

経済産業省受託調査研究

電子認証フレームワークとIPアドレス 認証の展開に関する調査報告書

2007年3月

社団法人日本ネットワークインフォメーションセンター

電子認証フレームワークと
IP アドレス認証の展開に関する
調査報告書

2007 年 3 月

社団法人日本ネットワークインフォメーションセンター

はじめに

電子証明書の普及が進まないと言われて久しい。日本政府の電子入札システムや地方自治体の公的個人認証基盤、電子署名法の認定認証業務に基づく電子証明書など、電子証明書の発行数が多い分野は存在するものの、必要に迫られずに日常生活の中で電子証明書（クライアント証明書）が使われる場面は未だに少ないのではないだろうか。

2007年3月18日にサービスが開始したICカード乗車券は、電車やバスに乗れるだけでなくコンビニエンスストアでの支払いなどにも対応している。日常生活の中で利用可能な場面が多い。非接触ICカードの場合、特にX.509形式の電子証明書の取り扱いに関しては暗号モジュールの安全性に関して一定の評価を得ていないものの、高度な認証技術が多くの場合で簡単に利用されるようにした意義は大きい。

これはコンピューター技術やインターネット技術においてはしばしば注目される点であるが、ユーザの利便性を向上させかつ利用場面が増える状況を作るには、「相互運用性」と「インターフェースの整理」が重要である。例えばICカード乗車券の場合には、読取装置に対するICカードの相互運用性がある。またどのICカード乗車券でも同一の読み取りインターフェースがあって整理が進んでいる。インターフェースが十分に整理されていれば、別のメーカーの読取装置であっても同じカードが利用できるはずである。

電子証明書の利用場面を増やし適切に普及させていくには、電子証明書やPKI（Public-Key Infrastructure）の「相互運用性」の確保と「インターフェースの整理」が必要なのではないかと考えられる。電子証明書自体のインターフェースを単純化して整理することは難しいが、相互運用性があるような「電子証明書の意味」を整理し、策定することは可能であろう。

電子証明書の利用用途に応じた整理は、電子認証におけるノウハウの蓄積がなければ難しい。本調査研究は電子認証に関するノウハウの蓄積を進め、より多くの利用場面で役立つような電子認証を作り出していくことが本調査研究の狙いである。

はじめに

目次

1. 本調査研究の背景と位置づけ	1
1.1. 2006 年度の調査研究の位置づけ	1
1.2. 調査研究の活動と本報告書の内容について	2
2. RIR におけるアドレス資源の認可機構	5
2.1. RIPE NCC	5
2.1.1. 第 53 回 RIPE ミーティングを通じた調査	5
2.1.2. 認可機構の詳細	8
2.2. ARIN	13
2.2.1. 第 18 回 ARIN ミーティングにおける調査	13
2.3. APNIC	18
2.3.1. 第 22 回 APNIC ミーティングでの議論	18
2.4. APNIC ミーティングでの ROA と IRR に関する発表	22
2.5. まとめ	32
3. 電子認証技術と技術文書策定に関する国際動向	33
3.1. 概要	33
3.2. 動向調査の目的	33
3.3. IETF における国際動向の調査	34
3.3.1. IETF の開催状況と注目した WG の開催状況	34
3.3.2. 第 66 回 IETF	34

3.4. 電子認証フレームワークに関連する動向.....	45
3.5. PKIX WG における電子認証技術の動向.....	48
3.6. まとめ.....	57
4. 経路情報の登録機構の設計と構築.....	59
4.1. 背景.....	59
4.2. 「経路情報の登録機構」の意義.....	60
4.2.1. 機能概要.....	63
4.2.2. 利用者の観点.....	68
4.3. 経路情報の登録機構の仕組みと構成.....	71
4.4. ネットワーク構成.....	72
4.5. JPIRR 認証局設計.....	73
4.5.1. 認証局と信頼階層.....	73
4.5.2. JPIRR 認証局の論理構成.....	74
4.5.3. JPIRR 認証局のプロファイル.....	77
4.5.4. CRL (失効リスト).....	79
4.5.5. JPIRR クライアント証明書.....	81
4.5.6. JPIRR 認証局のライフサイクル.....	86
4.6. リポジトリ設計.....	89
4.6.1. オブジェクトクラス定義.....	90
4.6.2. 属性定義.....	92
4.7. 業務設計.....	94
4.7.1. 利用者管理業務.....	94
4.7.2. 許可リスト管理業務.....	108
4.7.3. オブジェクト管理業務.....	112
4.8. インターフェース設計.....	118
4.8.1. 画面設計.....	118
4.9. 今後の課題.....	174

4.9.1. 利用者の管理業務について.....	174
4.9.2. 許可リストの管理業務について	174
4.9.3. JPIRR オブジェクトの管理業務について	175
4.10. まとめ.....	176
5. 電子認証フレームワークの定義と仕組み.....	177
5.1. 電子認証に関わるノウハウの蓄積とは.....	177
5.2. 電子認証プラクティスフォーラムとは.....	178
5.3. 電子認証プラクティスフォーラムの位置づけ	179
5.4. 持続的なフォーラムのための設計	182
5.5. フォーラムの仕組みとコミュニティ構成.....	183
5.6. 電子認証プラクティスフォーラムの趣意と基本的な BCP	186
5.7. フォーラムのドキュメント策定プロセス.....	189
5.8. フォーラムの為のシステム提供.....	192
5.9. 議論と策定が必要な BCP	193
5.10. まとめと今後の課題.....	194
6. 電子認証フレームワークと IP アドレス認証の展開の今後	197
6.1. これまでの IP アドレス認証と電子認証フレームワーク	197
6.2. IP アドレス認証の今後と電子認証フレームワーク	199
6.3. 今後の課題と活動.....	200
Appendix. 1 JPNIC 資源管理認証局 認証業務規程 英語訳	
Appendix. 2 JPNIC 認証局証明書 利用規約 英語訳	

第 1 章 本調査研究の背景と位置づけ

内容

- 調査研究の位置づけ
- 調査研究の活動と本報告書の内容

1. 本調査研究の背景と位置づけ

本調査研究は 2005 年度から 3 年度の計画で実施している「電子認証フレームワークと IP アドレス認証の展開に関する調査研究」の 2 年目である。「電子認証フレームワーク」とは電子認証に役立つ BCP (Best Current Practice) によって電子認証の分類やレベルを整理する枠組みを意味する。また「IP アドレス認証」は 2005 年度までに JPNIC において構築されてきた「IP アドレス認証局」を中心とする認証基盤を使った電子認証のことで、IP アドレスに関する登録情報を使った電子証明書を利用する点に特徴がある。この 2 つは一見別々のテーマのように見えるが、本質的には密に関連するテーマである。

本章では、本調査研究の進め方、重点、年度ごとの活動について述べ、最後に本報告書の章立てについて述べる。

1.1. 2006 年度の調査研究の位置づけ

本調査研究は、インターネットレジストリである JPNIC における認証基盤の構築と電子認証の適切な普及に必要な BCP を策定する仕組み作りの 2 つのアプローチを行う調査研究である。本調査研究のポイントは 2 つある。一つは IP アドレス認証の展開と電子認証フレームワークの各々を確立することである。もう一つは IP アドレス認証の展開によって構築された認証業務を電子認証フレームワークの中で整理し、ノウハウをドキュメント化して残していくことである。本調査研究の進め方は、はじめに各々を別個に進め、最終的にドキュメントにまとめるような形となる。

本調査研究は次に述べるような進め方で実施している。はじめに諸外国におけるドキュメント策定プロセスを調査し、電子認証フレームワークの要件を調査する。次にこのフレームワーク自体をドキュメントとして策定するための仕組み「電子認証プラクティスフォーラム」の試験的な設置を行い、専門家による議論を通じてノウハウとなるドキュメントの策定を行う。一方、「IP アドレス認証の展開」は次のように進める。はじめにインターネットレジストリにおける登録情報を利用した電子認証の役立つ分野について調査する。次に必要とされる認証局や関連システムを構築し、実験的な運用を行う。最後にこれらの電子認証の有効性が確認し本運用に向けた検討を行う。

2005 年度は、電子認証フレームワークと IP アドレス認証の展開の両方のあり方について調査研究を行った。電子認証フレームワークについては諸外国における BCP に近いドキュメントの策定プロセスについて調査を行い、日本国内での BCP の策定に対する要求事項などについてまとめた。IP アドレス認証の展開については、インターネットにおけるルーティングの安全性向上に役立つ電子証明書とルーティングプロトコルについて調査を行った。

第1章 本調査研究の背景と位置づけ

2006年度は、電子認証フレームワークに関する活動よりもIPアドレス認証の展開を先行させ「経路情報の登録機構」の開発を行った。これは本機構の実験運用を先行させることで、JPNIC内での電子認証に関するノウハウの蓄積が早まると考えられたためである。電子認証フレームワークについては専門家との議論を進め、フレームワークを策定するためのオープンなフォーラムである「電子認証プラクティスフォーラム」の具体化を進めた。

1.2. 調査研究の活動と本報告書の内容について

2006年度はドキュメント策定プロセスに関する調査と電子認証技術の動向、RIRにおけるIPアドレスに関する登録情報のセキュリティなどについて調査研究を実施した。本節では、それぞれの活動とテーマの関連性と、本報告書でのまとめ方について述べる。

- **RIRにおける登録情報データベースの動向調査**

2006年度、APNIC、RIPE NCC、ARINといった主要なRIRでは本調査研究と時期を同じくしてIPアドレスの経路制御に対する認可に関する議論が行われていた。主要なRIRのミーティングとIETFの関連するWGに参加し、現地の職員と情報交換を行うなどして詳細の調査を行った。調査の結果を第2章にまとめた。

- **ドキュメント策定プロセスについての調査**

国外では主にIETFのミーティングに参加し、また国内ではJANOGやJPOPMといったミーティングに参加し、オープンなミーティングやコミュニティでのドキュメント策定プロセスについて調査を行った。2006年度は次に述べる「経路情報の登録機構」の開発に重点を置いたため、この調査は技術最新動向に関する調査の一環として行う程度に留まった。主にIETFでの議論について第3章にまとめた。

- **電子認証技術の動向に関する調査**

主にIETFのミーティングに参加し、電子認証技術の最新動向について調査した。また近年の状況をわかりやすくするため、4.5年前以降からの動向とここ1年の動向という形でまとめなおし、電子認証技術の標準化で取り組まれている技術分野の変化などについて第3章にまとめた。

- **「経路情報の登録機構」の設計と開発**

RIRにおけるアドレス資源の認可機構、およびAPNICにおけるリソース証明書動向を受け、IPアドレス認証の展開の為に「経路情報の登録機構」の開発を行った。認証局システムの開発を伴うため、2006年度はこの活動に重点を置いた。詳細を第4章にまとめた。

- **電子認証フレームワークの定義と仕組みの検討**

国内外での電子認証の普及状況を鑑み、専門家との議論を通じて整理が進んだ電子認証フレームワークの定義や仕組みについてまとめた。フレームワークを策定する活動「電子認証プラクティスフォーラム」と、フォーラムの活動を実現するための要件とシステム構築について第 5 章にまとめた。

第 6 章では、電子認証フレームワークと IP アドレス認証の展開の今後の関わり方について整理し、調査研究の方向性を交えてまとめた。

また RIR や IETF での情報交換のなかで、JPNIC の認証局や本調査研究に対する関心は高いと感じる場面がたびたびあった。そこで JPNIC 認証局に関する情報提供のため、JPNIC の資源管理認証局（前 IP アドレス認証局（認証））の CPS（Certification Practice Statement）と、認証局証明書利用規約を英訳した。これらは Appendix として本報告書の最後に掲載する。

第 1 章 本調査研究の背景と位置づけ

第2章 RIRにおけるアドレス資源の認可機構

内容

- RIPE NCCにおける認可機構
- ARINにおける認可機構の議論
- APNICにおけるリソース証明書

ほか

2. RIR におけるアドレス資源の認可機構

2005 年度の調査研究を通じて、インターネットにおける大規模な不正利用排除にはアドレス資源の認可機構が重要であることが判明した。

RIR (Regional Internet Registry - 地域インターネットレジストリ)のうち、ヨーロッパ地域の RIPE NCC、北米地域の ARIN、アジア太平洋地域 APNIC は、JPNIC と同様に IP レジストリシステムと IRR (Internet Routing Registry) を持っているが、アドレス資源の認可に対する考え方が各々に異なっている。

これらの主要 RIR で現地調査を行い、アドレス資源の認可機構とアドレス資源情報のセキュリティ、およびリソース証明書の動向について調査した。リソース証明書はアドレス資源の利用認可を電子証明書を使って行うもので、主に APNIC が中心となって開発が進められている。

2.1. RIPE NCC

RIPE NCC はヨーロッパ地域の IP アドレスの管理を行っている地域インターネットレジストリである。RIPE NCC は 1 年に 3 回 RIPE ミーティングと呼ばれるミーティングを開いており、ここではデータベースのセキュリティや IP アドレス管理ポリシーなどについて議論されている。リソース証明書についての議論も開始している。そこで第 53 回 RIPE ミーティングに参加し、また現地のスタッフにヒアリングを行ってこれらについての動向を調査した。

2.1.1. 第 53 回 RIPE ミーティングを通じた調査

2006 年 10 月 2 日～6 日にオランダのアムステルダムで開かれた第 53 回 RIPE ミーティングに参加した。今回は、セキュリティに関する議論の動向を調べるとともに、RIPE NCC のスタッフに、RIPE データベースの仕組みや課題についてヒアリングを行った。

第 53 回 RIPE ミーティングでは、初日に主に LIR (Local Internet Registry) 向けのチュートリアルが行われ、初日から 3 日目にかけて全体会議である Plenary が行われた。3 日目以降は WG のセッションが開かれた。ミーティングの参加登録者は 355 名で、ここ 1 年ではほぼ平均的な人数である。

セキュリティに関しては、全体会議である Plenary と NCC Services WG でリソース証明書に関する議論が、Database WG で IRT オブジェクトと CRYPT-PW を廃止する案についての議論が行われた。

リソース証明書に関して

リソース証明書については、Plenaryをはじめ複数のWGで議論が行われていた。リソース証明書はIPアドレスやAS番号が入った電子証明書¹で、WHOISの代わりにIPアドレスの割り振りや割り当てを証明するために使われる。IPアドレスの割り振り構造に従って発行され、そのツリー構造の末端部分ではIPアドレスとAS番号の両方が入った電子証明書が発行される。この電子証明書はBGPなどにおける経路制御を安全にするために使われることが想定されている²。リソース証明書の実装は、2006年4月頃よりAPNICとRIPE NCCが中心となって進められてきた。

Plenary では、APNIC の Geoff Huston 氏によって、リソース証明書を使って IRR の登録情報に電子署名を行うデモが行われた。この電子署名は IRR の route-set オブジェクトに対して行われるもので、その route-set オブジェクトに含まれる route オブジェクトが authorize(認可)されたことを意味している。route オブジェクトには広告元(すなわちそのアドレスを持つノードの収容先)となる AS 番号が記載されているため、LIR がその AS に対してインターネットでその IP アドレスを使うことを認可した、という意味になる。この認可の概念は ROA(Route Origination Authorization)と呼ばれている。インターネットレジストリの割り振りを意味するリソース証明書は 2006 年 7 月の時点で既に実装されていたので、この ROA を示すリソース証明書の発行によって、ツリー構造の最上位から末端までのすべてのリソース証明書が発行できる状況になったことになる。

Plenary の会場では、このプログラムが無事に動作したことに対して拍手が送られる一方、リソース証明書の発行に使われるデータベースが信頼に足るかどうかという根本的な疑問が投げかけられた。リソース証明書自体が信頼できる仕組みであっても、証明書の元になるデータが間違っていたら意味がないからである。RIPE NCC では既にこの点に着目しており、リソース証明書の導入に関して、予測される効果やインパクトを評価する活動が提案されている。この活動は NCC Services WG で発表されていた。

2007 年度の RIPE NCC の活動計画によると³、RIPE NCC では 2006 年度の APNIC の実装プロジェクトへの参加は継続され、リソース証明書に着目した活動が行われていくとされている。NCC Services WG での RIPE NCC の Alex Pawlik 氏の発表では、2007 年度の本格的な活動に先立って、Evaluation Task Force(評価タスクフォース)⁴の立ち上

¹ RFC3779

<http://www.ietf.org/rfc/rfc3779.txt>

² Secure Border Gateway Protocol(S-BGP)

--- RealWorldPerformanceandDeploymentIssues

<http://www.ir.bbn.com/sbgp/NDSS00.S-BGP.ps>

³ Newor Significantly Developed Activitiesfor2007

<http://www.ripe.net/ripe/draft-documents/gm-october2006/ap-2007.html#3>

⁴ RIPE Certification Task Force

げが提案されていた。この評価は必要となる業務の詳細やポリシーへの影響を明らかにすることが目標になっている。Evaluation Task Forceは現行の開発活動やトライアルに参加しつつ、まずリソース証明書が持つ目標とその目標に現行のアプローチが適するかどうかを調査して報告することになっている。最終的には2007年5月に予定されている第55回RIPEミーティングで、導入の方向性について決定が行われることとなる。

これは、これまで実装を行ってきたAPNICをはじめ、リソース証明書の効果に対して同様の疑問が投げかけられているARINコミュニティ、そして認証局に関する調査研究を行ってきた当センターにとっても注目すべき活動である。というのもRIPE NCCのデータベースは、アドレスの割り振り/割り当て情報を登録するデータベースと経路に関する情報が登録されるIRRが統一されている上に、インターネットで経路広告されているアドレスとIRRの登録情報を比較する調査プロジェクトが行われてきていることが背景にある⁵。これによって、RIPE NCCでは、登録されているにもかかわらず実際には使われていないアドレスを調べることが可能である。使われていないアドレスや登録情報と異なる経路広告の量がわかれば、リソース証明書が現状で何割程度のアドレスに対して発行できるのか、またそれらの管理が現実的なものなのかどうか判明する可能性がある。

RIPE データベースのセキュリティ機能に関して

RIPE データベースには、ユーザ認証やユーザが編集できる登録情報の範囲を限定するようなデータベースを保護する機能の他に、あるアドレスで起こったコンピューターインシデントに関する連絡先となるIRT(Incident Response Team)の情報を提供するという、コミュニティのセキュリティを考慮した機能がある。

ここではRIPE ミーティングの5日目に行われたDatabase WGの議論の中から、ユーザ認証の機能であるCRYPT-PWの廃止に関する提案と、IRT情報を提供するIRTオブジェクトに関する議論を紹介する。

RIPEデータベースはLIRに対して4つの認証方式を提供しており、ユーザは好きなものを選んで使用できるようになっている。現在提供されている認証方式は、CRYPT-PW、MD5-PW、PGP-KEY、X509で、CRYPT-PWとMD5-PWはいわゆるパスワード認証方式である(2007年3月現在、CRYPT-PWを使った認証は廃止の方向で活動が進められている)。LIRがメールで申請業務を行う場合、送信するフォームの中であらかじめ登録されているパスワード文字列を記入する。パスワード文字列が正しければ、RIPEデータベースはユーザ本人によって送信されたと判断でき、申請内容のチェックに移ることができる。-PWの前についているCRYPTとMD5は、パスワード文字列をRIPEデータベースの中で処理する方式の名前である。CRYPTは昔のUNIXでパスワード文字列を隠蔽す

<http://www.ripe.net/ripe/tf/certification/index.html>

⁵ Routing Registry Consistency Check Project

<https://www.ripe.net/projects/rcc/index.html>

第2章 RIR におけるアドレス資源の認可機構

るために使われていた方式で、パスワードとして指定できる文字の長さは8文字である。一方、MD5 はメッセージダイジェスト関数のMD5 を用いた方式で、RIPEデータベースでは65文字のパスワードをつけることができる⁶。

今回の提案は、CRYPT-PW で利用できる文字列が短いために、ブルートフォース攻撃(総当たり攻撃)や辞書攻撃といった基本的な攻撃が通用してしまうため、今後この方式の利用を廃止しようというものである。既に第52回 RIPE ミーティングで基本的な方針についてはコンセンサスが得られており、今後はスケジュールについて検討したいとのことであった。しかし、約2300のメンテナーでCRYPT-PWが使われているそうで、完全な廃止にはやや時間がかかりそうである。また変更手続きが間に合わなかったユーザへの対応なども検討する必要があると考えられる。

一方、IRT オブジェクトに関する議論は潜在的な問題を抱えたままの提案となった。今回の提案は WHOIS を使って、ある IP アドレスを元に inetnum オブジェクトが検索された場合、検索時のオプションに-c が指定されていなくても WHOIS のサーバは関連する IRT オブジェクトを返すというものである。従って WHOIS で IP アドレスを調べるだけで IRT オブジェクトが自動的に表示されるようになる。このことはユーザの観点では便利になるという意味でとてもよいことである。また IRT オブジェクトは一度一つのメンテナーに対して定義しておけば、そのメンテナーによって管理されている割り振り/割り当て情報のすべてに対して適用されるという意味で、LIR にとっても利便性は高いと言える。そのため RIPE NCC では IRT オブジェクトの利用を推奨している。

IRT オブジェクトの普及に関する潜在的な問題は abuse-mailbox という類似した連絡先情報の存在である。abuse-mailbox は inetnum や inet6num といった個々の割り振り/割り当て情報に付加される情報で、そのアドレスブロックにおける abuse(不正や不具合に対する連絡)用のメールアドレスが記載されている。abuse-mailbox は2004年1月の第47回 RIPE ミーティングで採用されたもので、それ以降多くの inetnum/inet6num で登録されてきた。一方、IRT オブジェクトは100程度に留まっており、利用されているものは60程度に留まっている。しかし両者共に効果が見えにくいことなどから、議論の余地が大きく、RIPE のコミュニティの中でも扱いにくい話題になっているようである。

2.1.2. 認可機構の詳細

RIPE NCC では route object の authorization 機構に関するヒアリングを行った。その結果、RIPE データベースは IP アドレスの割り振り/割り当て情報と IRR が統合さ

⁶ Crypted password generation
<https://www.ripe.net/cgi-bin/crypt.cgi>

れたシステムであるだけでなく、LIRがAS管理者に対して経路情報(route オブジェクト)の登録認可する機構を備えていることがわかった。この機構によって、IPアドレスの割り振り先とASの運用が別の組織によって行われていても、どのIPアドレスがどのASから経路広告されるのかが、絞り込めるようになっている。

他の組織によって間違っただけの経路広告をされてしまうことで、本来は自分のネットワークで使われるべきIPアドレスが使えなくなってしまうことは「経路ハイジャック」と呼ばれている。これを検出し防止するためには、RIPEデータベースが持つ機構は有効である。この後の調査で、ARINのコミュニティでもIPアドレスとAS番号の組み合わせがわかる仕組みが提案されていることがわかった。

ヒアリングの目的

JPNICの「経路情報の登録機構」はroute objectの登録者をauthorization(認可)する機構を通じて、IRRの提供する経路に関する情報の信頼性向上を図るものである。本機構はAPNIC、RIPE NCCで検討が進んでいるリソース証明書の原本となると考えられるが、APNICからは特にauthorizationに関する見解が見えない。認可機構を持つRIPE NCCの仕組みを調査し、経路情報の登録機構を設計することの意義の正しさを確認する。また本機構の開発にあたって参考になる認可の仕組みのもつ課題や今後の展開についても調査を行うことを目的とした。

ヒアリングの結果

ヒアリングの結果は3つのポイントにまとめられる。

a. RIPEデータベースにおける認可機構

RIPE NCCのデータベースは認可機構を持っており、これまでも運用されていた。RIPE NCCのデータベースはメンテナーと呼ばれる認証情報を用いてユーザ認証と割り振り済みIPアドレスおよび割り当て済AS番号等の管理が行われている。認可はLIRのメンテナーと登録者のメンテナーにおける認証(例えばPGPを使った電子署名)の両方が行われなければ登録されない、というものである。登録される情報自体に認可情報が記載されていることになる

b. 運用上の課題

登録済のroute オブジェクトのうち、管理者が不在になったものが削除されてこなかった。そのため本来は使われていない経路の情報が登録されたままとなり、これをインターネット上の経路情報と比較すると不整合または余計な登録情報となる可能性がある。

第2章 RIRにおけるアドレス資源の認可機構

項目 a で述べた mnt-route 及び mnt-by は、別々のメンテナーである。どちらかの組織がISP事業をやめた場合、route オブジェクトは本来の意味では不適切な登録であり、削除する必要がある。しかしこの削除によって起こる影響、つまり IRR として参照された場合に重要な経路情報が伝達されなくなる状況を懸念して削除されることにはなっていない。

このことで不要な route オブジェクトが存在し続けている状況がある。aut-num オブジェクトの mnt-by に指定されたメンテナーの LIR が ISP 事業をやめた場合にその aut-num オブジェクトが削除されないことも指摘されていた。これは一度取得された AS 番号は基本的に再利用されず、消費し続けられることになる。

c. ポリシー実施の課題

LIR の解約の際などに割り振り済および認可済 route オブジェクト及び AS オブジェクトの削除が実施されてこなかった。登録上明らかに削除できるものは一括削除できるものの、これまでは特に行われてこなかった。これは AS 番号の枯渇の一因になっている。しかし 32bit 化の提案があることから、RIPE NCC IP アドレス管理部門では特に問題視されていない。技術部門のスタッフは不要な route オブジェクトが残存することに対して懸念を示しており、今後の課題だと結論付けていた。

認証対象について

メンテナーには admin-c (運用責任者) tech-c (技術連絡担当者) の連絡先がそれぞれ複数登録可能である。登録される情報は nic-hdl と呼ばれ、これがユーザー一人に使われるか、複数のユーザによって使われるかは規定されない。

nic-hdl として person オブジェクトが指定された場合であっても、role オブジェクトという person オブジェクトを複数指定できるオブジェクトの場合でも、各々が複数のユーザによって使われるかどうかはケアしないという方針である。

認証する方式はメンテナーで指定される。使用される方式は CRYPT-PW, MD5-PW, PGP-KEY, X509 である。申請を送付しているユーザが前述した person であるかどうかはケアされず、純粋に認証方式に準じた確認が取れば認証を完了する仕組みである。

認可に使われるメンテナーの指定について

割り振り済 IP アドレスおよび再割り振り済の IP アドレスは inetnum オブジェクトとして登録され、また割り振り済 AS 番号は aut-num オブジェクトとして登録される。これらのオブジェクトには以下のフィールドを使って管理元(すなわち割り振り / 割り当て先)が記載される。

mnt-by: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。メンテナー名は当該オブジェクトの登録時に RIPE NCC が記載する。

mnt-lower: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。mnt-lower は IP アドレスの再割り振りの際に使われ再割り振り先のメンテナー名が記載される。これは同オブジェクトの mnt-by で指定された LIR が記載する。

mnt-route: <メンテナー名>

メンテナー名によって指定されたメンテナーの権限を使って内容の変更を行うことができる。mnt-route は route オブジェクトの登録を認可する先のメンテナー名を指定するために使われる。これは同オブジェクトの mnt-by で指定された LIR が記載する。

例：

inetnum: 10.10.0.0-10.10.255.0

mnt-by: MNT-A

10.10.0.0/16 は MNT-A に割り振られ、本 inetnum オブジェクトを MNT-A が変更できることを示す。例えば、再割り振りを行うために mnt-lower の追記や管理元を増やすための mnt-by の追記、特定の AS 管理者(AS 番号の管理を行っているメンテナー)による route オブジェクトの新規登録を認可するための mnt-route の追記を行うことなどができる。

inetnum: 10.10.0.0-10.10.255.0

mnt-by: MNT-A

mnt-lower: MNT-B

mnt-route: MNT-R

10.10.0.0/16 は MNT-A に割り振られ、本 inetnum オブジェクトを MNT-A が変更できることを示す。本アドレスブロックはそのまま MNT-B に再割り振りされ、MNT-B も同様に本 inetnum オブジェクトを変更できる。

第2章 RIRにおけるアドレス資源の認可機構

mnt-route は本 inetnum に含まれる IP アドレスブロックの route オブジェクトを登録できるメンテナの指定に使われる。この指定がない場合は mnt-by および mnt-lower で指定された MNT-A, MNT-B の両方が route オブジェクトの登録できる。しかし mnt-route がある場合、MNT-R のみが route オブジェクトを登録できるようになる。

経路情報の登録機構はいわば mnt-by, mnt-lower, mnt-route をリスト形式で格納するものであると考えられる。

2.2. ARIN

ARIN は北アメリカ地域を対象とする地域インターネットレジストリである。ARIN は年に 2 回ミーティングが開かれており、データベースのセキュリティや IP アドレスポリシーに関する議論が行われている。

北アメリカ地域には、RADB⁷と呼ばれる国際的に著名なIRRがある一方、ARINでは多くのネットワークオペレーターに利用されているIRRは運用されてきていなかった。しかしIPアドレスの申請業務の電子証明書をいち早く取り入れると共に、リソース証明書に関連する議論も行われつつある。そこで第 18 回ARINミーティングに参加すると共に、関連するポリシーの提案を行っている複数の人物にヒアリングを行って調査を行った。

2.2.1. 第 18 回 ARIN ミーティングにおける調査

本調査研究で取り組んでいる「経路情報の登録機構」と同様の目的をもつ仕組みに関して、ポリシーに関するセッションにおいて議論が行われた。

この議論はPolicy Proposal 2003-3 "Capturing Originations in Templates"⁸に基づくもので、ARINの割り振り・割り当ての申請書式に、そのアドレスを経路情報として広告しうるAS番号のリストを登録できるようにするものである。登録された情報は

OriginatingASList:

という属性の値として保存され、WHOIS 等で提供されるとされている。この情報によってWHOIS 利用者が、IP アドレスの prefix と AS 番号のマッピングを得ることができるようになり、経路制御の安全性向上に寄与すると考えられている。会場での挙手の結果は、賛成：60 程、反対：30 弱であった。

以下、提案とプレゼンテーションの詳細などについて述べる。

本提案は IETF SIDR WG の chair 及び RFC4272 の著者である Sandra Murphy 氏によって、2006 年 2 月頃に ML にて行われたもので、ミーティングでの議論は前回の ARIN ミーティングで初めて行われた。今回の氏のプレゼンテーションは 150 名程の参加者がいる中で行われた。プレゼンテーションで話された内容などは以下の通りである。

⁷ RADB

<http://www.nic.ad.jp/ja/tech/glos-kz.html#03-radb>

⁸ Policy Proposal 2006-3: Capturing Originations in Templates

http://www.arin.net/policy/proposals/2006_3.html

第2章 RIRにおけるアドレス資源の認可機構

提案のモチベーション

リソース PKI と同じモチベーションで認可リストを whois の返答に含める。

ARINにおける提供方法

- ・ IRR
- ・ bulk 転送
- ・ ftp

ARINにおいて提供されないもの

- ・ データの検証

テンプレートを使う理由

- ・ オペレーターへの認可業務の啓発
- ・ IRR のデータを正確に保つ
- ・ リソース証明書に移行するためのデータ収集

IRR との違い

- ・ IRR は mnt-by を POC と同様に検証していない。
- ・ IRR は mnt-by があるが、route オブジェクトを ARIN は検証せずに登録している。

必要になること

- ・ POC と mnt-by の同期
- ・ route オブジェクトの検証

導入のインパクト

- ・ 実装に 3-6 か月かかると考えられる。

ARIN がリストに責任を持てるかどうか

- ・ これは rwhois と同じ。

議論された内容は以下の内容である。

- ・ ARIN 以外から割り振られた情報について扱えない。現行の運用を変えることに対して、目標とすることと得られることの見出せない(反対意見)
- ・ 認証対象(OrgID)と結び付ける案があるのでは。弱い認証が行われた上で登録されうる。(反対意見)
- ・ 取り組みの重要性 x 2 (賛成意見)

Policy Proposal 2006-3 の要約

参考のため、本提案の要約を以下にまとめる。

提案の主旨

IPv4 アドレス及び IPv6 アドレスの割り振り、再割り振り、割り当て、再割り振り、再割り当て等の情報に、それらを広告する AS 番号を付加した情報を収集する。

この情報は少なくとも 1 日に 1 回生成され、IP アドレスとそれを広告することが許可された AS のマッピングの為に使われる。個々のアドレスと AS 番号の組み合わせや、検索サービス等で必要とされる形式のデータの、ARIN における生成に関しても本件の対象とする。

ARIN はコミュニティの要望に応じてバルク転送やその他の形式での提供ができるようにする。再配布に関する制限はなく、再構成(repackage)も許される。なおバルク転送で提供される WHOIS データは WHOIS データへのバルクアクセスに関する AUP (Acceptable Use Policy) に従うものとする。本ポリシーは NRPM (Number Resource Policy Manual) 3.4 節に結合されると考えられる。本ポリシーは承認後 60 日以内に実装されるものとする。

提案の根拠

プリフィックスの広告元である AS(Origination of prefixes by ASes)がその広告元であることの authority を持たないことは、現在のルーティングシステムの根本的な問題となっている。認可されたプリフィックスの広告元のリストは、オペレーターの利益となる。

オペレーターの利益

- ・ 広告の偽装に対処するためのルーティングフィルターの生成
- ・ プリフィックスの広告を必要とする顧客との連携
- ・ 経路制御の問題の原因究明

ARIN はアドレス資源を IRR に変換するメカニズムを持たず、またオペレーターは (IRR の)route オブジェクトをメンテナンスする程勤勉ではないという点を考慮し、アドレス資源を管理する ARIN においてプリフィックスの広告元に関する認可の情報収集における主な目的を以下の 2 点とする。

ARIN における認可情報収集の目的

- ・ 初期及びそれに続くトランザクションを、ARIN において精密に検証できることによる利点
- ・ リソース要求等を生成するなどのオペレーターの習熟を継承することによる利点

第2章 RIRにおけるアドレス資源の認可機構

申請の書式

既存の属性

NetRange:

NetType:

追加される属性

OriginatingASList:

OriginatingASList の値はプリフィックスの広告元となる AS 番号のリストである。

登録情報のプライバシー保護に関する議論

登録情報のプライバシー保護については「2006-1: Residential Customer Privacy」⁹という提案に関して議論が行われた。

はじめに ARIN の Ray Plzak 氏によって概説があり、次に提案者の Samuel Weiler 氏によるプレゼン、続いて議論と挙手があった。

Ray 氏の概説

コンセンサス：現行のものを見直して提案すること

PPML への投稿：46、16 名参加、2 名賛成、3 名反対

Samuel 氏のプレゼン

モントリオールでのディスカッション

- より包括的なものが必要
- ARIN に対する情報提示の制限かどうかの確認
 - ARIN における影響
- 部分的な郵便番号での実施の可否
 - 極小地域での実施の難しさ
 - ARIN 地域内で司法権の及ばない地域での実施の難しさ
- 匿名となるセットをより縮小し他のデータとの相関関係により個人が特定できるようにする

議論で出た意見

- 賛成意見 3 ないし 4
 - ・現行のポリシーでは顧客のプライバシー保護に不十分
 - ・データベースの信頼性を維持できる。ただ登録されるすべてのデータは同じデータを持っていないといけない

⁹ Policy Proposal 2006-1: Residential Customer Privacy
http://www.arin.net/policy/proposals/2006_1.html

SWIP の場合部分的に登録できるのか 他

- 反対意見 5~7 (Randy Bush 氏含む) 以下その理由
 - ・ 既存の住所のデータとマスクされた公開データの違い
 - ・ 政府による利用
 - ・ ARIN が既存のデータを保持していること
 - ・ WHOIS の本来の目的に沿うべき

挙手の結果

賛成 : 8 反対 : 52

Policy Proposal 2006-1: Residential Customer Privacy の要約

参考のため、JPNIC で作成した要約を以下に載せる。

提案者 : Samuel 氏

概要

2006 年 2 月 PPML にて提案。ARIN17 での議論に引き続き 2 回目。NRPM 4.2.3.7.6 と 6.5.5.1 節に関連。(3.2 も)居住地利用を想定したユーザへのダウンストリームを行う組織は顧客名の代わりに組織名を使うことができる。"Private customer - XYZ Network"ユーザのすべてのアドレスは"Private Residence"と置き換えることができる。各ダウンストリームはアップストリームの abuse と Technical POC (Point of Contact) を WHOIS に正確に持たなければならない。

根拠

本ポリシーは顧客の住所を秘匿することができるようにする。多くの場合、郵便番号や市町名だけで個人を特定することができる。特に IP アドレスの割り振りと合わせるとポリシー提案 2003-3 の意図が覆されてしまう。

2.3. APNIC

APNIC はアジア太平洋地域の地域インターネットレジストリで、リソース証明書に関する開発プロジェクトを推進しているレジストリである。

APNIC では年に2回ミーティングが開かれており、IP アドレスに関するポリシーの議論や、NIR のシステムに関する議論が行われている。リソース証明書の開発プロジェクトが進められているため、APNIC ミーティングにおけるリソース証明書に関連するセッションでは詳しい内容のプレゼンテーションが行われるなどしている。

そこで第22回 APNIC ミーティングに参加し、動向の調査を行った。

2.3.1. 第22回 APNIC ミーティングでの議論

APNIC ではリソース証明書と呼ばれる電子証明書を発行する仕組みを作るプロジェクトが進んでいる。このプロジェクトは2006年4月頃から始まった1年間のプロジェクトで、2007年4月以降、APNIC 会員に対する試験的なサービスを始めることを目標に進められている。

本章では、リソース証明書の概要を紹介するとともに、第22回 APNIC ミーティングの参加を通じてわかってきた、プロジェクトの考え方と状況について述べる。

APNIC と IETF におけるリソース証明書

リソース証明書は、IPアドレスとAS番号の利用権利を示す電子証明書である。2004年6月に発行されたRFC3779¹⁰でその構造が提案された、インターネットレジストリのIPアドレスの割り振り構造と同じツリー構造でPKI(Public-Key Infrastructure)の認証局を構築することで、利用されているIPアドレスとAS番号の正当性を保証するための仕組みである。リソース証明書はアドレスの割り振り先に対して発行される。証明書の発行元はCA(Certification Authority)と呼ばれている。割り振り先がさらに割り振りを行うとそこでもリソース証明書が発行されるので、割り振り先にはCAとしての証明書が発行されることになる。IANA (Internet Assigned Numbers Authority) CAの部分は現在の提案内容としては存在せず、RIRが頂点になる案が有力である。

証明書の書式には基本的に X.509v3 の形式が使われ、IPAddr(IP アドレス)やASIdentifier(AS 番号)の値は X.509v3 拡張フィールドと呼ばれる拡張のひとつとして証明書の中に記載される。発行元のリソース証明書は、発行先のリソース証明書に記載さ

¹⁰ X.509 Extensions for IP Addresses and AS Identifiers
<http://www.ietf.org/rfc/rfc3779.txt>

れるアドレスブロックを内包するようなアドレスブロックが記載される。

この証明書は、ルーティングのセキュリティとアドレス資源管理のセキュリティに役立つと考えられている。ルーティング・セキュリティのための応用として代表的なのが S-BGP¹¹である。S-BGPはBBNテクノロジー社のStephen Kent氏によって提案されたプロトコルで、ルーティングプロトコルのBGPを拡張し、ルータ間で交換される経路情報の正当性を電子的に確認できるようにするものである。

APNIC におけるリソース証明書プロジェクトの進捗状況

APNIC ではリソース証明書について以下のスケジュールが立てられている。

フェーズ 1 (2006/5/1-2006/6/30)

- ・ 認証局の実装
- ・ リポジトリの実装
- ・ IETF SIDR WG への提案

フェーズ 2 (7/1-8/31)

- ・ 電子署名付き経路要求の作成
- ・ 電子署名付き IRR オブジェクトの取り組み
- ・ CP/CPS 完了

フェーズ 3 (9/1-12/1)

- ・ LIR toolkit (の整備)
- ・ RIR Portal web サービスツール (の整備)

フェーズ 1 は 7 月上旬に行われた第 66 回 IETF に向けた活動、フェーズ 2 は 9 月上旬に行われた第 22 回 APNIC ミーティングに向けた活動であることが読み取れる。認証局の実装は RIPE NCC と共同で開発が進められており、既にフェーズ 1 の認証局の実装とリポジトリの実装が完了していることは、第 66 回 IETF の会期中に行った JPNIC と APNIC の打ち合わせの際に確認されている。

第 22 回 APNIC ミーティングでは、オペレーター向けのセッションである APOPS (Asia Pacific OperatorS Forum) で、APNIC の Geoff Huston 氏によって進捗状況が報告された。今回新しく発表があったのは以下の 4 点である。

¹¹ Secure BGP Project (S-BGP)
<http://www.ir.bbn.com/projects/sbgp/>

第2章 RIRにおけるアドレス資源の認可機構

- a. APNIC の Web ポータルで証明書発行サービスを提供すること
- b. LIR が証明書管理に利用できるツールの提供
- c. IRR の route オブジェクトに対する電子署名
- d. Web インターフェースを持つ電子署名ツール

a は、AP 地域のコミュニティに対して情報提供することでフェーズ 3 で取り組む Portal web での実装に関する意見集約を開始したものと考えられる。b、c、d については実際の画面イメージが提示され、フェーズ 2 の実装が完了に近いことが示された。ただし署名ツールの利用者を LIR の中のどの立場にするのか、その電子署名をどのように検証するのか、といった利用面での検討はまだ進んでいないようである。

リソース証明書にかかわる課題

リソース証明書の実装は、RIPE NCC と APNIC を中心に順調に進められているように見える。しかしその背景には、証明書の発行だけでは解決できない大きな課題がある。筆者はその課題について第 22 回 APNIC の APOPS のセッションで発表した。

一つはリソース証明書に入るアドレスブロックが運用に適するように調節できない問題である。リソース証明書に入るアドレスブロックはアドレスの割り振り元によって決められる。しかし ISP では、割り振られたアドレスをさらに分割し、ネットワークの接続先に応じて伝達される経路情報を切り替えるような運用がしばしば行われる。従って ISP がリソース証明書に記載されるアドレスブロックをあらかじめ選択できるようにしておく必要がある。そうでないと、追加割り振りがあったような場合に、ルータに既に設定された多くの証明書を一齐に入れ替える必要が出てきてしまう。また逆に接続先に対して不必要な経路の情報を、リソース証明書を通じて伝えてしまうことにもなりかねない。

もう一つは ISP におけるリソース証明書の管理の煩雑さである。リソース証明書が使われるようになると、ISP ではルータと経路の管理の他に CA の管理を行う必要が出てくる。CA は CA 自身の暗号鍵の管理や証明書の失効処理といった複雑な業務を必要とする。その上、アドレスの割り振りや返却といった処理はインターネットレジストリによって行われるため、ISP でその情報を基にした証明書管理を行うことは、一部を自動化したとしても煩雑なものになると考えられる。

これらの課題に対して、JPNIC から、IRR と外部 RA(Registration Authority)の 2 つを使う解決案のプレゼンテーションを行った。IRR は ISP のルーティング・オペレーターによって登録情報の管理が行われている。IRR に登録されている route オブジェクトを使ってリソース証明書の発行が行うことができれば、経路制御のために都合のよい証

明書の発行ができると考えられる。また外部 RA と呼ばれている"証明書管理を行うユーザ"を設けることで、ISP 自身が自分に発行される証明書の申請管理を行うことができ、また同時に ISP で CA のシステムを持たなくて済む。

これらの課題と解決策は証明書管理に限定されたものであるが、S-BGP の利用にはさらに大きな課題がある。それはルータにおけるリソース証明書の扱いである。経路情報を交換するたびに電子証明書を検証していたのでは経路を確定するまでに時間がかかり過ぎてしまう。またリソース証明書が完全に検証できなかったからといって接続を切ってしまうと、接続が切れやすいネットワークができてしまう可能性がある。リソース証明書の検証のタイミングや検証結果を経路情報にどのように反映すべきか、といった検討が必要である。

リソース証明書の今後

第 22 回 APNIC ミーティングの発表を見る限り、APNIC におけるプロジェクトは順調に進んでいる。このまま進んでいけばフェーズ 3 も無事終了し、2007 年 4 月には APNIC の Web ポータルである MyAPNIC で試験的に利用できるようになる可能性がある。

一方、前述した課題をクリアするためには、インターネットレジストリと IRR の関係作りが重要になってくると考えられる。これまでは IP アドレスの割り振り構造であるインターネットレジストリとルーティング・オペレーターの信頼構造の根拠となる IRR は分離しており、またそれが望ましいと考えられてきた。インターネットレジストリが経路制御に関与しないという歴史的な状況が守られてきた反面、ルータの設定における簡単なアドレスの打ち間違いが他のネットワークの接続性を失わせてしまうことがあったり、本来割り振られていないアドレスが IRR に登録されてしまったりして、アドレスが不正利用されてしまう状況がある。

多くのルーティング・オペレーターに使われている RADB は、ARIN と運営組織が異なるだけでなく、インターネットレジストリと連動する仕組みを持っていない。

一方、RIPE NCC で運用されている RPSL ベースのレジストリシステムは IRR とインターネットレジストリが連携する仕組みを持っているようである。RIPE NCC のレジストリシステムは、IRR を兼ねているだけでなく、LIR が route オブジェクトを登録できるユーザを限定する機能を持っている。詳細については、今後調査を進めていく予定であるが、リソース証明書の管理にこの仕組みが使われると前述の課題は解決し、ルーティング・オペレーターにとって使いやすいリソース証明書ができることになる。RIPE NCC の 2007 年度の活動計画にある電子証明書がどのような形で実装されていくのか、RIR の中で注目されると思われる。

2.4. APNIC ミーティングでの ROA と IRR に関する発表

第 22 回 APNIC ミーティングでは、JPNIC から ROA とリソース証明書取り扱いについて発表した。その発表の内容はリソース証明書の運用を現実的なものにするためのモデルであり、IP アドレス認証の展開には大きな意味を持つ。この発表の考え方について以下にまとめる。



図 2-1 2つのポイント（第 22 回 APNIC ミーティングにて）

この発表では 2 つのポイントに絞って発表を行った（図 2-1）。

一つ目の「Use of IIR for handy and legitimate information for certificates」は IRR をリソース証明書を発行するための、利便性が高くかつ正当性が確保されたデータベースとして利用する考え方である。

二つ目の「External RA for simple deployment」はリソース証明書をシンプルな構成で展開・利用促進するために、「外部 RA」（もしくはローカル RA）と呼ばれる手法を用いる考え方である。

これらについて以降のスライドで述べている。

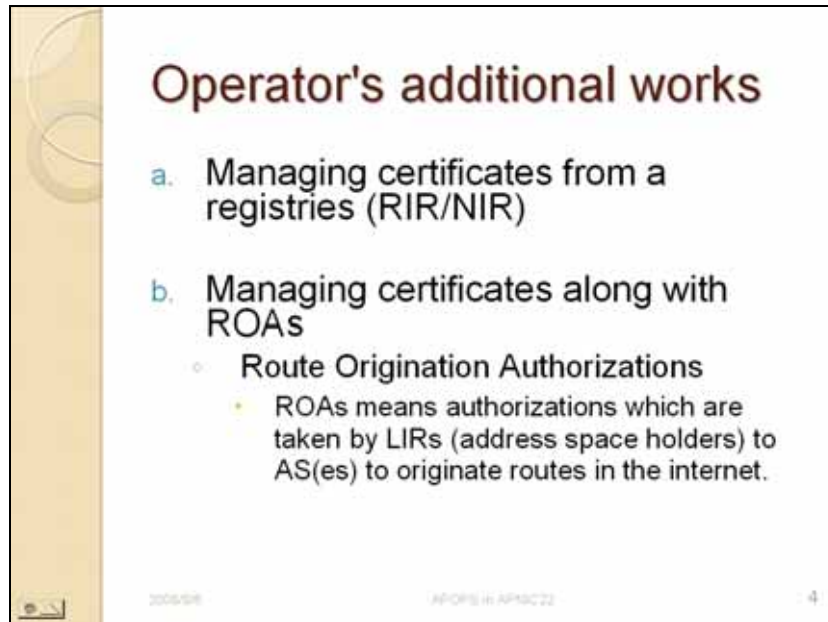


図 2-2 リソース証明書によってオペレータの付加される業務

図 2-2 では、背景としてネットワークオペレーターに付加される業務を挙げている。リソース証明書の導入により、リソース証明書自体を管理する必要が出てくるからである。

