認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成17年 8月31日** (IT**認証**5049)
認証番号	C0048
認証申請者	**株式会社リコー**
TOE**の名称**	(**日本語**) Remote Communication Gate **アプリケーションソフトウェア** (**英語**) Remote Communication Gate Application Software
TOE**のバージョン**	3.34
PP**適合**	**なし**
適合する保証要件	EAL3
TOE**開発者**	**株式会社リコー**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

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18年6月26日

独立行政法人 情報処理推進機構
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　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「(日本語) Remote Communication Gate アプリケーションソフトウェア、(英語)Remote Communication Gate Application Software」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、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

1.1 はじめに

この認証報告書は、「(日本語) Remote Communication Gate アプリケーションソフトウェア、(英語)Remote Communication Gate Application Software」（以下「本TOE」という。）についてみずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行った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ものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:　(日本語)
Remote Communication Gate Type N
Remote Communication Gate Type L
(英語)
Remote Communication Gate Type BN1
Remote Communication Gate Type BM1

バージョン:　3.34

開発者:　株式会社リコー

1.2.2 製品概要

TOEは遠隔サービス用仲介機器であるRC Gate（製品名称のRemote Communication Gate Type N/L/BN1/BM1を総称）に組込まれるアプリケーションソフトウェアである。RC Gate は主にビジネスオフィスに置かれ画像I/O機器と遠隔

監視サーバ"コミュニケーション・サーバ　(以降CS)"との仲介機器として利用される。RC Gateは収集したデータ（コピーカウンター、トナー残量や故障情報など）を、インターネットまたは電話回線（ダイアルアップPPP接続）経由で信頼されるCSに送信する。これによって利用者は適切な保守サービスを受けることが出来る。TOEはインターネットまたは電話回線上を流れる情報を保護するために、暗号化やCSの識別認証を行う。

1.2.3　　TOEの範囲とTOEの機能

(1) TOEの動作環境

RC Gateはオフィス内の内部ネットワークにつながっている機器から情報を収集しCSへ転送、あるいはCSから機器用のファームウェアをダウンロードする仲介機器である。製品のタイプは、RC GateとCS間でインターネットを用いるLAN対応型(Type N、BN1)と電話回線を用いるモデム対応型(Type L、BM1)の２種類がある。

図1-1に、RC GateのLAN対応型が想定する代表的な接続環境を示す。

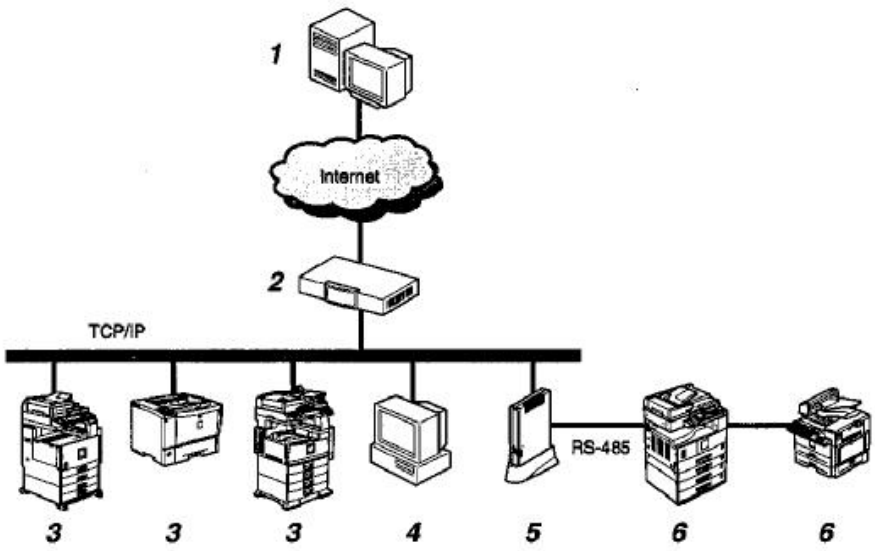

図 1-1　RC Gate(LAN対応型)の接続環境

以下、図１-1の番号にしたがって各機器の役割を説明する。

1.コミュニケーション・サーバ

RC Gateがインターネット経由で通信する監視サーバをこのように呼ぶ。前述のように略称でCSと呼ぶ。

2.プロキシサーバ・ファイアウォール

オフィスの内部ネットワーク環境を外部ネットワークから保護するためのセキュリティシステム。

3.画像I/O機器

リコーの遠隔サービスをサポートしている画像I/O機器、およびMIB機能を有する画像I/O機器。

4.RC Gate用PC

Webブラウザを経由してRC Gateにアクセスするための PC。

5.Remote Communication Gate Type N/BN1

RC Gateは画像I/O機器を管理する仲介機器であり、機器情報をCSに転送、あるいはCSから機器用のファームウェアをダウンロードする。RC GateとCSとの間の通信方式には2通りある。

