経済産業省委託調査

IP アドレス認証局の
マネジメントに関する
調査報告書

2004 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

平成 15 年度 情報セキュリティ基盤整備
IP アドレス認証局のマネジメントに関する調査研究　概要

背景と目的

IP アドレスはインターネットに接続する際に必ず必要になるアドレスである。世界各国で使われる IP アドレスはアドレス資源として位置づけられ、ICANN/IANA を頂点とするインターネットレジストリ（以下、レジストリと呼ぶ）によって割り振り業務が行われている。その際、レジストリは利用されているアドレス資源と利用組織を登録し、連絡先などを適宜公開することでネットワークの自律的な運用を支えている。従って、レジストリの保持する登録情報はインターネットにおける台帳の意味を持つ。

前年度に実施した IP アドレス認証局に関する調査研究から、アドレス資源管理と公開鍵基盤（PKI：Public Key Infrastructure）を利用した登録情報の保護および活用（電子証明書の利用）が有効であることが判明した。これはアドレス資源の登録管理を行うレジストリが認証局を運用し、アドレス資源の利用に関して電子的に検証可能な登録情報を持つことで、インターネットにおける基盤的な認証基盤の構築が可能なためである。国際的にアドレス資源管理を行っている APNIC（Asia Pacific Network Information Centre）や RIPE NCC（Réseaux IP Européens Network Coordination Centre）でも認証局を利用した登録情報の保護機能を実現する為の取り組みが進められ、既に運用が開始されている。どちらのシステムもその有効性が評価されており、特に昨年度から今年度にわたって機能拡張や技術開発の動きが見られている。

これらの状況を鑑み、本調査研究は、日本におけるアドレス資源の登録機関である JPNIC において認証局の構築を行い、アドレス資源の利用に関する登録情報の保護と活用の検討を行うものである。この調査研究は下記の柱を軸に実施される予定である。

- レジストリにおいて認証局を運用することにより、アドレス資源に関する登録情報の確実性を高める。
- 登録情報の確実性に基づいた証明書を発行することにより、インターネットを利用するアプリケーションにおいて応用可能な認証基盤の基礎を作る。

前者は、認証局における認証業務の構築を通じて登録情報の保護を行い、アドレス資源管理の確実性の向上を図る。後者は、アドレス資源管理の確実性に基づく証明書の利用とネットワークへの応用性について検討を行う。

実施内容

前述の通り、登録情報の保護に関してはAPNICやRIPE NCCにおいても検討が行われているが、これらはJPNICが目標としている強固な認証基盤とは異なり、CP/CPSの策定を伴うような認証業務については世界のレジストリにおいて前例がない。従って、認証業務の要件、方針といった検討から始め、認証業務の検討に繋げるという実施方法を取る。平成15年度までの活動内容を図 a に示す。

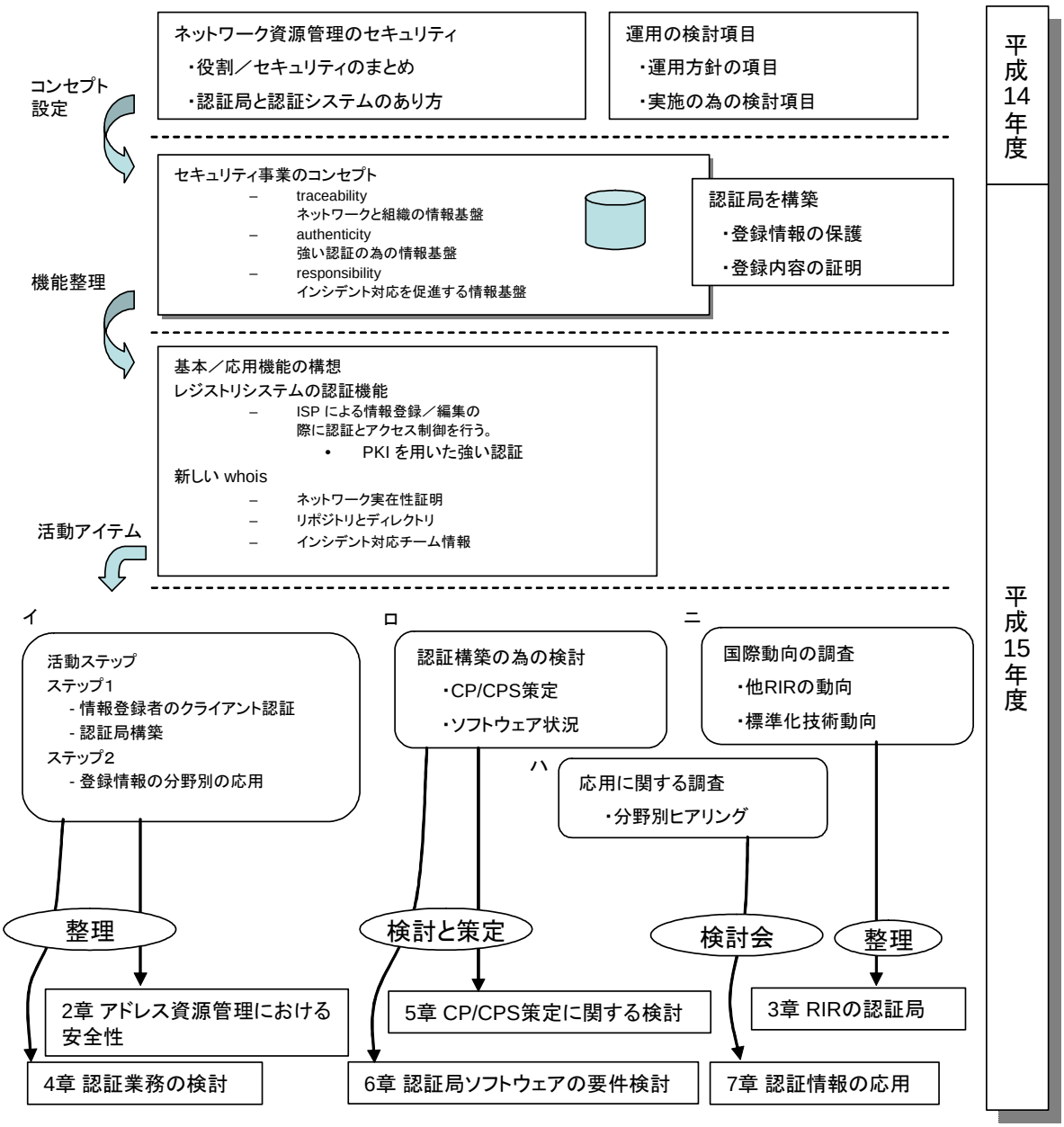


図 a　活動内容と本報告書の関連

はじめにインターネットにおける、認証技術利用の観点から、認証基盤の事業の考え方をまとめる。これが、traceability（ネットワークと組織の情報基盤）、authenticity（強い認証の為の情報基盤）、responsibility（インシデント対応を促進する情報基盤）の 3 つである。同時に、強い認証基盤と認証局の運用に関する調査研究を進め、JPNIC における認証局の機能を整理する。この認証機能実現のための構築／マネジメントのための検討活動をイ、ロ、ハ、ニのアイテムに分ける。これらは平成 15 年度に実施され、その後、開発・運用体制の確立・応用アプリケーションの検討などに繋げていく。

活動アイテム（イ）では、アドレス資源管理における安全性に関する調査を行い、レジストリにおける認証業務の検討を行う。この段階で業務モデルを設計する。これらの検討については報告書の 2 章と 4 章にまとめる。（イ）の調査および検討の結果を基に認証業務の為の検討（ロ）を行う。（ロ）では運用の要素（役割）と技術（ソフトウェア）の要素に分けて検討を進める。運用の要素は、（ロ）の認証業務規程（CP/CPS）の策定に反映し、技術の要素は認証局ソフトウェアの要件の検討を通じて行う。これらは報告書の 5 章と 6 章にまとめる。

これらの検討に並行して、RIR の認証局の動向調査および標準化技術の動向調査（ニ）を実施し、RIR における認証技術の利用や将来的な連携可能性等についての情報収集を行っておく。これは報告書の 3 章にまとめる。

更に JPNIC 認証局の持つ認証情報を応用するネットワークアプリケーションについての調査研究を行う（ハ）。これは各種ネットワーク利用分野（家電メーカー、グループウェアベンダ、通信事業者など）の専門家にヒアリングを行った上で、検討会を通じた意見交換を行いアイディアの集約を行う。その後は、集約されたアイディアを基に実現方法と課題の解決方法について検討を行っていく。

これらの検討を通じて、アドレス資源の登録業務を行う国内のレジストリ（JPNIC）による、強固な認証基盤の構築と、RIR との協調（認証基盤の国際化）、ネットワークを使うアプリケーションのための認証機能の基盤作りを進めていく。

調査結果

- アドレス資源管理における安全性の調査

  レジストリにおけるアドレス資源管理と登録管理業務の安全性について調査した。登録管理業務の安全性は登録データの安全性に依存しており、登録データの不正利用におけるリスクを検討すると、レジストリのシステムには登録時の強力な認証機能が必要であることが判明した。この認証機能は、アドレス資源管理の構造に則ってアドレス資源の割り振りを受けた組織によって利用される。更に電子署名を使ったデータ認証を行う仕組みができれば RIR との連携の際の安全性を向上させることが可能であり、世界規模の証明の基盤が構築可能であることも示された。

- 認証業務の為の検討調査

  CP/CPS の策定の為に、認証業務の検討、認証モデルの構築などを行なった。レジストリにおける担当者の権限管理に合わせ、様々な要因を検討した。認証業務の検討には、RFC3280 などのフレームワークが存在するが、業務モデルの構築と役割の検討を基に多数の資料を用意し、適切な業務負荷と運用を導いた。この検討資料は、他の認証業務の検討の場合にも参考情報になりうる内容を含んでいるため、できる限り多くの資料を報告書にまとめた。

- 国際動向（RIR の認証局と標準化技術）の調査

  RIR（Regional Internet Registry：地域インターネットレジストリ）の APNIC や RIPE NCC では既に認証局を構築し、ユーザ認証の為の証明書の発行を行なっている。ユーザ認証は主に Web サービスで利用され、資源管理機能の実現を目標に活動が行われている。認証局の運用形態は、スタンドアローンで認証局証明書はユーザが各自で組み込む形態である。

  一方、APNIC および RIPE NCC の技術担当者の間では、電子署名を用いた認証基盤の構築に関してもアイディアが議論されていた。

  また IETF においてレジストリにおける登録情報の扱いに関連したプロトコル（CRISP と EPP）の策定が進んでいる。

  これらのことから IP アドレス認証局は、まず登録者の認証機能を実現し、次に電子署名の仕組みを構築した上で RIR との連携を図ることでインターネット全体のアドレス資源管理に則った認証基盤の構築が可能であることが考察された。ただし、CP/CPS を策定し運用レベルの高い業務を構築することで、インターネットにおける基盤的な認証局の構築が可能と考えられる。

- 認証情報の応用に関する調査

  認証情報の応用に関しては、アドレス資源と属性情報の証明という考え方を基本に、様々なアイディアを集約した。アドレスブロックを用いた証明書の発行をはじめ組織属性の検証、地域属性の検証、用途属性の検証など、様々な用途が考えられることが示された。

結論と今後の活動

今年度の調査研究を通じて、レジストリと ISP によるアドレス資源管理の業務体系にあわせた認証業務について調査研究を行った。またアドレス資源の登録情報に属性情報を付加することにより、IP アドレス認証局が安全な IP ネットワークの構築に利用できることが示された。

