RICOH Remote Communication Gate A2
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　　: 2016-11-10
バージョン　　: 0.42

更新履歴

Version	Date	Author	Description
0.10	2013-07-23	株式会社リコー	第1版
0.11	2014-02-19	株式会社リコー	以下の節、図から“一般ユーザー”を削除。 ・1.4.3 関係者定義 ・1.4.5 保護資産 ・3.1 脅威 ・図 3. TOE の論理的範囲
0.12	2014-02-19	株式会社リコー	メール通知機能追加
0.13	2014-10-27	株式会社リコー	・4 章以降を追加
0.14	2014-11-12	株式会社リコー	cPP に近い記載に修正 ・3章 ・4章
0.15	2014-11-17	株式会社リコー	cPP に近い記載に修正 ・5 章 ・6 章 ・7 章
0.16	2014-11-20	株式会社リコー	メール通知機能時の S/MIME について追記など
0.17	2014-11-27	株式会社リコー	印刷時図 2 の表示が乱れを解消
0.18	2015-02-09	株式会社リコー	・評価者コメント RDZ-ASE_COM-0001-00 No.1～21 の対応 ・組織のセキュリティ対策方針を脅威に移動
0.19	2015-02-17	株式会社リコー	・評価者コメント RDZ-ASE_COM-0001-01 No.12、No.22～27,30,32～36 の対応
0.20	2015-02-24	株式会社リコー	5.1 章 FPT_FUD の記述変更と関連箇所の変更 7 章 FAU_GEN.1 の TSS 記述訂正
0.21	2015-02-26	株式会社リコー	・評価者コメント RDZ-ASE_ECOM-0001-02 No.37～40 の対応
0.22	2015-03-09	株式会社リコー	FPT_FUD.2 の誤記修正 5.1 章、6.1.5 章、7 章
0.23	2015-04-30	株式会社リコー	・評価者コメント RDZ-ECOM-ASE-0001-03 No34～42 の対応
0.24	2015-05-14	株式会社リコー	・RDZ-ERE-0003-00 に対応
0.25	2015-06-29	株式会社リコー	・機器ファームウェア更新履歴は TOE で扱わない仕様になったため保護資産から削除 ・PC から操作が無い場合はオートログアウトではなくスクリーンロクだったため、FTP_SSL.3 から FTP_SSL.1 に変更 ・RDZ-ECOM_ASE-0001-04 に対応
0.26	2015-07-24	株式会社リコー	・RDZ-ECOM_ASE-0001-07 に対応

0.27	2015-07-30	株式会社リコー	・RDZ-ECOM_ASE-0001-08 に対応
0.28	2015-08-07	株式会社リコー	・RDZ-ECOM_ASE-0001-09 に対応
0.29	2015-08-07	株式会社リコー	図3アクセス制御機能を削除
0.30	2015-08-21	株式会社リコー	図 1 の SMTP サーバを追加
0.31	2015-10-16	株式会社リコー	・RDZ-ECOM_ASE-0001-10　No.119-120 に対応
0.32	2015-12-17	株式会社リコー	・RDZ-ECOM_ASE-0001-10　No.121 に対応
0.33	2016-01-08	株式会社リコー	・RDZ-ECOM_ASE-0001-12　No.122-130 に対応
0.34	2016-01-13	株式会社リコー	ガイダンス名称追加。誤記訂正。
0.35	2016-02-09	株式会社リコー	・RDZ-ECOM_ASE-0001-12　No.131-132 に対応 ・TOE 改修による TOE バージョン変更
0.36	2016-03-16	株式会社リコー	・ガイダンスの版を変更
0.37	2016-05-19	株式会社リコー	・RDZ-ECOM_ASE-0001-14　No.133-137 に対応
0.38	2016-05-23	株式会社リコー	・RDZ-ECOM_ASE-0001-15　No.138-143 に対応
0.39	2016-07-05	株式会社リコー	・誤字修正 ・監査関連訂正
0.40	2016-08-25	株式会社リコー	・誤字修正 ・監査関連訂正
0.41	2016-09-15	株式会社リコー	・ガイダンス一覧を訂正
0.42	2016-11-10	株式会社リコー	・脅威訂正 ・誤字修正 1.4.4.2 セキュリティ機能修正 2.1 CC 適合主張 ・図表番号修正

目次

図一覧

表一覧

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　　: RICOH Remote Communication Gate A2 セキュリティターゲット

バージョン　　: 0.42

作成日付　　: 2016-11-10

作成者　　:株式会社リコー

1.2 TOE 参照

TOE である、RICOH Remote Communication Gate A2(以下、RC Gate A2)の識別情報を以下に記す。

製造者　　:株式会社リコー

製品名称　　: RICOH Remote Communication Gate A2

ファームウェアバージョン　　: V1.0.2

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を述べる。

1.3.1 TOE 種別

TOE は、デジタル複合機やプリンター（以下、デバイス）を保守センターのコミュニケーションサーバ（以下、CS）からリモートで保守をする@Remote サービスで利用する IT 機器である。TOE は、CS と@Remote サービスの対象となるデバイス（以下、@Remote 対象機）の間におかれ、@Remote サービスに必要な情報の通信を仲介する。

1.3.2 TOE の使用方法

TOE は、@Remote 対象機を接続している LAN に接続して使用する。TOE の利用者は、Web ブラウザから TOE へアクセスして操作をする。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。