1) HTTPS方式：HTTPSサーバとしてのCSと、HTTPSクライアントとしてのRC Gateの間でメッセージをやり取りする。

2) SMTP方式：SMTPサーバ経由でRC GateからS/MIME方式でCSへメッセージを送る。

6.シリアルバス(RS-485) 経由で管理される画像I/O機器

リコー製の画像I/O機器は、シリアルケーブルでRC Gateへ直接接続して管理することも可能である。シリアルでは最大5台まで画像I/O機器を接続できる。

また、RC Gateのモデム対応型の接続環境を図1-2に示す。

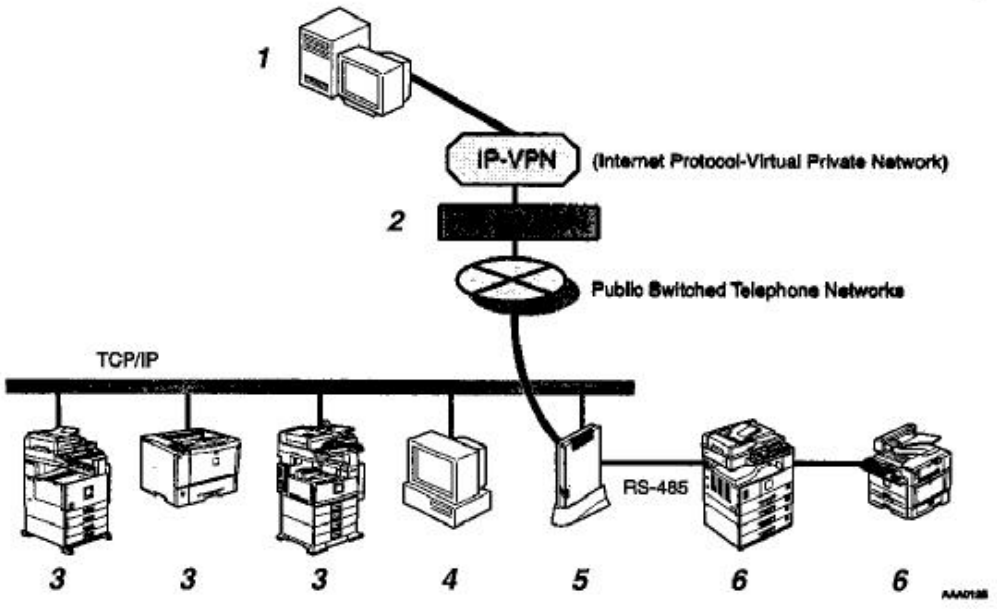

図 1-2 RC Gate(**モデム対応型**)**の接続環境**

以下、図１-2の番号にしたがって各機器の役割を説明する。

1.コミュニケーション・サーバ

RC Gateが電話回線経由で通信する監視サーバをこのように呼ぶ。前述のように略称でCSと呼ぶ。

2.アクセスポイント

電話回線でダイアルアップする場合のアクセスポイントである。RC Gate用のアクセスポイントはプリインストールされている。

3.画像I/O機器

リコーの遠隔サービスをサポートしている画像I/O機器､およびMIB機能を有する画像I/O機器。

4.RC Gate用PC

Webブラウザを経由してRC GateにアクセスするためのPC。

5.Remote Communication Gate Type L/BM1

RC Gateは画像I/O機器を管理する仲介機器であり、機器情報をCSに転送する。なお、LAN対応型と異なりCSからの機器用のファームウェアのダウンロードは行わない。RC GateとCSとの間の通信方式には以下の通りである。

1) HTTPS方式：HTTPSサーバとしてのCSと、HTTPSクライアントとしてのRC Gateの間でメッセージをやり取りする。

6.シリアルバス(RS-485) 経由で管理される画像I/O機器

リコー製の画像I/O機器は､シリアルケーブルでRC Gateへ直接接続して管理することも可能である。シリアルでは最大5台まで画像I/O機器を接続できる。

(2) TOEの範囲と機能概要

RC Gateは専用筐体で提供される製品で、TOEはその製品にインストールされたアプリケーションソフトウェアである。RC Gateは、画像I/O機器との内部ネットワーク通信、CSとの外部ネットワーク通信の仲介機器として動作する。RC Gateは主に一般的なLANが構築されているオフィスで使用されることを想定している。RC Gateのハードウェアとしての主要機能はメインボードに集約されている。メインボード上には､CPU､フラッシュメモリ､イーサネット回路､RS485､電源ユニットがある。 Type L/BM1ではメインボードの他にモデムボードが接続されている。モデムボードは、電話回線インタフェースを持つ。

