第 4 章　経路情報の登録機構の設計と構築

内容

- 「経路情報の登録機構」の背景と意義
- 機能の概要
- 仕組みと構成
- 認証局の設計

ほか

4. 経路情報の登録機構の設計と構築

本章では、インターネットレジストリにおける割り振り／割り当て情報を、ルーティングの分野における情報登録機構である RR（Routing Registry）に役立て、インターネットの可用性を向上させる仕組みの設計と構築について述べる。

経路情報の登録機構は、2005 年度の調査研究で明らかになっていた要件と、2006 年度に行った RIR・IETF における現地調査の結果を受けて、本機構の実験運用のために設計・構築された。

2005 年度から 2006 年度にかけて、APNIC、ARIN 等の RIR において IRR（Internet Routing Registry）の運用が始まりつつあるが、IP アドレスの割り振り情報／割り当て情報を活用して、既存の IRR における登録情報の正当性を維持するような仕組みは他に例がない。本機構の持つ機能は IRR と IP レジストリシステムが別の構成である場合に有効であり、例えば ARIN における IRR の登録情報の正当性維持にも役立つ可能性がある。

一方、本機構によって新たに発生する、LIR による IRR への情報登録の認可という業務は、日本国内の LIR では行われていない。RIPE NCC ではこの業務が行われていることが判明しているが、日本国内においては実験的な試みとなる。

4.1. 背景

現代のインターネットにおけるルーティングは AS（Autonomous System ― 自律システム）の考え方に基づいて行われている。各 AS は自 AS のネットワークを保護するために、他の AS から流入する経路情報の取捨選択を行っていることから、AS は統一されたルーティングポリシーを持つ範囲を意味すると共に、統一された”信頼ポリシー”の範囲を意味しているとも考えられる。AS 間の経路情報の情報交換のために IRR が使われている場合、その AS の対外的な安定性やネットワークの可用性はその IRR に依存していると考えられる。

一方、IP アドレスはインターネットレジストリの構造に則って管理されており、AS とは独立した構造を持っている。IP アドレスの返却や移管は本来 AS におけるルーティングポリシーの変更に反映されるべき情報であるが、IRR ではインターネットレジストリの割り振り／割り当てとは独立した情報登録が行われている。このことで、現在の IRR を使ったルーティングでは以下のような問題が起こる可能性がある。

○割り振られていない IP アドレスの不正利用

インターネットレジストリに割り振られていない IP アドレスが使用されると、IP アドレスの想定外の早期枯渇を招くだけでなく、今後割り振られる組織に対する迷惑行為が起こってしまう。また割り振られていない IP アドレスを使って大規模な不正行為が行われた場合に、その不正行為の発生源を特定することが難しく、再発を防ぐために IP アドレスを大量に浪費してしまう可能性がある。

○他の組織に割り振られた IP アドレスの不正利用

本来他の組織に割り振られている IP アドレスを不正に利用すると、その組織のインターネットとの接続性を失わせたり、その組織のトラフィックを迂回させすべての通信を盗聴したりできる可能性がある。この不正利用は、故意に行われているものだけでなく、オペレータによる IP アドレスの打ち間違いによっても起こりうる。

これらの問題を防ぐにはいくつかの対策が考えられるが、根本的な解決を図るには、インターネットレジストリの持つ割り振り情報／割り当て情報を IRR における登録情報のチェックに使い、IRR への不正登録やインターネットでの不正な経路制御を検知／防止するという方法が考えられる。

4.2. 「経路情報の登録機構」の意義

○本機構の目的

経路情報の登録機構は、割り振り情報／割り当て情報との整合性を持たない不正なオブジェクトを JPIRR に登録できないようにする仕組みである。JPIRR は、IP アドレスの割り振り／割り当てを管理しているインターネットレジストリの JPNIC によって運用されている。

インターネットレジストリにおける割り振り情報／割り当て情報と比較し、割り振られていない IP アドレスや、他の AS に使われていることが想定されている IP アドレスである場合には、IRR に当該範囲の IP アドレスの情報を登録することができない。

IRR に登録されている情報の正当性を維持することで、インターネットにおける不正な IP アドレスの利用を検知することが可能になる。これにより不正な経路制御によって特定の AS のネットワークの可用性が損なわれたり、登録されていない IP アドレスを使った不正行為の影響範囲を拡大させられたりすることを防ぐことが可能になる。

これには AS の境界にあるルータが IRR の情報を利用することにより、インターネットで交換されている経路情報を検証する仕組みが必要になるが、その仕組みに先立って IRR が登録情報の正当性を維持しておく必要がある。

○IRR の情報の正しさとは

本機構の設計にあたり、IRR に登録される情報の正しさを以下のように定義した。

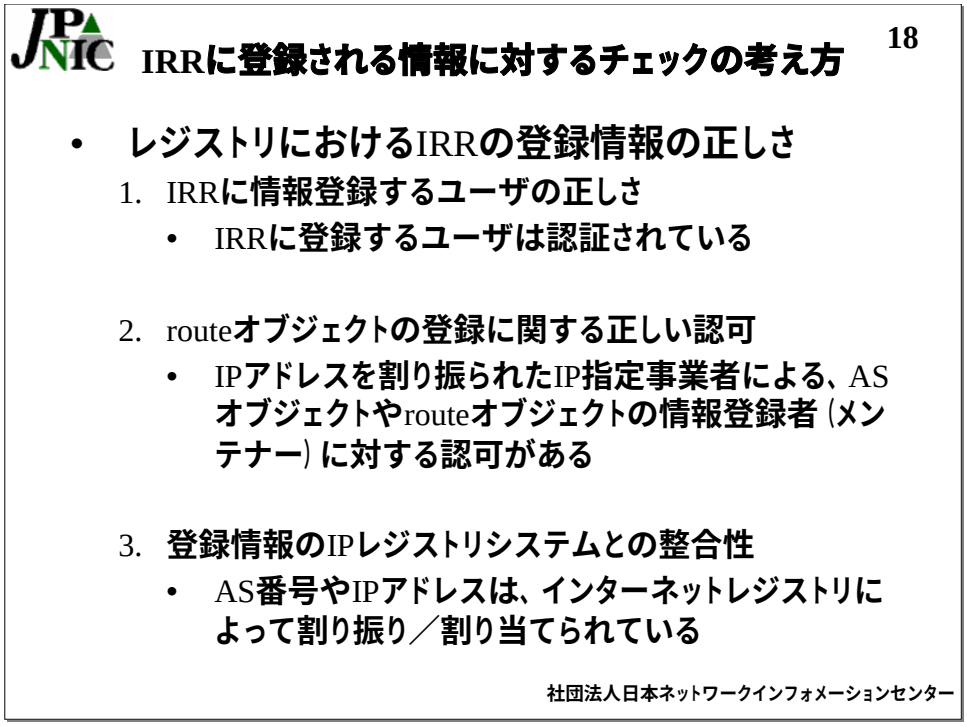


図 4-1　本機構における IRR の登録情報の正しさの定義

図 4-1 は、本機構についてインターネットコミュニティからの意見を集約するために、JPOPM（JPNIC Open Policy Meeting）での発表に用いたスライドの一部である。

○IRR に情報登録するユーザの正しさ

既存の IRR では、自己申告の情報を元に管理主体のメンテナー（Maintainer）情報が登録されている。メンテナーの認証方法としては crypt パスワード、mail-from、PGP-KEY の 3 種類から選択することになっている。crypt パスワードは、登録時にパスワードが平文で転送されるだけでなく、情報登録時には電子メールに平文で書かれたパスワードが転送される。また mail-from は情報登録時の電子メールの From に予め指定された電子メールアドレスが記述されているかで本人性の判断を行う方法である。From 行に書かれる電子メールアドレスは JPIRR の公開情報でもあるため、本質的に認証しているとは考えにくい。PGP-KEY は PGP の鍵を登録し、それ以降の情報登録で PGP の電子署名を使った電子認証を行う手法である。一旦鍵が正常に登録されると以降はなりすまし行為は難しくなるが、初期の登録で man-in-the-middle 攻撃等が行われると、以降の登録ではすべてなりすまされた状況が続いてしまう危険性がある。

IRR に情報登録するユーザの正しさを確保するには、ユーザ登録、登録業務の実施、担当者の変更の 3 つのケースにおいて対策が必要になると考えられる。またすべてのユ

ーザは、IRR に情報登録する際に電子的な認証を受け、既知のユーザであることが確認されるものとした。

○route オブジェクトの登録に関する正しい認可

IRR における登録情報がインターネットにおけるルーティングで問題になるケースは、IP アドレスの範囲（以下、prefix と呼ぶ）と AS 番号の間違いや組み合わせの間違いによって起こる。

IRR は、ある prefix が本来どの AS によって使われているかを確認するために使われることがある。その為に参照される登録情報は route オブジェクトと呼ばれるもので、prefix と Origin AS（prefix の経路広告を行う AS）が記載されたものである。既存の IRR では、route オブジェクトに記載された Origin AS が正しいものであるかどうかのチェックは行われていない。従って本来他の AS から経路広告されるべき prefix が記載されている可能性があり、インターネットにおける経路情報と比較をしてもその真偽を発見するためには役立たない可能性がある。

一方、IP アドレスの割り振りを受けた LIR が、すべての prefix に対して Origin AS を把握することは、現代の大規模化した LIR にとっては難しい。LIR によっては AS の運用を外部の組織に委託しているケースもある。従って、具体的な Origin AS の AS 番号としてチェックするのではなく、より大きな粒度で正確性をチェックできるような考え方を導入する必要がある。

本機構では、この正確性を LIR と IRR に登録されたメンテナーの組み合わせで確認するものとした。IP アドレスの割り振りを受けた LIR は、その prefix が入った route オブジェクトを登録しうるメンテナーを指定する。指定されたメンテナーは、任意の Origin AS を記載した route オブジェクトを IRR に登録できる。この指定のことを本機構では認可と呼ぶ。

○登録情報の IP レジストリシステムとの整合性

route オブジェクトに記載された prefix は、少なくともインターネットレジストリによって割り振り／割り当てが行われた IP アドレスであると考えることができる。

JPIRR のようにインターネットレジストリで運用されている IRR では、データベースを照合することで、割り振られていない prefix が route オブジェクトに登録されないようにすることを検知できるはずである。

本機構では IRR に登録される prefix は、JPNIC に割り振られたものである点の確認を行うものとした。なお JPNIC 以外に割り振られた prefix を登録することは可能であるが、その場合には JPNIC のデータベースを使って検証することができないことから、

識別が可能なフラグを表示するものとした。

4.2.1. 機能概要

本機構の機能概要を図 4-2 に示す。

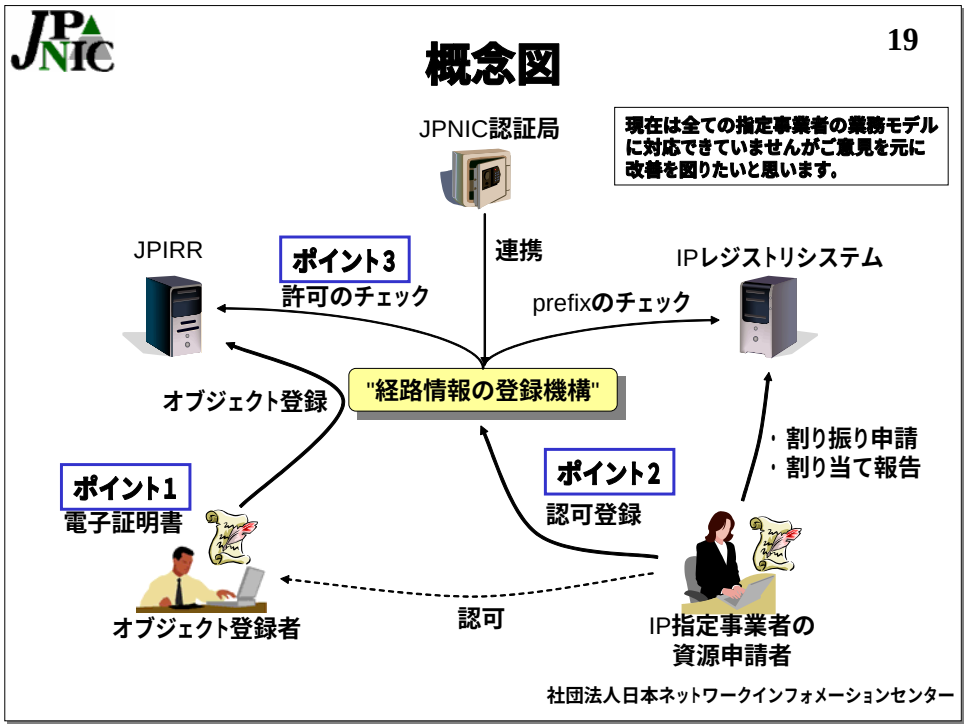


図 4-2　経路情報の登録機構の機能概要

前節で述べた登録情報の正当性維持のため、経路情報の登録機構は、大きく分けて 3 つの機能を持つこととなった。一つ目の機能は電子証明書を用いたユーザ認証である。オブジェクト登録者はクライアント認証用の電子証明書が発行され、JPIRR への情報登録の際の認証のための電子署名に利用できる（ポイント１）。二つ目の機能は IP 指定事業者によるメンテナーへの「認可」である。IP レジストリシステムで IP アドレスの割り振り申請／割り当て報告等の業務に使われている電子証明書を使って、IRR のメンテナーに対して、route オブジェクトの登録を認可する（ポイント２）。三つ目の機能は route オブジェクトが JPIRR に登録する前の、記載内容のチェックである（ポイント３）。

各々について以下に述べる。

○ポイント１：JPIRR ユーザ向け電子証明書

図 4-3　JPIRR ユーザ向け電子証明書

本機構では、IRR に情報の登録を行うユーザを 2 種類に分類した（図 4-3）。IRR に情報登録を行うものを「オブジェクト登録者」と呼び、オブジェクト登録者の管理を行うものを「証明書管理者」と呼ぶ。証明書管理者はオブジェクト登録者の本人性確認手続きを行うと共に、オブジェクト登録者の追加／削除を行うことができる。

オブジェクト登録者のユーザ登録は証明書管理者が行う。ユーザ登録が行われるとオブジェクト登録者の電子証明書が発行され、登録業務ではその電子証明書を使った電子認証が実施される。オブジェクト登録者の鍵の漏洩の疑いがあるときは証明書管理者がそのオブジェクト登録者のクライアント証明書を失効させ、必要があれば新たな電子証明書を発行することができる。Web ブラウザ等のソフトウェアトークンに保存された電子証明書や秘密鍵は、バックアップ等の理由で Web ブラウザ外に保存されることが多く、一旦ファイルとして保存されるとユーザが知らないうちに漏洩する危険性がある。しかしその危険性がわかった時点で、気軽に電子証明書の再発行ができれば、秘密鍵が漏洩した可能性のある電子証明書を使い続ける必要はなく、安心して使うことができる。

証明書管理者のユーザ登録は、オフラインでの書類検査を通じて行い、証明書管理者の電子証明書と秘密鍵はハードウェアトークンを用いて配布する。証明書管理者がオンラインの認証を受けるときにはハードウェアトークンが必要であり、その担当者が変わるときにはハードウェアトークンの受け渡しまたは再発行を行うことで、秘密鍵の漏洩を防ぐことができる。（ハードウェアトークンの漏洩は、物品の紛失であるためソフトウェアトークンのコピーと異なり、ユーザが感知しやすいと考えられる）

○ポイント２：許可リストを使った認可登録

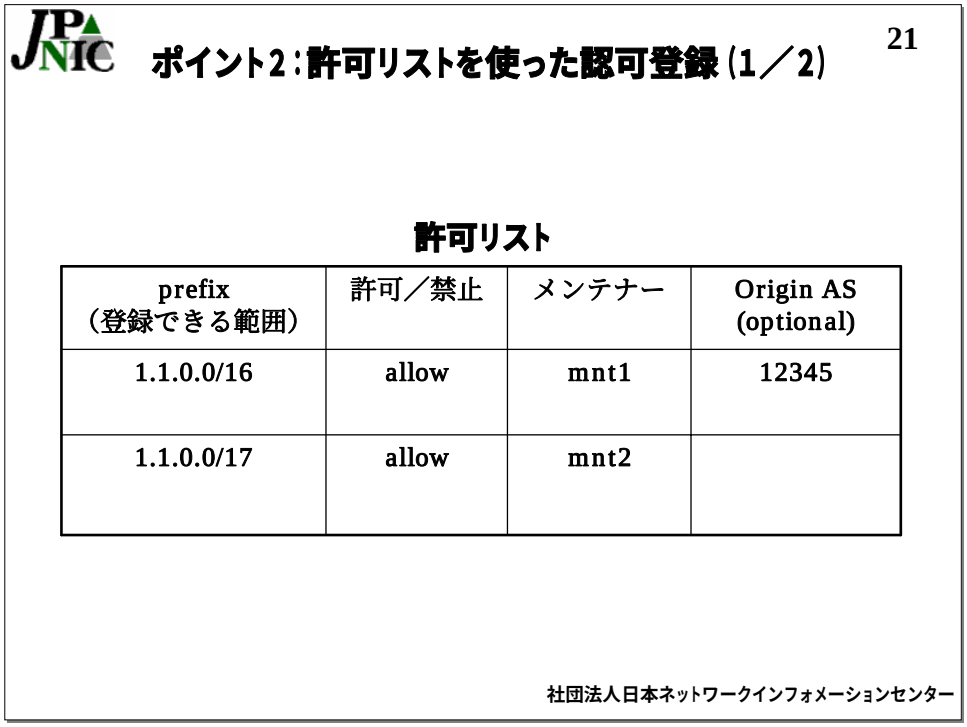


図 4-4　許可リスト

図 4-1 は本機構が持つ「許可リスト」データベースを、LIR が表示させた際の表である。1 行 1 エントリーで許可ないし禁止が示される。prefix の列には LIR が割り振られた IP アドレスの範囲が記載されており、メンテナーの列で指定されたメンテナーに対して、route オブジェクトの登録を許可（allow）ないし禁止（deny）している。Origin AS の列では route オブジェクトに記載される Origin AS を指定することができ、指定されている場合にはその他の AS 番号を記載することはできない。Origin AS が指定されていない場合には、どの AS 番号を記載した route オブジェクトを登録してもよい。

1.1.0.0/16 の行は、mnt1 というメンテナーに対して Origin AS が 12345 と記載された route オブジェクトの登録が許可されている。1.1.0.0/17 の行は、mnt2 に対して任意の Origin AS を含む route オブジェクトの登録が許可されている。1.1.0.0/17 は 1.1.0.0/16 に含まれる prefix であり、総合すると 1.1.0.0/16 全体は mnt1 に、そのうちの半分である 1.1.0.0/17 は mnt2 に認可されていることになる。

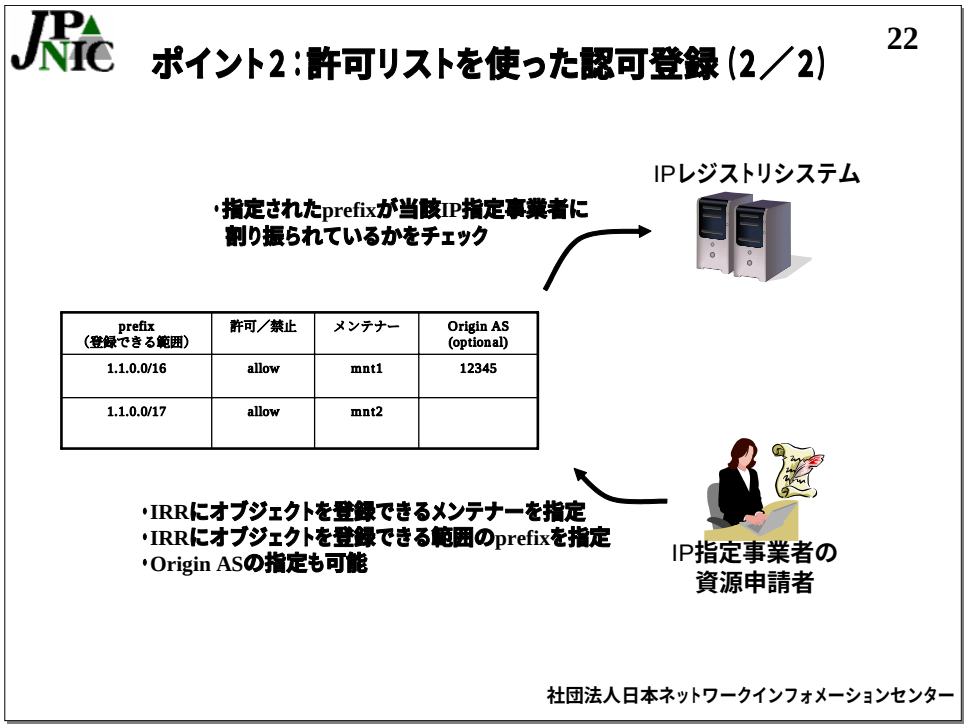


図 4-5　許可リストへの登録

許可リストは JPNIC から IP アドレスの割り振りを受けた LIR（IP 指定事業者）が編集する。許可リストに prefix を登録する際に、本機構は IP レジストリシステムへの問い合わせを行い、その IP 指定事業者に割り振られている prefix であるかどうかのチェックを行う。この段階で、LIR による認可の範囲が、その LIR が管理する prefix の範囲であることが確認される。

許可リストへの登録は、IP 指定事業者以外でも可能だが、認証手続きとデータエントリーの簡素化のため、今の段階ではその処理を JPNIC が代理で行うものとした。日本国内の ISP の中には JPNIC 以外のインターネットレジストリから IP アドレスの割り振りを受けている事業者があるため、この手続きの簡素化は大きな課題である。

○ポイント３：許可のチェック

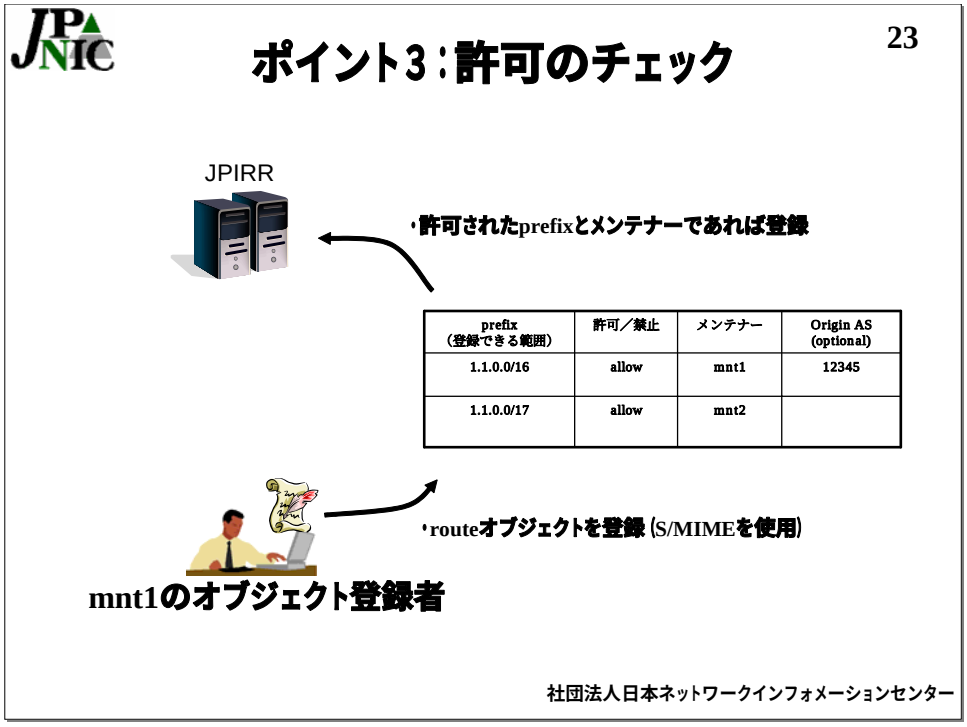


図 4-6　許可のチェック

許可リストで許可されたメンテナーオブジェクト登録者は、route オブジェクトの登録ができる。1.1.0.0/16 の route オブジェクトの登録が許可されている mnt1 のオブジェクト登録者は、S/MIME（Secure Multipurpose Internet Mail Extensions）を使って登録申請のメールに電子署名をつけ JPIRR の登録受付用メールアドレスに送信する。本機構は登録申請を受け付け、route オブジェクトに記載された prefix と AS 番号が許可リストに登録されたものの範囲内であることを確認する。問題がなければ JPIRR に登録する。

オブジェクト登録者にとっては、これまでの CRYPT-PW、PGP-KEY に加えて X.509 形式の電子証明書を用いた認証方式が新たに使えるようになった状況であり、登録自体は特に既存の業務と大きな差はない。しかし許可されていない prefix は登録できないため、IP 指定事業者の許可リストの編集を行うものと連絡を取って必要かつ正当な route オブジェクトを登録できるよう業務を行う必要がある。

以上の手続きによって、図 4-7 に示すような効果が得られる。

図 4-7　経路情報の登録機構によって得られる効果

経路情報の登録機構によって得られる効果は、３つのポイントから得られる。まず本機構が使われていながらも間違った登録が見つかった場合、ユーザ認証で間違いがあったのか（ポイント１）、意図どおりに認可されていなかったのか（ポイント２）、意図どおりの割り振り／割り当てに則って登録されていたのか（ポイント３）という整理ができる。

IRR の登録情報の正しさを確認する既存の方法には、インターネットで広告されている経路情報の prefix との比較があったが、これでは不正に IP アドレスや AS 番号を利用し、更に IRR に登録してしまっていた場合には検知する方法はなかった。

しかし経路情報の登録機構を利用することで、インターネットレジストリが持つ情報を活用し、ルーティングにおける安全性向上に役立つ登録情報を維持する仕組みを実現できる。