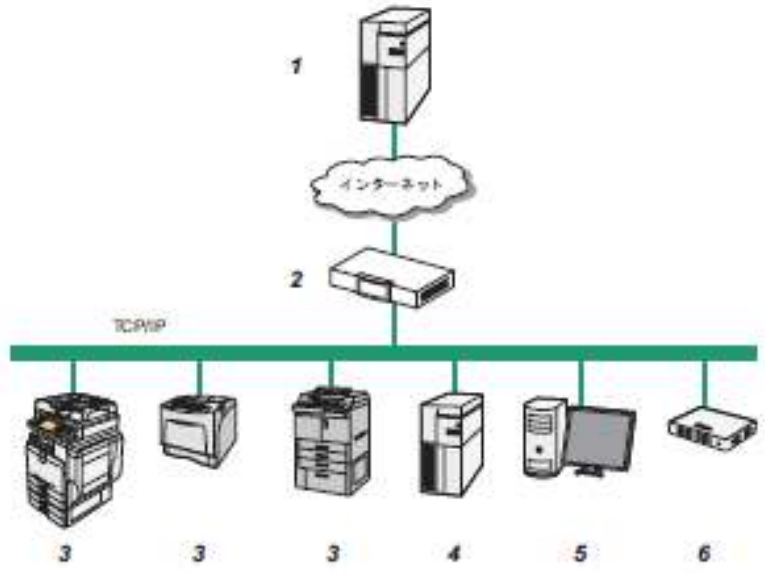


図 1: TOE の接続形態

1. CS
   保守センターのサーバ。@Remote 対象機から@Remote サービスに必要な情報を、TOE を介して送受信する。TOE との通信は、TOE からの起動のみとなる。
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[1]
   TOE との通信機能を持ったデジタル複合機とプリンターのことであり（以下、@Remote 対象機）、リコー製のデバイスに限らない。この中でリモート管理サービス機能を持ったリコー製のデバイスを HTTPS 対応機と言い、リモート管理サービス機能を持たず SNMP の機能をもつ他社製品を含むデバイスを SNMP 対応機という。デバイスが HTTPS 対応機の場合は、リコーのホームページと当該デバイスのマニュアルにリモート管理サービス機能を実装していることを記載している。
   TOE に@Remote サービス対象と登録しているデバイスを@Remote 対象機と言う。
   さらに、@Remote サービスの対象となる HTTPS 対応機と SNMP 対応機を、それぞれ登録 HTTPS 対応機、登録 SNMP 対応機と言う。TOE との通信が保護されるのは登録 HTTPS 対応機である。
4. SMTP サーバ
   TOE がメール送信する際に使用するメール送信用サーバ。TOE は、CS へ送付する機器カウンター情報、障害情報、およびサプライ情報を管理者が TOE へ設定したメールアドレスへメール送信する。
5. PC
   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、PC 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、Internet Explorer 8 以降と Firefox 28.8 以降[2]。

[1] CC 評価に使用したデバイス（HTTPS 対応機）は RICOH MP C305、RICOH IPSiO SP 8300、RICOH MP C401 の 3 機種である。

[2] CC 評価構成では Web ブラウザは Internet Explore 及び Firefox の双方が利用可能であることを想定している。また、CC 評価のテストにて使用したブラウザは、Internet Explorer 8/9/10/11 と FireFox 44.0.2 である。

6. RC Gate A2
   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 SD カード（以下、SD カードオプション、製品名：RICOH Remote Communication Gate A2 Storage 1000）が TOE に搭載可能である。SD カードオプションを搭載した環境も利用環境に含める。

1.3.3 TOE の主要なセキュリティ機能

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 A2 ファームウェア正当性確認機能、セキュリティ管理機能、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、および登録 HTTPS 対応機)の通信経路と TOE から送信するeメールの情報を保護する機能である。
利用者制限機能は、PC から TOE を利用しようとするものに対して利用者の識別認証を行い（以下、利用者識別という）、利用者識別認証に成功した利用者に対し、TOE の操作を許可する機能である。
RC Gate A2 ファームウェア正当性確認機能は、ネットワーク経由で受信した 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する機能である。
セキュリティ管理機能は、TOE の設定を許可された利用者だけに許可する機能である。
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。

1.4 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。

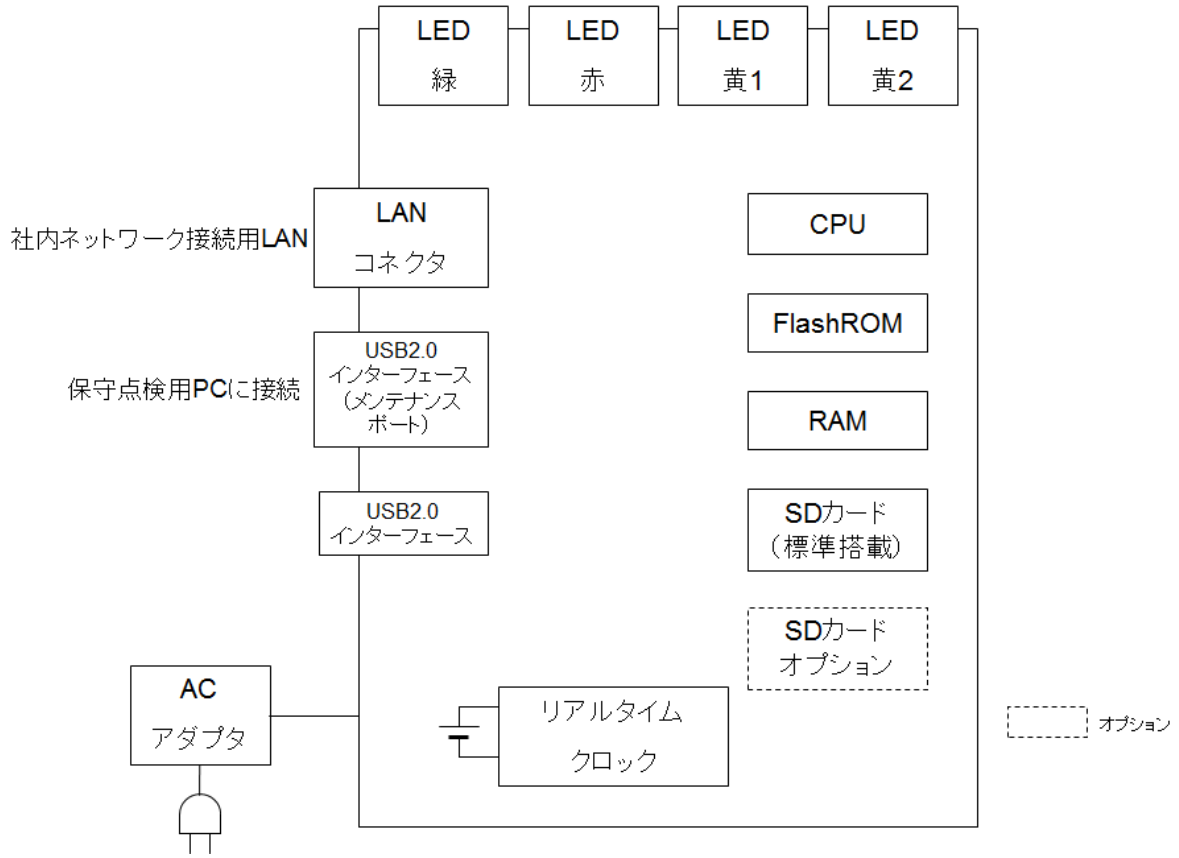


図 2: TOE のハードウェア構成

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。

FlashROM

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、証明書が記録されている。

RAM

揮発性の半導体メモリであり、TOE がデータを一時的に記憶するために利用する。

SD カード（標準搭載）

不揮発性の半導体メモリである。RC Gate A2 ファームウェア（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）、初期情報が工場で書き込まれる。運用時には、監査ログ、@Remote 対象機のデータの書き込み、一時的な蓄積メモリとして利用される。