IP アドレス認証局は、レジストリのアドレス管理業務にともなって運用されることにより、基盤的かつ世界規模の認証基盤となりうる。インターネットにおける認証基盤を構築するにあたり、レジストリのような登録機関がアドレスと実体との対応付けを証明し、また属性情報を付加することで、応用性の高い認証基盤となる。

今後、IP アドレス認証局の構築を進めると共に認証情報を応用するアプリケーションの実現に向けた検討を継続して行う。

本編

はじめに

本調査研究を開始して以来、IP アドレス認証局という名称に関して多くの方から質問を頂いた。IP アドレスで何が認証できるのか、IP アドレス認証とは何か、IP アドレスが個人に割り当てられるのか、他の認証局との関係はどうなのか、といった質問である。調査研究を始めた当初、これらの質問に答えることはできず、議論の材料もほとんどなかった。しかしある専門家との議論をしているときに、これらの質問には、そもそも IP アドレスが何を示すのか、という根本的な疑問が隠れていることに気づいた。技術的な意味を除いて、IP アドレスを使うと現実社会の何を識別することが可能なのか、という事である。

JPNIC において本調査研究を進める動機となっていた考えは、まさにこの点である。表現を変えて書くと「インターネットで使われる IP アドレスのような識別子と、現実社会を結びつけるものはなにか」ということである。インターネットは電子的なデータを届けるネットワークであって、これだけでは通信相手の実体を確認することはできない。通信相手を一意に識別する名前やアドレスは存在するが、それが現実に存在する人や組織とどう結びついているかを認識することはできない。

既存の電話のネットワークの場合、この点は明瞭である。電話番号は契約者に割り当てられており、契約者の実在性は契約時点で確認される。つまり電話番号から実在する人や法人への対応を調べられる。このことはユーザが利便を感じるものではないが、ネットワークの運用には必要となる。過多な利用による不通といった不具合が発見されたときに、電話番号から契約者を調べ問題解決に取り組むことができるのである。ところがインターネットの場合にはこの部分が大きく異なる。はじめに問題の IP アドレスの登録機関（インターネットレジストリ）を調べ、次にネットワーク利用組織（単一の法人とは限らない）を特定し、更にその連絡先を調べる。実際の問題解決はその後に開始される。自律的な管理であるとはいえ、このような状況下では、特に利用者は IP アドレスを現実社会と結びつけて考えることはできない。

しかし今日のようにインターネットが世界各国で利用できるようになったのは、開発・運用・管理といった活動が、一つの国や組織の範囲にとらわれない形態で行われたためであろう。アドレス資源を管理するインターネットレジストリは常に国際的な連携を図り、識別子の一意な割り当てを実施している。更に、IP アドレスを利用するプロバイダの登録を始め、ネットワーク情報の登録、管理責任者の登録を行って、各々のネットワーク利用組織が自律的に運用する為の情報源となっている。調査研究の半ばを過ぎた今の段階では、このインターネットレジストリの機構において認証の機能を持つことが IP アドレス認証局の意義と考えている。本調査研究は、先に述べた、「インターネットにおける識別子と現実社会を結びつけるものは何か」という疑問に答えるために、アドレス資源の管理と認証局に着目したのである。

本報告書は、2003 年度の調査研究「IP アドレス認証局のあり方に関する調査研究」の成果である基本概念に基づき、IP アドレス認証局のマネジメントに関する調査研究をまとめたものである。IP アドレス認証局の運用を検討するにあたり、まずアドレス資源管理における安全性と地域インターネットレジストリの認証局に関する調査を行った。次に IP アドレス認証局の認証業務を検討し認証業務規程の策定を行った。更に認証局のシステム構築を視野に、認証局ソフトウェアの状況調査を行った。また IP アドレス認証局がアドレスの属性を証明する基盤となったときに、どのようなネットワークの応用が考えられるかのアイディア集約を行った。

本報告書はこの調査活動の流れに沿ってまとめられている。各々の活動の各章との関連をまとめると図 i にようになる。

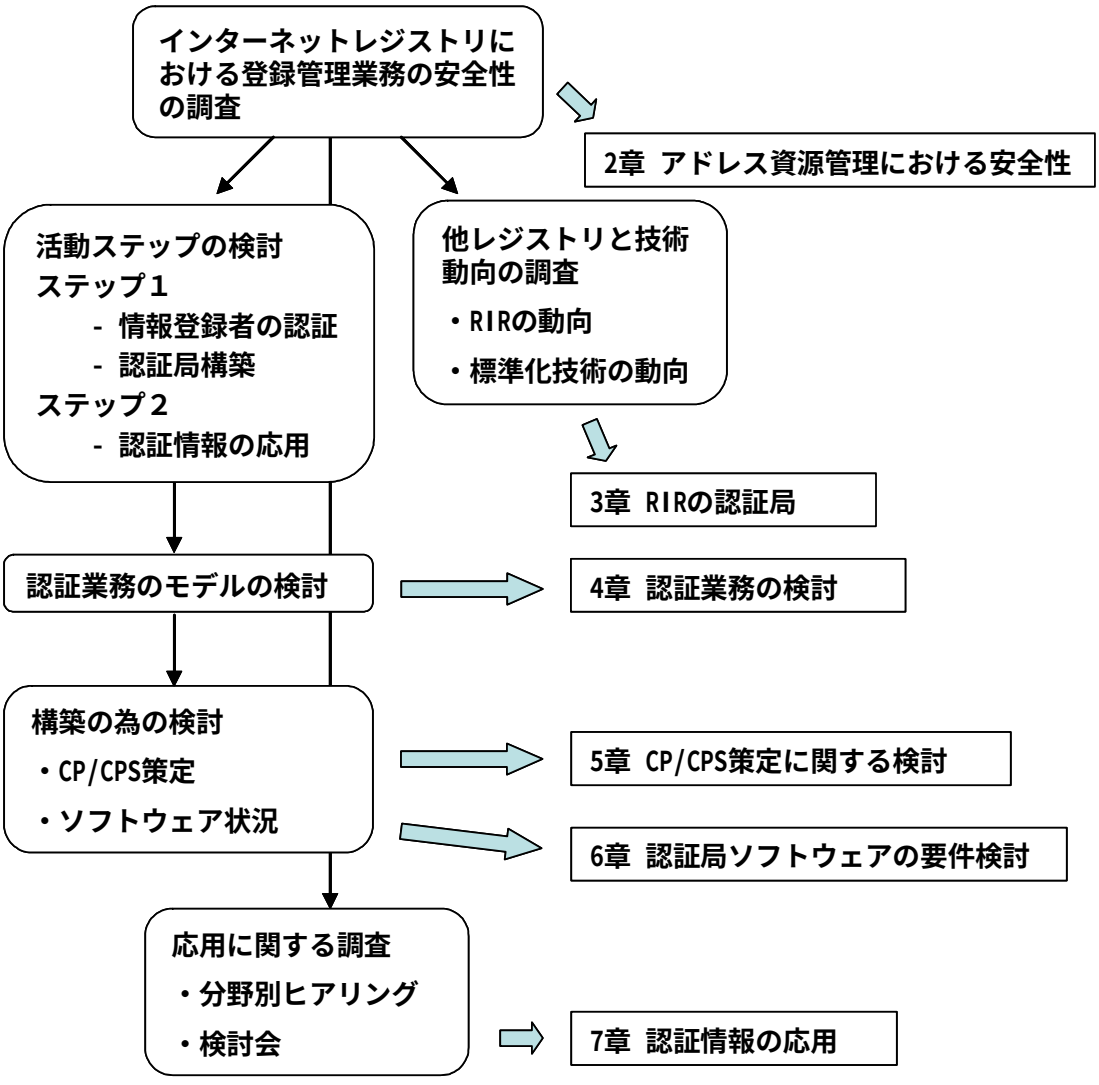


図 i　今年度の活動と各章との関連

第 1 章　IP アドレス認証局のマネジメントに関する調査研究について

内容

- 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

1. IP アドレス認証局のマネジメントに関する調査研究について

本調査研究は、受託研究であると同時に JPNIC における事業の検討であり、確実性を確保したアドレス資源の保護と活用に関する検討を行うプロジェクトである。このプロジェクトの目標大きく分けると二つある。一つはインターネットレジストリにおける認証局とアドレス資源管理の業務を活用した認証業務を構築することである。もう一つは、登録情報の確実性に基づいた証明書を発行し、ネットワークを活用するアプリケーションにおいて利用可能な認証基盤の基礎を作ることである。

本章では、はじめに活動の手順、重点、年度ごとの活動について述べ、次に本報告書の概要をまとめる。

1.1. 今年度の調査研究の位置づけ

本調査研究は、IP アドレス認証局に関するあり方から構築までの一連の活動を網羅する調査研究である。本調査研究の進め方は次のようになる。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、最後に本運用に繋げるという手順である。

IP アドレス認証局をインターネットにおける一つの認証基盤として捉えると、この調査研究の中で重点となるのは、「IP アドレス認証局をどのように運用するか」と「IP アドレス認証局を利用した認証システムはどのようなアプリケーションに適用が可能であるか」の二点だと考えられる。これらに対応する活動は、前者は CP/CPS の策定と RIR（Regional Internet Registry：地域インターネットレジストリ）の動向調査に、後者は技術的要件の調査と応用に関する検討にあたる。したがって今年度は、重点の一つである認証業務の検討と CP/CPS の策定を実施する。また二つ目の重点である応用に関する検討は、今年度から 2004 年度にかけて実施する予定である。

次に、年度ごとの活動内容について述べる。

本調査研究を開始した 2002 年度のテーマは 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 の調査もこの時に開始した。

今年度は 2002 年度の IP アドレス認証局の考え方に基づき、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 CP/CPS の策定、認証情報の応用に関する検討などを行った。

2004 年度は認証局のシステムと運用体制の構築を行い、本運用に向けた各種準備の活動を行う予定である。またこれに並行して応用分野における利用の検討を行い、インターネットにおける認証基盤として技術的な検討を進める予定である。

