遠隔サービス仲介機器RC Gateのセキュリティ

Security Functions of Remote Communication Gate

柿井　弘*　　佐藤　淳*
Hiroshi KAKII　　Jun SATOH

要　　旨

Remote Communication Gate（以下 RC Gate）は，リコーで開発されたインターネット対応遠隔サービスの仲介機器である．@Remoteというサービス名称で，お客様のオフィス内に設置されることにより，リコーの管理センターと自動接続し，オフィス内の画像I/O機器故障時の即時通報や定期的なカウンター通知あるいはトナーの自動発注などを実現している．インターネットの高速性を利用して，管理センターからのファームウェア更新サービスの提供をも可能とした．

RC Gateの開発にあたっては，お客様のLAN環境を利用することやインターネットで通信することなどから，セキュリティ面を特に重要視した．主なセキュリティ機能は，利用者権限に基づくRC Gateへのアクセス制御，デジタル証明書を搭載することによる管理センターとの相互認証，さらにSSLやS/MIMEの技術を搭載することで実現する暗号化通信などである．

ABSTRACT

Remote Communication Gate (hereafter “RC Gate”) developed in Ricoh acts as a relay unit, which connects the user’s image I/O devices to the remote service center of Ricoh via Internet. It is used mostly in general office and communicates with the center and the image I/O devices automatically. This system, called “@Remote”, realizes immediate machinery trouble call, automated counter checking and ordering supplies like toner. RC Gate is also able to download the firmware for the image I/O devices from the center via fast Internet network to update them.

Security functions of RC Gate are reinforced to protect the information assets from Internet & Intranet threats. The major security features of RC Gate are access control facility for operator, mutual recognition between RC Gate and the center based on digital certificate and encrypted communication using SSL or S/MIME technology.

* ソリューションプラットフォーム開発本部　開発センター
System Solution Center，Solution Platform Development Division

1. 背景と目的

今日のようなあらゆる情報が瞬時にして世界を駆け巡るインターネット社会では，情報セキュリティの重要性を疑う余地はないであろう．オフィス機器の情報管理保護も例外ではない．複写機，ファクシミリまたはプリンタのようなほとんどの画像I/O機器は，多くの情報をその内部に保持しているからである．

一方，私たちはインターネットを利用したさまざまなサービスの恩恵に浴していることもまた事実である．オフィス内の画像I/O機器を例にとれば，故障時の即時通報や課金用コピー利用枚数などのカウンタ値の通知あるいはトナー残量が少なくなったときの自動発注などもインターネットを利用して実現できるからである．その高速性を利用して，これまで多くの労力と時間を費やしていた画像I/O機器のファームウェア更新作業も管理センターからのダウンロードサービスで可能となる．

リコーは，2005年2月より“@Remote”というサービス名称（Fig.1参照）でこのような遠隔サービスを世界展開し始めている．Remote Communication Gate（以下 RC Gate）は，リコーで独自に開発されたインターネット対応の遠隔サービス仲介機器であり，この遠隔サービスの中核をなす．このRC Gateがお客様のオフィス内に設置されることにより，リコーの管理センターと自動接続できるようになるのである．

Fig.1　Logo image of @Remote.

@Remoteのサービスメニューは複数用意されているが，代表的なサービスとその導入による効果を最初に説明しておこう．なお，国内と海外では，ほぼ同様なサービスを提供しているが，そのサービス内容や提供時期は多少異なっている．

(1) 自動故障通報

遠隔サービスでは，リコーのカスタマーエンジニア（以下 CE）に画像I/O機器が故障であることを知らせるサービスコールを自動通報することができるので，画像I/O機器のダウンタイムは大幅に短縮される．

(2) ファームウェア更新

画像I/O機器のファームウェア更新をインターネット経由で行うことができる．お客様にとってもCEにとっても，これまでのようなオフラインによる煩雑な作業はなくなる．

(3) 定期カウンタ通知

RC Gateが管理対象としている複数の画像I/O機器のカウンタ値を取得し管理センターに通知することにより，完全な自動支払請求も可能となる．お客様の煩雑な作業量が減らされ，支払請求のミスや面倒なルーチンワークも減る．