SD カードオプション

オプションの不揮発性の半導体メモリである。@Remote 対象機の管理台数を拡張する場合に利用される。運用時には、拡張した@Remote 対象機のデータが書き込まれる。

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。

LAN コネクタ

PC、CS、および@Remote 対象機と通信するための社内ネットワーク接続用 LAN コネクタである

USB2.0 インターフェース（メンテナンスポート）

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 PC を接続する USB コネクタである。

USB2.0 インターフェース

オプションの 3G モジュールを接続する USB コネクタである。

LED（緑、赤、黄1、黄 2）

TOE のステータス、エラー状態によって点灯/消灯/遅点滅/早点滅するランプである。

AC アダプタ

電力を供給するための電源装置である。

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。

TOE の利用者向けガイダンス(日本仕向け)

- Remote Communication Gate A2 安全上のご注意 (D3AR-8500)
- Remote Communication Gate A2 セットアップガイド (D3AR-8520)
- Remote Communication Gate A2 使用説明書 (D3AR-8540C)

TOE の利用者向けガイダンス(北米仕向け)

- Remote Communication Gate A2 Safety Information (D3AR-8610)

TOE の利用者向けガイダンス(欧州仕向け)

- Remote Communication Gate A2 Safety Information (D3AR-8600)

TOE の利用者向けガイダンス(北米/欧州仕向け)

- Remote Communication Gate A2 Setup Guide (D3AR-8620)
- Remote Communication Gate A2 Operating Instructions (D3AR-8640C)

1.4.3 関係者定義

TOE に係る関係者を以下定義する。

管理者

TOE を管理するお客様の管理者をさす。PC から TOE の設定変更、ステータス閲覧、監査ログ閲覧ができる。本文中で単に「管理者」と呼ぶときは、この TOE の管理者をさす。

機器管理者

機器管理者とは、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。

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、管理者の指示のもと TOE の保守をする者をさす。

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。

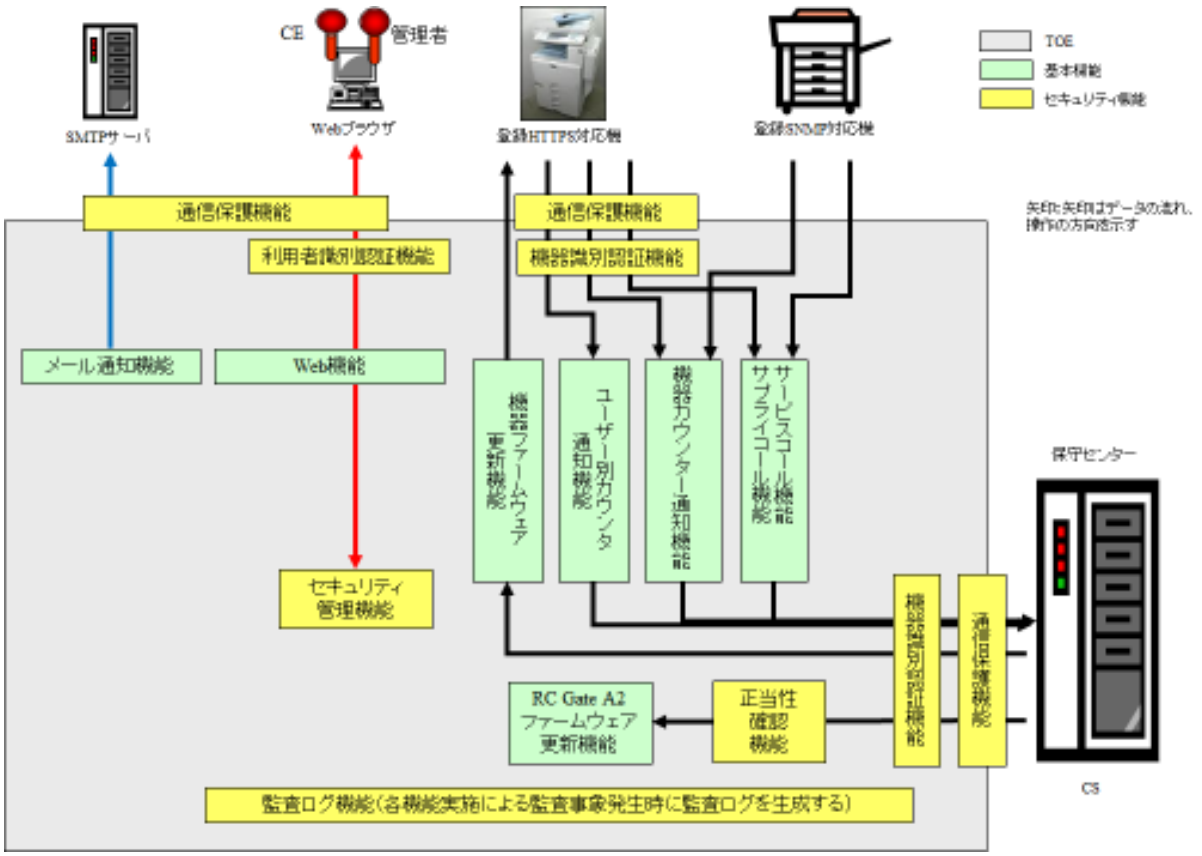


図 3: TOE の論理的範囲

1.4.4.1 基本機能

サービスコール機能

TOE は、登録 HTTPS 対応機および登録 SNMP 対応機から受信した機器障害情報を CS に通報する。

機器カウンター通知機能

TOE は、登録 HTTPS 対応機および登録 SNMP 対応機から受信した、各デバイスの印刷枚数(以下、機器カウンター情報)を定期的に CS に通知する。

ユーザー別カウンター取得機能

TOE は、登録 HTTPS 対応機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。

サプライコール機能

TOE は、登録 HTTPS 対応機および登録 SNMP 対応機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。