4.2.2. 利用者の観点

本節では経路情報の登録機構の利用開始にあたり、IP 指定事業者と JPIRR に情報登録を行うものがどのような手続きを踏むのかをまとめる。

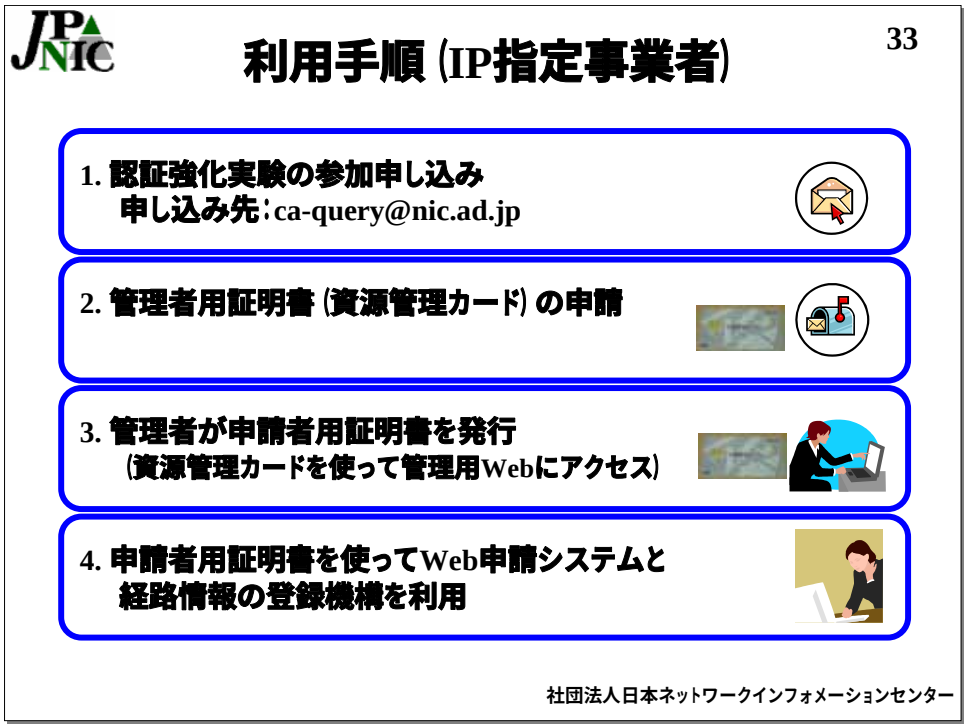


図 4-8　IP 指定事業者の利用手順

図 4-8 は IP 指定事業者の利用手順を示したものである。まず IP 指定事業者は、IP アドレスの割り振り申請／割り当て報告等の業務を行うための電子証明書を申請する（１）。申請によって発行される電子証明書は「資源管理カード」と呼ばれる IC カードに格納されており、この IC カードを使うことで各種申請を行うための申請者用証明書の管理を行うことができる。資源管理カードを使って発行した申請者用証明書は、IP アドレスの申請だけでなく、許可リストの編集に利用できる。申請者用証明書を使って、割り振られた IP アドレスを許可リストに登録する業務を行う。

図 4-9　JPIRR の情報登録者の利用手順

図 4-9 は JPIRR の情報登録者の利用手順を示したものである。JPIRR に情報登録を行うものは初めにメンテナーオブジェクト（Maintainer オブジェクト）の登録を申請する。本機構を使うためには、メンテナーオブジェクトの策定と同時または事後に認証トークン（USB トークン）の発行の申請を行う。この認証トークンには証明書管理者の証明書が入る。認証トークンを使うと、本機構のオブジェクト登録者の証明書を管理する画面にアクセスすることができ、ユーザ数に応じて証明書を発行することができる。オブジェクト登録者の証明書を受け取ったものは、S/MIME を使って JPIRR への情報登録を行うことができる。

4.3. 経路情報の登録機構の仕組みと構成

経路情報の登録機構は「利用者(証明書)の管理」「許可リストの編集」「オブジェクト登録者の S/MIME を使った認証といった複数の機能を提供する。

本機構のシステム構成を図 4-10 に示す。

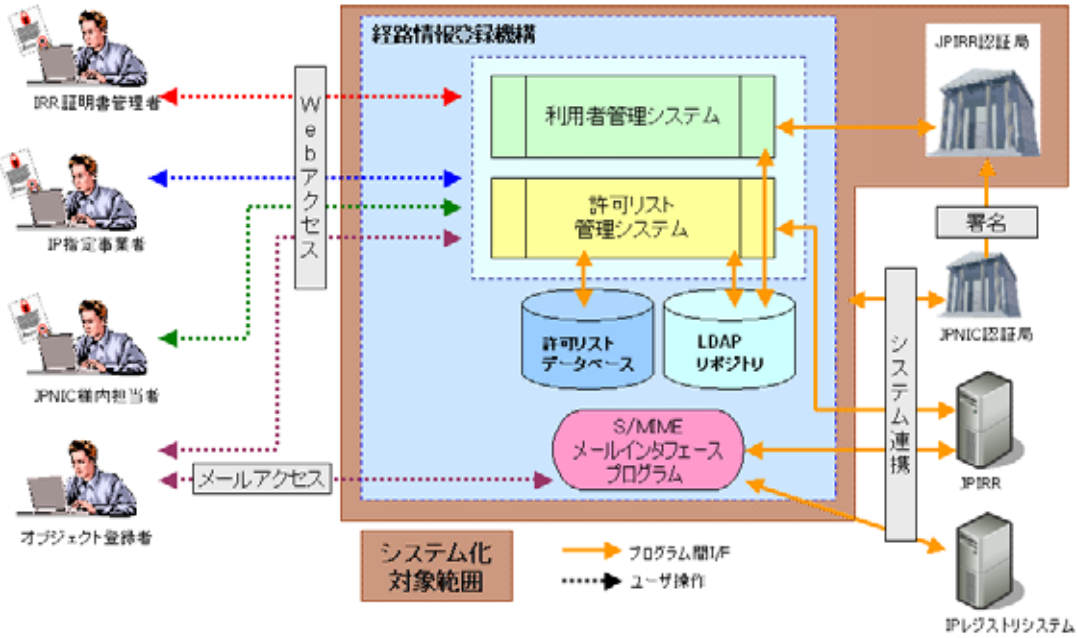


図 4-10　経路情報の登録機構のシステム構成

各担当者は、本システムを使用して、主に３つの業務を処理する。（１）利用者管理システムを使用した利用者管理業務、(２)許可リスト管理システムを使用した許可リスト管理業務、（３）S/MIME メールインターフェースプログラムを使用したオブジェクト管理業務の処理を行う。

本機構では、JPNIC Primary Root CA により署名された JPIRR 認証局を構築し、本機構を利用するための JPIRR クライアント証明書を発行する。

4.4. ネットワーク構成

本機構は安全上、性質が異なる複数の機能を提供している。提供する機能への不正アクセスを受けた時の影響を想定し、サーバの論理的・物理的な配置を工夫した。

○サーバの役割に応じた論理的な配置

Web インターフェースを提供するサーバは、通信元が特定のホストに限定されないようなユーザにアクセスされる。従って不正アクセスが起こったときにアプリケーション機能への影響が最小限に留まるよう、DMZ に配置し、更に提供する機能を最小限に留めた。

アプリケーション機能を提供するサーバは、限定されたホストからの接続のみを受け付けるよう、内部のセグメントに配置し、また重要なサーバとの通信には認証なしには接続が確立しないような制限を設けた。サーバ管理の為の接続元にも制限を設け、インターネットからの攻撃に対して直接的な影響を受けないようにした。

○通信機器におけるアクセス制御機能

すべての機器は必要以上の通信を行うことができないように、ネットワーク機器でアクセス制御を実施した。不正アクセス時の IP レジストリシステムや IP アドレス認証局（認証）との影響を最小限に抑えつつ、管理負荷を抑えられる構成とした。

○リスクの度合いに応じた物理的な配置

認証局機能を提供するサーバの一部は地理的に別の地点に配置し、アプリケーション機能を持つサーバが物理的に攻撃にさらされた場合に隔離し、影響を受けないような対策が取れるようにした。この場合、アプリケーション機能が攻撃にさらされる危険性があるが、データおよびサービスを復旧させるための負荷と障害時の信頼度への影響を考慮し、認証局機能の鍵の保護を安全上の優先事項とした。

4.5. JPIRR 認証局設計

4.5.1. 認証局と信頼階層

各種サービスで利用される認証局とその信頼階層を図 4-11 に示す。

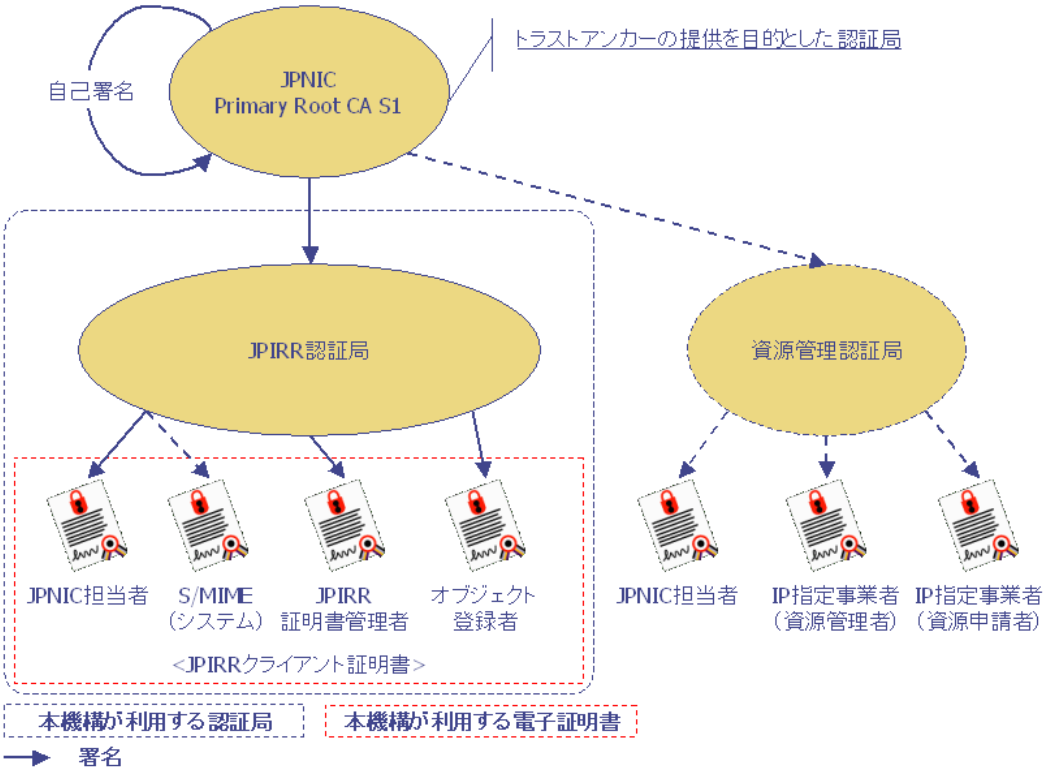


図 4-11　JPNIC 認証局の階層構造

JPIRR 認証局は、上位の認証局（ルート認証局）である「JPNIC Primary Root CA S1」により署名される。

4.5.2. JPIRR 認証局の論理構成

JPIRR 認証局の論理構成を図 4-12 に示す。

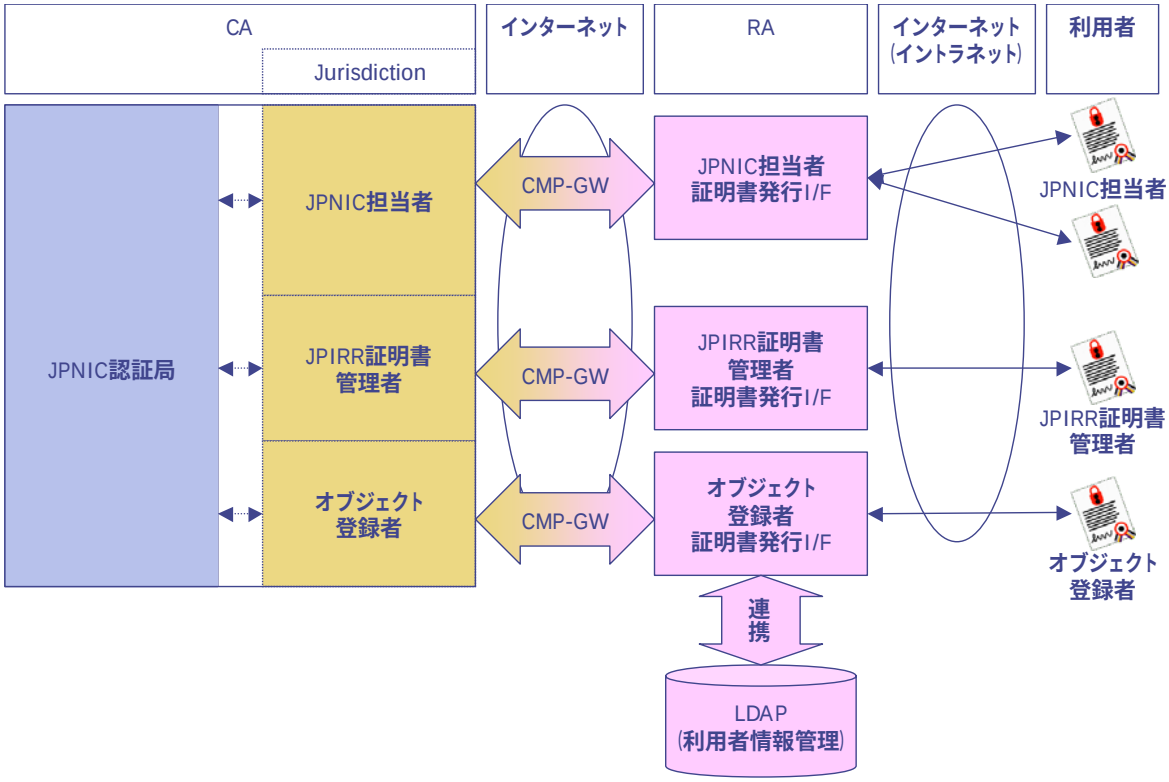


図 4-12　JPIRR 認証局の論理構成

4.5.2.1. CA／Jurisdiction

CA は、JPNIC 認証局のポリシー（プロファイル）を管理する。主に次の役割を行う。

- 認証局のプロファイル管理（認証局証明書の発行）
- JPIRR 認証局から発行される利用者証明書（JPIRR クライアント証明書）への署名付与
- CRL（失効リスト）の発行および CRL への署名付与

また CA の中に設定される Jurisdiction は、RA 側の利用者向け発行インターフェース（以下、「証明書発行 I/F」という）と対応し、JPIRR 認証局から発行される利用者証明書のプロファイルを管理する。

4.5.2.2. 証明書発行 I/F

証明書発行 I/F は、JPNIC 内の RA システムの一部として、利用者からの証明書発行要求を受け付け、利用者認証を行った後、CA に対して証明書の発行リクエストを行う。証明書発行 I/F における利用者からの JPIRR クライアント証明書受付けから証明書発行完了までの大まかな流れは、図 4-13 の通りである。なお図 4-13 では、正常系の処理のみを記載する。

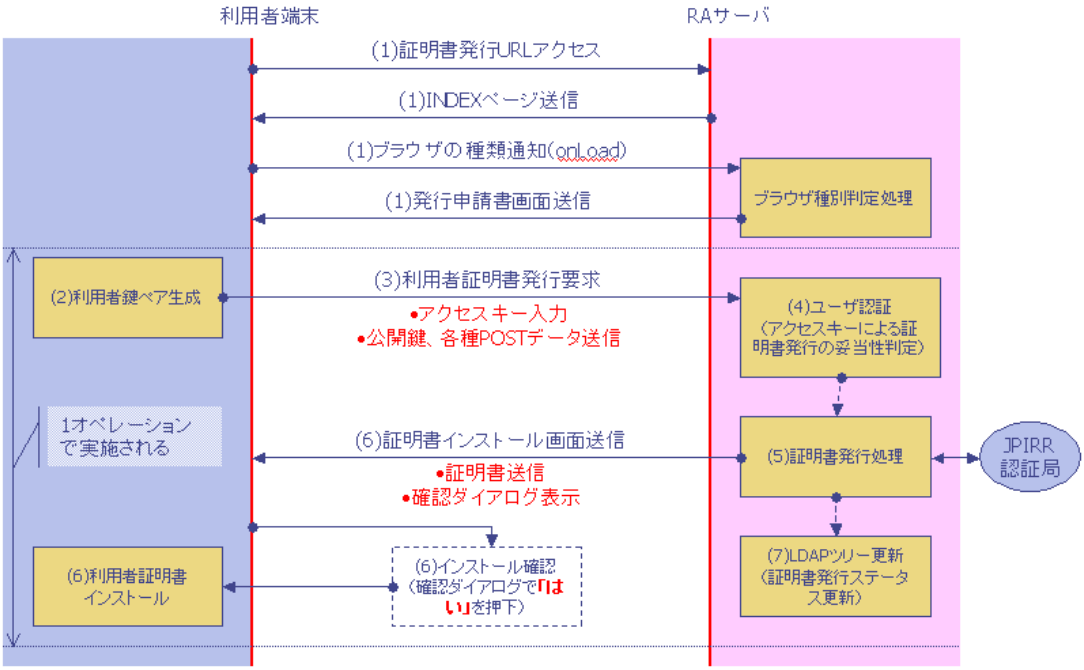


図 4-13　証明書発行 I/F 処理フロー

- 利用者のブラウザより、JPIRR クライアント証明書発行要求を受付け、利用者が利用するブラウザに応じた証明書発行 I/F 画面を表示する。
- 利用者のブラウザに対して、利用者秘密鍵・公開鍵の鍵ペア生成要求を行う。証明書発行 I/F は、生成要求をブラウザ側に要求するのみであり、証明書発行 I/F 側での利用者鍵の生成は、一切行わない。またこのとき証明書発行 I/F の設定により、クライアントにマウントされたデバイス（ハードウェアセキュリティトークン）内の鍵生成モジュールに対して、鍵生成要求を行うことも可能である。
- 利用者ブラウザ内で鍵生成が正常に行われると、クライアント（ブラウザ）より PKCS#10 形式の公開鍵情報（証明書発行リクエストデータ）を受け取る。
- 利用者が入力したライセンスキーおよび証明書発行用一時パスワードを利用者情報管理 LDAP と照合し、利用者を認証する。
- 受取った PKCS＃10 を、CMP-GW を介して CA に送信し、JPIRR クライアント証明書の発行を CA に要求し、CA より発行された JPIRR クライアント証明書を受け

取る。

- 受け取った JPIRR クライアント証明書を利用者のブラウザ内の証明書ストアに格納する。このとき証明書発行 I/F の設定により、クライアントにマウントされたデバイス（ハードウェアセキュリティトークン）に当該証明書を格納することも可能である。
- 利用者情報を管理する LDAP ツリーに対し、証明書発行ステータスを“発行済”に更新する。

4.5.2.3. CMP-GW

JPIRR 認証局と JPNIC 側に設置された RA サーバとの間の CMP[1]通信を、インターネットを経由して SSL でトンネリングするゲートウェイシステムである。これにより証明書発行 I/F と外部にある認証局サービスサイト間の CMP プロトコルによる通信をセキュアに接続する環境を提供する。

本ゲートウェイシステムは、RA サーバ側にある CMP-GW/C と外部認証局サービスサイト内にある CMP-GW/S との間で SSL コネクションを確立する。証明書発行 I/F と JPIRR 認証局は、この SSL コネクションを介して、インターネット上で HTTPS プロトコルにより CMP データを相互に送受信することが可能となる。

本ゲートウェイシステムの構成を図 4-14 に示す。

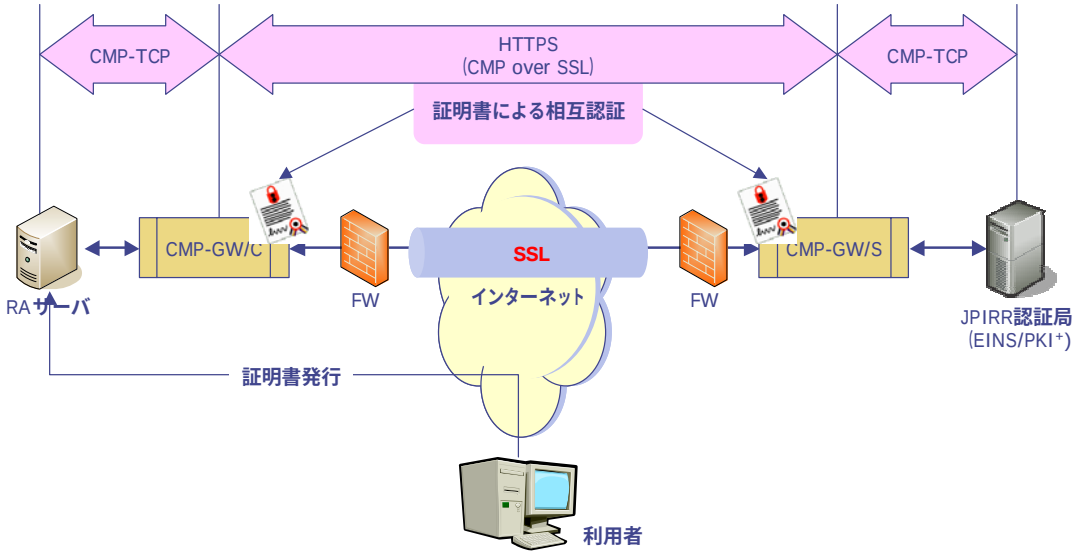


図 4-14　CMP ゲートウェイシステム（CMP-GW）

[1] RFC 4210 で定められた証明書管理に関する通信プロトコル。証明書発行、更新、失効、鍵回復などの機能が含まれる。

4.5.2.4. LDAP（利用者情報管理）

LDAP は、証明書発行 I/F と連携し、JPIRR クライアント証明書を発行するための次の機能を提供する。

- 利用者ごとの JPIRR クライアント証明書に記載される利用者固有（主に証明書の Subject 属性に記載される内容）の情報管理
- 証明書発行 I/F で証明書を発行する際の利用者認証に使用する ID、パスワード管理
- 利用者ごとの JPIRR クライアント証明書のステータス管理

4.5.3. JPIRR 認証局のプロファイル

JPIRR 認証局証明書の詳細プロファイルを次に示す。

4.5.3.1. 基本領域の詳細プロファイル

表 4-1　JPIRR 認証局 証左プロファイル（基本領域）

領域名		設定値	備考
version （バージョン番号）		v3	X.509 証明書 バージョン 3 を示す。
serialNumber （シリアル番号）			CA システムにより自動生成
signature （署名アルゴリズム）		SHA1withRSA	
issuer （発行者）			JPNIC Primary Root CA の Subject と同値
	C	JP	
	O	Japan Network Information Center	
	OU	Internet Resource Service	
	OU	JPNIC Resource Service Certification Authority	
validity （有効期間）			10 年間
notBefore （開始日）		YYYYMMDDHHMMSS	

領域名		設定値	備考
notAfter（終了日）		YYYYMMDDHHMMSS	
subject（主体者）			
	C	JP	
	O	Japan Network Information Center	
	OU	JPIRR Certification Authority 01	
subjectPublicKeyInfo（主体者公開鍵情報）			
algorithm（アルゴリズム識別子）		1.2.840.113549.1.1.1	RSA 2048bit
subjectPublicKey（主体者公開鍵）			CAシステムにより自動生成

4.5.3.2. 拡張領域の詳細プロファイル

表 4-2　JPIRR 認証局 詳細プロファイル（拡張領域）

領域名	critical flag	設定値	備考
authorityKeyIdentifier（認証局鍵識別子）	Non		JPNIC Primary Root CA 証明書の公開鍵のハッシュ値
subjectKeyIdentifier（主体者鍵識別子）	Non		JPIRR 認証局証明書の公開鍵のハッシュ値
keyUsage（鍵使用法）	Critical	keyCertSign（証明書の署名検証） cRLSign（失効リスト<CRL>の署名検証）	
basicConstraints（基本制約）	Non		
Subject Type		CA	

領域名		critical flag	設定値	備考
	Path Length Constraints		01	

4.5.4. CRL（失効リスト）

JPIRR 認証局より発行される CRL は、まず認証局サービスサイト内の共用リポジトリに定期的にアップロードされる。その後、HTTP により JPNIC 内のリポジトリサーバが定期的に CRL の取り込みを行う。

利用者は、JPNIC 内のプロキシサーバより当該 CRL にアクセスする。

CRL の発行ならびに利用者からのアクセスについて図 4-15 に示す。

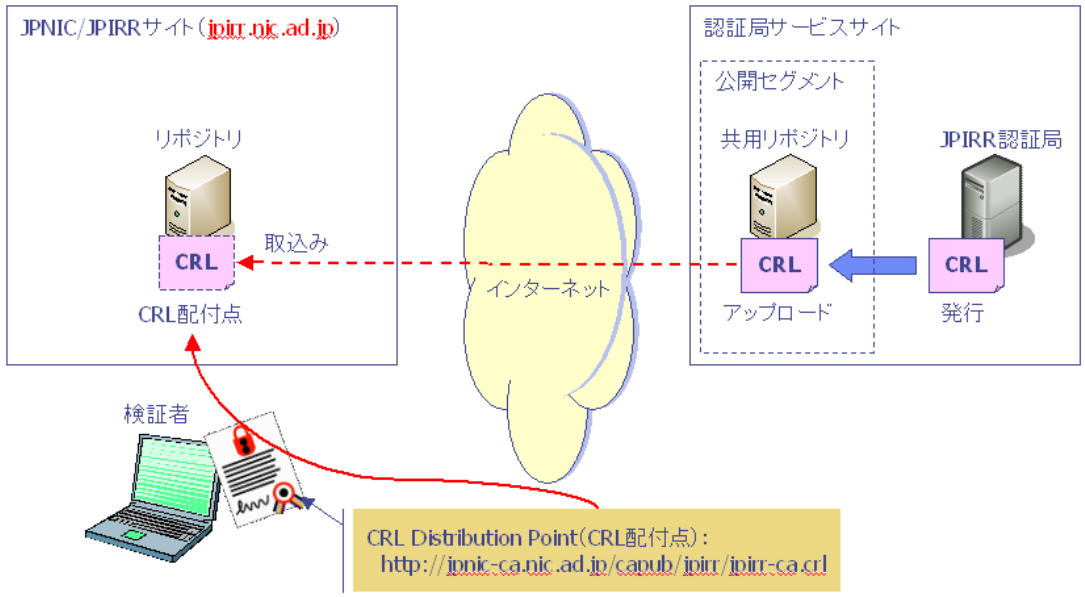


図 4-15　JPIRR 認証局 CRL 詳細プロファイル

4.5.4.1. CRL のプロファイル

JPIRR 認証局より発行される CRL のプロファイルを表 4-3 に示す。

表 4-3　JPIRR 認証局 CRL 詳細プロファイル

領域名		設定値	備考
version （バージョン番号）		v2	バージョン 2 を示す。
signature （署名アルゴリズム）		SHA1withRSA	
subject （主体者）			
	C	JP	
	O	Japan Network Information Center	
	OU	JPIRR Certification Authority 01	
thisUpdate （今回の更新日時）		YYYYMMDDHHMMSS	CRL が発行されたシステム時刻
nextUpdate （次回の更新日時）		YYYYMMDDHHMMSS	thisUpdate より 15 日後の日時
revokedCertificates（失効された JPIRR 証明書のリスト）			
userCertificate （失効した利用者証明書）			失効した証明書のシリアル番号
revocationDate （失効日時）		YYYYMMDDHHMMSS	失効処理が実施された日時

crlExtensions（CRL 拡張領域）			
領域名	critical flag	設定値	備考
authorityKeyIdentifier （認証局鍵識別子）	Non		JPIRR 認証局証明書の公開鍵のハッシュ値
cRLNumber	Non		CA システムにより自動生成

