経済産業省受託調査研究

IPアドレス認証局のマネジメントに関する調査報告書

2005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

IP アドレス認証局の
マネジメントに関する
調査報告書

2005 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

日本における IT 化は 1990 年代に引き続き 2000 年以降に大きく進展してきた。その最たるものはインターネットの利用環境の向上であろう。ISP における競争は激しく、ブロードバンドと呼ばれる広帯域のネットワークが世界で最も安く提供されるに至っている。また行政サービスを始め、民間企業における電子商取引は拡充しつつある。インターネットはユーザ自身がネットワークアプリケーションやビジネスモデルを作り出し、自ら普及を図ることができるという特徴があることから、技術開発やシステム開発、情報メディア等、様々な分野への強い影響力を持つ。その為、インターネットの利用環境の改善は国民生活の向上に直接結びつくものとなる。

WWW（World Wide Web）を使ったアプリケーションを始め、音楽・動画配信、IP 電話、P2P 等の技術開発が進み、ポータルサイトや広告・小売の Web サイトのビジネスモデルが定着してきた。電子メールや WWW は今や企業活動に欠かせないツールであり、また各種電子申請システムをはじめ、インターネットに依存したネットワークサービスは数多い。すなわちインターネットは、インターネットならではのサービスの多様化によって、生活基盤（インフラストラクチャ）の性質を帯びてきたと言える。”ディペンダブル・インターネット”という言葉が示すように、様々なサービスがインターネットにディペンド（依存）している状況なのである。

しかしインターネットにおけるセキュリティの面、特にインターネットにおける認証、情報の安全性、バックボーンネットワークの安全性については 1990 年代後半から大きな変化が見られていない。個人情報の漏洩やインターネットを使った詐欺行為といった社会問題に対し、情報セキュリティ対策やスパム対策といった対応活動が一般化している。一方で問題対応型ではなく、積極的にセキュアなインフラを作る活動には何があるだろうか。本調査研究は、その「セキュアなインフラ」を運用面から実現するため、日本の NIR（National Internet Registry：国別のインターネットレジストリ）における認証局のあり方をテーマとして扱ってきた。

インターネットにおける通信ノードの識別番号である「IP アドレス」を使う為にはインターネットレジストリにおける登録が必要となる。この登録情報を用いて認証基盤を構築することで国際的なインターネットにおける「認証基盤」を構築することが可能になるというのが本調査研究の基本的なアイディアである。IP アドレスは一つの通信ノードに対して変化しうる識別子であり、またユーザとの組み合わせは保障されない。従って最終的に「登録情報」を軸にして検討を進めるに至った。登録情報が正しい認証の下に提供され、認証やネットワークの問題解決に活用できる状況を作ることが IP アドレス認証局の本質である。

2004 年度は 2003 年度に引き続いて、標準化技術の動向と RIR における認証局の動向を調査した。更に実験的な認証業務を想定した IP アドレス認証局の構築を行ない、認証業務規定の更新を行った。

目次

第 1 章　IP アドレス認証局に関する調査研究について

内容

- 三年度の調査研究
- 今年度の調査研究の位置づけ
- 調査研究の活動と各章の関連

第1章 IP アドレス認証局に関する調査研究について

本調査研究は、2002 年度から 2004 年度までの三年の計画で行ってきた調査研究である。初年度の 2002 年度は「IP アドレス認証局のあり方に関する調査研究」を行ない、2003 年度は「IP アドレス認証局のマネジメントに関する調査研究」を行った。2004 年度は 2003 年度と同じ題目「IP アドレス認証局のマネジメントに関する調査研究」を行った。

本章では三年間の調査研究と 2004 年度の調査研究について述べる。

1.1. 三年で行われた調査研究

本調査研究は、次のような進め方で行われた。はじめに、インターネットレジストリの業務形態やアドレス資源管理について調査し、「IP アドレス認証局のあり方」を調査研究する。次に IP アドレス認証局の業務内容の検討を進め、CP/CPS（運用業務規程）の策定とともに技術的要件の調査を行う。最後に認証業務の概要を明らかにした後、システムの開発および運用体制の構築を行い、最後に認証業務の運用に繋げる。

2002 年度は IP アドレス認証局のあり方の検討と調査であった。アドレス資源の管理構造に関して調査を行い、RIR の登録情報の確実性に関する調査を行った。更に認証局の監査基準の調査を通じて、安全性のレベルを決める運用の要素について調査を行った。RIR（Regional Internet Registry）の調査もこの時に開始した。

2003 年度は認証局のマネジメントについて検討を行った。「アドレス資源の確実性に基づく認証基盤の構築には、その基礎となる確実な登録管理業務が必要である」という観点から、アドレス資源管理の安全性の調査、RIR の認証局の動向調査、技術動向調査、認証局のシステムの検討といった活動を行った。また IP アドレス認証局の初期版の認証局業務規程 CPS（Certification Practice Statement）のドラフト作成、認証情報の応用構想に関する検討などを行った。

2004 年度は認証局のシステムの構築を行った。また、RIR の認証局の動向調査、技術動向調査、認証局のシステムの検討を継続して行ない、CPS の更新を行った。IP アドレス認証局の応用については、より具体的な利用方法を検討した。

三年間の調査研究活動と 2004 年度の報告書との関係を図 1-1 に示す。

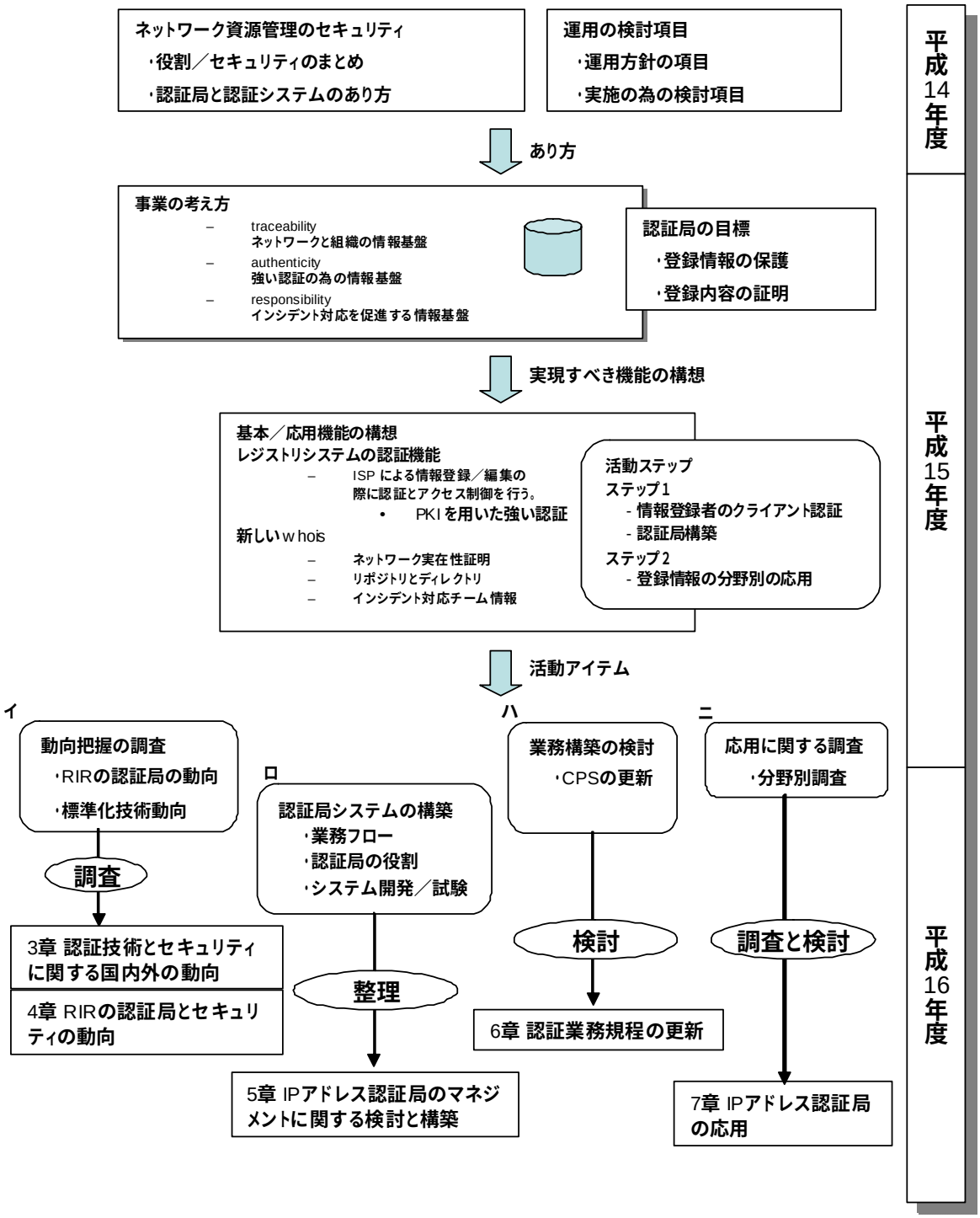


図 1-1　三年間の活動内容

1.2. 調査研究の活動と本報告書について

本調査研究では、2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」に引き続き、RIR の認証局の動向、標準化技術の動向、応用方法など、いくつかに分類される活動を行った。本節では、それぞれの活動が本報告書のどの章に関連するかについて述べる。

- **認証技術とセキュリティに関する国内外の動向**
  2003 年度に引き続き、認証技術に関する国際的な標準化活動の動向調査を行った。動向調査は IETF（Internet Engineering Task Force）の PKIX WG を中心に行われた。この内容を第 3 章にまとめる。

- **RIR の認証局とセキュリティの動向調査**
  RIR では既に認証局が構築され、運用が開始されている。これらの認証局の運用状況と登録情報のセキュリティについて調査した。調査は APNIC、RIPE NCC、ARIN でのヒアリングと定期ミーティングへの参加を通じて行われた。この調査の内容と結果を第 4 章にまとめる。

- **IP アドレス認証局のマネジメントに関する検討と構築**
  2003 年度に作成した業務概念図を基に、更に内容を具体化し、業務フローや認証局システムの構成を検討した。また実験的な認証業務を実現する為の認証局システムの構築を行った。検討内容ついて第 5 章で述べる。

- **認証業務規程 CPS の更新**
  2002 年度に調査の結果明らかにした認証業務の検討方法に基づき、認証業務規程の更新を行った。IP アドレス認証局の認証業務規程は 2003 年度に一度ドラフト作成されたが、2004 年度の認証業務の具体化によっていくつかの考え方の変更が行われた為、認証業務規程に反映する必要が生じた。2004 年度は、2002 年度、2003 年度の調査資料を元に、認証局業務規程の更新を行った。この更新の内容について第 6 章にまとめる。

- **IP アドレス認証局の応用**

  インターネットレジストリにおける登録情報の確実性の向上と認証基盤の構築が進むと、登録情報を応用した新たなネットワークサービスが考えられる。2003 年度の調査研究では、情報家電などのネットワーク機器やソフトウェアのベンダー業界においてヒアリングを行った。その上で検討会を開き、様々なネットワークの安全性が向上された状況での、ネットワークアプリケーションの構想を挙げ、整理した。

  2004 年度は、これらのネットワークアプリケーションを実現する為に必要となる、インターネットのバックボーンとレジストリにおけるセキュリティに関わる具体的なプロトコルや事例について調査を行った。この調査結果については第 7 章で述べる。

第 2 章　各章の概要

内容

- 第 1 章から第 7 章までの概要

第2章 各章の概要

本章では、今年度の調査研究の内容を簡単に把握できるよう、各章のポイントをピックアップする。詳細に関しては適宜各章の該当部分を参照されたい。

第 1 章　IP アドレス認証局に関する調査研究について

今年度の調査研究の位置づけや、活動内容と各章との関連について述べた。

第 2 章　各章の概要

各章の概要を 1 パラグラフ程度にまとめたものである。

第 3 章　認証技術とセキュリティに関する国内外の動向

電子認証の技術的な最新動向を調査するため、IETF の PKIX WG を中心に情報収集を行った。PKIX WG では IP アドレスと AS 番号の情報を X.509 形式の証明書（以下、証明書とよぶ）に含める RFC3779 の標準化がされ、また CRISP（Cross Registry Service Protocol）WG では AREG の RFC 化の最終段階に入った。RPSEC WG では S-BGP（Secure BGP）の議論が行われており、RIR が発行する RFC3779 形式の証明書の利用が想定されている。IETF では認証技術の実践的な議論や技術の標準化の必要性が指摘されており、EasyCert を始めとする新たな WG や BoF が始まっている。

ネットワークオペレータの会議である NANOG では、ルーティング技術を利用したバックボーンのセキュリティ技術に関する議題が多かった。国内では JANOG でもルーティングのセキュリティに関する議論が始まっており、JPNIC の IRR 企画策定専門家チームでは IRR の経路情報を使ったインターネットのセキュリティが活動の柱の一つとして位置づけられている。JNSA（日本ネットワークセキュリティ協会）ではセキュリティの複雑な機能をミドルウェアで吸収しその認証のセキュリティインフラ運用を各種認証局が行っていくというモデルについて議論が行われていた。

第 4 章　RIR の認証局とセキュリティの動向

RIR のうち、APNIC や RIPE NCC、ARIN ではすでに認証局を構築している。これらの認証局はすべて電子証明書使ったユーザ認証の為に利用されている。APNIC CA は HSM（Hardware Security Module）の導入を行ない、また証明書を利用する Web アプリケーションの MyAPNIC の機能拡張が徐々に進んでいる状況である。証明書の発行数は二年間で 1000 を超え順調にユーザを増やしている。RIPE NCC は Webupdates といった Web での認証だけでなく、S/MIME を使った申請にも証明書が使えるようになった。RIPE NCC に発行された証明書は自動的に Database に登録さ

れるようになって利便性が上がり、証明書の発行数は 700 を超えた。RIPE NCC では別途登録された証明書を認証に用いることが可能だがその数は除いている。ARIN は S/MIME を使った申請者の認証にのみ証明書を利用している。

APNIC を中心に RFC3779 形式の証明書を RIR で運用する際の課題抽出や方向性の確認が行われはじめている。この証明書は割り振りと割り当ての証明に使われ、現在 S-BGP で利用することが想定されている。

第 5 章　IP アドレス認証局のマネジメントに関する検討と構築

IP アドレス認証局の実験的な業務を想定した業務フローと認証局システムの設計を行った。業務のモデルは 2003 年度の調査研究の一環として行った専門家チームによる検討結果を活用した。認証業務は、既存のインターネットレジストリにおける登録者の扱いを踏襲し、またアクセスコントロールも既存のルールに近くなるようにした。

第 6 章　認証業務規程 CPS 策定の更新

2003 年度のドラフト版を元に、第 5 章で設定を行った認証局システムの運用に合った記述を行った。認証局システムは安全上の要点を押さえつつ費用を押さえたものになった。一方 CPS の記述については全章にわたって改編が行われ、より実際の運用に即した規程となった。

第 7 章　IP アドレス認証局の応用

NIR における認証局の応用として、具体的なプロトコルと事例についてまとめた。一つ目は経路情報の安全性で、インターネットバックボーンの保護に利用される構想である。二つ目は登録情報の効率的かつ安全なやり取りを実現する Web トランザクションである。登録申請業務の自動化だけではなく IP アドレス認証局が上位認証局となるような状況では、登録情報をオンラインで迅速にやり取りできる必要がある。三点目はオーストリアにおける ENUM（tElephone Number Mapping）の登録における認証の事例である。レジストリの情報登録に使われる証明書と認証のスキームが直接利用される。

Appendix.1

認証業務と方針の検討の結果、更新を行った CPS ドラフト版を添付する。

Appendix.2

前年度の CPS との差異を表にまとめた。

第3章 認証技術とセキュリティに関する国内外の動向

内容

- 技術の標準化動向と国内外での議論
  - IETF
    1. S-BGP の展開に関する議論
    2. 認証技術の実践的な議論
    3. 各回の報告
  - NANOG での話題
  - 国内での議論

第3章 認証技術とセキュリティに関する国内外の動向

3.1. はじめに

認証技術は様々な要素が組み合わった複合的な技術である。認証技術の導入にあたって検討されるべきことは色々と考えられるが、まず技術そのものと技術の運用という二つの大きな側面に分けられるであろう。技術の側面は様々な研究の情勢や国際会議での標準化動向、システム導入の技術検討といった活動がある。運用の側面は技術を利用する組織での運用や業界での運用、ミクロな視点では利用環境が挙げられる。それぞれの組織や業界に合った使い方をしなければ、認証技術はセキュリティの向上を図るどころか、意味のないものになってしまうだろう。

認証局はこの認証技術の二つの側面を考慮する必要がある。インターネットで使われているプロトコルで使われるような形式で証明書を発行できなければ、その証明書の普及はなく認証局の存在意味がなくなってしまう。更に目的とする電子認証に対して、妥当な組織によって認証局が運営されていなければ、ユーザの信頼を得ることが難しく電子認証のレベルの向上を図ることはできない。

本調査研究は NIR における認証局のマネジメントに関する調査研究である。従って NIR における技術と運用の両面に重点を置いた動向調査が必要である。JPNIC における電子認証の技術の要素は、プロトコルの標準化動向であり、運用の要素は他の認証局、特にインターネットレジストリの認証局の動向である。

3.2. 本章の内容

本章では、プロトコルの標準化動向として IETF [1]における認証技術の動向を、インターネットレジストリの認証局に関しては RIR における認証局の動向を中心に報告する。インターネットレジストリのセキュリティが大きく影響を持つグローバル・インターネットのネットワークセキュリティに関して、北米のネットワークオペレータの会議である NANOG から最新の話題について報告する。この他に日本国内における認証技術とネットワークセキュリティに関わる動向を報告する。インターネットレジストリの認証局に関しては、第 4 章でまとめている。

[1] Internet Engineering Task Force
http://www.ietf.org/

なお、ネットワークセキュリティにおける「運用」という言葉は、ネットワークオペレーション（ネットワーク機器等の運用）を指すことがある。本調査研究では基本的に認証技術の運用（認証局や認証サービスの運用）を指すこととする。

3.3. 認証技術(PKI)とネットワークセキュリティに関わる国内外の動向

認証技術で使われている要素技術の多くは、国際的な学術会議（カンファレンス）とオペレータの知見を通じて発展してきた。またインターネットにおける通信の基本となるプロトコルである IP を始め、アプリケーションのプロトコルに至る多くの技術は、国際的な標準化活動の成果でもある。

RFC の公開を行っている IETF は標準化活動のよい例であろう。PKI に関わる RFC である RFC3280、RFC3647、IPsec に関わる RFC2401、SSL/TLS の RFC2246 など、インターネットで使われている電子認証のプロトコルは必ずといっていいほど IETF の標準化プロセスを経ているのが現状である。

電子認証の技術的な最新動向を調査するには IETF のような国際会議の動向を調査するのが早道である。認証技術をはじめ、情報科学の技術は企業の研究所や大学で研究されることが多い。しかし実装されインターネットで本格的に利用されるようになるのは、標準化され文書化されたあとになる。従ってプロトコルの標準化を行うような国際会議は、インターネットで使われている、もしくは将来使われるようになる技術の最新動向を知るのに適している。IETF では、運用に関する知見の集約も早い段階で行われる。インターネットにおけるアドレス資源の管理がその代表的な活動であろう。

3.4. 国際会議について

本調査研究では国内外で開催される国際会議に参加し、直接的な情報交換を図った。

この調査について、ここでは三つの構成に分けて報告する。

一つ目は国際的なプロトコルの標準化と、グローバル・インターネットのオペレーション（技術的な管理運用）である。ここでは IETF と NANOG について述べ、インターネットの技術面と、ネットワーク運用面の動向について報告する。

二つ目は国内の認証技術の動向である。ここでは JNSA の PKI 相互運用技術 WG と WIDE Project にについて述べ、日本の認証技術の普及と技術的な課題について述べる。

三つ目は国内のネットワーク・オペレータの動向である。

ここでは JANOG と JPNIC の IRR 企画策定専門家チームについて述べ、日本のネットワークオペレータが議論を行っているネットワークの最新動向と、グローバル・インターネットにおける経路制御の安全性についての最新動向について述べる。

3.5. プロトコルの標準化とインターネット・セキュリティに関わる国際動向

IETF はインターネットで使われる各種プロトコルの標準化を行っているグループである。ISOC から資金援助を受けて活動しており、RFC と呼ばれる技術文書を公開している。議論の技術的なレベルが高く、文書化されたプロトコルの適用性が高い。従って参加費用はやや高額（約 55000 円）であるが、毎回 1300 名以上の参加者を確保している。参加者のうちの 50%以上がアメリカの企業や大学からの参加であるが、残りの 50%近くは日本、ドイツ、フランス、イギリス、韓国、といった様々な国の企業や大学からの参加者である。政府組織の技術者の参加も多い。

NANOG は北米地域のネットワークオペレータ（技術的な管理運用を行う担当者）を対象にした会議である。主に参加者同士の運用に関わる技術的な情報交換を目的としており、会議は発表形式である。参加者のほとんどがアメリカからで、2004 年 11 月に行われた第 32 回の参加者は 600 名程であった。日本からの参加者は 20 名程であった。

3.5.1. IETF における RIR の技術者との情報交換

IETF はプロトコルの標準化活動を行う会議である性質上、インターネットに関連するベンダ、政府組織等から技術者が一堂に集まる機会である。この機会を利用して、RIR における認証局の状況に関する情報交換を行ったり、JPNIC 認証局の応用技術に関する情報交換を行ったりした。IETF の動向の報告に先立ち、この個別の情報交換について述べる。

3.5.2. S-BGP の展開に関する情報交換

第 60 回および第 61 回 IETF における情報交換において特筆すべきことは、S-BGP に関することであろう。第 60 回 IETF において PKIX WG のドキュメントとして RFC3779 が I-D から RFC になっただけでなく、S-BGP の提案者や APNIC の職員と技術と運用に関する情報交換を行った。本節では、RFC3779 の意義について述べると共に得られた情報を元に今後予想される動きについて述べる。

グローバル・インターネットにおける経路制御のセキュリティは、経路情報が正しいのか、本来想定されたルータによって特定の経路情報が流されているか等の要素がある。その中でレジストリの登録情報に関連することは、経路情報交換における認証と、経路情報とアドレスの割り振り／割り当て情報との整合性である。

RFC3779 [2] は、X.509 形式の電子証明書に IP アドレスと AS 番号を含める拡張フィールドを定義している。この RFC は、拡張フィールドの定義や RIR の認可（authorization）の概念がまとめられたものであるが、このプロトコルの目指していることはグローバル・インターネットにおける経路制御のセキュリティに対して、PKI を用いたアプローチを行っていると言える。

RFC3779 の概要を以下に示す。

■RFC3779 の概要

Abstract

This document defines two X.509 v3 certificate extensions.　The first binds a list of IP address blocks, or prefixes, to the subject of a certificate.
The second binds a list of autonomous system identifiers to the subject of a certificate.
These extensions may be used to convey the authorization of the subject to use the IP addresses and autonomous system identifiers contained in the extensions.

RFC3779 の電子証明書の利用を想定している S-BGP は、1980 年代より研究が進んでいたプロトコルであったが、2001 年以降、アドレス資源の割り当てを行うインターネットレジストリで認証局が立ち上がり始めたことで、やっと普及の方法を検討できる段階になった。

S-BGP とグローバル・インターネットにおけるセキュリティについては、RPSEC WG [3] でドキュメント化の活動が進んでいる。グローバル・インターネットで経路情報の交換に使われている BGP のセキュリティにとって、AS パスの正しさが大きな意味を持つ。経路情報はルータ間をバケツリレー方式で転送されるため、集約やフィルタを行いやすくネットワークを拡張しやすい。しかし同時に情報が間違っていてもその間違いがどこで起こったか特定することが難しい。従って、既知であるかもしくは正しいことが分かっている伝播順序 AS パスであるかどうか、または経路情報の出所が正しいの

[2] X.509 Extensions for IP Addresses and AS Identifiers
http://www.ietf.org/rfc/rfc3779.txt

[3] RPSEC WG
http://www.ietf.org/html.charters/rpsec-charter.html

か、といった判断が各ネットワークの管理者に必要になる。

RPSEC WG のメーリングリストでは、改めて経路の安全性の要件をまとめなおしており、今後のバックボーン・インターネットにおける安全性の確保の仕方、ひいてはインターネットレジストリの業務のあり方に影響してくると考えられている。

なお、第 60 回 IETF では RFC3779 で言及されているインターネットレジストリの重要性や、IP アドレス認証局の応用に位置づけられる点等について S-BGP の提案者と意見交換を行った。

この情報交換でわかったことは、既に APNIC CA において検討が進められており、次回の APNIC ミーティングにおいて RFC3779 に関するミーティングが予定されていることであった。RIR における運用面の検討がまさに始められた状況と言える。

また電子証明書の適用手法について興味深い意見があった。はじめに認証用の証明書を運用し、次に登録情報を証明する証明書を運用する手法がよいとのことである。これは当センターにおける IP アドレス認証局の適用方法と同じである。レジストリにおける登録情報のセキュリティは、登録、公開の行為におけるセキュリティ機構を整備することによって一連の業務の安全性が向上すると考えている。まず登録時の認証強化を行い、暗号技術を使った強い認証のもとに登録された情報を証明（authorization の証明）していくという順序になる。

なお、JPNIC の IP アドレス認証局は、前者の認証を IP アドレス認証局(認証)が、後者の証明を IP アドレス認証局(証明)がそれぞれ役割を担うとしている。

3.5.3. APNIC CA における RFC3779 に関する検討

第 61 回 IETF のセッション後に APNIC CA の運用を行っている担当者と意見交換を行った。ここでおこなった意見交換では技術と運用の両面が話題になった。

技術面の話題は RFC3779 に則った証明書の発行が可能な環境についてである。APNIC ではオープンソースソフトウェアを使った認証局のシステムを運用しており、この対応の為の改良を行っているようであった。JPNIC の IP アドレス認証局は RFC3779 に対応した証明書を GUI（Graphical User Interface）を使って発行することができる。これは割り振り、割り当ての証明を行うことができる点で、意味的にレジストリ業務の安全性向上を望むことができるが、しかし技術的な観点では、アプリケーションの整備が必要であり、今後の大きな課題である。

また割り振り／割り当て業務との連携が必要となる。

運用面の課題は、共有プール化に伴うアドレスブロックの証明性である。アジア太平洋地域の NIR において、割り振りの為のアドレスブロック（プール）は共有プールと呼ばれる。これは APNIC が管理するプールとして扱われるため、アジア太平洋地域の

NIR は自らが管理するプールを予め固定的に持つことがない。

これは、全体的にアドレスブロックの連続的な割り振りをしやすくする効果があると同時に、各 NIR の立場では割り振り行為自体の正当性を保障することが難しい状況であると考えられる。

RFC3779 に準拠した証明書は各レジストリの割り振りを証明する意味を持つため、共有プールから割り振りを行っている NIR にとってこの証明書の発行業務はどれほどの保障性を持つのかが判断しにくい。なお DNS サーバの登録権限が NIR にあることで、運用上の正当性は NIR が管理する状況ではある。

一方ユーザネットワークの立場ではアドレスの一意性だけでなく、割り振り／割り当て情報、連絡先情報の維持がレジストリに期待される。その直接のやりとりのある NIR は、ユーザネットワークと LIR にとってのアドレス管理業務における信頼点である。今後 RFC3779 の証明書を使うアプリケーションが現れるに従って、信頼点の置き方を含めて適切な運用方法を検討していく必要があるであろう。

APNIC 担当者は APNIC における発行に意欲を示しているが、割り振りと整合性を持った証明書を適切な信頼点をもって運用できるか、など認証技術の運用に関しては今後の課題になると思われる。

3.5.4. IETF における認証技術の実践的な議論

近年の IETF において標準化活動の対象となっている認証技術は、Kerberos と PKI である。Kerberos は元々MIT Athena Project [4] で開発されたものだが RFC1510 が出されたり、スウェーデン王立技術研究所(KTH)で eBones を元に作られた Heimdal が配布されて以降、IETF KRB-WG を中心に多くの技術者によって拡張がなされている。一方 PKI は、W3C における XML 署名に関連する標準化 [5]、OASIS における PKI TC [6] といった活動はあるものの、IETF PKIX WG における標準化活動が最も先行しており、またその為に議論の結果の影響は大きい。

しかし IETF PKIX WG は PKI における証明書の書式と適切な処理に注目した WG であり、アプリケーションにおける適用を目的とした議論を行う WG ではない [7]。

---

[4] Kerberos: The Network Authentication Protocol
http://web.mit.edu/kerberos/

[5] W3C Technical Reports and Publications
http://www.w3c.org/TR/

[6] OASIS Public Key Infrastructure (PKI) TC
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pki

[7] Public-Key Infrastructure (X.509) (pkix) Charter

本調査研究の期間に参加したここ二年間の IETF PKIX WG の活動は、クローズ（WG の終了）に向けた活動を行っており、新たな話題が WG のトピックに入ることに対してとても慎重になっている。これまでは PKI を適用したアプリケーションに関する議論は PKIX WG で議論することができた状況であるが、今後はますます難しくなるであろう。

IETF に参加している日本の PKI の専門家の中には、影響力の大きい IETF PKIX WG の中で今後実用的な議論がしにくくなると、標準化された技術に基づく適用の議論をする場が少なくなるという状況に危機感を持っている人が多い。PKI を利用するアプリケーションには、https を使う World Wide Web やグループウェア、Windows におけるログオン等が現れているものの、依然限られている状況がある。

同様の危機感は日本の PKI の専門家だけでなく、IETF 参加者の多くにも共通しており第 60 回 IETF の SAAG(Open Security Area Directorate) のセッション [8]でも議論が行われていた。第 60 回 IETF の SAAG では、会場から認証技術と deployment（利用・展開）に関して次のような議論が起こっている。

- PKI の deployment
  PKI の deployment について、広範囲で、かつ工学的な取り組みが必要である。その為には組織的な導入活動が必要である。
- 認証の仕組みの透過性
  ネットワークにアクセスする仕組みとの透過的な関連性が必要である。

PKIX WG が、新たな実践面での話題を扱いにくくなっており、ネットワーク・プロトコルでの認証技術の利用といった実践的な話題を扱う場が、より多く必要になっている状況がうかがわれた。

この他に、各参加者より下のような意見が挙がっていた。

第 60 回 IETF SAAG で各参加者から出された意見

- 組織的な意図は複雑だが、一斉の導入はやっている事例がある。
- BCP(Best Current Practice)を出すべき。

IETF では他に EasyCert [9] というグループが作られて議論されているが、これまでに具体的な利用に向けた対策は挙がってきていない。

---

http://www.ietf.org/html.charters/pkix-charter.html

[8] 61th SAAG minutes
http://www1.ietf.org/proceedings_new/04nov/saag.html

[9] Easy-to-User Certificate
http://www1.ietf.org/proceedings_new/04nov/easycert.html

第 61 回 IETF の EasyCert BoF では、成功している事例から今後 IETF においてどのような活動ができるのかを見出すという主旨で、事例紹介が行われた。

この BoF の主旨は、PKI の成功した導入事例から使いやすい要素を洗い出し、IETF としてできる活動を明らかにする、というものである。

いずれの事例紹介でも話題になったのは、失効方法（CRL を使っているか）と証明書管理モデルの妥当性である。

これらの事例紹介に対し、会場から出る意見は多く、活発に議論が行なわれた。しかし IETF でできる活動の方向性を見出すまでの議論には発展しなかった。

今後はより多くの事例を集め、PKI のガイドブックとなる Informational RFC を作ることを目指す、ということになったが、IETF 参加者の中で利用性に関する意見をあげる人が多いことから、今後もこの認証技術の実践に関する議論が行われることが予想される。

以降、2004 年度に参加した IETF ごとにまとめる。

3.6. 第 60 回 IETF

調査研究の一環として参加した第 60 回 IETF について報告する。

■会議の概要

2004 年 8 月 1 日(日)～2004 年 8 月 6 日(金)、アメリカ合衆国のカリフォルニア州・サンディエゴにある Sheraton San Diego Hotel & Marina で第 60 回 IETF が開かれた。

IETF チェアの発表によると、今回の IETF における参加登録の人数は 1511 名(8 月 4 日現在)だったようである。第 59 回(韓国・ソウルにて開催)の 1255 名、第 58 回(アメリカ・ミネアポリスにて開催)の 1233 名、第 57 回(オーストリア・ウィーンにて開催)の 1304 名に比べて増加している。参加者の国籍は、最も参加人数が多かったのはアメリカで、次いで日本、韓国、ドイツ、フランスと続いていた。合計で 40 ヶ国からの参加があった。

今回の IETF では、120 以上のセッションが開かれ、その中で 11 の BoF が開かれた。前回と同様に、Plenary(全体会議)は IETF Business Meeting と IETF Planning Meeting の二つに分かれて行われた。

■IETF Business Meeting

IETF Bussiness Meeting では、今回の IETF でのネットワークに関する報告、RFC Editor からの報告、IANA による報告、IESG による報告、IESG のプロセスチーム

(PROTO)の紹介、WSIS における議論の紹介、IAB からの報告が行われた。

RFC Editor からの報告では、2004 年 4 月 7 日は RFC1 が発行されてから丁度 35 周年であることや、RFC2223 の記述に代わる新たな著作権表示と知的所有権に関するアナウンスがあった。下記の Web ページにまとめられている。

RFC Copyrights
http://www.rfc-editor.org/copyright.html

IESG からは PROTO チームに関する報告があった。PROTO チームとは、AD（エリアディレクター）のドキュメントプロセスの一部を担うグループで、2004 年 1 月に結成されている。PROTO チームに関する詳細は下記の Web ページにまとめられている。

IESG Process and Tools (PROTO) Team
http://www.mip4.org/proto/
WSIS：http://www.nic.ad.jp/ja/tech/glos-kz.html#03-wsis
IAB：http://www.nic.ad.jp/ja/tech/glos-ij.html#02-IAB

■IETF Planning Meeting

IETF Planning Meeting では、IRTF[10]の ASRG[11]から SPAM の現状と対策に関するプレゼンテーションと、IAB による Security workshop に関する報告、IETF の新たなドキュメント体制チームのステータスレポート、IETF の管理組織に関するステータスレポートが行われた。

ASRG のプレゼンテーションでは、SPAM メールが、必要なメールよりも多く配送されている現状や対策、関連するプロトコルの標準化活動を行っている MARID WG[12]の紹介が行われた。

IAB の Security workshop に関する報告では、CERT に報告されるインシデント数の増加や金銭や規模といった脅威の変化、SSH や VPN といった技術の適用場面の特徴、Peer-to-Peer のセキュリティや DDoS、フィッシング（銀行などの Web サーバと似たような発信元（ドメイン名）のメールを使った詐欺行為）といった未対策の分野の遍歴などが紹介された。

---

[10] IRTF：http://rfc-jp.nic.ad.jp/what_is_ietf/ietf_section3.html
[11] ASRG：Anti-Spam Research Group　http://asrg.sp.am/
[12] MARID WG：MTA AuthorizationRecords in DNS WG
MARID WG はライセンスと他技術に関する議論の結果、クローズとなった。

IETF の新たなドキュメント体制チームについては、General AD の Harald Alvestrand 氏よりステータスレポートが行われた。第 59 回 IETF の頃から始まった、ドキュメント化プロセスの効率化は ICAR[13]、NEWTRK[14]、PROTO、EDU といったチーム（一部 WG）によって進められており、それぞれの人数や活動内容のドキュメント化が進んでいるといった報告が行われた。

最後に IETF の運用組織（Administrative Group）に関して、ドキュメント化が進行中である旨の報告、コンサルタントの Carl Malamud 氏の紹介、Administrative Group がどのように ISOC[15]と関連していくかについてのプレゼンテーションが行われた。

■認証技術と PKI に関連する WG 活動

■PKIX（Public-Key Infrastructure (X.509)）WG[16]

PKIX WG は 8 月 4 日(水)の午前に行われた。参加者は 100 名ほどで、前回の約 50 名から比べると大幅に増えている。ただし各ドキュメントに特化した議論がほとんどであるためか、途中退席される方が見受けられた。

PKIX WG は第 57 回 IETF 以降終息に向け、既存のトピックのドキュメント化を中心に議論を進めている。最初にドキュメントステータスの発表が行われた。前回の IETF 以降から今回の IETF までに、下記の RFC が発行された。

RFC 3739　"Qualified Certificates Profile"
RFC 3770　"Certificate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN"
RFC 3779　"X.509 Extensions for IP Addresses and AS Identiers"
RFC 3820　"Internet X.500 Public Key Infrastructure Proxy Certificate Profile"

この他に四つの Internet-Draft（以下、I-D）が IESG に承認され、10 の I-D が AD または WG のレビュー中の状態である。

次に、提案された WG のマイルストーンが提示された。このスケジュールによると 2005 年の春までに、RFC3279 と RFC3280 の更新、テキスト文字列の処理、OCSPv2

[13] ICAR：Improved Cross-Area Review
[14] NEWTRK：New IETF Standards Track Discussion
http://www.ietf.org/html.charters/newtrk-charter.html
[15] ISOC：http://www.nic.ad.jp/ja/tech/glos-ij.html#02-ISOC
[16] PKIX WG
http://www.ietf.org/html.charters/pkix-charter.html

の拡張に関する活動を完了する予定になっている。

続いて、ドラフト・ドキュメントに関する議論が行われた。今回の議論では LDAP[17] 関連、文字列比較ルール、RFC3280 の更新、証明書検証プロトコルの SCVP といった話題があった。

LDAP に関しては、LDAP スキーマとエントリの記述方法に関するプレゼンテーションがあった。LDAP スキーマは、エントリの DIT（Directory Index Tree）構造と OpenLDAP（http://www.openldap.org）バージョン 2.2.1 に設定が含まれていることが発表されていた。正式に組み込まれるのは OpenLDAP 側のレビューの後であるとのことである。

文字列比較ルールについては、UTF8String といった文字データの種別の違いを超えた比較ルールの必要性や DC コンポーネントに対するルールなど、既存のルールとの使い分けなどについて議論が行われていた。

最後に、恒例のリエゾンによるプレゼンテーションとして、韓国の KISA（Korea Information Security Agency）の研究員から PKI の為のユーザインターフェースの要件に関するプレゼンテーションと、IKEv2（Internet Key Exchange version 2）から OCSP（Online Certificate Status Protocol）を効率よく利用するためのメッセージ交換方法について Mike Myers 氏によるプレゼンテーションが行われた。

■PKI4IPSEC（Profiling Use of PKI in IPSEC）WG

2004 年 5 月に、IKE で使われる証明書プロファイルに関する提案 draft-ietf-ipsec-pki-profile-04 が、WG で扱われるドキュメントの位置づけになり、draft-ietf-pki4ipsec-ikecert-profile-00 に改訂され、さらに-01 に更新された。そのため、多くの変更点がプレゼンテーションされた。

変更があった点は、IKE における IP アドレスペイロードの書式と検証方針、一度検証された証明書の扱いや、CERTREQ ペイロードに含めていた識別名（DN）が鍵情報になるなど、多岐にわたっている。また-00 から-01 での更新では、証明書の鍵用途拡張のフィールドがある場合の解釈方法や、認証局が拡張の鍵用途拡張フィールドを加えないなど、PKIX WG の仕様を深く解釈したうえでの提案がなされていた。

また証明書管理の要求事項をまとめた draft-bonatti-pki4ipsec-profile-reqts-01 を PKI4IPSEC WG で扱うことになり、今後、議論が進められるようである。

■MASS（Message Authentication Signature Standards）BoF

MASS BoF は、8 月 5 日(木)の午前に開かれた。定員 100 名弱の部屋には入りきれないほどの人数が参加したため、大きな部屋に移動して行われるという一幕があった。

[17] LDAP：http://www.nic.ad.jp/ja/tech/glos-kz.html#03-ldap

MASS BoF で提案している WG は、MARID WG で扱っている認証用途の DNS レコードを利用して、メールメッセージを認証できるようにするという目的を持っている。SPAM 等のメールで使われるような著名なドメイン名と類似するドメイン名をかたった場合に、判別ができるという効果を狙っている。

この BoF では、WG のゴールやチャーターが始めに提示され、次に DomainKey と呼ばれる認証の為に使われる鍵の使い方や、DomainKey を使ったメールメッセージ、MTA signature と呼ばれる署名に関するプレゼンテーションがあった。

しかし、会場からはフィッシングにおいて根本的な解決にならない、S/MIME との違いは何か、といった厳しい意見が出された。

■SAAG （Open Security Area Directorate：セキュリティエリア全体会議）

今回の SAAG では認証技術の適用に関する議論が行われた。議事録を下記に示す。

SAAG Minutes, August 2004

There were working group and BoF reports from PERM, SASL, KRBWG, INCH, PKIX, SMIME, LTANS, MOBIKE, PKI4IPSEC, ENROLL, MSEC, KITTEN, ISMS, and MASS. See the individual WG's minutes for details.

Joe Touch gave a talk on Anonymous IPsec (draft-touch-anonsec-00.txt). (Slides attached.)

Jordi Palet spoke on IPv6 Distributed Security; again, see the slides. (draft-palet-v6ops-ipv6security-01.txt)

Ian Bryant proposed work on exploit reporting.

During the open mike session, the primary topic of discussion was the difficulty of using certificates and PKI. A mailing list was created (https://www.machshav.com/mailman/listinfo.cgi/easycert) for discussion of this topic; the aim is to work towards an EASYCERT BoF in Washington. The goal of that BoF is to explore what the IETF can do to help with that problem. During the SAAG meeting, we heard of some success stories. The hard parts seemed to be at the political layer; success came when there was an already-existing authentication infrastructure that could be leveraged to issue certificates.

（60th SAAG minutes）
http://www.ietf.org/proceedings/04aug/205.htm

IETF の SAAG では、会場から認証技術と deployment に関して以下のような議論が起こっていた。

- PKI の広範囲で工学的な deployment が必要。それには組織的な導入活動が必要。
- 認証の仕組みとネットワークアクセスのユーザにとっての透過的な関連の必要性。

PKIX WG が、新たな実践面でのトピックを扱いにくくなっており、ネットワーク・プロトコルでの認証技術の利用といった実践的な話題を扱う場が、より多く必要になっている状況がうかがわれた。

セッションの最後には、エリアディレクターより、次回の IETF で実践的なトピックを扱う BoF が開催されることが示唆された。今後、認証技術の deployment に関する議論は、注目を集めることが予想される。

3.7. 第 61 回 IETF

■概要

2004 年 11 月 7 日(日)～2004 年 11 月 12 日(金)、アメリカ合衆国のワシントン D.C. にある Hilton Washington ホテルで第 61 回 IETF が開催された。

第 61 回の参加登録は 26 ヶ国から 1314 名が行ない、前回よりも参加国数、登録人数共に少ない状況であった。しかし IETF チェアの発表資料によると日本からの参加者はアメリカに次いで多く、全参加者の一割以上を占めていたようである。参加者のうち 50%以上を占めるのはアメリカ、次いで日本、韓国、ドイツ、フランスの順とのことであった。国際的な技術標準化の活動の場でこれほど多くの日本人が参加していることは大変素晴らしいことである。

■プレナリー（全体会議）

今回の IETF では、通常二回に分けて行なわれる Plenary(全体会議)が一回にまとめて行なわれた。RFC の発行前の編集を行なっている RFC Editor からは、2001 年には月に 20 程度の文書の編集依頼が来ていたが、2003 年以降は平均 28 に増加していることや XML を使った原稿が増えていること、新しい Word 用のテンプレート[18]に対する

[18] RFC Templates and Info. (Joe Touch 氏のページの一部)
http://www.isi.edu/touch/tools/

コメントを募集していることなどが発表されていた。IANA からは、コード番号やパラメータといった IANA の判断が関連する Internet-Draft(以下、I-D)の状況を見られる Web ページの紹介があった。http://www.iana.org/reporting-and-stats/で見ることができる。

IESG からは AD(Area Director)による I-D の処理状況で、第 60 回までの増加傾向から一転し、第 60 回 IETF から第 61 回 IETF の間はドキュメントの処理(レビュー)依頼件数が減少したことなどが発表された。この統計は主に AD のレビューを支援する PROTO チーム[19] の評価のために取られているそうである。IAB からは第 60 回 IETF で説明があった IETF の運営構造の再編成[20] についての現状報告がありた。ISOC の活動として IAB や IESG をサポートし、また IETF 運営の費用管理を行なう、IASA(IETF Administrative Support Activity)モデルについての RFC(BCP)が作られるようである。

■認証と PKI に関連した WG と BoF

PKIX、BTNS BoF、EasyCert BoF について報告する。

■PKIX

第 61 回 IETF における PKIX WG は 11 月 10 日(水)の午後 1 時から行なわれた。参加者は 60 名程であった。はじめにドキュメントステータスの確認が行なわれた。今回の IETF までに、RFC3874 "A 224-bit One-way Hash Function: SHA-224"が発行された。

以下の三つの I-D は IESG によって承認され、RFC Editor の編集待ちの状態にある。
"Additional Algorithms and Identifiers for RSA Cryptography"
draft-ietf-pkix-rsa-pkalgs-03.txt
"Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)"
draft-ietf-pkix-rfc2510bis-09.txt
"Internet X.509 Public Key Infrastructure Permanent Identifier"
draft-ietf-pkix-pi-11.txt
Certification Path Building を始めとする 6 つの I-D が AD によるフォローかコメントを待っている状態である。SCVP の第 16 版は WG Last Call がかけられた。

---

[19] Workgroup Chair Document Shepherding
draft-ietf-proto-wgchair-doc-shepherding-01.txt

[20] IETF AdminRest Homepage
http://www.alvestrand.no/ietf/adminrest/

今回のセッションではSCVPの16版(draft-ietf-pkix-scvp-16.txt)、RFC3280の改良、CRL の発行者を特定するための拡張フィールド(AIA)、CRL の検証ルール、証明書とCRL を格納する LDAP のスキーマ、簡易版の OCSP、ECC アルゴリズム識別子など、多くのプレゼンテーションが行なわれた。ここでは大きな動きのあった、SCVP と CRL の拡張フィールドについて紹介する。

SCVP の 16 版は、CA 証明書のフルサポートを始め、15 版から様々な機能追加や文書の変更があった。基本的な記述作業は一段落したようで、あとは ASN.1 の記述が正しいかを確認することが指摘されていた。

CRL 発行者を特定する仕組みについては、前回の IETF 以降に ML で必要性が指摘されていた。今回の提案は認証局と鍵を特定できるよう、CRL の拡張フィールドである Authority Information Access を使うことである。新しい作業項目ではあるが、短いドキュメントなので気にせず ML に投稿しては、というアドバイスが出されていた。

リエゾンによるプレゼンテーションは、韓国 KISA の研究員の方によって"User Interface Requirements for PKIX"と題して行なわれた。証明書を扱う GUI の要件について紹介するため、SSL/TLS に加えてオンライン取引に使用するといったデモが行なわれた。

WGチェアのTim氏によると、LDAPスキーマ関連のドキュメントやRFC 3279/3280の改良は2005年の春までに完了させる予定だそうである。PKIX WG のクローズに向け、ラストスパートをかけている様子である。

■EasyCert BoF

EasyCert BoF は、前回の IETF のセキュリティエリア会議(SAAG)で挙がった"PKIの利用が広まらない状況を踏まえて実践的な議論を進めるべき"という指摘を受け、エリアディレクターの Steve Bellovin 氏、Russ Housley 氏がチェアとなって開かれた。180 名近い参加者がいて、会場の部屋は超満員となった。

この BoF の主旨は、PKI の成功した導入事例から使いやすい要素を洗い出し、IETFとしてできる活動を明らかにする、というものである。BoF では MIT の Jeffley Shiller 氏、Johnson&Johnson の Robert Stahl 氏によって 2 つの事例が紹介がされた。

MIT では、学生と教職員の認証に PKI を利用していて、Web のクライアント認証の為の証明書を発行しているそうである。CRL はあえて発行せず、アカウントの無効化はサーバアプリケーションで対応、Kerberos のアカウントと連携しているようである。

Johnson&Johnson は、職員の認証に利用しているようで、大規模な導入の事例として紹介されているようである。上長による承認を経て証明書が発行されるモデルを採用しており、ハードウェアトークンを利用しているとのことであった。また大規模な事例として、Robert 氏に続いて DoD（米国防総省）の方が口頭で DoD PKI の紹介を行っていた。

いずれの事例紹介でも話題になったのは、失効方法（CRL を使っているか）と証明書管理モデルの妥当性である。DoD を除くどの事例でも、証明書は基本的に認証用に用いており、CRL に頼らず、サービスシステム側で認証用のデータベースを持っていた。ちなみに DoD で発行している CRL は 40 メガバイトにもなるそうである。

これらの事例紹介に対し、会場から出る意見は多く、活発に議論が行なわれた。PKI を簡単にする観点については、ISP が証明書を発行してはどうか、PKI の導入スケールを下げて考えるべき、フォーマットが複雑なのが問題、といった意見が挙がった。IETF としてできる活動については、色々な場面で使えるような証明書発行のブートストラッピング（初期立ち上げ）のプロトコルを標準化してはどうか、アカウントを管理するデータベースの議論が必要なのでは、といった意見が出ていた。この他に認証時にどのクライアント証明書を使うべきなのか戸惑う、といった意見があり、TLS WG へのフィードバックになるといったコメントが返されていた。しかし IETF でできる活動の方向性を見出すまでの議論には発展しなかった。

今後はより多くの事例を集め、PKI のガイドブックとなる Informational RFC を作ることを目指す、ということになり、この作業は IAB の Eric 氏が担当することになった。

EasyCert は、ML での議論も平行して行なわれていた。EasyCert ML に関する情報は"Easycert -- Easy-to-Use Certificates"にてまとめられている。

■その他

今回の IETF のセキュリティエリア会議(SAAG)で、Steven Bellovin 氏がエリアディレクターを引退することが発表され、後任には MIT の Sam Hartman 氏が着任することになった。

IETF はプロトコルの標準化活動を行う団体であるが、議論の中で運用面／利用面の意見が重要なフィードバックとなる。特に PKI の議論に関して、利用経験のある日本の技術者や研究者が標準化活動に参加することで、RFC に知見を盛り込み、利用性向上を図る活動の牽引力になると考えられる。

3.8. NANOG

3.8.1. 概要

NANOG は「The North American Network Operator's Group」の略でバックボーン・ネットワークや企業ネットワークに関連する技術情報の普及や、協調運用のための議論や教育を目的とした会議である。米国の非営利団体である Merit Network 社により、会議が年に三回行われている。このミーティングは主に米国とカナダの ISP を対象としているが、1985 年に始まった NFS-NET の運用上の会議から派生した歴史を持ち、それゆえ実践的で専門的な技術に関する議論が行われることが多い。

本調査研究ではアドレス資源管理の安全性がルーティングや DNS の管理といった ISP やバックボーン・ネットワークの安全性に影響することを踏まえて、NANOG においてどのような話題が扱われているかの調査を行った。

2004 年 10 月 17 日～19 日に開かれた第 32 回 NANOG に参加したところ、"BGP Multihoming Techniques", "Options for Blackhole and Discard Routing", "ISP Security Toolkits"といったバックボーン・ネットワークのセキュリティに関するアジェンダが多く、ネットワークオペレータが可用性（availability）を含めたネットワークセキュリティに高い関心を持っていることが伺えた。

NANOG32 のアジェンダにある話題は大手 ISP にとって先進的な話題であり、日本の ISP においても十分に有用な内容である。日本におけるネットワークセキュリティに関するセミナーは数多いが、特にバックボーン・セキュリティに関して、NANOG32 のような実践的な技術的な知識共有の場は依然少ない状況である。日本でディペンダブル（依存可能な）・インターネットを目標とする活動が見られるように、インターネットのネットワーク運用の側面からの普及・啓発活動が今後ますます重要になると思われる。

NANOG に関する詳細は下記の Web ページを参照されたい。

About NANOG
http://www.nanog.org/about.html

3.8.2. 第 32 回 NANOG における話題

第 32 回 NANOG では、企業や ISP におけるバックボーン・ネットワークの安全性

に関する話題が多く扱われていた。第 32 回 NANOG のアジェンダの中で、ネットワークセキュリティに関するものについて述べる。

Sunday Tutorials
1:30 - 3:00　BGP Multihoming Techniques
1:30 - 3:00　Options for Blackhole and Discard Routing
3:00 - 3:30　Coffee break
3:30 - 5:00　BGP Multihoming Techniques (cont'd.)
3:30 - 5:00　Internet Number Resource Management and Administration
5:00 - 7:00　AOL WELCOME RECEPTION !
7:30 - 8:15　ISP Security Toolkits
7:30 - 9:00　IPv6 Deployment and Case Studies

2004 年 10 月 17 日(日)の初日に行われたチュートリアルの中では、"BGP Multihoming Techniques"、"Options for Blackhole and Discard Routing"、"ISP Security Toolkits"が特に関連するであろう。

"BGP Multihoming Techniques"は、インターネットにおける経路交換の上で複数の上流接続を持つための具体的な設定方法を解説したものである。複数の上流接続を持つことによって、一つの回線が使えなくなった場合でも他の回線にトラフィックを振り替えることができ、ネットワークの可用性を上げることができる。

"Options for Blackhole and Discard Routing"は、ネットワークの利用不能攻撃（DoS）に対してよく知られている Blackhole ルーティングと Discard ルーティングを活用するための話題である。ネットワークの利用不能攻撃は、大量のパケットを特定の相手の送信することによって回線容量やルータの処理能力を限界に近づけ、本来の利用を妨げる攻撃である。このチュートリアルでは Blackhole ルーティングや Discard ルーティングを活用して、利用不能攻撃を意図したパケットをできるだけ発信源に近い場所で遮ったり、自組織のコンピュータから利用不能攻撃のパケットが発生した場合に他組織に迷惑がかからないようにしたりする方法が解説されていた。

次に一般セッションについて述べる。一般セッションはチュートリアルと異なり、技術の解説など自由な形式で行われる。以下に一般セッションのアジェンダを示す。

Monday General Session(Grand Ballroom)

8:00-9:00 a.m. Continental Breakfast, Grand Ballroom Foyer
9:00 a.m. Welcome, Introductions
9:20 a.m. Good Engineering Practice as it Applies to Unlicensed Wireless Networks
10:05 a.m. 802.1X: Deployment Experiences and Obstacles to Widespread Adoption
10:35 a.m. BREAK
11:05 a.m. Extension of Multi-Service Networks Dave Siegel, Global Crossing
11:35 a.m. Network Design to Support Very High-Capacity Streaming and Caching Infrastructures
12:00 p.m. LUNCH (on your own)
2:00 p.m. Botnets John Kristoff, Northwestern University
2:45 p.m. What Will Stop Spam? Charles Stiles, AOL
3:05 p.m. Optical Switching, a Great Tool in Platform Migration at AMS-IX
3:35 p.m. BREAK
4:05 p.m. Research Forum
Sizing Router Buffers

Performing BGP Experiments on a Semi-Realistic Internet Environment
Guido Appenzeller, Stanford University

Monday Evening BOFs +
Key Signing Party

7:30 - 9 p.m. ISP Security and NSP-SEC BOF VII (Grand Ballroom)
9 - 9:30 p.m. PGP Key Signing Party
9 - 10:30 p.m. Optimizing Operational Input to ARIN: What Is Needed and How Do We Get It?

2004 年 10 月 18 日(月)と 19 日(火)は、一般セッションである。17 日(日)のチュートリアルと異なり、発表者だけでなく参加者がディスカッションに参加する形で行われる。

一般セッションの中で特に注目を集めていたのは"What Will Stop Spam?"である。第 60 回 IETF で話題となった、スパム・メールの転送を防止するために使われる

SenderID,SPF,DomainKeys を利用しても防ぎきれない状況を解説し、今後どのような技術によってスパム・メールを減らすことができるのか、という議論であった。しかしまだ具体的な方策を見出すことは難しく、別途議論の場を設けて検討を進めていく、という段階である様子であった。

NANOG ミーティングにおけるセキュリティの話題

NANOG ミーティングのこれまでのアジェンダを見ても、今回は特にバックボーン・ネットワークのセキュリティに関連する話題が多い。1990 年代後半から 2001 年年頃は、インターネットでの不正アクセス行為に対しては、ファイアウォールが一定の効果を上げていると考えられていた。しかし近年の不正アクセスはネットワークの内外から大量のトラフィックを送りつける使用不能攻撃であったり、ウィルスやスパム・メールを活用し内部から攻撃したりするものになりつつある。インターネットの家庭への普及が手伝って、これらの不正アクセスの対策は多様な側面を持ってきた。

NANOG ミーティングに参加していると、まずこのようなバックボーンとしてのインターネットのセキュリティに関する意見交換の場が、日本ではまだまだ限られているということを再認識した。日本はブロードバンド・ネットワークの一般家庭への普及が進んでいる世界でも有数の国であり、バックボーン・ネットワークのセキュリティは今後ますます重要になる。また家庭用のネットワークでありながらネットワークの回線容量が大きいことから、前述したネットワークの使用不能攻撃が甚大な被害を発生しうる。

インターネットはネットワーク同士が自律的に問題解決を行って運営されているネットワークの集合体である。その自律的な問題解決の為の相互連絡手段を提供している立場であるインターネットレジストリが、今後どのような役割を果たすべきなのか、オペレータとの意見交換を進めて行うことが必要になってくるであろう。

3.9. 認証技術に関わる国内動向

3.9.1. JNSA における調査研究と取り組み

日本ネットワークセキュリティ協会(JNSA)はネットワークセキュリティに関連するベンダ、システムインテグレータ、インターネットプロバイダといったベンダを中心に、ネットワークセキュリティの社会へのアピール、諸問題の解決といった活動を行う特定非営利活動法人（NPO）である。

政策部会、技術部会等の部会に分かれて活動しており、その内容は調査、実験、勉強会等多岐にわたっている。

JNSA 技術部会の PKI 相互運用技術 WG は、PKI の必要性のアピールと問題解決を目的としており、2004 年度は勉強目的で開催された。

これまでに行われた三回の勉強会では、IETF の標準化動向、運用技術、法制度の三つが主な話題であった。

JNSA の勉強会の議論のテーマとして挙げられるキーワードは「マルチドメイン PKI」「ミドルウェア」「PKI の知見蓄積」であろう。

「マルチドメイン PKI」は JNSA の勉強会の中で中心的な考え方である。IETF の PKIX WG は PKI のフォーマットや証明書の処理方法といった、基本的な技術を対象としている WG である。「マルチドメイン PKI」は現実社会の複数の認証のドメイン（範囲）が存在する環境に、電子的な認証を導入するのに適しているモデルであると考えられている。

「ミドルウェア」と「PKI の知見蓄積」は、普及の段階の議論の中で互いに近い関係している。IETF PKIX WG で進められているような証明書の処理方法だけでなく、運用に必要となる技術（運用技術）の議論を進めることで、認証技術の知見蓄積を進めるという考え方である。ミドルウェアとして捉えることで、アプリケーション開発や基盤機能構築が容易になる状況を想定している。このミドルウェアの概念を図示したものが次頁の表 * である。

法制度については e-文書法の議論が多かった。アプリケーションの課題や電子文書の継続性の課題などが主な話題である。

＊ ミドルウェアの二つの側面

	技術	運用
上位層	アプリケーション	制度、業務形態に合った運用
中間層	セキュリティ ミドルウェア（API）	セキュリティ・インフラの運用
下位層	ネットワーク等の インフラ、API	セキュリティ以外の基本機能

セキュリティ・ミドルウェア(API)の取り組みによって、アプリケーションに対する複雑なセキュリティの要求を吸収し、より簡単で安全なアプリケーションの開発が期待できる。一方、運用面のセキュリティ・インフラは、未開拓の領域である。

本調査研究の IP アドレス認証局は、セキュリティ・インフラの運用に対する取り組みと言える。第 2 回の会合で IP アドレス認証局に関する発表の時間を頂いたところ、様々な方面から意見を頂くことができた。

第 2 回 PKI 相互運用技術 WG で頂いた IP アドレス認証局の応用に関する意見

- IP アドレスに地域の属性を関連づけ、リージョンコードや ISP の識別、地域網の構築が可能になるのではないか。
- AS 番号の証明書を発行することでネットワークの単位で相互の認証ができるようになる。
- POS システムで IP アドレスを利用し、各店舗の無線 POS の一元管理に利用することはできないか。
- IP トレースバックの際に参照するルータの証明書
- IP アドレスに関連づいた情報を使った動的なフィルタ

また進め方として「漠然と利用可能性を挙げるのではなく何をどう認証するのかを考えるべきである。ISP 等のサービスプロバイダを含めた議論が必要ではないか」という意見を頂いた。

前年度の調査研究では IP アドレス認証局の応用可能性を調査したが、今後の構想を念頭に置いた活動には、認証対象や運用方法といった、具体的な検討を行っていく必要があると考えられる。

3.10. JANOG

JANOG(JApan Network Opetators' Group)はインターネットの技術的事項やオペレーションに関する議論、検討、紹介等を行っているグループである。参加は自由に行うことができ、通常はメーリングリストを使った情報交換を行い、一年に三回程度ミーティングを行っている。運営委員会が設置されて運営されているが、インターネットに接続されるバックボーン・ネットワークの運用を有志で行ってきた人の集まりといった、技術者特有のフランクな雰囲気を持つグループである。

IRS(Interdomain Routing Security Workshop)は JANOG のメーリングリストで呼びかけられ、開催された中規模の会議である。IRS も有志によって開催された。

2004 年 7 月 7 日に行われた IRS では下記のアジェンダで情報交換が行われた。

IRS のアジェンダ（http://www.bugest.net/irs/docs_20040707/ より）

- Interdomain Routing Security(IRS) とは？
- IRS の動向
  Control Plane　　---　GTSM、BTSH ほか
  （Forwarding Plane　---　ACL、RPF ほか）
  （Management Plane　---　AAA、Management Port Separation ほか）
  soBGP の motivation と Implementation/Deployment 想定
- TCP Vulnerability 対策について

IRS では経路情報交換における認証だけに注目しているわけではないが、7 月 7 日以降、JANOG のメンバの間では BGP において認証の強化を行った soBGP、S-BGP の議論が活発に行われた。

日本のインターネット・バックボーンの強化を考えると、経路情報の交換のセキュリティは大きな課題である。現在は各 ISP の自助努力によってネットワークの安定性／安全性の確保が図られているが、日本のインターネット全体の安定性／安全性向上の為には、ISP の間でセキュリティの整備が進めることが必要になると考えられる。

今回の IRS でアジェンダにあがった手法が普及していく場合、認証は何を元にして行うかといった、セキュリティの運用の重要性が増してくると考えられる。

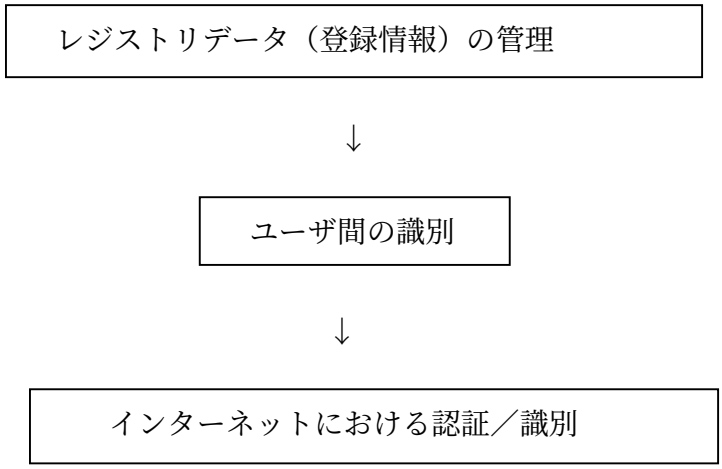
その中で、アドレス資源の管理を行うインターネットレジストリの役割は大きな意味を持つであろう。

3.11. IP アドレス認証局の技術的検討の方向性

IP アドレス認証局は、アドレス資源の登録に関わる認証強化と登録情報の証明の役割を持つが、国内外の技術動向を調査研究するに従って、その意味と技術的な検討の方向性が具体化してきた。

インターネットレジストリが管理しているレジストリデータは、ネットワーク利用組織の IP アドレスと AS 番号の台帳と考えることができる。インターネットに接続しているネットワーク利用組織は、IP アドレスで通信相手を識別する。認証を行う際にもドメイン名だけではなく IP アドレスに変換した結果を元に通信相手を調査するといったこともおこなわれている。

つまりインターネットレジストリは、レジストリデータの情報登録と公開を通じて、ユーザ間の識別手段を提供しているのである(下図)。



IP アドレスを用いた「インターネットにおける認証／識別」は、ユーザ・インターフェースに現れる「認証／識別」ではないが（一般的にユーザに覚えやすいドメイン名が使われるであろう)、DNS で調べることができるドメイン名と異なり、経路制御に直接影響している。これは IP アドレスを成りすますと、即座に通信相手や本来の IP アドレスを持つネットワーク・インターフェースが到達不能になり、成りすましたまま通信を行うことが困難であったり、すぐに気づかれてしまったりする性質がある。

将来的に、BGP における認証をはじめ、逆引きネームサーバを使ったメールサーバの識別（スパムの防止)、通信相手のネットワークの識別、ISP の識別といった、重要な識別にレジストリデータが使われることを想定することができる。

インターネットレジストリは、登録情報である IP アドレスや AS 番号をユーザ間の認証に使えるような技術的検討を進めることで、インターネットの安定性／安全性の向上に資することが可能であると考えられる。

3.12. JPNIC IRR 企画策定専門家チーム

前章で述べたインターネットレジストリの登録情報の応用例として、IRR(Internet Routing Registry)が挙げられる。whois と同様にコマンドラインや Web で登録情報を検索するインターフェースが実装されている。IRR は、経路情報に関する情報の登録・公開機能であり、インターネット・バックボーンに接続されるルータの管理者によって利用されることが想定されている。

JPNIC では IRR 企画策定専門家チームを通じて、IRR のサービスをより広範囲で利用性、安全性の高い機能に高める検討が進められている。広範囲とは RIR の IRR との連携によって、世界中の経路情報の登録情報を検索できることを意味する。この連携はミラーと呼ばれデータを交換する機構を使って行われる。

利便性については IRR に登録された情報をルータの設定に反映したり、経路情報の齟齬を検出することができたりする為の研究や調査が行われている。

広範囲でかつ利便性の高い経路情報の登録情報を提供することで、ユーザネットワークを収容しバックボーンに接続するルータが、インターネット全体に対して矛盾なく経路情報の交換ができる状況を実現することが可能になる。

JPNIC の IRR 企画策定専門家チームでは 2004 年度からセキュリティに関する調査が本格化し、認証局を用いた安全性向上、AS 間のメッセージ認証、IRR の提供情報の信頼性向上などが検討されている。詳細は本報告書第 7 章にて述べる。

3.13. 認証技術(PKI)の動向から見た適切な普及の課題について

PKI は IP アドレス認証局の中心的な役割を果たす技術である。IETF における PKI の標準化活動は現在も続いており、また Mozilla や Internet Explorer をはじめ多くのプログラムは PKI の一部しか実装していないという現状がある。PKI の実用化自体が課題となっている IETF SAAG における議論に見られるように、この状況の要因として利用／運用のための知見が十分に揃っていないことが挙げられる。普及が進まないために利用の知見が蓄積されにくいという悪循環の状況なのである。

JNSA 等の国内での多くの議論の中では、この悪循環を打開する方法は二つの方針があると考えられている。一つは簡単に認証技術を使える状況、つまりユーザが認証技術自体を意識することなく利用している状況を目指すという強制的な普及の方法である。もう一つ既存の制度の中に認証技術を取り入れ、現行業務の安全性向上を目指す方法である。前者は Mozilla や Internet Explorer、Opera といった Web ブラウザが SSL や証明書処理の機能を持つことに見られるように、技術の普及が進んでいると見ることができる。一方、後者は各業界における業務との折り合いが必要であり、現在は進んでいない。個人情報保護のために電子認証技術を採用する動きがあるのは後者の手法に分類されるであろう。

今後、認証技術の適切な普及は、既存の制度に対して適合する形で認証技術を適用していくことが肝要であると考える。国内における「認証」という行為は、各事業や業務における信頼点（事務局や執行役員、企業における代表など）の元に行われていると考えられるであろう。これをインターネットを使った電子認証に落とし込むに当たって、Web ブラウザに組み込まれた認証局証明書が適切かどうか、検討を要するであろう。

本調査研究はその検討の一つの事例として考えられる。本調査研究はインターネットレジストリにおける認証局に関する調査研究であるが、本質的には認証技術をアドレス資源管理の業界でどのように適用していくか、という点が主題となった。前年度の調査研究の結果、レジストリにおける認証業務に適合するモデルは外部に登録主体を持つモデルとなった。これはレジストリ内での認証局と IP 業務部分の分離、外部 RA（Registration Authority）を用いた IP 指定事業者自身による証明書管理という、既存の IP 業務との親和性を意識したものである。またレジストリにおける認証局は、RIR との相互連携を視野に入れておかねばならない。また今後実施されていくと考えられるバックボーン・ネットワークのセキュリティの為に、最新の技術を使った証明書の扱いを検討する必要があった。

第4章 RIR の認証局とセキュリティの動向

内容

- APNIC における動向
    1. RFC3779 BoF
    2. MyAPNIC と証明書発行数
- RIPE NCC における動向
    1. 認証局と Database の連携
    2. 今後の方向性に関する情報交換
- ARIN における動向
    1. 証明書の用途
    2. チュートリアルの内容

第4章　RIR の認証局とセキュリティの動向

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」を通じて、各 RIR が、認証局の構築をはじめとする安全性向上の方策を取っていることがわかった。ユーザの管理と認証局を組み合わせ方は RIR によって様々な方法を取っている。またレジストリデータの登録者の考え方が異なっていた。

2004 年度の調査研究では、更に各 RIR の担当者および責任者と直接的にヒアリングを行い、認証局のマネジメントに関する知見の交換を行なった。これらのヒアリングを通じて、レジストリデータの登録者に対する認証を目的とした限定的な認証局であることが判明してきた。また APNIC や RIPE NCC の認証局は、利用が強制されていないにも関わらず証明書発行数が伸びている。逆に JPNIC において検討が進んでいる業務モデル、CP/CPS の策定、レジストリデータの応用の為の認証局について、RIR の認証局の担当者にとっての参考情報として、一定の注目があることがわかった。各 RIR が認証局の構築の模索を行ってきており、参考事例が少ないという経緯が原因として考えられる。

本章では各 RIR のミーティングと各 RIR の認証局担当者と行ったミーティングを通じて得られた認証局と登録情報のセキュリティに関する動向について報告する。

4.1. APNIC における認証局マネジメントの動向

■APNIC CA の動向

APNIC CA は APNIC メンバに使われる証明書を発行している認証局である。証明書は、APNIC とメンバとのメールの保護や MyAPNIC（Web インターフェースを持つ資源管理システム）へのアクセスの保護に使われる。

APNIC CA が発行した証明書の発行数は順調に増加しており、担当者の話によると 2002 年 11 月の運用開始から一年後の 2003 年 11 月には 600 を超え、2004 年 8 月には 1000 を超えているとのことである。

このことから APNIC CA は利用者が順調に増加していることも容易に想像でき、アドレス資源管理の認証用の認証局として成功している事例と見ることができるであろう。そこで第19回APNICミーティングで運用状況と今後の活動方向についてヒアリングを行った。

このヒアリングの為のミーティングは APNIC CA の構築と運用を行っているプロジェクト担当者と個別に行った。このミーティングでの情報交換は非公式に行っているため、必ずしも APNIC の今後の活動を示すものではないが現状と今後の活動方向性の情報を得ることができた。ミーティングの内容を以下に示す。

- APNIC CA の運用状況
  APNIC CA と JPNIC CA の連携可能性があるか。またその場合はどのような形になるか。
  連携を踏まえた crossCertificate の可能性
- CPS のドラフト状況
  APNIC CA が発行した証明書を認証に利用するアプリケーション S-BGP と soBGP における証明書の応用。S-BGP に関するミーティングについての情報。
  IP アドレスを含めた証明書について。
  ルーティングセキュリティへの影響。

このミーティングの結果、以下のような情報交換を行うことができた。

- APNIC CA の運用状況

申請の頻度	一日に 2,3 通
運用場所	オーストラリアのブリスベン
運用に関わる人数	登録（RA）は IP アドレス管理業務を行うホストマスター（10 名）が兼務。認証局自体はプログラマを含め 3 名。
運用体制	システムの運用は 24 時間 365 日。承認と発行業務は通常の業務時間と同じ。登録は午前 7 時から午後 7 時まで。認証局（発行）は午前 9 時から午後 5 時まで。

- 認証局の連携可能性について
  相互認証は運用が簡単ではないので調査が必要と考える。JPNIC 側で調査が進んでいるようであれば情報交換したい。

- CPS のドラフト状況
  特に進展はなく、ドラフトしている状況である。正式なリリースはしていない。

- S-BGP、soBGP に関して
  APNIC にとって潜在的な次のサービスとなるかもしれない。
  RFC3779 に準拠した証明書の管理がポイントになる。階層構造でなければならないので、NRO がルート証明書に署名し、APNIC が NIR 用の証明書に署名するなどというように考えている。サンプル証明書を数ヶ月以内に作成することを考えている。
  第 18 回 APNIC ミーティングで S-BGP の提案者と RIR の認証局関係者を交えたミーティングが予定されていたが、彼の参加ができなくなったため、第 19 回 APNIC ミーティングに延期された。

- その他の特記事項

- APNIC CA 証明書の再発行
  APNIC CA において HSM（Hardware Security Module）の導入が行われた。また認証局証明書の再発行が行われ有効期限が 2014 年 6 月 3 日になった。以前の証明書の有効期限は 3 年間であったが、今回 10 年間の証明書に切り替えられたことになる。

次に第 19 回 APNIC ミーティングの期間中に行われた RFC3779 について述べる。

4.1.1. RFC3779 BoF

RFC3779 は IP アドレスと AS 番号を X.509 形式の電子証明書に含める為の書式を提案した RFC である。またこの RFC ではこの証明書がインターネットレジストリにおける「アドレスブロック利用／管理権限の証明」を行うとされている。（RFC3779 の内容は章末を参照）

APNIC の認証局プロジェクト担当者の呼びかけでこの RFC3779 に関する BoF（Birds of Feather：興味を持つ人が集まる非公式の会議）が開かれた。この BoF のアジェンダを下に示す。