機器ファームウェア更新機能

TOE が、CS から受信した機器ファームウェアで、登録 HTTPS 対応機のファームウェアを更新する機能。

RC Gate A2 ファームウェア更新機能

TOE が、CS から受信した更新用ファームウェアで TOE 自身のファームウェアをアップデートする機能。

Web 機能

利用者が、TOE に情報の入出力をするためのユーザーインターフェース機能。利用者は、PC から Web ブラウザを使って TOE へアクセスし本機能を利用する。

メール通知機能

サービスコール機能、機器カウンター通知機能、ユーザー別カウンター機能、およびサプライコール機能で TOE から CS へ送付する情報を、管理者が指定するメールアドレスに TOE が送信する機能。

1.4.4.2 セキュリティ機能

利用者識別認証機能

TOE は、PC から Web ブラウザを介して TOE へアクセスする利用者の識別認証を行い、成功した場合のみ利用者に TOE の操作を許可する。

機器識別認証機能

TOE は、ネットワークを介してアクセスする IT 製品が正規の CS または登録 HTTPS 対応機であることの検証を行う。

通信保護機能

TOE は、登録 HTTPS 対応機、CS、PC、および SMTP サーバとの通信において通信する情報の漏えいを防止し、改ざんを検出する。TOE と SNMP 対応機の通信は本機能の対象とはならない。

正当性確認機能

TOE は、CS からネットワーク経由で受信した TOE の更新用のファームウェアが、製造元が提供するファームウェアであることを確認する。

セキュリティ管理機能

TOE は、利用者の役割に応じて TOE の管理機能の利用を制限する。

監査機能

TOE は、利用者識別認証機能、セキュリテイ管理機能、正当性確認機能、及び CS の識別認証機能事象発生時に、監査に必要な情報を監査ログとして TOE 内に記録する。また、TOE 内の監査ログの変更、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、機器ファームウェア、RC Gate A2 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、@Remote 対象機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、@Remote 対象機から 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。@Remote 対象機から CS へ送信される機器カウンター情報が改ざんされると、@Remote 対象機が適切な@Remote サービスを受けられなくなる。
本情報についてはインターネット通信では CS と TOE 間での機密性と完全性を維持する。LAN 環境では、HTTPS 対応機と TOE の通信において機密性と完全性を維持する。

障害情報、サプライ情報

障害情報、サプライ情報は、@Remote 対象機から TOE に送信され、随時 TOE から CS へ送信される。@Remote 対象機から 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、@Remote 対象機が適切な@Remote サービスを受けられなくなる。
本情報についてはインターネット通信では CS と TOE 間での機密性と完全性を維持する。LAN 環境では、HTTPS 対応機と TOE の通信において機密性と完全性を維持する。

機器ファームウェア

機器ファームウェアとは、登録 HTTPS 対応機のファームウェアのことである。機器ファームウェアは、CS から TOE を経由して登録 HTTPS 対応機にインストールされる。

本情報についてはインターネット通信では CS と TOE 間での機密性を維持する。機器ファームウェアの完全性は、CS がファームウェアに署名し、HTTPS 対応機が署名検証するというメカニズムによって、本 TOE の機能とは別に保証されている。従って、本 TOE は、この署名―署名検証メカニズムに追加して、CS と TOE 間の通信経路上で機器ファームウェアを保護するメカニズムのみを提供し、HTTPS 対応機と TOE 間の保護メカニズムは提供しない。

RC Gate A2 ファームウェア

RC Gate A2 ファームウェアは、TOE のファームウェアのことである。製造工場で TOE にインストールされ利用者に配付される。また、TOE の管理者が許可することによって、RC Gate A2 ファームウェア更新機能で更新することもある。RC Gate A2 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。
本情報についてはインターネット通信で CS と TOE 間での機密性と完全性を維持する。

TSF データ

TSF データは、TOE 内に記録されているデータで管理者パスワード、CE パスワード、年月日・時刻、CE アクセス許可設定、機器ファームウェア更新許可設定、RC Gate A2 ファームウェア更新許可設定、スクリーンロック時間、およびメール通知の送信先、機器証明書情報、SSL/TLS 設定がある。
本情報については LAN 環境で Web ブラウザと TOE の通信において機密性と完全性を維持する。

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。
機器受信情報	TOE が@Remote 対象機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。
スクリーンロック機能	PC から RC Gate にログイン中に操作されない時間が、管理者が設定するスクリーンロック時間を越えた場合に、認証に成功するまでログイン中の画面からの操作を禁止する機能。

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 4 版［翻訳第 1.0 版］

  CCMB-2012-09-001

  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 4 版［翻訳第 1.0 版］

  CCMB-2012-09-002

  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 4 版［翻訳第 1.0 版］

  CCMB-2012-09-003

- 機能要件: パート 2 拡張
- 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 EAL2+ALC_FLR.2 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.UNAUTHORIZED_ADMINISTRATOR_ACCESS

攻撃者は、管理者または CE として TOE を利用するかもしれない。

T.UNTRUSTED_COMMUNICATION_CHANNELS

攻撃者は、TOE が CS と通信する際の通信情報、およびメール通知機能にて TOE から利用者に送信するメールを、通信経路上で盗聴あるいは改ざんするかもしれない。

T.FAKE_NOTICE_POINT

攻撃者は、CS、メール通知機能の送信先になりすまして、TOEから情報を取得するかもしれない。

T.UPDATE_COMPROMISE

攻撃者が、ネットワーク経由で不正なソフトウェアを TOE へインストールするかもしれない。

T.HTTPS_DEV

TOE と HTTPS 対応機のユーザー別カウンター通知機能、機器カウンター通知機能、サプライコール機能、およびサービスコール機能の通信において、攻撃者が登録 HTTPS 対応機になりすます、または通信データを盗聴あるいは改ざんするかもしれない。

T.PC_WEB

TOE と PC の通信において攻撃者が、通信データを盗聴あるいは改ざんするかもしれない。

3.2 組織のセキュリティ方針

本 TOE に、組織のセキュリティ方針はない。

3.3 前提条件

この章では、TOE の前提条件を記述する。

A.PHYSICAL_PROTECTION

TOE は、物理的な保護対策をとって運用されるものとする。

A.NO_THRU_TRAFFIC_PROTECTION

TOE は、他のネットワーク装置（例えば、ファイアウォール）で外部のネットワークから保護されているネットワークに接続するものとする。

A.TRUSTED_ADMINISTRATOR

管理者及び機器管理者は、それぞれ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それぞれの役割を遂行するものとする。