本報告書の内容を示すに当たり、2002 年度から今年度にかけての調査研究活動を図 1-1 に示す。

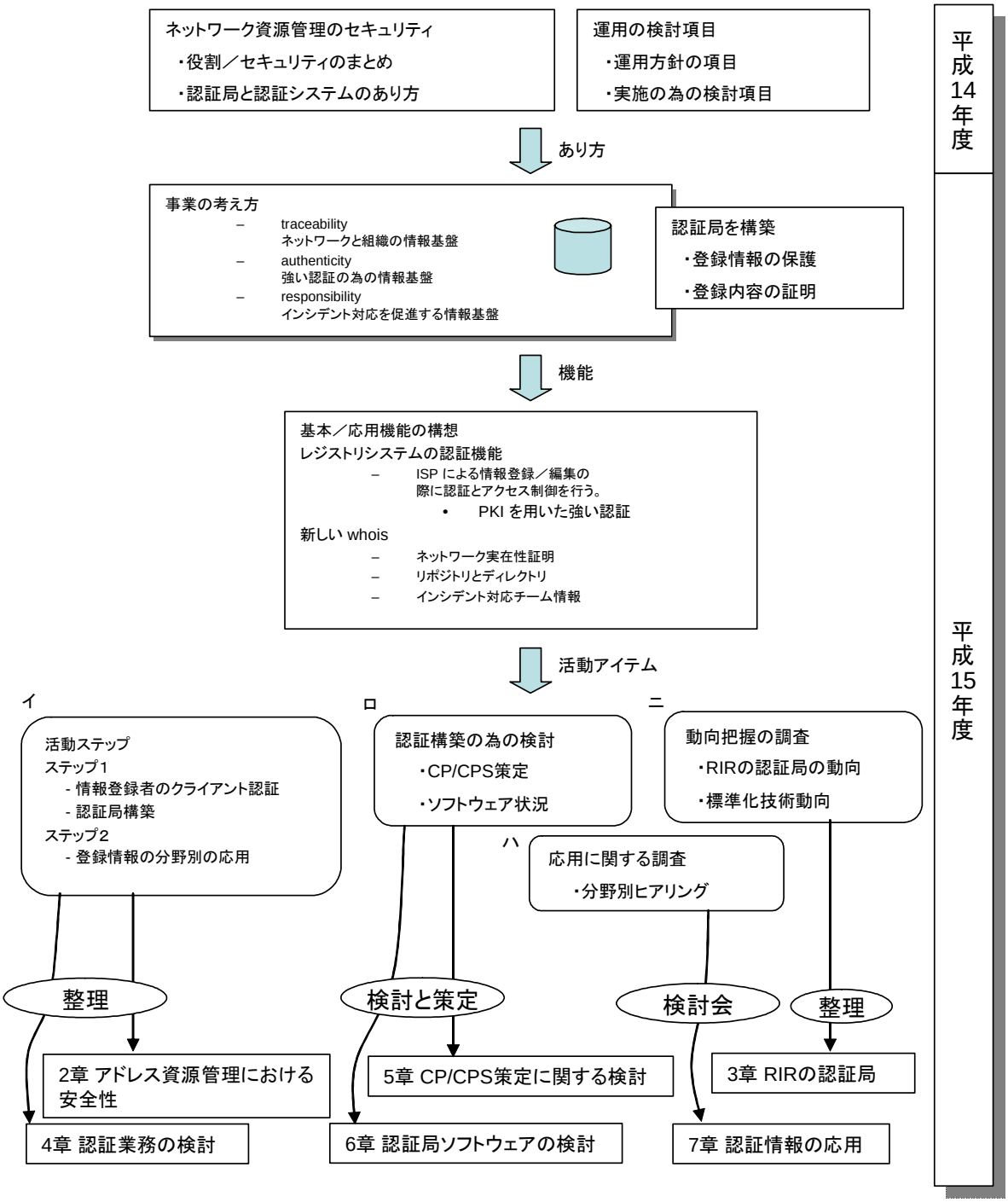


図 1-1　年度とこれまでの活動内容

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、2002 年度の「IP アドレス認証局のあり方に関する調査研究」に引き続き、アドレス資源管理における安全性のあり方から検討を開始し、RIR の状況、技術動向、応用方法など、いくつかに分類される活動が行なわれた。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。

- **アドレス資源管理における安全性の調査**

  インターネットレジストリにおけるアドレス資源管理と登録管理業務の安全性についての調査である。アドレス資源管理はインターネットレジストリ同士の申請／審議といった活動を通じて行われる。このトランザクションの持つリスクと、安全性の機能についての要点を、第 2 章にまとめる。

- **RIR の認証局の動向調査**

  RIR では既に認証局を構築しアドレス資源管理におけるユーザ認証に利用している。RIR における認証局が持つ役割や実施しているサービスを調査するとともに、APNIC、RIPE NCC で今後の展望についてのヒアリングを行なった。この調査結果については第 3 章にまとめる。

- **認証業務の検討**

  インターネットレジストリにおける認証局を構築するには、登録管理業務の業態にあった認証業務を想定して検討を行なう必要がある。本調査研究では、アドレス資源管理の形態を元に業務概念図を作成した。業務概念図の作成にあたり、認証対象の扱いをはじめ認証局の挙動を含めた業務概念の検討を行った。この業務概念図は認証局運用規程の策定と、認証局のシステム検討に使われる。

  本報告書では、この検討を下記のようにまとめた。

  - アドレス資源管理における認証基盤

    アドレス資源管理における認証の目標とする姿と、実現の手順について述べる。

  - 認証業務のテーマ

    認証業務の概念決定の際に、今後の業務を見据えた留意事項（テーマ）について述べる。

  - 業務概念図の作成

    認証業務の概念をモデル化し、図示する。このモデル図を元に各担当者の役割や、認証局のシステムに必要となる機能を導き出す。

  これらの検討内容ついては第 4 章で述べる。

- **IP アドレス認証局の CP/CPS（認証業務規定）策定の為の検討**

  信頼性の高い強固な認証局を運用するには、高いセキュリティレベルの認証業務を行う必要がある。高いセキュリティレベルの認証業務にはどのような要素があるかについては 2002 年度に調査を行っており、認証局監査の監査基準の比較を行っている。今年度の調査研究ではこれらの資料を元に、認証局業務規程の策定を行った。

  認証局業務規程の策定には、基本方針から設備に至る多くの事項について検討を行う必要があった。各々の検討について検討資料を交えて解説すると共に、今回対象とした認証業務の案（記述案）を結論として述べる。この検討については第 5 章にまとめる。また策定された認証局業務規定（ドラフト版）を Appendix として添付する。

- **認証局のシステムの検討**

  認証業務の遂行にあたって運用される認証局のシステムに関する検討を行った。実際に認証局ソフトウェアを使って、前述の認証局運用規程に従った証明書を発行したり、運用環境を想定した証明書の利用を行ったりした。この実験環境ではディレクトリサーバの運用等の技術的検証も行った。

  また認証局ソフトウェアのベンダから評価版等を利用させて頂き、認証局ソフトウェアの利用形態や認証業務との関連性について調査した。第 6 章では、認証局ソフトウェアの導入検討に役立つと思われる事項をまとめる。

- **認証情報の応用**

  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。そこで、開発が進みつつあるネットワーク利用機器の業界の方々にヒアリングを行った。ヒアリング先は、家電業界、移動体通信の業界、医療、ネットワーク(インターネット)、タグ、グループウェア等、多岐に渡り、様々な意見を頂くことができた。また JPNIC において検討会を行い、意見交換を行った。

  これらの活動の結果、分野や規模が多岐に渡る応用のアイディアが上がってきた。第 7 章では、応用の可能性と JPNIC の業務との関連性を述べると共に、上がってきたアイディアを分類し、概要を述べる。

第 2 章　アドレス資源管理における安全性

内容

- アドレス資源管理におけるセキュリティ
  - JPNIC におけるアドレス資源管理の仕組み
  - レジストリデータの保護

2. アドレス資源管理における安全性

2.1. アドレス資源管理におけるセキュリティ

JPNIC のようなインターネットレジストリはアドレス資源管理と呼ばれる業務を行なっている。アドレス資源管理とは、アドレス資源を利用する組織を登録し、アドレス資源の割り振りに関する情報管理を通じて、アドレス資源の健全な利用を図る業務である。

本節では、まずアドレス資源管理に利用されているレジストリデータ（登録情報）について認証と管理権限の観点で述べる。次に申請業務におけるリスクについて述べ、業務データの保護の必要性について述べる。業務データの保護については、アジア太平洋地域の地域インターネットレジストリである APNIC やヨーロッパ地域の地域インターネットレジストリである RIPE NCC で活用されている仕組みについても言及する。

2.1.1. レジストリデータとは

有限であるアドレス資源の割り振り／割り当てを効率的に行なうためには、アドレスがどのように分割されているのかを把握している必要がある。また、アドレスブロックの使用率を調べる、使用されていないアドレスを回収するなどを行なうために、アドレスブロックの使用者は誰かを知る必要がある。

このようなアドレス資源の管理を行なうために維持管理すべきデータは、インターネットレジストリのリポジトリに収められている。このデータをレジストリデータと呼ぶ。レジストリデータには様々なものが存在するが、ここでは四つのデータに着目する。そのデータとは、LIR（Local Internet Registry：ローカルインターネットレジストリ、日本におけるプロバイダを意味する）の情報、ネットワーク情報、AS 情報、割り当て情報である。

2.1.1.1. アドレス資源管理の仕組み

インターネットのアドレス資源管理は、Internet Assigned Numbers Authority（以下、IANA と呼ぶ）機能を実施する非営利法人 Internet Corporation for Assigned Names and Numbers（以下、ICANN と呼ぶ）と、この ICANN／IANA からアドレス資源の割り振りを受けたインターネットレジストリによって行われている。

インターネットレジストリはアドレス資源の割り振り業務の形態に従い、ICANN／IANA を頂点とする木構造を成している。ICANN／IANA は Regional Internet Registry（地域インターネットレジストリ：以下、RIR と呼ぶ）に割り振りを行って

いる。

RIR（Regional Internet Registry：地域インターネットレジストリ）は北米、ラテンアメリカ・カリブ地域、ヨーロッパ地域、アフリカ地域、アジア太平洋地域のそれぞれに存在している。北米にはAmerican Registry for Internet Numbers（以下、ARINと呼ぶ）が、ラテンアメリカ・カリブ地域には Latin America and Caribbean Internet Address Registry（以下、LACNIC と呼ぶ）が、ヨーロッパ地域には Reseaux IP Europeens Network Coordination Centre（以下、RIPE NCC と呼ぶ）が、アフリカ地域には African Network Information Center（以下、AfriNIC）が、アジア太平洋地域の RIR には Asia Pacific Network Information Centre（以下、APNIC）がある。この構造を図 2-1 に示す。

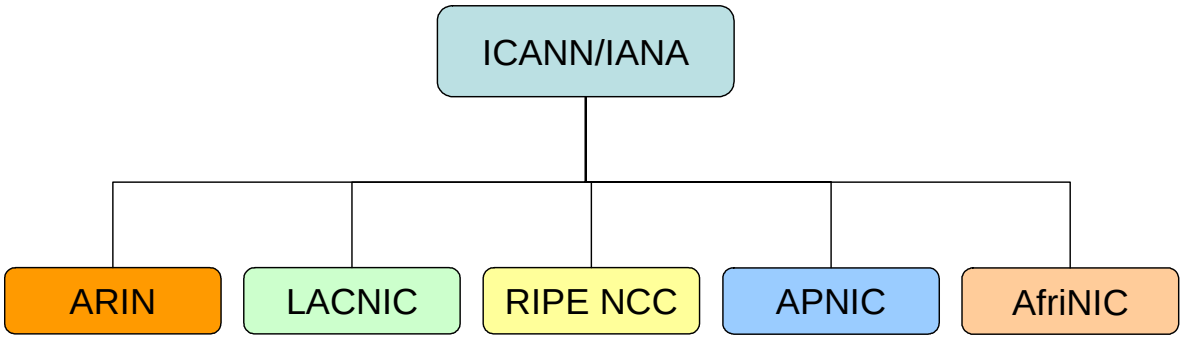


図 2-1 ICANN/IANA と RIR の構造

アドレス資源に関する登録情報は RIR が管理業務を行うが、個々のデータの内容のほとんどは登録主体である LIR などが管理するようになっている。RIR は、NIR や LIR を対象とするメンバーシップ制度を設けており、会費の収入を得ると同時にポリシー策定のための会議を開催したり、教育活動を行ったりしている。

以下で、各 RIR におけるメンバーシップについて述べる。

（1） ARIN におけるメンバーシップ

ARIN では地域内の IP アドレスユーザからの意見を集約する目的でメンバーシップ制度を設けている。ARIN から直接の割り振りを受けている ISP は自動的にメンバーとなる。この場合のメンバーシップ年会費は、更新費用に含まれている。割り振りを受けていない組織または個人の場合には年会費 500 ドルを支払って、申し込みを行う必要がある。この手続きは次の様になる。

