。

OE.PHYSICAL　TOE は物理的に保護されていなければならない。

信頼された管理者は悪意を持った人間が RC Gate に物理的にアクセスすることができないように、オープンスペースではない安全な場所に設置しなければならない。

OE.NETWORK　TOE は安全な内部ネットワーク環境で保護されていなければならない。

RC Gate が設置されているオフィスの内部ネットワーク管理は信頼されている人が担当していなければならない。その担当者は、その内部ネットワークが正常に動作していることを監視しなくてはいけない。TOE がインターネットを利用する場合、その担当者は内部ネットワークを外部の攻撃者から保護するために “ファイアウォール ”を設置しなければならない。

OE.CE　TOE は信頼された CE によって保守されなければならない。

CE はリコーまたはリコー関連会社に所属する者で、メンテナンス用ドキュメント (サービスマニュアル) を熟読理解し、適切に RC Gate を保守しなければならない。CE は適切な教育を受け、RC Gate について精通していなければならない。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用しなければならない。また容易に推測できるパスワードは使用してはならない。

OE.ADMIN　TOE は信頼された管理者及び登録者により管理運用されなければならない。

RC Gate 責任者は、信頼のおける人を管理者及び登録者として人選しなければならない。人選された管理者と登録者はユーザーズドキュメント(セットアップガイドとオペレーティングインストラクションあるいは使用説明書)を熟読理解し、適切に RC Gate を管理運用しなければならない。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用し、すくなくとも 6 ヶ月に 1回は変更しなければならない。また容易に推測できるパスワードは使用してはならない。

OE.CS　CS は信頼された会社により正しく運用されていなければならない。

CS が信頼された会社によって運営されるようにリコーは管理会社を選抜し、その会社と契約を結ばねばならない。さらに CS を正しく運用保守していくために管理運用規定を定め、その会社はその運用規定に従って CS 運用を実施しなければならない。

5 IT セキュリティ要件

5.1 TOE セキュリティ機能要件

この章では、セキュリティ対策方針を達成するための、TOE の機能要件を記述する。[CC]で定義された“割付”や“選択”を行った部分は**[ボールド文字と括弧]**で識別し、“詳細化”を行った部分は**ボールド文字と下線**で識別している。また、“繰返し”を行った部分は、例えば、“(a)”というように括弧とアルファベットサフィックスで識別している。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1 TSF は、**[割付: 表 5 に示したサブジェクトとオブジェクト、及びサブジェクトとオブジェクト間の操作のリスト]**に対して**[割付: RC Gate オペレータアクセス制御ポリシー]**を実施しなければならない。

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

表 5: サブジェクトとオブジェクトと操作

サブジェクト	オブジェクト	サブジェクトとオブジェクト間の操作
管理者プロセス	管理者の設定項目（ただし、設定項目には CE 操作権限は含まれない）	閲覧処理と変更処理
登録者プロセス	登録者の設定項目	閲覧処理と変更処理
CE プロセス	CE の設定項目	閲覧処理と変更処理

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1 TSF は、以下の**[割付: 表 6 に示したサブジェクトとオブジェクトのリスト、及び各々に対応するセキュリティ属性]**に基づいて、オブジェクトに対して、**[割付: RC Gate オペレータアクセス制御ポリシー]**を実施しなければならない。

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: **[割付: 以下のルール：**

1. 管理者識別を持つオペレータを代行する管理者プロセスは、管理者に割り当てられた RC Gate 内の設定情報の操作が許可される。

2. 登録者識別を持つオペレータを代行する登録者プロセスは、登録者に割り当てられた RC Gate 内の設定情報の操作が許可される。

3. CE 識別、及び、CE 操作権限を持つオペレータを代行するCE プロセスは、CE に割り当てられた RC Gate 内の設定情報の操作が許可される。

]

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: **[割付: なし]**。

FDP_ACF.1.4 TSF は、**[割付: 追加の規則はなし]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

表 6: サブジェクトとオブジェクトとセキュリティ属性

分類	サブジェクト またはオブジェクト	セキュリティ属性
サブジェクト	管理者プロセス	管理者識別
サブジェクト	登録者プロセス	登録者識別
サブジェクト	CE プロセス	CE 識別、及び、CE 操作権限
オブジェクト	設定項目	設定項目識別

FTP_ITC.1 TSF 間高信頼チャネル

下位階層: なし

FTP_ITC.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及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSF は、**[選択: TSF]**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_ITC.1.3 TSF は、**[割付: 表 7 記載の機能のリスト]**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。

依存性: なし

Note: この要件は、直接通信時のみ適用され、電子メール利用時には適用されない。

表 7: 高信頼チャネルが要求される機能

機能	左記機能にて扱われる情報
CS へのデータエクスポート機能	収集された画像 I/O 機器情報
	RC Gate 内の設定情報
CS からのデータインポート機能	画像 I/O 機器用ファームウェア（プログラム）等の画像 I/O 機器用データ
	RC Gate 内の設定情報

FCS_CKM.1 暗号鍵生成

下位階層: なし

FCS_CKM.1.1 TSF は、以下の**[割付: 表 8 にリストされた 標準)]**に合致する、指定された暗号鍵生成アルゴリズム**[割付: 表 8 にリストされた 暗号生成アルゴリズム)]**と指定された暗号鍵長**[割付: 表 8 にリストされた 鍵長)]**に従って、暗号鍵を生成しなければならない。

依存性: [FCS_CKM.2 暗号鍵配付

または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 8: 暗号鍵生成のリスト

暗号鍵生成	標準	暗号鍵生成アルゴリズム	鍵長
データ暗号鍵の生成	ANSI X9.31	RSA 擬似乱数生成	168 ビット

FCS_COP.1(a) 暗号操作

下位階層: なし

FCS_COP.1.1 TSF は、**[割付: 表 9 にリストされた暗号操作 リストの標準]**に合致する、特定された暗号アルゴリズム**[割付: 表 9 にリストされた暗号アルゴリズム]**と暗号鍵長**[割付: 表 9 にリストされた鍵長]**に従って、**[割付: 表 9 にリストされた暗号操作]**を実行しなければならない。

