認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤江　一正　原紙押印済

評価対象

申請受付日（受付番号）	平成22年8月10日 (IT認証0306)
認証番号	C0283
認証申請者	株式会社リコー
TOEの名称	Remote Communication Gate A
TOEのバージョン	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
PP適合	なし
適合する保証パッケージ	EAL3
開発者	株式会社リコー
評価機関の名称	株式会社電子商取引安全技術研究所 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23年2月25日

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3
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3

評価結果：合格

「Remote Communication Gate A」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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「Remote Communication Gate A、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」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が平成23年2月10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に関心を持つ消費者や調達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、本書の付属書であ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、EAL3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行うサービス（以下「@Remoteサービス」という。）である。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対象のデバイスと保守センターの通信を仲介する。

本TOEでは、保守サービス情報などの保護資産が暴露あるいは改ざんされないために、TOEとデバイス間の通信、TOEと保守センターのサーバ（以下「CS」とい

う。）間の通信はSSLプロトコルにより保護する。また、TOEの許可利用者以外の操作や、一般ユーザーが誤ってセキュリティ管理機能を操作しないために、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。

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サービス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SSL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。

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。

TOEの許可利用者以外がTOEにアクセスすること、また、TOEがデバイスから収集した情報の閲覧のみが許可されている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が想定される。これらの対策として、利用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ができる。また、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。

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している。

本TOEは、オフィスなどのLAN環境において使用されることを想定している。また、LAN上のパソコンから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。また、LAN上でのTOEの通信情報は変更されないようネットワーク管理者によって指導される。LANに接続されているデバイスはデバイス管理

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、いずれも遠隔診断保守サービスの対象である。

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た不正を行わない。

また、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HTTPS対応機間の通信では、デバイスファームウェア更新機能においては、SSL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SNMP対応機との通信では､汎用性を考えてSSL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ファームウェア更新機能により、A2.06-C2.04-P2.01-K2.02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。
- 本TOEは､登録デバイス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に通知する機能を持つが、機能を使用できないように設定した上で評価が実施されている。本機能を有効にした場合は本評価の対象外である。

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セキュリティ認証申請手続等に関する規程」[2]、「ITセキュリティ評価機関承認申請手続等に関する規程」[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23年2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]、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、本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： Remote Communication Gate A

バージョン： 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

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。

TOEの機種コードは、ハードウェアの筐体に貼られている定格銘版（銀色のラベル）に印刷されている機種コードの上位4桁により確認できる。尚、本TOEはオプションとして増設メモリ、増設ストレージが搭載可能であるが、TOEの機種コードは増設メモリ、増設ストレージを搭載していないハードウェアを識別している。

TOEのファームウェアバージョンは、パソコンのWebブラウザ経由でRemote Communication Gate A （以下、「RC Gate」と言う）のログイン画面（ページ右上）から確認できる。

また、本TOEは以下の２つの方法により入手することが可能である。

① 上記バージョンで識別される本TOEを株式会社リコーからの物理的配送により入手する。

② 本評価とは別の認証製品（認証番号：C0277、機種コード（上４桁）：D459、ファームウェアバージョン：A1.18-C1.14-P1.12-K1.04）が、ガイダンスに従って認証製品として運用されている状態で、当該製品の「RC Gateファームウェア更新機能」を用いて本TOEのファームウェアバージョン（A2.06-C2.04-P2.01-K2.02）へ更新する。
ただし、株式会社リコーのサービス部門担当者から説明されるガイダンスの手順に従って作業を行う必要がある。

3 セキュリティ方針

本章では、本TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEは、オフィスなどのLANに設置されたデバイスから受信した情報を外部ネットワーク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デバイスの状態を診断し、デバイス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は外部ネットワークを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、保守情報へのアクセス、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。

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。

なお、本TOEでは、利用者を「管理者（TOEの管理者）」と「一般ユーザー」に分類している。「管理者（TOEの管理者）」は本TOEを導入し運用する者であり、TOEの設定変更、TOEがデバイスから収集した印刷枚数や障害情報、監査ログの閲覧をパソコンから行うことができる。「一般ユーザー」は、管理者によりTOE利用アカウントを与えられた者であり、TOEがデバイスから収集した情報の閲覧のみをパソコンから行うことができる。

表3-1　想定する脅威

識別子	脅　威
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、株式会社リコーにより提供されているものではない偽のCSを立ち上げ、TOEに登録された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内にウイルスなど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。 【補足説明】通信データには、課金情報・障害情報を含む保守サービス情報や更新用ファームウェアなどが含まれる。
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、デバイスから収集した情報の閲覧などのTOEの操作をするかもしれない。一般ユーザーが誤って、管理者にしか許可されていないセキュリティ管理機能を利用するかもしれない。

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.FAKE_CS」への対抗

本TOEでは、「RC Gate-CS間通信保護機能」により対抗する。

「RC Gate-CS間通信保護機能」は、TOEとCS間の通信においてSSLプロトコルを用いて、証明書によりCSの正当性を検証する。それにより、株式会社リコーが提供する正規のCSとだけ通信を許可する。