（1） 申請フォームに記入する（http://www.arin.net/membership/join.html）
↓
（2）初年度の会費 500 ドルを支払う

メンバーに与えられる権利には次のものがあげられている。

- ARIN のオペレーションについて報告および討議を行うため、年に二度開催される ARIN のメンバー会議への二人分の参加権
- 二年に一度開催される Public Policy Meeting への二人分の参加権（無料分）
- Board of Trustee および Advisory Council メンバーの指名および投票権
- アナウンスおよび討議用メーリングリストへの参加権
- 企業または個人のウェブサイトに ARIN メンバーロゴを表示する権利
- 今後提供されるメンバーシップの享受

（2） RIPE NCC におけるメンバーシップ

RIPE NCC では、アドレス資源を受け取るためには LIR としてメンバーになることが求められる。メンバーは RIPE NCC General Meeting への参加を通じて RIPE NCC の活動とサービスに影響を与えることが出来るとされている。

メンバー加入手続きは次の様になる。

（1） 登録希望者は「RIPE NCC のメンバーとなる手続き[1]」を理解し、記入した申請フォームを new-lir@ripe.net に送信する

↓

（2） RIPE NCC はレジストリファイルを作成し、料金請求書を登録希望者に送付する

↓

（3） 登録希望者は「RIPE NCC におけるローカルインターネットレジストリを構築する手続き」について理解し、契約に合意することを new-lir@ripe.net に送信する

↓

（4） RIPE NCC は構築作業の詳細を登録希望者に電子メールで通知する

[1] Procedure for Becoming a Member of the RIPE NCC（RIPE-257）
http://www.ripe.net/ripe/docs/newlir.html

↓

（5）　登録希望者は「標準 RIPE NCC サービス合意書[2]」の署名済みコピーを提供する

↓

（6）　登録希望者は料金を支払う

↓

（7）　RIPE NCC は、料金と署名済み合意書を受け取った後、登録希望者のサービスレベルが上がったことを通知する

（3） APNIC におけるメンバーシップ

アジア太平洋地域を管理する APNIC では、各国別のアドレス資源管理を National Internet Registry（以下、NIR と呼ぶ）に委譲している。APNIC から割り振り／割り当てを受けている NIR としては、Japan Network Information Center（以下、JPNIC と呼ぶ）、Korean Network Information Center（以下、KRNIC と呼ぶ）、China Internet Network Information Center（以下、CNNIC と呼ぶ）、Taiwan Network Information Center（以下、TWNIC と呼ぶ）、Asosiasi Penyelenggara Jasa Internet Indonesia（以下、APJII と呼ぶ）が存在する。

APNIC ではメンバーに対し、アドレスの割り振り、会議への参加などのサービスを提供している。

メンバーとなる手続きは次のように定められている。

（1）メンバー申込書を申請する

↓

（2）APNIC よりメンバーキットが送られる

↓

（3）メンバーシップ同意書にサインし、メンバー料金を支払う

↓

（4）APNIC は同意書にサインし、コピーを送る

---

[2] The Standard RIPE NCC Service Agreement
http://www.ripe.net/ripe/docs/service-agreement.html

APNIC のメンバーのアドレス資源の割り振り構造を図 2-2 に示す。

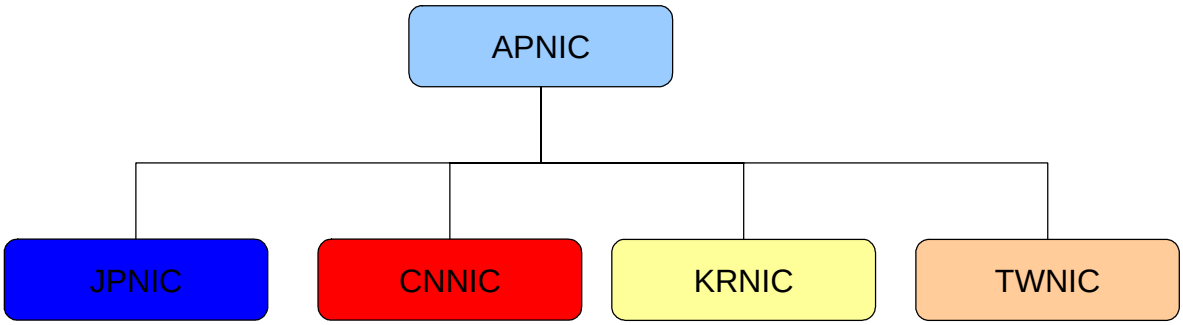


図 2-2 APNIC メンバー

メンバー申し込み申請はウェブから行う（図 2-3）。

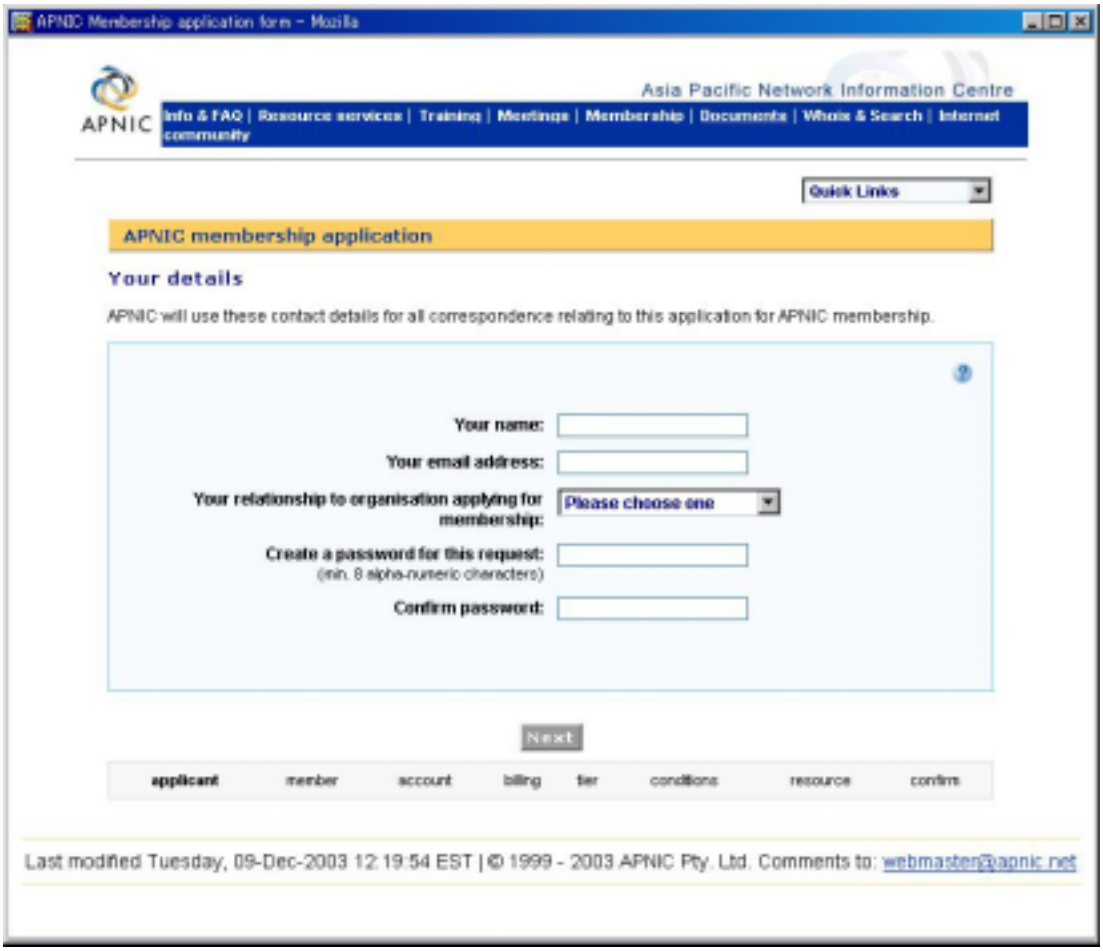


図 2-3 APNIC メンバー申請フォーム

メンバーシップ料金は表 2-1 のように定められている。利用できるアドレス空間の大きさによって年会費が変わる。

表 2-1 APNIC メンバー料金（2004 年 2 月現在）

メンバーシップ	年会費（US$）	IPv4 アドレス空間	IPv6 アドレス空間
Associate	625	None	None
Very small	1,250	/22	/35
Small	2,500	/19 から /22	/32 から /35
Medium	5,000	/16 から /19	/29 から /32
Large	10,000	/13 から /16	/26 から /29
Very large	20,000	/10 から /13	/23 から /26
Extra large	40,000	/10 以上	/23 以上

メンバーの検索フォームが公開されており、Extra large メンバーには、JPNIC、KRNIC、CNNIC、TWNIC など、各国の NIR が登録されている。

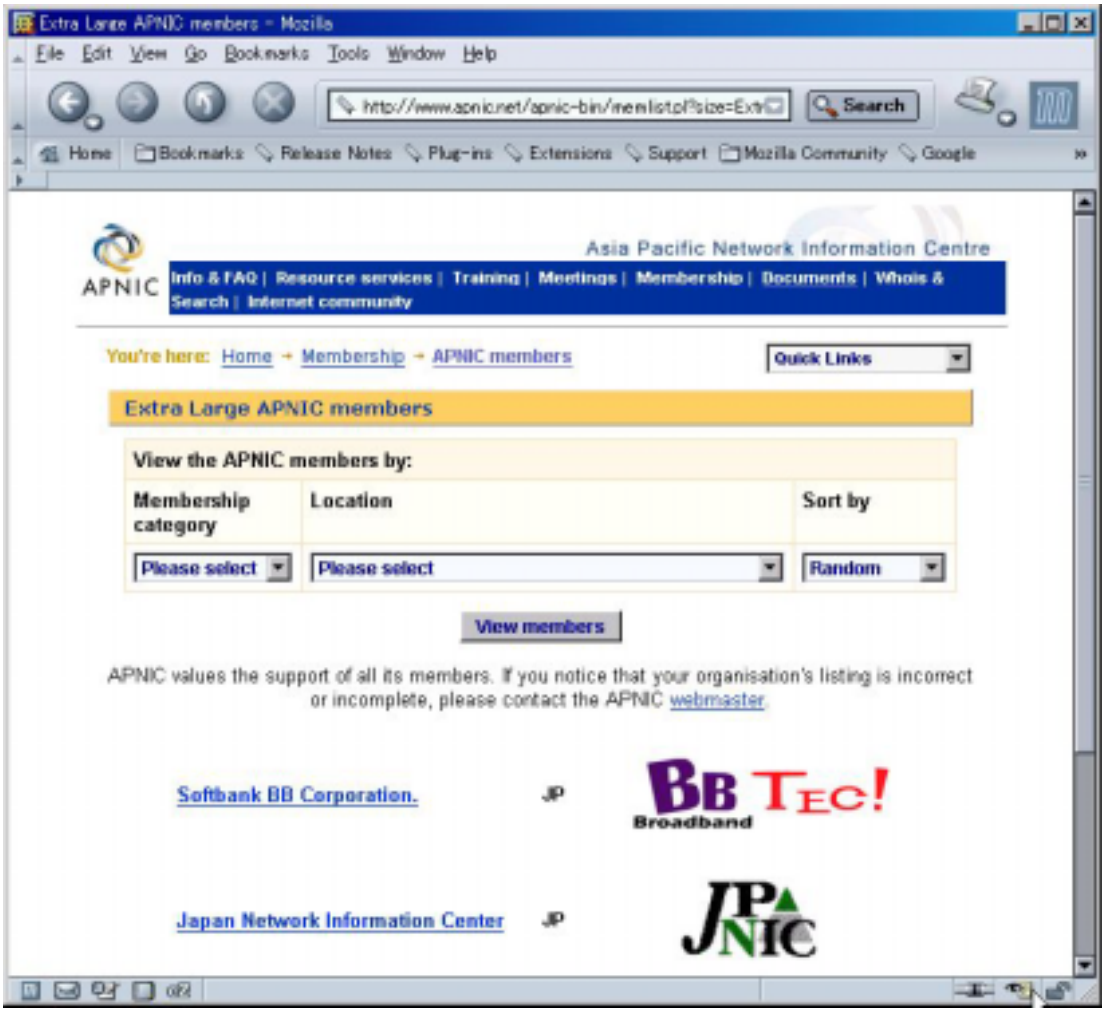


図 2-4 APNIC メンバー検索画面

RIR のメンバーである NIR と LIR は、アドレス資源の管理権限の委譲を受けると共に、そのアドレス資源のサイズに応じた費用を負担する。インターネットレジストリにおける収入は、ポリシー策定、レジストリシステムの運用、審議、教育といった活動費用に当てられ、継続的なアドレス資源の運用の財源に充当される。

