認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成26年12月9日 (IT認証4523)
認証番号	C0535
認証申請者	株式会社リコー
TOEの名称	RICOH Remote Communication Gate A2
TOEのバージョン	V1.0.2
PP適合	なし
適合する保証パッケージ	EAL2及び追加の保証コンポーネントALC_FLR.2
開発者	株式会社リコー
評価機関の名称	株式会社 ECSEC Laboratory 評価センター

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成28年12月27日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「RICOH Remote Communication Gate A2」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、株式会社リコーが開発した「RICOH Remote Communication Gate A2」（以下「本 TOE」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が平成 28 年 12 月 5 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である株式会社リコーに報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書とともに提供されるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、株式会社リコー製のデジタル複合機などの遠隔診断保守サービスを導入する消費者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL2 及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、オフィスのローカルエリアネットワーク上（以下「LAN」という。）のデジタル複合機及びプリンタ（以下「デバイス」という。）を、保守センターからインターネットを経由して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、保守センターからインターネットを経由してオフィスの LAN 上のデバイスから保守情報を取得し、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行うサービス（以下「@Remote サービス」という。）である。@Remote サービスの対象とするデバイスは利用者が指定する。指定されたデバイスを「@Remote 対象機」と呼ぶ。TOE はオフィスの LAN に接続され、@Remote サービスをするにあたって、@Remote 対象機と保守センターの通信を仲介する。TOE は、保守センターに送信する保守情報を、指定されたメールアドレスにも送信する。

本 TOE では、@Remote サービスの対象であり「リモート管理サービス機能」を持った株式会社リコー製のデバイス(以下「登録 HTTPS 対応機」という)と TOE 間の通信[1]、TOE と保守センターのサーバ（以下「CS」という。）間の通信が正当な通信相手との間で行われ、暴露あるいは改ざんされないために、暗号のメカニズムにより保護する。また、TOE から送信するメールが改ざんされず、正当な受信者のみ閲覧できるように、暗号のメカニズムにより保護する。

セキュリティ管理機能が不正に操作されないように、識別認証に成功した許可利用者(管理者または CE)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。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおり。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

保護資産である保守情報などを含む通信データについて、インターネット上の第三者からの暴露及び改ざんから保護するために、CS との通信には TLS プロトコルを用いる。これにより TOE と CS 間の通信データを秘匿し、改ざんを検知することができる。

同様に LAN 上の第三者からの暴露及び改ざんから保護するために､登録 HTTPS 対応機との通信[1]には TLS プロトコルを用いる。これにより TOE と登録 HTTPS 対応機間の通信データを秘匿し、改ざんを検知することができる。

攻撃者がインターネット上に偽 CS を立ち上げ LAN 内に悪意のあるプログラムを送り込むことに対抗するために、CS の認証を行い、偽の CS との通信を制限する。これにより TOE は株式会社リコーが提供する正規の CS と認めた場合だけ通信することを保証する。

攻撃者が登録 HTTPS 対応機になりすました機器から偽の保守情報を送信することに対抗するために、登録 HTTPS 対応機の認証を行い、偽の登録 HTTPS 対応機との通信を制限する。これにより TOE は正当な登録 HTTPS 対応機から情報を受け取ることを保証する。

TOE が送信するメールの内容の改ざんや､正当な受信者以外の者が閲覧することに対抗するために、TOE は送信するメールに S/MIME を使用する。これにより、正当な受信者のみがメールを閲覧でき、改ざんを検知することができる。

---

[1] 保護の対象は、TOEと登録HTTPS対応機間の通信のすべてではない。免責事項参照。

TOE の許可利用者(管理者または CE)以外が TOE にアクセスする脅威が想定される。この対策として、利用者による PC 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ができる。また、TOE は、利用者に対して、その役割(管理者、CE)に応じた管理機能の使用を保証する。

TOE のファームウェアが不正なファームウェアにアップデートされる脅威が想定される。この脅威に対し、TOE はファームウェアが正規の者により提供されたことを検証することにより対抗する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

- 本 TOE は、オフィスの LAN 環境において使用されることを想定している。また、LAN 上の PC から Web ブラウザを介して管理が行われる。
- TOE をセキュアに管理運用するために必要な知識を持った TOE の管理者によって、TOE は物理的に保護される。LAN 環境はインターネットを通じた外部者からの攻撃から保護される。LAN に接続されている@Remote 対象機は機器管理者によって保守管理され、正規のデバイスのみが購入され運用される。
- デバイスは、対応可能な通信方法の違いにより HTTPS 対応機と SNMP 対応機に分類されるが、いずれも@Remote サービスの対象である。
- TOE の管理者、機器管理者は、それぞれの特権を利用した不正を行わない。
- TOE の管理者は、TOE の保守の際に、株式会社リコーが認める正規のカスタマーエンジニア（以下「CE」という。）だけに保守を許可しなければならない。