RC Gateのソフトウェアは、アプリケーションソフトとOSで構成されている。TOEはアプリケーションソフトウェアであり､OSは含まない｡本TOEの物理的範囲を図1-3に示す。TOEはソフトウェア実行プログラムとしてSDメモリに格納され、RC Gate電源投入時にRAMに展開される。

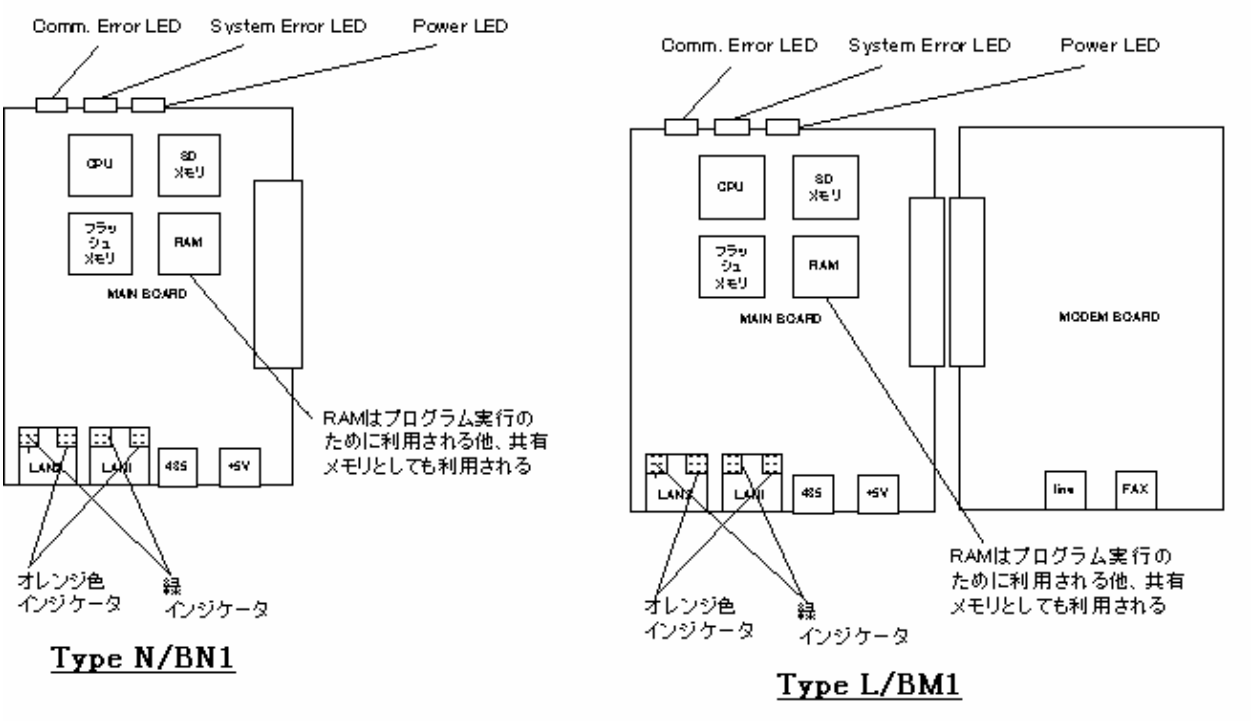

図 1-3 RC Gateの物理構成

RC Gateはハードウェアとソフトウェアで構成されている。ソフトウェア部分は、OSとアプリケーションソフトウェアで構成されている。OSはMontaVista LinuxをRC Gate用にポーティングした組込みLinuxであり、RC Gate OSと呼んでいる。OSはTOEの範囲外になる。本TOEの論理的範囲を図1-4に示す。セキュリティ機能としては、アプリケーションソフトウェアが提供しているオペレータ識別認証機能、アクセス制御機能、HTTPS時のCS識別認証機能、S/MIMEメール送信機能がある。