概要：
S-BGP で利用可能な RFC3779 形式の証明書のインターネットレジストリでの運用に関する BoF
日時：
2005 年 2 月 24 日 18:00 から
アジェンダ：
Meeting objective and agenda bashing
Participant introductions
RFC3779 summary
Open discussion
Meeting conclusion
Action plans (if any)

この BoF には IETF セキュリティエリアのエリアディレクターや RIPE NCC の技術統括、APNIC の技術統括と認証局プロジェクト担当者、S-BGP の提案者、各 RIR の会議に参加し活躍している技術研究者といった著名な人物が参加した。

議論に先立ち、APNIC の認証局プロジェクト担当者よりこの BoF での議論の側面が示された。ポリシー、技術、オペレーションの三つである。

ここでいうポリシーとは IP アドレスの管理ポリシーと認証における信頼のポリシーである。RFC3779 の形式の証明書はアドレス資源の割り振り／割り当てに従って発行されるものであり、インターネットレジストリにおける実際の割り振り／割り当てと連動することが必要となる。

技術については、PKI と RFC3779 の形式の証明書の用途に関する議論が行われた。電子証明書は割り振り行為と対応する形で発行されツリー構造が形成される。また明文化はされていないもののこの形式の証明書は S-BGP で利用されることが想定されている。

オペレーションはインターネットレジストリと認証局における運用である。RIR では認証局を立ち上げるプロジェクトが次々に実施されており、既に APNIC、ARIN、RIPE NCC が認証局の運用を行っている。また RIR におけるアドレス資源の階層的な管理が始まる前のアドレスに対する証明書を扱うため、IANA の認証局が必要かどうかを検討する必要がある。

BoF では以下のような議論が行われた。

論点：

- AS Holder とネットワーク管理者の違い
  そのため RFC3779 では S-BGP に言及していない。
- レジストリに対する信用とルーティングシステムの信用の違い
  対応を取る方法（subjectAltName を使うなど）は考えられるが、
  運用上の課題がある。
- 証明書の有効期限
  保障の上では短いほうが望ましいが、ルーティングの混乱を避けるには
  ある程度の長さが必要になる。
- アドレスブロックの切り替え(ERX 等)への対応
  歴史的な経緯で RIR を通さず IANA から直接割り振られているアドレスの証明書など、アドレスの移管や割り振りの変更があった際の影響に対応する必要がある。この点はまだ議論が続いており、メールで継続してやりとりされている。
- IANA による認証局か他の認証局か
  歴史的な経緯のアドレスに対する証明書を扱うには、IANA で認証局を構築することが必要になる。NRO（Number Resource Organization）によって認証局が運用されるという案も挙がっている。
- アドレスの追加割り振りと鍵ペアを再生成
  アドレスの追加割り振りは新たに証明書が発生することを意味する。
  しかし議論の結果、追加割り振りは同じ鍵ペアの保有者に対して行われる

- 認証局の実装方法
  商用認証局を利用するには証明書要求の際に入れ込んでおく必要がある。またオープンソースの認証局のどちらでも、レジストリが拡張フィールドを管理する必要がある。
- 全ての証明書に CA フラグが必要
  RFC3779 の証明書は割り振り先に対する証明書を、上位が発行した証明書の鍵ペアを使って発行する。つまりすべての証明書が認証局の役割を持つ。
  https や S/MIME の用途で発行した証明書では一般的に行われないことであるが、証明書に CA フラグ（認証局証明書であることを示すフラグ）を含める事になる。また拡張フィールドの keyUsage に keyCertSign といった証明書発行を意味するフラグが立てられることが予想される。

今後どのように議論が進められるかは未定だが、IETF RPSEC WG のメーリングリストの動向を見ると、ルーティングプロトコルの安全性の議論が更に進み証明書の適用方法にまでつながっていく必要があると考えられる。

なお、電子証明書については次回 IETF でも議論が行われる様子であった。

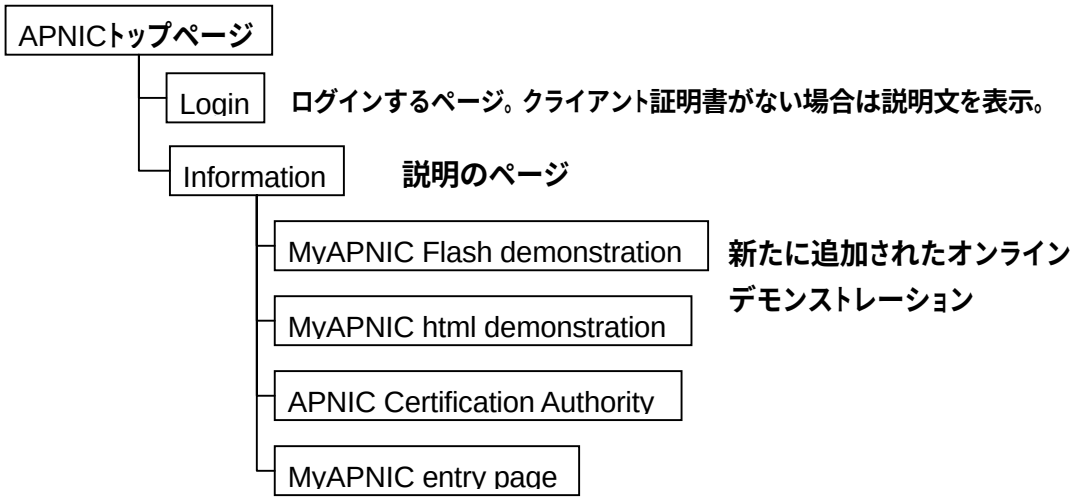
今後は IETF などを通じて議論を進めていくということになった。

4.1.2. MyAPNIC と認証局に関するガイドの充実

APNIC CA が発行する認証用の証明書は MyAPNIC と呼ばれる資源管理の為のシステムで利用されている。MyAPNIC は Web を利用したシステムでアドレス資源の申請等を行うユーザは Web ブラウザを使ってアクセスする。通信には https（SSL/TLS を用いた HTTP）を用い、通信路の暗号化、やり取りされるメッセージの保護、通信相手の認証が行われている。

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」以降、MyAPNIC 自体の主な機能の向上は見られないが、ユーザに対する説明資料は拡充していた。

MyAPNIC に関する Web ページの構造を示す。



今回追加されたデモは認証を含めて MyAPNIC の利用法を三つの部分に分けて説明している。はじめに「セキュリティ」が説明される。https を使った通信路の保護、https を使った相互認証、証明書を使った認証が挙げられている。

次に資源管理の方法、アカウント管理（連絡先、費用）の方法が説明され、最後に選挙のための投票機能の使い方と APNIC が実施しているトレーニング状況の表示方法について説明される。

このように MyAPNIC はクライアント証明書を用いた認証を実施すると共に、その認証結果をアクセスコントロールのために利用している。

[http://www.apnic.net/member/corp-contacts/index.html] 権限の説明

MyAPNIC のセキュリティの機能には、X.509 形式の証明書を使ったクライアント認証だけではなく、ユーザの権限管理がある。MyAPNIC での権限の分類を以下にあげる。

MyAPNIC における権限の分類

* Policy development
* Internet resource management
* Technical issues
* Administration/billing
* Training

なお権限分離の機能は 2003 年度の調査時と変わっていないが、Training の役割に対してトレーニングコースの受講結果を表示する機能が実装されている。

4.1.3. 登録情報のセキュリティの動向

APNIC ミーティングにおける登録情報のセキュリティに関する動向について述べる。

APNIC ミーティングにおける登録情報に関する議論の場は、Database WG である。第 18 回 APNIC ミーティングの Database WG のアジェンダを以下に示す。

第 18 回 APNIC ミーティング Database WG のアジェンダ

Review of action items
Proposal on IPv6 IRR service at APNIC
Privacy of customer assignment records - project update
Protecting historical records in the APNIC Whois Database - project update
Modification of Whois domain object authorisation
RIPE database software update

このうち登録情報のセキュリティに関連する話題は、「Protecting historical records in the APNIC Whois Database - project update」が挙げられる。

「Protecting historical records in the APNIC Whois Database - project update」は RIR によるアドレス資源管理が始まる前の IANA から割り振られたという歴史的経緯を持つアドレスの保護に関するプロジェクト中間報告である。歴史的経緯を持つアドレスの中でハイジャックと呼ばれるのっとり行為が行われており、問題になっている。ハイジャックされた登録情報の一覧を作っている Web サイトが存在している。
http://www.completewhois.com/hijacked/hijacked_qa.htm

なおこの Web ページは 2002 年度の「IP アドレス認証局のあり方に関する調査研究」でも取り上げた。登録情報ののっとり行為は RIR や NIR で階層的に管理しているアドレスよりも歴史的経緯を持つアドレスの方が行われやすいと言われており、APNIC ミーティングでのプレゼンテーションではその傾向を受けたものであると考えられる。ハイジャック自体は歴史的経緯を持つアドレスの登録情報に限られた問題ではない。

このプレゼンテーションでは、歴史的経緯を持つアドレスに対して APNIC のメンテナを用いた管理（一旦登録情報を APNIC の管理下におく）とし、継続して管理を行う場合には一つのメンテナを設けるごとに 100 米ドルを維持料として APNIC に支払うとしている。

第 19 回 APNIC ミーティングでは、登録情報とスパム、認証局に関する議論が行われていた。第 19 回 APNIC ミーティングの概要とスケジュールを次頁に示す。

概要：
2 月 21 日（月）Tutorial
Dynamics of policy process
Spam prevention

2 月 22 日（火）Tutorial
Keynote: Security protocol
Certification Authority
ISP security strategy
Internet governance（一部 ISP security strategy と併催）
APOPS
PGP key signing party（APOPS と併催）
APRICOT opening event

2 月 23 日（水）Policy meetings
APRICOT plenary
IPv6 technical SIG
NIR SIG（IPv6 technical SIG と併催）
Routing SIG
APNIC 19 reception
＃RFC3779 BoF は APNIC19 reception の直前の一時間に行われた。

2 月 24 日（木）Policy meetings
Policy SIG
Database SIG
IX SIG（Database SIG と併催）
DNS operations SIG（IX SIG と併催）
CRISP/EPP BOF
APRICOT closing reception

2 月 25 日（金）Member meeting
APNIC Member Meeting

第 19 回 APNIC ミーティングで行われたセッションのうち、登録情報とネットワーク・セキュリティに関連するものに、2 月 21 日と 2 月 22 日のチュートリアルでスパムメールと認証局に関するプレゼンテーションが挙げられる。また 2 月 23 日に行われた

Database SIG では登録情報の記述言語である RPSLng に関連する APNIC での状況報告が行われた。

2005 年 2 月 21 日のチュートリアルセッションでは「Dynamics of the policy development process」、「Introduction to spam prevention」、「Anti spam activities in Japan」の三つが行われた。最初のものは APNIC におけるポリシー策定プロセスに関するチュートリアルである。二番目と三番目はインターネットにおけるスパムメールの一般的な話題であるが、APNIC や JPNIC といったインターネットレジストリは登録情報の中に、ネットワーク管理者同士が連絡を取り合うことに利用されるコンタクト情報を持っていることから、インターネットレジストリの情報提供機能における課題抽出が可能な話題であると考えられる。

「Anti spam activities in Japan」では最近になって日本で見られるようになった、機械的なフィルタにかかりにくいスパムメールや携帯電話を使ったスパムメール、日本における法制度の動向などについてプレゼンテーションされた。

スパムメールをフィルタする為に、メールで使われているフレーズに基づいた技術が多くのプログラムで使われているが、あたかも人が発信したかのようなスパムメールはこのフィルタにかからない。このような巧妙なスパムメールは増加しつつある。

スパムメールの配送をフィルタする技術には、メールの発信元であるメールサーバの DNS への登録状況を確認する方法や、メールメッセージに含められた署名データを検証する方法がある。このようなネットワークの登録情報を使う場合、その登録情報の正当性が重要性を持つ。現在、アドレス資源の割り振り情報を使ったメッセージ発信元の認証技術は普及していないが、IETF における DNS のゾーン情報を使った技術標準化が進むに伴って今後インターネットレジストリにおける登録情報の管理上の役割が発生する可能性が考えられる。

2005 年 2 月 24 日の Database SIG では RPSLng に関する情報共有のプレゼンテーションが APNIC の技術部門担当者によって行われた。このプレゼンテーションでは IETF における RPSLng に関する標準化と開発の活動 * 、APNIC における IPv6 をサポートした IRR（Internet Routing Registry）IETF CRISP WG における標準化活動 * といった RPSLng に関連した APNIC における活動についての情報共有が図られた。

RPSLng に関する標準化と開発の活動

- IETF における Internet-Draft の新バージョン
  draft-blunk-rpslng-08.txt
- IRR における IPv6 とマルチキャストルーティングのサポート
- Merit におけるプログラム開発
  2004 年 10 月　初バージョン
  2004 年 12 月　RIPE NCC の whois での組み込み
  2005 年第二四半期　IPv6 のルーティングレジストリでの組み込み

CRISP WG における標準化活動

- 2004 年 1 月　利用上の仕様の PS（Proposed Standard）化
- 2004 年 1 月　ドメイン名のスキーマ（dreg）の PS 化
- 2004 年 6 月　IP アドレスのスキーマ（areg）の PS 化

2005 年 2 月のドキュメント化の状況

RFC 発行済み

- RFC3707　CRISP requirements

CRISP（Cross Registry Information Service Protocol）は whois に変わる登録情報の効率のよい閲覧を実現するプロトコルである。このプロトコルには「レジストリの管理化にある情報の適切な特定」「情報伝送と問い合わせ応答のプロトコルの実現」といった機能が必要とされている。

この RFC ではディレクトリサービスの実現や転送プロトコルについて定義している。

- RFC3981　IRIS core protocol
  IRIS（The Internet Registry Information Service）はクライアント・サーバモデルで登録情報の問い合わせ・応答を実現する為のプロトコルである。
  XML（Extensible Markup Language）を用いており、特定の種類の登録情報に依存しない、汎用的な問い合わせ・応答の定義を行っている。
- RFC3982　DREG schema
  IRIS のドメイン名のスキーマを定義する RFC である。
- RFC3983　IRIS over BEEP
  IRIS のやり取りの転送の為に BEEP（Blocks Extensible Exchange Protocol）と呼ばれるトランスポート上のプロトコルで利用するとし、BEEP を定義した RFC である。

Internet-Draft の状況

- Draft-ietf-crisp-iris-areg-09.txt
  アドレス登録情報のスキーマを定義することを目的とした Internet-Draft
- Draft-ietf-crisp-iris-areg-urires-00.txt
  IRIS のアドレスと登録情報のスキーマで使われる URI（Uniformed Resource Identifier）を定義することを目的とした Internet-Draft
- Draft-ietf-crisp-iris-dchk-02.txt
  IRIS のフレームワークを用いてあるドメイン名の存在を確認する簡易なサービスに関する定義を行うことを目的とした Internet-Draft

- Draft-ietf-crisp-iris-lwz-01.txt
  IRIS のための UDP（User Datagram Protocol）を用いたトランスポート（伝送路）の提供の為の定義を行うことを目的とした Internet-Draft

新しい動きについては二つ紹介された。RREG（ルーティング・レジストリのスキーマ)が JPNIC の IRR 企画策定専門家チームによって行われていることと、第 62 回 IETF で RREG に関する議論が行われ、CRISP WG のチャーターの調整が行われることである。

また将来の方向性として CRISP が一方向性の問い合わせ・応答のプロトコルであるのに対し、登録と問い合わせの両方向をサポートするような活動を目指すこと、単一のクライアントで全ての CRISP を使ったレジストリとのやりとりの実現、などが紹介された。詳細は第 20 回 APNIC で示されるとの事であった。

2005 年 2 月 24 日（木）CRISP/EPP BoF が開催された。この BoF は CRISP と EPP（Extensible Provisioning Protocol）に関して、特に IETF CRISP WG の活動の状況について議論を行う BoF である。

この BoF では RREG の標準化と RIR/NIR における取り組みを進めることの必要性や IETF CRISP WG での RREG の扱い方に関して議論が行われた。

インターネットにおける経路情報の正しさを検証する必要性が一部の専門家に指摘されているが、その状況を受けてか、ISP における IRR のサービスが立ち上がりつつある。しかし経路情報の正しさは IP アドレスの割り振り／割り当てと AS 番号の割り当ての正しさに基づいているため JPNIC のようなインターネットレジストリにおける適切な情報公開が肝要になる。APNIC や JPNIC の IRR 企画策定専門家チームでは whois と同様に、登録情報に基づく IRR サービスの提供が、要求されている機能を実現する方法であると考えられている。情報の正確さと規模拡張性の観点から CRISP の利用が重要であるという見方も一致している。

一方、この BoF の APNIC の技術担当者は CRISP WG で RREG を扱うことに関して慎重な態度であった。ルーティングレジストリはアドレスレジストリとは異なるフラットな構造であり、AS のルーティングレジストリにおける登録情報の信頼は歴史的な経緯からインターネットレジストリの構造とは若干異なっている。（例えば米国 Merit による IRR のサービス RADB は、ARIN の役割とは独立している。）

BoF の中で、ルーティングレジストリの機能を RIR や NIR といったインターネットレジストリで検討されることで解決する問題は多くあるという見方が強い。しかし IETF CRISP WG は、このようなモデルの再検討が必要になる可能性に対応できるような長期的なマイルストーンを設けておらず、現在取り組んでいるドメイン名とアドレスのスキーマのドキュメント化を進め当面の目標を達成したいという意図があると感じられた。

Database SIG における RPSLng に関するプレゼンテーションの中で、IETF CRISP WG のチャーターの調整は、必ずしも RREG を含めた目標の拡大であるとは限らない状

況であると考えられた。技術的な観点ではドメイン名のスキーマやアドレスのスキーマと同様に、ルーティングレジストリのスキーマを定義するに留め、サービスや運用方法の取り決めは CRISP WG の活動外とする方法が考えられる。

4.2. RIPE NCC における認証局のマネジメントと登録情報の安全性に関する動向

RIPE NCC では X.509 形式の電子証明書を用いたクライアント認証を既に実施しており、その電子証明書の発行に使われる認証局の運用も実施されている。2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」で述べたように、RIPE NCC では X.509 形式の電子証明書を資源管理の情報を表記する言語 RPSL で記述したデータオブジェクトに組み込む活動を行っている。この活動は既存のアドレス資源管理の手法に新たな認証の機能と加えるという、やり方である。このように書くと特段変わった方法ではないようにも取れるが、例えば APNIC では既存のアドレス資源管理の認証とは分けて管理し、ARIN では既存の認証で使われている識別子を電子証明書に含め、whois などの既存の登録情報には影響させない手法が取られている。

RIPE NCC における認証局のプロジェクトは” Improved Secure Communication System for RIPE NCC Members” * で文書化されている。この文書では PKI の X.509 形式の証明書を使ってコミュニケーションシステムの安全性向上を図るとしている。ただし、認証局の機能を全て満たすようなシステムの提供は目標ではなく、あくまで安全性向上の範囲での構築とされている。そのため認証局に関連するプロジェクトのゴールは認証局の構築を中心としたものではない。

”Improved Secure Communication System for RIPE NCC Members ”で挙げられているゴール

Access to the services and data

The goal in this area is to make communication faster and easier by introducing stronger and more uniform security mechanisms. This will make it easier for the user to maintain and use their security tokens and will allow the seamless use of some of the advanced interfaces (such as web-based interfaces) with strong security support.

Privilege management

The system will provide unified privilege management support for the users. X.509 PKI certificates used in the system as security tokens have intrinsic revocation and expiry mechanisms that, together with support for their maintenance, make the system less vulnerable.

Minimal deployment and maintenance efforts for the users

Based on an industry standard and being well deployed in commercial and open source software, the communication system will require no additional client-side software.

「**Access to the services and data**」における「より強固で統合化された認証」は X.509 形式の証明書を、現行の資源管理機構における認証方式の選択手法の中で利用していく方針であることがわかる。また「**Privilege management**」での権限管理は、資源管理のために使われている RPSL を使って行われることがわかる。「**Minimal deployment and maintenance efforts for the users**」は、クライアント側に Web ブラウザ等の多くの環境で利用可能なプログラムを用い、それらの改良や開発が必要ない状況を目標にしていることがわかる。

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」で、RIPE NCC が whois データベースに登録された証明書を認証に利用する方式を採用したことを報告した。この方式では、ユーザが LIRPortal 等の Web のシステムにアクセスしたときに、そこで提示されたクライアント証明書の検証で PKI のパス検証行わない。そこで提示された証明書が whois データベースに事前に格納されていれば認証が成功する方式である。これは RPSL の key-cert クラスと呼ばれるデータ形式で whois データベースに証明書を格納して実現している。

なお、JPNIC における認証局の取り組みは、key-cert クラスを用いた手法を除き、RIPE NCC における「既存の登録情報の扱い方を生かした新しい認証技術の導入」という手法に似ている。JPNIC では既存の登録情報の管理形態を引き継ぎつつ新たな PKI を用いた認証の機構を導入している。

本調査研究では、2004 年度 RIPE ミーティングに参加し、実際に認証局のプロジェクトを進めた技術担当者との個別のミーティングを行った。また他の RIR のミーティングで行われた RIPE NCC の近況報告を入手し、調査を行った。

■RIPE NCC CA の動向

2005 年 2 月に行われた第 19 回 APNIC ミーティングで、RIPE NCC の whois データベースソフトウェアの近況についてプレゼンテーションが行われた。なお RIPE NCC における認証局機能は whois データベースソフトウェアの一環として位置づけられている。

このプレゼンテーションで述べられた認証機能に関する報告を以下に示す。

X.509 Support
- KEY-CERT class changed
- Update mechanisms updated
  - E-mail supports S/MIME
  - webupdates/syncupdates support client SSL certificates

Organization Object Type

NONE Authentication Deprecated

X.509 Support は、X.509 形式の証明書を使った認証に関するデータベースと登録情報の変更機構の改良である。key-cert クラスはユーザが証明書を格納するために使われるデータ構造で、今回の変更で認証方式を指定する method のフィールドで key-cert クラスの識別子を指定する書式が若干変更された。また自動登録の機能が実現された。RIPE NCC の認証局にクライアント証明書を発行してもらった場合に、自動的に key-cert クラスのオブジェクトが登録されるようになった。以前は証明書の発行後にユーザが登録操作を行う必要があり、RIPE NCC の担当者の間では証明書の利用を複雑にする要因と位置づけられていた。

Update mechanism の E-mail supports S/MIME とは、暗号化された電子メールを使った申請の受付が可能になったことである。RIPE NCC の whois データベースは key-cert クラスを使って証明書の格納とアドレス資源の管理権限の管理を一元化しており、LIR（日本の ISP にあたる）は Web を利用するシステムである LIRPortal を使っても、S/MIME を使った電子メールのどちらでも、同じアドレス資源に関する申請／情報変更業務を行うことができる。Webupdates は Web を使ったデータベース操作のインターフェースで、LIR が RPSL で表現されたデータ・オブジェクトを個別に生成／変更する方法で登録情報を変更することができる。このシステムでもクライアント証明書を用いたクライアント認証を利用することになった。

NONE Authentication Deprecated は、認証方式に”none”（なし）が指定されている登録情報の削除に関する活動内容の説明である。認証方式が”none”に指定されており、また管理情報のメンテナが存在しない場合には、その登録情報を変更することができなくなり、新しいメンテナを生成するための連絡先が通知される。認証方式が”none”でメンテナが存在する場合は新たにパスワードが設定される。

次に第 49 回 RIPE ミーティングで行った調査について述べる。

■認証局に関する情報交換

2004 年 9 月 20 日（月）～2004 年 9 月 24 日（金）に行われた第 49 回 RIPE ミーティングで、RIPE NCC の認証技術と whois データベースの技術を担当しているソフトウェア・マネージャーと RIPE NCC の認証局関連の技術担当者を交えて、認証局と登録情報における認証に関する個別のミーティングを行った。

個別ミーティングのアジェンダ（議題）を以下に示す。

認証局に関する個別ミーティングの議題

- JPNIC CA Updates
  CP/CPS ドラフト、プロジェクトに関する意見交換
- CA management model
  認証局システムに関する意見交換
- One big picture
  RIR と NIR における登録情報のセキュリティレベル／アドレス情報に基づく証明基盤
- A Protection mechanism in RPSL
  big picture 実現の為の手法

個別ミーティングでは、はじめに JPNIC の IP アドレス認証局に関する意見交換を行った。

前回情報交換を行った第 46 回 RIPE ミーティングでの個別ミーティング以降、JPNIC では CPS のドラフトと CA プロジェクトの進行等が変わった部分となる。先方が興味を持った点は、CPS の作成にかかる期間である。IP アドレス認証局の CPS のドラフトには約 6 ヶ月かかっている。

CA management model は、2003 年度に行われた IP アドレス認証局のマネジメントに関する調査研究の一環として定義された認証業務のモデルに関する情報交換である。これは External RA（外部 RA）と呼ばれるもので、LIR に所属するユーザ（業務責任者等）がその管理下のユーザアカウント（申請業務を行う業務担当者等）の作成／管理を行うことができる。

このモデルと、このモデルに基づいてドラフトされた CPS に関して情報提供を行い、意見交換を行った。モデルに関しては興味を持って頂いた様子で、特に問題点の指摘はなかった。APNIC や ARIN の認証局で External RA のモデルを採用している例をみないため、同じレジストリの認証機構として受け入れにくいという意見が上がる可能性を考えていたが、特に問題はないことが確認できた。

One big picture は、インターネットレジストリにおける PKI の活用に関する意見交換である。これは JPNIC における IP アドレス認証局の調査研究を通じて練ってきた構想を紹介し、意見を頂くという主旨で行った。これに対し、彼らはこの構想の整理の仕方に興味を持ち、特に登録情報の正当性を確認する（電子署名等の）方式がないという問題意識の共有を行うことができた。その際に、全体の構想を NRO（Number Resource Organization）に持ちかけてはどうか、という意見を頂いた。本調査研究ではそこまで活動を行うことはできなかったが、ICANN をはじめアドレス資源管理の安全性向上の必要性がいくつかの団体から指摘されていることから、インターネットレジストリ全体

の取り組みとして捉えるための活動があると有効であると考えられる。

本構想について意見交換を行った内容を以下に示す。

ここではインターネットレジストリのアドレス資源管理構造に、PKI のツリー構造を当てはめ、割り振り／割り当てに対してアドレス資源の利用権利の証明と、インターネットレジストリが発行した証明書を使ってユーザ間またはホスト間の認証を行うという概念を説明している。

この概念の実現には、登録情報のミラーの機構、証明と検証の機構、登録手続きの安全かの三つが必要であるとしている。

Components

- Good mechanism for mirroring and referring
  - CRISP / RPSL
  - whois?
- Good mechanism for certification and verification
  - We don't have yet.
    - https and server certificate is not suitable for us I think.
- Making registration process secure
  - strong authentication (certificate and PGP)

Japan Network Information Center　17

登録情報のミラーの機構にはRPSLを使ったアドレス資源管理情報の統一的な表現や、CRISP を使った透過的な参照を可能にする検索が必要になる。証明と検証の機構には、まだ適切なものがないがインターネットレジストリが発行している証明書を使い、登録情報に電子署名を施す手法が候補として挙げられる。最後の登録手続きの安全化は、LIR によって実施される登録プロセスに強い認証機構を導入することである。ここでは証明書と PGP を挙げている。

Assuming users

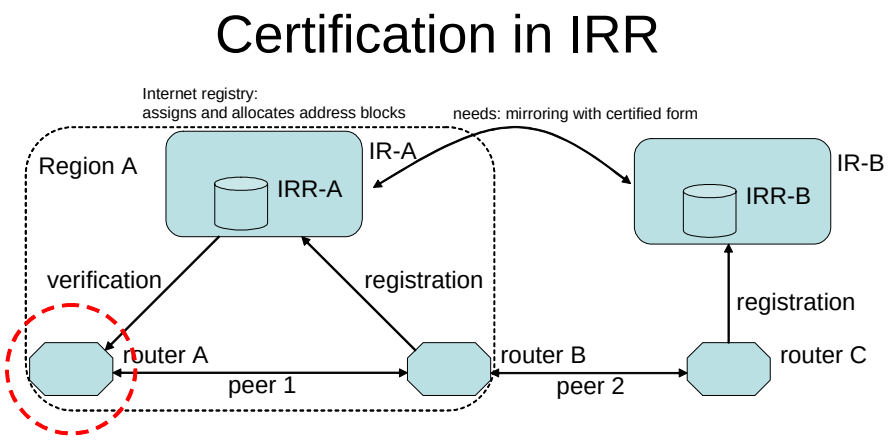
- Users
  - LIRs in World Wide
    - for secure routing in global level
      - e.g. S-BGP, soBGP
  - Service Providers
    - for verifying and controlling access
      - e.g. commercial CA, CDN, small but many IPv6 nodes
  - Incident Response Team

⇒ They all use registered information (objects in RPSL).

Japan Network Information Center 18

ここでは本構想で構築される認証基盤のユーザを想定している。まず全世界の LIR が挙げられる。これはグローバル・インターネットにおける安全なルーティングの実現には、インターネットレジストリの登録情報である割り振り／割り当て情報が必要になるためである。ルーティング情報をやり取りするプロトコルの安全性向上に関しては、S-BGP や soBGP を利用するという例を挙げている。

更に、登録情報に関する証明と検証の例を、IRR を使って説明を行った。なお、この機構はまだ標準化等は一切されておらず、本調査研究の一環で構想として練られただけの状態である。（次頁図）



ここでは RIR や NIR で運用されている IRR が、登録情報のミラーリングを行っている状況を前提としている。IRR-A に互いの登録情報を持つ router A と router B は、互いの流す経路情報の正当性を IRR-A を使って確認することができる。しかし IRR-B に登録されている router C が流す経路情報の正しさを検証するには IRR-B から IRR-A にミラーリングされた情報を検証することになる。ミラーリング（情報のコピー）が行われる状況で、その情報に改ざんがないか、登録者が誰であるかといった検証を行うことが必要になる。

次頁の図は、IRR の登録情報における登録者が意図しない変更（unintended）の場合わけを行っている。

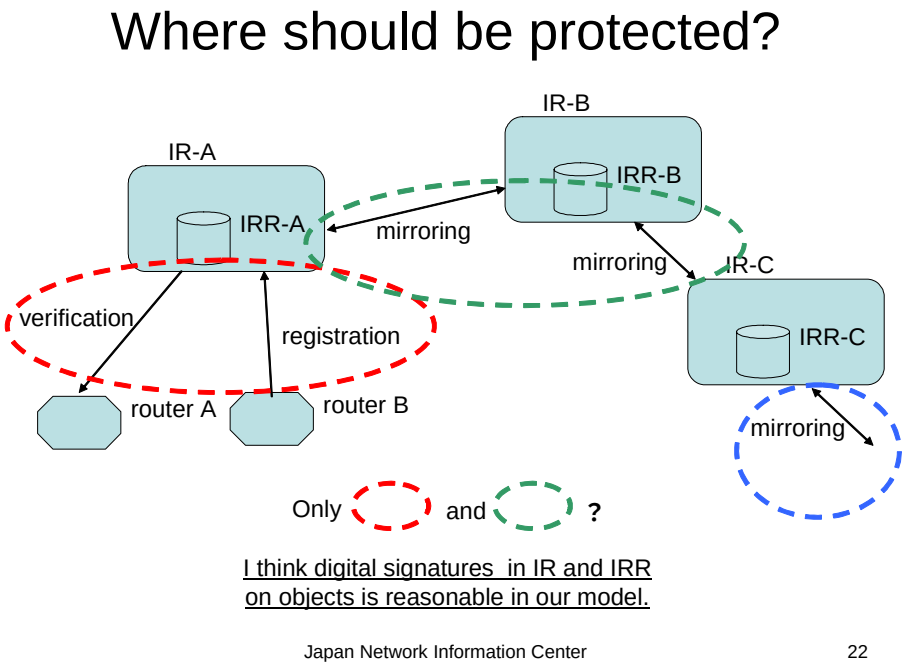
Unintended modifications

- Registered data it self
  - deletes, modifications in DB
    - Disasters
    - Dugs in servers/clients
    - Impersonation for legitimate users
- Unintended modifications on transferring data
  - spoofing (servers, clients)
  - man-in-the-middle attack
  - modifying in mirroring

⇒ We should have a mechanism which can let us know these modifications.

Japan Network Information Center 21

サーバの成りすまし（spoofing)、マン・イン・ザ・ミドル攻撃、ミラーリングされた情報の改ざんがあるような状況では、サーバ認証やクライアント認証ではメッセージの正当性を守ることはできない。従って少なくともメッセージが元々の状態から変更されていることが検出できる仕組みが必要になる（次頁の図)。



この情報共有の後、この同じ構想もしくは同じ問題意識を持つことと、それぞれの問題解決を行う準備を行うことについて呼びかけた。彼らは、このモデルは単一のレジストリが取り組む問題でないと考え、NRO で提案することを進めてくれた。

2005 年度の本調査研究ではそこまで活動を行うことができなかったが、今後 NRO 等を通じた包括的な取り組みが可能であればより効率的に各 RIR がセキュリティに関するプロジェクトを推進できるのではないかと考えられる。

■RIPE NCC の認証局の証明書発行数

第 49 回 RIPE ミーティングの個別ミーティングの後、RIPE NCC の認証局の運用状況について質問を行った。特にクライアント証明書の発行数をたずねたところ、調査して頂いた上で回答を頂くことができた。2004 年 10 月現在 766 のクライアント証明書が失効されずに有効な状態であるとのことである。

■第 49 回 RIPE ミーティングのアジェンダに見るネットワークセキュリティの動向

RIPE ミーティングには European Operators Forum（略称 EOF）と呼ばれるオペレータの情報交換の場が設けられている。EOF は各 RIPE ミーティングの主に初日に行われ、ネットワーク運用の近況報告や話題提供が行われている。

第 49 回 RIPE ミーティングの EOF のアジェンダを以下に示す。

Monday, 20 September 2004
16:00 - 17:30 The Peering Simulation Game
Tuesday, 21 September 2004
09:00 - 10.30 Core Network SecurityTutorial
11.00 - 12.30 Core Network Security Tutorial (continued), Discussion

「The Peering Simulation Game」は参加者が ISP となり、ISP のピア（ISP 同士の一対一の接続）や IX の形成を通じてネットワークの形成を体験するゲームである。小規模な ISP が大規模な（提供地域の多い）ISP とピアを形成すると莫大な費用がかかるため、早期に協力して IX を形成するほうが全体の提供範囲を広げやすいといった状況を体験することができる。

「Core Network Security Tutorial」はサービスプロバイダのコア・ネットワークにおけるセキュリティに関するチュートリアルである。コア・ネットワークはユーザのコピューターが接続されるネットワークからの不正な通信を想定した ACL（Access Control List）の設定が必要になる。また意図どおりのルーティングを維持するために、経路情報を交換するプロトコルの安全性をいかに確保するかが課題となる。

ミーティング全体では、Anti-SPAM をはじめ Database、RIPE NCC Services でスパムに関する議論が活発に行われた。RIPE NCC におけるスパムの議論は、主に登録情報を利用したスパムメールを阻止する観点で行われている。特に第 49 回の Database のセッションでは、whois の検索結果において連絡先のメールアドレスを表示することがスパム防止の観点でよくない、という問題意識を確認した上で、いかに連絡先情報の提供を行うべきか、という議論が行われた。

連絡先情報は、whois を使ってだれもが調べることができ、またネットワークの不具合に対応する目的の連絡先であることから、スパムが発生したときの連絡先に使われやすい。しかしアドレス資源の管理とスパム対応とは必ずしも同じ連絡先ではない。ネットワーク管理の観点ではネットワーク運用に関わる重要なメールがスパム対応のメールにうまってしまっては意味がない。

Anti-SPAM WG のセッションでは、下記の提案が既に受け入れられていることが確認された。

A. IRT-object に abuse-mail を含めること、PGP 等の認証の必須条件なくすこと。
もしくは新しい似た働きを持つオブジェクトを導入すること。
B. whois のデフォルトの動作において abuse のメールアドレスを表示し、
そのアドレスが一つであるならばその他のアドレスを表示しないこと

更にネットワーク情報（inetnum, inet6num, route の各オブジェクト）の検索結果に含まれていたメールアドレスをデフォルトでは表示しないこと、person オブジェクトや role オブジェクトには abuse-email というフィールドを設け、表示される連絡先がスパム対応の目的であることを明示するという提案がなされた。

■第 49 回 RIPE ミーティング全体を通じて

本節では第 49 回 RIPE ミーティングのこれまでに述べた以外の話題を含め全体について述べる。

○概要

第 49 回 RIPE ミーティングは 2004 年 9 月 20 日(月)～9 月 24 日(金)、イギリスのマンチェスターで行われた。RIPE ミーティングは、ヨーロッパ地域のレジストリである RIPE NCC が定期的に開催しているミーティングで、アドレスポリシーを始め、レジストリシステムや IPv6、Routing 等について議論が行われる。

Working Group Agenda
http://www.ripe.net/ripe/meetings/ripe-49/agendas/index.html

■RIPE NCC スタッフとの個別ミーティング

2004 年 9 月 21 日(火) 9:00 から 1 時間 40 分にわたり、RIPE NCC の認証局関連業務の担当者と個別のミーティングを行った。

このミーティングは、RIR の認証局に関する情報交換とネットワーク・セキュリティの為のレジストリの役割について議論することを目的としたものである。認証局に関する情報交換は、第 46 回 RIPE ミーティングの際のミーティングで行ったことがあるため、今回はそれ以降の活動の情報交換が主な話題となった。今回はそれに加えて、インターネットレジストリによる証明基盤の構築に関して話し合った。

このミーティングを通じて、類似する問題に取り組んでいることや、問題解決の際に共通に重点をおいた点などを相互に確認することができた。また JPNIC にて構想中のアドレス資源に基づく証明基盤について、NRO で提案してはどうかといったアドバイスを頂くことができた。

第 49 回 RIPE ミーティングでは、各 WG セッションにおけるレジストリのセキュリティに関連する話題についての情報収集を行った。

■Opening Plenary, RIPE NCC Services

開催の挨拶の後、RIPE ミーティングのコスト、RIPE NCC からの Update、WG からの話題の紹介が行われた。

RIPE NCC からの Update の中では、IANA への大きな IPv6 アドレスブロックの割り振り（承認）、AfriNIC への業務移転、レジストリシステムの LIRPortal の Organization オブジェクトの追加などが報告された。また新しいプロジェクトである AS 番号に関する Web インターフェースである myASN を始め、X.509 証明書の LIRPortal での扱いの変更、IRRToolsSet の ISC への移管、k ルートサーバの IPv6 対応などがプレゼンテーションされた。

X.509 証明書の LIRPortal での扱いの変更については、第 46 回 RIPE ミーティングで提案された方式が LIRPortal で実施されたとの報告があった。この方式は RIPE NCC の CA 以外の CA から発行された証明書であっても Database に登録することで認証に利用されるというものである。

■WG セッション

今回の RIPE ミーティングでは、WG セッションは概ね 2 つが平行して行われた。以下に各 WG セッションの概要とポイントを簡潔に報告する。

○Routing WG

Routing WG は 9/21 16:00 と 9/22 11:00 の二回セッションが開かれた。最初のセッションは EOF で行われたチュートリアルに関する議論と BGP を使ったマルチホームの陥りやすいミス、日本の NICT（情報通信研究機構）の研究員の方による経路情報の不安定性をモニタするツールの紹介が行われた。

○EIX WG

EIX はヨーロッパの IX 運営に関する WG である。はじめに、各 IX（AMSIX、DE-CIX、LINX、LoNAP、MIX、Netnod、NIX.CZ、VIX、XchangePoint、NAP ofthe Americas）による近況報告が行われた。

このセッションの最後には KIX(Korean Internet eXchange)による報告が行われていた。参考事例としてのプレゼンテーションのようである。会場からは ISP 事業はあるのか、韓国国内 IX との関係などの質問が挙がっていた。

○IPv6 WG

IPv6 WG は、IPv6 に関わる各種話題を扱う WG である。このセッションでは

Global IPv6 routing table status、v6 traffic volume に関する話題、大きな IPv6 アドレスブロックの割り振りに関する話題、IPv6 アドレスの割り当てに関する話題などがアジェンダに挙がっていた。

セッションの後半では、IETF で提案されている IPv6 を使ったマルチホームの新しい手法の紹介が行われていた。

○Anti-SPAM WG

Anti-SPAM WG は、RIPE NCC のコミュニケーションサービス（RIPE NCC の提供する ML や whois）において SPAM メールを抑止する方針・方法について議論を行う WG である。

今回のセッションでは、"Database WG に対する要望事項(Request to Database WG)"がまとめられた。その内容を要約すると以下のようになる。

- アドレスの割り振りにおける abuse contact の利用可能性の向上に対してなるべく早くアクションを起こすこと。

既に提案されている方法で受け入れられるもの：

A. IRT-object に abuse-mail を含めること、PGP 等の認証の必須条件をなくすこと。もしくは新しい似た働きを持つオブジェクトを導入すること。
B. whois のデフォルトの動作において abuse のメールアドレスを表示し、そのアドレスが一つであるならばその他のアドレスを表示しないこと

この他に、LINX によって出されている BCP の update[ube]の紹介、IETF で提案されている MARID や PRA、SPF といった手法の紹介などが行われた。

[ube] New LINX BCP v2.0
http://www.linx.net/noncore/bcp/ube-bcp-v2_0.html

○Database WG

Database WG は RIPE NCC のレジストリシステムと whois や RPSL に関する議論を行う WG である。このセッションは以下のアジェンダに沿って進められた。

1. DB Operational Update
2. ERX Report [196/8, 198/8]
3. IRRToolSet software maintenance

4. Routing Registry Courses
5. CRISP Update
6. IRT / Abuse-c roundup

セキュリティ事業に特に関連のあるセッションであるため、それぞれの話題について報告する。

1. DB Operational Update

   RIPE NCC における Database の運用報告である。統計上の大きな動きとして、inet6num(IPv6 アドレスブロックの割り振り情報)が 7400 あり、年間で 100%以上の伸び率(倍増以上)であること、そのうち 85%が割り当て済みであることなどが紹介された。また統計資料が公開された。

   その他に、whois サーバの性能向上の為、問い合わせ／参照のみのサーバを増加させてロードバランスを行い、update 等の操作を行うためのサーバをバックエンドの扱いとすることなどが紹介された。

   RIPE NCC のデータベースで使われているメンテナーオブジェクトのセキュリティモデルが変更されるとの報告があった。現在はだれでもこのオブジェクトを作成することができる。ハイジャックを防ぐため、セキュリティモデルを変更し、認証方式の mail-from や none を削除すること、mnt-lower フィールドをデフォルトでは mnt-by にするとのことであった。

   その他に、"AUTO-" を使った参照がすべて行われるようになったこと、認証方式を指定する auth のオブジェクトからそれを含む検索（逆の検索）ができるようになったこと、PGP の fingerprint を格納する fingerpr 欄が検索できるようになったことといった変更があった。

   各プロジェクトの進行についての報告も行われた。

   ・RPSLng

   今までは対応していなかった RPSLng に対応したこと、IETF の Internet-Draft が RFC Editor の編集待ちになったこと（すなわち IESG の承認は既にあり、RFC になることが決まっている）などが報告された。

   ・rERX 及び Afritrans

   ERX および Afiritrans（AfriNIC へのアドレスブロックの移転）を進めるプロジェクトの説明。

・KEY-CERT/MNTNER LIR Portal Integration

第 46 回 RIPE ミーティングで提案された、X.509 証明書のデータベースへの登録手続きの改善に関する報告。これまでは証明書の発行とデータベースへの登録が別の手順で利便性が低かった。（登録数が少ない(担当者によると 20 程度)のはことため、という見解であった）新たに導入された方法では、RIPE NCC の認証局を使って証明書を発行すると、自動的に key-cert オブジェクトが生成される。

2. ERX Report

〜 Early Registration TransferStage 3 -“ Class C ” space 〜

ERX の進行状況の報告である。AS 番号の移管は 2002 年 8 月に始まり、IPv4 アドレスの移管は 2002 年 12 月に始まっている。2004 年 4 月までにいわゆるクラス B は、48 (/8) が移管されており、いわゆるクラス C は 196/8 と 198/8 が 2004 年 7 月に開始、合計で 1964 が移管されている。

いわゆるクラス C の移管は、192/8, 196/8 & 198/8 であと 3000 以上が残っている。これらの移管を進める "Stage 3" では、メールの送信の必要がない Web のシステムを使い、レスポンスを早くするとのことである。このシステムやプロジェクトについては[erx-ip]および[db-erx]から資料を入手することができる。

[erx-ip] Project Web Page

http://www.ripe.net/db/erx/erx-ip/

[db-erx] Project Outline

http://www.ripe.net/ripe/meetings/archive/ripe-44/presentations/ripe44-db-erx/

3. IRRToolSet software maintenance

whois のプログラムセットである IRRToolSet は、もともと ISI によって開発されたもので（当時 RAToolSet と呼ばれていた）RIPE NCC に移管されたものであった。しかしソフトウェアの質の向上とソースコードの公開の為、ISC に移管しオープンソースプロジェクトとして進めることになった。

この移管は既に進んでおり、ソースコードのリポジトリ、ML、Web などの移動は終わっているとの事である。またこの機会に RPSLng への対応、各種バグフィックス、パッチの適用、gcc 3.x でのコンパイル対応などを済ませたとの報告があった。

4. Routing Registry Courses

IRR の利用法の説明会の実施報告である。2004 年には 16 回行われた。2005 年は、ドイツ、スペイン、ロシア、オランダ、イギリス、フランスで開催される予定である。資料などは[training-rr]から入手することができる。

[training-rr] Material & Info
http://www.ripe.net/training/rr/

5. CRISP Update

IETF で標準化作業が進んでいる CRISP(Cross-Registry Information Service Protocol)に関する状況報告が資料に沿って行われた。概要は以下の通りである。

・IETF CRISP WG の紹介
・whois に代わるもので、構造化されている
・IRIS の紹介
・whois と IRIS の違い
　－mntner, irt オブジェクトの情報がない
　－import:, export: といった経路情報がない
・VeriSign のリファレンス実装を使ったプロトタイプなどの今後の活動。

このプレゼンテーションの発表者は、IETF CRISP WG において IP アドレスを AS 番号の書式の提案を行っている。この資料は CRISP と whois の違いを理解する上でわかりやすい。

6. IRT / Abuse-c roundup

データベースにおける IRT オブジェクト／abuse-c の追加に関する議論が紹介された。いくつかの選択肢が紹介されたため、事後に発表者に意見を聞いてみると、mail-abuse の追加が現実的だという見解であった。

○DNS

DNS WG では、RIPE NCC に関連する DNS の話題（登録情報や AAAA レコード等）についての議論を行っている。WG セッションでは、IETF レポートとして DNSEXT WG および DNSOP WG の報告、MARID、CRISP（ドメイン名）の状況報告が行われた。その他には k ルートサーバに関する報告、SiteFinder に関する報告、BIND に関する報告などが行われていた。

○ENUM

ENUM WG は ENUM に関する各種の話題を扱う WG である。各国の ENUM プロジェクトの状況をまとめたり、ENUM 利用に関する報告を行うフォーラムを開催したりしている。今回のセッションでは集められた質問集に関する議論（ここではインフラストラクチャ ENUM は扱わない）やスウェーデンとイギリスで行われたプレゼンテーションの紹介が行われた。

○RIPE NCC Services

RIPE NCC Services WG は、RIPE NCC の提供するサービスについて包括的に扱う WG である。今回は RIPE NCC の提供する ML における Anti-SPAM の観測や、RIPE NCC の会計に関する方針、トレーニングに関する報告が行われた。

RIPE NCC の会計報告では、2004 年度までの収入構造と評価方針と 2005 年度以降の変更とそれに伴う料金の変更などが説明された。

○Address Policy

Address Policy WG のセッションでは、RIPE NCC および ICANN ASO AC の報告のほかに、ポリシー策定プロセスに関する議論と、IPv6 の初期割り振り、IPv6 の IANA から RIR への割り振りの方針などに関するプレゼンテーションが行われた。また whois への登録の必要性とプライバシーに関する議論が行われた。

4.3. ARIN における認証局マネジメントの動向

ARIN（American Registry of Internet Numbers）における認証局のマネジメントの動向に関する情報収集の為、第 14 回 ARIN ミーティングに参加し、また認証局の担当者と個別のミーティング（ヒアリング）を行った。

■ARIN CA の動向

ARIN CA の目的はアドレス資源に関する申請者の、ARIN による認証を実現することとしている。ユーザ同士の認証を想定しておらず、また ARIN が用意した Web サーバ等の申請者による認証（サーバ認証）を想定していない。公開されている CPS によると https を使ったクライアント認証も想定していない模様である。
第 14 回 ARIN ミーティングは、この認証局を用いた申請業務の方法に関するチュートリアルが行われた。

はじめに ARIN の認証局に関して Web 等を通じて調査した認証業務の内容を述べる。

○ARIN における証明書

POC *1 の認証を行うための証明書である。POC とは Point of Contact の略で、RSA (Registration Services Agreement) に合意した組織が予め登録している Admin(管理責任者)もしくは Tech(技術担当者)の POC であるユーザが利用することができる。

POC Template:
http://www.arin.net/library/templates/poc.txt

ARIN が登録している POC アカウントには、複数のユーザが利用可能である role アカウントと個々のユーザに対する個別アカウントの二種類がある。証明書の発行対象となるのは、個別アカウントとして登録された Admin POC といずれの種類の Tech POC である。

○証明書発行対象の認証

証明書の発行要求を出すユーザに対して、三種類の情報の提示を求め、有効性が確認できた場合に証明書の発行を行っている。三種類の情報とは政府によって発行された個人証明と組織の証明、組織と個人の関係を証明する情報である。

○証明書の用途

証明書は、申請書であるメールに対する電子署名に用いることができる。ARIN では、現在これ以外の用途を想定していない。申請書における電子署名によって、

転送中のメールに対する改変や本物であること(genuine)を確認できるものとしている。

○申請方法

Web ページ http://ca.arin.net/request/ にアクセスし Web ブラウザの証明書申請機能を用いて申請を行う。Web ブラウザを利用しない場合には Web ページから入手できる CERT-REQUEST 書式を使って申請を行う。その場合には OpenSSL 等を利用して、ユーザ自身が CSR (Certificate Signing Request) を生成する。

申請に利用できる Web ブラウザについては、テストされた Web ブラウザという形で情報提供がされている。テストされたブラウザは Internet Explorer と Mozilla である。Opera も利用可能だが、証明書を扱う機能はまだ不十分であり推奨されていない。w3m の利用も可能であるという記述がされている。

○証明書の入手

証明書の発行が行われると、Web 経由か電子メールで入手することができるようになる。

○証明書の共有

role アカウント間で証明書を共用してもよいが、role アカウントに含まれる個別アカウントに対する証明書発行も行う。それぞれリクエストに対する署名が複数の人によってできてしまうというリスクと、最初の証明書保持者が残りの証明書リクエストフォームに署名する必要があるという欠点が説明されている。

○証明書の利用に先立つ ARIN CA 証明書の登録

証明書の配布のあと、MUA(Mail User Agent - メールソフト)への組み込みに先立って、ARIN CA 証明書の組み込みをする必要がある。

FAQ では、Internet Explorer と Netscape など、証明書リポジトリを共有していて、Web ブラウザへの証明書の CA 証明書の組み込みによって、メールソフトでのユーザの証明書の利用が可能になるものについての説明がある。しかし証明書とメールソフトの利用方法などの個別の説明は、多種のメールソフトが存在するという理由で、行われていない。

○申請書類を生成するスクリプトの利用

多くのユーザが申請書類の生成にスクリプトを使っているようで、スクリプトを使って電子署名を利用する方法についての説明が提供されようとしている。ただし現在は例示のタイトルがあるものの、文書自体はまだ提供されていない。

○MAIL-FROM の共用

FAQ によると、一度証明書の利用に移行したユーザは MAIL-FROM による申請書の送信はできなくなる。

○証明書について

有効期限は 2 年間。ARIN では有効期限が近くなると更新をメールで知らせるとしている。

○証明書の更新

有効な証明書を使って署名された更新の申請が行われた場合、再度書類を用いた本人確認を行う必要はない。なお証明書の有効期限が切れ、かつ証明書の更新が行われていない場合にも MAIL-FROM を利用できるようにはならない。

○証明書の紛失

証明書を紛失した場合には、ヘルプデスクに連絡することになっている。ヘルプデスクはメールに加え電話による問い合わせにも対応している。

○認証局の鍵更新

CA 証明書の EE への配布によって、証明書の秘密鍵の危殆化の影響を最小化するため、ARIN CA は 6 ヶ月おきに鍵生成を行う。CA 証明書は 3 年間の有効期限を持っているため、最大で 6 つの CA 証明書が存在することになる。

EE 証明書は 6 ヶ月おきに異なる CA 証明書から発行されることになるが、CA 証明書の危殆化の影響（再発行対象の証明書数）は最大で 6 分の 1 になる。

参考文献：
Certificate Cryptographic Authentication at ARIN - FAQ
http://www.arin.net/CA/ca_faq.html

■ARIN の認証局担当者のヒアリング

第 14 回 ARIN ミーティングの期間中、認証局構築の担当者と個別のミーティングを行うことができた。

ヒアリングの内容と結果を以下に述べる。

ヒアリング内容は大きく 4 つに分類される。

○ARIN PKI

認証局自体に関する質問である。認証局には、証明書の発行に関わる認証業務とそのためのシステムという二つの側面を持っていると考えられる。またポリシーの公表による責任分解／問題対応の方針を明らかにするという活動も関連する。

CPS の記述内容を元に ARI CA の特徴のある点､運用の内容についてヒアリングを行った。質問内容を以下に示す。

認証業務の運用人員について

RA(hostmaster) 1 名、他に発行担当者と技術者がいる。管理者は他のシステムと共用で、特定の人員ではない。

認証局の証明書をサイクルする手法について

CA の秘密鍵の危殆化の影響を最小化するための方法。CPS 4.7 の記述に詳しい。

CA 証明書の配布

CA の信頼性に依存して証明書の検証を行う Relying Party が ARIN だけである､という設計に従い､CA 証明書を EE 側で検証する必要はない｡Relying Party については CPS への記述されている。

ユーザ自身の登録に関する安全性の提供の意味はなく、ARIN 側からユーザの認証を強化し、ARIN 側にとっての安全性向上のみを目的としている。

認証局システムについて

基本的にオープンソースソフトウェアを用いている。申請などのメールを受け付けるメールと､認証局の連携のためのソフトウェアは ARIN 内部で開発されたプログラムを用いている。

運用方法は、hostmaster である RA が USB ドングル（鍵ペアと X.509 証明書を格納できるハードウェアトークン）を用いて鍵生成を行い、認証局の運用担当者に渡す、認証局の運用担当者はそれに格納された証明書への署名を行う。つまり認証局側ではメンバかどうかの確認などは行わない。このモデルは APNIC CA の運用モデルを参考にしたとのことであった。

○データベース

電子証明書を既存の業務の認証や電子署名に用いる場合、既存の業務システムと

の連携が必要になる。認証局は既存の業務システムのユーザ管理とは独立して運用されるため、二つのシステムを如何に連携するか、がポイントになる。

主に二つのシステムの設計の中で留意した点についてインタビューを行った。

質問内容を以下に示す。

ユーザ数の上限について

ユーザ数の上限に関する想定は行っていない。理論的には上限値はない。

認可機構について。RPSL を利用しているか。

RPSL のような認可機構は持っていない。RPSL には組織の概念がないが、ARIN では組織を基準にした認可構造を持っており、メンバである組織に関係付けられたユーザ(POC)の特定を元に権限が検証される。

◯ユーザの認証

電子証明書の発行対象であるユーザの認証方法は、認証業務の強度に影響する。またユーザ数の見込みは、認証局システムと業務運用の継続性に影響する。ARIN CA の設計の上でユーザについての想定についてインタビューを行った。またチュートリアル（後述）の内容が充実していたため、ユーザ教育についての質問を行った。質問内容を以下に示す。

ユーザの登録について

CPS には 3 種類の書類が必要であるという記述ある。具体的な書類の内容は明らかにせず、メンバ組織の歴史的な信頼性に基づいて適宜選択されるとのことであった。アドレス資源の多くを管理しており、長期間メンバである組織のユーザの登録は、そうではない組織のユーザの登録よりも簡易かつ少ない確認によって行うとしている。

証明書とユーザに関する予測

新規プロジェクトであるため、事前に規模の想定を行った。説明会を通じて興味を持つユーザがどれくらいいるかの検討を行ってきた、との事であった。

ユーザの教育と証明書ユーザの確保について

ユーザの教育と、証明書ユーザの増加に関する既存の計画についての質問である。これに対し、メンバミーティングでの認証局プロジェクトについて説明を行ったり興味を持つユーザに対するダイレクトメールで連絡を行ったりしたとのことであった。

議論を重ね、ユーザにとってできる限りシンプルな利用法になるように留意した

とのことである。

○実験的な活動

インターネット・レジストリにおける PKI の利用は、アドレス資源の登録内容に応じた認証基盤の構築にも繋がる活動と捉えることができる。APNIC, RIPE NCC における、PKI を用いた BGP の安全化の検討と同様に、ARIN において実験的な活動が行われているかについてインタビューを行った。質問内容を以下に示す。

soBGP や S-BGP といった新しいプロトコルに関連するプロジェクトについて

この認証局に関連しては、実験的なプロジェクトの活動はないとのことであった。この認証局は ARIN によるメンバの認証のみを目的としており、他の用途は禁止している。従ってメンバ同士の認証を伴う BGP での利用はできない。またもしそのようなプロジェクトを実施するにしても、この認証局を利用せず別の認証局を必要とするとのことであった。

○インタビュー結果を受けて

ARIN 認証局の大きな特徴は、やはり証明書の用途の限定であろう。ARIN 側のユーザ認証であること、電子メールのメッセージを使った認証であることの二つである。これによって CA 証明書のユーザへの確実な配布の手段を検討する必要がなくなる。一方、ユーザの登録情報に対する信頼性、実態としての ARIN が設置するサーバやメッセージの電子的な認証は、今の段階では達せられていない。情報登録必要な認証はレジストリによる登録者の認証だけでよいのか、やや疑問に残る点はある。

JPNIC の認証局システムの設計と導入に関して参考になった点は、特に運用面である。証明書の用途をシステムの認証に限定する方針にすることで CA 証明書の配布の問題が少なくなる点である。これはメッセージ認証（S/MIME 利用）を利用目的としている為に実現できると考えられる。Web サーバの場合には man in the middle 攻撃を避ける意味で相互認証を想定する必要がある。

■登録情報におけるセキュリティの動向

次に第 14 回 ARIN ミーティングの期間中に行われたチュートリアルについて述べる。このチュートリアルは「暗号技術を用いた認証のチュートリアル」と題して ARIN の認証局担当者自身によって行われた。

チュートリアルの資料は

http://www.arin.net/library/minutes/ARIN_XIV/tut.html

より入手できる。

このチュートリアルは利用者を対象にしており、具体的な利用方法を説明することを

目的としている様子であった。概要を以下に示す。

暗号技術を用いた認証のチュートリアル概要

- X.509 を使った保護機能
- 証明書の要求方法
- 識別処理とプライバシーについて
- 証明書のインストール方法と mail-from の利用停止
- ARIN 宛のメールへの電子署名

このプレゼンテーションによると、ARIN におけるテンプレート（申請書式）におけるユーザの認証は mail-from を用いており、より安全な方法に切り替えること、その方法として X.509 形式の証明書を用いることが始めに説明されている。

ARIN ではユーザによる証明書の入手の為の Web ページを用意しており、ユーザは Web ブラウザを用いて鍵の生成と証明書の申請、組み込みを行うことができる。一度証明書を使った認証に切り替えると mail-from は基本的に利用できなくなる、という説明があった。

4.4. まとめ

本節では、今回調査を行った RIR における認証局のマネジメントのポイントについて述べる。

4.4.1. APNIC CA

APNIC CA はメンバの認証用の証明書を発行することを目的とした認証局である。証明書の申請には申請書と写真付きの身分証明書を必要とする。申請書には予め登録されたメンテナの情報を記述する必要がある。発行される証明書は Web ブラウザで利用することができるクライアント証明書である。MyAPNIC と呼ばれる各種申請業務を行うことができる Web インターフェースが用意されており、この MyAPNIC へのログインに利用することができる。

APNIC CA はオープンソースソフトウェアを用いており、またできるだけシンプルな構成で運用している。クライアント証明書の登録業務は、IP 業務のユーザ登録業務と兼ねており、認証局部門とは独立している。認証局部門は証明書管理と認証局システムの運用に専念できる体制となっている。

2003 年度の調査以降、証明書発行数の順調な増加、CA の増強（HSM 導入、鍵ペアの作り直し）、RFC3779 に関する取り組み、説明資料の充実といった動きが見られた。今後も RFC3779 に関連して S-BGP 等の新たな取り組みを行う模様である。

4.4.2. RIPE NCC

RIPE NCC の認証局は、LIR の認証用の証明書を発行することを目的とした認証局である。証明書の申請には組織 ID とパスワードを必要とし、パスワードを知っている LIR の ID 管理者が証明書申請を行うことができる。証明書は各種申請業務における電子メールの暗号化に使われ、また LIRPortal、WebUpdates といった Web インターフェースを利用する際のクライアント認証にも用いることができる。証明書と既存のユーザ情報（person オブジェクト、role オブジェクト）との組み合わせを RPSL（Routing Policy Specification Language）を用いており、既存の資源管理情報との統一的な扱いを実現している。データベースには RIPE NCC の認証局以外から発行されたクライアント証明書を登録することもでき、その証明書を使った各種申請業務を可能にしている。

RIPE NCC における認証局はオープンソースソフトウェアを用いており、RPSL ベースのデータベースと連携するための開発、Web インターフェースとの連携といった開発が行われている。

2003 年度の調査以降の動向として、LIRPortal の証明書発行と RPSL のデータベースの連携により、証明書発行数が大幅に増加した点、電子メール（S/MIME）を用いた各種申請業務が挙げられる。

担当者のレベルでは S-BGP 等の新たな証明書の用途に興味を示しているが証明書の新たな用途に関する RIPE ミーティングでの議論はまだ行われていない。

4.4.3. ARIN

ARIN の認証局は、メンバの認証用の証明書を発行することを目的とした認証局である。証明書の申請には本人確認書類が必要とされているが、詳細は明らかにされていない。Web インターフェースを使って証明書の申請を行うとしている。資源管理情報との関連付けは、POC（Point of Contacts：連絡先）の識別子を用いている。各種申請を行うユーザの ARIN による認証を S/MIME の電子署名を用いて実現することが目的である。従って申請業務の為の Web インターフェースが使われることは今の時点では想定されていない。

認証局システムにはオープンソースソフトウェアが使われており、POC との関連性を確認する機能等を除いて大きな開発を行わずに運用されている。CA 証明書を複数発行し、CA の秘密鍵の危殆化に対応するとしている。

2003 年度の調査以降の動向には、メンバ全体への告知およびチュートリアルの実施、CPS の公開が挙げられる。CPS は必要最低限の記述に留められており、特に「POC に対応する証明書所有者の ARIN による認証」の主旨を明文化する目的で記述されたと考えられる。

第5章 IP アドレス認証局のマネジメントに関する検討と構築

内容

- 認証情報の検討
- 認証業務の設計
- システム構成
- 業務フロー
- 画面イメージ

第5章　IP アドレス認証局のマネジメントに関する検討と構築

本年度の調査研究は、2003 年度、2002 年度の調査研究をもとに IP アドレス認証局の構築を行い、更に実験的に運用を行った。

IP アドレス認証局の構築あたり、はじめにマネジメントの形態の検討を行い、次に認証業務の設計と構築を行った。

5.1. 認証情報の検討

インターネットレジストリにおける登録者の認証情報は、割り振りを行ったアドレス資源の情報と関連する形で保持している必要がある。本調査研究では、認証業務の検討に先立ち、資源管理情報を管理する IP レジストリシステムにおいて証明書の情報を含む認証情報をどのように格納すべきかについて検討を行った。

本節では認証情報をまとめ、資源管理情報と関連させる”メンテナー”のあり方について述べる。ここでいうメンテナーは RIPE NCC 等で利用されている RPSL（Routing Protocol Specification Language）で使われている概念とは若干異なり、日本の資源管理の形態に合わせて設計しなおしたものである。

本節は現状調査と各モデルの不具合を洗い出しながら、クライアント証明書の扱いに最も適するメンテナーのモデルについて述べる。

5.1.1. 現状の IP レジストリシステム上の認証

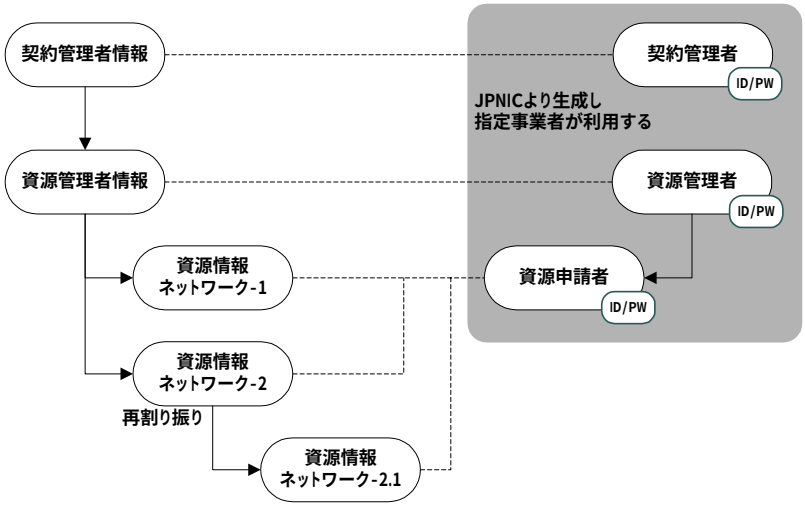
契約が成立した指定事業者には、JPNIC より表 5.1.2.1.-1、図 5.1.2.1.-2 にて業務に応じた３通りの権限に応じた認証を提供している。これは、対象となる業務申請権限となり、各種申請の正当性を図る目的がある。

表 5.1.2.1-1　主な業務毎の処理実施可否について

主な業務名称	契約管理者	資源管理者	資源申請者
指定事業者契約関連	○	×	×
資源管理情報関連	○	○	×
資源情報関連	×	×	○

- 契約管理者：契約情報の保守及び、配下の資源管理者に対しての請求先情報の保守も可能となる。
- 資源管理者：資源情報（割り振り/割り当てアドレス）を統括する管理者情報の保守が可能となる。
- 資源申請者：資源情報（割り振り/割り当てアドレス）の申請業務が可能となる。

図 5.1.2.1-2　IP レジストリデータと利用権限の関連図



5.1.2. メンテナー情報の導入目的

指定事業者で管理している割り振り/割り当てアドレス情報（以下、資源情報）全体に対して、申請権限があるが、指定事業者内の部署別利用制限や、ダウンストリーム（二次指定事業者以降）の利用制限をすることで、より細かな申請制限が必要と考えられてきた。また、現状の認証 ID/パスワードに加え、IP アドレス認証局によるクライアント証明書を導入する事で、更なる情報の安全性に繋がるものとする必要がある。

これらを踏まえて、現状の認証 ID/パスワード及び、クライアント証明書を権限グループとして管理するメンテナー情報を設け、操作対象単位に連結する事により実現させる事となる。

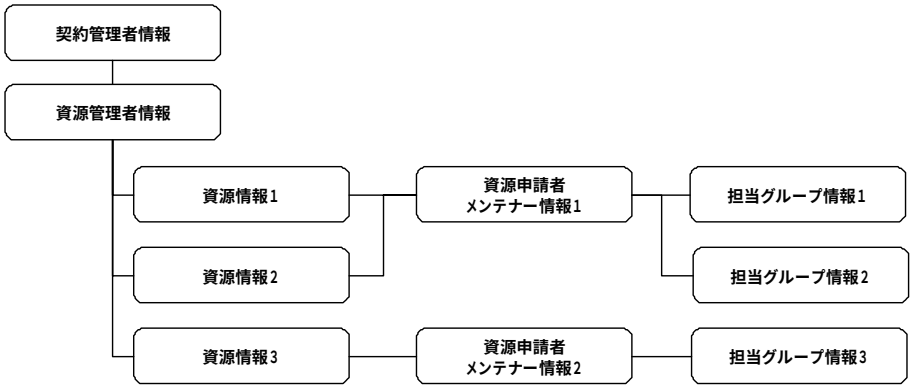
JPNIC のデータには、担当グループ情報が存在する。これは、各種資源情報に、1 担当者の連絡先連絡先となる担当者情報が別に設けており、何らかの問い合わせをする際に利用されている。担当者が所属する指定事業者の組織名や住所等の変更により、関わる膨大な担当者情報変更申請を指定事業者がおこなう必要があった。

そこで、次期 IP レジストリシステムでは、連絡先となる情報を部署単位に設定する担当グループ情報を新たに設置し対処する考えで進められている。

この担当グループ情報には､メンテナー情報のグループの考えと一致していた事から､図 5.1.2.1-3 に示しているデータ構成が考えられる。

メンテナー情報内の組織名・住所等の変更で、属する担当グループ情報にも反映される。これにより、指定事業者の情報変更申請への手間を軽減する事に繋がるものと考えられてきた。また、メンテナー情報導入目的にもある、クライアント証明書を担当グループ単位に設定する事により、認証管理及び指定事業者内の所属管理にも繋がると考えられる。

図 5.1.2.1-3　担当グループ情報とメンテナー情報の関連図



しかし、担当グループ情報は、指定事業者情報つまり資源管理者情報とは無関係となっている為に、組織部署単位に登録が出来たとしても、その情報と指定事業者との関わりが安易な情報と捕らえられる。また、他組織の資源情報についても連結が可能となっており、柔軟なデータ構成で利用するユーザにとって扱い易い反面、メンテナー情報と連結し認証情報を付加させるには、問題があると想定される。その結果、担当グループ情報については、考慮せず検討を進めて行くこととなる。

5.1.2.1. メンテナー情報と認証ID/パスワードについて

現状の認証 ID/パスワードを次期 IP レジストリシステムでもそのまま引継ぎ、利用している指定事業者に対して、無用な混乱をさける必要があると考えられる。図 5.1.2.1.-4 で、メンテナー情報への移行方法を記載している。各情報は権限（契約管理者・資源管理者・資源申請者）の識別子も移行対象となる。移行されたメンテナー情報を直接的に、指定事業者が保持している資源情報と連結する事により、現状のデータ構成と変わりなく利用可能となる。

図 5.1.2.1-4　認証 ID/パスワードとメンテナー情報への移行図

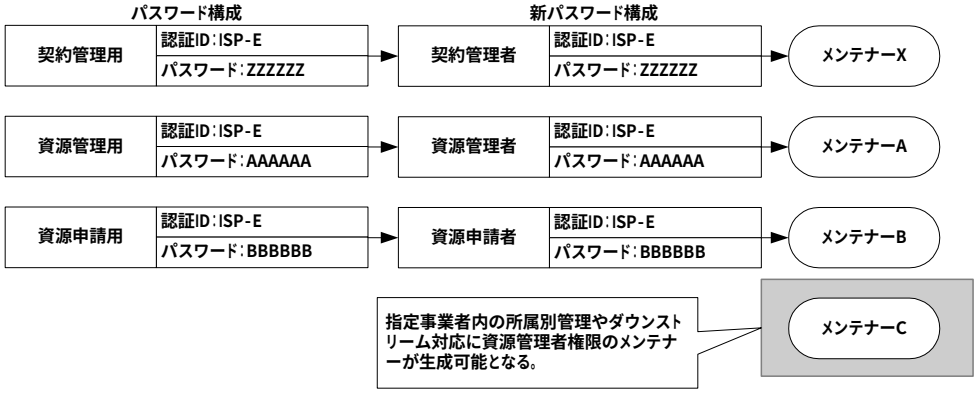
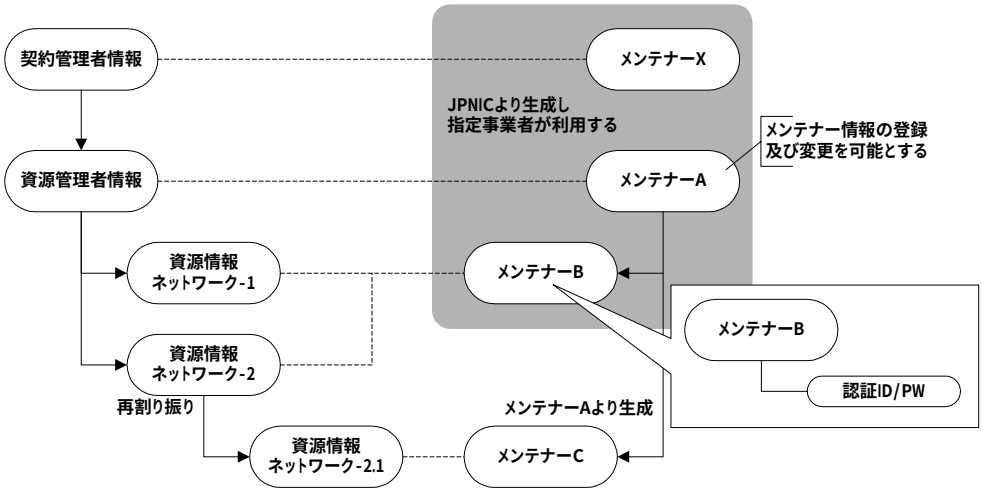


図 5.1.2.1.-5 では､IP レジストリデータとメンテナー情報との関連を記載している。資源管理者メンテナー（図中のメンテナーA）が、必要に応じて資源申請者メンテナー（図中のメンテナーC）を生成し、対象資源情報へ連結する事により、メンテナー情報導入目的にもある、指定事業者内の部署別利用制限や、ダウンストリーム（二次指定事業者以降）の詳細的な利用制限が実現する事になる。