依存性: **[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**

または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 9: 暗号操作のリスト(1)

暗号操作	標準	暗号アルゴリズム	鍵長
データ暗号化	FIPS PUB 46-3	3DES	168 ビット

FCS_COP.1(b) 暗号操作

下位階層: なし

FCS_COP.1.1 TSF は、**[割付: 表 10 にリストされた暗号操作 リストの標準]**に合致する、特定された暗号アルゴリズム**[割付: 表 10 にリストされた暗号アルゴリズム]**と暗号鍵長**[割付: 表 10 にリストされた鍵長]**に従って、**[割付: 表 10 にリストされた暗号操作]**を実行しなければならない。

依存性: **[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**

または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 10: 暗号操作のリスト(2)

暗号操作	標準	暗号アルゴリズム	鍵長
暗号鍵の暗号化	PKCS#1	RSA	512 ビット

FCS_COP.1(c) 暗号操作

下位階層: なし

FCS_COP.1.1 TSF は、**[割付: 表 11 にリストされた暗号操作 リストの標準]**に合致する、特定された暗号アルゴリズム**[割付: 表 11 にリストされた暗号アルゴリズム]**と暗号鍵長**[割付: 表 11 にリストされた鍵長]**に従って、**[割付: 表 11 にリストされた暗号操作]**を実行しなければならない。

依存性: **[FDP_ITC.1 セキュリティ属性なし利用者データのインポート**

または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

表 11: 暗号操作のリスト(3)

暗号操作	標準	暗号アルゴリズム	鍵長
データのハッシュ	FIPS PUB 180-1	SHA1	N/A

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 TSF は、**[割付: Web を通して間違ったオペレータパスワードの連続的な入力]**に関して、**[割付: 3 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。

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: Web を通してのアクセスを 1 分間拒絶]**しなければならない。

依存性: FIA_UAU.1 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト**[割付: CE 操作権限]**を維持しなければならない。

依存性: なし

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が**[割付: 8 文字以上の ASCII コード (0x20～0x5F, 0x61～0x7A)]**に合致することを検証するメカニズムを提供しなければならない。

依存性: なし

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1

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

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.6 再認証

下位階層: なし

FIA_UAU.6.1 TSF は、条件**[割付:**
1. 管理者による管理者パスワード変更要求時
2. 登録者による登録者パスワード変更要求時
3. CE による CE パスワード変更要求時
]
のもとで利用者を再認証しなければならない。

依存性: なし

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

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

依存性: なし

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1 TSF は、セキュリティ属性**[割付: CE 操作権限]**に対し**[選択:改変]**をする能力を**[割付: 管理者]**に制限するために**[割付: RC Gate オペレータアクセス制御ポリシー]**を実施しなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御

または

FDP_IFC.1 サブセット情報フロー制御]

FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MTD.1(a) TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、**[割付: 管理者パスワード]**を**[選択: 改変]**する能力を**[割付: 管理者]**に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

Note: 各オペレータは、自身のパスワードを保持している。

FMT_MTD.1(b) TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、**[割付: 登録者パスワード]**を**[選択: 改変]**する能力を**[割付: 登録者]**に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

Note: 各オペレータは、自身のパスワードを保持している。

FMT_MTD.1(c) TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、**[割付: CE パスワード]**を**[選択: 改変]**する能力を**[割付: CE]**に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

Note: 各オペレータは、自身のパスワードを保持している。

FMT_SMF.1 管理機能の特定

下位階層：なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:**[割付: 表 12 にリストされたセキュリティ管理機能]**。

依存性：なし

表 12: セキュリティ管理機能

セキュリティ管理機能
管理者による CE アクセス権管理機能
管理者による管理者パスワード変更機能
登録者による登録者パスワード変更機能
CE による CE パスワード変更機能

FMT_SMR.1(a) セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割**[割付: 管理者]**を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1(b) セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割**[割付: 登録者]**を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1(c) セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割**[割付: CE]**を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性: なし

5.2 最小機能強度（SOF）宣言

本 TOE の最小機能強度レベルは SOF-基本である。

確率的、順列的メカニズムを利用する TOE セキュリティ機能要件は

- FIA_SOS.1（秘密の検証）
- FIA_UAU.2（アクション前の利用者認証）
- FIA_UAU.6（再認証）

であり、機能強度レベルは SOF-基本である。

ただし、暗号アルゴリズムの強度は本機能強度の対象としない。

5.3 TOE セキュリティ保証要件

TOE の保証コンポーネントを表 13 に示す。これは評価保証レベル EAL3 で定義されたコンポーネントであり、要件は追加していない。

表 13: TOE セキュリティ保証要件(EAL3)

保証クラス	保証コンポーネント	
構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立ち上げ手順

保証クラス	保証コンポーネント	
開発	ADV_FSP.1	非形式的機能仕様
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト:上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト – サンプル
脆弱性評定	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.4 IT 環境に対するセキュリティ機能要件

TOE の IT 環境が満たすべきセキュリティ機能要件はない。

5.5 IT 環境に対するセキュリティ保証要件

TOE の IT 環境が満たすべきセキュリティ保証要件はない。

6 TOE 要約仕様

6.1 TOE 要約仕様

SF.OPE_I&A

TOE は、オペレータ（管理者、登録者、CE）を識別認証する。TOE は、オペレータの識別認証を Web インターフェースのログイン時に行う。それぞれのオペレータは Web インターフェースからオペレータ選択とパスワード入力を行う。TOE は自身が保持しているオペレータとパスワード情報から、そのオペレータを正しいと判断した場合のみ RC Gate 内情報の閲覧、変更を可能とする。誤ったパスワードが 3 回入力された場合、TOE は Web インターフェースでのアクセスを 1 分間拒否する。

パスワード変更の際、各オペレータの現在のパスワード入力を要求する。新しいパスワードは 8 文字以上の文字コードでなければならず、これを満たさない場合にはパスワード変更を拒否する。