(2) 脅威「T.INTERNET」への対抗

本TOEでは、「RC Gate-CS間通信保護機能」により対抗する。

「RC Gate-CS間通信保護機能」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についてSSLプロトコルを用いて秘匿し、改ざんを検知する。それにより、通信データの暴露、改ざんを防止する。

(3) 脅威「T.ACCESS」への対抗

本TOEでは、「利用者識別認証機能」、「セキュリティ管理機能」、「デバイス受信情報アクセスコントロール機能」により対抗する。

「利用者識別認証機能」では脅威に対して、以下の対策を行う。

- TOEをリモート操作しようとする者には識別・認証に成功することを要求する。
- 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以外がTOEを操作する機会を減少する。
- 識別認証に用いられるパスワードには解析が困難になる品質を維持する。また、ブルートフォース攻撃に必要となる十分な時間は与えない。
- 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、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う。

「セキュリティ管理機能」では脅威に対して、以下の対策を行う。

- セキュリティ管理を管理者だけに許可する。

「デバイス受信情報アクセスコントロール機能」では脅威に対して、以下の対策を行う。

- ユーザー種別によって閲覧可能な情報を制限する。

以上により、識別・認証に成功した許可利用者のみにTOEの操作が許可され、さらにユーザー種別ごとに操作できるTOEの機能を制限することで、TOEへの不正なアクセスを防止する。

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

3.1.2.1 組織のセキュリティ方針

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を表3-2に示す。

これらは、具体的な要求事項・法律などが存在するわけではないが、本TOEの導入を検討する組織において課せられるであろうと、開発者である株式会社リコーが想定したセキュリティ方針である。

表3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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、及びサプライコール機能において、TOEがHTTPS対応機（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）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、株式会社リコーが提供する正規のRC Gateファームウェア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.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。
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。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOEは、表3-2に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.ATR_DEVICE」への対応

本セキュリティ方針は、TOEが「RC Gate-デバイス間通信保護機能」を実装していることにより、実施することができる。

「RC Gate-デバイス間通信保護機能」は、機器カウンター通知機能、サービスコール機能、及びサプライコール機能でのTOEとHTTPS対応機間の通信おいて、SSLプロトコルを用いて、証明書によりHTTPS対応機の正当性を検証する。また、通信経路上の通信データを秘匿し、改ざんを検知する。

(2) 組織のセキュリティ方針「P.SOFTWARE」への対応

本セキュリティ方針は、TOEが「RC Gateファームウェア正当性確認機能」を実装していることにより、実施することができる。

「RC Gateファームウェア正当性確認機能」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、株式会社リコーが提供する正規のRC Gateファームウェアであることを検証する。

(3) 組織のセキュリティ方針「P.PC_WEB」への対応

本セキュリティ方針は、TOEが「RC Gate-パソコン間通信保護機能」を実装していることにより、実施することができる。

「RC Gate-パソコン間通信保護機能」は、TOEと利用者がリモート操作で利用するパソコン間はSSLプロトコルを用いて、通信経路上の通信データを秘匿し、改ざんを検知する。

(4) 組織のセキュリティ方針「P.AUDIT_LOGGING」への対応

本セキュリティ方針は、TOEが「監査ログ機能」を実装していることにより、実施することができる。

「監査ログ機能」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。

4 前提条件と範囲の明確化

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使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。

なお、本TOEに係わる管理者を「管理者（TOEの管理者）」、「ネットワーク管理者」、「デバイス管理者」に分類している。本報告書内で単に「管理者」と呼ぶときは、前述したTOEの管理者をさす。「ネットワーク管理者」とは、TOEが設置されている顧客LANを管理するITマネージャをさす。「デバイス管理者」とは、TOEが設置されている顧客LANに接続されるデバイスの保守管理を行う者をさす。

表4-1　前提条件

識別子	前提条件
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）	TOEの管理者は、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、TOEの管理者は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。 【補足説明】HTTPS対応機以外のデバイスとは、TOEとの通信が保護されないSNMP対応機をさす。
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。 【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 使用環境と構成

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クライアントから利用される。本TOEの一般的な使用環境を図4-1に示す。