4.5.4.2. CRL の発行周期

CRL は、完全 CRL のみをサポートし、JPIRR 認証局より 24 時間おきに発行する。

なお本機構内に設置され、利用者の SSL クライアント認証を行う Web サーバでは、7 日ごとに完全 CRL を取り込む。

このため CRL 中に記載される thisUpdate（今回更新日時）と nextUpdate（次回更新日時）の間隔は、15 日間を設定する。CRL の有効期間を 15 日間とすることで、7 日周期での CRL の取り込みでも有効期限切れになることなく、JPIRR クライアント証明書の有効性検証が可能となる。

CRL の発行周期、CRL 中に記載される有効期間（thisUpdate と nextUpdate の間隔）、および Web サーバでの CRL の取り込み周期の関係を図 4-16 に示す。

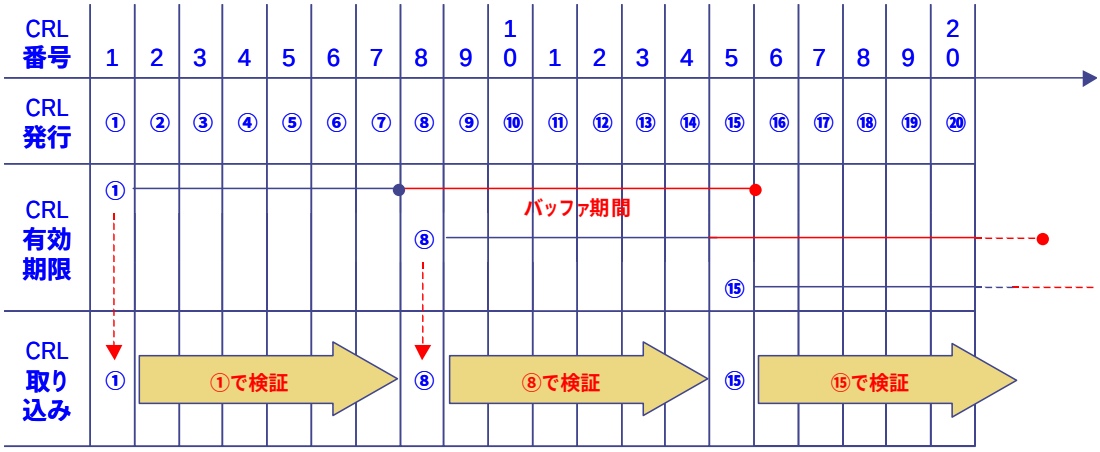


図 4-16　CRL の発行周期、有効期限と Web サーバでの取り込み

4.5.5. JPIRR クライアント証明書

JPIRR 認証局が発行する JPIRR クライアント証明書は、

- JPNIC 担当者
- JPIRR 証明書管理者
- オブジェクト登録者

に対して発行し、付与される。

また本機構の S/MIME メール I/F で使用する S/MIME 署名・暗号化のための証明書も JPIRR 認証局より発行する。本証明書は、JPNIC 担当者により発行される。

JPIRR クライアント証明書を付与される利用者の種類と役割を表 4-4 に示す。

表 4-4　利用者の種類と役割

利用者	役割	鍵・証明書格納媒体
JPNIC 担当者	JPIRR 認証局を管理･運営し、本機構に係る、次の業務を行う。 • JPIRR 証明書管理者のアカウント登録および JPIRR クライアント証明書の付与 • JPIRR 証明書管理者の JPIRR クライアント証明書の失効 • 本機構における許可リスト・メンテナー全体の管理	FIPS140-1 レベル 3 を満たしたセキュリティモジュールを実装するハードウェアトークン（IC カード、USB トークン）
JPIRR 証明書管理者	次の役割を持つ。 • オブジェクト登録者のアカウントの登録、および JPIRR クライアント証明書の付与 • 管理下のオブジェクト登録者の JPIRR クライアント証明書の失効 • メンテナーの申請、管理	FIPS140-1 レベル 3 を満たしたセキュリティモジュールを実装するハードウェアトークン（IC カード、USB トークン）
オブジェクト登録者	JPIRR へのオブジェクトの登録申請を行う。 • 自身に付与された JPIRR クライアント証明書の発行 • 許可リストの参照 • S/MIME による JPIRR へのオブジェクトの登録・変更・削除	特に定めない

4.5.5.1. JPIRR クライアント証明書のプロファイル

JPIRR 認証局証明書の詳細プロファイルを表 4-5 に示す。

（1） 基本領域の詳細プロファイル

表 4-5　JPIRR クライアント証明書 詳細プロファイル（基本領域）

領域名		設定値	備考
version （バージョン番号）		v3	X.509 証明書 バージョン 3 を示す。
serialNumber （シリアル番号）			CA システムにより自動生成
signature （署名アルゴリズム）		SHA1withRSA	
issuer （発行者）			JPNIC Primary Root CA の Subject と同値
	C	JP	
	O	Japan Network Information Center	
	OU	JPIRR Certification Authority 01	
Validity （有効期間）			2 年 ＋ 30 日
notBefore （開始日）		YYYYMMDDHHMMSS	
notAfter （終了日）		YYYYMMDDHHMMSS	
subject （主体者）		【別表に記載する】	
subjectPublicKeyInfo （主体者公開鍵情報）			
algorithm （アルゴリズム識別子）		1.2.840.113549.1.1.1	RSA 1024bit
subjectPublicKey （主体者公開鍵）			CA システムにより自動生成

JPIRR クライアント証明書を付与される利用者ごとの subject（主体者）属性に設定される値について、表 4-6 に示す。

表 4-6　JPIRR クライアント証明書の利用者ごとの主体者情報

<table>
<tr><th rowspan="2">DN</th><th colspan="4">利用者</th></tr>
<tr><th colspan="2">JPNIC 担当者</th><th>JPIRR 証明書管理者</th><th>オブジェクト登録者</th></tr>
<tr><th></th><th>S/MIME I/F</th><th></th><th></th></tr>
<tr><td>C</td><td colspan="4">“ JP ”</td></tr>
<tr><td>O</td><td colspan="2">“ Japan Network Information Center ”</td><td colspan="2">“ Resource Holder ”</td></tr>
<tr><td>O</td><td colspan="2"></td><td colspan="2">“ ASN Holder ”</td></tr>
<tr><td>OU</td><td colspan="2">“ Internet Resource Service ”</td><td>“ IRR Maintainer Administrator ”</td><td>“ IRR Object Registrant ”</td></tr>
<tr><td>OU</td><td>“ Secretariat ”</td><td></td><td>（付与された利用者の管理対象のメンテナー名）</td><td>（付与された利用者の管理対象のメンテナー名）</td></tr>
<tr><td>OU</td><td>“ IRR Administrator ”</td><td></td><td></td><td></td></tr>
<tr><td>CN</td><td>以下の各項目を半角スペースで区切り、併記。
① “ IRR-AD ”
② [64 文字以内の任意の名称]
③ シーケンス番号･･･①および②の組合せで同一の利用者内で、証明書発行回数のシーケンス。新規発行時は“ 01 ”。</td><td>以下の各項目を半角スペースで区切り、併記。
⑤ “ Secure MIME Gateway ”
⑥ シーケンス番号･･･同一の利用者で、証明書発行回数のシーケンス。新規発行時は“ 01 ”。</td><td>以下の各項目を半角スペースで区切り、併記。
⑦ IRR-MA ”
⑧ メンテナーオブジェクトの admin-c 項目
⑨ シーケンス番号･･･④および⑤の組合せ（同一の利用者）で、証明書発行回数のシーケンス。新規発行時は“ 01 ”。</td><td>以下の各項目を半角スペースで区切り、併記。
⑩ “ IRR-OR ”
⑪ メンテナーオブジェクトの tech-c 項目
⑫ シーケンス番号･･･⑦及び⑧の組合せ（同一の利用者）で、証明書発行回数のシーケンス。新規発行時は“ 01 ”。</td></tr>
</table>

利用者は、subject（主体者）属性に設定された DN のうち、CN により一意に識別される。また CN 内にシーケンス番号を付加することで、利用者ごとに発行した JPIRR クライアント証明書を一意に特定できる。なお実際に使用する利用者が同一の利用者であっても、JPIRR クライアント証明書に記載された CN 情報のうちシーケンス番号を除く項目に変更があった場合、シーケンス番号は“ 01 ”が設定される（新規発行と同様の扱いとなる）。

（2） 拡張領域の詳細プロファイル

表 4-7　JPIRR クライアント証明書 詳細プロファイル（拡張領域）

領域名	critical flag	設定値	備考
authorityKeyIdentifier （認証局鍵識別子）	Non		JPIRR 認証局証明書の公開鍵のハッシュ値
subjectKeyIdentifier （主体者鍵識別子）	Non		本 JPIRR クライアント証明書の公開鍵のハッシュ値
keyUsage （鍵使用法）	Critical	digitalSignature（デジタル署名の検証） keyEnciperment（鍵の暗号化）	
extendedKeyUsage （拡張鍵使用法）	Non	1.3.6.1.5.5.7.3.2 ： SSL／TLS クライアント認証 1.3.6.1.5.5.7.3.4 ： 電子メールの保護	
certificatePolicies （証明書ポリシー）	Non	[1]Certificate Policy: Policy Identifier=1.2.392.200175.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://jpnic-ca.nic.ad.jp/capub/jpirr/jpirr-ca_cps.html	
subjectAltName （主体者別名）	Non	[rfc822name]	利用者の電子メールアドレス
basicConstraints （基本制約）	Non		
Subject Type		End Entity	
Path Length Constraints		None	
cRLDistributionPoints （CRL 配付点）	Non	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://jpnic-ca.nic.ad.jp/capub/jpirr/jpirr-ca.crl	

領域名		critical flag	設定値	備考
basicConstraints（基本制約）		Non		
	Subject Type		CA	
	Path Length Constraints		01	

4.5.6. JPIRR 認証局のライフサイクル

JPIRR 認証局と JPNIC Primary Root CA ならびに JPIRR クライアント証明書のライフサイクルの関係について述べる。

4.5.6.1. JPIRR 認証局のライフサイクルの基本的な考え方

JPIRR クライアント証明書の有効期間は、これを発行する JPIRR 認証局の認証局証明書の有効期限を越えることができない。従って、エンドエンティティに発行する JPIRR クライアント証明書の有効期間を保証するためには、JPIRR 認証局証明書の有効期間をオーバーラップさせる必要が生じる。

JPIRR 認証局に関係する各証明書の有効期限は、表 4-8 の通りである。

表 4-8　JPIRR 関連証明書の有効期限

証明書種別		有効期間	発行者
JPIRR 認証局証明書		10 年	JPNIC Primary Root CA
JPIRR クライアント証明書			
	JPNIC 担当者	2 年+30 日	JPIRR 認証局
	JPIRR 証明書管理者	2 年+30 日	JPIRR 認証局
	オブジェクト登録者	2 年+30 日	JPIRR 認証局
JPNIC Primary Root CA[2]		20 年+25 日	自己署名

2 年 1 ヶ月の有効期間を持つ JPIRR クライアント証明書を発行するためには、少なくとも 2 年 1 ヶ月を超えるオーバーラップ期間が必要となる。

このためキーセレモニーに要する準備期間等を考慮し、オーバーラップ期間を 2 年 2

[2] JPNIC Primary Root CA の 2006 年 10 月現在で有効な証明書の有効期間　：　2005/8/24 ～　2025/9/18

ヶ月（26 ヶ月）と定める。

4.5.6.2. JPIRR 認証局のライフサイクル

JPNIC 認証局および本認証局より発行される JPIRR クライアント証明書のタイムチャートを図 4-17 に示す。

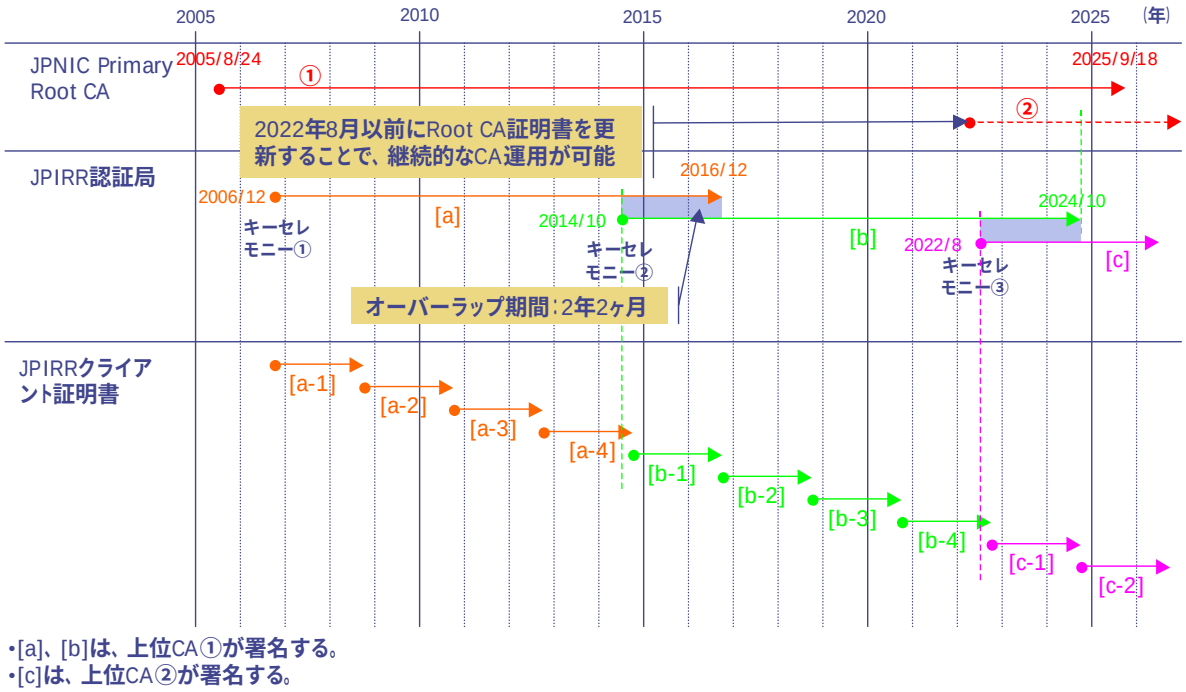


図 4-17　JPIRR 認証局の更新周期（ライフサイクル）

オーバーラップ期間が 2 年 2 ヶ月（26 ヶ月）のため、JPIRR 認証局証明書の更新は、7 年 10 ヶ月（94 ヶ月）周期で実施される。JPIRR 認証局証明書の更新にあたっては、認証局鍵ペアの更新も行うため、94 ヶ月ごとにキーセレモニーも実施される。

また JPIRR 認証局の上位認証局である JPNIC Primary Root CA の有効期間は、20 年であり、本 CA が JPIRR 認証局の発行者となることから、2022 年 8 月に実施予定のキーセレモニーに先立ち、JPNIC Primary Root CA の認証局証明書を更新しなくてはならない。

4.5.6.3. キーセレモニー

JPIRR 認証局の構築および認証局証明書更新時は、本認証局の鍵ペアを生成する。JPIRR 認証局の秘密鍵が生成され、本認証局の公開鍵へ JPNIC Primary Root CA より署名されて、JPIRR 認証局にインストールされるまでの一連の手続が適切に行われていることを確認するためにキーセレモニーを実施する。

キーセレモニーの実施者・確認者は、外部サービス要員から選任される。また承認者は JPNIC により選任されたメンバーとする。

（1）　キーセレモニーの概要

JPIRR 認証局におけるキーセレモニー実施手順のおおまかな流れについて、図 4-18 に示す。

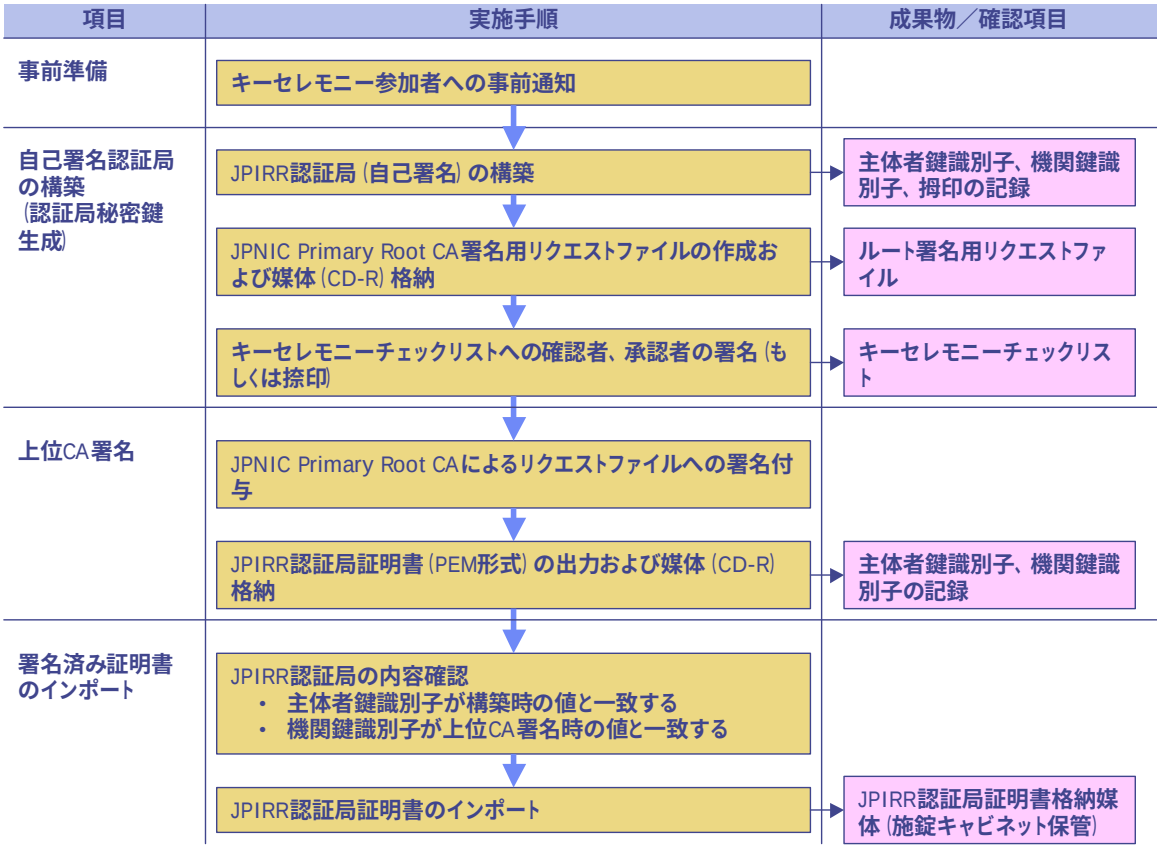


図 4-18　キーセレモニー実施手順

この手順における「自己署名認証局の構築」は、承認者ならびに確認者の立会いの下で実施される。また、「自己署名認証局の構築」および「署名済み証明書のインポート」については、常に複数の認証局サービス要員の関与（相互牽制）の下で実施する。

4.6. リポジトリ設計

本機構のディレクトサーバにおける LDAP ツリー構成を図 4-19 に示す。

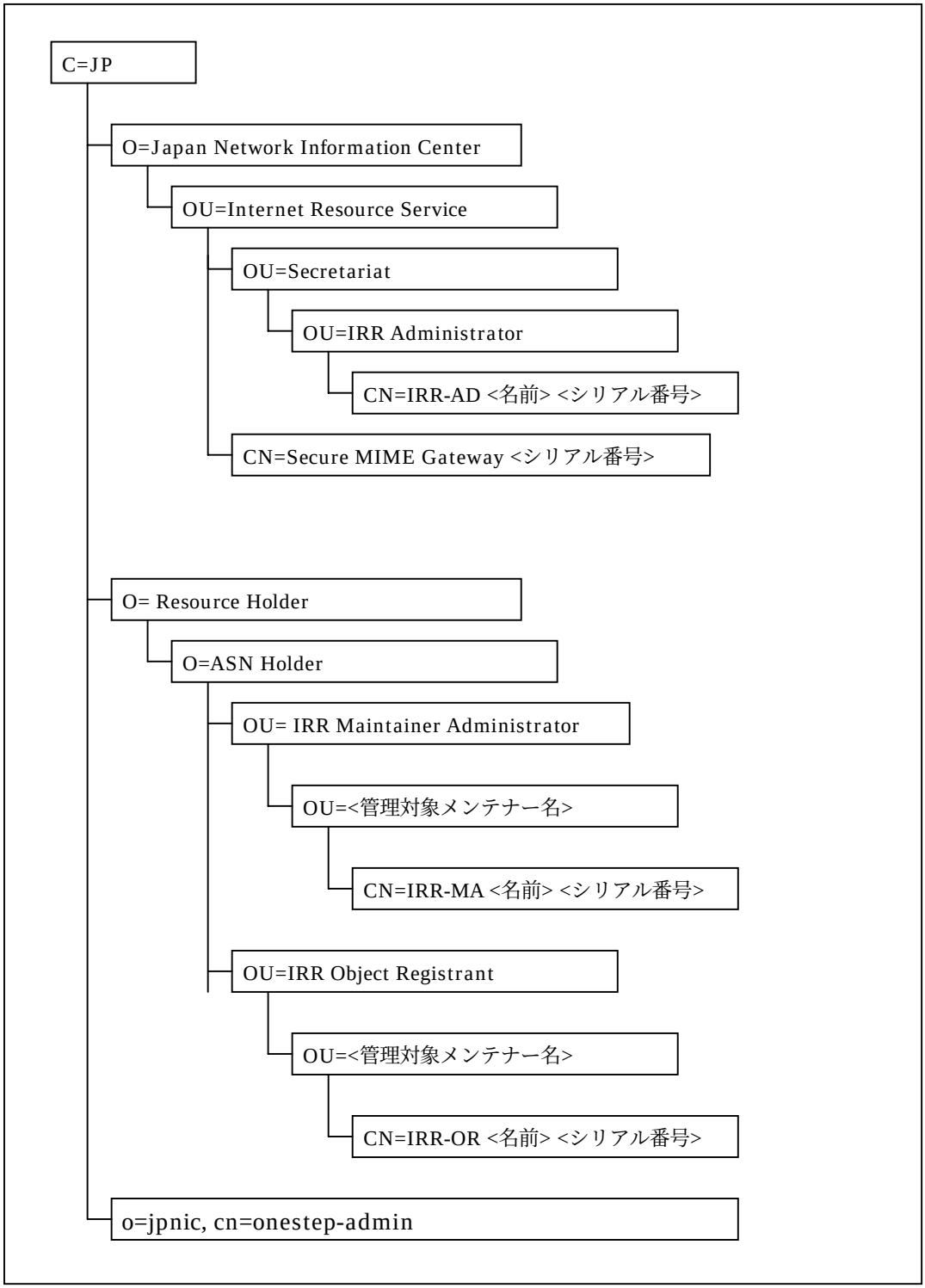


図 4-19　リポジトリ構成

4.6.1. オブジェクトクラス定義

4.6.1.1. 標準オブジェクトクラス

本機構で使用するオブジェクトクラスのうち、LDAP の標準スキーマに定義されているオブジェクトクラスを表 4-9 に示す。

表 4-9　標準オブジェクトクラス

DN	オブジェクトクラス	説明	備考
O=Japan Network Information Center C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	RFC 2256
	organization	組織オブジェクトクラス	同上
OU= Internet Resource Service O=Japan Network Information Center C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上
OU=Secretariat OU= Internet Resource Service O=Japan Network Information Center C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上
OU=JPIRR Secure MIME Gateway OU= Internet Resource Service O=Japan Network Information Center C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上
OU=IRR Administrator OU=Secretariat OU= Internet Resource Service O=Japan Network Information Center C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上

O= Resource Holder, C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization	組織オブジェクトクラス	同上
O=ASN Holder, O= Resource Holder, C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization	組織オブジェクトクラス	同上
OU= IRR Maintainer Administrator O=ASN Holder, O= Resource Holder, C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上
OU=<管理対象メンテナー名> OU= IRR Maintainer Administrator O=ASN Holder, O= Resource Holder, C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上
OU=<管理対象メンテナー名> OU=IRR Object Registrant O=ASN Holder, O= Resource Holder, C=JP	top	トップ オブジェクトクラス階層のルートとなる抽象型クラス	同上
	organization alunit	組織オブジェクトクラス	同上

4.6.1.2. ユーザ定義オブジェクトクラス

本機構で使用するオブジェクトクラスのうち、独自に定義されているユーザ定義オブジェクトクラスを表 4-10 に列挙する。

表 4-10　ユーザ定義オブジェクトクラス

オブジェクトクラス名	onestepPerson
親オブジェクトクラス	top
必須属性	cn、uid
許可された属性	mail、 userPassword、userCertificate、onestepCertIssueDate 、onestepCertExpirationTime、onestepCertSerialNo 、onestepCertStatus、onestepUpdateStatus 、onestepCmpSender、onestepCmpSecret

4.6.2. 属性定義

4.6.2.1. 標準属性

本機構で使用する属性のうち、LDAP の標準スキーマに定義されている属性を表 4-11 に示す。

表 4-11　標準属性

属性名	データ名	備考
ユーザ ID	uid	RFC 1274
コモンネーム	cn	RFC 2256
メールアドレス	mail	RFC 1274
パスワード	userPassword	RFC 2256
利用者証明書	userCertificate	RFC 2256

4.6.2.2. ユーザ定義属性

本機構で使用する属性のうち､スキーマをカスタマイズして新規に定義する属性を表 4-12 に示す。

表 4-12　ユーザ定義属性

属性名	データ名	備考
証明書発行日	onestepCertIssueDate	DirectoryString
証明書有効期限	onestepCertExpirationTime	DirectoryString
証明書シリアル番号	onestepCertSerialNo	DirectoryString
証明書発行フラグ	onestepCertStatus	DirectoryString
更新状況	OnestepUpdStatus	DirectoryString
CMPSender	onestepCmpSender	DirectoryString
SharedSecret	onestepCmpSecret	DirectoryString