SF.OPE_AC

TOE は、オペレータ（管理者、登録者、CE）の役割に応じて RC Gate 内の設定情報へのアクセス権を与える。ただし、CE 操作権限が"許可しない"に設定されている場合は、TOE は CE に対して RC Gate 内の設定情報へのアクセスを許可しない。TOE は、管理者のみに CE 操作権限の設定を許可する。

SF.CS_HTTPS

CS の認証のために、TOE は HTTPS 認証メカニズムを使用する。TOE は CS から送られてくる公開鍵証明書と対応するルート証明書の検証によるその正当性及びその公開鍵証明書の内容チェックにより、HTTPS で CS とデータ通信する前に、CS の識別、認証を行う。CS の識別、認証が成功したとき、表 14 に示される機能、すなわち、CS へ情報をエクスポートまたは、CS から情報をインポートすることを許可する。識別、認証が失敗したとき、CS 間での情報のエクスポート、インポートを拒否する。

CS 認証が成功したとき、TOE は CS へエクスポートするための情報を暗号化し、CS からインポートされた情報を復号する。

この通信ではハッシュによりデータの完全性を保証する。

なお、TOE は、表 15 にリストされた標準、暗号アルゴリズムと鍵長に従って、暗号操作を行う。また、表 16 にリストされた標準、暗号鍵生成アルゴリズムと鍵長に従って、暗号鍵生成を行う。

表 14: データエクスポート機能とデータインポート機能

機能	左記機能にて扱われる情報
CS へのデータエクスポート機能	収集された画像 I/O 機器情報
	RC Gate 内の設定情報
CS からのデータインポート機能	画像 I/O 機器用ファームウェア（プログラム）等の画像 I/O 機器用データ
	RC Gate 内の設定情報

表 15: 暗号操作のリスト

暗号操作	標準	暗号アルゴリズム	鍵長
データ暗号化	FIPS PUB 46-3	3DES	168 ビット
データ復号	FIPS PUB 46-3	3DES	168 ビット
完全性のための MAC データ生成	FIPS PUB 198	HMAC	N/A
完全性のための MAC データ検証	FIPS PUB 198	HMAC	N/A
鍵交換（鍵の暗号化と復号）	PKCS#1	RSA	512 ビット

表 16: 暗号鍵生成のリスト

暗号鍵生成	標準	暗号鍵生成アルゴリズム	鍵長
データ暗号化鍵の生成	ANSI X9.31	RSA 擬似乱数生成	168 ビット
データ復号鍵の生成	ANSI X9.31	RSA 擬似乱数生成	168 ビット

SF.CS_SMIME

TOE が E-Mail を使用して CS に表 17 に示した情報をエクスポートするとき、TOE は S/MIME によって E-Mail メッセージを暗号化する。TOE は、CS 以外にメッセージを読まれることを防ぐために CS の公開暗号鍵によって、メッセージを暗号化する。
改ざん検知のためのハッシュ値を付加し、メールの完全性を保証する。

なお、TOE は、表 18 にリストされた標準、暗号アルゴリズムと鍵長に従って、暗号操作を行う。また、表 19 にリストされた標準、暗号鍵生成アルゴリズムと鍵長に従って、暗号鍵生成を行う。

表 17: データエクスポート機能

機能	左記機能にて扱われる情報
CS へのデータエクスポート機能	収集された画像 I/O 機器情報
	RC Gate 内の設定情報

表 18: 暗号操作のリスト

暗号操作	標準	暗号アルゴリズム	鍵長
データ暗号化	FIPS PUB 46-3	3DES	168 ビット
データ暗号鍵の暗号化	PKCS#1	RSA	512 ビット
データのハッシュ	FIPS PUB 180-1	SHA1	N/A

表 19: 暗号鍵生成のリスト

暗号鍵生成	標準	暗号鍵生成アルゴリズム	鍵長
データ暗号鍵の生成	ANSI X9.31	RSA 擬似乱数生成	168 ビット

6.2 セキュリティ機能と機能要件との対応関係

表 20 にセキュリティ機能と機能要件との対応関係を示す。表中の「X」は、対応関係にあることを示している。

表 20: 機能要件とセキュリティ機能の対応関係

	SF.OPE_I&A	SF.OPE_AC	SF.CS_HTTPS	SF.CS_SMIME
FDP_ACC.1		X		
FDP_ACF.1		X		
FTP_ITC.1			X	
FCS_CKM.1				X
FCS_COP.1(a)				X
FCS_COP.1(b)				X
FCS_COP.1(c)				X
FIA_AFL.1	X			
FIA_ATD.1		X		
FIA_SOS.1	X			
FIA_UAU.2	X			
FIA_UAU.6	X			
FIA_UID.2	X			
FMT_MSA.1		X		
FMT_MTD.1(a)	X			
FMT_MTD.1(b)	X			
FMT_MTD.1(c)	X			
FMT_SMF.1	X	X		
FMT_SMR.1(a)	X			
FMT_SMR.1(b)	X			

FMT_SMR.1(c)	X			
FPT_RVM.1	X			
FPT_SEP.1		X		

SF.OPE_I&A は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.6、FIA_UID.2、FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_MTD.1(c)、FMT_SMF.1、FMT_SMR.1(a)、FMT_SMR.1(b)、FMT_SMR.1(c)、FPT_RVM.1 の 13 個の機能要件に対応している。

SF.OPE_AC は、FDP_ACC.1、FDP_ACF.1、FIA_ATD.1、FMT_MSA.1、FMT_SMF.1、FPT_SEP.1 の 6 個の機能要件に対応している。

SF.CS_HTTPS は、FTP_ITC.1 の 1 個の機能要件に対応している。

SF.CS_SMIME は、FCS_CKM.1、FCS_COP.1(a)、FCS_COP.1(b)、FCS_COP.1(c)の 4 個の機能要件に対応している。

したがって、各セキュリティ機能は、少なくとも 1 つの機能要件に対応していると言える。

6.3 機能強度の主張

確率的または順列的メカニズムによって実現されるセキュリティ機能は SF.OPE_I&A, SF.CS_HTTPS, SF.CS_SMIME であるが、SOF レート付け対象はパスワードメカニズムである SF.OPE_I&A とし、SF.CS_HTTPS とSF.CS_SMIME は暗号化メカニズムにより実現されているので除外する。
SF.OPE_I&A の機能強度は SOF-基本である。