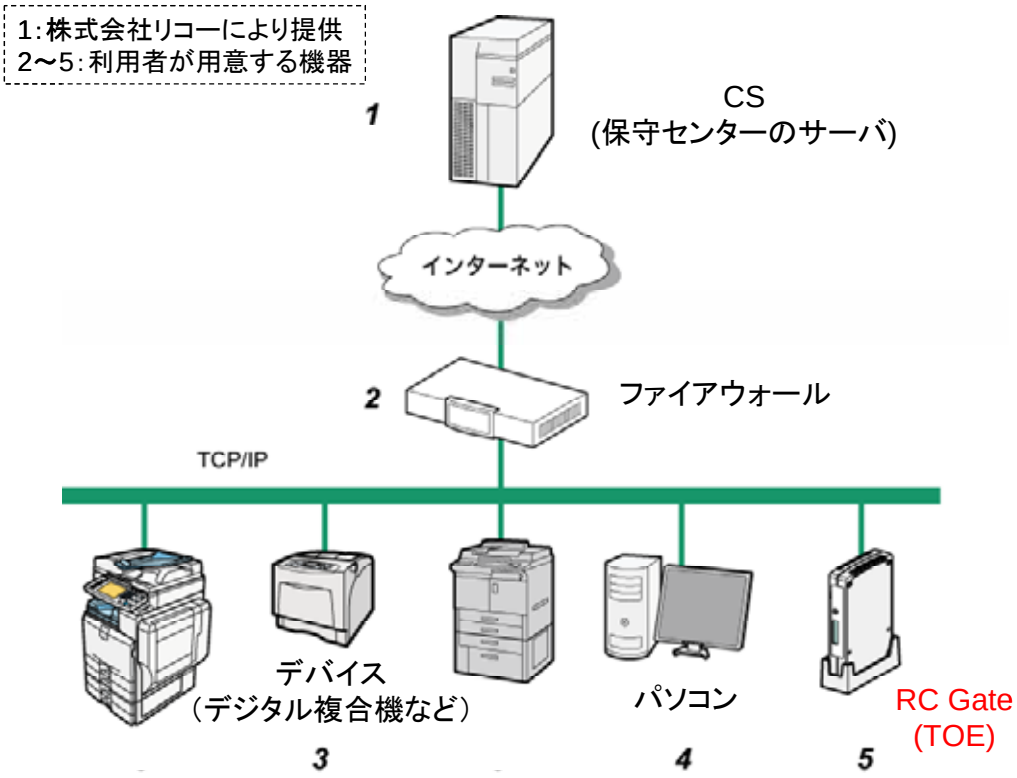

図4-1　TOEの使用環境

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. デバイス
　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

複合機及びプリンタのことをいう。

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SNMPによる通信をする能力を持ったデバイス。

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、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に搭載可能であり、これらオプションを搭載した環境も利用環境に含める。ただし、これらのオプションはTOE範囲外の要素である。

4.3 使用環境におけるTOE範囲

開発者は組織のセキュリティ方針として、TOEとHTTPS対応機間の通信では、デバイス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。そのため、デバイスファームウェア更新機能においては、SSL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SNMP対応機間の通信においては、汎用性を考えてSSLプロトコルによる通信保護機能を提供していない。このため、本TOEの使用環境においては、ネットワーク管理者は、ネットワーク利用者に対して、TOEとSNMP対応機との通信情報を変更したりしないように指導することを前提としている。

