



# Remote Communication Gate A

## セキュリティターゲット

作成者 : 株式会社リコー  
作成日付 : 2011-02-07  
バージョン : 2.02

## 更新履歴

Version	Date	Author	Description
2.02	2011-02-07	株式会社リコー	公開版

## 目次

<b>1</b>	<b>ST 概説</b> .....	<b>5</b>
1.1	ST 参照 .....	5
1.2	TOE 参照 .....	5
1.3	TOE 概要 .....	5
1.3.1	TOE 種別.....	5
1.3.2	TOE の使用方法.....	5
1.3.3	TOE の主要セキュリティ機能.....	6
1.3.4	TOE の利用環境.....	6
1.4	TOE 記述 .....	8
1.4.1	TOE の物理的範囲 .....	8
1.4.2	ガイダンス .....	9
1.4.3	関係者定義 .....	10
1.4.4	TOE の論理的範囲 .....	11
1.4.4.1	基本機能 .....	11
1.4.4.2	セキュリティ機能.....	12
1.4.5	保護資産 .....	13
1.5	用語解説 .....	14
<b>2</b>	<b>適合主張</b> .....	<b>15</b>
2.1	CC 適合主張.....	15
2.2	PP 主張 .....	15
2.3	パッケージ主張 .....	15
<b>3</b>	<b>セキュリティ課題定義</b> .....	<b>16</b>
3.1	脅威 .....	16
3.2	組織のセキュリティ方針 .....	16
3.3	前提条件 .....	17
<b>4</b>	<b>セキュリティ対策方針</b> .....	<b>18</b>
4.1	TOE のセキュリティ対策方針 .....	18
4.2	運用環境のセキュリティ対策方針.....	19
4.3	セキュリティ対策方針根拠 .....	20
4.3.1	セキュリティ対策方針とセキュリティ課題の対応関係.....	20
<b>5</b>	<b>拡張コンポーネント定義</b> .....	<b>23</b>
<b>6</b>	<b>セキュリティ要件</b> .....	<b>24</b>
6.1	セキュリティ機能要件 .....	24
6.1.1	クラス FAU: セキュリティ監査 .....	24
6.1.2	クラス FDP: 利用者データ保護.....	28
6.1.3	クラス FIA: 識別と認証.....	30
6.1.4	クラス FMT: セキュリティ管理.....	31
6.1.5	クラス FPT: TSF の保護.....	33

---

6.1.6	クラス FTA: TOE アクセス.....	33
6.1.7	クラス FTP: 高信頼パス/チャネル .....	33
<b>6.2</b>	<b>セキュリティ保証要件 .....</b>	<b>35</b>
<b>6.3</b>	<b>セキュリティ機能要件根拠 .....</b>	<b>36</b>
6.3.1	追跡性 .....	36
6.3.2	追跡性の正当化.....	37
6.3.3	依存性分析 .....	40
<b>6.4</b>	<b>セキュリティ保証要件根拠 .....</b>	<b>41</b>
<b>7</b>	<b>TOE 要約仕様.....</b>	<b>42</b>

## 図一覧

図 1: TOE の接続形態.....	6
図 2: TOE のハードウェア構成.....	8
図 3: TOE の論理的範囲.....	11

## 表一覧

表 1: TOE 関連用語.....	14
表 2: セキュリティ対策方針とセキュリティ課題の対応関係.....	20
表 3: 監査対象事象リスト.....	24
表 4: サブジェクトとオブジェクトと操作.....	28
表 5: サブジェクトとオブジェクトとセキュリティ属性.....	29
表 6: アクセスを管理する規則.....	29
表 7: 属性の最初の関連付けに関する規則.....	31
表 8: TSF 情報管理のリスト.....	32
表 9: 管理機能の特定のリスト.....	32
表 10: RC Gate-CS 間通信において高信頼チャンネルが要求される機能(a).....	34
表 11: RC Gate-登録 HTTPS 対応機間通信において高信頼チャンネルが要求される機能(b).....	34
表 12: TOE セキュリティ保証要件(EAL3).....	35
表 13: セキュリティ対策方針と機能要件の関連.....	36
表 14: TOE セキュリティ機能要件の依存性対応表.....	40

## 1 ST概説

本章では、ST 参照、TOE 参照、TOE 概要、TOE 記述および用語解説を記述する。

### 1.1 ST参照

ST の識別情報を以下に示す。

ST 名称	: Remote Communication Gate A セキュリティターゲット
バージョン	: 2.02
作成日付	: 2011-02-07
作成者	: 株式会社リコー

### 1.2 TOE参照

TOE である、Remote Communication Gate A は、機種コード(6桁のコード)の上4桁とファームウェアバージョンで識別する。尚、ファームウェアバージョンは、ファームウェアを構成するアプリケーション(A)、ファームウェア共通部(C)、プラットフォーム(P)、OS(K)の各モジュールのバージョンを組合せたものである。

製造者	: 株式会社リコー
製品名称	: Remote Communication Gate A (注)これ以降、上記製品を"RC Gate"とする
機種コード(上4桁)	: D459
ファームウェアバージョン	: A2.06-C2.04-P2.01-K2.02

### 1.3 TOE概要

本章では、本 TOE の種別、TOE の使用方法、および主要セキュリティ機能、TOE の利用環境を述べる。

#### 1.3.1 TOE種別

TOE は、LAN 上のデジタル複合機およびプリンタ(以下、デバイスと言う)を遠隔診断保守するサービスに利用する IT 機器である。遠隔診断保守するサービスとは、TOE が遠隔診断保守サービス対象のデバイスから受信した情報を保守センターに送信し、その情報をもとに保守センターでデバイスの状態を診断し、デバイス毎に必要な保守をするサービスであり、@Remote あるいは@Remote サービスと言う。

#### 1.3.2 TOEの使用方法

TOE は、@Remote サービスをするにあたって、遠隔診断保守サービスデバイスと保守センターの通信を仲介する。利用者は、遠隔診断保守サービスを受けるデバイスを接続しているオフィスのローカルエリア

ネットワーク(以下、LANと言う)に TOE を接続して使用する。

また、利用者は LAN 上のパソコンから Web ブラウザを使って TOE を操作することができる。

### 1.3.3 TOEの主要セキュリティ機能

TOE の主要なセキュリティ機能には、通信保護機能、利用者制限機能、RC Gate ファームウェア正当性確認機能、および監査ログ機能がある。

通信保護機能は、TOE との通信相手(保守センター、パソコン、および TOE と SSL 通信する機能を持ったデバイス)の通信経路を保護する機能である。

利用者制限機能は、パソコンから TOE を利用しようとするものに対して識別認証を行い、識別認証に成功した許可利用者に対し、予め与えられた操作権限内の操作だけを提供する機能である。

RC Gate ファームウェア正当性確認機能は、TOE のファームウェアが製造元で作られたものであることを確認し、確認結果を利用者に提供する機能である。

監査ログ機能は、ログを記録し、そのログを特定の利用者に提供する機能である。

### 1.3.4 TOEの利用環境

TOEの接続イメージを図 1に示し、TOEおよびTOE以外の要素について解説する。

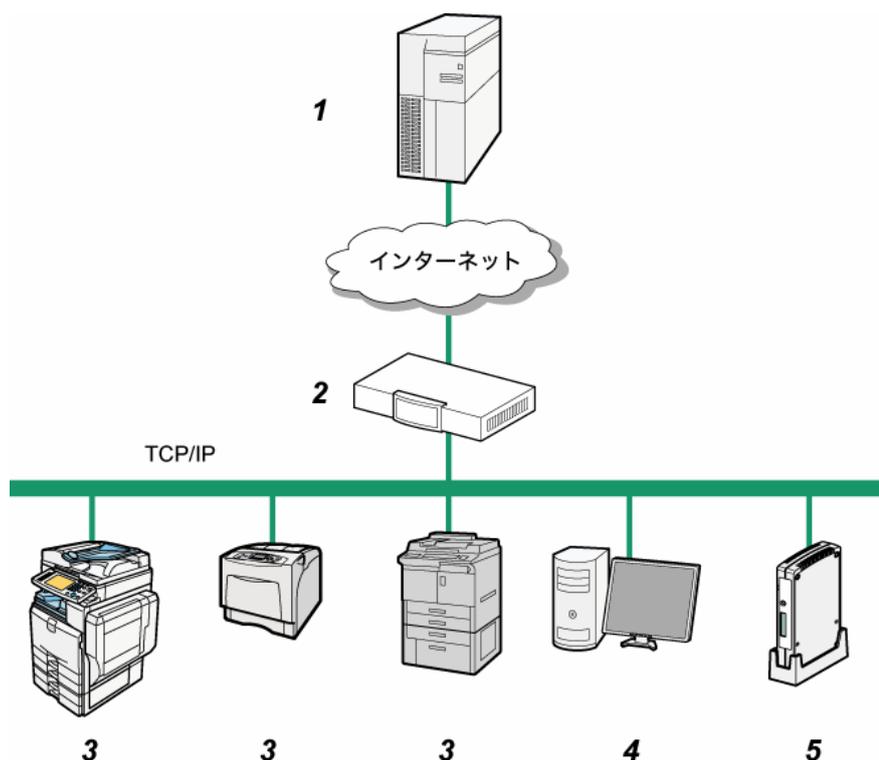


図 1: TOE の接続形態

#### 1. CS(Communication Server)

保守センターのサーバ。TOE から通信開始の要求をし、TOE と CS 間で保守サービスのための情報を送受信する。

## 2. ファイアウォール

オフィスの LAN 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. デバイス

本書でデバイスとは、オフィスの LAN 環境に接続され TOE と通信する能力を持ったデジタル複合機およびプリンタのことを言う。デバイスは、TOE との通信方法によって HTTPS 対応機と SNMP 対応機に分類される。HTTPS 対応機は、TOE と RC Gate - デバイス間通信保護機能による通信をする能力を持ったデバイス、SNMP 対応機は、HTTPS 対応機以外で TOE と MIB による通信をする能力を持ったデバイス。遠隔診断保守サービスの対象となるのは、TOE に登録された HTTPS 対応機と SNMP 対応機で、それぞれ登録 HTTPS 対応機、登録 SNMP 対応機と言う。また、登録 HTTPS 対応機と登録 SNMP 対応機の総称を登録デバイスと言う。登録デバイスは、保守サービスに係わる情報を TOE に送信する。