4.6.2.3. 使用属性定義

本機構の各利用者の属性定義について表 4-13 に示す。なお、属性値にカンマを含めないことを前提とする。（長さについては単位をバイトとする。）

表 4-13　ユーザ使用属性

項目名	属性名	必須	桁数	説明
ユーザ ID	uid	○	15	利用者証明書発行時に使用するアクセスキーを格納
コモンネーム	cn	○	64	利用者を一意に表す名前 各利用者ごとに以下のようなフォーマットで表す IRR-AD <名前> <シリアル番号> IRR-MA <名前> <シリアル番号> IRR-OR <名前> <シリアル番号> Secure MIME Gateway <シリアル番号>
E-mail アドレス	mail	○	128	利用者のメールアドレス
パスワード	userPassword	○	128	利用者のパスワード
利用者証明書	userCertificate			利用者証明書（バイナリ）
証明書発行日	onestepCertIssueDate		14	利用者証明書の発行日（UTC） YYYYMMDDhhmmss 形式
証明書有効期限	onestepCertExpirationTime		14	発行された利用者証明書の有効期限（UTC） YYYYMMDDhhmmss 形式
証明書シリアル番号	onestepCertSerialNo		34	発行された利用者証明書のシリアル番号(16 進数表記)
証明書発行フラグ	onestepCertStatus	○	1	証明書発行状態 0：未発行　　1：発行済 8：失効済み　　9：有効期限切れ
更新状況	onestepUpdateStatus	○	1	利用者情報の更新状況 0：更新なし　　1：更新通知送信済み 2：更新登録済み
CMPSender	onestepCmpSender		16	利用者証明書失効処理時に、CA サーバと内部通信を行う際に使用される値
SharedSecret	onestepCmpSecret		16	利用者証明書失効処理時に、CA サーバと内部通信を行う際に使用される値

4.7. 業務設計

4.7.1. 利用者管理業務

本機構を使用する利用者のユーザ情報の管理と JPIRR 認証局クライアント証明書の発行・失効を行う。

利用者の情報は、本機構内の LDAP ツリーにて維持・管理される。

JPIRR 認証局クライアント証明書のプロファイルによって識別される各担当者の種類によって、その操作や対象範囲を以下のとおり制限する。

- JPNIC 担当者
  - JPNIC 担当者の利用者情報の登録、修正
  - JPIRR クライアント証明書管理者の利用者情報の参照、登録、修正
  - オブジェクト登録者の利用者情報の参照、変更
  - JPNIC 担当者の JPIRR クライアント証明書の発行・失効
  - JPIRR クライアント証明書管理者の JPIRR クライアント証明書の発行・失効
  - オブジェクト登録者の JPIRR クライアント証明書の失効
  - S/MIME メール I/F 用 JPIRR クライアント証明書の発行
- JPIRR クライアント証明書管理者
  - オブジェクト登録者の利用者情報の参照、登録、修正
  - オブジェクト登録者の JPIRR クライアント証明書の失効
- オブジェクト登録者
  - 自身の JPIRR クライアント証明書の発行

4.7.1.1. 主な管理項目

利用者情報として管理する主な項目は表 4-14 の通りである。

表 4-14　利用者情報管理項目

項目名	一覧表示	照会表示	説明
CN	○	○	発行される JPIRR クライアント証明書の CN 属性 利用者ごとに以下のようなフォーマットで表す IRR-AD <利用者名> <シリアル番号> IRR-MA <利用者名> <シリアル番号> IRR-OR <利用者名> <シリアル番号>

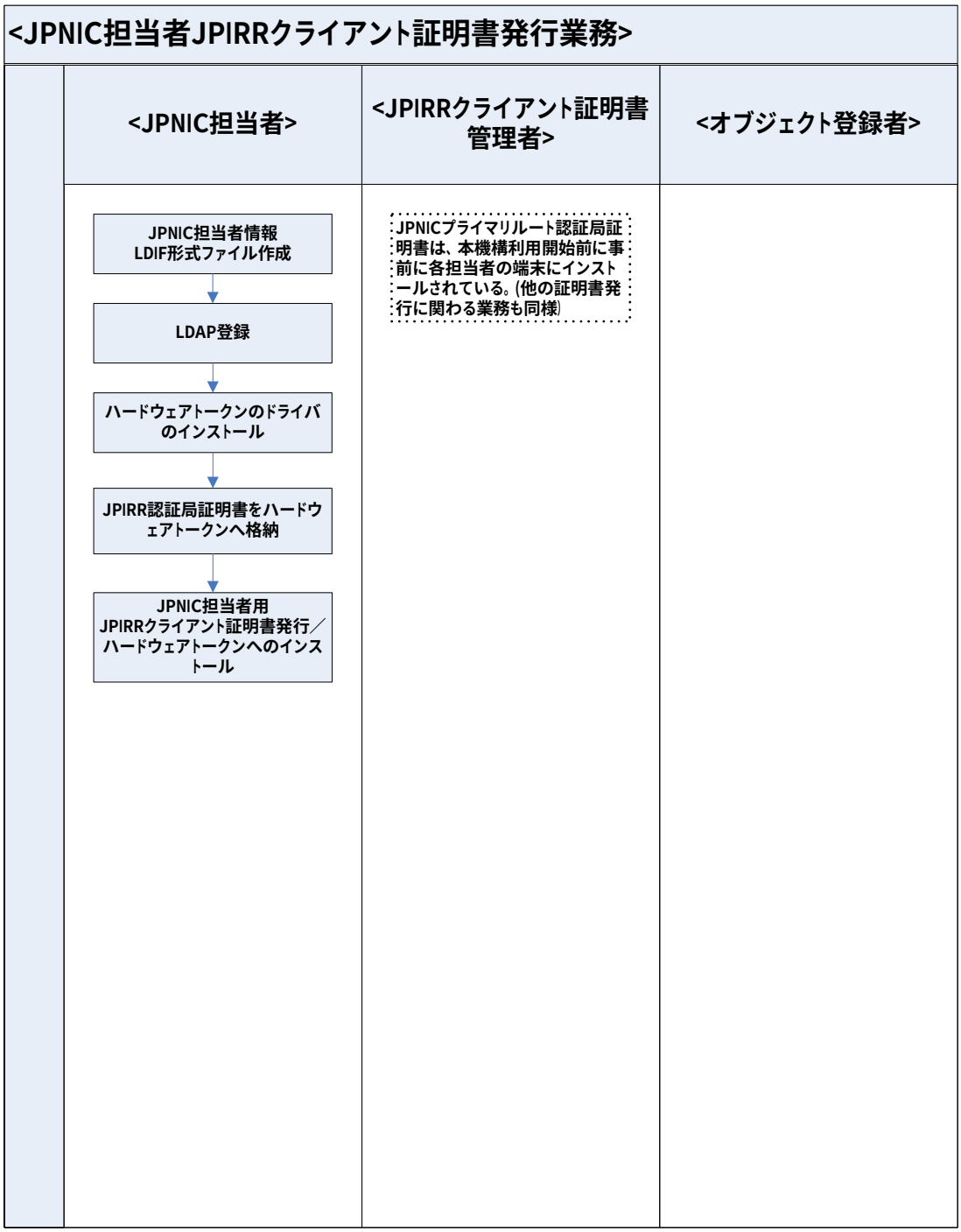
管理対象メンテナー名	○	○	管理対象のメンテナー名
アクセスキー			JPIRR クライアント証明書発行時に使用するアクセスキー
E-mail アドレス	○	○	利用者のメールアドレス
状態	○	○	証明書発行状態 ・未発行・・・まだ証明書が発行されていない ・発行済み・・証明書が発行され、証明書有効期限が満了していない ・有効期限切れ・・・証明書の有効期限が満了した ・失効済・・・証明書有効期限が満了する前に証明書が失効された
更新状況	○	○	利用者情報の更新状況 ・更新なし・・・更新通知が送信されていない ・更新通知送信済・・更新通知が送信されており、まだ更新登録されていない ・更新登録済・・・該当利用者の情報を基に更新登録されている
利用者証明書			JPIRR クライアント証明書
notBefore	○	○	JPIRR クライアント証明書の有効期限開始日時
notAfter	○	○	JPIRR クライアント証明書の有効期限終了日時
証明書シリアル番号		○	発行された JPIRR クライアント証明書のシリアル番号

凡例

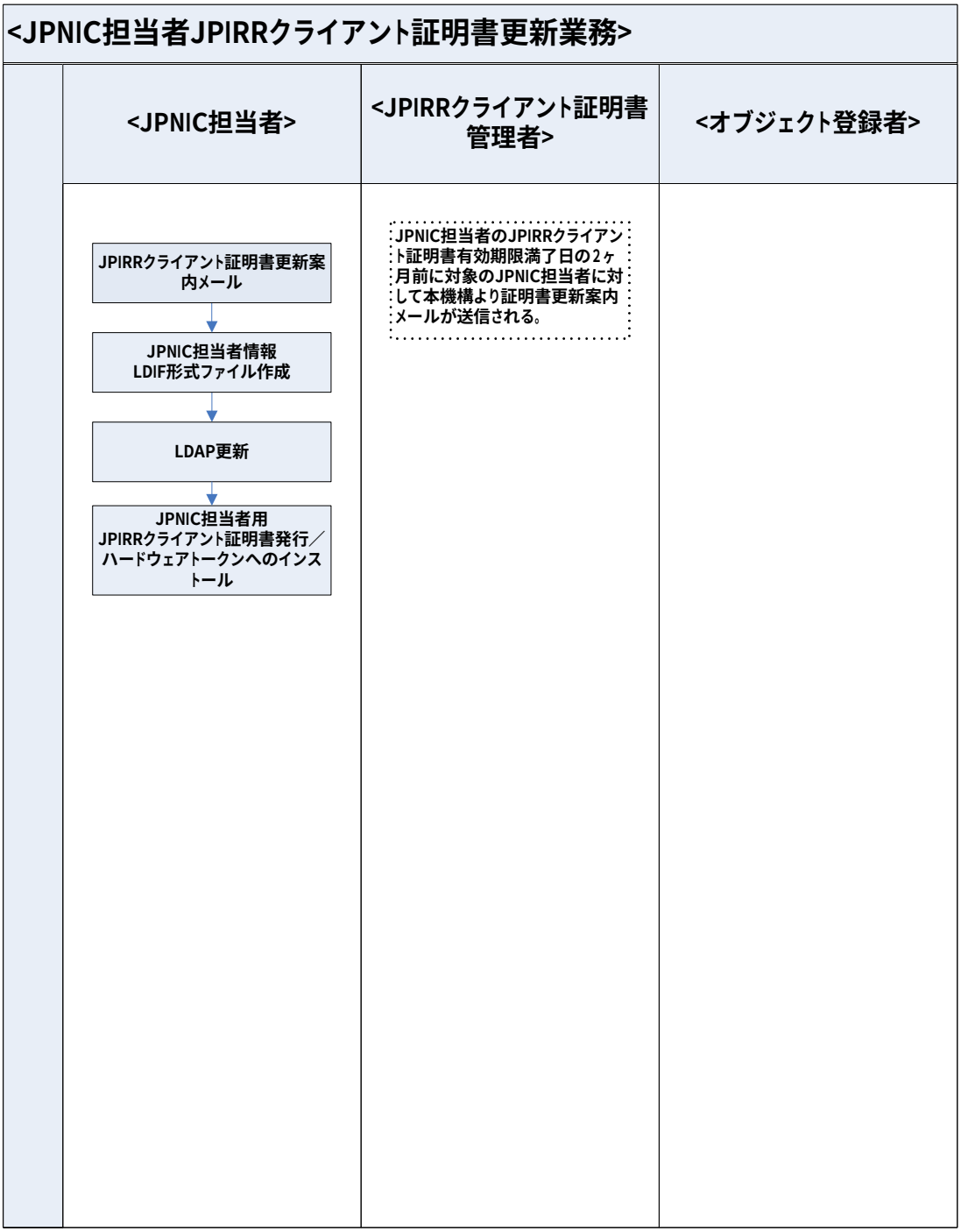
一般業務（WEB画面・アプリケーション操作・メール送受信等）

システム処理（バッチ処理など）

4.7.1.2. JPNIC 担当者 JPIRR クライアント証明書発行業務

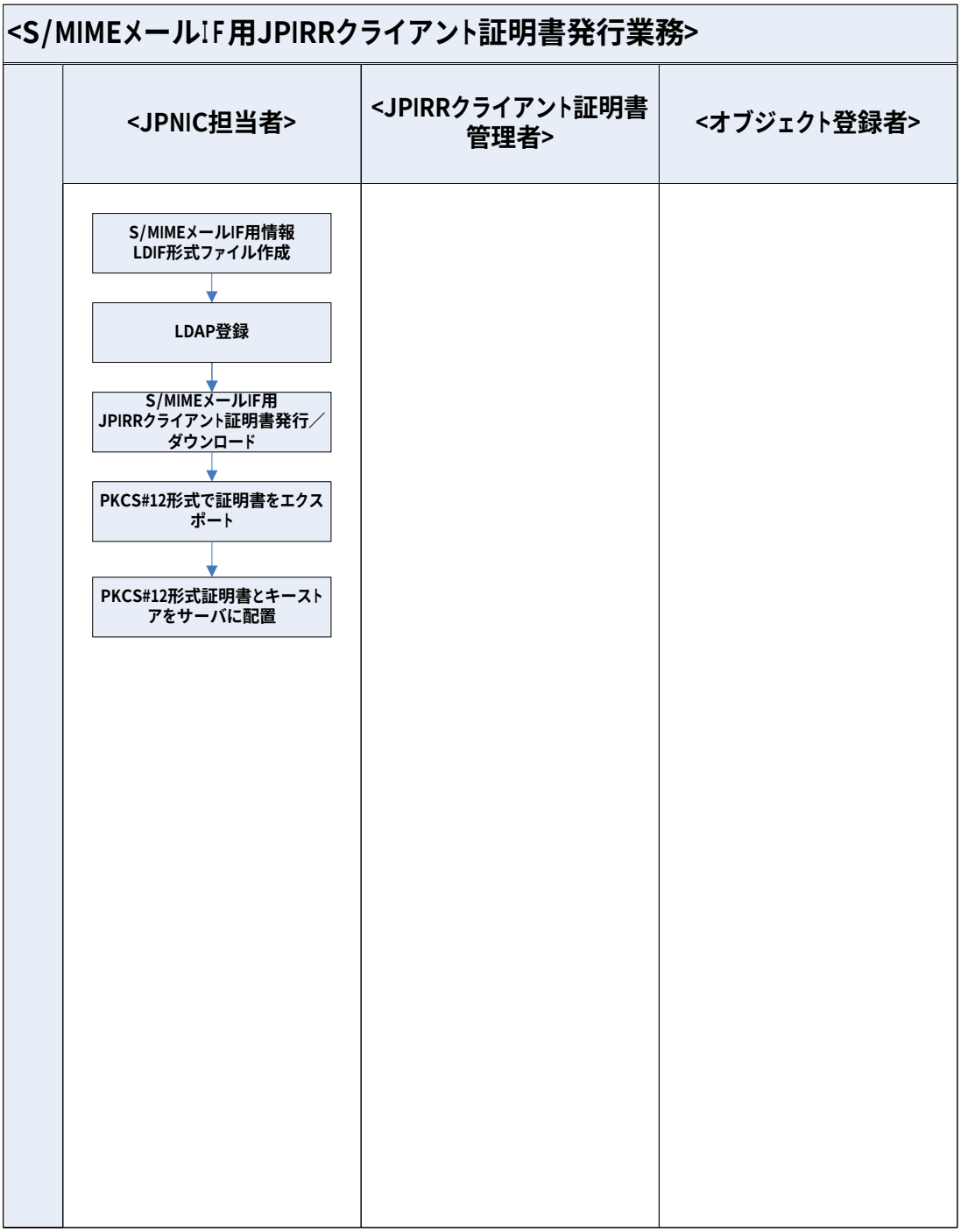


4.7.1.3. JPNIC 担当者 JPIRR クライアント証明書更新業務

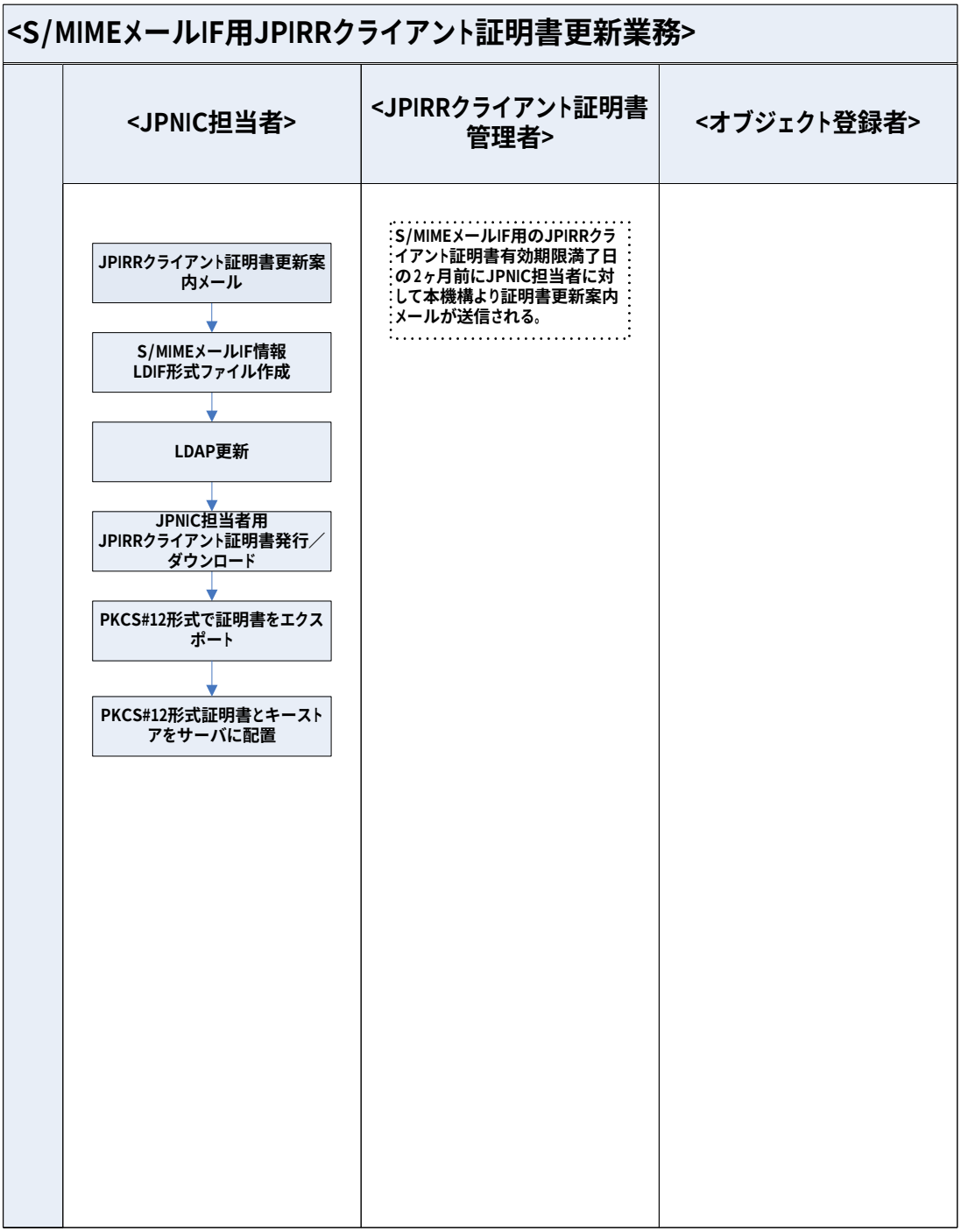


4.7.1.4. JPNIC 担当者 JPIRR クライアント証明書失効業務

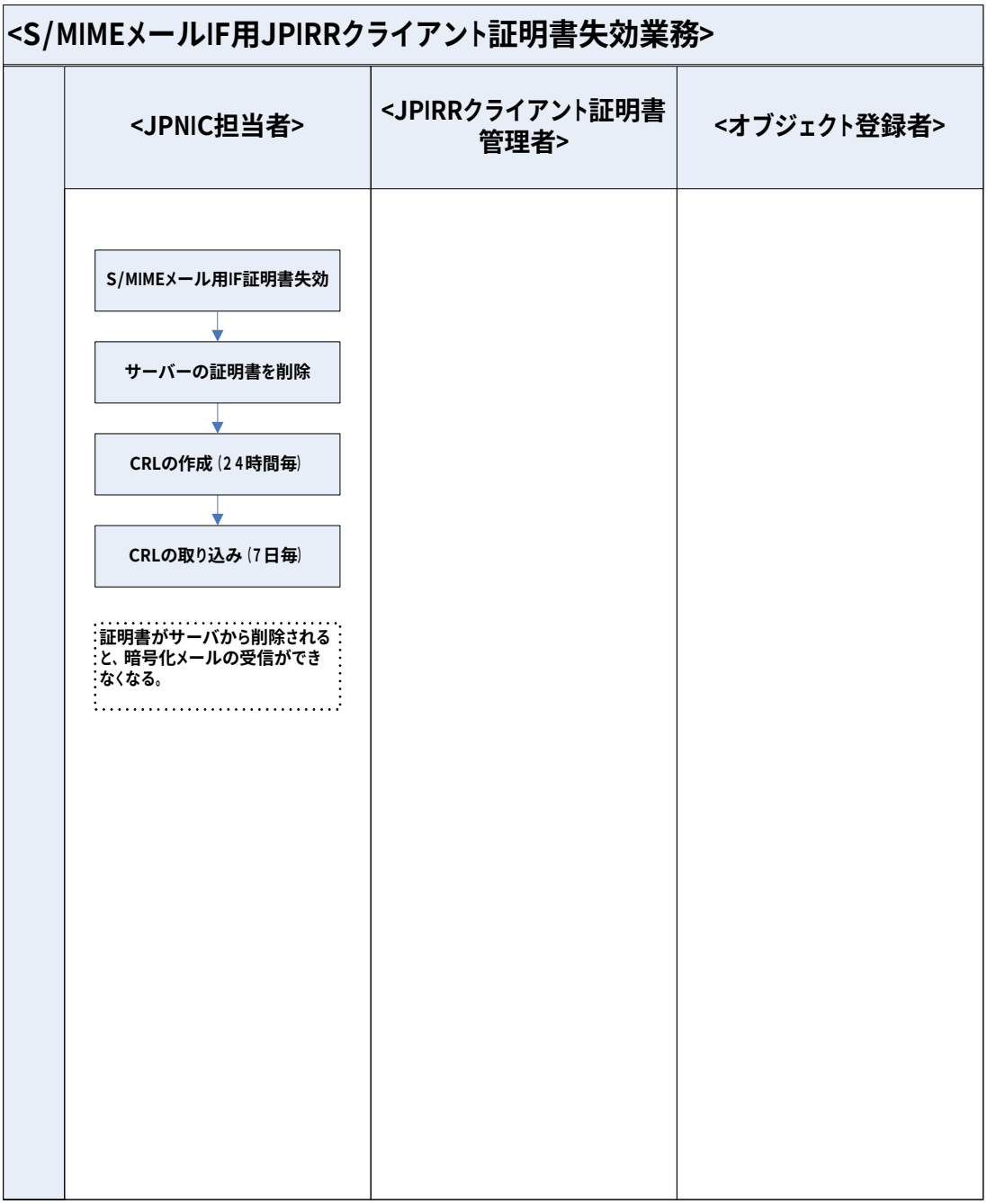
4.7.1.5. S/MIME メール IF 用 JPIRR クライアント証明書発行業務



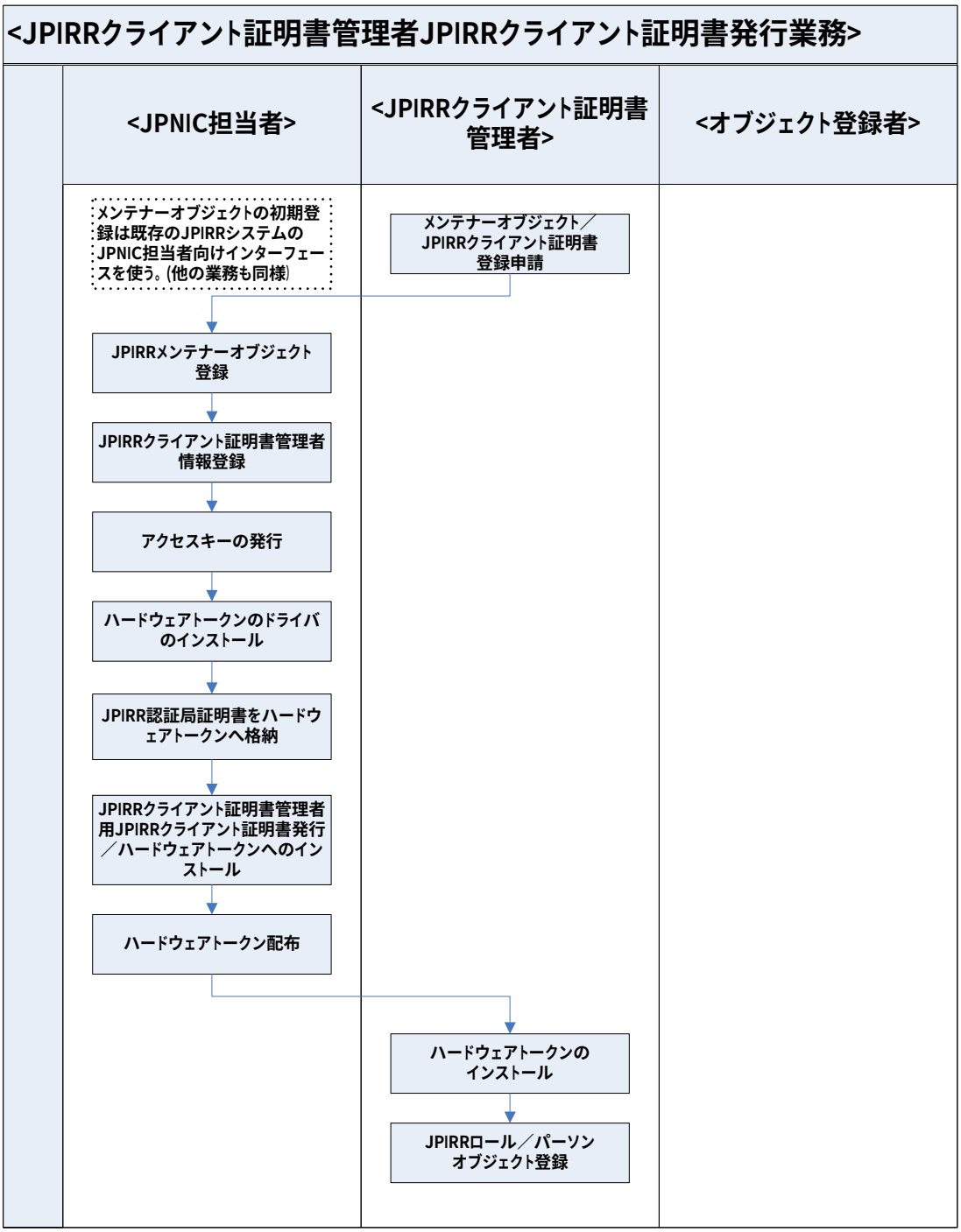
4.7.1.6. S/MIME メール IF 用 JPIRR クライアント証明書更新業務