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について、目的と関連を説明する。

5.1 TOE境界とコンポーネント構成

TOEはRC Gate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。

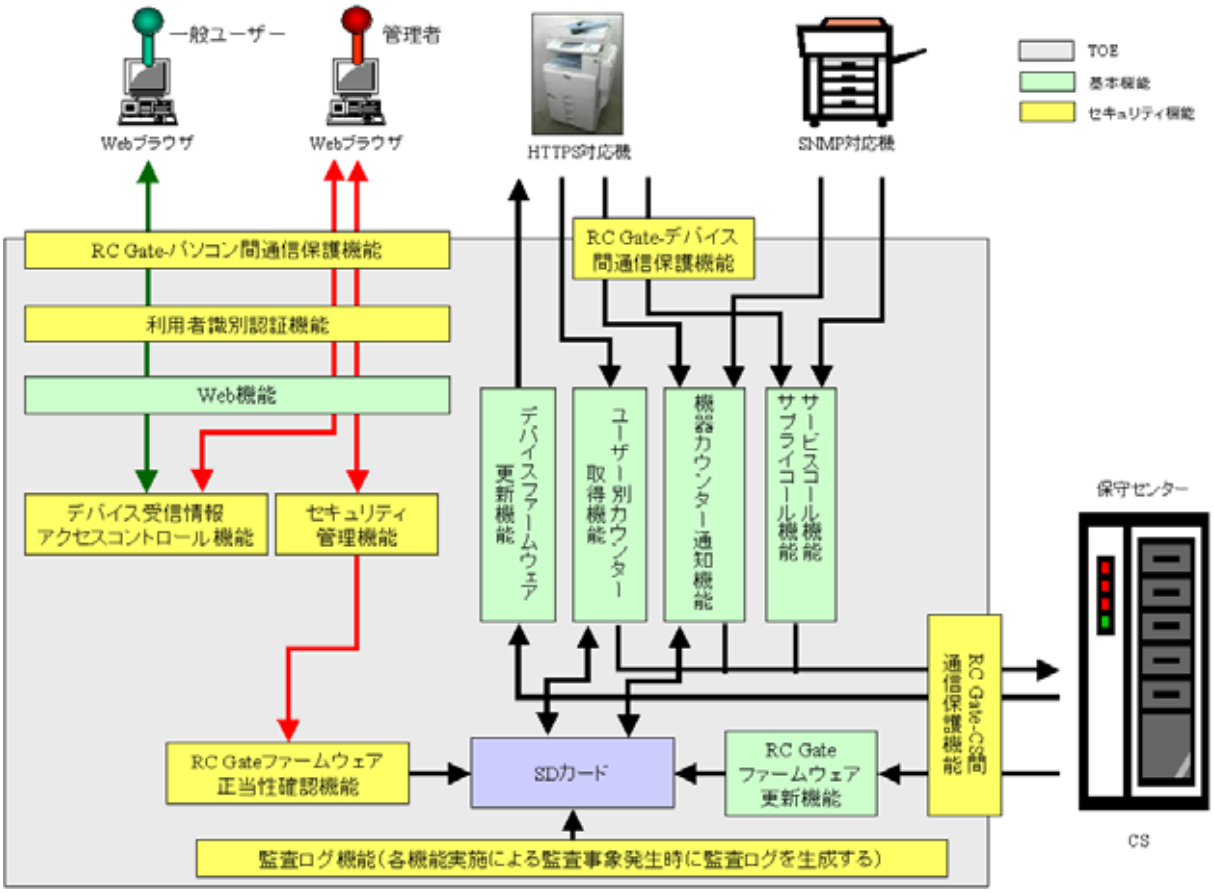

図5-1　TOE境界

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と、それに対するセキュリティ機能の関連性について説明する。

- 機器カウンター通知機能

  TOEが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に通知する機能である。

  TOEとHTTPS対応機間の通信には、組織のセキュリティ方針として、「RC Gate-デバイス間通信保護機能」によりSSLプロトコルが使用される。

TOEとCS間の通信には「RC Gate-CS間通信保護機能」により、SSLプロトコルが使用され、通信データは改変暴露から保護される。

- サービスコール機能

TOEがデバイスから受信したデバイス障害情報をCSに通報する機能である。

TOEとHTTPS対応機間の通信には、組織のセキュリティ方針として、「RC Gate-デバイス間通信保護機能」によりSSLプロトコルが使用される。

TOEとCS間の通信には「RC Gate-CS間通信保護機能」により、SSLプロトコルが使用され、通信データは改変暴露から保護される。

- サプライコール機能

TOEが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に通知する機能である。

TOEとHTTPS対応機間の通信には、組織のセキュリティ方針として、「RC Gate-デバイス間通信保護機能」によりSSLプロトコルが使用される。

TOEとCS間の通信には「RC Gate-CS間通信保護機能」により、SSLプロトコルが使用され、通信データは改変暴露から保護される。

- 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､HTTPS対応機のファームウェアを更新する機能である。

TOEとCS間の通信には「RC Gate-CS間通信保護機能」により、SSLプロトコルが使用され、通信データは改変暴露から保護される。

ただし､「セキュリティ管理機能」でデバイスファームウェア更新許可設定を有効にした場合にのみ、デバイスファームウェアは更新可能となる。

- 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のファームウェアを更新する機能である。

TOEとCS間の通信には「RC Gate-CS間通信保護機能」により、SSLプロトコルが使用され、通信データは改変暴露から保護される。

ただし､「セキュリティ管理機能」でRC Gateファームウェア更新許可設定を有効にした場合にのみ、RC Gateファームウェアは更新可能となる。

- 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。利用者はパソコンからWebブラウザを使ってTOEへアクセスする。

TOEとパソコン間の通信には、組織のセキュリティ方針として、「RC Gate-

パソコン間通信保護機能」によりSSLプロトコルが使用される。

Web機能の利用は、「利用者識別認証機能」により、識別・認証に成功したTOEの許可利用者だけに限定される。

TOEの許可利用者の内、管理者にのみ「セキュリティ管理機能」と「RC Gate ファームウェア正当性確認機能」が提供され、パソコンからWebブラウザを使用して実行する。

SDカード内に保存されているデバイスから受信した情報へのWebブラウザを使用した閲覧は、「デバイス受信情報アクセスコントロール機能」により、ユーザー種別（管理者、一般ユーザー）ごとに閲覧可能な情報が制御される。

SDカード内には「監査ログ機能」により、セキュリティ監査に必要な事象発生時に必要な情報が監査ログとして記録され、管理者にのみWebブラウザによる閲覧操作が許可される。

- 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。

本評価は、ユーザー別カウンター取得機能を使用できない設定にて行われている。

5.2 IT環境

利用者はLAN環境に接続されたパソコンの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。

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 A 使用説明書(D459-8501A)
- Remote Communication Gate A セットアップガイド(D459-8504A)
- Remote Communication Gate A 安全上のご注意/セットアップガイド (D459-8500A)

海外向けガイダンス

- Remote Communication Gate A Operating Instructions(D459-8502A)
- Remote Communication Gate A Setup Guide(D459-8503A)
- Remote Communication Gate A Safety Information/Setup Guide (D459-8510A)
- Remote Communication Gate A Safety Information/Setup Guide (D459-8530A)

Remote Communication Gate A Safety Information/Setup Guideに関して(D459-8510A)と(D459-8530A)の差異は国によるレギュレーションの違いである。

7 評価機関による評価実施及び結果

7.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

7.2 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22年8月に始まり、平成23年2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。

平成22年11月には開発・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、構成管理・配付・開発セキュリティ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。