## 4. パソコン

オフィスの LAN 環境に接続されたパーソナルコンピュータ。利用者は、パソコンの Web ブラウザから TOE をリモートで操作することができる。Web ブラウザは、Flash Player (Ver.9.0 から Ver.10.0) をプラグインした Internet Explorer (Ver.6.0 から Ver.8.0) を使用する。

## 5. RC Gate

本 TOE である。TOE は、オフィスの LAN 環境に接続される。尚、TOE 以外の要素としてオプションのメモリ (Remote Communication Gate Memory 1000) とオプションのストレージ (Remote Communication Gate Storage 1000) が TOE に搭載可能である。これらオプションを搭載した環境も利用環境に含める。

## 1.4 TOE記述

本章では、TOE の物理的範囲、ガイダンス、関係者定義、TOE の論理的範囲、および保護資産を記述する。

### 1.4.1 TOEの物理的範囲

TOEの物理的範囲は、図 2に示すハードウェア/ファームウェアから構成される。

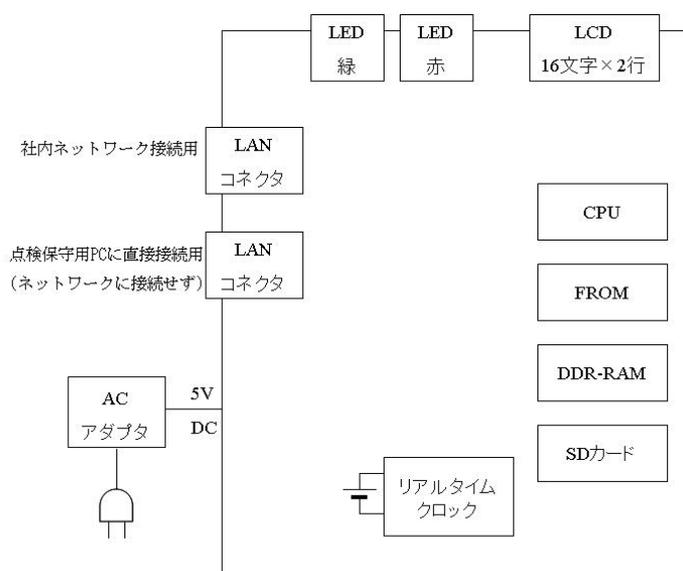


図 2: TOE のハードウェア構成

#### CPU

TOE 動作における基本的な演算処理をおこなう半導体チップ。

#### FROM

電源を切ってもデータが消えない不揮発性の半導体メモリであり、ブートローダなどが記録されている。フラッシュメモリとも呼ばれる。

#### DDR-RAM

揮発性の半導体メモリであり、TOE 起動時にプログラム、データがロードされる。

#### SD カード

不揮発性の半導体メモリである。RC Gate ファームウェア、初期情報が工場書き込まれる。運用時には、蓄積メモリとして利用される。

### リアルタイムクロック

現在時刻を刻み続ける時計である。電源が切られていても時刻を刻み続けるための電池も搭載されている。

### 社内ネットワーク接続用 LAN コネクタ

パソコン、CS、デバイスと通信するための LAN コネクタである

### PC 接続用 LAN コネクタ

IP アドレスの初期設定のため、または、故障時の保守点検のために使用するパソコンを接続する LAN コネクタである。

### LCD

TOE の IP アドレス、ステータス、エラーメッセージを表示するディスプレイ装置である。

### LED 緑

電源 On/Off を示すランプである。電源 On の時に点灯する。

### LED 赤

RC Gate のステータスを示すランプである。点灯/消灯/点滅/早い点滅それぞれで TOE のステータスを表示する。

### AC アダプタ

電力を供給するための電源装置である。

### RC Gate ファームウェア

TOE の組込みシステムで、アプリケーション、ソフトウェア共通部、プラットフォーム、および OS のモジュールで構成されている。

## 1.4.2 ガイダンス

本 TOE を構成するガイダンス文書は以下のとおりである。

#### 国内向けガイダンス

- Remote Communication Gate A 安全上のご注意
- Remote Communication Gate A セットアップガイド
- Remote Communication Gate A 使用説明書

#### 海外向けガイダンス

- Remote Communication Gate A Safety Information
- Remote Communication Gate A Setup Guide
- Remote Communication Gate A Operating Instructions

### 1.4.3 関係者定義

RC Gate に係る関係者を以下定義する。

#### 利用者

利用者とは、次に記述する RC Gate の管理者と一般ユーザーを総称した名称である。本文中で単に「利用者」と呼ぶときは、RC Gate の管理者と一般ユーザーをさす。

#### 管理者

RC Gate を管理するお客様の管理者をさす。パソコンから RC Gate の設定変更ステータス閲覧、監査ができる。本文中で単に「管理者」と呼ぶときは、この RC Gate の管理者をさす。

#### 一般ユーザー

一般ユーザーとは、管理者により TOE 利用アカウントを与えられた者をさす。一般ユーザーはパソコンからデバイスのステータス閲覧ができる。

#### ネットワーク管理者

ネットワーク管理者とは、TOE が設置されているお客様の LAN を管理する IT マネージャをさす。

#### デバイス管理者

デバイス管理者とは、TOE が設置されているお客様の LAN に接続されるデバイスの保守管理をおこなう者をさす。

#### 組織の責任者

組織の責任者とは、TOE を設置運用する組織のお客様の責任者をさす。組織の責任者は各管理者の任命権をもつ。

#### CE

CE(カスタマーエンジニア)とは、TOE を取り扱うための教育を受け、TOE の保守をする者をさす。保守をする際 CE は、パソコンの Web ブラウザから CE 用のインターフェースを使って TOE を操作することができる。ただし、CE 用のインターフェースは、設置時に管理者によって利用を禁止される。

#### ネットワーク利用者

ネットワーク利用者とは、TOE が設置されているお客様の LAN 環境を利用する者の総称である。TOE 利用アカウントをもたない者も含まれる。

### 1.4.4 TOEの論理的範囲

TOEの運用イメージと、運用イメージにおける論理的範囲を図 3に示し、TOEが提供する基本機能(非セキュリティ機能)と、TOEのセキュリティ機能について解説する。