図 5.1.2.1.-5　IP レジストリデータとメンテナー情報の関連図



5.1.2.2. メンテナー情報とクライアント証明書について

既に、個々の資源情報へ連結されているメンテナー情報に対して、クライアント証明書を付加させる事により、権限識別が含まれたクライアント証明書が利用可能となる。

図 5.4.2.2.-1 において、資源申請者メンテナー毎にクライアント証明書を設置した場

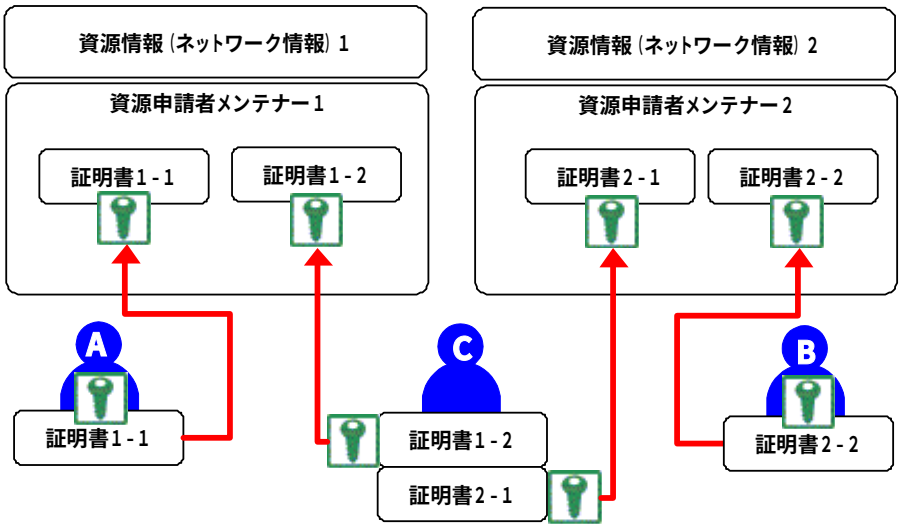
合に、図中の A が保持している証明書１－１で資源情報１へのアクセスが可能となる。また、図中の B においても同様の方法で資源情報２へアクセス可能となる。

しかし、資源情報１と資源情報２へ、それぞれに対してアクセスしたい図中の C については、メンテナー単位にクライアント証明書が異なる為に、必要に応じて利用するクライアントへの取り込む必要があり、その保守対象となる資源情報別に使い分けをする必要がある。また、クライアント証明書を管理する上で、どの証明書を無効にするべきか判断する必要があり、何らかのトラブルで特定クライアントまで追う事が出来ず、他のクライアントにも影響があると考えられる。

これらの懸念していた問題点を、回避する為に以下のモデル案を検討してきた。

- メンテナー情報のグループ管理モデル
- メンテナー情報での共有利用モデル

図 5.4.2.2.-1　メンテナー情報内のクライアント証明書



5.4.2.2.1. メンテナー情報のグループ管理モデル

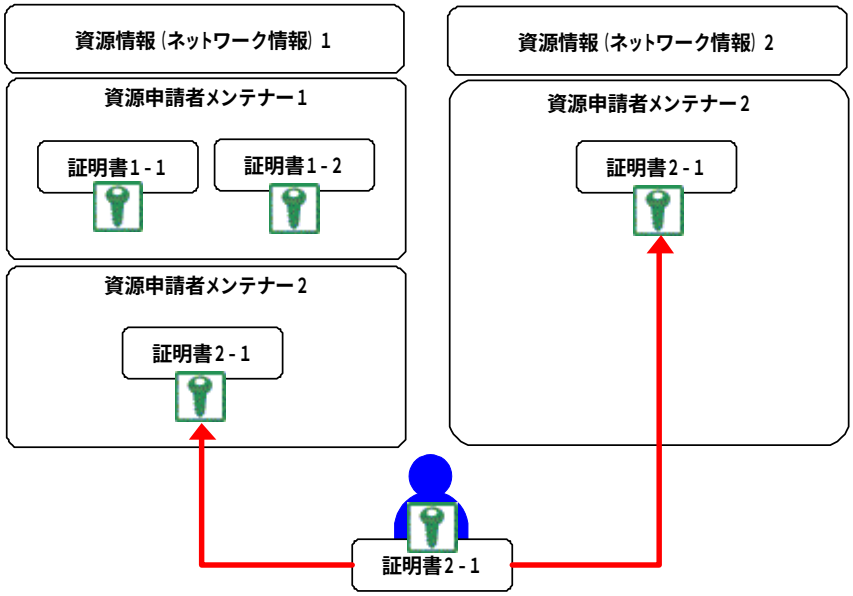
図 5.4.2.2.1.-1 では、資源情報に応じて資源申請メンテナーが異なりそのクライアント証明書もまた違う。ある一定のグループに集約し、資源申請者メンテナー単位に資源情報へ連結するモデルである。

利用するクライアントには、既に取り込まれている単一のクライアント証明書で簡略化されるが、資源情報には複数の資源申請者メンテナーを連結させる必要があり、その管理が必要と考えられる。また、クライアント証明書を別の資源申請者メンテナーへ移す場合に、保守可能な資源情報の把握が必要となる。それは、図中の証明書２－１を資源申請者メンテナー１へ移した場合、資源情報２の保守が不可能となる。

当モデルは、利用する側を考慮した場合であり、そのクライアント証明書や保守可能

となる資源情報との管理が必要である。回避策としては、資源情報に属するメンテナー管理及びメンテナー内のメンバ管理を容易におこなう管理者用機能を提供する事が考えられる。

図 5.4.2.2.1.-1　メンテナー情報単位のグループ管理モデル案



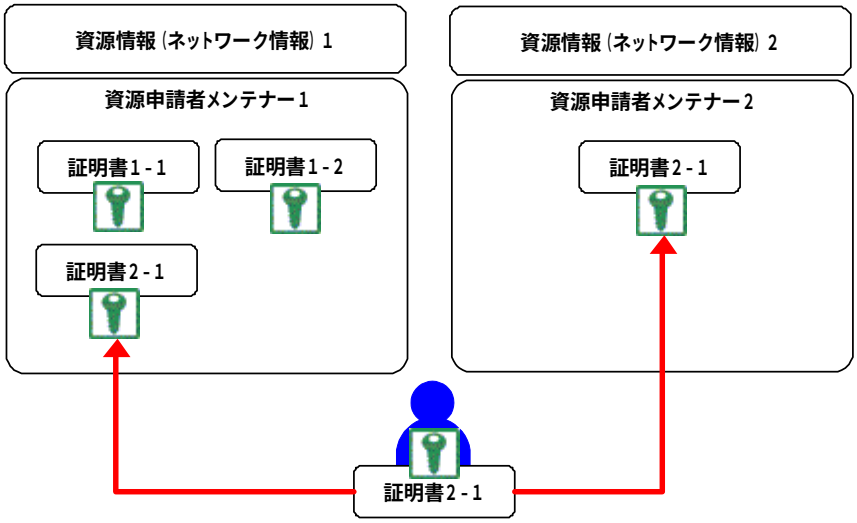
5.4.2.2.2. メンテナー情報での共有利用モデル

図 5.4.2.2.2.-1 では、クライアント証明書を各資源申請者メンテナーで共有利用をおこなうモデルである。

既に利用されるクライアントに取り込まれている為に、資源申請メンテナーのメンバ変更をおこなうだけで簡略化できる。また、失効手続きについても、単一クライアント証明書さえ把握していれば、最小限の対応で回避出来ると考えられる。

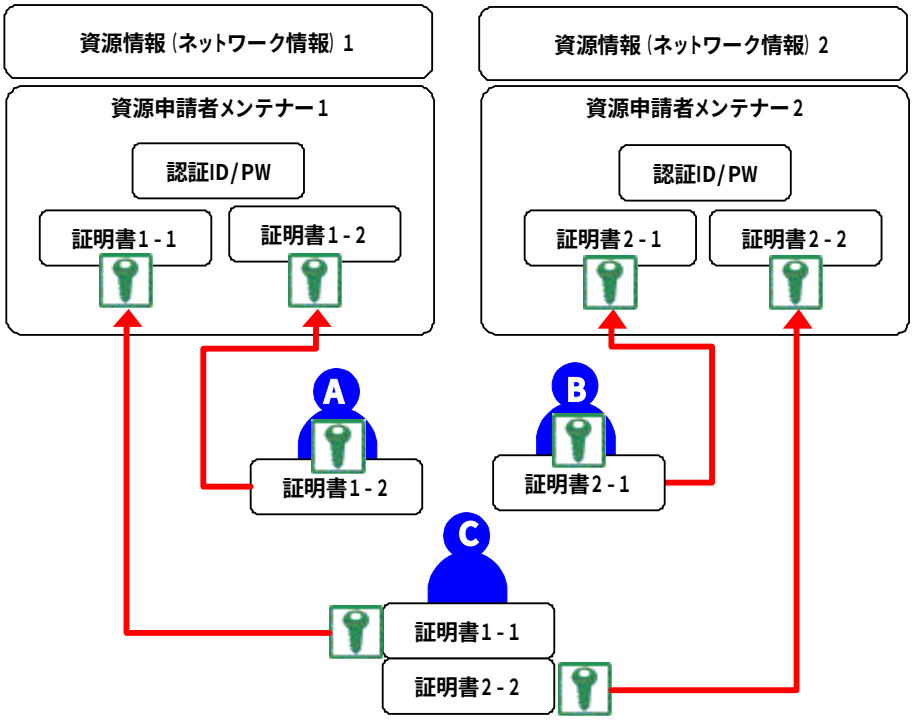
しかし、資源申請者メンテナーに対して、どのクライアント証明書が設定されているのか情報管理が困難と考えられる。

図 5.4.2.2.2.-1　クライアント証明書共有利用モデル案



5.4.2.2.3. クライアント証明書の扱い

これらの検討結果により、クライアント証明書の管理を複雑におこなうよりも、簡略的に対応するのが望ましいと考えられる。そこで、懸念していた状態（図中の C）は、それぞれのメンテナー情報に設定されているクライアント証明書を使い分けて利用することとし、今後の利用状況に応じて改良する事となる。



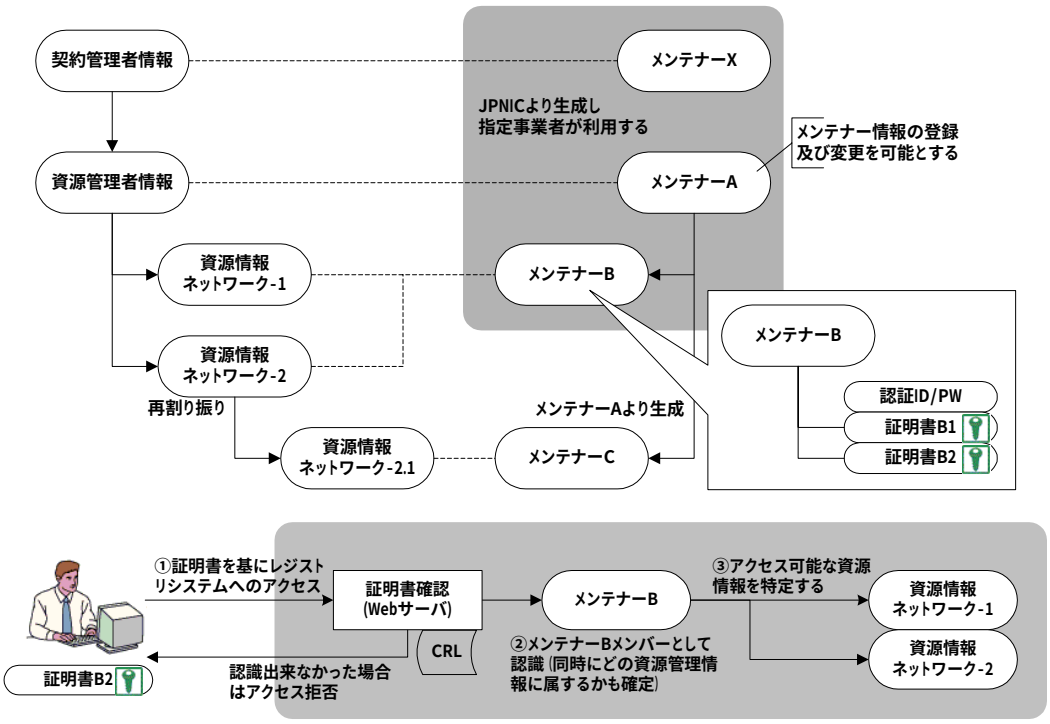
5.1.2.3. IPレジストリシステムとクライアント証明書の関連について

図 5.4.2.3.-1 でメンテナー情報内には、認証 ID/パスワードと複数のクライアント証明書が権限グループとなり管理され、連結されている資源情報のみ保守可能となる。

認証 ID/パスワード又は、クラアント証明書にてアクセスされたら、メンテナー情報を特定し、そのメンテナー情報が保守可能となる資源情報へ紐づく事になる。

クライアント証明書が漏洩した場合の対応策としては、特定のメンテナー又はクライアント証明書を無効化にする管理機能を提供し、被害は最小限に抑える事が可能となる。

図 5.1.2.3.-1　IP レジストリデータとメンテナー情報の関連図



5.2. 認証業務の設計

IP アドレス認証局は役割ごとに認証局を設け、それぞれの認証局の構築が行われた。IP アドレス認証局は、JPNIC ルート認証局、IP アドレス認証局（認証）、IP アドレス認証局（証明）の三つである。2003 年度に行った業務モデルは、IP アドレス認証局（認証）に適用された。

IP アドレス認証局（認証）は、IP レジストリシステム等における認証を目的とした証明書を発行する認証局である。アドレス資源管理におけるユーザの定義に合わせて設計しつつ、クライアント証明書を用いることのメリット（強い認証と個別の有効性管理）を生かす設計を行った。

なお、下記に述べる設計および業務フローは 2004 年度の調査研究を行っている段階のものであり、基本的な設計方針は変わらないものの実際の業務とは異なることがある。

5.2.1. IP アドレス認証局の要求仕様

IP アドレス**認証局**の設計および構築に先立って、IP アドレス認証局の機能を実現する「認証局システム」の要求仕様の明確化を行った。この要求仕様を以下に述べる。

5.2.1.1. 目的

当センターでは、認証局の運用実験を計画している。開発中の IP レジストリシステムにおける利用者認証に SSL/TLS クライアント認証を用いるため、当センターの契約者に証明書を発行する認証局と、それに付随する WEB 申請受付けサーバの開発を行なう。また、実証実験向けの認証局として IP アドレス認証局（証明）を構築し、RFC3779 で提案されているフィールドをもつ証明書の発行を行なう。

5.2.1.2. 基本方針

認証局に関する要件として、ルート認証局である「JPNIC ルート認証局」の構築、その下位の認証局である「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」の構築、さらに IP アドレス認証局（証明）の下位の認証局である「実証実験向け LIR 認証局」の構築を行なう。このうち、JPNIC ルート認証局と IP アドレス認証局（認証）を運用環境用として運用し、IP アドレス認証局（証明）と実証実験向け LIR 認証局を実証実験環境として運用することを目的とする。

それぞれの認証局には証明書を出力するリポジトリが必要であり、運用向けと実証実験向け環境にそれぞれハードウェアを用意し、LDAP サーバをリポジトリとして運用する。

IP レジストリシステムとの連携により発生する業務は以下の通りである。

(1) JPNIC 業務管理者認定業務

IP アドレス認証局（認証）を構築後、CA 管理ツール（GUI）を使用して JPNIC 業務管理者に対して証明書を発行する。発行した証明書は直接 JPNIC 業務管理者に手渡す。

(2) 内向き用（JPNIC 業務管理者）申請受付業務
業務管理者は、業務担当者に対して証明書の発行、更新、失効操作を行なう。

(3) 内向き用（JPNIC 業務担当者）申請受付業務
業務担当者は、契約者（メンバ管理者）のリスト表示と、新規契約者に対して証明書の発行、契約者に対して証明書の更新、失効操作を行なう。

(4) 外向き用（メンバ管理者）申請受付業務
IP レジストリシステムと連携し、メンバ管理者によるメンバの追加とメンバの削除業務を行なう。メンバの追加を行なうと、ライセンス ID の表示と登録完了通知メールの送信が行われる。

(5) 外向き用（ホストマスタ）申請受付業務
メンバ管理者からライセンス ID を受け取り、この ID を使用してメンテナー申請者自身が使用する証明書の申請を行なう。

これらの業務が行なえるように、CGI モジュールの開発を行なっていく。

5.2.1.3. システム構築の要求事項

前節で定義した認証局と認証局システムの構成に対し、仕様上、それぞれに要求される事項をいかに満たすかという検討を行った。

（1） 認証局の役割の実現

	要求事項	内容	対応方針
1	運用向け CA 構成	「JPNIC ルート認証局」「IP アドレス認証局（認証）」の認証局を構成する。	JPNIC ルート認証局と IP アドレス認証局（認証）を構築し、HSM を付加する。
2	実証実験向け CA 構成	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」の認証局を構成する。	IP アドレス認証局（証明）と実証実験向け LIR 認証局を構築する。
3	ルート認証局	「JPNIC ルート認証局」は、「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」の認証局証明書の発行と管理を行なう。	JPNIC ルート認証局にて Sub-CA のプロファイルを適用した証明書発行が可能である。鍵ペアの生成と下位 CA 証明書の発行を行ない、それぞれ下位の CA に対して PKCS#12 ファイルを提供できる。

4	IP アドレス認証局（認証）	IA、RA、PA の機能、および開発を伴った Web インタフェースと連携するための機能。	IA、RA については 1 つの CA サーバがこれらの代用として動作する。PA については項番 5「運用向けリポジトリ」を参照のこと。Web インタフェースの開発については、項番 7「内向き用申請受付けサーバ」、項番 8「外向き用申請受付けサーバ」を参照のこと。
5	運用向けリポジトリ	「JPNIC ルート認証局」「IP アドレス認証局（認証）」のリポジトリを構成する。	JPNIC ルート認証局と IP アドレス認証局（認証）のリポジトリを構成する。リポジトリのプロトコルには LDAP を使用する。
6	実証実験向けリポジトリ	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」のリポジトリを構成する。	IP アドレス認証局（証明）と実証実験向け LIR 認証局のリポジトリを構成する。リポジトリには LDAP を使用する。
7	内向き用申請受付けサーバ	JPNIC 業務担当者による申請を受付けるサーバ。Web ブラウザによりアクセス可能であり、申請者「契約管理者/資源管理者」「JPNIC 業務担当者」向けの証明書を発行する。	Web エンロール CGI プログラムがあり、CA サーバに対してリモートで証明書の発行を要求できる。これをベースに申請受け付け用 CGI プログラムの開発を行なう。
8	外向き用申請受付けサーバ	「契約管理者/資源管理者」は WEB ブラウザにてアクセスし、認証コードの発行を行なう。認証コードをメンテナー申請者に渡し、メンテナー申請者は自身で証明書の発行を要求する。	ユーザ情報を入力し、認証コードを発行する CGI プログラムを開発する。また、WEB エンロール CGI プログラムを修正し、認証コードでユーザ認証後に LDAP からユーザ情報を取得し証明書を発行する CGI プログラムの作成を行なう。
9	全ての認証局	全ての認証局はソフトウェア的に分離している必要がある。	1 つのサーバに複数の CA を構成することができ、それぞれの CA はソフトウェア的に分離している。
10	全ての認証局	それぞれが独立して秘密鍵を管理する必要がある。	1 つのサーバに複数の CA を構成することができ、それぞれの CA の秘密鍵は独立して管理される。
11	ハードウェア	「IP アドレス認証局（証明）」は「IP アドレス認証局（認証）」と、ハードウェア的に独立している。	項番 1「運用向け CA 構成」と項番 2「実証実験向け CA 構成」の通り、これらの CA はハードウェア的に分離して運用される。

12	リポジトリ	「JPNIC ルート認証局」「IP アドレス認証局(認証)」「IP アドレス認証局(証明)」「実証実験向け LIR 認証局」はそれぞれ異なるリポジトリが必要。	項番 5「運用向けリポジトリ」と項番 6「実証実験向けリポジトリ」の通り、2 台のハードウェアにて構成し、CA のサブジェクトにより異なるエントリ以下に独立したリポジトリを構成する。
13	IP アドレス認証局(証明)	「IP アドレス認証局（証明)」は、プロファイルの柔軟な変更、証明書とプロファイルデータの分析・保管、他認証局との相互認証の機能が必要。	柔軟なプロファイル管理機能を有しており、証明書と共にこれを保管・分析することが可能である。また、相互認証の機能も持っており、Cross CertificatePair ファイルの出力も可能である。
14	ユーザ利用端末	ユーザが利用する端末は開発対象ではない。	開発は行なわない。

（2） 運用上の役割の実現

15	JPNIC 登録局と発行局	外向き／内向き申請受付けサーバからの申請を受付け、証明書の発行、失効、CRL の発行が必要。	リモートからの証明書発行要求を受付け、アクセス制限の元で即時に証明書の発行が可能である。また定期的な CRL の発行が可能である。
16	JPNIC 登録局と発行局	証明書の管理業務を行なう GUI が必要。それらとは独立した運用担当者のユーザインタフェースが必要。	業務担当者は項番 7 の通り Web 画面を通じて証明書の管理が行なえる。これとは独立して、CA 運用の GUI が用意される。
17	リポジトリ	管理に必要なデータを格納する。IP レジストリシステムからの参照要求を受付け、返答を行なう。LDAP と HTTP（参照のみ）を用いる。	リポジトリには LDAP を使用しユーザ管理情報を保管する。アクセス時には認証を行ない、適切なアクセス制御を施す。
18	リポジトリ	内向き申請受付けサーバ、外向き申請受付けサーバ等の他のサーバとはハードウェア的に独立している必要有り。	項番５、項番６の通り、独立したハードウェアにて運用する。

（3） IP レジストリシステムとの連携

項番７、項番８に従い、IP レジストリシステムとの連携を行う為の開発を行なう。また IP レジストリシステムの開発プロジェクトと並行して開発を行う為、依存度に関しては疎な関係を保つよう留意する。従って二つのシステム間での登録データの矛盾を防ぎまたは解消する機構を持つ。

（4） IP アドレス認証局（証明）および LIR 認証局

19	実証実験向け認証局機能	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」は、RFC3779 に準拠したフィールドを扱うことができ、プロファイルの変更を行える必要がある。	作成した DER バイナリを証明書拡張情報としてプロファイルに取り込むことが可能である。設定されたプロファイルをもとに証明書を発行できる。
20	実証実験向け認証局機能	「IP アドレス認証局（証明）」「実証実験向け LIR 認証局」は、RIR またはアジア太平洋地域の NIR 等との相互認証証明書の発行が可能でなければならない。	CrossCertificatePair ファイルの出力も可能である。

(5) セキュリティの機能

21	セキュリティ	不正な操作の防止／抑止を行なうために、運用における記録や作業者の操作内容を保管する機能が必要である。	CA サーバには、発行ログ、アクセスログ、エラーログを出力する機能がある。また、開発を行なう CGI モジュールにおいても、これらのログ出力機能を持たせる。
22	セキュリティ	「JPNIC ルート認証局」は、FIPS140-2 レベル 2 に準拠した HSM を使用する必要がある。	項番 1 にある通り、ルート認証局には HSM を使用する。
23	セキュリティ	契約管理者/資源管理者と JPNIC 業務管理/担当者はハードウェアトークン（IC カード、USB トークン等）を使用する必要がある。秘密鍵を取り出すのが困難である。	ハードウェアトークンを使用して各 Web サイトにアクセス、もしくは証明書の発行を行なう。

(6) 環境の変更

24	環境の変更	障害が起きた場合、ハードウェアが変更されることを前提として構成される必要がある。ただし、HSM についてはこの限りではない。	CA フォルダと証明書ストアのバックアップが行われていれば、このデータを新たなマシンにリストアし、自動起動設定を行なうことでシステムの復旧が可能である。

(7) シンプルな構成

25	シンプルな構成	要求システムは、シンプルなシステムを実現することが望まれる。	CA はシンプルかつ少ないリソースで動作が可能である。また、リポジトリと連携しシンプルな証明書発行管理のシステムを開発する。

(8) 拡張性

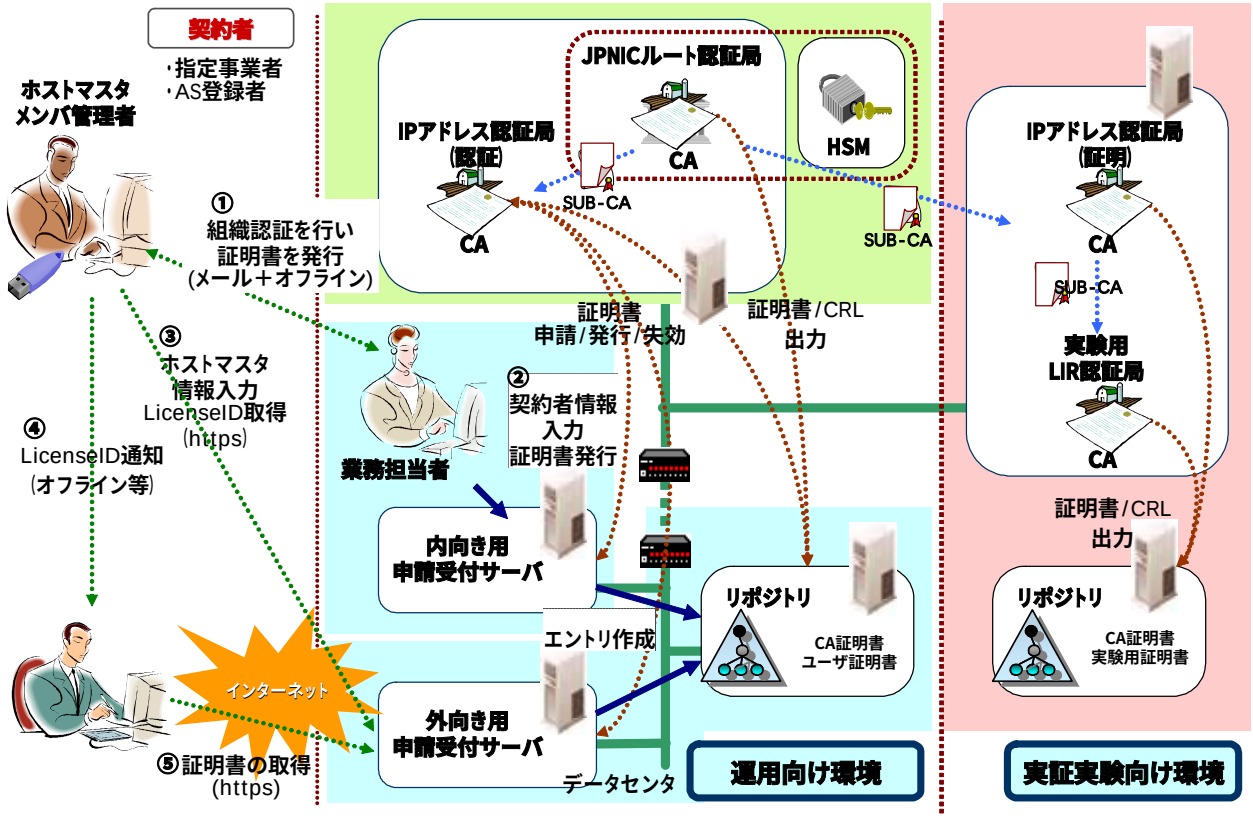
26	拡張性	収容した証明書の世代管理が可能であることが望まれる。複数の証明書プロファイルを切り替えることが望まれる。	1 つのサーバにて複数の CA を同時に運用可能である。CA の中で複数のプロファイルが管理でき、それぞれのプロファイルを適用して柔軟な証明書発行が可能である。
27	HSM の拡張利用	「IP アドレス認証局（認証）」「IP アドレス認証局（証明）」は、HSM を使うことが望まれる。各認証局は独立した秘密鍵の管理ができる。	「JPNIC ルート認証局」には HSM が接続されており、この HSM を「IP アドレス認証局（認証）」にて利用することができる。

(9) 運用管理の GUI

28	JPNIC 登録局と発行局	運用管理のユーザインタフェースには GUI もしくは Web インタフェースが望まれる。証明書管理、運用管理のユーザインタフェースおけるアクセス制御が望まれる。	管理ツールとして GUI のツールが利用可能である。パスワードによる認証や、リモートでは指定した権限によるアクセス制御が可能である。

5.2.2. システム構成

5.2.2.1. システム図



システム構成は、運用向け環境と実証実験向け環境に大別される。運用向け環境では主に 4 つの業務を処理する。（1）業務管理者による業務担当者の情報登録、証明書発行業務、（2）業務担当者による契約者（メンバ管理者）の情報登録、証明書発行業務、（3）メンバ管理者によるメンテナー申請者情報登録、証明書発行用認証 ID の払い出し業務、（4）メンテナー申請者による証明書の申請、発行業務の処理を行なう。これらの業務向けに Web インタフェースが提供され、(1)(2)は内向き用申請受付けサーバ)、（3）（4）は外向き用申請受付けサーバ上で動作する CGI によって処理される。

運用向け環境では、2 つの認証局が運用される。1 つは JPNIC ルート認証局で、下位の認証局に対して証明書を発行する。この認証局からは EE 証明書は発行しない。なお、秘密鍵を HSM に保管することで高い安全性を確保する。もう 1 つの認証局は IP アドレス認証局（認証）と呼ばれ、JPNIC ルート認証局の下位に位置している。この認証局から、JPNIC 業務管理者と JPNIC 業務担当者、契約者（メンバ管理者)、メンテナー

申請者向けの証明書の発行を行なう。これら 2 つの認証局は運用向け認証局サーバにより運営される。このうち、ルート認証局については常時稼動ではなく、必要なときに秘密鍵トークンを起動して動作させるような運用を想定する。

この他、運用環境向けにリポジトリが用意される。このリポジトリには契約者とメンテナー申請者の DN を持つエントリが作成され、証明書の保管が行われる。リポジトリは常時稼動しており、IP レジストリシステムからのアクセスも受付ける。

外向き申請受付けサーバは、インターネットからのアクセスを受付けるため、DMZ に配置され FW 経由で認証局サーバ、リポジトリ、IP レジストリシステムの RDB にアクセスする。

実証実験向け環境では 2 つの認証局が運用される。1 つは IP アドレス認証局（証明）で JPNIC ルート認証局の下位に位置している。この認証局の更に下位に実証実験向け LIR 認証局が存在し、RFC3779 に対応した拡張フィールドを持つ証明書を発行し、実証実験向けに使用する。

5.2.3. 認証局設計

5.2.3.1. JPNICルート認証局

（1） 方針

JPNIC ルート認証局は、下位の認証局に対してのみ証明書を発行するものとする。ルート認証局の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 2048bit とし、証明書の有効期限は 10 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。CA の名称は「JPNIC ルート認証局」とする。

本来であれば ARL（Authority Revocation List）の発行が必要となるが、ルート認証局は通常非アクティブとして稼動させないため、ARL の発行は行なわないものとする。なお、ルート認証局の秘密鍵が漏洩、もしくは下位の認証局である IP アドレス認証局（認証）の秘密鍵が漏洩するようなインシデントが発生した場合、ルート認証局から CA の再構築を行なう。

（2） CA 証明書プロファイル設計

基本情報を以下に示す。

Field	ルート証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
validity	20年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
subjectPublicKeyInfo	2048bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	ルート証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	○
cRLSign	○
encipherOnly	
decipherOnly	
BasicConstraints	non-critical
cA	○
pathLenConstraint	

拡張情報には、AuthorityKeyIdentifier、SubjectKeyIdentifier、KeyUsage、BasicConstraints の 4 つを設定する。全て non-critical とし、CA 証明書に必要な情報を入力する。

(3)　EE 証明書プロファイル設計

EE 証明書は、IP アドレス認証局（認証）の CA 証明書となる。それぞれの項目を参照のこと。

5.2.3.2. IPアドレス認証局（認証）

（1） 方針

IP アドレス認証局（認証）は、JPNIC 業務管理者と JPNIC 業務担当者、契約者（メンバ管理者）、メンテナー申請者全てに証明書を発行する。CA 証明書の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 1024bit とし、証明書の有効期限は 10 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。CA の名称は「JPNIC 資源管理認証局」、通称「メンテナー認証局」とする。

EE 証明書の鍵アルゴリズムは RSA 公開鍵暗号、鍵長は 1024bit とし、証明書の有効期限は 3 年とする。署名アルゴリズムは sha1WithRSAEncryption とする。登録担当者とメンバ管理者、メンテナー申請者の証明書について、「証明書プロファイル」という単位にグループ分けし管理する。

IP アドレス認証局（認証）は常時稼動し、CRL の発行も行なう。CRL は定期的に運用向けリポジトリに出力される。出力するリポジトリの DN は CA のサブジェクト DN と同じエントリとする。

（2） CA 証明書プロファイル設計

基本情報を以下に示す。

Field	CA証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	JPNIC Root Certification Authority
validity	10年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	CA証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	○
cRLSign	○
BasicConstraints	non-critical
cA	○
pathLenConstraint	
certificatePolicies	non-critical
policyIdentifier	CP/CPSのOID
policyQualifiers	
policyQualifierID	CPSUri
qualifier	CP/CPSのURL
cRLDistributionPoint	non-critical
destributionPoint	
destributionPoint	CRLのURL

拡張情報には、AuthorityKeyIdentifier、SubjectKeyIdentifier、KeyUsage、BasicConstraints の 4 つを設定する。全て non-critical とし、CA 証明書に必要な情報を入力する。

(3)　EE 証明書プロファイル設計

JPNIC 業務管理者、業務担当者の基本情報は以下の通りである。

Field	EE証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
validity	2年
notBefore	発行時点
notAfter	指定可能

Field	EE証明書
subject	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	Secretariat
organizationalUnitName	Administrator
organizationalUnitName	<メンテナーコード>
commonName	JPNIC-AD <JPNIC従業員コード> <NAME>
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

JPNIC 管理者は ou=Administrator、JPNIC 業務担当者は ou=Hostmaster となる。

契約管理者の基本情報は以下の通りである。なお、管理者メンテナーのサブジェクトの OU が Maintainer Administrator となり、契約者メンテナーは Corporate Administrator、メンテナー申請者は Hostmaster を入力する。

Field	EE証明書
version	v3(2)
serialNumber	○
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
validity	2年
notBefore	発行時点
notAfter	指定可能
subject	
countryName	JP
organizationName	<組織名>
organizationName	LIR Corporate Administrator
organizationalUnitName	<メンテナーコード>
commonName	LIR-CO <認証ID> <NAME>
subjectPublicKeyInfo	1024bit
algorithm	rsaEncryption
parameters	NULL
subjectPublicKey	○
signatureAlgorithm	
algorithm	sha1WithRSAEncryption
parameters	NULL
signatureValue	○

拡張情報を以下に示す。

Field	EE証明書
AuthorityKeyIdentifier	non-critical
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
SubjectKeyIdentifier	non-critical
keyIdentifier	○
KeyUsage	non-critical
digitalSignature	○
nonRepudiation	
keyEncipherment	○
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
BasicConstraints	non-critical
cA	FALSE
pathLenConstraint	
certificatePolicies	non-critical
policyIdentifier	CP/CPSのOID
policyQualifiers	
policyQualifierID	CPSUri
qualifier	CP/CPSのURL
cRLDistributionPoint	non-critical
destributionPoint	
destributionPoint	CRLのURL
subjectAltName	non-critical
rfc822Name	○

（4） CRL プロファイル設計

CRL の基本情報は以下の通りである。

Field	CRL
version	v2(1)
signature	
algorithm	sha1WithRSAEncryption
parameters	NULL
issuer	
countryName	JP
organizationName	Japan Network Information Center
organizationalUnitName	Internet Resource Service
organizationalUnitName	JPNIC Resource Service Certification Authority
thisUpdate	○
nextUpdate	24時間後
revokedCertificates	
userCertificate	○

拡張情報を以下に示す。

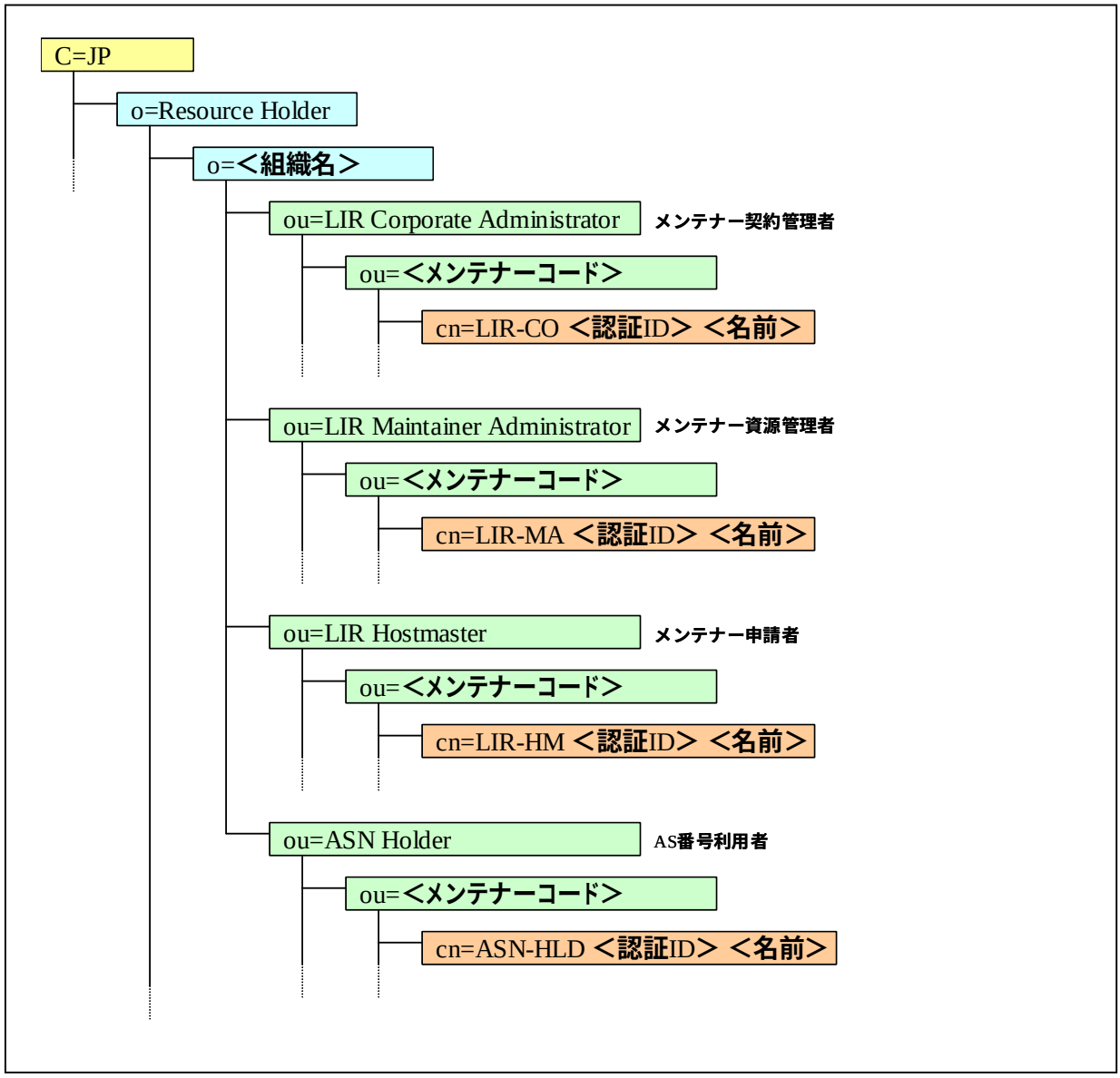
Field	CRL
authorityKeyIdentifier	
keyIdentifier	○
authorityCertIssuer	
authorityCertSerialNumber	
issuerAltName	
cRLNumber	○
deltaCRLIndicator	

5.2.4. リポジトリ設計

5.2.4.1. 指定事業者（組織）情報ツリー

（1） ツリー構成

指定事業者（組織）情報ツリーについては、下図のとおりである。



ツリーの頂点として“ o=Resource Holder,c=JP ”を作成し、この配下に様々なエントリを作成する。

指定事業者（組織）ごとに“ o=＜組織名＞,o=Resource Holder,c=JP ”を作成し、その直下には、“ ou=LIR Corporate Administrator ”、“ ou=LIR Maintainer Administrator ”、“ ou=LIR Hostmaster ”が作成される。

“ ou=LIR Corporate Administrator ”は、メンテナー契約管理者の格納場所である。

この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-CO ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=LIR Maintainer Administrator ”は、メンテナー資源管理者の格納場所である。

この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-MA ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=LIR Hostmaster ”は、メンテナー申請者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=LIR-HM ＜認証 ID＞ ＜名前＞ ”を作成する。

“ ou=ASN Holder ”は、AS 番号利用者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=ASN-HLD ＜認証 ID＞ ＜名前＞ ”を作成する。

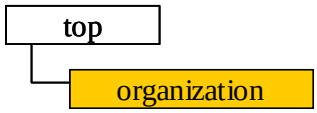
(2)　オブジェクトクラス

指定事業者（組織）情報ツリーで使用するオブジェクトクラスは、以下である。

「使用する属性」は、アプリケーションからの利用に基づいた定義である。そのため、ディレクトリ内における定義とは異なる場合がある。

■ コンテナ用オブジェクトクラス（1）

コンテナを作成するために、organization オブジェクトクラスを使用する。
organization オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成を持つ。



ツリー内における対象オブジェクトは、以下である。

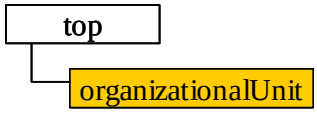
o=Resource Holder
o=**＜組織名＞**

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、組織名	o	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organization

■ コンテナ用オブジェクトクラス（2）

コンテナを作成するために、organizationalUnit オブジェクトクラスを使用する。
organizationalUnit オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成を持つ。



ツリー内における対象オブジェクトは、以下である。

ou=LIR Corporate Administrator
ou=LIR Maintainer Administrator
ou=LIR Hostmaster
ou=ASN Holder
ou=**＜メンテナーコード＞**

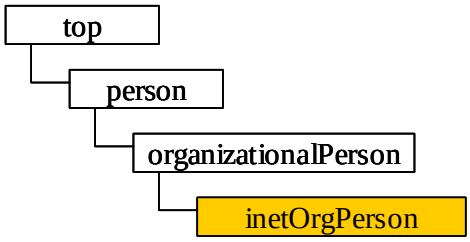
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、メンテナーコード	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit

■ 証明書格納用オブジェクトクラス

証明書を格納するために、inetOrgPerson オブジェクトクラスを使用する。

inetOrgPerson オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

cn=LIR-CO ＜認証ID＞ ＜名前＞
cn=LIR-MA ＜認証ID＞ ＜名前＞
cn=LIR-HM ＜認証ID＞ ＜名前＞
cn=ASN-HLD ＜認証ID＞ ＜名前＞

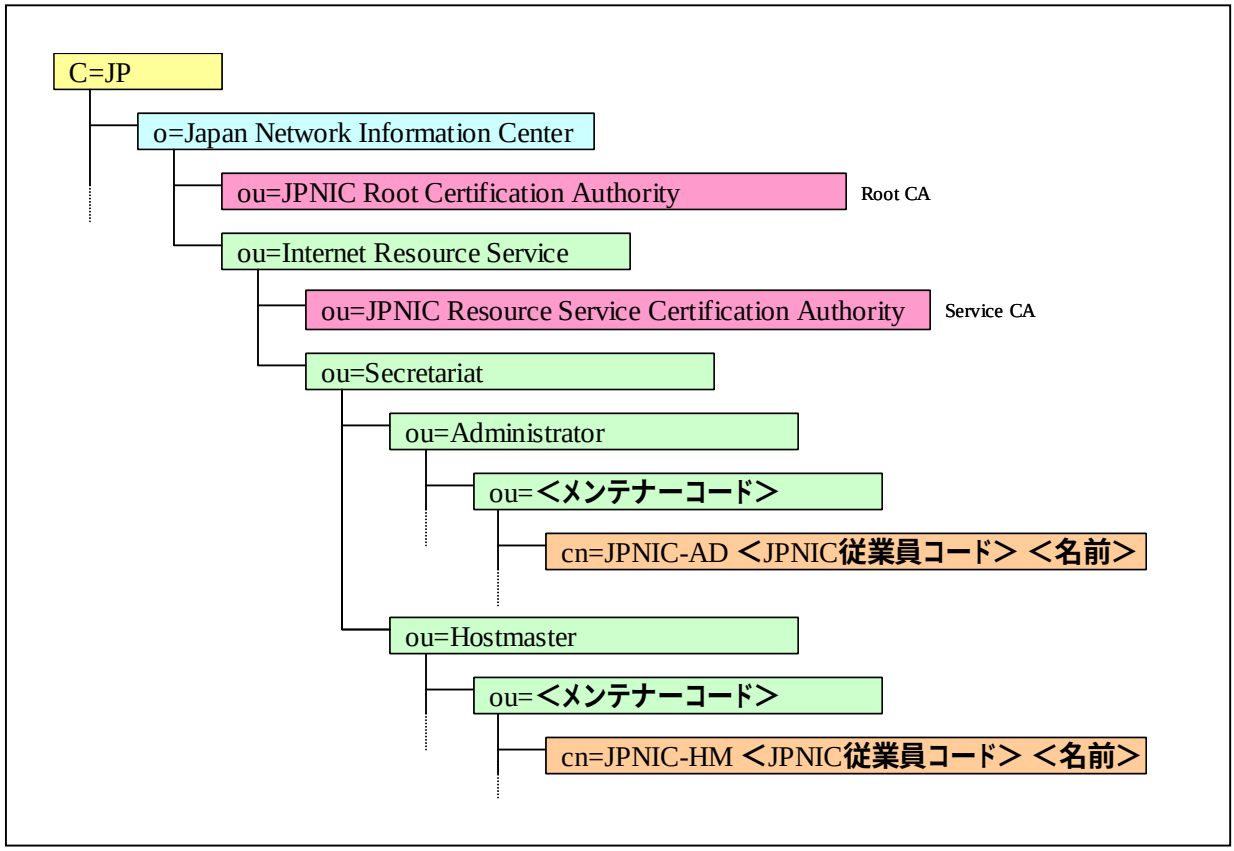
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名	cn	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	inetOrgPerson
3	名前	sn	○	－	cn と同値
4	ライセンス ID	uid	－	－	
5	電子メールアドレス	mail	○	－	
6	オンラインフラグ	o	○	－	“online”,“offline” 文字列
7	証明書	userSMIMECertificate	－	－	binary、カレントの証明書
8	証明書＜履歴＞	userCertificate	－	○	binary、証明書の履歴

JPNIC CA 情報ツリー

ツリー構成

JPNIC CA 情報ツリーについては、下図のとおりである。



ツリーの頂点として“ o=Japan Network Information Center,c=JP ”を作成し、この配下に様々なエントリを作成する。

“ o=Japan Network Information Center,c=JP ”の直下に、“ ou=JPNIC Root Certification Authority ”、“ ou=Internet Resource Service ”を作成する。

“ ou=JPNIC Root Certification Authority ”は、JPNIC ルート認証局である。

“ ou=Internet Resource Service ”は、IP アドレス認証局に関する情報の格納場所である。この直下に、“ ou=JPNIC Resource Service Certification Authority ”、“ ou=Secretariat ”を作成する。

“ ou=JPNIC Resource Service Certification Authority ”は、IP アドレス認証局である。

“ ou=Secretariat ”は、証明書格納用エントリの格納場所である。

この直下に、“ ou=Administrator ”、“ ou=Hostmaster ”を作成する。

“ ou=Administrator ”は、契約者の格納場所である。この配下に、メンテナーコード別に証明書格納用エントリ“ cn=JPNIC-AD ＜JPNIC 従業員コード＞ ＜名前＞ ”を作成する。

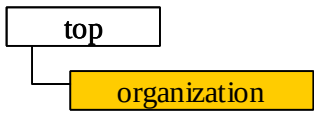
“ ou=Hostmaster ”は、メンテナー申請者の格納場所である。この配下に、メンテナーコード別に、証明書格納用エントリ“ cn=JPNIC-HM ＜JPNIC 従業員コード＞ ＜名前＞ ”を作成する。

オブジェクトクラス
JPNIC CA 情報ツリーで使用するオブジェクトクラスは、以下である。

「使用する属性」は、アプリケーションからの利用に基づいた定義である。そのため、ディレクトリ内における定義とは異なる場合がある。

■ コンテナ用オブジェクトクラス（1）

コンテナを作成するために、organization オブジェクトクラスを使用する。
organization オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

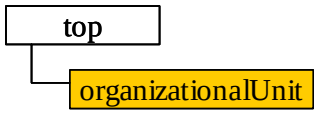
o=Japan Network Information Center

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、組織名	o	○	―	RDN 属性
2	オブジェクトクラス	objectClass	○	―	organization

■ コンテナ用オブジェクトクラス（2）

コンテナを作成するために、organizationalUnit オブジェクトクラスを使用する。
organizationalUnit オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

ou=Internet Resource Service
ou=Secretariat
ou=**＜メンテナーコード＞**
ou=Administrator
ou=Hostmaster

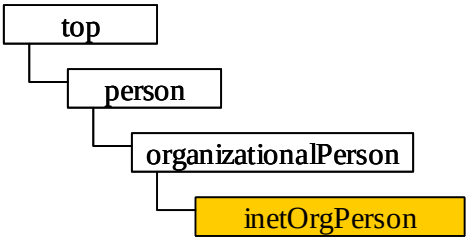
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、メンテナーコード	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit

■ 証明書格納用オブジェクトクラス

証明書を格納するために、inetOrgPerson オブジェクトクラスを使用する。

inetOrgPerson オブジェクトクラスは構造型オブジェクトクラスであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

cn=JPNIC-AD ＜JPNIC**従業員コード**＞ ＜**名前**＞

cn=JPNIC-HM ＜JPNIC**従業員コード**＞ ＜**名前**＞

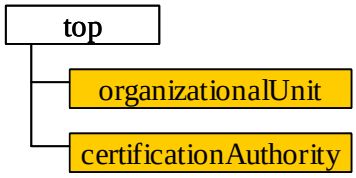
使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名	cn	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	inetOrgPerson
3	名前	sn	○	－	cn と同値
4	ライセンス ID	uid	－	－	
5	電子メールアドレス	mail	○	－	
6	オンラインフラグ	o	○	－	“ online ”,“ offline ”,“ ”(値無し)
7	証明書	userSMIMECertificate	－	－	binary、カレントの証明書
8	証明書＜履歴＞	userCertificate	－	○	binary、証明書の履歴

■ CA 用オブジェクトクラス

CA を作成するために、ornaginzationalUnit オブジェクトクラス、certificationAuthority オブジェクトクラスを使用する。

organizationalUnit オブジェクトクラスは構造型オブジェクトクラス、certificationAuthority オブジェクトクラスは補助型オブジェクトであり、以下の構成である。



ツリー内における対象オブジェクトは、以下である。

ou=JPNIC Root Certification Authority

ou=JPNIC Resource Service Certification Authority

使用する属性は、以下である。

	名称	LDAP 属性	必須	複数値	備考
1	表示名、CA	ou	○	－	RDN 属性
2	オブジェクトクラス	objectClass	○	－	organizationalUnit
3	補助クラス	objectClass	○	－	certificationAuthority
4	CA 証明書	cACertificate	○	－	binary
5	ARL	authorityRevocationList	○	－	binary
6	CRL	certificateRevocationList	○	－	binary

5.2.5. 業務設計

業務設計では、すべての業務関係者の業務フローを作成した。その上で必要な機能の洗い出し、やりとりが発生する情報の洗い出し等を行った。

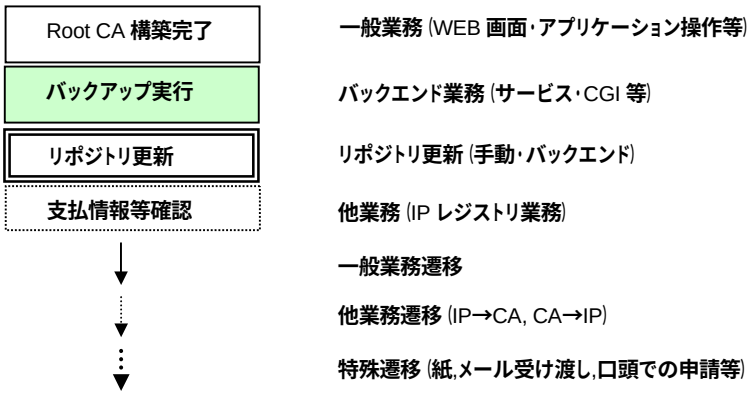
5.2.5.1. 業務フロー一覧

	業務内容	JPNIC CA 運用担当者	JPNIC RootCA 管理者	JPNIC IP アドレス CA 管理者	JPNIC 業務管理者	JPNIC 業務担当者	契約管理者	資源管理者	一般申請者
1	JPNIC ルート認証局構築業務	○	○						
2	JPNIC ルート認証局失効業務	○	○						
3	JPNIC ルート認証局鍵更新業務	○	○						
4	JPNIC ルート認証局 CRL 発行業務	○	○						
5	JPNIC ルート認証局バックアップ業務	○							
6	IP アドレス認証局(認証)構築業務	○	○	○					
7	IP アドレス認証局(認証)失効業務	○	○	○					
8	IP アドレス認証局(認証)鍵更新業務	○	○	○					
9	IP アドレス認証局(認証) CRL 発行業務	○		○					
10	IP アドレス認証局(認証)バックアップ業務	○							
11	JPNIC 業務			○	○				

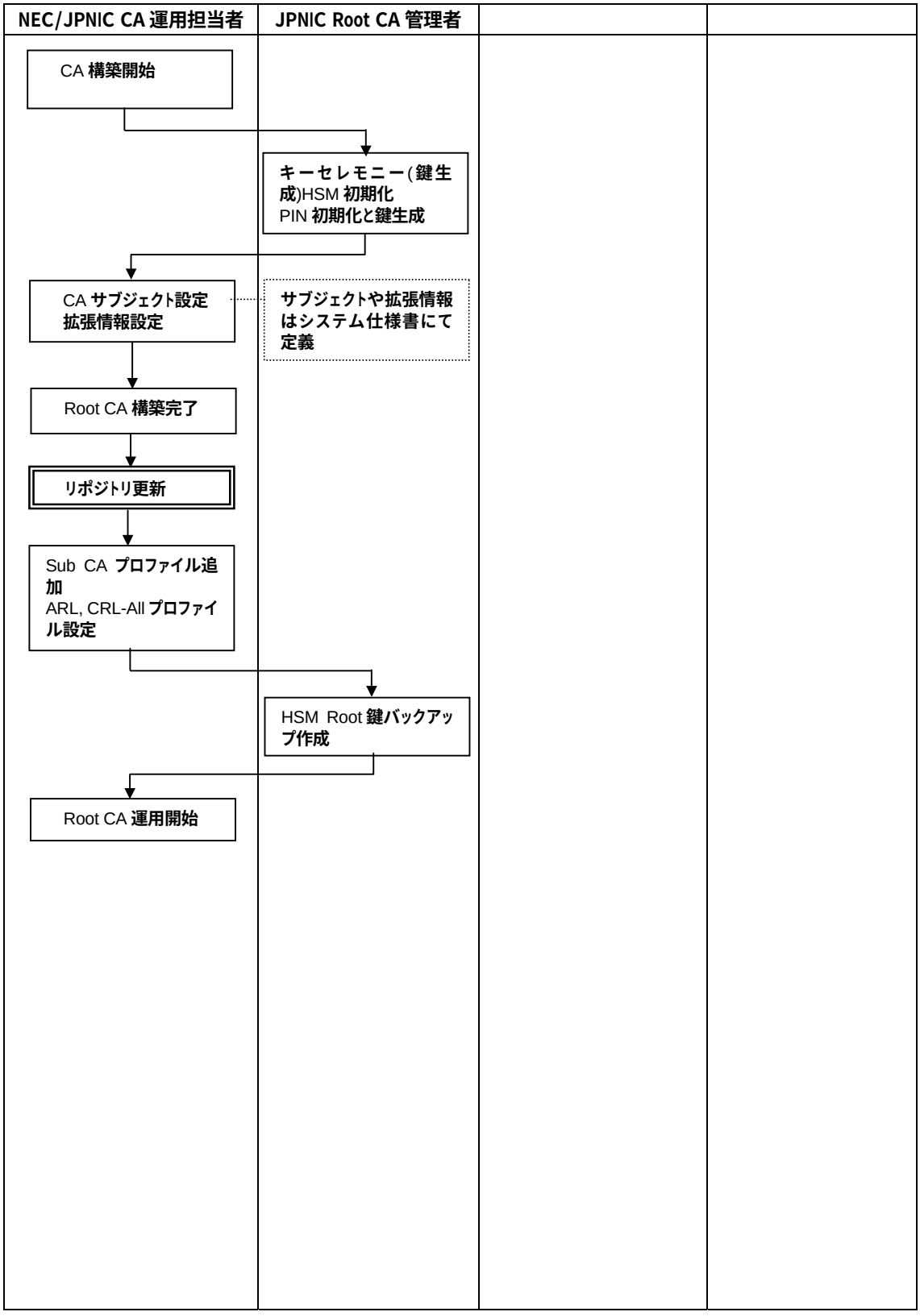
	管理者証明書 発行業務								
12	JPNIC 業務 管理者証明書 失効業務			○	○				
13	JPNIC 業務 管理者証明書 更新業務			○	○				
14	JPNIC 業務 担当者証明書 発行業務			○	○	○			
15	JPNIC 業務 担当者証明書 失効業務			○	○	○			
16	JPNIC 業務 担当者証明書 更新業務			○	○	○			
17	メンテナー契約 管理者証明書 発行業務			○	○	○	○		
18	メンテナー資源 管理者証明書 発行業務			○	○	○		○	
19	メンテナー契約 管理者証明書 失効業務				○	○	○		
20	メンテナー資源 管理者証明書 失効業務				○	○		○	
21	メンテナー契約 管理者証明書 更新業務			○	○	○	○		
22	メンテナー資源 管理者証明書 更新業務			○	○	○		○	
23	メンテナー 申請者証明書 発行業務						○	○	○

24	メンテナー 申請者証明書 失効業務						○	○	○
25	メンテナー 申請者証明書 更新業務						○	○	○
26	指定事業者 サーバ証明書 発行業務			○		○	○		
27	指定事業者 サーバ証明書 失効業務			○		○	○		
28	指定事業者 サーバ証明書 更新業務			○		○	○		