平成22年11月、平成23年2月には開発者サイトで開発者のテスト環境を使用し、開発者が実施した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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

7.3 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。

7.3.1 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。評価した開発者テストの概要を以下に示す。

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、ハードウェア・ソフトウェアの構成を表7-1に示す。

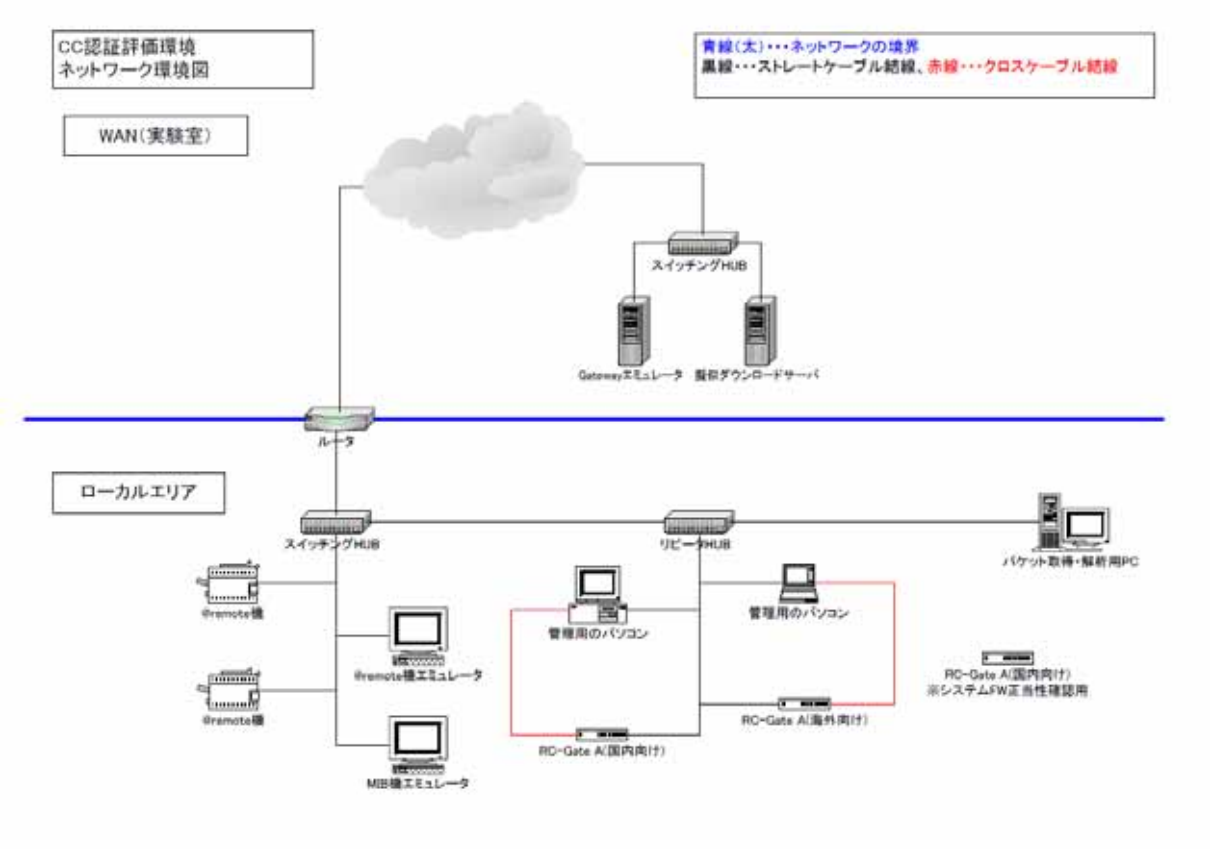

図7-1　開発者テストの構成図

表7-1　ハードウェア・ソフトウェア構成

ハードウェア種別		台数	仕様
RC Gate		3	日本仕向け（オプション増設有／なし）・英語仕向け（オプション増設有／なし）・ファームウェア不正テスト用 ※オプション増設有時は以下を搭載する 増設メモリ：Remote Communication Gate Memory 1000 増設ストレージ：Remote Communication Gate Storage 1000
Gateway エミュレータ		1	Gateway エミュレータ (V1.07)
デバイス	HTTPS 対応デバイス	2	RICOH imagio MP C3000
	HTTPS 対応デバイスエミュレータ	1	HTTPS 対応デバイスエミュレータ （Gateway エミュレータ同梱）
	SNMP 対応デバイスエミュレータ	1	MIB ツール
ルータ		1	LAN/WAN　10BASE-T/100BASE-TX
ネットワーク環境		1	プライベートネットワーク環境
SD カード		2	初期化ツールによるフォーマット済
疑似ダウンロードサーバ		1	TOE 及びデバイスファームウェアリリース用サーバ （TOE 及びデバイスのファーム更新機能実行時に、本 Web サーバからファームをダウンロードする）
クライアント PC		3	管理用のパソコン（日本仕向け操作用） OS:Windows XP Professional SP2 ブラウザ:Internet Explorer 8 FlashPlayer:FlashPlayer 10 管理用のパソコン（英語仕向け操作用） OS:Windows XP Professional SP2 ブラウザ:Internet Explorer 6、7 FlashPlayer:FlashPlayer 10 パケット取得・解析用 PC（評価者テスト用） OS:Windows XP Professional SP3 ブラウザ:Internet Explorer 8 FlashPlayer:FlashPlayer 10