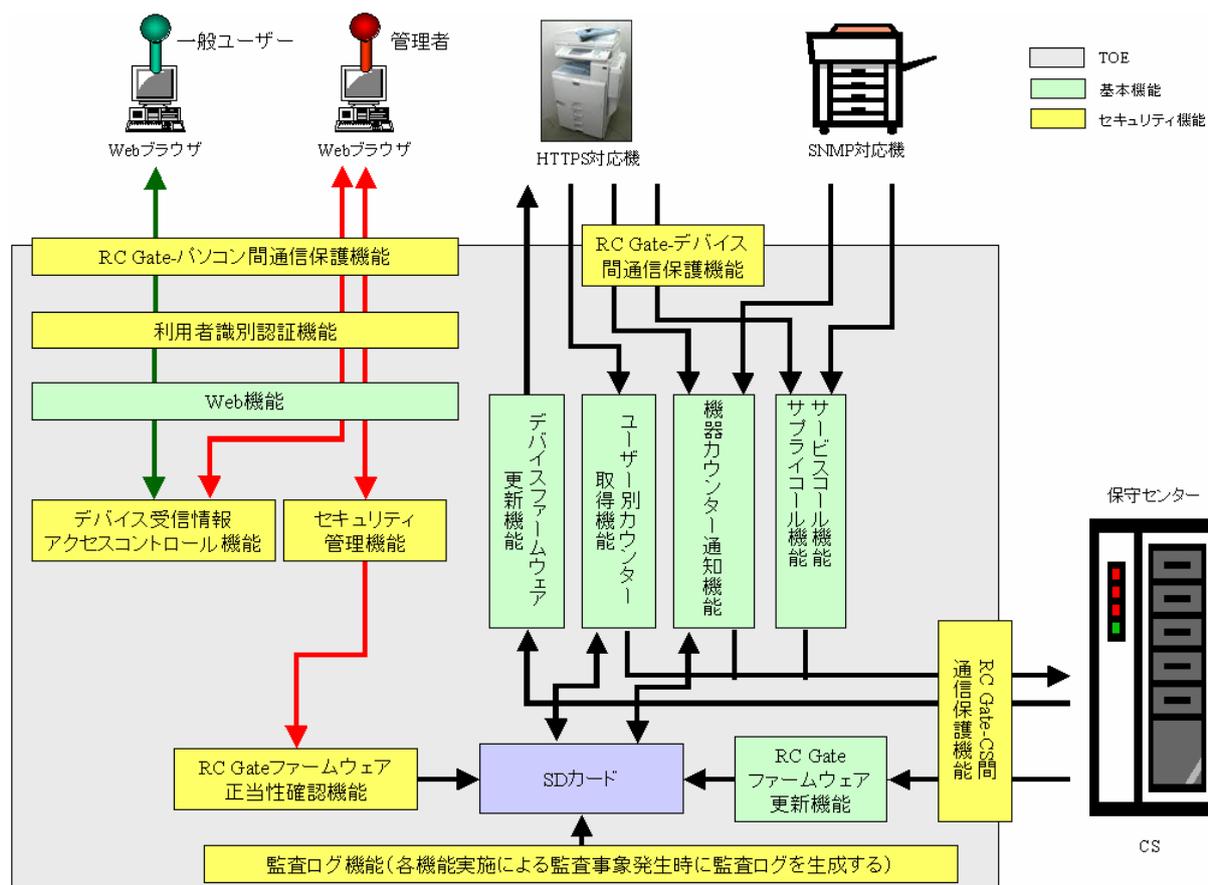


図 3: TOE の論理的範囲

#### 1.4.4.1 基本機能

##### サービスコール機能

TOE が登録デバイスから受信したデバイス障害情報を CS に通報する機能。保守センターでは、その通報内容に従って故障原因を解析し対応する。

##### 機器カウンター通知機能

TOE が登録デバイスから受信した機器カウンター情報(デバイス毎にカウントしている印刷枚数)を定期的に CS に通知する機能。カウンター値は課金情報として使われる。

#### ユーザー別カウンター取得機能

TOE が登録デバイスから取得したユーザー別カウンター情報(ユーザー毎にカウントしている印刷枚数)を定期的に CS に通知する機能。

本 ST においては、本機能を使用できない設定にして評価する。

#### サプライコール機能

TOE が登録デバイスから受信したサプライ情報(トナー、紙の残量)を CS に通知する機能。保守センターでは、その通知内容に従ってトナーや紙の補給対応をする。

#### デバイスファームウェア更新機能

TOE が CS から受信したデバイスファームウェアで、登録 HTTPS 対応機のファームウェアを更新する機能。

#### RC Gate ファームウェア更新機能

TOE が CS から受信した RC Gate ファームウェアで、RC Gate ファームウェアを更新する機能。

#### Web 機能

利用者が TOE をリモート操作するため、TOE が提供する機能。

利用者は、パソコンから Web ブラウザを使って TOE へアクセスする。

### 1.4.4.2 セキュリティ機能

#### RC Gate—デバイス間通信保護機能

サービスコール機能、機器カウンター通知機能、およびサプライコール機能における TOE と登録 HTTPS 対応機間の通信で、TOE と登録 HTTPS 対応機相互に、通信データの改ざんを検知する機能。  
ユーザー別カウンター取得機能の通信は、本機能の対象ではない。

#### RC Gate—CS 間通信保護機能

TOE がインターネットを介した通信する通信先を CS だけに限定し、さらに TOE と CS 相互に通信データを秘匿し、改ざんを検知する機能。

#### RC Gate—パソコン間通信保護機能

Web 機能における TOE とパソコン間通信で、通信データを秘匿する機能。

#### 利用者識別認証機能

TOE が、Web 機能の利用を TOE の許可利用者(管理者、一般ユーザー)だけに提供する機能。

TOE は、Web 機能を利用するとする利用者に識別認証のための情報(以下、アカウント情報)入力を要求する。利用者がアカウント情報を入力すると、その情報で識別認証し認証に成功した利用者だけに TOE 操作を許可する。

#### デバイス受信情報アクセスコントロール機能

TOEが、許可利用者によるデバイス受信情報のアクセスを制限する機能。TOEは、利用者識別認証機能で認証に成功した利用者に対し、その利用者役割に許可されたデバイス受信情報のアクセスだけを提供する。

#### RC Gate ファームウェア正当性確認機能

TOEが、利用者による要求でアプリケーション、ソフトウェア共通部、プラットフォーム、およびOSが、製造元が提供する正規のものであることを確認する機能。

#### セキュリティ管理機能

TOEが、管理者だけにTOEの管理権限を持たせるため、Web機能から管理者だけに提供する機能。

#### 監査ログ機能

TOEが監査ログを生成し、生成した監査ログの改ざん、損失を防止し、監査ログの読み出し操作を制限する機能。

TOEは、セキュリティ監査に必要な事象発生時にセキュリティ監査に必要な情報を監査ログとしてTOE内記録する。TOE内の監査ログは、変更、削除操作を許可せず、閲覧操作を管理者だけに許可する。

### 1.4.5 保護資産

本章では、TOEが保護する機器カウンター情報、障害情報、サプライ情報、コール通知履歴、デバイスファームウェア、デバイスファームウェア更新履歴、RC Gate ファームウェア、およびTSFデータについて解説する。

#### 機器カウンター情報

機器カウンター情報とは、デバイス毎にカウントしている印刷枚数のこと。

機器カウンター情報は、各デバイスからTOEへ送信され、一旦TOEの機器カウンター情報エリアに蓄積されてから、定期的にCSへ送信される。TOEからCSに送信された直後、機器カウンター情報エリア内の機器カウンター情報は消去される。TOEが、機器カウンター情報を蓄積している間は、管理者と一般ユーザーに閲覧が許可され、その他の操作は許可されない。デバイスからCSへ送信される機器カウンター情報が改ざんされると、登録デバイスが適切な@Remoteサービスを受けられなくなる。

#### 障害情報、サプライ情報、コール通知履歴

障害情報、サプライ情報は、各デバイスからTOEに送信され、随時TOEからCSへ送信される。デバイスからCSへ送信される障害情報、およびサプライ情報が改ざんされると、登録デバイスが適切な@Remoteサービスを受けられなくなる。

また、障害情報、サプライ情報をTOEが受信すると、TOEはサービスコール、サプライコールの履歴(以下、コール通知履歴と言う)をコール通知履歴エリアに記録する。コール通知履歴は、管理者と一般ユーザーに閲覧が許可され、その他の操作は許可されない。

### デバイスファームウェアとデバイスファームウェア更新履歴

デバイスファームウェア更新機能において、CS から各デバイスに送信されるデバイスのファームウェア。デバイスファームウェアは、CS から TOE を経由してデバイスにインストールされる。CS から TOE に送信されるデバイスファームウェアは、完全性を保証する必要がある。

また、TOE はデバイスファームウェア更新を実施時に履歴(以下、デバイスファームウェア更新履歴と言う)をデバイスファームウェア更新履歴エリアに記録する。デバイスファームウェア更新履歴は、管理者だけに閲覧が許可され、その他の操作は許可されない。

### RC Gate ファームウェア

RC Gate ファームウェアは、TOE の製造工場 TOE にインストールされ利用者サイトに配付される。また、TOE の管理者が許可することによって、RC Gate ファームウェア機能で更新することもある。RC Gate ファームウェアは、製造元が製造したファームウェアでなければならない。

### TSF データ

TSF データは、TOE 内に記録されている。TOE の許可利用者は、パソコンから TSF データを新規作成、変更、および削除することができる。これら TSF データの操作は、許可利用者のルールによって制限される必要がある。

## 1.5 用語解説

本STを明確に理解するため、表 1で用語の意味を定義する。

表 1: TOE 関連用語

用語	定義
@Remote	本遠隔サービスの商用名称。
デバイス受信情報	TOE が登録デバイスから受信する機器カウンター情報、障害情報、およびサプライ情報の総称。
ブートローダ	TOE へ電源投入直後に起動するプログラムで OS を起動する。
MIB	Management Information Base の略。SNMP 管理されるネットワーク機器が、自分の状態を外部に知らせるために公開する情報のこと。

## 2 適合主張

本章では適合の主張について述べる。

### 2.1 CC適合主張

本 ST 及び TOE の CC 適合主張は以下の通りである。

- 適合を主張する CC のバージョン

パート 1:

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

CCMB-2009-07-001

パート 2:

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

CCMB-2009-07-002

パート 3:

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

CCMB-2009-07-003

- 機能要件: パート 2 適合
- 保証要件: パート 3 適合

### 2.2 PP主張

本 ST 及び TOE が適合している PP はない。

### 2.3 パッケージ主張

本 ST 及び TOE が適合しているパッケージは、評価保証レベル EAL3 である。

### 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、及び前提条件について記述する。

#### 3.1 脅威

本 TOE の利用及び利用環境において想定される脅威を識別し記述する。

- T.FAKE\_CS**      インターネット上のなり済まし  
攻撃者はインターネット上に偽CSを立ち上げ、登録デバイスにデバイスファームウェアをインストールする、あるいはLAN内にウイルス等の悪意のあるプログラムを送り込むかもしれない。
- T.INTERNET**    インターネット上の通信情報改ざん  
攻撃者は、TOE が CS と通信する際にインターネット上を流れる通信データを暴露あるいは改ざんするかもしれない。
- T.ACCESS**        不正なアクセス  
TOEの許可利用者以外の者が、一般ユーザーあるいは管理者だけに許可されているTOEの操作をするかもしれない。一般ユーザーが誤って、セキュリティ管理機能を利用するかもしれない。