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

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

なって行われる。TOEはCSと情報交換する時には、暗号化ライブラリを使用してデータの暗号化と復号を行う。

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

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

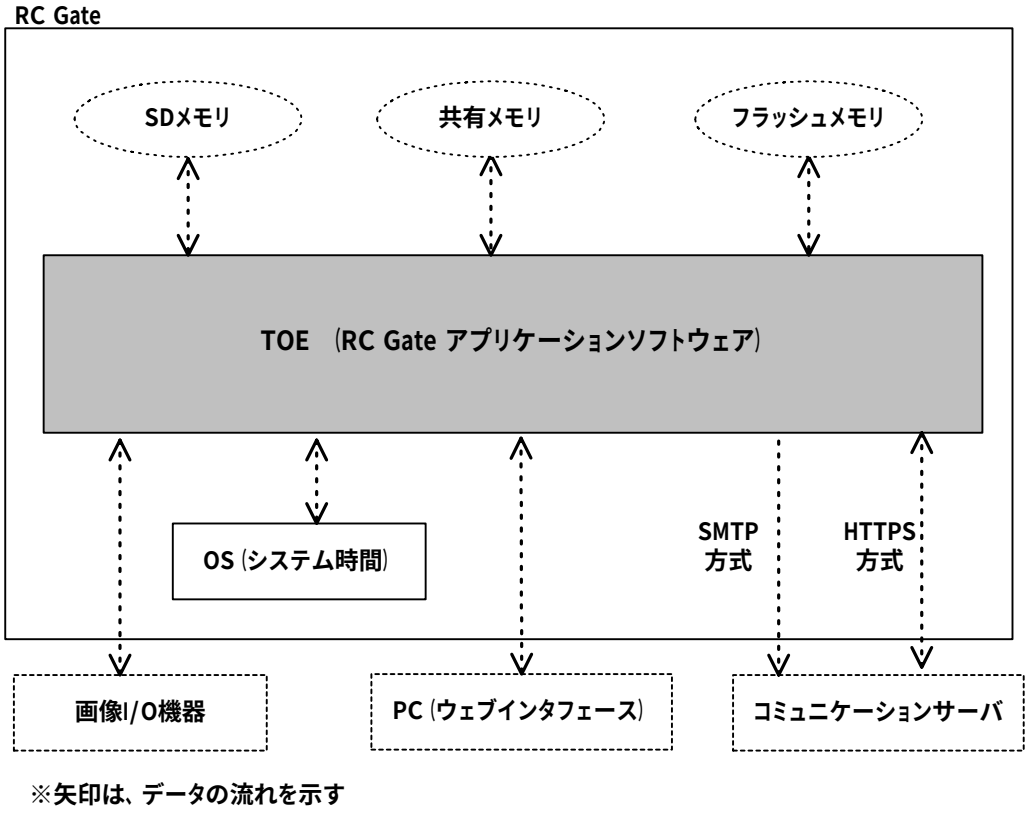

図 1-4 RC Gate **の**TOE**の論理的範囲**

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Remote Communication Gate Type N/L/BN1/BM1セキュリティターゲット Version 1.03」(以下「本ST」という。) [1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「Remote Communication Gateアプリケーションソフトウェア評価報告書」（以下「本評価報告書」という。）[22]に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21] のいずれか）の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、本評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE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。評価は、平成18年6月の評価機関による本評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3適合である。

1.5.3 セキュリティ機能強度

本STは、最小機能強度として、”SOF-基本”を主張する。

本TOEの環境において想定する攻撃の対象が、外部ネットワークを流れる保守管理データであり、利用者に対する直接的な金額的被害を与えない。そのデータ内容の動機付けより攻撃力は低レベルと想定している。また、組織のセキュリティ方針よりパスワードポリシーとしてSOF-基本の機能強度を満たすことを要求している。攻撃者のレベルの想定と組織のセキュリティ方針より、最小機能強度として ” SOF-基本 ” を主張することは妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

・オペレータ識別認証機能
オペレータ種別とパスワードによってオペレータを識別認証する。

・アクセス制御機能
識別認証されたオペレータに対して、そのオペレータに割り当てられているアクセス項目にしたがったアクセス制御をおこなう。

・HTTPS時のCS識別認証機能
CSからRC Gateに送られてくる公開鍵証明書とRC Gateが保持するCSルート証明書を検証することによりTOEは公開鍵証明書の正当性を判断する。さらにCSと情報交換する時には暗号通信を行う。