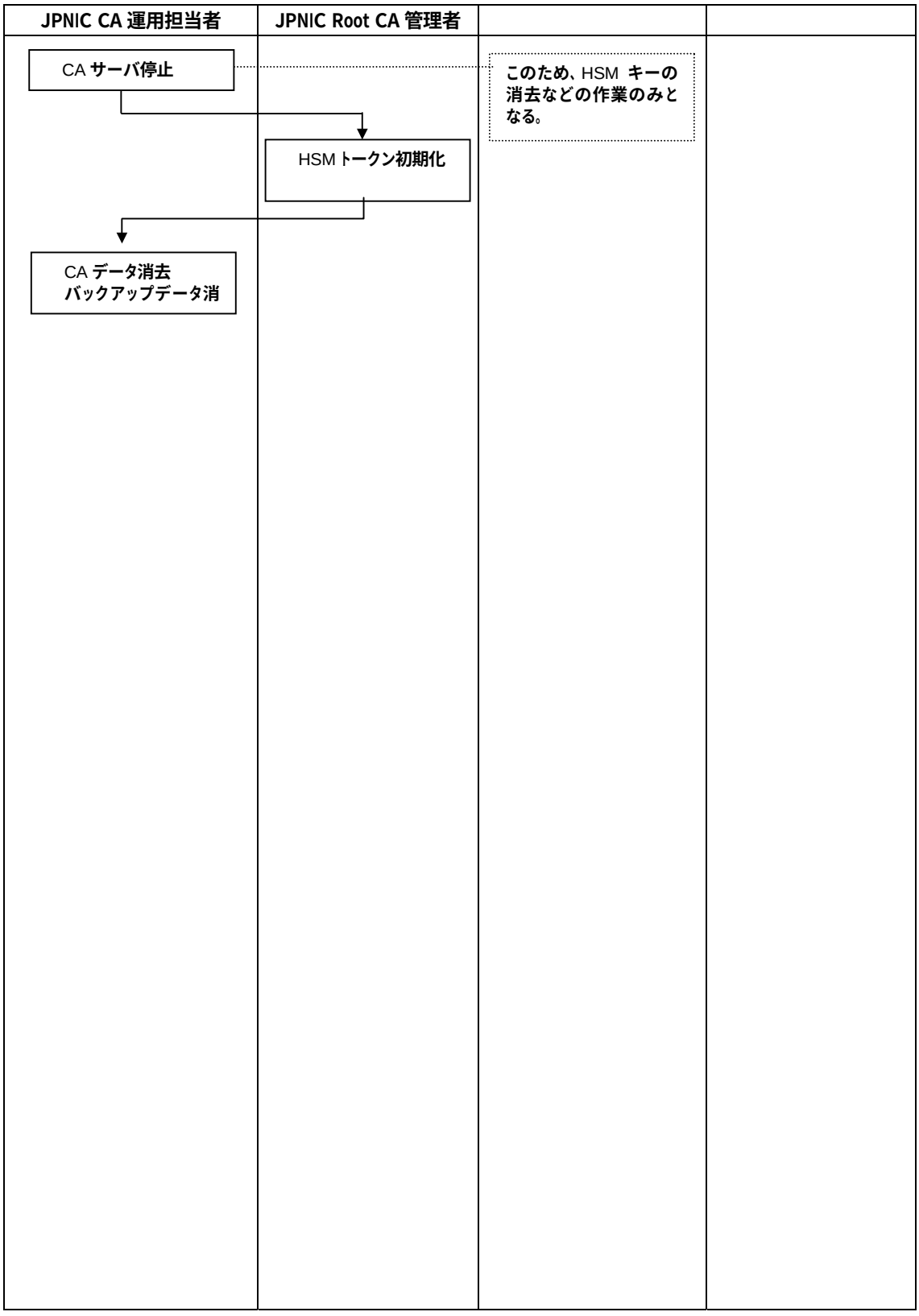
凡例



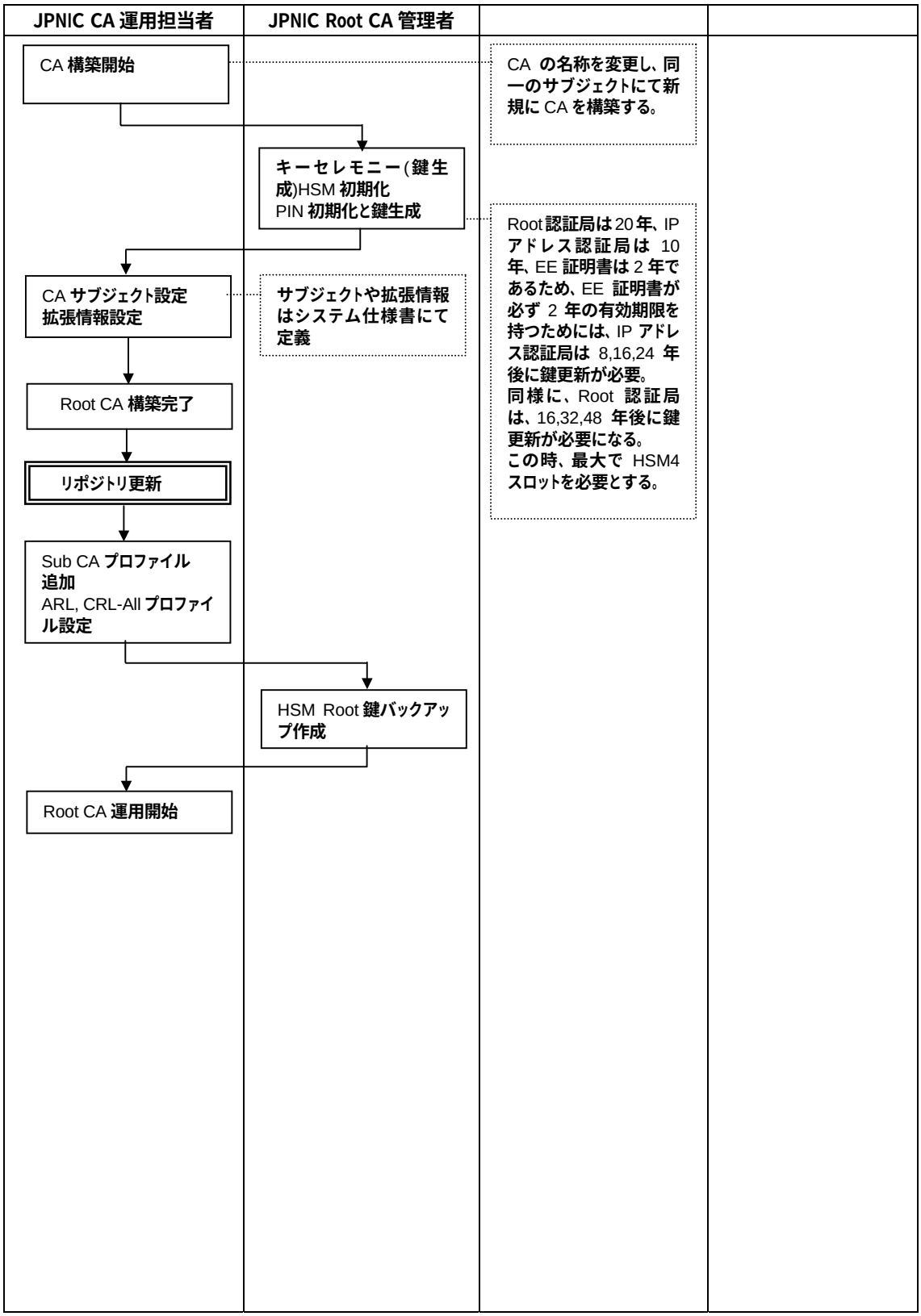
5.2.5.2. JPNICルート認証局構築業務



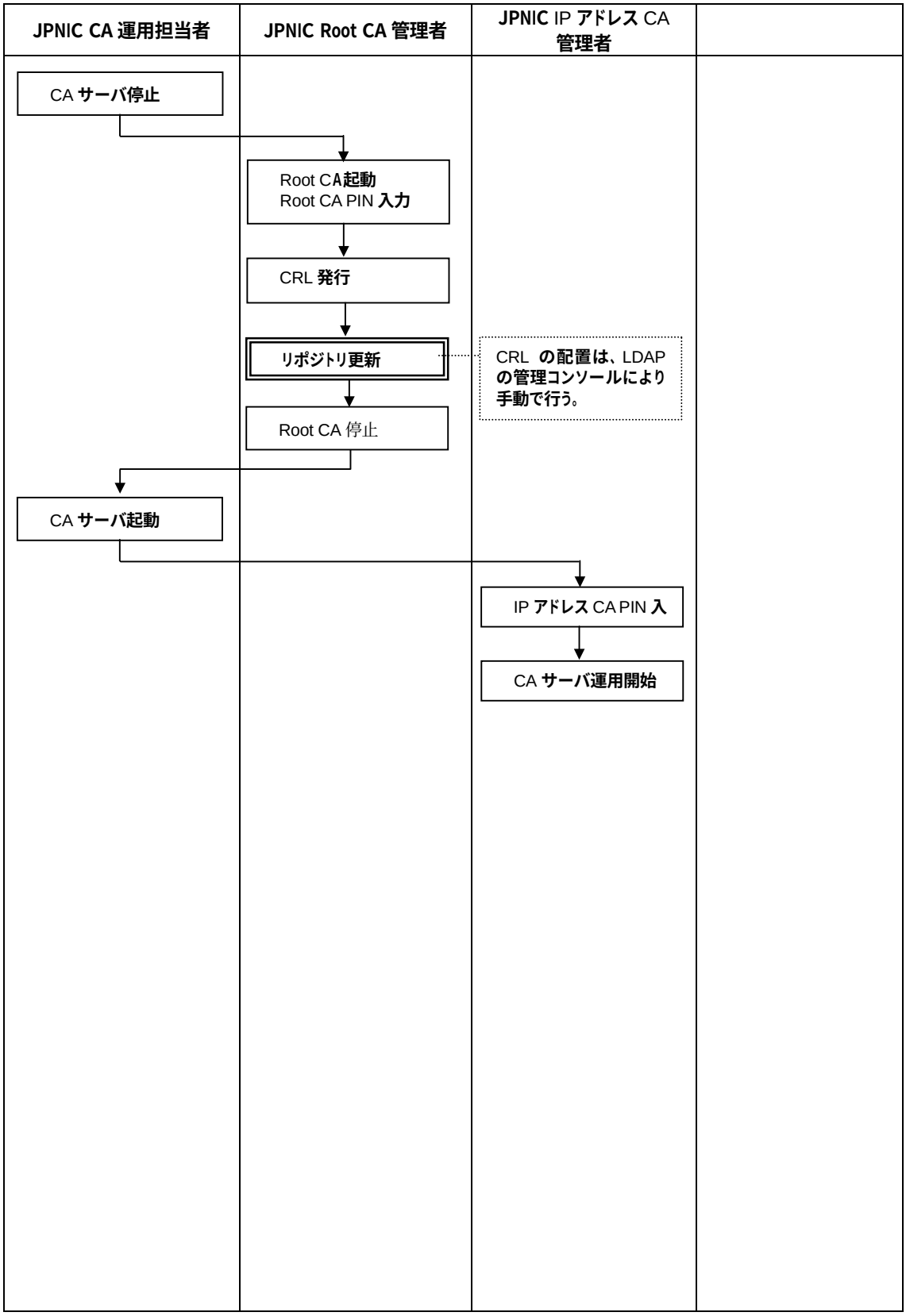
5.2.5.3. JPNICルート認証局失効業務



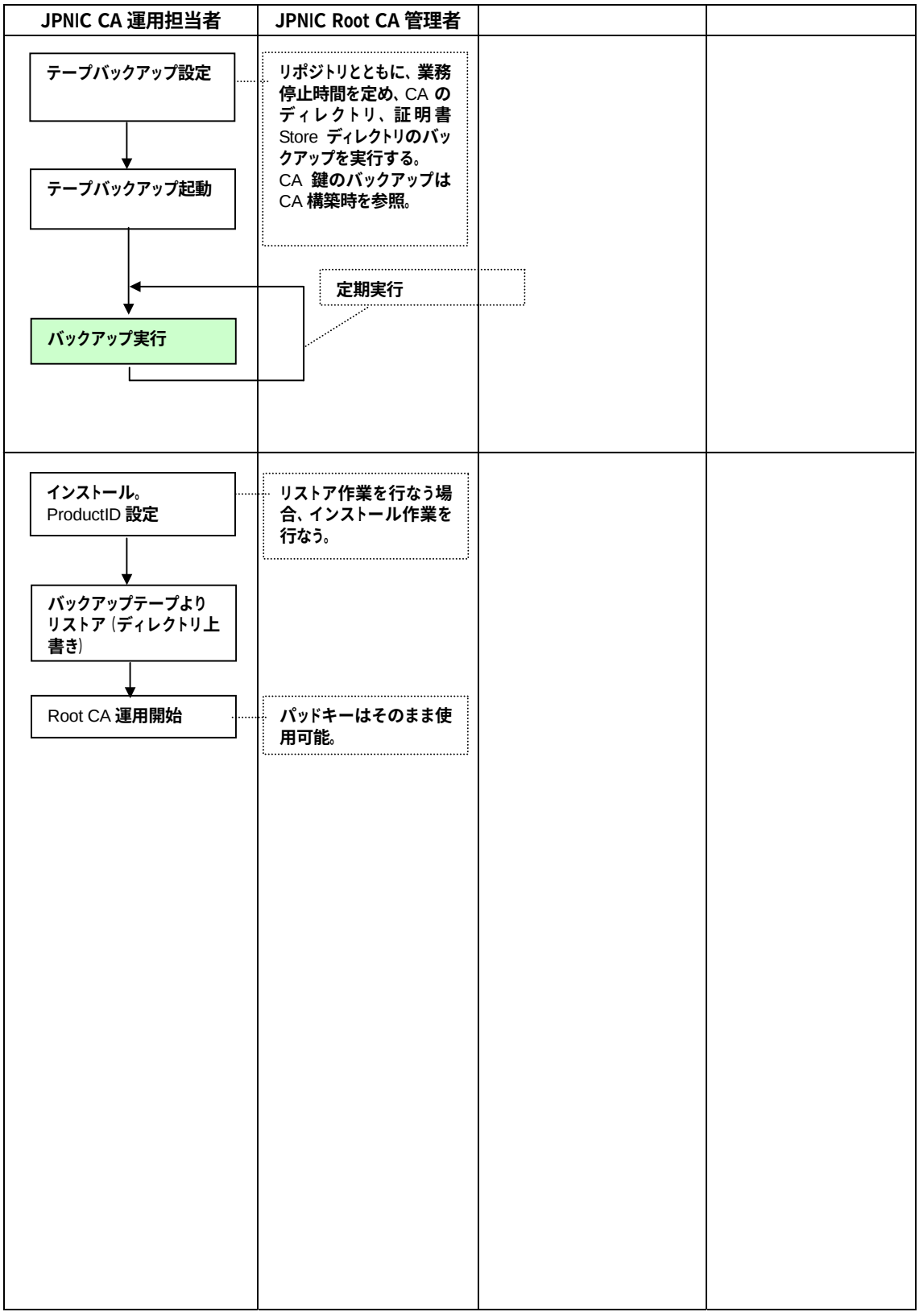
5.2.5.4. JPNICルート認証局鍵更新業務



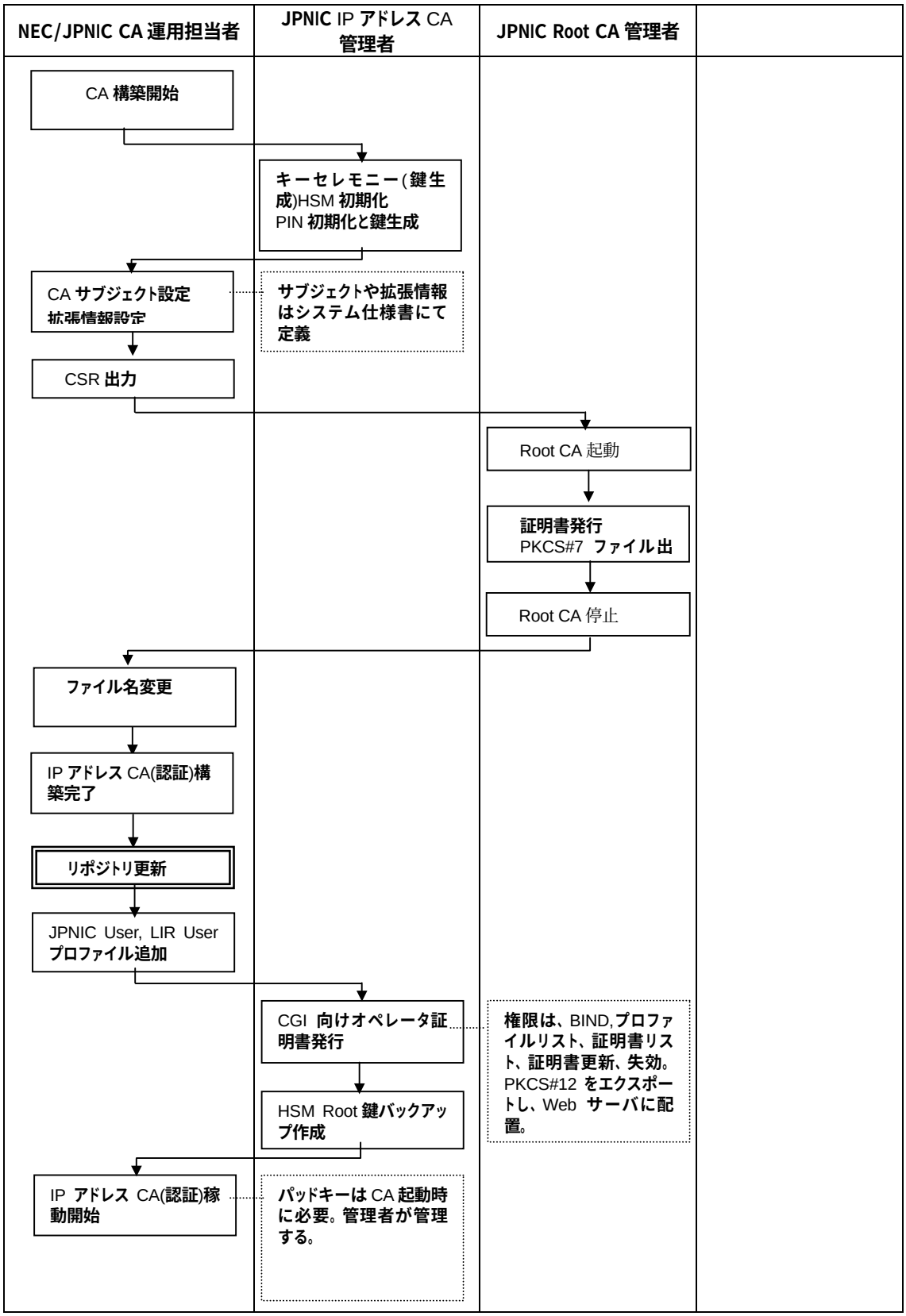
5.2.5.5. JPNICルート認証局CRL発行業務



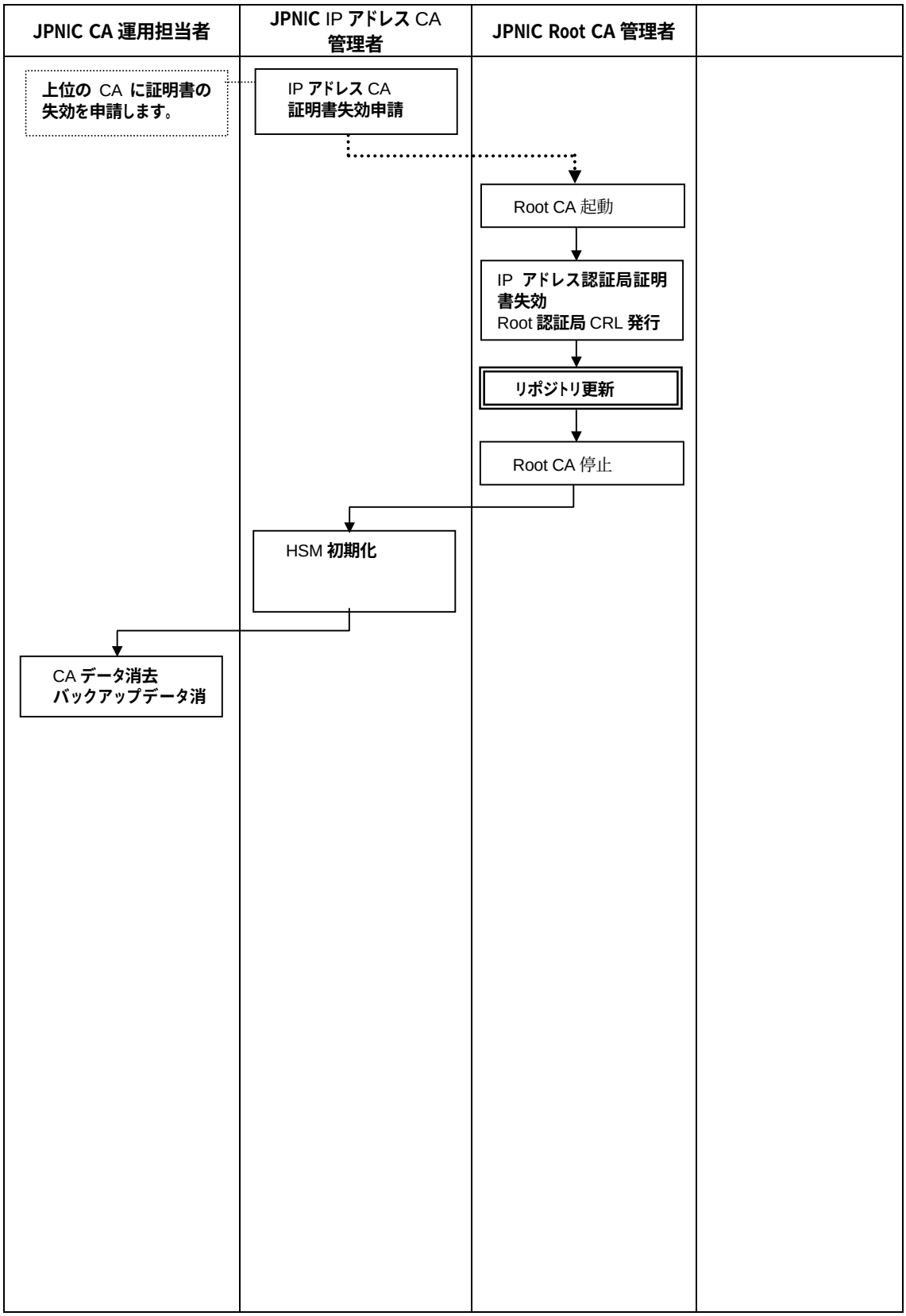
5.2.5.6. JPNICルート認証局バックアップ業務



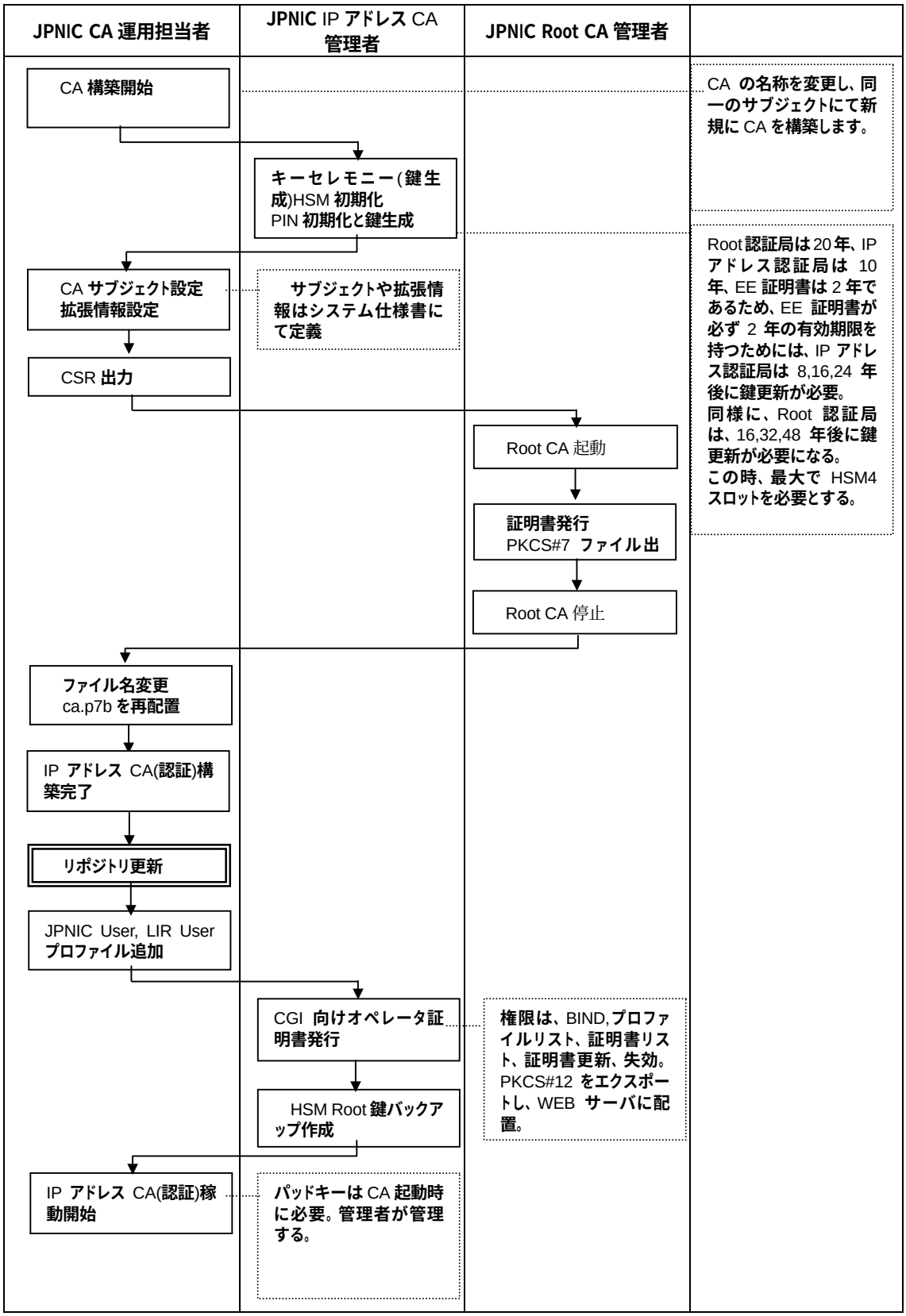
5.2.5.7. IPアドレス認証局(認証)構築業務



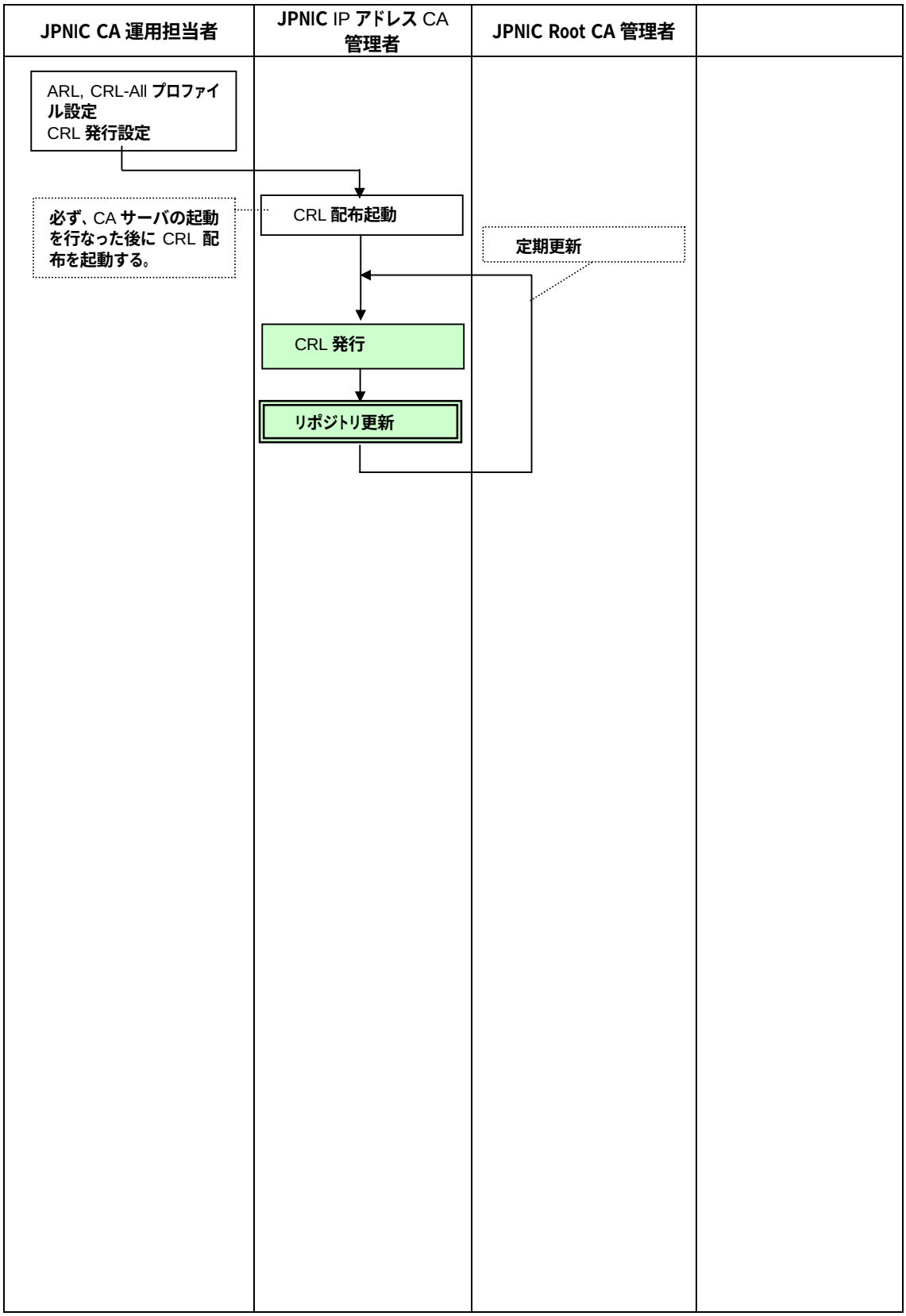
5.2.5.8. IPアドレス認証局(認証)失効業務



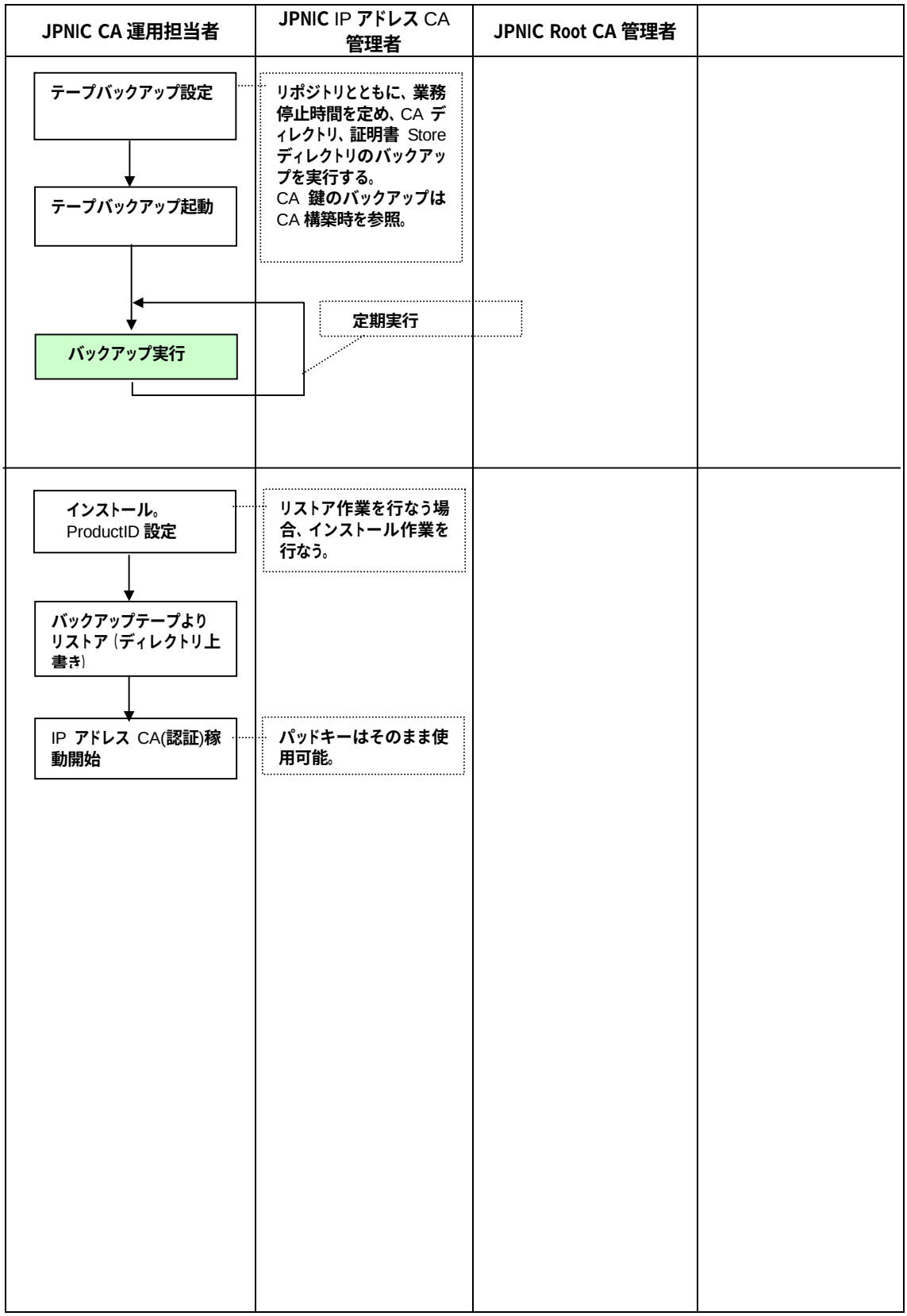
5.2.5.9. IPアドレス認証局(認証)更新業務



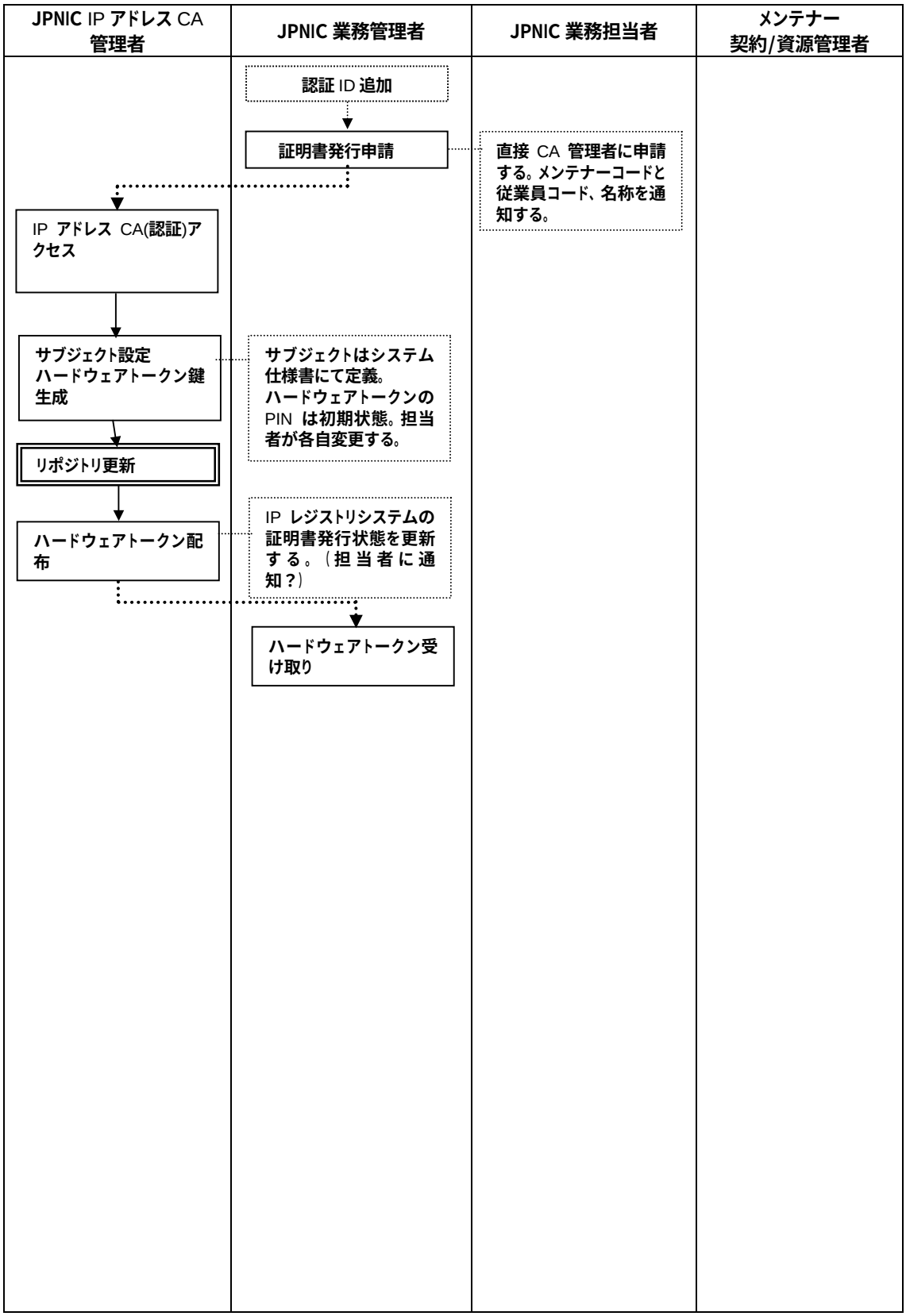
5.2.5.10. IPアドレス認証局(認証)CRL発行業務



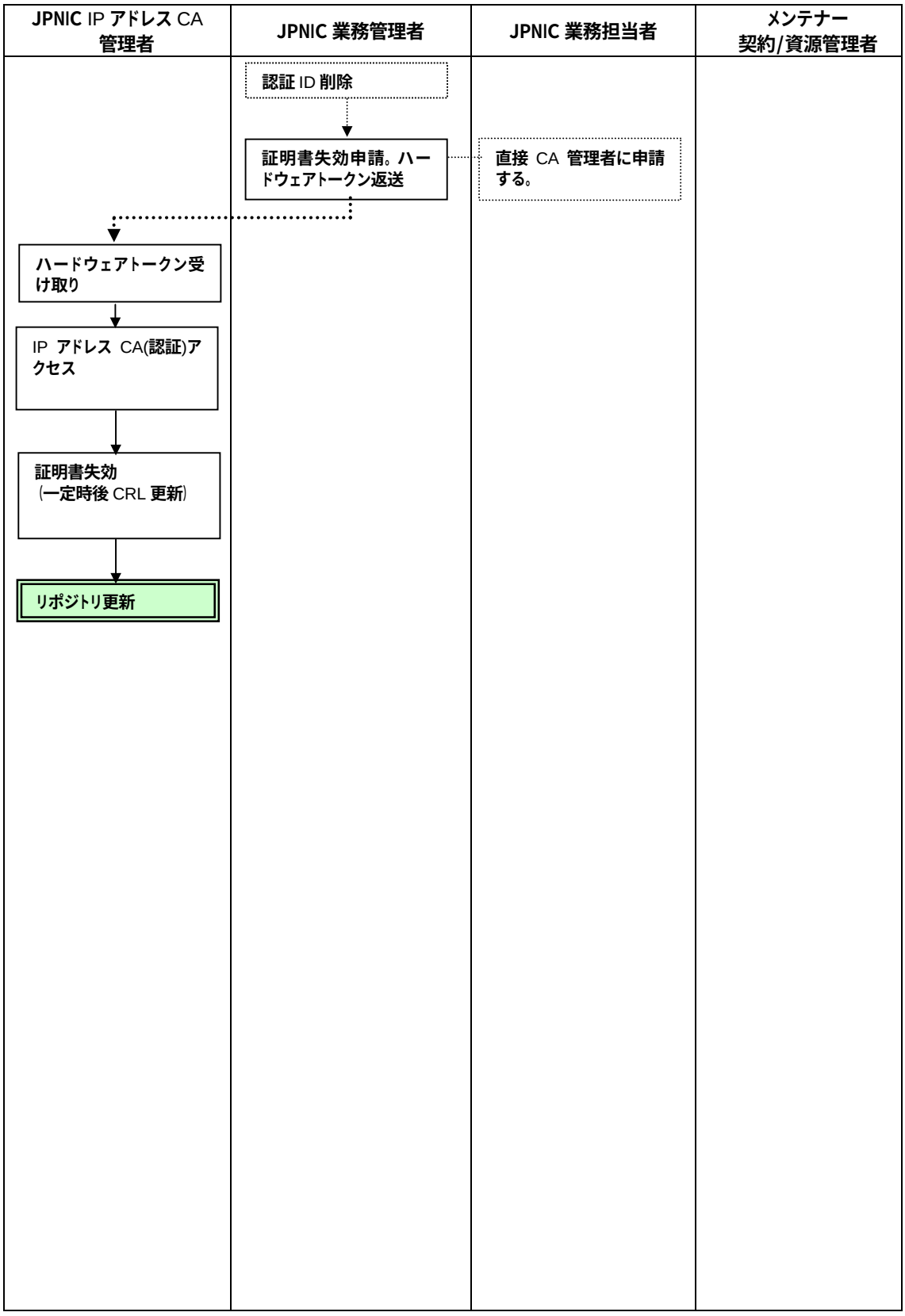
5.2.5.11. IPアドレス認証局(認証)バックアップ業務



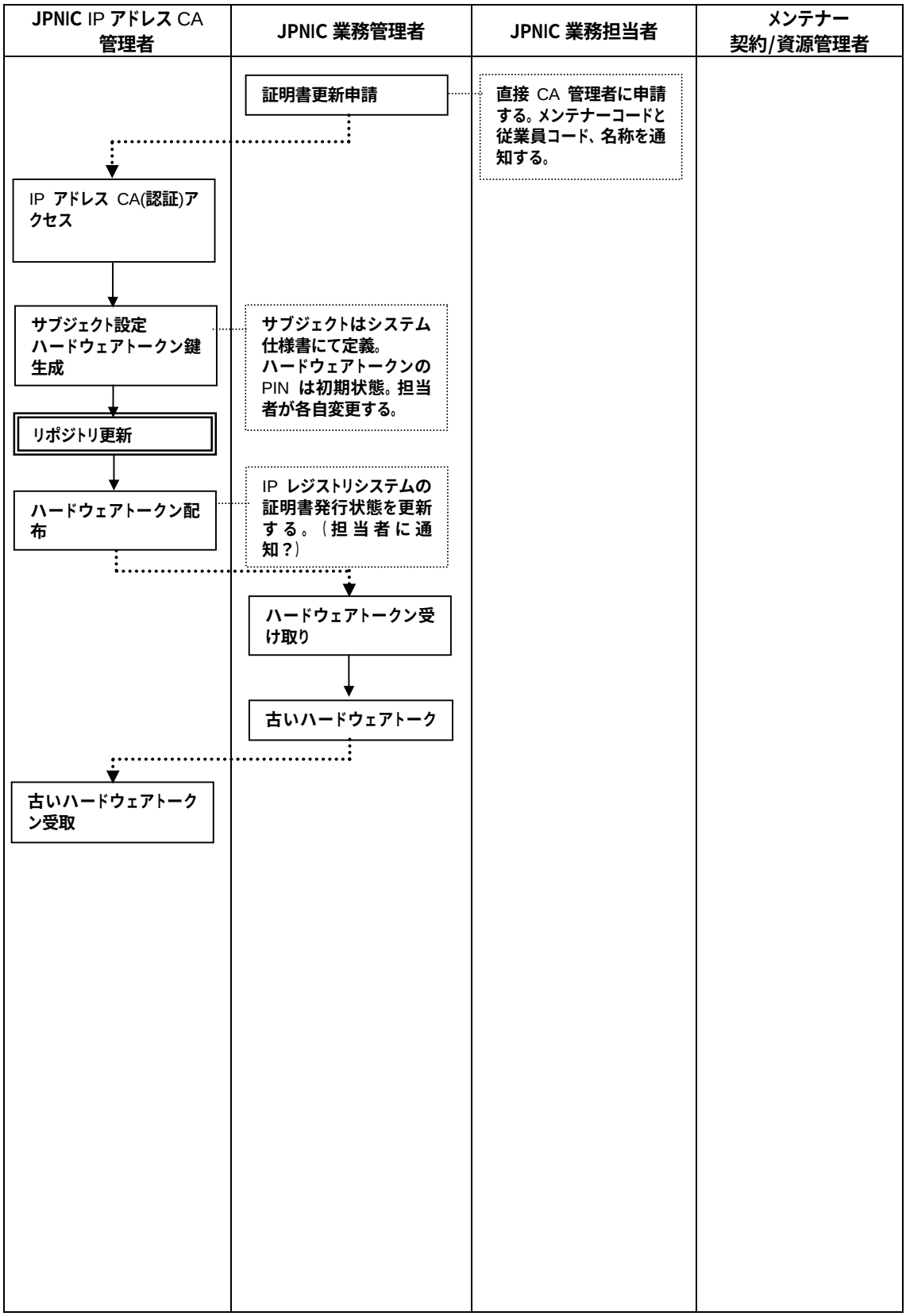
5.2.5.12. JPNIC業務管理者証明書発行業務



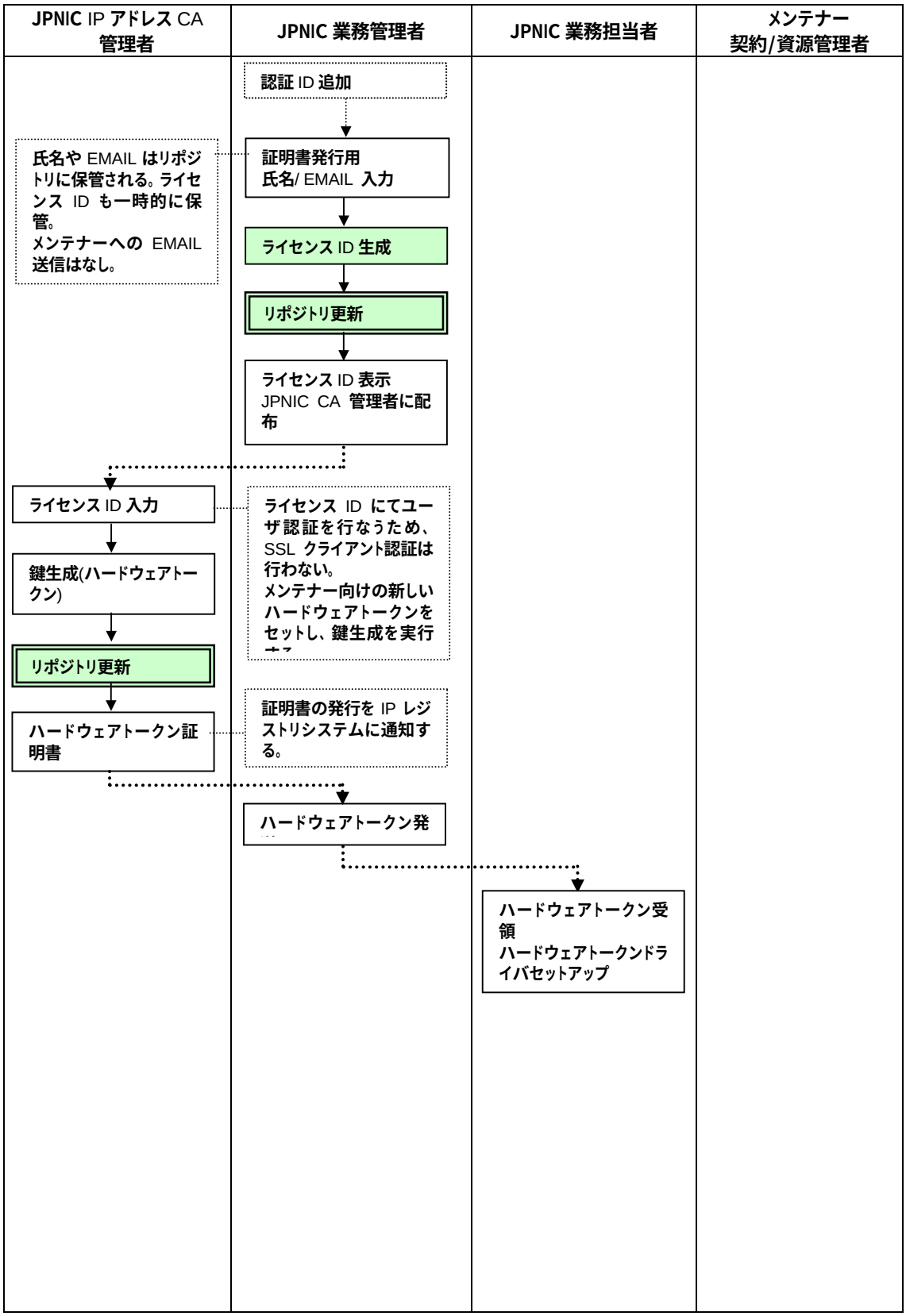
5.2.5.13. JPNIC業務管理者証明書失効業務



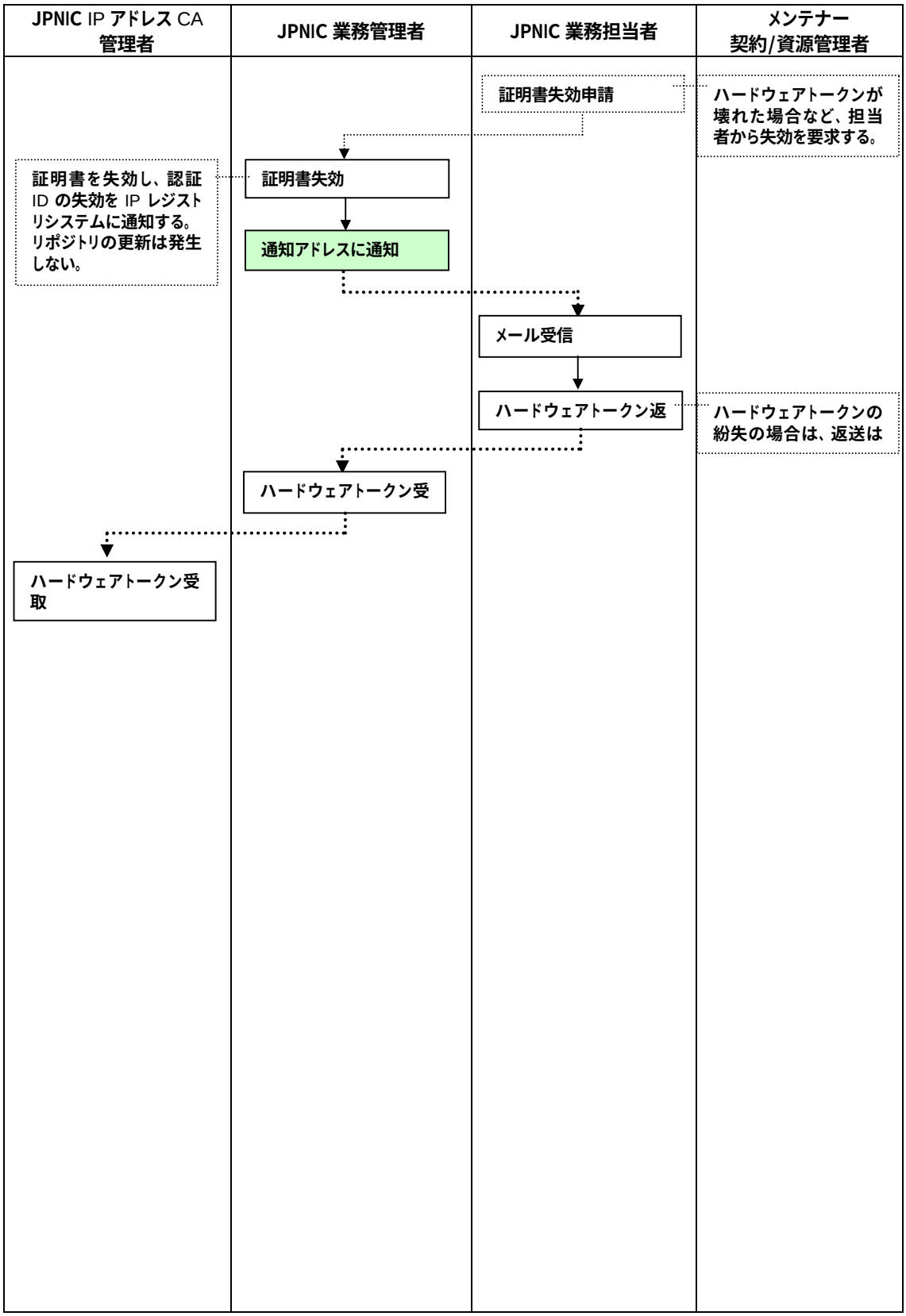
5.2.5.14. JPNIC業務管理者証明書更新業務



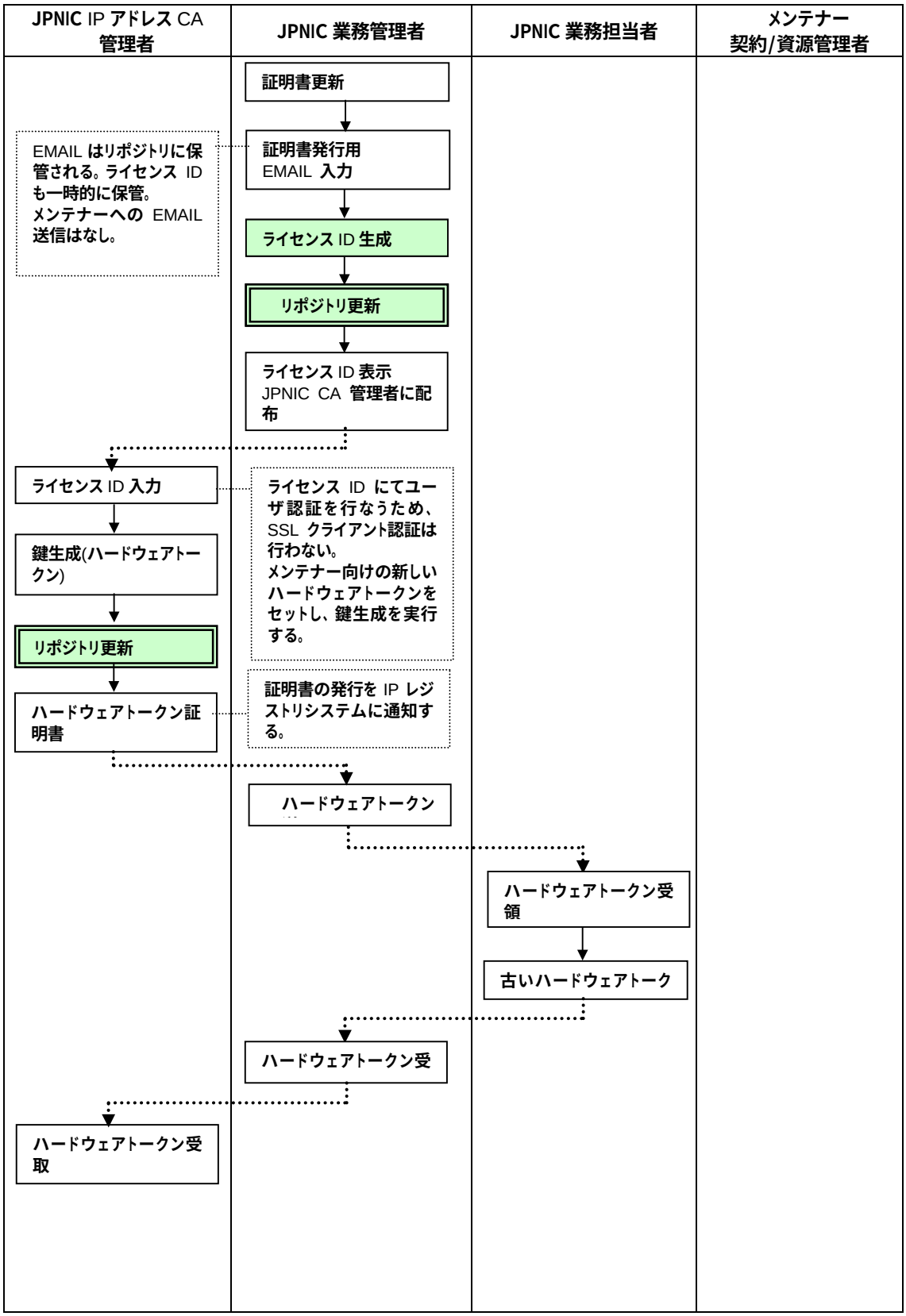
5.2.5.15. JPNIC業務担当者証明書発行業務



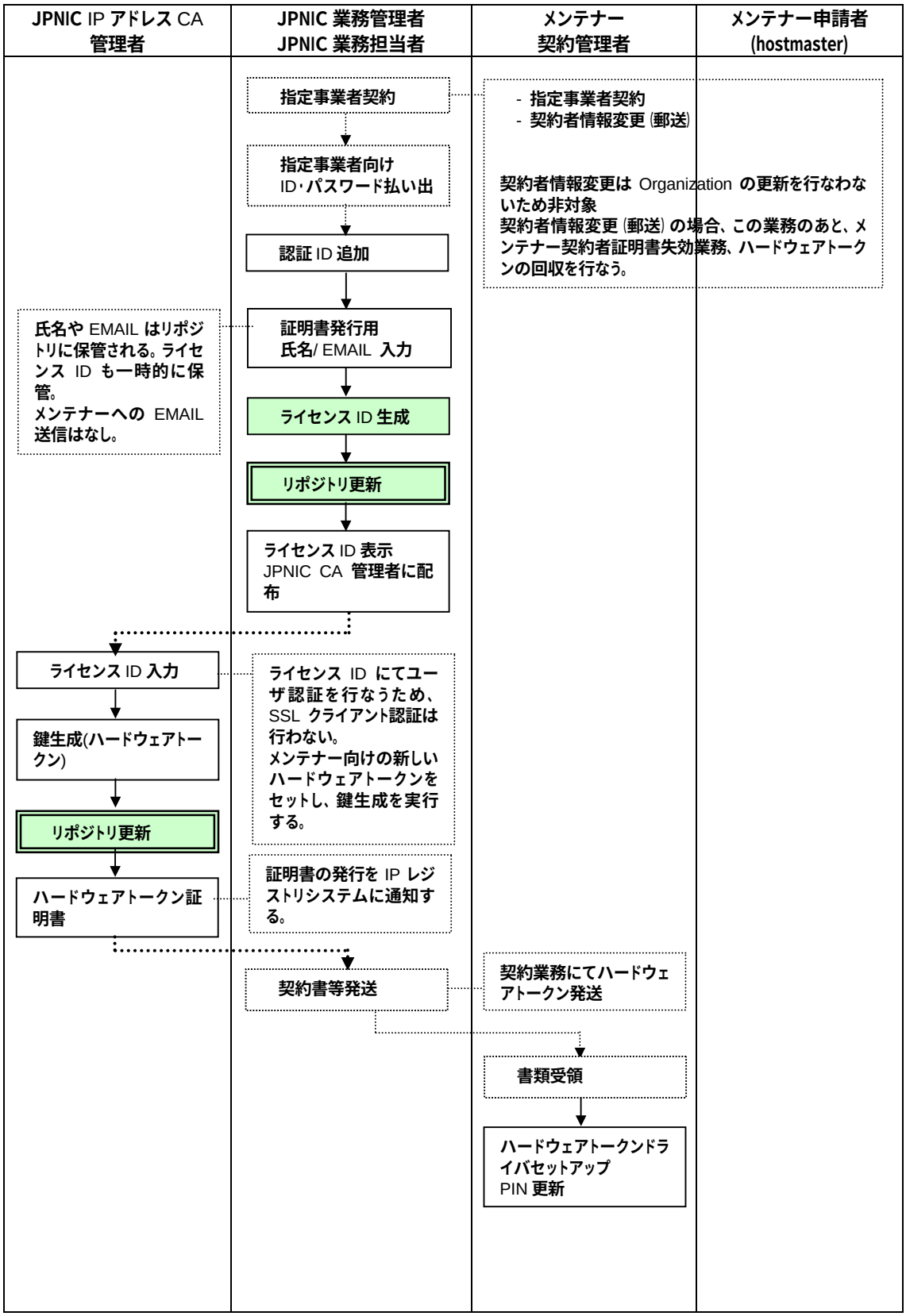
5.2.5.16. JPNIC業務担当者証明書失効業務



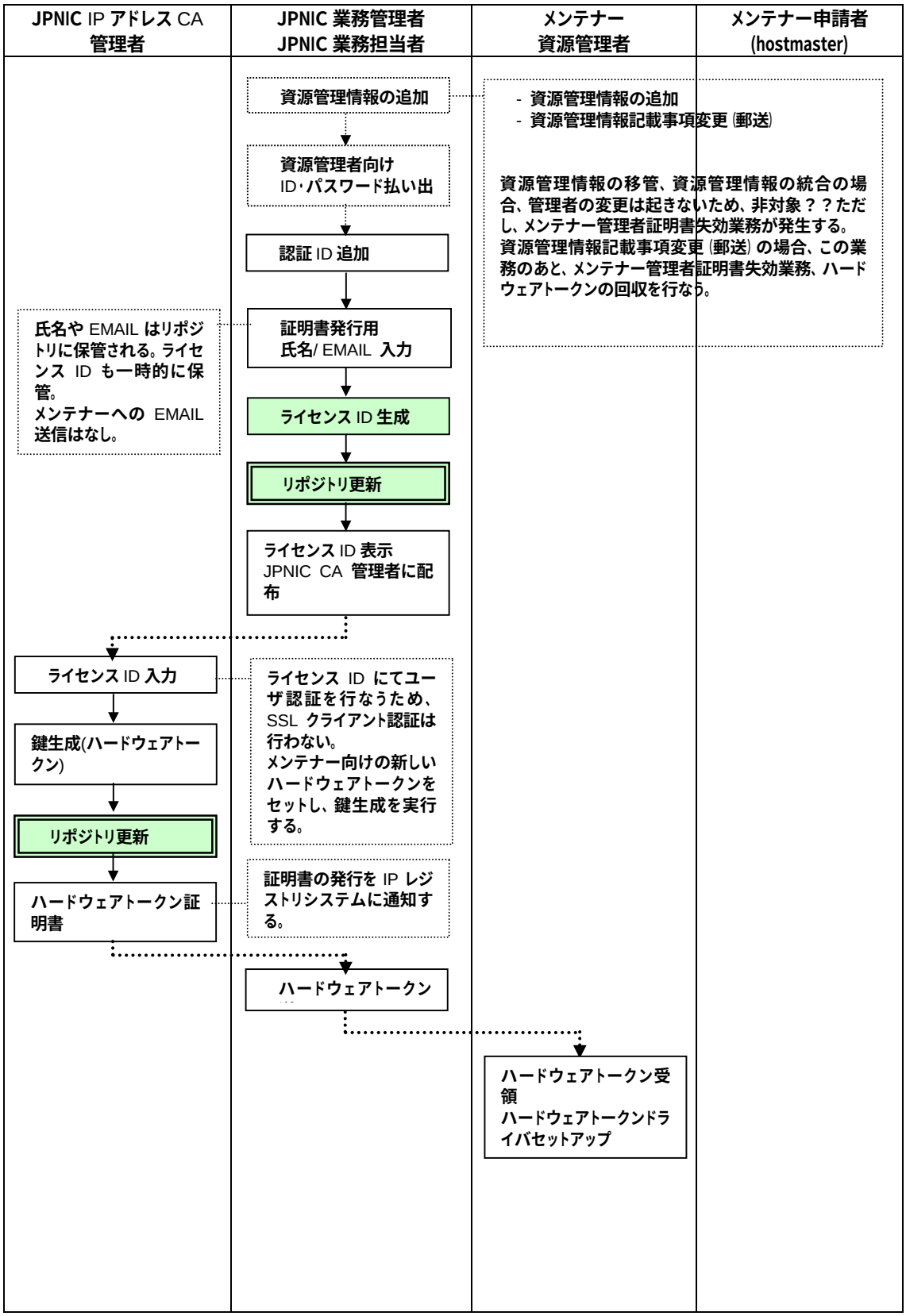
5.2.5.17. JPNIC業務担当者証明書更新業務



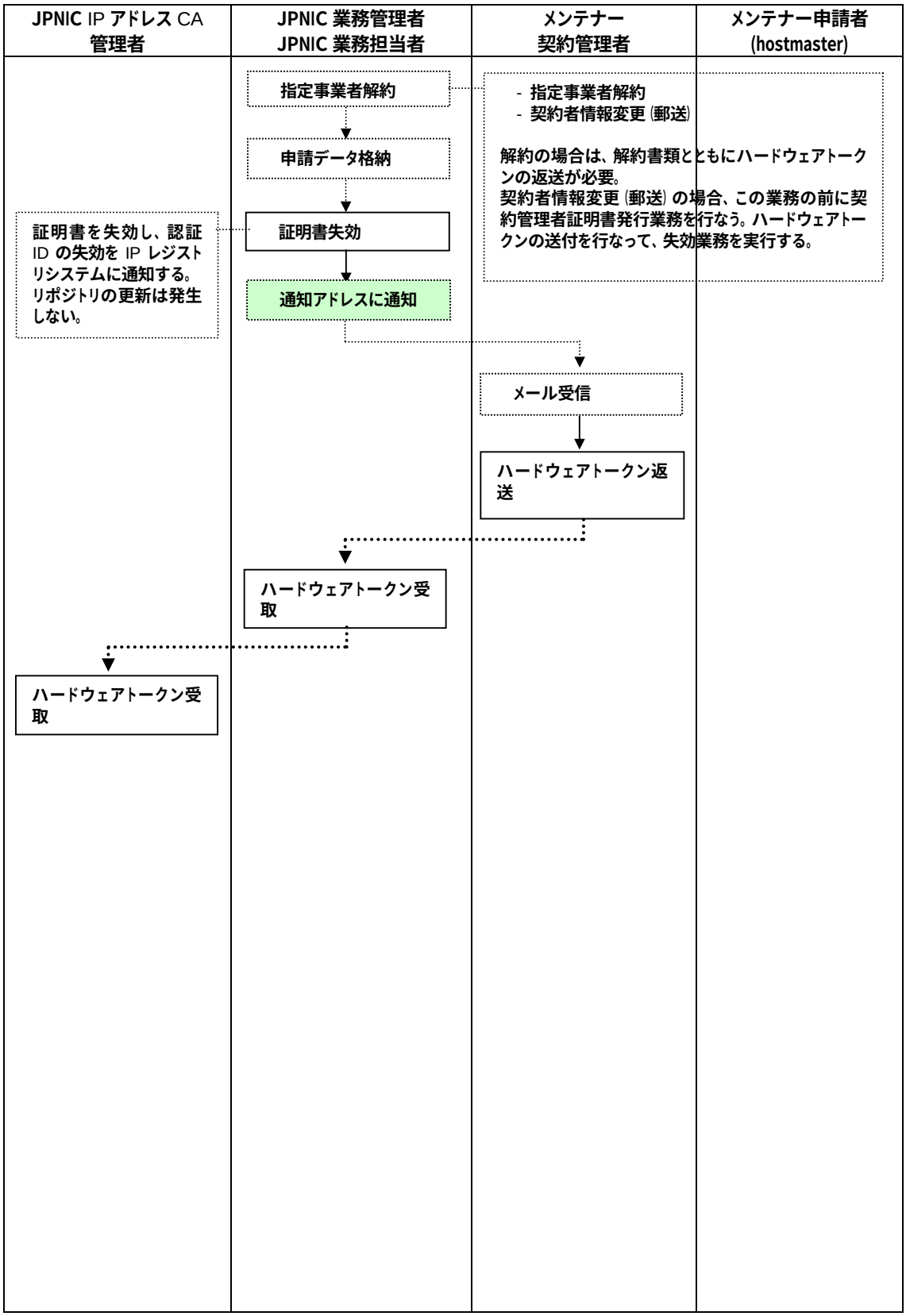
5.2.5.18. メンテナー契約管理者証明書発行業務



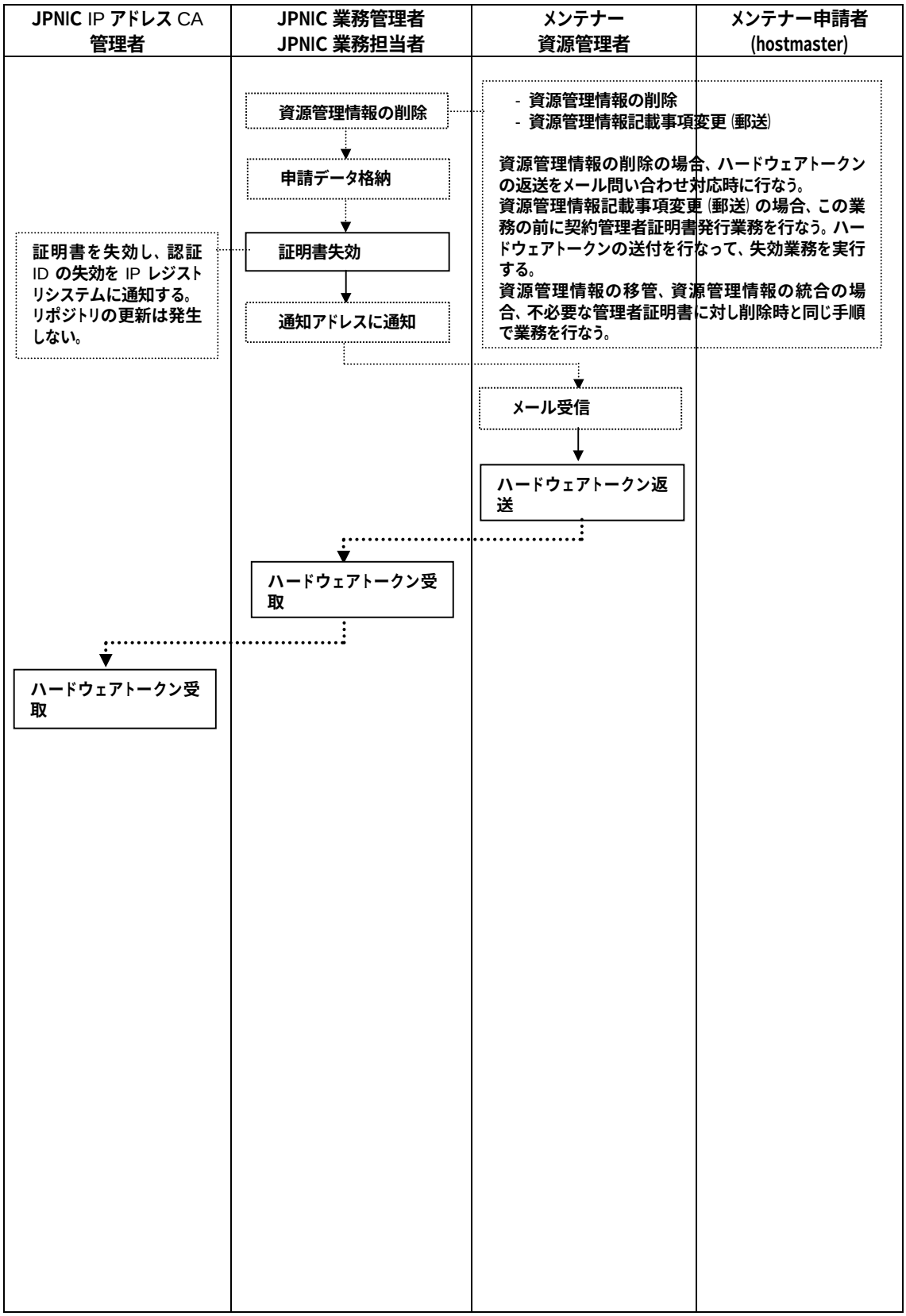
5.2.5.19. メンテナー資源管理者証明書発行業務



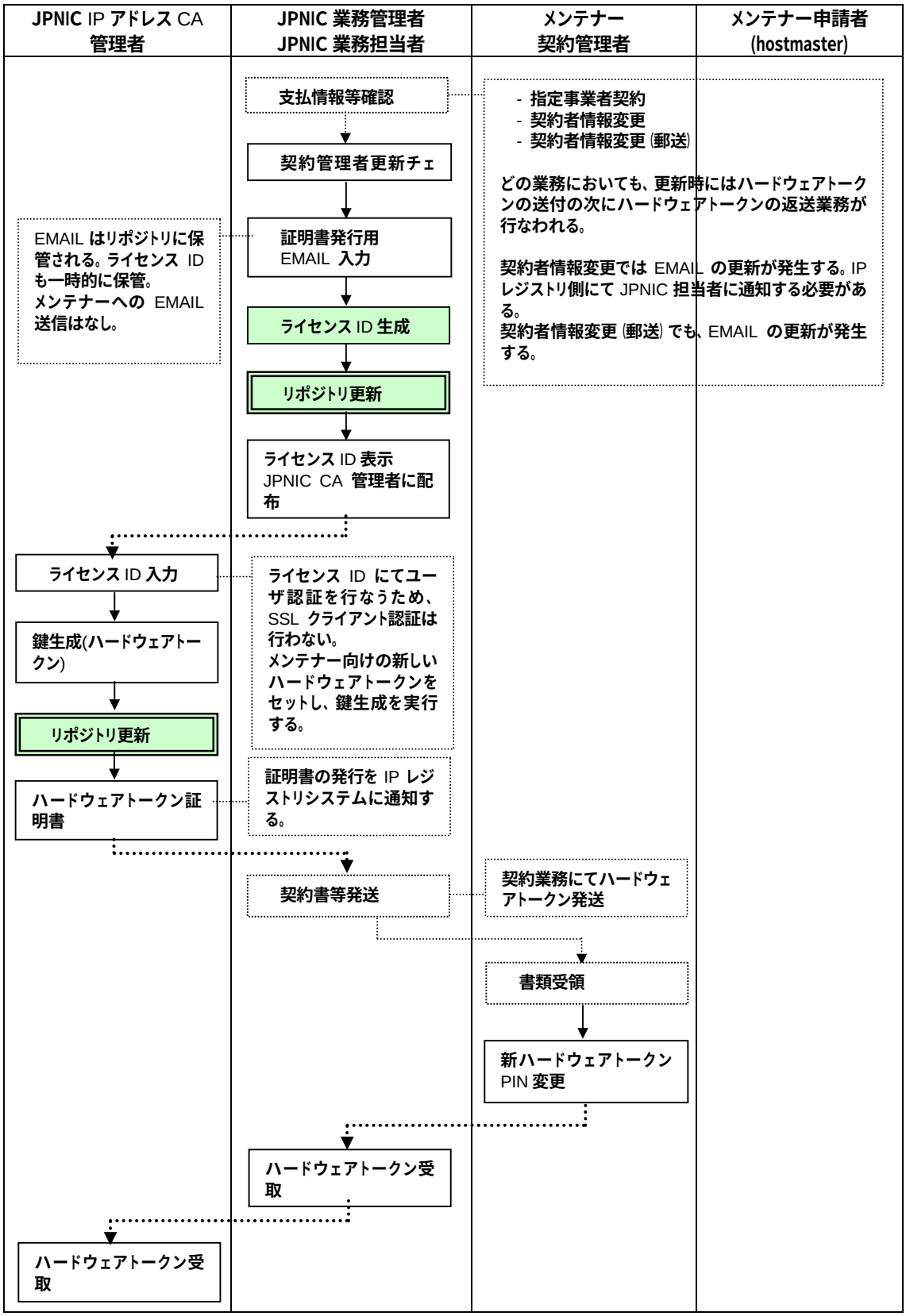
5.2.5.20. メンテナー契約管理者証明書失効業務



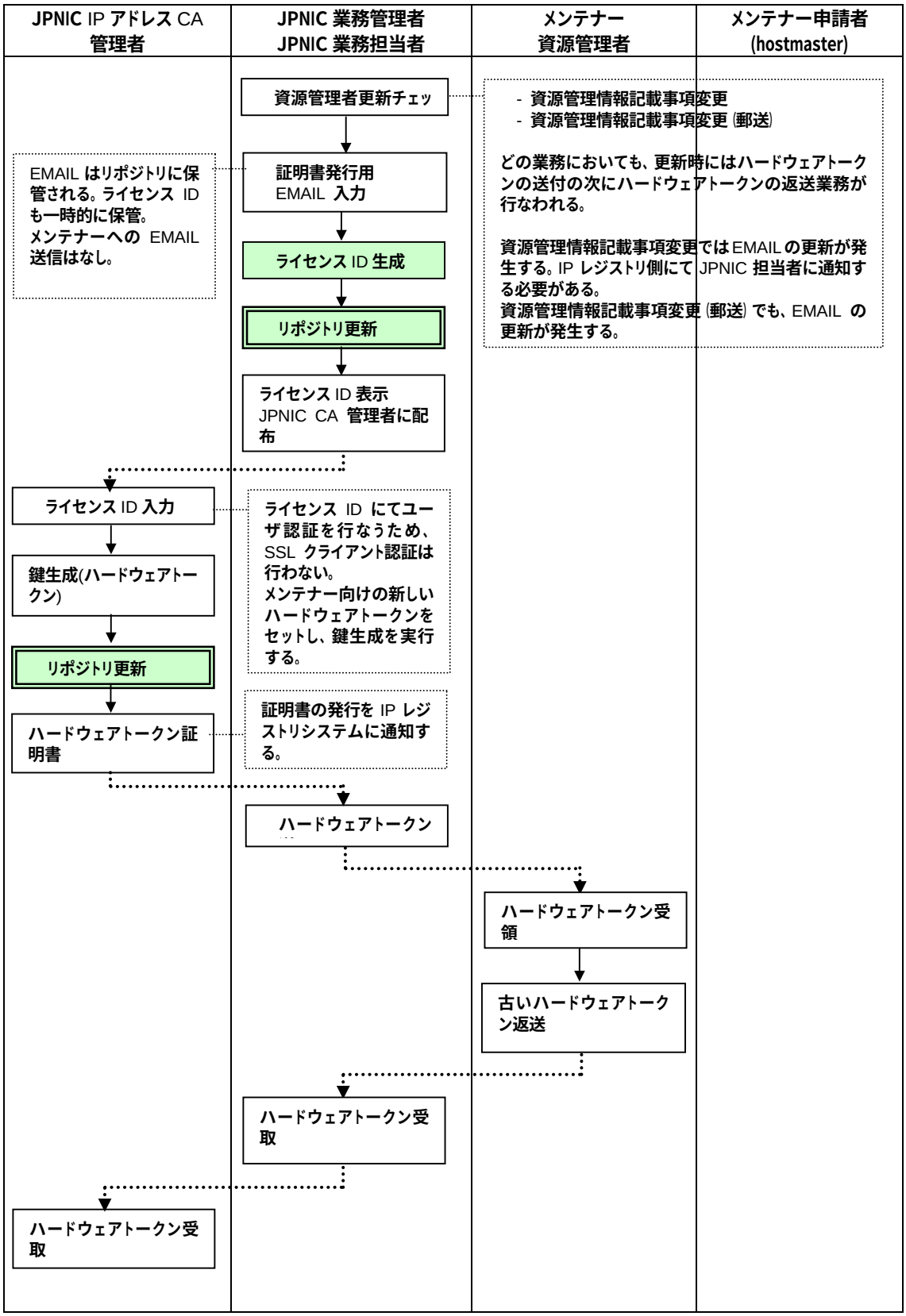
5.2.5.21. メンテナー資源管理者証明書失効業務



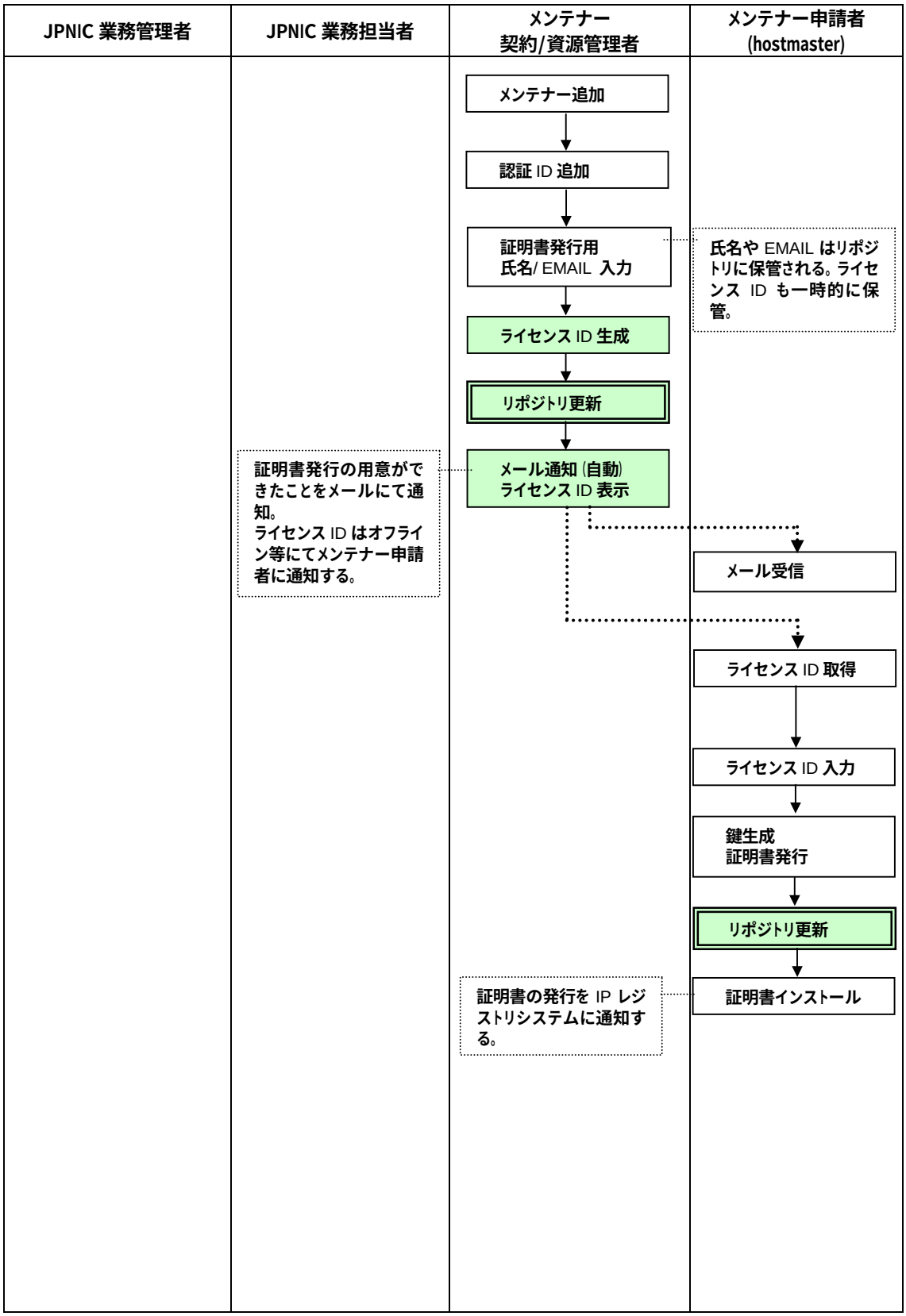
5.2.5.22. メンテナー契約管理者証明書更新業務



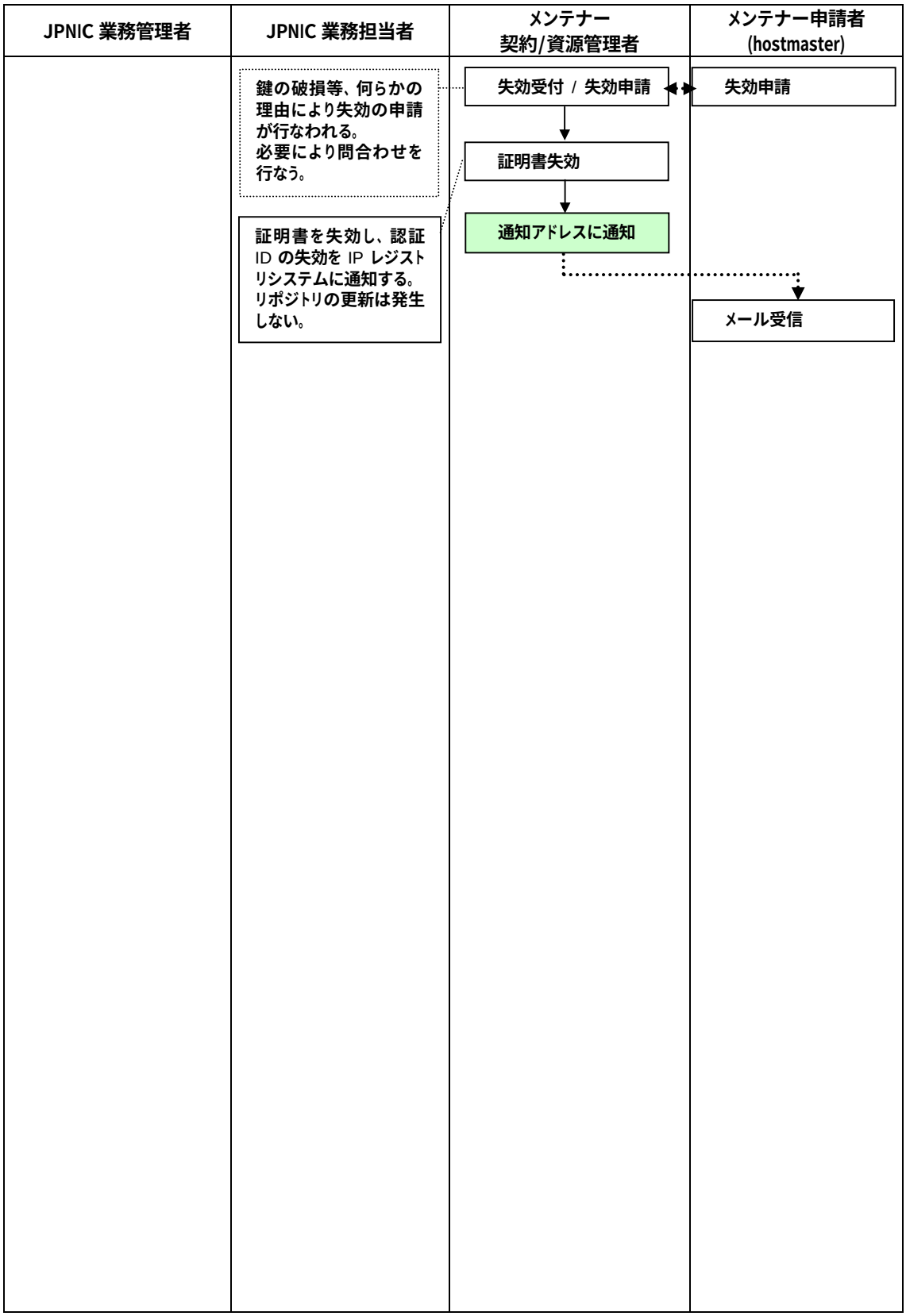
5.2.5.23. メンテナー資源管理者証明書更新業務



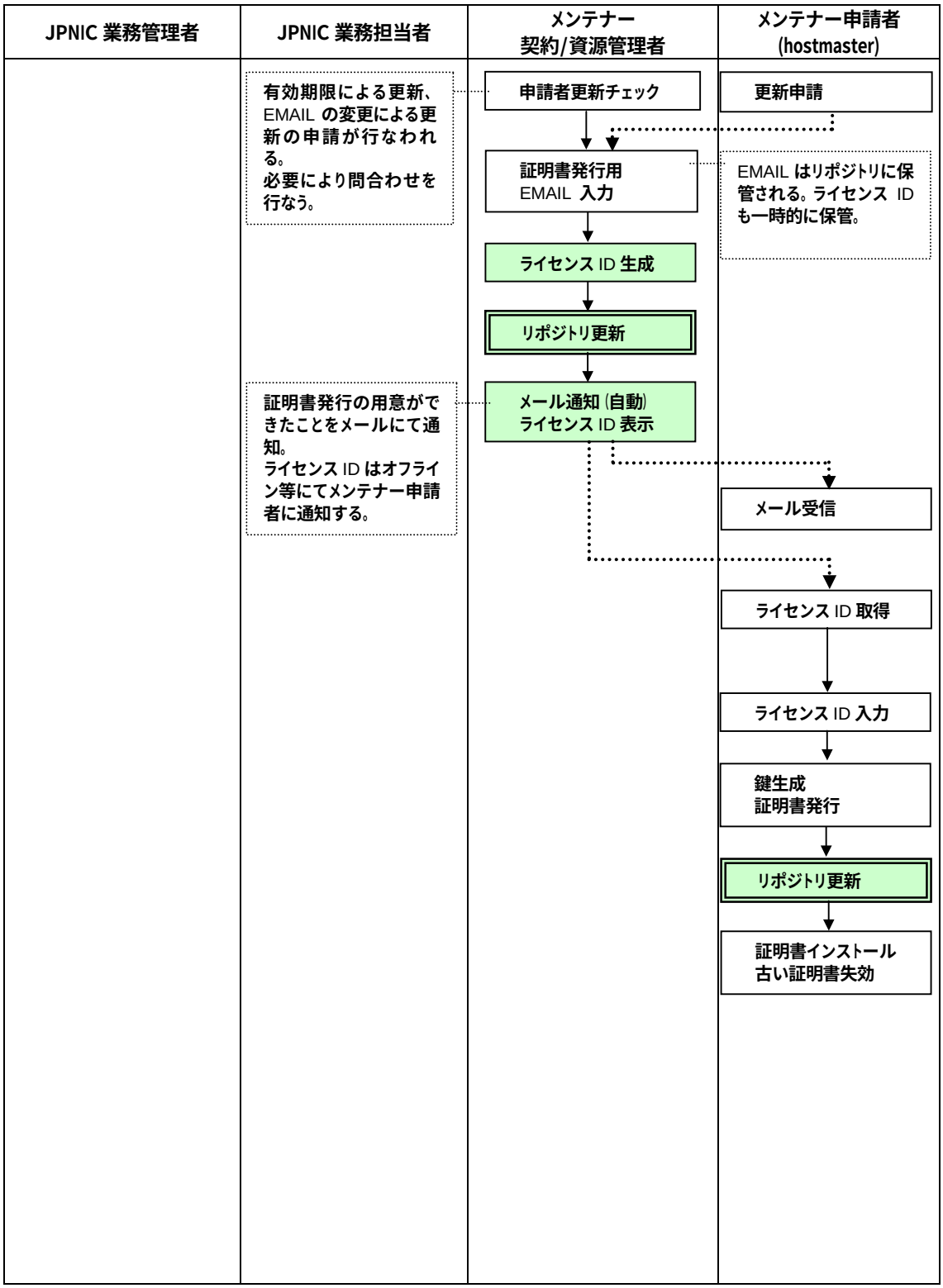
5.2.5.24. メンテナー申請者証明書発行業務



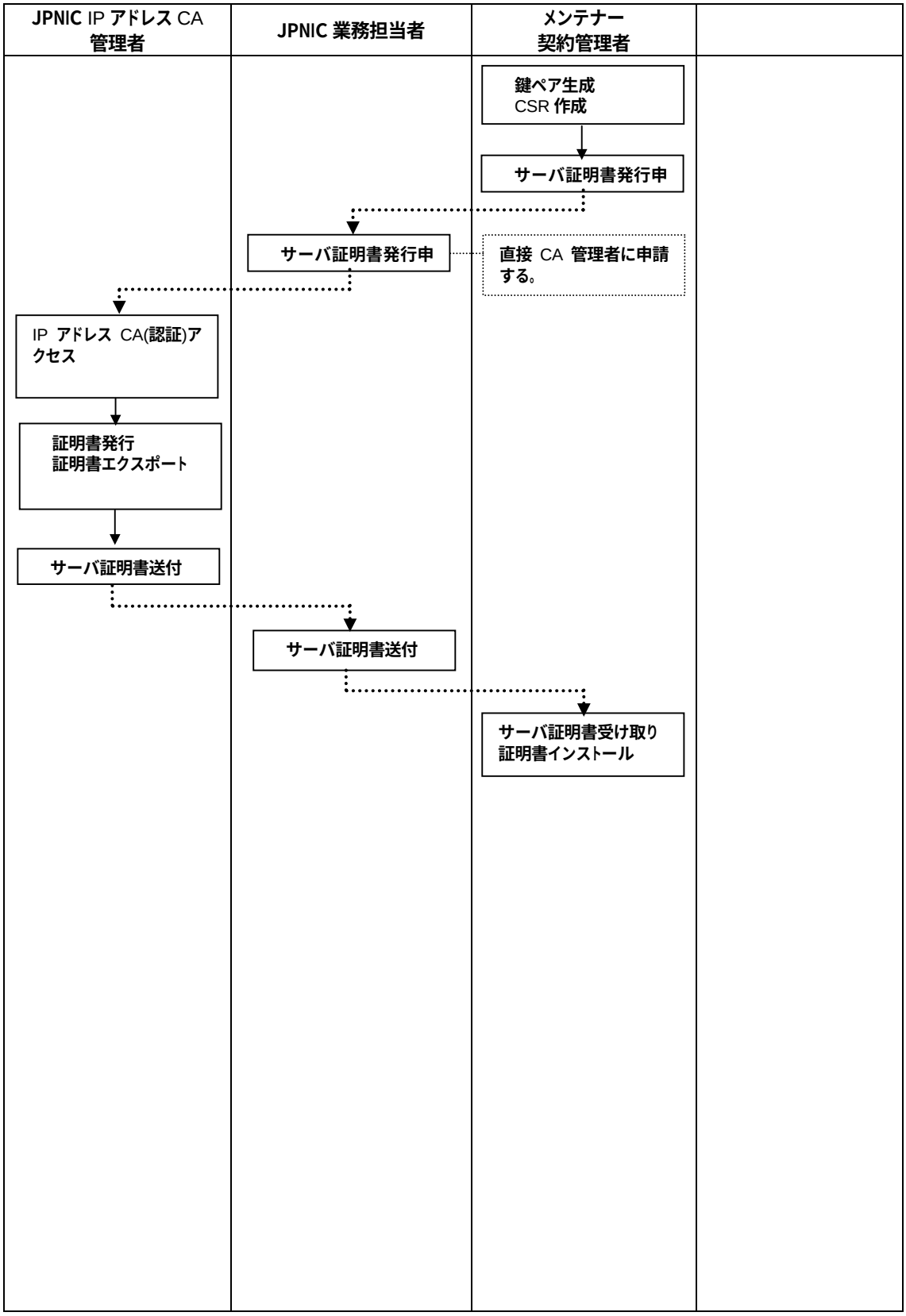
5.2.5.25. メンテナー申請者証明書失効業務



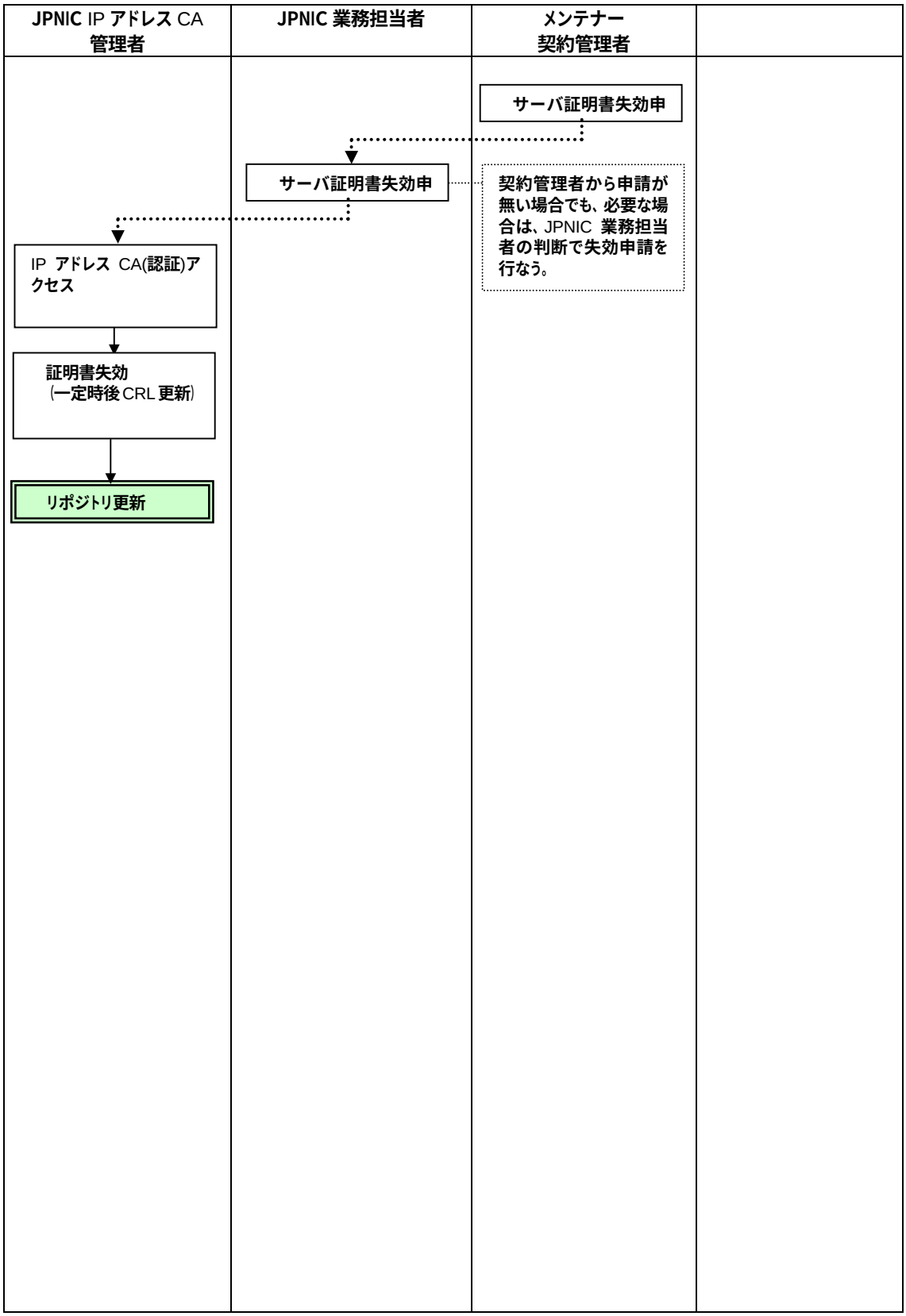
5.2.5.26. メンテナー申請者証明書更新業務



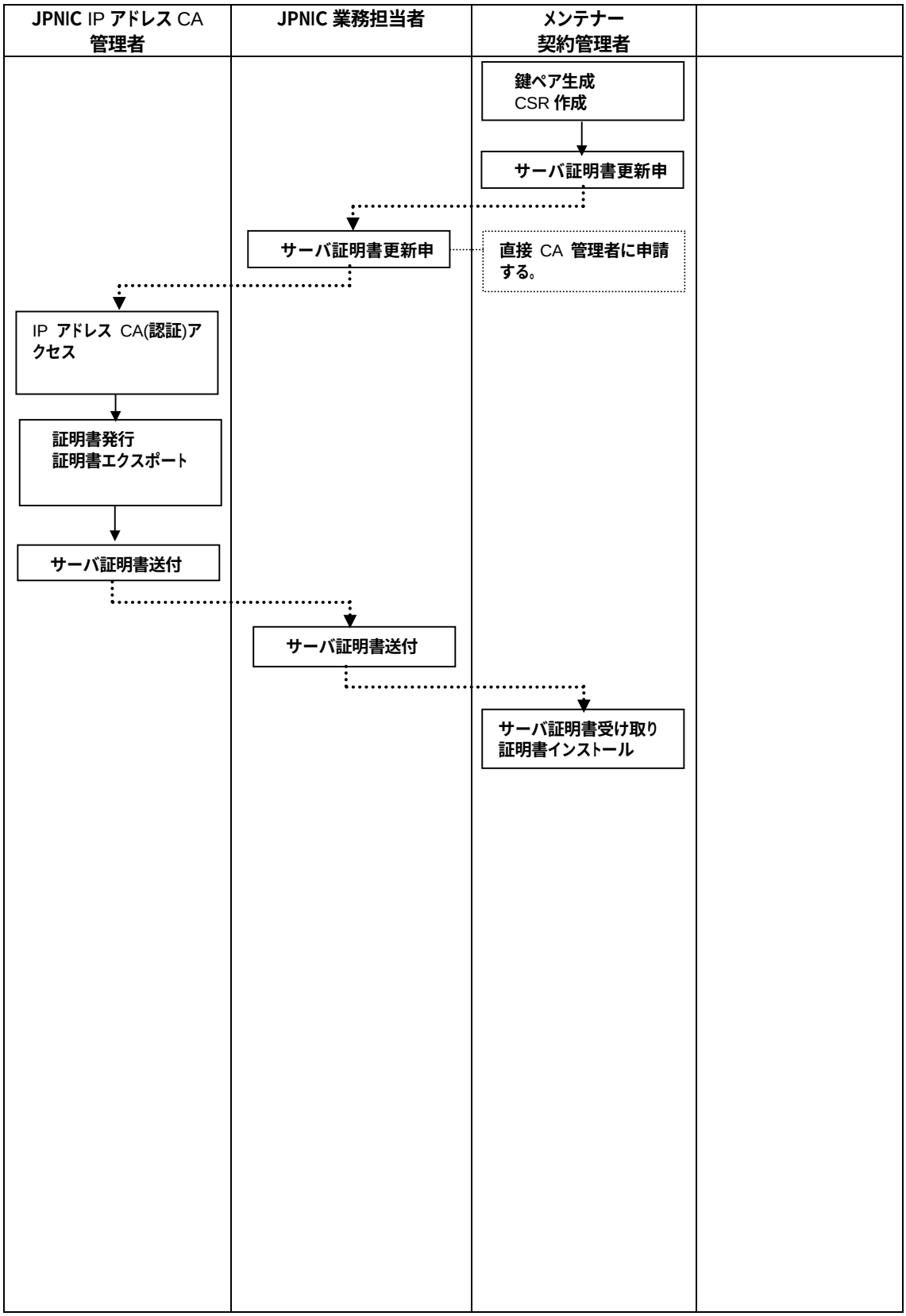
5.2.5.27. 指定事業者サーバ証明書発行業務



5.2.5.28. 指定事業者サーバ証明書失効業務



5.2.5.29. 指定事業者サーバ証明書更新業務



5.2.6. インタフェースの設計

IP アドレス認証局（認証）は、IP レジストリシステム等で使われる認証用途の証明書を発行するだけでなく、IP 指定事業者におけるメンバ管理者が申請業務で使われる証明書（ホストマスタ証明書）の発行申請、失効申請を受け付ける役割を持つ。証明書の発行対象であるユーザの概念は、登録情報における「認証 ID」を軸として定義される。「認証 ID」と IP 指定事業者の関連付けや、申請業務の対象となるアドレス資源との関連付けは「メンテナー」という概念を用いて行われる。

メンテナーは RPSL における mntner に似た概念で、アドレス資源を管理している主体とそのアドレスブロックの情報を併記したデータである。これによって一つの IP 指定事業者が複数のアドレスブロックの割り振りを受ける状況を表現することが出来る。また IP 指定事業者が更にアドレス資源の割り振りを行なった際に、その割り振り構造を表現することができるのである。

本節ではメンテナーに関連付けられた認証 ID の管理画面のイメージについて述べる。認証 ID は証明書の利用者一人一人に割り当てられる識別子である。IP 指定事業者はアドレス資源の申請業務に複数の担当者を設けることが出来るよう、一つのメンテナーに対して複数の認証 ID を定義できるものとした。

5.2.6.1. 外向き申請受付

（1） メンテナー一覧

証明書管理
管理者メンテナー：MNT-zxxxxxx **＜メンテナー一覧＞** **メンテナー** **MNT-zxxxxxx** **MNT-zxxxxxx** **MNT-zxxxxxx**

証明書管理画面ではメンテナーの一覧を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「認証 ID 一覧」に遷移する。

（2） 認証 ID 一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　申請者用

＜認証情報設定＞

認証ID	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

認証 ID 一覧画面ではメンテナーが保持する認証 ID の一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。認証 ID1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

(3)　証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称と申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

（4） 証明書申請完了

証明書申請完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書申請完了**

**証明書の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをメンテナーに通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、対象メンテナーに申請通知のメールを送信する。ライセンス ID がシンセ移管料画面に表示されるので、この画面を印刷するなどして、ユーザにライセンス ID を通知する。

(5)　証明書失効

証明書失効

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　**********

シリアル番号：　******
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

**(注意！) 失効処理を行うと、メンテナーがログインできなくなります。
よくご確認のうえ、失効処理を行ってください。**

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

（6） 証明書失効完了

証明書失効完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書失効完了**

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

(7)　証明書更新

証明書更新

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

EMAIL：

**(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。**

**(注意2) メンテナーのEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。**

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

（8） 証明書更新受付け完了

証明書更新受け付け完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　申請者用
認証ID:　　***********

証明書更新受け付け完了**

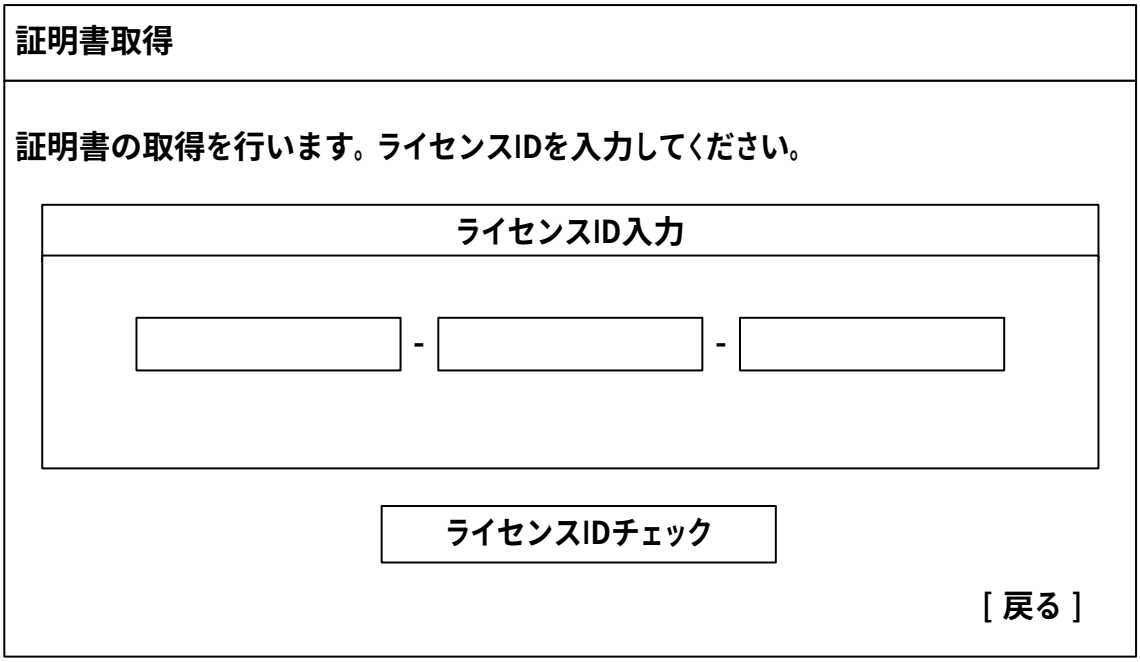
**証明書更新の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをメンテナーに通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、対象メンテナーに申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、ユーザにライセンス ID を通知する。

(9)　証明書取得



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（10） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。

メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

メンテナー情報確認

以下の情報で証明書を発行します。

名称: *******
EMAIL: ****@xxxｘｘ.ne.jp**

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを押して秘密鍵を生成し、CGI 側にて CA サーバにアクセス、証明書の発行を行なう。この後、「証明書インストール」に遷移する。

（11） 証明書インストール

証明書インストール

証明書を発行しました。お使いのPCに証明書をインストールします。

メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、認証 ID を表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（12） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

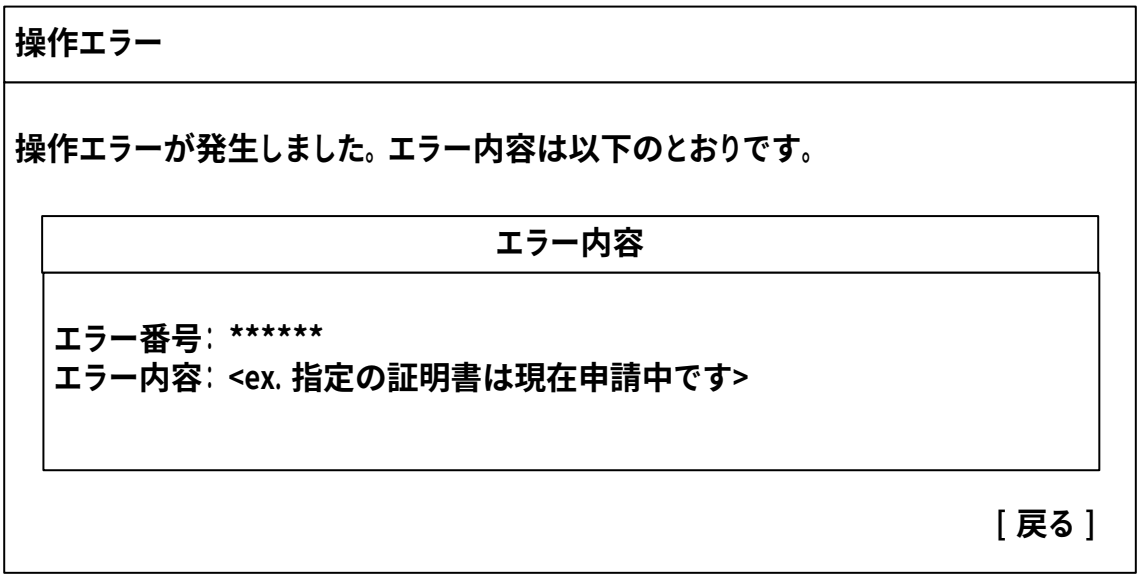
メンテナー: MNT-zxxxxxx
権限種別: 申請者用
認証ID: *********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、認証 ID を表示する。また、発行した証明書のサブジェクトの表示も行なう。

（13） エラー表示



エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.2.6.2. 内向き申請受付（業務管理者向け）

（1） メンテナー一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー	権限種別	名前
MNT-zxxxxxx	JPNIC業務担当者用	**********
MNT-zxxxxxx	JPNIC業務担当者用	**********
MNT-zxxxxxx	JPNIC業務担当者用	**********

証明書管理画面ではメンテナーの一覧を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「従業員コード一覧」に遷移する。

(2)　従業員コード一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用

＜認証情報設定＞

従業員コード	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

従業員コード（認証 ID）一覧画面ではメンテナーが保持する従業員コードの一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。従業員コード 1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

(3)　証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称、申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

（4） 証明書申請完了

証明書申請完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　********

証明書申請完了

証明書の申請を受け付けました。

名称：*******
EMAIL：****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコードを表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

(5)　証明書失効

証明書失効

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　************

シリアル番号：　******
サブジェクトDN：C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=********
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99

(注意！) 失効処理を行うと、業務担当者がログインできなくなります。
よくご確認のうえ、失効処理を行ってください。

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

(6)　証明書失効完了

証明書失効完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　　MNT-zxxxxxx
権限種別：　　JPNIC業務担当者用
従業員コード：　********

証明書失効完了

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

(7)　証明書更新

証明書更新

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　JPNIC業務担当者用
従業員コード：　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=********
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99

EMAIL：

(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。

(注意2) 業務担当者のEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

(8)　証明書更新受付け完了

証明書更新受け付け完了

管理者メンテナー：MNT-zxxxxxx

メンテナー：　　MNT-zxxxxxx
権限種別：　　JPNIC業務担当者用
従業員コード：　********

証明書更新受け付け完了

証明書更新の申請を受け付けました。

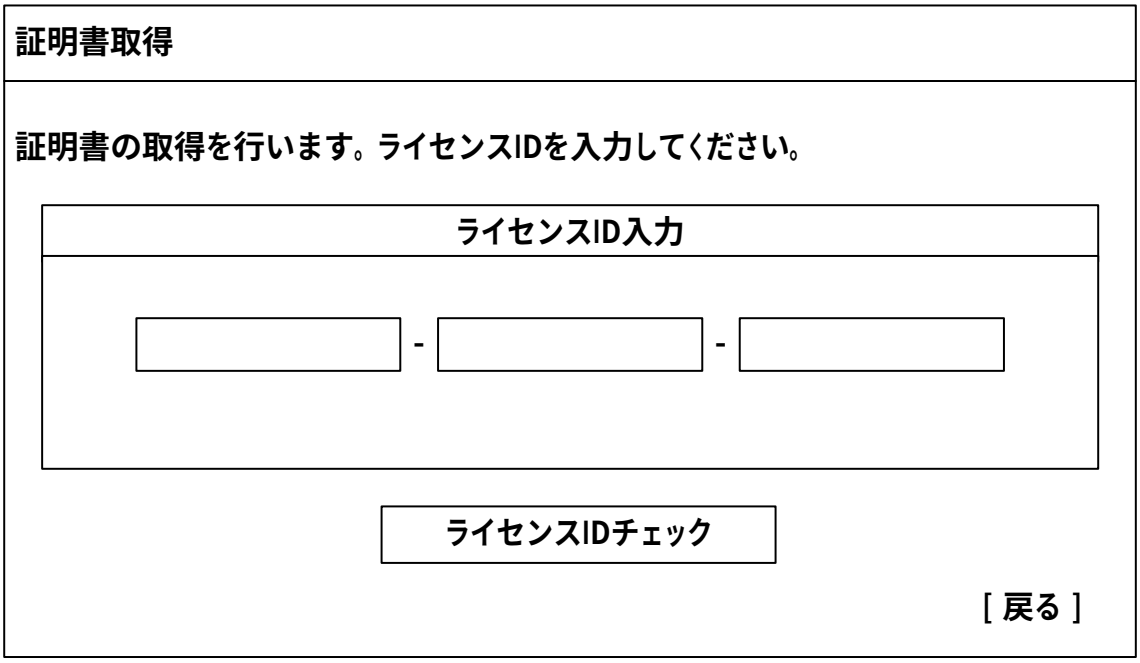
名称：　*******
EMAIL：　****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

(9)　証明書取得（ライセンス ID 入力）



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（10） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。HWキーを挿入してください。

メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

メンテナー情報確認

以下の情報で証明書を発行します。

名称: *******
EMAIL: ****@xxxｘｘ.ne.jp**

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、従業員コードを表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを押して秘密鍵を生成し、CGI 側にて CA サーバにアクセス、証明書の発行を行なう。この後、「証明書インストール」に遷移する。

（11） 証明書インストール

証明書インストール

証明書を発行しました。HWキーに証明書をインストールします。

メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、従業員コードを表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（12） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

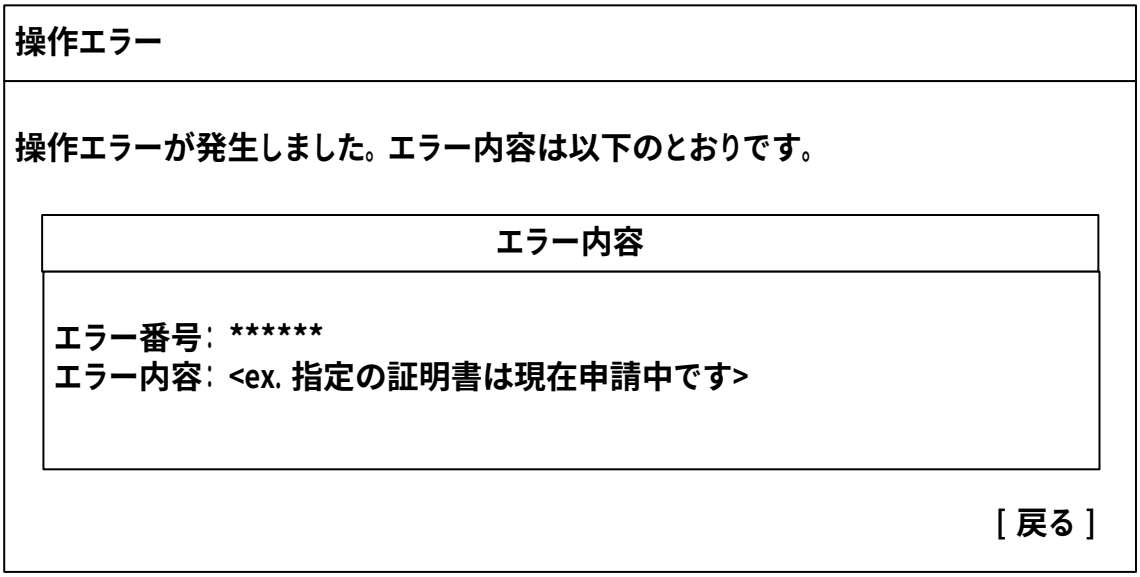
メンテナー:　　MNT-zxxxxxx
権限種別:　　JPNIC業務担当者用
従業員コード:　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、従業員コードを表示する。また、発行した証明書のサブジェクトの表示も行なう。

（13） エラー表示



エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.2.6.3. 内向き申請受付（業務担当者向け）

（1） メンテナー検索

証明書管理

管理者メンテナー：MNT-zxxxxxx

検索区分：
- ○ **契約管理者番号（完全一致）**
- ○ **資源管理者番号（完全一致）**
- ○ **資源管理者略称（完全一致）**
- ○ **組織名（部分一致）**
- ○ **メンテナーコード（完全一致）**

検索文字列：

検索を実行

証明書管理画面ではメンテナーの検索画面を表示する。SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。検索文字列を入力し、検索を開始すると「メンテナー一覧」へ遷移する。

(2)　メンテナー一覧

証明書管理

管理者メンテナー：MNT-zxxxxx

メンテナー	権限種別	名前	組織名
MNT-zxxxxx	契約管理者用	**********	**********
MNT-zxxxxx	資源管理者用	**********	**********
MNT-zxxxxx	契約管理者用	**********	**********

検索結果のメンテナー一覧を表示する。メンテナーコードはリンクとなっており、その 1 つをクリックすると「認証 ID 一覧」に遷移する。

(3)　認証 ID 一覧

証明書管理

管理者メンテナー：MNT-zxxxxxx

メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用

＜認証情報設定＞

認証ID	サブジェクトDN シリアル番号 有効期限	操作
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******	申請中
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	[失効][更新]
**********	C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=****** ***** 9999/99/99 99:99:99 ～ 9999/99/99 99:99:99	失効済み

認証 ID 一覧画面ではメンテナーが保持する認証 ID の一覧を表示する。操作対象のメンテナーの情報と SSL クライアント認証を行なった操作者の証明書から管理者メンテナーコードを取り出し表示する。認証 ID1 つにつき、それぞれ失効と更新のボタンが用意され、証明書に関する操作を行なえるようになっている。証明書失効の場合「証明書失効」に遷移し、証明書更新の場合は「証明書更新」に遷移する。

（4） 証明書申請

証明書申請の個人情報入力画面を表示する。CN に含まれる名称と申請が行なわれたことを通知する E-MAIL アドレスの入力フォーム（テキストフィールド）が存在する。証明書の申請を実行する場合は、「証明書を申請する」ボタンをクリックする。「証明書申請完了」へ遷移する。

(5)　証明書申請完了

証明書申請完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書申請完了**

**証明書の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp**

**以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書の申請の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

（6） 証明書失効

証明書失効

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　**********

シリアル番号：　******
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　　9999/99/99 99:99:99
終了日時：　　9999/99/99 99:99:99**

**(注意！) 失効処理を行うと、メンテナーがログインできなくなります。
よくご確認のうえ、失効処理を行ってください。**

証明書を失効する

[戻る]

証明書失効の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。証明書の失効を実行する場合は、「証明書を失効する」ボタンをクリックする。「証明書失効完了」に遷移する。

(7)　証明書失効完了

証明書失効完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書失効完了**

証明書の失効が完了しました。

シリアル番号：　****
サブジェクトDN：C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

[戻る]

証明書の失効の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。失効を行なった証明書のシリアル番号、サブジェクト DN、開始日時、終了日時を表示する。CGI は証明書が失効されたことを IP レジストリシステムに通知する。

（8） 証明書更新

証明書更新

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

シリアル番号：　******
サブジェクトDN：　C=JP,O=***,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******
開始日時：　9999/99/99 99:99:99
終了日時：　9999/99/99 99:99:99**

EMAIL：

**(注意1) 更新処理を行うと、現在の証明書は自動的に失効されます。
よくご確認のうえ、更新処理を行ってください。**

**(注意2) メンテナーのEMAILを更新する場合、EMAILを入力してください。
空欄の場合は、現在のアドレスを流用します。**

証明書を更新する

[戻る]

証明書更新の確認画面を表示する。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、リポジトリから証明書を取得し、シリアル番号やサブジェクト DN、開始日時、終了日時を表示する。EMAIL アドレスの変更を行なう場合、EMAIL テキストフィールドに入力する。証明書の更新を実行する場合は、「証明書を更新する」ボタンをクリックする。「証明書更新受付け完了」に遷移する。

(9)　証明書更新受付け完了

証明書更新受け付け完了

組織名(Organization)：*****
管理者メンテナー：MNT-zxxxxxx**

**メンテナー：　MNT-zxxxxxx
権限種別：　契約管理者用
認証ID:　　***********

証明書更新受け付け完了**

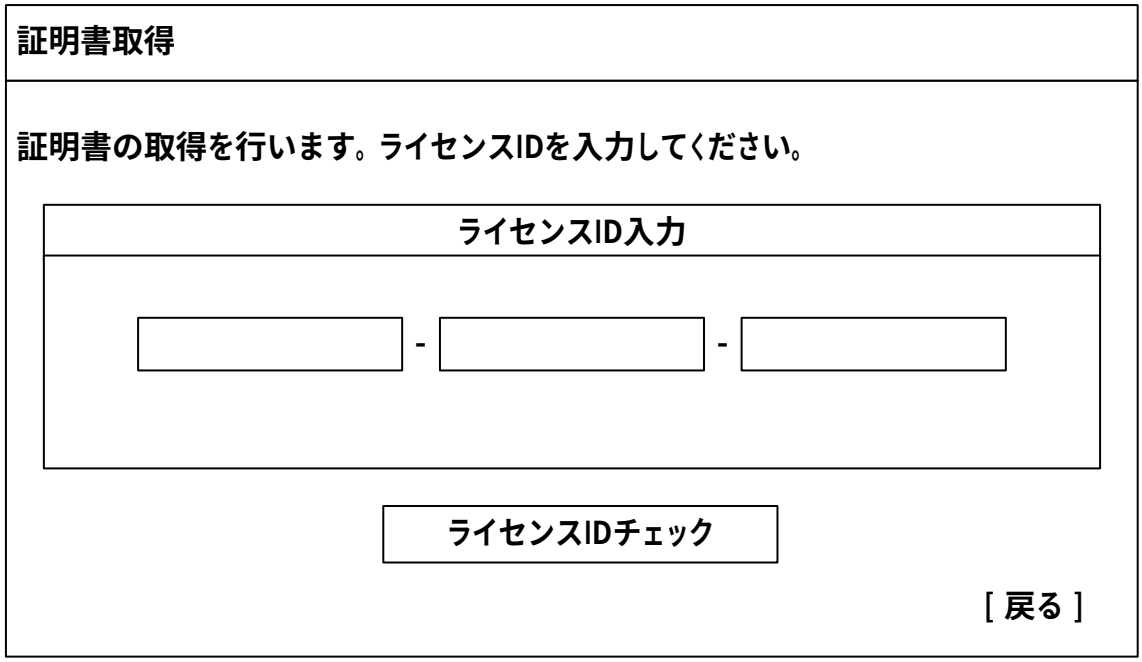
**証明書更新の申請を受け付けました。
名称：*********
EMAIL：****@xxxｘｘ.ne.jp

以下のライセンスIDをCA管理者に通知してください。
ライセンスID：******-******-******

[戻る]**

証明書更新の完了を知らせる。操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。CGI にてライセンス ID を生成して、リポジトリへ保管するとともに、CA 管理者に申請通知のメールを送信する。ライセンス ID が申請完了画面に表示されるので、この画面を印刷するなどして、CA 管理者にライセンス ID を通知する。

（10） 証明書取得（ライセンス ID 入力）



証明書の取得を行なう。ライセンス ID を 3 つに別れているテキストフィールドに入力する。「ライセンス ID チェック」ボタンを押すことで、認証を行ない「証明書取得（鍵生成）」に遷移する。

（11） 証明書取得（鍵作成）

証明書取得

証明書の鍵ペアを生成し、証明書を取得します。HWキーを挿入してください。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

メンテナー情報確認

以下の情報で証明書を発行します。

名称:　*******
EMAIL:　****@xxxｘｘ.ne.jp**

サブジェクトDN:　C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書を取得する

[戻る]

証明書取得の確認画面を表示する。指定のライセンス ID から証明書を発行するメンテナーの情報を検索し、操作を行なっている管理者メンテナーコードや操作対象のメンテナーコード、認証 ID を表示する。また、申請内容の名称と EMAIL を表示する。「証明書を取得する」ボタンを証明書インストール」に遷移する。

（12） 証明書インストール

証明書インストール

証明書を発行しました。HWキーに証明書をインストールします。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

証明書をインストール

証明書のインストール画面を表字する。操作を行なっているメンテナーコード、認証 ID を表示する。この画面が表示される時点で、CA から証明書が発行されローカル PC にダウンロードされており、「証明書をインストール」ボタンを押すことで、証明書のインストールが行なえる。インストール後に「証明書インストール完了」に遷移する。

（13） 証明書インストール完了

証明書インストール完了

証明書のインストールが完了しました。

メンテナー:　MNT-zxxxxxx
権限種別:　契約管理者用
認証ID:　　********

サブジェクトDN: C=JP,O=*,OU=Hostmaster,OU=MNT-zxxxxxx, CN=******

[戻る]

証明書インストールの完了を表示する。操作を行なっているメンテナーコード、認証 ID を表示する。また、発行した証明書のサブジェクトの表示も行なう。

（14） エラー表示

操作エラー

操作エラーが発生しました。エラー内容は以下のとおりです。

エラー内容

エラー番号：****
エラー内容：<ex. 指定の証明書は現在申請中です>**

[戻る]

（15） エラー一般の表示を行なう画面。エラー番号やそのエラーの内容を表示する。

5.3. まとめ

IP アドレス認証局（認証）の構築はいくつかの検討と設計を重ねた上で行われた。はじめに認証情報と証明書の関連性を調査し検討を行った。これは指定事業者に利用されている IP レジストリシステムと連動した形で IP アドレス認証局（認証）が証明書を発行するという協働型の構築である為である。認証情報と証明書の関連性の検討の次に、証明書関連業務（認証業務）を想定した業務フローを作成した。業務フローがあると認証業務に必要な、すなわちシステムが提供すべき機能が明らかになり、業務担当者の間でやり取りされる情報が明らかになる。更に認証業務に必要な機能を満たすシステム構成を検討し、仕様を決め、開発を行った。この作業と平行して認証業務規程（CPS）の更新を行った。

このように認証局の構築にはいくつかの検討が必要となるが、それらの多くは想定している認証の要件を明確にする作業であったと言える。つまり予め想定する認証の内容が明らかであったり、明らかにする為に必要な検討が少なかったりすると、比較的短期間で構築が可能であると考えられる。なお、本調査研究の一環として、前年度には認証の適用先の検討、モデルの設計、証明書アプリケーションの検討、証明書パスの検討等を既に行っていた。これらが今年度の構築の検討資料として役立った。

なお、PKI を認証に利用する場合には、証明書のフィールドの検討、証明書の失効とアカウントの無効化に関する検討、CPS への準拠性の検討および対策などの作業が必要になったことを記しておく。PKI は様々な状況を想定した仕組みを持っているが、認証システムの即時性や利便性の向上の為には更にいくつかの工夫が必要になった。

第6章 認証業務規程（CPS）の更新

内容

- 再検討の目的
- コミュニティの定義
- 前提条件の整理
- ギャップの整理

第6章 認証業務規程（CPS）の更新

6.1. CPS の再検討の目的

CPS（Certification Practice Statement：認証業務規程）は、認証局がその業務方針を明文化した文書である。認証局において CPS の公開は任意であり、CPS なくして認証局はありえないかというとそうではないが、商取引や政府認証基盤といった多くのユーザを収容する規模の認証局の多くは CPS を定め公開している状況がある。2002 年度「IP アドレス認証局のあり方に関する調査研究」では日本における特定認証業務のガイドライン、米国およびカナダにおける WebTrust for CA といった認証局の監査基準の調査研究を行ったが、これらの監査はすべて CPS を基にして行われる。

CPS を定め、公開するには大きく分けて二つの意味がある。一つは認証局の運用主体が、その認証局の位置づけや役割、規模といった事項を再認識し業務の適正化を図る基準にするという意味である。もう一つはその認証局が発行した証明書を検証する際の判断基準である。証明書検証者は認証局を「信頼できる第三者」として位置づけ、検証しようとしている証明書の信頼性を測ろうとする。なぜなら証明書の発行自体に信憑性がなければ、認証相手の正しさ（なりすましや偽造行為）を検証するができない為である。

IP アドレス認証局は自然人を認証することを目的としていない為、特定認証業務の業務レベルとは性質が異なる。また WebTrust for CA のような「Web サーバ証明書」の発行を目的としたものでもない。しかしインターネットにおけるアドレス資源の管理を行うインターネットレジストリにおいて実施される認証業務である。本報告書の第 6 章で述べるように、インターネットを使うノードの間での認証に証明書が使われる可能性を持っている。

2003 年度や 2004 年度の IP アドレス認証局に関する報告書で述べてきたように、アドレス資源の信頼性はインターネットの運用の信頼性を左右する要素である。安全な運用を図る為のアドレス資源の元本としての登録情報は、十分に強い方式を使いかつ現実的な運用によって登録者を認証し、登録内容の信頼性向上と公開時の原本性の確保が必要となるであろう。登録情報の公開（whois）はインターネットを利用する多くのユーザに対して意味を持つ。

このような背景を受け、IP アドレス認証局の CPS は 2003 年度よりドラフト作成を開始し、認証業務の定義づけを行ってきた。2004 年度は認証局システムの構築によって、いよいよ証明書検証者に対する信頼の確立が必要になる。しかし 2004 年度に行った認証局の構築活動から、2003 年度にドラフトした CPS から修正が必要になることがわかってきた。例えば認証業務の規模はより簡易になり、認証局システムで利用される機器構成や設備が具体的になってきた。そこで 2004 年度は、具体化してきた認証業務を受けて CPS の全面的な見直しを行った。

CPS の編纂作業は、CPS に関する知識とノウハウが必要になる作業である。本章では当センターで行った CPS の見直しの内容について述べ、IP アドレス認証局の業務規程について述べると共に、多くの認証局で懸案事項となっている CPS を編纂に関する

参考情報となるよう、そのプロセスについて述べる。

6.2. CA とアプリケーション専門家チーム

CPS に関する検討や記述には、認証技術としての PKI に関する知識だけでなく証明書の運用業務や証明書管理の手法といった知識を必要とする。また CPS として記述するための問題点・記述の分解作業が必要である。これらの作業を進める為、当センターでは「専門家チーム」と呼ばれるチームを設立し、CPS の見直し作業を行なった。