テストを実施するために使用した機器に関しては、デバイス、CS、クライアントPCのソフトウェアと、STで識別された構成と異なる箇所が存在するが、以下の理由によりSTの構成と同等であるとみなせる。

①デバイス：

テストではデバイス実機とHTTPS対応機及びSNMP対応機と同等の通信機能をエミュレートするエミュレータソフトウェアを使用している。テストに使用するエミュレータはHTTPS対応機及びSNMP対応機と同等の通信プロトコルをエミュレートするソフトウェアであるため、テスト環境にて使用されるデバイスはSTと一貫している。

②CS：

STには、CSは保守センターに設置されること、TOEから通信を開始し、TOEとCS間で保守サービスのための情報を送受信することが説明されている。テスト環境では、実際のCSの代わりにGatewayエミュレータを使用しており、またファームウェアのダウンロードのために疑似ダウンロードサーバをTOE及びデバイスのファームウェアリリース用サーバとして使用している。

Gatewayエミュレータは実際のCSではないが、その通信プロトコルの点からCSをエミュレートするものであること、疑似ダウンロードサーバも実際に使用されるTOE及びデバイスのファームウェアリリース用サーバの機能性をエミュレートする機能性をもつことから、TOEからみた場合の機能性はSTの構成と同等であることが評価者により確認されている。

③クライアントPCのソフトウェア：

テストでは管理用のパソコン（国内向け操作用）、管理用のパソコン（海外向け操作用）の2台のクライアントPCが使用されている。各PCでInternet Explorerのバージョンが異なっているが、Webブラウザ画面にて提供される入出力項目やチェック機能はすべてFlashファイル（アプリケーションソフトウェア）にて提供されているため、Internet Explorerのバージョンの影響は受けない。

また、Flash Player に関しては、Flash Player 10のみが使用されているが、本TOEではFlash Player9から変更・追加された機能は使用していないため、バージョンの影響は受けない。

以上より、STに記述されたすべてのソフトウェア（Internet Explorer (Ver.6.0からVer.8.0)、Flash Player (Ver.9.0からVer.10.0)）にてテストしているとみなせることから、テスト環境にて使用されたソフトウェアはSTと一貫し

ていると判断した。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

＜開発者テスト手法＞

開発者テストは以下の２つの手法にて実施された。

①外部インタフェースを利用したテスト手法

TOEに接続されたPC上のWebブラウザや直接ボタンなどを操作することにより外部インタフェースを刺激し、応答を観察することによって行われた。

外部インタフェースへの入力は、ボタンの押下やブラウザに表示されるボタンや入力欄に指定されるパラメタなどである。外部インタフェースの応答は、Webブラウザ画面に表示されるメッセージ類や、LCDなどの表示である。

これらのテストは、外部インタフェース毎に、処理の実行が正常終了する場合/異常終了する場合、入力パラメタが許容範囲内の場合/許容範囲外の場合、処理の同時実行などの排他制御テストが行われた。また、初期条件や入力パラメタによってモジュールのふるまいが異なる場合は、それぞれの初期条件や入力パラメタでテストが行われた。

②外部インタフェースを利用できないテスト項目のテスト手法

外部インタフェースによって観察できないふるまいのテストは、解析ツールやエミュレータを操作することによって代替手法で実行された。採用されている主な代替手法の概略は、以下のとおり。

- SSLプロトコルを用いた通信

通信回線上でSSLプロトコルを用いた通信を行っているか否かを確認には、パケットキャプチャ解析ツール（Wireshark）を用いて回線のパケットの順序性やその内容を確認した。

- 通信の開始や終了などのアクションの応答

通信の開始や終了などのアクションを検証には、TOEからの要求を受け付ける都度出力されるGatewayエミュレータのログの内容を確認した。

＜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7-2に示す。Wiresharkはネットワーク管理などの用途のため、一般的に広く用いられているオープンソースのパケット解析ツールである。Winpcapはネットワーク管理などの目的のため、Wiresharkとともに一般的に使用されているパケットキャプチャライブラリである。

表7-2　開発テストツール

No	ツール名称	Ver.	機能	動作環境
1	Wireshark	1.0.5	パケット解析	Windows
2	WinPcap	4.1.2	パケットキャプチャライブラリ	Windows

＜開発者テストの実施＞

外部インタフェースに関する機能ついては、利用者が刺激することにより、そのエラーメッセージや画面の状態などからその結果を確認し、期待されるテスト結果との比較が行われた。

TOEとCSやデバイス、クライアントPCとのSSLプロトコルを用いた通信については、パケットキャプチャ解析ツール（Wireshark）を用いて、回線のパケットの順序性やその内容の確認が行われた。