・S/MIMEメール送信機能
SMTP方式による通信では、RC GateからCSへのメールはS/MIME形式で転送される。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.CS_COMM	RC GateがCSと直接通信するとき、保護資産の情報漏れや不当な変更がインターネットまたは電話回線を介して起こるかもしれない。 外部ネットワーク上の悪意のある攻撃者はインターネットまたは電話回線に対してプロトコルアナライザを使用し、直接RC GateとCSの間で送受信される通信データ(保護資産: RC Gate内の設定情報、収集された画像I/O機器情報、画像I/O機器用データ）を盗み見るかもしれない。あるいは、その通信データに変更を加え、送信者が送信したデータとは異なったデータを受信者に受信させるかもしれない。
T.CS_MAIL	RC GateがCSへの通信に電子メールを使用するとき、保護資産の情報漏れや不当な変更がインターネットを介して起こるかもしれない。 外部ネットワーク上の悪意のある攻撃者はインターネットにおいてプロトコルアナライザを使用し、RC GateからCSへ送信するメール情報（保護資産：RC Gate内の設定情報、収集された画像I/O機器情報）を盗み見るかもしれない。あるいは、そのメールに変更を加え、送信者が送信したデータとは異なったメールを受信者に受信させるかもしれない。
T.FAKE_CS	偽CSが立ち上げられてCSになりすまし、RC Gateと通信をし、不正な情報を送りこんだり、あるいは保護資産を盗んだりするかもしれない。 悪意のある攻撃者は偽CSを立ち上げ、その偽CSの管理者はインターネットまたは電話回線を介して、収集された画像I/O機器情報などの保護資産を取得するかもしれない。

1.5.6 組織のセキュリティ方針

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1-2に示す。

表1-2 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.ACCESS	セキュリティ関連機器にアクセスして操作できる人は、その機器を管理する役割を持っているオペレータに制限しなければならない。 機器を管理する役割をもっている特定のオペレータだけが、TOEにアクセスできるようにしなければならない。CEのアクセスを禁止する機能を、管理者に提供しなければならない。アクセス管理にパスワードを利用し、パスワードポリシーとしてSOF-基本を満たす機能強度を持たなければならない。

1.5.7 構成条件

本TOEは専用筐体で提供されるRemote Communication Gate Type N/L/BN1/BM1のアプリケーションソフトウェアとして、メインボード上のSDメモリ内にプリインストールされ提供される。TOEは専用のプロトコルおよびMIBにより他の機器との通信をネットワークを介して行い、これに準拠した機器が内部ネットワークにつながることが、TOE管理の対象となる条件である。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3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1-3 TOE使用の前提条件

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

	もできないものとする。
A.NETWORK	内部ネットワークは外部ネットワークから守られていることを想定する。 RC Gateと画像I/O機器が動作している内部ネットワークは、インターネットを通して攻撃する外部者から守られているものとする。
A.CE	信頼されたカスタマーエンジニア(CE)は与えられた権限に対する責務を果すことを想定する。 CEは必要な教育を受け、信頼されている。CEはユーザー管理者の許可なしにRC Gateの構成を変更したり、RC Gateを持ち出したり、RC Gateに不必要なプログラムをインストールしないものとする。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用する。また容易に推測できるパスワードは使用しないものとする。
A.ADMIN	信頼された管理者と登録者は与えられた権限に対する責務を果すことを想定する。 管理者と登録者は信頼されている人が担当していることを想定する。管理者と登録者は同じ人であってもよいが、管理者と登録者はRC Gateの構成を設定、変更することができ、RC Gateが正常に動作するように保守するものとする。パスワードは半角の英大小文字、数字、指定された記号の組合せを使用し、すくなくとも6ヶ月に１回は変更するものとする。また容易に推測できるパスワードは使用しないものとする。
A.CS	CSは信頼された会社によって正しく運用されていることを想定する。 CSは信頼された会社によって運営され、その会社はCSを正しく運用保守しているものとする。

1.5.9 製品添付ドキュメント

本製品に添付されるガイダンスドキュメントを以下に示す。

製品名	仕向地	ガイダンス	識別
Remote Communication Gate Type N	日本	Remote Communication Gate Type N/L 安全上のご注意、セットアップガイド	A768-8559
Remote Communication Gate Type L	日本		
Remote Communication Gate Type BN1	北米	Remote Communication Gate Type BN1/BM1 Safety Information and Setup Guide (North American version)	A768-8605B
Remote Communication Gate Type BM1	北米		
Remote Communication Gate Type BN1	欧州	Remote Communication Gate BN1/BM1 Safety Information and Setup Guide (European version)	A768-8603B
Remote Communication Gate Type BM1	欧州		

なお、管理者ガイダンスはSSL通信でのWeb公開形式をとる。

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2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、本評価報告書において報告されている。本評価報告書では、本TOEの概要説明、CEMパート2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。

2.2 評価実施概要

以下、本評価報告書による評価実施の履歴を示す。

評価は、平成17年9月に始まり、平成18年6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17年11月に札幌開発センター、岡崎事業所、大森事業場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクル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18年1月に大森事業所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。

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、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。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

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2-1(A)、図2-1(B)、図2-1(C)に、テストに要するツール一覧を表2に示す。