A.DEVICE

機器管理者は、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

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

TOE は、TOE を利用しようとする者に対して利用者識別認証を行なう。

O.ACCESS

TOE は、認証された利用者に対してのみ TSF データへのアクセスを保証する。

O.TRUSTED_NOTICE_POINT

TOE は、CS、メール通知機能の送信先と通信する際に、正規の送信先に送信し、送信時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.GENUINE

TOE は、CS から受信した TOE のファームウェアが正規のものである場合のみ、そのファームウェアをインストールすることを保証する。

O.AUDIT_LOGGED

TOE は、『利用者識別認証に関連する事象、TSF データの改変に関連する事象、CS との通信の失敗事象、および TOE ファームウェア更新に関連する事象』の発生時に、監査ログを記録し、管理者だけにセキュリティ侵害を監査できる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。

O. TRUSTED _HTTPS_DEVICE

機器カウンター通知機能、サービスコール機能、サプライコール機能、およびユーザー別カウンター通知機能において、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. TRUSTED _OPERATOR

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。

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.PHYSICAL

TOE は、物理的セキュリティで保護されていなければならない。

OE.NO_THRU_TRAFFIC_PROTECT

TOEを接続するネットワーク環境は、外部のネットワークからの攻撃から保護されなければならない。

OE.TRUSTED_ADMIN

管理者及び機器管理者は、TOE のガイダンスを理解し、その記載内容に従って TOE 及びデバイスを管理運用しなければならない。

OE.DEVICE

機器管理者は、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

TOE の保守は、正規の CE だけに許可を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

	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	T.UNTRUSTED_COMMUNICATION_CHANNELS	T.FAKE_NOTICE_POINT	T.UPDATE_COMPROMISE	T.HTTPS_DEV	T.PC_WEB	A.PHYSICAL_PROTECTION	A.NO_THRU_TRAFFIC_PROTECTION	A.TRUSTED_ADMINISTRATOR	A.DEVICE	A.CE
O.I&A	✓										
O.ACCESS	✓										
O.TRUSTED_NOTICE_POINT		✓	✓								
O.GENUINE				✓							
O.AUDIT_LOGGED	✓	✓	✓	✓							
O.TRUSTED_ HTTPS_DEVICE					✓						
O.TRUSTED_ OPERATER						✓					
OE.PHYSICAL							✓				
OE.NO_THRU_TRAFFIC_PROTECT								✓			
OE.TRUSTED_ADMIN									✓		
OE.DEVICE										✓	
OE.CE											✓

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS は、O.I&A、O.ACCESS、および O.AUDIT_LOGGED で対抗できる。なぜなら、O.I&A が、TOE を利用しようとする者に対して利用者識別認証を行い、3 回以内に成功した場合のみ利用を許可し、さらに O.ACCESS が O.I&A で認証に成功した利用者のみに TSF データのアクセスを許可するためである。また、O.AUDIT_LOGGED により利用者認証に関する事象及び TSF データの改変に関連する事象を記録し追跡できるため、脅威を軽減することができる。

T.UNTRUSTED_COMMUNICATION_CHANNELS は O. TRUSTED_NOTICE_POINT と O.AUDIT_LOGGED で対抗できる。なぜなら、O.TRUSTED_NOTICE_POINT は、TOE と CS および

SMTP サーバと通信する際に、正規の送信先に送信し、送信時の通信経路上にある通信データを秘匿し、改ざんを検知するからである。また、O.AUDIT_LOGGED によりCSとの通信失敗事象を追跡できるため、脅威を軽減することができる。

T.FAKE_NOTICE_POINT は、O.TRUSTED_NOTICE_POINT と O.AUDIT_LOGGED で対抗できる。なぜならTOEは、CS、SMTPサーバ、および登録HTTPS対応機と通信する際に、正規の送信先に送信するからである。また、O.AUDIT_LOGGED により CS との通信失敗事象を追跡できるため、脅威を軽減することができる。

T.UPDATE_COMPROMISE は O.GENUINE と O.AUDIT_LOGGED によって実施できる。なぜなら、O.GENUINE は、CS から受信した RC Gate A2 ファームウェアが正規のものである場合のみインストールするからである。また、O.AUDIT_LOGGED によりTOEファームウェア更新に関連する事象を追跡できるため、脅威を軽減することができる。

T.HTTPS_DEV は O.TRUSTED_ HTTPS_DEVICE で実施できる。なぜなら、O.TRUSTED_ HTTPS_DEVICE は、機器カウンター通知機能、サービスコール機能、サプライコール機能、およびユーザー別カウンター通知機能においてTOEとデバイスの通信は、登録HTTPS対応機だけを許可し、TOEと登録HTTPS対応機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。

T.PC_WEB は O.TRUSTED_ OPERATER で対抗できる。なぜなら、O.TRUSTED_ OPERATER は Web機能におけるLAN上のTSFデータの改ざんを検知し、パスワードを秘匿するとしているためである。

A.PHYSICAL_PROTECTION は OE.PHYSICAL で実現できる。なぜなら、OE.PHYSICAL は、TOEを物理的な攻撃から保護される環境に設置するためである。

A.NO_THRU_TRAFFIC_PROTECTION は OE.NO_THRU_TRAFFIC_PROTECTION で実現できる。なぜなら、OE.NO_THRU_TRAFFIC_PROTECTION は、TOE を接続するネットワーク環境を、外部のネットワークからの攻撃から保護するためである。

A.TRUSTED_ADMINISTRATOR は OE.TRUSTED_ADMIN で実現できる。なぜなら、OE.TRUSTED_ADMIN は、管理者及び機器管理者が、TOE のガイダンスを理解し、その記載内容に従ってTOE及びデバイスを管理運用するためである。

A.DEVICE は OE.DEVICE で実現できる。なぜなら、OE.DEVICE は、機器管理者に 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

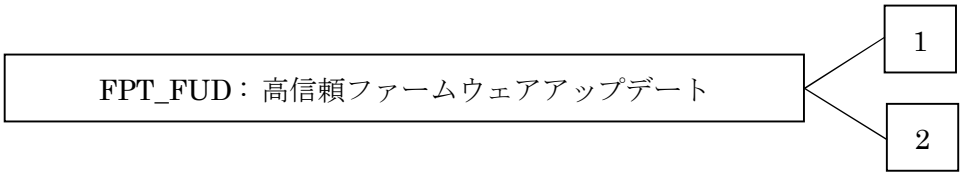
本章では、拡張したセキュリティ機能要件を定義する。

5.1 高信頼ファームウェアアップデート (FPT_FUD)