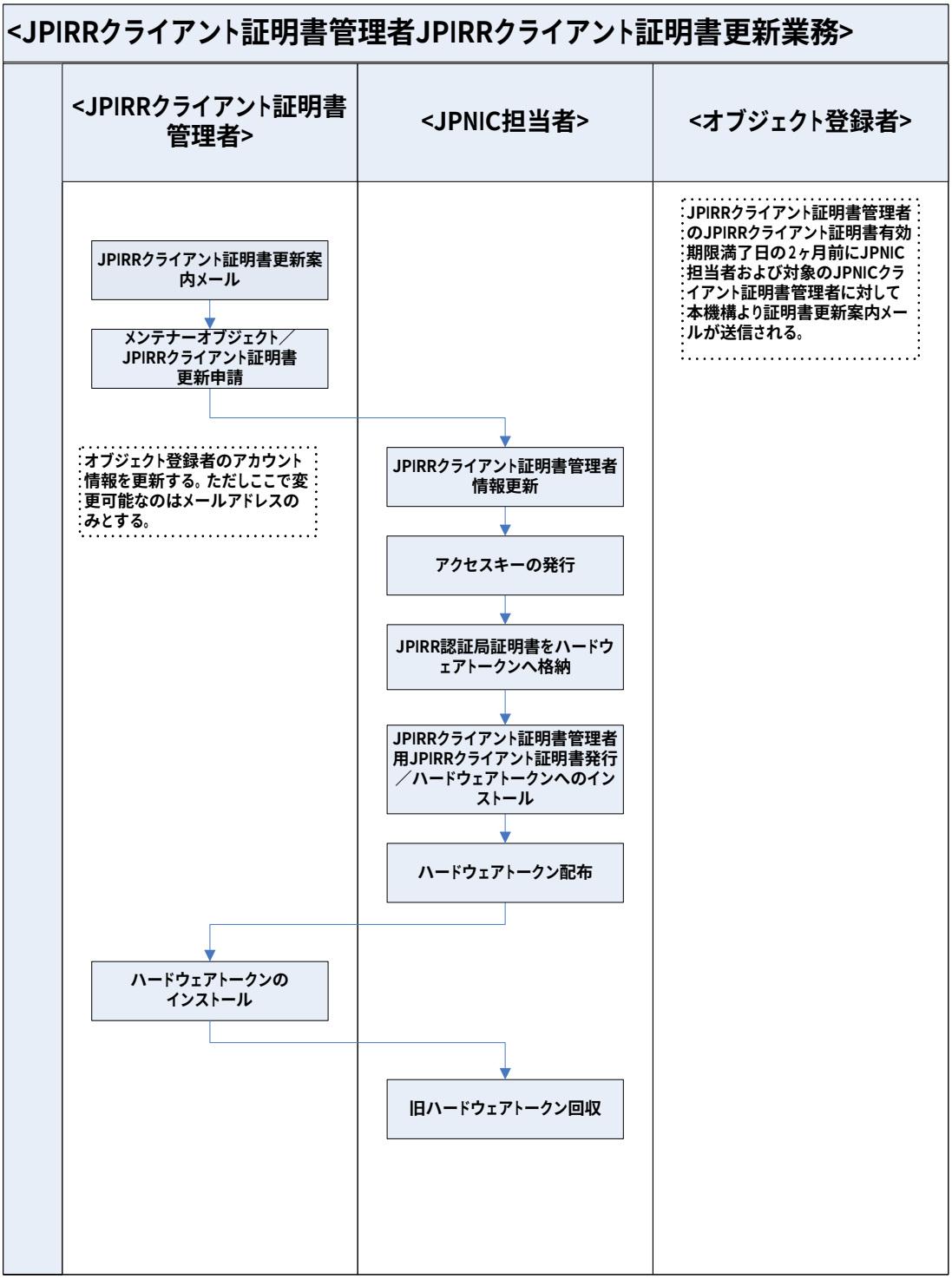
4.7.1.7. S/MIME メール IF 用 JPIRR クライアント証明書失効業務



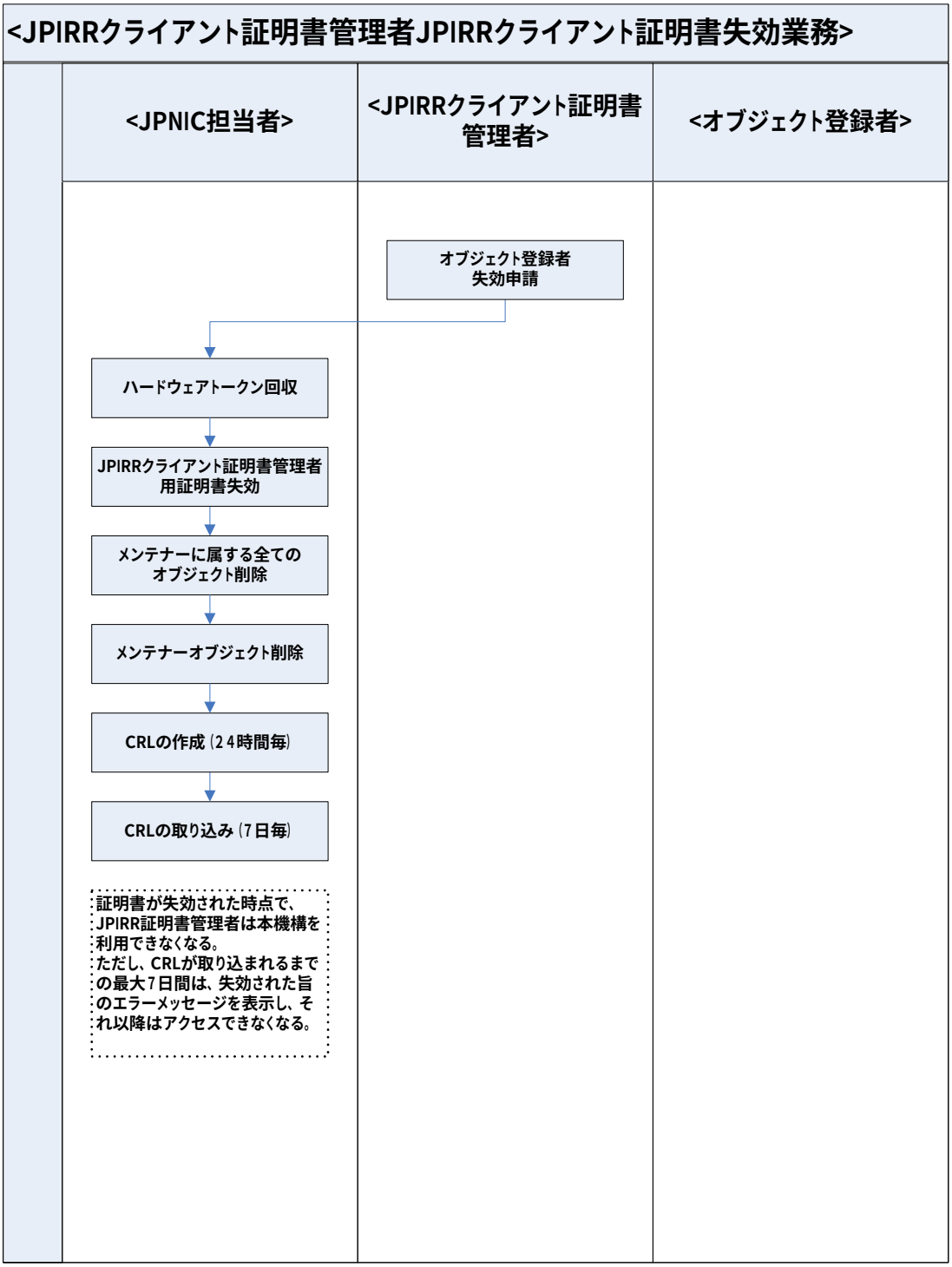
4.7.1.8. JPIRR クライアント証明書管理者 JPIRR クライアント証明書発行業務



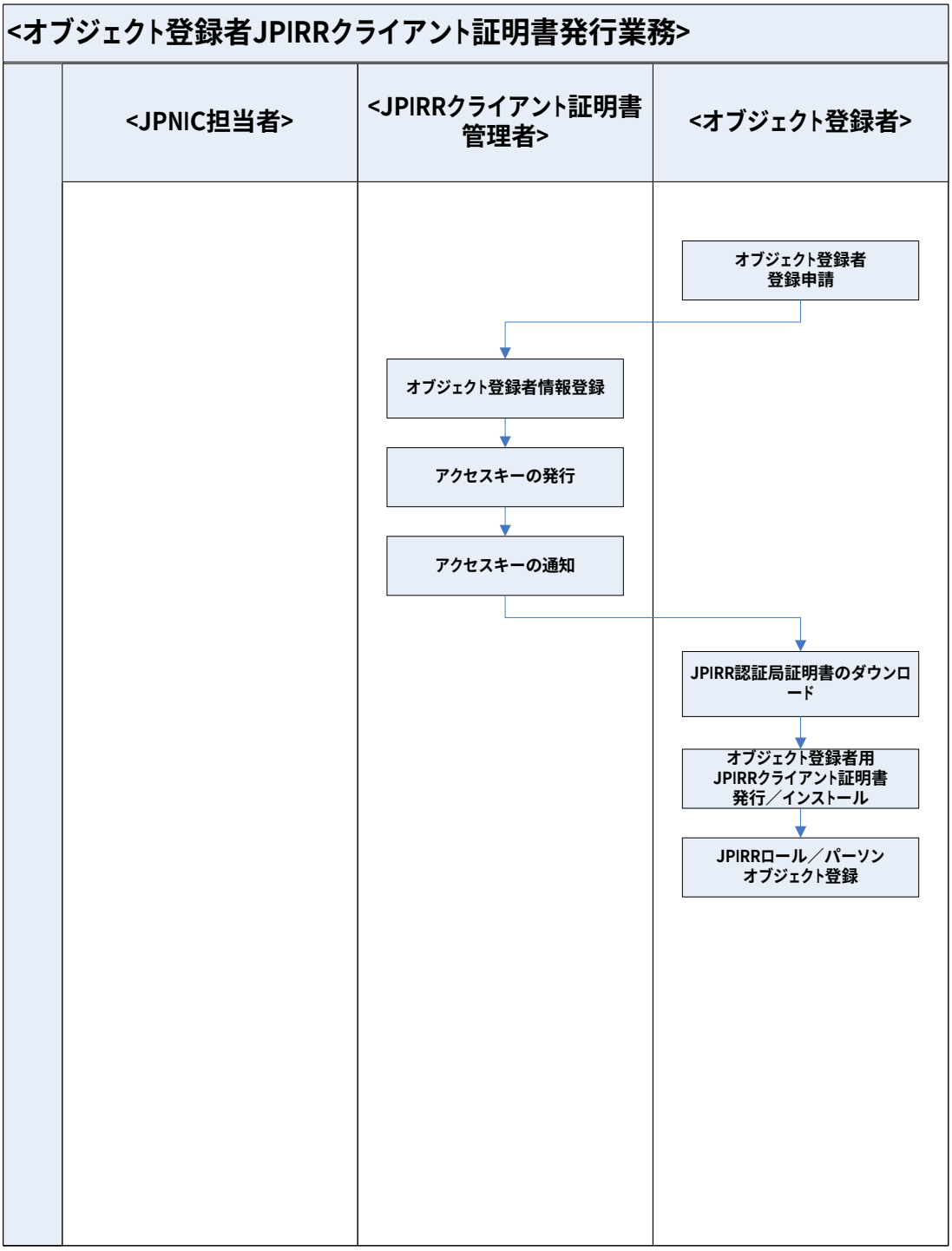
4.7.1.9. JPIRR クライアント証明書管理者 JPIRR クライアント証明書更新業務



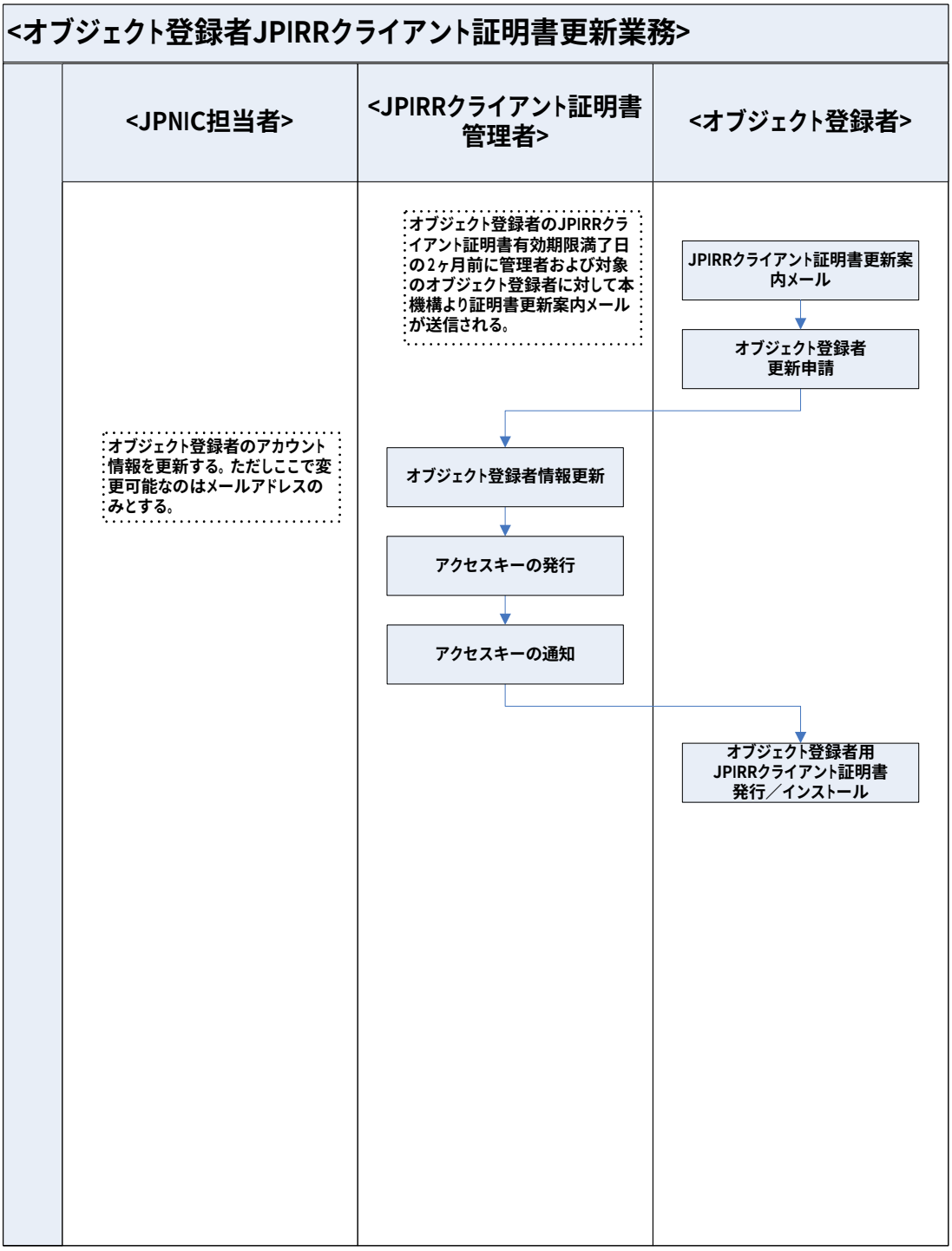
4.7.1.10. JPIRR クライアント証明書管理者 JPIRR クライアント証明書失効業務



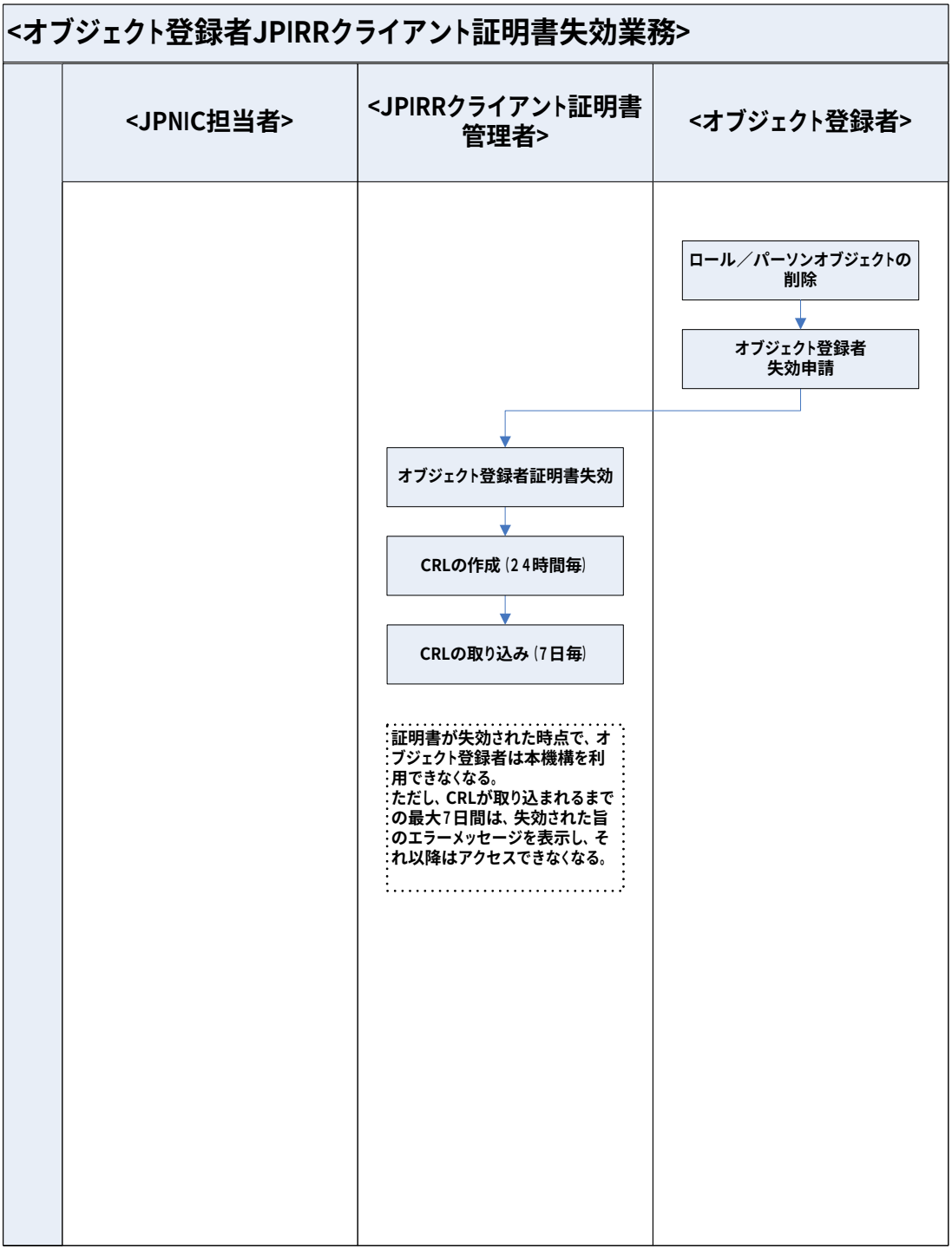
4.7.1.11. オブジェクト登録者 JPIRR クライアント証明書発行業務



4.7.1.12. オブジェクト登録者 JPIRR クライアント証明書更新業務



4.7.1.13. オブジェクト登録者 JPIRR クライアント証明書失効業務



4.7.2. 許可リスト管理業務

許可リストの管理は、資源管理 CA クライアント証明書及び JPIRR 認証局クライアント証明書のプロファイルによって識別される各担当者の種類によって、その操作や対象範囲に以下の通りに制限する。

- JPNIC 担当者
  全ての許可リストの参照、登録、変更、削除
- LIR 資源申請者
  自身の資源に関する許可リストの参照、登録、変更、削除
- オブジェクト登録者
  自身のメンテナーに関する許可リストの参照

4.7.2.1. 主な管理項目

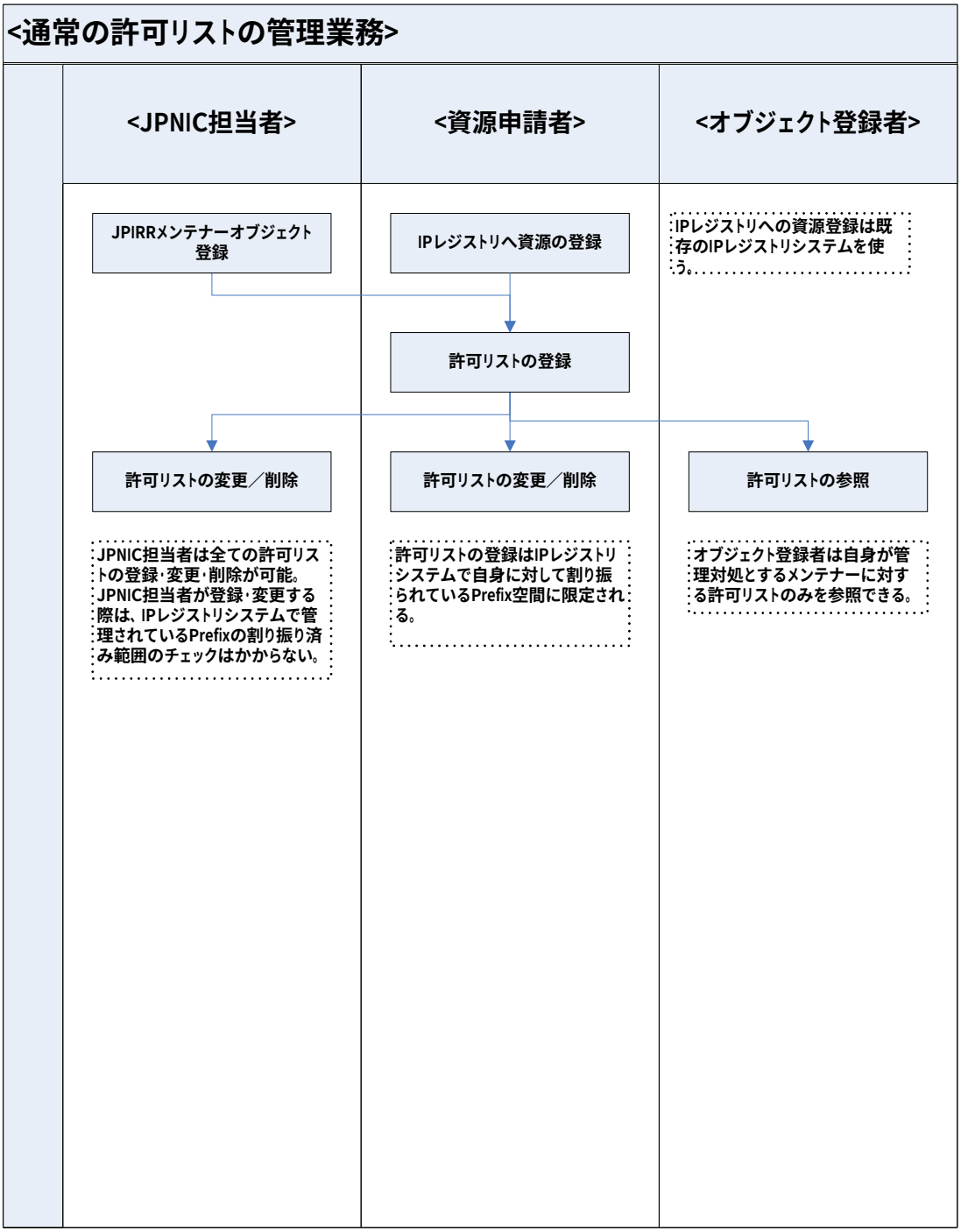
許可リストで管理する主な項目を表 4-15 に示す。

表 4-15　許可リスト管理項目

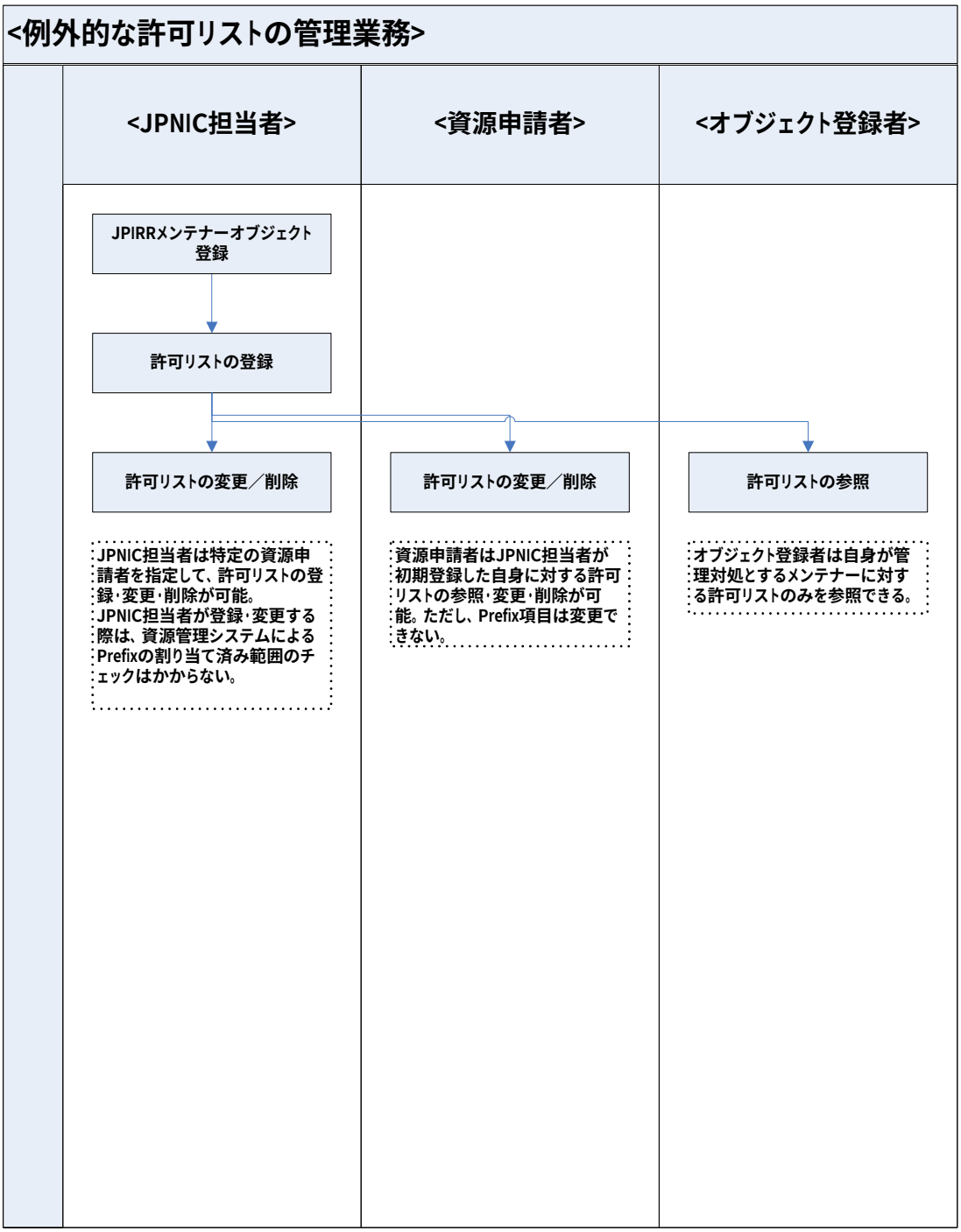
項目名	説明
許可リスト ID	システムが自動採番する許可リスト ID
資源管理番号	● JPNIC 担当者が管理する場合 入力された資源管理者略称から対応する資源管理番号を IP レジストリシステムから取得し、登録時に設定する。 ● 資源申請者が管理する場合 資源管理 CA クライアント証明書から、対応する資源管理番号を IP レジストリシステムから取得し、登録時に設定する。（変更不可） JPNIC 担当者の画面でのみ表示される。
資源管理者略称	● JPNIC 担当者が管理する場合 IP レジストリシステムに存在する資源管理者略称を画面から入力する。 ● 資源申請者が管理する場合 資源管理番号に対応する略称を IP レジストリシステムから取得し、登録時に設定する。（変更不可）
Prefix	ルートオブジェクトのアドレスブロック
メンテナー名	対象とするメンテナー名を１つ指定可能
ＡＳ番号	複数指定可能。指定無しも可能