(4) トナー自動発注

RC Gateはトナー残量の通知機能を持っているので，お客様は追加注文のための電話をする必要もなく，トナーのストック忘れや供給遅れについて心配することもない．つまり，お客様自身での在庫管理や発注作業の必要がなくなるのである．ここでも画像I/O機器のダウンタイムは短縮される．

(5) 利用状況レポート

管理センターに集められた機器情報は，そのお客様に利用状況レポートというかたちで提供されている．リコーのポータルサイトであるNetRICOHに登録されている国内のお客様であれば，そのレポートをウェブ経由でダウンロードできる．これにより，お客様は自分のオフィス内にある複数の画像I/O機器の利用状況を簡単に把握できる．この利用状況レポートはオフィス内での画像I/O機器の最適配置のための参考資料にもなる．

これらの特徴から分かるとおり，このシステムを実現するには画像I/O機器と管理センターとの間で，情報が正確かつリアルタイムに伝わらなければならない．なぜなら間違いのない課金やサービス業務をおこなうためには，正確な情報伝達が必要であるからである．また，自動故障通報も故障が発生してから通報するまであまりにも時間がかかるようでは，自動化する意味がない．したがって，仲介機器であるRC Gateは，このシステムではとても重要な位置付けになる．

現在の遠隔サービスでは，画像I/O機器のカウンタ，ト

ナー残量や故障情報を課金処理や保守をするために取得しているが，特にカウンタ値は課金処理に使われるため，カウンタ値の改ざん，あるいは偽センターによって情報を横取りされるといったセキュリティ脅威は，まず防がなくてはならない．画像I/O機器のファームウェア更新においても，不正なファームウェアがダウンロードされるようなことは決してあってはならない．RC Gate自体も，悪意のある第三者により踏み台になったりすることのないよう通信機器としても十分なセキュリティ水準を保つことが重要である．要するに，多くのネットワークセキュリティ脅威に対抗する必要があるのである[1)]．

RC Gateは，これらのセキュリティ上の脅威を防止するよう開発当初から検討が進められてきた．RC Gateの開発にあたっては，お客様のLAN環境を利用することやインターネットを利用することなどから，通信面でのセキュリティを特に重要視してきた．

2. RC Gateの概要

2-1 システム構成

一般的な構成例として，インターネット接続タイプであるRC Gate Type N/BN1（国内版がType N，海外版がType BN1）のネットワーク接続形態を，Fig.2の数値と対応させながら以下説明する．

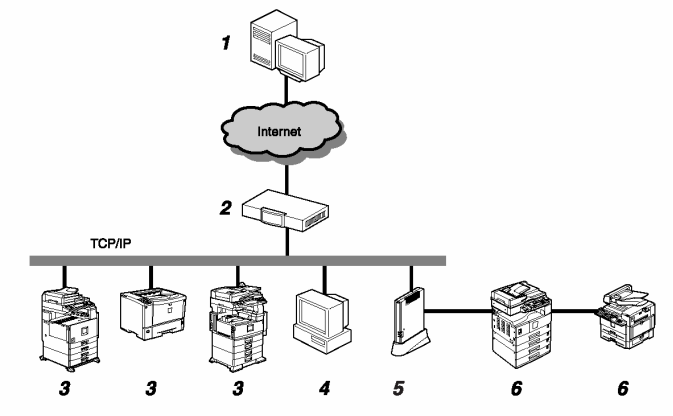

Fig.2 Network environments around RC Gate Type N/BN1.