「a. Managing certificates from a registries (RIR/NIR)」は、RIR や NIR から発行された証明書を管理する必要がある点である。「b. Managing certificates along with ROAs」は、ROA (Route Origination Authorization) によって発行されるリソース証明書の管理する必要がある点である。

ROA は、アドレス資源が割り振られた LIR によって AS に対して行われるもので、対象の AS が LIR に割り振られている IP アドレスの origin (経路情報の発信源) になることの認可を意味する。ルーティングの安全性向上には、origin の他に AS パスの検証などの手法が考えられるが、リソース証明書は origination (発信源の正しさ) に着目しているためここでは ROA の証明書に注目している。

これらの業務負荷を下げるのがリソース証明書を適切に deployment (展開) するための要件であると言える。

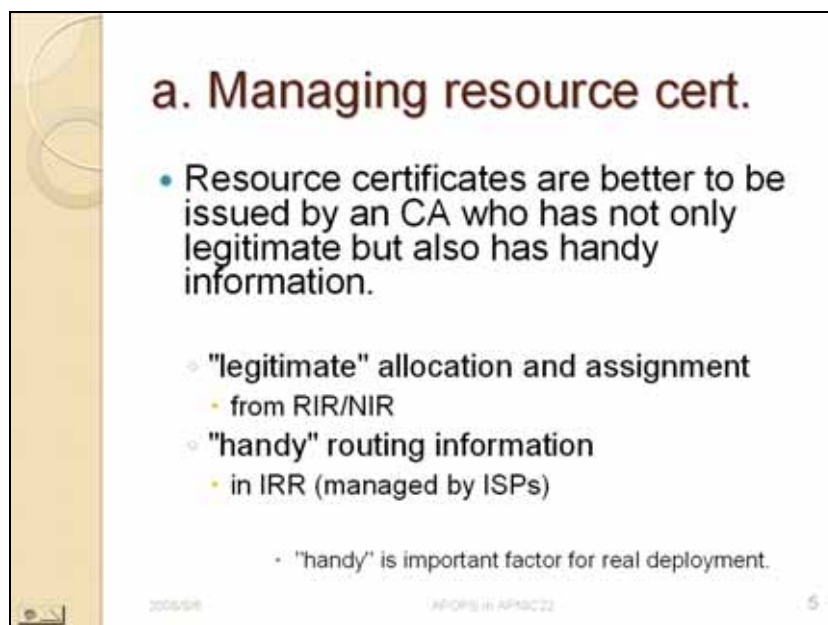


図 2-3 リソース証明書の管理

「Resource certificates are better to be issued by and CA who has not only legitimate but also has handy information」は、「リソース証明書は、正当性のある情報に基づいて発行されるべきであるだけでなく、利便性が高い情報に基づいて発行される必要がある」ということ意味している。

「legitimate allocation and assingment」とは RIR や NIR による割り振りや割り当てが行われているという意味である。

また「handy routing information」は、ISP 自身によって管理されている、IRR に登録された情報を意味している。IRR は ISP 自身が情報を登録するため、ISP のネットワーク事業に添った情報が登録されることになる。ISP が非公開とする情報があれば、それは IRR に登録されないため、公開されている情報は公開情報であることを前提にした解釈を行うことができる。

ここで課題になるのは、「handy」である IRR の情報が以下に正当な情報を担保するかという点である。

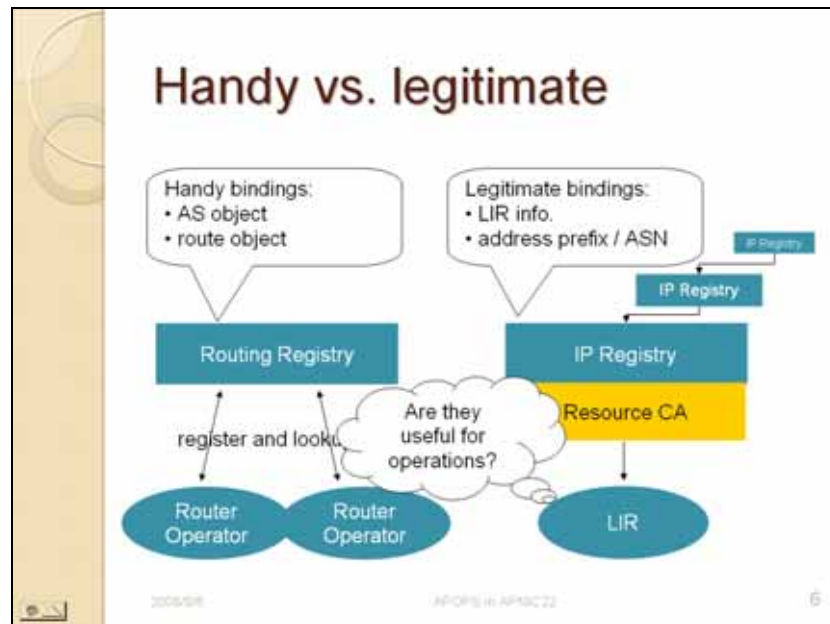


図 2-4 利便性と正当性の違い

「Handy vs. legitimate」は利便性を一義的に考えるか、正当性を一義的に考えるかという比較を提起している。「Routing Registry」に登録される情報は「Router Operator」すなわちルーティングのオペレーター自身が情報を登録する。ここでいう情報は「AS object」すなわち AS 情報や、「route object」すなわち経路情報である。ルーティングレジストリにおける AS 情報と経路情報の組み合わせが登録されることで、ある AS から間違っただ経路が広告されたときに、ルーティングレジストリの参照を行っているものは、それを検出できるようになる。ルーティングレジストリではオペレーター自身が登録するため、運用のための情報交換のために必要最低限のものが登録 / 公開され、また prefix のサイズも運用の事由に一致した「handy」なものとなる。

一方「IP Registry」すなわちインターネットレジストリも、LIR（日本国内の IP 指定事業者など IP アドレスの割り振りを受けている組織）と「address prefix」すなわち IP アドレスブロック、そして「ASN」すなわち AS 番号の情報を持っている。これら情報はインターネットレジストリが、自ら割り振り / 割り当てを行った結果であるため正当「legitimate」な情報であると言える。しかしネットワークの運用上の都合で分割された IP アドレスの情報や、その一部が非公開である場合であってもそれが逐次反映されているわけではない。ルーティングレジストリは常にルーティングのオペレーターに参照されていると考えられるが、インターネットレジストリの割り振り / 割り当て情報は、LIR に対する割り振り / 割り当ての情報でしかないので、ネットワークの状況を反映しなくてもルーティングには影響が少ないためである。

インターネットレジストリに登録されている情報は正当「legitimate」であるが、ネットワークオペレーターにとって利便性が低い意味で、「Resource CA」リソース証明書

の発行の為にどの情報を利用すべきかについて、検討する必要がある。

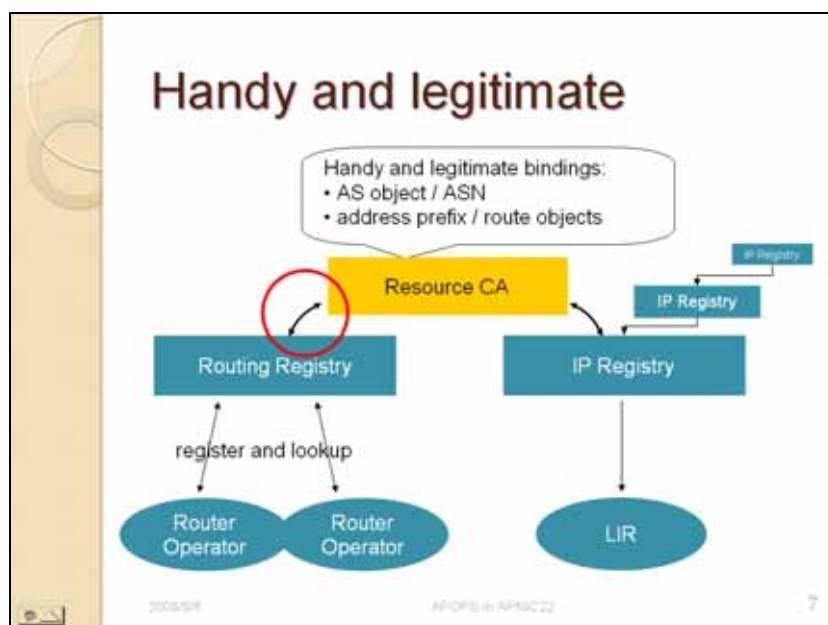


図 2-5 リソース証明書のための利便性が高くかつ正当な情報源

「Handy and legitimate」すなわち利便性が高くかつ正当な情報源を確保するには、「Routing Registry」（ルーティングレジストリ）と「IP Registry」（インターネットレジストリ）の情報の両方の参照が必要であると考えられる。図 2-5 はリソース証明書の発行を行う「Resource CA」がルーティングレジストリとインターネットレジストリの両方の情報を参照し、「AS object / ASN」（AS 情報）と「address prefix / route objects」（アドレスブロックと経路情報）の両面から「bindings」（組み合わせ）を抽出することを示している。

APNIC で進められているリソース証明書プロジェクトでは、インターネットレジストリの割り振り情報 / 割り当て情報を一元的な情報源とするため、図 2-5 のマルで示された連携を行うことができない。

なお後に判明したことであるが、2006 年 11 月に ARIN のミーティングや IETF で行われた、APNIC Geoff 氏のプレゼンテーションによると、IRR に登録される情報である as-set オブジェクトが使用されており、上記の考え方に沿っていることがわかる。

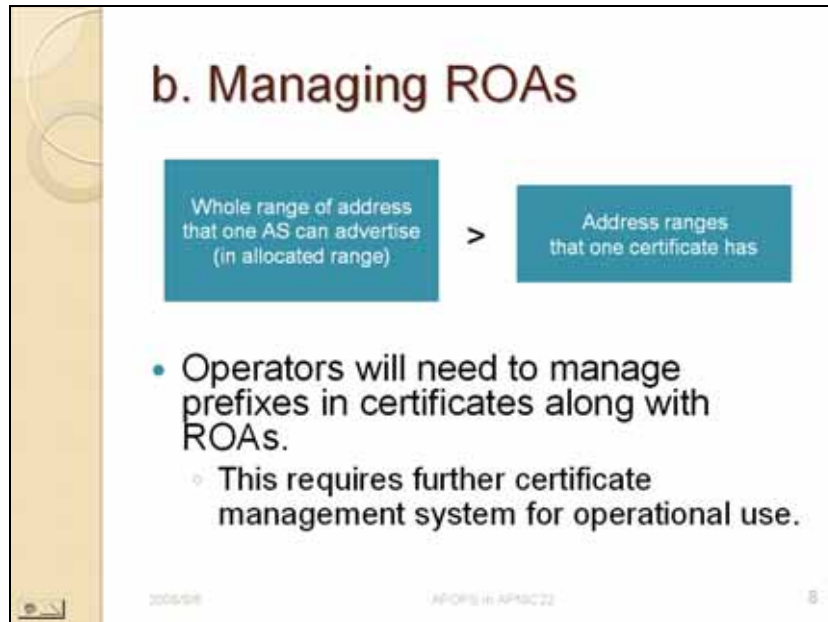


図 2-6 ROA の管理

「b. Managing ROAs」すなわち ROA (Route Origination Authorization) の管理は、ネットワークの prefix の管理と平行して行われる業務になると考えられる。そのためリソース証明書の管理は、アドレス prefix の分割などが業務上簡単に行えるような状況でなければ実現が難しい。

まず、ある LIR が割り振られた IP アドレスをそのままある AS が経路広告に使用することは少なく、分割された IP アドレスのブロックがネットワークのトポロジー（接続状況）に応じて配置されることが一般的である。

そして「Whole range of address that one AS can advertise (in allocated range)」すなわち、割り振り済みの IP アドレスの中である AS が広告できるアドレスの範囲は、「Address ranges that one certificate has」すなわち一つのリソース証明書が持つアドレスの範囲よりも大きいことが容易に考えられる。

この2点から、ある AS は経路広告の認可を示す ROA のリソース証明書を受け取った後、ネットワークのトポロジーに応じて prefix を分割し、その分割状況に合わせてリソース証明書を発行しなおす必要があることが考えられる。これが「Operators will need to manage prefixes in certificates along with ROAs」の意味である。これにより「This requires further certificate management system for operational use.」すなわち既存のリソース証明書発行システムよりも高度な、オペレーションに合った証明書管理システムが必要になることがわかる。

この問題が如実に表れるのは末端の LIR である。

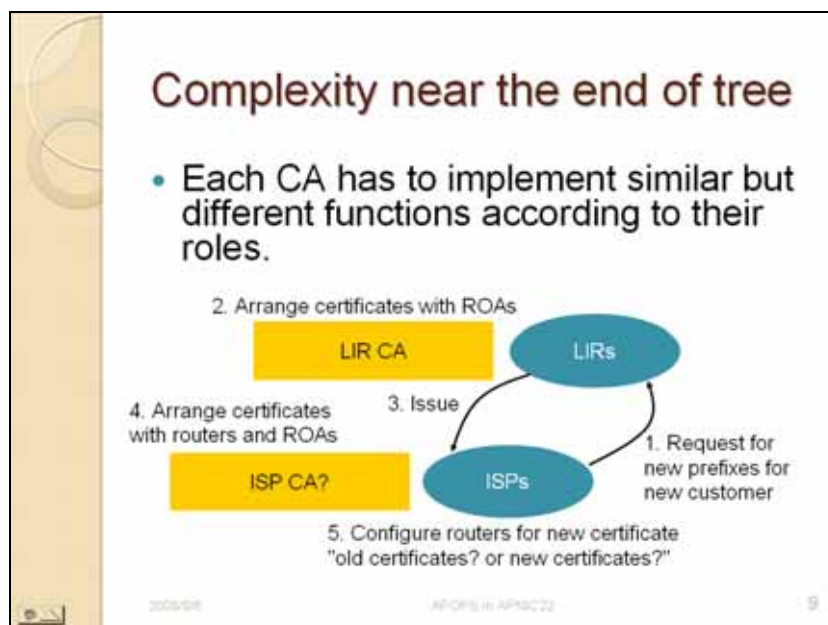


図 2-7 末端部分でのリソース証明書の複雑さ

「Complexity near the end of tree」広義のインターネットレジストリのツリー構造に則って考えた LIR では、AS のオペレーションを行っている ISP に対する IP アドレスの割り当て業務が行われている。この割り当ては JPNIC のようなインターネットレジストリに「割り当て報告」されていないケースもある。

リソース証明書は広義のインターネットレジストリのツリー構造に沿って発行されるものであるが、そのためには「Each CA has to implement similar but different functions according to their roles.」各々の CA が似て非なる機能を役割（NIR や LIR など）に応じて持っている必要がある。

「1. Request for new prefixes for new customer」は新規の顧客に対する新たな prefix の要求を ISP から LIR に対して出すことを示している。「2. Arrange certificates with ROAs」は LIR がその必要な prefix に応じた ROA を設定し「3. Issue」で LIR の CA がリソース証明書として発行する。「4. Arrange certificates with routers and ROAs」は ISP でリソース証明書の管理のために運用されている CA が存在する場合にはそこで証明書の組み込みが行われること示している。「5. Configure routers for new certificate "old certificates? or new certificates?"」はルータを新たなリソース証明書の為に設定することを示しているが、経路制御への影響を考慮して、古い証明書を使うべきなのか新しい証明書を使うべきなのかの判断は、この段階で必要になる。

これらの複雑さを解決するための提案が次のスライドである。

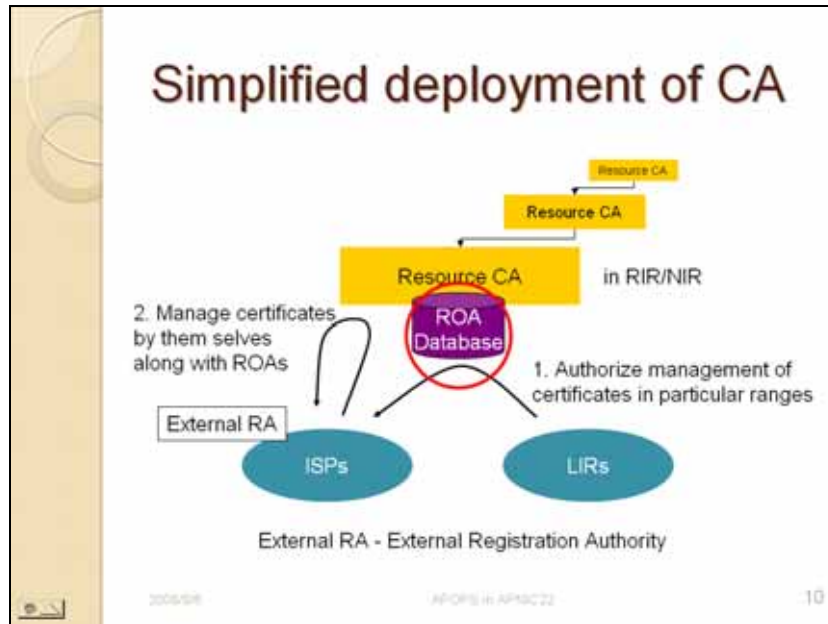


図 2-8 シンプルなリソース証明書用 CA の展開

リソース証明書の為の CA のシンプルな展開「Simplified deployment of CA」の為に、図 2-8 に示すようなモデルが考えられる。

RIR や NIR における「Resource CA」リソース証明書は従来通りであるが、新たに「ROA Database」を設置している。ROA Database は LIR における ISP への ROA を集めたもので、これらの ROA を LIR 自身が CA を構築して管理するのではなく、そのオリジナルデータを RIR や NIR が持つという考え方である。

元来 IRR は ISP 自身が持つべき情報のうち、共有すべき情報を集約したものである。IRR と同様にインターネットレジストリに自由に登録 / 参照なデータベースを設ければ、LIR や ISP 同士の登録 / 参照の為には自組織で認証局を構築管理するよりも利便性が高い。また登録される情報を RIR/NIR における割り振り情報 / 割り当て情報と比較すれば、登録情報の内容の正当性を維持することもできる。利用手順は以下ようになる。

「1. Authorize management of certificates in particular ranges」は、初めに特定のアドレスブロックに対する証明書の管理を ISP に対して「認可する」。このことで ISP はそのブロックに含まれるアドレスが入ったリソース証明書を管理できることになる。

「2. Manage certificates by them selves along with ROAs」は ISP 自身が ROA に則って証明書の管理を行うことを示す。このとき ISP は「External Registration Authority」というモデルに則って証明書の管理を行う。

External Registration Authority は「外部登録局」と呼ばれ、証明書発行業務を行う役割を CA に対して外部（すなわち ISP 自身）に持たせたモデルである。このモデルにすることで、ISP 自身では認証局ソフトウェアを管理運用する必要はなく、RIR/NIR に

ある証明書管理システムに Web ブラウザ等でアクセスして、証明書の発行業務を行えばよいことになる。



図 2-9 発表のまとめ

この提案では二つのアイデアを提示した。

「Use of IRR for resource certificates」はリソース証明書の管理の為に IRR を利用するという意味である。これによって ISP 自身の運用状況にあった「handy」便利なリソース証明書の発行を行うことができる。

「External RA for ISPs」はリソース証明書の管理の為に、外部登録局のモデルを利用し、ISP 自身が証明書の管理を行うことができるようにするという意味を意味する。ISP 自身が認証局ソフトウェアを運用する必要がないため、「simplified deployment」単純化された利用・展開を目指すことが可能になる。

なお、発表の最後には RIR と IRR の運用ケースの違いについて補足した(図 2-10)。

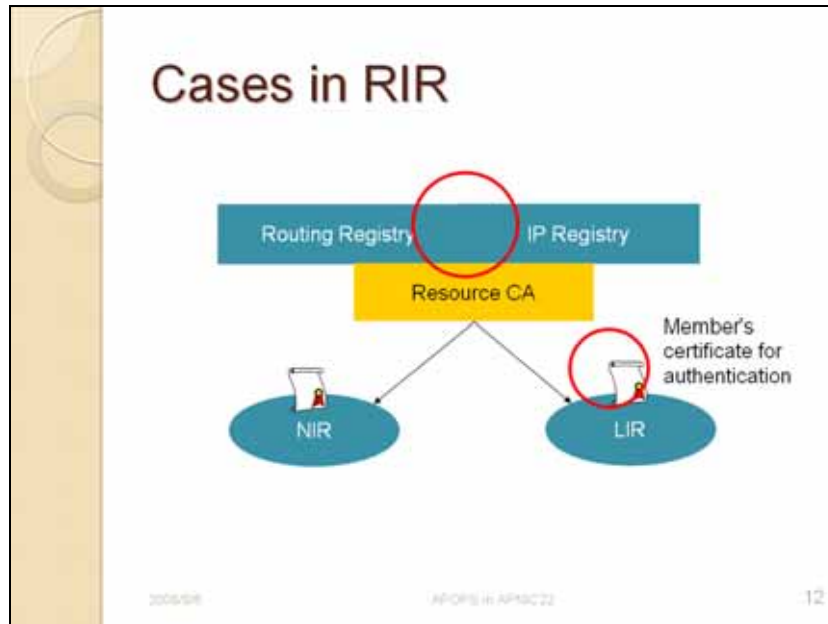


図 2-10 RIR における運用ケースの違い

RIR では、IRR を運用していないケースがあり、場合によってリソース証明書管理システムとの連携の仕方が異なってくる。

APNIC の場合には、IP アドレスの管理を行う IP レジストリシステムと IRR のシステムが同一であり、図 2-10 のようにリソース証明書のための認証局が直接連携して証明書の管理を行うことが可能である。また APNIC から IP アドレスの割り振りを受けている「メンバー」の認証用の証明書(図中では Member's certificate for authentication)が存在するため、ISP に対する authorization(認可)を業務上実現するためにこれを利用することができる。

このモデルは RIPE NCC の場合でも同様であるが、RIPE NCC の場合には IP レジストリシステム及び IRR の中に既に認可機構が組み込まれている。そのためリソース証明書の発行を行う認証局はこの認可情報を利用することが可能である。この意味で、RIPE NCC におけるリソース証明書の実現性は高いと考えられる。

ARIN の場合には、ARIN において IRR が本格運用されておらず、北アメリカ地域における大手の IRR の RADB を利用することが考えられる。(2007 年初めに IRR の運用開始のアナウンスがあった。しかしそのオリジナルデータはまだ少ない。) IP レジストリシステムと IRR が別である場合、JPNIC のモデルと似たシステム構成となる。

従って本調査研究の一環で設計/開発されている「経路情報の登録機構」は ARIN においても適用可能な仕組みであるといえる。

2.5. まとめ

本章では主に RIR における IP アドレスの認可機構の調査について述べた。IP アドレスの認可機構は IP アドレス認証の展開の最も肝要な機構であると共に、RIR でもその機構が見直され、リソース証明書管理システムの一部として検討が開始されている。

RIR の動向調査では、RIPE NCC、ARIN、APNIC のミーティングに参加し、また現地のスタッフにヒアリングを行った。調査の結果 RIPE NCC における認可機構を除いて未だ IP アドレスと AS 番号の組み合わせを確認する機構の開発は行われていないものの、リソース証明書の技術開発が進められていることがわかった。

一方、RIPE NCC のデータベースにおいて課題になっているように、時間が経って正当性がなくなったデータを消去する仕組みや、新たに LIR から ISP に認可する仕組みの構築はすべての RIR においてあまり取り組まれていないことがわかった。この結果を受け、JPNIC で IP アドレス認証の展開として取り組んでいる「経路情報の登録機構」では正当性がなくなったデータの整理の機能などが盛り込まれることになった。

第 22 回 APNIC ミーティングでは、JPNIC から、リソース証明書のより現実的な deployment (利用と展開) のために必要になるいくつかのポイントについて発表した。これらのポイントは「経路情報の登録機構」の設計に基づくものであり、今後本機構がリソース証明書の管理機能を持つことで、機能性・利便性の高いリソース証明書システムができると考えられる。

第3章 電子認証技術と技術文書策定に 関する国際動向

内容

- IETF における技術文書の策定プロセス
- 電子認証技術の動向
- 経路制御の安全性とリソース証明書

3. 電子認証技術と技術文書策定に関する国際動向

3.1. 概要

電子認証技術、および技術文書の策定の国際動向を調査するため、IETF のミーティング、および APNIC、RIPE NCC、ARIN といった RIR (Regional Internet Registry) のミーティングに参加し、また担当者との情報交換を行った。

電子認証技術は ITU-T の X.509 にて策定された PKI (Public-Key Infrastructure) を中心に調査しているが、IETF や RIR におけるその応用的な議論は、X.509 の仕様から大きく離れ、独立した議論となっている。また IETF における技術文書の策定方法は常に見直されており、その見直しのための議論は、電子認証フレームワークの策定に必要な策定プロセスのあり方を示唆するものであった。

本章ではこれらの調査結果について、まず各 IETF ミーティングの様子をまとめ、後半で数年間のスパンで捉えた PKIX WG (Public-Key Infrastructure (X.509) WG) の動向をまとめる。

3.2. 動向調査の目的

動向調査の目的は主に 3 点である。以下では各々について述べる。

技術文書の策定プロセス

IETF では RFC と呼ばれる技術文書を参加者のコンセンサスに基づいて策定する仕組みが運用されている。この仕組みは最新かつ多様な分野の技術者に受け入れられるアウトプットを得るという意味で、電子認証フレームワークを策定するためのプロセスのあり方に大きく影響するものであると考えられる。2006 年度は特に IETF における策定プロセスについて議論が行われた NewTrk WG の活動について調査した。

電子認証技術の動向

電子証明書の技術である X.509 は、PKIX WG で議論が進められている仕様が多くの実装で採用されている状況がある。そこで 2006 年度および近年の PKIX WG でどのような技術が策定されているかについての最新動向を調査した。

リソース証明書の動向

リソース証明書は IP アドレス等のアドレス資源の利用 / 管理権限を示す電子証明書で、主に APNIC で開発と仕様策定が行われている。APNIC は各 RIR のミーティングでデモンストレーションを行うとともに、技術的な仕様について IETF における RFC

第3章 電子認証技術と技術文書策定に関する国際動向

の策定を通じて標準化を図っている。そこでリソース証明書を扱っている SIDR(Secure Inter-Domain Routing) WG に参加し、技術的な動向について調査した。

3.3. IETF における国際動向の調査

3.3.1. IETF の開催状況と注目した WG の開催状況

2006 年度、IETF におけるミーティングは第 66 回、第 67 回、第 68 回と 3 回開催された。このうち本調査研究のために第 66 回と第 67 回に参加した。

IETF はインターネットにおける通信プロトコルの標準化において注目されている団体であるが、一方でその独自の策定方式を維持するための議論や特定の国やベンダーに傾倒しないような中立性を保ち最先端の知見を IETF の活動に盛り込むための議論が行われている点でも注目に値する。

電子認証フレームワークは、IETF においてカバーされていない一方で、中立的かつ最先端の知見をドキュメント化して共有することに意義がある。従って本調査研究では、IETF における議論とドキュメント策定プロセスに注目し調査を行った。

特に注目したのは IETF における新たな策定プロセスについて議論している NewTrk WG、電子認証技術である PKI の策定を行っている PKIX WG、また電子証明書を使って IP アドレス等のアドレス資源の管理を行う技術であるリソース証明書などである。

本節ではこれらの調査の結果についてまとめる。

3.3.2. 第 66 回 IETF

2006 年 7 月 9 日(日)から 7 月 14 日(金)まで、カナダのモントリオールにて、第 66 回 IETF ミーティングが開催された。今回の IETF はカナダ・モントリオールの Palais des Congres de Montreal (モントリオール・パレ会議場)で開かれた。会場は市の中心部から徒歩 10 分程のところ、同じ規模の国際会議を同時に二つ以上は開けそうな巨大な会場である。

今回の参加登録者数は 1,257 名で、参加国は 44 ヶ国であった。米国・ダラスで行われた前回の IETF の時に、いくつかの国からの参加者が米国への入国ができず、IETF の働きかけによって急遽ビザが発行されるという出来事があったようであるが、今回はそのような事態への配慮がなされて、カナダで開催された模様である。

IETF では、WG の会議と Plenary と呼ばれる全体会議が行われる。WG の会議では

主に RFC (Request for Comments) になる前のドキュメント(Internet- Draft)に関する議論が行われる。議論は基本的に ML で進められるが、IETF 期間中にオフラインで打ち合わせることでコンセンサスを確立したり、その場で実装をしてつきあわせたりして、RFC 化が目指される。一方、Plenary は会期中 2 回だけ行われる。

“ IETF Operations and Administration Plenary ” は IETF の運営面の全体会議で 7 月 12 日(水)に開かれた。技術面の全体会議である Technical Plenary は 7 月 13 日(木)に開かれた。

IETF Operations and Administration Plenary

IETF Operations and Administration Plenaryは、IETFの活動全体の運営に関する報告と議論を扱う全体会議である。今回はミーティングのホストを務めるEricsson社のプレゼンテーションとNOC(Network Operation Center)の報告、IAOC(IETF Administrative Oversight Committee)¹やIASA(IETF Administrative Supporting Activity)、TOOLSチーム²といったIETFを支える活動の報告と、IETFにおける標準化プロセスの再検討に関する議論などが行われた。

はじめに IETF チェアの Brian Carpenter 氏からチェア報告があった。前回の IETF 以降、4 つの WG が新設され 13WG が終了、RFC が 138 出されたそうである。IASA 報告の中では、RFC Editor の活動報告や前回の IETF の会計報告などが行われた。RFC Editor は RFC の校正を行い、体裁を整えるチームで、2 年程前より体制を建て直し徐々に作業効率の向上を図っている。2006 年度は 2005 年度よりも RFC 編集作業のペースが 58%近く向上しているとのことである。

IETFにおける標準化プロセスの再検討は、2004 年以降、IETFチェアのBrian氏自身によって進められてきた。これに関する Internet-Draft は、draft-carpenter-newtrk-questions-00.txtである。これまでNewTrk WG³の会議が何回か開かれてきたが、方向性が決められず今回のPlenaryで全体の意見を聞くことになったようである。しかし会場からは再検討の議論自体に意義を見いだせないといった意見が挙げられていた。

Technical Plenary

¹ IAOCは 2004 年初頭から行われている、IETFの運営管理体制の再編の活動の一環として作られた委員である。IETFの予算や活動計画、契約といったIAD(IETF Administrative Director)の提案に対してレビューを行い、活動の方向性を示す役割を担っている。

² TOOLS Team Charter
<http://tools.ietf.org/charter-page>

³ New IETF Standards Track Discussion (newtrk)
<http://www.ietf.org/html.charters/OLD/newtrk-charter.html>

Technical PlenaryはIETFの活動の中の技術的な議論を扱う全体会議である。IRTF(Internet Research Task Force)の活動報告、IRTFのSAM RG(Scalable Adaptive Multicast Research Group) ⁴の紹介、IABのチェア報告などが行われた。

IRTFは長期的な観点で技術を捉え、リサーチと議論・検討を行うグループである。必要性が認められるとIETFでの標準化作業を行う。SAM RGは前回のIETFの後に結成された。SAM RGは、複数のマルチキャスト・プロトコルの利点をそれぞれ生かし、展開・普及を図ることを目的としている。IPマルチキャストだけでなくアプリケーション層に分類されるようなものや、中間的な分類(Hybrid)に入るプロトコルも議論の対象に入っている。IPマルチキャストとして分類されるものはXCAST⁵のみである。

IABのチェア報告では、IAB主催のBoFやワークショップの紹介とRFC Editor⁶のあり方の検討に関する発表があった。これまで2005年10月のNANOG⁷や2006年3月のAPRICOT⁸で開いてきたIPv6 Multicast BoFが、2006年4月に行われたRIPE Meeting⁹でも行われたようである。またRouting and Addressingワークショップ(IABではRAWSと呼ばれている)の告知があった。このワークショップのようなIABが主催するオープンなミーティングについての情報は、下記のWebページにまとめられている。

IAB-Sponsored Open Meetings (IAB 主催のオープンミーティング)

<http://www.iab.org/documents/open-mtgs/>

IABでは今後30年という長期的な視点で、RFC Editorのあり方について検討してい

⁴ SAM Research Group
<http://www.samrg.org/>

⁵ XCAST
<http://www.xcast.jp/>

⁶ RFC-Editor Webpage
<http://www.rfc-editor.org/>

⁷ NANOGはThe North American Network Operators' Groupの略で、主に北アメリカ地域のインターネット関連のネットワーク運用管理担当者(ネットワークオペレータ)を対象にしたグループ。MLや1年に3回開催されるミーティングを通じて、主に技術的な議論や知見の共有、相互の普及・啓発活動が行われている。
<http://www.nanog.org/>

⁸ Asia Pacific Regional Internet Conference on Operational Technologiesの略で、アジア太平洋地域のインターネットインフラストラクチャーを発展させるため、技術者に必要な知識や技術を向上させることを目的として開催される非営利のフォーラムである。1996年の設立以来、毎年1回アジア太平洋地域のさまざまな都市で開催され技術者の人材養成、実用的な技術と知識の習得を目指したプログラムが行われている。
<http://www.apricot.net/>

⁹ ヨーロッパ地域のRIRであるRIPEが主催して行われるミーティングである。APNICやARINと同様に、IPアドレスに関するポリシーやインターネットの運用に関する議論が行われる。

る。(ちなみに最初の RFC である RFC1 が出たのは 1969 年 4 月 7 日で、今年で 37 年経ったことになる)特に RFC Editor のプロセスの中で IAB や IAOC (IETF Administrative Oversight Committee) そして IETF がどのように関わっているべきかといったことを議論しており、そのために RFC の目的やミッション、RFC 化の役割分担についての整理を試みている。また IAB では IAOC と共に RFC Editor の RFP (Request for Proposal - 提案依頼書) の作成を進めているようである。会場からは RFC Editor に関する議論に対して時間をかけ過ぎているといった意見が出ていたが、ドキュメント (Internet-Draft) の著者の主旨を正確に組み入れ、かつ RFC 化の作業がコミュニティの必要に応えるようなスピードで行われるための効率化を図るため、慎重な検討が進められている様子がうかがわれた。

この他に、IDN (Internationalized Domain Names) と IDNA (Internationalizing Domain Names in Applications) を組み合わせて使うことの問題点、例えば類似する文字で spoofing (だます行為) が行われてしまうこと等について、DNS のアーキテクチャの中で取り組む考え方などについて紹介されていた。

セキュリティエリアにおける電子認証関連 WG

第 66 回 IETF では、セキュリティエリアのセッションが 18 行われた。BoF は Network Endpoint Assessment BoF と Handover and Application Keying and Pre-authentication BoF の 2 つである。また PKIX WG と前回 WG になった SIDR WG とのジョイントセッションが行われた。

本節では、PKIX WG と SIDR WG、及びインターネットの経路制御における電子証明書の動向について報告する。また末尾で BoF について紹介する。

SIDR WG (Secure Inter-Domain Routing WG)

第 64 回および第 65 回の IETF で BoF が開かれていた SIDR が、2006 年 4 月 18 日に WG になった。今回の IETF で行われるミーティングが WG として行われる初めてのミーティングである。

SIDR は Secure Inter-Domain Routing の略で、ネットワーク・ドメイン間の経路制御におけるセキュリティメカニズムを開発することを目標としている。RPSEC WG で議論されてきたセキュリティの要件に則り、利用や展開 (deployment) を含めて検討を行う。

今回の WG セッションでは、IP アドレスや AS 番号が入った "リソース証明書" の実験を行っている APNIC の Geoff Huston、George Michaelson 両氏による、2 つのドキュメントプレゼンテーションが行われた。また経路制御プロトコルをより安全に利用するためのトランスポート層 (TCP) のセキュリティに関するドキュメントプレゼンテーショ

ンが行われた。リソース証明書に関するプレゼンテーションは以下の2つである。

"A Profile for X.509 PKIX Resource Certificates"

draft-huston-sidr-res-certs-01.txt

IP アドレスと AS 番号の利用権を検証するための電子証明書のプロファイルを定めたもの。この証明書はリソース証明書と呼ばれる。

"A Profile for Resource Certificate Repository Structure"

draft-huston-sidr-repos-struct-00.txt

リソース証明書を保持するリポジトリの構造を定めたもの。Subject Key Identifier(SKI)や Authority Key Identifier(AKI)を使って電子証明書を検索できるようにするため、Subject にそれらのハッシュ値を含めた名前を使う。

APNIC ではこれらの仕様を前提として実装を進めているようである。主な論点はリソース証明書の Subject とトラストポイント(信頼点、またはトラストアンカーと呼ばれる)の2つである。SKI のハッシュ値を Subject に含めるのは、リソース証明書の証明書パスにおける一意性を維持することを意図している。本来、Subject は電子証明書の発行対象の識別子を入れるために使われるが、証明書を識別しやすくするために特殊な使われ方がされているようである。

またリソース証明書に想定されるツリー構造の頂点をどうするか、トラストポイントをどう想定するか、といった点については議論が収束していない様子である。IP アドレスと AS 番号の管理を行っているインターネットレジストリの構造からすると、直感的には IANA が頂点となる認証局を運用し、RIR の認証局がその下位認証局となって、IANA の認証局を多くの利用者がトラストポイントと位置づけることが考えられる。しかし RIR の中にはその認証局の運用可能性に疑問を持っているところが多いようである。これは IANA に比べて RIR (もしくは RIR の連合体である NRO) が、IP アドレス及び AS 番号の割り振り / 割り当て業務の大半を実施している現状を鑑みたものと思われる。

標準技術的な観点では、絶対的な頂点の存在を規程することよりも Relying Party(証明書検証者)が、トラストポイントを使って必要十分なリソース証明書の検証ができるか、という点が重要である。そのため、頂点の認証局については、今のところは先に延ばせる議論である。

トランスポート層のセキュリティについては以下のドキュメントに関するプレゼンテーションが行われた。

"Key Change Strategies for TCP-MD5"

draft-bellovin-keyroll2385-00.txt

BGPのような長期的なTCPセッションにおける、MD5オプションのための鍵変更の方式である。既存の方式と互換性がありながら、片方のエンドだけで実施できるようになっている。

"Authentication for TCP-based Routing and Management Protocols"

draft-bonica-tcp-auth-04.txt

MD5に代わる、より強度の高い暗号アルゴリズムを使ったTCPオプションの取り決めである。

"Automated key selection extension for the TCP Authentication Option"

draft-weis-tcp-auth-auto-ks-01.txt

TCPのExtended Authenticationオプションのためのセッションキーの交換方式と、そのためのノンス(暗号文を変化させるためのランダム値)を使ったメッセージ認証の方式の取り決めである。

"The TCP Simple Authentication Option"

draft-touch-tcpm-tcp-simple-auth-01.txt

MD5オプションに代わる認証のためのTCPオプションである。IPsecのように別途のSA(Security Association)を確立する方式を提案している。

TCPにおける認証方式の改善は、強度と運用の容易さ、既存のTCPとの互換性といった様々な要素が関係している。ネットワーク・セキュリティの大家であるSteven Bellovin氏を中心に慎重に検討が進められている。

PKIX (Public-Key Infrastructure (X.509)) WG

PKIX WGは7月10日(月)の17時40分~21時に行われた。18時50分からはSIDR WGとのジョイントミーティングであった。約50名の参加があった。

第65回IETF(2006年3月)以降、AC Policies Extension(RFC4476)とGOST Cryptographic Algorithms(RFC4491)の2つがRFCになった。RFC3280の部分的な変更であるDirectoryStringのUTF-8の処理に関するドキュメントは、RFC3280の改定作業とは独立して、RFC Editor's queueに入っており、RFCになる直前の段階にある。

SIM(Subject Identification Method)、SCVP(Server-based Certificate Validation Protocol)、Lightweight OCSPの3つがWG Last Callを終え、Area Directorのレビュー

一中である(8月17日現在、SIMはIESGレビューを終え、RFC Editor's queueに入っている。)。SCVPのSは以前Simpleであったが、Server-basedに変わった。

SIMは元々韓国のJong-Wook氏から出されたドキュメントであったが、Tim Polk氏が引き継ぎ、現在IESGからのコメントに対応中である。SCVPは27版になり、いよいよIESGによるレビューの段階に入った。前回のIETF以降、編集上の変更や定義づけに関する追記といった比較的軽微な変更がなされた模様である。

Lightweight OCSPは、オンラインで証明書検証処理を依頼するためのプロトコルのOCSPを改良したものである。大量のやりとりに適するよう、メッセージサイズを小さくしたり、返答結果のキャッシングを行うことができたりしている。

X.509v3形式の電子証明書の基本的なプロファイルを記述したRFC3280の後継となるドキュメント、通称3280bisについてはnameConstraintsフィールドのエンコーディングに関する追記が行われている。またCRL Distribution PointsやAIA(Authority Information Access)/SIA(Subject Information Access)といったフィールドで、httpsを使用することに関する注意事項の追記が行われた。電子証明書の検証のためにhttpsが使われると、その処理のために更に電子証明書の検証が必要になり、場合によっては本来の検証処理が終わらなかつたり、状態が複雑になりすぎたりする。これを避けるための注意喚起のための追記が行われたようである。他にも議論が収束していない点が残っている。しかし部分的にドキュメントを分割して、3280bisの対象外とするなどして整理を進められる模様である。

Joint PKIX/SIDR Meeting

PKIX WGの2セッション目に、PKIX WGとSIDR WGのジョイントミーティングが行われた。内容はSecure BGP(S-BGP)の提案者であるStephen Kent氏による"A PKI for Internet Address Space"というプレゼンテーションである。PKIX WGの参加者に加えて、SIDR WGのチェアであるSandra Murphy氏らが加わった形で意見交換が行われた。

Stephen Kent氏は、IPアドレスとAS番号の使用権を示す電子証明書を使ってインターネットのルーティングプロトコルであるBGP(Border Gateway Protocol)の安全性の向上を図る仕組み"S-BGP"の提案をしている。これは、RFC3779に記述されている電子証明書の拡張フィールドを使ってIPアドレスの割り振りとAS番号の割り当てを証明し、経路情報として広告されたprefixが、所有者(利用者)によって正しく使われていることを検証できるようにする仕組みである。インターネットにおける経路情報の中で、誤ったIPアドレスとAS番号が使われると、経路ハイジャックと呼ばれる大規模な利用不能攻撃が可能になる。S-BGPがうまく利用されると、このような攻撃を未然に防ぐことができると考えられている。

このセッションでは、RIRが運営する認証局を使ってこの電子証明書の発行を行うモ

デルが紹介された。電子証明書の手にはrsync¹⁰が使われることとなっている。

ここでもトラストポイントに関する議論も行われた。APNIC や RIPE NCC からの参加者の間では、RIR が運用する認証局がトラストポイントとなることを想定して議論が行われている。しかし本来、トラストポイントとはプロトコルの提案者が決めるものではなく、電子証明書の検証を行う者、正確には証明書の検証結果に依存した処理を行う方針を持つもの(Relying Party)が決めるものである。そこで筆者は Address Space PKI の構造に含まれるとされる JPNIC でも、トラストポイントとして利用されることを想定した認証局を運用していることから、RIR の認証局だけがトラストポイントになるわけではないことを会場で確認した。これは、例えば日本国内の ISP の間で経路情報の交換を行う場合に、APNIC や RIPE NCC の認証局を利用する必要はないと考えられるためである。

会場では、この他に割り振りを受けたアドレスブロックを使ったまま地域を移動し、割り振り元を別の RIR に変更するケースの扱い方などについて議論が行われた。

IETF の会場で APNIC の方々と情報交換することでわかってきたことであるが、APNIC では、Address Space PKI に関する開発プロジェクトが 2006 年末の終了を目標として進んでいることがわかった。既に IP アドレスと AS 番号が入った電子証明書の発行やリポジトリの設置が実験的に行われていた。今後、MyAPNIC という申請業務用の Web システムに組み込まれることが考えられており、実用化に向けた活動が今後も引き続いて行われていくことが考えられる。

第 66 回 IETF で新たに行われた BoF を以下に示す。

Network Endpoint Assessment (NEA) (Proposed NEA WG Charter)

<http://www3.ietf.org/proceedings/06jul/agenda/nea.txt>

NEA は、ネットワークに接続するエンドポイント(ホスト等)の OS やパッチの適用状況に関する情報(posture)を交換し、エンドポイントの安全性が確認された場合にのみ会社のネットワークへの接続を許可するといった仕組み構築の為に利用できる。

Handover and Application Keying and Pre-authentication (HOAKEY)

モバイルネットワークにおけるハンドオーバーの為に、認証情報を交換する仕組みに関する BoF である。第 65 回 IETF に続いて 2 回目である。

¹⁰ rsync (遠隔のファイルやディレクトリを同期するソフトウェア)
<http://rsync.samba.org/>

第67回 IETF

第67回 IETF は2006年11月5日～10日、アメリカ・サンディエゴにある Sheraton San Diego Hotel & Marina で開かれた。会場の Sheraton Hotel はダウンタウンから車で15分ほど離れた所にある。サンディエゴ空港とヨットハーバーに隣接していて眺めは良いが、ショッピングセンターや飲食店はほとんど無く、また鉄道の駅が近くにない。そのためか IETF 開催中の夕方頃から夜にかけて、会場の裏手とダウンタウンの中心地にある Gaslamp 地区との間で参加者のためにチャーターされたバスが臨時運行されていた。

オンラインのサービスには、前回と同様にミーティング参加者向けのメーリングリストが提供されていた。更に今回は参加者が情報交換を行うためのブログと Wiki が設置されていた。メーリングリストでは Sheraton Hotel のゲストルームにあるインターネット接続機器の不具合や、会場の無線 LAN に関する情報交換が行われていた。

今回の IETF の参加登録者は1,199名で、41ヶ国からの参加があった。日本からの参加者は全体の10%強で、55%近くを占めるアメリカに次いで2番目の参加者数である。全体の人数はここ3回程では大きな変化はないようである。

初日の11月5日(日)に各種チュートリアルとレセプションが、11月6日(月)～11月10日(金)に WG と BoF が、8日(水)と9日(木)の夜に Plenary(全体会議)が行われた。

IETF Operations and Administration Plenary

IETF Operations and Administration Plenary は、IETF の運営全般に関する報告と議論が行われる全体会議である。この Plenary では、NOC(Network Operation Center) リポートやホストプレゼンテーション、IETF チェアの報告などが行われた。

NOC リポートでは IETF 会場のネットワークの利用状況などについて報告された。会場では毎回無線 LAN を使ったインターネットへの接続サービスが提供されており、最近では無線チャンネルの有効利用と効率化のために、802.11a の利用が推奨されている。IETF 期間中に 802.11a を利用していた端末は全体の25%程で、前回に比べて徐々にその数が増えつつあるようである。

IETF チェアの Brian Charpenter 氏からは、IASA (IETF Administrative Support Activity) と IAD (IETF Administrative Director) の活動報告が行われた。前回の第66回 IETF 以降二つの WG が設立され、12の WG がクローズ、現在120程の WG が活動しているとのことである。RFC は99出され、新規の Internet-Draft は440程作成されたとのことである。ちなみに去年の同じ期間には100程度の RFC が出され、新しい Internet-Draft は435作成されていたので、昨年と比べると若干少なかった模様である。