1.1.3 免責事項

① 本TOEは以下の機能は提供していない。

- TOEと登録HTTPS対応機間の通信では、機器ファームウェア更新機能においては、TLSプロトコルを用いた通信保護機能を提供していない。
- TOEと登録SNMP対応機との通信では、汎用性を考えてTLSプロトコルを用いた通信保護機能を提供していない。

② 本TOEにおいては、以下は本評価の範囲外である。

・ RC Gate A2 ファームウェア更新機能により、V1.0.2以外のバージョンに更新した場合は本評価の対象外となる。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 12 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： RICOH Remote Communication Gate A2
バージョン： V1.0.2
開発者： 株式会社リコー

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

ガイダンスに従い管理者が Web ブラウザから操作することにより、TOE 名称とバージョンを表示させることができる。それを上記の TOE 名称とバージョンと比較することにより、設置された製品が評価を受けた本 TOE であることを確認できる。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOE は、オフィスの LAN に設置された@Remote 対象機から受信した情報をインターネット上の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@Remote 対象機の状態を診断し、@Remote 対象機毎に必要な保守を実施するサービスに利用される。サービスを安全に利用するために TOE は以下の機能を提供している。

TOE はインターネットを経由して流れる保守情報を含む通信データや LAN 上に流れる通信データに対する暴露あるいは改ざんから保護する機能を提供する。

TOE が不正な者によって利用されることを防ぐために、利用者を識別認証する機能、また認証に成功した利用者には、管理機能の設定・変更など、その役割に応じた利用が許可される。

TOE 自身のファームウェアが株式会社リコーにより製造された正規のものであることを確認する機能を提供している。

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 内に記録し、閲覧操作だけを管理者に許可する。尚、TOE は監査ログを削除・変更する機能を提供しない。

なお、TOE は、使用に関して以下の役割を想定している。

- 管理者（TOE の管理者）
  本 TOE を導入し運用する管理者。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。

- CE
  TOE を取り扱うための教育を受け、TOE の保守をする者。

以下の役割は、TOE を使用することは想定されないが、運用環境に関連する役割として想定される。

- 機器管理者
  TOE が設置されている LAN に接続されているデバイスの保守管理を行う者。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1　想定する脅威

識別子	脅威
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.HTTPS_DEV	TOEと登録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。 (補足) 機器ファームウェア更新機能によるTOEと登録HTTPS対応機の通信は、脅威の対象から除外される。
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。
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。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.UNAUTHORIZED_ADMINISTRATOR_ACCESS」への対抗

本 TOE は、管理者または CE として TOE を利用しようとする者を識別・認証する。識別・認証が成功した場合に限り、管理者または CE としての利用を許可する。

これらにより、TOE は脅威に対抗する。

(2) 脅威「T.UNTRUSTED_COMMUNICATION_CHANNELS」、「T.FAKE_NOTICE_POINT」及び「T.HTTPS_DEV」への対抗

本 TOE は、CS 及び登録 HTTPS 対応機との通信に TLS を使用する。TLS の認証機能により CS 及び登録 HTTPS 対応機へのなりすましを防止し、通信内容の暗号化とメッセージ認証の機能により通信内容の漏えいと改ざんを防止する。

本 TOE は、メール通知機能により送信するメールに S/MIME を使用する。S/MIME の暗号化と電子署名の機能により、メールの内容の漏えいと改ざんを防止する。本 TOE はメールの送信側になるため、暗号化の機能により送信先へのなりすましも防止する。

これらにより、TOE は脅威に対抗する。

(3) 脅威「T.PC_WEB」への対抗

本 TOE は、PC との通信に TLS を使用する。TLS による通信内容の暗号化とメッセージ認証の機能により通信内容の漏えいと改ざんを防止する。

これらにより、TOE は脅威に対抗する。

(4) 脅威「T.UPDATE_COMPROMISE」への対抗

本 TOE は、ファームウェアのインストール前に、電子署名の検証によりファームウェアが正規のものであるかどうかを確認する。正規のものであることが確認できた場合に限りファームウェアをインストールする。

これらにより、TOE は脅威に対抗する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

本 TOE の利用に当たって要求される組織のセキュリティ方針はない。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

表4-1 前提条件

識別子	前提条件
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。 【補足説明】本前提条件を満たすために､TOEの管理者は､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。

4.2 運用環境と構成

本 TOE はオフィスに設置され、社内ネットワークで接続され、同様に社内ネットワークに接続された PC から利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