6.4 保証手段

以下のドキュメントを保証手段として提供する。

Remote Communication Gate TypeN/L/BN1/BM1 セキュリティターゲット
Version 1.03, 2006-06-07

Remote Communication Gate TypeN/L/BN1/BM1 機能仕様書
Version 0.23, 2006-04-11

Remote Communication Gate TypeN/L/BN1/BM1 上位設計書
Version 0.16, 2006-04-11

Remote Communication Gate TypeN/L/BN1/BM1 表現対応書
Version 0.15, 2006-04-11

Remote Communication Gate TypeN/L
安全上のご注意、セットアップガイド
A768-8559, 2006-01-31

Remote Communication Gate TypeN/L
使用説明書
A768-8558, 2006-02-08

Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (European version)
A768-8603B, 2006-01-30

Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (North American version)
A768-8605B, 2006-01-31

Remote Communication Gate Type BN1/BM1 Operating Instructions (European version)
A768-8604B, 2006-02-03

Remote Communication Gate Type BN1/BM1 Operating Instructions (North American version)
A768-8606B, 2006-02-03

Remote Communication Gate TypeN/L/BN1/BM1 テスト文書
Version 0.19, 2006-04-11

Remote Communication Gate TypeN/L/BN1/BM1 機能強度分析書
Version 0.11, 2006-03-08

Remote Communication Gate TypeN/L/BN1/BM1 脆弱性分析書
Version 0.14, 2006-03-16

Remote Communication Gate TypeN/L/BN1/BM1 構成管理
Version 0.21, 2006-04-11

Remote Communication Gate TypeN/L/BN1/BM1 構成リスト
Version 0.20, 2006-06-07

Remote Communication Gate TypeN/L/BN1/BM1 開発セキュリティ
Version 0.14, 2005-12-15

Remote Communication Gate TypeN/L/BN1/BM1 配付
Version 0.11, 2005-11-28

Remote Communication Gate TypeN/L/BN1/BM1 設置、生成、及び立ち上げ書
Version 0.11, 2005-11-01

Remote Communication Gate TypeN/L/NB/LB サービスマニュアル
Version 1.3, 2006-02-08

Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL
1.0 revised, 2005-05-24 & Technical Bulletin No.RA768002, 2006-02-07

7 PP 主張

本 ST において適合する PP はない。

8 根拠

8.1 セキュリティ対策方針根拠

この章では、4 章で記述されたセキュリティ対策方針が、3 章のセキュリティ環境で識別されたすべての側面にまで辿れることができ、かつそれを網羅することを実証する。

表 21 に、それぞれのセキュリティ対策方針が少なくとも1つの脅威か前提を対応していることと、それぞれの脅威または前提が少なくとも1つのセキュリティ対策方針によって対抗あるいは実現されていることを示す。

表 21: セキュリティニーズとセキュリティ対策方針の対応

	O.OPE_I&A	O.CS_ID	O.T_CH	O.CIPHER	O.SIGNATURE	OE.PHYSIAL	OE.NETWORK	OE.CE	OE.ADMIN	OE.CS
T.CS_COMM			X							
T.CS_MAIL				X	X					
T.FAKE_CS		X								
P.ACCESS	X									
A.PHYSICAL						X				
A.NETWORK							X			
A.CE								X		
A.ADMIN									X	
A.CS										X

T.CS_COMM は O.T_CH で対抗できる。なぜなら、TOE とCS 間の通信データは O.T_CH によって確保されるからである。

T.CS_MAIL は O.CIPHER、O.SIGNATURE で対抗できる。なぜなら、CS に送られるメール情報が O.CIPHER によって暗号化されることを保証するからである。暗号化されたメール情報は、CS の秘密鍵によってのみ復号される。また、O.SIGNATURE の改ざん検知のためのハッシュ値により、不当な変更を検出できる。

T.FAKE_CS は O.CS_ID で対抗できる。なぜなら、TOE は CS から送られてくる公開鍵証明書と対応するルート証明書の検証によるその正当性と有効期限確認及びその公開鍵証明書の内容チェックにより、正しい CS と通信することを保証するからである。

P.ACCESS は O.OPE_I&A で実施できる。なぜなら、O.OPE_I&A によりオペレータ（管理者、登録者、CE）をパスワードで認証することにより、特定のオペレータだけが操作するようなポリシーとなるからである。また、管理者に CE 操作権限を提供することにより、CE のアクセスを禁止する機能を、管理者が保有するポリシーとなるからである。さらに、アクセス管理にパスワードを利用し、SOF-基本を満たす機能強度を保つパスワードポリシーとなるからである。

A.PHYSICAL は OE.PHYSICAL で実現できる。なぜなら、記憶媒体およびその中に保存された保護資産が外部の悪意ある人間から守られることを保証するからである。

A.NETWORK は OE.NETWORK で実現できる。なぜなら、内部ネットワークが正常に機能し、その LAN 環境がファイアウォールによって外部攻撃から守られることを保証するからである。

A.CE は OE.CE で実現できる。なぜなら、ユーザーが適切なディーラーに修理を委託してから信頼された CE が RC Gate の保守を行うことを保証するからである。CE はリコーから認定された人物または適切な業者であり、RC Gate を正しい状態に保つために尽力する。

A.ADMIN は OE.ADMIN で実現できる。なぜなら、管理者及び登録者はユーザーズマニュアルを熟読理解し RC Gate の保守管理を適切に行うことができるからである。

A.CS は OE.CS で実現できる。なぜなら、CS が信頼された会社によって運営されるようにリコーは管理会社を選抜し、その会社と契約を結ぶからである。さらに CS を正しく運用保守していくために管理運用規定を定め、その会社はその運用規定に従って CS 運用を実施するからである。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ機能要件根拠

この章では、セキュリティ機能要件がセキュリティ対策方針を達成することを実証する。環境セキュリティ対策方針の中で、OE.NETWORK、OE.PHYSICAL、OE.CE、OE.ADMIN、OE.CS は運用に対するものである。表 22 に、TOE セキュリティ機能要件が TOE のセキュリティ対策方針を実証することを示す。