また今回はJon Postel賞¹¹の受賞者の発表があった。Jon Postel賞はRFCの編纂やIANAとしてIPアドレスの管理などに貢献したJonathan B. Postel氏にちなんで1999年に設けられたもので、技術的な貢献やリーダーシップの発揮といったコミュニティに対する継続的な貢献のあった人物に対して贈られる。受賞者は毎年選ばれ、クリスタルグロブと賞金2万ドルが贈られる。

今年の受賞者は、南カリフォルニア大学のISI(Information Sciences Institute)におけるRFC Editorのco-leaderであったJoyce K. Reynolds氏と、Bob Braden氏であった。Jon Postel氏より引き継いでRFCの編纂にあたり、RFCの品質向上や現在に至るRFCの認知度向上に対する貢献が称えられた。

会場での参加者の発言に基づいて議論を行うオープンマイクの時間には、主にIETFで提供されているツールに関して議論が行われていた。IETFによるツールの提供は、IETFの予算の中で行われているにも関わらず、開発の際に参加者が意見を出す機会が設けられていない、という指摘から議論が始まった。これについて、オープンソースにすることでノウハウがたまりやすくなる(と同時に多くの人の考えを反映できる)、ツールの位置付けを知っているところでないとか開発が難しいことから、事務局の契約が特定の会社に結びつきやすいのではないかと、といった意見が挙げられていた。その他に、IETFの音声継ぎは参加者でなくても聞くことができるが著作権の提示がないといった指摘が挙げられていた。この件についてはIPR(Intellectual Property Rights) WG¹²で議論されていく模様である。

Technical Plenary

Technical Plenaryは、IETF全体に関係した技術に関する議論を行う全体会議である。IABのチェアレポート、IRTFの活動報告、テクニカルプレゼンテーションなどが行われた。

IABのチェアレポートはIABチェアのLeslie Daigle氏によって行われた。IABではインターネットのアーキテクチャの観点で、WGとは独立したドキュメント作成を行っており、中にはRFCになっているものがある。最近作成されたドキュメントは以下の三つである。

draft-iab-iwout-report-00.txt

"Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"

¹¹ Postel Awards

<http://www.isoc.org/awards/>

¹² Intellectual Property Rights (ipr)

<http://www.ietf.org/html.charters/ipr-charter.html>

第3章 電子認証技術と技術文書策定に関する国際動向

draft-iab-multilink-subnet-issues-00.txt
"Multilink Subnet Issues"

draft-iab-net-transparent-00.txt
"Reflections on Internet Transparency"

はじめの Internet-Draft は、2006 年 3 月に行われた "IAB Unwanted Traffic Workshop" の報告である。Technical Plenary の後半でサマリー報告も行われた。質疑応答の際の Leslie Daigle 氏の補足によると、このワークショップは主に(コミュニティの)意識向上を図ることが目的であったようである。

インターネットの利用者に対する脅威は Code Red や Blaster ワームが流行した 2001 年～2003 年頃に比べて深刻になりつつある。ワークショップでは "アンダーグラウンドエコノミーの発展" を主な要因と位置づけ、現状の問題を明文化して今後の活動の方向性を探るための議論が行われた模様である。

ある Web サイトではクレジットカード情報や銀行口座に加えて、ISP で稼動しているルータのアカウントやボットネットが売り買いされている。このような経済活動の結果、スパムメールや DDoS 攻撃といった Unwanted Traffic を生み出す基盤が維持され、またマルウェア(不正な挙動をするソフトウェア)の発達を促すような競争が行われている、と言われている。一方でさまざまなデータが全て HTTP の中でやりとりされていたり不正行為を隠すための IP アドレスの詐称や、インターネットの経路広告の交換をハイジャックできたりしてしまうことなど、Unwanted Traffic を止められない現状が指摘されている。

これに対して、中長期的な対策と短期的にできる活動が挙げられた。中長期的には、まずルーティングのセキュリティ向上を図る点が挙げられた。そのため、IRR(Internet Routing Registry)の登録情報をクリーンアップして、経路情報の検証ができるようにすることが必要だと指摘された。次にボットネットを止めること、そして TCP の MD5 オプションやパットフィルタリングの BCP(Best Current Practice)といった既存の技術の普及を図ること、といった提案がなされた。

短期的にできることとしては、既に RFC になっている host requirement、route requirement、ingress filtering に関するドキュメントを更新することや、IAB による啓発活動、IRTF における効果的な対策に関する調査などが挙げられた。Security Area Director の Sam Hartman 氏によると、このワークショップのレポート¹³は興味深く、一読することが薦められていた。

Technical Plenary の後半では、IAB の Internet-Draft である "Reflections on Internet

¹³ "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"
<http://www.ietf.org/internet-drafts/draft-iab-iwout-report-00.txt>

Transparency¹⁴とIAB Routing and Addressing Workshopの報告が行われた。

このドキュメントはインターネットの原則的な考え方である「透過性」に関するもので、これまでのIABの見解を見直し、新たな透過性の考え方に関する議論を紹介したものである。プレゼンテーションではTCP/IPの階層モデルの中で、様々なプロトコルが透過性に影響する要素を持っているという点が紹介されていた。

IAB Routing and Addressing Workshop¹⁵は、2006年10月18日にオランダのアムステルダムで開かれたもので、近年の経路情報の増大にどのように対処すべきかについて、主にバックボーンオペレーターを対象として行われたものである。現在、Tier-1レベルのISPでは交換されている経路情報が20万経路に達しているという報告がある。もし現在のままIPv6とのdual stack(IPv4とIPv6を同時に使える構成)にすると50万経路に達するという予測が立っており、インターネットのアーキテクチャとしては規模拡張性に欠けるのではないかと指摘されている。会場では現在最も普及しているBGPにこだわらず、この問題を解決するための議論を行うBoFを今後開くことの提案があった。試しに会場で挙手をしてもらったところ、多くの人が賛成に手を挙げていた。その他にIPv6は今後様子を見ながら検証すべき、(ルーティングにおける)セキュリティに関する議論も必要である、といった意見が挙げられていた。

このワークショップは第53回RIPEミーティングの後、同じアムステルダムで行われていた。今後も、ISPのコミュニティとIETFのコミュニティの情報交換が進んでいくと考えられる。

3.4. 電子認証フレームワークに関連する動向

本節では、2006年度に限らずにIETFの活動の中で電子認証フレームワークに関連すると考えられる話題について述べる。

NewTrk WGにおける策定プロセスの議論

NewTrkは”New IETF Standards Track”の略で、IETFにおける標準化プロセスを見直すことを目的としたWGである。電子認証フレームワークを策定する活動は、IETFと同様かまたは「ノウハウの文書化と蓄積」に適する策定プロセスを持つことが考えられるため、IETFにおけるNewTrkの議論の内容は参考になると考えられる。

¹⁴ Reflections on Internet Transparency

<http://www.ietf.org/internet-drafts/draft-iab-net-transparent-01.txt>

¹⁵ The IAB Workshop on Routing and Addressing

<http://www.iab.org/about/workshops/routingandaddressing/index.html>

第3章 電子認証技術と技術文書策定に関する国際動向

このWGは2003年11月中旬に行われた第58回IETFで最初のBoFが開かれ、その後2005年7月末の第63回IETFまでに4回のWGミーティングが開かれた。

NewTrk BoFでは、既存の標準化プロセスを変更する必要性が確認された。当時上がっていた論点を以下に示す。

- 既存のように一つの段階ではなく複数の段階を設けること
- WG内での状態も文書として認めること
- 明確さの裏づけとなる複数の実装が確認できる段階の新設
- 著作権に関する確認の段階を設けること

また、以下の団体における標準化プロセスと比較が行われた。

- W3C
- ISO
- GGF
- Open Group
- ITU-T
- 3GPP

後にISD (Internet Standards Documentation) と呼ばれる新しい策定プロセスが提案された。しかしドキュメントのグループ化に関する詳細ルールについてWG内で意見が分かれた記録が残っている。

本WGは、電子認証フレームワークの為のドキュメントの策定プロセスを検討する際、以下の点で参考になることがわかる。

ドキュメント策定の段階の設計

IETFの策定プロセスでは、WG Last Call、IETF Last Callのようにコミュニティの大きさに応じた確認が行われている。段階を設けることで、一つの話題ないしドキュメントについて各段階でチェックすべき事項が明らかにできる。先の段階に進んだときに、当該の内容を見直す必要が出た場合には、適宜戻ってくる事ができる。

ドキュメントのグルーピング

IETFの策定プロセスでは、ドキュメントのグルーピングは行われておらず、RFCの中で関連するドキュメント(RFC)の番号が参考文献として引用されているにとどまっている。閲覧する側の立場では、関連した内容のドキュメントがグループ化されている方がドキュメントを参照しやすいと考えられる。しかしすべてのドキュメントがグルー

ブ化される必要はなく、その判断が著者に委ねられた場合にグループ化自体の品質が変化する可能性がある。

結果として、NewTrk WG は現行の策定プロセスをすぐに変更するまでの提案には至っていないが、既存の策定プロセスがもつ問題点とあるべき姿が明らかになった点は大きな成果であるといえる。電子認証フレームワークを作るための策定プロセスでは、特に著作権の扱いと各ドキュメントに対する確認方法について検討する必要があると考えられる。

3.5. PKIX WG における電子認証技術の動向

PKIX WG は” Public-Key Infrastructure (X.509)” WG の略で、ITU-T の X.509 として策定された公開鍵基盤を、インターネットの観点で標準化することを目的とした WG である。

本節では、PKIX WG の動向をわかりやすくするため、4～5年と1年程度の二つのスパンでまとめる。

PKIX WG の近年（4～5年）の動向

4～5年のスパンで見ると、PKIX WG では図にまとめたような話題が議論されている（本節で示す以下の図は、説明の為に作成したものである）



図 3-1 PKIX WG の動向

4,5年程の中期的な動向としては、“Certificate and CRL Profile”、応用的な証明書に関する RFC、オンラインの証明書検証プロトコルの3点がポイントとして挙げられる。

“Certificate and CRL Profile”は、電子証明書の形式と CRL (Certificate Revocation List – 証明書失効リスト) の形式を定めたものである。応用的な証明書は、電子証明書を使ってアプリケーションで電子認証を行うための標準化である。

オンラインの証明書検証プロトコルは、電子証明書の検証処理がある程度の計算機資源やネットワーク資源を使うことから、軽量の処理を行うための機器（例えば PDA や

携帯電話など)で、電子証明書の処理ができるようにするためのプロトコルである。

1年程の短期的な動向としては、“Hash Algorithm Agility”、“リソース証明書”の2点が挙げられる。以降では、各々の動向の内容について述べる。

“Certificate and CRL Profile”は、数年来に渡って改訂が進められてきた(図3-2)。改訂に伴い、詳細な標準化が必要であると考えられる機能や処理内容については別のRFCとしてまとめ直されるなどしている。図3-2ではこれらを「派生」と呼んでいる。

Certificate and CRL Profile

- 変遷
 - rfc2459(1999/01) rfc3280(2002/04), rfc4325(2005/12), [rfc3280bis](2006?) WG Last Call
- rfc3280bis
 - 名前形式のセマンティクス [詳述]
 - 証明書拡張の要件 [詳述]
 - CRLv2の書式 [詳述]
 - パス検証の詳述 [追加]
- 派生
 - rfc3647: Certificate Policy
 - rfc4158: Path Building
 - rfc4325: CRL AIA rfc3280bisに統合

2006年度 社団法人日本ネットワークインフォメーションセンター 4

図 3-2 Certificate and CRL Profile の動向

RFC2459 は日本国内における PKI の普及の始まりの頃に出された RFC で、2006 年現在では RFC3280 に置き換わっている。RFC3280 を置き換える次のバージョンはいくつかの詳細化と追記が行われ、WG Last Call の段階にある。記述の詳細化が行われたのは、電子証明書に入れられる名前形式のセマンティクス(形式)、証明書拡張(extension)の要件に関する記述、CRL バージョン 2 の書式、電子証明書の発行関係を確認するパス検証などについてである。また RFC3280 の作成に伴い、いくつかのドキュメントが派生した。rfc3647: Certificate Policy (電子証明書の発行状況や管理に対する想定を記載したもの)、rfc4158: Path Building (電子証明書の検証のために、発行した認証局を辿っていくルールなど)、rfc4325: CRL AIA (CRL を発行した認証局の証明書を得るための情報)である。RFC4325 は今後 RFC3280 の後継バージョンに統合される予定となっている。

通信相手の認証を行う為の Protokol として使ったり、電子証明書の書式を使ってアプリケーション機能を実現したりするような、応用的な証明書の RFC の作成が進められている (図 3-3)。



図 3-3 応用的な証明書に関する RFC のリスト

「PPP and WLAN (rfc4334)」はパソコンを ISP や企業に接続する際などに使われている Point-to-Point Protocol や WLAN (Wireless LAN – 無線 LAN) における電子認証のために電子証明書を使うための電子証明書の扱い方を策定したものである。

「Proxy Certificate (rfc3820)」は、様々な理由で本人性確認のための証明書よりも代理で権限を行使できるようなアクセスを実現するための証明書の書式を策定したものである。

「IP address and AS Identifiers (rfc3779)」は電子証明書の中に IP アドレスや AS 番号を入れ、それらのアドレス資源の利用権限や管理権限を示す電子証明書の書式を策定したものである。APNIC において実験が進められているリソース証明書で使われている書式である。

「Logotypes (rfc3709)」は電子証明書の中に画像のデータを入れ、ユーザが電子証明書を識別しやすくするための書式を策定したものである。

これらの電子証明書を応用するための書式の出現によって、電子証明書を利用する場面が増えると共に、電子証明書が持つ意味も多様化しつつある。特に「IP address and AS Identifiers (rfc3779)」は個々の電子証明書をユーザの識別ではなく、アドレス資源の

利用権限の確認に使われるため、電子証明書に含まれる値の扱い方が、人による識別よりもプログラムによる識別に重点を置いたものになっている。

電子証明書の利用場面が増えると、電子証明書を処理するプログラムが必ずしも計算機資源を豊富に持つ環境で実行されない場合を想定する必要がでてくる。例えば PDA や携帯電話のように、通信帯域が限られていたり計算能力のために電力を多く消費しない方がよい計算機環境がある。電子証明書の内容に応じて処理結果を変化させるようなプログラムで処理されることは重要であるが、計算処理や通信帯域を要する電子証明書の処理を他のコンピューターに任せ、その結果のみを利用するという考え方もある。この処理を実現するのが「オンラインの証明書検証プロトコル」である（図 3-4）。



図 3-4 は「オンラインの証明書検証」に関するスライドのスクリーンショットである。スライドのタイトルは「オンラインの証明書検証」で、左側には黄色、赤、青の幾何学的なデザインがある。リストには以下の項目が記載されている。

- Server-based Certificate Validation Protocol - SCVP (draft-ietf-pkix-scvp-31.txt)
- Delegated Path Validation and Delegated Path Discovery (DPV/DPD) (rfc3379)
- Lightweight OCSP (draft-ietf-pkix-lightweight-ocsp-profile-08.txt) in IESG
 - Online Certificate Status Protocol - OCSP (rfc2560)

スライドの下部には「2006年度 社団法人日本ネットワークインフォメーションセンター 6」と記載されている。

図 3-4 オンラインの証明書検証プロトコル

オンラインの証明書検証プロトコルは、大きな処理能力を持たない PDA や携帯電話などの機器でも電子証明書を扱えるようにするものである。「Server-based Certificate Validation Protocol – SCVP」は電子証明書の検証を検証専用のサーバに任せてしまうプロトコルである。証明書を検証するための情報の入手などもサーバに任せてしまうため、クライアントは電子証明書を処理する必要がない。

「Delegated Path Validation and Delegated Path Discovery (DPV/DPD)」は、パス検証 (Path Validation) とパス構築 (Path Discovery) をサーバに任せるもので、電子証明書の検証方針などをクライアント側が持つことができるプロトコルである。パス検証やパス構築といった計算能力や、通信帯域を要する処理をサーバに任せることができる。

「Lightweight OCSP」は Online Certificate Status Protocol の軽量版で、メッセージサイズを小さくするなどの工夫がなされたものである。サーバが証明書の検証した結果に対して、クライアントが検証を行うため、このほかのプロトコルよりもクライアント側に処理能力が必要とされるが、メッセージサイズなどの工夫によって一度に大量の処理ができるような効果が期待できる。

PKIX WG の近年（ここ1年）の動向

SHA-1 などの一方向性ハッシュアルゴリズムを弱体化する攻撃方法が実証されたことを受け、PKIX WG ではこのアルゴリズムの代替手段が検討されてきた。

新たなアルゴリズムをはじめから検討することは、IETF のプロトコル策定の場ではなく研究の分野で行われるべきであるという考え方から、PKIX WG では既存のプロトコルに対して「Hash Algorithm Agility」と呼ばれる考え方を導入することとしている。これはアルゴリズムを代替できるようにするもので、単に書式として変えられるようにするだけでなく、例えば電子証明書を検証する側の処理がしやすいように、扱うことができるアルゴリズムの一覧を事前に伝達できるような工夫が行われることが考慮されている。一方、代替手段となるアルゴリズムを選択する作業は米国の NIST (National Institute of Standards and Technology) にて行われている。

Hash Algorithm Agility (1 / 2)

- 背景
 - NIST brief comments on Hash Standards (2004/08)
 - 2010年までにSHA-2 (SHA-256, SHA-386, SHA-512)へ移行
 - SAAG in IETF-64
 - Security Area Response to Hash Function Breaks
 - “Directives to WGs/Chairs:
Do analysis on every protocol in the WG by IETF 65
Start standards work on transition to sha-256, but plan for future transitions.”

2006年度 社団法人日本ネットワークインフォメーションセンター 8

図 3-5 IETF における Hash Algorithm Agility の動向

多くのベンダーによる認証局の実装に、共通のアルゴリズムを導入させるためには、指

針となる期限やアルゴリズムの候補が必要であるという考え方から、NIST では 2010 年までに SHA-2 シリーズのアルゴリズムを実装するというコメントを発表している。また IETF でも既に第 64 回 IETF で SHA-256 (SHA-2 シリーズのアルゴリズムの一つ) を使ったプロトコルへ移行する方針を打ち出した (図 3-5)。

PKIX WG では初めに OCSP を取り上げ、Hash Algorithm Agility への対応が進められることになっている (図 3-6)。

Hash Algorithm Agility (2 / 2)

- PKIX WGでの活動
 - OCSP Algorithm Agility
 - 送信元のエンティティが扱うことのできるアルゴリズムの識別子を証明書拡張として入れておく。
 - X.509 Certificate Extensions for S/MIME Capabilities (rfc4262)

2006年度 社団法人日本ネットワークインフォメーションセンター 9

図 3-6 PKIX WG における Hash Algorithm Agility への対応

OCSP ではリクエスト側(証明書検証を依頼するクライアント)がレスポンス側(証明書検証の依頼を受け付けるサーバ側)の返答につけられた署名検証を行う必要がある。そこでリクエスト側が、レスポンス側が使う可能性がある一方向性ハッシュアルゴリズムを知っておくことができれば、リクエストを行う前にレスポンス側に証明書検証の依頼を出すべきかどうかを判断できる。この機能は電子メールにおける電子署名機能の標準である S/MIME でも同様であり、すでに rfc4262: X.509 Certificate Extensions for S/MIME Capabilities でドキュメント化されている。

リソース証明書の動向

電子証明書を用いて IP アドレス等のアドレス資源の管理を安全にする仕組みであるリソース証明書は、主に SIDR (Secure Inter-Domain Routing) WG で議論されている。SIDR WG は APNIC の Geoff Huston 氏と SPARTA 社の Sandra Murphy 氏がチ

エアを務めている WG で、第 65 回 IETF から第 68 回 IETF にかけて 4 回のミーティングが行われている。RPSEC (Routing Protocol Security) WG と異なり、新たなセキュリティの仕組みを提案し策定することを目的としており、そこで検討に使われるセキュリティ要件は RPSEC WG での議論に基づいて行われるものとされている。

第 65 回 IETF で BoF として行われた SIDR のミーティングでは、リソース証明書を中心とする電子証明書を基本とする新たなルーティングセキュリティの仕組みと、BGP (Border Gateway Protocol) における安全性の強化の 2 つの仕組みに関する RFC の策定に取り組むこととなった()。しかし第 66 回 IETF 以降の WG となって以降のミーティングでは、主に前者の電子証明書の議論が主に取り上げられている。


リソース証明書関連動向 (1 / 4)

- Secure Inter-Domain Routing WG(2006/03)
 - RFC3779を踏まえたI-D
 - draft-ietf-sidr-res-certs-01.txt
 - draft-huston-sidr-repos-struct-00.txt
 - S-BGP提案者Stephen Kent氏、名前仕様の内容と
トラストポイントを規定することに疑問
 - TCP MD5オプションの鍵変更や別の方式に関する
議論
 - Steven Bellovin氏によって淡々と進む

2006年度 社団法人日本ネットワークインフォメーションセンター 10

図 3-7 SIDR WG におけるリソース証明書の動向

SIDR WG における議論によって、RIR によるリソース証明書の管理運用と、BBN 社の Stephen Kent 氏が提案した S-BGP (Secure BGP) によるリソース証明書の利用という構造が作られつつある。PKI の概念を踏襲するという考え方によるためか、PKIX WG との JOINT ミーティング (合同ミーティング) が開かれることがあり、いくつかの課題について PKI の概念を使うことで解決を図っている (図 3-8)。



リソース証明書関連動向(2 / 4)

- PKIX WGとのJointミーティング
(内容はSIDR WGの続き)
 - Address Space & As Number PKI (60 min.)
 - 話題
 - RIRによる認証局の運用
 - RIR間のアドレス・ブロックの移動への対処方法
 - 信頼点(Trust Anchor)
 - 質疑(木村分)
 - 「日本ではJPNICの認証局がJPコミュニティに"信頼点"を提供している。ユーザが信頼点を選べるのならば、RIRだけでなくJPNICの認証局も使えるか？」 「Yes」 by Stephen Kent

2006年度 社団法人日本ネットワークインフォメーションセンター 11

図 3-8 リソース証明書に関する Joint ミーティング

しかし、リソース証明書は「アドレス資源の利用/管理権限」を表す証明書であって管理者の認証のために利用されるものではないという考え方から、証明書リポジトリのアクセス方法や証明書の発行先を示す Subject フィールドの値が独自の形式を持っている。これらの独自の形式は APNIC におけるリソース証明書プロジェクトを通じて考案されたもので、主にチェアの Geoff Huston 氏によって提案されている。

APNIC ではリソース証明書のプロジェクトを 2006 年 4 月頃から開始しており、2007 年末にプロジェクトが一旦終了し、APNIC から IP アドレスの割り振りを受けているメンバー向けの Web ページ MyAPNIC で利用のためのインターフェースが実験的に提供される予定になっている(図 3-9)。

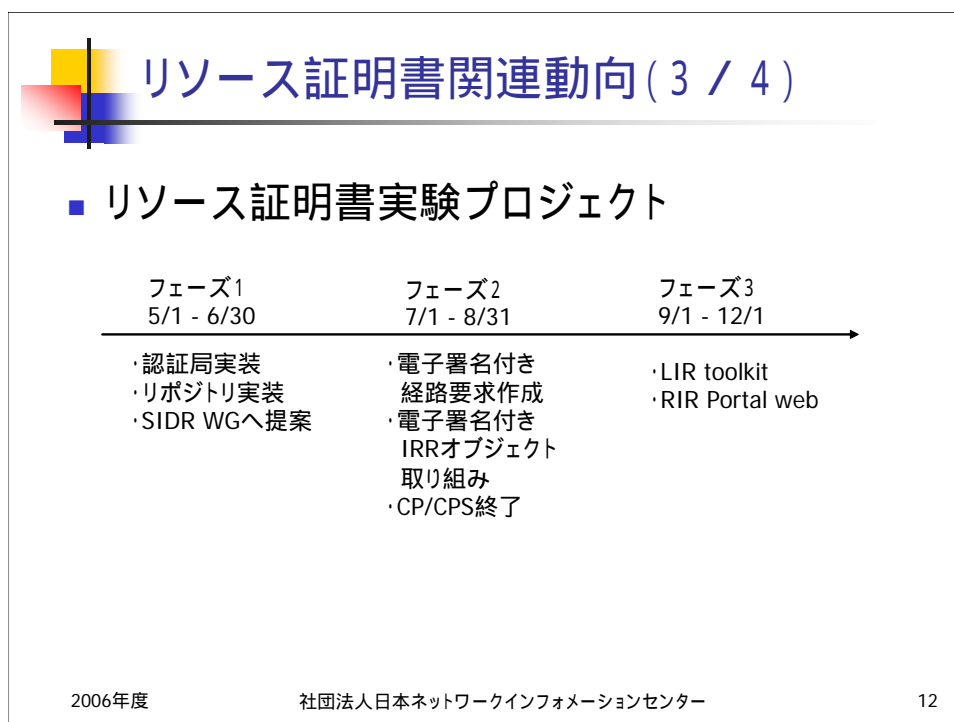


図 3-9 APNIC のリソース証明書プロジェクト

リソース証明書における課題

リソース証明書は PKI を用いてアドレス資源の利用 / 管理権限を示す電子証明書の中で、APNIC ではアドレス資源のより厳密な管理のために資する有効な手段だと位置づけられていると言える。一方、提唱されているリソース証明書には技術的な課題がある。一つはアドレス資源の移管のサポートとアドレス資源管理の実効性である。

RIPE NCCにおけるERXプロジェクト¹⁶のように、アドレス資源はRIRの間で移管が行われることがある。これは頻繁に起こることではないが技術的に対応できなければ実施ができなくなってしまう。APNICでは移管が起こりうる状況でもRIR同士で齟齬のないリソース証明書が発行できるようにするため、各々のRIRに移管用の認証局を設け、移管されたアドレス資源の証明書はその認証局によって収容されるものを提案している。これにより各RIRは他のRIRに管理されているアドレス資源のリソース証明書を発行することができなくなる一方、認証局の構造の複雑さと管理負荷が上がるという課題がある。

またリソース証明書の実効性については、割り振り情報 / 割り当て情報の正確性を向上させるわけではないことから、本来有効かどうかがわからない証明書が普及してしまうという懸念がある。その場合、リソース証明書が無効になった場合に、割り振り先組織への割り振りを停止してよいかどうか分からない事態に陥り、結果的にリソース証明

¹⁶ Early Registration Transfer [ERX] Project
<http://www.ripe.net/projects/erx/index.html>

書を導入する意味がなくなってしまう。

RIPE NCCはAPNICのリソース証明書の開発プロジェクトに協力しつつも、これらの課題に対して静観しておりその効果を評価するプロジェクトを立ち上げている¹⁷。

3.6. まとめ

本章では主に IETF への参加を通じて調査した、ドキュメント策定プロセスと電子認証技術、およびリソース証明書に関して述べた。IETF では RFC の策定プロセス自体に対する議論も盛んに行われており、RFC を効果的に策定し、また理念に即した形で議論できるような基盤が再確認された。

電子認証フレームワークの策定は、IETF と異なり技術自体ではなくノウハウの蓄積を目的とするものであるが、活動の中立性およびオープンさの維持、新技術をいち早く取り入れる意味では、IETF における段階定義や簡便な提案手続き、オープンな情報公開などは参考になる手法であると考えられる。

PKIX WG では近年、電子証明書技術の派生的および応用的な RFC が策定されつつあり、また携帯電話や PDA といった処理能力が小さい端末をサポートできるようなサーバを使った電子証明書の検証プロトコルが策定されつつある。また一方向性ハッシュアルゴリズムの攻撃可能性の向上に伴い、SHA-2 への対応方針が取られ、実施されつつある。

SIDR WG では、RIR におけるリソース証明書プロジェクトと連携する形でリソース証明書関連の RFC の策定が進められている。リソース証明書にはいくつかの技術的な課題があり、RIPE NCC などの RIR では採用に慎重な姿勢を保っている。

RIPE NCC 等の RIR ではリソース証明書の有効性に関する議論が行われつつあり、今後も注目していく必要があると考えられる。

¹⁷ RIPE Certification Task Force
<http://www.ripe.net/ripe/tf/certification/index.html>

第3章 電子認証技術と技術文書策定に関する国際動向

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

第4章 経路情報の登録機構の設計と構築

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。



18

IRRに登録される情報に対するチェックの考え方

- レジストリにおけるIRRの登録情報の正しさ
 1. IRRに情報登録するユーザの正しさ
 - IRRに登録するユーザは認証されている
 2. routeオブジェクトの登録に関する正しい認可
 - IPアドレスを割り振られたIP指定事業者による、ASオブジェクトやrouteオブジェクトの情報登録者(メンテナ)に対する認可がある
 3. 登録情報のIPレジストリシステムとの整合性
 - AS番号やIPアドレスは、インターネットレジストリによって割り振り/割り当てられている

社団法人日本ネットワークインフォメーションセンター

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 (Maintainer) 情報が登録されている。メンテナ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

第4章 経路情報の登録機構の設計と構築

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するメンテナを指定する。指定されたメンテナは、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られることができる。

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。

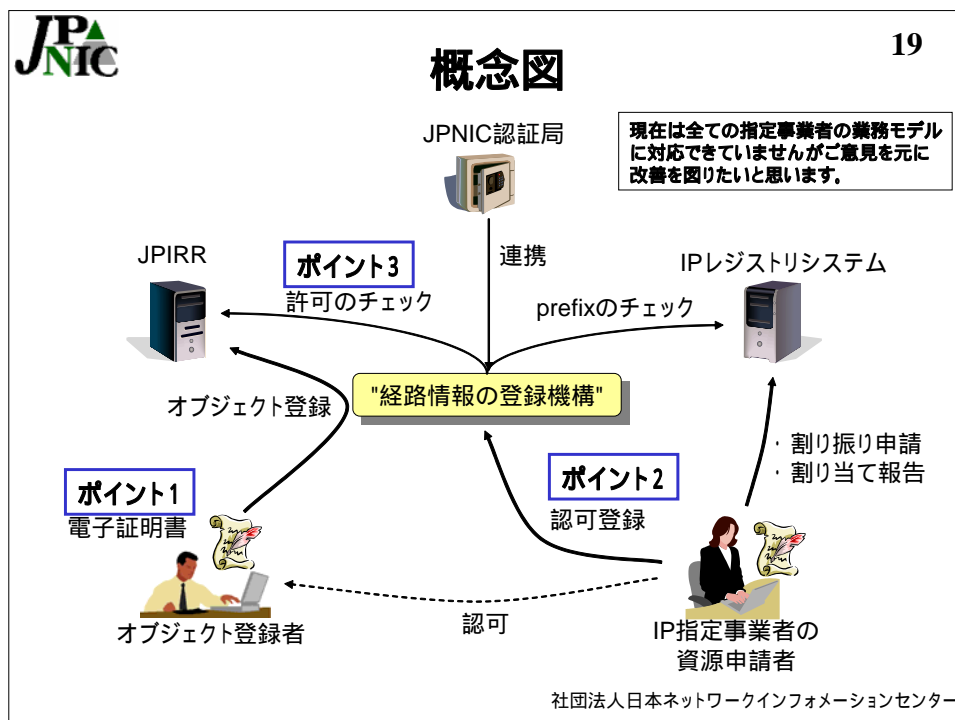



図 4-2 経路情報の登録機構の機能概要

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。

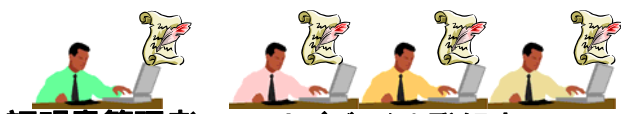
ポイント 1 : JPIRR ユーザ向け電子証明書



ポイント1: JPIRRユーザ向け電子証明書

20

- JPIRR証明書管理者
 - オブジェクト登録者の証明書を発行 / 失効
- オブジェクト登録者
 - S/MIMEの電子署名を使ってIRRのオブジェクトを登録



証明書管理者 オブジェクト登録者

mmtnerオブジェクトのadmin-c、tech-c

社団法人日本ネットワークインフォメーションセンター


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


21

ポイント2：許可リストを使った認可登録(1 / 2)

許可リスト

prefix (登録できる範囲)	許可 / 禁止	メンテナー	Origin AS (optional)
1.1.0.0/16	allow	mnt1	12345
1.1.0.0/17	allow	mnt2	

社団法人日本ネットワークインフォメーションセンター

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。

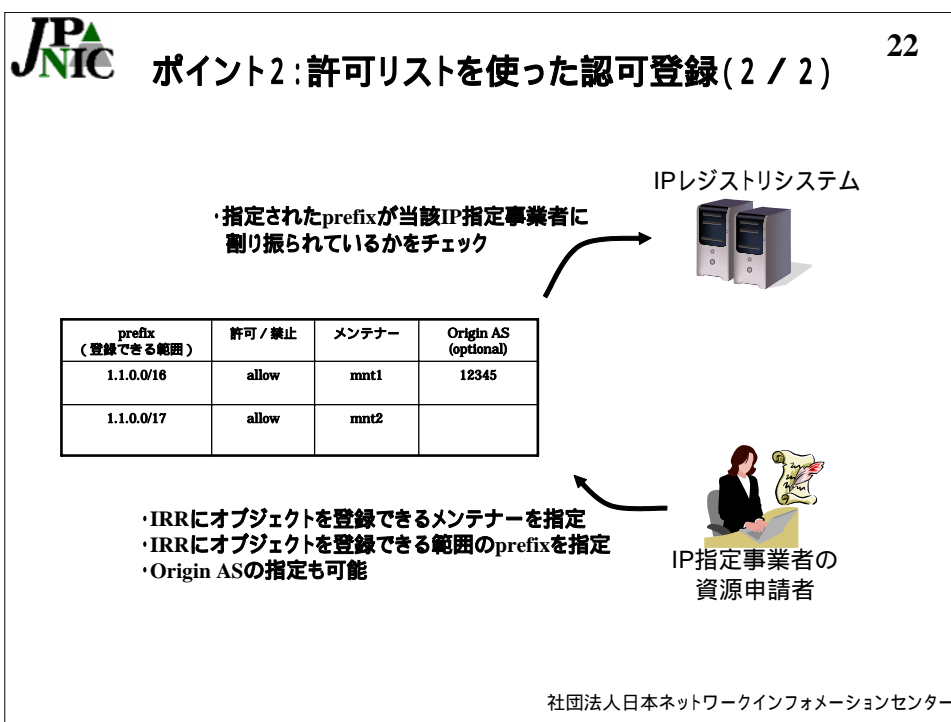


図 4-5 許可リストへの登録

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

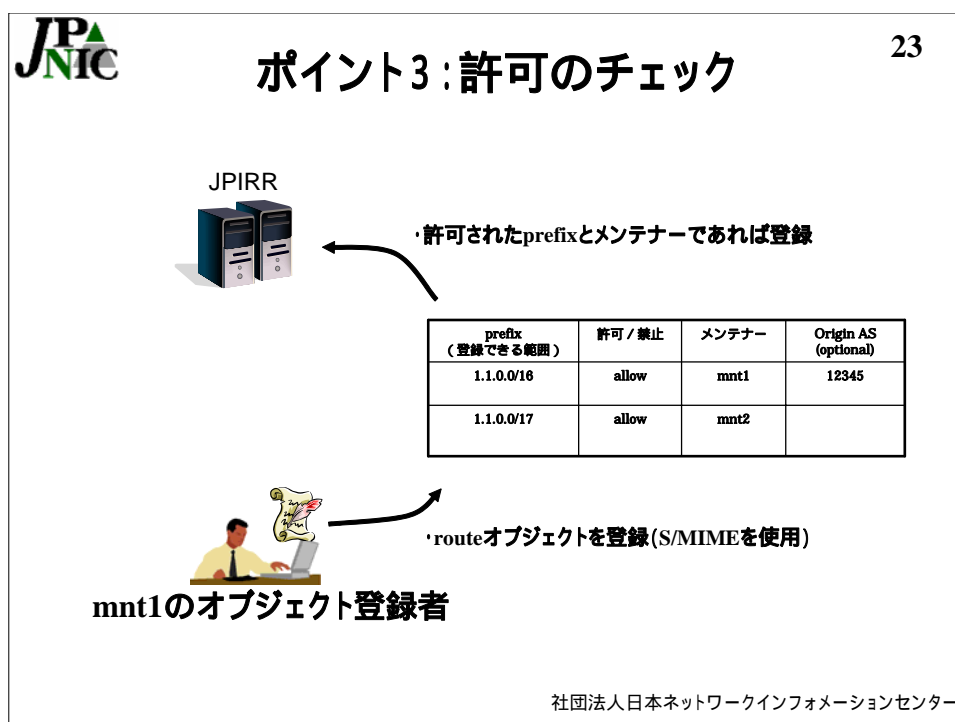


図 4-6 許可のチェック

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。


	<h2>得られる効果</h2>	24
<ol style="list-style-type: none">1. IRRに情報登録するユーザの正しさ<ul style="list-style-type: none">- 電子証明書でユーザの認証を担保できる。2. routeオブジェクトの登録に関する正しい認可<ul style="list-style-type: none">- 許可リストに載ったメンテナだけが、IP指定事業者が指定したprefixの範囲で登録できるようになる。3. 登録情報のIPレジストリシステムとの整合性<ul style="list-style-type: none">- 割り振られていないような不正なprefixが登録されなくなる。		
<small>社団法人日本ネットワークインフォメーションセンター</small>		

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だけの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。

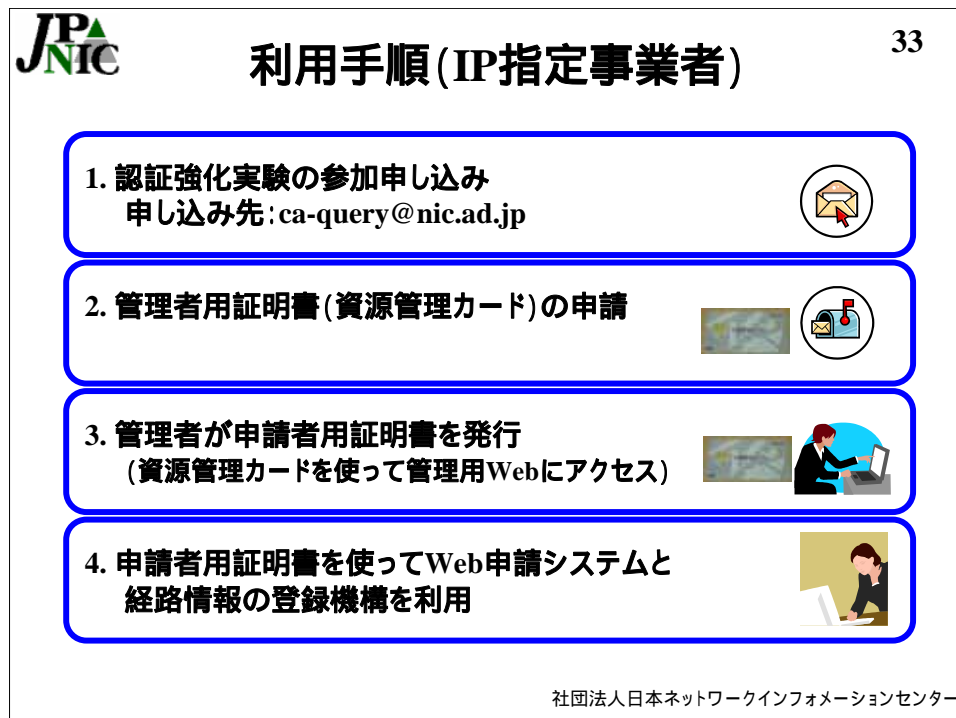


図 4-8 IP 指定事業者の利用手順

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。

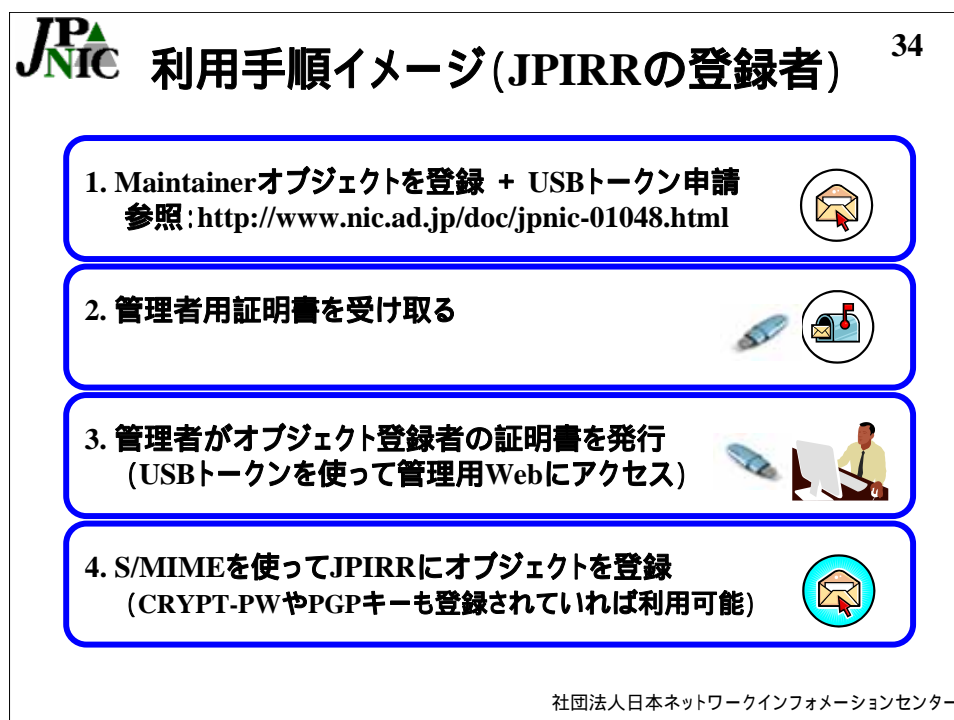


図 4-9 JPIRR の情報登録者の利用手順

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。

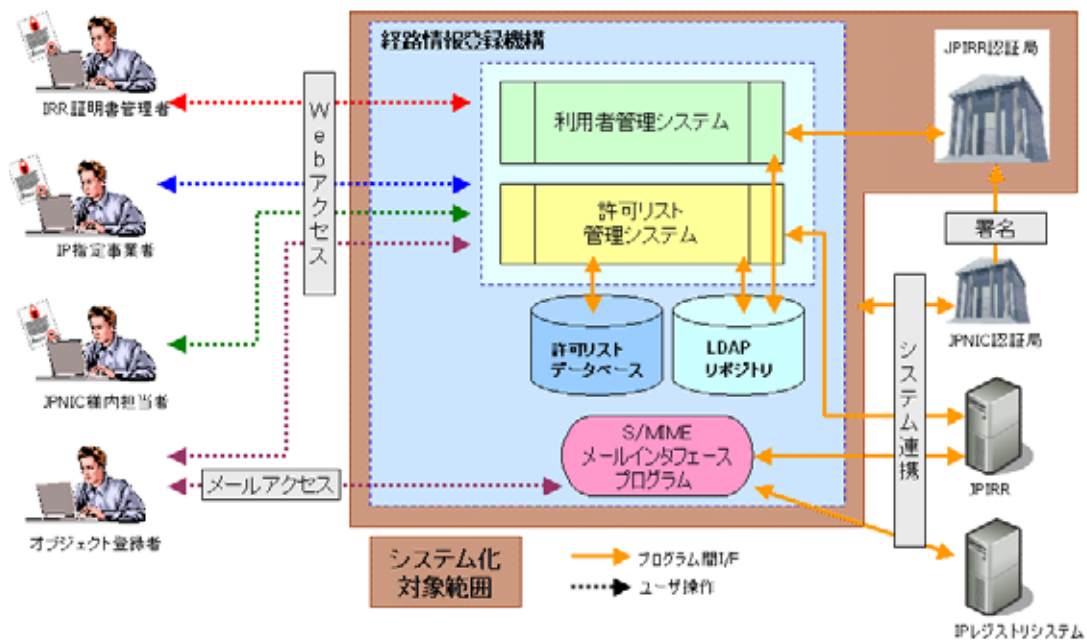


図 4-10 経路情報の登録機構のシステム構成

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イ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。

第4章 経路情報の登録機構の設計と構築

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。

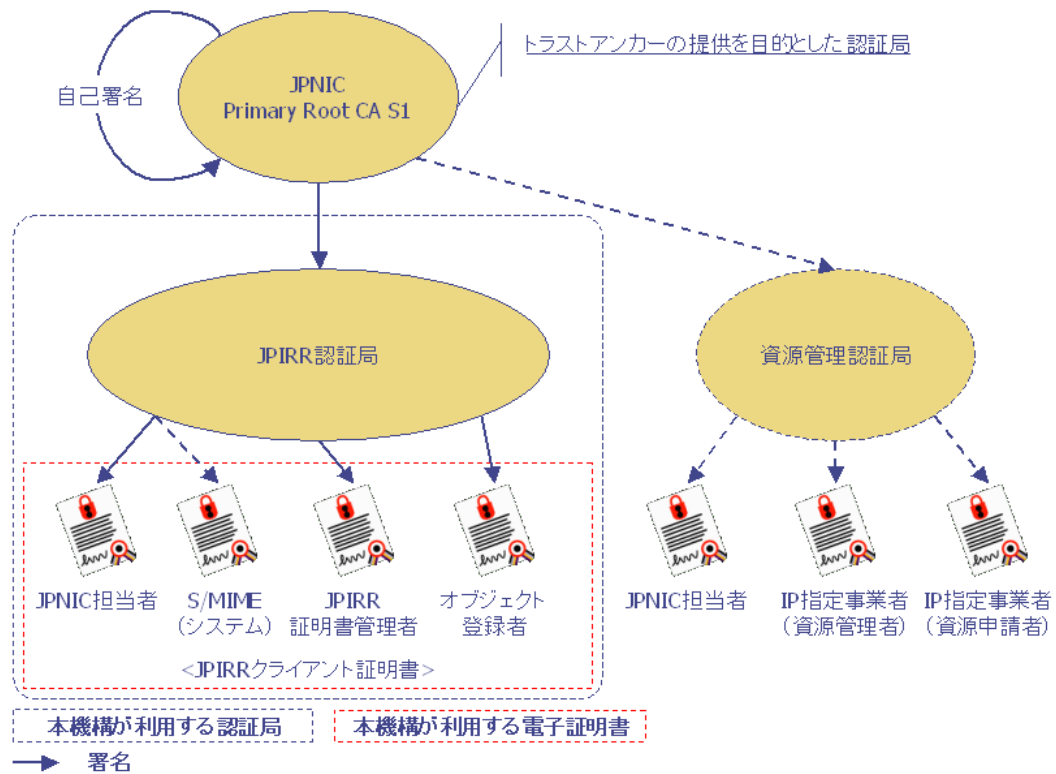


図 4-11 JPNIC 認証局の階層構造

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。

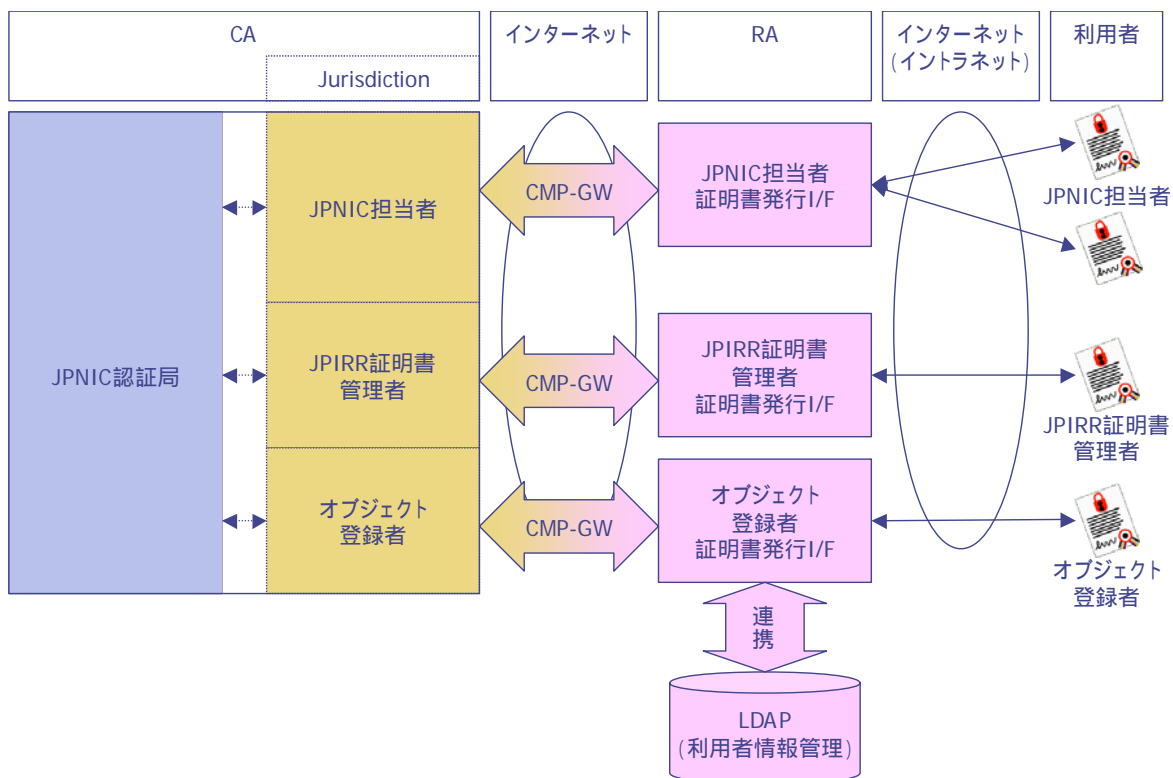


図 4-12 JPIRR 認証局の論理構成

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け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。