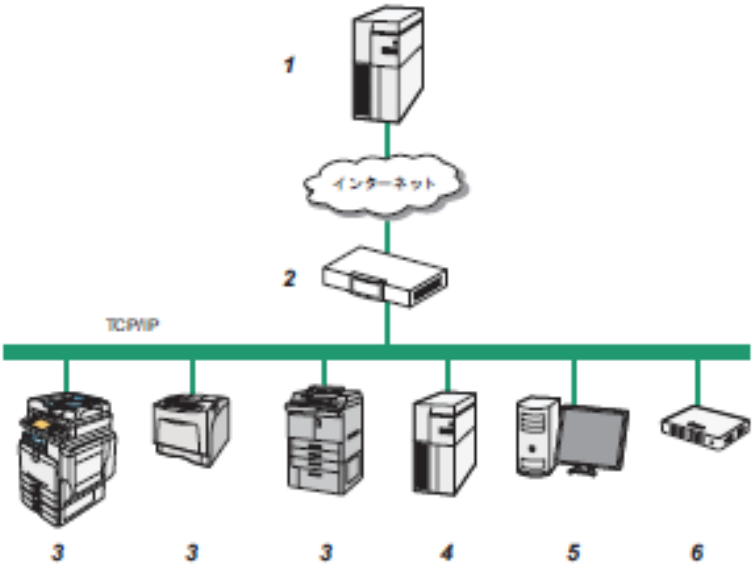

図4-1 TOEの運用環境

以下、図4-1の番号にしたがって各機器の役割を説明する。

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. @Remote対象機
以下の2種類が想定される。
・登録HTTPS対応機
リモート管理サービス機能を持った株式会社リコー製のデバイス。本評価では、以下のデバイスが使用された。
- RICOH MP C305
- RICOH IPSiO SP 8300
- RICOH MP C401
・登録SNMP対応機
SNMPエージェントの機能を持ったデバイス(株式会社リコー製である必要はない)

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。

5. クライアント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、クライアント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。

本評価では、以下のWebブラウザが使用された。なお、(a)と(b)の両方が必要である。

(a) Internet Explorer 8/9/10/11 のいずれか

(b) FireFox 44.0.2

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、オプションのSDカード(RICOH Remote Communication Gate A2 Storage 1000)がTOEに搭載可能であり、このオプションを搭載した環境も利用環境に含める。ただし、このオプションはTOE範囲外の要素である。

4.3 運用環境におけるTOE範囲

TOE と登録 HTTPS 対応機間の通信では、機器ファームウェア更新機能における通信データの保護は想定していない。この間の通信における機器ファームウェアの完全性は、CS により付加される電子署名を登録 HTTPS 対応機が検証することで確保されることが想定されている。そのため、機器ファームウェア更新機能においては、TLS プロトコルによる通信保護機能を提供していない。

また、TOE と登録 SNMP 対応機間の通信においては、汎用性を考えて TLS プロトコルによる通信保護機能を提供していない。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE は RC Gate A2 のハードウェア全体とそれに搭載されるファームウェアから構成され、図 5-1 の機能コンポーネントで構成される。