許可・禁止区分	許可または禁止
初期登録者	初期登録時にその登録者が JPNIC 担当者か資源申請者かを設定する（変更不可）

4.7.2.2. 通常の許可リストの管理業務



4.7.2.3. 例外的な許可リストの管理業務



4.7.2.4. 不整合許可リストの修正業務

4.7.3. オブジェクト管理業務

各担当者は既存の JPIRR システムの仕様に従ったフォーマットのメール（以下、リクエストメールと呼ぶ）を作成し、S/MIME で本機構に送信する。
本機構では、以下の通り処理を行う。

（1） 処理の起動
cron により S/MIME メール I/F プログラムを定期的に起動し、メールの受信を行う。メールが存在すれば以降の処理を開始する。
（2） クライアント証明書・署名の検証
JPIRR クライアント証明書の有効性および署名の検証を行う。（詳細は「クライアント証明書による認証について」を参照。）
（3） 暗号化メールの復号化
暗号化されている・いないにかかわらず受け付ける。暗号化されている場合は復号する。
（4） オブジェクトや項目の識別
実行権限や許可リストのチェックのため、別途定める仕様にしたがって、リクエストメールからチェックに必要なオブジェクトや項目を識別する。
その際、本文に PGP 署名を示す特定のキーワードが含まれる場合は、本機構向けのリクエストメールでは無いと判断し、エラーとする。
メンテナーオブジェクトの更新・削除時に remark 項目に所定の文字列が設定されていない場合は、本機構向けのリクエストメールでは無いと判断し、エラーとする。
（5） 実行権限のチェック
JPIRR クライアント証明書のプロファイルによって識別される各担当者の種類および対象とするオブジェクトやその操作によって、下表に従って操作可能か否かのチェックを行う。
メンテナーオブジェクトの登録については、JPNIC 担当者によって本機構とは別に処理を行う。

オブジェクト	操作	実行可能担当者
メンテナー	削除	JPNIC 担当者
メンテナー	変更	JPIRR 証明書管理者
ロール、パーソン	登録、変更、削除	JPIRR 証明書管理者
ロール、パーソン	登録、変更、削除 (自身のオブジェクトのみ)	オブジェクト登録者
その他のオブジェクト	登録、変更、削除	オブジェクト登録者

（6） 対象メンテナーの検証
JPIRR 証明書管理者及びオブジェクト登録者が操作可能なオブジェクトは、JPIRR クライアント証明書のプロファイルで指定されたメンテナー及びそのメンテナーに属するオブジェクトであるかチェックする。（リクエストメールの mnt-by 項目がプロファイルと一致して

いること）

ただし、JPNIC 担当者の場合はチェック対象外とし、全てのメンテナーに対する操作が可能とする。

（7） 対象オブジェクト名の検証

オブジェクト登録者がロールまたはパーソンオブジェクトの操作をする場合、自身のオブジェクトであるかチェックする。（ロール名またはパーソン名が、クライアント証明書のプロファイル（CN）に含まれる名称と一致していること）

（8） 許可リストによるチェック

Route(Route6)オブジェクトに対するオブジェクト操作（登録、変更、削除）時は、許可リストに基づいてオブジェクトの正当性をチェックする。（許可リストに関係しないチェックは別途 JPIRR により行われることとする。）

チェックロジックは以下の通りとする。

1. オブジェクト登録者の証明書に関連づけられるメンテナーを対象とした許可リストで、リクエストメールの route 項目で指定されたアドレス範囲が１行で指定された Prefix 項目の範囲内である許可リスト（以下では該当の許可リストという）が存在しない場合、エラーとする。
2. 該当の許可リストが存在し、その許可・禁止区分が禁止（deny）である場合、エラーとする。（該当する allow より優先する。）
3. 該当の許可リストが存在し、その許可・禁止区分が許可（allow）であり、かつ AS 番号区分が指定されていない場合、正常とする。
4. 該当の許可リストが存在し、その許可リストの許可・禁止区分が許可（allow）であり、かつ AS 番号区分が指定されていた場合、リクエストメールの origin 項目で指定される AS 番号がその許可リストで指定されている AS 番号に含まれている場合は正常とし、含まれていない場合はエラーとする。

Route(Route6)オブジェクト以外のオブジェクト操作についてはチェックを行わない。

（9） エラーメール送信

認証エラーおよび許可リストによる正当性チェックエラーが発生した場合はその原因をエラーメールでオブジェクト登録者（リクエストメールの Repry-to または From アドレス）及び JPNIC 担当者（固定の担当者メールアドレス）に送信する。

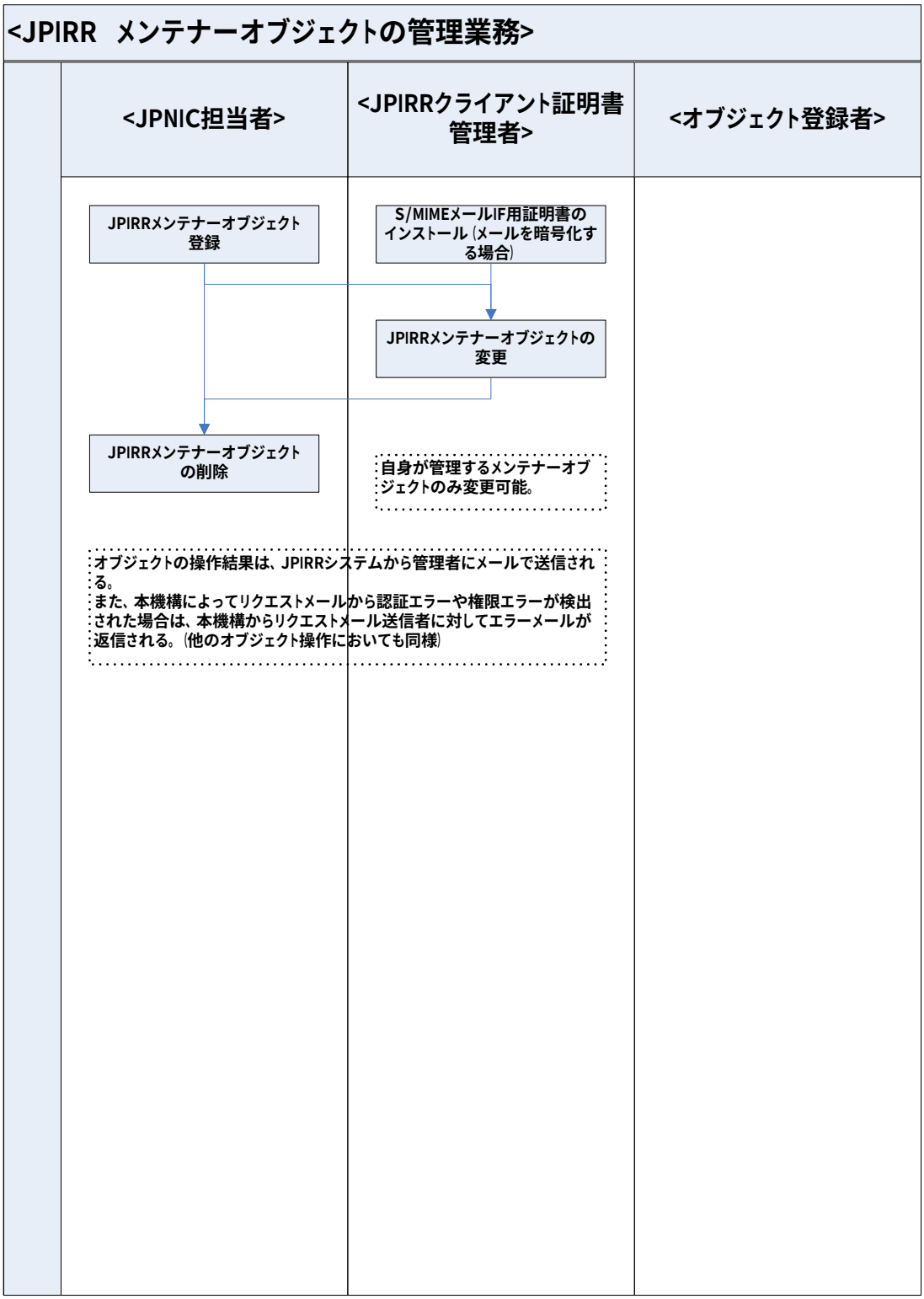
１通のメールで複数のオブジェクト操作があった場合、１つでもエラーが発生した場合は、全てを無効とする。

（10） JPIRR へのリクエストメール送信

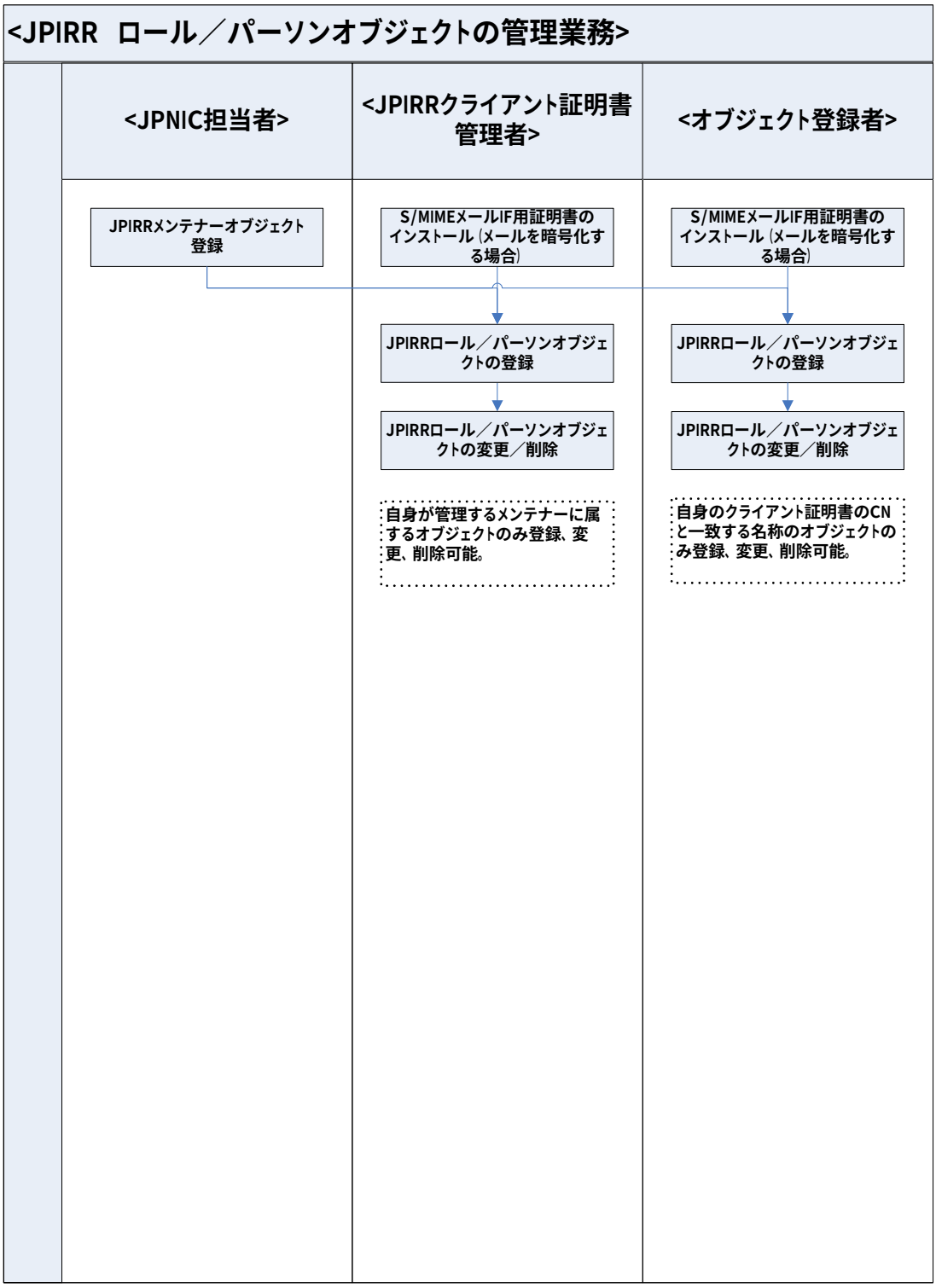
認証及び許可リストによるチェックでエラーがない場合は、本機構は JPIRR の本機構専用のアドレスに対してリクエストメールを平文で送信する。

そのアドレスでは、IRR システムで既存の認証機能を経ずに処理されることとする。また、セキュリティのため外部からのメールを直接受信できないような設定がされていることとする。

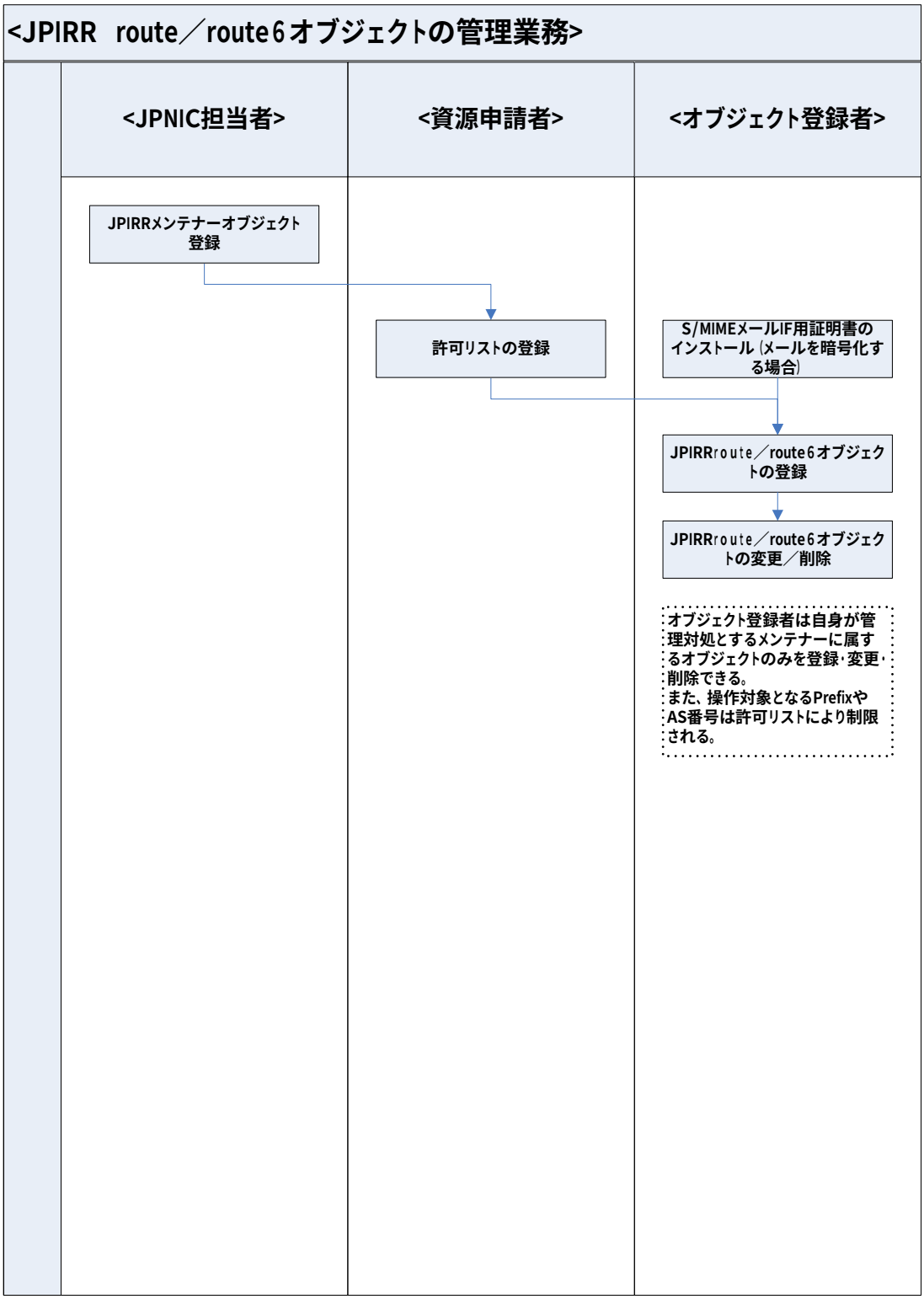
4.7.3.2. メンテナーオブジェクトの管理業務



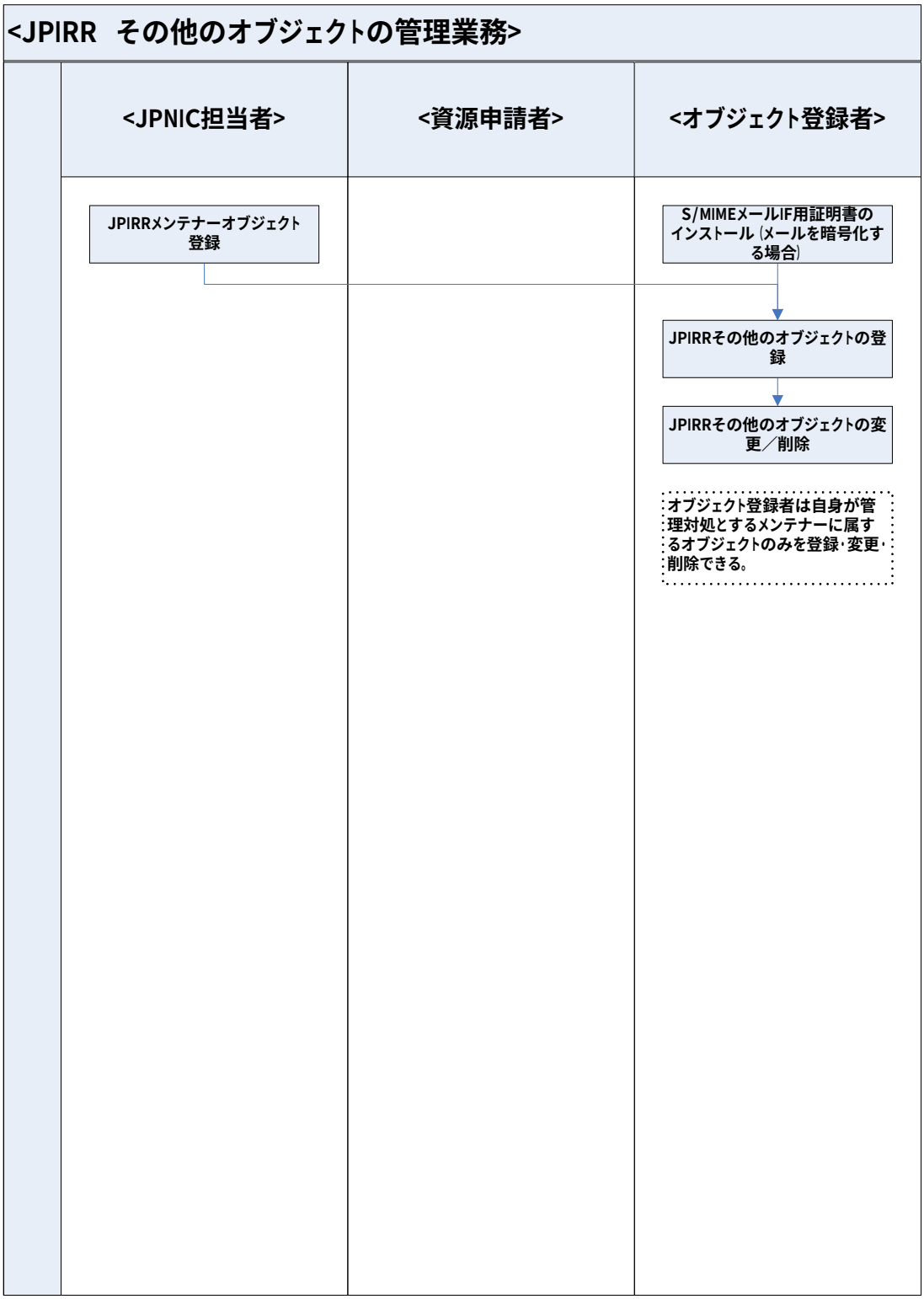
4.7.3.3. ロール／パーソンオブジェクトの管理業務



4.7.3.4. route オブジェクトの管理業務



4.7.3.5. その他のオブジェクトの管理業務



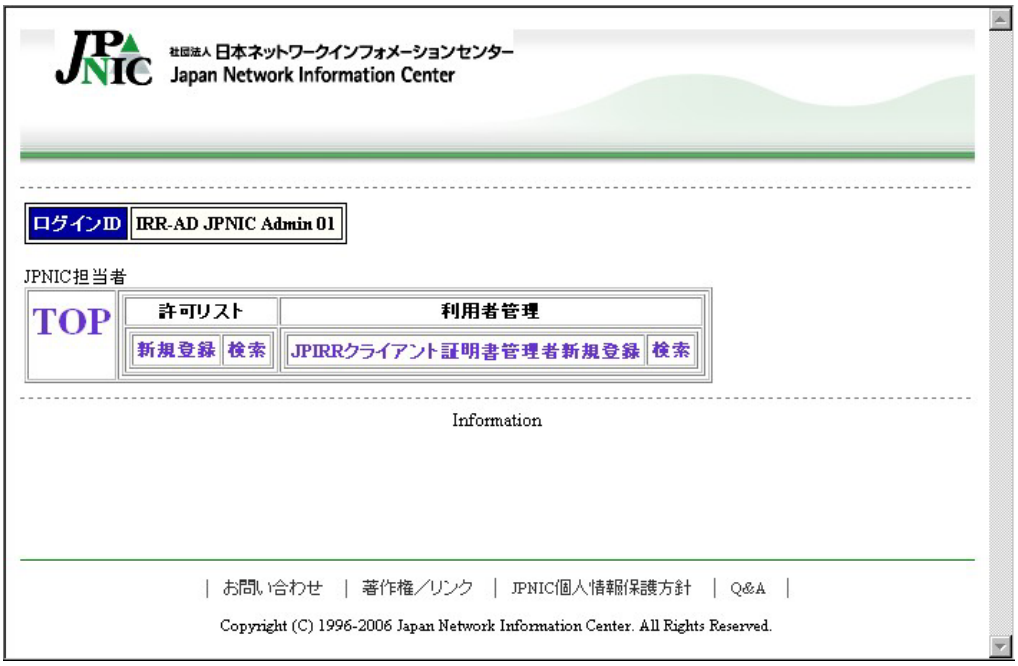
4.8. インターフェース設計

4.8.1. 画面設計

4.8.1.1. JPNIC 担当者用インターフェース

利用者が最初に本機構にアクセスした際に表示する画面。SSL クライアント認証を行った利用者の証明書から CN 属性を取得し、ログイン ID として表示する。画面上部のリンクをクリックし、許可リストの管理と利用者の管理を行う。

（1）　トップ画面



お知らせは所定のテキストファイルで管理し、html 方式で表示する。

（2）　許可リスト登録

資源申請者に成り代わって例外許可リスト情報を入力する。任意の Prefix に対して許可リストを登録することができる。Prefix について以下の入力チェックを行う。

- 同一のメンテナー名かつ同一の許可・禁止区分で、登録済み許可リストと範囲が重なる Prefix がある場合、エラーとし登録不可とする。
- 同一のメンテナー名で、「禁止」の登録済み許可リストの範囲に含まれるまたは等しい Prefix がある「許可」を新規登録しようとした場合、エラーとし登録不可とする。
- 同一のメンテナー名で、「許可」の登録済み許可リストの範囲を含むまたは等しい Prefix がある「禁止」を新規登録しようとした場合、エラーとし登録不可とする。