インターネットで利用される各種アドレス資源は、論理的識別子であり、管理権限の割り振りによって物品の移動が伴わない。つまりインターネットにおけるアドレス資源の流通は、インターネットレジストリにおける各種手続きによって実現している。インターネットレジストリの活動の本質は、ユーザによる自律的で適切なアドレス資源の利用を目的とした、情報登録および後述する情報公開である。

（4） whois によるデータ公開

レジストリにおけるレジストリデータの公開には whois が用いられる[3]。これはサーバクライアントによる簡易検索を提供するものである。このプロトコルが策定されたのは 1982 年（RFC812 の公開年）のことである。当初は、ARPANET の利用者に関するディレクトリサービスとして、氏名、電話番号、メールアドレスなどを提供していた。

現在では、インターネットレジストリそれぞれが、保有するレジストリデータの公開手法として、whois サーバを運営し、必要に応じて whois クライアントによる問い合わせを受け付けるという方法を採用している。

whois サーバへの問い合わせは、ドメイン及びネットワークに障害が発生した際の連絡先の問い合わせなど、ネットワーク管理上の必要がある場合に行うことになっている。

[3] RFC954 NICNAME/WHOIS
http://www.ietf.org/rfc/rfc0954.txt?number=954

表 2-2 whois による問い合わせの例

```
% whois -h whois.nic.ad.jp www.nic.ad.jp

[ JPNIC & JPRS database provides information on network administration. Its   ]
[ use is restricted to network administration purposes. For further infor-    ]
[ mation, use 'whois -h whois.nic.ad.jp help'. To suppress Japanese output,   ]
[ add'/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.       ]

Domain Information: [ドメイン情報]
a. [ドメイン名]                NIC.AD.JP
e. [そしきめい]                しゃだんほうじん にほんねっとわーくいんふぉめーしょんせんたー
f. [組織名]                    社団法人 日本ネットワークインフォメーションセンター
＜省略＞
```

（5） JPNIC 割り振りの申請、審議、登録、情報公開

自組織のネットワークをインターネットに接続するためには、ネットワークアドレスの割り当て（assignment）を受ける必要がある。この割り当ては JPNIC から割り当て業務を委託されている IP アドレス管理指定事業者に対して申請を行う。

割り当てに先立って、IP アドレス管理指定事業者は JPNIC から管理するアドレスブロックの割り振り（allocation）を受ける。この管理の委託構造は図 2-5 のように表される。

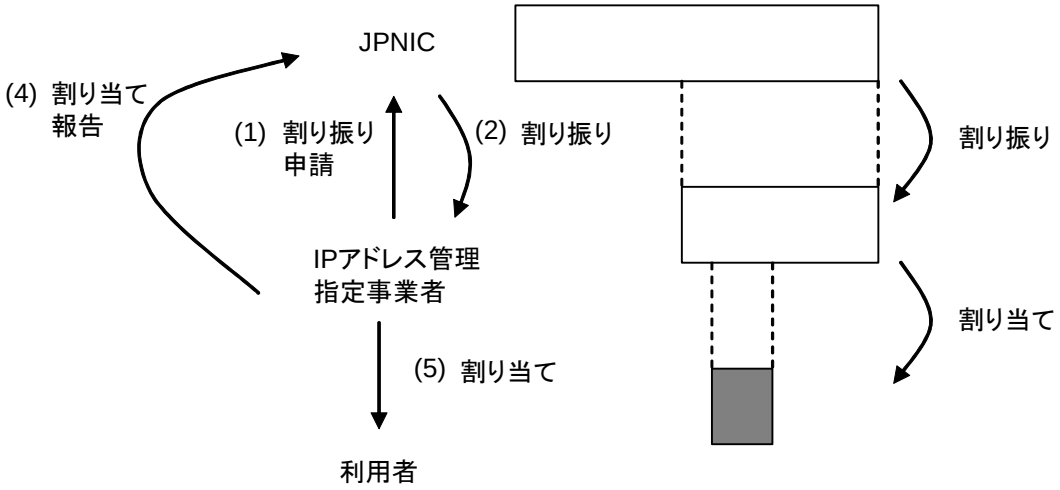


図 2-5 JPNIC における割り振り、割り当て概念図

なお、割り振り、割り当ての定義は表 2-3 のように示される。

表 2-3 割り振り、割り当ての定義

割り振り（Allocation） 　再分配用としてプロバイダ集成可能アドレス空間を IP アドレス管理指定事業者に分配することです。 割り当て（Assignment） 　IP アドレス管理指定事業者が割り振られたアドレス空間の一部または全部を、接続組織のネットワーク利用のために分配することです。また、IP アドレス管理指定事業者が自身のバックボーンネットワークや内部ネットワークとして使うときも割り当てられたアドレス空間と呼びます。 （JPNIC 用語集 http://www.jpnic.jp/ja/tech/glos-wa.html より）

利用者、IP アドレス管理指定事業者、JPNIC の三階層モデルを採用することで管理業務の集約化が図られ、アドレス資源管理の効率化が実現されている。

LIR である IP アドレス管理指定事業者は企業その他法人によって構成され、一般的に ISP（Internet Service Provider：インターネットサービスプロバイダ）と呼ばれる。ISP はインターネットを利用するための各種サービスを提供する。一方、NIR および RIR は、インターネットにおける公共性のあるインフラストラクチャーとして、継続的な運用を推進する役割を持つ。LIR に対するアドレスの割り振りに、審議が行われるのはこのためである。

2.1.1.2. IP アドレス管理指定事業者情報

IP アドレス管理指定事業者とは、IP アドレスの割り当て業務およびそれに付随する業務の一部（以下、IP 割り当て管理業務と呼ぶ）を JPNIC から委託された事業者のことである[4]。

ある組織が IP アドレス管理を行うために IP アドレス管理指定事業者として登録されるには、JPNIC との間に IP アドレス管理指定事業者契約を締結する必要がある。この契約により IP アドレス管理指定事業者となった場合には、IP アドレス管理指定事業者情報がレジストリデータとしてリポジトリに格納され、その一部は公開される。

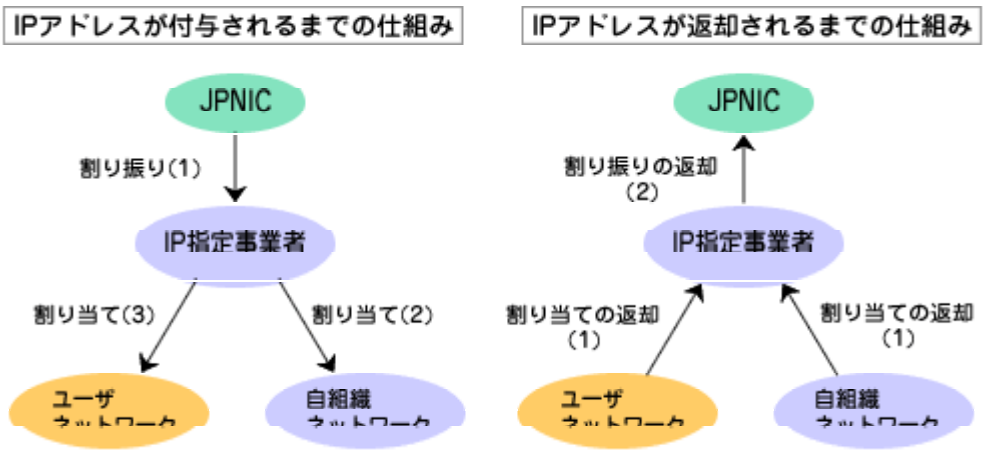


図 2-6 IP アドレス付与／返却の仕組み[5]

公開されるデータを表 2-4 に示す。

[4] IP アドレス管理指定事業者について
http://www.jpnic.jp/ja/ip/member/index.html
[5] IPv4 アドレスの申請
http://www.nic.ad.jp/ja/ip/ipguide.html

表 2-4 IP アドレス管理指定事業者データ

データ項目	概要
指定事業者名	指定事業者の正式名称。JPNIC 会員登録申請の際に登録されたもの。
指定事業者略称	指定事業者を一意に識別するための符号。
管理アドレスブロック	指定事業者が管理しているアドレスブロック
連絡先	電子メールアドレス
住所	一般利用者から指定事業者に関する問合せ等を受けた場合に紹介すべき連絡先
電話番号	同上
ファックス番号	同上

IP 管理指定事業者はインターネットレジストリの管理権限を委譲されているため、インターネットのサービス利用が可能である。RIR と NIR の契約関係と同時に NIR と LIR の契約（登録）関係があることは、アドレス資源の確実性を確保する上で重要である。

インターネットの自律的管理の場面では、アドレスの利用者を特定するために、RIR から NIR、NIR から LIR という風に、それぞれの登録の記録を確認していくことが可能である。

2.1.1.3. ネットワーク情報

JPNIC の技術文書「JPNIC-00820 公開・開示対象情報一覧[6]」によると、ネットワーク情報は次のように定義されている。

> インターネットリソースである IP アドレスを利用しているのがどの組織、 または個人であるかを示すための情報。組織名、または個人名が公開される。 組織、または個人を特定するための住所は、請求により開示される。

公開されるネットワーク情報を表 2-5 に示す。

[6] JPNIC-00820 公開・開示対象情報一覧
http://www.nic.ad.jp/doc/jpnic-00820.html

表 2-5 ネットワーク情報公開データ

データ項目	概要
IP ネットワークアドレス	ネットワークアドレス
ネットワーク名	ネットワークを表す、意味のある任意の文字列
組織名	ネットワークを運用する組織の正式名称
運用責任者	運用に対して責任を負う担当者の JPNIC ハンドル
技術連絡担当者	技術面で責任を負う担当者の JPNIC ハンドル
ネームサーバ	ネットワークアドレスに関するネームサーバ（/24 より大きなアドレスブロックの場合のみ）
通知アドレス	変更登録された場合に通知すべき電子メールアドレス
割り当て年月日	割り当てが行われた年月日
返却年月日	（返却されている場合）返却年月日
最終更新	データが更新された年月日

JPNIC のネットワークアドレスに関して、実際に検索できる情報は表 2-6 のようになる。

表 2-6 JPNIC の公開ネットワーク情報

項目名	データ
a. [IP ネットワークアドレス]	202.12.30.0
b. [ネットワーク名]	JPNICNET
f. [組織名]	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
g. [Organization]	Japan Network Information Center
m. [運用責任者]	SN3603JP
n. [技術連絡担当者]	HK8068JP
n. [技術連絡担当者]	NM050JP
p. [ネームサーバ]	ns1.nic.ad.jp
p. [ネームサーバ]	ns2.nic.ad.jp
y. [通知アドレス]	system@nic.ad.jp
[割当年月日]	1995/11/17
[返却年月日]	
[最終更新]	2002/08/19 13:08:04 (JST)
	koreeda@nic.ad.jp