CA とアプリケーション専門家チームの活動主旨を以下に示す。

6.2.1. 活動内容

a. メーリングリストにおける意見交換
   CP/CPS 記述上の論点をまとめるための議論を行った。

b. 個別会議の開催
   CP/CPS の検討方針について議論と論点整理を行なう為、個別の会議を行った。
   人数は一名ないし二名の少人数を想定し、12 月から月に二回の開催を想定した。

c. 全体レビュ会議の開催
   ML と個別会議等を通じて明らかになった論点と記述についてレビュを行い
   CP/CPS での記述方法について具体的な検討を行った。1 月と 2 月の二回の開催を想定した。

6.2.2. 活動スケジュール

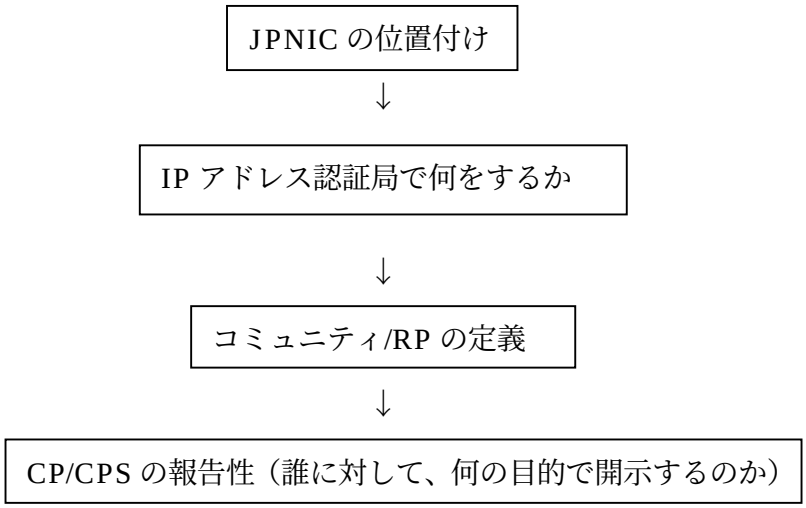
2004 年 12 月　専門家チームを編成し、検討方針の決定と CP/CPS 記述上の論点整理を行った。
2005 年 1 月　論点ごとに記述案をまとめ、全体レビュ会議にかける。そこで課題抽出を行った。
2005 年 2 月　1 月の全体レビュ会議で明らかになった課題に対して行った対策についてレビュを行い、CP/CPS をまとめる為に必要な作業が更にあればその検討を行った。
2005 年 3 月　CP/CPS 文書としてまとめた。

6.2.3. 作業手順

はじめに CPS の記述に取り掛かる前に検討順序を定めた。

6.2.3.1. 検討順序と項目

2003 年度にドラフトした CPS を元に、下記の検討順序のうち前半は概ね明らかになっていた。しかし「IP アドレス認証局で何をするか」には JPNIC による登録者の認証用途に限定するか JPNIC に情報登録を行っている日本のインターネットコミュニティの中でユーザ同士が認証に用いることが出来るようにするのか、という異なる二つの目的が挙がっていた。



CPS では認証用途に限定し RP（Relying Party）等を想定した。RP とは主に証明書検証者を指し、認証局を信用し証明書の信頼性に基づいた行動（認証行為と一連の処理）行う主体のことである。

次に 2003 年度の CPS とのギャップの分析を行った。

1. ギャップの整理
   - 制約条件（コスト等）からのギャップ
   - 方針の変更によるギャップ（RP を特定した等）
2. 前提条件の整理
   - RP、コミュニティ、CPS の目的
   - 制約条件（コスト、体制）
3. 検討課題
   - 論点
   - 各認証局の目的と用途

認証業務の目的や証明書の用途を限定することで、認証局に関わる主体が限定され、前提条件が整理された。

更に検討のスケジュールと重点を置く配分を決める為、既存の CPS の分量と重み付けを調査した。

章立てとページ数	（全体 127 ページ）
はじめに	17 ページ
一般条項	25 ページ
識別と認証	9 ページ
運用上の要件	34 ページ
建物人員設備	20 ページ
技術的なセキュリティ管理	14 ページ
プロファイル	6 ページ
仕様の管理	2 ページ

以下に、これらの検討の内容を述べる。

6.3. IP アドレス認証局の位置づけとコミュニティの定義

2003 年度および 2004 年度の検討の結果、IP アドレス認証局は細分化され役割ごとに異なる認証局を構築するものとした。
主に登録情報の登録者を認証する為の証明書を発行する IP アドレス認証局（認証）について行った検討について述べる。

はじめに JPNIC の役割を明文化する。しかしここでは詳細にせず主体と責任についてのみ記述する。

6.3.1. 認証局における JPNIC の役割

JPNIC は、IP アドレス認証局(認証)の運用主体。
認証の結果とその権限分離に対する責任を持つ。

次に IP アドレス認証局（認証）の業務の種別を検討した。

6.3.2. IP アドレス認証局で何をするか

JPNIC における認証のための証明書発行および失効を行なう。
ここで候補と考えられる認証業務を列挙し RP やコミュニティの違いを検討した。ここでは挙げられた A、B、C の三種類を以下に示す。

A. IP レジストリシステムによる IP 指定事業者(契約管理者、資源管理者、申請者)の認証

IP レジストリシステムは、本人性の確認ができた場合にログインを許可し、本人性に基づく権限の実施を許す。
なお IP レジストリシステムにもアカウントの失効機能がある。

認証対象の種別：

- IP 指定事業者(契約管理者、資源管理者)
  申請者の証明書の発行申請を行うことができる。
- 申請者
  アドレス資源の各種申請を行うことができる。

B. JPNIC 職員による IP 指定事業者(契約管理者、資源管理者、申請者)の認証

JPNIC 職員が IP 指定事業者のメッセージ認証と本人性確認と行なう。電子メールのやりとりの際に用い、暗号化と署名を用いる。認証対象の種別にも用いられる。

C. IP 指定事業者同士による IP 指定事業者(契約管理者、資源管理者、申請者)の認証

「すること」の拡大解釈であり、IP アドレス認証局(認証)は本認証に対する責任を一切持たない。

IP 指定事業者が、メッセージ認証と本人性確認に用いる。電子メールのやりとりの際に用い、暗号化と署名を用いる。認証対象の種別にも用いられる。

更にそれぞれについてコミュニティと RP の定義を行った。

6.3.3. コミュニティ/RP の定義

D. IP レジストリシステムによる IP 指定事業者(契約管理者、資源管理者、申請者)の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員 - RAA
- IP アドレス認証局(認証) 認証局システム
- IP レジストリシステム - RP
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - EE, RA, 申請者の任命
- IP 指定事業者 資源管理者 - EE, RA, 申請者の任命
- IP 指定事業者 申請者 - EE

E. JPNIC 職員による IP して事業者(契約管理者、資源管理者、申請者)の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員 - RP
- IP アドレス認証局(認証) 認証局システム
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - RA, EE, 資源管理者の任命
- IP 指定事業者 資源管理者 - RA, EE, 申請者の任命
- IP 指定事業者 申請者 - EE

F. IP 指定事業者同士による IP 指定事業者(契約管理者、資源管理者、申請者)
の認証

登場人物：

- JPNIC セキュリティ事業部(仮) - 職員の任命
- JPNIC セキュリティ事業部 職員 - CA の運用
- JPNIC IP 事業部 - 職員の任命
- JPNIC IP 事業部 職員
- IP アドレス認証局(認証) 認証局システム
- IP 指定事業者 契約組織 - アドレス資源管理組織の契約組織
  アドレス資源管理組織と同一の場合がほとんど。
- IP 指定事業者 アドレス資源管理組織 - 契約管理者、資源管理者の任命
- IP 指定事業者 契約管理者 - RA, EE, RP, 資源管理者の任命
- IP 指定事業者 資源管理者 - RA, EE, RP, 申請者の任命
- IP 指定事業者 申請者 - EE, RP

更に CPS の報告性を文章化した。

6.3.4. CP/CPS の報告性（誰に対して、何の目的で開示するのか）

A. IP 指定事業者と一般に対して、認証用証明書の運用の信頼性を周知

本人性確認手段の運用レベルを一般に示すこと。目的は一般に参照される WHOIS に対する信頼性の向上。また申請者に対する認証強化への安心の提供。

B. 同上 ただし WHOIS は除く。

C. IP 指定事業者に対して、認証用証明書の運用の信頼性を周知

JPNIC における本人性確認手段の運用レベルを一般に示すことで、推測可能な本人性を提供する状況を作ること。

6.4. コミュニティに基づく前提条件の整理

前節の認証業務の候補からコミュニティを記述し比較を行った。

- RP
  業務 A：IP レジストリシステム(JPNIC)
  業務 B：IP レジストリシステム(JPNIC)、JPNIC 職員(JPNIC)
  業務 C：IP 指定事業者
- コミュニティ
  業務 A：
  IP レジストリシステム、契約管理者、資源管理者、申請者、IP 事業部担当者、認証局管理者、証明書管理者、運用責任者、理事会
  業務 B：
  業務 A＋JPNIC 職員
  業務 C：
  契約管理者、資源管理者、申請者、IP 事業部担当者、認証局管理者、証明書管理者、運用責任者、理事会
- CPS の目的
  業務 A：
  申請者の認証レベルを IP 指定事業者と一般に示す。
  間接的に whois の信頼性向上させるため。

  IP レジストリシステムにおける、契約管理者、資源管理者、申請者
  JPNIC 事業部担当者の認証業務を記述
  業務 B：
  登録者の認証強度を IP 指定事業者に示す。
  業務 C：
- 制約条件
  ・コスト
  認証業務は実験の位置づけの為、事業収入はない。
  ・体制
  理事会：理事
  認証局：担当 1、スタッフ 1
  IP 事業部：担当 1
- 各認証局の役割整理

  JPNIC ルート認証局：
  JPNIC のレジストリデータにおける(PKI)認証業務の信頼性を代表し認証業務を代表し、下位認証局を監督する権限を持ち、その証明書を失効することが可能。統一方針に従った管理を適用する。

IP アドレス認証局（認証）
　JPNIC の申請者認証の為の認証局で、JPNIC による IP 指定事業者の認証を目的とする。

IP アドレス認証局（証明）
　JPNIC の登録情報に基づいて証明書を発行し、ユーザ間の認証を目的とする。

業務 A、B、C の比較の結果、主に業務 B を対象とした CPS とすることにした。

6.5. ギャップの整理

RFC3647 のフレームワークを元に、2003 年度にドラフトした CPS とのギャップの整理を行った。この段階では単なる違いの洗い出しではなく、記述方針をできるだけ決めておくこととした。

- 制約条件（コスト等）からのギャップ

  ・(全体)
  当時は運用費用のシミュレーションを行なっておらず、運用内容に大きな幅があった。収入に基づいた運用を考慮し始めること自体が大きなギャップ。
  ・(システム維持費)
  システム維持費用の特定の根拠認証局システムの構築に、維持費用の特段の根拠はなく、最低のコストで External RA を実施するに留めた程度。

あとは個別に記述することにする。

- 方針の変更によるギャップ（RP を特定した等）

  上位概念的な懸案事項
  ・ IP アドレス認証局(認証)をツリーに含めるか
  ⇒ ツリーに入れると ISP の証明書を一般に検証できる状況ができる。
  IP アドレス認証局(認証)の認証業務が、ルート認証局の業務の信頼性に影響を持つことである。RP が異なるため、例えば一般の RP が認証用途の証明書を検証できる必要はない。

  これに対して組み立てたロジックは、ルート認証局はレジストリデータの業務の信頼性を代表する認証局であり、IP アドレス認証局(認証)の業務を監督する権限を持ち、その証明書を失効することが可能である。傘下に置くことによって、統一的な管理を適用する。

  報告書の本文に入るべき内容：
  ルート認証局の存在目的が決まると、ルート認証局の指導に従って IP アドレス認証局(認証)の CPS を見直す可能性がある。

  個別
  ・ ルート認証局の役割候補の列挙（本文）
  ・ IP アドレス認証局(認証)の鍵サイクル
  ⇒ 追加も可能
  ・ "ISP 管理者を（契約管理者、資源管理者）に分ける"等の違い

⇒ プロファイルの列挙。注にて対応。

6.6. RFC2527 に沿った更新の方針

2003 年度の CPS の検討は RFC2527 に沿って行われた為（当時の最新の RFC は RFC2527 であった)、検討内容と照らし合わせた更新案（該当部分のみ記述）を作成した。

- 契約管理者、資源管理者の本人特定 rfc2527:3.1.9

  契約管理者・資源管理者の本人特定方法の候補：

  - 指定事業者契約
  - 業務委託契約
  - 雇用契約書類
  - 電話確認

  既存の業務に従う。

  申請者の本人特定方法の候補：
  - 雇用契約書類
  - メール到達性

  「ホストマスタ業務をする人に発行してください。」と書く。
  CPS にて：「<Name>に入る名前は自然人を確認したものではない」

  発行申請に必要事項の候補：契約印、担当部署名、所在地、連絡先、担当者印、角印＋callback

- 失効時の本人確認方法 rfc2527:3.4

  契約管理者・資源管理者：
  - 指定事業者契約
  - 業務委託契約
  - 雇用契約書類
  - 電話確認

  申請者の本人特定方法の候補：

  - 雇用契約書類
  - メール到達性

失効申請：契約印、部署名 or 申請時の担当者印

運用に関わる事項（後に検討、ルール化）
・fingerprint の確認方法
・ハードウェアトークン送付方法（タンパーシールの使用）

・鍵の切り替え方法 rfc2527:4.7 ⇒ なし

・建物の要件：JPNIC マシンルームの想定に変更 rfc2527:5.1.2

認証設備室：（CA サーバ及び HSM を設置する部屋、以下同じ）
常時施錠とし、許可されたものだけが入室できるように管理する。
常時施錠された設備内で運用される。

入退室管理
"ＲＡシステム設備室"

・必要とされる人数 rfc2527:5.2.2

認証局システムサーバ ⇒ CA サーバ

キーセレモニーをはじめとする特に重要な業務については複数人
での実施する。特に重要な業務：キーセレモニー

－認証局 2 名（うち一名スタッフさん）
－IP 事業部 受付 1 ないし 2 名
－技術部 システム管理者 1 名

・5.3.8 要員に必要とされるべき文書
どこまで用意できるか（業務マニュアル）

「認証業務に必要となる文書を用意する。」でよい。

－業務手順書、書式、災害復旧計画書（新たな作成が必要とされている）
－操作マニュアル

・6.1.1 鍵ペアの生成主体
キーセレモニーどうするか検討

－キーセレモニー
　実験的な位置づけになりそうなので事務局内

FIPS-140-2level2 の認定の機器を利用し、複数人の立会いの元、
生成する。

・6.1.2 利用者への私有鍵の送付方法

－契約管理者・資源管理者：認証局で安全な方法で JPNIC で生成送付する。
　削除する（安全な削除方法をルール化）。
　配送されるトークンの保管場所

－申請者は申請者側で生成するので規定しない。

・6.1.9 鍵の使用目的
S/MIME を書いてしまってよいか。

・6.2.2 複数人による秘密鍵の管理
HSM の利用上、可能か確認
　－人員
　　「複数の要員」等とする。

・6.2.4 私有鍵のバックアップ
手順の確認
　－複数の CAO
　⇒CAO といわずに、「複数の要員」とする。

・6.2.7 私有鍵の活性化方法
複数の CAO が可能か確認
　－同上
　⇒CAO といわずに、「複数の要員」とする。

・6.5.1 信頼されるコンピューティング基本コンセプト
複数の CAO が可能か確認
　－同上
　⇒CAO といわずに、「複数の要員」とする。

・8.3 承認手続き
認証局の運営に関する承認主体

－運営委員会
⇒承認は必要

6.7. RFC3647 に沿った CP/CPS の更新案

最後に 2003 年度の CPS を記述に利用した RFC3647 のフレームワークに沿って、ギャップを整理しなおし記述方針を決定した。

●用語の変更
IP アドレス認証局 ⇒ IP アドレス認証局(認証)
LRA ⇒ メンバ管理者
＃契約管理者、資源管理者のことをさすが、CPS では総称する

●認証用認証局とすることの影響（リポジトリ-CRL,CPS のみ公開の影響）
2.1 リポジトリ
2.2. 証明情報の公開
2.3. 公開の時期又は頻度
2.4. リポジトリへのアクセス管理
3.4. 失効申請時の本人性確認と認証
4.5.2. 検証者の公開鍵及び証明書の使用
⇒「本認証局における証明書検証者は JPNIC 自身であるため規定しない」
でもよい。
6.1.4. 検証者に対する認証局の公開鍵の交付
⇒認証局証明書は公開

●LRA 契約という概念をなくすこと
4.1.1. 証明書申請を提出することができる者
＃単に認証されたメンバ管理者という扱いとする。
⇒「申請者」はメンバ管理者かホストマスタかわかりにくい。
また、ホストマスタが申請することにせず、メンバ管理者が
割り当てることにすれば、シンプルかつ実情に合う。

●認証局システムの開発内容の影響
4.1.2. 登録手続及び責任
⇒署名検証しているかＮＥＣに確認
4.3.1. 証明書の発行過程における認証局の行為
⇒IP 指定事業者からメンバ管理者としての任命を受けていることを
確認する。

●メンバ管理者はセンター発行であることの影響

4.3.2. 認証局の所有者に対する証明書発行通知
4.4.1. 証明書の受領確認の行為
⇒到達確認のできる方法で郵送する。
「PKI 環境」はわかりにくい。「証明書ファイルが自身の環境で利用できることを確認する。」などに。

●運用予定の設備
5. 設備上、運営上、運用上の管理
⇒「高層部に設置する」などにしてあまり書かない方法がある。
⇒防火区画は多くの建物で設置されている（天井に達する仕切り壁等）為、建築の設計書を確認する。消化設備を設置する。

●現実の運用体制（人数と部署）
5.2. 手続的管理
⇒JPNIC では CA 秘密鍵管理など特に重要な業務については、権限を分離している。権限分離の表は載せない。
5.4. 監査ログの手続
「必要な監査ログとして、本認証局が必要と認めた監査ログを取得する。」具体的には書かない。
5.5. 記録の保管
5.4.2. 監査ログを処理する頻度
⇒精査するとできるか。
5.4.3. 監査ログを保持する期間
⇒「規定の期間を保管する。」
5.4.3. 監査ログを保持する期間
⇒改ざん検出までは書かない。外部媒体へのバックアップの際に電子署名する方が効率的か。
「コンピュータの中にある間は、権限のないものがアクセスすることは難しいため」「バックアップ媒体へのタンパーシール」
6.1. 鍵ペアの生成及びインストール
⇒センター発行の分を記述

6.8. 更新された認証業務規程（CPS）

前節までに述べた更新案に基づき、CPS の更新を行った。更新された CPS を本報告書の Appendix.1 として添付する。また前年度の CPS との違いをまとめた表を Appendix.2 として添付する。

第7章 IP アドレス認証局の応用

内容

- 経路情報の安全性
    1. 今後のシナリオ
- アドレス資源管理の効率化
    1. Web トランザクション
- 商用 ENUM サービスでの適用事例

第7章　IP アドレス認証局の応用

IP アドレス認証局は、インターネットにおける登録情報の安全性向上と登録情報の内容を用いた認証に利用することができる認証局である。当センターではアドレス資源管理に必要となるネットワーク情報（割り振り先の情報、割り当て先の情報）、ホスト情報、AS 情報といった登録情報のデータベースを管理しており、インターネットの自律的な運用を支える役割を担っている。これらの情報の登録は IP 指定事業者を中心として、多くのネットワーク利用組織が行ってきたものである。アドレス資源の一意となる割り振りというインターネットレジストリにおいて、登録情報は登録者自らが集約する役割を持っているモデルはインターネット以外で使われている識別子の管理モデルとは異なり独特なものであろう。

本章では、この独特のモデルによるアドレス資源管理がインターネットの安全な識別（認証）に対してどのようなアプローチが可能であるか、という点に着目し、インターネットレジストリにおける認証局である IP アドレス認証局がどのような応用の方向性を持っているかについて述べる。

2003 年度の「IP アドレス認証局のマネジメントに関する調査研究」でも IP アドレス認証局の応用について述べた。2003 年度は新たなネットワークアプリケーションやビジネスモデルの登場といった広い視野で行ったのに対し、本章では具体的に応用可能なプロトコルについて述べる。本章で紹介するプロトコルにおいて IP アドレス認証局が発行する証明書が利用可能になったとしても、2003 年度で述べたようなネットワークアプリケーションがすぐに実現するわけではないが、インターネットにおける安全なアドレス資源の管理とノード間の認証の実現に向けた活動によって生活基盤としてのインターネットを確立し、向上された安全性にのっとった様々なアプリケーション開発が可能になると考えられる。

本章では三つの応用について述べる。一つは IRR における認証局の応用である。もう一つはアドレス資源管理をより効率的に行う Web トランザクションについて述べる。アドレス資源管理における組織間の連携は RIR と NIR の間において行われてきているが、より迅速さや安全さが効果を発揮する連携は NIR と LIR の間であろう。2004 年度にシステム開発の一環として行われた連携の仕組みについて述べる。更に、ENUM の登録における認証局の利用の事例を紹介する。

7.1. インターネットにおける経路情報の安全性

インターネットにおける経路制御はインターネットレジストリにおけるアドレス資源の割り振りと割り当てに則って行われる。経路制御で使われるアドレス資源は IP アドレスと AS（Autonomous System）番号である。

また AS（Autonomous System：自律システム）は、ネットワーク利用組織が経路を管理する上での方針に則って経路制御を行う。この方針の中には、割り振られていないはずのアドレスの経路情報を排除したり、あまりに経路の変動が激しい場合にその情報を伝播しないようにしたりといった、ネットワークの運用上の安全性を考える上で重要な要素が含まれている。

IRR（Internet Routing Registry）は、AS 番号と prefix（経路情報で使われるアドレスブロック）に加え、経路情報の伝播に関する方針を登録することが出来るインターネットレジストリの機能である。

近年当センターにおいて、IRR における経路情報の安全な交換に向けた活動が行われている。

はじめに 2003 年度に当センターの IRR 企画策定専門家チームで検討された IRR とルーティングの安全性に関する記述を紹介する。

2004 年 3 月 31 日に公開された「JPNIC における IRR サービスに関する検討報告書」から該当部分を抜粋する。

6.8　IRR のセキュリティ

IRR におけるセキュリティを考慮するに当たっては、「IRR が果たす役割」を考えます。そして、その役割を満たすために何を守らなくてはならないのかを定義し、対策を打つことで IRR のセキュリティを高めます。

IRR の果たす役割は、実際にインターネット上に流れる経路に対する台帳　としての役割とそれら経路に関する情報の提供という役割があります。これらの役割を言い替えると、前者は「ルーティングのリスクに対する IRR の役割」であり、後者は「安全な情報提供と情報登録を(ユーザに対して)実施させる役割」と言うことができます。そこで今回は、この 2 点についてフォーカスを絞り検討を実施しました。

これまでの検討においては、その多くが情報そのものの信憑性(意味的な正当性)について実施されてきましたが、上記の 2 点にフォーカス絞るため情報そのものよりも手続き的な信憑性(形式的な正当性)に注目しています。この「形式的な正当性」

とは、登録されている内容が正しいかどうかと言うことではなく、登録される際に、その登録者が正しいかどうかという認証の問題と、登録される内容がいかに検証されるべきかを指しています。

この章では、これらの前提条件のもと、ルーティングと IRR の役割、さらにその役割に対する登録情報の正当性について検討した内容について述べ、最後に、登録情報の正当性をどのような仕組みで実現するかについて述べます。

6.8.1 ルーティングと IRR の安全性

IRR の安全性を検討するに当たっては、「IRR の目的は何か」を定義し、その目的を阻害する要素を分析する必要があります。

IRR とは、ルータによる適切なルーティングを助けるための適切な参照情報を提供することが目的です。このため、IRR の安全性を検討するには、この目的が阻害される脅威に対する検討が必要となってきます。

以下は、この定義に準じた形で、検討項目を明らかにするための簡単なリスク分析を行います。分析は、(a)IRR の目的(要件の定義)、(b)目的を達成するために守るべき資源の定義、(c)それら資源に対する脅威の分析の 3 段階で脅威(いわゆる、リスク)を分析します。

(a)IRR の目標とする要件は何か

- *該当経路のルーティングを行うための参考情報の提供*
- *適切な経路情報を入手するための参考情報の提供*
- *適切な範囲で経路情報の交換を行うための参考情報の提供*

(b)IRR が守るべき資源は何か

- *各ルータが持つ正しい経路情報*
- *経路情報の正しい伝達*
- *意図した通りの AS-PATH の伝達*

(c)資源に対する脅威は何か

- *変更された経路情報の伝達*
  - *・意図された変更*
  - *・意図されない変更*

- *根拠のない経路情報の伝達*
- *経路情報の意図通りでない伝達*

経路情報に対する脅威(上記(c)であげた脅威)から守るためには、いかに伝達されてくる経路情報が正しいかを検証する必要があります。しかし、伝達されてくる経路情報は、BGP の Peer を張っているルータが正しいかどうかというような単純な問題ではなく、Origin AS が発行した経路情報が、伝達過程の AS の中で、その AS の意図通りに加工され、複数の経由 AS の意図が正しく盛り込まれ、最終的な AS に伝達されていることを検証する必要があります。

このような検証を実施できるようにするために IRR を利用するには、IRR は、経路情報の元来あるべき内容と、経路情報流入の根拠を調べられるような情報源になっている必要があります。

そして、この場合の IRR の安全上のあり方は、ルータの挙動と IRR の登録情報が密接に関わる場合に限られています。公共的な IRR の場合は、登録情報が AS に対して強い影響を及ぼさないことがあります。例えば、インターネットレジストリの割り振り情報と IRR の登録情報が対応しているべき、といった要件がどれほど強く適用されるべきなのかを検討する必要があります。

一方、IRR の利用者の観点では、登録情報の正当性に対する依存が発生します。これは他者の登録した情報が、どの程度正当なのかがわからなければ参照の意味が薄れてしまうからです。例えば弱い認証方式を利用して情報の登録を行った利用者は、他者の情報の登録に対しても弱い保護しか期待しなくなります。弱い認証方式が破られ、書き換えられている可能性を考慮しながら参照することは、ルータの管理者にとって上記の脅威を避ける手段としては弱いものになります。その結果、メールなどの他の手段を取らざるを得ず、IRR の効力が薄れてしまいます。

これらのことを考えると、IRR に求められる安全性を決める要素には下記のものがあることがわかります。

- *意図通りのルーティングのための安全性の観点*
  IRR の登録情報が AS に及ぼす影響の強さを想定する必要がある

- *IRR の利用者の観点*
  利用者の IRR に対する依存度を想定する必要がある

つまり、プライベートな IRR に比較して公共的な IRR は蓄積される情報の性質から、IRR の登録情報が AS に及ぼす影響の強さは低いと想定した場合、IRR の安全性は、利用者の IRR に対する依存度によって決定されるということになります。また、依存度は、不慮の操作の禁止、悪意のある操作の不可能性、適正な利用を促す仕組み(制約事項)などの対策を打つことで高めることが可能ということになります。

6.8.2 登録情報の安全性

前節までは、IRR とルーティングシステム全体を考慮したうえでの安全性について検討してきました。ここでは、さらにフォーカスを絞って、IRR への情報登録とそこからの情報提供に関する安全性に検討を進めます。

一般に「安全性」と呼ばれる性質の中には、いくつかの要素があります。
ここで、IRR における安全性という観点で考えると、その登録情報が安全に提供されことや、登録情報が正当性、可用性(availablity)を持ったものであるといった点が重視されると考えられます。その他に、機密性の要素も重要な要素の 1 つではありますが、公共的な IRR では、認証情報のような一部の情報を除くと、あまり重視されない要素であると考えています。

本節では、登録情報の正当性を分類し、「形式的な正当性」について述べます。次に、形式的な正当性が失われる場面と原因について述べ、対策を検討します。

IRR における登録情報の正当性は、まず IRR への登録内容が正しいこと、そして、登録や参照手続きの処理が確実であること、この 2 つが両立してはじめて成り立ちます。登録や閲覧手続きが確実であるとは、正しい登録者による登録結果が、その通りに誰もが閲覧できるような状態のことを指します。
ここでは、内容の正しさを「意味的な正当性」と呼び、登録や閲覧手続きの確実性に基づく正当性を、「形式的な正当性」と呼ぶことにします。

形式的な正当性が失われる状況を挙げると、以下のようになります。

- *登録情報自体の正当性が失われる状況*
  - *意図しない変更・削除*

・*災害*
・*サーバ・クライアントのバグ*
・*クライアント・ユーザへのなりすまし行為*

- *登録時の不正*
・*サーバへのなりすまし行為*
・*クライアント・ユーザへのなりすまし行為*

- *利用上の登録情報の正当性が失われる状況*

- *参照時の不正*
・*サーバへのなりすまし行為*
・*伝送路での書き換え(参照時、ミラー時)*

これまで、RPSL では「登録時の不正」に着目し、CRYPT-PW, PGP-KEY と言った認証機能を用意していました。しかし、形式的な正当性という見方をすると、登録者の認証だけでは、「意図しない変更・削除」や「参照時の不正」の対策をとることができません。これらの状況には、登録時以外での登録情報の変化が含まれており、登録者の認証だけでは、検出や回避することはできないためです。

つまり、登録情報の形式的な正当性を確認する仕組みが必要になります。
例えば、登録情報にハッシュ値を付加し、閲覧時に確認するといった方法です。登録者との関連性を保障するため、ハッシュ値に電子署名を加える方法が考えられます。しかし、RPSL ではオブジェクトに電子署名を加える書式は提供されていません。参照のために、Whois プロトコルの代わりに https を利用したとしても、「参照時の不正」や「サーバへのなりすまし行為」を検知することができるだけで、ミラーリングを行っているときの伝送路での書き換えを防ぐことはできません。

今後、形式上の正当性を確保するためには、CRISP や EPP(Extensible Provisioning Protocol)において電子署名を利用した登録情報の保護機能が必要になると考えられます。しかし、そのためには認証情報(署名鍵)の管理や登録の手続きなどを、今後検討する必要があります。

6.8.3 IRR のセキュリティ向上のための今後の対応

IRR のセキュリティを検討するために、いくつかの言葉の定義や IRR における安全性について基本的検討から行いました。

これらの検討の中で、登録情報の形式上の正当性について検討を進めましたが、その一方で、意味的な正当性の向上についてはほとんど検討がされていません。また、IRR に必要な安全性を決める要素として、ルーティングの安全性と IRR の利用者の観点を挙げましたが、これについても、運用者や IRR 情報のミラーリング時の検討が行われていません。さらに、形式的な正当性を確保するためには、登録時の認証ではなく、登録された情報を保護する仕組み(電子署名)を利用する仕組みについて述べましたが、現行の RPSL では電子署名を利用することはできません。

IRR に関するセキュリティの議論は、ルーティングシステムとの関連の中で検討する必要があるため、検討のポイントはルーティングシステム自体へとずれてしまいがちです。今後は、IRR そのもののセキュリティの検討と、ルーティングシステムと関連させたセキュリティの検討に分割すると共に、今回の検討で残されている検討項目をさらに検討していく必要があります。

2004 年度は、この IRR 企画策定専門家チームにおける検討を元に認証局の応用のシナリオを検討した。

7.1.1. 2004 年度に行われた議論とシナリオ

2003 年度の議論を受け、IRR 企画策定専門家チームの 2004 年度の議論では、IRR におけるセキュリティの目標の設定が行われた（図 7-1)。

概要

- **次世代（本来）のIRRのセキュリティ上のゴール**
  - **登録内容を信じて設定できること ⇒ 今回**
    - **考え方：信じて設定（例えば自動設定） ⇒ 楽 ⇒ 利用価値**
    - **仕組み：登録時の認証強化 ⇒ 登録内容のチェック ⇒ 正しい形で提供 ⇒ 機能的に利用**
  - **登録内容を使って相手認証できること ⇒ 将来**
    - **考え方：S-BGP、soBGP で使える ⇒ 経路ハイジャックに対する防衛強化**
    - **仕組み：登録時の認証強化 ⇒ 登録内容のチェック ⇒ 証明書発行 ⇒ 証明書を使ってAS認証**

図 7-1 IRR におけるセキュリティの目標の設定

またこの二つの目標を達成する為に、必要になる仕組みの提案がされた（図 7-2）。

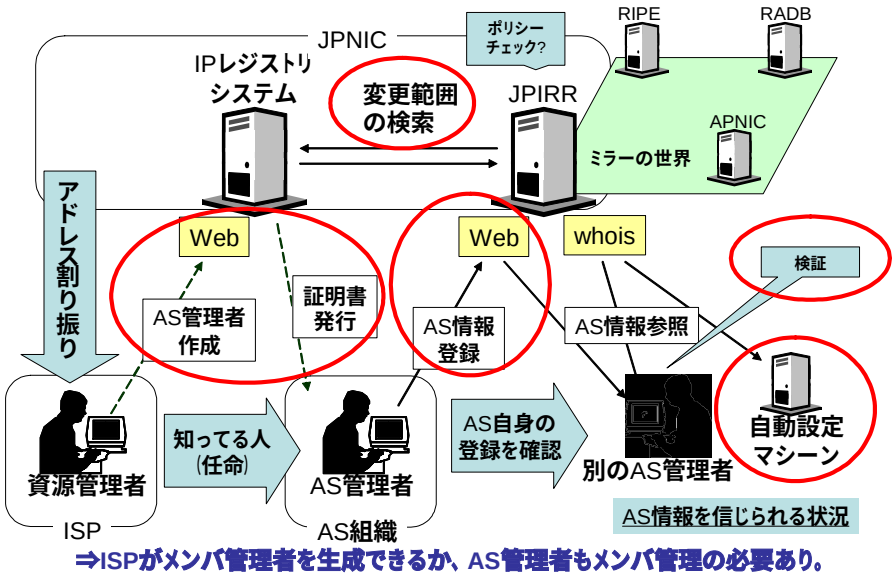


図 7-2 セキュリティの目標を達成するための仕組み

この仕組みは IRR への登録時の認証を強化し、登録情報と登録者の関係をたどれる状況を作ることで、IRR に登録された情報を使ったネットワーク機器の設定を行うことができるというものである。また登録情報に電子署名を付けることで、登録者と登録情報の正当性（改竄がないこと）を検証することが出来るようになるとしている。電子署名であれば他の IRR からミラーの仕組みを使って伝播してきた情報であっても、検証ができるとしている。