#### 3.2 組織のセキュリティ方針

この章では、組織のセキュリティ方針を記述する。

- P.ATR\_DEVICE HTTPS 対応機との通信**  
機器カウンター通知機能、サービスコール機能、およびサブライコール機能において、TOE が登録 HTTPS 対応機と通信する場合は、通信開始時に正当な HTTPS 対応機であることを確認する手段が提供され、かつ TOE と登録 HTTPS 対応機間の通信情報は保護されていなければならない。
- P.SOFTWARE RC Gate ファームウェアの完全性確認**  
TOEに組み込まれているRC Gateファームウェアが正規のRC Gateファームウェア(本書で正規のRC Gateファームウェアとした場合、製造元のRC Gateファームウェアと同意)であることを確認する手段が提供されていなければならない。

**P.AUDIT\_LOGGING 監査ログ記録管理**

セキュリティ侵害を事後監査するために必要な事象発生時に監査ログをTOE内に記録しなければならない。さらに権限を持つものだけが、そのログを閲覧できるようにしなければならない。権限を持たないものによる、そのログの改変や削除を防止しなければならない。

**P.PC\_WEB パソコンとの通信**

Web機能において、パソコンとTOE間の情報の改ざんを検知し、パスワードの漏えいを防止しなければならない。

**3.3 前提条件**

この章では、TOE の前提条件を記述する。

**A.ADMINSHIP 管理者の条件**

TOE の管理者、ネットワーク管理者、デバイス管理者は、それぞれの特権を利用して悪意を持った不正をしないものとする。

**A.TOE\_ADMIN TOE の管理**

管理者は、管理者に課せられた作業において TOE をセキュアに管理運用するために必要な知識を持ち管理者の役割を遂行するものとする。また、管理者は TOE を物理的に保護しなければならない。

**A.NETWORK ネットワークの管理**

ネットワーク管理者は、LAN の保守管理をするものとする。ネットワーク利用者に HTTPS 対応機以外のデバイスと TOE の通信情報を変更したりしないように指導し、また、インターネットを通して攻撃する外部者から LAN 環境を保護するものとする。

**A.DEVICE デバイスの管理**

デバイス管理者は、LAN に接続されているデバイスの保守管理をするものとする。正規で改造されていないデバイスが購入運用されているものとする。

**A.CE TOE の保守**

正規の CE だけが TOE の保守をすることができるものとする。

## 4 セキュリティ対策方針

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

### 4.1 TOEのセキュリティ対策方針

本章では、TOE のセキュリティ対策方針を記述する。

- O.I&A**           **識別認証**
- 利用者(一般ユーザーと管理者)によるパソコンの Web ブラウザからの TOE リモート操作において、TOE は、リモート操作に先立って識別認証し、利用者に TOE のリモート操作を許可することを保証する。
- O.ACCESS**       **アクセス制限**
- TOE は、利用者に対して、その役割(一般ユーザー、管理者)に応じた保護資産へのアクセスを保証する。
- O.COM\_CS**       **CS との通信チャネル保護**
- TOE は、CS との通信において、正規の CS と通信し、その通信経路上にある通信データを秘匿し、改ざんを検知することを保証する。
- O.COM\_ATR\_DEVICE**       **デバイスとの通信チャネル保護**
- 機器カウンター通知機能、サービスコール機能、およびサブライコール機能において、TOE は、登録 HTTPS 対応機と通信し、その通信経路上にある通信データを秘匿し、改ざんを検知することを保証する。
- O.COM\_OPERATOR**   **利用者のリモート操作データ保護**
- TOE は、利用者によるパソコンの Web ブラウザを使った TOE のリモート操作時の通信における通信経路上にある通信データを秘匿し、改ざんを検知することを保証する。
- O.GENUINE**       **RC Gate ファームウェアの完全性確認**
- TOE は、TOE に組み込まれている RC Gate ファームウェアが正規の RC Gate ファームウェアであることを、利用者が確認できることを保証する。
- O.AUDIT\_LOGGED**   **監査ログ記録管理**
- TOE は、セキュリティ侵害を事後監査するために必要な事象(監査ログ機能の起動と終了、監査ログの読出し、利用者識別認証機能の実施、アカウント情報の操作、日

時の更新、CS との通信失敗、セルフチェックの実施)発生時に、監査ログを記録し、管理者だけがセキュリティ侵害を監査できるよう、監査ログを提供することを保証する。また、監査ログは改変及び消去されないことを保証する。

## 4.2 運用環境のセキュリティ対策方針

本章では、運用環境のセキュリティ対策方針について記述する。

### OE.SUPER TOE に係わる管理者の任命

組織の責任者は、TOE の納入に先立って、組織の中の信頼できる者から TOE の管理者、ネットワーク管理者、デバイス管理者を任命しなければならない。

### OE.ADMIN TOE の管理

管理者は、TOE のガイダンスを理解し、その記載内容に従って TOE を物理的に保護し、管理運用しなければならない。

### OE.NETWORK ネットワークの管理

ネットワーク管理者は、ネットワーク利用者に対して、HTTPS 対応機以外のデバイスと TOE の通信情報を変更したりしないように指導しなければならない。

ネットワーク管理者は、インターネットを通して攻撃する外部者から LAN 環境を守るために、ファイアウォール等のセキュリティ装置を外部のネットワークとの間に設置しなければならない。

### OE.DEVICE デバイスの管理

デバイス管理者は、正規のルートからデバイスを購入設置し、その後、デバイスが改造されたりしないように保守管理しなければならない。

### OE.CE CE の確認

管理者は、TOE の保守の際に、正規の CE だけに保守を許可しなければならない。

### 4.3 セキュリティ対策方針根拠

本章では、セキュリティ対策方針根拠として、セキュリティ対策方針とセキュリティ課題の対応関係を記述する。

#### 4.3.1 セキュリティ対策方針とセキュリティ課題の対応関係

セキュリティ対策方針とセキュリティ課題として定義した前提条件、脅威、および組織のセキュリティ方針の対応関係を表 2に示す。

表 2に示すとおり、セキュリティ対策方針いずれかが、前提条件を充足し、脅威に対抗し、組織のセキュリティ対策方針を実現する。また、各セキュリティ対策方針は、少なくとも 1 つの前提条件、脅威、あるいは組織のセキュリティ対策方針に対応している。

表 2: セキュリティ対策方針とセキュリティ課題の対応関係

	O.I&A	O.ACCESS	O.COM_CS	O.COM_ATR_DEVICE	O.COM_OPERATOR	O.GENUINE	O.AUDIT_LOGGED	OE.SUPER	OE.ADMIN	OE.NETWORK	OE.DEVICE	OE.CE
T.FAKE_CS			✓									
T.INTERNET			✓									
T.ACCESS	✓	✓										
P.ATR_DEVICE				✓								
P.SOFTWARE						✓						
P.AUDIT_LOGGING							✓					
P.PC_WEB					✓							
A.ADMINSHIP								✓				
A.TOE_ADMIN									✓			
A.NETWORK										✓		
A.DEVICE											✓	
A.CE												✓

**T.FAKE\_CS**は、**O.COM\_CS**で対抗できる。なぜなら、**TOE**は正規の**CS**と認めた場合だけ通信することを保証するからである。

**T.INTERNET** は **O.COM\_CS** で対抗できる。なぜなら、**O.COM\_CS** は、TOE と CS 間のインターネットを含む通信路上の通信データを秘匿し、改ざんを検知するからである。

**T.ACCESS** は **O.I&A**、**O.ACCESS** で対抗できる。なぜなら、TOE の利用者以外が TOE にアクセスする脅威と、一般ユーザーが管理者だけに許可される TOE 操作を誤操作する脅威に対して **O.I&A** が、TOE 管理情報にアクセスするため、および管理機能を操作するための唯一の手段であるパソコンの Web ブラウザからの TOE 操作に先立って識別認証を行い、予め定められた回数内で認証に成功した利用者だけに TOE を操作すること許可し、**O.ACCESS** で利用者の役割に応じて、TOE の管理情報の操作を許可するためである。

**P.ATR\_DEVICE** は **O.COM\_ATR\_DEVICE** で実施できる。なぜなら、**O.COM\_ATR\_DEVICE** は、カウンター情報通知機能、サービスコール機能、およびサブライコール機能において TOE とデバイスの通信は、予め登録しているデバイスだけを許可し、TOE とデバイスの通信路上の保護資産を秘匿し、改ざんを検知するためである。

**P.SOFTWARE** は **O.GENUINE** によって実施できる。なぜなら、**O.GENUINE** は、RC Gate ファームウェアが正規の RC Gate ファームウェアであることを利用者が確認できるからである。

**P.AUDIT\_LOGGING** は **O.AUDIT\_LOGGED** によって実施できる。なぜなら、**O.AUDIT\_LOGGED** はセキュリティ侵害を事後監査するために必要な事象(監査ログ機能の起動と終了、監査ログの読出し、利用者識別認証機能の実施、アカウント情報の操作、日時の更新、CS との通信失敗、セルフチェックの実施)発生時に監査ログを記録し、記録した監査ログの閲覧は管理者だけ許可し、改変及び削除は、利用者に許可しないとしているからである。

**P.PC\_WEB** は **O.COM\_OPERATOR** で対抗できる。なぜなら、**O.COM\_OPERATOR** は Web 機能における LAN 上の TSF データの改ざんは検知し、パスワードを秘匿するとしているためである。

**A.ADMINSHIP** は **OE.SUPER** で実現できる。なぜなら、**OE.SUPER** では、TOE の納入に先立って組織の責任者が、組織の中の信頼できる者から、TOE の管理者、ネットワーク管理者、デバイス管理者を任命するとしているため、それぞれの管理者特権を利用して悪意を持った不正をしないからである。