ネットワーク情報を検索することで、どの IP アドレスがどの団体によって管理されているのか、（公開されてはいない情報ではあるが）どのように使われているのかがわかる。本質的には、インターネットレジストリによる登録情報の維持と連携によって、アドレスの台帳といえるものが世界規模で構成できるはずである。ただし、インター

ネットの黎明期に行われていたインターネットの利用を促進するための利用といった経緯や、現行業務の証明性、または安全上の理由により、一元的な台帳になる状況は考えにくい。アドレス資源の台帳が、どのような性質の情報を保持し、また公開するべきかであるかを定義することは、本調査研究の課題でもある。

2.1.1.4. AS 情報

AS（Autonomous System：自律システム）は、経路制御の上で運用ポリシーを統一することのできるネットワークの範囲のことである。インターネットで経路情報を交換する AS は ASN（AS Number）と呼ばれる識別番号を持っている。ASN は IP アドレスと同様に世界で一意に行われる必要があり、インターネットレジストリが割り当て業務を行っている。ASN の割り当ての際に登録される情報は AS 情報と呼ばれる。

JPNIC の技術文書「JPNIC-00820 公開・開示対象情報一覧」によると、AS 情報は次のように定義されている。

インターネットリソースである AS 番号を利用しているのがどの組織、 または個人であるかを示すための情報。組織名、または個人名が公開される。 組織、または個人を特定するための住所は、請求により開示される。

公開される AS 情報は表 2-7 のようになる。

表 2-7 AS 情報公開データ

データ項目	
AS 番号	
AS 名	AS につける名称
組織名	ネットワークを運用する組織の正式名称
運用責任者	運用に対して責任を負う担当者の JPNIC ハンドル
技術連絡担当者	技術面で責任を負う担当者の JPNIC ハンドル
AS-IN	外部からの経路情報受け入れに関するポリシー
AS-OUT	外部へ広告する経路情報に関するポリシー
通知アドレス	変更登録された場合に通知すべき電子メールアドレス
割り当て年月日	割り当てが行われた年月日
返却年月日	（返却されている場合）返却年月日
最終更新	データが更新された年月日

表 2-8 は whois データベース上で公開される、JPNIC の所有する AS に関する情報である。

表 2-8 JPNIC 公開 AS 情報

データ項目	
a. [AS 番号]	2515
b. [AS 名]	JPNIC
f. [組織名]	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
g. [Organization]	Japan Network Information Center
m. [運用責任者]	SN3603JP
n. [技術連絡担当者]	NM050JP
n. [技術連絡担当者]	HK8068JP
o. [AS-IN]	from AS2500 10 accept ANY
o. [AS-IN]	from AS2497 10 accept ANY
p. [AS-OUT]	to AS2500 announce AS2515
p. [AS-OUT]	to AS2497 announce AS2515
y. [通知アドレス]	system@nic.ad.jp
[割当年月日]	1994/11/21
[返却年月日]	
[最終更新]	2002/08/19 13:08:15 (JST)
	ip-alloc@nic.ad.jp

AS はグローバルインターネットで経路情報を交換する組織の単位である。従って、IP アドレスの割り当てと AS による経路情報の交換に矛盾が生じると、膨大なアドレス資源の不正利用が可能になる。アドレス資源の不正利用は、追跡が不可能な通信ノードの設置を可能にし、広域における通信障害を故意に起こすことが可能な状況を作り出すことがある。

2.1.1.5. 割り当て情報

割り当て情報とは、割り当てられたネットワーク情報である。IP アドレス管理指定事業者が申請者に IP アドレスを割り当てる際には、JPNIC に対して、IP アドレス割り当て報告申請を行う必要が有る。JPNIC では、IP アドレス割り当て報告申請受理後に申請が適正なものであるかの審議を行い、適正であると判断された場合、申請内容をデータベースに記録し、申請を行った IP アドレス管理指定事業者に受理の返答を行う。

これらの情報を元にアドレス資源の管理を行うのがインターネットレジストリである。新たなアドレス資源の割り振りに伴う審議や、ネットワーク情報の公開などの活動は、すべて登録情報に基づいて行われている。すなわち登録情報はアドレス資源管理の元本となる情報である。

2.1.2. レジストリデータの保護

ここでは前節で示されたレジストリデータに関する脅威を明らかにし、保護すべき対象を示す。このために、それぞれのデータについて、発生から利用、消滅の過程を示し、セキュリティ上の問題を明らかにする。

2.1.2.1. 申請業務における認証業務と安全性

レジストリデータは申請とともに発生し、削除申請とともに消滅する。ここでは、申請の概要を示し、安全性の議論を行う。

現状の業務では、データの申請（および更新）は図 2-7 のように行われる。

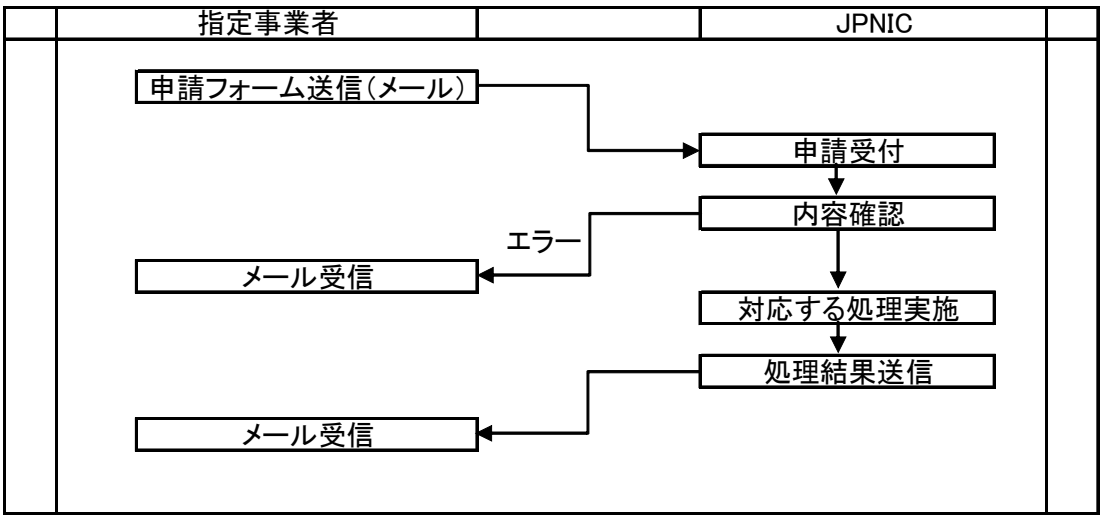


図 2-7 申請処理概要

JPNIC から提供される申請フォーム[7]は電子メールを使って送受信される。電子メールは盗聴や改ざんが可能な情報伝達手段である。保護機能のない電子メールを利用すると、虚偽の申請や不正な申請が行われる恐れがある。そのため JPNIC を含め、多くのインターネットレジストリではパスワードや暗号技術を利用したメールなど、保護機能の実現に取り組んできた。

多くのインターネットレジストリで取られてきた保護機能は authentication（認証）のスキームと呼ばれ、申請者自身が登録した認証情報（パスワードや暗号鍵）を使って当事者であることを確認する手法が使われてきた。しかし暗号の解読技術や巧妙な業務分析の手法が発展するに従って、より強固なユーザ認証方式が必要になってきた。

[7] http://www.jpnic.jp/ja/doc/validity.html 以下に配置されている

ここでいう強固なユーザ認証方式とは、単に暗号強度の高い方式であるだけでなく登録手続きやユーザ管理といった運用の面でも安全性に配慮した方式を意味している。例えば、Web ベースで申請業務を行うことを考えると、HTTPS を用いてクライアント認証を行うことが可能であるが、転送されるメッセージ（つまり申請）が予め登録されたユーザが作り出したものであるという関連付けをアプリケーションで行う必要がある。

電子メールベースの申請業務上で、認証を行うための現実的な手法として、PGP（Pretty Good Privacy[8]）を使ったメッセージ認証、S/MIME を使ったメッセージ認証などがあげられる。実際に RIPE NCC では PGP を使ったメッセージ認証を取り入れている。

RIPE NCC ではデータベースに RPSL（Routing Policy Specification Language）と呼ばれるルーティングポリシー記述言語を用いている。この言語は ARIN,APNIC においても使われており、RIPE NCC が採用している PGP を用いたメッセージ認証は、他組織においても参考となると考えられる。以下に、そのメッセージ認証について説明を行なう。

（1） RIPE NCC における PGP によるデータ保護

RIPE NCC のレジストリ操作は MIME 形式の電子メールを利用して行われる。この際に MIME の各パートに対し、PGP の署名を行い、データベースに登録する。

まず、データの登録を電子メールベースで行う[9]。コンタクト情報の登録作業は次のようになる。

（1） コンタクト情報登録テンプレートを作成する。
（2） テキストエディタで必須項目を記入する（nic-hdl 属性に「AUTO-1」、source 属性に「TEST」、changed 属性に記入者の電子メールアドレスを記入する（表 2-9））。
（3） 完成したテキストを test-dbm@ripe.net に送信する。
（4） 数分で TEST データベースから登録の可否と新しい nic-hdl が通知される。

[8] PGP Corporation
http://www.pgp.com/

[9] RIPE Database User Manual:Getting Started, 2.3.2 Registering contact information
http://www.ripe.net/ripe/docs/db-start.html

表 2-9 コンタクト情報登録例

データオブジェクト	データ
person	John Smith
Address	Example LTD, High street 12 St. Mery Mead Essex, UK
Phone	+44 1737 892 004
e-mail	John.smith@example.com
nic-hdl	AUTO-1
remarks	******************************
remarks	This object is only an example!
remarks	******************************
Changed	John.smith@example.com
Source	TEST

レジストリデータの操作が許されるオペレータは person オブジェクトのうち、mntner オブジェクトの所有者である。この mntner オブジェクトには、所有者の公開鍵情報を、key-cert オブジェクトとして格納することが許される。

このオブジェクトには、編集作業を認証するための公開鍵が格納される。現在、Open PGP[10] 準拠の鍵だけがサポートされている。

key-cert オブジェクトの構成は表 2-10 のように定義されている

[10] RFC2440 OpenPGP Message Format
http://www.ietf.org/rfc/rfc2440.txt?number=2440

表 2-10 key-cert オブジェクト

データオブジェクト	
key-cert	データベースに格納された公開鍵の識別子。PGPKEY-<ID>の形式で登録される。
method	公開鍵のタイプ。現在は PGP のみが認められる。
owner	公開鍵の所有者
fingerpr	公開鍵証明書のフィンガープリント
certif.	公開鍵（テキスト形式）
remarks	注釈
notify	通知アドレス
mnt-by	このオブジェクトの操作を認証するために使われる mntner オブジェクトの識別子。
changed	オブジェクトの最終更新者と最終更新日。
source	オブジェクトの登録先

key-cert オブジェクトの生成手続きは以下のようになる。

（1） GnuPG（Gnu Privacy Guard[11]） の鍵をファイルにエクスポートする

（2） gpg –list-keys の出力の中から自分の電子メールアドレスに対応するものを探し、Key ID を記録する（この ID に PGPKEY-を加えたものが key-cert ID となる）