登録時の認証強化は Web インターフェースを使うなどすることで、既存のソフトウェアやプロトコルを使って実現する見込みがあるが、IRR の登録情報における電子署名を行う仕組みはこれまでにはなく、実現の為には新たに提案・開発を行っていく必要がある。

7.2. アドレス資源管理の効率化　－Web トランザクション－

本節では、IP レジストリシステムの Web トランザクション機能の目標、運用管理されているデータ及び業務を明らかにし、IP 指定事業者と交換するレジストリデータの安全性確保について述べる。

7.2.1. Web トランザクションの目標

レジストリデータ、中でもアドレス資源の管理において、指定事業者もしくは ISP が行う業務は多岐に渡る。ただし業務によっては年間数件のみの処理が必要な業務から、日常的に発生する業務まで、業務内容により様々である。そこで、今回は指定事業者が ISP の申請を受け、指定事業者が JPNIC へ申請をするという二段構成を検討し、指定事業者と JPNIC の間の連携実現を目指す。

IP アドレス管理業務において、基本となる 3 つの業務を以下に示す。

- IP アドレスの割り振り
  指定事業者からの割り振り申請に対して、IP アドレスの範囲を割り振る(割り振られた IP アドレスの範囲を、アサインメントウィンドウサイズ　以下 ASWS と略す)。
- IP アドレスの割り当て
  指定事業者が、割り振られた IP アドレスを実際に使用する場合に、割り振られたアドレスを割り当てる。
- 追加割り振り申請
  JPNIC から IP アドレスを指定事象者へ割り振り続けると、指定事業者へ割り振ることができるアドレスが不足することがある。その場合に、JPNIC が APNIC から、新しい IP アドレスの範囲を取得する必要がある。

3 つの業務のユースケース図を次頁に示す。

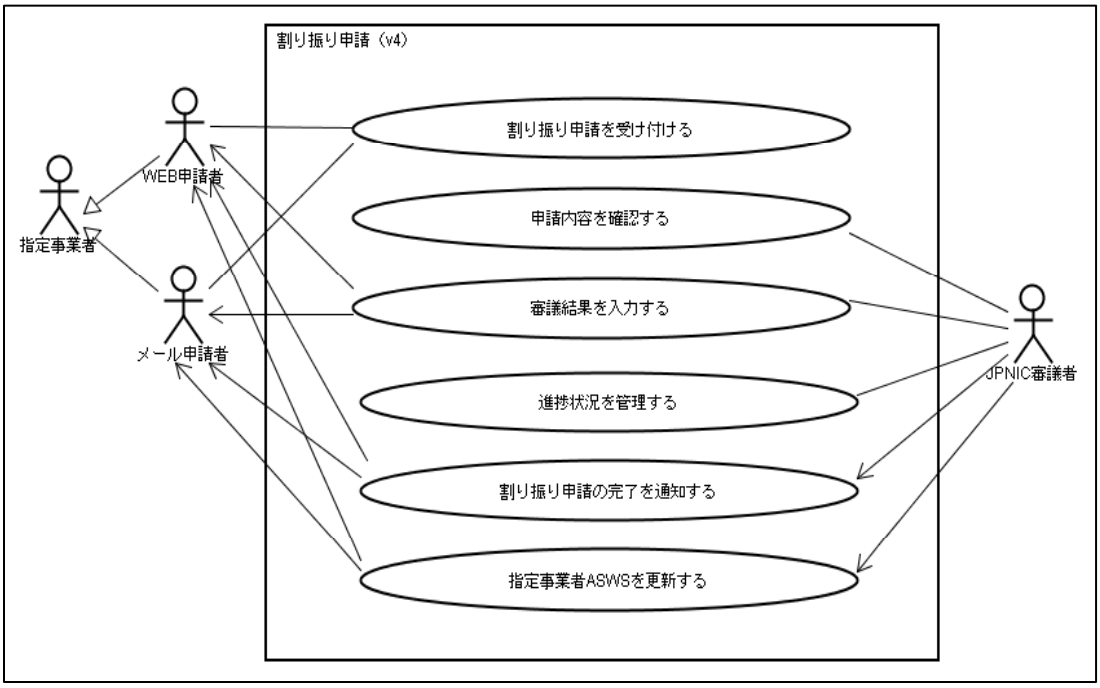


図 7-3　IP アドレス割り振り申請のユースケース図

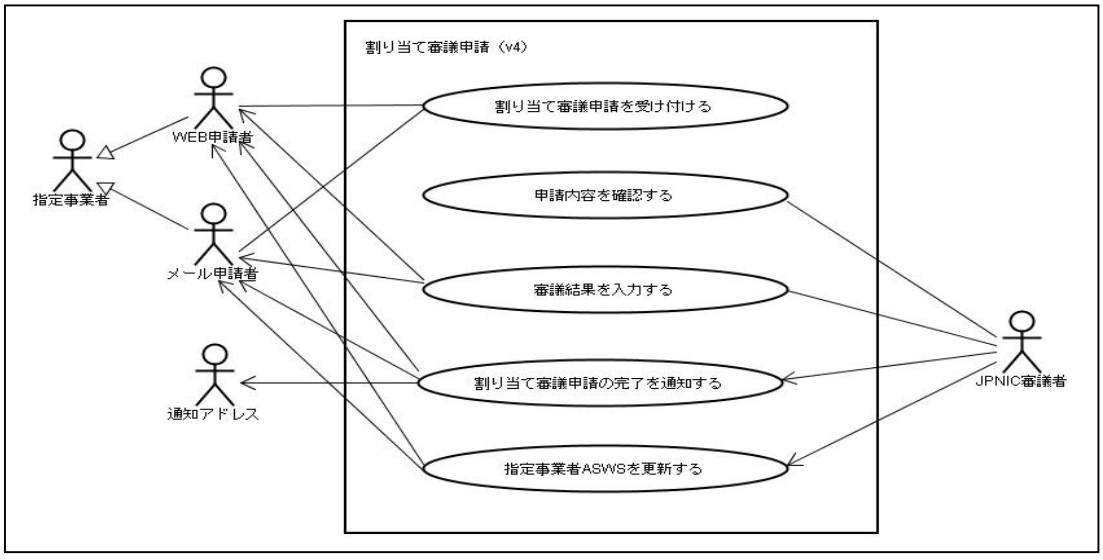


図 7-4　IP アドレス割り当て申請のユースケース図

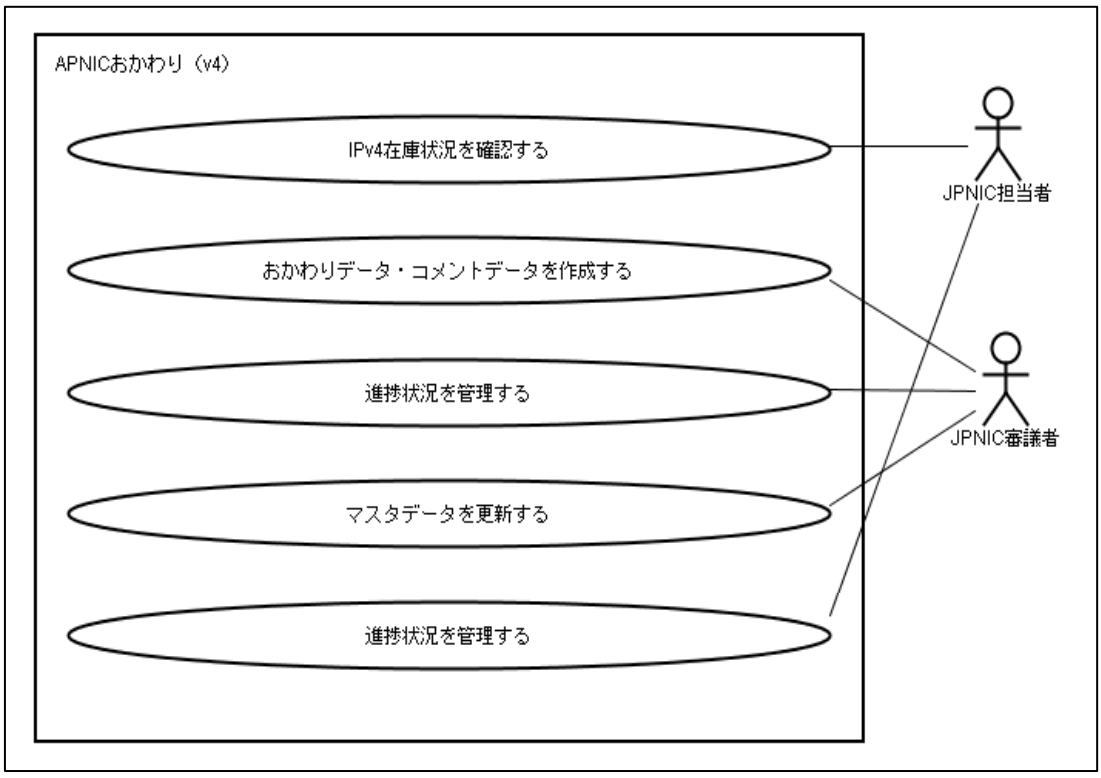


図 7-5　APNIC への追加割り振り申請のユースケース図

そこで、現在日常的にメールにて行われている、IP アドレス割り当て報告時における申請処理について、Web トランザクション方式を用いて処理の迅速化を図り、エンドユーザからの申請に対する指定事業者側の負担軽減を目的とする。

7.2.2. IP レジストリシステムが提供する機能リスト

IP レジストリシステムとは、JPNIC の IP 事業部の業務担当者が IP アドレス及び関連資源提供業務を行うにあたり、必要とする情報の保持、伝達、保守及び公開を行うことを目的としたシステムである。

IP レジストリシステムは、IPv4 アドレスの管理をはじめとする IP アドレス関連資源の管理業務を行う。主な機能は以下の通り。

- 指定事業者から、IP アドレスおよび関連資源の割り振りや返却の申請を受け付け、処理結果を IP レジストリシステムから指定事業者へ通知する。（表 7-1①）
- 指定事業者および指定事業者を含む一般申請者から、AS 番号の割り当て、返却、変更等の申請を受け付け、処理結果を IP レジストリシステムから指定事業者へ通知する（表 7-1②）

- APNIC に対して、共有プールの申請、指定事業者からの IPv6 に関する申請の取次ぎ申請、日本国内の IP アドレス割当報告等を行う（表 7-1③）
- 指定事業者を含めたインターネット利用者に対して、Whois データベース情報および逆引き DNS 情報の公開を行う（表 7-1④）
- 上記の各機能を JPNIC の業務担当者やシステム運用者が運用する（表 7-1⑤）

IP レジストリシステムの利用者、接続システムとの関係イメージを図 7-6 に示す。

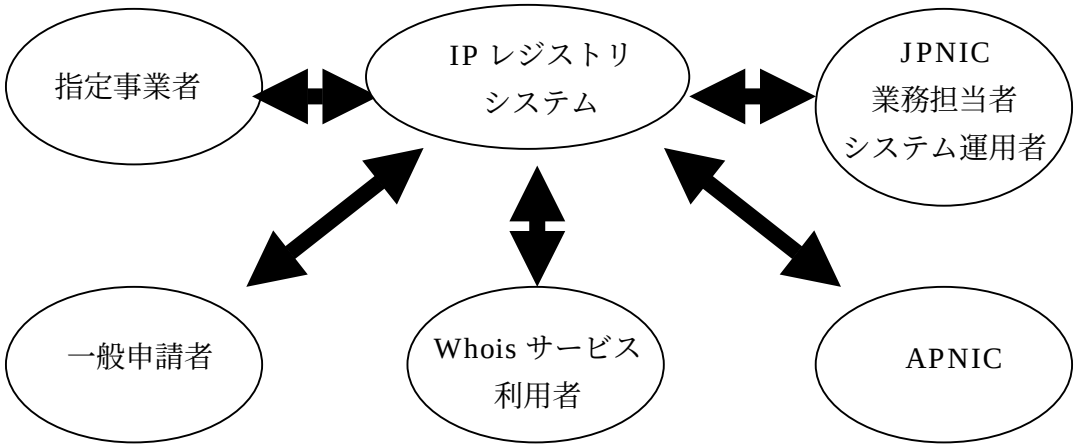


図 7-6　IP レジストリシステムの関係イメージ

IP レジストリシステム内で処理する主な申請業務を、次の表に示す。

表 7-1　主な申請業務一覧

申請名	利用方法			対象者			申請概要
	①	②	③	④	⑤	⑥	
割り振り申請(v4)	○	○		○		○	指定事業者からの割り振り申請を受付け、申請内容について JPNIC 審議を行い、APNIC 共有プールまたは追加割り振り申請のプールから割り振り処理を行う。
割り振り返却申請(v4)	○	○		○		○	指定事業者からの割り振り返却申請を受付け、申請内容について JPNIC 審議を行い、追加割り振り申請のプールへ割り振り返却処理を行う。

APNIC への返却申請	○					○	割り振り返却申請(v4)において、追加割り振り申請のプールへ割り振り返却処理されたアドレスブロックを一定期間エージングし、APNIC 共有プールへ返却処理を行う。
割り当て審議申請(v4)	○	○		○		○	指定事業者からの割り当て審議申請を受付け、申請内容について JPNIC 審議を行い、審議結果を通知する。
割り当て報告申請	○	○		○			指定事業者からの割り当て報告申請を受付け、申請内容について JPNIC 審議を行い、割り当て情報の更新処理を行う。
割り当て・リナンバ報告・返却の取下申請	○			○		○	指定事業者からの割り当て・リナンバ報告・返却の取下申請を受付け、申請の取下処理を行う。
イベント割り当て申請	○			○		○	指定事業者からのイベント割り当て申請を受付け、申請内容について JPNIC 審議を行い、イベント割り当て処理を行う。
割り当て済アドレスの統廃合申請	○			○		○	指定事業者からの割り当て済アドレスの統廃合申請を受付け、申請内容について JPNIC 審議を行い、アドレス統廃合処理を行う。
割り当て IP アドレスの返却申請	○	○		○			指定事業者からの割り当て IP アドレスの返却申請を受付け、割り当て返却処理を行う。
割り当て返却年月日変更申請	○			○			指定事業者からの割り当て返却年月日変更申請を受付け、割り当て返却年月日の更新処理を行う。
ネットワーク記載事項変更申請	○	○		○		○	指定事業者からのネットワーク記載事項変更申請を受付け、申請内容について JPNIC 審議を行い、ネットワーク情報の更新処理を行う。
IP 指定事業者情報変更申請	○	○		○		○	指定事業者からの IP 指定事業者情報変更申請を受付け、申請内容について JPNIC 確認を行い、指定事業者情報の更新処理を行う。
逆引きネームサーバ申請	○	○		○		○	指定事業者からの逆引きネームサーバ申請を受付け、申請内容について JPNIC 審議を行い、逆引き DNS の更新処理を行う。
個人情報申請	○	○		○		○	指定事業者からの個人情報申請を受付け、申請内容について JPNIC 審議を行い、個人情報の更新処理を行う。

AS 割り当て申請	○			○	○	○	指定事業者または一般利用者からの AS 割り当て申請を受付け、申請内容について JPNIC 審議を行い、AS 番号割り当て処理を行う。
AS 返却申請	○	○		○	○	○	指定事業者または一般利用者からの AS 返却申請を受付け、申請内容について JPNIC 審議を行い、AS 番号割り当て返却処理を行う。
AS 情報変更申請	○	○		○	○	○	指定事業者または一般利用者からの AS 情報変更申請を受付け、申請内容について JPNIC 審議を行い、AS 番号情報の更新処理を行う。
指定事業者契約申請	○		○	○	○	○	指定事業者または一般利用者からの指定事業者契約申請を受付け、申請内容について JPNIC 審議を行い、郵送で契約関連書類を取り交わし、契約締結処理と行う。
指定事業者解約申請	○	○	○	○		○	指定事業者からの指定事業者解約申請を受付け、郵送で解約関連書類を取り交わし、申請内容について JPNIC 審議を行い、契約解約処理と行う。
APNIC 向け追加割り振り申請 (v4)	○					○	V4 アドレスブロックが不足した際に、JPNIC 業務担当者が APNIC へ v4 アドレスブロックの割り振り依頼を行う。
APNIC 向け追加割り振り申請(AS)	○					○	AS 番号が不足した際に、JPNIC 業務担当者が APNIC へ AS 番号の割り振り依頼を行う。
V6 割り振り申請取次ぎ	○	○		○		○	指定事業者からの割り振り申請取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ割り振り依頼を行う。
V6 割り振り変更取次ぎ	○	○		○		○	指定事業者からの割り振り申請取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ割り振り情報の更新依頼を行う。
V6 割り振り返却取次ぎ	○	○		○		○	指定事業者からの割り振り返却取次ぎを受付け、申請内容について JPNIC 審議を行い、APNIC へ返却依頼を行う。
V6 割り当て申請取次ぎ	○	○		○			指定事業者からの割り当て申請取次ぎを受付け、APNIC 向けデータベースの更新処理を行う。
特殊用途 PI アドレス割当取次ぎ	○		○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス割り当て取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で契約関連書類を取り交わし、契約締結処理を行う。また、APNIC へ割り当て依頼を行う。

特殊用途 PI アドレス変更取次ぎ	○		○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス変更取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で変更関連書類を取り交わし、契約更新処理を行う。また、APNIC へ割り当て情報の更新依頼を行う。
特殊用途 PI アドレス解約取次ぎ	○	○	○	○	○	○	指定事業者または一般利用者からの特殊用途 PI アドレス解約取次ぎを受付け、申請内容について JPNIC 審議を行い、郵送で解約関連書類を取り交わし、解約処理を行う。また、APNIC へ割り当て情報の更新依頼を行う。
アドレスリスト申請	○		○	○	○	○	指定事業者または一般利用者からのアドレスリスト申請を受付け、申請内容について JPNIC 確認を行い、パスワード発行処理を行う。
情報開示請求申請	○		○	○	○	○	指定事業者または一般利用者からの情報開示請求申請を受付け、申請内容について JPNIC 確認を行い、開示情報リストの作成処理を行う。

利用方法　①：Web　②：メール　③：郵送

対象者　④：指定事業者　⑤一般利用者　⑥：JPNIC 業務担当者

また、表 7-2 にレジストリデータの管理や外部連携等、主な機能を示す。

表 7-2　IP レジストリシステムの主な提供機能

機能区分	機能名	機能概要
資源管理	V4 割り振り管理	割り振り申請(v4)、割り振り返却申請(v4)、APNIC への返却申請、APNIC 向け追加割り振り申請 (v4)、指定事業者契約申請における v4 割り振り管理を行う。
	V4 割り当て管理	割り当て審議申請(v4)、割り当て報告申請(v4)、割り当て・リナンバ報告・返却の取下げ申請、イベント割り当て申請、割り当て済アドレスの統廃合申請、割り当て IP アドレスの返却申請、割り当て返却年月日変更申請における v4 割り当て業務を行う。
	V6 割り振り管理	V6 割り振り申請取次ぎ、v6 割り振り変更取次ぎ、v6 割り振り返却取次ぎにおける v6 割り振り管理を行う。
	V6 割り当て管理	V6 割り当て申請取次ぎにおける v6 割り当て管理を行う。

	AS 割り当て管理	AS 割り当て申請、AS 返却申請、AS 情報変更申請、APNIC 向け追加割り振り申請 (AS)、指定事業者契約申請における AS 割り当て管理を行う。
	特殊用途 PI 割り当て管理	特殊用途 PI アドレス割り当て取次ぎ、特殊用途 PI アドレス変更取次ぎ、特殊用途 PI アドレス解約取次ぎにおける特殊用途 PI 割り当て管理を行う。
	個人情報管理	個人情報申請における個人情報管理を行う。
	ネットワーク情報管理	ネットワーク記載事項変更申請におけるネットワーク情報管理を行う。
	ML リスト管理	日次処理として、ML リストの更新処理を行う。
	IP リスト管理	日次処理として、IP リストの更新処理を行う。
	AS 番号リスト管理	日次処理として、AS 番号リストの更新処理を行う。
	Whois 情報管理	Whois データ更新時に、JPNIC　Whois データベースの更新処理を行う。
契約管理	指定事業者契約管理	指定事業者契約申請における指定事業者契約関連処理を行う。
	指定事業者変更管理	IP 指定事業者情報変更申請における指定事業者変更処理を行う。
	指定事業者解約管理	指定事業者解約申請における指定事業者解約処理を行う。
外部連携	APNIC 連携	APNIC 向け Whois 情報、逆引き DNS 情報を作成し、APNIC データベースへの連携を行う。
	JPRS 連携	JPRS 向け Whois 情報、逆引き DNS 情報を作成し、JPRS データベースへの連携を行う。
Whois	Whois 検索 (Web)	Web ブラウザからの Whois 検索を行う。
	Whosi 検索（Whois クライアント）	Whois クライアントからの Whois 検索を行う。

表 7-1 および表 7-2 に示す通り、IP アドレス管理業務は多岐に渡る。申請業務のほとんどが、メールによる申請と、Web での申請状態確認という位置付けであるため、申請担当者及び JPNIC 業務担当者の双方にとって、効率が悪い。

そこで、メールでの申請ではなく、Web により直接申請が可能なように効率化を図る。従来、メールによる申請担当者の認証は、メールの送信元アドレスを基本としている。Web での申請の場合も、申請担当者の認証が同様に必要となる。Web での認証としては、証明書による認証基盤を利用する。

7.2.3. IP レジストリシステムの構成

まず、現在、IP アドレス管理業務を運用している IP レジストリシステムの構成を明らかにする。続いて、IP レジストリシステム上に、証明書による認証基盤を連携する場合に、どのようなシステム連携で、申請担当者認証を行うのかを明らかにしていく。

IP レジストリシステムの論理ネットワーク構成図を図 7-7 に示す。

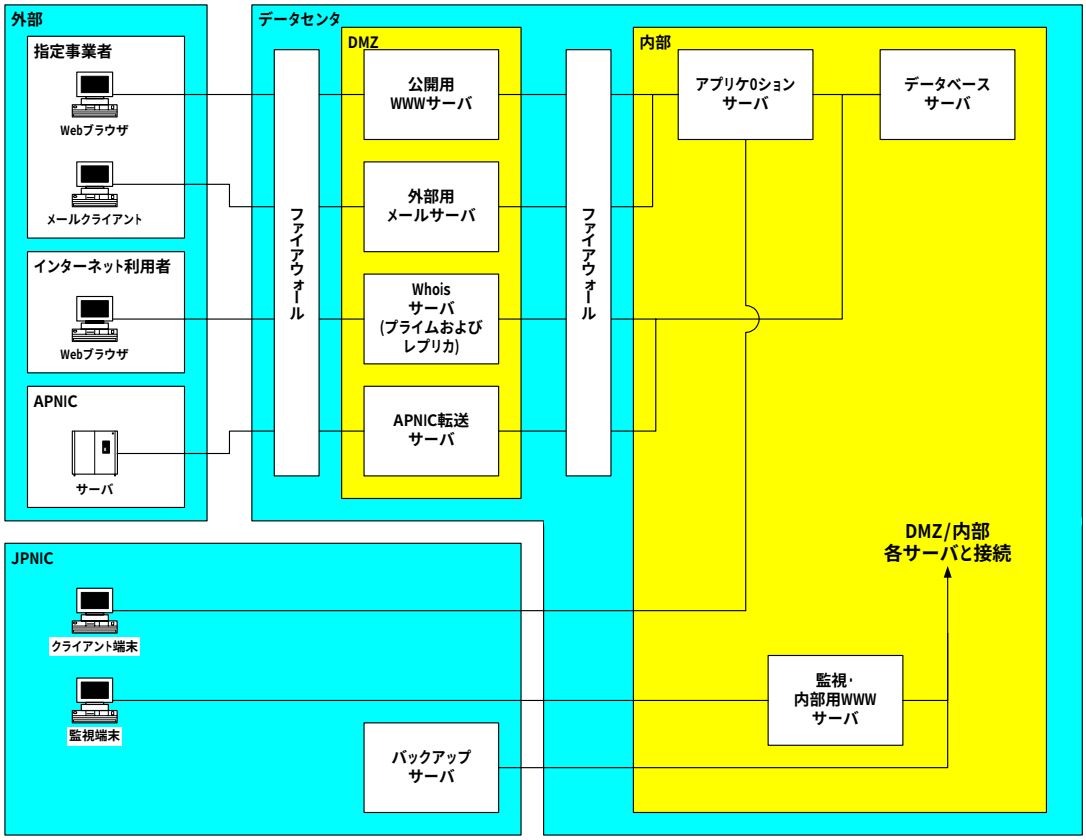


図 7-7　IP レジストリシステムの論理ネットワーク構成図

また、各サーバでの提供機能を表 7-3 に示す。

表 7-3　IP レジストリシステム内サーバの提供機能

サーバ名	提供機能
メールサーバ	・インターネットを経由した指定事業者からのメールによる各種申請の受付け及び応答を行う。
公開用 WWW サーバ	・インターネットを経由した指定事業者からの Web ブラウザによる各種申請等の受付け及び応答を行う。
Whois サーバ(プライム)	・インターネットを経由した一般利用者からの Web ブラウザによる Whois サービスの受付け及び応答を行う。 ・Whois サーバ(レプリカ)との複数構成により、負荷分散と障害時のサービス継続を行う。
Whois サーバ(レプリカ)	・インターネットを経由した一般利用者からの Web ブラウザによる Whois サービスの受付け及び応答を行う。
APNIC 転送サーバ	・APNIC システムとの間で、逆引き DNS データ、Whois データの送受信を行う。
アプリケーションサーバ	・公開用 WWW サーバ、メールサーバからの要求を元に、各種申請を処理する。
データベースサーバ	・主なデータを格納し、アプリケーションサーバからの処理要求を受付ける。
監視・内部用 WWW サーバ	・IP レジストリシステム内の各サーバ及びネットワーク機器の動作状態を監視する。 ・JPNIC 内部用 WWW サーバを兼ね、JPNIC 業務管理者が申請業務を処理する際に利用する。
バックアップサーバ	IP レジストリシステム内の各サーバのデータについて、バックアップを行う。

7.2.4. IP アドレス認証局と IP レジストリシステムとの連携

IP レジストリシステムで表 7-1 及び表 7-2 で示した各種申請を行う際に重要となるのは、申請担当者の認証である。申請担当者を認証するために、IP アドレス認証局システムが IP レジストリシステムと連携してクライアント証明書を発行するまでの処理の流れを、図 7-8 に示す。認証情報の連携は、2003 年度の“IP アドレス認証局のマネジメントに関する調査研究”の際に策定したモデルを適用し、設計する。

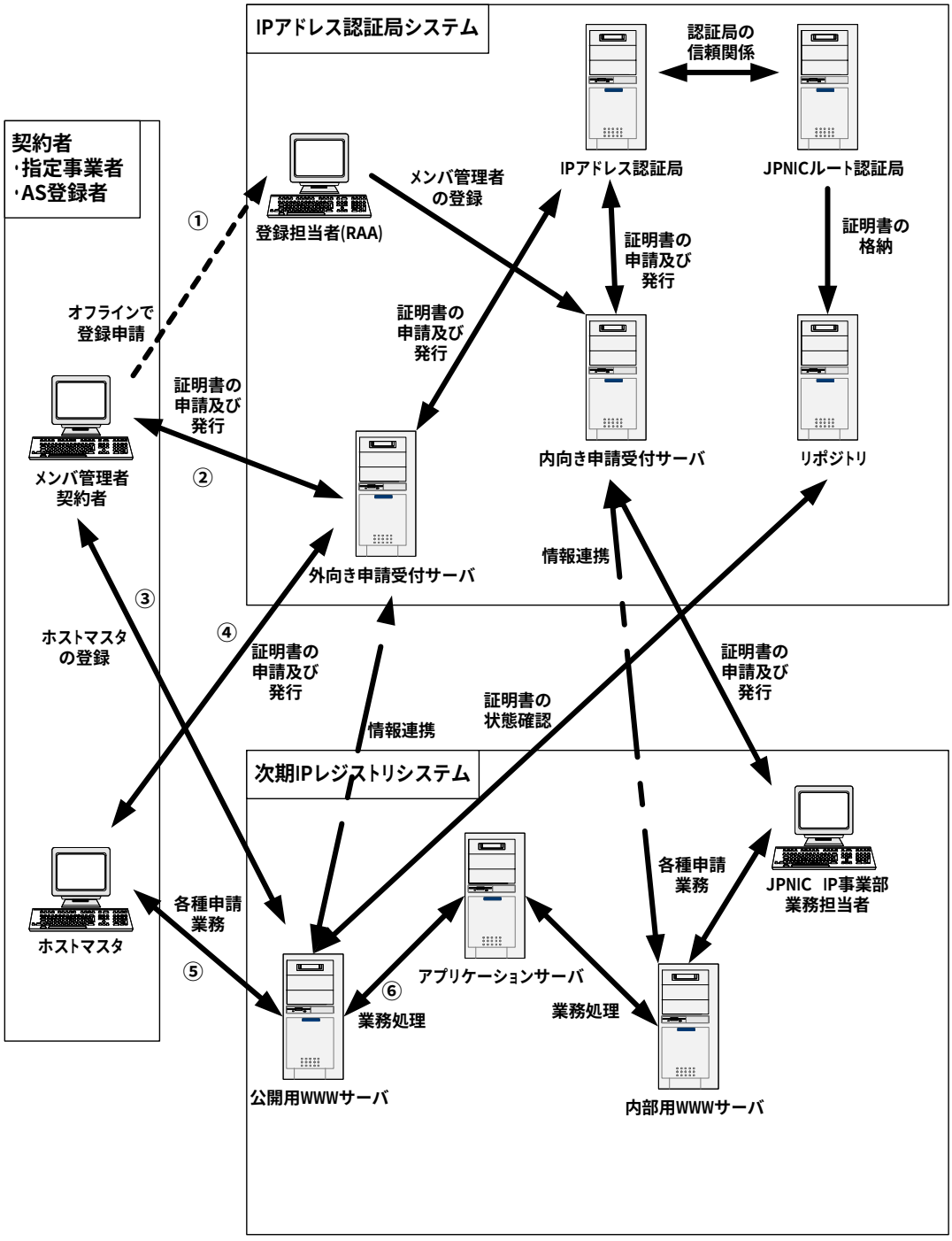


図 7-8　IP レジストリシステムと IP アドレス認証局システムの連携

図 7-8 において、ホストマスタが申請業務を行うまでの流れを、以下に示す。

- ①において、メンバ管理者自身の証明書の発行申請を行う
- ②において、登録担当者から返却された情報を元に外向き申請受付サーバへアクセスし、メンバ管理者が自身の証明書を取得する

- ③において、ホストマスタの情報を登録しておく
- ④において、③で登録された情報でホストマスタが外向き申請受付サーバへアクセスし、ホストマスタ自身の証明書を取得する
- ⑤において、ホストマスタ自身の証明書を使用して公開用 WWW サーバへアクセスし、申請業務を行う
- ⑥において、申請者（すなわちホストマスタ）の権限および申請内容を確認し、処理する

図 7-8 に示すように、IP レジストリシステム上のユーザを IP アドレス認証局システム上で認証するためには、IP レジストリシステムと IP アドレス認証局システムを連携するための設計が必要となる。

IP レジストリシステムと IP アドレス認証局システムそれぞれでユーザが利用する Web ページの遷移及び両システム間でインターフェースしあうデータの流れ(図 7-8 中の外向き申請受付サーバと公開用 WWW サーバ間及び内向き申請受付サーバと内部用 WWW サーバ間の情報連携部分)を詳細化したものを図 7-9 に示す。

外向き申請受付サーバおよび公開用 WWW サーバは、インターネットを介した契約者からのアクセスに利用される。内向き申請受付サーバおよび内部用 WWW サーバは、JPNIC IP 事業部の業務担当者からのアクセスに利用される。

IP レジストリシステムと IP アドレス認証局システム間で連携されるデータは、クライアント証明書を申請するために利用される。クライアント証明書と 1 対 1 に対応する証明書認証 ID は、メンテナーコードというグループに所属する。メンテナーコードとは、操作対象資源と操作権限を持つグループである。

IP レジストリシステム内のデータベースにて保管されているメンテナー及び証明書認証 ID に関するデータを、クライアント証明書への処理の際に IP アドレス認証局システムからの問い合わせに対して適切に回答するインターフェースが、図 7-9 におけるメンテナートランザクション CGI である。このインターフェースにより、IP レジストリシステムと IP アドレス認証局システムの間で、認証のためのデータの連携が実現可能となる。

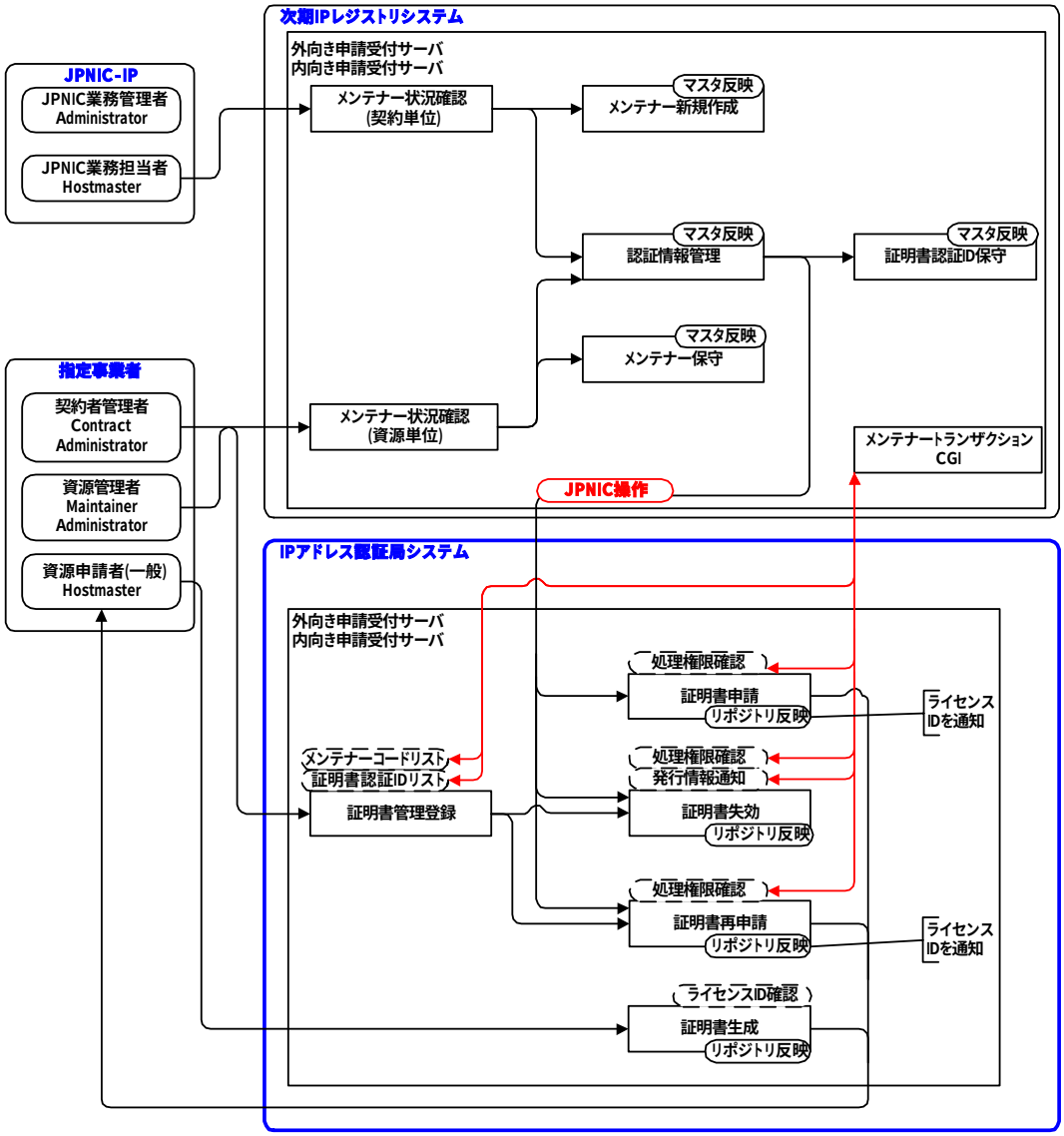


図 7-9　IP レジストリシステムと IP アドレス認証局間のデータの流れ

図 7-9 中において、IP アドレス認証局が IP レジストリシステムにて動作するメンテナートランザクション CGI との通信を行う 4 つのインターフェースについて、表 7-4 に示す。

表 7-4　インターフェース一覧

インターフェース名	処理内容
メンテナーコードリスト取得	証明書に関する処理を行いたいメンテナーを検索するためのインターフェース。 メンテナーコードを直接指定するのみではなく、メンテナーコードが所属している組織や、対応する契約管理番号もしくは資源管理者番号からも検索可能である。
証明書認証 ID リスト取得	特定のメンテナーコードに紐付いている証明書認証 ID のリストを取得するためのインターフェース。
処理権限確認	証明書に関する操作を行う場合、処理対象となる証明書認証 ID が紐付いているメンテナーコードの権限を管理可能か、確認するためのインターフェース。
発行情報通知	証明書に関する操作が完了した場合、操作に関する情報(証明書の発行もしくは失効)を IP レジストリシステムへ通知するためのインターフェース。

表 7-4 に示した 4 つのインターフェースについて、問い合わせ内容、返却値および返却例について、表 7-5 から表 7-14 に示す。

表 7-5　メンテナーコードリスト取得インターフェース

項番	項目名	備考
1	検索区分	1：契約管理番号、2：資源管理者番号、3：資源管理者略称、4：組織名、5：メンテナー検索
2	検索対象	検索したい文字列

表 7-6　メンテナーコードリスト取得インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	メンテナー情報	複数回指定可
3-1	メンテナーコード	検索された情報に紐付いているメンテナーコード
3-2	権限識別子	3-1 で返却するメンテナーコードの権限

3-3	組織名	3-1 で返却するメンテナーコードの所属組織
3-4	メンテナー識別名	3-1 で返却するメンテナーコードの識別名
4	件数	返却するメンテナーコード数

表 7-7　メンテナーコードリスト取得インターフェースへの返り値例

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Tue, 28 Sep 2004 02:15:06 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Tue, 28 Sep 2004 02:09:24 GMT
Content-Length: 101

RET=00
RET_CODE=00000000
MNTNER=MNT-JP000001¥tMNT_AR=4¥tORG_NUM=
Japan Network Infomation Center¥tMNT_NM=山田太郎
MNTNER=MNT-JP000002¥tMNT_AR=5¥tORG_NUM=
Japan Network Infomation Center¥tMNT_NM=佐藤次郎
COUNT=2
```

表 7-8　証明書認証 ID リスト取得インターフェース

項番	項目名	備考
1	メンテナーコード	証明書認証IDのリストを取得したいメンテナーコード

表 7-9　証明書認証 ID リスト取得インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	権限識別子	問い合わせされたメンテナーコードの権限 1：JPNIC 業務管理者、2：JPNIC 業務担当者、3：契約管理者、4：資源管理者、5：資源申請者

4	組織名	問い合わせされたメンテナーコードの所属組織
5	証明書認証 ID	問い合わせされたメンテナーコードに紐付いている証明書認証 ID
6	件数	返却する証明書認証 ID 数

表 7-10　証明書認証 ID リスト取得インターフェースへの返り値例

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Date: Tue, 28 Sep 2004 02:15:06 GMT
Content-Type: text/plain
Accept-Ranges: bytes
Last-Modified: Tue, 28 Sep 2004 02:09:24 GMT
Content-Length: 150

RET=00
RET_CODE=00000000
MNT_AR=4
ORG_NUM = Japan Network Infomation Center
CERT_ID=1234567
CERT_ID=2345678
COUNT=2
```

表 7-11　処理権限確認インターフェース

項番	項目名	備考
1	処理者メンテナーコード	証明書の発行を依頼するユーザのメンテナーコード
2	被処理者メンテナーコード	証明書を発行する対象ユーザのメンテナーコード

表 7-12　処理権限確認インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000

表 7-13　発行情報通知インターフェース

項番	項目名	備考
1	メンテナーコード	証明書状態が変更された証明書認証 ID が紐付いているメンテナーコード
2	証明書認証 ID	証明書状態が変更された証明書認証 ID
3	申請状態フラグ	証明書状態 1：発行済み、2：失効済み

表 7-14　発行情報通知インターフェースへの返り値

項番	項目名	備考
1	処理結果	正常時：00
2	理由コード	正常時：00000000
3	メンテナーコード	通知されたメンテナーコード
4	証明書認証 ID	通知された証明書認証 ID

7.2.5. LIR 認証局と IP レジストリシステムとの連携

前節では、申請担当者を認証するためのクライアント証明書を発行及び失効する際の処理の流れを示した。ここでは、申請担当者ではなく指定事業者システムを利用する複数のユーザを仮想的に申請担当者とみなす場合を検討する。

図 7-10 において、指定事業者システムの WWW サーバが、IP レジストリシステムからは一人の申請担当者として見ることができる。すなわち、IP レジストリシステムと関連するクライアント証明書を所有しない複数の申請担当者は、指定事業者システムの WWW サーバに認証を肩代わりしてもらうことにより、認証の通った申請業務を遂行可能となる。

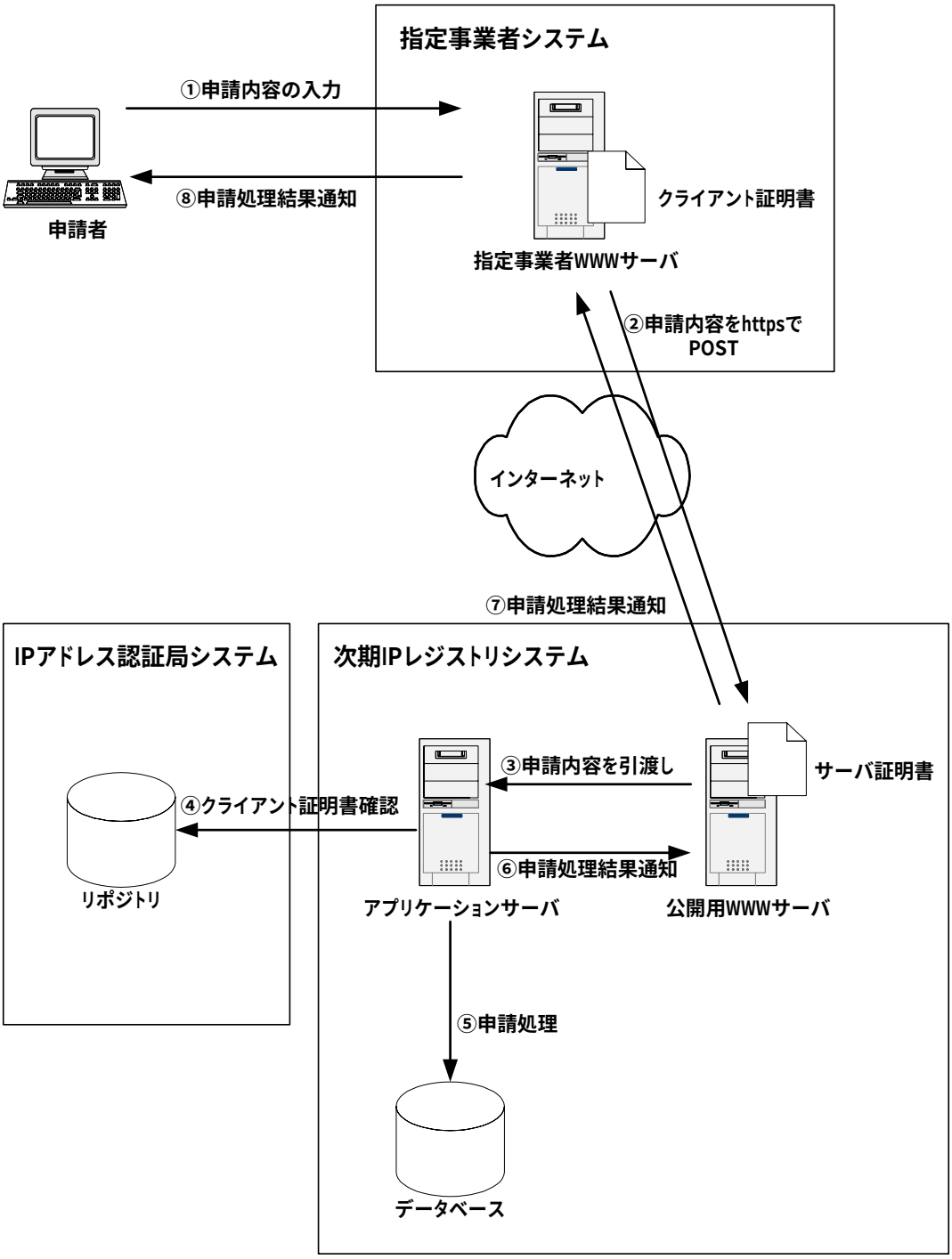


図 7-10　Web トランザクションによる申請の流れ

7.2.6. LIR の認証モデル

https での通信において、通信の暗号化とともにクライアント認証も重要である。ここでは、Web トランザクションによるアクセスと、一般申請者が Web ブラウザでアクセスする際の 2 種類のアクセスについて、クライアント証明書を利用したクライアント認証処理の流れを示す。

まずは Web トランザクションによるアクセスの場合を示す。図 7-10 において、「② 申請内容を https で POST」の部分で、クライアント認証を行う必要がある。トランザクションの流れを以下に示す。(図 7-11 参照)

- 事前に、IP アドレス認証局にて発行したクライアント証明書を https クライアントに組み込んでおく必要がある。
- １、指定事業者 WWW サーバ内の https クライアントが、IP レジストリシステムの公開用 WWW サーバへ https 通信を開始する。
- ２、公開用 WWW サーバが、自身の WWW サーバ証明書を https クライアントに通知し、https クライアントは WWW サーバ証明書を確認する。
- ３、https クライアントが、自身のクライアント証明書を公開用 WWW サーバへ通知し、公開用 WWW サーバはクライアント証明書を確認する。その際に、クライアント証明書の有効期限チェック、IP アドレス認証局のリポジトリ内 CRL のチェックを経て、問題がない場合はクライアント証明書内に格納されているメンテナーコードを取得する。
- ４、メンテナーコードから権限や処理可能な資源情報をデータベースから取得し、申請内容との整合性を確認する。

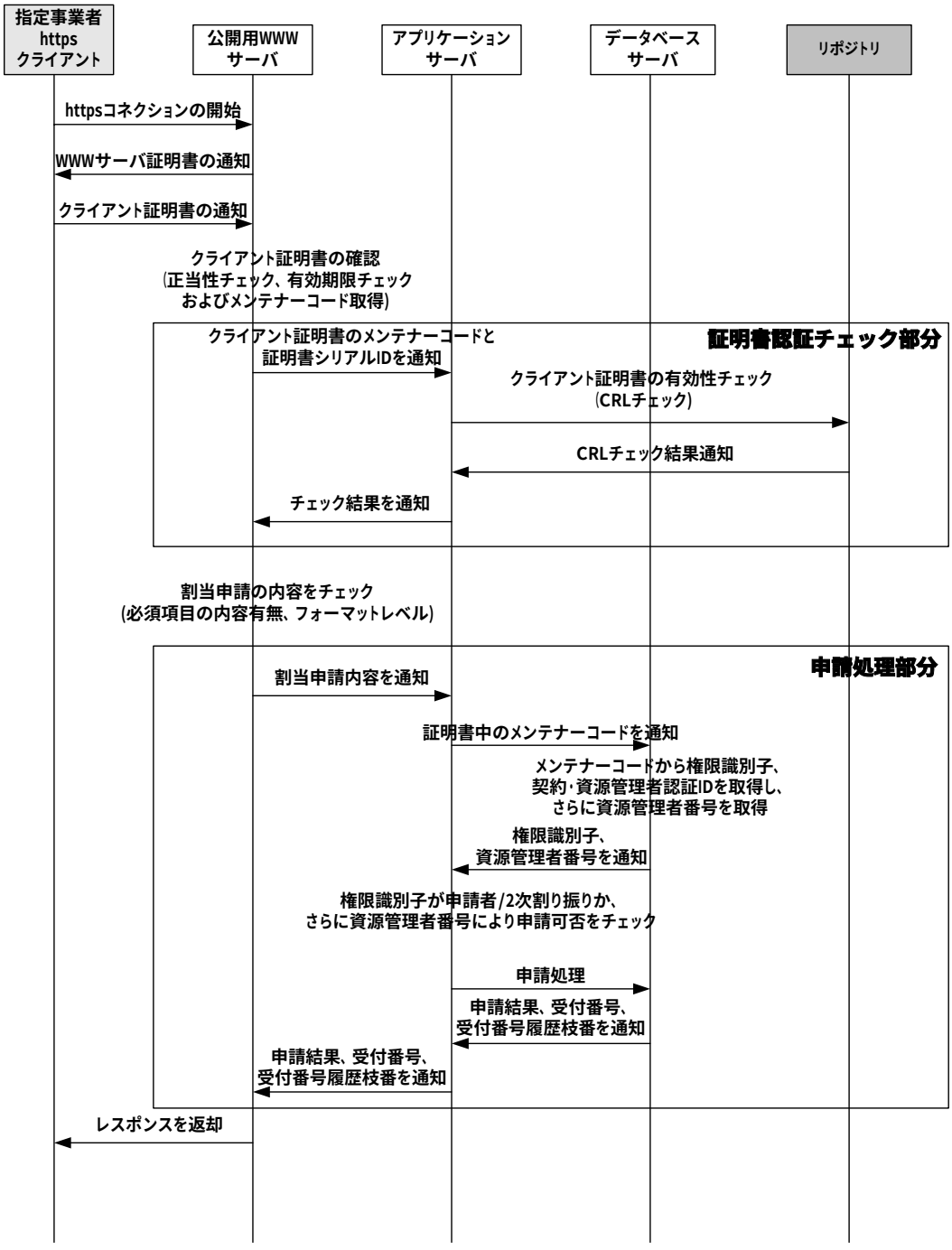


図 7-11　トランザクション処理の流れ

Web トランザクションにおけるクライアント認証と同様に、一般申請者が Web ブラウザを使用して、クライアント証明書による認証により公開用 WWW サーバへアクセスする実装も可能である。

- 事前に、IP アドレス認証局にて発行したクライアント証明書を Web ブラウザに組み込んでおく必要がある。
- １、Web ブラウザにより公開用 WWW サーバへ https を使用してアクセスする。
- ２、公開用 WWW サーバが、自身の WWW サーバ証明書を Web ブラウザに通知し、Web ブラウザは WWW サーバ証明書を確認する。
- ３、Web ブラウザが、組み込まれているクライアント証明書を公開用 WWW サーバへ通知し、公開用 WWW サーバはクライアント証明書を確認する。その際に、クライアント証明書の有効期限チェック、IP アドレス認証局のリポジトリ内 CRL のチェックを経て、問題がない場合はクライアント証明書内に格納されているメンテナーコードを取得する。
- ４、メンテナーコードから権限や処理可能な資源情報をデータベースから取得し、権限に対応した Web ページを Web ブラウザへ返す。

7.2.7. 運用上の問題点と課題

クライアント証明書による認証は、アクセス元を特定する手段として有効であるが、クライアント証明書の管理に慎重になる必要がある。本節では、クライアント証明書の運用上の問題点と課題について述べる。

まず、指定事業者への証明書提供(運用管理部分)に関する問題点と課題について検討する。

クライアント証明書を利用した認証システムにおいては、クライアント証明書の管理に注意する必要がある。

証明書は、有効期限を設定して発行される。一般的には、クライアント証明書の有効期限は１年間である。発行から１年間経過した場合、そのクライアント証明書は無効となり、認証に使用できない。よって、クライアント証明書の再発行、引渡し、設定を考慮すると、有効期限が切れる１ヶ月前程度を目安とし、更新処理を行う必要がある。クライアント証明書を利用するすべての指定事業者に対して、同じタイミングでクライアント証明書を発行するならば、更新処理も同じタイミングで可能だが、契約時期が異なる場合はクライアント証明書の発行タイミングも異なることとなり、指定事業者毎に異なるタイミングで更新処理を行う必要がある。

クライアント証明書自体の管理も厳重に行う必要がある。現在の不正アクセス、個人情報漏洩問題と関連し、以下のような問題点がある。

- クライアント証明書が組み込まれているモバイル PC を盗難され、不正アクセスされてしまう。
- クライアント証明書のファイルが不正に複製され、外部に漏洩し、不正アク

セスされてしまう。

- また、有事の際の対処としては、機能面と業務面の 2 つの方向からの対処が挙げられる。まずは機能面での対処について、以下に示す。
- 不正アクセスに使用されたユーザのアカウントを、IP レジストリシステム側で無効とする。IP アドレス認証局システム側でクライアント証明書として正当なものと認識されたとしても、IP レジストリシステム側のアカウントが無効となっている場合は、ログインおよび申請業務を不可とする。
- 不正アクセスに使用されたユーザのクライアント証明書を、IP アドレス認証局システム側で失効扱いとする。IP レジストリシステム側での認証の際に、CRL に挙がっているクライアント証明書からのアクセスを拒否する。
- 業務面での対処としては、以下が挙げられる。
- クライアント証明書を組み込んだ PC の厳重管理。
- クライアント証明書を組み込んだ PC が盗難された場合の、クライアント証明書失効処理の明確化。
- 日常的な、クライアント証明書によるアクセス及び申請内容の確認。
- クライアント証明書を利用する PC の IP アドレス管理。
- 管理者のクライアント証明書に対して、責任を集中させることによる不正の抑止。(申請担当者の不正によるペナルティを、申請担当者の管理者も負わせることによる、指定事業者内での抑止効果を目的とする)

次に、提供業務の拡張に関する問題点と課題について検討する。6.4.6.5 において、IP アドレス割当申請業務について、メールによる申請を Web トランザクション化することによる申請業務の円滑化を図った。さらなる申請業務の円滑化を拡大することを目的とし、別の申請業務を Web トランザクション化する場合、各申請業務を実施可能な権限が問題となる。Web トランザクションを処理する指定事業者側 WWW サーバに組み込むクライアント証明書を、どの権限のメンテナーコードで発行するか、考慮する必要がある。

表 7-15　主な業務毎の処理実施可否について

主な業務名称	契約管理者	資源管理者	資源申請者
指定事業者 契約関連	○	×	×
資源管理情報関連	○	○	×
資源の割り振り 申請	×	×	○
資源の割り当て 報告	×	×	○

表 7-15 にて、権限によって可能な業務が分けられていることを示す。この場合、指定事業者 WWW サーバに組み込んでいるクライアント証明書のメンテナーの権限によっては、申請を受理できない。契約管理者の権限を持つメンテナーコードのクライアント証明書を使用すると、資源管理者や資源申請者が行う業務については、権限が合わず、申請ができない。(図 7-12 参照)

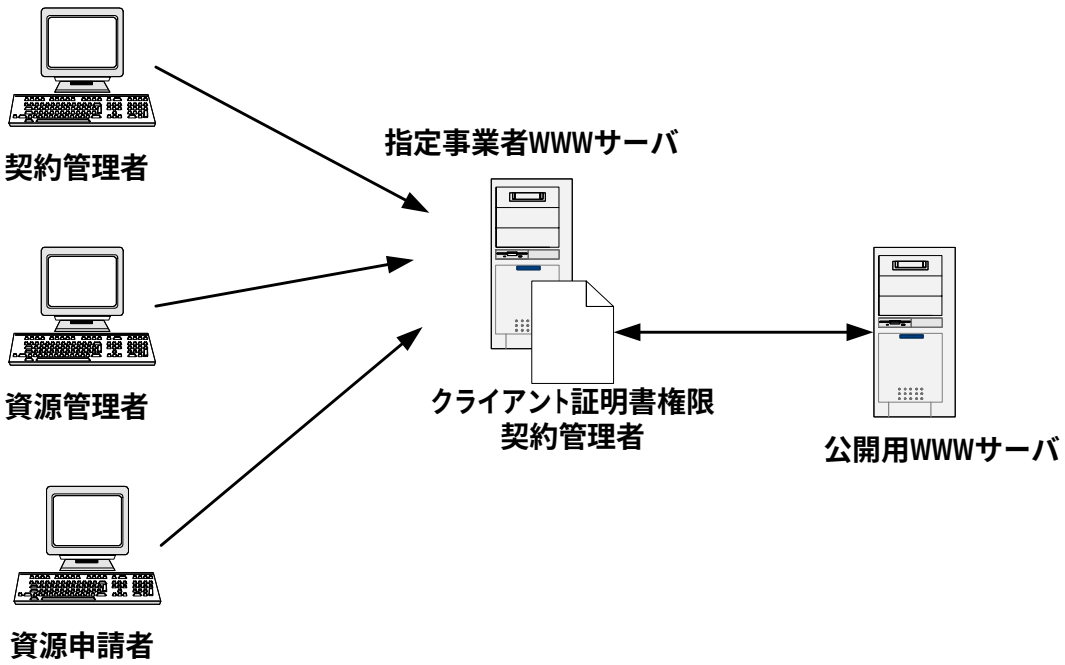


図 7-12　クライアント証明書の権限を共有した場合

よって、Web トランザクションで対応する申請業務を拡張する場合は、図 7-12 のように、申請業務を実施可能な権限毎に WWW サーバを分け、公開用 WWW サーバに申

請情報を POST するクライアントを分けることが考えられる。もしくは、クライアント証明書を、契約管理者用、資源管理者用、資源申請者用それぞれを WWW サーバに入れておき、申請内容によって、使用するクライアント証明書を分けることも考えられる。(図 7-13 参照)

ただしその場合でも、利用者から指定事業者 WWW サーバへの認証に、ユーザ ID とパスワードを使用する場合は、不正アクセスによる権限のなりすましが発生した場合、意図しないユーザからの申請が通ってしまうことが発生する。可能な限り、利用者と指定事業者 WWW サーバの間についても、クライアント証明書による認証を施すべきであると考える。

サーバ構成として単純にする場合は、使用するクライアント証明書毎に Web サーバを分離する方法も考えられる。(図 7-14 参照)

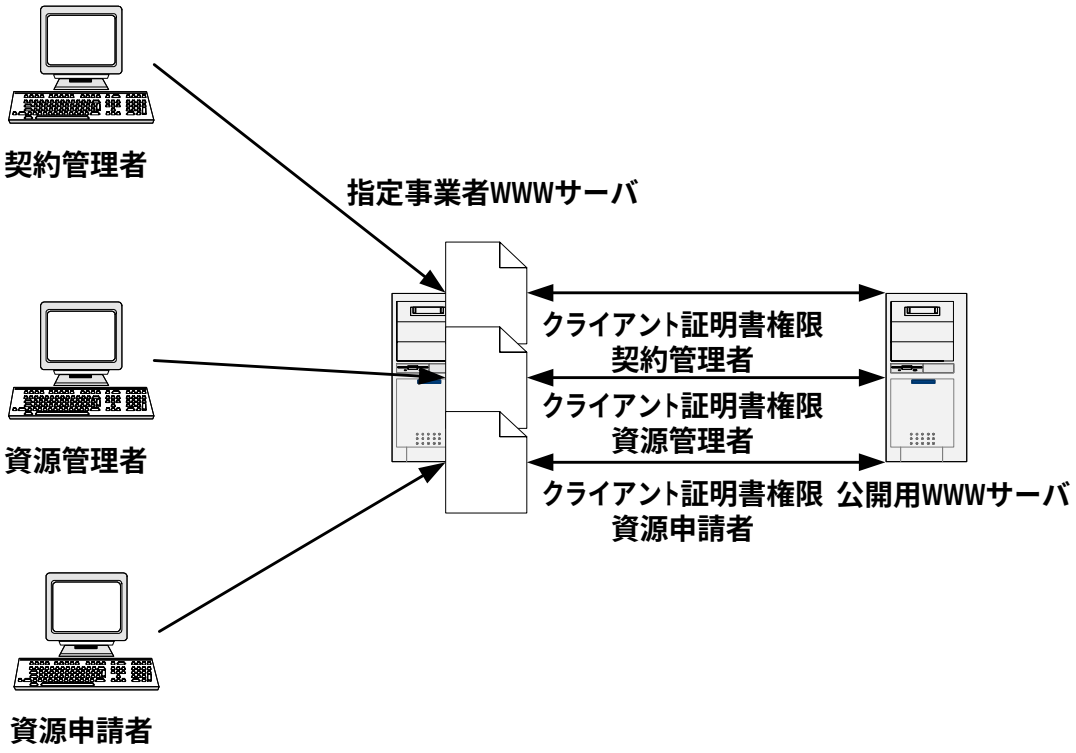


図 7-13　クライアント証明書の権限を分離する手段１

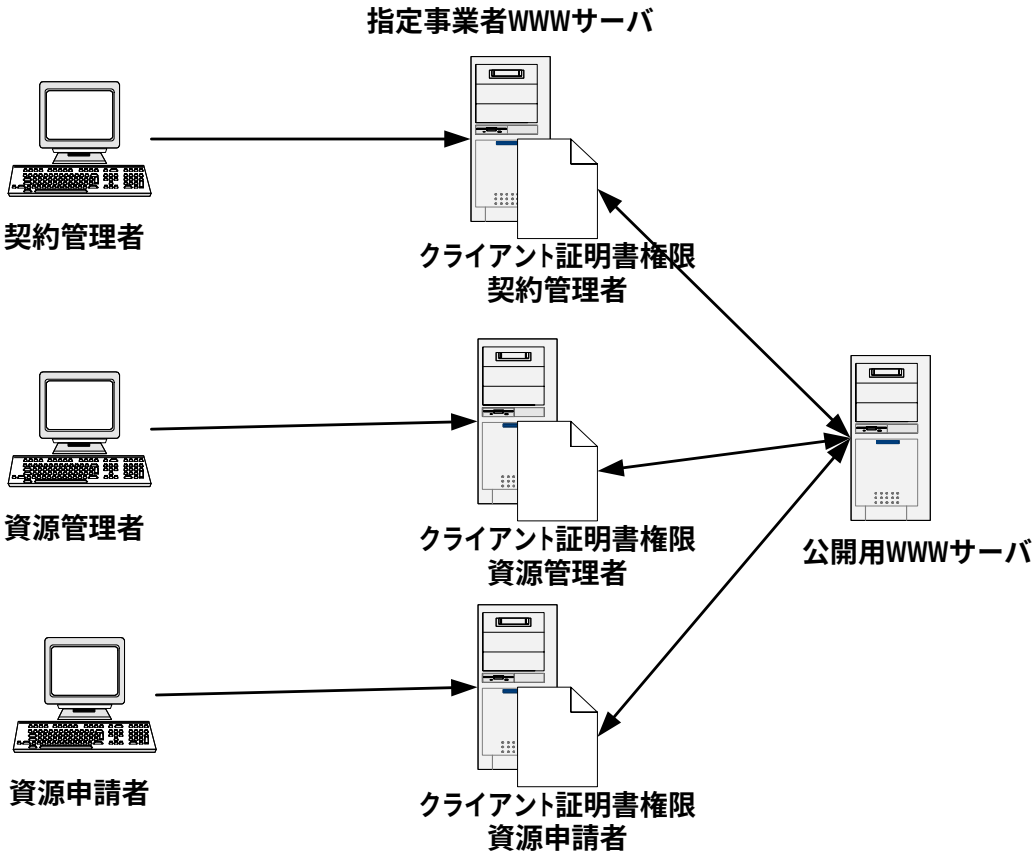


図 7-14　クライアント証明書の権限を分離する手段２

7.3. 商用 ENUM サービスの登録情報管理における適用事例

ENUM（tElephone NUmber Mapping）は、電話番号をインターネット上のアドレスやサービスと対応づけ、アクセスの手段として利用する仕組みである。日本でも 2003 年 9 月より、任意団体「ENUM トライアルジャパン」によって接続の実証実験が続けられている。

この ENUM について、2004 年 12 月にオーストリアが世界で最初の ”商用サービス” を生み出すことに成功した。ENUM はそのサービスの特性上、強固な本人認証がレジストリ・レジストラ業務の中で不可欠である。そのためオーストリアでは、認証局を通じて証明書を発行するモデルを実践している。ここでは、レジストリ(レジストラ)の行う登録管理業務の中で、実際にトークンを使用している事例として、このオーストリアの ENUM サービスの概略を紹介する。

7.3.1. ENUM とは

まず、ENUM の概略を述べる。

ENUM とは、電話番号を用いて、インターネット上のサービスで使われるアドレスを識別する仕組みである。まず、電話番号をドメイン名の形（e164.arpa）に変換し、それを DNS（Domain Name System）で、文字や数字そして特殊記号から成る通常のインターネットアドレス(メールアドレスや Web サイトの URL、SIP アドレス等)である相手の URI（Uniform Resource Identifiers）と対応づける。それによりその URI で指定されたアプリケーション、たとえば IP ネットワーク上の電話やメール、FAX などに接続することが可能となり、異なる通信サービスを 1 つの番号で利用することができる。

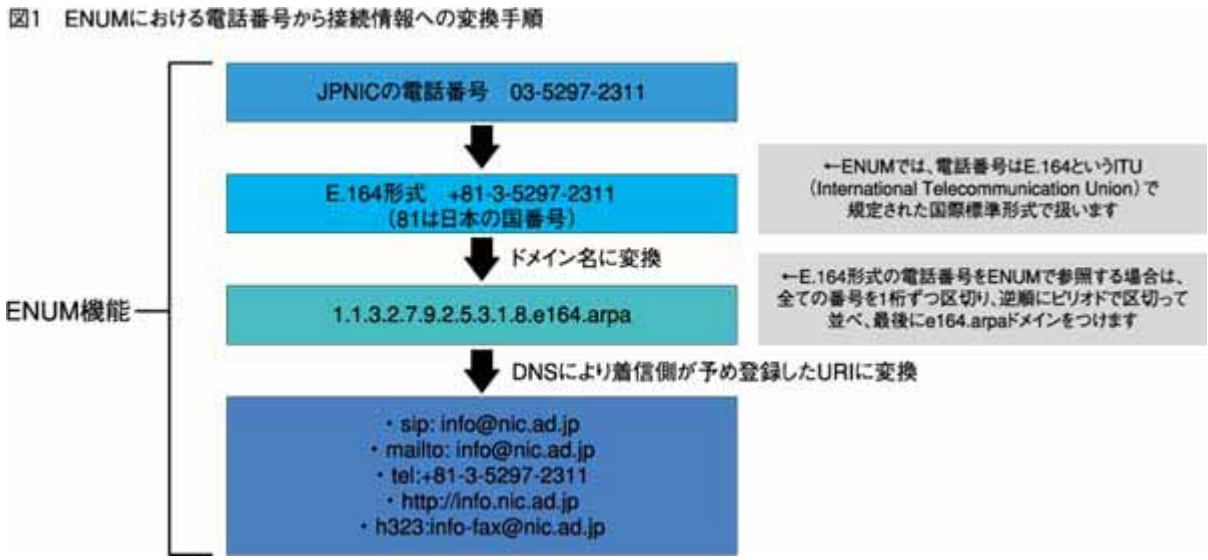


図 7-15　ENUM における電話番号から接続情報への変換手順

電話番号（E.164 番号）は、国際接続を考慮して、国際的な階層構造のもと管理されている。世界中でユニークであり、数字だけを用いていて各国の言語に依存していないという特性があるため、ENUM は世界に跨るグローバルなコミュニケーション構造の基礎としては大変高いポテンシャルを持っているといえる。

このような背景から、ENUM の実際に導入に向けて、国別でトライアルを進めるところが増えている。トライアル用のドメイン空間である「e164.arpa」は、IETF の IAB(Internet Architecture Board)からの委託を受け、RIPE NCC（Reseaux IP Europeens Network Coordination Centre）が管理運用を行っている。トライアルを行う際には、この Tier0 のレジストリである RIPE NCC に申請する必要がある。

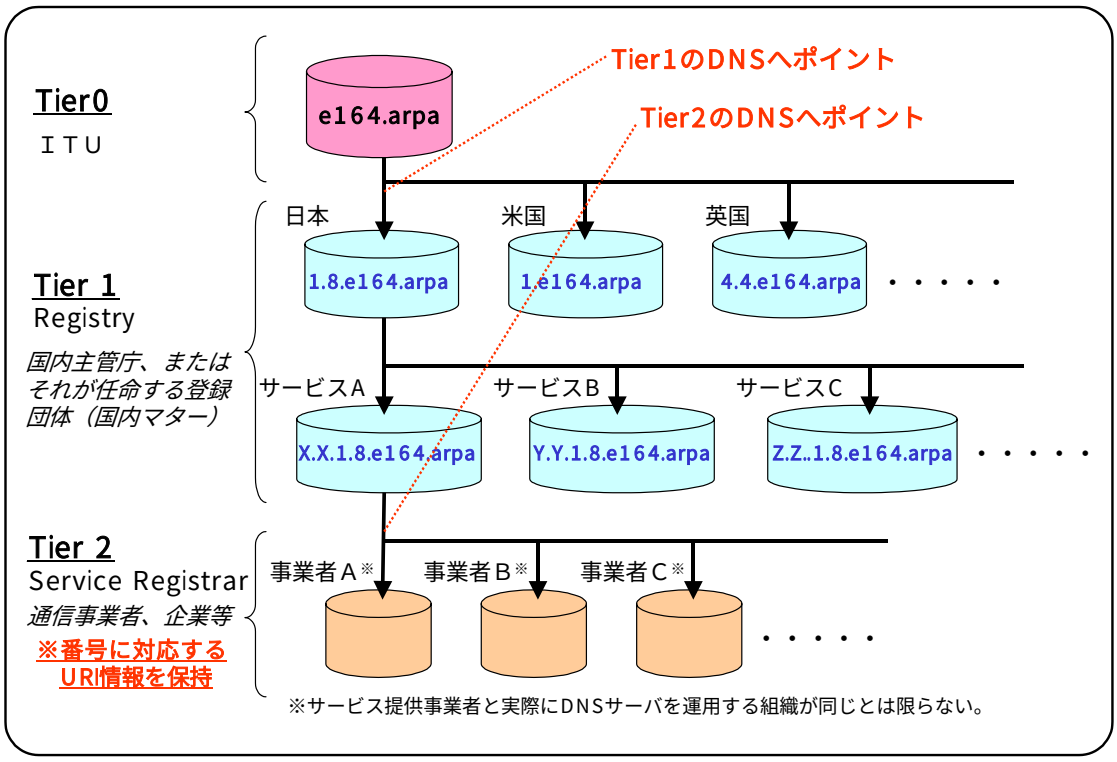


図 7-16　ENUM　DNS サーバの階層構造[1]

また、ENUM の導入に向けた技術の標準化に関しては、IETF（Internet Engineering Task Force）と ITU-T （International Telecommunication Union Telecommunication Standardization Sector ：国際電気通信連合の電気通信標準化部門）が共同で行っている。IETF は主に技術の標準化を行っており、ITU-T では管理基準の議論を行っている。

7.3.2. なぜ ENUM には強固な認証が必要か

ENUM は、存在する番号と適正な URI が結びついて初めてその機能を果たすものである。そのためには ENUM ドメイン名を登録申請した者が保持する電話番号が、本当にその人に属している(その人自身が使用している)という同一性を証明しなくてはならない。この定義ミスがあった場合、インターネットからの呼が ENUM を通じてルーティングされた際に適切でない人に接続されてしまう。そのため、ENUM ドメイン名の登録管理業務の中において、いかなる登録、変更、あるいは削除の作業の際に認証が不可欠となる。

1　総務省「IP ネットワーク技術に関する研究会 報告書」2002 年 2 月
http://www.soumu.go.jp/s-news/2002/020222_3.html
より抜粋

7.3.3. オーストリアでの商用 ENUM サービスの状況について

7.3.3.1. オーストリアでの ENUM 普及の背景と登録モデル

オーストリアは、1998 年の通信法改正により開放された通信市場をもち、欧州で最も競争力を備えた通信市場の一つとなっている。中・東欧市場を視野に入れてオーストリアをハブとして活動する企業が多いということ、また電気通信分野が完全に自由化されたことにより各種サービスが豊富になり、改善され、結果として料金が安くなったことが理由として挙げられる。こうした背景から、オーストリアでは携帯電話や DSL の普及率も非常に高く、これらの充実したインフラを利用しての利便性が高いアプリケーションが生まれる土壌が肥沃である。

ENUM については標準化団体の一つである ITU-T の本部に近いヨーロッパ地域でトライアルの準備が積極的に進められたという経緯もあり、RIPE NCC や ETSI(European Telecommunications Standards Institute：欧州通信規格協会)、CENTR (Council of European National Top Level Domain Registries)等の場を中心として ENUM の技術に関する議論や共同実験プロジェクトが盛んに行なわれたが、その中でアプリケーションに強いオーストリアは ENUM 先進国として ENUM に関するチュートリアルやトライアルを行い、また Asterisk[2]への ENUM 機能の実装もサポートにも積極的に取り組みに指導的な役割を果たしていた。RIPE　NCC からの受けるトライアル用ドメイン名空間のデリゲーション(3.4.e164.arpe)についても 2002 年 6 月と、世界で 4 番目という早さで取得している。

オーストリアで、この 3.4.e164.arpe についてのデリゲーションを受けて 3.4.e164.arpa ドメイン名ホルダーであり運用責任者となっているのは RTR 有限会社 (Rundfunk und Telekom Regulierungs-GmbH：放送テレコム規制有限会社) [3]である。nic.at(nic.at Internet Verwaltungs- und Betriebsgesellschaft m. b. H.：nic.at インターネット管理有限会社)[4] を始めとした関連組織を中心とした 2 年あまりのトライアル期間を経て、RTR は 2004 年 8 月 24 日に enum.at 有限会社[5]との間でレジストリ契約を