表 22: セキュリティ対策方針と機能要件の対応

	FDP_ACC.1	FDP_ACF.1	FTP_ITC.1	FCS_CKM.1	FCS_COP.1(a)	FCS_COP.1(b)	FCS_COP.1(c)	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2	FIA_UAU.6	FIA_UID.2	FMT_MSA.1	FMT_MTD.1(a)	FMT_MTD.1(b)	FMT_MTD.1(c)	FMT_SMF.1	FMT_SMR.1(a)	FMT_SMR.1(b)	FMT_SMR.1(c)	FPT_RVM.1	FPT_SEP.1
O.OPE_I&A	X	X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
O.CS_ID			X																				
O.T_CH			X																				
O.CIPHER				X	X	X																	
O.SIGNATURE							X																

O.OPE_I&A は、FDP_ACC.1、FDP_ACF.1、FIA_AFL.1、FIA_ATD.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.6 、FIA_UID.2 、FMT_MSA.1 、FMT_MTD.1(a) 、FMT_MTD.1(b) 、FMT_MTD.1(c) 、FMT_SMF.1、FMT_SMR.1(a)、FMT_SMR.1(b)、FMT_SMR.1(c)、FPT_RVM.1、FPT_SEP.1 で達成できる。

なぜなら、

FDP_ACC.1 によって、オペレータのアクセス制御を行い認証されたオペレータのみが TOE データにアクセスできることを保証し、

FDP_ACF.1 によって、各アクセス権限が付与されたオペレータが実行できる操作とその操作対象となるオブジェクトが管理されており、

FIA_AFL.1 によって、連続する認証失敗を検出し、失敗が 3 回に達するとアクセス拒絶を行い

FIA_ATD.1 によって、サービス（CE）によるアクセス制御を維持しており

FIA_SOS.1 によって、認証に使われるパスワードは 8 文字以上の ASCII コード（0x20～0x5F,0x61～0x7A）に合致しており、

FIA_UAU.2 によって、認証されていない人物は TOE にアクセスできないことを保証し、

FIA_UAU.6 によって、パスワード変更の際、各オペレータの再認証を行い、

FIA_UID.2 によって、利用者識別をしなければ TOE データにアクセスできないことを保証し、

FMT_MSA.1 によって、CE 操作権限の可否を管理する能力を管理者に制限しており、

FMT_MTD.1(a)によって、管理者パスワードを改変する能力を管理者に制限しており、

FMT_MTD.1(b)によって、登録者パスワードを改変する能力を登録者に制限しており、

FMT_MTD.1(c)によって、CE パスワードを改変する能力を CE に制限しており、

FMT_SMF.1 によって、表 12 に示したセキュリティ管理要件が管理され、

FMT_SMR.1(a)によって、役割（管理者）が維持管理され、

FMT_SMR.1(b)によって、役割（登録者）が維持管理され、

FMT_SMR.1(c)によって、役割（CE）が維持管理される、

からである。

上記の機能は、FPT_RVM.1 によりTSP がバイパスされることがなく、また FPT_SEP.1 によりセキュリティドメインを分離および維持することで、他の信頼できないサブジェクトによる干渉や改ざんから保護することにより満足される。

O.CS_ID は FTP_ITC.1 で達成できる。

なぜなら、

FTP_ITC.1 によって、TOE とCS 間の通信において CS 識別を提供する通信チャネルを提供し、TOE が偽 CS に接続することはない、

からである。

O.T_CH は FTP_ITC.1 で達成できる。

なぜなら、

FTP_ITC.1 によって、TOE とCS 間の通信において通信用に信頼されるチャネルを確立し、通信データは暗号化され、また、流れるデータが改ざんされたことを検出（完全性を保証）する、

からである。

O.CIPHER は FCS_CKM.1、FCS_COP.1(a)、FCS_COP.1(b)で達成できる。

なぜなら、

FCS_CKM.1 によって、TOE はメールデータ暗号鍵の生成を行い、

FCS_COP.1(a)によって、メールデータの暗号化を行い、

FCS_COP.1(b)によって、メールデータ暗号鍵の暗号化を行う

からである。

O.SIGNATURE は FCS_COP.1(c)で達成できる。

なぜなら、

FCS_COP.1(c)によって、通信データのハッシュ値を生成する、

からである。

8.2.2 最小機能強度レベルの根拠

本 TOE は，商用製品であり、画像 I/O 機器の遠隔サービスを行うための保守用ソフトウェアである。TOE はオフィス環境に設置され、外部ネットワークを介して画像 I/O 機器用データを CS に送信する。RC Gate が設置されるオフィス環境においては、組織のセキュリティ方針に基づき、SOF-基本の機能強度を実現する。また、RC Gate は画像 I/O 機器の保守管理データだけを扱い、お客様の金銭的な資産を直接管理することはないので、外部ネットワークにおいても中レベル以上の攻撃者は存在せず攻撃力は “低レベル ”である。以上のことから、TOE の最小機能強度レベルとして SOF-基本は妥当である。

8.2.3 保証要件の根拠

RC Gate は画像 I/O 機器から送られるデータだけを管理し、金銭的な資産を直接管理することはないため、TOE に対して過度な保護メカニズムが要求されるものではないが、TOE 開発段階のセキュリティ対策の分析により、セキュリティ機能の実装における保証をカバーすることは重要であると、リコーは考えている。セキュリティ機能の機能仕様と上位レベル設計に基づく開発者テストの実施と分析、すなわち上位レベル設計評価(ADV_HLD.2)はその正確さを示すのに充分である。明白な脆弱性の分析(AVA_VLA.1)は一般的なニーズにとって充分である。開発環境や開発成果物の管理に関する評価による開発セキュリティ(ALC_DVS.1) からもセキュリティの確かさを得ることが重要である。上述の理由により、本 TOE に対する EAL3 の評価保証レベルは妥当である。