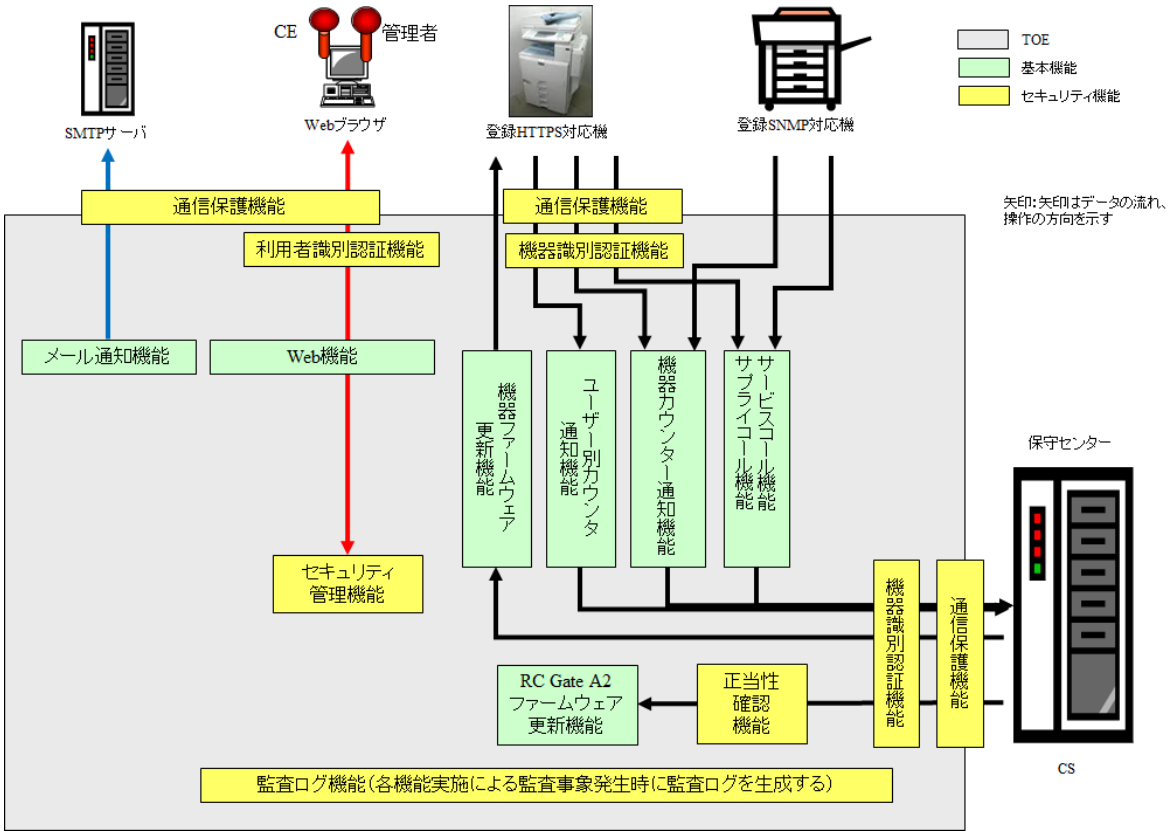

図5-1　TOE境界

TOE は機能コンポーネントとして、基本機能とセキュリティ機能で構成されている。以下に@Remote サービス提供における基本機能の概要を説明する。

- サービスコール機能

  TOE が@Remote 対象機から受信したデバイス障害情報を CS に通報する機能である。

- サプライコール機能

  TOE が@Remote 対象機から受信したサプライ情報(トナー、紙の残量)を CS に通知する機能である。

- 機器カウンター通知機能

TOE が@Remote 対象機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 に通知する機能である。

- ユーザー別カウンター取得機能

TOE が@Remote 対象機から受信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 に通知する機能である。

- 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である。

- 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更新する機能である。

- Web機能

利用者が TOE をリモート操作するため、TOE が提供する機能である。利用者は PC から Web ブラウザを使って TOE へアクセスする。

- メール通知機能

サービスコール機能、サプライコール機能、機器カウンター通知機能、およびユーザー別カウンター機能で 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 が送信する機能である。

以下、TOE のセキュリティ機能について説明する。

- 機器識別認証機能, 通信保護機能

以下の通信に対し、TLS プロトコルにより通信先の正当性を確認し、漏えいと改ざんを防止する。(通信先の正当性を確認する機能が機器識別認証機能、漏えいと改ざんを防止する機能が通信保護機能に該当する。)

- TOE と登録 HTTPS 対応機の間の通信のうち、以下の機能によるもの
  - > サービスコール機能
  - > サプライコール機能
  - > 機器カウンター通知機能
  - > ユーザー別カウンター取得機能
- TOE と CS の間の通信

Web 機能の利用に対し、TLS プロトコルにより漏えいと改ざんを防止する。(通信保護機能に該当する。)

メール通知機能に対し、S/MIME により漏えいと改ざんを防止する。(通信保護機能に該当する。)

- 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 Web 機能の使用を許可する。

- 正当性確認機能

  TOE は、RC Gate A2 ファームウェア更新機能で受信するファームウェアの電子署名を検証し、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(管理者または CE)に応じて TOE の管理機能の利用を制限する。

- 監査ログ機能

  TOE は、セキュリティ監査に必要な事象発生時に必要な情報を監査ログとして記録する。管理者にのみ Web ブラウザによる閲覧操作が許可される。

5.2 IT環境

Web ブラウザ、登録 HTTPS 対応機、CS は、TOE の機器識別認証機能, 通信保護機能のため、TLS プロトコルに対応する。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

国内向けガイダンス

- 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）

海外向けガイダンス（北米仕向け、欧州仕向け 共通）

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

海外向けガイダンス（北米仕向け）

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

海外向けガイダンス（欧州仕向け）

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

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 26 年 12 月に始まり、平成 28 年 12 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 27 年 11 月、平成 28 年 1 月、及び 3 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 28 年 7 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 に示す。