**A.TOE\_ADMIN** は **OE.ADMIN** で実現できる。なぜなら、**OE.ADMIN** は、管理者が、管理運用方法についてガイダンスから理解し、実施するとしているからである。

**A.NETWORK** は **OE.NETWORK** で実現できる。なぜなら、**OE.NETWORK** は、ネットワーク管理者に対して、HTTPS 対応機以外のデバイスと TOE の通信情報を変更しないようネットワーク利用者を指導することと、ファイアウォール等のセキュリティ装置を設置しインターネットから LAN へは適切な通信だけを許可することで、LAN をインターネットから保護することを要求しているからである。

**A.DEVICE** は **OE.DEVICE** で実現できる。なぜなら、**OE.DEVICE** は、デバイス管理者に **TOE** と通信するデバイスは正規のデバイスのみとなるよう、正規のルートからデバイスを購入し、そのデバイスを改造しないよう管理することを要求するからである。

**A.CE** は **OE.CE** で実現できる。なぜなら管理者は、**TOE** の保守の際に、正規の **CE** だけに **TOE** の保守を許可するためである。

## 5 拡張コンポーネント定義

本 ST 及び TOE では、拡張したセキュリティ要件、すなわち「2.1 CC 適合主張」にて適合を主張する CC に記載されていない新規のセキュリティ機能要件とセキュリティ保証要件は定義しない。

## 6 セキュリティ要件

本章は、セキュリティ機能要件、セキュリティ保証要件、及びセキュリティ要件根拠を述べる。

### 6.1 セキュリティ機能要件

本章は、TOEのセキュリティ機能要件を記述する。セキュリティ機能要件は、CC Part2に規定のセキュリティ機能要件から引用する。

CC Part2で定義された割付と選択操作を行った部分は、**[太文字と括弧]**で識別する。詳細化を行った部分は、(詳細化:)で識別する。繰返しを行った部分は、"(a)"、"(b)"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する。

#### 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:

- a) 監査機能の起動と終了;
- b) 監査の**[選択: 指定なし]**レベルのすべての監査対象事象; 及び
- c) **[割付: 表 3に示す監査対象事象]**。

機能要件毎に割り付けられた監査対象とすべき基本レベル以下のアクション(CCにおける規定)と、それに対応するTOEが監査対象とする事象を表 3に記す。

表 3: 監査対象事象リスト

機能要件	監査対象とすべきアクション	TOEの監査対象事象
FAU_GEN.1	なし	—
FAU_GEN.2	なし	—
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	a) 基本 監査ログの読み出し
FAU_SAR.2	a) 基本: 監査記録からの成功しなかった情報読み出し。	監査事象は記録しない
FAU_STG.1	なし	—
FAU_STG.4	a) 基本: 監査格納失敗によってとられるアクション	監査事象は記録しない

機能要件	監査対象とすべきアクション	TOE の監査対象事象
FDP_ACC.1	なし	—
FDP_ACF.1	<p>a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。</p> <p>b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。</p> <p>c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。</p>	監査事象は記録しない
FIA_AFL.1	<p>a) 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)。</p>	<個別に定義した監査対象事象> ロックアウトの開始
FIA_ATD.1	なし	—
FIA_SOS.1	<p>a) 最小: TSF による、テストされた秘密の拒否;</p> <p>b) 基本: TSF による、テストされた秘密の拒否または受け入れ;</p> <p>c) 詳細: 定義された品質尺度に対する変更の識別。</p>	<p>b) 基本 管理者のパスワードの変更(結果: 成功/失敗) 一般ユーザーのパスワードの変更(結果: 成功/失敗) 一般ユーザーのユーザー名の追加(結果: 成功/失敗)</p>
FIA_UAU.2	<p>a) 最小: 認証メカニズムの不成功になった使用;</p> <p>b) 基本: 認証メカニズムのすべての使用。</p>	<p>b) 基本 ログイン(結果: 成功/失敗)</p>
FIA_UAU.6	<p>a) 最小: 再認証の失敗;</p> <p>b) 基本: すべての再認証試行。</p>	監査事象は記録しない
FIA_UID.2	<p>a) 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;</p> <p>b) 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すべての使用。</p>	<p>b) 基本 ログイン(結果: 成功/失敗)</p>
FIA_USB.1	<p>a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。</p> <p>b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)。</p>	<p>b) 基本 ログイン(結果: 成功/失敗)</p>

機能要件	監査対象とすべきアクション	TOE の監査対象事象
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	<個別に定義した監査対象事象> 管理者のパスワードの変更 一般ユーザーのユーザー名の新規作成 一般ユーザーのパスワードの新規作成 一般ユーザーのユーザー名の削除 一般ユーザーのパスワードの削除 一般ユーザーのパスワードの変更 システム時計の日時
FMT_SMF.1	a) 最小: 管理機能の使用	a) 最小 管理者のログインの成功
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	a) 最小 管理者のパスワードの変更 一般ユーザーのユーザー名の新規作成 一般ユーザーのパスワードの新規作成 一般ユーザーのユーザー名の削除 一般ユーザーのパスワードの削除 一般ユーザーのパスワードの変更
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供	a) 最小: 年月日・日時の変更
FPT_TST.1	a) 基本: TSF 自己テストの実行とテストの結果。	a) 基本: 自己テストの実施
FTA_SSL.3	a) 最小: セッションロックメカニズムによる対話セッションの終了。	監査事象は記録しない
FTP_ITC.1(a)	a) 最小: 高信頼チャンネル機能の失敗。 b) 最小: 失敗した高信頼チャンネル機能の開始者とターゲットの識別。 c) 基本: 高信頼チャン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ンネル機能の開始者とターゲットの識別。	a) 最小: RC Gate-CS 間通信の失敗
FTP_ITC.1(b)	a) 最小: 高信頼チャンネル機能の失敗。 b) 最小: 失敗した高信頼チャンネル機能の開始者とターゲットの識別。 c) 基本: 高信頼チャン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ンネル機能の開始者とターゲットの識別。	監査事象は記録しない

機能要件	監査対象とすべきアクション	TOE の監査対象事象
	別。	
FTP_TRP.1	a) 最小: 高信頼パス機能の失敗。 b) 最小: もし得られれば、すべての高信頼パス失敗に関する利用者の識別情報。 c) 基本: 高信頼パス機能のすべての使用の試み。 d) 基本: もし得られれば、すべての高信頼パス呼出に関する利用者の識別情報。	監査事象は記録しない

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:  
 a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗); および  
 b) 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は無い]**

**FAU\_GEN.2 利用者識別情報の関連付け**

下位階層: なし

依存性: FAU\_GEN.1 監査データ生成  
 FIA\_UID.1 識別のタイミング

FAU\_GEN.2.1 識別された利用者のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

**FAU\_SAR.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 TSF は、**[割付: 管理者]**が、**[割付: FAU\_GEN.1 で生成する]**とした**監査データ**を監査記録から読み出せるようにしなければならない。

FAU\_SAR.1.2 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\_SAR.2 限定監査レビュー**

下位階層: なし

依存性: FAU\_SAR.1 監査レビュー

FAU\_SAR.2.1 TSF は、明示的な読出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読出しアクセスを禁止しなければならない。

**FAU\_STG.1 保護された監査証拠格納**

下位階層: なし

依存性: FAU\_GEN.1 監査データ生成

FAU\_STG.1.1 TSF は、監査証拠に格納された監査記録を不正な削除から保護しなければならない。

FAU\_STG.1.2 TSF は、監査証拠内に格納された監査記録への不正な改変を[選択: 防止]できなければならない。

**FAU\_STG.4 監査データ損失の防止**

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 保護された監査証拠格納

FAU\_STG.4.1 TSF は、監査証拠が満杯になった場合、[選択: 最も古くに格納された監査記録への上書き]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はない]を行わなければならない。

**6.1.2 クラスFDP: 利用者データ保護**

**FDP\_ACC.1 サブセットアクセス制御**

下位階層: なし

依存性: FDP\_ACF.1 セキュリティ属性によるアクセス制御

FDP\_ACC.1.1 TSFは、[割付: 表 4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: TOE管理情報アクセス制御ポリシー]を実施しなければならない。

表 4: 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
利用者プロセス (ユーザー種別が管理者)	機器カウンター情報エリア	閲覧
	コール通知履歴エリア	閲覧
	デバイスファームウェア更新履歴エリア	閲覧
利用者プロセス (ユーザー種別が一般ユーザー)	機器カウンター情報エリア	閲覧
	コール通知履歴エリア	閲覧

- 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  
 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
- FDP\_ACF.1.1** TSFは、以下の[割付: 表 5]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: TOE管理情報アクセス制御ポリシー]を実施しなければならない。

表 5: 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	利用者プロセス	ユーザー種別
オブジェクト	機器カウンター情報エリア	ユーザー種別リスト
オブジェクト	コール通知履歴エリア	ユーザー種別リスト
オブジェクト	デバイスファームウェア更新履歴エリア	ユーザー種別リスト

- 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: 表 6]に示すオブジェクトに対する操作のアクセスを管理する規則]。

表 6: アクセスを管理する規則

オブジェクトに対する操作	アクセスを管理する規則
機器カウンター情報エリアの閲覧	機器カウンター情報エリアに関連付けられたユーザー種別リストにリストされているユーザー種別(管理者、一般ユーザー)のいずれかが、利用者プロセスに関連付けられたユーザー種別と一致した場合、機器カウンター情報エリアの閲覧を許可する。
コール通知履歴エリアの閲覧	コール通知履歴エリアに関連付けられたユーザー種別リストにリストされているユーザー種別(管理者、一般ユーザー)のいずれかが、利用者プロセスに関連付けられたユーザー種別と一致した場合、コール通知履歴エリアの閲覧を許可する。
デバイスファームウェア更新履歴エリアの閲覧	デバイスファームウェア更新履歴エリアに関連付けられたユーザー種別リストにリストされているユーザー種別(管理者)のいずれかが、利用者プロセスに関連付けられたユーザー種別と一致した場合、デバイスファームウェア更新履歴エリアの閲覧を許可する。