（3） 鍵をエクスポートしたファイルをエディタで開き、各行の先頭に certif: を加える

（4） ファイルの先頭に「key-cert: PGPKEY-<自分の KeyID>」を加える

（5） ファイルの終わりに次の各要素を加える（mnt-by: changed: source）

（6） mntner オブジェクトがパスワードで保護されている場合には、パスワード要素を加える

（7） 作成されたファイルを auto-dbm@ripe.net に送信する

ここで作成されたファイル、つまり key-cert オブジェクトの属性は次のようになる。

[11] The GNU Privacy Guard – GnuPG.org
http://www.gnupg.org/

表 2-11 ker-cert 登録データ

データ項目	内容
key-cert	PGPKEY-XXXXXXXX
certif...	------BEGIN PGP PUBLIC KEY BLOCK------
certif...	Version: GnuPG v1.2.2(cygwin)
certif...	mQGiBEAfEesRBCCTD0koyPykQv/lJj4q7eSiZv62qVA794bWmeydTBT5nxNdzoGT
certif.	鍵の内容が続く
certif	-----END PGP PUBLIC KEY BLOCK-----
mnt-by	EXAMPLE-MNT
changed	john.smith@example.com 20020827
source	RIPE

作成された key-cert オブジェクトを mntner オブジェクトに結びつけるためには、mntner オブジェクトに表 2-12 の属性を追加する。

表 2-12 mntner オブジェクトに追加する key-cert ID

auth: PGPKEY-XXXXXXXX

結び付けられた公開鍵で更新するデータを署名する手続きは次のようになる。

（1） 更新データをファイルに保存する

（2） データファイルに署名する（gpg –clearsign データファイル）

（3） 出力ファイルを auto-dbm@ripe.net に送信する。

署名データは表 2-13 のようになる。

表 2-13 署名データ例

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

person: Adam Smith
address: RIPE NCC
address: Singel 258
address: 1016 AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 545 4445
e-mail: adam-example@ripe.net
nic-hdl: AUTO-1
notify: Adam-example@ripe.net
mnt-by: EXAMPLE-MNT
changed: ripe-dbm@ripe.net
source: RIPE
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.2 (Cygwin)