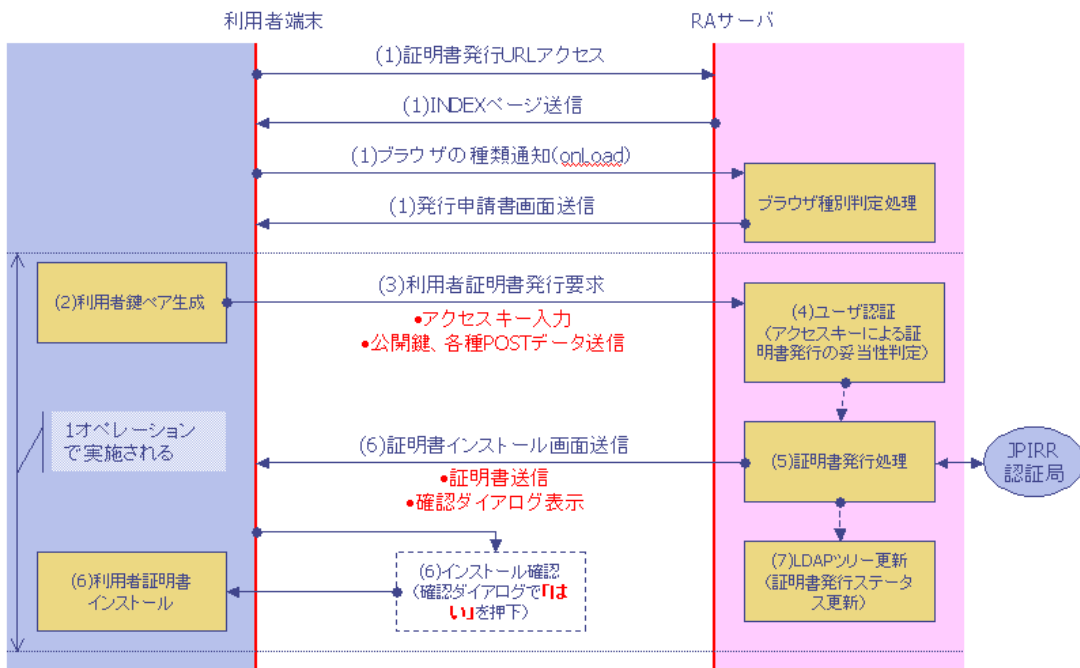


図 4-13 証明書発行 I/F 処理フロー

- 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け付け、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

第4章 経路情報の登録機構の設計と構築

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 CMP¹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。

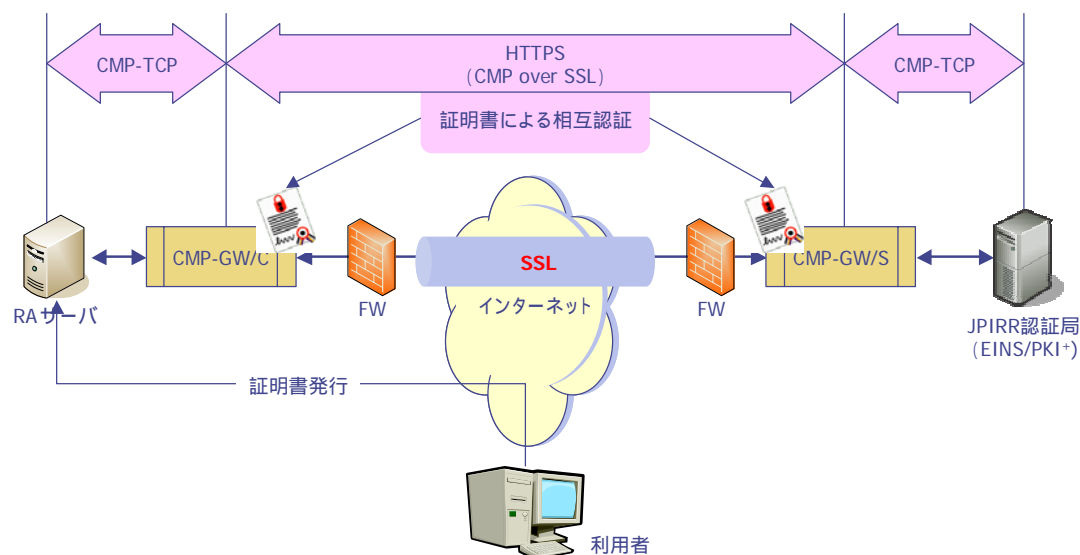


図 4-14 CMP ゲートウェイシステム (CMP-GW)

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	

第4章 経路情報の登録機構の設計と構築

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ィール

表 4-2 JPIRR 認証局 詳細プロフィール(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。

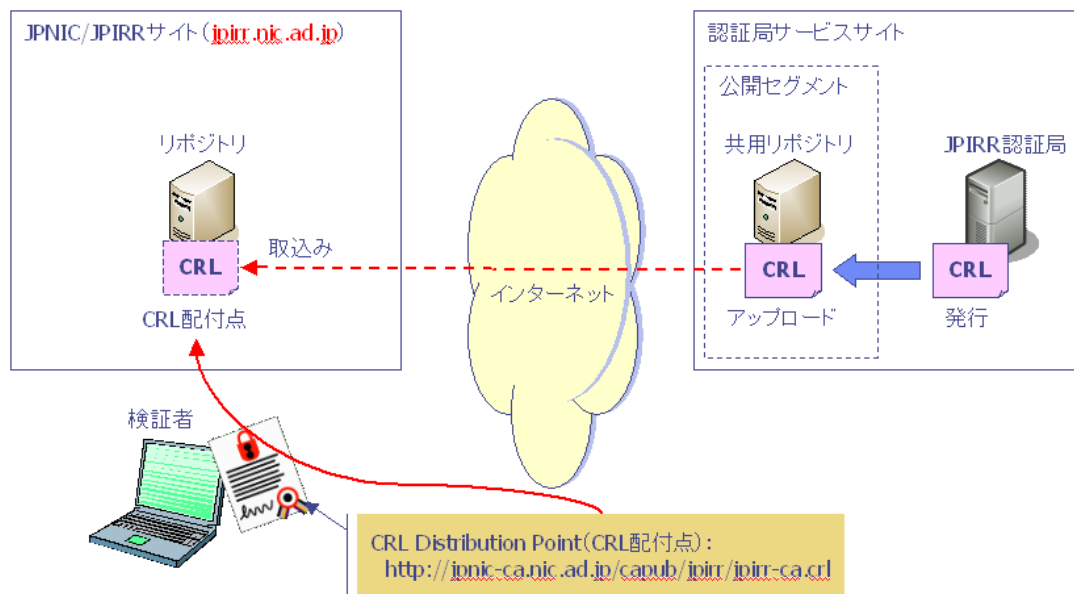


図 4-15 JPIRR 認証局 CRL 詳細プロフィール

第4章 経路情報の登録機構の設計と構築

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。

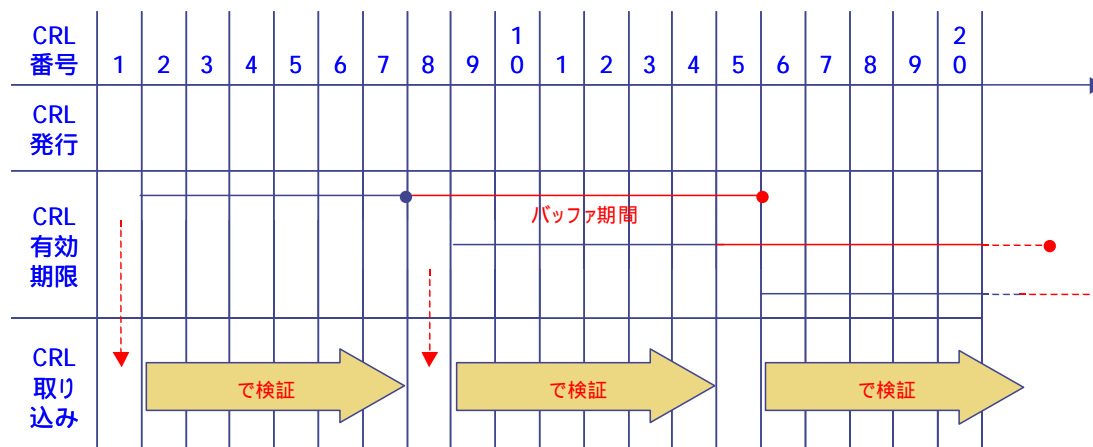


図 4-16 CRL の発行周期、有効期限と Web サーバでの取り込み

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	<p>JPIRR 認証局を管理・運営し、本機構に係る、次の業務を行う。</p> <ul style="list-style-type: none"> • 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	<p>次の役割を持つ。</p> <ul style="list-style-type: none"> • 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	<p>JPIRR へのオブジェクトの登録申請を行う。</p> <ul style="list-style-type: none"> • 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

DN	利用者			
	JPNIC 担当者		JPIRR 証明書 管理者	オブジェクト登録者
	S/MIME I/F			
C	“ JP ”			
O	“ Japan Network Information Center ”		“ Resource Holder ”	
O			“ ASN Holder ”	
OU	“ Internet Resource Service ”		“ IRR Maintainer Administrator ”	“ IRR Object Registrant ”
OU	“ Secretariat ”		(付与された利用者の管理対象のメンテナ名)	(付与された利用者の管理対象のメンテナ名)
OU	“ IRR Administrator ”			
CN	以下の各項目を半角スペースで区切り、併記。 “ IRR-AD ” [64文字以内の任意の名称] シーケンス番号… および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 ”。	以下の各項目を半角スペースで区切り、併記。 “ Secure MIME Gateway ” 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 ”。	以下の各項目を半角スペースで区切り、併記。 IRR-MA ” メンテナオブジェクトの admin-c 項目 シーケンス番号… およびの組合せ(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 ”。	以下の各項目を半角スペースで区切り、併記。 “ IRR-OR ” メンテナオブジェクトの tech-c 項目 シーケンス番号… 及びの組合せ(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 ”。

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) keyEncipherment (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://jpnica.nic.ad.jp/capub/jp-irr/jp-irr-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://jpnica.nic.ad.jp/capub/jp-irr/jp-irr-ca.crl	

第4章 経路情報の登録機構の設計と構築

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 認証局に係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。

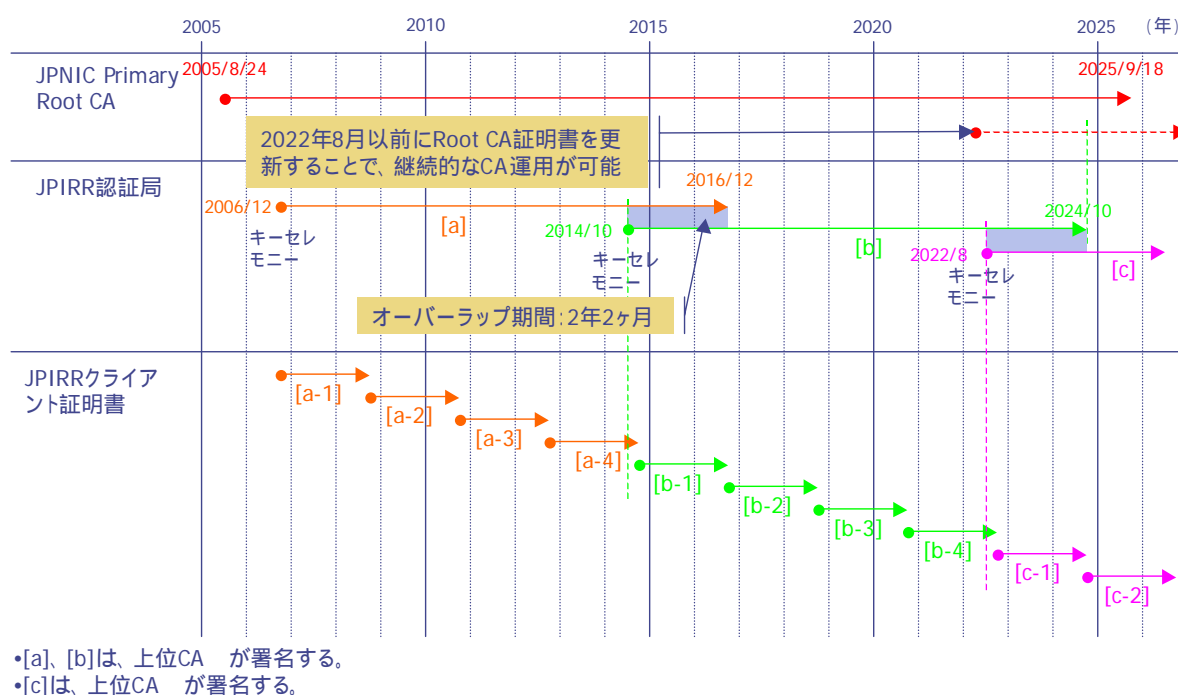


図 4-17 JPIRR 認証局の更新周期 (ライフサイクル)

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

第4章 経路情報の登録機構の設計と構築

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き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。

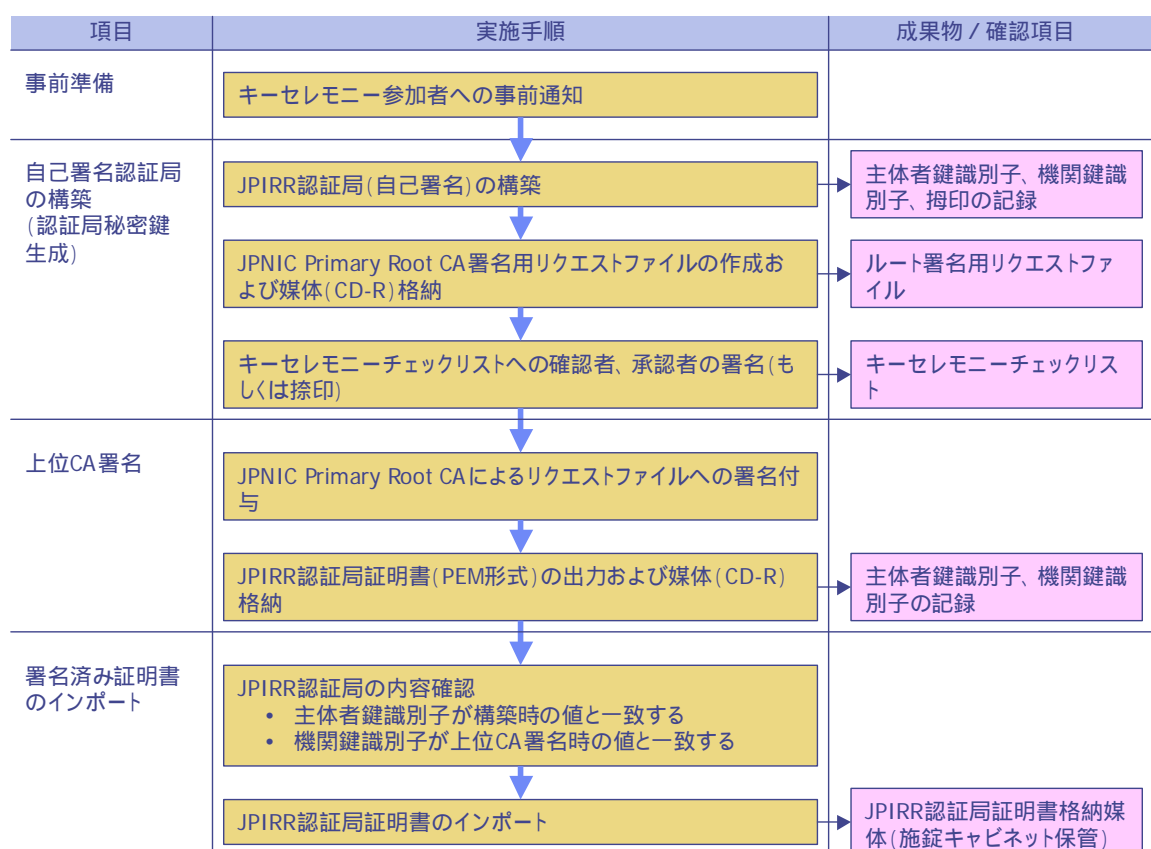


図 4-18 キーセレモニー実施手順

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。

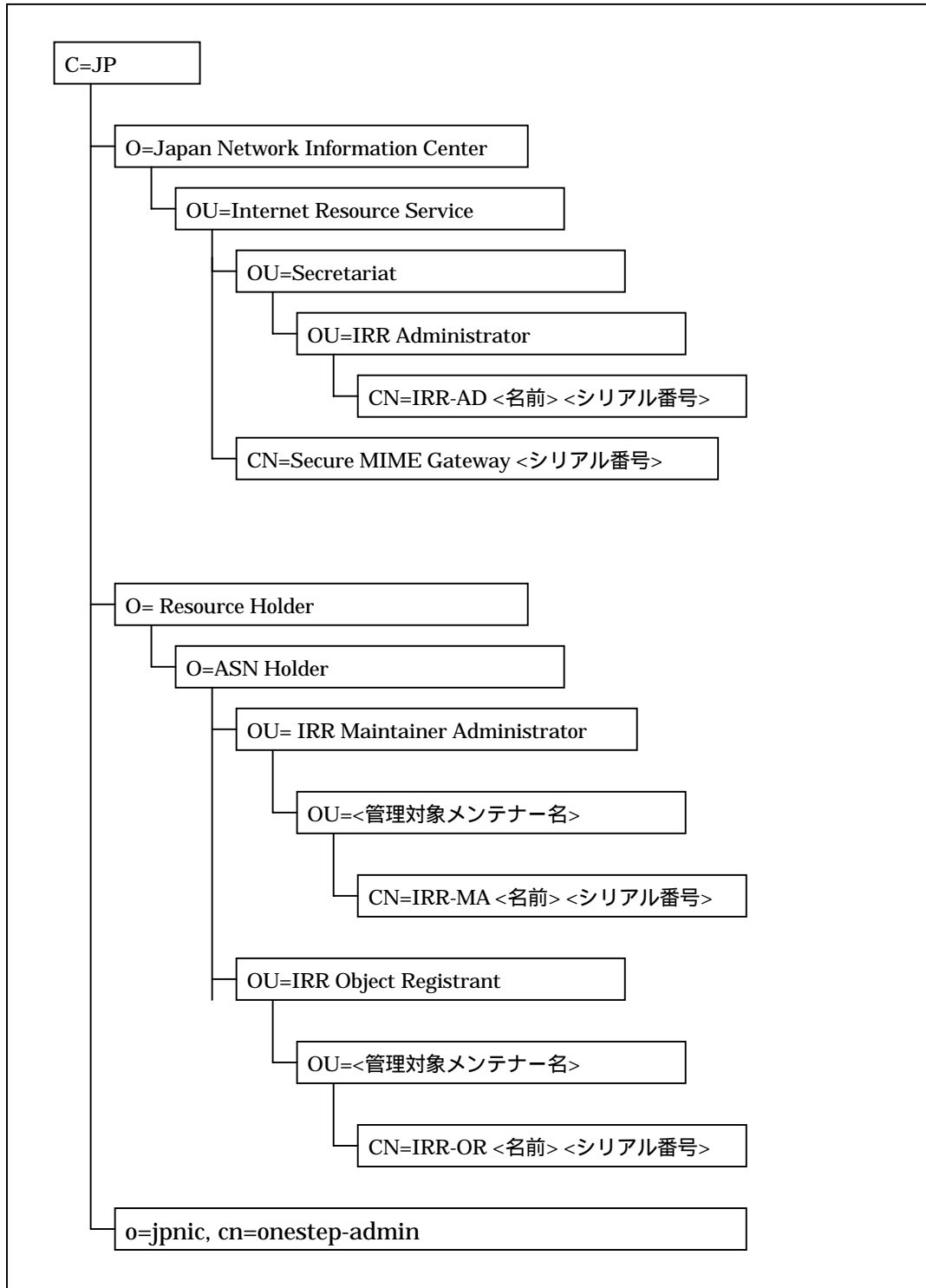


図 4-19 リポジトリ構成

第4章 経路情報の登録機構の設計と構築

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

第4章 経路情報の登録機構の設計と構築

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

第4章 経路情報の登録機構の設計と構築

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

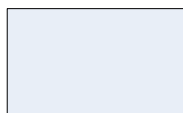
利用者情報として管理する主な項目は表 4-14 の通りである。

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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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



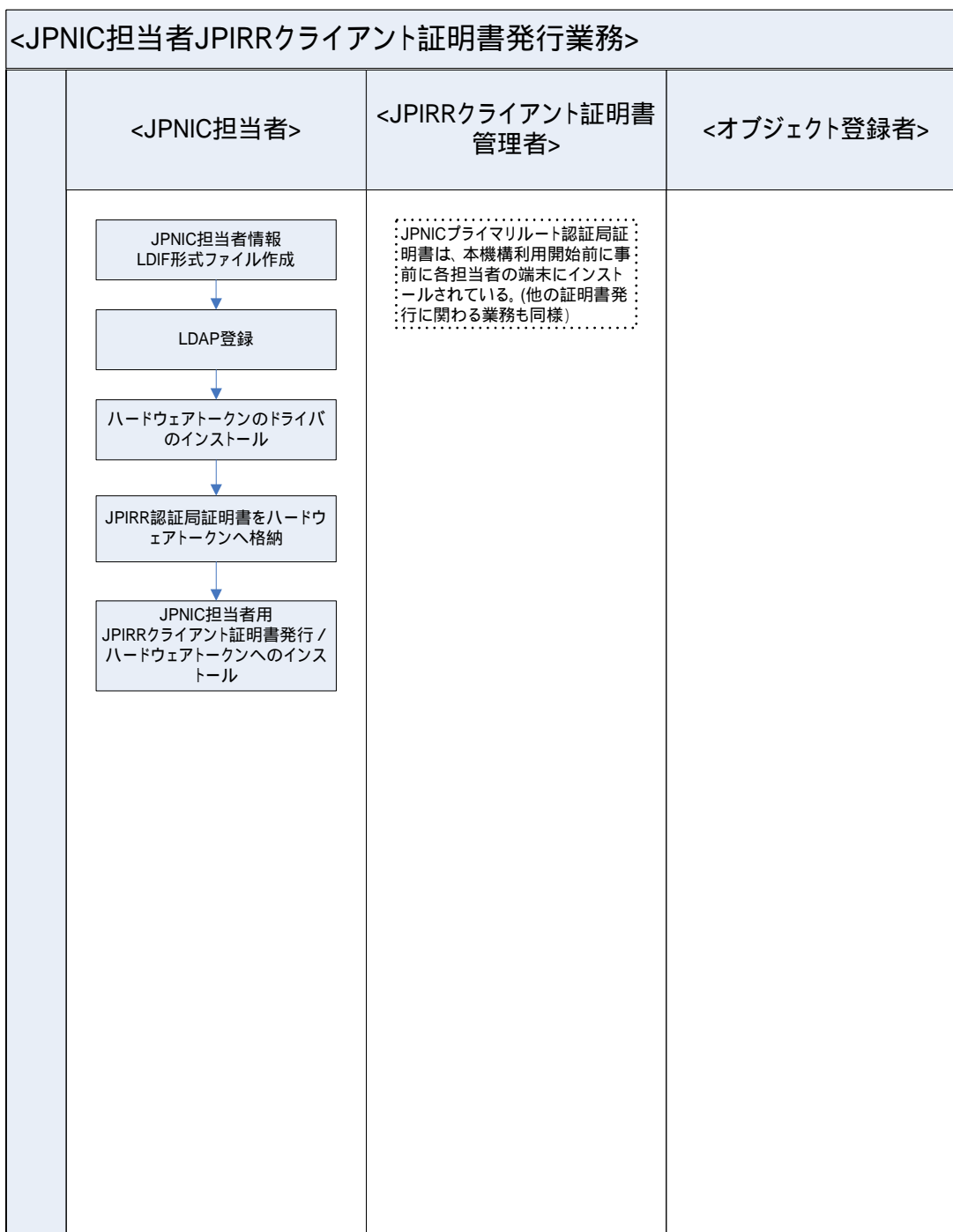
一般業務 (WEB
画面・アプリケーション操作・
メール送受信等)



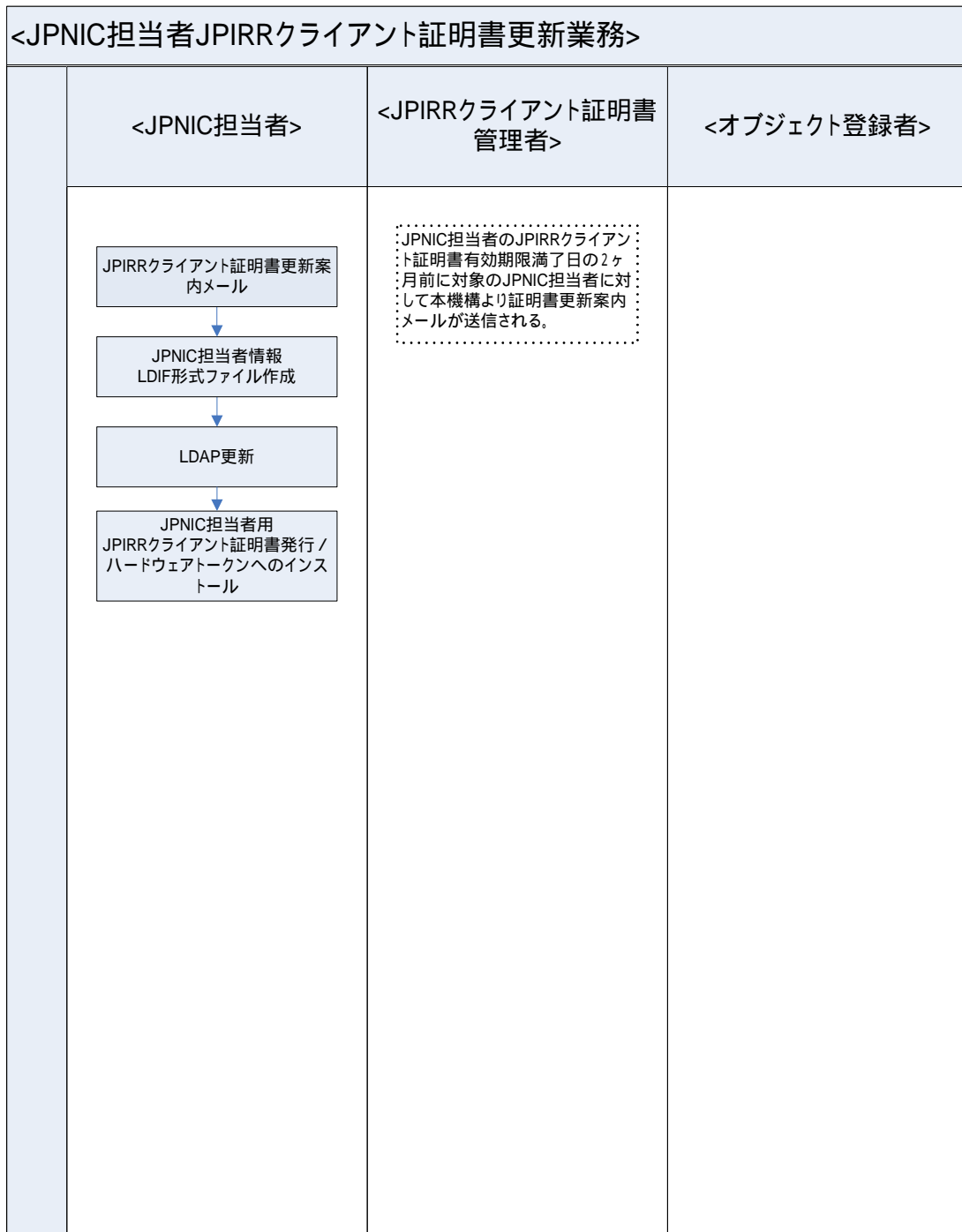
システム処理
(バッチ処理など)

第4章 経路情報の登録機構の設計と構築

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

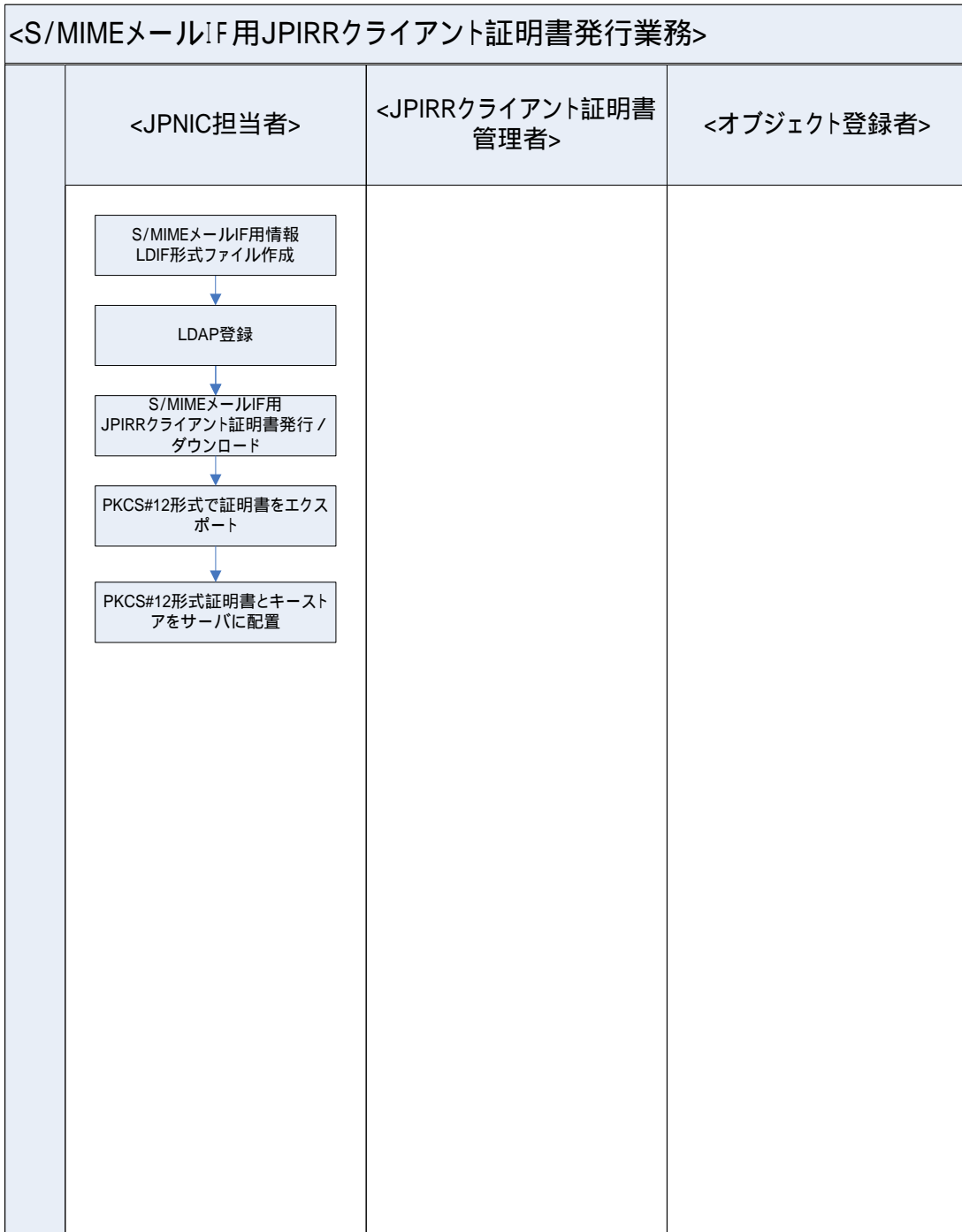


第4章 経路情報の登録機構の設計と構築

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

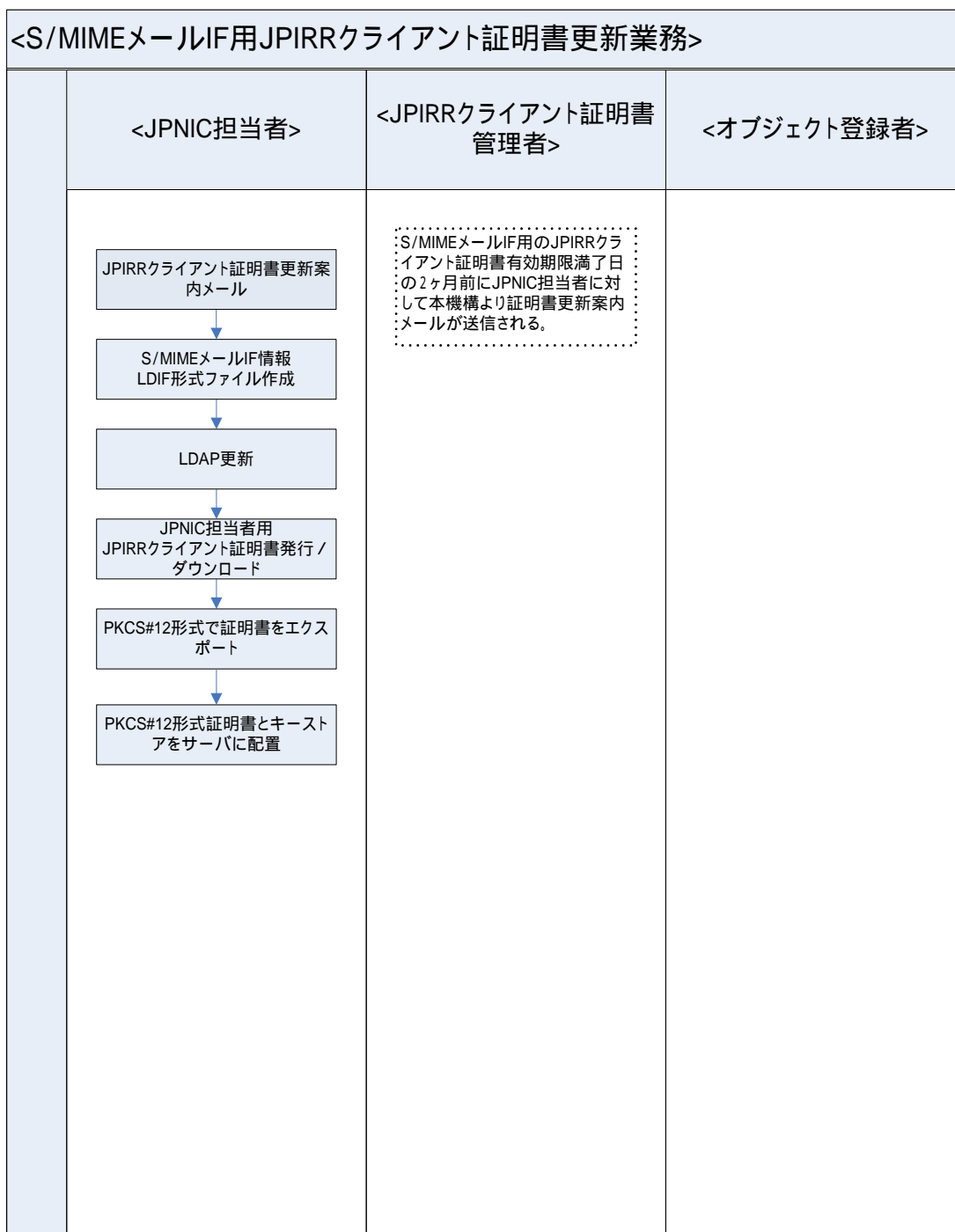


4.7.1.5. S/MIME メール IF 用 JPIRR クライアント証明書発行業務



第4章 経路情報の登録機構の設計と構築

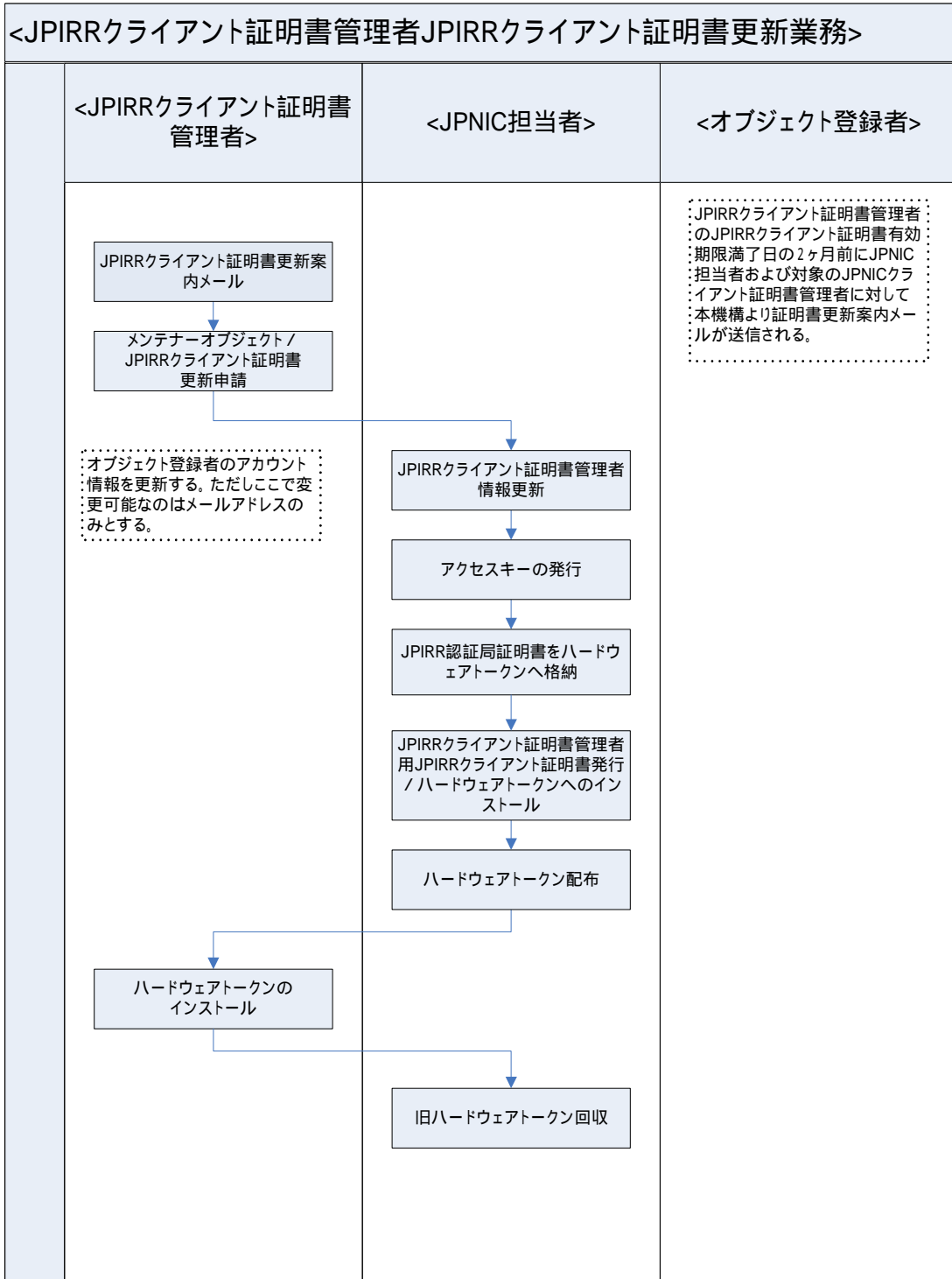
4.7.1.6. S/MIME メール IF 用 JPIRR クライアント証明書更新業務