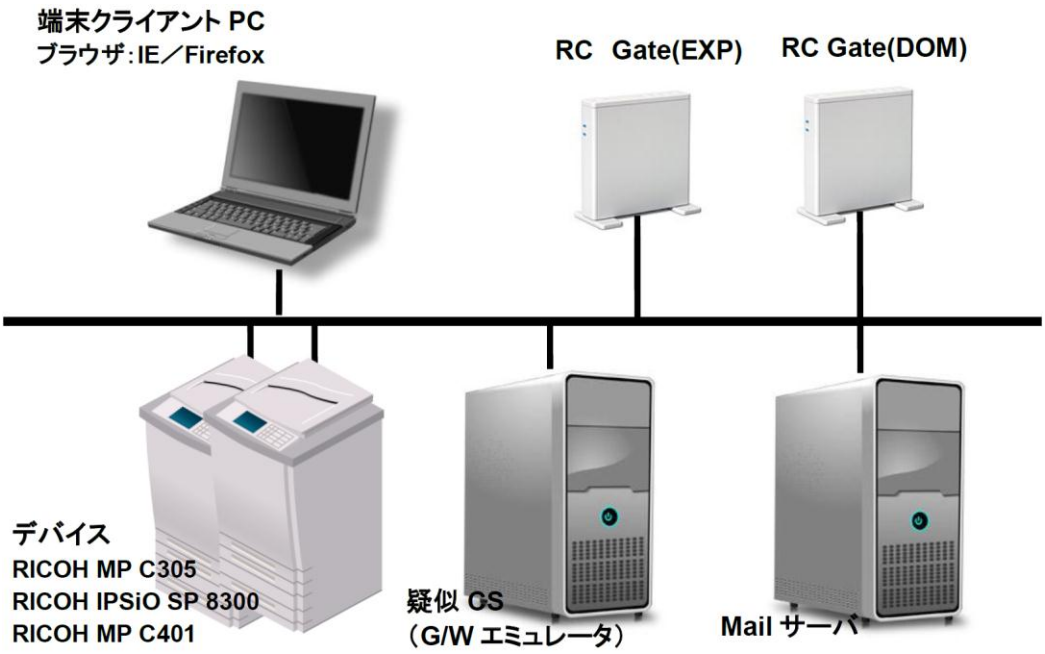

図7-1　開発者テストの構成図

開発者テストは、以下の機器をネットワーク環境に接続して実施された。ネットワーク環境は IPv4 の環境と IPv6 の環境の双方が使用された。

・CS (図 7-1 の疑似 CS)
CS の通信をエミュレートする機器が使用された。

・デバイス(@Remote 対象機)
以下のデバイス(すべて HTTPS 対応機)が使用された。
- RICOH MP C305
- RICOH IPSiO SP 8300
- RICOH MP C401

・SMTP サーバ(図 7-1 の Mail サーバ)
以下のソフトウェアが動作する PC が使用された。
- BlackJumboDog 6.2.0

・クライアント PC
OS は Windows 7 Professional SP1 であり、以下の Web ブラウザが動作する PC が使用された。
- Internet Explorer 8 / 9 / 10 / 11
- FireFox 44.0.2

・RC Gate A2 (図 7-1 の RC Gate)
TOE であり、ST に記載されている識別と一致する。
- Remote Communication Gate A2 V1.0.2

国内仕向けの設定(図 7-1 で DOM と記載)と、海外仕向けの設定(図 7-1 で EXP と記載)の 2 台が使用された。

以下の点について開発者テストの構成は ST で識別される構成と異なるが、ST において識別されている構成と同等であり、本 TOE の機能の確認には問題ないことが以下のように評価者により評価されている。

・CS の代わりに CS の通信をエミュレートする機器が使用された。この機器は TOE からは CS と同じふるまいに見えるため、CS の代わりの機器として適切である。

・ファイアウォールを設置しないネットワーク構成である。ファイアウォールの有無は TOE と CS 間の通信に影響しないため、ファイアウォールを設置しないネットワーク構成はテスト構成として適切である。

・SMTP サーバ(図 7-1 の Mail サーバ)は IPv6 の環境のみで使用された。TOE のメールを送信する機能が IP プロトコルスタックの実装に依存しないため、テストの不足は生じない。

以下の点について、ST で識別される一部の環境の構成が開発者テストの構成に含まれない。セキュリティに関連する動作に影響しないとみなされているが、実際に影響していないことの確認が評価者独立テストで補われる。

・登録 SNMP 対応機が構成に含まれていない。

・オプションの SD カード (RICOH Remote Communication Gate A2 Storage 1000)が構成に含まれていない。

⑵ 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

利用者識別認証機能及び監査機能は、TOE の外部インタフェース(Web ブラウザ、登録 HTTPS 対応機及び CS との通信インタフェース)を使用して TOE を刺激し、Web ブラウザの画面表示や監査ログの出力結果、CS に出力される通信ログや登録 HTTPS 対応機の状態などの TOE 以外の機器に出力または記録される情報を観察することでふるまいを確認する。