---

[2] Linux で動く、IP PBX ソフトウェアのこと

[3] 1997 年に設立のテレコム・コントロール有限会社(Telekom-Control GmbH)を統合して 2001 年 4 月 1 日に設立された通信産業の独立した規制機関。http://www.rtr.at/web.nsf 日本での規制当局。規制関連機関は、総務省と社団法人電波産業会である。

[4] オーストリアのトップレベルドメイン名".at"の登録管理業務を行う ccTLD レジストリ。

[5] 正式名称 enum.at 有限会社。http://www.enum.at/ 非営利財団 Internetprivatstiftung Austria (ipa：インターネット個人財団オーストリア)の 100%の子会社で、at、.co.at、.or.at

締結し、2007 年末まで Tier1 レジストリ業務を enum.at に委託、enum.at が 3.4.e164.arpa の ENUM ゾーンの管理を行う事となった。enum.at が行う事が可能である ENUM ドメイン名配布の範囲・条件などは RTR とのレジストリ契約で規定されている。enum.at は、ENUM ドメイン名の登録管理業務にかかる申請(登録・変更・削除)の手順等を決め、レジストラインターフェースを作成し、国の ENUM-TLD の下にゾーンのネームサーバを運用することが主な業務となる。この enum.at のもと、商用サービスの ENUM ドメインの登録は、2004 年 12 月 6 日から可能となり、トライアルからの転換は、2004 年 12 月 9 日の 12 時に実施された。

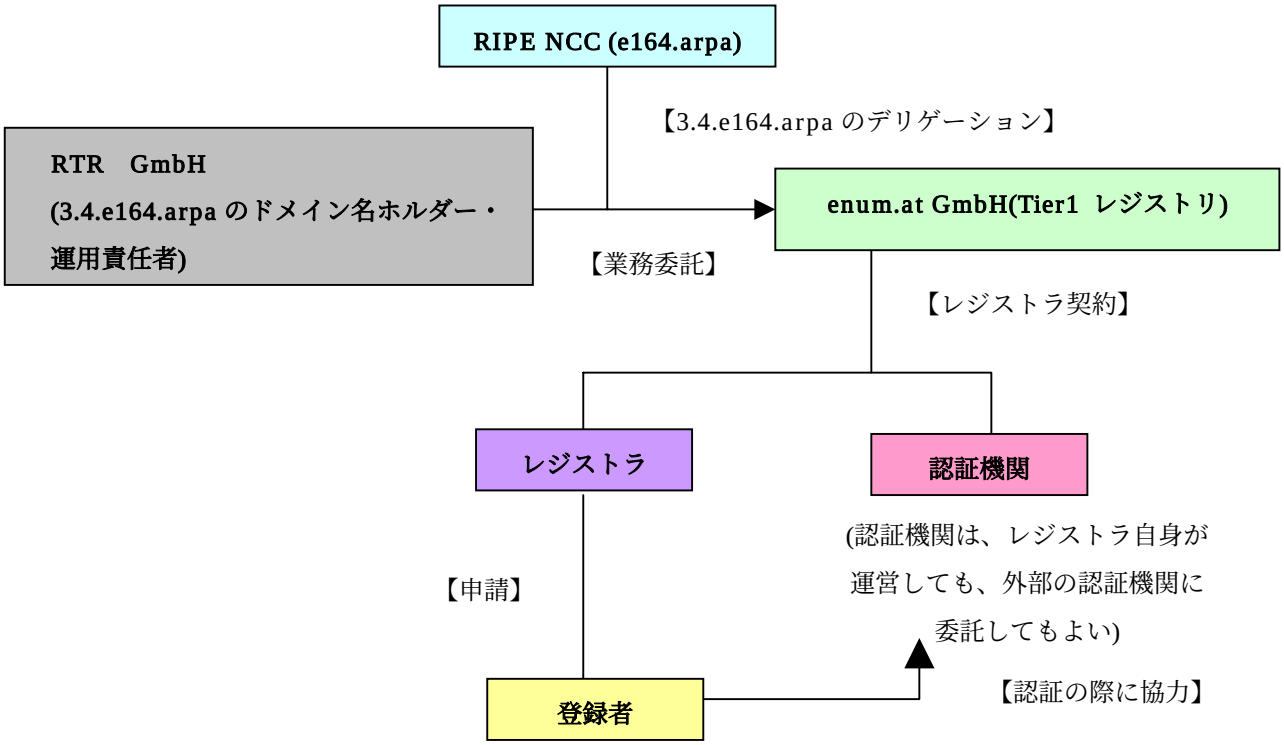


図 7-17　オーストリア ENUM の管理構造

等オーストリアのドメイン名の登録管理に責任を負うレジストリである nic.at の関連会社である。nic.at のマネージャでもある Robert Schischka が、enum.at の管理を引き継いでいる。

7.3.3.2. 各機関の役割と契約関係について

関連プレイヤーとの契約関係を、以下に図示し、整理する。[6]

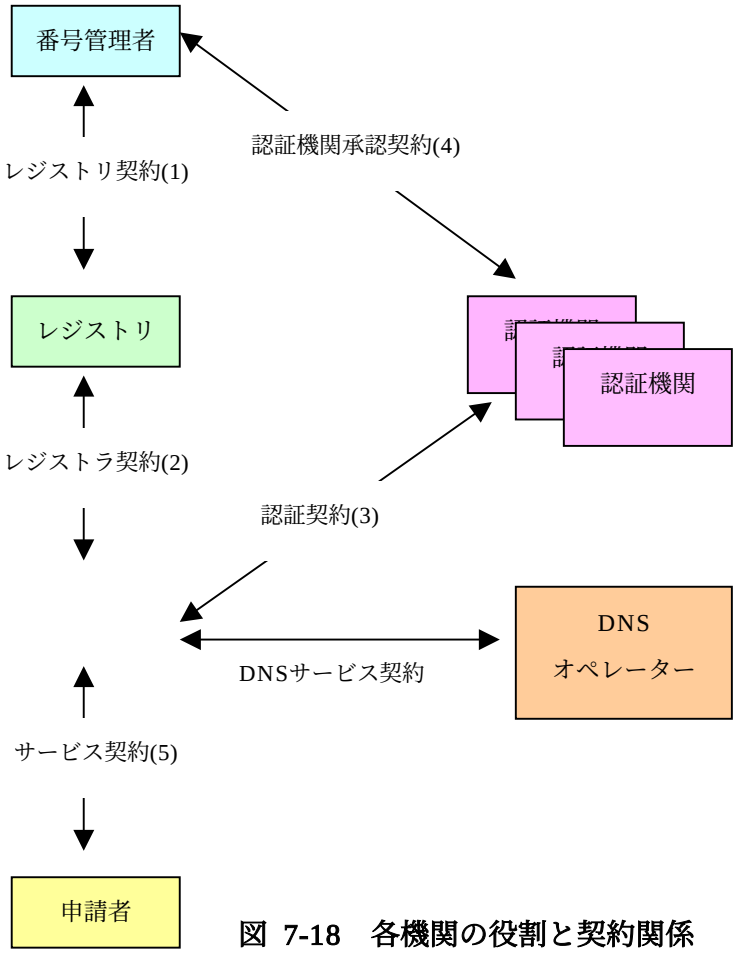


図 7-18　各機関の役割と契約関係

(1) レジストリはレジストリオペレーションについて番号管理者との契約を締結する。

(2) 各レジストラは、番号を割り当てることができるレジストリとレジストラ契約を締結する。

(3) 各レジストラは、レジストラのための認証トークンの作成にあたっては少なくとも最低一つの認証機関と認証契約を締結する。レジストラは、認証機関といかなる契約も存在しない場合においては、組織内の認証機関を利用することも

[6] 「ENUM Registry system specification」８ページより

できる。

(4) 各認証機関は、確認ポリシーについて番号管理者との契約を持つ、それに基づいて処理する。

(5) 各レジストラは、顧客(申請者)の代理で申請する事について申請者との間でサービス契約を締結している。

(6) 申請者に番号割り当てサービスをしようとする各レジストラは、番号範囲ホルダーとの契約を締結する。(オーストリア:+43 780番号)

以上がプレーヤー間の契約であるが、それにより以下の2点が明らかになる事を特記したい。

(7) レジストリには、申請者と締結するいかなる契約もない

(8) レジストリには認証機関と締結する契約はない(レジストリ⇔番号管理者⇔認証機関　のラインとなる)

但し、これに加え、例えば「+43 780」(後述するENUM専用番号)の登録の際にはこれ以外の他の契約関係も加わるかもしれないとされている。

また「レジストラ契約」を結ぼうとする ENUM 登録のレジストラ要件については、下記が課せられている。

(1) enum.atとレジストラ契約を締結する必要あり

(2) 申請者の委任を受けて登録等の申請を行う

(3) レジストラは、番号認証の責任を持つ。この場合、認証機関についてはレジストラ自身で運営しても、外部の認証機関に委託してもよい。が、

(4) 認証方法については enum.at の承認を得なければならず、また、enum.atに対する責任はいかなる場合もレジストラが持つ

また、enum.at と結ぶレジストラ契約では主として下記が規定されている。

(1) 営業規則を持っていること

(2) 従業員教育をすること

(3) EPP[7]登録とホスティングについての技術的基盤を有すること

(4) 銀行口座を有すること

(5) 申請者の意思がたえず優先されること

(6) 瑕疵のあるデリゲーションを行った場合、デリゲーションや番号空間利用の一時停止や禁止を行うことがある

2005 年 3 月現在、このレジストラ契約を締結しているレジストラはインスブリュックに本拠地を置く SI である nemox.net Steiner und Würtenberger OEG[8]、nic.at GmbH、ウイーンの ISP である Silver Server GmbH[9]の 3 社となっている。なお、nemox.net Steiner und Würtenberger OEG については、オーストリアで始めての ENUM レジストラであると同時に、認証局の役割も持っており、nic.at と認証契約を締結し認証業務を請け負っている。

また、認証機関については下記が要件とされている。[10]

(1) 認証情報は、鍵つきの証明書(Token)でやりとりすること

(2) 認証方法を開示すること

(3) 定められた番号空間の認証のみを行うこと

(4) 全てのレジストラにサービスを提供することも出来る

尚、申請者(ENUM 利用者)は、番号の適正使用のために、認証の際には認証機関に協力することとされている

---

[7] Extensible Provisioning Protocol の略で RFC3730 に規定されているレジストリデータの登録・更新のためのプロトコル。ドメイン名レジストリは複数のレジストラに対して、自組織データベースにアクセスさせなければならなく、また、単一のレジストラから複数のレジストリへのアクセス要求も出てきた中、 ドメイン名レジストリ・レジストラ間通信のためのプロトコルとして Network Solutions 社（現在は VeriSign 社に買収されている）によって開発された NSI RRP が存在したが、これでは登録者情報のやりとりはできなかったためそれに替わるものとして EPP が開発された。

[8] nemox.net Steiner und Würtenberger OEG　http://nemox.net/index.html

[9] Silver Server GmbH　http://www.sil.at/

[10] 詳細については、enum.at が発行している認証についての考え方ガイドライン「Identifizierung und Validierung für ENUM IN ÖSTERREICH」がある
http://enum.nic.at/documents/AETP/Permanent_Documents/Drafts/0032-ENUM_Validierung_v_1.0.doc

7.3.4. ENUM に登録出来る番号空間について

ENUM に登録出来る番号空間は下記のとおりであり、それ以外の番号空間の登録は基本的に不可となっている。

(1) 地域別番号

(2) プライベート網用番号(05)

(3) モバイル用番号(06)

(4) 地域に左右されない固定網(0720)

(5) ENUM用番号(0780)

(6) フリーダイアル用番号(0800)

(5)の ENUM 用の番号空間である「0780」は、RTR が ENUM を利用したコンバージェントサービスのために導入した空間であり、この空間下では申請者はその番号が誰にも割り当てられていない場合には好きな番号を選ぶことができる。つまり、ENUM 用の番号である 0780 以外の空間では、その電話番号の存在が適切に認証されて初めて ENUM ドメインが割り当てられるが、0780 に関しては、番号と ENUM ドメイン名を同時に割り当てるという形式をとる。0780 の登録は、通常のドメイン名の登録手順・方法に非常に似ている。但し、デリゲーションには期限が存在する。

7.3.4.1. 課金体系

レジストラへの課金は、その時点でデリゲーションされているドメイン名の数をベースに月ごとに計算する事となる。500 ドメイン名までは、250 ユーロ/月が最低課金料金[11]で、それ以上は、数に応じた表の単価を、数にかけた料金(ドメイン数×単価)としている。

[11] 但し、契約して最初の半年は、最低課金料金(250 ユーロ)の 50%引きを実施

ドメイン数	1 ドメイン辺りの値段(ユーロ/1 ヶ月辺り)
0 -　 500	0,5　ユーロ
501 -　2500	0,45 ユーロ
2501 - 10000	0,4　ユーロ
10001 - 50000	0,35 ユーロ
＞50000	0,25 ユーロ

表 7-16 レジストラへの課金

例:　392 ドメインの場合　→　500 ×　0,5 ユーロ = 250 ユーロ(1 ヶ月辺り)
4612 ドメインの場合　→　500 × 0,5 ユーロ + 2000 x 0,45 ユーロ + 2112 ×　　0,4 ユーロ = 1994,8 ユーロ(1 ヶ月辺り)　となる。

7.3.5. ENUM レジストリシステムの要求事項について

enum.at が、2005 年 1 月 3 日に Ver1.1 を発行した「ENUM Registry system specification」を元に、このレジストリシステムの要求事項と登録手順を述べる。

7.3.5.1. 登録手順について

どの番号空間の利用するかによって、登録手順は多少異なってくるが、ここでは、代表的な例として、地理的識別要素をもった電話番号についての登録手順についての概要を述べる。[12]

[12] 「ENUM Registry system specification」13 ページ～16 ページより
なお、ENUM 専用番号 0780 については 9～12 ページに、SMS を利用した携帯用の番号については 16～17 ページに記載されている。

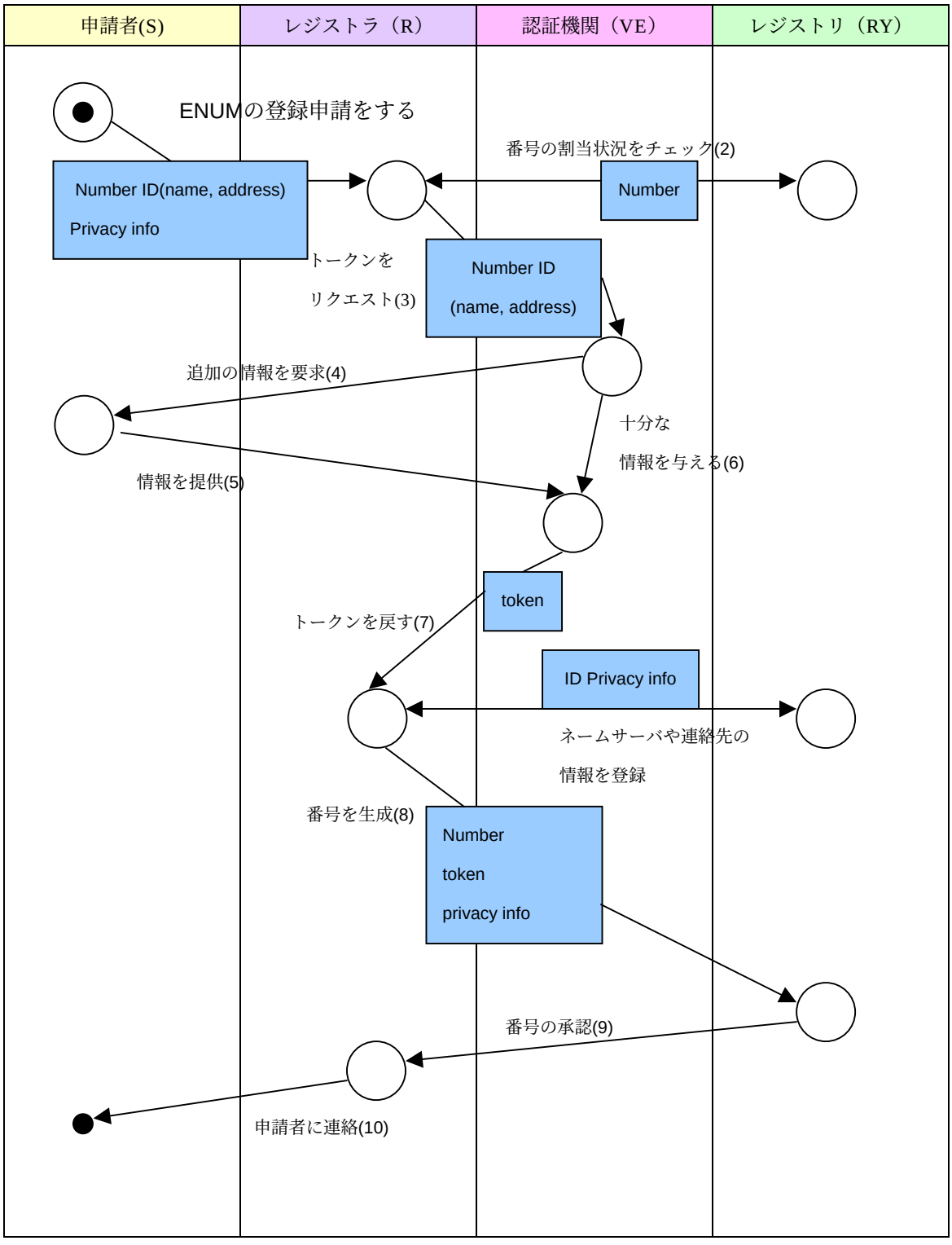


図 7-19　地理的識別要素をもった電話番号についての登録手順

(1)現存する地理的識別性を持った番号のためのENUM 申請者(S)は、レジストラ（R）にサービスを申請する。申請者は申請者認証に必要な情報を提供する

S -> R: Name: Joe User

S -> R: Address: Karlsplatz 1/9, A-1010 Wien

S -> R: Number: +43 1 234234

S -> R: email: joe.user@nic.at

S -> R: validation information (請求書のコピー, IDのコピー等)

(2)レジストラ（R）はレジストリ（RY）と共にその番号がENUMですでに割り当てられていないかどうかをチェックする(万一そのようなことがあれば、CREATENUMBER(番号作成申請)でなくTRANSFERNUMBER(番号移転申請)をしてもらうよう申請者と交渉する必要があるため)。このチェックは、問題の番号がそもそも有効かどうか、ログイン画面の将来のバージョンでは確認する事ができるようになる予定である。

R -> RY: +43 1 234234 available?

RY -> R: +43 1 234234 NOTFOUND – no number resource found

(3)レジストラ（R）は認証機関(VE)を選びその認証機関が必要とする情報を手渡す。この情報にはその認証機関の認証ポリシーに従った文書も含まれる事とする。

R -> VE: number: +43 1 234234

R -> VE: numberholder: Joe User, Karsplatz 1/9, A-1010 Wien

R -> VE: email: joe.user@nic.at

(4)認証機関(VE)は、申請者(S)に追加情報を要求したり、あるいは確認することが可能である。例えば申請とされる電話番号についての最も最近の請求書のコピーを V 申請者に送って欲しいと頼むというようなことである。

VE -> S: email: please fax invoice for +43 1 234234

(1) 申請者(S)は認証機関(VE)からの要求事項に応える。

S -> VE: receives email, faxes invoice

(2) 上記の 4.や 5.の手続きの際、レジストラ（R）が認証機関（VE）に対して認証に必要とされる十分な情報を提供した場合においては、認証機関が

申請者（S）に直接コンタクトすることなくして認証が終了する事もある。(例えばレジストラが電話番号の最新の請求書のコピーを認証機関に提供した場合など)。

(3) 上記の通り認証が成功したら、認証機関がサインした Token をレジストラに返す。

VE -> R: valid, signed token, containing:
VE -> R: number: +43 1 234234
VE -> R: firstname: Joe
VE -> R: lastname: User
VE -> R: creation date: 2004-06-21
VE -> R: expiration data: 2004-12-21

(4) レジストラは、申請者が例えば電話帳ディレクトリのために提供するようなデータのサブセットを含んだ新しいコンタクト・オブジェクトの作成をレジストリに依頼しレジストリはをれを作成する。[13]

R -> RY: CREATECONTACT
R -> RY: type=person
R -> RY: firstname: Joe
R -> RY: lastname: User
R -> RY: email: joe.user@nic.at
RY -> R: contact successfully created, new roid „JU1234“

(5) レジストラは、たった今作成された番号保持者のコンタクトオブジェクトを参照して、番号を割り当てる。コマンドには認証機関から受け取った認証トークンが含まれる。

R -> RY: CREATENUMBER
R -> RY: number: +43 1 234234
R -> RY: numberholder: JU1234
R -> RY: nameserverset: NSSET1234
R -> RY: token: ...
RY -> R: create number OK

(6) レジストラは、申請者に ENUM ドメインの登録が終了した事を伝える。

[13] nameserverset（必要なら)の作成はここでは示されていないが、コンタクトを作成した際の前後になると考えられている。

申請者は、構成データ等を受け取ることもある。

R -> S: Ok, ENUM domain created, here's your account information

R -> S: And now, hand us over your money.

7.3.5.2. レジストリシステムインターフェース

レジストリとの連携のためには、次の図のように、インターフェースが提供されている。[14]

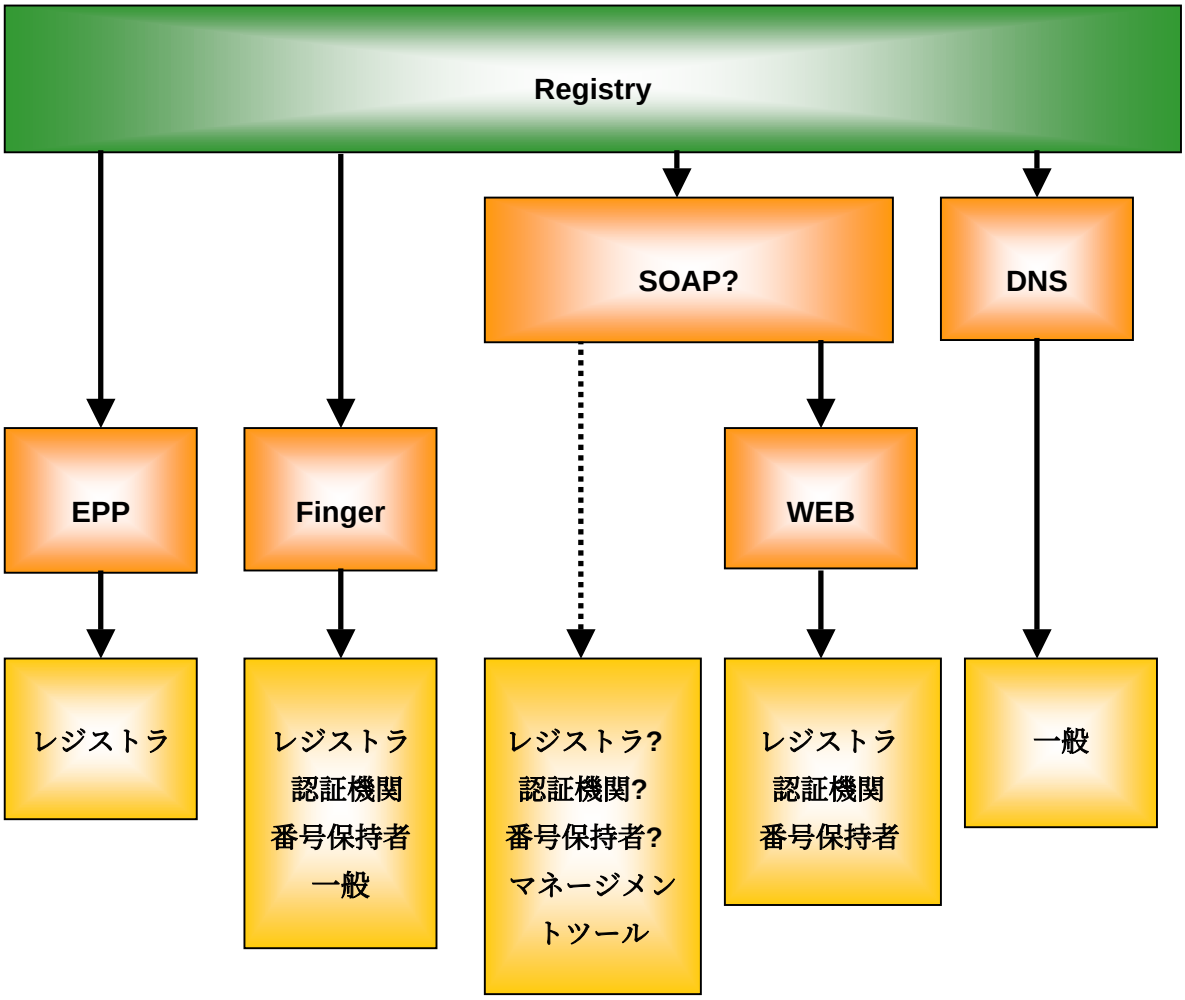


図 7-20　レジストリシステムインターフェース

[14] 図 7-20 の中の DNS のインターフェースは、パブリック ENUM ツリーが管理される場合にのみ適用される。プライベート/キャリア ENUM アプリケーションで、DNS へのアクセスは、あるクライアントに制限されたり、もしくはいかなる DNS も、そもそも使われない可能性もある。

7.3.5.3. サーバポリシー15

ここでは、あるトランザクションが成功したのかそうでないのかを定義するレジストリサーバに適用するルールである、ENUM管理サーバのポリシーについて述べる。但し、ポリシーは、ある処理で運ばれるデータやレジストリ・データベースの状況に依存しているため、時とともに変わる可能性があるものである。

（1） 権限の定義

トランザクションは、サーバによって許される場合と許されない場合があるが、一つのトランザクションを有効に進めるには、真正性を証明されたクライアントによって、以下にあげる許可がされる必要がある。また許可に加えて、処理にはすべてのポリシーがクリアされている事が必要とされる。

(1) クライアントに対して許されるトランザクションのタイプ　：
クライアント(レジストラ)は、問題の処理を許されなくてはいけない。それは、クライアントトランザクションタイプを制限するのに有用である(例えば不払いの場合の新しい番号は付与しない)
(2) クライアントに対して許される番号の種類　：
クライアントは、ある種類の番号だけに制限されることがある。例えば、モバイル・オペレーターは、モバイル番号だけの割り当てを許される。これは非番号トランザクションには適用されない。
(3) 認証機関に対して許される番号の種類　：
認証機関は、自分達が取り扱っている種類の番号のみを扱う事ができる。その種の彼(それ)らが出す番号で制限することができる。モバイル・オペレーターは、例えばモバイル番号だけの認証を許される。
(4) トークン証明書に対して許されるトランザクションタイプ　：
トークンにサインするために使われた証明書は、トークンをサポートするトランザクションのサブセットに制限されていることができる。
(CREATENUMBER、RENEWNUMBER、TRANSFERNUMBER)

（2） ポリシーの依存関係

ポリシーは、以下のものに依存するとされ、ポリシーを通した、ある処理の流れは、

15 「ENUM Registry system specification」63 ページ～64 ページより

次の図の通りとなる。

(1) 番号(番号型エンジン経由で番号から抽出された)の種類

(2) レジストラID

(3) 認証機関

(4) 処理型

(5) オブジェクト(フラグ)の状態

(6) リンクされたり関係付けられたオブジェクトの状態(およびそれらのフラグ)

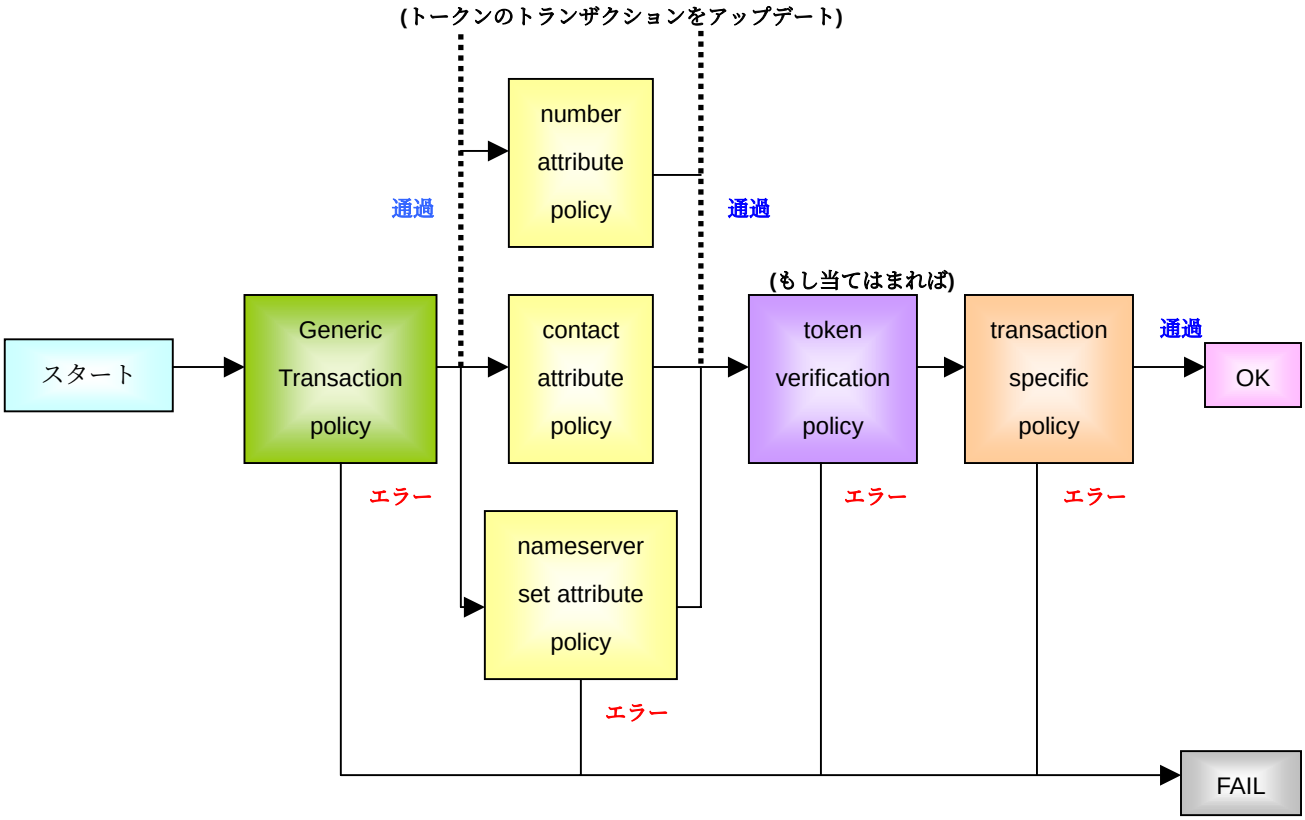


図 7-21　ポリシーの関係

7.3.5.4. 認証[16]

認証のプロセスは、ENUM 登録インフラの基礎的な概念だ。ある番号の認証をするということは、ENUM ドメインの保持者がその番号保持者と完全に一致することを明らかにするということである。これは ENUM 経由の通信が、PSTN(Public Switched Telephone Networks：公衆交換電話網)経由でルーティングされた通信と同じエンティティに届くということを確実にする必要があるということでもある。

何度も述べているが、認証の手順に関しては、特別の役割である「認証機関」のみが実行することができるものである。認証機関はレジストラに対して、あるトランザクションは番号保持者によってオーソライズされたので進める事ができると主張することができる。

ENUM で使われる認証の種類には、まず「最初の認証」と「再認証」の二つがあるが、ここでは「最初の認証」のやり方と考え方について述べる。

「最初の認証」では、一つの番号があるレジストラと認証機関の組み合わせによって割り当てられるということが要求される。または、以前に有効とされた番号が、再割り当てられることも要求される。従って、最初の認証では、以下 3 つのプロセスが必要となる。

(1) 「デリゲーションにあたり番号保持者の同意を確かめる」
これには二つの方法がある。

(a)本人確認→使用権の確認→その後権限付与・・・利便性とセキュリティの間のトレードオフに応じて、これらの3つの要素(三ステップ)がENUM申請手続きの際に組み込まれることが必要となる。

I：Authentication(本人確認) :
このステップは、カスタマーの同一性を確立する。ENUMユーザとなる人の住所と名前を確認する。これには、例えばIDカードやクレジットカードあるいは他の暗号のトークン等を使って行われる。
Ⅱ：Right-to-Use(使用権の確認)　:
第2のステップとして、その番号とその人に関係があることを確認する。

16 「ENUM Registry system specification」67 ページ～72 ページより

これは例えば電話帳を検索したり、請求書のコピーなどを使って行われる。
Ⅲ：Authorization(権限付与)　：
最終のステップは、このレジストラから付与されるENUMドメイン名を、本当に申請者が欲しているかを確かめる事だ。

(b)番号ホルダーによる直接承認・・・時には、番号ホルダーを識別することのプロセスを飛ばすことは、可能である。例えば、SMSハンドシェイクが認証リクエストを承認した場合には、認証機関はその携帯電話の所有者の同一性を確認することを必要としない。

(2) トークンを生成

上記(1)のプロセスが終了したらトークンが生成される。トークンには、選ばれた認証方法に応じて要求されたデータは少なくとも含まれなくてはいけない。トークンにいれられたデータは、番号保持者について追加で調べられたデータなしでも再認証を許される。

(3) トークンにサイン

トークンは、認証機関がレジストリに渡し、そしてそれは、対象のトランザクションおよび種類の番号の参加資格を得る証明書でサインされる必要がある。

7.3.5.5. 証明書管理について

いままでで記述された認証の仕組みの中では、証明書管理プロセスも要求している。証明書管理は、認証トークン(認証機関)の署名者と署名(レジストリ)を確かめる組織の間で必要となるものである。

レジストリは、それぞれの認証機関の証明書リストを管理する。認証機関は「アウトオブバンド」プロセス経由でこのリストに証明書を追加したり削除したりする可能性がある。レジストリは、例えばパブリックCA、プライベートCA、自己サイン証明書等々どんな形式であろうと認証機関が発行した証明書が有効でサインされたX.509証明書だ

という条件で受け取ることとなっている。

ある認証機関の現在有効な証明書のリストは、認証トークンの検証のために有効と見なされる。検証に利用される証明書は、検証プロセスの際には有効でなくてはいけないとされる。

また、認証機関は、特定のトランザクションにおいてトークンの正当性を制限するかもしれないとされている。制限はトークンがサインされた証明書に基づき、ある証明書の制限は、証明書がレジストリによってインストールされるときに、伝えられる必要がある。認証機関は、証明書をCREATENUMER・RENEWNUMBER・TRANSFERNUMBERの1つ以上の処理に制限することもある。

ある証明書の制限というものは変えることができない。認証機関は、追加の証明書を多かれ少なかれトークンが望まれるときに提供する必要がある。制限の目的において、例えばちょうど + 43780番号の作成のため等に、ライトウエイトな認証機関を運営する事ができる。また一つの認証機関は、この数種の番号のためのトークンだけを作る事ができると、制限される事がある。

7.3.5.6. 汎用的なトークン検証プロセス

レジストリによって受け取られたいくらかのトークンは、以下のトークン検証プロセスをパスしなくてはいけない。汎用的なトークンへの検証への追加の要求は、トークンを含む処理・リクエストに依存することを適用するかもしれない。処理詳細ポリシーは、これでより多くの詳細を含む。汎用的トークン検証をパスするために、トークンは、以下の要求を果たさなくてはいけない。

(1) トークンは、書式が正しくなくてはいけない。(分解して解釈できること「paseable」)

(2) トークンのシグネチャは、含まれた証明書に対して有効にしなくてはいけない。

(3) 含まれた証明書は、レジストリのアクティブな証明書のデータベースの中で見つけられなくてはいけない。

(4) 証明書の使い方の制約がトークンを含む処理を許さなくてはいけない

(5) レジストリ・データベースで見つけられた証明書に連合させられた認証機関ID(VE-ID)は、トークンの認証機関ID(VE-ID)の属性につり合わなくてはいけない。

(6) トークンに含まれる番号は、レジストリに知られている番号の一種に地図にマップされなくてはいけない。

(7) 証明書に関連付けられた認証機関ID(VE-ID)は、番号種類のトークンを作り出すことが許される。

(8) トークンの有効期限のタイムスタンプは、それが処理されている時以降でなければならない。

(9) トークンの作られたタイムスタンプは、有効期限のあとであってはならない。

(10) トークンの認証機関ID(VE-ID)との認証シリアルは、レジストリ・データベースでユユニークでなくてはいけない。

7.3.6. まとめ

これまでに述べたとおり、オーストリアではじまったこの商用 ENUM サービスの登録情報管理では、(1)レジストリと独立した認証局を運営していること、(2)「レジストリ‐レジストラ‐認証機関‐申請者」で業務のフローを定義していること、(3)認証局と独立したレジストリが、認証のためにトークンを利用している事などが特徴として挙げられる。

(1)のレジストリと独立した認証局の運営により、レジストリにおける認証業務のコストを下げることだけでなく、既存の認証局の参入を可能にするモデルであると考えられる。(2)では単に認証局を利用した認証を実現するだけでなく登録のスキームを定義し、その中で認証機関が果たす役割を定義している。(1)と(2)を可能にする為に仕組みが(3)のトークンであろう。トークンは電子証明書ではなく、署名つきの認証子の意味で、電子証明書を使った相手の認証だけでなく、登録できる番号の種類といった付随する情報を持っている。

この応用は EPP とトークンの技術によってレジストリにおける認証の実現した事例である。レジストリ・レジストラ間およびレジストリ間の連携のプロトコルが開発され普及するに従って、この事例のような応用例が今後も現れてくる状況になると考えられる。インターネットレジストリの場合には whois に置き換わる CRISP の開発により認証スキームを新たに定義し、実現していく必要性が現れると考えられる。

7.4. 認証局の応用と IP アドレス認証局の役割

IP アドレス認証局は、JPNIC ルート認証局のサブ CA として、IP アドレス認証局（認証）と IP アドレス認証局（証明）の二つの種類を持つとして構築を行った。前者の IP アドレス認証局（認証）はメンテナー認証局とも呼ばれ、アドレス資源管理に関わる情報登録を行う者の認証を行うことを目的とした認証局である。後者の IP アドレス認証局（証明）は相互領域認証局とも呼ばれ、登録情報の内容に基づいた証明書の発行により証明書の利用者が相互認証を行えるような状況を目標とする認証局である。

様々なネットワークサービスやインフラとしてのインターネットを支える要素として電子認証を考えると、IP アドレス認証局（証明）は応用性が広いと考えられる。本章で述べる経路情報の安全性の向上に当たっては、IP アドレス認証局（証明）が利用されることが想定できる。一方、ネットワークサービスのアドレス資源管理の多様化に伴って安全性や効率性の向上を図る要素として電子認証を考えると、IP アドレス認証局（認証）が利用されることが想定できる。本章で紹介する Web トランザクションや ENUM の事例はこれに分類されるであろう。

このように IP アドレス認証局は、それぞれの認証業務にあわせて細分化され、役割を持っていくことが考えられる。特に IP アドレス認証局（証明）は、更に下位認証局を持つ等して、様々な電子認証のテストベッドとして活用され、本章で述べた以外の応用についても検討されていくことが考えられる。

Appendix 1

IP アドレス認証局（認証）

認証業務規定（CPS）

更新版

<添付資料１について >

- この資料は、IP アドレス認証局の認証業務規定（CP/CPS）のドラフト版である。本 CP/CPS 策定の為の検討については本報告書第 6 章で述べる。
  - 本 CP/CPS は RFC3647 のフレームワークに則って記述
  - URL などを含め、公開が行われる前に一部改定されることを想定

目次

1. はじめに

1.1. 概要

本 JPNIC 資源管理認証局 認証業務規定（以下、CPS という）は、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（以下、JPNIC という）と IP アドレス管理指定事業者等との間における、IP アドレス及び AS 番号に関する各種管理業務に用いる証明書を発行する JPNIC 資源管理認証局（以下、本認証局という）の認証業務に関する運用規則を定める。

本認証局は、本 CPS に基づき、IP アドレス管理指定事業者に所属し、各種申請処理業務を行う者（以下、ホストマスタという）等に証明書を発行する等の認証サービスを提供する。また、安全な通信を実現するため、JPNIC の各種サーバに対してサーバ証明書を発行する。

本 CPS の構成は、IETF PKIX WG において標準化されている RFC3647「証明書ポリシと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework）」に準拠している。

本認証局は、CP（証明書ポリシ）及び CPS（認証実施規程）をそれぞれ独立したものとして定めず、本 CPS として証明書ポリシ及び運用規程を定めるものとする。

JPNIC は、認証業務の提供にあたり、自らのポリシ、証明書所有者及び証明書検証者の義務等を、本 CPS、証明書所有者同意書によって包括的に定める。なお、本 CPS と証明書所有者同意書の内容に齟齬がある場合は、証明書所有者同意書が優先して適用されるものとする。

本 CPS は、証明書所有者及び証明書検証者がいつでも閲覧できるように JPNIC のホームページ上（URI は決定後に記述される）に公開する。

(1)CPS

CPS は、証明書の目的、適用範囲、証明書プロファイル、本人認証方法及び証明書所有者の鍵管理並びに認証業務に関わる一般的な規定を記述した文書である。本 CPS は、必要に応じて証明書所有者同意書を参照する。

(2)証明書所有者同意書

証明書所有者同意書は、認証サービスの内容や証明書所有者の義務等、証明書所有者と JPNIC 間における、認証サービス利用上の諸規則を記述した文書である。

1.2. 文書の名前と識別

本 CPS の正式名称は「JPNIC 資源管理認証局 認証業務規程」という。

JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。

表 1-1 JPNIC 及び JPNIC 資源管理認証局に関連するオブジェクト識別子

オブジェクト	オブジェクト識別子
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	1.2.392.200175
JPNIC 資源管理認証局 認証業務規程（CPS）	1.2.392.200175.1.2.1 （OID の詳細は決定後に記述される）
EE 証明書ポリシ	1.2.392.200175.1.2.1 （OID の詳細は決定後に記述される）

1.3. PKI の関係者

1.3.1. 認証局、登録局、所有者及び検証者

本認証局が発行する証明書の流通するコミュニティの PKI 関係者には、表 1-2 に示す登場者が含まれる。

表 1-2 コミュニティに関係する登場者と役割

登場者	略称	役割、説明
ホストマスタ		IP アドレス及び AS 番号の割当て・返却等のレジストリ業務を行う者
サーバ		レジストリ業務に用いる JPNIC 内のサーバのうち、証明書が発行されるもの
ホストマスタ証明書		ホストマスタに対して発行される証明書
サーバ証明書		JPNIC の各種サーバに対して発行される証明書
メンバ管理者証明書		本認証局の認証業務に必要な運用用証明書の一つ。ホストマスタへの証明書発行時のメンバ管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。
エンドエンティティ	EE	証明書の発行対象である、ホストマスタ、メンバ管理者及び各種サーバの総称
エンドエンティティ証明書	EE 証明書	EE に発行される証明書の総称
証明書申請者	申請者	証明書を申請中の者
証明書所有者	所有者	証明書発行申請を行い、自ら鍵を生成し、認証局により証明書を発行される主体をあらわす。本 CPS では、EE 証明書を所有している者又はサーバの管理者となる。
証明書検証者	検証者	証明書を受け取る者で、その証明書を用いて検証することにより、その証明書及び/又はディジタル署名に依拠して行動する者
JPNIC 発行局	JPNIC IA	JPNIC ルート認証局内の発行局及び JPNIC 資源管理認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 資源管理認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。 認証局（CA）の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。

登場者	略称	役割、説明
JPNIC 登録局	JPNIC RA	証明書発行の証明書申請者の本人を確認し、主として登録業務・失効業務をつかさどる組織。証明書の所有者の本人確認と認証に責任を持っている。
運営委員会		JPNIC の理事により構成される会議であり、JPNIC 認証局の運営方針の決定等を行う。運営委員会は、JPNIC の定款・規程に従って運営される。
認証局管理者	CAO	認証局サーバ、ディレクトリサーバ等認証局システムの運用管理をする者。
登録局管理者	RAO	登録局（RA）を管理し運営する者。証明書発行、失効の登録作業を行う。
リポジトリ		認証局が署名した証明書及び CRL 等を格納し公表するデータベース。
JPNIC ルート認証局		JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局（資源管理認証局）の証明書に電子署名を行う。
JPNIC 資源管理認証局		JPNIC が運営を行う IP アドレスの管理業務に関連する証明書の発行を行う認証局。JPNIC 資源管理認証局証明書は、JPNIC ルート認証局により電子署名される。
JPNIC 認証局		JPNIC が運営を行う認証局の総称。JPNIC ルート認証局、JPNIC 資源管理認証局、JPNIC 登録局及びリポジトリから構成される。
LRA		証明書を発行する組織とは異なる組織若しくは団体であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が LRA となる。
LRA 責任者		IP アドレス管理指定事業者の中における、LRA 業務の責任者。メンバ管理者の任命・解任を行う。
メンバ管理者	メンバ管理者	IP アドレス管理指定事業者の中で、ホストマスタのメンバ管理と認証及びホストマスタ証明書の発行申請操作を行う。

1.3.2. その他の関係者

規定しない。

1.4. 証明書の使用方法

1.4.1. 適切な証明書の使用

本 CPS に基づき発行される証明書は、JPNIC の行う IP アドレス管理業務における各種の申請及び連絡等を目的として、レジストリシステムがユーザ及びメッセージを検証する為に使われるものとする。

1.4.2. 禁止される証明書の使用

本 CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものである。また JPNIC は、IP アドレス管理指定事業者のホストマスタ相互間での証明書の使用を制限するものではないが、本使用に対してなんら責任を負うものではない。

1.4.3. 証明書の相互運用性

JPNIC 認証局は、他の認証局と相互認証を行うことがあるものとする。

1.5. ポリシ管理

1.5.1. 文書を管理する組織及び連絡担当者

本 CPS を管理する組織及び問い合わせ先を次に定める。

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

受付時間：月～金 （年末年始／祝祭日は除く） 10:00～18:00

電子メールアドレス：（電子メールアドレスは決定後に記述される）

1.5.2. CPS のポリシ適合性を決定する者

本 CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会という）が行う。

1.5.3. CPS 承認手続

本 CPS の改定は、運営委員会により承認を受けた後に公表されるものとする。

1.6. 定義と略語

本 CPS にて使用される用語は、表 1-3 に示すとおりである。

表 1-3 用語

用語	略称	説明
電子証明書	証明書	ある公開鍵を、記載されたものが保有することを証明する電子的文書。認証局が電子署名を施すことで、その正当性が保証される。本 CPS では、特に断らない限りホストマスタ証明書、サーバ証明書及び運用用証明書を総称して「証明書」と呼ぶ。
認証局	CA	証明書の発行・更新・失効、認証局等私有鍵の生成・保護及び証明書申請者の登録を行う機関。本 CPS 内で、単に認証局という場合は証明書の発行業務及び登録業務を含む。
RFC 3647（Request For Comments 3647）		認証局 や PKI のための CPS の執筆者を支援するフレームワーク。
オブジェクト識別子（Object Identifier）	OID	世界で一意となる値を登録機関（ISO、ITU）に登録した識別子。PKI で使うアルゴリズム、証明書内に格納する名前（subject）のタイプ（Country 名等の属性）等は、オブジェクト識別子として登録されているものが使用される。
X.509		ITU-T が定めた証明書及び証明書失効リストのフォーマット。X.509 v3 では、任意の情報を保有するための拡張領域が追加された。
公開鍵		公開鍵暗号方式において用いられる鍵ペアの一方。私有鍵に対応する、公開されている鍵。
私有鍵		公開鍵暗号方式において用いられる鍵ペアの一方。公開鍵に対応する、本人のみが保有する鍵。
証明書発行要求（Certificate Signing Request）	CSR	証明書を発行する際のもととなるデータファイル。CSR には証明書の発行要求者の公開鍵が含まれており、その公開鍵に発行者の署名を付与して証明書を発行する。

用語	略称	説明
CRL （Certificate Revocation List）		証明書の有効期間中に、認証局私有鍵の危殆化等の事由により失効された EE 証明書及び運用用証明書の失効リスト。
PIN （ Personal Identification Number）		個人を識別するための情報。

2. 公開とリポジトリの責任

2.1. リポジトリ

本認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理を行う。リポジトリには証明書リポジトリと情報公開用リポジトリがある。システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくはホームページ上で公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。

2.2. 証明情報の公開

次の情報を情報公開用リポジトリ上に公開する。

- CPS

また次の情報を証明書リポジトリ上に公開する。

- EE 証明書
- CRL

ただし EE 証明書と CRL は検証者のみに公開する。

また本認証局は、自己署名証明書のフィンガープリントを情報公開用リポジトリより http を使用して公開する。フィンガープリントを公開するリポジトリの URI は次のとおりである。

（URI は決定後に記述される）

なお、CPS 及び認証局に関する重要情報は、次に示す URI のホームページにおいても公開される。

（URI は決定後に記述される）

2.3. 公開の時期又は頻度

本認証局が公開する情報について、公開の時期及び頻度は次のとおりである。

- CPS については改定の都度に公表される。
- 自己署名証明書、リンク証明書、下位認証局証明書については、発行及び更新の都度公表される。
- CRL については、発行の都度公表される。発行の頻度は本 CPS「4.9.7.証明書失効リストの発行頻度」で規定される。
- 認証局に関する重要情報若しくはその他の情報は、必要に応じて適宜更新が行われる。
- EE 証明書については、発行及び更新の都度公表される。

2.4. リポジトリへのアクセス管理

本認証局は公開情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。認証に使われる EE 証明書の証明書検証者は JPNIC であるとする。従って基本的に証明書リポジトリは JPNIC に向けて提供される。

3. 識別及び認証

3.1. 名前決定

3.1.1. 名前の種類

証明書発行者の名前と発行対象の名前は、X.500 シリーズ定義の識別名の規定に従って設定する。

3.1.2. 名前が意味を持つことの必要性

証明書に記載される名前は、個人名、組織名、役割名、および機器名をあらわすものである必要がある。

3.1.3. 所有者の匿名性

証明書には、個人、組織、役割、および機器が特定できる名前であれば、実名を使用する必要はない。

3.1.4. 種々の名前形式を解釈するための規則

様々な名前の形式を解釈するルールは、X.500 シリーズ定義の識別名の規定に従う。

3.1.5. 名前の一意性

証明書に記載される名前は、本認証局が同一ポリシのもとで発行する全ての証明書において一意とする。

3.1.6. 商標の認識、認証及び役割

規定しない。

3.2. 初回の本人性確認

3.2.1. 私有鍵の所持を証明する方法

本認証局は、PKCS#10（Public-Key Cryptography Standards #10）に従った電子署名のされた証明書発行要求の利用、その他本認証局が認めた方法を通じて、ホストマスタ証明書の申請者が私有鍵を所有していることを確認する。

サーバ証明書に関しては、本認証局は、予め規定された方法により証明書申請者が私有鍵を所有していることを確認する。

3.2.2. 組織の認証

本認証局は、LRA に対して組織若しくは団体の認証を行う。LRA としての認証を受けようとする組織若しくは団体は IP 指定事業者でなければならない。

サーバ証明書に関しては、本認証局は、証明書の発行対象となるサーバを運用・管理する組織若しくは団体が、JPNIC 又は JPNIC が認める組織若しくは団体であることを確認する。

3.2.3. 個人の認証

JPNIC は、メンバ管理者証明書の申請者の発行登録を行う際に、所定の手続きに従ってメンバ管理者証明書の申請者の認証を行うこととする。

メンバ管理者は、ホストマスタ証明書の申請者の発行登録を行う際に、所定の手続きに従ってホストマスタ証明書の申請者の認証を責任を持って行うこととする。

サーバ証明書に関しては、本認証局は、証明書の発行を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを、予め規定された方法により確認する。

3.2.4. 確認しない所有者の情報

規定しない。

3.2.5. 権限の正当性確認

本認証局は、メンバ管理者からホストマスタ証明書の申請登録を受け付けるにあたって、当該メンバ管理者の正当性を確認する。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申請時の本人性確認と認証

3.3.1. 通常の鍵更新の本人性確認と認証

本 CPS「3.2.初回の本人性確認」に定める手続と同様とする。

3.3.2. 証明書失効後の鍵更新の本人性確認と認証

本 CPS「3.2.初回の本人性確認」に定める手続と同様とする。

3.4. 失効申請時の本人性確認と認証

JPNIC は、メンバ管理者証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

メンバ管理者は、ホストマスタ証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。

サーバ証明書に関しては、本認証局は、証明書の失効を申請する者が、JPNIC 又は JPNIC が認める組織若しくは団体より証明書の発行の許可を受けている者であることを、予め規定された方法により確認する。

4. 証明書のライフサイクルに対する運用上の要件

4.1. 証明書申請

4.1.1. 証明書申請を提出することができる者

メンバ管理者証明書の申請を行うことができる者は、IP 指定事業者に所属する者とする。

ホストマスタ証明書の申請を行うことができる者は、認証されたメンバ管理者とする。

サーバ証明書の申請を行うことができる者は、JPNIC の職員若しくは JPNIC が指定した者とする。

4.1.2. 登録手続及び責任

メンバ管理者証明書の申請者は、JPNIC により事前に周知された方法に従い、JPNIC に対して証明書の発行申請を行う。メンバ管理者は申請書の記載によって役割を確認される。

ホストマスタ証明書の申請者は、メンバ管理者により事前に周知された方法に従い、メンバ管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 等の証明書発行要求のデータ形式に従った電子署名のされた証明書発行要求をセキュアなオンライン通信を介して送付する。証明書発行要求の電子署名は検証される。

サーバ証明書の申請者は、本認証局に対して予め規定された方法により証明書の発行申請を行う。

証明書申請者は証明書を申請するにあたって、次の責任を負うものとする。

- 本 CPS、その他本認証局により開示された文書の内容の承諾
- 証明書申請内容の正確な提示

4.2. 証明書申請手続

4.2.1. 本人性確認と認証機能の実行

メンバ管理者証明書の申請者の本人性確認は JPNIC の登録局管理者が行う。

ホストマスタ証明書の申請者の本人性確認はメンバ管理者が行う。メンバ管理者は、本 CPS「1.1.1.個人の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。メンバ管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。

サーバ証明書の申請者の本人性確認は、本認証局が予め規定された方法により行う。

4.2.2. 証明書申請の承認又は却下

メンバ管理者はホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。メンバ管理者は申請の審査に関して責任を負うものとする。

JPNIC の登録局管理者はメンバ管理者証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は本認証局に対し証明書の申請登録を行う。JPNIC の登録局管理者は申請の審査に関して責任を負うものとする。

なお、本認証局は、ホストマスタ証明書の申請登録を行うメンバ管理者の本人性確認を行った後、証明書の発行手続を開始する。

サーバ証明書に関しては、本認証局が申請の諾否を決定する。

4.2.3. 証明書申請の処理時間

メンバ管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。

JPNIC の登録局管理者はメンバ管理者証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。

本認証局は、メンバ管理者又は JPNIC の登録局管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。

サーバ証明書に関しては、本認証局は、本 CPS「4.1.1.証明書申請を提出すること

ができる者」にて規定した者より発行申請を受理した場合、速やかに証明書の発行を行う。

4.3. 証明書発行

4.3.1. 証明書の発行過程における認証局の行為

本認証局は、メンバ管理者からのホストマスタ証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。またメンバ管理者証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。本認証局は、申請登録の真正性を確認した後、ホストマスタ証明書の申請者に対し、本 CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。

本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。

本認証局は、メンバ管理者証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、オフラインの手段を介してメンバ管理者証明書の申請者に対し証明書を発行する。

サーバ証明書に関しては、本認証局は、申請者の本人性確認を行った後、予め規定された方法により証明書の発行を行う。

4.3.2. 認証局の所有者に対する証明書発行通知

メンバ管理者証明書はオフラインの手段により申請者に対し発行通知を行う。

本認証局は、証明書発行に必要な 2 種類の情報を生成し、二つの異なる方法を用いてメンバ管理者経由でホストマスタ証明書の申請者へ通知する。

サーバ証明書に関しては、本認証局は、予め規定された方法により申請者に対し発行通知を行う。

4.4. 証明書の受領確認

4.4.1. 証明書の受領確認の行為

メンバ管理者証明書に関してはオフラインの手段を使い受領する。証明書に不具合がある場合は JPNIC へ連絡を行う。配達後一週間後までに連絡がない場合は受領したとみなす。

本認証局は、到達確認のできる方法でメンバ管理者の証明書を配達する。ホストマスタ証明書の申請者による証明書のダウンロードし、確認した上で受領するものとする。証明書に不具合がある場合はメンバ管理者を通じて JPNIC へ連絡を行う。ダウンロード後一週間後までに不具合の連絡がない場合は受領したとみなす。

サーバ証明書に関しては、本認証局は予め規定された方法により証明書の受領を確認する。

なお、証明書の申請者は、証明書ファイルが自身の環境で利用可能であること、証明書の記載内容が正しいことを確認しなければならない。

4.4.2. 認証局による証明書の公開

本認証局は、本 CPS「2.2.証明情報の公開」に規定する証明書をリポジトリにて公開する。

4.4.3. 他のエンティティに対する認証局の証明書発行通知

本認証局は、他のエンティティに対して証明書の発行通知を行わない。

4.5. 鍵ペアと証明書の用途

4.5.1. 所有者の私有鍵及び証明書の使用

本 CPS に基づき発行される証明書は、JPNIC と IP アドレス管理指定事業者間での申請等業務に利用することを意図するものである。

証明書所有者は、私有鍵及び証明書の使用に関して、次の責任を負うものとする。

- 証明書の記載内容の受領時確認と誤記内容の申告
- 私有鍵の盗難・漏えい・紛失・他者による不正利用等を防ぐことへの十分な注意と管理
- 鍵の危殆化又はその可能性がある場合の速やかな失効申請
- 使用目的の確認及び、その目的内での使用
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

4.5.2. 検証者の公開鍵及び証明書の使用

証明書検証者は、証明書を信頼するにあたって、次の責任を負う。

- 証明書を信頼する時点で、本 CPS の理解と承諾
- 証明書の使用目的と自己の使用目的が合致していることの承諾
- 証明書に行われた電子署名の検証と発行者の確認
- 証明書の有効期間や記載項目の確認
- CRL に基づいて、証明書が失効していないことの確認
- 証明書パス上の全証明書の改ざん、有効期間、失効、使用目的の確認

4.6. 証明書の更新

本認証局では、鍵ペアの更新を伴わない証明書の更新は行わない。証明書を更新する場合は、新たな鍵ペアを生成することとし、本 CPS「4.7.証明書の鍵更新」に定める手続とする。

4.6.1. 証明書更新が行われる場合

規定しない。

4.6.2. 証明書の更新を申請することができる者

規定しない。

4.6.3. 証明書の更新申請の処理

規定しない。

4.6.4. 所有者に対する新しい証明書の通知

規定しない。

4.6.5. 更新された証明書の受領確認の行為

規定しない。

4.6.6. 認証局による更新された証明書の公開

規定しない。

4.6.7. 他のエンティティに対する通知

規定しない。

4.7. 証明書の鍵更新

4.7.1. 証明書の鍵更新の場合

証明書の鍵更新は、次の場合に行われるものとする。

- 証明書の有効期間が終了する場合
- 鍵の危殆化を理由に証明書が失効された場合

4.7.2. 新しい公開鍵の証明申請を行うことができる者

本 CPS「4.1.1.証明書申請を提出することができる者」と同様とする。

4.7.3. 証明書の鍵更新申請の処理

本 CPS「4.2.証明書申請手続」及び「4.3.証明書発行」に定める手続と同様とする。

4.7.4. 所有者に対する新しい証明書の通知

本 CPS「4.3.2.認証局の所有者に対する証明書発行通知」と同様とする。

4.7.5. 鍵更新された証明書の受領確認の行為

本 CPS「4.4.1 証明書の受領確認の行為」と同様とする。

4.7.6. 認証局による鍵更新済みの証明書の公開

本 CPS「4.4.2.認証局による証明書の公開」と同様とする。

4.7.7. 他のエンティティに対する通知

本 CPS「4.4.3.他のエンティティに対する認証局の証明書発行通知」と同様とする。

4.8. 証明書の変更

4.8.1. 証明書の変更の場合

証明書の変更は、次の場合に行われるものとする。

- 証明書に含まれる公開鍵以外の情報に変更が生じた場合

4.8.2. 証明書の変更を申請することができる者

本 CPS「4.7.2.新しい公開鍵の証明申請を行うことができる者」と同様とする。

4.8.3. 変更申請の処理

本 CPS「4.7.3.証明書の鍵更新申請の処理」と同様とする。

4.8.4. 所有者に対する新しい証明書の通知

本 CPS「4.7.4.所有者に対する新しい証明書の通知」と同様とする。

4.8.5. 変更された証明書の受領確認の行為

本 CPS「4.7.5.鍵更新された証明書の受領確認の行為」と同様とする。

4.8.6. 認証局による変更された証明書の公開

本 CPS「4.7.6.認証局による鍵更新済みの証明書の公開」と同様とする。

4.8.7. 他のエンティティに対する認証局の証明書発行通知

本 CPS「4.7.7.他のエンティティに対する通知」と同様とする。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の場合

ホストマスタ証明書の証明書所有者は、メンバ管理者に証明書の失効申請を行わなければならない。

メンバ管理者証明書の証明書所有者は、JPNIC に証明書の失効申請を行わなければならない。

本認証局は次の項目に該当すると認めた場合、メンバ管理者証明書とホストマスタ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- 証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者あるいは LRA が、本 CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合
- その他本認証局が失効の必要があると判断した場合

サーバ証明書の証明書所有者は次の項目に該当する場合に本認証局に対し失効申請を行わなければならない。

- サーバの使用を停止する場合
- サーバの私有鍵が危殆化した（又はそのおそれがある）場合

また本認証局は、証明書所有者からの失効申請の他に、次の項目に該当すると認めた場合、サーバ証明書の失効処理を行うことができる。

- 本認証局を廃止する場合
- 認証局私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書記載事項が事実と異なる場合
- サーバの私有鍵の危殆化、若しくはそのおそれがある場合
- 証明書の不正使用、若しくはそのおそれがある場合
- 証明書所有者が本 CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合
- その他本認証局が失効の必要があると判断した場合

4.9.2. 証明書失効を申請することができる者

ホストマスタ証明書の失効要求ができる者は、次のとおりである。

- 証明書所有者
- 証明書所有者の法律上の正式な代理人
- 証明書所有者が所属する組織の LRA 責任者、メンバ管理者
- 本認証局

サーバ証明書の失効要求ができるものは、次のとおりである。

- 証明書所有者
- 本認証局

4.9.3. 失効申請手続

メンバ管理者は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

JPNIC は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。

サーバ証明書の所有者は、本認証局に対し予め規定された方法により失効申請を行う。

なお、「4.4.1.証明書が失効される理由」にて列挙する項目に該当すると本認証局が認めた場合には、本認証局が自身の判断により証明書の失効登録を行うことがある。

4.9.4. 失効申請の猶予期間

証明書の失効要求は、失効すべき事象が発生した場合、可能な限り速やかに行われるものとする。

4.9.5. 認証局が失効申請を処理しなければならない期間

本認証局における証明書の失効処理は、失効申請の受領後、24 時間以内に行われる。

4.9.6. 検証者の失効調査の要求

証明書検証者は、本認証局により発行された証明書を信頼し利用するにあたって、最新の CRL を参照し当該証明書の失効処理が行われていないことを確認しなければならない。

4.9.7. 証明書失効リストの発行頻度

CRL は証明書失効の有無に関わらず、24 時間以内に更新される。証明書の失効が申請された場合は、失効手続が完了した時点で更新される。

4.9.8. 証明書失効リストの発行最大遅延時間

本認証局は、CRL が生成された後、速やかにリポジトリに公開する。

4.9.9. オンラインでの失効/ステイタス確認の適用性

OCSP 等のオンラインの失効又はステータスチェックの機能はサポートしない。

4.9.10. オンラインでの失効/ステイタス確認を行うための要件

規定しない。

4.9.11. 利用可能な失効通知の他の形式

規定しない。

4.9.12. 鍵更新の危殆化に対する特別要件

本認証局は、本認証局の私有鍵に危殆化又は危殆化のおそれがある場合は、直ちに全ての証明書の失効処理を行い、CRL に登録し、証明書所有者に対してメール等の手段で本認証局の私有鍵の危殆化等の事実と証明書失効の通知を行う。

4.9.13. 証明書の一時停止の場合

本認証局は、発行した証明書の一時停止を行わない。

4.9.14. 証明書の一時停止を申請することができる者

規定しない。

4.9.15. 証明書の一時停止申請手続き

規定しない。

4.9.16. 一時停止を継続することができる期間

規定しない。

4.10. 証明書のステイタス確認サービス

4.10.1. 運用上の特徴

本認証局は、証明書検証者における証明書ステイタスの確認手段として、CRL を提供する。CRL へのアクセス要件は、本 CPS「2.4.リポジトリへのアクセス管理」に規定する。また、CRL の発行頻度及び発行最大遅延時間については、本 CPS「4.9.7. 証明書失効リストの発行頻度」及び「4.9.8. 証明書失効リストの発行最大遅延時間」に規定する。

4.10.2. サービスの利用可能性

本 CPS「2.1.リポジトリ」に規定する。

4.10.3. オプショナルな仕様

規定しない。

4.11. 登録の終了

証明書所有者が本認証局のサービスの利用登録を終了する場合、本認証局は証明書所有者に対して発行した証明書の全てを失効する。

4.12. キーエスクローと鍵回復

本認証局は私有鍵を第三者に対して寄託しない。

4.12.1. キーエスクローと鍵回復ポリシ及び実施

規定しない。

4.12.2. セッションキーのカプセル化と鍵回復ポリシ及び実施

規定しない。

5. 設備上、運営上、運用上の管理

5.1. 物理的管理

5.1.1. 立地場所及び構造

本認証局に係わる重要な設備については、火災、水害、地震、落雷その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。

また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5.1.2. 物理的アクセス

本認証局は、認証設備室に関して、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理を行う。本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。

5.1.3. 電源及び空調

本認証局は、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電及び電圧・周波数の変動に備えた対策を講ずる。また空調設備に関して、各種使用する機器類に悪影響を与えないよう維持管理を行う。

5.1.4. 水害及び地震対策

本認証局の設備を設置する室は防水対策を施し､浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。

5.1.5. 火災防止及び火災保護対策

本認証局は、設備を防火壁によって区画された防火区画内に設置する。また防火区画内では電源設備や空調設備の防火措置を講じ、火災報知器及び消火設備の設置を行う。

5.1.6. 媒体保管場所

アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、本認証局の設置場所とは別の適切な入退管理が行われた室内の保管庫に保管される。

5.1.7. 廃棄処理

本認証局は、機密扱いとする情報を含む書類・記録媒体について、情報の初期化・裁断等、事前に定められた方法に従い適切に廃棄処理を行う。

5.1.8. 施設外のバックアップ

規定しない。

5.2. 手続的管理

5.2.1. 信頼される役割

証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担っている。認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。

5.2.2. 職務ごとに必要とされる人員

認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。

5.2.3. 個々の役割に対する本人性確認と認証

認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。

5.2.4. 職務分割が必要となる役割

権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。

5.3. 人事的管理

5.3.1. 資格、経験及び身分証明の要件

JPNIC は、職員に認証局の役割を任命する際及びその後定期的に、適切な人物審査を実施のうえ、任命を行う。任命の際には守秘義務契約を結び、情報の適切な管理を行う。また日常業務においては、メンタルヘルス、健康管理及び適正な処遇等による継続した人事管理を行う。

5.3.2. 人員配属に関する規定事項

認証局業務に関わる要員を任命するにあたって、業務の遂行上支障が出ない適切な人員を配置する。配属されるものは機密保持及び内部規定の遵守に対する誓約書を提出する。

5.3.3. 研修要件

運用要員の教育を次のように行う。

- 運用要員が役割に就く前に、認証局の運用に必要な教育を実施する。
- 役割に応じた教育・訓練計画を策定し、計画に沿って定期的に教育・訓練を実施する。
- 業務手順に変更がある場合は遅滞なく事務取扱要領の必要箇所を変更し、その変更に関わる教育・訓練を実施する。

5.3.4. 再研修の頻度及び要件

JPNIC は定期的に本認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。

5.3.5. 仕事のローテーションの頻度及び順序

JPNIC は、本 JPNIC 認証局の運営が損なわれないよう職員の退職又は解任に備えて適切な対策を講ずる。

5.3.6. 認められていない行動に対する処罰

JPNIC は、本認証局の運用要員による認可されていない行為に対し、予め決められ

た規程に従って処罰する。

5.3.7. 独立した契約者の要件

JPNIC は、委託契約において委託業務の内容を明確にするとともに、受託者に対して JPNIC の指示の遵守、責任分担、保証、違反時の罰則等について明確にし、かつ受託者と守秘義務契約を結ぶ。また委託後は受託者の業務が適切に行われていることを監督し管理する。

5.3.8. 要員へ提供される資料

運用に必要な文書を運用要員に開示し周知する。

5.4. 監査ログの手続

5.4.1. 記録されるイベントの種類

本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。

認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。

- 認証局の私有鍵の操作に関する記録
- 証明書の発行及び失効等の作業に関する記録
- 失効情報の作成作業に関する記録
- 監査ログの確認に関する記録

また、認証局設備へのアクセスに関する履歴を記録する。

5.4.2. 監査ログを処理する頻度

本認証局は、監査ログ及び関連する記録を定期的に精査する。

5.4.3. 監査ログを保持する期間

監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に一定期間保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。

5.4.4. 監査ログの保護

本認証局は、JPNIC によって認可された人員のみが監査ログファイルにアクセスすることができるようにするために権限者を定め、許可されていない者が閲覧、修正又は削除をすることから保護する。また定期的に監査ログのバックアップを外部記憶媒体に取得し、適切な入退室管理が行われている室内において、施錠可能な保管庫に保管する。

5.4.5. 監査ログのバックアップ手続

監査ログは、認証局システムのデータベースとともに、事前に定められた手続に従

い、外部記憶媒体に定期的にバックアップがとられ、それらの媒体は安全な施設に保管される。

5.4.6. 監査ログの収集システム

監査ログの収集機能は認証局システムの一機能として内在しているものとし、セキュリティに関する重要なイベントを監査ログとして収集する。

5.4.7. イベントを起こしたサブジェクトへの通知

本認証局では、監査ログの収集を、イベントを発生させた人、システム又はアプリケーションに対して通知することなく行う。

5.4.8. 脆弱性評価

認証業務において用いるハードウェア及びソフトウェアは、監査ログ検査等によるシステム面及び運用面におけるセキュリティ上の脆弱性評価に加え、最新の実装可能なセキュリティ・テクノロジの導入等、セキュリティ対策の向上を図るものとする。

5.5. 記録の保管

5.5.1. アーカイブ記録の種類

本 CPS「5.4.1.記録されるイベントの種類」に規定する監査ログに加えて、本認証局は次の記録を保存する。

【認証局システムに記録されるイベント】

- 本認証局の署名用鍵ペアの生成
- システムからの証明書所有者の追加及び削除
- 証明書の発行・失効を含めた鍵の変更
- 登録局管理者権限の追加、変更及び削除

【紙媒体又は外部記憶媒体として保存するもの】

本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。

- 本 CPS、証明書所有者同意書及びその変更に関する記録
- 認証業務に従事する者の責任及び権限に関して記載した文書及びその変更に関する記録
- 認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本
- 監査の実施結果に関する記録及び監査報告書

5.5.2. アーカイブ保持期間

本認証局は、認証局システムのデータベースの履歴及び監査ログファイルの履歴を一定期間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本 CPS「5.5.1.アーカイブ記録の種類」に規定する。

5.5.3. アーカイブ保護

アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。本認証局は、アーカイブデータのバックアップを定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した者以外の者がアクセスできないように制限し、温度、湿度等の環境上の脅威から保護された施設に保管する。

5.5.4. アーカイブのバックアップ手続

本認証局は、認証局システムのデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、監査ログも定期的に外部記憶媒体に格納する。

5.5.5. 記録にタイムスタンプを付ける要件

本認証局は、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。ここでいうタイムスタンプとは暗号技術を用いたものではない。

5.5.6. アーカイブ収集システム

認証局サーバデータベース用の履歴収集システムは、認証局サーバシステムに内在している。監査ログファイル用の履歴収集システムについては、本 CPS「5.4.6.監査ログの収集システム」に規定する。

5.5.7. アーカイブの情報を入手し、検証する手続

アーカイブデータは、厳格に管理された区画からアクセス権限者が入手し、外部記録媒体の可読性確認を定期的に行う。また必要に応じ、アーカイブデータの完全性及び機密性の維持に留意し、新しい媒体へ複製を行うとともに、保管期間の過ぎた古い媒体は破棄する。

5.6. 鍵の切替

本認証局の私有鍵は、その有効期間の残りが EE 証明書の最大有効期間よりも短くなる前に、JPNIC はその鍵による新たな EE 証明書の発行を中止し、新たな認証局鍵ペアを本 CPS「6.1. 鍵ペアの生成及びインストール」に定める方法で生成する。新たな公開鍵は JPNIC ルート認証局から証明書の発行を受け、本 CPS「6.1.4.検証者に対する認証局の公開鍵の交付」に定めた方法と同様に配布を行う。

5.7. 危殆化及び災害からの復旧

5.7.1. 事故及び危殆化の取扱手続

認証局私有鍵の危殆化又は危殆化のおそれがある場合、及び災害等により認証業務の中断又は停止につながるような問題が発生した場合、本認証局は予め定められた計画及び手順に従い、認証業務の再開に努める。

5.7.2. コンピュータの資源、ソフトウェア及び/又は、データが破損した場合

JPNIC 認証局は、ハードウェア、ソフトウェア又はデータが破壊された場合、事前に定められた復旧計画に従い、バックアップ用のハードウェア、ソフトウェア及びデータにより、速やかに復旧作業に努める。

5.7.3. エンティティの私有鍵が危殆化した場合の手続

認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。

- ホストマスタ証明書、サーバ証明書等の失効手続
- 認証局私有鍵の廃棄及び再生成手続
- ホストマスタ証明書、サーバ証明書等の再発行手続

また、証明書所有者の私有鍵が危殆化した場合は、本 CPS「4.9.証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。