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

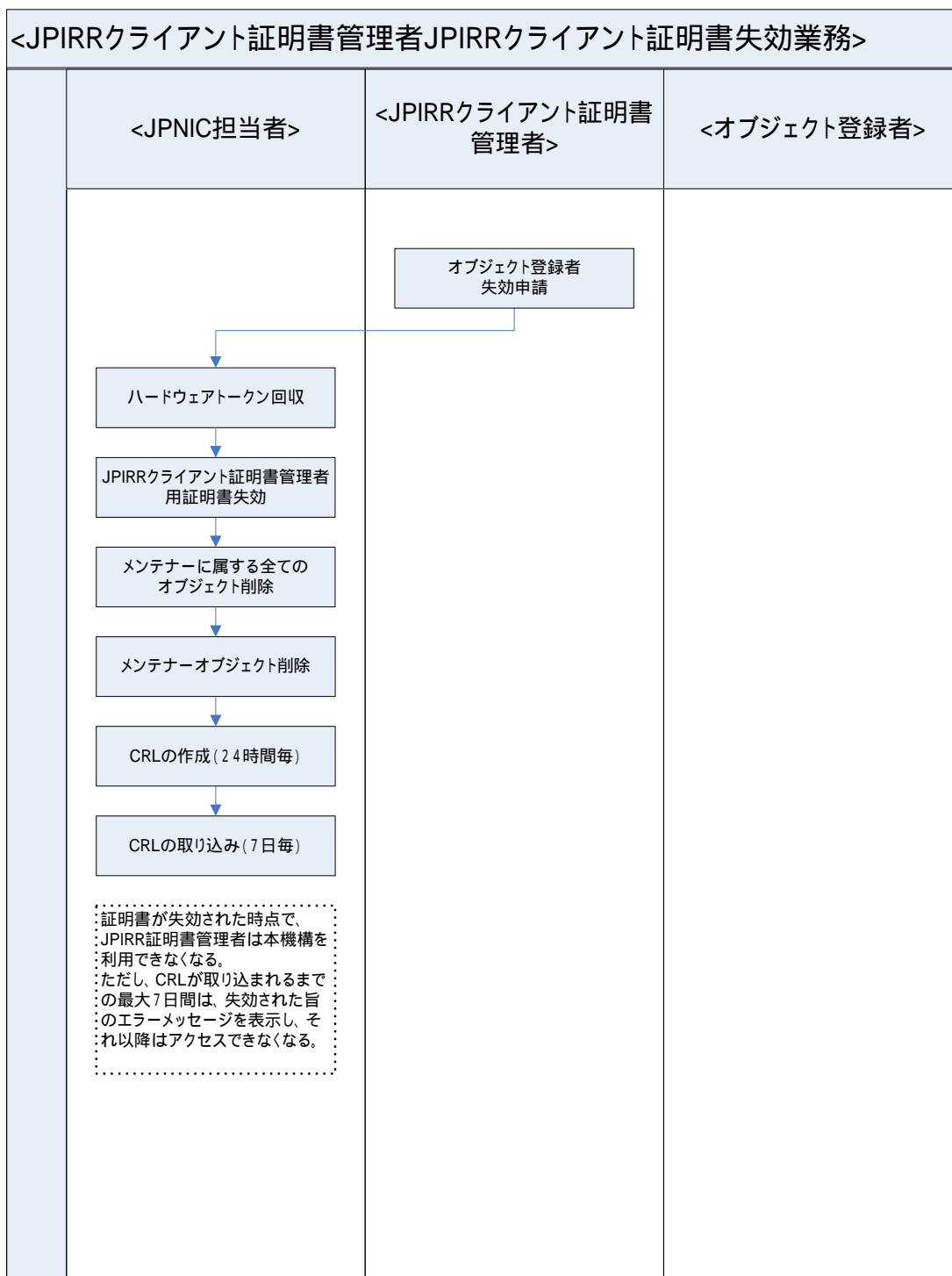


4.7.1.9. JPIRR クライアント証明書管理者 JPIRR クライアント証明書更新業務

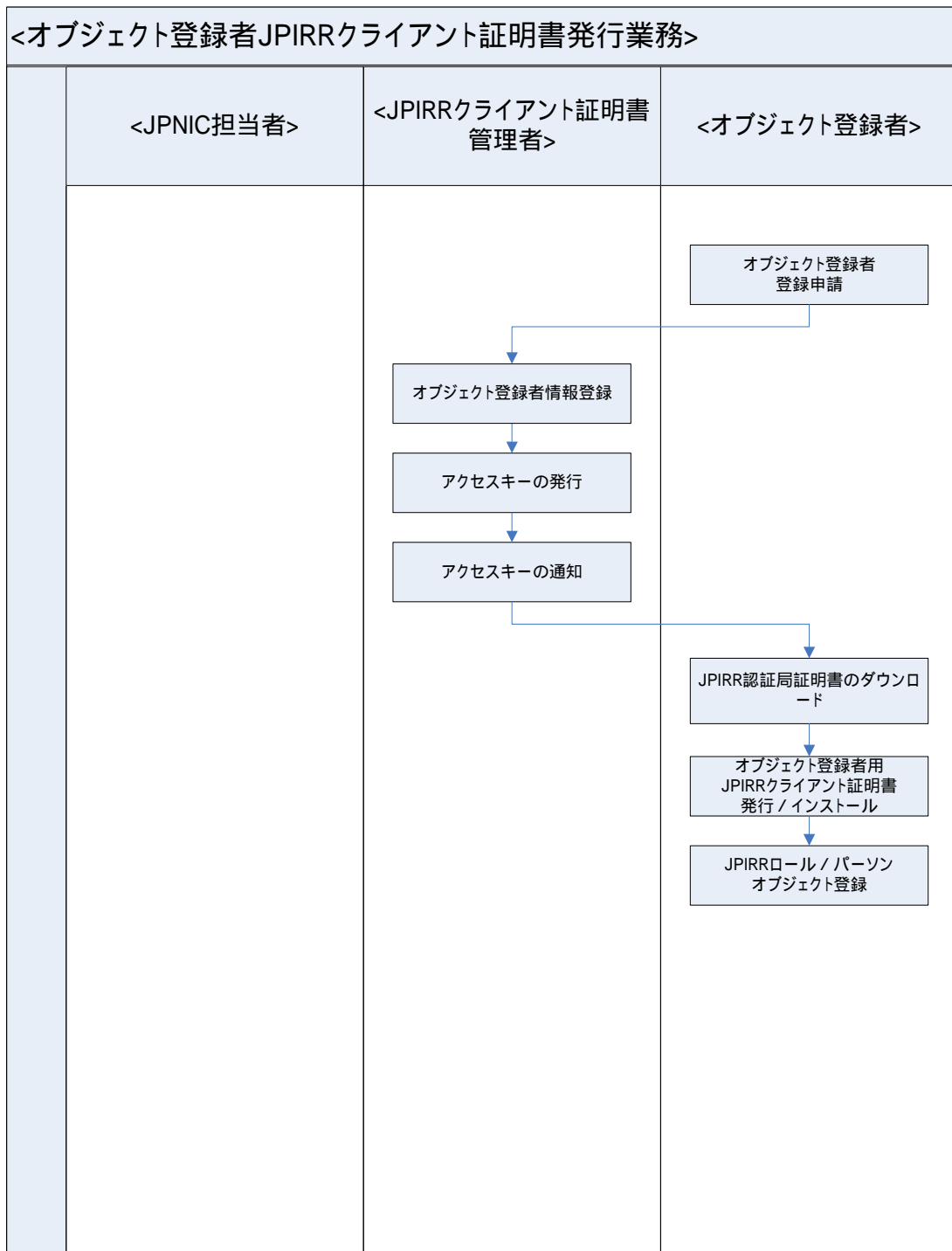


第4章 経路情報の登録機構の設計と構築

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

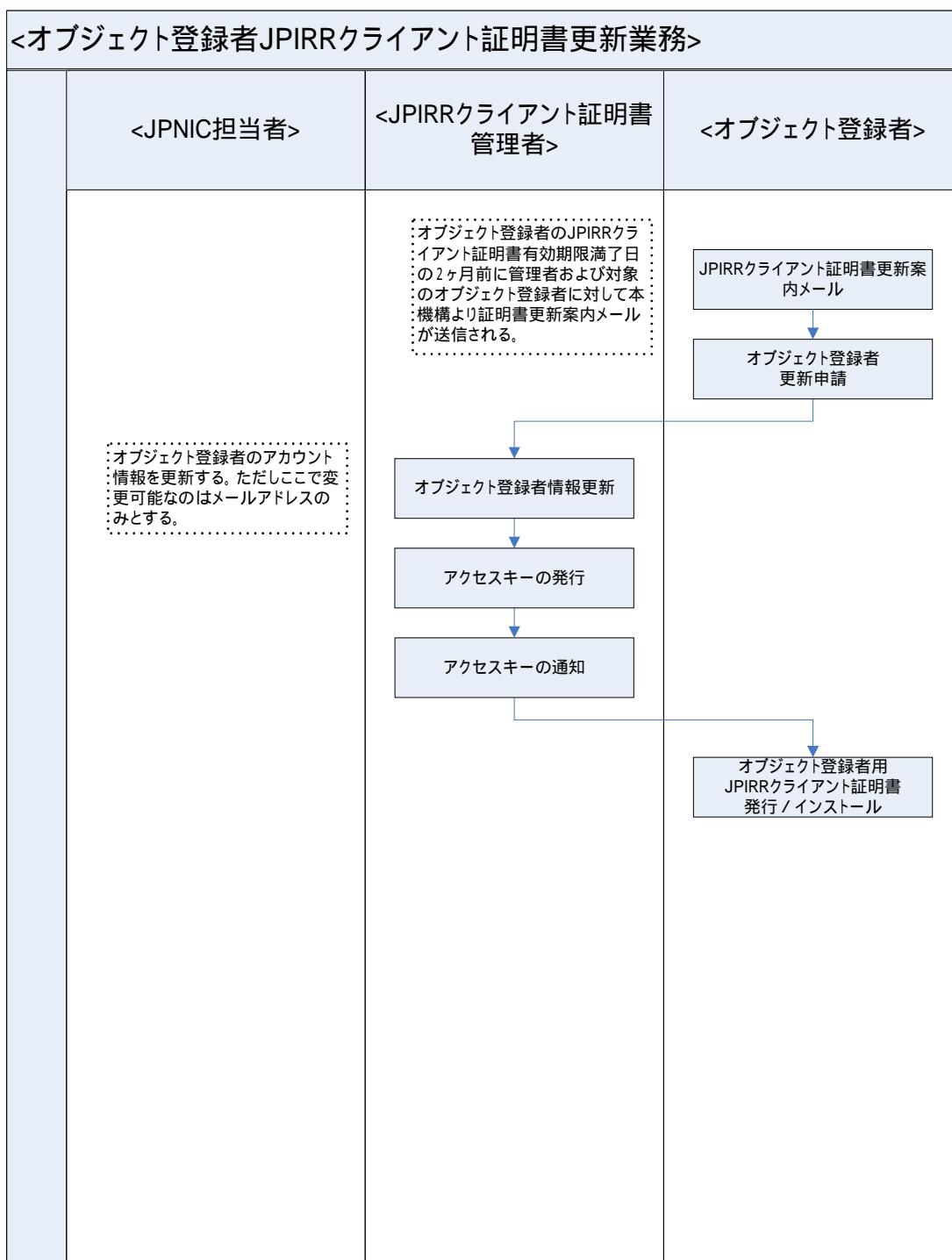


4.7.1.11. オブジェクト登録者 JPIRR クライアント証明書発行業務

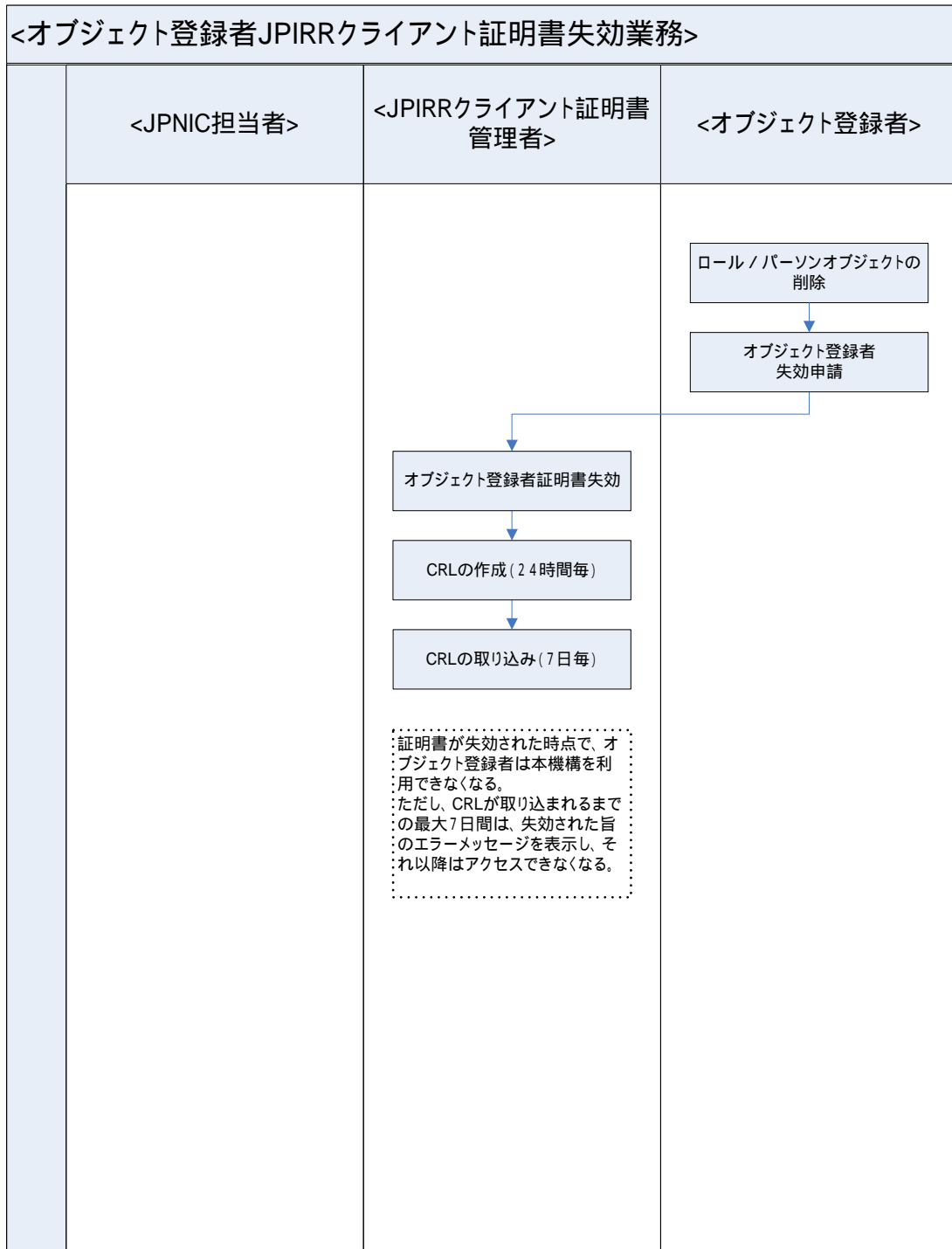


第4章 経路情報の登録機構の設計と構築

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



第4章 経路情報の登録機構の設計と構築

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

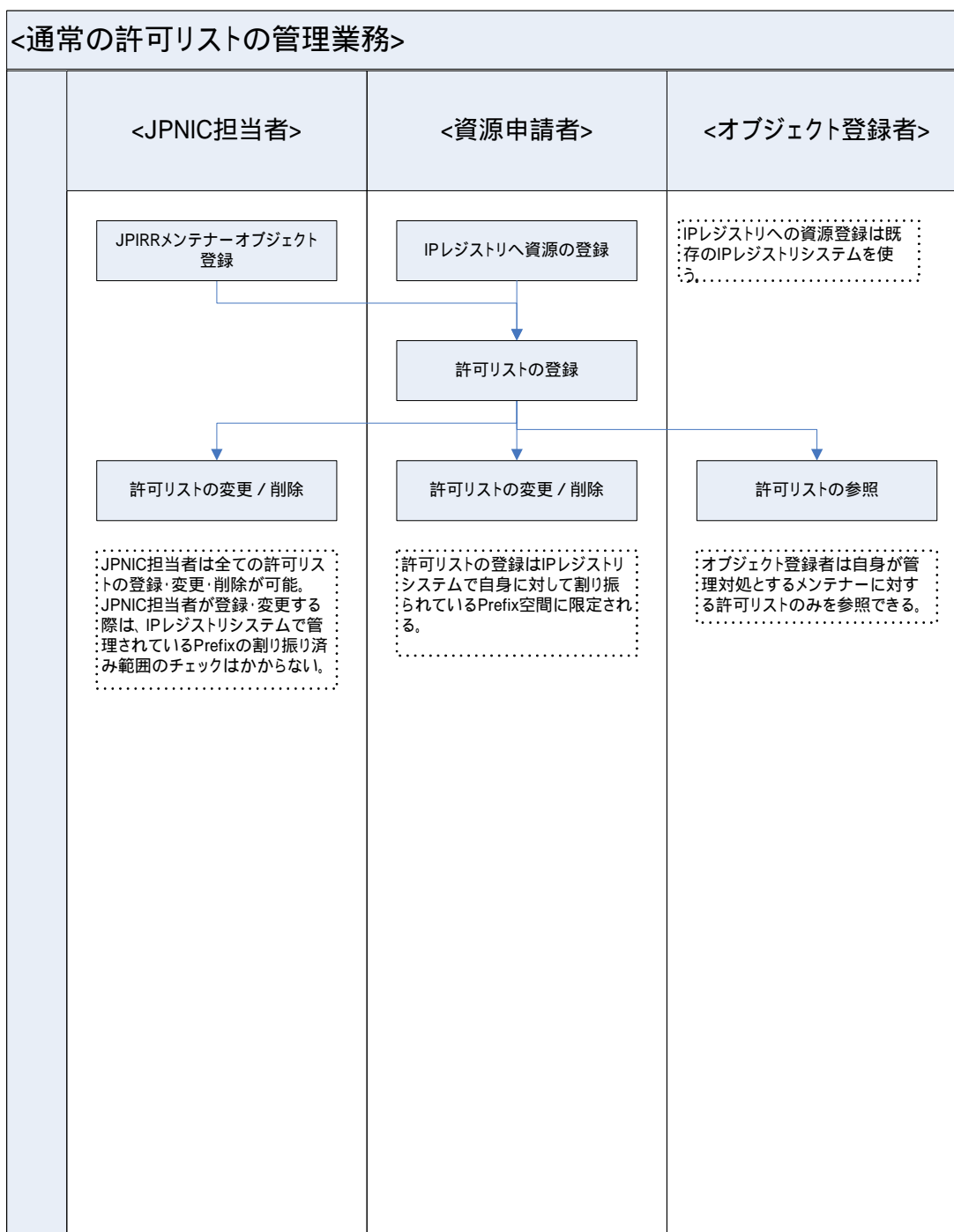
許可リストで管理する主な項目を表 4-15 に示す。

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	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 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
A S 番号	複数指定可能。指定無しも可能

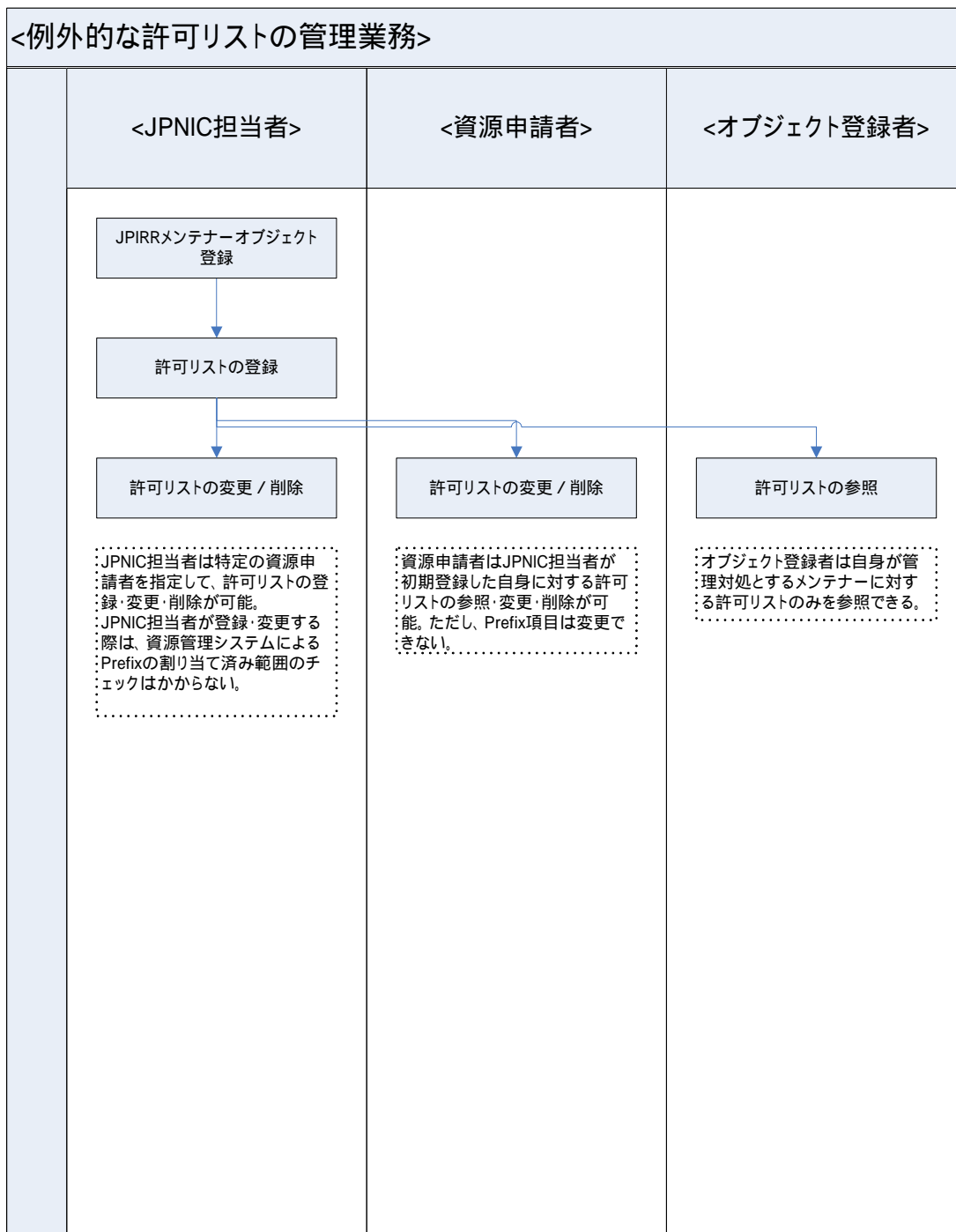
許可・禁止区分	許可または禁止
初期登録者	初期登録時にその登録者が JPNIC 担当者が資源申請者かを設定する（変更不可）

4.7.2.2. 通常の許可リストの管理業務



第4章 経路情報の登録機構の設計と構築

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



第4章 経路情報の登録機構の設計と構築

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	削除	JPNIC 担当者
メンテナ	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及びそのメンテナ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 Reply-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。

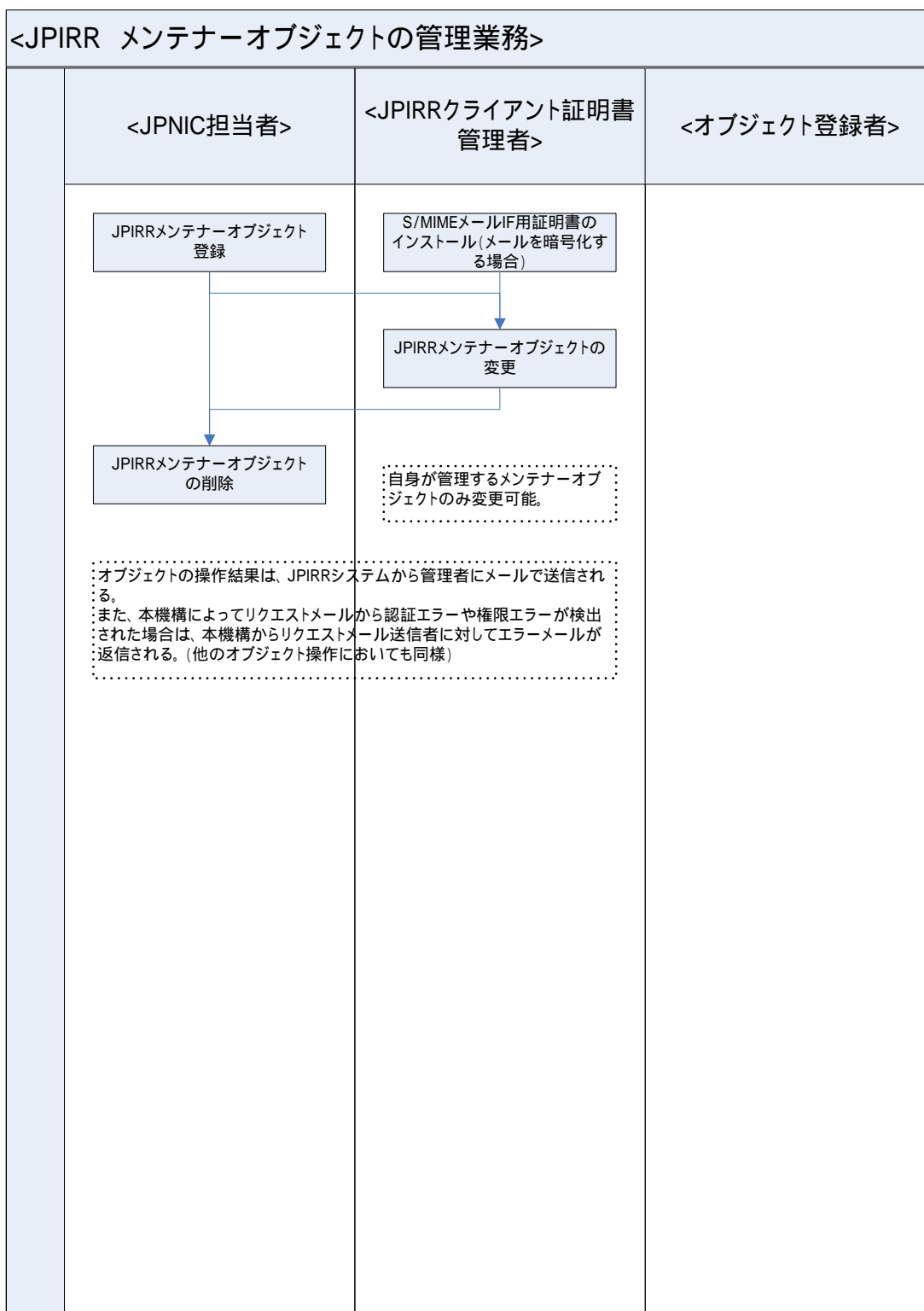
(10) JPIRR へのリクエストメール送信

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。

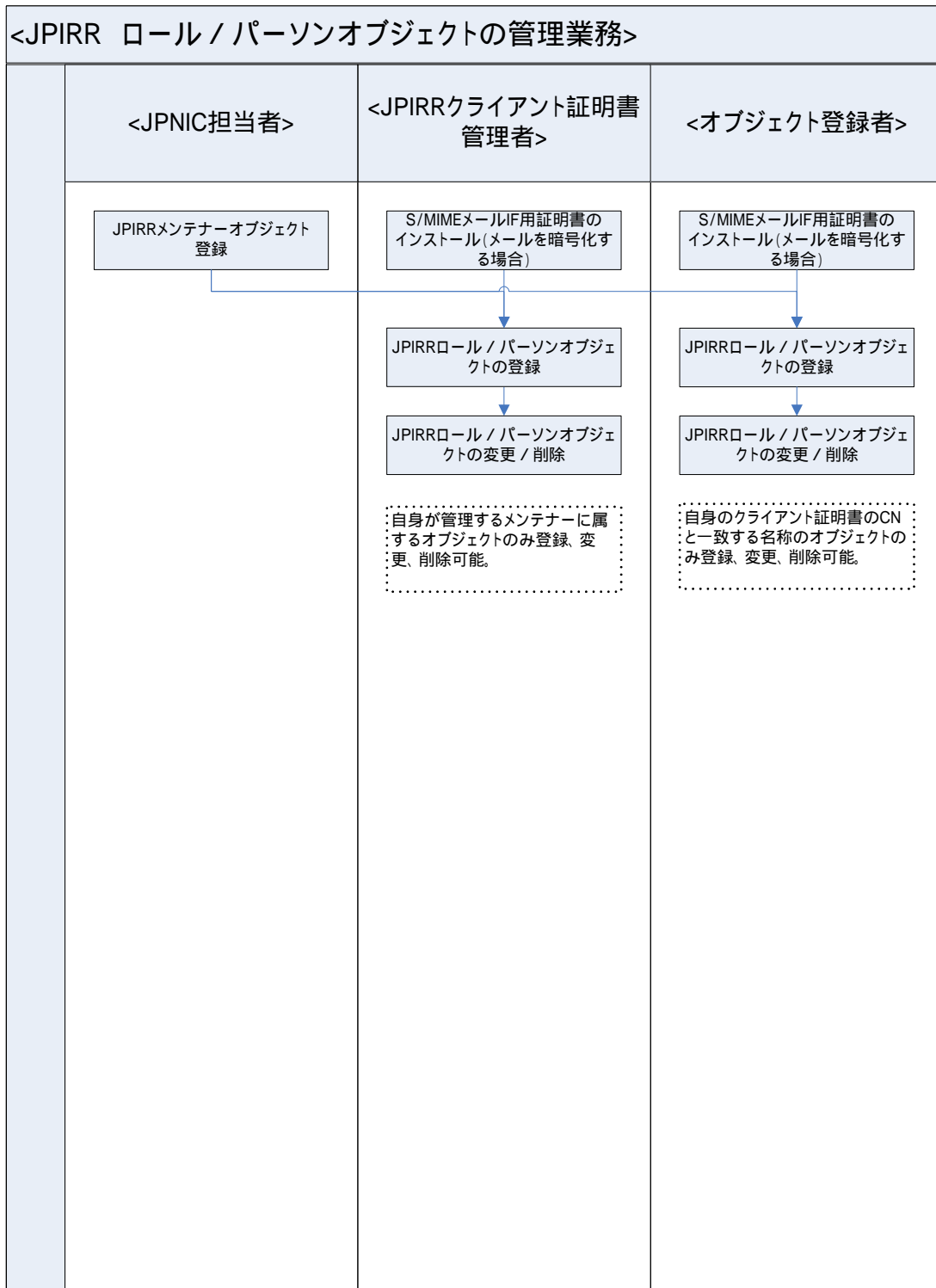
そのアドレスでは、IRR システムで既存の認証機能を経ずに処理されることとする。また、セキュリティのため外部からのメールを直接受信できないような設定がされていることとする。

第4章 経路情報の登録機構の設計と構築

4.7.3.2. メンテナーオブジェクトの管理業務

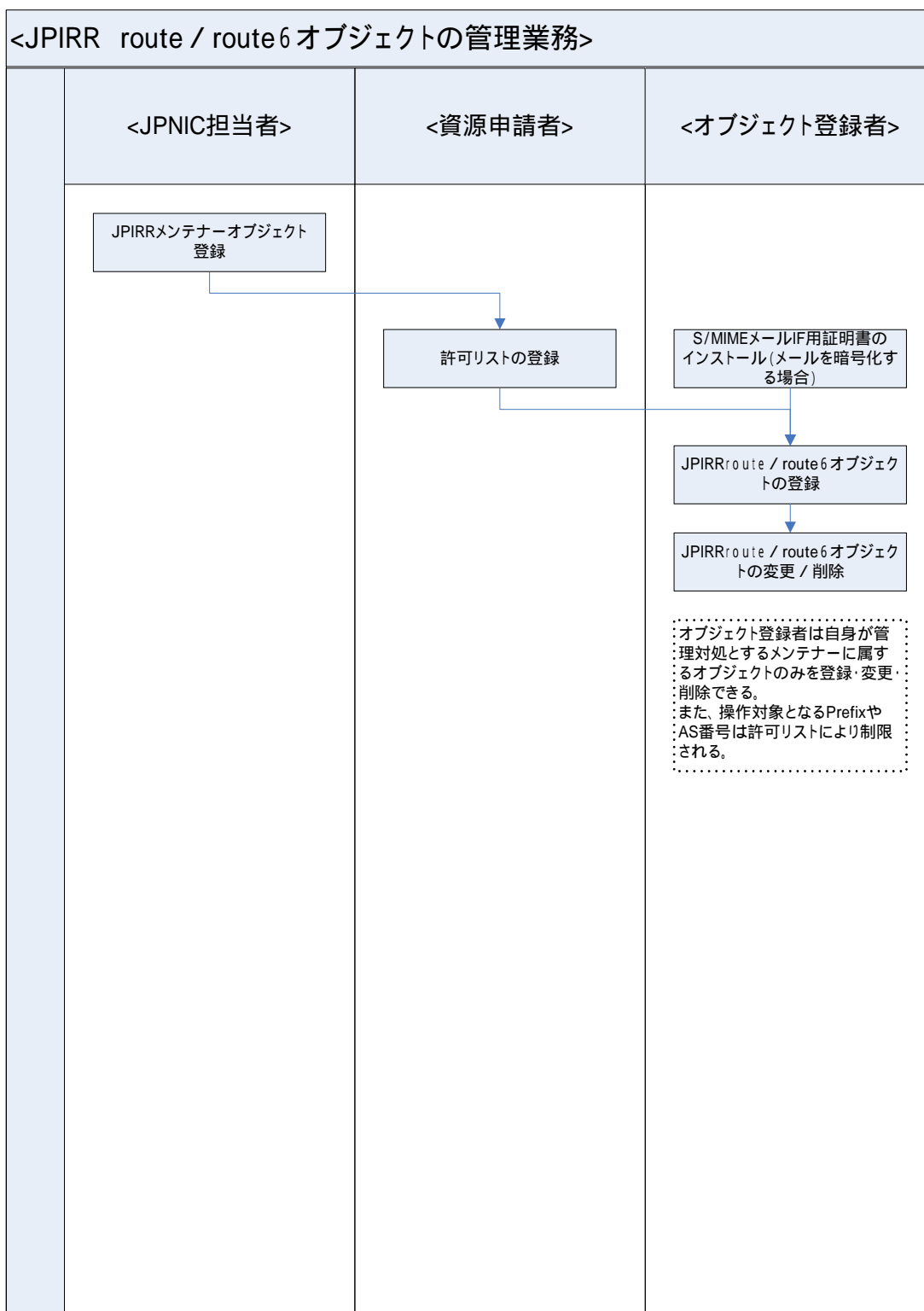


4.7.3.3. ロール/パーソンオブジェクトの管理業務

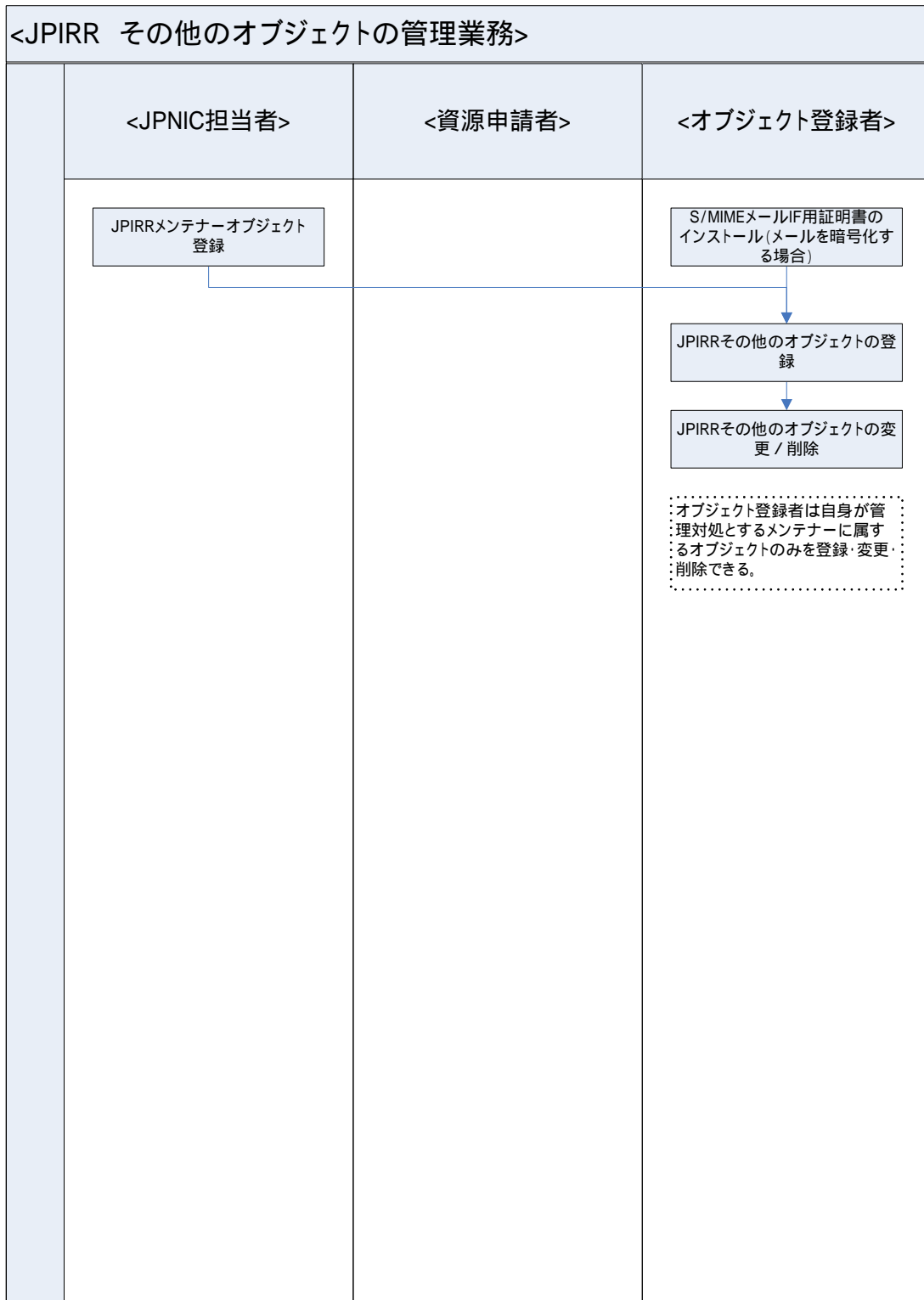


第4章 経路情報の登録機構の設計と構築

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



第4章 経路情報の登録機構の設計と構築

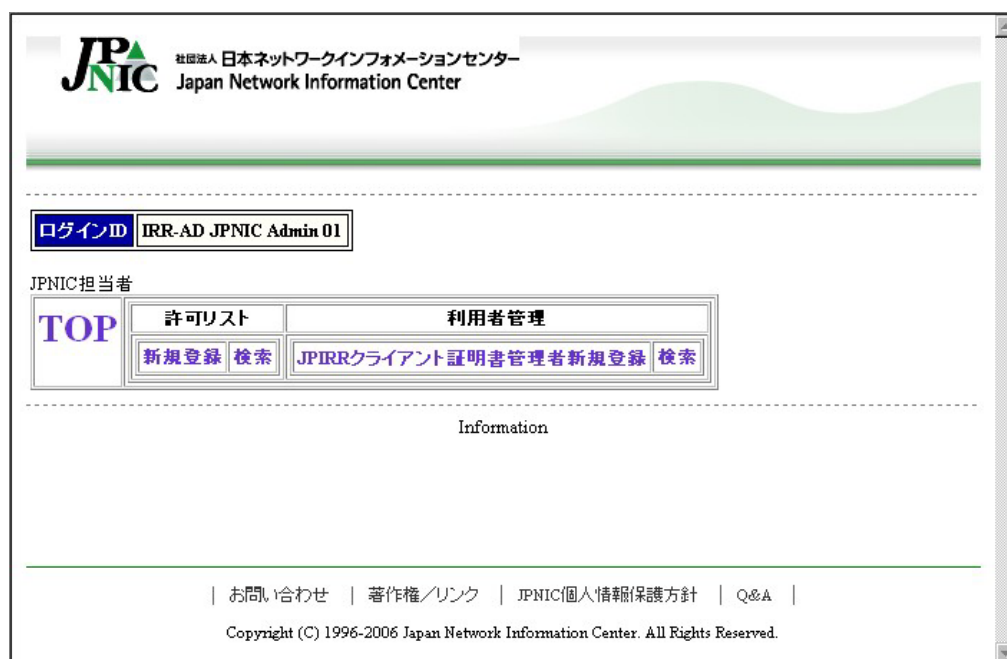
4.8. インターフェース設計

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

The screenshot shows the JPNIC website interface for registering a permitted list. At the top, there is a navigation menu with 'TOP', '許可リスト', and '利用者管理'. Below the menu, the main heading is '許可リスト登録'. The registration form contains the following fields:

- 資源管理者名称: [Text input field]
- Prefix: [Text input field with example: v4[1.0.0/16],v6[3000:102::/32]]
- メンテナー名: [Text input field]
- AS番号 (オプション、カンマ区切りで複数入力可): [Text input field]
- allow/deny: [Dropdown menu with 'allow' selected]

At the bottom of the form, there are two buttons: '登録' (Register) and 'クリア' (Clear). The footer of the page includes contact information and a copyright notice: 'Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

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。

第4章 経路情報の登録機構の設計と構築

(3) 許可リスト登録確認

The screenshot shows the JPNIC website interface. At the top, there is a header with the JPNIC logo and the text '日本ネットワークインフォメーションセンター Japan Network Information Center'. Below the header, there is a navigation menu with 'ログインID' (Login ID) set to 'IRR-AD test 01'. The main content area is titled '許可リスト登録確認' (Permitted List Registration Confirmation). It contains a table with the following data:

資源管理番号	1000
資源管理者略称	ROOT-REG-TEST
Prefix	1.1.0.0/24
メンテナー名	MAINT-AS0000
AS番号	
allow/deny	allow

Below the table, there is a question: '上記の内容で登録してよろしいですか?' (Is it okay to register with the above information?). There are two buttons: '登録' (Register) and '戻る' (Back).

At the bottom of the page, there is a footer with the text: 'お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A | Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

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。

第4章 経路情報の登録機構の設計と構築

(5) 許可リスト検索

許可リストの検索画面を表示する。

JPNIC 社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID IRR-AD JPNIC Admin 01

JPNIC担当者

TOP 許可リスト 利用者管理

新規登録 検索 JPIRRクライアント証明書管理者新規登録 検索

許可リスト一覧

検索条件入力

許可リストID 資源管理番号

資源管理者略称 IPバージョン

Prefix メンテナ名

AS番号 allow/deny

フラグ

複数項目の条件はAND条件として検索します。

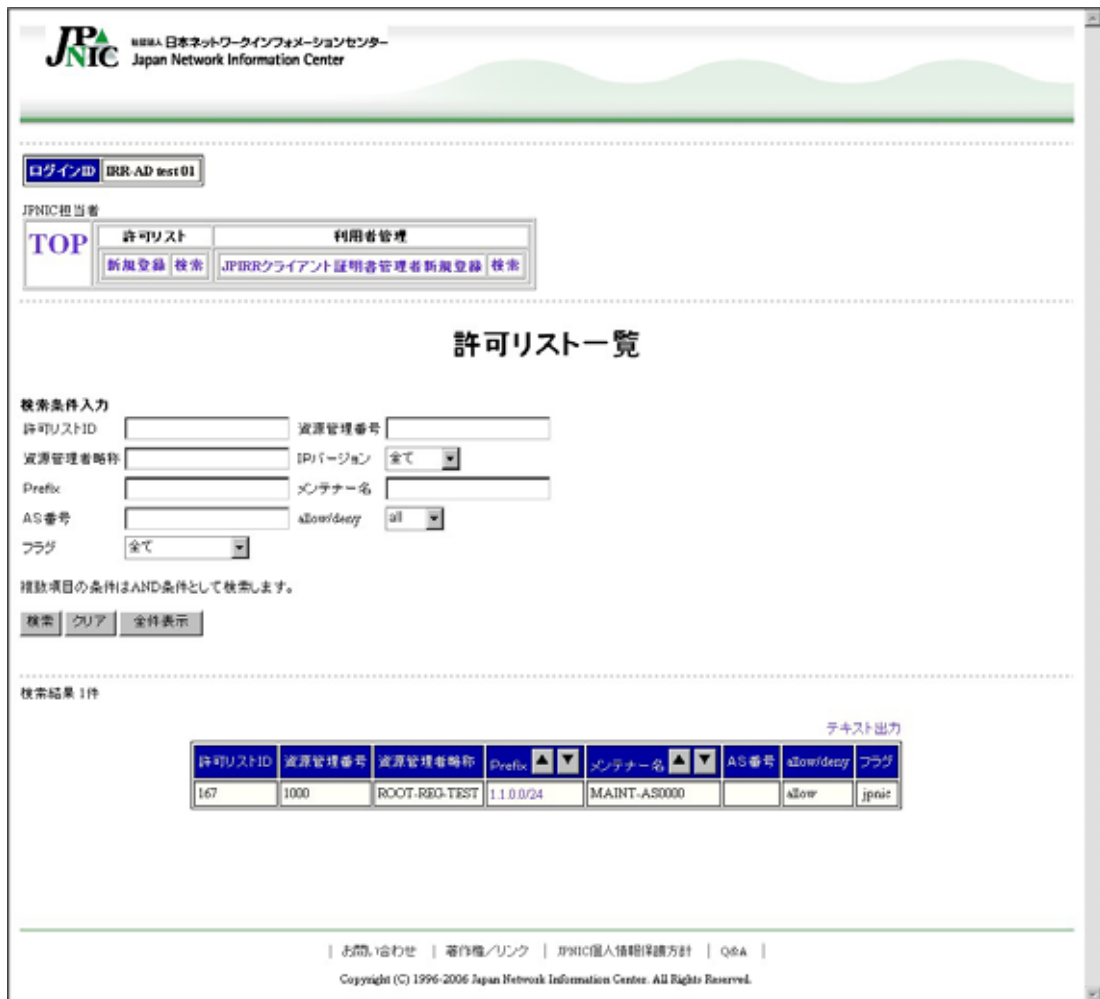
検索 クリア 全件表示

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |

Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

「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。

The screenshot shows the JPNIC website interface. At the top left is the JPNIC logo and the text '日本ネットワークインフォメーションセンター Japan Network Information Center'. Below the logo is a login field with the text 'ログインID IRR-AD test01'. A navigation menu contains 'TOP', '許可リスト', and '利用者管理'. Under '許可リスト' are links for '新規登録' and '検索'. Under '利用者管理' are links for 'JPIRRクライアント証明書管理者新規登録' and '検索'. The main content area is titled '許可リスト変更確認' and contains a table with the following data:

許可リストID	265
高層管理番号	0
高層管理者略称	JPNIC
Prefix	0.0.0.0/24
メンテナ名	MAINT-A30001
AS番号	111
allow/deny	allow

Below the table is the text '上記の内容で登録してよろしいですか?' and two buttons: '登録' and '戻る'. At the bottom of the page, there is a footer with links for 'お問い合わせ', '著作権/リンク', 'JPNIC個人情報保護方針', and 'Q&A', along with the copyright notice 'Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

「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。

第4章 経路情報の登録機構の設計と構築

(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。

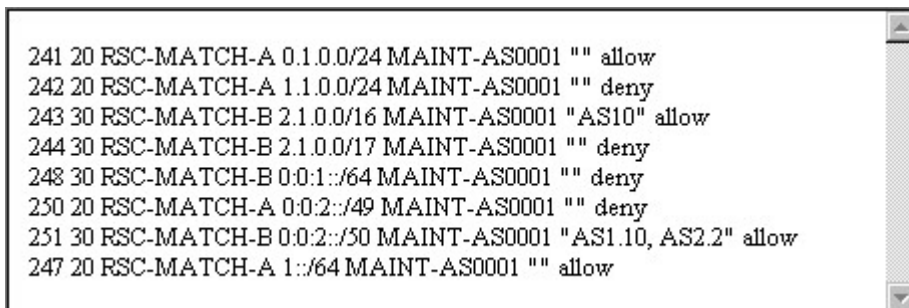
(10) 許可リスト削除完了

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。

第4章 経路情報の登録機構の設計と構築

(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。

第4章 経路情報の登録機構の設計と構築

(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。

第4章 経路情報の登録機構の設計と構築

(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。



第4章 経路情報の登録機構の設計と構築

(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。

The screenshot shows the JPNIC (Japan Network Information Center) user management interface. At the top, there is a navigation menu with 'TOP', '許可リスト', and '利用者管理'. Under '利用者管理', there are links for '新規登録 検索' and 'JPIRRクライアント証明書管理者新規登録 検索'. The main heading is '利用者管理一覧'.