- FDP\_ACF.1.3** TSFは、次の追加規則、[割付: セキュリティ属性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許可する規則はなし]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許可しなければならない。

FDP\_ACF.1.4 TSFは、次の追加規則、[割付: セキュリティ属性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拒否する規則はなし]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。

### 6.1.3 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: パソコンのWebブラウザからの5分以内の識別認証]に関して、[選択: [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[選択: に達する]とき、TSFは、[割付: 不成功となった管理用あるいは一般ユーザーのユーザー名によるパソコンからの識別認証に対して1分間拒絶]をしなければならない。

**FIA\_ATD.1** 利用者属性定義

下位階層: なし

依存性: 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を維持しなければならない。:[割付: ユーザー種別、一般ユーザーのユーザー名]

**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: 8文字以上13文字以下の次の括弧内のASCII文字(スペース!"#\$%&'()\*,-./0123456789:;<=>?@ABCDEFGHIJKLMNPOQRSTUVWXYZ[^\\_`abcdefghijklmnopqrstuvwxyz{|}~)で構成されたパスワード]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。

**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\_UAU.6**      **再認証**  
 下位階層:      なし  
 依存性:      なし  
 FIA\_UAU.6.1    TSF は、条件[割付: 管理者による管理者の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。
- 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。
- FIA\_USB.1**      **利用者・サブジェクト結合**  
 下位階層:      なし  
 依存性:      FIA\_ATD.1 利用者属性定義  
 FIA\_USB.1.1    TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: ユーザー種別、一般ユーザーのユーザー名]  
 FIA\_USB.1.2    TSFは、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 表 7にリストした属性の最初の関連付けに関する規則]

表 7: 属性の最初の関連付けに関する規則

利用者	利用者代行サブジェクト	セキュリティ属性の最初の関連付けルール
管理者	利用者プロセス	ユーザー種別に管理者を設定する ユーザー名をクリアする
一般ユーザー	利用者プロセス	ユーザー種別に一般ユーザーを設定する ユーザー名に一般ユーザーのユーザー名を設定する

- FIA\_USB.1.3    TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の変更の規則はなし]

**6.1.4 クラスFMT: セキュリティ管理**

- FMT\_MTD.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 TSFは、[割付: 表 8のTSFデータ]を[選択: 改変、削除[割付: 新規作成]]する能力を  
 [割付: 表 8のユーザー種別]に制限しなければならない。

表 8: TSF 情報管理のリスト

TSF データ	操作	ユーザー種別
管理者のパスワード	改変	管理者
一般ユーザーのユーザー名	新規作成、削除	管理者
一般ユーザーのパスワード	新規作成、改変、削除	管理者
年月日・時刻	改変	管理者
CE アクセス許可設定	改変	管理者
デバイスファームウェア更新許可設定	改変	管理者
RC Gate ファームウェア更新許可設定	改変	管理者

**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: 表 9にリストする管理機能]

表 9: 管理機能の特定のリスト

管理機能
管理者による管理者パスワードの改変
管理者による一般ユーザーのユーザー名の新規作成と削除
管理者による一般ユーザーのパスワードの新規作成、改変、および削除
管理者による年月日・時刻の改変
管理者による CE アクセス許可設定の改変
管理者によるデバイスファームウェア更新許可設定の改変
管理者による RC Gate ファームウェア更新許可設定の改変

**FMT\_SMR.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 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付けなければならない。

### 6.1.5 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。

**FPT\_TST.1** TSF テスト

下位階層: なし

依存性: なし

FPT\_TST.1.1 TSF は、[選択: [割付: CS 間通信保護機能]]の正常動作を実証するために、[選択: 許可利用者の要求時に]自己テストのスイートを実行しなければならない。

FPT\_TST.1.2 TSF は、許可利用者に、[選択: TSF データ]の完全性を検証する能力を提供しなければならない。

FPT\_TST.1.3 TSF は、許可利用者に、[選択: TSF]の完全性を検証する能力を提供しなければならない。

### 6.1.6 クラスFTA: TOEアクセス

**FTA\_SSL.3** TSF 起動による終了

下位階層: なし

依存性: なし

FTA\_SSL.3.1 TSF は、[割付: Web ブラウザよりログインした管理者および一般ユーザーの最終操作から、固定オートログアウト時間(5分)]後に対話セッションを終了しなければならない。

### 6.1.7 クラスFTP: 高信頼パス/チャンネル

**FTP\_ITC.1(a)** TSF 間高信頼チャンネル

下位階層: なし

依存性: なし

FTP\_ITC.1.1(a) TSF は、それ自身と他の高信頼 IT 製品(詳細化: CS)間に、他の通信チャン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ンネルデータの保護を提供する通信チャンネルを提供しなければならない。

FTP\_ITC.1.2(a) TSF は、[選択: TSF]が、高信頼チャン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(a) TSFは、[割付: 表 10記載の機能のリスト]のために、高信頼チャンネルを介して通信を開始しなければならない。

表 10: RC Gate-CS 間通信において高信頼チャンネルが要求される機能(a)

機能
機器カウンター通知機能
サービスコール機能
サブライコール機能
デバイスファームウェア更新機能
RC Gate ファームウェア更新機能

**FTP\_ITC.1(b) TSF 間高信頼チャンネル**

下位階層: なし

依存性: なし

FTP\_ITC.1.1(b) TSF は、それ自身と他の高信頼 IT 製品(詳細化: 登録 HTTPS 対応機)間に、他の通信チャン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ンネルデータの保護を提供する通信チャンネルを提供しなければならない。

FTP\_ITC.1.2(b) TSF は、[選択: TSF、他の高信頼 IT 製品]が、高信頼チャン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(b) TSFは、[割付: 表 11記載の機能のリスト]のために、高信頼チャンネルを介して通信を開始しなければならない。

表 11: RC Gate-登録 HTTPS 対応機間通信において高信頼チャンネルが要求される機能(b)

機能
機器カウンター通知機能
サービスコール機能
サブライコール機能

**FTP\_TRP.1 高信頼パス**

下位階層: なし

依存性: なし

FTP\_TRP.1.1 TSF は、それ自身と[選択: リモート]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、[選択: 改変、暴露]からの通信データの保護を提供する通信パスを提供しなければならない。

FTP\_TRP.1.2 TSF は、[選択: リモート利用者]が、高信頼パスを介して通信を開始することを許可しなければならない。

FTP\_TRP.1.3 TSFは、[選択: [割付:利用者によるパソコンの Web ブラウザを利用した TOE のリモート操作]]に対して、高信頼パスの使用を要求しなければならない。

## 6.2セキュリティ保証要件

本TOEの評価保証レベルはEAL3 である。TOEの保証コンポーネントを表 12に示す。これは評価保証レベルのEAL3 によって定義されたコンポーネントのセットであり、他の要件は追加していない。

表 12: 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
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.3 完全な要約を伴う機能仕様
	ADV_TDS.2 アーキテクチャ設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.3 許可の管理
	ALC_CMS.3 実装表現の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	ATE_COV.2 カバレッジの分析
	ATE_DPT.1 テスト: 基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テストサンプル
AVA: 脆弱性評価	AVA_VAN.2 脆弱性分析

### 6.3 セキュリティ機能要件根拠

本章では、追跡性、追跡性の正当化、および依存性が満たされていることから、「6.1 セキュリティ機能要件」であげたセキュリティ機能要件が妥当であることを示す。

#### 6.3.1 追跡性

TOEセキュリティ機能要件が1つ以上のTOEセキュリティ対策方針までさかのぼれること(追跡性)を、それぞれの対応関係を表 13に明記することで示す。表中「✓」は、対応関係にあることを示している。

表 13: セキュリティ対策方針と機能要件の関連

	O.I&A	O.ACCESS	O.COM_CS	O.COM_ATR_DEVICE	O.COM_OPERATOR	O.GENUINE	O.AUDIT_LOGGED
FAU_GEN.1							✓
FAU_GEN.2							✓
FAU_SAR.1							✓
FAU_SAR.2							✓
FAU_STG.1							✓
FAU_STG.4							✓
FDP_ACC.1		✓					
FDP_ACF.1		✓					
FIA_AFL.1	✓						
FIA_ATD.1	✓						
FIA_SOS.1	✓						
FIA_UAU.2	✓						
FIA_UAU.6	✓						
FIA_UID.2	✓						
FIA_USB.1	✓						
FMT_MTD.1		✓					
FMT_SMF.1		✓					
FMT_SMR.1		✓					
FPT_STM.1							✓
FPT_TST.1						✓	

FTA_SSL.3	✓						
FTP_ITC.1(a)			✓				
FTP_ITC.1(b)				✓			
FTP_TRP.1					✓		

### 6.3.2 追跡性の正当化

本章では、TOE セキュリティ機能要件が TOE セキュリティ対策方針を満たすことを示す。

#### O.I&A 識別認証

O.I&A は、一般ユーザーあるいは管理者だけに TOE のリモート操作を許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