5.7.4. 災害後の事業継続能力

災害等により JPNIC 認証局の設備が被害を受けた場合は、JPNIC は予備機を確保しバックアップデータを用いて運用の再開に努める。

5.8. 認証局又は登録局の終了

JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ及びアーカイブデータ等の保管組織及び開示方法を業務終了 14 日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。

6. 技術的セキュリティ管理

6.1. 鍵ペアの生成及びインストール

6.1.1. 鍵ペアの生成

本認証局の鍵ペアの生成は鍵管理者立会いのもと、複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、FIPS140-1 レベル 3 の暗号化モジュールを使用して行われる。

メンバ管理者証明書の鍵ペアの生成は、FIPS140-2 レベル 3 の暗号化モジュールを使用して行われる。

6.1.2. 所有者に対する私有鍵の交付

メンバ管理者証明書の鍵ペアの生成は、本認証局において暗号化モジュール内で行われる。生成された鍵ペアは暗号化モジュールを含むハードウェアトークンを使って、メンバ管理者証明書の申請者に交付される。

本認証局はホストマスタ証明書の鍵ペアの作成を行わないため、本項の規定を行わない。

6.1.3. 証明書発行者に対する公開鍵の交付

ホストマスタ証明書の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルを本認証局へ送付することで行われる。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の証明書の配布は、次の 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。

- （URI は決定後に記述される）にて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。証明書検証者は（URI は決定後に記述される）より本認証局の証明書をダウンロードして使用することとする。証明書検証者はダウンロードした本認証局の証明書のフィンガープリントと（URI は決定後に記述

される）にて公開されているフィンガープリントを比較し、一致していることを確認する。
- サーバ証明書の管理者には RAO が、ホストマスタにはメンバ管理者が本認証局の証明書を手渡しする。

6.1.5. 鍵サイズ

本認証局は 2048 ビットの RSA 鍵ペアを使用する。EE については、1024 ビット以上の RSA 鍵ペアを使用することを義務とする。

6.1.6. 公開鍵のパラメータの生成及び品質検査

本認証局の鍵ペアを生成するための公開鍵パラメータは、鍵ペア生成に使用される安全性の高い暗号化モジュールを含むソフトウェアに実装された乱数生成モジュール（以下、RNG という）を用いて生成される。

公開鍵パラメータの品質検査については、特に規定しない。

6.1.7. 鍵用途の目的

本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書、サーバ証明書及び CRL の発行にのみ使用する。

ホストマスタ証明書の keyUsage は digitalSignature、keyEncipherment、dataencipherment のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用するものとする。

サーバ証明書の keyUsage は digitalSignature、keyEncipherment のビットを使用する。SSL/TLS サーバ証明書としてのみ使用するものとする。

6.2. 私有鍵の保護及び暗号モジュール技術の管理

6.2.1. 暗号モジュールの標準及び管理

規定しない。

6.2.2. 私有鍵の複数人管理

本認証局の私有鍵の管理は、複数の CAO に権限を付与することによって行う。2名以上の CAO が揃わなければ本認証局の私有鍵を操作することはできない。

6.2.3. 私有鍵のエスクロー

本 CPS「4.1.2.キーエスクローと鍵回復」に規定する。

6.2.4. 私有鍵のバックアップ

本認証局の私有鍵は、予め定める外部記憶媒体にバックアップされる。バックアップ作成時も鍵管理者の立会いと複数名の CAO を必要とする。

本認証局は、そのバックアップを予め定める保管場所に保管する。

なお、本認証局は、EE の私有鍵のバックアップを行わない。

6.2.5. 私有鍵のアーカイブ

本認証局の私有鍵のアーカイブは行わない。

EE の私有鍵についても同様にアーカイブは行わない。

6.2.6. 私有鍵の暗号モジュールへの又は暗号モジュールからの転送

本認証局の私有鍵は、安全性の高い暗号化モジュールを含むソフトウェアで生成され、他のハードウェア及びソフトウェア等が介入することはない。

6.2.7. 暗号モジュールへの私有鍵の格納

本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。

ホストマスタの私有鍵はホストマスタ自身が私有鍵の生成を行い、ホストマスタ自身で格納を行う。メンバ管理者の秘密鍵は JPNIC において、安全性の高い暗号化モジュール内で生成、格納される。ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。

6.2.8. 私有鍵の活性化方法

本認証局の私有鍵の活性化は、認証設備室内において複数名の CAO を必要とする。

EE の私有鍵に関しては、規定しない。

6.2.9. 私有鍵の非活性化方法

本認証局の私有鍵の非活性化は、認証設備室内において複数名の CAO を必要とし、操作をする者とその監視をする者とに分かれて行われる。

EE の私有鍵に関しては、規定しない。

6.2.10. 私有鍵の破棄方法

本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者と複数名の CAO によって、私有鍵の格納されたハードディスクを完全に初期化又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続によって破棄する。

EE の私有鍵は、EE 自身で確実に破棄するものとする。メンバ管理者の秘密鍵は基本的に JPNIC において破棄するものとする。ただし、紛失等の場合はこの限りではない。

6.2.11. 暗号モジュールの評価

規定しない。

6.3. その他の鍵ペア管理

6.3.1. 公開鍵のアーカイブ

本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。

6.3.2. 証明書の運用上の期間及び鍵ペアの使用期間

本認証局の証明書の有効期間は 10 年、私有鍵の有効期間は 8 年とする。本認証局は私有鍵の有効期限前に鍵ペアの更新を行う。

EE 証明書の有効期間は 2 年とする。私有鍵は復号を行う場合においてのみ、2 年を超える使用を認めるものとする。

6.4. 活性化データ

6.4.1. 活性化データの生成及び設定

本認証局の私有鍵に対するものを含め、本認証局で使用される PIN やパスワードは、英大文字、英小文字、数字を全て含む 8 文字以上の長さのものとする。

6.4.2. 活性化データの保護

本認証局で使用される PIN やパスワードについては、封印されたうえで運用管理者による管理のもと保管される。また、CAO によって定期的に変更を行う。

6.4.3. 活性化データの他の考慮点

規定しない。

6.5. コンピュータのセキュリティ管理

6.5.1. 特定のコンピュータのセキュリティに関する技術的要件

本認証局のサーバシステムに関わる業務は、原則として複数人の CAO によって行われる。ただし、ハードウェア障害時等に発生する専門的な知識を必要とする作業については、複数人の CAO 立会いのもとで保守員によって行うものとする。システムに対して行われた重要な操作については、全てログが残るよう設定する。システムにアクセスするための全てのパスワードについては、適切な管理を行う。本認証局のサーバシステムについては、常時リソース監視を行い、システムの異常や不正運用を検知した場合には、速やかに適切な対策を実施する。

6.5.2. コンピュータセキュリティ評価

本認証局は使用する全てのソフトウェア、ハードウェアに対して事前に運用テストを行い、信頼性の確認を行う。

6.6. ライフサイクルの技術上の管理

6.6.1. システム開発管理

システムの品質及びセキュリティを保つために、開発時における各工程の管理、導入前の評価等を実施する。

6.6.2. セキュリティ運用管理

システムのセキュリティ管理として、入退室管理、教育を含む要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のシステム的なセキュリティ対策、セキュリティ対策ソフトウェアの適時更新等を実施する。

6.6.3. ライフサイクルのセキュリティ管理

規定された管理方法により、システムが管理されているかの評価を行う。

本認証局のシステムに対して、セキュリティに関する情報収集を行い、最新の動向を考慮し、適切な評価及び改善を行う。

6.7. ネットワークセキュリティ管理

本認証局の存在するネットワークにはファイアウォールを使用し、ファイアウォール外からのアクセスについては必要最低限のプロトコルに制限する。またアクセス可能なホストも限定する。

6.8. タイムスタンプ

タイムスタンプの使用に関する要件は、本 CPS「5.5.5.記録にタイムスタンプを付ける要件」に規定する。

7. 証明書と、証明書失効リスト及び OCSP のプロファイル

7.1. 証明書のプロファイル

本認証局が発行する証明書は、X.509 証明書フォーマットのバージョン 3 に従う。証明書プロファイルは、表 7-1 のとおりである。

7.1.1. バージョン番号

本認証局が発行する証明書は全て X.509 バージョン 3 証明書フォーマットに従う。

7.1.2. 証明書拡張

本認証局が発行する証明書に使用される拡張領域を次に示す。

7.1.2.1. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.2. subjectKeyIdentifier

当該証明書所有者の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.3. keyUsage

ホストマスタ証明書は digitalSignature、keyEncipherment、dataEncipherment を使用する。サーバ証明書は digitalSignature と keyEncipherment のみを使用する。この拡張は non-critical である。

7.1.2.4. certificatePolicies

ホストマスタ証明書、サーバ証明書共に certificatePolicies 拡張を使用する。policyIdentifier の値は本 CPS「7.1.6.証明書ポリシ OID」、policyQualifiers の値は本 CPS「7.1.8.ポリシ修飾子の記述と意味」に示す。この拡張は non-critical である。

7.1.2.5. subjectAltName

この拡張はホストマスタ証明書にのみ使用する。rfc822Name として証明書所有者の電子メールアドレスを記述する。この拡張は non-critical である。

7.1.2.6. cRLDistributionPoints

本認証局が発行する CRL の URI を記述する。この拡張は non-critical である。

7.1.3. アルゴリズム OID

本認証局が発行する証明書において使用されるアルゴリズム OID は次の 2 つである。

- sha1withRSAEncryption（1.2.840.113549.1.1.5）
- rsaEncryption（1.2.840.113549.1.1.1）

7.1.4. 名前形式

本 CPS「3.1.1.名前の種類」に従う。

7.1.5. 名前制約

本認証局は、発行する全ての証明書において nameConstraints 拡張を使用しない。

7.1.6. 証明書ポリシ OID

ホストマスタ証明書、メンバ管理者証明書、サーバ証明書のいずれも本 CPS「1.2. 文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。

7.1.7. ポリシ制約拡張

本認証局は、発行する全ての証明書において policyConstraints 拡張を使用しない。

7.1.8. ポリシ修飾子の記述と意味

ホストマスタ証明書、サーバ証明書共にポリシ修飾子の値として本 CPS が公開されている URI を使用する。

7.1.9. critical な証明書 certificatePolicies 拡張の処理

本認証局が発行する証明書に含まれる certificatePolicies 拡張は全て non-critical であり、本項の規定を行わない。

表 7-1 JPNIC 資源管理認証局が発行する証明書プロファイル

Field	critical flag	ホストマスタ証明書	サーバ証明書
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString[*1]	PrintableString[*1]
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime notBeforeの時刻より2年後	UTCTime notBeforeの時刻より2年後
subject	NA		
		PrintableString[*2]	PrintableString[*3]
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		ホストマスタ公開鍵のBIT STRING	サーバ公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNIC IPアドレス認証局公開鍵の160bit SHA-1ハッシュ値	JPNIC IPアドレス認証局公開鍵の160bit SHA-1ハッシュ値
authorityCertIssuer		使用しない	使用しない
authorityCertSerialNumber		使用しない	使用しない
subjectKeyIdentifier	n	ホストマスタ公開鍵の160bit SHA-1ハッシュ値	サーバ公開鍵の160bit SHA-1ハッシュ値
keyUsage	n		
digitalSignature		1	1
nonRepudiation		0	0
keyEncipherment		1	1
dataEncipherment		1	0
certificatePolicies	n		
policyIdentifier		本CPのOID	本CPのOID
policyQualifiers			
policyQualifierId		CPSUri	CPSUri
qualifier		本CP/CPSを公開するURI	本CP/CPSを公開するURI
subjectAltName	n		
rfc822Name		ホストマスタのメールアドレス	使用しない
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC IPアドレス認証局がCRLを公開するURI	JPNIC IPアドレス認証局がCRLを公開するURI
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

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

※2　C=JP, O=（組織名称）, O=Resource Holder, O=LIR Corporate Administrator, OU=（LIR Corporate Administrator、LIR Administrator、LIR Hostmaster のいずれか）, OU=（JPNIC が資源管理の単位ごとに割り当てるメンテナーコード） CN=（LIR-CO、LIR-AD、LIR-HM のいずれか）＋（JPNIC がユーザごとに割り当てる認証 ID）＋（証明書発行対象ホストマスタの名称をアルファベット表記したもの）

※3　C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=Resource Management System, CN=（証明書発行対象サーバの FQDN）

7.2. 証明書失効リストのプロファイル

本認証局が発行する CRL は、X.509CRL フォーマットのバージョン 2 に従う。CRL プロファイルは、表 7-2 のとおりである。

7.2.1. バージョン番号

本認証局が発行する CRL は全て X.509 バージョン 2CRL フォーマットに従う。

7.2.2. CRL 及び CRL エントリ拡張

本認証局は次の 2 つの CRL 拡張を使用し、CRL エントリ拡張は使用しない。

7.2.2.1. cRLNumber

本認証局が発行する CRL において一意となる非負の整数を使用する。

7.2.2.2. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

表 7-2 JPNIC 資源管理認証局が発行する CRL プロファイル

Field	critical flag	証明書失効リスト
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString[*1]
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより24時間後
revokedCertificates	NA	
revokedCertificate		
userCertificate		失効された証明書の シリアル番号
revocationDate		UTCTime 証明書の失効された時刻
crlEntryExtensions		
		使用しない
crlExtensions	NA	
cRLNumber	n	non-negative integer
authorityKeyIdentifier	n	JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値

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

7.3. OCSP プロファイル

7.3.1. バージョン情報

使用しない。

7.3.2. OCSP 拡張

使用しない。

8. 準拠性監査とその他の評価

8.1. 評価の頻度又は評価が行われる場合

本認証局は必要に応じて監査を実施する。

8.2. 評価人の身元又は資格

JPNIC は、認証局の準拠性監査を、運営委員会が選定する認証業務に精通した監査者により実施する。

8.3. 評価人と評価されるエンティティとの関係

JPNIC は、本認証局の認証業務に関わる要員以外から監査者を選定する。

8.4. 評価で扱われる事項

本認証局の準拠性監査は、認証局の運営が本 CPS 及び関連する規定を遵守して運営されているかを監査するものである。

また、運営委員会が必要と認めた場合、運営委員会が指定する監査目的による監査を実施する。

なお、JPNIC は LRA の監査を行う権利を有する。

8.5. 不備の結果としてとられる処置

本認証局は、監査報告書で指摘された事項に対して、運営委員会がその対応を決定する。運営委員会は、指摘事項に関して、セキュリティ技術の最新動向も踏まえ、問題が解決されるまでの対応策も含め、その措置を JPNIC 認証局の運営責任者に指示する。講じられた対応策は、運営委員会に報告され、評価されるとともに、次の監査において確認される。監査において発見された不備等の指摘事項への対応をしない場合は、運営委員会によって予め定められた罰則が課される。

8.6. 評価結果の情報交換

監査結果の報告は監査者から運営委員会に対して行われる。本認証局は、法律に基づく開示要求があった場合以外は、監査結果を外部へ開示しない。

なお、監査報告書については、JPNIC 認証局運営責任者が最低 5 年間保管管理するものとする。

9. 他の業務上の問題及び法的問題

9.1. 料金

本認証局が発行する証明書に関わる発行料金、更新料金、利用料金等は、別途定めるものとし、事前に関係者に周知する。

9.2. 財務的責任

規定しない。

9.3. 情報の秘密性

9.3.1. 秘密情報の範囲

本認証局が保持する情報は、本 CPS「2.2.証明情報の公開」で公表すると定めた情報、本 CPS の一部として明示的に公表された情報、ホームページで公表している情報、証明書の失効理由及び失効に関するその他の詳細情報を除き、秘密扱いとする。

証明書所有者の私有鍵は、その証明書所有者によって秘密扱いとされる情報とする。

9.3.2. 秘密情報の範囲外の情報

本 CPS で公表すると定めた情報、本 CPS の一部として明示的に公表された情報、ホームページ等で公表している情報、証明書の発行者である認証局情報と失効日時を含む CRL は秘密扱いとしない。その他、次の状況におかれた情報は秘密扱いとしない。

- JPNIC の過失によらず知られるようになった情報
- JPNIC 以外の出所から、機密保持の制限なしに JPNIC に知られるようになった情報
- JPNIC によって独自に開発された情報
- 開示対象の情報に関連する人又は組織により承認を得ている情報

9.3.3. 秘密情報を保護する責任

本認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を

開示することができる。また、本認証局で取扱う情報に関して、調停、訴訟、仲裁、その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。更に、本認証局では、メンバ管理者から、メンバ管理者の管理する証明書所有者に関連する情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、メンバ管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、メンバ管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。

JPNIC 認証局は、業務の一部を委託する場合、秘密情報を委託先に開示することがある。ただし、その委託契約においては秘密情報の守秘義務を規定する。

JPNIC 認証局は、前述の場合を除いて秘密情報を開示しない。秘密情報が漏えいした場合、その責任は漏えいした者が負う。

なお、個人情報の保護に関する取扱いは、本 CPS「9.4.個人情報のプライバシ保護」に定める。

9.4. 個人情報のプライバシ保護

9.4.1. プライバシポリシ

本認証局は個人情報保護の重要性を認識し、個人情報を本 CPS「9.3.3.秘密情報を保護する責任」と同様に取扱うことに加え、次のポリシを遵守する。

（1） 管理責任者をおき、個人情報の適切な管理を行う。

（2） 個人情報を収集する場合、収集目的を知らせたうえで、必要な範囲の情報のみを適法かつ公正な手段で収集する。

（3） 証明書所有者から提出を受けた個人情報は、次の目的にのみ使用する。

- IP アドレス管理業務の潤滑な運用を行うため
- 証明書における、認証サービス上の責任を果たすため
- その他認証業務に関連した目的のため

（4） 証明書所有者の同意がある場合及び法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対し本書と同等の条件を義務付けるものとする。

（5） 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざん及び漏えい等から保護するよう努める。

（6） 証明書所有者自身の個人情報について開示を求められた場合、第三者への個人情報の漏えいを防止するため、証明書所有者自身であることが JPNIC 認証局において確認できた場合に限り、JPNIC 認証局において保管している証明書所有者の個人情報を本人に開示する。また、証明書所有者の個人情報に誤りや変更がある場合には、証明書所有者からの申出に基づき、合理的な範囲で速やかに、不正確な情報又は古い情報を修正又は削除する。証明書所有者は JPNIC 認証局に開示を求める場合、JPNIC 認証局により定められた方法により申請を行うものとする。

（7） JPNIC 認証局は、認証業務に従事する職員に対して個人情報保護の教育活動を実施する。

（8） 証明書所有者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護方針を適宜見直し、改善を行う。

9.4.2. プライバシとして扱われる情報

規定しない。

9.4.3. プライバシとはみなされない情報

規定しない。

9.4.4. 個人情報を保護する責任

JPNIC 認証局は、本 CPS「9.4.1.プライバシポリシ」に則って個人情報を保護する責任を負う。

9.4.5. 個人情報の使用に関する個人への通知及び承諾

規定しない。

9.4.6. 司法手続又は行政手続に基づく公開

規定しない。

9.4.7. 他の情報公開の場合

規定しない。

9.5. 知的財産権

別段の合意がなされない限り、知的財産権の扱いは次に従うものとする。

- JPNIC 認証局の発行した証明書、CRL は JPNIC に帰属する財産とする
- 本 CPS は JPNIC に帰属する財産とする
- JPNIC 認証局の私有鍵及び公開鍵は JPNIC に帰属する財産とする
- JPNIC 認証局から貸与されたソフトウェア、ハードウェア、その他文書、情報等は JPNIC に帰属する財産とする

9.6. 表明保証

9.6.1. 発行局の表明保証

JPNIC 発行局は、JPNIC 発行局の業務を遂行するにあたり次の義務を負う。

- JPNIC 発行局の証明書署名鍵のセキュアな生成・管理
- JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理
- JPNIC 発行局のシステム稼動の監視・運用
- CRL の発行・公表
- リポジトリの維持管理
- 本 CPS に従った受付時間内の問合せ受付

9.6.2. 登録局の表明保証

JPNIC 登録局は、JPNIC 登録局の業務を遂行するにあたり次の義務を負う。

- 登録端末のセキュアな環境への設置・運用
- 証明書発行・失効申請における JPNIC 発行局への正確な情報伝達
- 証明書失効申請における JPNIC 発行局への運用時間中の速やかな情報伝達

9.6.3. ローカル登録局の表明保証

LRA は、LRA 業務を遂行するにあたり次の義務を負う。

- 証明書所有者と証明書申請者が同一であることの検証
- JPNIC 登録局への正確な申請情報の伝達
- 証明書使用におけるホストマスタの教育
- 正当な証明書申請者への確実な証明書配布
- 証明書失効の妥当性の確認
- その他、JPNIC との契約に準拠した運用の厳守

9.6.4. 所有者の表明保証

証明書所有者は、証明書所有にあたり次の義務を負う。

- 本 CPS 及び本認証局が提示するその他の文書（文書名は決定後に記述される）の理解と承諾
- 本 CPS「4.5.1.所有者の私有鍵及び証明書の使用」に規定する義務

9.6.5. 検証者の表明保証

証明書検証者は、本 CPS「4.5.2.検証者の公開鍵及び証明書の使用」に規定する義務を負う。

9.6.6. 他の関係者の表明保証

規定しない。

9.7. 保証の制限

JPNIC は、本 CPS「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害、派生的損害に対する責任を負わない。

9.8. 責任の制限

本 CPS「9.6.1.発行局の表明保証」かつ「9.6.2.登録局の表明保証」の内容に関し、次の場合には JPNIC は責任を負わないものとする。

- JPNIC に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- LRA 又は証明書所有者が自己の義務の履行を怠ったために生じた損害
- LRA 又は証明書所有者の端末のソフトウェアの瑕疵、不具合その他の動作自体によって生じた損害
- JPNIC の責に帰することのできない事由で証明書及び CRL に公開された情報に起因する損害
- JPNIC の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害
- 天変地異、地震、噴火、火災、津波、水災、落雷、戦争、動乱、テロリズムその他の不可抗力に起因する、認証局業務の停止に起因する一切の損害
- 証明書発行申請における本人認証手続等の LRA が行った業務に起因する損害

9.9. 補償

本認証局が発行する証明書を申請、受領、信頼した時点で、証明書所有者及び証明

書検証者には、JPNIC に対する損害賠償責任及び保護責任が発生する。当該責任の対象となる事象には、各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるようなミス、怠慢な行為、各種行為、履行遅滞、不履行のうち、証明書申請時に証明書申請者が本認証局に最新かつ正確な情報を提供しなかったことに起因するもの又は各種責任、損失、損害、訴訟、あらゆる種類の費用負担の原因となるような証明書所有者及び証明書検証者の行為、怠慢な行為、各種行為、履行遅滞、不履行等が含まれる。

9.10. 有効期間と終了

9.10.1. 有効期間

本 CPS、契約書及び協定等の文書は、正当な承認手続にて発行されてから正当な承認手続にて改訂されるまで有効とする。

9.10.2. 終了

本 CPS、契約書、協定等の文書全部又は一部、若しくは特定の関係者に対して規定されている条項が無効になった場合、その該当部分は終了とする。

9.10.3. 終了の効果と効果継続

本認証局は、本 CPS、契約書、協定等に変更又は終了が発生する場合においても、合意事項に責任を持ち続けることに最善を尽くすものとする。

9.11. 関係者間の個別通知と連絡

規定しない。

9.12. 改訂

9.12.1. 改訂手続

本認証局は、証明書ポリシ及びその保証、義務に著しい影響を与えない範囲での本 CPS 変更の必要性が生じた場合、証明書所有者又は証明書検証者に事前の承諾なしに、随時、本 CPS を変更することができる。なお、改訂の通知から改訂が有効になるまでの期間に改訂に対する異議の申出がない場合は、改訂に対する合意が得られたものとする。改訂に対し合意できない関係者においては、即時に本認証局から発行された証明書の使用を中止するものとする。

9.12.2. 通知方法及び期間

本認証局は、変更された CPS をその改訂が有効になる 10 営業日前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知

を行うものとする。

9.12.3. オブジェクト識別子が変更されなければならない場合

規定しない。

9.13. 紛争解決手続

本認証局が発行する証明書に関わる紛争について、JPNIC に対して、訴訟、仲裁等を含む法的解決手段に訴えようとする場合は、JPNIC に対して事前にその旨を通知するものとする。仲裁及び裁判地は東京都区内における紛争処理機関を専属的管轄とすることに、全ての当事者は合意するものとする。また、本 CPS、契約書にて定められていない事項やこれらの文書の解釈に関し疑義が生じた場合は、各当事者はその課題を解決するために誠意を持って協議するものとする。

9.14. 準拠法

本認証局、証明書所有者及び証明書検証者の所在地に関わらず、本 CPS の解釈、有効性及び本認証局の証明書発行に関わる紛争については、日本国の法令が適用される。

9.15. 適用法の遵守

本認証局は、国内における各種輸出規制を遵守し、暗号ハードウェア及びソフトウェアを取扱うものとする。

9.16. 雑則

9.16.1. 完全合意条項

本 CPS、契約書又は協定等における合意事項は、これらが改訂又は終了されない限り他の全ての合意事項より優先される。

9.16.2. 権利譲渡条項

規定しない。

9.16.3. 分離条項

本 CPS、証明書所有者同意書及び本認証局より示す協定等において、その一部の条項が無効であったとしても、当該文書に記述された他の条項は有効に存続するものとする。

9.16.4. 強制執行条項

規定しない。

9.17. その他の条項

規定しない。

Appendix 2

IP アドレス認証局（認証）

認証業務規程（CPS）

新旧比較表

新：JPNIC 資源管理認証局認証業務規定(CPS)	旧：JPNIC IP アドレス認証局認証業務規定 (CP/CPS)
1.1.概要 本 JPNIC 資源管理認証局 認証業務規定(以下、CPS という）は、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(以下、JPNIC という）と IP アドレス管理指定事業者等との間における、IP アドレス及び AS 番号に関する各種管理業務に用いる証明書を発行する JPNIC 資源管理認証局（以下、本認証局という）の認証業務に関する運用規則を定める。 本認証局は、本 CPS に基づき、IP アドレス管理指定事業者に所属し、各種申請処理業務を行う者（以下、ホストマスタという）等に証明書を発行する等の認証サービスを提供する。また、安全な通信を実現するため、JPNIC の各種サーバに対してサーバ証明書を発行する。 本 CPS の構成は、IETF PKIX WG において標準化されている RFC3647「証明書ポリシと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework)」に準拠している。	**1.1. 概要** 本 CP/CPS は、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(以下、JPNIC と呼ぶ)と IP アドレス管理指定事業者等との間における、IP アドレス及び AS 番号に関する各種管理業務に用いる証明書を発行する JPNIC IP アドレス認証局（以下、本認証局と呼ぶ）の認証業務に関する運用規則を定める。 本認証局は、本 CP/CPS に基づき、IP アドレス管理指定事業者に所属し、各種申請処理業務を行う者（以下、ホストマスタと呼ぶ）等に証明書を発行する等の認証サービスを提供する。また、安全な通信を実現するため、レジストリシステムの各種サーバに対してサーバ証明書を発行する。 本 CP/CPS の構成は、IETF PKIX が提唱する RFC3647「証明書ポリシと認証実践の枠組み（Certificate Policy and Certification Practices Statement Framework)」に準拠している。 → 本項以降、全て「CP/CPS」を「CPS」に置き換え
1.2.文書の名前と識別 本 CPS の正式名称は「JPNIC 資源管理認証局 認証業務規程」という。 JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。 表 1-1 JPNIC 及び JPNIC 資源管理認証局に関連するオブジェクト識別子 オブジェクト：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 → オブジェクト識別子：1.2.392.200175 オブジェクト：JPNIC 資源管理認証局 認証業務規程（CPS） → オブジェクト識別子：1.2.392.200175.1.2.1（OID の詳細は決定後に記述される） オブジェクト：EE 証明書ポリシ → オブジェクト識別子：1.2.392.200175.1.2.1（OID の詳細は決定後に記	**1.2. 文書の名前と識別** 本 CP/CPS の正式名称は「JPNIC IP アドレス認証局 認証業務規程」という。 JPNIC 及び本認証局に関連するオブジェクト識別子を表 1-1 に示す。 表 1-1 JPNIC 及び JPNIC IP アドレス認証局に関連するオブジェクト識別子 オブジェクト：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 → オブジェクト識別子：1.2.392.00200175 オブジェクト：JPNIC IP アドレス認証局 認証業務規程（CP/CPS） → オブジェクト識別子：1.2.392.00200175.2（OID は決定後に記述される） オブジェクト：EE 証明書ポリシ → オブジェクト識別子：1.2.392.00200175.2（OID は決定後に記述される）

述される）	→ 本項以降、全て「IP アドレス認証局」を「資源管理認証局」に置き換え
1.3.1.認証局、登録局、所有者及び検証者 表 1-2 コミュニティに関係する登場者と役割 ・ メンバ管理者証明書…本認証局の認証業務に必要な運用用証明書の一つ。ホストマスタへの証明書発行時のメンバ管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。 ・ エンドエンティティ(EE)…証明書の発行対象である、ホストマスタ、メンバ管理者及び各種サーバの総称 ・ エンドエンティティ証明書(EE 証明書)…EE に発行される証明書の総称 ・ 証明書申請者…証明書を申請中の者 ・ JPNIC 発行局(JPNIC IA) …JPNIC ルート認証局内の発行局及び JPNIC 資源管理認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 資源管理認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。認証局（CA）の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。 ・ JPNIC ルート認証局…JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局（資源管理認証局）の証明書に電子署名を行う。 ・ JPNIC 資源管理認証局…JPNIC が運営を行う IP アドレスの管理業務に関連する証明書の発行を行う認証局。JPNIC 資源管理認証局証明書は、JPNIC ルート認証局により電子署名される。 ・ JPNIC 認証局…JPNIC が運営を行う認証局の総称。JPNIC ルート認証局、JPNIC 資源管理認証局、JPNIC 登録局及びリポジトリから構成される。 ・ LRA…証明書を発行する組織とは異なる組織若しくは団体であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が LRA となる。	**1.3.1.認証局、登録局、所有者及び検証者** 表 1-2 コミュニティに関係する登場者と役割 ・ LRA 管理者証明書…本認証局の認証業務に必要な運用用証明書の一つ。ホストマスタへの証明書発行時の LRA 管理者の認証に必要な証明書であり、その取扱いについては運用規則に則って厳格に管理・運用されるものとする。 ・ エンドエンティティ（EE）…証明書の発行対象である、ホストマスタ(追加)及び各種サーバの総称 ・ エンドエンティティ証明書（EE 証明書）…ホストマスタ証明書及びサーバ証明書の総称 ・ 証明書申請者…EE 証明書を申請中の者 ・ JPNIC 発行局（JPNIC IA）…JPNIC ルート認証局内の発行局及び JPNIC IP アドレス認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC IP アドレス認証局で発行業務をつかさどる組織。RA より依頼された証明書の発行を行う。認証局（CA）の内、証明書の発行、失効等の証明書管理機能を表す場合に使用。 ・ JPNIC ルート認証局…JPNIC が運営を行う認証局全体のルート認証局。JPNIC における認証階層経路の最上位に位置し、自己署名し、かつ配下にある下位認証局（IP アドレス認証局）の証明書に電子署名を行う。 ・ JPNIC IP アドレス認証局…JPNIC が運営を行う IP アドレスの管理業務に関連する証明書の発行を行う認証局。JPNIC IP アドレス認証局証明書は、JPNIC ルート認証局により電子署名される。 ・ JPNIC 認証局…JPNIC が運営を行う認証局の総称。JPNIC ルート認証局、JPNIC IP アドレス認証局、JPNIC 登録局及びリポジトリから構成される。 ・ ローカル登録局(LRA)…証明書を発行する組織とは異なる組織若しくは団体であり、RA 業務において、本人の確認・審査、証明書発行申請処理及び証明書失効申請処理を行う組織。JPNIC 認証局の場合、IP アドレス管理指定事業者が LRA となる。

・ LRA 責任者…IP アドレス管理指定事業者の中における、LRA 業務の責任者。メンバ管理者の任命・解任を行う。 ・ メンバ管理者(メンバ管理者)…IP アドレス管理指定事業者の中で、ホストマスタのメンバ管理と認証及びホストマスタ証明書の発行申請操作を行う。	・ ローカル登録局責任者(LRA 責任者)…IP アドレス管理指定事業者の中における、LRA 業務の責任者。LRA 管理者の任命・解任を行う。 ・ ローカル登録局管理者(LRA 管理者)…IP アドレス管理指定事業者の中で、ホストマスタのメンバー管理と認証及びホストマスタ証明書の発行申請操作を行う。
1.3.2.その他の関係者 規定しない。	(新設)
1.4.1 適切な証明書の使用 本 CPS に基づき発行される証明書は、JPNIC の行う IP アドレス管理業務における各種の申請及び連絡等を目的として、レジストリシステムがユーザ及びメッセージを検証する為に使われるものとする。	**1.4.1 適切な証明書の使用** 本 CP/CPS に基づき発行される証明書は、JPNIC の行う IP アドレス管理業務における各種の申請及び連絡等を目的として、レジストリシステムにおけるユーザ認証及びメッセージ認証のために使われるものとする。
1.4.2 禁止される証明書の使用 本 CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものである。(削除) また JPNIC は、IP アドレス管理指定事業者のホストマスタ相互間での証明書の使用を制限するものではないが、本使用に対してなんら責任を負うものではない。	**1.4.2 禁止される証明書の使用** 本 CP/CPS に基づき発行される証明書は、JPNIC における各種申請処理業務等に利用することを意図するものであり、電子商取引での利用に意図されているものでも、認められているものでもない。また JPNIC は、IP アドレス管理指定事業者のホストマスタ相互間での証明書の使用を制限するものではないが、本使用に対してなんら責任を負うものではない。
1.5.2.CPS のポリシ適合性を決定する者 本 CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会という）が行う。	**1.5.2.CP/CPS のポリシ適合性を決定する者** 本 CP/CPS が、本認証局の運営方針として適切か否かの判断は、JPNIC の認証業務に関する運営委員会（以下、運営委員会と呼ぶ）が行う。
2.1 リポジトリ 本認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理を行う。リポジトリには証明書リポジトリと情報公開用リポジトリがある。システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくはホームページ上で公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。	**2.1.リポジトリ** 本認証局を含む JPNIC 認証局は、リポジトリを一日 24 時間、一週 7 日間利用できるように維持管理を行う。(追加)システムの保守等において、一時的に停止を行う必要がある場合は、証明書所有者、証明書検証者及び関係者に対して、事前に通知若しくはホームページ上で公表するものとする。ただし、災害、事故、障害発生時等やむを得ない事態が発生した場合はこの限りではない。
2.2.証明情報の公開 次の情報を情報公開用リポジトリ上に公開する。 ・CPS また次の情報を証明書リポジトリ上に公開する。 ・EE 証明書	**2.2.証明情報の公開** 本認証局を含む JPNIC 認証局は、次の情報を、JPNIC 認証局のリポジトリ上に公開する。 ・自己署名証明書（JPNIC ルート認証局） ・リンク証明書（JPNIC ルート認証局）

・CRL ただし EE 証明書と CRL は検証者のみに公開する。	・下位認証局証明書（JPNIC ルート認証局） ・EE 証明書（JPNIC IP アドレス認証局） ＊公表時のみ ・CRL（JPNIC ルート認証局、JPNIC IP アドレス認証局） ・CP/CPS（JPNIC ルート認証局、JPNIC IP アドレス認証局） リポジトリの URI は次のとおりである。 （URI は決定後に記述される）
また本認証局は、自己署名証明書のフィンガープリントを情報公開用リポジトリより http を使用して公開する。フィンガープリントを公開するリポジトリの URI は次のとおりである。 （URI は決定後に記述される） なお、CPS 及び認証局に関する重要情報は、次に示す URI のホームページにおいても公開される。 （URI は決定後に記述される）	また、JPNIC が運営する認証局は、フィンガープリントを、リポジトリより SSL/TLS を使用して公開する。フィンガープリントを公開するリポジトリの URI は次のとおりである。 （URI は決定後に記述される） なお、CP/CPS 及び認証局に関する重要情報は、JPNIC の次に示す URI のホームページにおいても公開される。 （URI は決定後に記述される）
2.3.公開の時期又は頻度 本認証局が公開する情報について、公開の時期及び頻度は次のとおりである。	**2.3.公開の時期又は頻度** 本認証局を含む JPNIC 認証局が公開する情報について、公開の時期及び頻度は次のとおりである。 → 本項以降、全て「本認証局を含む JPNIC 認証局」を「本認証局」に置き換え
2.4.リポジトリへのアクセス管理 本認証局は公開情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。認証に使われる EE 証明書の証明書検証者は JPNIC であるとする。従って基本的に証明書リポジトリは JPNIC に向けて提供される。	**2.4.リポジトリへのアクセス管理** 本認証局を含む JPNIC 認証局は、公開情報に関して、読み取り専用の制御以外に特段のアクセスコントロールは行わない。証明書所有者及び証明書検証者は、JPNIC が運営する認証局が発行した証明書に関する公開情報を、リポジトリを通じて入手することができる。
3.1.2 名前が意味を持つことの必要性 証明書に記載される名前は、個人名、組織名、役割名、および機器名をあらわすものである必要がある。	**3.1.2.名前が意味を持つことの必要性** 証明書に記載される名前は、個人名、組織名及びその個人、組織が管理する機器名をあらわすものである必要がある。
3.1.3.所有者の匿名性 証明書には、個人、組織、役割、および機器が特定できる名前であれば、実名を使用する必要はない。	**3.1.3 所有者の匿名性又は仮名性** 証明書に記載される名前として匿名又は仮名を使用することはできない。
3.2.2.組織の認証 本認証局は、LRA に対して組織若しくは団体の認証を行う。LRA としての認証を受けようとする組織若しくは団体は IP 指定事業者でなければならない。	**3.2.2.組織的本人性の認証** 本認証局は、LRA に対して組織若しくは団体の認証を行う。LRA としての認証を受けようとする組織若しくは団体は、登記簿及び代表者の印鑑証明、その

	他本認証局が必要と認める書類を本認証局に提出し、審査を受けなければならない。
3.2.3. 個人の認証 JPNIC は、メンバ管理者証明書の申請者の発行登録を行う際に、所定の手続きに従ってメンバ管理者証明書の申請者の証明を行うこととする。 メンバ管理者は、ホストマスタ証明書の申請者の発行登録を行う際に、所定の手続きに従って干すとマスタ証明書の申請者の認証を責任を持って行うこととする。	**3.2.3. 個人的本人性の認証** (追加) LRA 管理者は、ホストマスタ証明書発行対象者の発行登録を行う際に、人事情報 DB、雇用契約等本人を特定できる情報を用いて発酵対象者の本人確認を行う。また、証明書発行対象者が、LRA 責任者より証明書の発行の許可を受けている者であることを認識する。
3.2.5.権限の正当性確認 本認証局は、メンバ管理者からホストマスタ証明書の申請登録を受け付けるにあたって、当該メンバ管理者の正当性を確認する。	**3.2.5.権限の正当性確認** 本認証局は、LRA 管理者からホストマスタ証明書の申請登録を受付けるにあたって、当該 LRA 管理者の正当性を確認する。
3.4.失効申請時の本人性確認と認証 JPNIC は、メンバ管理者証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。 メンバ管理者は、ホストマスタ証明書に対する失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。	**3.4.失効申請時の本人性確認と認証** LRA 管理者は、ホストマスタから署名付き電子メールによる失効申請を受付けた場合には、その署名を検証する。また署名付き電子メールによらないその他の失効申請の場合は、LRA が事前に定め、本認証局から承認を受けた方法によって申請者の本人確認を確実に行うものとする。 LRA 管理者は、失効申請者の本人確認を行った後、本認証局の定めた方式により、本認証局に失効登録を行うものとする。
4.1.1.証明書申請を提出することができる者 メンバ管理者証明書の申請を行うことができる者は、IP 指定事業者に所属する者とする。 ホストマスタ証明書の申請を行うことができる者は、認証されたメンバ管理者とする。	**4.1.1.証明書申請を提出することができる者** ホストマスタ証明書の申請を行うことができる者は、LRA 契約を結んだ IP アドレス管理指定事業者の従業員若しくは LRA が指定した者とする。
4.1.2.登録手続及び責任 メンバ管理者証明書の申請者は、JPNIC により事前に周知された方法に従い、JPNIC に対して証明書の発行申請を行う。メンバ管理者は申請書の記載によって役割を確認される。 ホストマスタ証明書の申請者は、メンバ管理者により事前に周知された方法に従い、メンバ管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 等の証明書発行要求のデータ形式に従った電子署名のされた証明書発行要求	**4.1.2.登録手続及び責任** （追加） ホストマスタ証明書の申請者は、LRA 管理者により事前に周知された方法に従い、LRA 管理者に対して証明書の発行申請を行う。また、証明書申請者は、本認証局より鍵ペア生成及び証明書発行に必要な 2 種類の情報が通知されたならば、鍵ペアを生成し、本認証局へ PKCS#10 に従った電子署名のされた証明書発行要求をセキュアなオンライン通信を介して

をセキュアなオンライン通信を介して送付する。証明書発行要求の電子署名は検証される。	送付する。 （追加）
4.2.1 本人性確認と認証機能の実行 メンバ管理者証明書の申請者の本人性確認はJPNIC の登録局管理者が行う。 ホストマスタ証明書の申請者の本人性確認はメンバ管理者が行う。メンバ管理者は、本 CPS「1.1.1.個人の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。メンバ管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。	**4.2.1.本人性確認と認証機能の実行** （追加） ホストマスタ証明書の申請者の本人性確認は LRA 管理者が行う。LRA 管理者は、本 CP/CPS「3.2.3.個人的本人性の認証」に基づき、ホストマスタ証明書の申請者の本人確認を実施する。LRA 管理者は、ホストマスタ証明書の申請者の本人確認に関して責任を負うものとする。
4.2.2.証明書申請の承認又は却下 メンバ管理者はホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。メンバ管理者は申請の審査に関して責任を負うものとする。 JPNIC の登録局管理者はメンバ管理者証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は本認証局に対し証明書の申請登録を行う。JPNIC の登録局管理者は申請の審査に関して責任を負うものとする。 なお、本認証局は、ホストマスタ証明書の申請登録を行うメンバ管理者の本人性確認を行った後、証明書の発行手続を開始する。	**4.2.2.証明書申請の承認又は却下** LRA 管理者は、ホストマスタ証明書の申請者からの申請に対し、予め規定された審査基準に基づき、証明書申請の諾否を決定する。申請を承諾した場合は、本認証局に対し証明書の申請登録を行う。LRA 管理者は、申請の審査に関して責任を負うものとする。 (追加) なお、本認証局は、ホストマスタ証明書の申請登録を行う LRA 管理者の本人性確認を行った後、証明書の発行手続を開始する。
4.2.3.証明書申請の処理時間 メンバ管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 JPNIC の登録局管理者はメンバ管理者証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 本認証局は、メンバ管理者又は JPNIC の登録局管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。	**4.2.3.証明書申請の処理時間** LRA 管理者は、ホストマスタ証明書の申請者からの発行申請を受理した場合、速やかに証明書の発行申請登録を行う。 (追加) 本認証局は、LRA 管理者からの発行申請登録を受理した場合、速やかに証明書の発行を行う。
4.3.1.証明書の発行過程における認証局の行為 本認証局は、メンバ管理者からのホストマスタ証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。またメンバ管理者証明書の発行申請登録を受け付けるにあたって、予め定められた方法によりメンバ管理者の権限確認を行う。本認証局は、申請登録	**4.3.1.証明書の発行過程における認証局の行為** 本認証局は、LRA 管理者からのホストマスタ証明書の発行申請登録を受付けるにあたって、予め定められた方法により LRA 管理者の本人性確認を行う。 (追加) 本認証局は、申請登録の真正性を確認した後、ホス

の真正性を確認した後、ホストマスタ証明書の申請者に対し、本 CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。 本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。 本認証局は、メンバ管理者証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、オフラインの手段を介してメンバ管理者証明書の申請者に対し証明書を発行する。	トマスタ証明書の申請者に対し、本 CP/CPS「4.3.2.認証局の所有者に対する証明書発行通知」に定められた方法で証明書の発行が許可されたことを通知する。 本認証局は、ホストマスタ証明書の申請者から送付された証明書発行要求の電子署名を検証し、証明書発行要求の真正性を確認した後、セキュアなオンライン通信を介してホストマスタ証明書の申請者に対し証明書を発行する。 (追加)
4.3.2.認証局の所有者に対する証明書発行通知 メンバ管理者証明書はオフラインの手段により申請者に対し発行通知を行う。 本認証局は、証明書発行に必要な 2 種類の情報を生成し、二つの異なる方法を用いてメンバ管理者経由でホストマスタ証明書の申請者へ通知する。	**4.3.2.認証局の所有者に対する証明書発行通知** （追加） 本認証局は、証明書発行に必要な 2 種類の情報を生成し、一方を（電子メール若しくは郵送：決定後に記述される）を用いて直接ホストマスタ証明書の申請者へ、もう一方を（電子メール若しくは郵送：決定後に記述される）を用いて LRA 管理者経由でホストマスタ証明書の申請者へ通知する。
4.4.1 証明書の受領確認の行為 メンバ管理者証明書に関してはオフラインの手段を使い受領する。証明書に不具合がある場合は JPNIC へ連絡を行う。配達後一週間後までに連絡がない場合は受領したとみなす。 本認証局は、到達確認のできる方法でメンバ管理者の証明書を配達する。ホストマスタ証明書の申請者による証明書のダウンロードし、確認した上で受領するものとする。証明書に不具合がある場合はメンバ管理者を通じて JPNIC へ連絡を行う。ダウンロード後一週間後までに不具合の連絡がない場合は受領したとみなす。	**4.4.1 証明書の受領確認の行為** (追加) 本認証局は、ホストマスタ証明書の申請者による証明書のダウンロードをもって、証明書の受領を確認する。
4.6.1 証明書更新が行われる場合 規定しない。	(新設)
4.6.2 証明書の更新を申請することができる者 規定しない。	(新設)
4.6.3.証明書の更新申請の処理 規定しない。	(新設)

4.6.4 所有者に対する新しい証明書の通知 規定しない。	(新設)
4.6.5.更新された証明書の受領確認の行為 規定しない。	(新設)
4.6.6.認証局による更新された証明書の公開 規定しない。	(新設)
4.6.7.他のエンティティに対する通知 規定しない。	(新設)
4.9.1.証明書失効の場合 ホストマスタ証明書の証明書所有者は、メンバ管理者に証明書の失効申請を行わなければならない。 メンバ管理者証明書の証明書所有者は、JPNIC に証明書の失効申請を行わなければならない。 本認証局は次の項目に該当すると認めた場合、メンバ管理者証明書とホストマスタ証明書の失効処理を行うことができる。 ・本認証局を廃止する場合 ・認証局私有鍵の危殆化、若しくはそのおそれがある場合 ・証明書記載事項が事実と異なる場合 ・証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合 ・証明書の不正使用、若しくはそのおそれがある場合 ・証明書所有者あるいは LRA が、本 CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合 ・JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合 ・その他本認証局が失効の必要があると判断した場合	**4.9.1.証明書失効の場合** LRA 組織に所属する証明書所有者は、LRA が別途定める基準に基づき、LRA 管理者に証明書の失効申請を行わなければならない。 (追加) 本認証局は、証明書所有者及び LRA 管理者からの失効申請の他に、次の項目に該当すると認めた場合、ホストマスタ証明書の失効処理を行うことができる。 ・本認証局を廃止する場合 ・認証局私有鍵の危殆化、若しくはそのおそれがある場合 ・証明書記載事項が事実と異なる場合 ・証明書所有者の私有鍵の危殆化、若しくはそのおそれがある場合 ・証明書の不正使用、若しくはそのおそれがある場合 ・証明書所有者が本 CP/CPS に違反した場合 ・証明書所有者あるいは LRA が、本 CP/CPS 又はその他の契約、規則、法律に基づく義務を履行していない場合 ・JPNIC 認証局と IP アドレス管理指定事業者との間の LRA に関する契約が解除された場合 ・その他本認証局が失効の必要があると判断した場合
4.9.2.証明書失効を申請することができる者 ホストマスタ証明書の失効要求ができる者は、次のとおりである。 証明書所有者 証明書所有者の法律上の正式な代理人 証明書所有者が所属する組織の LRA 責任者、メンバ管理者 本認証局	**4.9.2.証明書失効を申請することができる者** ホストマスタ証明書の失効要求ができる者は、次のとおりである。 証明書所有者 証明書所有者の法律上の正式な代理人 証明書所有者が所属する組織の LRA 責任者、LRA 管理者 本認証局
4.9.3. 失効申請手続	**4.9.3. 失効申請手続**

メンバ管理者は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。 JPNIC は所定の手続きに従って失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。	LRA 組織に所属する証明書所有者若しくは LRA 責任者は、LRA 組織により定められた手続によって、LRA 管理者に失効申請を行う。LRA 管理者は失効要求の正当性を確認のうえ、本認証局に証明書失効登録を行う。 (追加)
4.9.5 認証局が失効申請を処理しなければならない期間 本認証局における証明書の失効処理は、失効申請の受領後、24 時間以内に行われる。	**4.9.5 認証局が失効申請を処理しなければならない期間** 本認証局における証明書の失効処理は、失効申請の受付後、(時間は決定後に記述される) 時間以内に行われる。
4.9.14.証明書の一時停止を申請することができる者 規定しない。	(新設)
4.9.15 証明書の一時停止申請手続き 規定しない。	(新設)
4.9.16.一時停止を継続することができる期間 規定しない。	(新設)
4.12.キーエスクローと鍵回復 本認証局は私有鍵を第三者に対して寄託しない。 (削除)	**4.12.キーエスクローと鍵回復** 本認証局は私有鍵を第三者に対して寄託しない。 EE は私有鍵を EE 自身で生成及び管理する。
4.12.1 キーエスクローと鍵回復ポリシ及び実施 規定しない。	(新設)
4.12.2 セッションキーのカプセル化と鍵回復ポリシ及び実施 規定しない。	(新設)
5.1.1.立地場所及び構造 本認証局に係わる重要な設備については、火災、(削除)水害、地震、落雷(削除)その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。	**5.1.1.立地場所及び構造** 本認証局に係わる重要な設備については、火災、電磁界、水害、地震、落雷、空気汚染その他の災害の被害を容易に受けない場所に設置し、建物構造上、耐震、耐火及び不正侵入防止のための対策を講ずる。建物の内外には、認証設備室の所在についての表示を行わない。
5.1.2.物理的アクセス 本認証局は、認証設備室に関して、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理を行う。(削除) 本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。	**5.1.2.物理的アクセス** 本認証局は、認証設備室に関して、事前に定められた本人の特定及び入室権限の確認を可能とする入退室管理を行い、また監視カメラによる記録を行う。認証設備室への立入には、入室権限を有する複数人が同時に操作する必要がある。本認証局は、入室権限を有しない者の入室を原則として認めない。やむを得ずこれを認める場合は、予め認証局運用管理者の許可を得て、入室権限者同行のうえこの者を入室させることとする。

5.1.4.水害及び地震対策 本認証局の設備を設置する室は防水対策を施し、浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。	**5.1.4.水害及び地震対策** 本認証局の設備を設置する建物及び室には漏水検知器の設置等、防水対策を施して浸水による被害を最小限に抑える。また、JPNIC 認証局は、地震等による機器及び什器の転倒及び落下を防止する対策を講ずる。
5.1.6 媒体保管場所 アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、本認証局の設置場所とは別の適切な入退管理が行われた室内の保管庫に保管される。	**5.1.6. 媒体保管場所** アーカイブデータ、バックアップデータを含む媒体は、適切な入退管理が行われた室内の保管庫に保管される。また複製された重要な媒体は、別地の適切な入退管理が行われた室内の保管庫に保管される。
5.2.1. 信頼される役割 証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担っている。認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。 (表 5-1 とともに削除)	**5.2.1.信頼される役割** 証明書の発行、更新、失効等の重要な業務に携わる者は、本 CP/CPS 上信頼される役割を担っている。JPNIC 認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。JPNIC 認証局運営上の役割を表 5-1 に示す。
5.2.2.職務ごとに必要とされる人員 (削除) 認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。	**5.2.2.職務ごとに必要とされる人数** JPNIC 認証局システムサーバの操作は複数人の CAO によって行う。また、JPNIC 登録局の端末を用いた発行・失効等の操作は複数人の RAO によって行う。 JPNIC 認証局設備の保守、JPNIC 認証局機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。
5.2.3.個々の役割に対する本人性確認と認証 認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。	**5.2.3.個々の役割に対する本人性確認と認証** JPNIC 認証局の設備は、操作者及び必要権限を識別する機能を有するものとする。また、JPNIC 認証局設備を操作する権限は、操作者ごとに設定可能であるものとする。
5.2.4.職務分割が必要となる役割 (削除)権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。	**5.2.4.職務分割が必要となる役割** JPNIC 認証局では、権限を特定の個人に集中させず複数人に権限を分離することで、単独操作で発生する不正行為等の防止を図る。システム操作、承認行為及び監査に関する権限は分離される。
5.3.2.人員配属に関する規定事項 認証局業務に関わる要員を任命するにあたって、業務の遂行上支障が出ない適切な人員を配置する。配属されるものは機密保持及び内部規定の遵守に対する誓約書を提出する。	**5.3.2.経歴の調査手続** JPNIC 認証局業務に係わる要員を採用するにあたって、JPNIC は予め定めた適切な方法を用いてその人物の背景調査を行う。
5.3.3.研修要件	**5.3.3.研修要件**

(削除)運用要員の教育を次のように行う。	JPNIC 認証局は、運用要員の教育を次のように行う。
5.3.4.再研修の頻度及び要件 JPNIC は定期的に本認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。	**5.3.4.再研修の頻度及び要件** JPNIC は定期的に JPNIC 認証局の要員に対して適切な教育を行い、以降必要に応じて再教育を行う。
5.3.6.認められていない行動に対する処罰 JPNIC は、本認証局の運用要員による認可されていない行為に対し、予め決められた規程に従って処罰する。	**5.3.6.認められていない行動に対する制裁** JPNIC は、JPNIC 認証局の運用要員による認可されていない行為に対し、(罰則規定書の名称は決定後に記述される）に従って制裁を与える。
5.3.8.要員へ提供される資料 運用に必要な文書を運用要員に開示し周知する。 (削除)	**5.3.8.要員へ提供される資料** JPNIC 認証局は次の文書を運用要員に開示し周知する。 ・本 CP/CPS ・認証局運用に関する諸規程、手続書、マニュアル、災害復旧計画書等 ・運用要員が遵守しなければならない各種関連規程（その他、要員に提供されるべき文書があれば決定後に記述される。）
5.4.1.記録されるイベントの種類 本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。 認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。 ・認証局の私有鍵の操作に関する記録 ・証明書の発行及び失効等の作業に関する記録 ・失効情報の作成作業に関する記録 ・監査ログの確認に関する記録 また、認証局設備へのアクセスに関する履歴を記録する。	**5.4.1.記録されるイベントの種類** 本認証局システム上で起こったイベントは、それが手動、自動であるかにかかわらず、日付、時刻、イベントを発生させた主体、イベント内容等が記録される。 認証局システムにおける誤操作、不正操作の検知及び運用の正当性を証明するために必要な監査ログとして、次の操作について履歴を記録する。 ・認証局の私有鍵の操作 ・システムの起動･停止 ・データベースの操作 ・権限設定の変更履歴 ・証明書の発行 ・証明書の失効 ・CRL の発行 ・監査ログの検証　　等 また、次のような認証設備室内のネットワーク機器並びに監視システムについても履歴を記録する。 認証設備室への入退室に関する記録 認証局設備への不正アクセスに関する記録　　等

5.4.3.監査ログを保持する期間 監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に一定期間保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。	**5.4.3.監査ログを保持する期間** 監査ログは、最低 2 ヶ月間は認証局サーバ内に保持される。その後、外部記憶媒体に最低 10 年間は保管される。また、認証設備室への入退室に関する記録や不正アクセスに関する記録は、次回の監査終了まで保存されるものとする。
5.5.1.アーカイブ記録の種類 本 CPS「5.4.1.記録されるイベントの種類」に規定する監査ログに加えて、本認証局は次の記録を保存する。 【認証局システムに記録されるイベント】 ・本認証局の署名用鍵ペアの生成 ・システムからの証明書所有者の追加及び削除 ・証明書の発行・失効を含めた鍵の変更 ・登録局管理者権限の追加、変更及び削除 (削除) 【紙媒体又は外部記憶媒体として保存するもの】 ・本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。 (削除) ・本 CPS、証明書所有者同意書及びその変更に関する記録(削除) ・認証業務に従事する者の責任及び権限(削除)に関して記載した文書及びその変更に関する記録(削除) (削除) ・認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本(削除) ・監査の実施結果に関する記録及び監査報告書(削除)	**5.5.1.アーカイブ記録の種類** 本 CP/CPS「5.4.1.記録されるイベントの種類」に規定する監査ログに加えて、本認証局は次の記録を保存する。 【認証局システムに記録されるイベント】 ・本認証局の署名用鍵ペアの生成 ・システムからの証明書所有者の追加及び削除 ・証明書の発行・失効を含めた鍵の変更 ・登録局管理者権限の追加、変更及び削除 ・証明書有効期限の変更等、ポリシの何らかの変更 【紙媒体又は外部記憶媒体として保存するもの】 ・本認証局は次に掲げる運用関連記録のアーカイブを維持、管理する。 （　）内は保管期間 ・本 CP/CPS、証明書所有者同意書及びその変更に関する記録（その作成又は変更を行ってから 10 年間） ・認証業務に従事する者の責任及び権限並びに指揮命令系統に関して記載した文書及びその変更に関する記録（その作成又は変更を行ってから 10 年間） ・証明書の発行、失効時に提出を受ける申請書（該当する証明書の有効期間の満了日から最低 10 年間） ・証明書申請者の真偽の確認のために提出を受けた書類（該当する証明書の有効期間の満了日から最低 10 年間） ・証明書の発行、失効申請に対する諾否を決定した者の氏名の記載した書類及び、申請に対して承諾をしなかった場合においてその理由を記載した書類（該当する証明書の有効期間の満了日から最低 10 年間） ・認証業務の一部を他に委託する場合においては、委託契約に関する書類の原本（その作成を行ってから 10 年間） 監査の実施結果に関する記録及び監査報告書（その作成を行ってから 10 年間）
5.5.2.アーカイブ保持期間	**5.5.2.アーカイブ保持期間**

本認証局は、認証局システムのデータベースの履歴及び監査ログファイルの履歴を一定期間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本CPS「5.5.1.アーカイブ記録の種類」に規定する。	本認証局は、認証局サーバデータベースの履歴及び監査ログファイルの履歴を最低 10 年間保存する。紙媒体及び外部記憶媒体の保存期間に関しては本CP/CPS「5.5.1.アーカイブ記録の種類」に規定する。
5.5.3.アーカイブ保護 アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。本認証局は、アーカイブデータのバックアップを定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した者以外の者がアクセスできないように制限し、温度、湿度（削除）等の環境上の脅威から保護された施設に保管する。	**5.5.3.アーカイブ保護** アーカイブデータには、アクセス制御を施すとともに、改ざん検出を可能とする措置を講ずる。本認証局は、アーカイブデータのバックアップを定期的に外部記憶媒体に取得し、JPNIC の管理部門が許可した者以外の者がアクセスできないように制限し、温度、湿度、磁気等の環境上の脅威から保護された施設に保管する。
5.5.4.アーカイブのバックアップ手続 本認証局は、認証局システムのデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、（削除）監査ログも定期的に外部記憶媒体に格納する。	**5.5.4.アーカイブのバックアップ手続** 本認証局は、認証局サーバデータベースに対して、自動的かつ定期的にサーバ上にバックアップを行う。更に、認証局サーバシステム、監査ログとともに定期的に外部記憶媒体に格納する。
5.5.5.記録にタイムスタンプを付ける要件 本認証局は、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。ここでいうタイムスタンプとは暗号技術を用いたものではない。	**5.5.5.記録にタイムスタンプを付ける要件** 本認証局は、正確な時刻源から時刻を取得し、NTP（Network Time Protocol）を使用し認証局システムサーバの時刻同期を行ったうえ、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。
5.7.3.エンティティの私有鍵が危殆化した場合の手続 認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。 ・ホストマスタ証明書、サーバ証明書等の失効手続 ・認証局私有鍵の廃棄及び再生成手続 ・ホストマスタ証明書、サーバ証明書等の再発行手続 また、証明書所有者の私有鍵が危殆化した場合は、本 CPS「4.9.証明書の失効と一時停止」において定める手続に基づき、証明書の失効手続を行う。	**5.7.3.エンティティの私有鍵が危殆化した場合の手続** 認証局私有鍵が危殆化した場合は、予め定められた計画に基づいて認証業務を停止し、次の手続を行う。 ・ホストマスタ証明書、サーバ証明書等の失効手続 ・認証局私有鍵の廃棄及び再生成手続 ・ホストマスタ証明書、サーバ証明書等の再発行手続 また、証明書所有者の私有鍵が危殆化した場合は、本 CP/CPS「4.9.」において定める手続に基づき、証明書の失効手続を行う。
5.8.認証局又は登録局の終了 JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ及びアーカイブデータ等の保管組織及び開示方法を業務終了 14 日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。	**5.8.認証局又は登録局の終了** JPNIC において本認証局の認証業務の終了が決定した場合は、業務終了の事実、並びに業務終了後の本認証局のバックアップデータ及びアーカイブデータ等の保管組織及び開示方法を業務終了（日は決定後に記述される）日前までに証明書所有者及び証明書検証者に告知し、所定の業務終了手続を行う。
6.1.1.鍵ペアの生成 本認証局の鍵ペアの生成は鍵管理者立会いのもと、	**6.1.1.鍵ペアの生成** 本認証局の鍵ペアの生成は鍵管理者立会いのもと、

複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、FIPS140-1 レベル 3 の暗号化モジュールを使用して行われる。 メンバ管理者証明書の鍵ペアの生成は、FIPS140-2 レベル 3 の暗号化モジュールを使用して行われる。	複数人の CAO によって認証設備室内で行われる。本認証局の鍵ペアの生成は、安全性の高い暗号化モジュールを含むソフトウェアを使用して行われる。 （追加）
6.1.2.所有者に対する私有鍵の交付 メンバ管理者証明書の鍵ペアの生成は、本認証局において暗号化モジュール内で行われる。生成された鍵ペアは暗号化モジュールを含むハードウェアトークンを使って、メンバ管理者証明書の申請者に交付される。 本認証局はホストマスタ証明書の鍵ペアの作成を行わないため、本項の規定を行わない。	**6.1.2.所有者に対する私有鍵の交付** （追加） 本認証局は EE 鍵ペアの作成を行わないため、本項の規定を行わない。
6.1.3.証明書発行者に対する公開鍵の交付 ホストマスタ証明書の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルを本認証局へ送付することで行われる。	**6.1.3.証明書発行者に対する公開鍵の交付** EE の公開鍵の本認証局への送付は、暗号化された通信下で、PKCS#10 形式のファイルを本認証局へ送付することで行われる。
6.1.4.検証者に対する認証局の公開鍵の交付 本認証局の証明書の配布は、次の 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。 ・（URI は決定後に記述される）にて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。証明書検証者は（URI は決定後に記述される）より本認証局の証明書をダウンロードして使用することとする。証明書検証者はダウンロードした本認証局の証明書のフィンガープリントと（URI は決定後に記述される）にて公開されているフィンガープリントを比較し、一致していることを確認する。 ・サーバ証明書の管理者には RAO が、ホストマスタにはメンバ管理者が本認証局の証明書を手渡しする。	**6.1.4.検証者に対する認証局の公開鍵の交付** 本認証局の証明書の配布は、次にあげる 2 つの方法のうち EE に応じてどちらかより適切な方法を使用して行う。 ・JPNIC 認証局は（URI は決定後に記述される）にて本認証局の証明書を公開する。本認証局の証明書の公開には暗号機能を持つセキュアなプロトコルを使用し、改ざん防止措置をとる。証明書検証者は（URI は決定後に記述される）より本認証局の証明書をダウンロードして使用することとする。証明書検証者はダウンロードした本認証局の証明書のフィンガープリントと（URI は決定後に記述される）にて公開されているフィンガープリントを比較し、一致していることを確認する。 ・サーバ証明書の管理者には RAO が、ホストマスタには LRA 管理者が本認証局の証明書を手渡しする。
6.1.7.鍵用途の目的 本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書、サーバ証明書及び CRL の発行にのみ使用する。 ホストマスタ証明書の keyUsage は digitalSignature、keyEncipherment、dataencipherment のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用す	**6.1.7.鍵用途の目的** 本認証局の証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。本認証局の私有鍵は EE 証明書（追加）及び CRL の発行にのみ使用する。 ホストマスタ証明書の keyUsage は digitalSignature、keyEncipherment（追加）のビットを使用する。S/MIME、SSL/TLS のクライアント証明書としてのみ使用するものとする。

るものとする。	
6.2.7.暗号モジュールへの私有鍵の格納 本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。 ホストマスタの私有鍵はホストマスタ自身が私有鍵の生成を行い、ホストマスタ自身で格納を行う。メンバ管理者の秘密鍵は JPNIC において、安全性の高い暗号化モジュール内で生成、格納される。ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。	**6.2.7.暗号モジュールへの私有鍵の格納** 本認証局の私有鍵は、安全性の高い暗号化モジュール内で生成、格納される。 EE の私有鍵は EE 自身が私有鍵の生成を行い、EE 自身で格納を行う。（追加） ただし、サーバにおいてはサーバ証明書の管理者が格納を行う。
6.2.10.私有鍵の破棄方法 本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者と複数名の CAO によって、私有鍵の格納されたハードディスクを完全に初期化又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続によって破棄する。 EE の私有鍵は、EE 自身で確実に破棄するものとする。メンバ管理者の秘密鍵は基本的に JPNIC において破棄するものとする。ただし、紛失等の場合はこの限りではない。	**6.2.10.私有鍵の破棄方法** 本認証局の私有鍵を破棄しなければならない状況の場合は、鍵管理者と複数名の CAO によって、私有鍵の格納されたハードディスクを完全に初期化又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続によって破棄する。 EE の私有鍵は、EE 自身で確実に破棄するものとする。（追加）
6.3.1.公開鍵のアーカイブ 本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。 （削除）	**6.3.1.公開鍵のアーカイブ** 本認証局は、本認証局の証明書及び本認証局によって発行される全ての証明書のバックアップを行う。 バックアップデータは改ざん防止のため暗号化して保管される。
7.1.2.3.keyUsage ホストマスタ証明書は digitalSignature、keyEncipherment、dataEncipherment を試用する。 サーバ証明書は digitalSignature と keyEncipherment のみを使用する。この拡張は non-critical である。	**7.1.2.3.keyUsage** ホストマスタ証明書、サーバ証明書共に digitalSignature と keyEncipherment のみを使用する。この拡張は critical である。
7.1.6.証明書ポリシ OID ホストマスタ証明書、メンバ管理者証明書、サーバ証明書のいずれも本 CPS「1.2.文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。	**7.1.6.証明書ポリシ OID** ホストマスタ証明書、（追加）サーバ証明書共に本 CP/CPS「1.2.文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。
7.1.9.critical な証明書 certificatePolicies 拡張の処理 表 7-1 JPNIC 資源管理認証局が発行する証明書プロファイル ・keyUsage…n (Field 追加)	**7.1.9.critical な証明書 certificatePolicies 拡張の処理** 表 7-1JPNIC IP アドレス認証局が発行する証明書プロファイル ・ keyUsage…c data Encipherment　ホストマスタ証明書 1 サーバ証明書　0

※2　C=JP, O=（組織名称）, O=Resource Holder, O=LIR Corporate Administrator, OU=（LIR Corporate Administrator、LIR Administrator、LIR Hostmaster のいずれか）, OU=（JPNIC が資源管理の単位ごとに割り当てるメンテナーコード）CN=（LIR-CO、LIR-AD、LIR-HM のいずれか）＋（JPNIC がユーザごとに割り当てる認証 ID）＋（証明書発行対象ホストマスタの名称をアルファベット表記したもの）	※ 2　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=Resource Holder, OU=（JPNIC が LRA 組織に一意に割り当てる ID）（LRA 組織名称）, CN=（証明書発行対象ホストマスタの氏名をアルファベット表記したもの）+ serialNumber=（LRA 組織ごとに一意に管理される ID）
7.3.1.バージョン情報 使用しない。	（新設）
7.3.2.OCSP 拡張 使用しない。	（新設）
8.1.評価の頻度又は評価が行われる場合 本認証局は必要に応じて監査を実施する。	**8.1.評価の頻度又は評価が行われる場合** 本認証局を含む JPNIC 認証局は、毎年一回以上、認証局運用についての準拠性監査を実施する。また、必要に応じて、不定期な監査を実施する。
8.3.評価人と評価されるエンティティとの関係 JPNIC は、本認証局の認証業務に関わる要員以外から監査者を選定する。	**8.3.評価人と評価されるエンティティとの関係** JPNIC は、本認証局を含む JPNIC 認証局の認証業務に係わる要員以外から監査者を選定する。
8.4.評価で扱われる事項 本認証局の準拠性監査は、認証局の運営が本 CPS 及び関連する規定を遵守して運営されているかを監査するものである。 （削除） また、運営委員会が必要と認めた場合、運営委員会が指定する監査目的による監査を実施する。 なお、JPNIC は LRA の監査を行う権利を有する。	**8.4.評価で扱われる事項** 本認証局を含む JPNIC 認証局の準拠性監査は、認証局の運営が本 CP/CPS 及び関連する規定を遵守して運営されているかを監査するものである。 主な監査項目は次のとおりである。 ・認証局の業務担当者の業務運用 ・認証局私有鍵の管理 ・証明書のライフサイクル管理 ・ソフトウェア、ハードウェア、ネットワーク ・物理的環境及び設備 ・セキュリティ技術の最新動向への対応 ・規定等の妥当性評価 また、運営委員会が必要と認めた場合、運営委員会が指定する監査目的による監査を実施する。 なお、JPNIC は LRA の監査を行う権利を有する。
9.2.財務的責任 規定しない。	**9.2.財務的責任** JPNIC は本 CP/CPS に規定した内容を遵守して認証業務を提供し、認証局私有鍵の信頼性を含む認証業務の信頼性の確保を保証する。JPNIC がこの保証に違反して損害賠償を負う場合には、IP アドレス管理指定事業者等との契約における該当条項に従う。
9.3.3.秘密情報を保護する責任	**9.3.3.秘密情報を保護する責任**

本認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を開示することができる。また、本認証局で取扱う情報に関して、調停、訴訟、仲裁、その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。更に、本認証局では、メンバ管理者から、メンバ管理者の管理する証明書所有者に関連する情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、メンバ管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、メンバ管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。	本認証局を含む JPNIC 認証局で取扱う情報に関して、捜査機関、裁判所その他法的権限に基づいて情報を開示するように請求があった場合、JPNIC は法の定めに従って法執行機関へ情報を開示することができる。また、本認証局を含む JPNIC 認証局で取扱う情報に関して、調停、訴訟、仲裁、その他の法的、裁判上又は行政手続の過程において、裁判所、弁護士、その他の法律上の権限を有する者から任意の開示要求があった場合、当該要求情報に関し開示することができる。更に、本認証局では、LRA 管理者から、LRA 管理者の管理する証明書所有者に関連する情報について、権利、利益を侵害又は侵害するおそれがあるとの申出を受けた場合、LRA 管理者の本人確認及び開示要求の対象情報との関連を確認のうえ、LRA 管理者から受領した証明書所有者に関する情報及び証明書記載情報を開示することができる。
9.4.2.プライバシとして扱われる情報 規定しない。	（新設）
9.4.3.プライバシとはみなされない情報 規定しない。	（新設）
9.4.4.個人情報を保護する責任 JPNIC 認証局は、本 CPS「9.4.1.プライバシポリシ」に則って個人情報を保護する責任を負う。	（新設）
9.4.5.個人情報の使用に関する個人への通知及び承諾 規定しない。	（新設）
9.4.6.司法手続又は行政手続に基づく公開 規定しない。	（新設）
9.4.7.他の情報公開の場合 規定しない。	（新設）
9.6.1.発行局の表明保証 JPNIC 発行局は、JPNIC 発行局の業務を遂行するにあたり次の義務を負う。 ・JPNIC 発行局の証明書署名鍵のセキュアな生成・管理 (削除) ・JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理 ・JPNIC 発行局のシステム稼動の監視・運用	**9.6.1.発行局の表明保証** JPNIC 発行局は、JPNIC 発行局の業務を遂行するにあたり次の義務を負う。 ・JPNIC 発行局の証明書署名鍵のセキュアな生成・管理 ・（本 CP/CPS、証明書所有者同意書、証明書検証者同意書、JPNIC ルート認証局の自己署名証明書・自己発行証明書、CRL）の値を（SHA-1（仮のアルゴリズム））で変換した値の公開 ・JPNIC 登録局からの申請に基づいた証明書の正確な発行・失効管理 ・JPNIC 発行局のシステム稼動の監視・運用

・CRL の発行・公表 ・リポジトリの維持管理 （削除） ・本 CPS に従った受付時間内の問合せ受付	・CRL の発行・公表 ・リポジトリの維持管理 ・JPNIC の判断によって EE 証明書を失効させた場合の当該証明書の所有者への通知 ・本 CP/CPS に従った受付時間内の問合せ受付
9.6.3.ローカル登録局の表明保証 LRA は、LRA 業務を遂行するにあたり次の義務を負う。 ・（削除）証明書所有者と証明書申請者が同一であることの検証	**9.6.3.ローカル登録局の表明保証** LRA は、LRA 業務を遂行するにあたり次の義務を負う。 ・申請書類上の証明書所有者と証明書申請者が同一であることの検証
9.12.2 通知方法及び期間 本認証局は、変更された CPS をその改訂が有効になる 10 営業日前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知を行うものとする。	**9.12.2.通知方法及び期間** 本認証局は、変更された CP/CPS をその改訂が有効になる（期間は決定後に記述される）前までに、変更履歴とともにリポジトリに公開することにより、証明書所有者及び関係者に改訂の通知を行うものとする。
9.17.その他の条項 規定しない。	（新設）