検索条件入力

利用者:

メンテナンス名:

cn:

E-mailアドレス:

状態: 未実行 実行済 失敗済 有効期限切れ

検索結果 6件

利用者一覧

利用者	管理対象メンテナンス名	cn	E-mailアドレス	状態	更新状況	notBefore	notAfter
クライアント証明書管理者	MAINT-AS0001	IRR-MA test ma 01	aaaa1@xxx.ne.jp	実行済	更新通知送信済	2007/01/20 12:00:00	2009/01/20 12:00:00
クライアント証明書管理者	MAINT-AS0001	IRR-MA test ma user2 01	aaaa1@xxx.ne.jp	実行済	更新通知送信済	2007/01/20 12:00:00	2009/01/20 12:00:00
クライアント証明書管理者	MAINT-AS0001	IRR-MA test ma user4 01	aaaa1@xxx.ne.jp	実行済	更新登録済	2007/01/20 12:00:00	2009/01/20 12:00:00
クライアント証明書管理者	MAINT-AS0001	IRR-MA test ma user4 02	a@xxx.ne.jp	未実行	更新なし		
オブジェクト登録者	MAINT-AS0002	IRR-OR test or user1 01	aaaa@xxx.ne.jp	実行済	更新登録済	2007/01/20 12:00:00	2009/01/20 12:00:00
オブジェクト登録者	MAINT-AS0001	IRR-OR test or user1 01	aaaa@xxx.ne.jp	未実行	更新なし		

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |

Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

「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。



第4章 経路情報の登録機構の設計と構築



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。



第4章 経路情報の登録機構の設計と構築

ログインID: IRR-AD test 01

JPNIC担当者

TOP

許可リスト

利用者管理

新加登録 検索

JPNICクライアント証明書管理者新規登録 検索

オブジェクト登録者修正

オブジェクト登録者

管理対象ゾナ名	MAINT-A30001
cn	IRR-OR test or user1 01
利用者名	test or user1
E-mailアドレス	aaaa@test.xxx.ne.jp

OK | クリア

一覧へ

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A

Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

「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。

第4章 経路情報の登録機構の設計と構築

(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。

JPNIC 日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID: IRR-AD test01

JPNIC担当者

TOP | 許可リスト | 利用者管理

新加登録 検索 | JPIRRクライアント証明書管理者新規登録 検索

JPIRRクライアント証明書管理者更新登録

JPIRRクライアント証明書管理者

管理対象メンテナンス名	MAINT.A20000
id	IRR.MA.test.ma.for.maint-as1234567.02
利用者名	test.ma.for.maint-as1234567
E-mailアドレス	test_new@xxx.ne.jp

OK | クリア

一覧へ

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |
Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

「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。

第4章 経路情報の登録機構の設計と構築

(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。



第4章 経路情報の登録機構の設計と構築

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

The screenshot shows the JPNIC website interface. At the top left is the JPNIC logo and the text 'JPNIC 日本ネットワークインフォメーションセンター Japan Network Information Center'. Below this is a navigation area with a 'TOP' button and a '利用者管理' (User Management) section containing 'オブジェクト登録者新規登録' (Object Registrant New Registration) and '検索' (Search) buttons. The main content area is titled 'オブジェクト登録者新規登録' (Object Registrant New Registration) and 'オブジェクト登録者' (Object Registrant). It features a form with two input fields: '利用者名' (User Name) with a dropdown menu currently showing 'test or', and 'E-mailアドレス' (E-mail Address). Below the form are 'OK' and 'クリア' (Clear) buttons. At the bottom of the page, there is a footer with links for 'お問い合わせ' (Contact Us), '著作権/リンク' (Copyright/Link), 'JPNIC個人情報保護方針' (JPNIC Personal Information Protection Policy), and 'Q&A', along with a copyright notice: 'Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

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名 of 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。

第4章 経路情報の登録機構の設計と構築

(3) 利用者登録確認

JPNIC 日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID: IRR-MA test ma 01
管理対象メンテナ: MAINT-AS0001

JFRRクライアント証明書管理者
TOP 利用者管理
オブジェクト登録者新規登録 検索

オブジェクト登録者新規登録確認

cn	IRR-OR test or 01
利用者名	test or
E-mailアドレス	test@occc.na.jp

上記内容で登録します。よろしいですか？

OK 戻る

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |
Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

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。

第4章 経路情報の登録機構の設計と構築

(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

検索条件入力

cn

Emailアドレス

状態 未発行 発行済 失効済 有効期限切れ

検索結果: 5件

利用者一覧

cn	Emailアドレス	状態	更新状況	notDefcon	notADist
JPR-CR test.or.01	test@cr.na.jp	未発行	更新なし		
JPR-CR test.or.sasak1.01	w@cr.na.jp	未発行	更新なし		
JPR-CR test.or.sasak2	sa@cr.na.jp	発行済	更新通知済済済	2007/01/20 12:00:00	2009/01/20 12:00:00
JPR-CR test.or.sasak3	ssw@cr.na.jp	発行済	更新通知済済済	2007/01/20 12:00:00	2009/01/20 12:00:00

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | JPNIC

Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

証明書の管理対象メンテナ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。

第4章 経路情報の登録機構の設計と構築

(9) オブジェクト登録者修正確認

The screenshot shows the JPNIC (Japan Network Information Center) website interface. At the top left, the JPNIC logo and name are displayed. Below the logo, there is a navigation menu with a 'TOP' link and a '利用者管理' (User Management) section containing 'オブジェクト登録者新規登録' (New Object Registrant Registration) and '検索' (Search) links. The main content area is titled 'オブジェクト登録者修正確認' (Object Registrant Modification Confirmation). It features a form with three rows of input fields: 'cd' (containing 'IRR-OR test or 01'), '利用者名' (containing 'test or'), and 'E-mailアドレス' (containing 'test@or.or.jp'). Below the form, a confirmation message asks '上記内容で登録します。よろしいですか?' (I will register with the above content. Is it okay?). There are two buttons: 'OK' and '戻る' (Back). At the bottom of the page, there is a footer with links for 'お問い合わせ' (Contact Us), '著作権/リンク' (Copyright/Link), 'JPNIC個人情報保護方針' (JPNIC Personal Information Protection Policy), and 'Q&A', along with a copyright notice: 'Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

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

JPNIC 日本ネットワークインフォメーションセンター
Japan Network Information Center

ログインID: IRR-MA test ma 01
管理対象メンテナ: MAINT-AS0001

JFIRRクライアント証明書管理者

TOP 利用者管理
オブジェクト登録者新規登録 検索

オブジェクト登録者更新登録

オブジェクト登録者

on	IRR-OR test or 02
利用者名	test or
E-mailアドレス	test@xxx.ne.jp

OK クリア
一覧へ

お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |
Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

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。

第4章 経路情報の登録機構の設計と構築

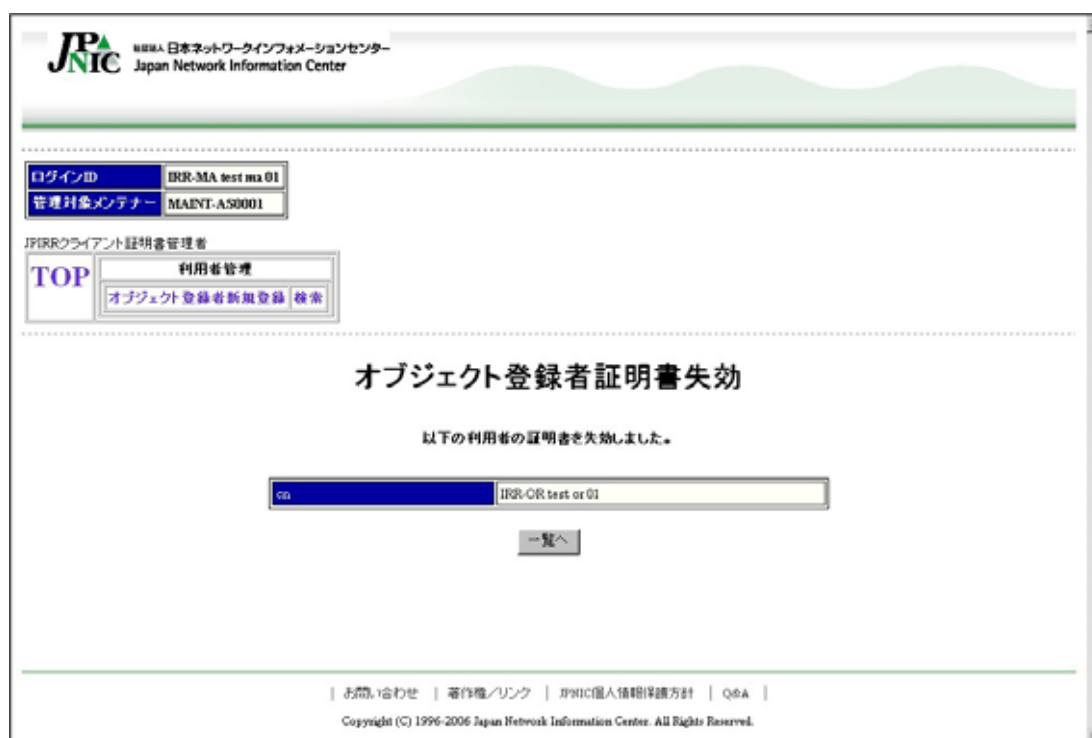
(13) オブジェクト登録者更新登録完了



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

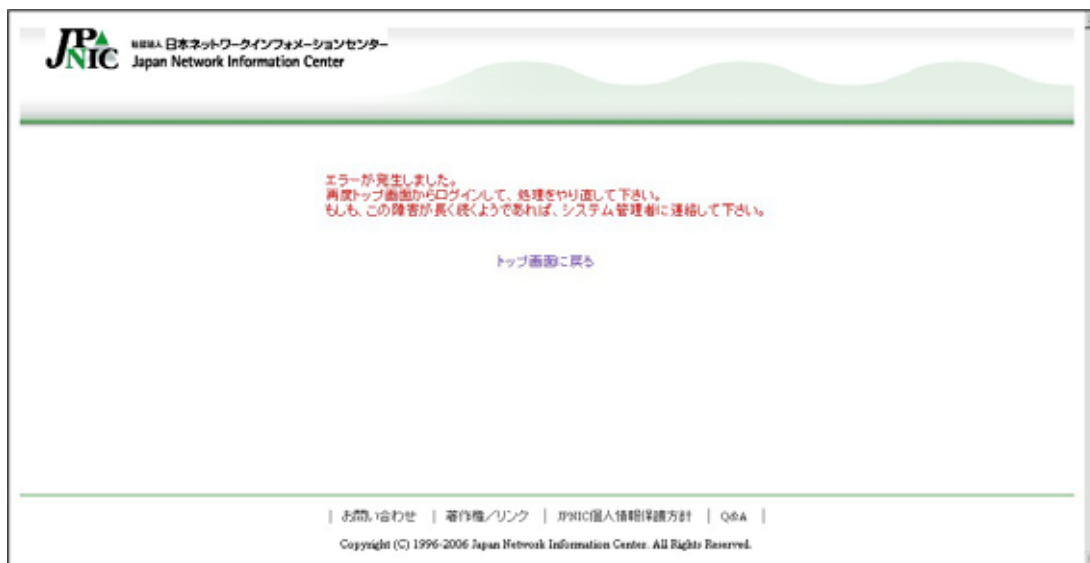


証明書失効の完了を知らせる。

「一覧へ」をクリックすると「利用者管理一覧」に遷移する。

第4章 経路情報の登録機構の設計と構築

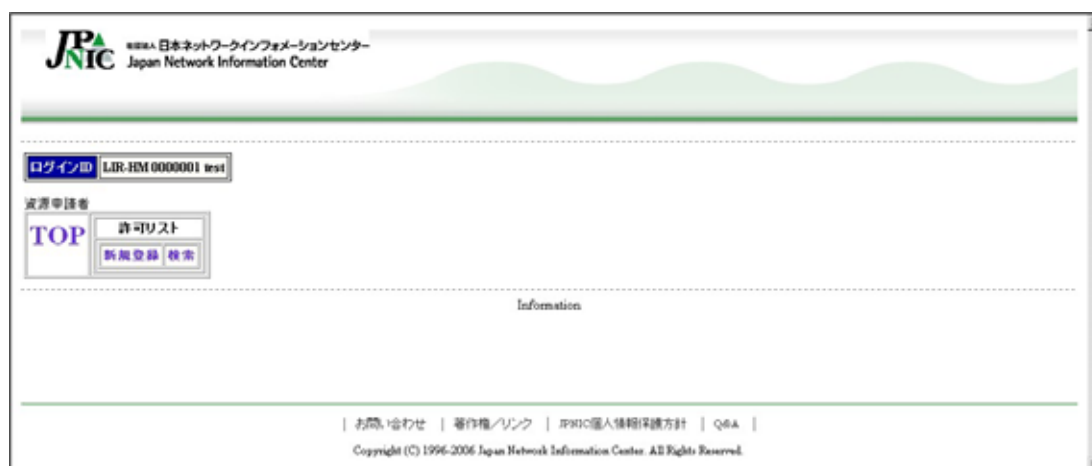
(15) エラー表示



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

The screenshot shows the JPNIC website interface for registering a permitted list. At the top, there is a login field with the ID 'LAR-HM000001 test'. Below it, there are navigation links for 'TOP', '許可リスト', '新規登録', and '検索'. The main heading is '許可リスト登録'. The form contains the following fields:

Prefix	<input type="text" value="v4[3.10.0/16]-v6[2001:102::/52]"/>
メンテナー名	<input type="text"/>
AS番号 (オプション、カンマ区切りで複数入力可)	<input type="text"/>
allow/deny	<input type="text" value="allow"/>

Buttons: 登録, クリア

Footer: お問い合わせ | 著作権/リンク | JPNIC個人情報保護方針 | Q&A |
Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.

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。

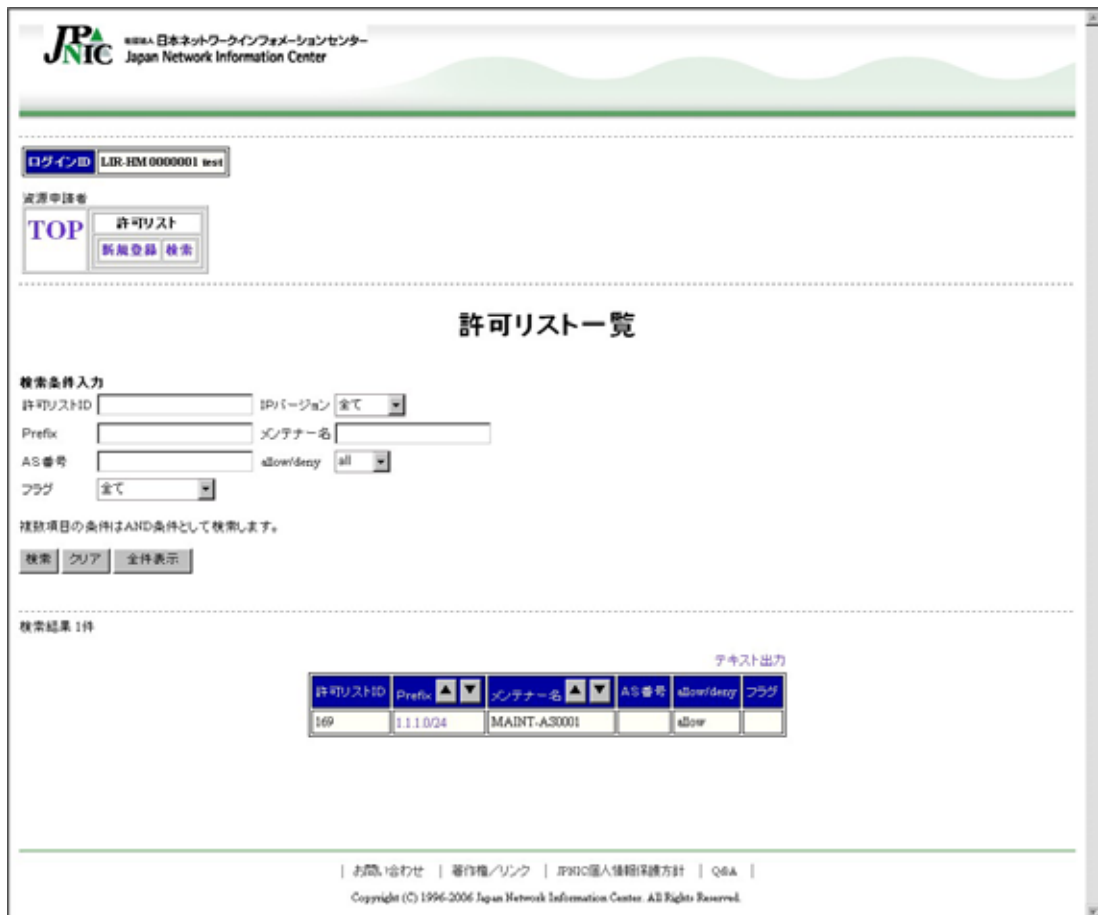
第4章 経路情報の登録機構の設計と構築

(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

The screenshot shows the JP NIC website interface for changing an allow list. The page title is '許可リスト変更'. The form contains the following fields:

許可リストID	169
Prefix	1.1.1.0/24
メンテナ名	MAINT-AS0001
AS番号 (オプション、カンマ区切りで複数入力可)	
allow/deny	allow

Below the form are buttons for '変更', 'クリア', '削除', and '一覧へ'. The footer contains contact information and copyright notice: 'Copyright (C) 1996-2006 Japan Network Information Center. All Rights Reserved.'

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。

第4章 経路情報の登録機構の設計と構築

(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。

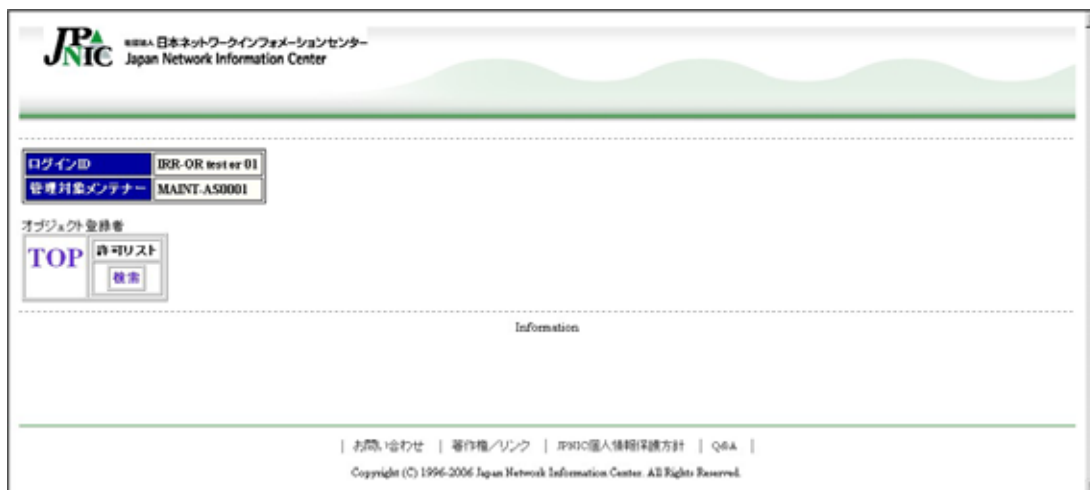
第4章 経路情報の登録機構の設計と構築

(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。

第4章 経路情報の登録機構の設計と構築

(2) 許可リスト一覧

検索結果 1件

許可リストID	資源管理者略称	Prefix	AS番号	allow/deny	フラグ
168	ROOT-REG-TEST	1.1.0.0/24		allow	ipraic

「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

```
168 ROOT-REG-TEST 1.1.0.0/24 "" allow
```

「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。

第 5 章 電子認証フレームワークの定義と仕組み

内容

- 電子認証に関わるノウハウの蓄積とは
- 電子認証プラクティスフォーラムとは
- フォーラムの設計
- フォーラムの仕組みとコミュニティ構成
- 実現の為にシステムの機能と構築
- 認証局の運用に関する技術的な BCP

5. 電子認証フレームワークの定義と仕組み

RIR における電子認証技術の利用や IETF における電子認証技術の標準化と実用化の現状を鑑みると、電子認証技術は標準化が先行してインターネットにおける実用化が遅れていると言える。

本調査研究のひとつのテーマである「電子認証フレームワーク」は、この状況を改善し、標準化が進んでいる電子認証技術を適切に普及させる機構、およびコミュニティの形成に関する調査研究である。

2005 年度は、電子認証技術の適切な普及を促進するには電子認証に関するノウハウをドキュメント化し、継続的に更新・公開していく枠組みのあり方について調査した。この調査では国内外の既存のドキュメント策定プロセスについて調査すると共に、電子認証フレームワークに期待されることを列挙した。

2006 年度は、電子認証フレームワークを構築するためのフォーラム「電子認証プラクティスフォーラム」の設立のため、BCP の議論とシステムの整備を行った。このフォーラムは IETF や JPOPM と同様にドキュメント策定プロセスを持ち、一般に公開した文書を元に BCP (ベストカレントプラクティス) の策定を目指す活動である。

ここでは本フレームワークに関する議論の結果、見えてきたフォーラムの構成とフォーラムのシステムについて述べる。今後、本フォーラムの構成自体を継続的に更新していける仕組みとするため、本フォーラムの趣意及び規定を BCP としてまとめていく活動が考えられる。

5.1. 電子認証に関わるノウハウの蓄積とは

IETF や日本国内での PKI 普及の動向から、電子認証技術の普及が遅れている理由は、技術そのものの発展が遅れているためではなく、適切に利用し活用するノウハウが普及していないことに原因として考えられる。

電子認証技術の適切な普及には知見の共有が重要であり、この重要性事態は IETF SAAG (セキュリティエリアの全体会議) でも指摘されていた。しかし IETF の BCP では、概念モデルなどをカバーできない。

しかし日本国内においても、電子認証に関わる運用面での調査研究は行われており、むしろ一定の調査をすれば必要十分なノウハウが得られることが、本調査研究の結果から判明している。

第5章 電子認証フレームワークの定義と仕組み

すなわち電子認証に関わるノウハウは、既に公開されているか、認証局の運用を行った後には自明の事実であることが多い。

そこで重要になるのは、これらのドキュメントを継続的に参照可能な仕組みで管理し、新たなノウハウの集約や既存のノウハウの見直しを進められるような仕組み作りが重要であると考えられる。

例えばこれが電子認証技術自体の標準化についてであれば IETF が該当し、IP アドレスポリシーについて JPOPM が、日本国内のインターネットの運用に関するノウハウであれば JANOG が該当すると考えられる。JANOG は JANOG Comment と呼ばれるノウハウのドキュメント化活動を行っており、すでに一般公開が行われている¹。電子認証技術の運用や利用・活用に関するノウハウについても議論と標準的なドキュメントとしての蓄積があれば、コミュニティ参加者の間で共有できる。IETF や JPOPM、JANOG のすべてに共通する点であるが、コミュニティの参加者は当該分野の専門家ないし業務上の改善に取り組む「提供者」ないし「供給者」の立場が多い。一般ユーザに対するノウハウの提供よりも、このような提供者側でのノウハウの共有によってノウハウが一般ユーザの環境向上に対しても効果を発揮しやすいと考えられる。

5.2. 電子認証プラクティスフォーラムとは

2005 年度および 2006 年度の調査研究の結果から、電子認証プラクティスフォーラムとは、コミュニティにおけるコンセンサスを得ながら、電子認証で必要となるドキュメントを策定し、BCP (Best Current Practice) として普及、改善を図っていく活動になると考えられる。

既存の調査研究などによって明らかになりドキュメントとして公開されているものについては、位置づけを整理した上で本フォーラムの中の位置づけを明らかにする。これによって電子認証の利用に関するノウハウの全体の中で、専門的な調査研究がどのような位置づけにあるのか、ユーザ自身が読む必要があるのかどうか、どのような場面で役立つノウハウであるのか、などがわかるようになる。

なお、本調査研究のテーマである「電子認証フレームワーク」は本フォーラムで初期の段階で策定されるべき BCP の集合であると考えられる。電子認証の用途は、本人性確認手法の違いや保証レベルの違いによって内容が大きく異なる。はじめにこの整理を行うことで、各電子認証技術の位置づけが明らかになるため、逆にその後の BCP がど

¹ JANOG Comment Index
<http://www.janog.gr.jp/doc/janog-comment/index.html>

の電子認証に適用できるものであるのかの整理が可能になると考えられる。

例えば、以下のような BCP が電子認証フレームワークにあたるドキュメントになると考えられる。

- ・インターネットで使われる電子認証の保証レベル（分類）
- ・保証レベルごとの電子認証のユーザインターフェースの違い
- ・ユーザの組織所属に使われる電子認証のレベル
- ・商用で使われるユーザアカウントの電子認証のレベル

これらの BCP が整備されることで、SSL/TLS のサーバ証明書の保証レベルや、商用 Web サイトを利用するための電子証明書などについての共通認識の形成に役立つと考えられる。

本フォーラムで扱う BCP には、電子認証技術の運用に役立つ技術情報なども含まれると考えられる。

5.3. 電子認証プラクティスフォーラムの位置づけ

本節では、具体的なフォーラムの内容を述べる前に、本フォーラムの整理（位置づけ）について述べる。以下の文章は、本フォーラムへの参加を呼びかける際に参加者に位置づけの理解を図るために作成されたものである。

2007/02/16

JPNIC

電子認証プラクティスフォーラムについて

はじめに

電子認証はインターネットを使ったサービスにおける安全や安心の基本である。インターネットを使った業務システムを始め、様々なオンラインのサービスでは予め定められた程度にユーザを特定し区別する行為が必要である。そうでなければ、ユーザやシステムが混乱するだけでなく不正行為等の再発を防止することは難しい。

第5章 電子認証フレームワークの定義と仕組み

1990年代以降、インターネットの普及が進む一方インターネットにおける不正行為が数多く露見し、セキュリティ意識を強める必要性が高まりつつある。また電子証明書等のオンラインサービスにおける電子認証技術やICカード等の認証デバイスの普及に伴い、電子認証技術の厳密かつ適切な利用が図られるようになりつつある。

しかし電子認証技術の普及が促進されるにつれて、これを適切に利用することには多くの課題があることがわかってきた。その課題は実装面と実践面の両方にある。

まず電子認証技術の実装技術は複雑で適切な実装を行うことが難しい。特に相互運用性を確保することは大きな課題である。実践については、更に制度面と実用化面に分かれ、各々に大きな課題がある。制度面では現実社会における電子認証の解釈(制度)の違いによって、公的な認証やビジネスにおける認証において利便性が上がらない問題を起す。また現実社会において実用的でなければ、安全性向上に寄与しない不適切な利用が起こりうる。

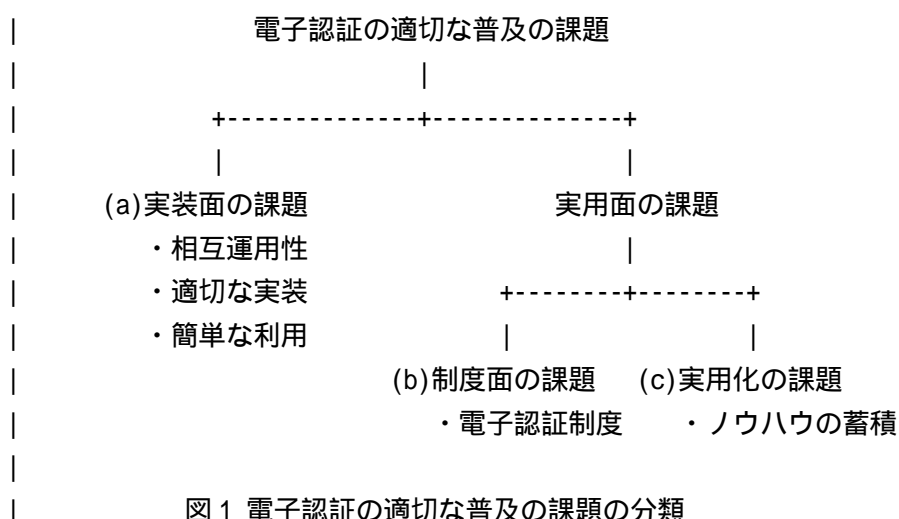


図1 電子認証の適切な普及の課題の分類

図1は電子認証の適切な普及における課題を分類したものである。これらの課題に対して、日本国内ではいくつかの取り組みが行われている。(a)に対する取り組みにはJNSAのChallengePKIおよびPKI相互運用性WGの活動が挙げられる。特にChallengePKIは電子政府における認証基盤の仕様策定に役立っている。(b)に対する取り組みには土業を中心とする電子認証局会議や日本PKIフォーラムにおける次世代認証基盤プロジェクトが挙げられる。いずれもWebを使った情報公開が行われており多くの研究者に役立っている。

JPNICでは2002年よりIPアドレスの管理を行うレジストリにおける認証局について調査研究を行ってきた。その一環としてIETFや国内外のPKIの動向について調査を行ってきたが、図1の(c)にあたる活動は専門家による必要性が指摘されているにも関わらずほとんど存在しないことがわかってきた。JPNICでは更に2005年度から2006年度にかけて(c)の活動のあり方について調査研究を行ってきた。

この文書の(c)にあたるものが「電子認証プラクティスフォーラム」であり、(a)および(b)の活動とは補完関係にあると考えられる。この考え方に基づいて、後述する本フォーラムのWebページに掲載することを想定した趣意を以下に示す。

JPNIC

電子認証プラクティスフォーラムとは

電子認証プラクティスフォーラムとは

電子認証プラクティスフォーラムとは、電子認証の適切な普及と発展を図るため、電子認証に関わるノウハウをBCP(Best Current Practice)として策定する活動を行うためのフォーラムである。

本フォーラムは基本的に考え方に基づいて活動を行う。

- ・ラフコンセンサスを重視
- ・議論と成果の一般公開

活動はメーリングリストと一年間に複数回のミーティングを通じて行う。

本フォーラムは、電子認証技術の実用的な利用に役立つノウハウの普及と蓄積を目的としており、技術を標準化することを目的としていない。活動の成果物はBCPと呼ばれるドキュメントである。本ドキュメントは基本的に参照情報であり、強制力を持つものではない。但し本フォーラムの活動内容を規定するものについてはこの限りではない。

本フォーラムの運営は経済産業省からの委託事業の一環として行われる。委託事業に先立ち、PKI(Public-Key Infrastructure)等の電子認証技術には

第5章 電子認証フレームワークの定義と仕組み

ノウハウの蓄積と共有が重要であることがわかってきている。本フォーラムは本事業の一環として実験的に運営され、2007年度の後半に成果と効果の検証が行われる。

運営に関する情報

本フォーラムの事務局を JPNIC が行う。

問い合わせ先：

社団法人日本ネットワークインフォメーションセンター
(省略)

以上。

5.4. 持続的なフォーラムのための設計

電子認証の技術的な分野においてコミュニティの形成とノウハウの共有が重要である点は前節で述べた通りだが、持続的な活動によってノウハウを蓄積していく仕組みを作るためには、ある程度慎重な設計が必要になる。

これまでも本調査研究の一環として専門家チームを設立し、技術的な議論やドキュメント策定の活動を行ってきた。しかしいずれもその設立目的を達するか主要な議論を終えてしまうと議論そのものが収束してしまう。持続可能なコミュニティの形成には、IETF でとられているようないくつかの手法を取り入れる必要があると考えられる。

持続的なコミュニティ形成に効果があると考えられる手法（IETF 等の調査より）

- ・ テーマごとの活動をライフサイクルとして捉え、全体のフォーラムは個別のテーマにとらわれずに持続させる意味を持たせる。
- ・ 議論自体を目的とするのではなく、予め想定されるアウトプットを定めてから活動を始め、議論に参加していないものにも活動状況がわかるようにする。
- ・ 趣意はドキュメント化し、実態と離れないようにする。
- ・ 活動自体の見直しを行うことができるよう、活動自体についての文書化を進めておく。

これらの手法を取り入れ、持続的にノウハウの蓄積を行えるようにしたコミュニティが本調査研究で想定するプラクティスフォーラムになると考えられる。電子認証プラクティスフォーラムは、技術の標準化ではなくノウハウを扱うため、話題が多岐に渡る可能性があるため、これらの手法以外にも実施すべき工夫が必要となる可能性はある。

5.5. フォーラムの仕組みとコミュニティ構成

本節では、電子認証プラクティスフォーラムのコミュニティの構成について、これまでの調査研究の一環として行った議論の結果を示す。本節で示す資料は、本報告書作成の為にまとめたものである。

電子認証プラクティスフォーラムにおけるコミュニティとドキュメントの扱いを図5-1に示す。

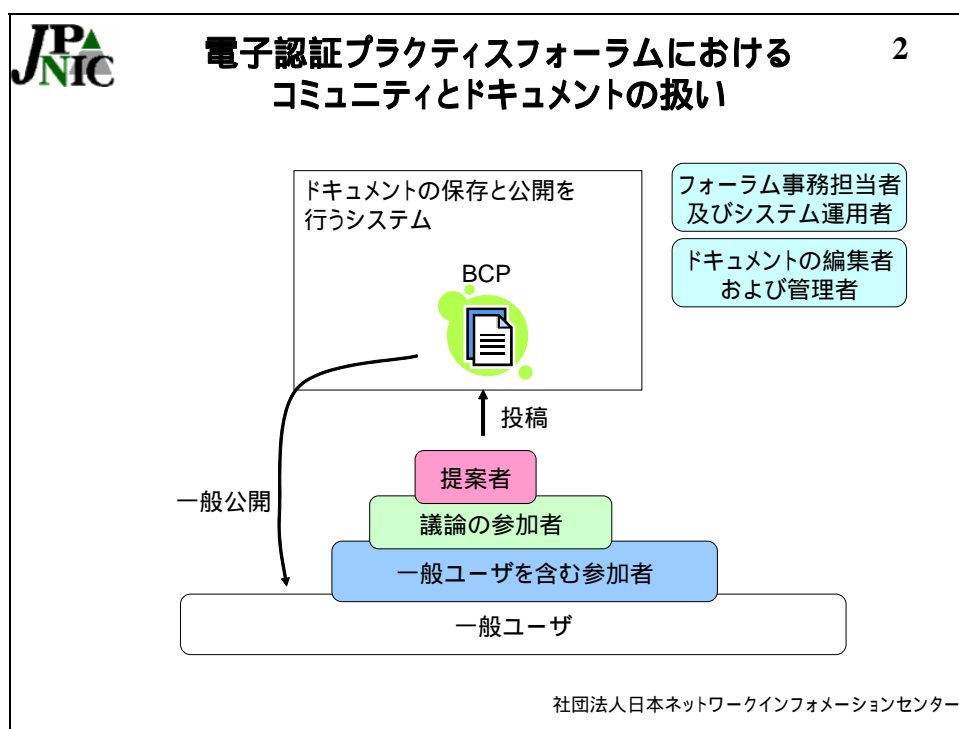


図 5-1 コミュニティとドキュメントの扱い

電子認証フレームワークにおけるコミュニティは、大きく分けて4種類のユーザに分けられる。「一般ユーザ」は電子認証の利用の有無に関わらず、Web などを使って本フォーラムが提供するドキュメントを閲覧できるユーザである。「一般ユーザを含む参加

者」は本フォーラムに参加しつつも議論への参加や提案を行わず、策定されたドキュメントの閲覧や議論の動向を追っているユーザである。「議論の参加者」は特定のドキュメントについての議論に参加し、ドキュメントを BCP 化することに協力しているユーザである。ここでは特に WG 等への参加を意味しているわけではなく、アクティブな「議論の参加者」ということを意味している。「提案者」はあるドキュメントを BCP 化することを提案したユーザである。提案者は、本フォーラムに投稿された文書が BCP 化されること、および「議論の参加者」や「一般ユーザを含む参加者」に情報公開されることを承知しており、本フォーラムを実現するシステムはその機能を提供する。BCP や議論の途中にあるドキュメントは、一般公開され一般ユーザでも閲覧できる。

本フォーラムを実現するために、参加者や一般ユーザ以外に「フォーラム事務担当者」や「システム運用者」、「ドキュメントの編集者」や「ドキュメントの管理者」が必要である。

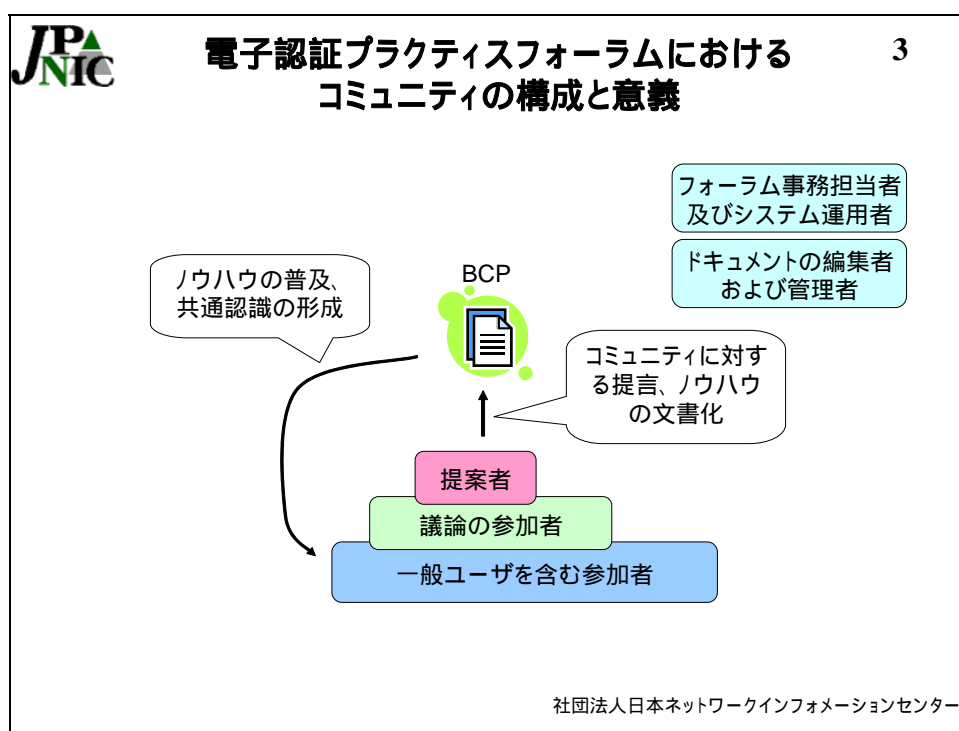


図 5-2 コミュニティの構成と意義

図 5-2 は本フォーラムのコミュニティに対する BCP の意義を示したものである。本フォーラムは提案者や参加者に対する活動に対する見返りは想定していない。従って、ドキュメントの提案者には BCP 化することのモチベーションを維持させ、また一般ユーザを含む参加者には策定された BCP を閲覧し、場合によっては議論に参加するモチベーションを維持させる必要がある。

本フォーラムにおける提案者のモチベーションとして考えられるものは、一般ユー

ザを含む参加者を含むコミュニティに対する提言と、公益性に配慮したノウハウの文書化である。コミュニティに対する提言は、技術情報の整理や分野に応じた利用技術の推奨を通じて共通認識の形成に資すると考えられる。従って技術分野における製品開発やサービス開発に役立つと考えられる。しかし特定の製品やサービスの促進を図ったものは、コミュニティの合意や後に述べる専門家によるレビューを通じて排除される可能性が高い。公益性に配慮したノウハウの文書化は、技術の適切な普及、例えばタイムスタンプビジネスの普及を図るといった観点で行われる提案になると考えられる。

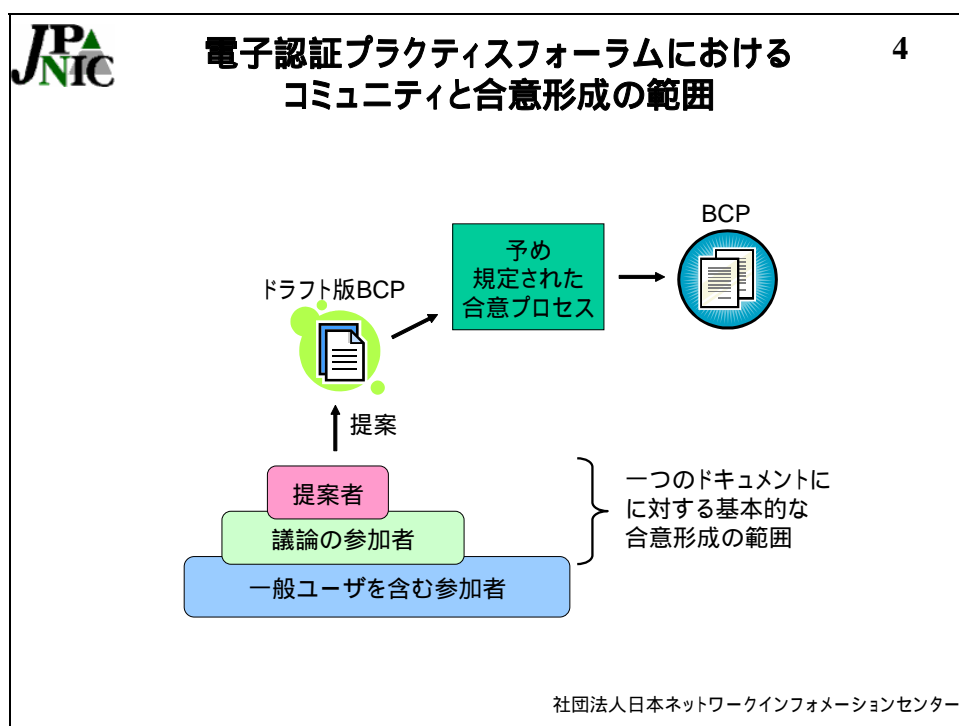


図 5-3 コミュニティと合意形成の範囲

図 5-1 で示したように、本フォーラムで策定されるドキュメントは参加者以外の一般ユーザにも公開されるが、BCP 化のプロセスの中では合意形成の範囲が設けられることが望ましい(図 5-3)。これは各ドキュメントには一定程度の専門性があると考えられ、本質的には、議論に参加していない、またはコミュニティに参加していない(参加者ではない)一般ユーザを合意形成の範囲に含めてしまうと議論が発散し、BCP 化を図ることが難しいと考えられる。従って現在の想定では提案者及び議論の参加者までの範囲とし、なおかつ合意プロセスは予め規定されドキュメント化されている必要がある。あるドキュメントの BCP 化に反対するものは議論に参加し、合意形成プロセスに含まれるようにする。また合意プロセスに反対するものは、合意プロセスを定めた BCP(事前に策定する必要がある)の「議論の参加者」として新たな BCP の形成に参加する必要があるものとする。

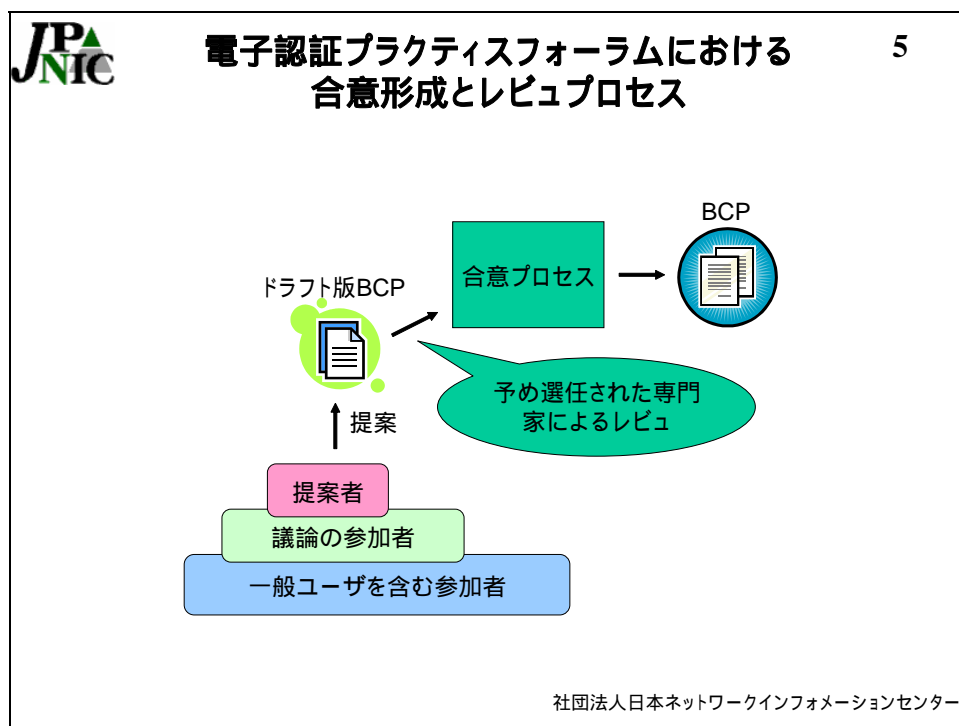


図 5-4 合意形成とレビュープロセス

本フォーラムでは、ドキュメント策定の基本原則は参加者によるコンセンサスに基づく合意プロセスであると考えられるが、専門的な技術に対するドキュメントの論旨を大きく外れないように修正する役割が必要になると考えられる。

図 5-4 は合意プロセスに入る前に「予め選任された専門家によるレビュー」が入っており、ドキュメントの洗練や技術の方向性に対する助言などができるような仕組みを示している。なお、IETF では参加者による合意プロセスの後に IESG (各エリアのエリアディレクター) によるレビューが行われることになっており、複数の専門家によるレビューが入る仕組みとなっている。本フォーラムでこれを実施するには、専門家のチームを予め作成しておき、更に本フォーラム全体の活動のレビューができるようなメンバーを選定しておく必要がある。

5.6. 電子認証プラクティスフォーラムの趣意と基本的な BCP

本節では、2006 年度の調査研究の一環で議論され、また可能な範囲で文書化した本フォーラムの趣意と基本的な BCP について述べる。本フォーラムは、フォーラム自身のルールを BCP として扱い、適宜再検討や更新を可能にする必要があると考えられている。基本的な規定を高頻度で変更することはコミュニティの活動を阻害する可能性があ

るが、ルールに関する BCP の提案者や専門家によるレビューが、その頻度を適切なものにすると考える。

本フォーラムにおける BCP の目的と書式を規定するドキュメント (BCP 案) を以下に示す。

BCP name: bcp-bcpformat-2007-01-draft.txt

Date: 2006/02/18

JPNIC

電子認証プラクティスフォーラムにおける BCP の目的と書式

1. 概要

電子認証プラクティスフォーラムで策定される BCP(Best Current Practice)の目的と書式についてまとめたものである。本ドキュメントは本フォーラムの活動を規定するものであるため、一部に強制力がある。

2. BCP の対象

電子認証プラクティスフォーラムにおける BCP の読者および作成者

3. BCP の目的

電子認証フレームワークにおける BCP は、電子認証技術の適切な普及を図ることを目的として、ノウハウをドキュメント化したものである。

ここでいうノウハウとは、BCP の提案者による十分な議論か既存の実用化を通じて得られた知識を指す。ドキュメント化の対象は一般公開が可能であるものに限り、特定の製品やサービスに限定されない情報に限る。

4. BCP の経緯が想定される状況

電子認証フレームワークにおける BCP を作成する場合や、BCP を理解するために

第5章 電子認証フレームワークの定義と仕組み

役立つ。

本ドキュメントがなければ、BCPの書式がまちまちになって作成や理解の妨げになるだけでなく、ノウハウが蓄積されない恐れがある。

5. BCPの項目と書式

5.1. 項目

BCPは以下の項目を含まなければならない。

・ヘッダー

- BCP name

BCPの名前を示す。"bcp-"に続いて作成または公開された年と改定番号をつなげたもの。最後に本フォーラムにおける状態をつなげたものとする。

例：bcp-bcpname-2007-01-draft

2007年の1番目に公開されたもので、

状態についてはbcp-bcpprocess-2007-01-draft.txtを参照。

- Date

公開された日付を示す。

- 著者の所属と氏名

著者の所属と氏名。所属組織の記入は任意である。

・タイトル

タイトルは全角で12文字～48文字とする。

・概要

BCP全体概要を示す。6行以内で記述する。

・BCPの対象

BCPの対象読者を示す。「BCPの経緯や想定される状況」と合わせて閲覧者がドキュメントを読むべきかどうかを判断するのに役立つように記述する。

- ・ BCPの目的

BCPによって当該ノウハウをまとめることの目的を示す。

- ・ BCPの経緯や想定される状況

BCPとしてまとめるべき知識が得られた経緯や、その知識が役立つと思われる状況を記述する。

- ・ 連絡先

BCPの改善のために使われる連絡先を記述する。所在地、所属、連絡先、担当または氏名などで、メールアドレスは必ず記述する必要がある。個人のアドレスである必要はない。メールアドレスの '@' は ' AT ' に置き換えること。

5.2. 記述の書式

BCPの書式はテキストファイルとする。図は基本的に罫線を利用してテキストで記述する。

書式の統一化は、事務局にて行う。公開に先立って著者の確認は行われる。

6. 連絡先

- ・ 社団法人日本ネットワークインフォメーションセンター
(省略)

以上。

5.7. フォーラムのドキュメント策定プロセス

2006年度の調査研究の段階での策定プロセスを定めたBCPを以下に示す。今後、コ

第5章 電子認証フレームワークの定義と仕組み

コミュニティの作成後、これらのプロセスをレビューし、参加者からのフィードバックを得て策定していく必要がある。

BCP name: bcp-bcpprocess-2007-02-draft.txt

Date: 2006/02/18

JPNIC

電子認証プラクティスフォーラムにおける策定プロセス

1. 概要

電子認証プラクティスフォーラムにおけるドキュメントの策定プロセスをまとめる。全てのドキュメントは、ラフコンセンサスに基づいて参加者による BCP としての認定が行われる。BCP として認定されたドキュメントは Web ページにその旨が記載され公開される。本ドキュメントは本フォーラムの活動を規定するものであるため、一部に強制力がある。

2. BCP の対象

電子認証プラクティスフォーラムにおける BCP の読者および作成者

3. BCP の目的

本 BCP は、電子認証プラクティスフォーラムにおける BCP 策定のプロセスを明確化することを目的とする。

4. BCP の経緯が想定される状況

電子認証フレームワークにおける BCP を作成する場合や、BCP を理解するために役立つ。本ドキュメントがなければ、BCP の意味が不明瞭になりノウハウが蓄積されない恐れがある。

5. 策定プロセス

電子認証プラクティスフォーラムにおける策定プロセスを図1にまとめる。

A. ドラフト(草稿)ドキュメント
<draft ステータス>

B. BCP 提案ドキュメント
<proposed ステータス>

C. 認定 BCP ドキュメント
<bcp ステータス>

図1 策定プロセス

- ・ステータスの移動

「ドラフトドキュメント」は草稿段階のドキュメントである。このドキュメントの作成は誰もが行うことができる。基本的にメーリングリストに投稿される。

以下の2点は今後記述されるべきと考えられている項目である。

- ・ドラフトドキュメントの提案者
- ・ドキュメントの有効期限

6. 連絡先

- ・社団法人日本ネットワークインフォメーションセンター
(省略)

以上。

5.8. フォーラムの為のシステム提供

本フォーラムはコミュニティにおけるドキュメントの共有と一般ユーザへの公開、そして参加者や一般ユーザに策定状況をまとめた情報の提供の機能が必要となる。これまでの検討の結果以下のサービスを提供することが必要になると考えられる。

メーリングリスト (ML)

コミュニティへの参加者が議論を行うためのメーリングリストである。またコンセンサスを得るためや、策定プロセスの進行に関する各種連絡などにも使われることが想定される。

一般ユーザがコミュニティに自由に入れる状況を作るためには、このメーリングリストは一般ユーザ自身が操作して加入できるような仕組みである必要がある。一方、スパムメールの流入を防ぐため、メンバーのみが投稿できる制限や、参加者のメールアドレスからスパムメールが送られたときの対処などが必要になると考えられる。

メーリングリストアーカイブ

ドキュメント策定プロセスの中で過去の議論を参照したり、適切な議論が行われたことを証拠としてメーリングリストでの議論はアーカイブしたりされ、次の項で述べるWeb ページで提供されることが想定される。

Web ページ

Web ページでは参加者へのドキュメント (BCP) の提供の他にドキュメントの策定状況がわかるような「ステータスページ」が必要になる。この他に本フォーラムにおいてオフラインでのミーティングが行われる場合には、資料や議事録がおかれることが考えられる。