RC Gateは主に複数の画像I/O機器を利用しているビジネスオフィスに置かれ，画像I/O機器と管理センターとの仲介機器として動作する．RC Gateが収集したデータは，インターネットまたは電話線（ダイアルアップPPP接続）経由でリコーが運用している管理センターに送信される．逆方向の画像I/O機器のファームウェア更新時には，管理センターから受信されたファームウェアはRC Gateを経由し，対象とする画像I/O機器に転送される．

(装置1) 管理センター

RC Gateが通信するセンターをこのように呼ぶ．管理センターは全世界のRC Gateからのアクセスを一元管理している．実際には通信を制御する部分とサービス業務を行う部分は分離されているが，論理的には，すべてのRC Gateはこのインターネット上でひとつの管理センターに接続することになる．

(装置2) ファイアウォール

オフィスのネットワーク環境を保護するためのセキュリティ機器であり，@Remoteではファイアウォールはお客様のオフィス環境で動作していることを前提としている．広義には，プロキシサーバなどもここに含まれる．RC Gate自身は，ファイアウォール機能は持たない．

(装置3) LAN経由で接続可能な画像I/O機器

RC Gateは，@Remoteの遠隔サービスをサポートしている画像I/O機器（以下 @Remote対応機器），および標準規格のひとつであるMIB機能を有する画像I/O機器（以下 MIB対応機器）をLAN経由で管理することができる．RC Gateは，@Remote対応機器とはHTTPSで，MIB対応機器とはSNMPで通信する．

@Remote対応機器では，故障が発生した時はその詳細内容はすぐにRC Gateへ転送され，即時に管理センターへ通報され，自動故障通報のリアルタイム性を確保している．

(装置4) ウェブ端末用PC

RC Gateの管理センターへの登録，あるいは設定変更等は，ウェブブラウザを経由して行う．したがって，管理用にウェブブラウザを搭載した端末用PCが必要である．なお，PCはウェブ端末として利用しているだけで，全ての設定情報はRC Gate内に保持されている．

(装置5) Remote Communication Gate Type N/BN1

RC Gate本体．RC Gateはハードウェア，ソフトウェア込みの通信ボックスとしてリコーから提供されている．オフィ

ス内の複数の画像I/O機器を管理し，その機器と管理センターとの仲介機器として動作する．

(装置6) シリアル接続可能な画像I/O機器

@Remote対応でないリコーの画像I/O機器の多くは，シリアルインタフェース経由でRC Gateと接続することが可能である．このシリアル接続では，1台のRC Gateで最大5台までの同様な画像I/O機器が管理できる．これらの画像I/O機器の情報は，LANを経由せずシリアルインタフェース経由で転送される．

2-2 RC Gateの構成

ここでは，RC Gate本体のハードウェアとソフトウェアの構成を解説する．

Fig.3 The appearance of RC Gate.

ハードウェアは，単体の通信ボックスとして，写真（Fig.3参照）のような専用筐体で提供される．筐体内のメインボードには2つのLANインターフェースとシリアル用インターフェースさらに電源インターフェースが備えられている．ボード上には，CPU，フラッシュメモリ，SDメモリそれにLEDなどが搭載されている．このLEDの表示色と点滅パターンにより，RC Gateの動作状況は外部から確認できる．

電話回線接続の場合は，メインボードにモデムボードを接続した形態で提供される．また，オプションで，無線LANによる接続も可能となっている．

ソフトウェアは，オペレーティングシステム，データベースソフトウェア，暗号モジュール，それに通信モジュールを含めた各種アプリケーションソフトウェアから構成されている．ソフトウェアに関しては，われわれは定期/不定期に脆弱性を分析しており，もし脆弱性が発見された場合には，画像I/O機器同様に管理センターからのファームウェア更新という方法で対応している．

3. セキュリティ機能

RC Gateのセキュリティ機能としては，RC Gate内部情報の漏洩防止，インターネットおよび電話回線からの侵入，あるいはこれら通信経路での情報漏洩防止，偽センターとの情報送受信の防止などが必要と考えられた．そこで，利用者権限に基づくRC Gateへのアクセス制御，デジタル証明書利用によるセンターとの相互認証，さらにSSLやS/MIMEの技術を使った暗号化通信の仕組みを搭載することとした．以下，本題であるRC Gateのセキュリティ機能を解説しよう．