- (1) TOE をリモート操作する利用者は識別認証に成功していなければならない  
FIA\_UID.2 によって、TOE をリモート操作しようとする者が利用者であることを識別し、FIA\_UAU.2 によって、識別された利用者が認証に成功することを要求する。
- (2) 認証に成功した利用者は、セッション継続中 TOE をリモート操作できる  
FIA\_USB.1 によって一般ユーザーと管理者は、利用者プロセスに関連付けられ、利用者プロセスにはユーザー種別とユーザー名のセキュリティ属性を関連付けられ、FIA\_ATD.1 によって、これらセキュリティ属性が維持されることによって、一般ユーザーまたは管理者に TOE のリモート操作が許可される。
- (3) TOE リモート操作のセッションを自動で終了する  
FTA\_SSL.3 によって、一定時間操作がない場合にオートログアウトすることによって、認証に成功した利用者が、セッションが接続したままパソコンから離れても、認証に成功した利用者以外が、そのパソコンから TOE をリモート操作する機会を減少させる。
- (4) 一般ユーザーと管理者のパスワードの解析を困難にする  
FIA\_SOS.1 によって、パスワードは、文字数および文字種組合せにおいて、パスワードの解析が困難になる品質を維持し、FIA\_AFL.1 によって、パスワード解析のための十分な時間を与えない。
- (5) 管理者のパスワード変更前に利用者を再認証する  
管理者以外の者が管理者のパスワードを変更することを防ぐために、FIA\_UAU.6 によって、利用者が管理者のパスワード変更をする前に利用者の再認証を行なう。

O.I&A を実現するために必要な対策は(1)、(2)、(3)、(4)、(5)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FIA\_AFL.1、FIA\_ATD1、FIA\_SOS.1、FIA\_UAU.2、FIA\_UAU.6、FIA\_UID.2、FIA\_USB.1、FTA\_SSL.3 を達成することで O.I&A を実現できる。

#### O.ACCESS アクセス制限

O.ACCESS は、利用者のユーザー種別に応じて保護資産へのアクセスを制御できるようにするセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

- (1) 機器カウンター情報エリア、コール通知履歴エリア、およびデバイスファームウェア更新履歴エリアのアクセス制御を規定して実施する

FDP\_ACC.1、FDP\_ACF.1 によって、TOE 管理情報アクセス制御ポリシーに従い、利用者プロセスに関連付けられたユーザー種別が管理者の場合、機器カウンター情報エリア、コール通知履歴エリア、およびデバイスファームウェア更新履歴エリアの閲覧を許可し、一般ユーザーの場合は、機器カウンター情報エリアとコール通知履歴エリアの閲覧を許可する。

- (2) セキュリティ管理を管理者だけに許可する

FMT\_MTD.1、および FMT\_SMF.1 によって、TSF データの操作は管理者だけに許可する。

- (3) ユーザー種別を維持する

FMT\_SMR.1 によって、識別認証された管理者は、セッション中は管理者として維持しセキュリティ管理機能を許可する。

O.ACCESS を実現するために必要な対策は(1)、(2)、(3)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FDP\_ACC.1、FDP\_ACF.1、FMT\_MTD.1、FMT\_SMF.1、および FMT\_SMR.1 を達成することで O.ACCESS を実現できる。

### **O.COM\_CS CS との通信チャンネル保護**

O.COM\_CS は、正しい CS と通信することを保証し、CS と通信する際に通信データを秘匿し、改ざんを検知することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

- (1) 正しい CS と通信する

FTP\_ITC.1(a)によって、TOE と CS 間の通信において CS を識別する機能を提供する通信チャンネルを提供し、CS の正当性を検証する。

- (2) CS との通信データを保護する

FTP\_ITC.1(a)によって、TOE と CS 間の通信において信頼される通信チャンネルを確立し、通信経路上の保護資産の漏えいを保護し、改ざんを検知する。

O.COM\_CS を実現するために必要な対策は(1)、(2)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FTP\_ITC.1(a)を達成することで O.COM\_CS を実現できる。

### **O.COM\_ATR\_DEVICE デバイスとの通信チャンネル保護**

O.COM\_ATR\_DEVICE は、カウンター情報通知機能、サービスクール機能、およびサブライコール機能において、登録されたデバイスと通信することを保証し、LAN 内の登録 HTTPS 対応機と TOE 間の通信データを秘匿し、改ざんを検知することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

- (1) 正しい HTTPS 対応機と通信する

FTP\_ITC.1(b)によって、TOE と登録 HTTPS 対応機間の通信において HTTPS を識別する機能を提供する通信チャンネルを提供し、登録 HTTPS 対応機の正当性を検証する。

- (2) 登録 HTTPS 対応機との通信データを保護する

FTP\_ITC.1(b)によって、TOE と登録 HTTPS 対応機間の通信において信頼される通信チャンネルを確立し、通信経路上の通信データを秘匿し、改ざんを検知する。

O.COM\_ATR\_DEVICE を実現するために必要な対策は(1)、(2)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FTP\_ITC.1(b)を達成することで O.COM\_ATR\_DEVICE を実現できる。

### **O.COM\_OPERATOR 利用者のリモート操作データ保護**

O.COM\_OPERATOR は、利用者によるパソコンの Web ブラウザを使った TOE のリモート操作時の通信における通信経路上にある通信データを秘匿し、改ざんを検知することを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

(1) 利用者のリモート操作による通信データを保護する

FTP\_TRP.1 によって、TOE と利用者がリモート操作で利用するパソコン間には高信頼パスで通信し、通信経路上の通信データを秘匿し、改ざんを検知する。

O.COM\_OPERATOR を実現するために必要な対策は(1)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FTP\_TRP.1 を達成することで O.COM\_OPERATOR を実現できる。

### **O.GENUINE RC Gate ファームウェアの完全性確認**

O.GENUINE は、TOE に組み込まれている RC Gate ファームウェアが正規のものであることを保証するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

(1) RC Gate ファームウェアの完全性をチェックする

FPT\_TST.1 によって、TOE は、許可利用者の要求時に RC Gate ファームウェアの実行コードの完全性を検証し、正規の RC Gate ファームウェアであることを検証する。

O.GENUINE を実現するために必要な対策は(1)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FPT\_TST.1 を達成することで O.GENUINE を実現できる。

### **O.AUDIT\_LOGGED 監査ログ記録管理**

O.AUDIT\_LOGGED は、セキュリティ侵害を検証するために必要な事象(監査ログ機能の起動と終了、監査ログの読出し、利用者識別認証機能の実施、アカウント情報の操作、日時の更新、CS との通信失敗、セルフチェックの実施)発生時に監査ログを記録し、さらに監査ログの参照を RC Gate 管理権限を持つ管理者に許可するセキュリティ対策方針である。このセキュリティ対策方針を実現するには、下記の対策を満たすことが必要である。

(1) 監査ログを記録する

FAU\_GEN.1 および FAU\_GEN.2 によって、セキュリティ監査に必要な事象(監査ログ機能の起動と終了、監査ログの読出し、利用者識別認証機能の実施、アカウント情報の操作、日時の更新、CS との通信失敗、セルフチェックの実施)が発生した時に、その事象をもたらした利用者識別情報を含め、セキュリティ監査に必要な情報を記録する。

(2) 監査機能を提供する

FAU\_SAR.1 によって、RC Gate 管理権限を持つ管理者が検証できる形式で監査ログを読み出せるようにし、FAU\_SAR.2 によって RC Gate 管理権限を持つ管理者以外が監査ログを読み出すことを禁止する。

(3) 監査ログを保護する

FAU\_STG.1 によって、監査ログは改変から保護され、FAU\_STG.4 によって監査ログファイルがいったい状態の状態で監査対象の事象が発生した場合は、タイムスタンプの最も古い監査ログに新しい監査ログを上書きして記録する。

## (4) 信頼できる事象発生時間

FPT\_STM.1 によって、信頼できるタイムスタンプが提供され、監査ログには監査事象が発生した正確な時間が記録される。

O.AUDIT\_LOGGED を実現するために必要な対策は(1)、(2)、(3)、(4)である。したがって、これら対策に必要なセキュリティ機能要件として該当する FAU\_GEN.1、FAU\_GEN.2、FAU\_STG.1、FAU\_STG.4、FAU\_SAR.1、FAU\_SAR.2、FPT\_STM.1 を達成することで O.AUDIT\_LOGGED を実現できる。

## 6.3.3 依存性分析

TOEセキュリティ機能要件の依存性の対応状況を表 14に示し、依存性が満たされていないTOEセキュリティ機能要件については、その正当性について示す。

表 14: TOE セキュリティ機能要件の依存性対応表

TOE セキュリティ機能要件	CC が要求する依存性	ST の中で満たしている依存性	ST の中で満たしていない依存性
FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2	なし
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_STG.4	FAU_STG.1	FAU_STG.1	なし
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1	FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2	なし
FIA_ATD.1	なし	なし	なし
FIA_SOS.1	なし	なし	なし
FIA_UAU.2	FIA_UID.1	FIA_UID.2	なし
FIA_UAU.6	なし	なし	なし
FIA_UID.2	なし	なし	なし
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	なし
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.2	なし
FPT_STM.1	なし	なし	なし
FPT_TST.1	なし	なし	なし

TOE セキュリティ 機能要件	CC が要求する 依存性	ST の中で 満たしている 依存性	ST の中で 満たしていない 依存性
FTA_SSL.3	なし	なし	なし
FTP_ITC.1(a)	なし	なし	なし
FTP_ITC.1(b)	なし	なし	なし
FTP_TRP.1	なし	なし	なし