図 5-5 に本フォーラムの実現の為のシステムの機能を示す。

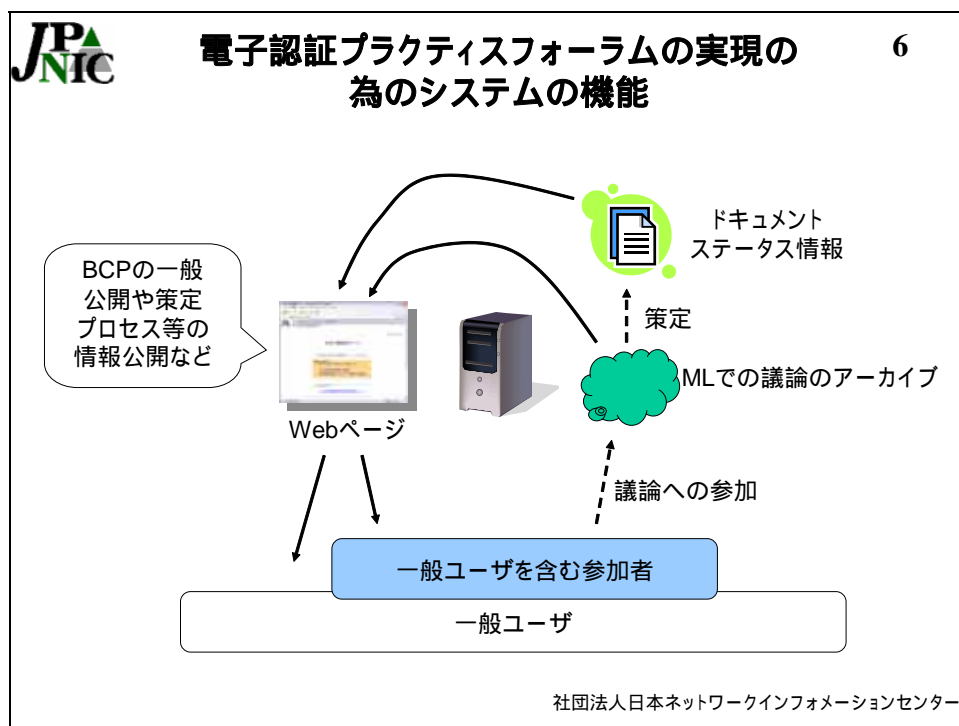


図 5-5 フォーラムの為のシステムの機能

本フォーラムでは議論され、合意プロセスを経たドキュメントは BCP として策定され Web ページで公開される。議論の内容も ML での議論のアーカイブとして公開される。従ってこれらを逐次保存し Web ページの更新を行う仕組みが必要となる。

2006 年度の調査研究では、これらの機能を実現するシステムの構築を行った。Web ページの提供や一般ユーザが参加できるような ML システムの設定も行った。今後、メーリングリストでの議論の内容を Web ページで逐次提供する機能を設置したり、本フォーラムに関する Web のコンテンツの準備などを進めたりする必要がある。

5.9. 議論と策定が必要な BCP

本調査研究では「IP アドレス認証の展開」の一環として「経路情報の登録機構」を構築し、その設計・開発の中で認証局の運用に関するノウハウがいくつか得られている。本フォーラムでは、これらの認証局の運用に役立つノウハウなどの BCP が策定できると考えられる。以下に本フォーラムで策定することが想定できる内容を挙げる。

第5章 電子認証フレームワークの定義と仕組み

認証局の運用に関する技術的な BCP

- CRL の管理運用
ネットワークアプリケーションにおける電子認証の為に電子証明書を発行する認証局では、電子証明書の失効情報の提供の仕方に工夫が必要になる。それはアプリケーション上でのユーザアカウントの有効性と電子証明書の有効性を、予め定めた状態に定める必要があるためである。例えば電子証明書は有効であってもログインはできないといった状態を作るには、予め失効情報をアプリケーション側に転送しておき、SSL/TLS のコネクションを張りつつ、アプリケーション上でのエラー表示が必要となる。「経路情報の登録機構」ではこれらの状態のあり方について検討し、設計・開発を行った。
- 認証局証明書のライフサイクル
認証局証明書は 20 年から 30 年といった長期的な有効期限を持つものであるが、クライアント証明書の有効期限と認証局証明書の有効期限の整合性を合わせるにはいくつかの工夫が必要となる。例えばクライアント証明書の有効期限を 2 年間で定める場合、認証局は認証局証明書の有効期限が切れる 2 年前には新しい認証局証明書を前提としたクライアント証明書の発行を行う必要がある。認証局証明書の更新の際に鍵の更新を行う方針で運用するならば、認証局において実際に一つの鍵を使ってクライアント証明書の発行を行うことができる期間は 18 年である。この点を踏まえてキーセレモニー（鍵生成）を行っていく必要がある。
- クライアント環境に応じた電子認証の保証レベル
クライアント証明書を使った電子申請や商用の Web サイトにおけるユーザ認証が多く行われているが、相互に利用可能であるかどうかの判断基準は少ない。クライアント証明書の利用環境（IC カードを使用しているか等）や、クライアント証明書の発行状況に応じた電子認証の保証レベルがわかる指標が普及すれば、相互の利用可能性を判断する材料になると考えられる。自然人を対象とした電子証明書である場合には、プライバシー保護の観点からインターネットを介した商取引に向かない場合があるが、社員証と同等の効力を持つクライアント証明書が他社ないし取引先でのネットワーク接続（無線 LAN における認証など）や、三文判としての電子署名としての効力を持たせられるような相互利用の可能性がある。他の認証局が発行した電子証明書の効力をどの程度のレベルであるかにマッピングすることで、同程度のレベルであれば相互の利用が可能になるような概念の普及を図ることが考えられる。

5.10. まとめと今後の課題

本章では、2005 年度より調査研究を行ってきた「電子認証フレームワーク」を策定するフォーラムである「電子認証プラクティスフォーラム」について述べた。本フォーラムは、電子認証に関わるノウハウを BCP としてドキュメント化し、一般ユーザにおける共通認識の形成などを目指したフォーラムである。「電子認証フレームワーク」は本フ

フォーラムで策定される BCP の一部に位置づけられる。電子認証フレームワークは、電子認証における保証レベルや電子認証技術の運用に関わるノウハウを BCP として扱い、複数の業界で共通認識として参照可能な概念を明文化する。

本フォーラムを実現するため、2006 年度はより詳細なフォーラムの機能とシステムの要件を明らかにした。更にそれらの機能を実現するためのサーバ構築等を行った。

今後、本フォーラムを運営するための資料作成や ML の立ち上げなどが課題となる。また今後一部の専門家だけでなく一般の人々の中から興味を持って参加して頂く方法について検討することも課題として挙げられる。

第5章 電子認証フレームワークの定義と仕組み

第6章 電子認証フレームワークとIPアドレス 認証の展開の今後

内容

- IPアドレス認証と電子認証フレームワーク
- 今後の電子認証の相互運用

6. 電子認証フレームワークとIPアドレス認証の展開の今後

2005年度および2006年度の調査研究の中で、「電子認証フレームワーク」と「IPアドレス認証の展開」を2つのテーマとして別々に扱ってきたが、実際にはこの二つは電子認証の適切な普及のために連携して進めることが必要な研究プロジェクトである。本章では、今後図られるべき連携について述べる。

6.1. これまでのIPアドレス認証と電子認証フレームワーク

本調査研究のテーマの一つである「IPアドレス認証の展開」は、日本国内のIPアドレスを管理しているNIRにおける電子認証の実践を主な活動内容として取り組まれてきた。

具体的にはJPNICに登録されたIPアドレスに関する情報を、登録・編集・削除する日本国内のISP(以下、IP指定事業者とよぶ)のクライアント認証を推進し、またその為にローカルRAといった利用環境の向上を図ってきた(図6-1)。

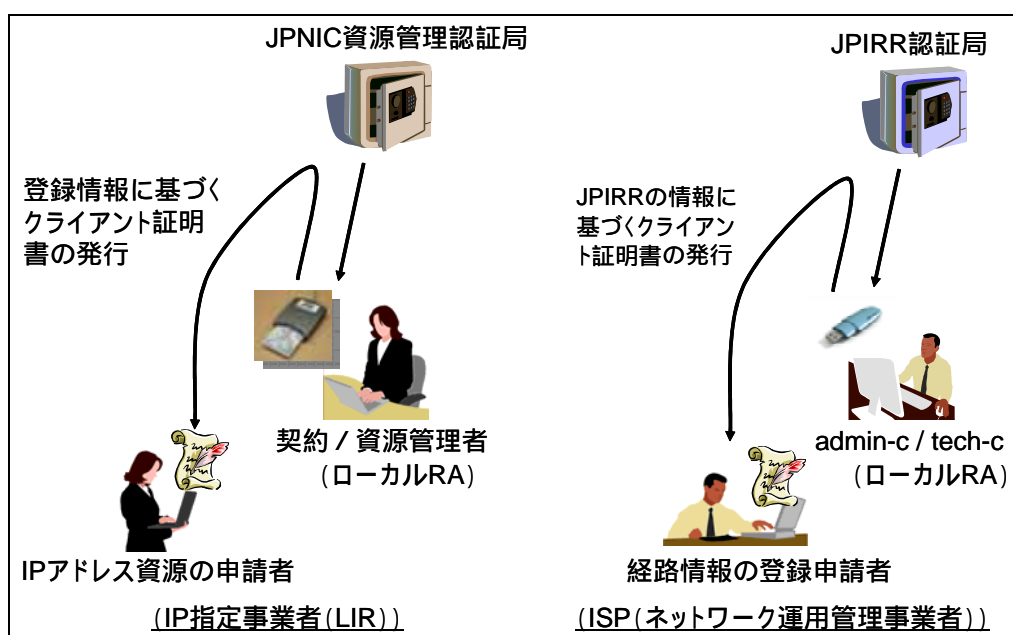


図 6-1 管理しやすいクライアント証明書の実環境整備

IP指定事業者とJPIRRのユーザ認証は、ユーザに対する電子証明書をローカルRAが管理できる仕組みで実現したものであり、証明書の発行対象は人である。この段階で電子認証フレームワークが関連することは、これらの電子認証の保証レベルである。

IP指定事業者やJPIRRのユーザに発行された電子証明書は、組織内で本人確認手続

第6章 電子認証フレームワークとIPアドレス認証の展開の今後

きが行われた、三文判的な電子証明書に位置づけることができる。これらの電子証明書はほぼ同一の保証レベルを持っているため、今後 ISP 業界やルーティングの業界で担当者同士が連絡をとり、暗号化もしくは電子署名を行う場合に、担当者印としての位置づけを持たせることが可能だと考えられる（図 6-2）。

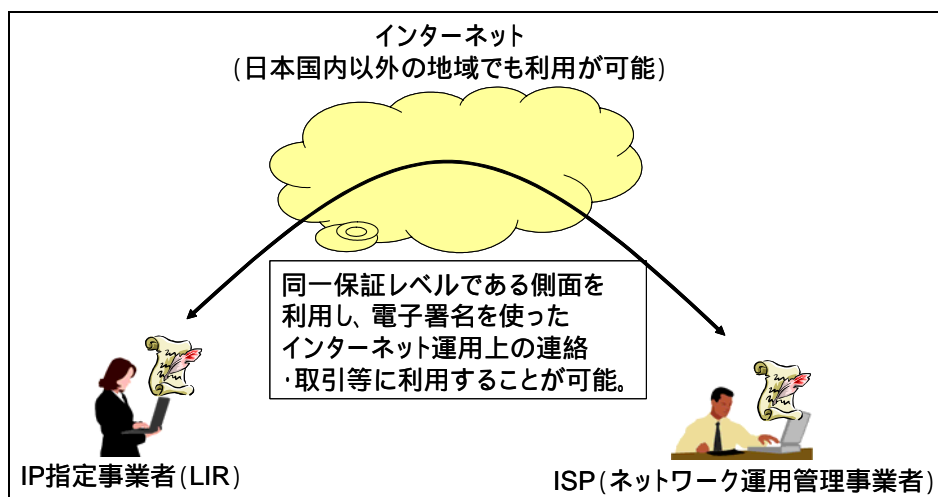


図 6-2 JPNIC 認証局の電子証明書を使った三文判的な PKI

また、これらはクライアント証明書の管理のしやすさを図った仕組みである一方、IPアドレスに関する登録情報に基づく認証情報の取り扱いを行う仕組みでもあった。ローカル RA モデルの構築によって、IPアドレスの管理者の電子証明書を使って、IPアドレスを割り当てられたホストのような人でないエンティティに対する電子証明書の管理体制を作ることができる（図 6-3）。

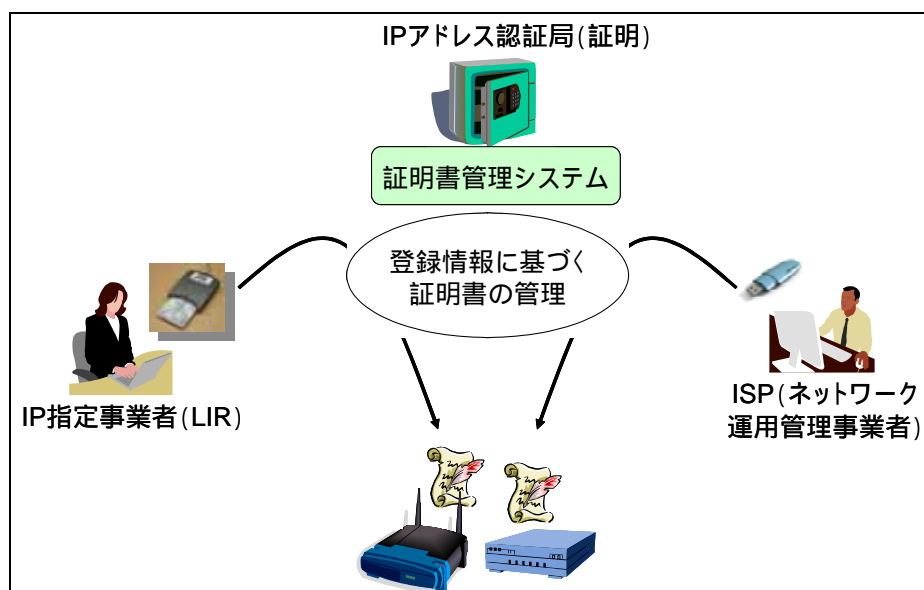


図 6-3 ローカル RA モデルの IP アドレス証明書の管理体制

6.2. IP アドレス認証の今後と電子認証フレームワーク

IP アドレス認証は今後、「経路情報の登録機構」に基づいた RFC3779 形式のリソース証明書への発展が可能である。また「経路情報の登録機構」や「JPNIC 資源管理認証局」は現在 IP レジストリシステムとの連携が行われていることから、「割り振り情報 / 割り当て情報」に基づくルーティング用の電子証明書や IPsec 用の電子証明書の発行なども検討可能な状態となった。

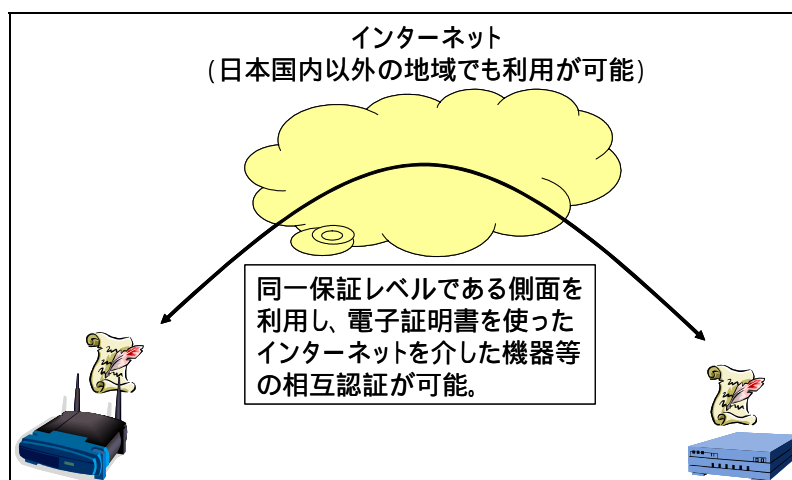


図 6-4 保証レベルに基づく人でない電子証明書の相互利用

今後、ユーザでない機器などのエンティティに対する電子証明書の位置づけを電子認証フレームワークの中で明らかにすることで、国際的に認知された電子証明書の相互利用を進めることが可能になると考えられる（図 6-5）。



図 6-5 ユーザ / IP 機器 向けの電子証明書の相互運用のイメージ

6.3. 今後の課題と活動

前節では、ユーザやインターネットに接続されたIP機器の相互認証の将来的なイメージについて述べたが、それには本調査研究で取り組んでいるノウハウの整理がある程度ついている必要がある。

今後、将来的な電子認証の相互運用を進めるためには、以下のような活動が必要になってくると考えられる。

- 電子認証の相互運用実験
実際に電子認証技術の運用を行い課題点の抽出を行っていく必要がある。得られた課題点が技術上の問題なのか運用上の問題なのかを整理し、ユーザにとってわかりやすい解決策を提示していく必要がある。
- 電子認証・電子署名技術に関する最新動向の調査
電子認証技術の問題点を整理するにあたり、技術の発展の方向性を把握しておく。例えば一方向性ハッシュアルゴリズムの代替性のように、標準化技術に変化があると運用面への影響が大きいと考えられる。
- 技術的なノウハウの整理
ノウハウを蓄積するだけでなく、文書化することでより広いユーザやサービス提供者と情報共有ができ、また運用上の問題を解決しやすくなると考えられる。

今後これらの活動に取り組み、より適切な電子認証技術の利用と普及を進める必要がある。

Appendix 1

JPNIC 資源管理認証局 認証業務規定

第 1 版 英語訳

<Appendix 1 について >

- この資料は、JPNIC 資源管理認証局の認証業務規程を英訳したものである。
 - 諸外国の技術者による内容の理解を図るために翻訳されたものである。
正確な内容確認には原文を参照する必要がある。

JPNIC Resource Service Certification Authority (IP Address Certification Authority
(Authentication)) Certification Practice Statement (CPS)

**JPNIC Resource Service Certification
Authority
Certification Practice Statement**

Version 1.0

Japan Network Information Center

CONTENTS

1. Introduction	1
1.1. Overview	1
1.2. Documentation Name and Identification.....	1
1.3. Individuals and Entities related to the PKI	3
1.4. Certificate Usage Methods	6
1.5. Policy Management.....	7
1.6. Definitions and Abbreviations	8
2. Disclosure and Repository Liability.....	10
2.1. Repository	10
2.2. Certification Information Disclosure	10
2.3. Disclosure Timing and Frequency.....	10
2.4. Repository Access Management	11
3. Identification and Authentication.....	12
3.1. Name Determination	12
3.2. Initial Authentication of Individual or Entity	13
3.3. Identification and Authentication of Individual or Entity when Applying for Key Update	15
3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application.....	15
4. Operational Requirements concerning Certificate Lifecycle.....	16
4.1. Certificate Application	16
4.2. Certificate Application Procedures.....	17
4.3. Certificate Issue	19
4.4. Certificate Receipt Confirmation	20
4.5. Utilization of Key Pairs and Certificates.....	21
4.6. Certificate Updating	22
4.7. Certificate Key Updating.....	23
4.8. Certificate Revision.....	24
4.9. Certificate Revocation and Temporary Suspension.....	25
4.10. Certificate Status Confirmation Service	29
4.11. Registration Completion.....	29
4.12. Key Escrow and Key Recovery	29
5. Facility, Management, and Operational Controls.....	30
5.1. Physical Controls.....	30
5.2. Procedural Controls	32
5.3. Personnel Controls	33
5.4. Audit Log Procedures.....	35
5.5. Record Storage	37
5.6. Key Switching.....	39
5.7. Recovery from Key Compromise and Disasters.....	40

JPNIC Resource Service Certification Authority (IP Address Certification Authority
(Verification)) Certification Practice Statement (CPS)

5.8. Termination of Certification Authority or Registration Authority Practices.....	41
6. Technical Security Management.....	42
6.1. Key Pair Generation and Installation.....	42
6.2. Private Key Protection and Cryptographic Module Technical Administration	44
6.3. Other Key Pair Administration	46
6.4. Activated Data.....	47
6.6. Administration of Life Cycle Technology	48
6.7. Network Security Management	48
6.8. Time-stamps	48
7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles	49
7.1. Certificate Profile	49
7.2. Profile of Certificate Revocation List	52
7.3. OCSP Profile.....	54
8. Compliance Audit and Other Assessments	55
8.1. Assessment Frequency and Circumstances requiring Assessment.....	55
8.2. Identity and Qualifications of Assessor	55
8.3. Relationship between the Assessor and the Entity Assessed	55
8.4. Items covered by the Assessment.....	55
8.5. Measures taken in Event of Unsatisfactory Results	55
8.6. Assessment Result Information Exchange	56
9. Problems relating to Other Practices and Legal Problems	57
9.1. Fees	57
9.2. Financial Liability.....	57
9.3. Information Confidentiality.....	57
9.4. Protection of Personal Data Privacy	59
9.5. Intellectual Property Rights	61
9.6. Representation Warranties.....	62
9.7. Limitations of Warranty	63
9.8. Limitations of Liability.....	64
9.9. Indemnity	65
9.10. Periods of Validity and Termination	65
9.11. Individual Notification and Contact between Related Persons.....	66
9.12. Amendments	66
9.13. Dispute Resolution Procedures	66
9.14. Governing Law.....	67
9.15. Compliance with Applicable Laws	67
9.16. Miscellaneous Regulations	67
9.17. Other Provisions	67

1. Introduction

1.1. Overview

This JPNIC Resource Service Certification Authority Certification Practice Statement (CPS) defines operational practices of JPNIC Resource Service Certification Authority (the Certification Authority) which issues digital certificates that are used in various authentications relating to IP addresses and AS numbers between Japan Network Information Center (JPNIC) and IP Address Management Agents.

Based on this CPS, the Certification Authority provides various certification services, such as issuing certificates, to persons belonging to the IP Address Management Agents who conduct various application processing practices (Resource Holders). The Certification Authority is operated on an experimental basis.

The structure of this CPS conforms to the RFC3647 Certificate Policy and Certification Practices Statement Framework standardized by the IETF PKIX WG.

The Certification Authority does not determine each of CP (Certificate Policy) and CPS (Certification Practices Statement) as independent items; rather it stipulates certificate policy and operations statement as this CPS.

Concerning a provision of certification practices, JPNIC comprehensively determines its own policies and obligations of certificate subjects and relying parties in this CPS and the certificate subject agreement. Note that if there is variance between the content of this CPS and the certificate subject agreement, the certificate subject agreement shall be given priority in application.

This CPS is disclosed on JPNIC CA's Website at <http://jpnica.nic.ad.jp/> in order that it may be viewed at any time by certificate subjects and relying parties.

(1) CPS

The CPS is a document that describes certificate purposes, applicable ranges certificate profiles, identification methods and certificate subject key administrations, together with the general regulations relating to certification practices. This CPS refers whenever necessary to the certificate subject agreement.

(2) Certificate Subject Agreement

The certificate subject agreement is a document that describes various practices for use of the certification service between subscribers and JPNIC, including details of certification services and obligations of subscribers.

1.2. Documentation Name and Identification

The official name of this CPS is the "JPNIC Resource Service Certification Authority

Certification Practice Statement”.

The object identifiers relating to JPNIC and the Certification Authority are shown in Table 1.1.

Table 1-1. Object Identifiers(OID) for JPNIC and JPNIC Resource Service Certification Authority

Object	Object Identifier
Japan Network Information Center	1.2.392.200175
JPNIC Resource Service Certification Authority Certification Practice Statement (CPS)	1.2.392.200175.1.2.1
End-entity Certification Policy	1.2.392.200175.1.2.1

1.3. Individuals and Entities related to the PKI

1.3.1. Certification Authority, Registration Authority, Certificate Subjects, and Relying Parties

The community of individuals or entities related to the PKI to whom the Certification Authority distributes certificates includes the participants shown in Table 1-2.

Table 1-2 Participants and Roles relating to the Community

Participant	Abbreviated Name	Role and Explanation
Resource Subscriber		Individuals or entities conducting IP address and AS number assignment and return practices.
Server		JPNIC server utilized in the certification practices
Resource Subscriber Certificate		Certificate issued to resource subscribers.
Contract/Resource Administrator		Individuals or entities conducting resource subscriber appointment, removal, and custody.
Contract/Resource Administrator Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate required for certification of contract/resource administrators when issuing certificates to resource subscribers. Concerning the handling of this certificate, management and operations are carried out while strictly following the operation regulations.
JPNIC Staff Certificate		One of the operations certificates required for the Certification Authority certification practices. It is the certificate issued for JPNIC staffs conducting practices such as management of contract/resource administrator identifiers in the IP registry system.
End-entity	EE	General name for subjects of certificate issuing, such as resource subscribers, contract/resource administrators, and JPNIC staffs.
End-entity Certificate	EE Certificate	General name for certificates issued to end-entities.

Participant	Abbreviated Name	Role and Explanation
Certificate Subscriber	Subscriber	Individuals or entities that are subscribing to certificates.
Certificate Subject	Subject	Signifies individuals or entities that have carried out certificate issue application, generated their own key, and have had certificates issued by the Certification Authority. In this CPS, this means individuals or entities that are EE certificate subjects, or server administrators.
Relying Party	RP	Individuals or entities that receive certificates, and who use these certificates for verification, carrying out their actions based on the certificate and/or a digital signature.
JPNIC Issuing Authority	JPNIC IA	General name for the Issuing Authority inside JPNIC Primary Root Certification Authority and the Issuing Authority inside JPNIC Resource Service Certification Authority. It is a conducting role that administers the certificate issuing practices in JPNIC Primary Root Certification Authority and JPNIC Resource Service Certification Authority. It issues certificates that have been requested from RA. It is used inside the Certification Authority (CA) in the situation where the certification administration functions, including certificate issuing and revocation, are to be shown.
JPNIC Registration Authority	JPNIC RA	A conducting role that confirms that the subscriber for the certificate issue is the correct individual or entity, and mainly administers registration and revocation practices. Takes responsibility for confirming and authenticating the certificate subject.
Trustee in Charge		This is the trustee in charge of JPNIC security operations, who determines JPNIC Certification Authority operations policy.
CA (Certification Authority) Operator	CAO	Individual or entity that operates and administers the Certification Authority system, including the CA Server and Directory Server.
RA (Registration Authority) Operator	RAO	Individual or entity that manages and operates Registration Authority (RA). Carries out registration work for certificate issuing and revocation.

Participant	Abbreviated Name	Role and Explanation
Repository		Database where certificates signed by the Certification Authority and CRLs are stored and published.
JPNIC Primary Root Certification Authority		This is the Root Certification Authority of all the Certification Authorities operated by JPNIC. It is positioned at the top of the certification hierarchy route in JPNIC, and carries out self-signing as well as the electronic signing of certificates for subordinate downstream Certification Authorities (Resource Service Certification Authority etc).
JPNIC Resource Service Certification Authority		This is the Certification Authority that carries out issuing of certificates relating to IP address administration practices operated by JPNIC. JPNIC Resource Service Certification Authority certificates are electronically signed by JPNIC Primary Root Certification Authority.
JPNIC Certification Authorities		General name for the Certification Authorities operated by JPNIC.
Local RA		This is an conducting role or group different from a role that issues certificates. In RA practices, this role carries out identification and judging of the correct individual or entity, certificate issue application processing, and certificate revocation processing. In the case of JPNIC Certification Authority, the IP Address Management Agents are Local RAs.
Local RA Manager		Manager of Local RA practices in the IP Address Management Agent, who conducts the appointment and removal of contract/resource administrators.
Contract/resource Administrator	Agreement/ Resource Administrator	Carries out resource subscriber member administration and certification, and resource subscriber certificate issue application operations inside the IP Address Management Agent.

1.3.2. Other Related Individuals or Entities

Not prescribed.

1.4. Certificate Usage Methods

1.4.1. Appropriate Usage of Certificates

Certificates issued according to this CPS are used by JPNIC's registry system for authentication of users and messages for the purpose of various applications and communications in IP address administration practices carried out by JPNIC.

1.4.2. Prohibited Usage of Certificates

Certificates issued according to this CPS are intended for use in various application processing operations in JPNIC. Although JPNIC does not restrict mutual use of certificates between resource subscribers of IP Address Management Agents, it does not accept any liability for use in this way.

1.4.3. Inter-operability

JPNIC Certification Authority may carry out reciprocal certification with another Certification Authority.

1.5. Policy Management

1.5.1. Organization Administrating the Documentation, and Contact Details

The organization administrating this CPS, and its contact details, are described as follows:

Japan Network Information Center

Inquiries accepted: Monday to Friday 10:00-18:00 (Excepting year-end, new year and public holidays)

E-mail address: ca-query@nic.ad.jp

1.5.2. Person determining CPS Policy Compatibility

JPNIC trustee in charge will conduct judgment of whether or not the CPS is compatible with the Certification Authority's operational policies.

1.5.3. CPS Approval Procedures

Revisions to this CPS will be disclosed after approval has been received from the trustee in charge.

1.6. Definitions and Abbreviations

The terms used in this CPS are as shown in Table 1-3.

Table 1-3 Terms Used

Term	Abbreviation	Explanation
Digital Certificate	Certificate	This is a digital document which certifies that the content described using a certain public key is held by the sender. The digital signing of the document by the Certification Authority ensures its correctness. In this CPS, provided there are no special restrictions, the resource subscriber certificate, server’s certificate, and operations certificate are all known under the general name of “certificate”.
Certification Authority	CA	This is a conducting role that carries out certificate issuing, update, and revocation, private key generation and protection, and certificate subscriber registration. In this CPS, in cases where only Certification Authority is mentioned, it includes the certificate issuing practices and the registration practices.
RFC 3647 (Request For Comments 3647)		Support framework for writers of CPS for Certification Authorities and PKI.
Object Identifier	OID	This is a name of identifier registered in a registration organization (such as ISO or ITU) that will become globally unique. Registered items such as the algorithm used by the PKI, the name stored in certificates (subject), and types (attributes such as the country name) and other items are used as object identifiers.
X.509		Format of certificates and certificate revocation lists standardized in ITU-T. In X.509 v3, extension fields are added for further optional information.
Public Key		This is the key that is made public which corresponds to the private key. The public key is utilized in encryption method and in verification method for signatures.

Term	Abbreviation	Explanation
Private Key		This is the key corresponding to the public key which is held only by the individual or entity concerned.
Certificate Signing Request	CSR	This is the data format makes the basis when issuing a certificate. The CSR includes the public key of the individual or entity requesting the certificate issuance and the certificate is issued with the signature of the issuer to certify this public key.
Certificate Revocation List	CRL	This is the revocation list of EE certificates and operational certificates that have been revoked during the certificate validity period for reasons such as compromise of EE's private key.
PIN (Personal Identification Number)		Information used for identification of individuals.

2. Disclosure and Repository Liability

2.1. Repository

The Certification Authority strives for maintenance and administration that will allow repository use 24 hours per day, seven days a week. The repository includes a certificate repository and an information disclosure repository. In the situation where it is necessary to suspend the system for system maintenance, notification will be sent to certificate subjects, relying parties and related individuals or entities beforehand, or an announcement will be made on the Webpage. However, this may not always be possible, such as on the occurrence of unavoidable situations, including natural disasters, incidents, and problems.

2.2. Certification Information Disclosure

The following information is disclosed on the information disclosure repository:

- CPS

Further, the following information is disclosed on the certificate repository.

- EE certificates
- CRL

However, the EE certificates and CRL will only be disclosed to relying parties.

Note that important information relating to the CPS and the Certification Authority is disclosed on the Webpage with the URL shown below.

<http://jpnica.nic.ad.jp/>

2.3. Disclosure Timing and Frequency

Regarding the information disclosed by the Certification Authority, the disclosure timing and frequency will be as follows:

- For the CPS, disclosure will be made whenever revisions are made.
- For self-signed certificates, linked certificates, and downstream Certification Authority certificates, disclosure will be made whenever issued or updates are made.
- For the CRL, disclosure will be made whenever issued. The frequency of issue will be as stipulated in “4.9.7 Certification Revocation List Issuing Frequency” in this CPS.
- Important information and other information concerning the Certification Authority will be updated as appropriate whenever necessary.
- For EE certificates, disclosure will be made whenever issued or updated.

2.4. Repository Access Management

Concerning the information disclosed by the Certification Authority, with the exception of read-only control, special degrees of access control are not implemented. The relying party for the EE certificates used for verification will be JPNIC. Accordingly, the certificate repository is basically provided to JPNIC.

3. Identification and Authentication

3.1. Name Determination

3.1.1. Types of Names

The certificate issuer name and issue subject name will be configured according to the regulations for the identifying name in the X.500 Series definitions.

3.1.2. Necessity for Names to Incorporate Meanings

It is necessary that names described in the certificate should show the subject individual's name, organization, role name, and equipment name.

3.1.3. Subject Anonymity

In the certificate, as long as the name allows specification of the individual, organization, role, and equipment, it is not necessary to use real names.

3.1.4. Rules for Interpreting Various Name Formats

The rules for interpreting the various name formats follow the rules for the identifying name in the X.500 Series definitions.

3.1.5. Uniqueness of Names

The names described in the certificates issued based on the same policy by the Certification Authority will be unique for all EEs. In the situation where an update has been carried out on a certificate for the same EE, there may be duplication of the certificate and name prior to updating.

3.1.6. Trademark Recognition, Authentication and Roles

Not specified.

3.2. Initial Authentication of Individual or Entity

3.2.1. Method used to Prove Possession of Private Key

The Certification Authority confirms that the applicant for the resource subscriber certificate possesses the private key utilizing a certificate signing request (CSR) that has been digitally signed following PKCS#10 (Public-Key Cryptography Standards #10) or another method determined by the Certification Authority.

Concerning the server's certificate, the Certification Authority uses a method stipulated beforehand to confirm that the certificate subscriber possesses its private key.

3.2.2. Authentication of Organization Identity

The Certification Authority conducts authentication of organizations and groups as Local Registration Authorities. Organizations and groups intending to receive authentication as Local RAs must be IP Agents.

Regarding server's certificates, the Certification Authority confirms that the organization or group conducting the operation and maintenance of the server for which the certificate is to be issued is JPNIC, or an organization or group approved by JPNIC.

3.2.3. Authentication of Individuals

When conducting issue registration of applicants for contract/resource administrator certificates, JPNIC authenticates the applicants following the prescribed procedures.

When conducting issue registration of applicants for resource subscriber certificates, contract/resource administrators take responsibility for carrying out authentication of the applicants following the prescribed procedures.

When conducting issue registration of applicants for JPNIC staff certificates, JPNIC will authenticate the applicants following the prescribed procedures.

Concerning server's certificates, the Certification Authority will confirm that persons requesting the issue of certificates are persons who have received permission for certificate issue from JPNIC or an organization or group approved by JPNIC.

3.2.4. Unconfirmed Subject Information

Not specified.

3.2.5. Confirmation of Authority Appropriateness

Regarding the receipt of application registration for resource subscriber certificates from contract/resource administrators, the Certification Authority will confirm the appropriateness of the contract/resource administrator concerned.

3.2.6. Interoperability requirements

Not stipulated.

3.3. Identification and Authentication of Individual or Entity when Applying for Key Update

3.3.1. Identification and Authentication of Individual or Entity for Normal Key Updating

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.3.2. Identification and Authentication of Individual or Entity for Key Updating after Certificate Revocation

Same as procedures defined in “3.2 Initial Authentication of Individual or Entity” in this CPS.

3.4. Identification and Authentication of Individual or Entity during Certificate Revocation Application

After conducting identification of an individual or entity as the revocation applicant for contract/resource administrator certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

The contract/resource administrator will in principle conduct identification of an individual or entity as the revocation applicant for resource subscriber certificates, and will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

After conducting identification of an individual or entity as the revocation applicant for JPNIC staff certificates, JPNIC will have the Certification Authority carry out revocation registration according to the methods determined by the Certification Authority.

Regarding server’s certificates, the Certification Authority will confirm using a method prescribed beforehand that the individual or entity applying for the certificate revocation has received permission to issue certificates from JPNIC or an organization or group approved by JPNIC.

4. Operational Requirements concerning Certificate Lifecycle

4.1. Certificate Application

4.1.1. Individuals or Entities that can Submit Certificate Applications

Individuals or entities that can apply for contract/resource administrator certificates will be persons employed by IP Agents.

Individuals or entities that may apply for resource subscriber certificates will be verified contract/resource administrators.

Individuals who may apply for JPNIC staff certificates will be persons employed by JPNIC.

Individuals who may submit applications for server certification will be JPNIC staffs or persons specified by JPNIC.

4.1.2. Registration Procedures and Responsibilities

Applicants for contract/resource administrator certificates should apply to JPNIC for issue of the certificate according to the method notified beforehand by JPNIC. According to the content of the application, the contract/resource administrator will confirm the role.

Applicants for resource subscriber certificates should submit the certificate issue application to the contract/resource administrator using the method notified beforehand by the contract/resource administrator. Further, providing that the certificate applicant has been notified by the Certification Authority of the 2 types of information necessary for key pair generation and certificate issue, the key pairs should be generated and the digitally signed certificate signing request should be sent via secure online communications to the Certification Authority following the certificate signing request data format such as PKCS#10. The digital signature of the certificate signing request will be verified.

Applicants for server's certificates should conduct certificate issue application using the method prescribed beforehand by the Certification Authority.

Applicants for JPNIC staff certificates should carry out certificate issue application using the method prescribed beforehand by the Certification Authority.

Concerning the application for certificates, the certificate applicant will bear the following responsibilities:

- Acceptance of the contents of this CPS and other documentation disclosed by the Certification Authority.
- Correct production of certificate application content.

4.2. Certificate Application Procedures

4.2.1. Individual or Entity Identification and Authentication Function Implementation

Authentication of individual or entity as an applicant for contract/resource administrator certificates is carried out by JPNIC Registration Authority administrator.

Authentication of an individual or entity as an applicant for resource subscriber certificates is carried out by the contract/resource administrator. The contract/resource administrator implements authentication of correct individual or entity as applicants for resource subscriber certificates based on “3.2.3 Authentication of Individuals” in this CPS. The contract/resource administrator takes responsibility relating to the authentication of an individual or entity as an applicant for resource subscriber certificates.

Authentication of an individual or entity as an applicant for JPNIC staff certificates is carried out according to the method prescribed in advance by the Certification Authority.

Authentication of an individual or entity as an applicant for server’s certificates is carried out according to the method prescribed in advance by the Certification Authority.

4.2.2. Certificate Application Approval and Rejection

Regarding the applications from applicants for resource subscriber certificates, the contract/resource administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. The contract/resource administrator will take responsibility for the application judging.

Regarding the applications from applicants for contract/resource administrator certificates, JPNIC Registration Authority administrator determines whether the certificate application will be accepted or rejected based on judging standards prescribed beforehand. In the case where the application is accepted, certificate application registration will be carried out for the Certification Authority. JPNIC Registration Authority administrator will take responsibility for the application judging.

Note that after conducting confirmation of correct individual or entity as the contract/resource administrator carrying out application registration of the resource subscriber certificate, the Certification Authority will begin the certificate issuing procedures.

Regarding JPNIC staff certificates, the Certification Authority will determine whether the application will be accepted or rejected.

Regarding server's certificates, the Certification Authority will determine whether the application will be accepted or rejected.

4.2.3. Certificate Application Processing Time

In the case where the issue application from applicants for resource subscriber certificates is accepted, the contract/resource administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application from applicants for contract/resource administrator certificates is accepted, JPNIC Registration Authority administrator will swiftly carry out the certificate issue application registration.

In the case where the issue application registration is accepted from the contract/resource administrator or JPNIC Registration Authority administrator, the certificate will be swiftly issued.

Regarding JPNIC staff certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

Regarding server's certificates, in the case where the Certification Authority accepts an issue application from an individual or entity prescribed in "4.1.1 Individuals or Entities that can Submit Certification Applications", it will swiftly carry out issue of the certificate.

4.3. Certificate Issuing

4.3.1. Certification Authority Actions in the Certificate Issuing Process

Concerning the receipt of the issue application registration for resource subscriber certificates from the contract/resource administrator, the Certification Authority will conduct authority confirmation of the contract/resource administrator using the method prescribed beforehand. Further, concerning the receipt of issue application registration for contract/resource administrator certificates, authority confirmation of the contract/resource administrator will be carried out according to previously prescribed methods. After confirming the authenticity of the application registration, the Certification Authority will give out notification of the permission for issue of the certificate to the applicant for the resource subscriber certificate using the methods prescribed in “4.3.2 Certificate Issue Notification for Certification Authority Subjects” in this CPS.

The Certification Authority verifies the digital signature of the certificate signing request sent by the applicant for the resource subscriber certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the resource subscriber certificate via secure online communications.

The Certification Authority verifies the digital signature of the certificate signing request sent by the applicant for the contract/resource administrator certificate. Then, after confirming the authenticity of the certificate signing request, the certificate is issued to the applicant for the contract/resource administrator certificate via offline means.

Concerning JPNIC staff certificates, after conducting confirmation of correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

Concerning server's certificates, after conducting confirmation of correct individual or entity for the applicant, the Certification Authority will issue the certificate using the method prescribed beforehand.

4.3.2. Certification Issue Notification for Certification Authority Subjects

Issue notification regarding contract/resource administrator certificates will be sent to applicants using offline means.

The Certification Authority will generate the 2 types of information required for the certificate issuing, and will notify the applicant for the resource subscriber certificate via the contract/resource administrator using two different methods.

Regarding JPNIC staff certificates, the Certification Authority conducts issue notification to applicants using methods prescribed beforehand.

Regarding server's certificates, the Certification Authority conducts issue notification to applicants using methods prescribed beforehand.

4.4. Certificate Receipt Confirmation

4.4.1. Certificate Receipt Confirmation Actions

Receipt of contract/resource administrator certificates will be conducted using offline means. In the case where there is a problem with the certificate, contact should be made with JPNIC. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

The Certification Authority will deliver contract/resource administrator certificates by a method that will allow confirmation of the certificate's arrival. Downloading of the certificate will be carried out by the applicant for the resource subscriber certificate, and the certificate should be received after confirming the content. In the case where there is a problem with the certificate, contact should be made with JPNIC via the contract/resource administrator. If no contact is received by JPNIC within 1 week of sending the certificate, it will be considered to have been received.

Regarding JPNIC staff certificates, the Certification Authority will confirm the receipt of the certificate using a method involving offline means prescribed beforehand.

Regarding server's certificates, the Certification Authority will confirm the receipt of the certificate using a method involving offline means prescribed beforehand.

Note that the applicant for the certificate must confirm that the certificate file is possible to be used on their computing environment, and that the details described in the certificate are correct.

4.4.2. Disclosure of the Certificate by the Certification Authority

The Certification Authority will disclose the certification using the repository according to "2.2. Certification Information Disclosure" in this CPS.

4.4.3. Certification Issue Notification by Certification Authority to Other Entities

The Certification Authority will not carry out certification issue notification to other entities.

4.5. Utilization of Key Pairs and Certificates

4.5.1. Subject Private Key and Certificate Use

Certificates issued based on this CPS are intended to be used for practices such as applications between JPNIC and IP Address Management Agents.

Certificate subjects will bear the following responsibilities regarding the use of the private key and the certificate:

- Confirmation and reporting of any errors in the content of the certificate on receipt of the certificate.
- Taking of adequate care and administration of the private key to prevent theft, leakage, loss, or inappropriate use by another entity.
- Swift revocation application in situations where there is a danger or possibility of the key becoming compromised.
- Confirmation of the usage purpose and use within this purpose.
- Maintaining the confidentiality of the private key and administering the correspondence of the private key and public key.

4.5.2. Relying Party Public Key and Certificate Use

The certificate relying party bears the following responsibilities concerning the reliability of the certificate:

- Understanding and agreement with this CPS at the point of time that the certificate is trusted.
- Agreement that the certificate usage purpose and the relying party's usage purpose are in accord.
- Verification of the digital signature used in the certificate and confirmation of the issuing authority.
- Confirmation of the certificate period of validity and the described items.
- Confirmation using the Certificate Revocation List (CRL) that the certificate has not been revoked.
- Confirmation of all certificates on the certificate path regarding falsification, periods of validity, revocation, and usage purpose.

4.6. Certificate Updating

In the Certification Authority, certification updating will not be conducted without revising the key pair. In the case where the certificate is updated, a new key pair will be generated using the procedure defined in “4.7 Certificate Key Updating” in this CPS.

4.6.1. Case where Certificate Updating is to be Conducted

Not stipulated.

4.6.2. Individuals or Entities that can Apply to Update Certificates

Not stipulated.

4.6.3. Certificate Updating Application Processing

Not stipulated.

4.6.4. Notification to Subjects of New Certificates

Not stipulated.

4.6.5. Updated Certificate Receipt Confirmation Actions

Not stipulated.

4.6.6. Disclosure of Certificates Updated by the Certification Authority

Not stipulated.

4.6.7. Notification to Other Entities

Not stipulated.

4.7. Certificate Key Updating

4.7.1. Situations where Certificate Key is Updated

Certificate key updating will be carried out in the following situations:

- Case where the certificate period of validity has expired.
- Case where certificate has been revoked due to the reason of key compromise.

4.7.2. Individuals or Entities that can Apply for New Public Key Certification

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.3. Certificate Key Updating Application Processing

Same as procedures defined in “4.2. Certificate Application Procedures” and “4.3. Certificate Issue” in this CPS.

4.7.4. New Certificate Notification for Subjects

Same as “4.3.2. Certificate Issue Notification for Certification Authority Subjects” in this CPS.

4.7.5. Key Updated Certificate Receipt Confirmation Actions

Same as “4.4.1. Certificate Receipt Confirmation Actions” in this CPS.

4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority

Same as “4.4.2. Disclosure of the Certificate by the Certification Authority” in this CPS.

4.7.7. Notification to Other Entities

Same as “4.4.3. Certificate Issue Notification by Certification Authority to Other Entities” in this CPS.

4.8. Certificate Revision

4.8.1. Case where Certificates will be Revised

Certificate revision will be carried out in the following situation:

- Case where information in the certificate other than the public key has been revised.

4.8.2. Individuals and Entities that can Apply for Revisions to Certificates

Same as “4.7.2 Individuals or Entities that can Apply for New Public Key Certification” in this CPS.

4.8.3. Revision Application Processing

Same as “4.7.3. Certificate Key Updating Application Processing” in this CPS.

4.8.4. New Certificate Notification for Subjects

Same as “4.7.4. New Certificate Notification for Subjects” in this CPS.

4.8.5. Receipt Confirmation Actions for Revised Certificates

Same as “4.7.5. Key Updated Certificate Receipt Confirmation Actions” in this CPS.

4.8.6. Disclosure of Revised Certificates by Certification Authority

Same as “4.7.6. Disclosure of Certificate that has had Key Updated by the Certification Authority” in this CPS.

4.8.7. Certificate Issue Notification by Certification Authority to Other Entities

Same as “4.7.7. Notification to Other Entities” in this CPS.

4.9. Certificate Revocation and Temporary Suspension

4.9.1. Circumstances of Certification Revocation

The subject of the resource subscriber certificate must carry out certificate revocation application to the contract/resource administrator.

The subject of the contract/resource administrator certificate must carry out certificate revocation application to JPNIC.