3-1 オペレータ認証及び権限付与

RC Gateへのオペレータからのアクセスには，ウェブインタフェースが利用される．アクセス可能なオペレータとしては，管理者，登録者およびCEが事前に定義されている．それぞれのオペレータのアクセス項目（閲覧可/不可，変更可/不可）は次のように分離されている．

管理者は，RC Gateの設定情報にアクセスし，その設定を閲覧変更できる．登録者は，管理する画像I/O機器とRC Gate本体を管理センターに登録するための情報にアクセスできる．管理者が登録者を兼ねる場合が少なくないが，次に説明するCEがこの役割を代行することもある．

CEは，RC Gateの保守管理情報にアクセスできる．ここでのCEとは，RC Gateを取り扱うための教育を受け，RC Gateの設置および障害対応ができるリコーが認定した信頼されたCEを指している．

ウェブアクセス時の通信方式は海外版ではHTTPSのみが有効であり，ネットワークモニタリングによるパスワードを含めた情報流出を防いでいる．HTTPSは，ご存知の方も多いと思われるがインターネットで広く利用されているHTTP上でのセキュアなSSL通信を実現する技術のひとつである．

ウェブのトップ画面では，オペレータ選択とそのパスワードが要求される．各オペレータは，対応するオペレータ

選択とそのパスワード入力を行う．RC Gateで認証されると，そのオペレータに与えられているアクセス項目のみが画面に表示される．認証が失敗したならば，オペレータはいっさいのアクセスを拒否され，その後の操作を実行することはできない．

パスワードに関しては，パスワードの入力が3回連続して失敗した場合，RC Gateにより1分間ウェブでのアクセスは拒否される．また，各オペレータは自分自身のパスワードを変更することができるが，新しいパスワードの長さは，8～13文字の間でなければならない．パスワードの長さがその範囲内でない場合，新しいパスワードへの変更は拒否される．これらの機能は，ランダムアクセス攻撃に対して十分な強度（Fig.4参照）を保つためにある．

Elapsed Time and Access to TOE:

It does not take long time for attackers to identify the attack method (< 0.5 hour)(*), and it is not necessary to access the TOE to identify (< 0.5 hour). The following calculation is for the actual exploiting.

According to the Access Code metric, the number of possible patterns is 36^8. So, the average number of tries for successful verification is $36^8 / 2$. It is possible to try authentications 3 times in 1[one] minute, so that, it takes 20 seconds for 1[one] trial. Then, the average time t to exploit this mechanism is:

$$t = 20 * 36^8 / 2 \text{ (sec)} = 326517350.4 \text{ (day)} \text{ “> 1 month”(*)}$$

Since it is necessary to access the TOE during the attacks against password mechanism, the average time of access to the TOE is equal to t.

* Four cases of elapsed time, “< 0.5 hour”, “< 1 day”, “< 1 month”, and “> 1 month”, are listed in [CEM].

Fig.4　Analysis of elapsed time and access.

また，CEのアクセス可/不可を付与する決定権は，管理者のみが保有している．管理者の設定項目でCEアクセスを不可にすることにより，たとえCEが正しいパスワードを入力したとしてもログインは拒否され，RC Gateにはいっさいアクセスできなくなる．この機能は信頼できるCEかどうかを管理者が判断してアクセス権を与えるためのものであるが，万が一CEのパスワードが漏洩しても管理者権限で悪意のある第三者からの侵入を防止できるという意味合いもある．同様に，RC Gate自身のリモートファームウェア更新の可/不可の決定権も管理者のみが保有している．

3-2　通信関連機能

RC Gateは，管理センターにアクセスするときは，データ通信に先立って管理センターの識別認証を行う．

RC Gateの特徴的な動作として，RC Gateは管理センターに対して必ずクライアントとして接続することが挙げられる．これは，お客様のオフィス環境のセキュリティ水準を維持するための対応のひとつである．