8.2.4 セキュリティ機能要件の依存性根拠

セキュリティ機能要件の依存性根拠について表 23 に記す。下表は、TOE セキュリティ機能要件が依存するセキュリティ要件とそれをカバーする TOE セキュリティ機能要件の項番を記す。依存性が満たされていないものは、その根拠を表の下で説明する。

表 23: セキュリティ機能要件の依存性

項番	TOE セキュリティ機能要件	依存するセキュリティ要件	参照先項番
1	FDP_ACC.1	FDP_ACF.1	2
2	FDP_ACF.1	FDP_ACC.1	1
		FMT_MSA.3	不要 :下記(1)参照
3	FTP_ITC.1	なし	―
4	FCS_CKM.1	FCS_CKM.2 または FCS_COP.1	5
		FCS_CKM.4	不要 :下記(2)参照
		FMT_MSA.2	不要 :下記(2)参照
5	FCS_COP.1(a)	FDP_ITC.1 または FCS_CKM.1	4
		FCS_CKM.4	不要 :下記(3)参照
		FMT_MSA.2	不要 :下記(3)参照
	FCS_COP.1(b)	FDP_ITC.1 または FCS_CKM.1	不要 :下記(4)参照
		FCS_CKM.4	不要 :下記(4)参照
		FMT_MSA.2	不要 :下記(4)参照
	FCS_COP.1(c)	FDP_ITC.1 または FCS_CKM.1	不要 :下記(5)参照
		FCS_CKM.4	不要 :下記(5)参照
		FMT_MSA.2	不要 :下記(5)参照
6	FIA_AFL.1	FIA_UAU.1	9
7	FIA_ATD.1	なし	―

8	FIA_SOS.1	なし	―
9	FIA_UAU.2	FIA_UID.1	11
10	FIA_UAU.6	なし	―
11	FIA_UID.2	なし	―
12	FMT_MSA.1	FDP_ACC.1 または FDP_IFC.1	1
		FMT_SMF.1	14
		FMT_SMR.1	15
13	FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c)	FMT_SMF.1	14
		FMT_SMR.1	15
14	FMT_SMF.1	なし	―
15	FMT_SMR.1(a) FMT_SMR.1(b) FMT_SMR.1(c)	FIA_UID.1	11
16	FPT_RVM.1	なし	―
17	FPT_SEP.1	なし	―

(1) **FDP_ACF.1 からFMT_MSA.3 への依存性が満たされないことの根拠**
TOE の設定情報へのアクセスは、管理者、登録者、CE に限られているため、これを変更することはできない。したがって、FMT_MSA.3 は不要である。

(2) **FCS_CKM.1 からFCS_CKM.4、FMT_MSA.2 への依存性が満たされないことの根拠**
TOE からCS へのメールデータは、TOE が生成した暗号鍵で暗号化される。この暗号鍵のライフサイクルは、CS へメール送信を行うときに暗号鍵生成と暗号操作となっており、送信のたびに暗号鍵を生成するので、長期的に維持管理する必要とセキュアなセキュリティ属性を必要としない。したがって、FMT_MSA.2 は不要である。また、暗号鍵は CS へ配布されるが、その際 FCS_COP.1(b)にて暗号化されて配布する。そして、CS以外への配布や置き換えたりする処理が存在しないため FCS_CKM.4 も不要である。

(3) **FCS_COP.1(a)からFCS_CKM.4、FMT_MSA.2 への依存性が満たされないことの根拠**
上記(2)記載内容と同等の理由により、FMT_MSA.2 とFCS_CKM.4 も不要である。

(4) **FCS_COP.1(b)から[FDP_ITC.1 または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2 への依存性が満たされないことの根拠**
メールデータ暗号鍵の暗号化に関して、暗号鍵の生成、管理に関する[FDP_ITC.1 または FCS_CKM.1]、FMT_MSA.2 は、RC Gate の使用過程ではなく製造過程において実現されているため、これらの依存関係は不要である。また、ここで対象となっている鍵は CS の公開鍵証明書であるため TOE が破棄する必要はなくFCS_CKM.4 も不要である。

(5) **FCS_COP.1(c)から[FDP_ITC.1 または FCS_CKM.1]、FCS_CKM.4、FMT_MSA.2 への依存性が満たされないことの根拠**
FCS_COP.1(c)はメールデータのハッシュであり、暗号鍵を利用しないため、暗号鍵の生成、廃棄、鍵のセキュリティ属性のような鍵管理の必要はなく[FDP_ITC.1 または FCS_CKM.1]、FMT_MSA.2、FCS_CKM.4 の機能要件は不要である。

8.2.5 セキュリティ機能要件の相互サポート

以下で、セキュリティ機能要件の相互サポートについて検証する。

表 24: セキュリティ機能要件の相互サポート

項番	機能要件	迂回	干渉	非活性化
1	FDP_ACC.1	N/A	N/A	N/A
2	FDP_ACF.1	FIA_UAU.2	FMT_MSA.1 FPT_SEP.1	N/A
3	FTP_ITC.1	N/A	N/A	N/A
4	FCS_CKM.1	N/A	N/A	N/A
5	FCS_COP.1(a)	N/A	N/A	N/A
6	FCS_COP.1(b)	N/A	N/A	N/A
7	FCS_COP.1(c)	N/A	N/A	N/A
8	FIA_AFL.1	N/A	N/A	N/A
9	FIA_ATD.1	N/A	N/A	N/A
10	FIA_SOS.1	N/A	N/A	N/A
11	FIA_UAU.2	FPT_RVM.1	FMT_MTD.1(a), FMT_MTD.1(b) FMT_MTD.1(c)	N/A
12	FIA_UAU.6	FPT_RVM.1	N/A	N/A
13	FIA_UID.2	N/A	N/A	N/A
14	FMT_MSA.1	N/A	N/A	N/A
15	FMT_MTD.1(a)	N/A	N/A	N/A
16	FMT_MTD.1(b)	N/A	N/A	N/A
17	FMT_MTD.1(c)	N/A	N/A	N/A
18	FMT_SMF.1	N/A	N/A	N/A
19	FMT_SMR.1(a)	N/A	N/A	N/A
20	FMT_SMR.1(b)	N/A	N/A	N/A
21	FMT_SMR.1(c)	N/A	N/A	N/A