以下に、依存性が満たされていなくても問題ない根拠を記述する。

#### FDP\_ACF.1 から FMT\_MSA.3 への依存性除去理由

オブジェクト(機器カウンター情報エリア、コール通知履歴エリア、デバイスファームウェア更新履歴エリア)のセキュリティ属性は固定で初期化されることは無い。サブジェクト(利用者プロセス)のセキュリティ属性は固定で初期化されることは無いしたがって、FMT\_MSA.3 は不要である。

## 6.4 セキュリティ保証要件根拠

本 TOE は、一般的なオフィス環境で使用する商用製品であり、想定する攻撃は、基本的な攻撃能力を持つ攻撃者によるインターネットからの攻撃と、TOE を設置するオフィス内での誤使用による保護資産の漏えいと変更である。

このような攻撃に対して、TOE 設計の評価、TOE をセキュアに利用する方法がガイダンスに記述されていることの評価、攻撃をより困難にするために関連情報の秘密を守る必要があり、開発環境についてもセキュアな環境であることの評価を含む。これら保証要件は、EAL3 適合であるため、すべての保証要件が依存性を満たすことは明白である。したがって、EAL3 は妥当である。

## 7 TOE要約仕様

本章は、6.1 章で記述されたセキュリティ機能要件を TOE が満たす方法・メカニズムについてセキュリティ機能要件ごとに記述する。

### FAU\_GEN.1 監査データ生成

TOE は、以下示す監査対象事象発生時に監査ログを生成し監査ログファイルへ追加する。

- 監査機能の開始
- 監査機能の終了
- ログイン
- ロックアウトの発生
- 管理者パスワードの変更
- 一般ユーザーの新規作成
- 一般ユーザーパスワードの変更
- 一般ユーザーの削除
- 年月日時分の設定
- CS との SSL 暗号化通信の失敗
- 自己テストの実施
- 監査ログの読み出し

※監査機能の開始と終了事象は、TOE の起動事象で代用する。

セキュリティ監査ログを構成する情報は以下の通りである。

- 事象の日付・時刻
- 事象の種別
- ユーザー種別
- ユーザー名(一般ユーザーの場合)
- 結果

### FAU\_GEN.2 利用者識別情報の関連付け

TOE は、監査対象事象の発生要因となった利用者が、管理者ならばユーザー種別、一般ユーザーならば当該一般ユーザーのユーザー名を監査ログに含めて記録する。

### FAU\_SAR.1 監査レビュー

TOE は、パソコンの Web ブラウザから監査ログを参照できる機能を持ち、この機能を管理者に提供する。

**FAU\_SAR.2 限定監査レビュー**

TOEは、パソコンの Web ブラウザから監査ログを参照できる機能をユーザー種別が管理者以外の利用者には提供しない。

**FAU\_STG.1 保護された監査証拠格納**

TOE は、監査ログおよび監査ログファイルに対する削除・変更するための機能を提供しない。

**FAU\_STG.4 監査データ損失の防止**

TOE は、監査ログファイルに監査ログを追加記録する領域がない場合には、最新の監査ログを最も古い監査ログに上書きする。

**FDP\_ACC.1 サブセットアクセス制御**

TOE は、TOE 管理情報アクセス制御ポリシーを実施する。TOE 管理情報アクセス制御ポリシーは、管理者と一般ユーザーに機器カウンター情報エリア、コール通知履歴エリアの閲覧を許可し、管理者にデバイスファームウェア更新履歴エリアの閲覧を許可するアクセス制御ポリシーである。

**FDP\_ACF.1 セキュリティ属性によるアクセス制御**

TOE は、識別認証で成功した利用者に機器カウンター情報エリア、およびコール通知履歴エリアを閲覧できる画面を提供し、識別認証で成功した利用者のユーザー種別が管理者の場合だけデバイスファームウェア更新履歴エリアの閲覧ができる画面を提供する。また TOE は、機器カウンター情報エリア、コール通知履歴エリアおよびデバイスファームウェア更新履歴エリアを変更あるいは削除するインターフェースを実装しない。

**FIA\_AFL.1 認証失敗時の取り扱い**

TOE は、パソコンの Web ブラウザから 5 分以内の認証失敗回数を利用者毎にカウントし、失敗回数が 3 回になった利用者に対して、3 回目の認証失敗した時点から 1 分間は識別認証機能で正しいパスワードを入力しても認証失敗にする。利用者認証に成功した場合は、その利用者の失敗回数を 0 にリセットする。

**FIA\_ATD.1 利用者属性定義**

TOE は、利用者が識別認証時に選択したユーザー種別をセッション終了まで維持する。利用者が一般ユーザーの場合は、識別認証時に入力したユーザー名も関連付けて維持する。

**FIA\_SOS.1 秘密の検証**

TOE は、管理者が、管理者および一般ユーザーのパスワードを変更する際、(1)に記載する文字で、かつ(2)の条件に合致することをチェックし、条件に合致した場合はパスワードを登録し、条件に合致しない場合はログインパスワード登録せずエラー表示する。

(1) 使用できる文字とその文字種: 次の ASCII 文字。

スペース!"#\$%&'()\*+,-./0123456789:;<=>?@`{|}~  
ABCDEFGHIJKLMNOPQRSTUVWXYZ[¥]^\_

abcdefghijklmnopqrstuvwxy

(2) 登録可能な桁数: 8 文字以上 13 文字以下

#### **FIA\_UAU.2**      **アクション前の利用者認証**

TOE は、パソコンの Web ブラウザから利用しようとする者に対して、ログイン画面を表示する。ログイン画面には、ユーザー種別、ユーザー名、パスワードを入力する領域があり、管理者はユーザー種別とパスワード、一般ユーザーはユーザー種別、ユーザー名、パスワードを入力する。TOE は、認証に成功するまでは他の画面に遷移しない。

#### **FIA\_UAU.6**      **再認証**

TOE は、管理者のパスワード変更を管理者用の画面から提供し、管理者が、パスワードの変更を選択した時に管理者パスワードの入力を要求し、入力されたパスワードで再認証する。

#### **FIA\_UID.2**      **アクション前の利用者識別**

TOE は、パソコンの Web ブラウザから利用しようとする者に対して、ユーザー種別、ユーザー名、パスワードを入力するログイン画面を表示し認証に成功するまでは他の画面に遷移しない。

#### **FIA\_USB.1**      **利用者・サブジェクト結合**

TOE は、識別認証に成功した利用者を利用者プロセスと結合する。利用者プロセスは、ユーザー種別とユーザー名をセキュリティ属性として関連付ける。

#### **FMT\_MTD.1**      **TSF データの管理**

TOE は、識別認証で成功した利用者のユーザー種別が管理者の場合だけ、下記の通り TSF データに対する操作をするための画面を提供する。

- 管理者のパスワードの変更
- 一般ユーザーのユーザー名の新規作成、削除
- 一般ユーザーのパスワードの新規作成、変更、削除
- 年月日・時刻の変更
- CE アクセス許可設定の変更
- デバイスファームウェア更新許可設定の変更
- RC Gate ファームウェア更新許可設定の変更

#### **FMT\_SMF.1**      **管理機能の特定**

TOE は、識別認証で成功した利用者のユーザー種別が管理者の場合だけ、下記の操作をするための画面を提供する。

- 管理者による管理者パスワードの変更
- 管理者による一般ユーザーのユーザー名の新規作成、削除
- 管理者による一般ユーザーのパスワードの新規作成、変更、削除

- 管理者による年月日・時刻の変更
- 管理者による CE アクセス許可設定の変更
- 管理者によるデバイスファームウェア更新許可設定の変更
- 管理者による RC Gate ファームウェア更新許可設定の変更

**FMT\_SMR.1 セキュリティの役割**

TOE は、識別認証に成功した管理者と結合した利用者プロセスに関連付けられたユーザー種別(管理者)は、識別認証に成功した時点から Web ブラウザからのセッションが終了するまで維持される。

**FPT\_STM.1 高信頼タイムスタンプ**

TOE は、監査ログに記録する日付(年月日)・時間(時分秒)のため TOE のシステム時計を提供する。

**FPT\_TST.1 TSF テスト**

TOE は、管理者の要求時に CS 間通信保護機能の正常動作を自己テストする。また、TOE は TSF データおよび RC Gate ファームウェアの実行コードの完全性を検証するための自己テストをする。

**FTA\_SSL.3 TSF 起動による終了**

TOE は、利用者が Web ブラウザよりログイン後、Web ブラウザからの最終操作から、固定オートログアウト時間(5分)経過した場合に、強制的にオートログアウトする機能を提供する。

**FTP\_ITC.1(a) TSF 間高信頼チャンネル**

TOE は、CS と SSL 通信をし正規の CS であることを認証するとともに、機器カウンター通知機能、サービスコール機能、サブライコール機能、デバイスファームウェア更新機能、および RC Gate ファームウェア更新機能において、TOE と CS 間の LAN 経由通信を SSL 暗号化通信する。

**FTP\_ITC.1(b) TSF 間高信頼チャンネル**

TOE は、登録 HTTPS 対応機と SSL 通信をし正規の登録 HTTPS 対応機であることを認証するとともに、機器カウンター通知機能、サービスコール機能、およびサブライコール機能において、TOE と登録 HTTPS 対応機間を SSL 暗号化通信する。

**FTP\_TRP.1 高信頼パス**

TOE は、パソコンの Web ブラウザからのリモートアクセスに対して SSL 通信をし、TOE とパソコン間の通信を SSL 暗号化通信する。