インターネットを利用した遠隔サービス導入にあたっては，遠隔サービス用のポートをファイアウォールに開けるという選択もあるが，これではオフィス環境全体のセキュリティ低下を招きかねない．インターネットの悪意のある第三者にその通信ポートからオフィス内に侵入されるかもしれないという脅威が発生してしまうからである．

RC Gateと管理センターとの通信においては，RC Gateはデジタル証明書（以下　証明書）を使ったPKI[2), 3)]によるセンター識別認証を行うので，この証明書の説明をしておこう．

@Remoteサービスでは，@Remote対応機器や仲介機器であるRC Gateはリコーから提供され，管理センターもリコーで運営されている．要するに，システムがほぼリコー内で閉じているのである．これは大きな特徴で，@Remoteサービスのための証明書発行局もプライベートCAとしてこのシステム内に立ち上げられることとなった．@Remote対応機器とRC Gateおよび管理センターの証明書は，すべてこの@Remote専用の証明書発行局からリリースされている．なお，証明書発行のための工場とのオンラインシステムも@Remoteサービスに先立ち，インフラとしてわれわれがまったく新たに構築したものである．

このような仕組みにより，全世界の市場に出まわっているRC Gateは，遠隔地からでもネットワーク経由で証明書による個体の特定が可能になっている．遠隔サービスにおける個体の確実な特定は，誤った課金などを防止する上でも大変重要である．

実際のセンター通信においては，まず，管理センターの証明書が@Remote専用の証明書発行局から発行されたものであること，かつ証明書が有効期限内であることを，SSLサーバ認証を使ってRC Gateがチェックする．これにより通信先が@Remoteに対応しているかどうかが判別できる．次に，証明書内の固有情報である管理センターの識別子を同じくRC Gateがチェックする．このチェックにより，管理センターが世界でただひとつの存在，言い換えれば偽の管理センターでないことを保証しているのである．

管理センターもアクセスしてきた通信機器が@Remote対応の機器であることを確認するためにSSLクライアント認証を行い，RC Gateと管理センターの両者が相互に認証して，は

じめてデータ通信を開始することになる．どちらかで認証が失敗したときは，その時点で通信は切断され，以降のデータ通信は行われない．

HTTPS方式では，SSLの相互認証を行った後に共通鍵でのデータ暗号化を行う．共通鍵としてはいくつかの暗号方式が利用可能である．管理センターも@Remote対応機器も複数の暗号方式をサポートしているため，実際の通信時はそれらの中で最強の暗号方式がネゴシエーションにより決定され利用される．

3-3　監査ログ

RC Gateは，監査ログとして，アクセスログ，通信ログそれにシステムログの3種類のログ情報を内部に保存している．

アクセスログは，ウェブインタフェースからRC Gateへのアクセス記録であり，日付・時刻，ターミナルIPアドレス，オペレータ種別，ログイン結果が記録されている．もちろん成功だけでなく，不正なパスワードでログインが失敗した時の情報も残される．

通信ログは，RC Gateと外部機器との通信を記録したもので，日付・時刻，通信機器のIPアドレス，通信方向，送受信情報が保存されている．ここでいう送受信情報とは，どのようなメッセージの送受が行われたかの情報であって，送受信の内容そのものはここには記録されない．

システムログは，アプリケーションプログラム及びオペレーティングシステムのタスクレベルの動作記録で，主に障害が発生した時の解析に利用される．

アクセスログ，通信ログはすべてのオペレータ権限で閲覧できるが，システムログは，CE権限でのみの閲覧が可能である．なお，どのオペレータもこれらの監査ログの変更や削除をする権限は持っていない．

3-4　利用ポートの制限

一般に，通信機器において利用しないポートをクローズするというのは最も簡単かつ効果的な脆弱性対策である．インターネットを利用した通信装置には，telnetやftpなどで侵入されて内部情報を破壊されるかもしれない，あるいは踏み台となって中継サーバになってしまったりするかもしれないといった脅威が存在している．これらの脅威を事前に排除する効果的な方法が利用ポートの制限なのである．悪意のある第三者がいたとしても，telnetやftpのポートをクローズしてしまえば，その機械にログインするといった行為そのものができなくなるからである．RC Gateは，セキュリティ上の観点から必要最小限の通信ポート以外は全てクローズするようにしている．