ファームウェア正当性確認機能などについては、正常終了したかの確認はLEDやLCDなどの筐体やWebブラウザ画面などの状態を観察することによりふるまいを間接的に確認し、期待されるテスト結果との比較が行われた。

b.　実施テストの範囲

テストは開発者によって380項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、TOE設計仕様書に記述されたすべてのサブシステムとそれらのインタフェースが十分にテストされたことが検証されている。

c.　結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

7.3.2 評価者独立テスト

評価者は、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の再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成は、図7-1に示すとおりである。ただし、以下に示すように管理用のパソコンのソフトウェアが変更されている。

- OSがWindows XP Professional SP2からSP3に変更（日本仕向け操作用、英語仕向け操作用）
- Internet Explorerのバージョンが6、7から8に変更（英語仕向け操作用）
- FlashPlayerのバージョンが10から9に変更（英語仕向け操作用）

上記の変更においては、TOEのセキュリティ機能に影響が無く、開発者のテスト環境と同一とみなせることが評価者により確認されている。

そのため、評価者独立テスト環境にて使用されたソフトウェアにおいてもSTと一貫していると判断した。

2) 評価者独立テスト概説

評価者独立テストでは、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。

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380件の内から93件サンプリングした。

① 全セキュリティ機能のインタフェースについて、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。

④ 独自テストにて、パラメタの変更やテスト方法の変更により、同じ機能がテスト可能であると判断したものについてはサンプリング対象から除外した。

＜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 開発者テストでは英語版のTOEにおいて1バイト文字と2バイト文字が混在している入力の確認などが不足しているため、独自テストに追加した。
⑥ 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

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。

＜独立テスト手法＞

独立テストは、開発テストと同じ手法で実施された。

＜独立テストツール＞

独立テストでは､開発者テストにおいて利用した表7-2のツールを用いた。

＜独立テストの実施＞

評価者により実施された独立テストに関して、開発者テストに対するサンプリングテストの93件の概要と項目数を表7-3に、評価者独自テストの

概要を表7-4に示す。

表7-3　開発者テストの概要とサンプリングテストを実施した項目数

開発者テストの概要	サンプリング項目数
利用者識別認証機能（管理者）の確認	8
日付・時刻設定の確認	10
通信テストコール機能（SSL通信）の確認	4
デバイス-TOE間の通信機能（SSL通信）の確認	16
管理者のみがアクセスできる機能の確認	2
ファームウェア正当性チェック機能の確認	4
CEアクセス許可機能の確認	4
RC Gateファームウェア更新の制限機能の確認	6
デバイスファームウェア更新の制限機能の確認	6
アクセス制御機能（カウンター覧）の確認	20
TOE-CS間の通信機能（SSL通信）の確認（サービスコール・サプライコール）	6
ユーザー別カウンター取得機能無効化の確認	7

表7-4　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
①	時刻変更機能における入力パラメタチェックの確認
②	同じユーザー名で同時ログインした場合などの動作確認
③	TOE電源切断時のユーザーセッションのふるまいなど異常時における機能性の確認
④	別の認証製品（認証番号：C0277）を、本TOEのファームウェアへアップデートした時のふるまいや、ログイン中の一般ユーザーのアカウント情報を変更・削除した場合の動作確認
⑤	ユーザー登録時に多言語文字を入力した場合の動作確認
⑥	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および監査ログ機能の動作の確認

c.　結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確

認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

7.3.3 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の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

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、以下の脆弱性を識別した。

表7-5 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	本TOEはJavaservletにより各種サービスを提供しているが、セッション情報を確認しないJavaservlet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。
③	本TOEのデバイスとの通信インタフェース(Webサーバ機能)について、クライアントPCなどからWebブラウザで誤って接続した場合、TOEのセキュリティ機能をバイパスし保護資産を暴露または改ざんすることが懸念される。
④	Webブラウザ画面の入力項目にSQLを入力することにより、TOEが意図しない動作をする可能性がある。 これにより、保護資産を暴露または改ざんすることが懸念される。
⑤	Webブラウザ画面の入力項目にスクリプトなどの不正な文字列を入力することにより、TOEが想定しない動作を起こす可能性がある。 これにより、保護資産を暴露または改ざんすることが懸念される。
⑥	WEBブラウザのURLなどに指定される入力が悪用されることによって、TOEの保護資産や、攻撃の手掛かりとなる情報が暴露されることが懸念される。

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があるかを決定するため、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者が実施したテストの構成は、評価者独立テストと同様の構成である。

評価者が実施したテストの構成は図7-1に示すとおりである。

使用したツールの詳細を表7-6に示す。

Wiresharkに関しては、開発者テストと異なっているが、ユーザインタフェースなどの違いのみでありパケットをキャプチャする機能性には違いがないため、バージョン間の違いによる結果の相違はない。

表7-6　侵入テストツール

No	ツール名称	Ver.	機能	動作環境
1	Wireshark	1.4.1	パケット解析	Windows
2	WinPcap	4.1.2	パケットキャプチャライブラリ	Windows
3	NMAP	5.21	ポートスキャンツール	Windows
4	Paros	3.2.13	Proxy 型脆弱性検査ツール	Windows