ファームウェア正当性確認については、TOE ファームウェアは正当なものと不正なもの(異なるファームフェアの証明書を付与したもの等)を用意し、CS からダウンロードさせることで TOE のふるまい(監査ログの出力結果)を確認する。

TLS による通信保護機能は、TOE と「TLS が適切に動作することがわかっている CS、登録 HTTPS 対応機及び Web ブラウザ」の間で適切に通信できることを確認する。また、Wireshark を使用して通信パケットをキャプチャして観察することで所定のプロトコルにて通信されていることを確認する。

S/MIME によるメールの内容の保護は、TOE から送信したメールが「S/MIME が適切に動作することがわかっている Windows 7 Professional SP1 のメールクライアント」で適切に受信できることを確認する。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表 7-1 に示す。このツールは評価者独立テストでも利用され、その際に仕様確認及び動作試験は評価者によって実施されている。

表7-1　開発テストツール

ツール名称（バージョン）	概要・利用目的
Wireshark (Ver.1.12.4)	LAN上の通信データをモニタし、解析するツール

＜開発者テストの実施内容＞

上記テスト手法により、各インタフェースに対し、適用されるセキュリティ機能が仕様通りに動作することを確認した。

b) 開発者テストの実施範囲

開発者テストは開発者によって108項目実施された。カバレージ分析によって、機能仕様に記述されたセキュリティ機能と外部インタフェースに対するテストのカバレージが確認された。一部の外部インタフェースに対してはカバレージが

不十分と判断され、評価者独立テストで補足された。

c) **結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの環境は、開発者テストと同じ環境である。

テスト環境の要素やテスト用プログラムは、開発者テストに用いられたものを利用しているが、これらの仕様確認及び動作試験と校正は評価者によって実施されている。

(2) 独立テスト概説

独立テストでは、開発者テストからのサンプリングテストと、評価者が考案した評価者独自テストを実施した。

評価者の実施した独立テストは以下のとおりである。

a) **独立テストの観点**

＜サンプリングテストの観点＞

評価者は以下の観点から、開発者テスト108項目の内から39項目サンプリングした。

① インタフェース、類似のテスト、テスト環境、TOEの構成といった各種の分類から最低1個のテストをサンプリングした。
② 本TOEにおいて、大半のセキュリティ機能が関連しており複雑であるWebインタフェースに関しては、テストケースを他のインタフェースより多く実施できるように選択した。
③ 1つのテストにおいて、正常系、異常系の2種類が実施されている場合

には、正常系のテストは他のテストにて暗黙に実施されていることから異常系をサンプリングした。

＜評価者独自テストの観点＞

評価者は以下の観点から、評価者独自のテストを考案した。

① Webインタフェース等について、開発者テストでパラメタの種類（たとえばパスワードの入力値など）が不足する箇所について、パラメタを変更したテストを追加した。
② 開発者テストではセキュリティ機能性を同時に確認するテストが扱われていないため、独自テストに追加した。
③ 開発者テストで実施されているインタフェースや機能性において開発者が実施していない検証方法があるものについては、そのような方法での動作の検証が不足しているため、独自テストに追加した。
④ 各インタフェースにおける例外処理にはバリエーションがあるため、開発者テスト内で実施されていないものについては、独自テストに追加した。
⑤ 機能仕様ではパスワードに関する順列的・確率的メカニズムが主張されているが、この機能が、主張・想定どおりであるかを独立して確認するテストを追加した
⑥ 開発者テストにより動作が確認されていないTOEのふるまいに対し、テストを補足した。
⑦ 開発者テストにより動作が確認されていない動作環境の構成の場合に、TOEのセキュリティのふるまいに影響しないことを確認した。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

独立テストでは､開発テストと同じ手法に加えて以下の手法が使用された。

- WebブラウザからではTOEに入力するのが困難なパラメタを入力する、及び､Webブラウザからでは観察が困難なTOEの出力を観察するため、TOE と Web ブラウザの間に Proxy 型の Web 脆弱性検査ツールを導入する。