22	FPT_RVM.1	N/A	N/A	N/A
23	FPT_SEP.1	N/A	N/A	N/A

[迂 回]

FDP_ACF.1 は、ただひとつのオペレータが識別認証されている必要があるが、これは FIA_UAU.2 により実施される。

FIA_UAU.2 は、オペレータが Web で設定項目を操作する前に実施されなければならないが、これは FPT_RVM.1 により実施される。

FIA_UAU.6 は、オペレータがパスワードを変更する前に実施されなければならないが、これは FPT_RVM.1 により実施される。

[干 渉]

FDP_ACF.1 は、サブジェクトまたはオブジェクトのセキュリティ属性によってアクセス制御を行うが、サブジェクトまたはオブジェクトのセキュリティ属性のうち改変可能なのは CE 操作権限のみである。CE 操作権限へのアクセスは FMT_MSA.1 によって管理者に制限されており干渉から保護される。また、セキュリティドメインを分離および維持することで、他の信頼できないサブジェクトによる干渉や改ざんから保護することにより満足されるが、これは FPT_SEP.1 で保証される。

FIA_UAU.2 は、管理者、登録者、CE に割り当てられたオペレータ以外が設定項目を操作するのを防ぐためにパスワードによる認証を行っている。FMT_MTD.1(a)、FMT_MTD.1(b)、FMT_MTD.1(c)はパスワードの変更を管理者、登録者、CE のそれぞれに制限することでパスワードを不正な変更から保護している。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能の根拠

この章では、セキュリティ機能がセキュリティ機能要件を実現することを実証する。

表 25 に、それぞれの TOE セキュリティ機能が少なくとも 1つの TOE セキュリティ機能要件を保証していることと、それぞれの TOE セキュリティ機能要件が少なくとも 1つのセキュリティ機能によって保証されていることを示す。

表 25: 機能要件とセキュリティ機能の対応

	SF.OPE_I&A	SF.OPE_AC	SF.CS_HTTPS	SF.CS_SMIME
FDP_ACC.1		X		
FDP_ACF.1		X		

FTP_ITC.1			X	
FCS_CKM.1				X
FCS_COP.1(a)				X
FCS_COP.1(b)				X
FCS_COP.1(c)				X
FIA_AFL.1	X			
FIA_ATD.1		X		
FIA_SOS.1	X			
FIA_UAU.2	X			
FIA_UAU.6	X			
FIA_UID.2	X			
FMT_MSA.1		X		
FMT_MTD.1(a)	X			
FMT_MTD.1(b)	X			
FMT_MTD.1(c)	X			
FMT_SMF.1	X	X		
FMT_SMR.1(a)	X			
FMT_SMR.1(b)	X			
FMT_SMR.1(c)	X			
FPT_RVM.1	X			
FPT_SEP.1		X		

FDP_ACC.1

FDP_ACC.1 は、SF.OPE_AC によりアクセスリストに基づくアクセス制限が成されるため満足される。

FDP_ACF.1

FDP_ACF.1 は、SF.OPE_AC によりオペレータ毎にアクセスできる情報を制御しているため満足される。

FTP_ITC.1

FTP_ITC.1 は、SF.CS_HTTPS によりRC Gate とCS 間の通信は、HTTPS 方式によって通信していることにより満足される。

FCS_CKM.1

FCS_CKM.1 は、SF.CS_SMIME においてデータを暗号化するために RSA 擬似乱数生成にて 168 ビットの 3DES 用暗号鍵を生成しているため満足される。

FCS_COP.1(a)

FCS_COP.1(a)は、SF.CS_SMIME によりCS に送信する情報を暗号化することによって満足される。

FCS_COP.1(b)

FCS_COP.1(b)は、SF.CS_SMIME により暗号鍵をCS に送信する際に RSA で暗号化しているため満足される。

FCS_COP.1(c)

FCS_COP.1(c)は、SF.CS_SMIME によりデータのハッシュに使用することによって満足される。

FIA_AFL.1

FIA_AFL.1 はSF.OPE_I&A によりオペレータパスワードの入力を3回連続で失敗した場合、TSF は 1分間アクセスを拒否することにより満足される。

FIA_ATD.1

FIA_ATD.1 は、SF.OPE_AC で満足される。なぜなら、CE 操作権限を TOE の中に維持しており、それを使用しオペレータに操作権限を与えているためである。

FIA_SOS.1

FIA_SOS.1 は、SF.OPE_I&A により、新しいパスワード登録の時に 8桁以上のパスワード入力を求めるため満足される。

FIA_UAU.2

FIA_UAU.2 は、SF.OPE_I&A により、WEB ブラウザからのアクセス開始時にオペレータ識別とパスワードで認証するため満足される。

FIA_UAU.6

FIA_UAU.6 は、SF.OPE_I&A により、パスワード変更の際、各オペレータの現在のパスワード入力を要求するため満足される。

FIA_UID.2

FIA_UID.2 は、SF.OPE_I&A により、オペレータ（管理者、登録者、CE）の操作前にオペレータ識別がされるため、満足される。

FMT_MSA.1

FMT_MSA.1 は、SF.OPE_AC により、CE 操作権限の設定（許可する／許可しない）は管理者のみに制限しているため満足される。

FMT_MTD.1(a)

FMT_MTD.1(a)は、SF.OPE_I&A により、管理者パスワードの変更は管理者のみに制限しているため満足される。

FMT_MTD.1(b)

FMT_MTD.1(b)は、SF.OPE_I&A により、登録者パスワードの変更は登録者のみに制限しているため満足される。

FMT_MTD.1(c)

FMT_MTD.1(c)は、SF.OPE_I&A により、CE パスワードの変更は CE のみに制限しているため満足される。

FMT_SMF.1

FMT_SMF.1 は、SF.OPE_I&A とSF.OPE_AC により、表 12 に示すセキュリティ管理機能を保持しているため満足される。
セキュリティ管理機能のうち、SF.OPE_I&A により、管理者による管理者パスワード変更機能、登録者による登録者パスワード変更機能、及び CE による CE パスワード変更機能を保持しており、SF.OPE_AC により、管理者による CE アクセス権管理機能を保持している。