＜脆弱性テストの実施＞

潜在的な脆弱性の探索において識別された表7-5の懸念される脆弱性について、これと対応する評価者侵入テストを表7-7に示す。

表7-7　侵入テストの概要

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	セッション情報のチェック機能が動作していることを確認するため、外部からアクセス可能なJavaServletに対して、直接WEBブラウザからアクセスを試みるテストを実施した。
③	デバイス用インタフェースに利用者がWEBブラウザでアクセスすることにより、保護資産の改ざんや暴露につながらないことを確認するテストを実施した。
④	WEBブラウザ画面の入力項目にSQLを含む文字列を入力し、識別認証

	をバイパスしたり、許可されない保護資産にアクセスできないことを確認するテストを実施した。
⑤	WEBブラウザ画面の入力項目にスクリプトなどの不正な文字列を入力し、セキュリティ機能を侵害するような動作をしないことを確認するテストを実施した。
⑥	TOEのWebサーバ機能に対して、ディレクトリトラバーサルが懸念される入力を与え、ディレクトリトラバーサルが起こらないことを確認するテストを実施した。 WEBブラウザのURLなどに指定される入力が存在しないことを確認するテストを実施した。

c. 結果

実施した評価者侵入テストでは、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。

7.4 評価構成について

本評価では、開発者テスト、評価者独立テスト、評価者侵入テストともに図7-1に示す評価構成で実施された。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、デバイス、CS、クライアントPCのソフトウェアと、STで識別された構成と異なる箇所が存在するが、STの構成と同等であるとみなせる妥当性は評価者により判断されている（7.3.1 開発者テスト 参照)。

7.5 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。

- EAL3パッケージのすべての保証コンポーネント

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.6 評価者コメント/勧告

消費者に喚起すべき評価者コメント/勧告は特にない。

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。尚、本評価において所見報告書は発行されていない。

① 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。
② 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。
③ 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EAL3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

開発者は組織のセキュリティ方針として、デバイスは自身のファームウェアの正当性を確認する機能を備えているため、TOEとHTTPS対応機間の通信ではデバイスファームウェア更新機能における通信情報の保護を想定していない。このような開発者が想定している組織のセキュリティ方針について消費者は注意する必要がある。

別の認証製品（認証番号：C0277、機種コード（上４桁）：D459、ファームウェアバージョン：A1.18-C1.14-P1.12-K1.04）を、「RC Gateファームウェア更新機能」によって本TOE のファームウェアバージョン（A2.06-C2.04-P2.01-K2.02）に更新したものも、本評価の対象である。それ以外の場合は本評価の対象外であるため、消費者は注意する必要がある。

その他にも、「1.1.3 免責事項」に記したように、本TOEには評価の範囲外である機能などが存在するので、本TOEを用いた遠隔診断保守サービスの導入を検討する消費者は注意する必要がある。

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。

Remote Communication Gate Aセキュリティターゲット バージョン 2.02
2011年2月7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
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MIB	Management Information Base
OS	Operating System
RC Gate	Remote Communication Gate A
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
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。
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、パソコンの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。
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-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、及びサプライコール機能におけるTOEとHTTPS対応機間の通信で、TOEとHTTPS対応機相互に、通信データの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。
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。
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、及びOSが、株式会社リコーが提供する正規のものであることを確認する機能。
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。
サービスコール機能	TOEが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。
サプライコール機能	TOEが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。
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。
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、HTTPS対応機のファームウェアを更新する機能。
デバイス管理者	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。
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。
ネットワーク管理者	TOEが設置されているLANを管理するITマネージャ。

ネットワーク利用者	TOEが設置されているLAN環境を利用する者の総称。 TOE利用アカウントを持たない者も含まれる。
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。
一般ユーザー	管理者によりTOE利用アカウントを与えられた者。 パソコンからTOEが収集したデバイスの情報を閲覧できる。
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。
管理者 （TOEの管理者）	本TOEを導入し運用する管理者。 パソコンからRC Gateの設定変更や、TOEが収集したデバイスの情報、監査ログが閲覧できる。
機器カウンター通知機能	TOEが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。
利用者	「管理者」と「一般ユーザー」を総称した名称。
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」という）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。

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19年5月　独立行政法人 情報処理推進機構　CCS-01

[2] ITセキュリティ認証申請手続等に関する規程　平成19年5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申請手続等に関する規程　平成19年5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 Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[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3版 2009年7月 CCMB-2009-07-001 (平成21年12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3版 2009年7月 CCMB-2009-07-002 (平成21年12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3版 2009年7月 CCMB-2009-07-003 (平成21年12月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 3 July 2009 CCMB-2009-07-004

[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3版 2009年7月 CCMB-2009-07-004 (平成21年12月翻訳第1.0版)

[12] Remote Communication Gate Aセキュリティターゲット バージョン 2.02 2011年2月7日　株式会社リコー

[13] Remote Communication Gate A 評価報告書 第1.4版 2011年2月10日 株式会社電子商取引安全技術研究所 評価センター