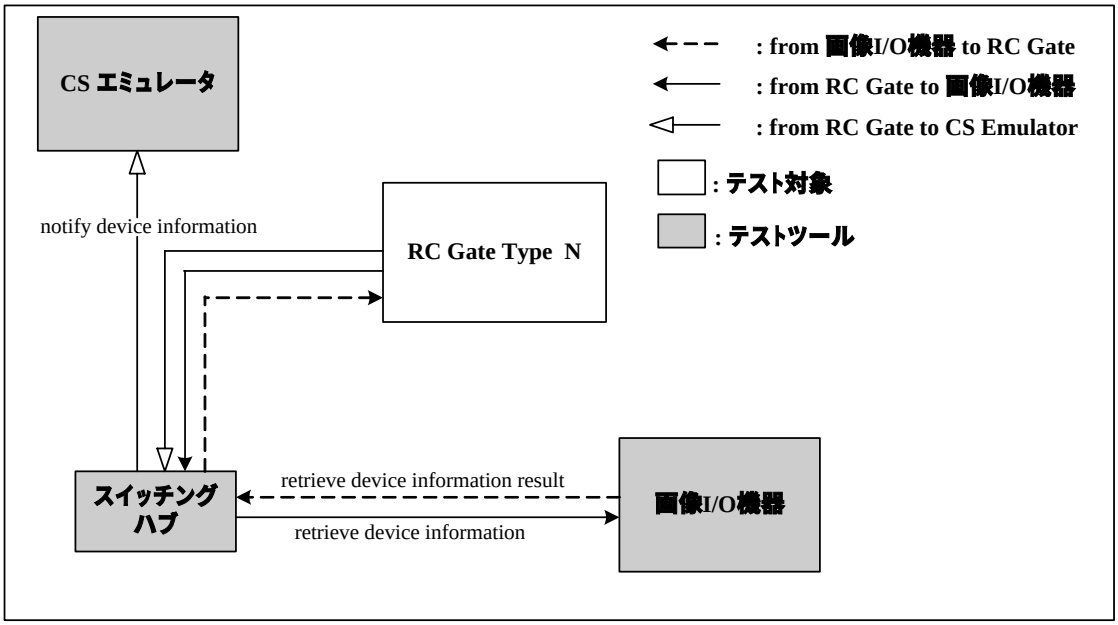

図 2-1(A) RC Gate Type N/BN1**の**HTTPS**方式テスト環境**

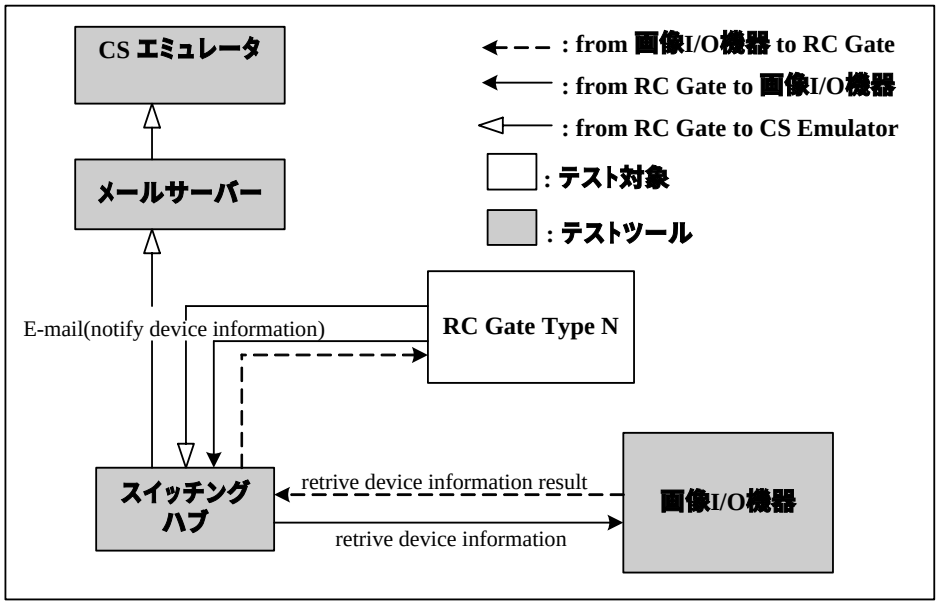

図 2-1(B) RC Gate Type N/BN1**の**SMTP**方式テスト環境**

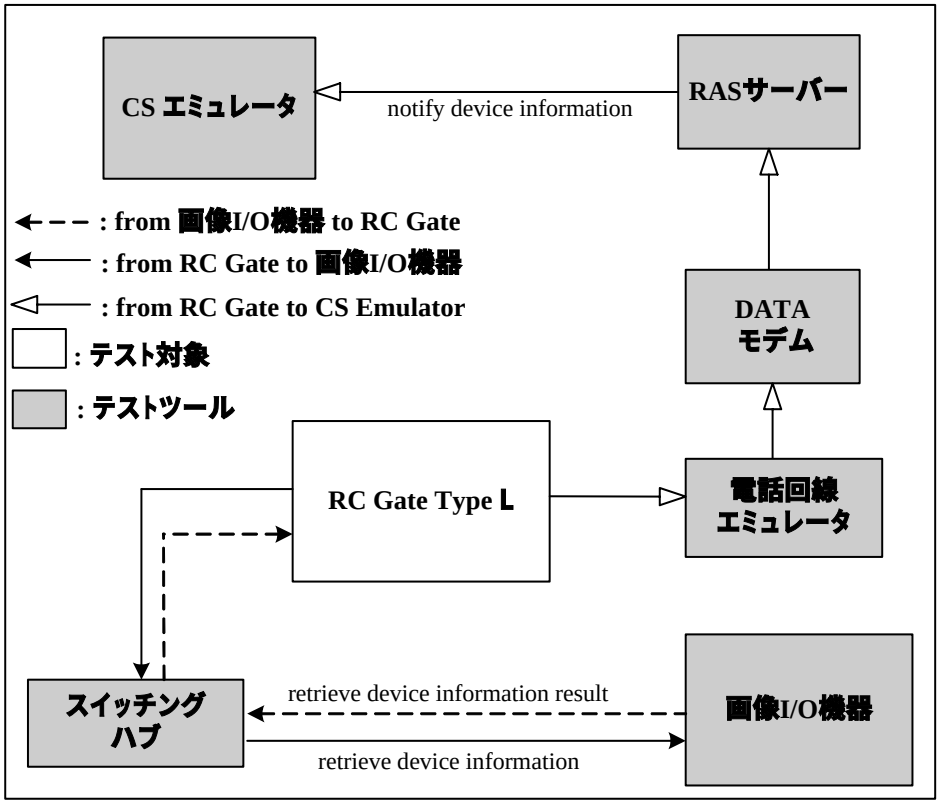

図 2-1(C) RC Gate Type L/BM1**の**HTTPS**方式テスト環境**

表 2 **テストに要するツール一覧**

種別	構成要素
CSエミュレータ	･ハードウェア：HITACHI PC8DK4-PA08P1C00 （PC/ＡＴ互換機機械） ･オペレーティング･システム：Windows 2000のProfessional （バージョン5.00.2195） ･エミュレータ：CS エミュレータソフトウェア（バージョン1.05） ･メール･サーバー：UNIXのsendmail (バージョン8.8.8)
画像I/O機器	･デジタル複合コピー機：RICOH Aficio 3025
RAS-Server	･ハードウェア：akia MICROBOOK 56 （PC/ＡＴ互換機機械） ･オペレーティング･システム：Windows 2000 Advanced Server （バージョン5.00.2195） ･RASサーバー：Windows 2000 Advanced Serverダイアルアップ･サーバー･ソフトウェア (バージョン5.00.2134) ･ファックス/データ･モデム：OMRON ME5614E2 ･ブロードバンド･ルータ：BUFFALO BBR-4HG ･電話線エミュレータ：NEWTECH PASOPHONY
解析ツールその他	･RC Gateアクセス用ブラウザ：Internet Explorer（バージョン6.0.2800.1106） ･ネットワーク･プロトコル･モニタ：EtherReal（バージョン0.9.16 （フリーウェア）） ･SSL通信解析ソフトウェア：SSL Dump（バージョン0.9b3） ･S/MIME解析ソフトウェア：OpenSSL（バージョン0.9.8a） ･WEBキャプチャソフトウェア：achilles（バージョン0.27） ･メール受信ソフトウェア：Outlook Express 6（バージョン6.00.2800.1106）

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。図2-1に示す通り、テスト構成として以下に示す３つのテスト環境が存在する。また、開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

①RC Gate Type N/BN1のHTTPS方式テスト環境 (図2-1(A)）

RC Gate（テスト対象）のネットワークインタフェースを使用して各種テストツールを接続し、RC Gate、CSエミュレータ間でHTTPS方式による接続、通信試験を実施する

②RC Gate Type N/BN1のSMTP方式テスト環境　(図2-1(B))