FMT_SMR.1(a)

FIA_SMR.1 は、SF.OPE_I&A により、管理者を特定することにより操作を実行する権限を割り当てているため満足される。

FMT_SMR.1(b)

FIA_SMR.1 は、SF.OPE_I&A により、登録者を特定することにより操作を実行する権限を割り当てているため満足される。

FMT_SMR.1(c)

FIA_SMR.1 は、SF.OPE_I&A により、CE を特定することにより操作を実行する権限を割り当てているため満足される。

FPT_RVM.1

FPT_RVM.1 は、SF.OPE_I&A が必ず実行されるため、満足される。

FPT_SEP.1

FPT_SEP.1 は、SF.OPE_AC によって、セキュリティドメインを分離および維持することで、他の信頼できないサブジェクトによる干渉や改ざんから保護することにより満足される。

8.3.2 機能強度主張の根拠

3つのセキュリティ機能(SF.OPE_I&A、SF.CS_HTTPS、SF.CS_SMIME)が確率的または順列的メカニズムを持っている。しかしながら暗号化アルゴリズムの強度は、CC の適用範囲外である。機能強度は、非暗号である確率的または順列的メカニズムにのみ適用する。したがって SF.OPE_I&A のみが SOF-基本の機能強度を持つ。

暗号化アルゴリズムを利用する機能(SF.CS_HTTPS、SF.CS_SMIME)は SOF レート付けから除外される。それに対して、TOE セキュリティ機能の最小機能強度は SOF-基本である。

これらの主張が一貫していることは明白である。

8.3.3 セキュリティ機能の組合せの根拠

4 つのセキュリティ機能はすべてのセキュリティ機能要件をカバーしている。また、セキュリティ機能はそれぞれ単独で対応する TOE セキュリティ機能要件を満たしており、一緒に機能することで TOE セキュリティ機能要件を満たすようなセキュリティ機能は存在しない。

8.3.4 保証手段の根拠

表 26 に、ASE クラスおよび EAL3 の保証要件すべてに保証手段が対応していることを示す。

表 26: 保証要件と保証手段の対応

保証クラス	保証コンポーネント	保証手段
ASE: セキュリティターゲット評価	ASE_DES.1 ASE_ENV.1 ASE_INT.1 ASE_OBJ.1 ASE_PPC.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1	Remote Communication Gate TypeN/L/BN1/BM1 セキュリティターゲット Version 1.03, 2006-06-07
ACM: 構成管理	ACM_CAP.3 ACM_SCP.1	Remote Communication Gate TypeN/L/BN1/BM1 構成管理 Version 0.21, 2006-04-11 Remote Communication Gate TypeN/L/BN1/BM1 構成リスト Version 0.20, 2006-06-07
ADO: 配付と運用	ADO_DEL.1 ADO_IGS.1	Remote Communication Gate TypeN/L/BN1/BM1 配付 Version 0.11, 2005-11-28 Remote Communication Gate TypeN/L/BN1/BM1 設置、生成、及び立ち上げ書 Version 0.11, 2005-11-01

保証クラス	保証コンポーネント	保証手段
ADV: 開発	ADV_FSP.1	Remote Communication Gate TypeN/L/BN1/BM1 機能仕様書 Version 0.23, 2006-04-11
	ADV_HLD.2	Remote Communication Gate TypeN/L/BN1/BM1 上位設計書 Version 0.16, 2006-04-11
	ADV_RCR.1	Remote Communication Gate TypeN/L/BN1/BM1 表現対応書 Version 0.15, 2006-04-11
AGD: ガイダンス文書	AGD_ADM.1 AGD_USR.1	Remote Communication Gate TypeN/L 安全上のご注意、セットアップガイド A768-8559, 2006-01-31 Remote Communication Gate TypeN/L 使用説明書 A768-8558, 2006-02-08 Remote Communication Gate TypeN/L/NB/LB サービスマニュアル Version 1.3, 2006-02-08 Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (European version) A768-8603B, 2006-01-30 Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (North American version) A768-8605B, 2006-01-31 Remote Communication Gate Type BN1/BM1 Operating Instructions (European version) A768-8604B, 2006-02-03 Remote Communication Gate Type BN1/BM1 Operating Instructions (North American version) A768-8606B, 2006-02-03 Remote Communication Gate Type BN1/BM1 (Machine Code: A768/A769) SERVICE MANUAL 1.0 revised, 2005-05-24 & Technical Bulletin No.RA768002, 2006-02-07
ALC: ライフサイクルサポート	ALC_DVS.1	Remote Communication Gate TypeN/L/BN1/BM1 開発セキュリティ Version 0.14, 2005-12-15
ATE: テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_INT.2	Remote Communication Gate TypeN/L/BN1/BM1 テスト文書 Version 0.19, 2006-04-11

保証クラス	保証コンポーネント	保証手段
AVA: 脆弱性評定	AVA_MSU.1	Remote Communication Gate TypeN/L 安全上のご注意、セットアップガイド A768-8559, 2006-01-31 Remote Communication Gate TypeN/L 使用説明書 A768-8558, 2006-02-08
	AVA_SOF.1	Remote Communication Gate TypeN/L/BN1/BM1 機能強度分析書 Version 0.11, 2006-03-08
	AVA_VLA.1	Remote Communication Gate TypeN/L/BN1/BM1 脆弱性分析書 Version 0.14, 2006-03-16

8.4 PP 主張根拠

本 ST において適合するPP はない。

9 付録

9.1 略語

CC	コモンクライテリア (Common Criteria)
CE	カスタマーエンジニア (Customer Engineer)
CS	コミュニケーションサーバ (Communication Server)
LAN	ローカルエリアネットワーク (Local Area Network)
OS	オペレーティングシステム (Operating System)
PP	プロテクションプロファイル (Protection Profile)
SC	サービスコール (Service Call)
SF	セキュリティ機能 (Security Function)
ST	セキュリティターゲット (Security Target)
TOE	評価対象 (Target of Evaluation)
TSF	TOE セキュリティ機能 (TOE Security Function)