4. セキュリティ認証

4-1　国際標準に基づくセキュリティ評価

RC Gateは，ISO/IEC 15408[4), 5)]に基づくセキュリティ認証を取得している．ISO/IEC 15408は，セキュリティについて，公的に認められた第三者評価機関が検査評価を行うことにより認証されるセキュリティ評価基準のひとつである．

製品が持つセキュリティ強度の評価ではなく，製品が矛盾のない設計に基づき安全な環境で正しく作られ，かつお客様が正しく使用できる方法を提供していることを保証するものである．評価の対象は，製品のセキュリティ機能だけでなく，仕様書や設計書の管理品質，マニュアル記述の妥当性，開発拠点のセキュリティ，製造現場のセキュリティおよび配送手順の安全性と多岐にわたる．

ISO/IEC 15408では検査の深さに応じて「評価保証レベル（EAL = Evaluation Assurance Level）」が規定されている．簡単な検査だけで済むEAL1から，非常に厳密な検査まで行われるEAL7まで，7段階のレベルが存在する．EALを上げると検査内容が厳密かつ複雑になるため評価コストも高くなる．一般の民間製品についてはEAL1～4のレベルが適用されることがほとんどである．

4-2　RC Gateのセキュリティ評価

RC Gateは，前章で述べたセキュリティ機能についてISO/IEC 15408 EAL3の認証を取得した．評価はドイツ連邦共和国の評価機関であるTUViT社に依頼し，評価文書の作成および連絡等は英語で行った．ISO/IEC 15408では，製品そのものの評価が行われるのはもちろんであるが，まず評価文書によりセキュリティ機能を明確に定義する必要がある．今回のセキュリティ評価のためにリコーが用意し，評価機関へ提出した文書は以下に示すとおりである．

4-2-1　評価文書（Evaluated Documents）

(1) 仕様・設計

・Security Target（セキュリティターゲット）

製品のセキュリティ設計の基本的な方針と，それに基づくセキュリティ機能を説明するもので，セキュリティ評価における最重要文書．想定されるセキュリティ脅威とその対策方法はこの文書の中で完結していなければならない．認証されるとインターネットに公開されるので，誰でもその内容を読むことができる．

・Functional Specification（機能仕様書）

セキュリティ機能を評価対象の外部インターフェースの観点から説明する文書．評価対象部分の論理的な外部インターフェースの定義から始まるので，一般的な機能仕様書のイメージとは異なる．

・High-level Design（上位レベル設計書）

製品がどのような構造でセキュリティ機能を実現しているかの詳細を記述説明する文書．詳細設計書に相当するものであるが，こちらは評価対象部分の論理的な内部インターフェースを最初に定義する必要があり，やはり一般的な詳細設計書とは異なるところも多い．

(2) 分析

・Correspondence Analysis（関係記述書）

上記3つの文書が矛盾なく記述されていることを分析する文書．セキュリティ機能と外部インターフェース，さらに内部インターフェースとの相関関係を，マトリックスを利用して表現する．

・Strength of Function Analysis（機能強度分析書）

製品が持つセキュリティ機能強度を，数学的な計算により分析する文書．前述したようにこのセキュリティ認証はセキュリティ強度の評価が目的ではないが，考えられる脅威に対して十分な強度があることは証明する必要がある．

・Vulnerability Analysis（脆弱性分析書）

どのような製品にもセキュリティ上の脆弱性は存在するが，その製品に内在する脆弱性が想定している利用環境のもとでは問題とならないレベルであることを分析説明する文書．

(3) テスト

・Security Test Documentation（テスト仕様/結果）

製品のセキュリティ機能が正しく動作していることを確認するためのテスト仕様を，前述のセキュリティターゲット，機能仕様書それに上位レベル設計書に対応させながら定義していく．このテスト仕様に従ったテストも行い，結果レポートとして提出する．