＜独立テストツール＞

独立テストは、開発者テストに表 7-2 に示すツールを追加し実施された。このツールの仕様確認及び動作試験は評価者によって実施されている。

表7-2 独立テストで使用したツール

ツール名称（バージョン）	概要・利用目的
Burp Suite (Ver.1.7.03)	Proxy型のWeb脆弱性検査ツール。
Wireshark (Ver.2.0.4)	LAN上の通信データをモニタし、解析するツール。 (補足) サンプリングテストでは開発者テストと同じVer.1.12.4、評価者独自テストで左記のVer.2.0.4が使用された。
AATOOL2 (version 1.10.2)	ASN.1形式のデータをデコードして観察するために使用された。
openssl-1.0.1k-13.fc22	公開鍵証明書の作成に使用された。
RICOH Remote Communication Gate A2 Storage 1000	TOEのオプションのSDカード。
Ricoh MP C306Z	SNMP対応機として使用された。

＜独立テストの実施内容＞

評価者独自テストの概要を表 7-3 に示す。

表7-3 実施した評価者独自テストの概要

独自テストの観点	評価者独自テストの概要
①⑤	使用できない文字が含まれる場合など、パスワード文字構成のバリエーションに対するTOEの動作の確認。
①②④	スクリーンロック解除のためにユーザー名・パスワードを入力する場合の、文字構成のバリエーションに対するTOEの動作の確認。
⑥	登録SNMP対応機が接続された環境において、登録SNMP対応機からの情報が正しく扱われることの確認。
①③④	利用者識別認証機能でWebブラウザとTOEの間のセッションの維持が正しく動作することを、Burp Suiteにより通信内容の観察や改変をして確認。
⑥	ファームウェアが改変された場合にファームウェア正当性確認で検出できることの確認。 ファームウェアをCSから取得する際に、正しくTLSが適用されることをWiresharkにより確認。
①	各種の想定されるWebブラウザからTOEを利用する場合に、仕様で想定されていない操作ができないことを確認。

独自テストの観点	評価者独自テストの概要
⑦	SDカード(RICOH Remote Communication Gate A2 Storage 1000)をTOEに搭載した構成で開発者テストと同様のテストの一部を実施し、セキュリティのふるまいに影響しないことを確認。
⑥	ユーザー別カウンター取得機能で発生するTOEと@Remote対象機間、TOEとCS間の通信に、正しくTLSが適用されることをWiresharkにより確認。
⑥	S/MIMEによるメールの内容の保護の確認のため、メールの内容をAATOOL2でデコードして、正しい暗号アルゴリズムの設定であることを確認。
③	WebブラウザからTOEを利用する場合に、仕様で想定されない情報の送受信がないことを、Burp Suiteにより通信内容の観察をして確認。
①	TLSの証明書検証機能に対し、不正なCAの署名または自己署名を持つ証明書が受け付けられないことを確認。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

表7-4　懸念される脆弱性

脆弱性識別子	内容
①	設計資料に記述されていないネットワークサービスが起動していることにより、セキュリティ機能をバイパスしてTOEの保護資産を暴露または改ざんすることが懸念される。
②	稼働しているネットワークサービスに公知の脆弱性の理由により、本来意図された操作以外の操作が実行可能であることにより、TOEのセキュリティ機能をバイパスして保護資産にアクセスされる可能性がある。
③	本TOEはURLを指定してリモートからアクセスできるが、セッション情報を確認しないURLが存在している場合、識別認証やアクセス制御をバイパスすることが懸念される。
④	監査ログ機能に関する機能仕様から、監査ログに任意の文字コードを混入させることが可能であることが懸念される。TOEが想定しない動作を起こし、結果的にTOEのセキュアな利用に影響を与えるかもしれない。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テスト環境は独立テストの環境と同じであり、さらに表 7-5 のツールが使用された。これらのツールの仕様確認及び動作試験は評価者によって実施されている。

表7-5　侵入テスト構成

ツール名称（バージョン）	概要・利用目的
NMAP (Ver 7.12)	ポートスキャンツール
Nessus (Ver 6.7.0)	脆弱性スキャナ
Netcat (v1.11)	汎用TCP･UDP操作ツール

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-6 に示す。

表7-6　侵入テスト概要

脆弱性識別子	侵入テストの概要
①	ポートスキャンツール（NMAP）を使用して、TOEが提供するポート以外にアクセスできないことを確認するテストを実施した。
②	脆弱性スキャナ（Nessus）によるスキャンを行い、TOEが提供するネットワークサービスに悪用可能な公知の脆弱性が存在しないことを確認した。 TOEが提供するネットワークサービスのうち、Webインタフェースに対して、netcatでのアクセスを試みる。ブラウザでのアクセスが想定されていないWebインタフェースに対してブラウザでのアクセスを試みる。その際にWiresharkによりキャプチャしたパケットを確認し、不審なパケットがないことを確認した。
③	認証後にアクセス可能となるURLをBurp suiteを使用して調査した。 認証されていない状態でこれらのURLを指定してアクセスし、認証後でないと該当画面にアクセスできないことを確認した。 （セッション情報のチェック機能の動作を確認した。）
④	監査ログに反映される可能性のある入力項目に対し、Burp suiteを使用して各種文字コードを含む入力を与えた。これらの入力で監査ログ機能に問題が発生しないことを確認した。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