ファミリのふるまい

このファミリは、TOE のファームウェア/ソフトウェアのアップデートの要件を定義する。

コンポーネントのレベル付け



FPT_FUD.1 高信頼ファームウェアアップデートは、管理ツールが TOE のファームウェア/ソフトウェアのアップデートにおいて、インストールする前にファームウェア/ソフトウェアを確認することを要求する。

FPT_FUD.2 高信頼ファームウェアアップデートは、高信頼ファームウェアアップデートの一環として、ファームウェア/ソフトウェアの検証に失敗した場合は更新版をインストールしないことを要求する。

管理: FPT_FUD.1、FPT_FUD.2

予見される管理アクティビティはない。

監査: FPT_FUD.1、FPT_FUD.2

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) 更新の開始

根拠:

TOE は、TOE のファームウェアアップデートにおいて、管理者がファームウェアアップデートを許可し、アップデートする前にファームウェアの正当性を確認し、正当なファームウェアの場合のみアップデートする。また、TOE にインストールされているファームウェアのバージョンを管理者が確認することができる。この機能は、TOE に不正なファームウェアをインストールしする攻撃に有効で TSF の完全性を維持するセキュリティ機能と言える。しかし、TSF の完全性を保護する FPT クラスには、TSF データや TOE の改ざん検知

についてのコンポーネントは存在するものの、TOE へインストールする前のファームウェアの検証のコンポーネントはない。よって、FPT クラスに本拡張コンポーネントを登録する。

FPT_FUD.1　　高信頼ファームウェアアップデート

下位階層:　なし

依存性:　なし

FPT_FUD.1.1　TSF は、管理者に TOE のファームウェア/ソフトウェアの現在のバージョンを問い合わせる能力を提供しなければならない。

FPT_FUD.1.2　TSF は、管理者に TOE のファームウェア/ソフトウェアに対する更新を開始する能力を提供しなければならない。

FPT_FUD.1.3　TSF は、それらの更新をインストール前に TOE のファームウェア/ソフトウェアを検証する手段を提供しなければならない。

FPT_FUD.2　　高信頼ファームウェアアップデート失敗時の取り扱い

下位階層:　なし

依存性:　FPT_FUD.1

FPT_FUD.2.1　TSF は、ファームウェア/ソフトウェア検証が失敗した場合、更新版のインストールをしない。

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。	なし（監査記録からの情報読出しの失敗事象は存在しないため、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	なし（監査格納失敗によって取られるアクションは存在しないため、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
FIA_AFL.1	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)。	a)最小 ロックアウトの開始
FIA_ATD.1	なし	ー
FIA_SOS.1	a) 最小: TSF による、テストされた秘密の拒否; 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; c) 詳細: 定義された品質尺度に対する変更の識別。	管理者のパスワードの変更(結果: 成功) CE のパスワードの変更(結果: 成功)
FIA_UAU.2	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	b) 基本 ログイン(結果: 成功/失敗)
FIA_UAU.6	a) 最小: 再認証の失敗; b) 基本: すべての再認証試行。	a)最小 再認証の失敗
FIA_UID.2	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; 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。	b) 基本 ログイン(結果: 成功/失敗)
FIA_USB.1	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)。 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)。	b) 基本 ログイン(結果: 成功/失敗)
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	a) 基本: TSF データの値のすべての改変。
FMT_SMF.1	a) 最小: 管理機能の使用	a) 最小: 管理機能の使用
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。	なし(役割の改変機能はないため、監査事象は発生しない)
FPT_STM.1	a) 最小: 時間の変更;	a) 最小: 年月日・日時の変更

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
	b) 詳細: タイムスタンプの提供	
FPT_FUD.1	a)更新の開始	更新の開始 更新結果(成功／失敗)
FPT_FUD.2	なし	-
FTA_SSL.1	a) 最小: セションロックメカニズムによる対話セションのロック。 b) 最小: 対話セションの、成功したロック解除。 c) 基本: 対話セションのロック解除におけるすべての試み。	c) 基本: ロックスクリーンロック解除(結果: 成功／失敗)
FTP_ITC.1(a)	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。	a) 最小: TOE -CS 間通信の失敗

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 保護された監査証跡格納

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、監査証跡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、監査証跡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 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡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 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 5 分以内のユーザー名ごとの利用者識別認証]**に関して、**[選択: [割付: 連続 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: 不成功となったユーザー名によるパソコンからの利用者識別認証に対して 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、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 文字以上の数字、英小文字、英大文字、記号("!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("、")")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と CE による CE 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、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 4 にリストした属性の最初の関連付けに関する規則]**

表 4: 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 ユーザー名に利用者識別認証に成功した利用者のユーザー名
CE	利用者プロセス	ユーザー種別に CE を設定 ユーザー名に利用者識別認証に成功した利用者のユーザー名

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]**

6.1.3　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 5 の TSF データ]**を**[選択: デフォルト値変更、改変、削除[割付: 新規作成、リセット]]**する能力を**[割付: 表 5 の許可された識別された役割]**に制限しなければならない。

表 5: TSF 情報管理のリスト

TSF データ	操作	許可された識別された役割
管理者のパスワード	デフォルト値変更 改変	管理者
管理者のパスワード	リセット	CE

TSF データ	操作	許可された識別された役割
CE のパスワード	改変	CE
年月日・時刻	改変	管理者 CE
CE アクセス許可設定	改変	管理者
機器ファームウェア更新許可設定	改変	管理者
RC Gate A2 ファームウェア更新許可設定	改変	管理者
スクリーンロック時間	改変	管理者 CE
メール通知の送信先	新規登録 改変 削除	管理者
機器証明書情報	新規登録 改変 削除	管理者 CE
SSL/TLS 設定	改変	管理者 CE

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 6 にリストする管理機能]**

表 6: 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デフォルト値変更、改変
CE による管理者パスワードのリセット
CE による CE パスワードの改変
管理者と CE 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
管理者による機器ファームウェア更新許可設定の改変
管理者による RC Gate A2 ファームウェア更新許可設定の改変
管理者と CE によるスクリーンロック時間の改変
管理者によるメール通知の送信先の新規登録、改変、削除
機器証明書情報の新規登録、改変、削除
SSL/TLS 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: 管理者および 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。