(4) ガイダンス

・Guidance Documentation（ユーザズマニュアル/サービスマニュアル）

マニュアルには，必要十分なセキュリティ情報が含まれていなければならない．かつ，誤った使い方を誘発するおそれのあるようなあいまいな記述がされていないことも求められる．

(5) 開発・製造・配送

・Development Security（開発セキュリティ）

製品の開発現場が安全な環境である（機密情報の漏洩がない）ことを説明する文書．仕様書の管理方法はもちろんのこと，開発時のネットワーク環境の安全性（社内LANであってもネットワークの暗号化通信が実現しているかなど）や開発を行っている建物自体の物理的なセキュリティも評価対象となる．

・Configuration Management（構成管理）

開発現場において，正しいバージョン管理がなされ，間違ったソフトウェアリリースなどが発生しないような方式を採用していることを説明する文書．

・Production Procedure（製造手順）

製造現場において，正しいバージョンの製品が間違いなく製造されていることを説明する文書．工場建物自体のセキュリティも評価対象となる．

・Delivery Procedure（配送手順）

正しいバージョンの製品がお客様の手元まで安全に配送されるような方法を採用していることを説明する文書．

4-3　具体的な対応事項

実際の評価作業では，仕様書や設計書およびマニュアル等の文書評価のほか，評価者テストや開発現場の監査等，様々な観点からの評価が行われた．評価機関は前章の評価文書がISO/IEC 15408に規定されている機能要件（Fig.5参照）や保証要件[6), 7), 8)]を満たしているかどうか検査を行い，実際に評価者が来日した上で開発現場のセキュリティを始めとするいくつかの点について現場を確認したり，評価者自身によ

る製品のテストが実施されたりした.

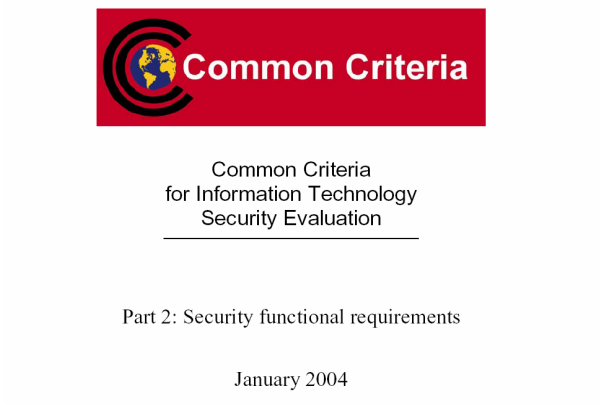

Fig.5　Security functional requirements.

今回の評価対象は，RC Gateに搭載しているアプリケーションソフトウェアとした．評価がスタートして間もないうちは，評価機関に全体の構成を正しく理解してもらうことが大切である．その後，Observation Reportと呼ばれる文書での質問や指摘の対応を通して，評価対象部分と対象外部分との境界，あるいはセキュリティ機能が正しく設計実装されていることを証明していく．RC Gateには暗号モジュールが搭載されているが，その部分の仕様/設計については，より詳細な記載を求められた.

RC Gateの開発は二拠点で行われた．当然，開発時には両者でデータのやり取りなどが頻繁に行われるが，双方で同期の取れた開発方式がとられていることを説明しなければならなかった．リリースされるアプリケーション，ソースコードやツール，その他文書類の構成管理が正しく行われているかも監査の対象となる．また，構成管理ツールを利用していたので，その利用手順，アクセス権，ログの管理まで監査の対象となった．開発されたアプリケーションのリリース時には，そのリリース形態，リリース通知の審査承認手順などの明確化が求められた.