メンテナー名について以下の入力チェックを行う。

- 指定されたメンテナー名が JPIRR のメンテナーオブジェクトとして存在する。

AS 番号については、１つの許可リストにつき最大１００件まで登録可能とする。
「登録」ボタンをクリックすると「許可リスト確認」に遷移する。

（3）　許可リスト登録確認

許可リスト登録の確認画面を表示する。「許可リスト登録」で入力された資源管理者略称に該当する資源管理番号を IP レジストリシステムから取得し表示する。

「登録」ボタンをクリックすると「許可リスト完了」に遷移する。

（4）　許可リスト登録完了

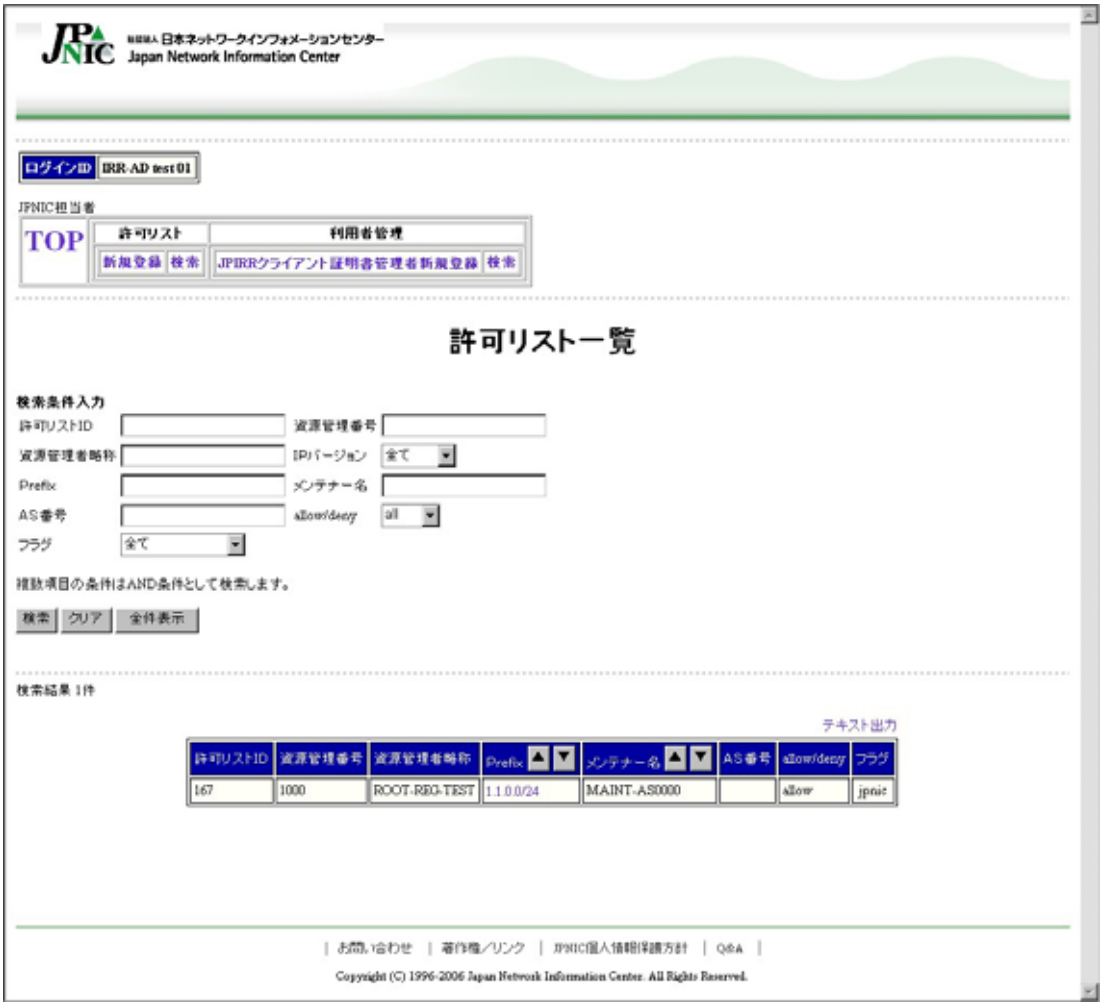
例外許可リスト登録の完了を知らせる。登録された許可リストの内容を表示する。「続けて登録する」リンクをクリックすると「許可リスト登録」に遷移する。

（5） 許可リスト検索

許可リストの検索画面を表示する。

「検索」ボタンまたは「全件表示」ボタンをクリックすると「許可リスト一覧」に遷移する。

（6） 許可リスト一覧



「許可リスト検索」、「許可リスト一覧」で入力された検索条件に該当する許可リストの情報を取得し表示する。

「検索」ボタンまたは「全件表示」ボタンをクリックすると「許可リスト一覧」に遷移する。

「Prefix」の横の▲をクリックすると検索結果を Prefix の昇順で表示する。「Prefix」の横の▼をクリックすると検索結果を Prefix の降順で表示する。

「メンテナー名」の横の▲をクリックすると検索結果をメンテナー名の昇順で表示する。「メンテナー名」の横の▼をクリックすると検索結果をメンテナー名の降順で表示する。「Prefix」リンクをクリックすると「許可リスト変更」に遷移する。「テキスト表示」リンクをクリックすると「許可リストテキスト表示」に遷移する。

（7） 許可リスト変更

資源申請者に成り代わって例外許可リスト情報を変更する。任意の Prefix に対して許可リストを登録することができる。Prefix とメンテナー名については「許可リスト登録」と同じ入力チェックを行う。

「変更」ボタンをクリックすると「許可リスト変更確認」に遷移する。

「削除」ボタンをクリックすると「許可リスト削除完了」に遷移する。

（8） 許可リスト変更確認

許可リスト変更の確認画面を表示する。

「登録」ボタンをクリックすると「許可リスト変更完了」に遷移する。

（9） 許可リスト変更完了

許可リスト変更の完了を知らせる。変更された許可リストの内容を表示する。

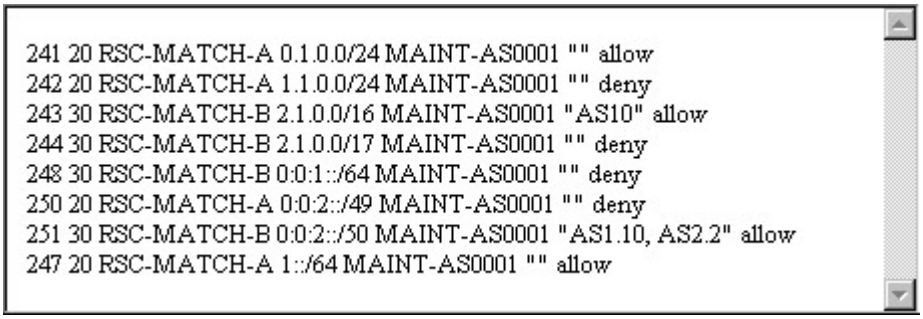
「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

（10） 許可リスト削除完了

許可リスト削除の完了を知らせる。削除された許可リストの内容を表示する。

「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

（11） 許可リストテキスト表示



「許可リスト一覧」に表示されている許可リストの情報を取得し表示する。

（12） 利用者新規登録

JPIRR クライアント証明書管理者新規登録画面を表示し、利用者情報を入力する。

「検索」ボタンをクリックすると管理対象メンテナー名の admin-c 項目をプルダウンで表示する。

「OK」ボタンをクリックすると「JPIRR クライアント証明書管理者新規登録確認」に遷移する。

（13） 利用者登録確認

JPIRR クライアント証明書管理者新規登録の確認画面を表示する。

「OK」ボタンをクリックすると「JPIRR クライアント証明書管理者新規登録完了」に遷移する。

（14） 利用者登録完了

JPIRR クライアント証明書管理者新規登録の完了を知らせる。

「アクセスキー発行」ボタンをクリックすると「アクセスキー発行完了」に遷移する。

（15）　アクセスキー発行完了

JPIRR クライアント証明書管理者アクセスキー発行の完了を知らせる。

「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

（16） 証明書の取得

JPIRR クライアント証明書管理者用証明書の取得を行う。

アクセスキーを入力し「証明書発行」ボタンをクリックすることで、認証を行い「証明書発行完了」に遷移する。

（17） 証明書発行完了

JPIRR クライアント証明書管理者用証明書の発行完了を表示する。

（18） 利用者管理一覧

検索条件に該当する利用者の情報を取得し表示する。

「cn」リンクをクリックすると「利用者管理詳細」に遷移する。

（19） 利用者管理詳細

JPIRR クライアント証明書管理者に関する詳細情報の表示を行う。

利用者管理一覧より取得した利用者を表示し、利用者、状態、更新状況により使用できるボタンを設定する。また、表示する利用者によりタイトル、表示内容を変えて表示する。

「修正」ボタンをクリックすると「利用者修正」に遷移する。

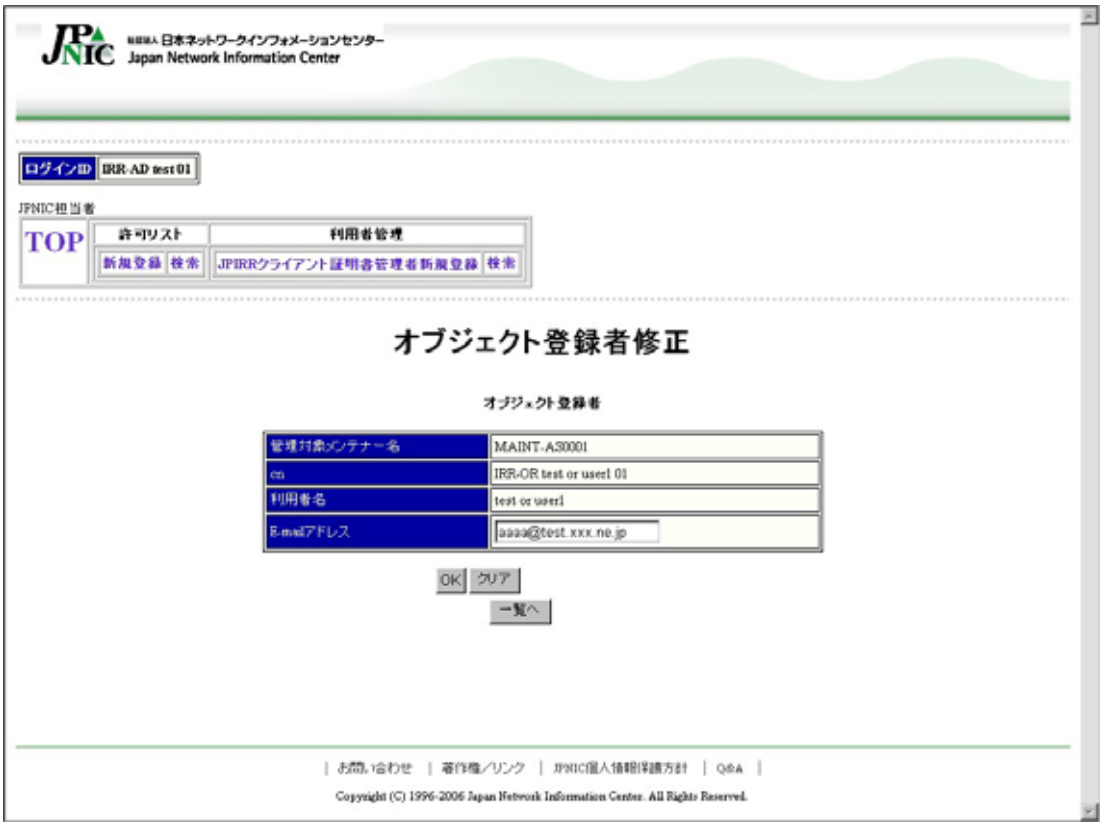
「アクセスキー発行」ボタンをクリックすると「JPIRR クライアント証明書管理者アクセスキー発行完了」に遷移する。

「更新登録」ボタンをクリックすると「JPIRR クライアント証明書管理者更新登録」に遷移する。

「証明書失効」ボタンをクリックすると「証明書失効完了」に遷移する。

（20） 利用者修正

利用者修正画面を表示し、利用者情報を入力する。利用者によりタイトル、表示内容を変えて表示する。



「OK」ボタンをクリックすると「利用者修正確認」に遷移する。

（21） 利用者修正確認

利用者修正の確認画面を表示する。利用者によりタイトル、表示内容を変えて表示する。
「OK」ボタンをクリックすると「利用者修正完了」に遷移する。

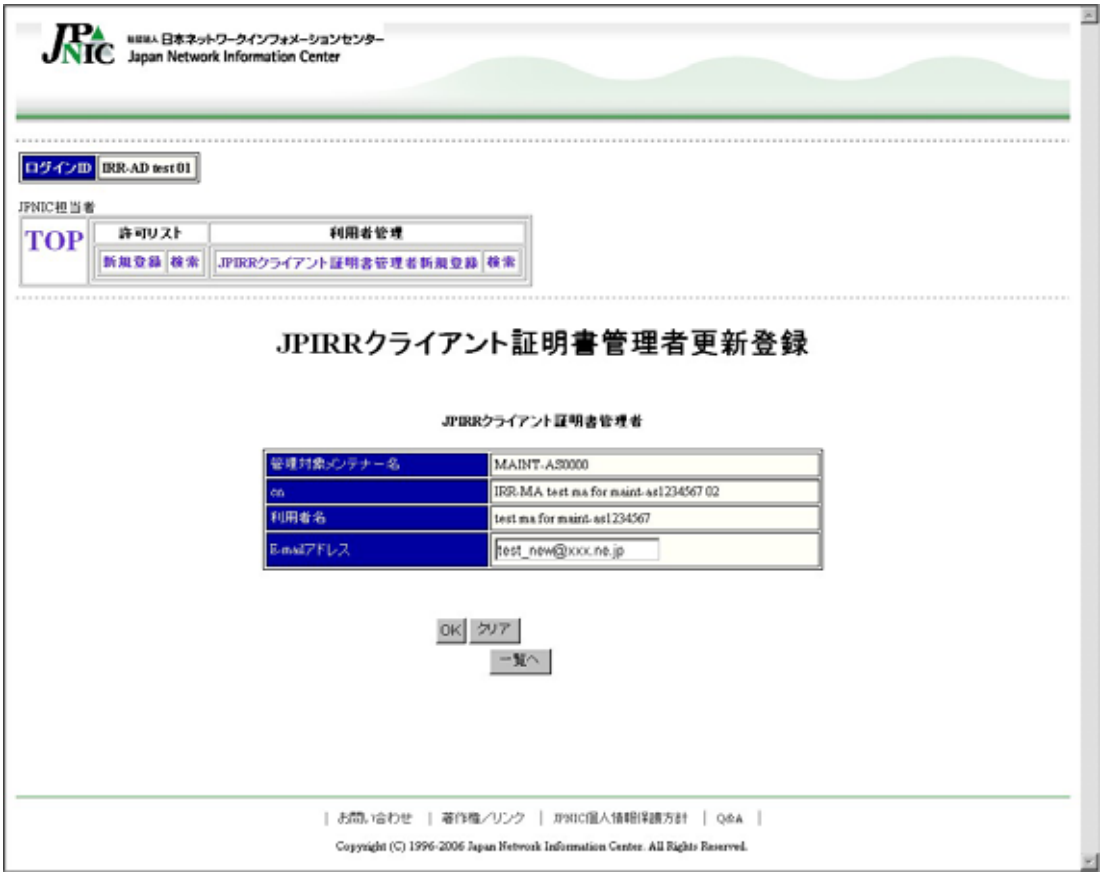
（22） 利用者修正完了

利用者修正の完了を知らせる。利用者によりタイトル、表示内容を変えて表示する。

「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

（23） 利用者更新登録

更新対象利用者の情報をもとに JPIRR クライアント証明書管理者の利用者情報を新たに作成する。



「OK」ボタンをクリックすると「JPIRR クライアント証明書管理者更新登録確認」に遷移する。

（24） 利用者更新登録確認

JPIRR クライアント証明書管理者更新登録の確認画面を表示する。

「OK」ボタンをクリックすると「JPIRR クライアント証明書管理者更新登録完了」に遷移する。

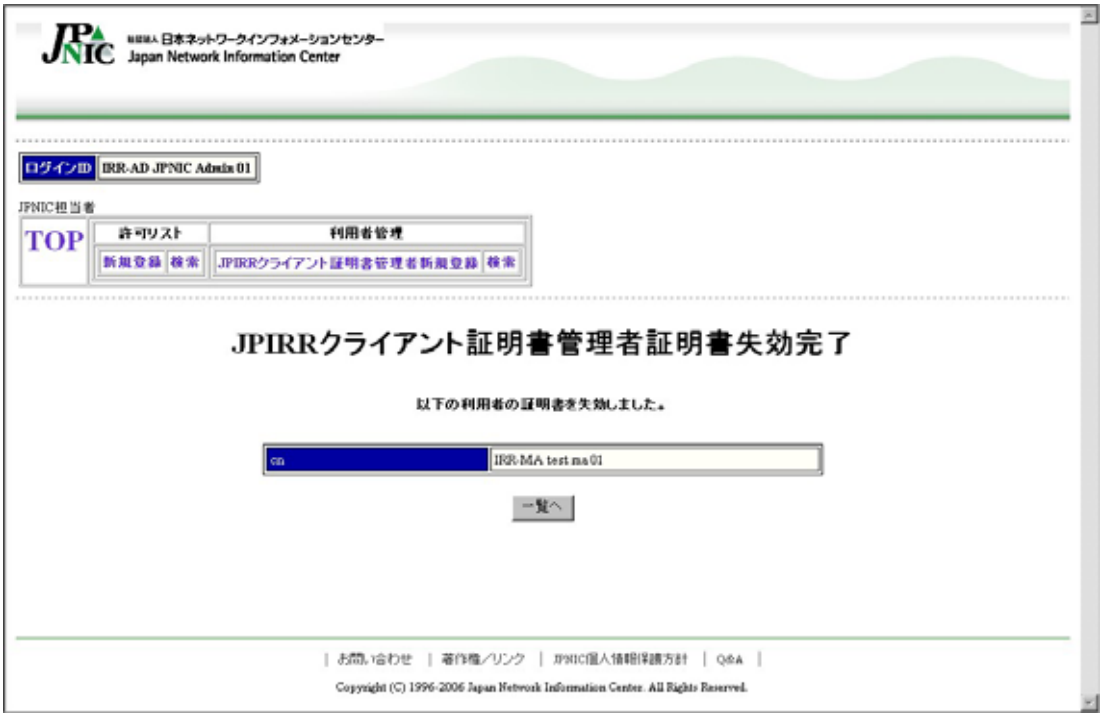
（25） 利用者更新登録完了

JPIRR クライアント証明書管理者更新登録の完了を知らせる。

「アクセスキー発行」をクリックすると「アクセスキー発行完了」に遷移する。

（26） 証明書失効完了

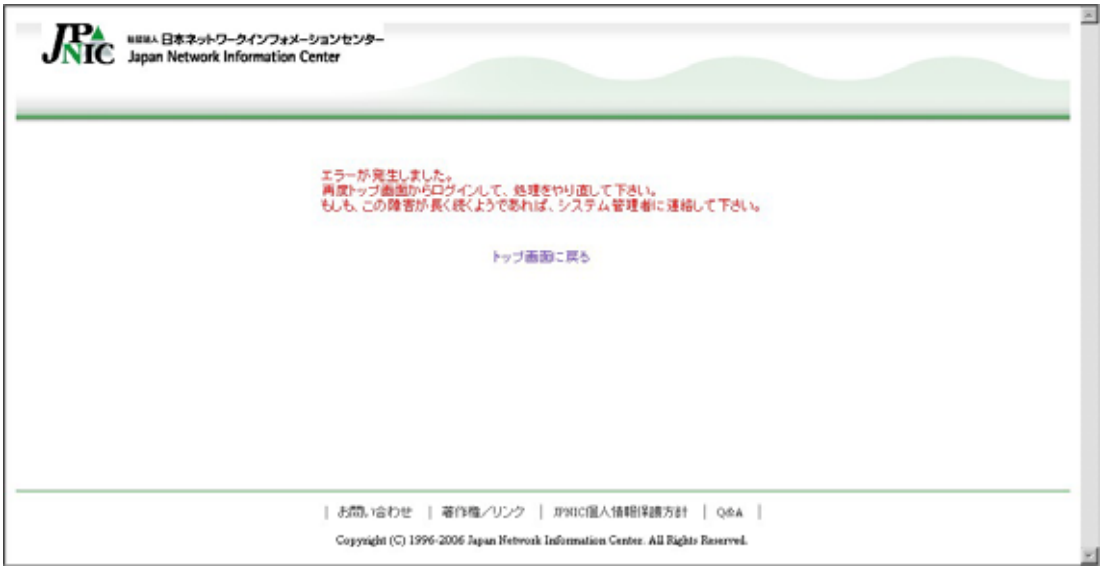
証明書失効の完了を知らせる。登録者によりタイトル、表示内容を変えて表示する。



「一覧へ」をクリックすると「利用者管理一覧」に遷移する。

（27）　エラー表示

エラー一般の表示を行う画面。エラーの内容を表示する。

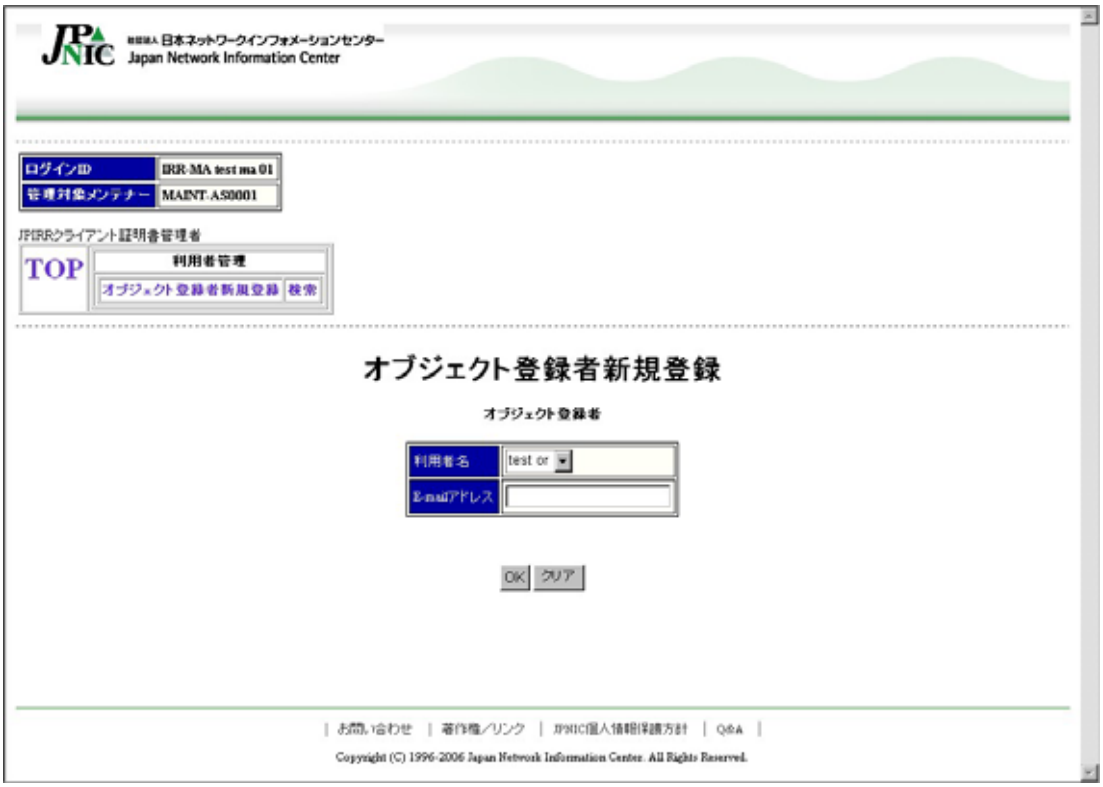


4.8.1.2. JPIRR クライアント証明書管理者用インターフェース

（1）　トップ画面

利用者が最初に本機構にアクセスした際に表示する画面。SSL クライアント認証を行った利用者の証明書から CN 属性、OU 属性を取得し、ログイン ID、管理対象メンテナーとして表示する。画面上部のリンクをクリックし、利用者の管理を行う。

（2） 利用者新規登録



オブジェクト登録者新規登録画面を表示し、利用者情報を入力する。証明書の管理対象メンテナー名の tech-c 項目をプルダウンで表示する。

「OK」ボタンをクリックすると「オブジェクト登録者新規登録確認」に遷移する。

（3） 利用者登録確認

オブジェクト登録者新規登録の確認画面を表示する。

「登録」ボタンをクリックすると「オブジェクト登録者新規登録完了」に遷移する。

（4） 利用者登録完了

オブジェクト登録者新規登録の完了を知らせる。

「アクセスキー発行」ボタンをクリックすると「オブジェクト登録者アクセスキー発行完了」に遷移する。

（5）　アクセスキー発行完了

オブジェクト登録者アクセスキー発行の完了を知らせる。

「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

（6） 利用者管理一覧

証明書の管理対象メンテナー名に該当する利用者の情報を取得し表示する。

「cn」リンクをクリックすると「オブジェクト登録者情報詳細」に遷移する。

（7）　オブジェクト登録者情報詳細

利用者管理一覧より取得した利用者の情報を表示し、状態、更新状況により使用できるボタンを設定する。

「修正」ボタンをクリックすると「オブジェクト登録者修正」に遷移する。

「アクセスキー発行」ボタンをクリックすると「オブジェクト登録者アクセスキー発行完了」に遷移する。

「更新登録」ボタンをクリックすると「オブジェクト登録者更新登録」に遷移する。

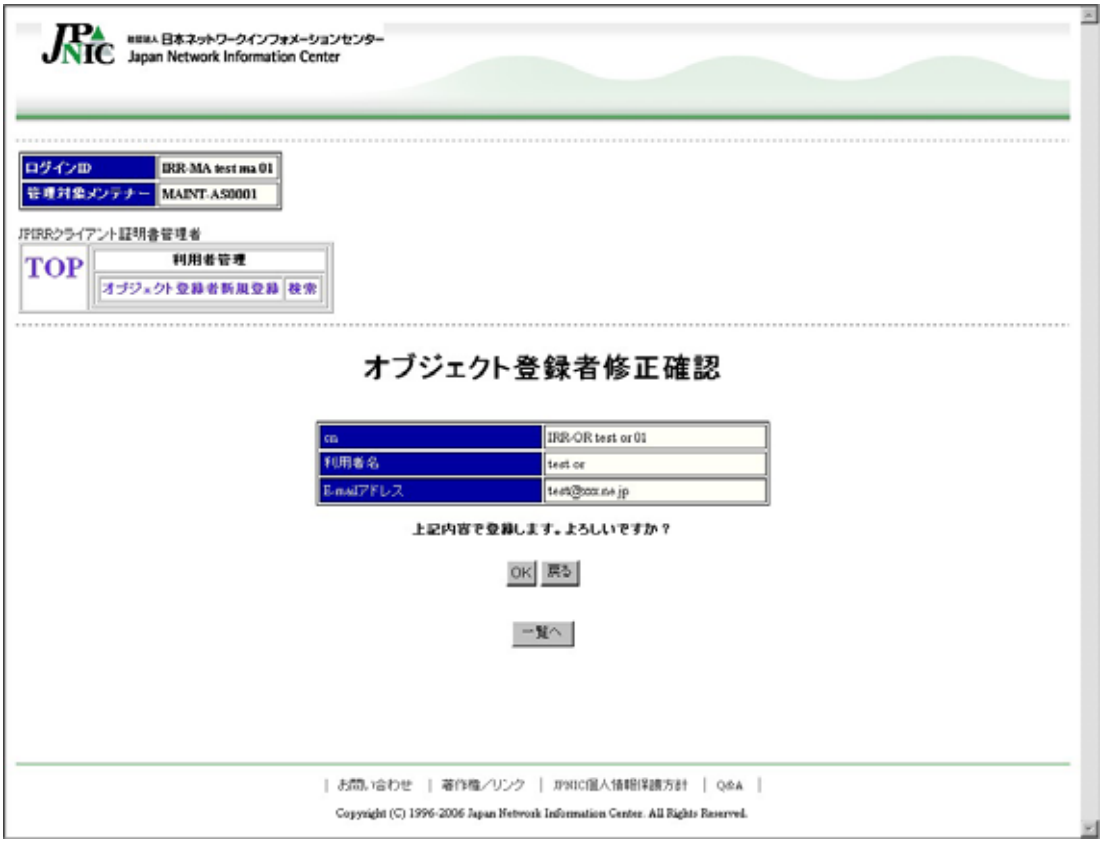
「証明書失効」ボタンをクリックすると「オブジェクト登録者証明書失効完了」に遷移する。