FPT_FUD.1　高信頼ファームウェアアップデート

下位階層:　なし

依存性:　なし

FPT_FUD.1.1　TSF は、管理者に TOE のファームウェア/ソフトウェアの現在のバージョンを問い合わせる能力を提供しなければならない。

FPT_FUD.1.2　TSF は、管理者に TOE のファームウェア/ソフトウェアに対する更新を開始する能力を提供しなければならない。

FPT_FUD.1.3　TSF は、それらの更新をインストール前に TOE のファームウェア/ソフトウェアを検証する手段を提供しなければならない。

FPT_FUD.2　高信頼ファームウェアアップデート検証失敗時の取り扱い

下位階層:　なし

依存性:　FPT_FUD.1

FPT_FUD.2.1　TSF は、ファームウェア/ソフトウェア検証が失敗した場合、更新版のインストールをしない。

6.1.5　クラス FTA: TOE アクセス

FTA_SSL.1　TSF 起動セッションロック

下位階層:　なし

依存性: FIA_UAU.1 認証のタイミング

FTA_SSL.1.1 TSF は、**[割付: Web ブラウザよりログインした利用者の最終操作から、管理者または CE が設定するスクリーンロック時間(1 分から 60 分)]** の後、以下によって対話セッションをロックしなければならない:

a) 表示装置を消去するか上書きして、現在の内容を読めなくする;
b) 利用者のデータアクセス/表示装置について、セッションのロック解除以外のいかなる動作も禁止する。

FTA_SSL.1.2 TSF は、セッションのロック解除に先立ち、**[割付: 利用者認証の成功]** の事象を生じさせることを要求しなければならない。

6.1.6 クラス FTP: 高信頼パス/チャネル

FTP_ITC.1(a) TSF 間高信頼チャネル

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(a) 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(a) 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。

表 7: RC Gate A2-CS 間通信において高信頼チャ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
サプライコール機能
機器ファームウェア更新機能
RC Gate A2 ファームウェア更新機能

FTP_ITC.1(b) TSF 間高信頼チャネル

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(b) TSF は、**[選択: TSF、他の高信頼 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_ITC.1.3(b) TSF は、**[割付: 表 8 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。

表 8: RC Gate A2-登録 HTTPS 対応機間通信において高信頼チャ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
サプライコール機能
ユーザー別カウンター通知機能

FTP_ITC.1(C) TSF 間高信頼チャネル

下位階層: なし

依存性: なし

FTP_ITC.1.1(C) TSF は、それ自身と他の高信頼 IT 製品**(詳細化:管理者が TOE に登録したメール通知の送信先)**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(C) 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(C) TSF は、**[割付:メール通知機能]**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。

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 EAL2+ALC_FLR.2 である。TOE の保証コンポーネントを表 9 に示す。これは評価保証レベルの EAL2 によって定義されたコンポーネントのセットに ALC_FLR.2 を追加したものである。

表 9: TOE セキュリティ保証要件(EAL2+ALC_FLR.2)

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.2	セキュリティ実施機能仕様
	ADV_TDS.1	基本設計
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.2	CM システムの使用
	ALC_CMS.2	TOE の一部の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_FLR.2	欠陥報告手続き
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.1	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テストーサンプル
AVA: 脆弱性評定	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 10 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 10: セキュリティ対策方針と機能要件の関連

	O.I&A	O.ACCESS	O.TRUSTED_NOTICE_POINT	O.GENUINE	O.AUDIT_LOGGED	O.TRUSTED _HTTPS_DEVICE	O. TRUSTED _OPERATOR
FAU_GEN.1					✓		
FAU_GEN.2					✓		
FAU_SAR.1					✓		
FAU_SAR.2					✓		
FAU_STG.1					✓		
FAU_STG.4					✓		
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_FUD.1				✓			
FPT_FUD.2				✓			
FTA_SSL.1	✓						
FTP_ITC.1(a)			✓				
FTP_ITC.1(b)						✓	
FTP_ITC.1(c)			✓				
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

O.I&A 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利用者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 によって管理者と CE 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、管理者と CE に TOE のリモート操作が許可される。

(3) TOE リモート操作を自動でロックする
FTA_SSL.1 によって、一定時間操作がない場合に操作画面をロックすることによって、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) 管理者、CE 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、CE のパスワード変更前に利用者を再認証する
利用者本人以外の者が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.1 を達成することで O.I&A を実現できる。

O.ACCESS

O.ACCESS は、認証された利用者に TSF データ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) セキュリティ管理を管理者と CE 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と CE だけに許可する。

(2) ユーザー種別を維持する
FMT_SMR.1 によって、管理者と CE の役割は維持する。

O.ACCESS 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 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.TRUSTED_NOTICE_POINT

O.TRUSTED_NOTICE_POINT は、@Remote 対象機から取得した情報を正しい送信先（CS と管理者が TOE に設定したメール通知機能の送信先）に送信することを保証し、そ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 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。

(3) メール通知機能の送信先に送信する
FTP_ITC.1(c)によって、TOE は管理者が設定した送信先のみに送信し、たとえ誤った送信先に送っても、受信者は受信したメールを読むことができない。

(4) メール送信先までのデータを保護する
FTP_ITC.1(c)によって、通信経路上の送信メールの漏えいを保護し、改ざんを検知する。

O.TRUSTED_NOTICE_POINT を実現するために必要な対策は(1) 、(2) 、(3) 、および(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 FTP_ITC.1(a) と FTP_ITC.1(c)を達成することで O.TRUSTED_NOTICE_POINT を実現できる。

O.GENUINE

O.GENUINE は、TOE に組み込まれている RC Gate A2 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) ファームウェア/ソフトウェア更新前の正当性確認
FPT_FUD.1 によって管理者が TOE にインストールされているファームウェア/ソフトウェアのバージョンを確認することができるためファームウェア/ソフトウェアを更新するべきか判断することが可能であり、管理者の判断によってファームウェア/ソフトウェアの更新の開始が許可される。ファームウェア/ソフトウェアの更新においては、インストール前に更新版の正当性を検証する。さらに、FPT_FUD.2 によって、検証で正当性が確認できなかった場合は、更新版のインストールを行わない。

O.GENUINE 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 FPT_FUD.1、および FPT_FUD.2 を達成することで O.GENUINE を実現できる。

O.AUDIT_LOGGED

O.AUDIT_LOGGED は、利用者識別認証に関連する事象、TSF データの改変に関連する事象、CS との通信の失敗事象および TOE ファームウェア更新に関連する事象の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 A2 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、表 3 に示した監査事象発生時に、その事象をもたらし