また，製品の開発現場は機密文書の漏洩などがなく安全に管理されていることを証明しなければならない．ひとつの拠点では，非接触IDカードにより開錠するオートロック施錠システムを採用し，入退室管理まで徹底した．もうひとつの拠点では，フロア単位に磁気カードによる施錠システムが設置されていたが，これでは物理的セキュリティとしてはまだまだ弱いとの指摘を受けた．そこで，フロア施錠の他にRC Gate開発部署をパーティションで囲み，さらにメカニカルキーによる施錠システムを設置することで対応した.

RC Gateの製造拠点も監査の対象となる．製造拠点からお客様までの配送中に第三者により製品が不正な扱いを受けないことを保障しなければならない．RC Gateの配送手段においては，梱包箱に開封検知シールを貼ることで対応した．これにより，お客様の元に製品が届いたときに配送途中で開封されていないことを保障することができた.

評価の中では，RC Gateのセキュリティ機能が正しく動作していることを確認するためのテスト仕様の提出とその結果報告をしなければならないが，その他に評価者自身がテスト仕様を考える評価者テストも行われた．評価者テストにおいては開発側で想定していないような使用方法を試してくることが多い．評価者が来日した際には，その評価者による監査の元で，基本的には日本側の評価者がテストを行いその結果を彼らが評価するという手順がとられた．RC Gateはインターネット対応製品であり，画像I/O機器や管理センターとつなげるテストが必要であるが，評価者テストにおいては画像I/O機器のエミュレータと管理センターのエミュレータを使用することで対応した.

お客様に製品のセキュリティ機能を正しく理解してもらうためのマニュアルの重要性も再認識させられた．せっかく実装したセキュリティ機能も正しく使われなくては，その機能も発揮できないからだ．また，お客様に注意していただかなければならない運用上のセキュリティ事項も少なくはない．それらの注意事項も，誤解のないようにマニュアルに明解に記述するよう心がけた．RC Gateでは，ユーザーズマニュアルはインターネットからダウンロードできるようにしているが，完全性を保証するためのダウンロード方法も評価対象になった.

4-4　成果

リコーは関連業界に先がけて，セキュリティに関する取り組みを実施してきた．今回，網羅的なセキュリティ設計を行い，RC GateにおいてISO/IEC 15408に基づく評価を受け，その認証を取得した．これは，RC Gateがセキュリティに関して正しい設計のもとで，確実にその機能が実装されていることを第三者評価機関によって認められたことを意味している．特に，お客様からの実際の要望が多いインターネットで

の情報漏洩を防ぐセキュリティ機能について，第三者機関による証明が得られたことの意義は大きい．

5. おわりに

以上が遠隔サービス仲介機器RC Gateのセキュリティの紹介である．@Remoteは，本稼動からもうすぐ1年近くなるが，すでに国内外の多くのお客様に利用していただいている．将来のRC Gateはお客様とリコーをつなぐ仲介機器として，これまでにはなかったような新しいサービスを提供できることであろう．

今後さまざまな形態でのサービスが提供されていくと思われるが，どのような形態であれお客様にセキュリティに関しては安心して利用していただけるものを提供していくことはわれわれの使命と考えている．

セキュリティ認証に関しては，バージョンアップ時にもそのセキュリティ水準が維持されていることを公的に保証する保証継続というISO/IEC 15408の新しい制度を積極的に利用していく方針である．

参考文献

1) 大澤文孝: ITセキュリティ・マニュアル，初版，工学社, (2000).
2) 塚田孝則: 企業システムのためのPKI，初版，日経BP社, (2001).
3) 小松文子: PKIハンドブック，初版，ソフト・リサーチ・センター, (2000).
4) 太田雄介，金井洋一: imagio Neo 350/450 シリーズのセキュリティ ～ ISO/IEC 15408 認証取得 ～，Ricoh Technical Report, No.28, (2002), pp.121-124.
5) 内山政人: ISO15408 情報セキュリティ入門，第1版，東京電機大学出版局, (2000).
6) ISO/IEC 15408-1, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model Version 2.2 (2004)
7) ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements Version 2.2 (2004)
8) ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security- Part 3: Security assurance requirements Version 2.2 (2004)