（8）　オブジェクト登録者修正

オブジェクト登録者修正画面を表示し、利用者情報を入力する。

「OK」ボタンをクリックすると「オブジェクト登録者修正確認」に遷移する。

（9） オブジェクト登録者修正確認



オブジェクト登録者修正の確認画面を表示する。

「OK」ボタンをクリックすると「オブジェクト登録者修正完了」に遷移する。

（10） オブジェクト登録者修正完了

オブジェクト登録者修正の完了を知らせる。

「一覧へ」ボタンをクリックすると「利用者管理一覧」に遷移する。

（11） オブジェクト登録者更新登録

更新対象利用者の情報をもとにオブジェクト登録者の利用者情報を新たに作成する。

「OK」ボタンをクリックすると「オブジェクト登録者更新登録確認」に遷移する。

（12）　オブジェクト登録者更新登録確認

オブジェクト登録者更新登録の確認画面を表示する。

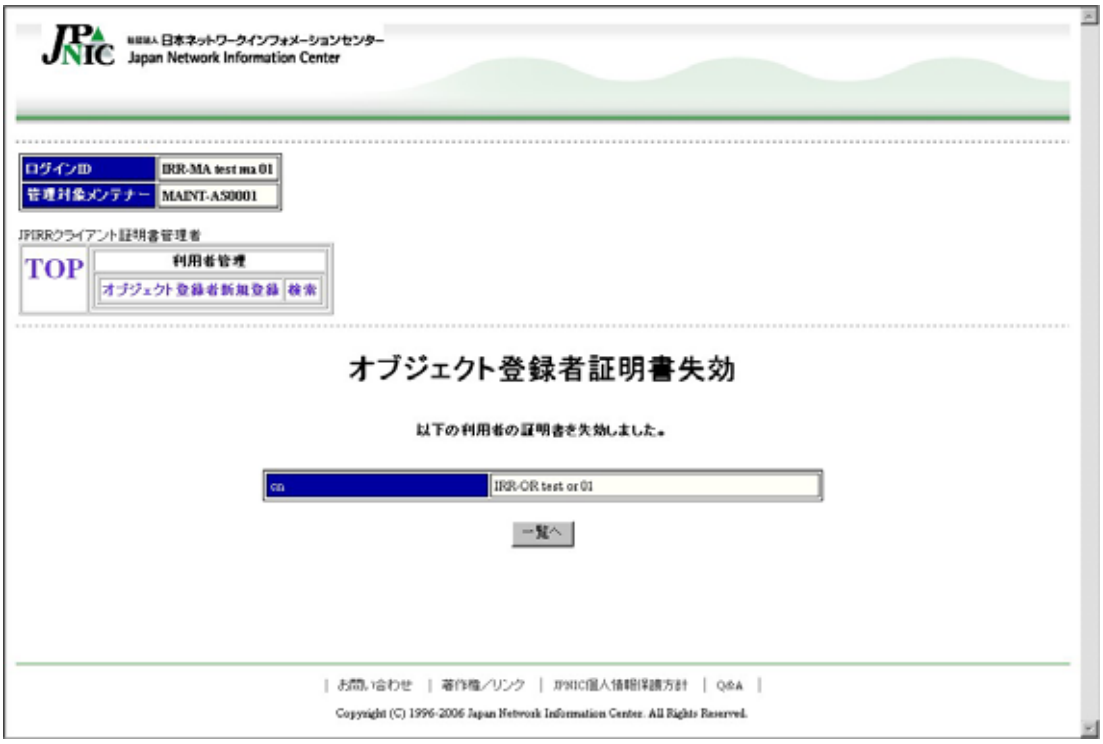
「登録」ボタンをクリックすると「オブジェクト登録者更新登録完了」に遷移する。

（13）　オブジェクト登録者更新登録完了

オブジェクト登録者更新登録の完了を知らせる。

「アクセスキー発行」をクリックすると「アクセスキー発行完了」に遷移する。

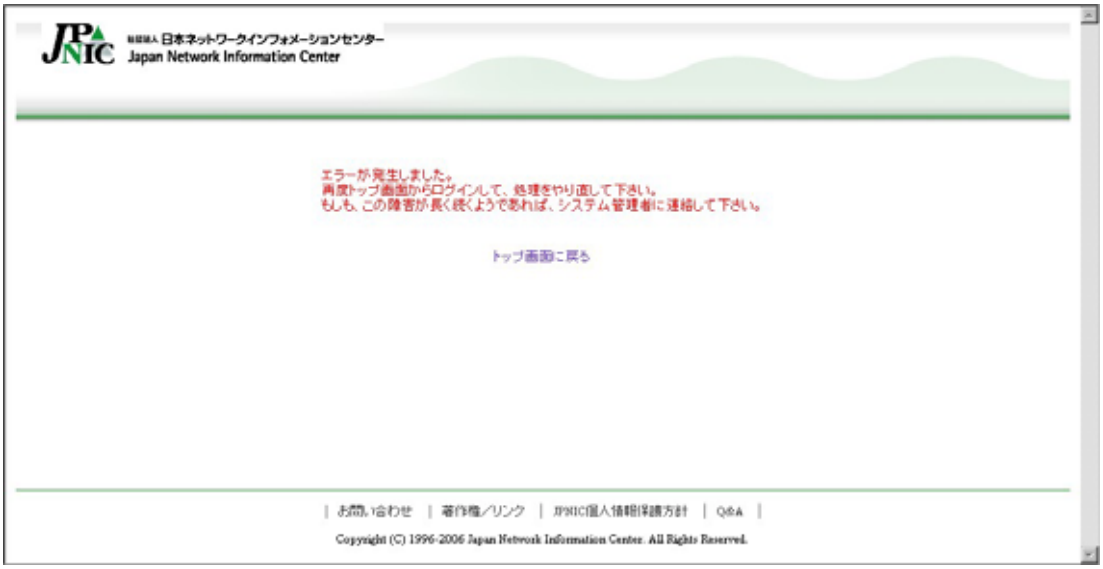
（14）　証明書失効完了



証明書失効の完了を知らせる。

「一覧へ」をクリックすると「利用者管理一覧」に遷移する。

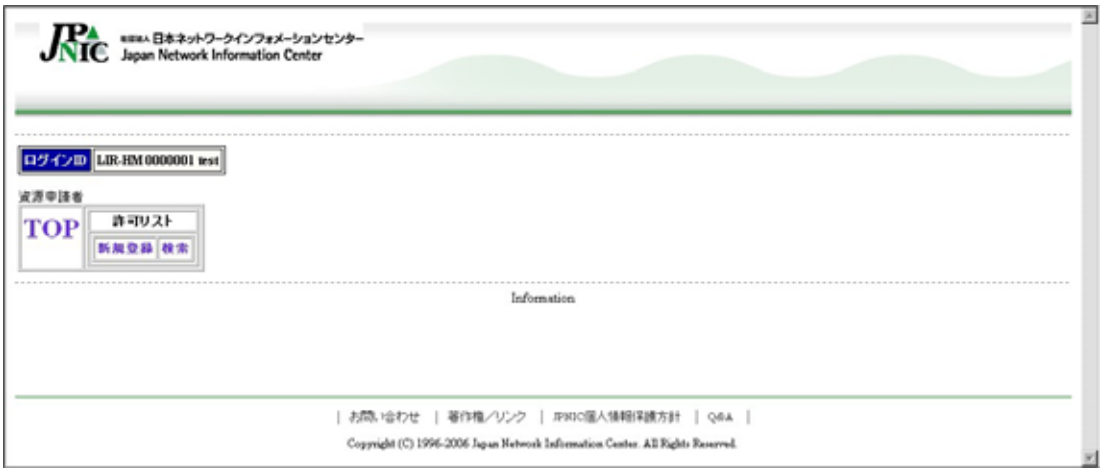
（15） エラー表示



エラー一般の表示を行う画面。エラーの内容を表示する。

4.8.1.3. 資源管理者用インターフェース

（1）　トップ画面



利用者が最初に本機構にアクセスした際に表示する画面。SSL クライアント認証を行った利用者の証明書から CN 属性を取得し、ログイン ID として表示する。画面上部のリンクをクリックし、許可リストの管理を行う。

（2）　許可リスト登録

許可リスト情報を入力する。自身が管理する Prefix のみ設定が可能である。自身の管理外のものについてはエラーとし、登録できない。その検証のため、資源管理 CA クライアント証明書のプロファイルに対応する資源管理番号により割り振り済みか否かのチェックを行う。また、JPNIC 担当者の許可リスト登録時と同様に、Prefix について以下の入力チェックを行う。

- 同一のメンテナー名かつ同一の許可・禁止区分で、登録済み許可リストと範囲が重なる Prefix がある場合、エラーとし登録不可とする。
- 同一のメンテナー名で、「禁止」の登録済み許可リストの範囲に含まれるまたは等しい Prefix がある「許可」を新規登録しようとした場合、エラーとし登録不可とする。
- 同一のメンテナー名で、「許可」の登録済み許可リストの範囲を含むまたは等しい Prefix がある「禁止」を新規登録しようとした場合、エラーとし登録不可とする。

メンテナー名について以下の入力チェックを行う。

- 指定されたメンテナー名が JPIRR のメンテナーオブジェクトとして存在する。

AS 番号については、１つの許可リストにつき最大１００件まで登録可能とする。
「登録」ボタンをクリックすると「許可リスト確認」に遷移する。

（3）　許可リスト登録確認

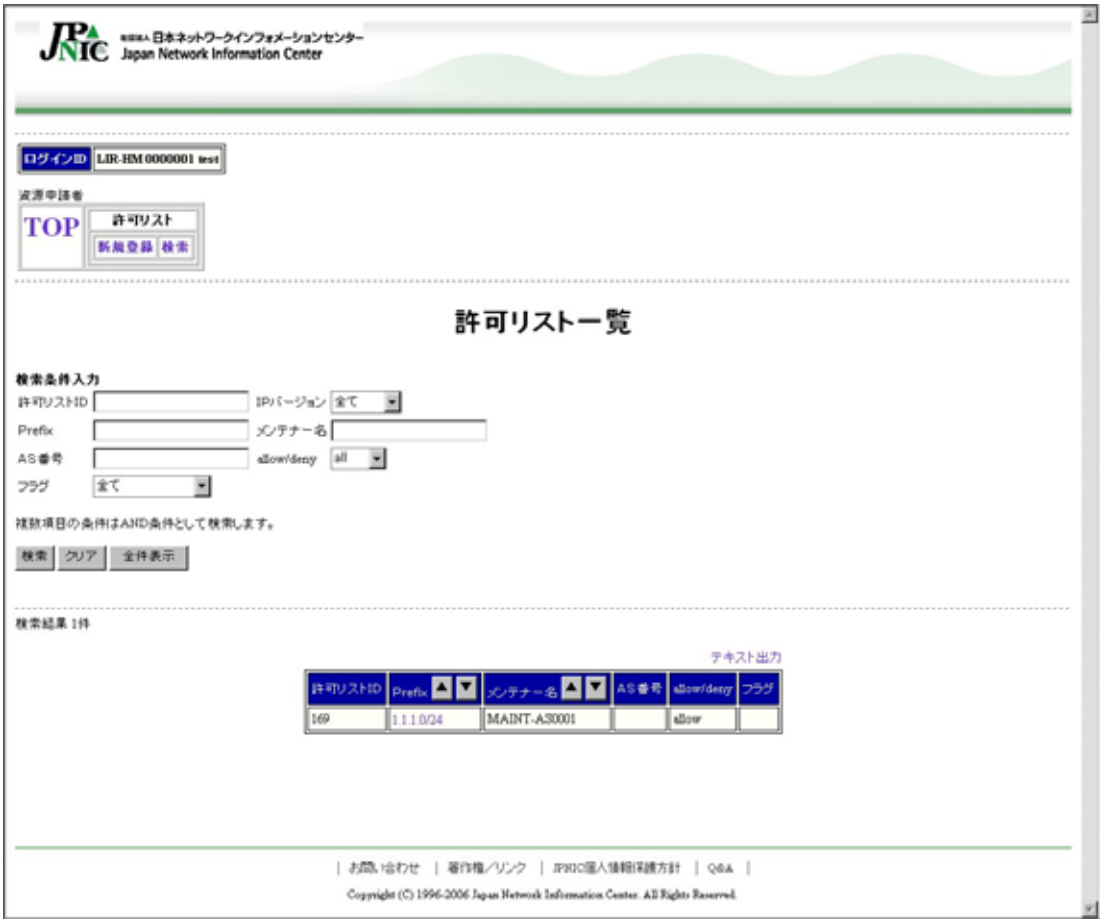
許可リスト登録の確認画面を表示する。

「登録」ボタンをクリックすると「許可リスト完了」に遷移する。

（4）　許可リスト登録完了

許可リスト登録の完了を知らせる。登録された許可リストの内容を表示する。「続けて登録する」をクリックすると「許可リスト登録」に遷移する。

（5） 許可リスト一覧



「許可リスト検索」、「許可リスト一覧」で入力された検索条件に該当する許可リストの情報を取得し表示する。

「検索」ボタンまたは「全件表示」ボタンをクリックすると「許可リスト一覧」に遷移する。

「Prefix」の横の▲をクリックすると検索結果を Prefix の昇順で表示する。

「Prefix」の横の▼をクリックすると検索結果を Prefix の降順で表示する。

「メンテナー名」の横の▲をクリックすると検索結果をメンテナー名の昇順で表示する。

「メンテナー名」の横の▼をクリックすると検索結果をメンテナー名の降順で表示する。

「Prefix」をクリックすると「許可リスト変更」に遷移する。

（6） 許可リスト変更

許可リスト情報を変更する。任意の Prefix に対して許可リストを登録することができる。Prefix とメンテナー名については「許可リスト登録」と同じ入力チェックを行う。

「変更」ボタンをクリックすると「許可リスト変更確認」に遷移する。

「削除」ボタンをクリックすると「許可リスト削除完了」に遷移する。

（7） 許可リスト変更確認

許可リスト変更の確認画面を表示する。

「登録」ボタンをクリックすると「許可リスト変更完了」に遷移する。

（8） 許可リスト変更完了

許可リスト変更の完了を知らせる。変更された許可リストの内容を表示する。

「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

（9） 許可リスト削除完了

許可リスト削除の完了を知らせる。削除された許可リストの内容を表示する。

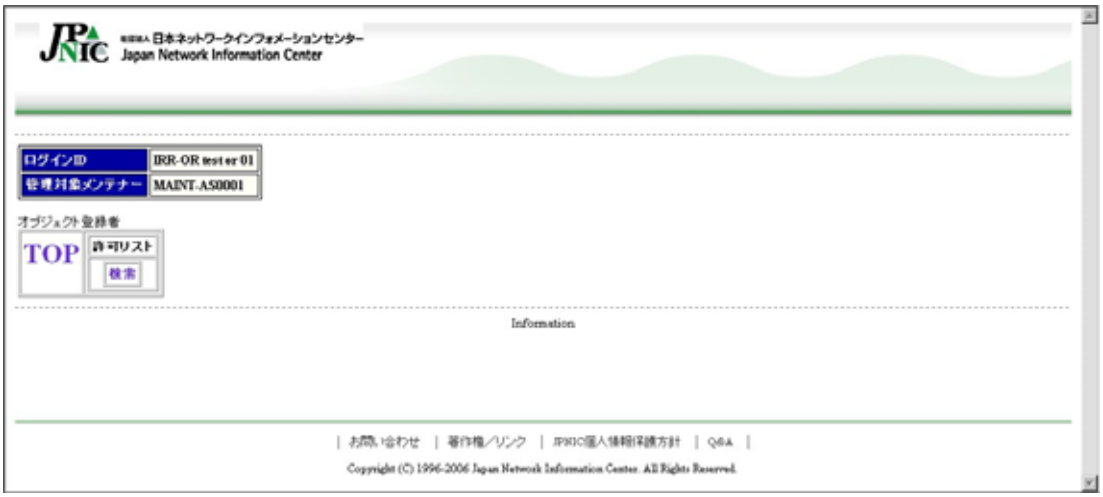
「一覧へ」ボタンをクリックすると「許可リスト一覧」に遷移する。

（10） 許可リストテキスト表示

「許可リスト一覧」に表示されている許可リストの情報を取得し表示する。

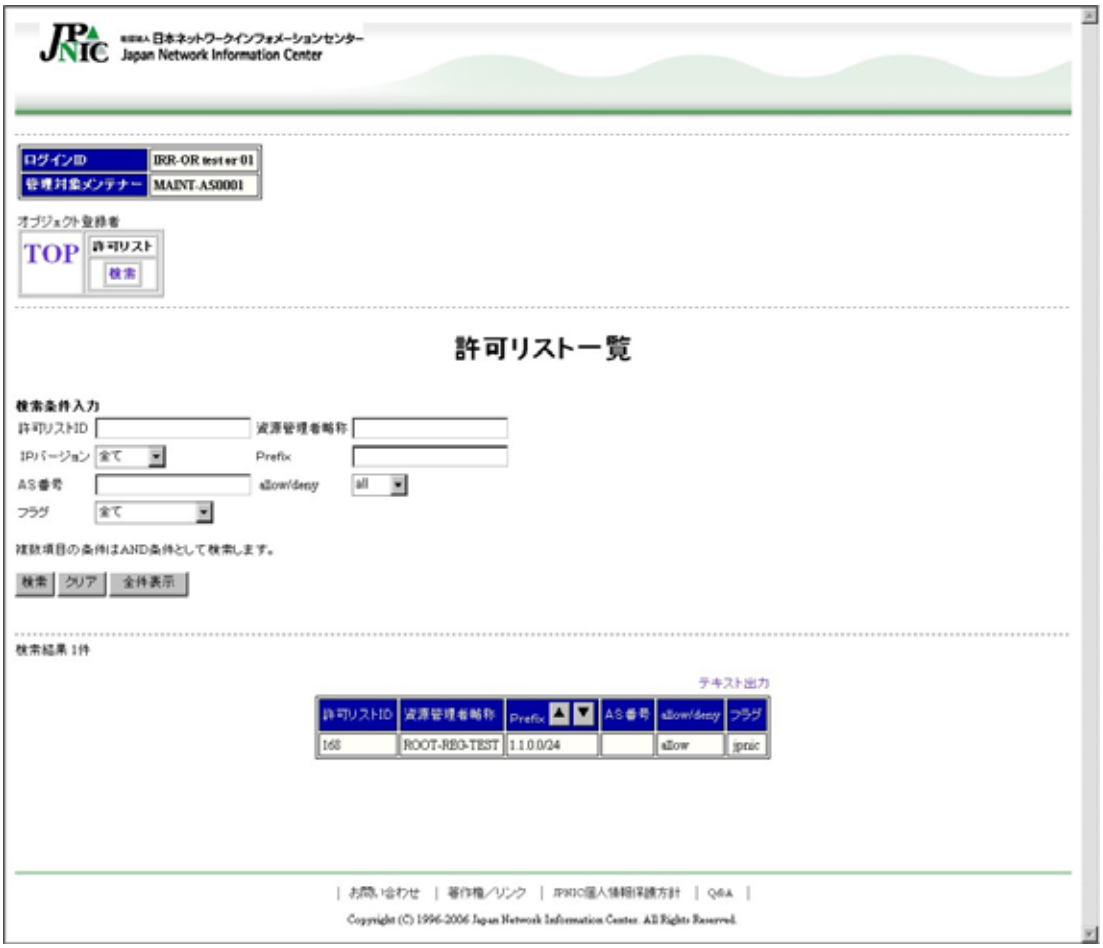
4.8.1.4. オブジェクト登録者用インターフェース

（1）　トップ画面



利用者が最初に本機構にアクセスした際に表示する画面。SSL クライアント認証を行った利用者の証明書から CN 属性、OU 属性を取得し、ログイン ID、管理対象メンテナーとして表示する。画面上部のリンクをクリックし、許可リストの検索を行う。

（2）　許可リスト一覧



「許可リスト一覧」で入力された検索条件と利用者の管理対照メンテナーに該当する許可リストの情報を取得し表示する。

「検索」または「全件表示」をクリックすると「許可リスト一覧」に遷移する。

「Prefix」の横の▲をクリックすると検索結果を Prefix の昇順で表示する。

「Prefix」の横の▼をクリックすると検索結果を Prefix の降順で表示する。

（3）　許可リストテキスト表示

「許可リスト一覧」に表示されている許可リストの情報を取得し表示する。

（4）　証明書の取得

オブジェクト登録者用証明書の取得を行う。

アクセスキーを入力し「証明書発行」ボタンをクリックすることで、認証を行い「証明書発行完了」に遷移する。

（5）　証明書発行完了

オブジェクト登録者用証明書の発行が完了したことを表示する。

4.9. 今後の課題

当初望ましい機能としてあげられたが、スケジュール、費用、その他の理由により本システムでは実装の対象外とした事項があった。以降にまとめると共に、その対処方針を示す。

4.9.1. 利用者の管理業務について

○JPNIC 担当者の利用者情報管理機能

JPNIC 担当者のアカウント情報の管理や証明書の発行・失効などは、その対象数や実行頻度が少ないことが予想される。そのため、本機構では専用の Web 画面を構築せず、スクリプトなどのコマンド実行により行うこととする。

○アカウント情報一覧のページング・ソート

本機構では、扱うアカウント件数が少ないため、一覧結果のページング機能、及び任意のソートキーによるソート機能は行わない。

○アカウント情報の削除

本機構では、扱うアカウント件数が少ないため、一度登録したアカウント情報は削除しないこととする。

4.9.2. 許可リストの管理業務について

○許可リストの大量登録・一括削除

大量登録または削除が必要な場合は RDB を直接操作するなど運用で対応することとする。

○例外的な許可リストの設定

許可リストの設定で、資源申請者は自身に割り振られていない Prefix に対する許可リストの設定はできない。例外的な許可リストが必要な場合は、JPNIC 担当者に連絡し、代理登録を依頼するなど運用で対応する。

○隣接する複数の Prefix を持つ許可リスト設定時の問題

route または route6 オブジェクトを登録する際、その Prefix のチェックは許可リスト１件毎に行われる。従って、隣接する Prefix を持つ複数件の許可リストをまたぐ範囲が指定されたオブジェクトの登録はできない。この場合、許可リストの設定で、隣接する Prefix を持つものを１件にまとめるか、オブジェクトの Prefix を許可リストの Prefix 以下の範囲で分割する必要がある。

また、許可リストを登録する際に IP レジストリシステムで割り当て済み Prefix をチェックする際も同様の問題がある。この場合、IP レジストリシステムの登録を１件にまとめるか、許可リストを分割して登録するか、JPNIC 担当者により例外的な許可リストとして登録する。

○整合性チェックの運用方法

本機構では整合性チェックができる機能の提供までとする。チェックの実施方法およびチェック結果の通知や反映については別途検討が必要である。

○IP レジストリ管理業務との連携について

IP レジストリで管理されるアドレス空間の割り振り状況については、もれなく許可リストに反映されていることが望ましい。たとえば、IP レジストリシステムに対して新たにアドレス空間が割り当てられた際に、許可リストにも自動的に反映される機能や、IP レジストリシステムの割り振りと許可リストの登録状況の対応をグラフ表示などで簡単に確認できる機能等の検討が必要である。

本機構では、既存業務およびシステムに対してはなるべく影響を与えない部分的な範囲で検討したが、上記のためには、IP レジストリ管理業務を含めた業務フローの見直しや各システム間のより密接な連携方法の検討が必要である。

4.9.3. JPIRR オブジェクトの管理業務について

○既存の経路を使ったオブジェクト登録の併用

本機構は実験運用のため、オブジェクト管理は既存の方法（本機構を通さず、直接 JPIRR に所定のメールを送信しオブジェクト管理する方法）との併用とする。従って、本機構稼働後も直接 JPIRR の情報を管理することが可能であるが、これについての制限は行わない。

○メール I/F プログラムの起動方法について

本機構のメール I/F プログラムを逐次起動とした場合、JVM の同時起動のメモリ容量やパフォーマンスの問題、及び S/MIME メールを STDIN で受けてハンドリングする場合の実現方法についての調査・検討によるスケジュール・費用に影響があるため、本機構では定期起動によるメールの取得とする。

その際に、実運用時の処理データ量と Web インターフェースを含む全体的なシステム負荷を検討し、起動時間の間隔をできる限り短くするようにチューニングし、また、一時的に負荷があがった状態になっても重複処理がおきないようにアプリケーション内部で対応をすることとする。

4.10. まとめ

経路情報の登録機構の構築にあたり、「本機構に対する認証機能の強化」、「不正なユーザ登録の排除」、「JPIRR の登録情報とアドレス資源管理との整合性の維持」を目的としてきた。これらの実現に向け、本機構内に新たに構築した JPIRR 認証局とそこから発行されるクライアント証明書を使用して、本機構 Web インターフェースに対するクライアント認証とオブジェクト登録時の S/MIME によるメールの暗号化とメッセージ認証を実現した。また、クライアント証明書記載内容にしたがって、本機構の使用可能機能を制御するアクセスコントロールを行った。さらに、許可リスト登録時の IP 指定事業者への割り振り済み Prefix 範囲のチェックと、オブジェクト登録時の許可リストを使用したメンテナー毎のルールに従ったオブジェクト操作内容のチェックを行うことで、不正利用者による JPIRR への誤情報の登録を排除し、JPIRR の登録情報と IP レジストリシステムとの整合性の確保を果たすことが出来ると考えられる。