た利用者識別情報を含め、セキュティ監査に必要な情報を記録する。表 3 の監査対象事象には、利用者識別認証に関する事象、TSF データの改変に関する事象、CS との通信の失敗事象および TOE ファームウェア更新に関連する事象を規定した SFR のすべてについて必要な事象が含まれている。

(2) 監査機能を提供する
FAU_SAR.1 によって、RC Gate A2 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 A2 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ぱい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。

O.TRUSTED _HTTPS_DEVICE

O. TRUSTED _HTTPS_DEVICE は、機器カウンター通知機能、サービスコール機能、サプライコール機能、およびユーザー別カウンタ通知機能において、@Remote 対象機だけ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. TRUSTED _HTTPS_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. TRUSTED _HTTPS_DEVICE を実現できる。

O. TRUSTED _OPERATOR

O. TRUSTED _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. TRUSTED _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. TRUSTED _OPERATOR 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 11 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がある場合は、その正当性について示す。

表 11: 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
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_FUD.1	なし	なし	なし
FPT_FUD.2	FPT_FUD.1	FPT_FUD.1	なし
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2	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
FTP_ITC.1(a)	なし	なし	なし
FTP_ITC.1(b)	なし	なし	なし
FTP_ITC.1(c)	なし	なし	なし
FTP_TRP.1	なし	なし	なし

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、Web ブラウザおよびネットワークを介した攻撃である。

このような攻撃に対して TOE が実装するセキュリティ機能で対抗できること、そのセキュリティ機能が正しく実装されていること、セキュリティ機能を実装した TOE が改ざんされることなく利用者に配付すること、TOE のセキュリティ機能を利用者が正しく使用するためのガイダンスが提供できることが評価されていることが必要であり、これは EAL2 に相当する。

また、TOE を継続してセキュアに運用するため、運用開始後に発見された欠陥を欠陥報告手続き(ALC_FLR.2)によって適切に修正することは重要である。

したがって、本 TOE に対する評価保証レベルは EAL2+ALC_FLR.2 が妥当である。

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
- 監査ログの読出し
- ログインの成功/失敗
- 再認証の失敗
- ロックアウトの発生
- 管理者パスワードの変更の成功
- CE パスワードの変更の成功
- 年月日時分の設定
- CE アクセス許可設定の変更
- 機器ファームウェア更新許可設定の変更
- RC Gate A2 ファームウェア更新許可設定の変更
- スクリーンロック時間の変更
- メール通知の送信先の新規登録/変更/削除
- 機器証明書情報の新規登録/変更/削除
- SSL/TLS 設定の改変
- CS との SSL/TLS 通信の失敗
- ファームウェアアップデートの開始・アップデートの成功/失敗
- スクリーンロック解除の成功/失敗

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
- ユーザー名
- 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管理者のみに提供する。

FAU_STG.1　　保護された監査証跡格納

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。

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 分間は利用者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、利用者識別認証時のユーザー種別とユーザー名をセッション終了まで維持する。

FIA_SOS.1　　秘密の検証

TOE は、管理者が管理者のパスワードを変更する、または CE が CE 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:数字、英小文字、英大文字、記号(”!”, ”@”, ”#”, ”$”, ”%”, ”^”,”&”, ”*”, ”(”, ”)”,)

(2) 登録可能な桁数: 8 文字以上

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。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/CE のパスワード変更を管理者/CE 用の画面から提供する。管理者/CE 用の画面からパスワードの変更を選択した時に、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、利用者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、利用者識別認証で成功した管理者または CE に、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デフォルト値変更、変更、リセット
- CE のパスワードの変更
- 年月日・時刻の変更
- CE アクセス許可設定の変更
- 機器ファームウェア更新許可設定の変更
- RC Gate A2 ファームウェア更新許可設定の変更
- スクリーンロック時間の変更
- メール通知の送信先の新規登録、変更、削除
- 機器証明書情報の新規登録、改変、削除
- SSL/TLS 設定の改変

FMT_SMF.1　　管理機能の特定

TOE は、利用者識別認証で成功した管理者または CE に、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デフォルト値変更、変更
- CE による管理者パスワードのリセット
- CE による CE パスワードの変更
- 管理者による年月日・時刻の変更
- CE 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
- 管理者による機器ファームウェア更新許可設定の変更
- 管理者による RC Gate A2 ファームウェア更新許可設定の変更
- 管理者によるスクリーンロック時間の変更
- CE によるスクリーンロック時間の変更
- 管理者によるメール通知の送信先の新規登録、変更、削除
- 管理者/CE による機器証明書情報の新規登録、改変、削除
- 管理者/CE による SSL/TLS 設定の改変

FMT_SMR.1　　セキュリティの役割

TOE は、ユーザー種別として管理者と CE を維持している。

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_FUD.1　　高信頼ファームウェアアップデート

TOE は、管理者に Web 機能からファームウェアのバージョン確認する機能を提供する。
TOE は、CS からのファームウェア更新機能の許可、拒否の設定を管理者だけに許可する。
TOE は、CS からファームウェアを受信すると、ファームウェアの正当性が確認した場合のみインストールする。RC Gate A2 ファームウェアは、ファームウェアを構成するファイルの署名検証を行う。

FPT_FUD.2　　高信頼ファームウェアアップデート検証失敗時の取り扱い

TOE は、CS から RC Gate A2 ファームウェアを受信した際の RC Gate A2 ファームウェアを検証し、正当性を確認した場合のみインストールする。RC Gate A2 ファームウェアは、ファームウェアを構成するファイルの署名検証を行う。

FTA_SSL.1　　TSF 起動セッションロック

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、管理者または CE が設定するスクリーンロック時間(1 分から 60 分)を経過した時に、強制的に操作画面をロックする機能を提供する。

FTP_ITC.1(a)　　TSF 間高信頼チャネル

TOE は、CS と SSL/TLS 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、サプライコール機能、機器ファームウェア更新機能、および RC Gate A2 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/TLS 通信する。

FTP_ITC.1(b)　　TSF 間高信頼チャネル

TOE は、登録 HTTPS 対応機と SSL/TLS 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、サプライコール機能、およびユーザー別カウンター通知機能において、TOE と登録 HTTPS 対応機間を SSL/TLS 通信する。

FTP_ITC.1(c)　　TSF 間高信頼チャネル

TOE は、メール通知機能にて送信するメールを S/MIME で保護する。

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/TLS 通信をし、TOE とパソコン間の通信を SSL/TLS 通信する。