In situations where it is determined that the following items apply, the Certification Authority will be able to revoke the various certificates:

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised, or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the private key of the certificate subject has been compromised, or there is a danger of compromise.
- Situation of inappropriate use of certification, or the danger of inappropriate use.
- Situation where the certificate subject or the local RA does not implement work according to this CPS or other agreements, regulations and laws.
- Situation where the agreement between JPNIC Certification Authority and the IP Address Management Agent has been cancelled.
- Other situations in which the Certification Authority has determined that revocation is necessary.

In the situation where the following items apply to the subject of the server's certificate, revocation application must be carried out through the Certification Authority.

- Situation where the server use is suspended.
- Situation where the server private key has been compromised (or if there is a danger of compromise).

Further, in the situation where the following items apply, it will be possible to carry out server's certificate revocation in addition to cases where the Certification Authority receives a revocation request from the certificate subject.

- Situation where the Certification Authority is abolished.
- Situation where the Certification Authority private key has been compromised, or there is a danger of compromise.
- Situation where the certificate content items differ from the actual situation.
- Situation where the server private key has been compromised, or there is a danger of compromise.
- Certificate inappropriate use, or the danger of inappropriate use.

- Situation where the certificate subject does not implement work according to this CPS or other agreements, regulations and laws.
- Other situations in which the Certification Authority judges that revocation is necessary.

4.9.2. Individuals or Entities that can Apply for Certificate Revocation

Individuals or entities that can request revocation of resource subscriber certificates are as follows:

- Certificate subject
- Legal representative of the certificate subject
- Local RA manager and contract/resource administrator of the organization to which the certificate subject belongs
- The Certification Authority

Individuals or entities that can request revocation of server's certificates are as follows:

- Certificate subject
- The Certification Authority

4.9.3. Revocation Application Procedures

After confirming the appropriateness of the revocation request according to the specified procedures, the contract/resource administrator carries out certificate revocation registration in the Certification Authority.

After confirming the appropriateness of the revocation request according to the specified procedures, JPNIC carries out certificate revocation registration in the Certification Authority.

The server's certificate subject carries out the revocation application for the Certification Authority using methods that have been previously prescribed.

Note that in the situation where the Certification Authority has determined that the items specified in "4.9.1. Circumstances of Certificate Revocation" are applicable; this Certificate Authority may carry out the certificate revocation registration following its own judgment

4.9.4. Revocation Application Delay Period

In the situation where conditions have occurred that require certification revocation, the revocation will be conducted as swiftly as possible.

4.9.5. Period during which the Certification Authority should carry out Processing of the Revocation Application

The certificate revocation processing will be carried out in the Certification Authority within five working days of receiving the revocation application.

4.9.6. Relying Party Revocation Checking Request

Concerning the reliance and use of the certificate issued by the Certification Authority, the certificate relying party must refer to the latest Certificate Revocation List (CRL) to confirm that the certificate in question has not had revocation processing carried out.

4.9.7. Certificate Revocation List Issuing Frequency

Regardless of whether or not there are certificate revocations, the CRL will be updated within 24 hours. In the situation where certificate revocation has been applied for, the CRL will be updated as soon as the revocation procedures have been completed.

4.9.8. Maximum Grace Period for Issue of Certificate Revocation List

After generating the CRL, the Certification Authority will swiftly disclose it on the repository.

4.9.9. Applicability of Revocation/Status Confirmation Online

Online revocation or status check functions such as OCSP are not supported.

4.9.10. Requirements for Conducting Online Revocation/Status Confirmation

Not stipulated.

4.9.11. Other Formats of Revocation Notification that may be Used

Not stipulated.

4.9.12. Special Conditions regarding Compromise of the Key Update

In the situation where there has been a compromise or danger of compromise of the private key of the Certification Authority, revocation processing of all of the certificates will be immediately conducted. Certificates will be registered in the CRL, and the facts of the compromise of the Certification Authority's private key and the notification of certificate revocation will be sent to certificate subjects using means such as E-mail.

4.9.13. Situation of Certificate Temporary Suspension

The Certification Authority will not temporarily suspend a certificate that has been issued.

4.9.14. Individuals or Entities that can Apply for Temporary Suspension of Certificates

Not stipulated.

4.9.15. Certificate Temporary Suspension Application Procedures

Not stipulated.

4.9.16. Period over which the Temporary Suspension can be Continued

Not stipulated.

4.10. Certificate Status Confirmation Service

4.10.1. Characteristics of Operation

The Certification Authority will provide CRLs as a means for relying parties to confirm certificate status. The conditions for accessing the CRL are specified in “2.4. Repository Access Management” in this CPS. Further, the CRL issue frequency and maximum issue grace period are specified in “4.9.7. Certificate Revocation List Issuing Frequency” and “4.9.8. Maximum Grace Period for Issue of Certificate Revocation List” in this CPS.

4.10.2. Service Usage Possibility

Specified in “2.1 Repository” in this CPS.

4.10.3. Optional Specifications

Not stipulated.

4.11. Registration Completion

In the situation where the certificate subject has completed the Certification Authority service usage registration, the Certification Authority will revoke all of the certification issued to the certificate subject.

4.12. Key Escrow and Key Recovery

The Certification Authority will not deposit its private key with any third party.

4.12.1. Key Escrow and Key Recovery Policy and Implementation

Not stipulated.

4.12.2. Session Key Encapsulation and Key Recovery Policy and Implementation

Not stipulated.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

The important facilities related to the Certification Authority are installed in locations where they will not be easily affected by damage from fire, water exposure, earthquakes, lightning or other natural disasters. The building structure incorporates measures for resistance to earthquakes and fire, and prevents against illegal entry. There is no indication of the location of the certification facilities room inside and outside the building.

Further, the equipment used will be located in a secure place, protected from disasters and improper access.

5.1.2. Physical Access

Concerning the certification facilities room, the Certification Authority conducts room entry-exit management that allows identification of persons who have been cleared for entry beforehand and confirmation of entry clearance. The Certification Authority in principle does not permit entry to the room of persons who do not have entry clearance. In situations where it is necessary for entry to be permitted, clearance will be obtained from the Certification Authority Operation Administrator beforehand, and the person granted entry will be accompanied at all times by a person who has clearance to enter the room.

5.1.3. Electric Power and Air Conditioning

In addition to securing an adequate capacity of electric power supply for operating the equipment, the Certification Authority will also implement measures to prepare against momentary power lapses, power failures, and fluctuations in voltage and frequency. Further, regarding air conditioning equipment, the room temperature will be maintained and administered at levels that will not adversely affect the various equipment being used.

5.1.4. Measures against Water Exposure and Earthquakes

Measures against water exposure will be implemented in the room where the Certification Authority is located in order to keep the level of damage due to water exposure to a minimum. Further, JPNIC Certification Authority will implement measures to prevent equipment and furniture from toppling over or falling down in the occurrence of an earthquake.

5.1.5. Fire Prevention and Fire Protection Measures

The Certification Authority has located the facilities inside fire prevention blocks that divide the area using firewalls. Further, inside the fire prevention blocks, fire prevention measures are implemented in the power source and air conditioning equipment, and fire detectors and fire-fighting equipment is also installed.

5.1.6. Media Storage Location

The media including archived data and backup data are stored in a storage warehouse inside a room where appropriate entry-exit management is carried out. Further, duplicates of important media will be stored in a storage warehouse that is separate from the Certification Authority's equipment location inside a room where appropriate entry-exit management is carried out.

5.1.7. Disposal Processing

For documentation and recording media including information that requires handling as confidential data, the Certification Authority will conduct appropriate disposal processing following methods prescribed beforehand including information initializing and deletion.

5.1.8. Backup Outside the Facilities

Not stipulated.

5.2. Procedural Controls

5.2.1. Trusted Roles

Persons carrying out key practices such as certificate issue, updating, and revocation undertake trusted roles in this CPS.

5.2.2. Employees Required for Each Operation

In the situation where it is necessary for persons who do not have entry authority to enter the Certification facilities room, such as for the maintenance of the Certification Authority facilities and responses during failures of JPNIC Certification Authority equipment, the people will at all times be accompanied by a person who is authorized to be in the room.

5.2.3. Identification and Authentication of Individual or Entity for Particular Roles

The Certification Authority equipment includes a function for discriminating between operators and necessary authorization. Further, the authorization for operation of the Certification Authority equipment can be configured for each operator.

5.2.4. Roles Requiring Task Division

By dividing authority among several persons rather than concentrating authority in a particular person, it is intended to prevent the occurrence of improper actions caused by individual operation. The authority will be divided for system operation, approval actions, and auditing.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Identification Requirements

When appointing employees to roles in the Certification Authority, and periodically afterwards, JPNIC will implement appropriate character investigations before making appointments. When making appointments, non-disclosure agreements will be signed, and appropriate information management will be carried out. Further, during daily practices, continuous personnel management will be carried out including mental health and health management and appropriate treatment.

5.3.2. Regulatory Items relating to Personnel Assignments

Concerning the appointment of key persons for the Certification Authority practices, appropriate personnel will be allocated to avoid problems occurring during operation execution. Allocated employees will be required to submit pledges to strictly maintain confidentiality and observe internal regulations.

5.3.3. Training Requirements

For the education of key operational personnel, the following will be carried out:

- Before the key operational personnel take up their roles, necessary education will be implemented regarding the Certification Authority operations.
- Education and training plans will be developed supporting each role, and regular education and training will be implemented following the plans.
- In the situation where changes are made to the practice procedures, the changes to the work handling points will be made without delay, and education and training relating to these changes will be implemented.

5.3.4. Retraining Frequency and Requirements

JPNIC will regularly conduct appropriate education for Certification Authority key employees, and will carry out re-education afterwards if necessary.

5.3.5. Work Rotation Frequency and Order

Not stipulated.

5.3.6. Penalties for Carrying out Unapproved Actions

Concerning unapproved actions carried out by Certification Authority key operational personnel, penalties will be imposed according to the regulations specified beforehand.

5.3.7. Independent Contractor Requirements

JPNIC will clearly explain the details of the commissioned work in the commissioning agreement, clarifying for the contractor the strict observance of JPNIC directions, liability sharing, warranty, and penalties for infringements, and will also enter into a non-disclosure agreement. Further, after commissioning the work, auditing and administration will be carried out to confirm that the practices are being implemented appropriately.

5.3.8. Materials Supplied to Key Employees

Documentation necessary for the operations will be disclosed and notified to the operations key employees.

5.4. Audit Log Procedures

5.4.1. Types of Events Recorded

For events occurring in the Certification Authority system, regardless of whether they occur manually or automatically, the date, time, subject of the event, and the event details will be recorded.

The following records will be recorded as the necessary audit log for detecting Certification Authority mistaken operation and improper operation, and certifying the appropriateness of operations:

- Records relating to the operation of the Certification Authority private key
- Records relating to certificate issue and revocation work
- Records relating to the revocation information production practices
- Records relating to the confirmation of the audit log

Further, the records of accesses to the Certification Authority equipment will be recorded.

5.4.2. Frequency of Processing the Audit Log

The Certification Authority regularly reviews the audit log and the related records.

5.4.3. Period during which the Audit Log is Retained

The audit log will be retained on the server inside the Certification Authority for a minimum of 2 months. After this time, it will be stored for a fixed period on an external recording medium. Records relating to the entry and exit from the certification facilities room, and records concerning improper access will be retained until completion of the next audit.

5.4.4. Audit Log Protection

In order that only authorized JPNIC staffs can access the audit log file, the Certification Authority appoints an authorizer to protect the log file from being viewed, edited, or deleted by unauthorized persons. Further, the audit log will be regularly backed-up to external recording media which will be stored in a lockable storage warehouse in a room with appropriate entry and exit administration.

5.4.5. Audit Log Backup Procedure

Following procedures determined beforehand, the audit log together with the Certification Authority system database will be regularly backed-up on external recording media, and the media stored in a safe facility.

5.4.6. Audit Log Collection System

An audit log collection function is incorporated as one of the functions in the Certification Authority system, and important events relating to security are collected as the audit log.

5.4.7. Notification to Subject causing the Event

In the Certification Authority, the audit log collection is carried out without giving notification to the person, system or application that caused the event.

5.4.8. Vulnerability Assessment

The hardware and software used in the certification practices is assessed for security vulnerabilities from the system and operations points of view using audit log inspections, and the latest applicable security technology is introduced to improve security measures.

5.5. Record Storage

5.5.1. Archive Record Types

In addition to the audit log specified in “5.4.1. Types of Recorded Events” in this CPS, the Certification Authority stores the following records:

[Events Recorded in the Certification Authority System]

- Generation of the Certification Authority signature key pair
- Additions and deletions of certificate subjects from the system
- Changes in keys, including certificate issues and revocations
- Additions, changes and deletions of Registration Authority administrator authority

[Events Recorded as Paper Media and External Recording Media]

The Certification Authority maintains and administers an archive relating to the following operations-related records.

- Records relating to this CPS and the certificate subject agreement, and changes made to them.
- Records relating to the responsibilities and authority of persons conducting the certification practices, and changes made to them.
- In the case where part of the certification practices are commissioned to another entity, the original documentation relating to the commissioning agreement.
- Records relating to the audit implementation result, and the audit report.

5.5.2. Archive Storage Period

The Certification Authority will store the Certification Authority system database records and the audit log file records for a fixed period. The storage period for paper media and external recording media are defined in “5.5.1. Archive Record Types” in this CPS.

5.5.3. Archive Protection

Access control is implemented for the archived data, together with measures that allow detection of alterations. The Certification Authority regularly backs up the archived data to external recording media, restricting access only to persons who have received clearance from JPNIC Administration Division, and storing the media in facilities that are protected from environmental dangers such as temperature and humidity.

5.5.4. Archive Backup Procedures

The Certification Authority implements automatic and regular backups of the Certification Authority system database on the server. Further, the audit log is also regularly stored on external recording media.

5.5.5. Requirements for Attaching Time-stamps to Records

The Certification Authority attaches time-stamps to each record of important information recorded in the Certification Authority. The time-stamps indicated here do not utilize cryptographic technology.

5.5.6. Archive Collection System

A Certification Authority server database record collection system is incorporated in the Certification Authority server system. The audit log file record collection system is defined in “5.4.6. Audit Log Collection System” in this CPS.

5.5.7. Procedures for Obtaining and Verifying Archived Information

For the archived data, a person permitted to access the strictly administered storage section will obtain the data and regularly confirm the readability of the external recording media. Further, when necessary, the data will be copied onto new media and the old media that has exceeded its storage period will be destroyed in consideration of maintaining the completeness and confidentiality of the archived data.

5.6. Key Switching

Before the remaining validity period of the Certification Authority private key becomes less than the maximum validity period of the EE certificates, JPNIC will prevent the issue of new EE certificates using the key. JPNIC will then generate a new Certification Authority key pair using the method specified in “6.1. Key Pair Generation and Installation” in this CPS. The new public key will receive issue of a certificate from JPNIC Primary Root Certification Authority, and will be distributed in the same way as the method specified in “6.1.4. Delivery of Certification Authority Public Key to Relying Parties” in this CPS.

5.7. Recovery from Key Compromise and Disasters

5.7.1. Handling Procedures for Incidents and Key Compromise

In situations where the Certification Authority private key has been compromised or there is a danger of compromise, or when a disaster has occurred that has led to the interruption or suspension of certification practices, the Certification Authority will strive to restart the certification practices following plans and procedures defined beforehand.

5.7.2. Case where Computer Resources, Software and/or Data has been Corrupted

In a situation where hardware, software or data has been corrupted, JPNIC Certification Authority will strive to quickly implement recovery work using backup hardware, software and data following recovery plans determined beforehand.

5.7.3. Procedures when Entity Private Key has been Compromised

In a situation where the Certification Authority private key has been compromised, plans defined beforehand will be followed to halt the certification practices and then carry out the following procedures:

- Revocation procedures for contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates
- Procedures to destroy the Certification Authority private key and generate new keys
- Procedures to re-issue the contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates

Further, in the situation where a certificate subject's private key has been compromised, certificate revocation procedures will be carried out based on procedures determined beforehand in "4.9. Certificate Revocation and Temporary Suspension" in this CPS.

5.7.4. Business Continuation Capability after Disaster Occurrence

In the situation where JPNIC Certification Authority facilities receive damage due to a disaster or incident, JPNIC will strive to re-start operations by securing reserve equipment and using backup data.

5.8. Termination of Certification Authority or Registration Authority Practices

In the case where JPNIC has decided to terminate its Certification Authority certification practices, the specified practices termination procedures will be implemented, in which notification will be given to certificate subjects and relying parties 14 days before the termination of practices, explaining that the certification practices of JPNIC Certification Authority will be terminated. The explanation will also describe the storage organization and disclosure method for the Certification Authority backup data and archive data after the termination of business

6. Technical Security Management

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Generation of Certification Authority key pairs should be carried out by several CAOs in the presence of the key administrator inside the certification facilities room. The generation of Certification Authority key pairs is carried out using FIPS140-1 Level 3 cryptographic modules.

Generation of key pairs for contract/resource administrator certificates and JPNIC staff certificates should be carried out using FIPS140-2 Level 3 cryptographic modules.

6.1.2. Delivery of Private Keys to Subjects

Generation of key pairs for contract/resource administrator certificates and JPNIC staff certificates is conducted by the Certification Authority inside the cryptographic module. The generated key pair will be delivered to applicants using a hardware token that includes a cryptographic module.

Because the Certification Authority does not carry out generation of key pairs for resource subscriber certificates, this item is not regulated.

6.1.3. Delivery of Public Keys to Certificate Issuers

The delivery of resource subscriber certificate public keys to the Certification Authority should be carried out by using encrypted communications to send the PKCS#10 format file to the Certification Authority.

6.1.4. Delivery of Certification Authority Public Keys to Relying Parties

Distribution of certificates by the Certification Authority is carried out using the most appropriate of the following two methods according to the EE.

- The Certification Authority certificates are disclosed on JPNIC Certification Authority Webpage. In the disclosure of the Certification Authority certificates, a secure protocol with an encryption function is used, and alteration prevention measures are applied. Certificate relying parties download the Certification Authority certificates from the same page for use. The relying parties compare the fingerprint of the downloaded Certification Authority certificates with the fingerprint that has been disclosed using a non-Internet method and confirm that they match.

- For resource subscribers, Certification Authority certificates will be handed over by the contract/resource administrator.

6.1.5. Key Size

The Certification Authority uses 2048-bit RSA key pairs. EEs are obliged to use RSA key pairs with 1024 bits or more.

6.1.6. Public Key Parameter Generation and Quality Inspection

The public key parameters for generating the Certification Authority key pairs use Random Number Generation (known henceforth as RNG) incorporated in software that includes highly secure cryptographic modules for use in the key pair generation.

For the quality inspection of the public key parameters, there is no particular specification.

6.1.7. Key Application Purpose

The Certification Authority certificate keyUsage uses the keyCertSign and cRLSign bits. The Certification Authority private key is only used for issuing EE certificates and the CRL.

The contract/resource administrator certificate, resource subscriber certificate, and JPNIC staff certificate keyUsage uses the digitalSignature, keyEncipherment, and dataencipherment bits. They are only used for S/MIME and SSL/TLS client certificates.

6.2. Private Key Protection and Cryptographic Module Technical Administration

6.2.1. Cryptographic Module Standards and Administration

Not stipulated.

6.2.2. Multi-person Control of Private Key

The Certification Authority private key administration is carried out by investing authority in a number of CAOs. It will not be possible to operate the Certification Authority private key unless there are two or more CAOs present.

6.2.3. Private Key Escrow

Specified in “4.12. Key Escrow and Key Recovery” in this CPS.

6.2.4. Private Key Backup

The Certification Authority private key will be backed-up on external recording media determined beforehand. During production of the backup, it will also be necessary for the key administrator and several CAOs to be in attendance.

The Certification Authority will store the backup in a storage location determined beforehand.

Note that the Certification Authority will not carry out backing-up of EE private keys.

6.2.5. Private Key Archiving

Archiving of the Certification Authority private key will not be conducted.

Similarly, archiving of EE private keys will not be carried out.

6.2.6. Transferring Into or From the Private Key Cryptographic Module

The Certification Authority private key is generated using software that includes a highly secure cryptographic module, with no intervention from other hardware or software.

6.2.7. Storage of Private Key in the Cryptographic Module

The Certification Authority private key is generated and stored in a highly secure cryptographic module.

For the resource subscriber private key, the resource subscriber will carry out generation and storage of the private key themselves. The confidential keys of contract/resource administrators and JPNIC staffs will be generated and stored inside highly secure cryptographic modules by JPNIC. However, for the server, the server's certificate administrator will carry out the storage.

6.2.8. Private Key Activation Method

Activation of the Certification Authority private key is carried out inside the certification facilities room.

The EE private key activation is not stipulated.

6.2.9. Private Key Deactivation Method

Deactivation of the Certification Authority private key is carried out inside the certification facilities room, with the work divided between the person conducting the operation and a person supervising.

The EE private key deactivation is not stipulated.

6.2.10. Private Key Destruction Method

In the situation where the Certification Authority private key must be destroyed, the key administrator will completely initialize or physically destroy the hard disk on which the private key was stored. At the same time, the backup private key will also be destroyed using the same procedures.

EE private keys should be completely destroyed by the EE itself. The confidential key of the contract/resource administrator will basically be destroyed by JPNIC. However, in situations such as when it has been lost, this may not be carried out.

6.2.11. Cryptographic Module Assessment

Not stipulated

6.3. Other Key Pair Administration

6.3.1. Public Key Archiving

The Certification Authority will back-up the Certification Authority certificates and all the certificates issued by the Certification Authority.

6.3.2. Period of Certificate Operation and Key Pair Usage Period

The period of validity of Certification Authority certificates is 10 years and the validity period of the private key is 8 years. The Certification Authority will update the key pair before the private key validity period ends.

The period of validity of EE certificates is 2 years. Use will be permitted for more than 2 years only in situations where private key decoding is carried out.

6.4. Activated Data

6.4.1. Activated Data Generation and Configuration

Including the Certification Authority private key, the PINs and passwords used in the Certification Authority have lengths of 8 or more capital or small alphanumeric characters.

6.4.2. Activated Data Protection

Regarding the PINs and passwords used in the Certification Authority, after sealing, they are stored under the administration of the operations administrator.

6.4.3. Other Considerations for Activated Data

Not stipulated.

6.5. Computer Security Management

6.5.1. Technical Requirements relating to the Security of Particular Computers

Practices relating to the Certification Authority server system will in principle be conducted by several CAOs. However, work that is necessary to be carried out such as during hardware failures by persons with specialized knowledge will be conducted by maintenance persons in the presence of the CAO. Important operations concerning the system are all configured to be stored in the log. All passwords used for accessing the system will have appropriate administration conducted. Regarding the Certification Authority server system, constant resource monitoring will be carried out, and appropriate measures will be implemented swiftly in the situation where a system abnormality or improper operation is detected.

6.5.2. Computer Security Assessment

All of the software and hardware used by the Certification Authority will have operation testing conducted before use to confirm the reliability.

6.6. Technical Administration of Life Cycle

6.6.1. System Development Administration

In order to maintain the system quality and security, administration of each process during development and assessment before introduction will be implemented.

6.6.2. Security Operations Administration

For the system security management, usage administration including room entry-exit administration, key employee administration including education, and authority administration will be carried out. Security measures such as improper entry measures and virus countermeasures, and the timely updating of security countermeasures software will be implemented.

6.6.3. Life Cycle Security Management

Using the specified administration method, assessment will be carried out regarding whether the system is being managed.

Regarding the Certification Authority system, information collection will be conducted relating to security, and appropriate assessment and improvements will be implemented while referring to the latest trends.

6.7. Network Security Management

A firewall is used for the network in the Certification Authority, and access from outside the firewall is restricted using the necessary minimum protocol. Further, the hosts that can be accessed are also limited.

6.8. Time-stamps

Requirements relating to the use of time-stamps are stipulated in “5.5.5. Requirements for Attaching Time-stamps to Records” in this CPS.

7. Profiles of Certificates, Certificate Revocation Lists, and OCSP Profiles

7.1. Certificate Profile

Certificates issued by the Certification Authority conform to X.509 certificate format v3. The certificate profile is as shown in Table 7-1.

7.1.1. Version No.

All certificates issued by the Certification Authority conform to X.509 v3 certificate format.

7.1.2. Certificate Extensions

The extension fields used in certificates issued by the Certification Authority are shown below:

7.1.2.1. authorityKeyIdentifier

The Certification Authority public key 160-bit SHA-1 hash value is used as the keyIdentifier value. This extension is non-critical.

7.1.2.2. subjectKeyIdentifier

The public key 160-bit SHA-1 hash value of the certificate subject concerned is used. This extension is non-critical.

7.1.2.3. keyUsage

Contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates use digitalSignature, keyEncipherment, and dataEncipherment. The server's certificates use digitalSignature and keyEncipherment only. This extension is non-critical.

7.1.2.4. certificatePolicies

Contract/resource administrator certificates, resource subscriber certificates, and JPNIC staff certificates use the certificatePolicies extension. The policyIdentifier value is shown in "7.1.6. Certificate Policy OID" in this CPS, and the policyQualifiers value is shown in "7.1.8. Policy Qualifier Description and Meaning" in this CPS. This extension is non-critical.

7.1.2.5. subjectAltName

The E-mail address of the certificate subject is written as the rfc822Name. This extension is non-critical.

7.1.2.6. cRLDistributionPoints

The URI of the CRLs issued by the Certification Authority is written. This extension is non-critical.

7.1.3. Algorithm OID

The algorithm OIDs used in certificates issued by the Certification Authority are the two shown below:

- sha1withRSAEncryption (1.2.840.113549.1.1.5)
- rsaEncryption (1.2.840.113549.1.1.1)

7.1.4. Name Format

Conforms to “3.1.1. Types of Names” in this CPS.

7.1.5. Naming Constraints

The nameConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.6. Certificate Policy OID

Resource subscriber certificates, contract/resource administrator certificates, and JPNIC staff certificates each use the EE certificate policy OID defined in “1.2. Documentation Name and Identification” in this CPS.

7.1.7. Policy Constraints Extensions

The policyConstraints extension is not used in any of the certificates issued by the Certification Authority.

7.1.8. Policy Qualifier Description and Meaning

The URI disclosed in this CPS is used both in resource subscriber certificates and server’s certificates as the policy qualifier value.

7.1.9. Processing of certificatePolicies Extensions for Critical Certificates

The certificatePolicies extensions included in certificates issued by the Certification Authority are all non-critical, and regulations are not carried out for this item.

Table 7.1 Profile of Certificates issued by JPNIC Resource Service Certification Authority

Field	Critical Flag	Contract/resource Administrator Certificate, Resource Subscriber Certificate, JPNIC staff Certificate
version	NA	2
serialNumber	NA	Non-negative integer
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString ¹
validity	NA	
notBefore		UTCTime
notAfter		UTCTime 2 years after notBefore time
subject	NA	
		PrintableString ²
subjectPublicKeyInfo	NA	
algorithm		rsaEncryption
parameters		null
subjectPublicKey		Public key BIT STRING
authorityKeyIdentifier	n	
keyIdentifier		160-bit SHA-1 hash value of JPNIC IP Address Certification Authority public key
authorityCertIssuer		Not used
authorityCertSerialNumber		Not used
subjectKeyIdentifier	n	160-bit SHA-1 hash value of public key
keyUsage	n	
digitalSignature		1
nonRepudiation		0
keyEncipherment		1
dataEncipherment		1
certificatePolicies	n	
policyIdentifier		OID of this CP
policyQualifiers		
policyQualifierId		CPSUri
qualifier		URI disclosed by this CP/CPS
subjectAltName	n	
rfc822Name		E-mail address
cRLDistributionPoints	n	
DistributionPoint		
distributionPoint		URL where CRL is disclosed by the Certification Authority
reasons		Not used
cRLIssuer		Not used

- 1 C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority
- 2 C=JP, O=(Organization Name), O=Resource Holder, O=LIR Corporate Administrator, OU=(One out of LIR Corporate Administrator, LIR Administrator, or LIR Hostmaster), OU=(Maintainer code allocated by JPNIC in resource administration units) CN=(One out of LIR-CO, LIR-AD, LIR-HM, ASN-HLD, JPNIC-AD, or JPNIC-CO) + (Certification ID allocated by JPNIC to each user) + (Alphabetical notation giving the name of the certificate issue subject)

7.2. Profile of Certificate Revocation List

CRLs issued by the Certification Authority comply with X.509 CRL format v2. The CRL profile is as shown in Table 7-2.

7.2.1. Version No.

All CRLs issued by the Certification Authority comply with X.509 v2 CRL format.

7.2.2. CRL and CRL Entry Extensions

The Certification Authority uses the following two CRL extensions, and CRL entry extensions are not used.

7.2.2.1. cRLNumber

CRLs issued by the Certification Authority use a non-negative integer that will become unique.

7.2.2.2. authorityKeyIdentifier

The Certification Authority public key 160-bit SHA-1 hash value is used as the keyIdentifier value. This extension is non-critical.

Table 7.2 Profile of CRLs Issued by JPNIC Resource Service Certification Authority

Field	Critical Flag	Certificate Revocation List
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString* ¹
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime 24 hours after thisUpdate
revokedCertificates	NA	
revokedCertificate		
userCertificate		Serial number of revoked certificate
revocationDate		UTCTime Time that certificate was revoked
crlEntryExtensions		
		Not used
crlExtensions	NA	
cRLNumber	n	Non-negative integer
authorityKeyIdentifier	n	160-bit SHA-1 hash value of Certification Authority public key

1 C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority

7.3. OCSP Profile

7.3.1. Version Information

Not stipulated

7.3.2. OCSP Extensions

Not stipulated

8. Compliance Audit and Other Assessments

8.1. Assessment Frequency and Circumstances requiring Assessment

The Certification Authority will implement audits whenever required.

8.2. Identity and Qualifications of Assessor

JPNIC will have the Certification Authority compliance audit implemented by an assessor who is knowledgeable of the certification practices selected by the trustee in charge.

8.3. Relationship between the Assessor and the Entity Assessed

JPNIC will select the assessor from among personnel excluding key persons relating to the Certification Authority certification practices.

8.4. Items covered by the Assessment

The Certification Authority compliance audit will assess whether the management of the Certification Authority strictly complies with this CPS and other related stipulations.

Further, in situations where the trustee in charge determines it necessary, audits will be implemented according to audit purposes specified by the trustee in charge.

Note that JPNIC has the authority to conduct audits of local RAs.

8.5. Measures taken in Event of Unsatisfactory Results

For items indicated in the audit report, the Certification Authority trustee in charge will decide the measures. For the specified items, the trustee in charge will give direction including measures for solving the problems to JPNIC Certification Authority manager responsible, based on the latest trends in security technology. The response measures implemented will be reported to the trustee in charge, and will be assessed and confirmed in the next audit. In the situation where a response is not made to the unsatisfactory items discovered by the assessment, penalties determined beforehand by the trustee in charge will be applied.

8.6. Assessment Result Information Exchange

Reporting of the assessment result will be carried out by the assessor to the trustee in charge. Except in situations where the Certification Authority is legally required to make a disclosure, the assessment results will not be disclosed outside the organization.

Note that JPNIC Certification Authority manager in charge has a responsibility to store and administer the audit reports for a period of at least 5 years.

9. Problems relating to Other Practices and Legal Problems

9.1. Fees

The issuing fees, updating fees, and usage fees relating to the certificates issued by the Certification Authority will be determined separately and notified beforehand to individuals and entities concerned.

9.2. Financial Liability

Not stipulated

9.3. Information Confidentiality

9.3.1. Scope of Confidential Information

Information retained by the Certification Authority will be treated as confidential information, with the exception of the information determined for disclosure in “2.2. Certification Information Disclosure” in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, reasons for certificate revocation and other detailed information relating to certificate revocation.

The private keys of certificate subjects are information that should be treated as confidential information by the certificate subject.

9.3.2. Information Outside the Scope of Confidential Information

Information determined for disclosure in this CPS, information explicitly disclosed as part of the CPS, information disclosed on the Website, and CRLs including information about the Certification Authority as the certificate issuer and the revocation date are not treated as confidential information. In addition, information satisfying the following conditions will not be treated as confidential information.

- Information that has become known through no negligence on the part of JPNIC.
- Information that has been provided to JPNIC from another source with no confidential restrictions attached.
- Information that has been independently developed by JPNIC.
- Information that has been confirmed by persons or organizations related to the subject of the released information.

9.3.3. Liability for Protecting Confidential Information

Concerning the information handled by the Certification Authority, in the situation where a request is received for information disclosure based on the legal authority of an investigative agency or court, JPNIC can disclose the information to the legal enforcing institution according to law. Further, regarding the information handled by the Certification Authority, in the case where an optional disclosure request is received from a court, lawyer, or other person with legal authority concerning arbitration, litigation, mediation, and other legal, judicial, or administrative processes, JPNIC can disclose the relevant information relating to the request. Additionally, concerning information received from contract/resource administrators relating to the certificate subject administered by the contract/resource administrator, in the situation where a request is received that violates or has a danger of violating the subject's rights or interests, the Certification Authority will confirm the relationship between the contract/resource administrator and the disclosure request subject information. The Certification Authority can then disclose the information received from the contract/resource administrator concerning the certificate subject and the information described in the certificate.

In the situation where a part of the practices are commissioned, JPNIC Certification Authority may disclose confidential information to the commissioned entity. However, the commissioning agreement incorporates an obligation to maintain the confidentiality of the information.

With the exceptions of the situations mentioned previously, JPNIC Certification Authority will not disclose confidential information. In the case where confidential information is leaked, the liability will be borne by the person leaking the information.

Note that handling concerning the protection of personal data is specified in "9.4. Protection of Personal Data Privacy" in this CPS.

9.4. Protection of Personal Data Privacy

9.4.1. Privacy Policy

The Certification Authority recognizes the importance of personal data protection. In addition to handling personal data in the same way as “9.3.3. Liability for Protecting Confidential Information” in this CPS, the following policy is strictly observed.

- (1) An administrator responsible will be appointed to carry out appropriate administration of personal data.
- (2) In the situation where personal data is collected, the purpose for collecting the data will be notified, and collection will be conducted only of information that falls within the necessary scope of purpose using legal and fair means.
- (3) Personal data received through submission by certificate subjects will only be used for the following purposes:
 - To allow smooth operation of IP address administration practices
 - To allow fulfillment of responsibilities regarding certification services for certificates
 - For other purposes relating to certification practices
- (4) With the exception of situations where the agreement of the certificate subject has been received or in cases when legally obligated, personal data will not be disclosed to third parties apart from commissioned practices entities. When disclosing personal data to commissioned practices entities, the commissioned practices entities concerned will be obliged to follow the same conditions as this document.
- (5) The personal data administrator responsible for the personal data will strive to protect the personal data using appropriate security measures to prevent improper access, loss, corruption, alterations, or leaks.
- (6) In situations where requests are received for disclosure of personal data from the certificate subjects themselves, in order to prevent disclosure of personal data to third parties JPNIC will only disclose the certificate subject personal data stored in JPNIC Certification Authority to the subject themselves after confirming the identity of the subject. Further, in the situation where there is an error or changes in the certificate subject personal data, incorrect data or old information will be swiftly revised or deleted over the logical range based on the notification received from the certificate subject. In a situation where the certificate subject requests disclosure from JPNIC Certification Authority, JPNIC Certification Authority will carry out the application following the specified method.

- (7) JPNIC Certification Authority will implement education activities relating to personal data protection for employees carrying out the certification practices.
- (8) Regarding the personal data of certificate subjects, in addition to strictly observing the applicable laws and regulations, the personal data protection policy will be revised whenever necessary for improvement to maintain appropriate personal data protection.

9.4.2. Information treated as Privacy

Not stipulated

9.4.3. Information not considered as Privacy

Not stipulated

9.4.4. Liability for Protecting Personal Data

JPNIC Certification Authority will bear liability for the protection of personal data according to “9.4.1. Privacy Policy” in this CPS.

9.4.5. Notification and Agreement to Individuals relating to Use of Personal Data

Not stipulated

9.4.6. Disclosure based on Judicial Procedures and Administrative Procedures

Not stipulated

9.4.7. Other Information Disclosure Situations

Not stipulated

9.5. Intellectual Property Rights

Providing there has been no particular agreement made, intellectual property rights will be treated as follows:

- Certificates and CRLs issued by JPNIC Certification Authority are the property of JPNIC.
- This CPS is the property of JPNIC.
- JPNIC Certification Authority private key and public key is the property of JPNIC.
- Software, hardware, and other documents and information loaned from JPNIC Certification Authority are the property of JPNIC.

9.6. Representation Warranties

9.6.1. Issuing Authority Representation Warranty

JPNIC Issuing Authority will fulfill the following obligations concerning the performance of JPNIC Issuing Authority practices:

- Secure generation and administration of JPNIC Issuing Authority certificate signing keys
- Correct certificate issue and revocation administration following requests from JPNIC Registration Authority.
- JPNIC Issuing Authority system operation audit and operation
- CRL issue and disclosure
- Repository maintenance and administration
- Receipt of questions relating to this CPS during the reception opening times.

9.6.2. Registration Authority Representation Warranty

JPNIC Registration Authority will fulfill the following obligations regarding the performance of JPNIC Registration Authority practices:

- Installation and operation of a secure environment for registration terminals
- Correct information transfer to JPNIC Issuing Authority of applications for certificate issuing and revocation.
- Swift information transfer to JPNIC Issuing Authority during operation times for certificate revocation applications.

9.6.3. Local Registration Authority Representation Warranty

The Local Registration Authority will fulfill the following obligations regarding the performance of the Local Registration Authority practices:

- Verification that the certificate subject and the certificate subscriber are the same.
- Correct application information transfer to JPNIC Registration Authority.
- Resource subscriber education for certificate use.
- Precise certificate distribution to the correct certificate subscriber
- Appropriate confirmation of certificate revocation
- Strict observance of other operations conforming with the agreement with JPNIC.

9.6.4. Subject Representation Warranty

The certificate subject will fulfill the following obligations regarding the holding of the certificate:

- Understanding and agreement with this CPS and other documentation (such as certificate subject agreements) shown by the Certification Authority.
- Obligations stipulated in “4.5.1. Subject Private Key and Certificate Use” in this CPS.

9.6.5. Relying Party Representation Warranty

The certificate relying party will fulfill the obligations stipulated in “4.5.2. Relying Party Public Key and Certificate Use” in this CPS.

9.6.6. Other Related Person Representation Warranty

Not stipulated

9.7. Limitations of Warranty

JPNIC will not bear liability for any indirect damages, special damages, accompanying damages and secondary damages relating to the warranty specified in “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS.

9.8. Limitations of Liability

Concerning the contents of “9.6.1. Issuing Authority Representation Warranty” together with “9.6.2. Registration Authority Representation Warranty” in this CPS, JPNIC will not bear liability in the following situations:

- All damages occurring due to illegal actions, improper use, or negligence not caused by JPNIC.
- Damages occurring due to negligence of the Local RA or certificate subject in fulfilling their obligations.
- Damages occurring due to Local RA or certificate subject computer terminal software defects, problems, or other actions themselves.
- Damages caused by information disclosed in certificates and CRLs for reasons that can not be attributed to JPNIC.
- All damages caused by conditions where normal communications cannot be carried out for reasons that can not be attributed to JPNIC.
- Damages caused by improvement in hardware or software encryption algorithms that are not possible to be foreseen at the current time.
- All damages caused by suspension of Certification Authority practices due to acts of God, earthquakes, volcanic eruptions, fires, tidal waves, water damage, lightning, wars, riots, terrorism, and other irresistible forces.
- Damage caused by practices carried out by Local RA such as in individual authentication procedures for certificate issue applications.

9.9. Indemnity

At the point of time that the certificate issued by the Certification Authority is applied for, received, and trusted, damage liability and protection liability is created for JPNIC regarding the certificate subject and the relying party. Among the liability phenomena covered will be mistakes, negligent actions, various actions, delays in implementation, and non-fulfillment caused by the certificate subscriber not supplying the latest and correct information to the Certification Authority when applying for the certificate, resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden. In addition, certificate subject and relying party actions, negligent actions, various actions and non-fulfillment resulting in various liabilities, loss, damage, and litigation, and any kind of financial burden will also be covered.

9.10. Periods of Validity and Termination

9.10.1. Periods of Validity

Documents including this CPS, contracts, and agreements are valid from the time they are issued based on appropriate approved procedures until the time they are amended based on appropriate approved procedures.

9.10.2. Termination

In the situation where all or parts of documentation including this CPS, contracts, and other agreements become invalid, or if specified conditions make the documents invalid for particular related persons, the parts concerned will be terminated.

9.10.3. Effect of Termination and Effect Continuation

Even in the situation where changes or terminations occur in this CPS, contracts, or agreements, the Certification Authority will endeavor to continue taking responsibility for the agreed items.

9.11. Individual Notification and Contact between Related Persons

Not stipulated

9.12. Amendments

9.12.1. Amendment Procedure

In the situation where it becomes necessary to amend this CPS over an extent that will not radically influence the certificate policy, warranties and obligations, the Certification Authority may amend this CPS whenever necessary without giving prior notice to certificate subjects and relying parties. Note that in the situation where no objections are received during the period between the amendment notification and the amendment becoming valid, this will be taken to signify agreement with the amendment. Related persons who do not agree with the amendment should immediately stop using the certificates issued by the Certification Authority.

9.12.2. Notification Method and Period

The Certification Authority will give notification of the amendment to certificate subjects and related persons by disclosing the amended CPS together with the amendment history on the repository more than 10 working days before the amendment is due to become valid.

9.12.3. Situation where Object Identifier must be Changed

Not stipulated

9.13. Dispute Resolution Procedures

For disputes arising relating to certificates issued by the Certification Authority, in the situation where legal means such as litigation or arbitration are to be used to solve the dispute this fact should be notified to JPNIC beforehand. All parties concerned agree that the arbitration and court location will be within the Tokyo metropolitan wards under the exclusive jurisdiction of a dispute handling institution. Further, regarding the situation where questions arise about items not determined in this CPS or in agreements, or about the interpretation of the documentation, all parties will resolve the issues through sincere discussions.

9.14. Governing Law

Regardless of the location of the Certification Authority, certificate subject, or relying party, Japanese laws will apply regarding the interpretation of this CPS, the validity, and disputes relating to the issue of certificates by the Certification Authority.

9.15. Compliance with Applicable Laws

The Certification Authority will strictly observe the various export restrictions, and will handle cryptographic hardware and software.

9.16. Miscellaneous Regulations

9.16.1. Entire Agreement

The agreed items in this CPS, contracts and agreements will have priority over all other agreed items until amended or terminated.

9.16.2. Transfer of Rights

Not stipulated

9.16.3. Severability

In this CPS, certificate subject agreements, and agreements provided by the Certification Authority, even if one part of the provisions is invalid, the other provisions described in the document concerned will continue to remain valid.

9.16.4. Enforcement

Not stipulated

9.17. Other Provisions

Not stipulated

Appendix 2

JPNIC 認証局証明書 利用規約

第 2 版 英語訳

<Appendix2 について >

- この資料は、JPNIC 認証局証明書の利用規約を英訳したものである。
 - 諸外国の技術者による内容の理解を図るために翻訳されたものである。
正確な内容確認には原文を参照する必要がある。

JPNIC Certification Authorities Certificates - Usage Agreement

This agreement describes the items that are necessary to be agreed with users in order to utilize Certification Authorities certificates (the CA certificates), supplied by the Japan Network Information Center (JPNIC).

Please carefully read this document before obtaining CA certificates and before carrying out the configurations for use of the CA certificates. Installing a CA certificate into your software such as Web browsers or e-mail applications and using it to carry out configurations of a trusted Certification Authority shall be assumed as agreeing with the items set forth in this agreement.

The CA certificate is digital certifications of the Certification Authorities operated by JPNIC (JPNIC Certification Authorities). The JPNIC Certification Authorities include the following Certification Authorities:

- JPNIC Primary Root Certification Authority S1
- JPNIC Resource Service Certification Authority

This agreement is applicable to the certificates of all of the JPNIC Certification Authorities.

Details

1. Purpose

The JPNIC Certification Authorities have the purpose of providing a certification infrastructure to allow the sound operation and development of the Internet. Each of the JPNIC Certification Authorities are operated for the following purposes:

- JPNIC Primary Root Certification Authority S1
Has the purpose of supplying the trust anchor for verification of all digital certificates and revocation lists issued by the JPNIC Certification Authorities.
- JPNIC Resource Service Certification Authority
Has the purpose of providing digital certification procedures when carrying out use of the IP registry system operated by JPNIC and the various application operations relating to IP addresses and AS numbers, etc.

2. Prohibition of Inappropriate Access

Users should not conduct the actions described below:

- Carrying out inappropriate access to the Certification Authorities system.
- Intentionally interfering with the management and operation of the Certification Authorities system.
- Interfering with the normal operations of the JPNIC Certification Authorities, such as by distributing certification that resembles CA certificates.

Persons carrying out the above actions will be prohibited from using CA certificates.

3. Verification Result and Indemnity Items

- Verification Result
JPNIC will strive to conduct sincere operations in order to be able to maintain uniform reliability regarding the result of the verification procedures using CA certificates.
- Indemnity Items
The operation of the CA certification based on this agreement is experimental. According to JPNIC's judgment, the operation may be halted and the system may be made unavailable for use. Further, regarding the obtaining, setting, and use of CA certificates by users, JPNIC will not accept any responsibility for damage caused to users or damage incurred by other third parties.

4. Changes to the Agreement

When recognized as necessary, JPNIC may change this agreement without giving prior notice to users. Regarding the use of CA certificates after changes have been made to this agreement, the agreement after changing will be applicable.

Note that notification before or after changes are made will be conducted according to the following methods:

- Placement of notices on the JPNIC Certification Authorities Website at <http://jpnica.nic.ad.jp/>
- Dissemination of E-mail notifications to E-mail addresses that were registered when using CA certificates issued by JPNIC.

5. Confirmation of CA Certificates

When carrying out setting or use of CA certificates, the user should be certain to check whether or not there is any disagreement with the CA certificates distributed by JPNIC, based on the fingerprint information provided by JPNIC.

Note that this confirmation should be carried out at the user's own responsibility.

- For the method of obtaining CA certificates, see “■ Information Supply Method” described below.
- Concerning the fingerprint confirmation procedures, see the separate document “Methods of Obtaining and Confirming JPNIC CA Certificates”.

■ Information Supply Method

Information relating to CA certification and the JPNIC Certification Authorities operations is supplied on the following Website:

- JPNIC Certification Authorities Website:
<http://jpnica.nic.ad.jp/>

CA certification and fingerprint information is supplied using the following methods:

- CA Certificates
JPNIC Certification Authorities Website:
<http://jpnica.nic.ad.jp/>
- Fingerprint Information
See “CA Certification Fingerprint Information” in this agreement.
Note that for the convenience of users, the following Website pages are also provided:

CA certification fingerprint information:
<https://serv.nic.ad.jp/capub/fingerprint.html>

■ CA Certification Fingerprint Information

JPNIC Primary Root Certification Authority S1

SHA-1: 07:B6:67:E7:73:04:0F:71:84:DB:0A:E7:B2:90:A3:38:D4:18:60:74

MD5: DF:A6:2B:6B:CD:C6:D3:00:18:D5:67:2E:BE:76:D7:E9

JPNIC Internet Resource Service Certification Authority

SHA-1: E1:0E:7E:2F:BE:C4:90:F7:89:74:2F:42:6D:8E:21:5E:12:D5:36:8E

MD5: E6:41:A4:62:3C:1E:D4:0B:C1:9E:9B:AD:FC:44:D1:DA

The “0” are all zeroes. There is no discrimination between capital and small letters.
Depending on the software used, colons (:) may not be displayed, or spaces may be shown.