評価開始時におけるTOEの初期設定は、ガイダンスにて推奨されている設定値を設定した。

テストを実施するために使用した機器に関しては、CS、ネットワーク構成と、STで識別された構成と異なる箇所が存在する。また、開発者テストでカバーされない構成(登録SNMP対応機とオプションの SDカードが含まれる構成)は、評価者テストで補われた。そのため、STで識別された構成でのTOEの動作が保証されたことが評価者により判断されている。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート２適合
- セキュリティ保証要件：　コモンクライテリア　パート３適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL2パッケージのすべての保証コンポーネント
- 追加の保証コンポーネント ALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

- 監査を実施するための機能として、監査ログを Web ブラウザ上に表示する機能が保証された。本 TOE は監査ログを CSV 形式でエクスポートする機能も持つが、この機能は保証の対象外となる。
  監査の実施のために監査ログを CSV 形式でエクスポートする機能を使用する場合、セキュアな運用は保証されないことに注意が必要である。

- 本 TOE との間の通信内容の保護のため、CS 及び登録 HTTPS 対応機も適切なセキュリティ機能を持つ必要がある。CS 及び登録 HTTPS 対応機は TOE と同じ開発者により提供されるが、そのセキュリティ機能は保証の対象外である。
  つまり、CS 及び登録 HTTPS 対応機のセキュリティ機能の信頼性についても、他の動作環境と同様、本評価による保証とは別に判断する必要がある。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL2 及び追加の保証コンポーネント ALC_FLR.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」、「7.5 評価構成について」及び「7.7 評価者コメント/勧告」の記載内容を参照し、本 TOE の制約事項や評価対象範囲が、各自の想定する運用条件に合致しているかどうか注意が必要である。

以下に、TOE の動作が保証される運用環境について注意すべき点を特記する。

- 登録 HTTPS 対応機として、特定の 3 機種の場合が保証された。これ以外の機種を登録 HTTPS 対応機とする場合の安全性については、本評価による保証とは別に判断する必要がある。
  - RICOH MP C305
  - RICOH IPSiO SP 8300
  - RICOH MP C401

・ クライアント PC では、監査ログを閲覧するために、以下の(a)と(b)の両方の Web ブラウザが利用可能になっている必要がある。

(a) Internet Explorer 8/9/10/11 のいずれか
(b) FireFox 44.0.2

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

RICOH Remote Communication Gate A2 セキュリティターゲット バージョン 0.42　2016 年 11 月 10 日　株式会社リコー

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

CS	Communication Server
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
LAN	Local Area Network
OS	Operating System
RC Gate A2	Remote Communication Gate A2
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator

本報告書で使用された用語の定義を以下に示す。

@Remote	本TOEを用いた遠隔サービスの商用名称。
@Remote対象機	@Remoteサービスの対象として利用者が指定したデバイス。
CE (カスタマーエンジニア)	TOEを取り扱うための教育を受け、TOEの保守をする者。保守をする際、PCのWebブラウザからCE用のインタフェースを使って操作することができる。
HTTPS対応機	「リモート管理サービス機能」を持った株式会社リコー製のデバイス。(「リモート管理サービス機能」の有無は株式会社リコーにより公表される。)
SNMP対応機	SNMPエージェントの機能を持ったデバイス。(株式会社リコー製である必要はない)

管理者 (TOEの管理者)	本TOEを導入し運用する管理者。 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。
機器管理者	TOEが設置されているLANに接続されているデバイスの保守管理を行う者。
登録HTTPS対応機	@Remoteサービスの対象として利用者が指定したデバイスであり、HTTPS対応機であるもの。
登録SNMP対応機	@Remoteサービスの対象として利用者が指定したデバイスであり、SNMP対応機であるもの。
保守情報	@Remote対象機からTOEを介して保守センターへ送信される情報。機器カウンター情報、ユーザー別カウンター情報、障害情報、サプライ情報が該当する。
保守センター	@Remote対象機の保守を運営する施設。
利用者	「管理者」と「CE」を総称した名称。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア 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, 2012年9月, CCMB-2012-09-002, (平成24年11月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア 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, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] RICOH Remote Communication Gate A2セキュリティターゲット バージョン 0.42　2016年11月10日　株式会社リコー

[13] RICOH Remote Communication Gate A2 評価報告書 第2.0版 2016年12月5日 株式会社 ECSEC Laboratory 評価センター