RC Gate（テスト対象）のネットワークインタフェースを使用して各種テストツールを接続し、RC Gate、CSエミュレータ間でSMTP方式による通信試験を実施する

③RC Gate Type L/BM1のHTTPS方式テスト環境 (図2-1(C))

RC Gate（テスト対象）の電話回線インタフェースを使用して各種テストツールを接続し、電話回線を用いたダイアルアップ接続をエミュレートするテスト環境

RC Gate、CSエミュレータ間でHTTPS方式による接続、通信試験を実施する

b.テスト手法

テストには、以下の手法が使用された。尚、以下のテスト手法は全テスト環境に共通している。

①利用者が操作可能な外部インタフェースを持つ機能については、開発者の手動操作により機能を実行し、動作結果を確認する

②利用者が操作可能な外部インタフェースを持たない機能については、ツールにより通信データをキャプチャし、解析することで結果を確認する

c.実施テストの範囲

テストは開発者によって17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、上位レベル設計に記述されたすべてのサブシステムとサブシステム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。

d.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。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テスト手法は開発者テストと同じ手法がとられた。

c.実施テストの範囲

評価者が独自に考案したテストを7項目、開発者テストのサンプリングによるテストを11項目、計18項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 評価者が独自に考案したテストに関する考慮点

・使用頻度が高い、Webインタフェースを提供するセキュリティ機能に関するテスト

・パスワードによる認証処理が含まれるテスト

・開発者テストにおいて使用頻度が低いテスト構成を使用したテスト

② 開発者テストのサンプリングテストに関する考慮点

・全てのセキュリティ機能を網羅するようにテスト項目を選択

d.結果

実施したすべての評価者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。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

3 認証実施

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 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

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本評価報告書で示されたように評価されていること。

④ 本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 本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及び本評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された本評価報告書、当該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EAL3保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでに

	なされた所見報告書による指摘も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.3.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査相当の方法により確認している。

ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。

ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、TOEの管理者でない利用者が利用可能なセキュリティ機能は存在しかいことを確認している。したがって利用者ガイダンスに該当するものがなく非適用であることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.1.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。

AVA_MSU.1.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法が記述されていることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation

CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

CE	CE（Customer Engineer）はRC Gateの故障時などに点検保守操作する権限が与えられている。CEはリコーまたはリコー関連会社の従業員である。
CE操作許可フラグ	管理者のみ改変可能な設定項目の一つ。CEによるアクセスを許可する場合は、本項目を”許可する”に設定する。
CGI	Common Gateway Interfaceの略。 Webサーバ上のプログラム。Webインタフェースからの要求に応じて、このプログラムは起動される。
CS	Communication Server コミュニケーション・サーバ。RC Gateが画像I/O機器から収集したデータを送信するサーバ。
DBMS	Database Management Systemの略。データベース管理システム。設定情報や収集された情報はこのソフトウェアのもとで管理される。
MFP	MFP(Multi Function Printer)プリンター機能を搭載したデジタル複合機
MIB	MIB（Management Information Base）は管理情報ベースのことである。RC GateはMIBをサポートするネットワーク機器から情報を取得することができる。RFC1156として規定されているMIB1と、RFC1213で規定されているMIB2があり、RC GateはMIB1とMIB2を扱う。
PKI	PKI（Public Key Infrastructure）は公開鍵暗号方式のことで、安全な通信のために使用されるデジタルキーテクノロジーのことである。
RC Gate	Remote Communication Gate Type N、同 Type L、同 TypeBN1、同 TypeBM1 の総称。
SDメモリ	Secure Digital memoryの略。SDメモリはセキュアデジタルメモリ

	カードである。画像I/O機器用の情報やRC Gateアプリケーションそのものを保存、提供するために使用されている。
SSL	Secure Sockets Layerの略。

6 参照

[1] Remote Communication Gate Type N/L/BN1/BM1セキュリティターゲット Version 1.03（2006年6月7日）

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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1: 概説と一般モデル バージョン2.1 1999年8月 CCIMB-99-031 (平成13年1月翻訳第1.2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2: セキュリティ機能要件 バージョン2.1 1999年8月 CCIMB-99-032 (平成13年1月翻訳第1.2版)

[10] 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: セキュリティ保証要件 バージョン2.1 1999年8月 CCIMB-99-033 (平成13年1月翻訳第1.2版)

[11] ISO/IEC15408-1: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC15408-2: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC15408-3: 1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月 (平成13年2月翻訳第1.0版)

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407　平成16年8月

[21] 補足-0210 第2版、補足-0407　平成16年8月

[22] Remote Communication Gateアプリケーションソフトウェア評価報告書
(05000481・01・R03・04) 2006年6月7日