iD8DBQeAMb6kOSlVyjdJy2cRAtIGAJ9tBvs43L7YUbb9asWWccI7CLS2JQCeM5gR
pZkDih+FApJqYa38dSy+oF4=
=nv9y
-----END PGP SIGNATURE-----
```

つまり、公開鍵によるデータ編集者の認証と完全性を提供することが目的であり、経路の機密は提供されない。

2.1.2.2. ネットワーク情報、AS 情報、割り当て情報

登録情報の一部は whois サービスを利用してインターネット上で公開される。登録情報の確実性を向上させるため、認証、暗号化、完全性の検証、可用性の保証などといった安全上の対策の強化が求められている。

安全上の脅威が、レジストリデータのうち、ネットワーク情報、AS 情報、割り当て情報に与えるリスクについて述べる。

始めにこれらの情報に共通のリスクを述べ、後に個々の情報に関するリスクを述べる。

（1）　アドレス資源運用管理の阻害

インターネットが健全に運用されるためにアドレス資源の適正な管理が求められている[12]。このアドレス資源の管理が阻害された場合に考えられるリスクを表 2-14 にあげる。

表 2-14 アドレス資源運用管理上のリスク

問題	リスク
アドレス資源の利用状況の把握不可能	アドレスの枯渇 偏ったアドレス利用の発生(ネットワーク/ISP 的偏り) 地域レベルでのアドレス資源管理負荷の増大
追跡不可能な通信ノードのなりすまし	登録されたネットワーク利用組織と異なる組織の利用による連絡と原因追跡の不能状況の発生 不能となるサービスで発生する損害
特定不可能なアドレス資源の不正利用(将来的に IRR との連動があるケース)	割り当てられていないアドレスブロックの利用によるネットワークの不正利用 不正利用によって阻害されたサービスで発生する損害

（2）　自律的運用の阻害

JPNIC では、独自のポリシーに基づいてリポジトリ業務を運営している。データベース公開についても例外ではなく、公共の資源として、正しく活用されるための努力を行なっている[13]。

しかし、不正な手法によるデータベースの改ざん、成りすましなどにより、自律的運用のための適切な連絡活動が阻害される危険性がある。適切な連絡活動ができないと、DNS サーバの設定などの運用が阻害されたり、不正アクセスの対応に大きな遅れが発生したりする。表 2-15 に、そのリスクをまとめる。

12 IPv4 アドレスの審議について
http://www.nic.ad.jp/ja/ip/eval.html
13 JPNIC データベースの情報公開について
http://www.nic.ad.jp/ja/db/dbpi/index.html

表 2-15 自律的運用の阻害におけるリスク

問題	リスク
不本意な連絡活動の発生（DNS の運用、不正アクセス）	登録された組織の信頼性･社会的地位の劣化 登録情報の目的外利用(書き換えによる営利用途等) 本来業務の阻害による間接的被害 紛争等直接経費

（3） DNS の運用阻害

DNS はインターネットを支える重要な基盤技術である。JPNIC では、IP アドレスからホストネームを引くための逆引きネームサーバを運用している。データの改ざんなどにより､誤ったレコードの提供が引き起こすリスクについて表 2-16 にまとめる。

表 2-16 DNS 運用阻害のリスク

問題	リスク
逆引きネームサーバの運用阻害 （ISP と APNIC,JPNIC の DNS サーバで、間違ったレコードが提供される）	多様な他のサービスに使われる DNS サーバの運用に障害をきたす。 メールの配送に支障 SSL 等の利用に支障 クレームケース:本来業務の阻害による間接的被害 クレームケース：紛争等直接経費

以下では情報別のリスクについて議論する。

（4） ネットワーク情報

ネットワーク情報とは 2.1.1.3 で述べたように、IP アドレスを使用している組織、個人に関する情報である。この情報の利用目的には次のものがあげられる。

- 割り振り／割り当て済みアドレスの確認
- ネットワークトラブルの解決
- 登録情報の確認

IR が管理するネットワークブロックについて効率的な割り振り／割り当てを行うためには、使われているブロックの分布状況を正確に把握していなければならない。

このためにネットワーク情報が使われている。

盗聴が行われた場合のリスクについては、公開情報であるため、特段のものはないと考えられる。

なりすましが行われた場合､つまり whois サーバが偽のサーバに代わられた場合と、改ざんが行われた場合とは、意図的な情報が渡されるという点で同じ状況と考えられる。さらに、サービス不能攻撃が行われた場合を考えると、必要なときに正しいデータを参照できないことになる。このことから考えられるリスクを以下にあげる。

ネットワーク情報の割り振り／割り当て要求を行う全てのサービス事業者が、ネットワーク情報の提供に関して、ある程度の障害時間を見込んでいるのであれば、短時間のサービス不能状態は許容できるといえるが、その保証は無く、ネットワーク情報提供サービスの中断が長い時間にわたった場合の影響は大きいと考えられる。

ネットワークトラブルが発生した場合、つまり、あるホストから不正なパケットが送られた、あるネットワークが到達不能となったなどの際に、トラブル解決の糸口として、運用責任者及び技術責任者に電子メールまたは電話などで連絡をとる必要性がある。この際に、ネットワーク情報中のコンタクト情報を用いる。

なりすまし及び改ざんが行われた場合、存在しない連絡先が示される場合と、別の連絡先が示される場合が考えられる。前者の場合、問題の発生しているネットワーク側の対処が自発的に行われるまでトラブルが解決しないため、ネットワークの切断という自体に発展する恐れがある。後者の場合、第三者にトラブル情報を公開してしまう危険性がある。

盗聴が行われた場合のリスクについては、ネットワーク情報の検索及び提供そのこと自体に機密性は無いので、特段の問題は無いと考えられる。しかし、ネットワークトラブル情報には機密情報が含まれる可能性が高いので、コンタクト先とのやりとりには注意が必要となる。

サービス不能攻撃が行われた場合、これは改ざんが行われ、トラブル発生元と連絡が取れない状態と同じことになる。

運用責任者及び技術責任者は自分たちが利用しているネットワークに関する情報が whois で正しく提供されていることを確認し、間違いがあればただちに訂正する、また変更があればただちに変更申請を行うことが求められている。このためには whois を用いて登録情報の確認を定期的に行う必要がある。

（5） AS 情報

AS 情報とは 2.1.1.4 で述べたように、AS を使用している組織、個人に関する情報

である。「JPNIC における AS 番号割り当てに関するポリシ[14]」によれば、この情報の利用目的には次のものがあげられる。

- 一意性の保証（割り当ておよび割り振られた AS 番号空間が世界でただひとつしかないことを保証する）
- 登録（一意性を保証するとともに、トラブル時の参照情報として利用するため）
- 効率的な利用（限られた資源を効率的に利用するため）
- 公平性（いかなる要因に左右されることなく公平に適用されるべきである）

AS 番号自体は運用ポリシーを持ったネットワークのかたまりを識別するためにつけら、BGP（Border Gateway Protocol、AS 同士で経路情報を交換するための外部経路制御プロトコルの一種）を利用して他の AS へ経路制御する際に用いられる。

もし、他 AS の所有する AS 番号を詐称したとしたら、経路情報に本来の状態との齟齬が生じることとなり、正常な経路制御が行えない可能性がある。また、割り振られたが割り当てられていない AS 番号、割り振られていない AS 番号を勝手に使い、経路情報を広告したらどうなるだろうか。これは接続する先の AS の運用状況にもよるが、将来、その AS 番号の正当な所有者が現れた際に混乱の元となるだろう。

実際に、このような割り当てが行われていないはずの AS 番号を含んだ経路情報が広告されていることが観測されている[15]。

AS 番号を用いた経路制御は、インターネットの中核技術の一つである。AS 番号を正しく管理、運営するためには、成りすまし、改ざんの脅威を取り除かなければならない。

AS 情報の登録と公開を行う機能である IRR（Internet Routing Registry）の役割は大きいため、今後、安全性について検討が進められると考えられる。

（6） 割り当て情報

割り当て情報とは 2.1.1.5 で述べたように、割り当てられたネットワーク情報である。

この情報に関するリスクはネットワーク情報と同じものになると考えられる。

---

[14] JPNIC における AS 番号割り当てに関するポリシ
http://www.nic.ad.jp/doc/jpnic-00890.html

[15] General Routing Registry Consistency Check Report
http://rrcc.ripe.net/RRCC_general_report.html

2.1.2.3. 提供する際（whois）と安全性

レジストリデータの提供手段として使われるプロトコルは RFC954 NICNAME/WHOIS で策定されている whois プロトコルである。

このプロトコルは単純な検索を実現するもので、TCP コネクション確立後、クライアントから検索文字列が送信され、サーバはこれをキーとした検索結果を送り返す、といったものとなっている。

このプロトコルでは、認証、機密、完全性といったセキュリティ機能が提供されていない。

whois データ、特にネットワークの運用担当者、技術連絡担当者の正確性は、ネットワークインシデント解決に重要なデータである。正しいサーバから正しいデータを受け取る必要があるが、これを脅かすリスクとして次のようなものが考えられる。

（1） なりすまし

whois クライアントはサーバを認証する機能を持たないため、whois サーバが本来のものであるのかどうかを判断することができない。

例えば whois サーバがドメインネームで指定された場合、DNS データの改ざんにより不正なサーバへクライアントが誘導されるリスクが存在する。また、一部のクライアントではデフォルトの　whois サーバが埋め込まれており、ソースコード改ざんにより、不正サーバへ誘導されるリスクが存在する。

なりすましを防止するためには、サーバ認証を実施しなければならない。なお、そのためには認証に必要な鍵の配布などの仕組みが必要になる。

（2） 盗聴

一般に whois でやりとりされるデータは公開データであり、機密性は無い。このために盗聴による情報漏えいのリスクは無いと考えられる。

（3） データ改ざん

転送経路が保護されていないため、第三者中継によるデータ改ざんのリスクが存在する。データ改ざんを防止するためには、元のデータに署名を行う方策が有効である。

（4） サービス不能攻撃

サービス不能攻撃によるリスクは、サービスのリアルタイム性が重要であるほど高いものとなる。whois サービスを参照する他のサービスにはリアルタイムと言うほど

の高い頻度で問い合わせを行うものは無いと考えられるが、whois のデータ登録件数は、数十万、数百万といったオーダーに達するため、データの参照自体は常に行われていると考えられる。

それらの参照に対する whois サーバの遅延がどれほどの影響を与えるのか、正確に判断することは難しい。しかし、本来の whois の機能が失われないためにはサービス不能攻撃に対する十分な対処が必要である。

JPNIC の whois サーバは、一定時間に一定量以上のアクセスがあると該当のクライアントに対しての返答を遅らせる仕組みが導入されている。またサーバのクラスタリング等の対策方法もある。

2.1.2.4. 申請業務におけるデータ保護

レジストリデータは申請とともに発生し、削除もしくは解約申請とともに消滅する。ここでは以下にあげる主要な申請業務について、現行業務を抽象化した手続きフローを図示し、業務手続きにおける問題点を明らかにする。

- IP アドレス割り振り申請
- 割り当て報告申請
- 個人情報登録/変更
- 指定事業者契約/解約
- ネットワーク記載事項変更申請
- IP 指定事業者情報変更申請

ここでは申請業務における安全性をいくつかの典型的な攻撃を想定して検討を行う。典型的な攻撃とは、なりすまし、盗聴、改ざん、サービス不能攻撃である。電子メールを利用したアドレス資源管理の申請業務において考えられるリスクについて以下に述べる。なお JPNIC ではパスワードや PGP を利用した保護機能を実現しつつある。

なりすましの例として、IP アドレス管理指定事業者のふりをして不正に IP アドレス割り振りの申請を行ったとする。割り振られたアドレスブロックは IP アドレス管理指定事業者によって管理されないため、（不正な）利用状況について把握することができない。そのアドレスブロックで問題が発生したとしても、連絡先がわからない。実際には、不正に割り振られたアドレスブロックを運用することは困難であるため、実用上の特別な問題が発生する可能性は高くはないが、そのアドレスブロックは再利用困難であり、アドレス資源の損失となる。

申請情報の盗聴のリスクは、送信される情報の機密性による。申請情報の中には whois を使って公開されない情報が含まれており、本来公開されるべきでない情報が漏洩する危険性がある。JPNIC では IP アドレスの割り振り審議の際に、ネットワー

クプランと呼ばれるネットワークの詳細情報を利用する。ネットワークノードの数を予測するため、顧客の統計に関する情報が必要になったりネットワークトポロジーがわかる情報が審議のために必要になったりする。IP アドレス管理指定事業者にとっての情報漏えいが、申請情報の機密性に関するリスクである。

サービス不能攻撃については、リアルタイム性が求められる情報については、リスクが存在する。しかし、週に一度の変更、月に一度の変更が行われればよい情報などでは、リスクは存在しつつも大きいものとはいえない。

一般に、脅威から生じるリスクの重大性は、リスクの大きさに蓋然性（possibility）を乗じたものとして評価される。リスク対策には相応のコストが要求されるため、制約の中で対策可能なリスクに重点的に対処し、大きなリスクであっても蓋然性が極めて低いものについては、たとえば保険などでリスクを転化することで、制約の範疇に収めることが考えられる。

以下に個別の申請業務の概要を示し、現状の体系の中で考えられるリスクを指摘する。

（1） IP アドレス割り振り申請

この手続きは、IP アドレス管理指定事業者が、新規の IP アドレスブロックの割り振りを JPNIC に申請するためのものである。

現行業務は図 2-8 のように示される。

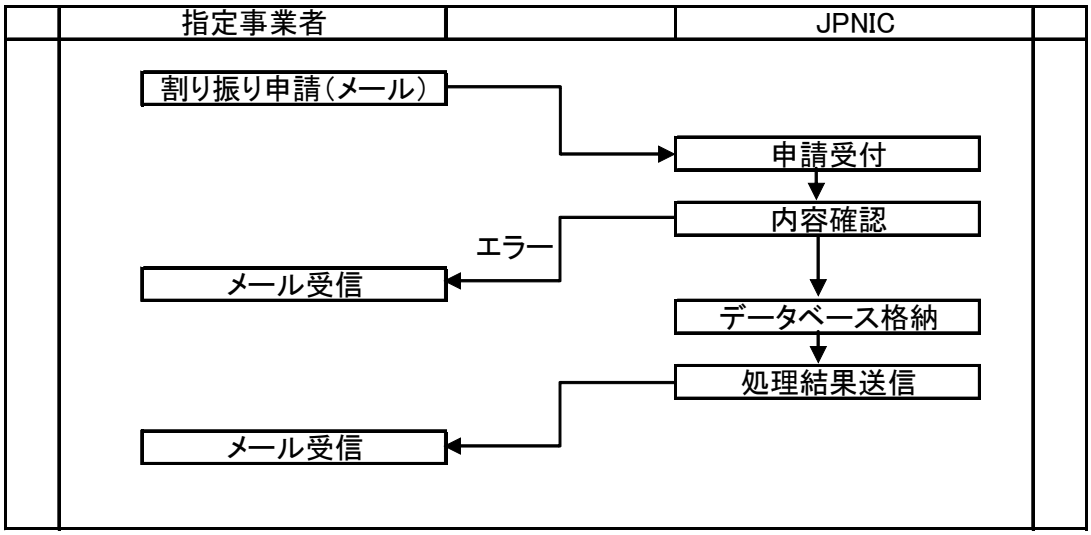


図 2-8 IP アドレス割り振り申請手続きフロー

（1） IP アドレス管理指定事業者から電子メールにて割り振り申請が送られる
（2） JPNIC では申請内容を確認し、問題があればエラーをメールで通知する
（3） 問題が無ければ申請を受理し、データベースにデータを格納する
（4） 処理の結果をメールで申請者に送信する

割り振り申請フォームに記載される内容は表 2-17 のようになっている[16]。

表 2-17 割り振り申請フォーム

番号	項目名	概要
a.	会員略称	申請を行なう IP アドレス管理指定事業者の会員略称。
b.	接続性	どのようにインターネット接続を行なうのかを表す数字。Internet eXchange（相互接続点：以下、IX）経由、ISP 経由、それ以外などの接続形態が示されている。
c.	接続先	接続先が IX または ISP の場合、その事業者名。IP アドレス管理指定事業者の場合は会員略称を記載する。
d.	Addr-3mo	3ヵ月後の IP アドレス管理指定事業者の累計割り当て済みアドレス空間に関する予測値。
e.	Addr-6mo	6ヵ月後の IP アドレス管理指定事業者の累計割り当て済みアドレス空間に関する予測値。
B.	Network-plan	IP アドレス管理指定事業者自身が構築するインフラネットワークで、今後 1 年間で新規に構築するネットワークの詳細情報。
D.	Old-network	IP アドレス管理指定事業者自身が構築するインフラネットワークとして割り当てられたアドレスで構築している、現在のネットワークの構成。

割り振り申請業務において、考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により割り振りに支障を来たし、指定事業者のアドレスブロックが一時的に枯渇し、申請者に対する割り当てが行えない。

（2） IP アドレス割り当て報告申請

この申請は、IP アドレス管理指定事業者が、IP アドレス利用者にアドレスブロッ

[16] IP アドレス管理指定事業者の IP アドレス割り振り／返却申請フォーム
http://www.nic.ad.jp/doc/jpnic-00865.html

クを割り当てる際に、事前の審査を受けることを目的として、「IP アドレス割り当て報告申請フォーム(ユーザネットワーク用)」を JPNIC に提出する。

IP アドレス割り当て報告申請は、表 2-18 のように定義される。

表 2-18 IP アドレス割り当て報告申請

JPNIC から委託を受けた CIDR ブロック内の IP アドレスの割り当てを行ったときは、JPNIC データベースへの登録が必要となります。割り当て報告申請により、割り当てに関する情報は「ネットワーク情報」として JPNIC データベースへ登録されます。IP アドレス割り当て報告申請は、IP アドレス管理指定事業者ネットワーク用とユーザネットワーク用で必要な項目が異なります。（http://www.nic.ad.jp/ja/ip/ipguide-m.html）

この申請フォームには、割り当てを行うネットワーク情報と、そのネットワークに関する連絡先個人情報を記入する。

現行業務は図 2-9 のように示される。

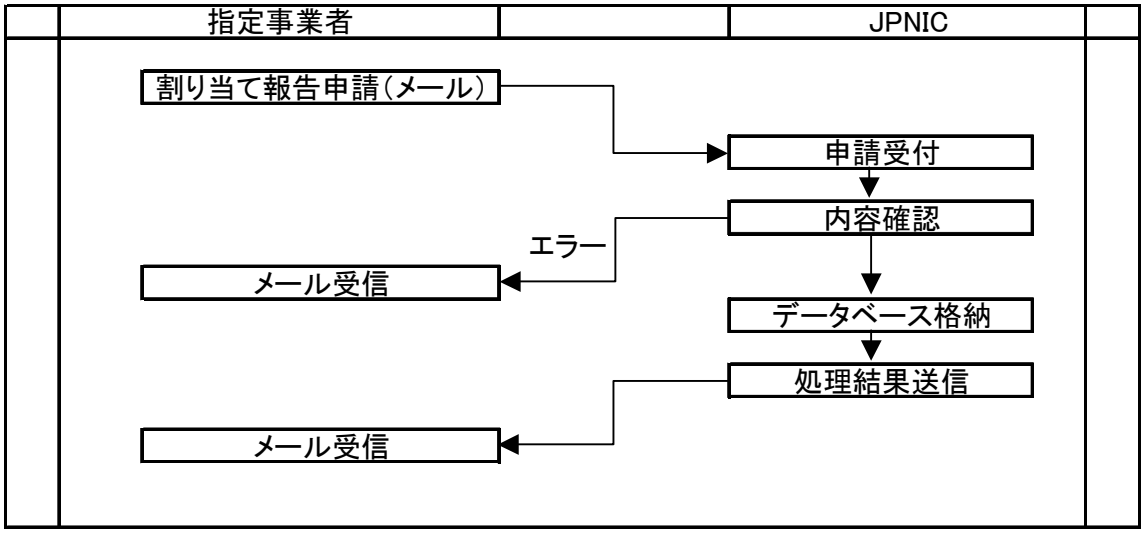


図 2-9 IP アドレス割り当て報告申請フロー

割り当て報告申請フォームに記載される内容は表 2-19 のようになっている[17]。

[17] IP アドレス割り当て報告申請フォーム(ユーザネットワーク用)
http://www.nic.ad.jp/doc/jpnic-00889.html

表 2-19 割り当て報告申請フォーム

番号	項目名	概要
a.	IP ネットワークアドレス	割り当てを行う IP ネットワークアドレス
b.	ネットワーク名	ネットワークを表す任意の文字列。
c.	組織名	ネットワークを運用する会社、組織などの正式名称
H	郵便番号	組織が所在する住所の郵便番
i.	住所	組織が所在する住所
m.	運用責任者	割り当てられる IP アドレスを使用する組織の責任者の JPNIC ハンドル。
n.	技術連絡担当者	割り当てられる IP アドレスを使用するネットワークに関する技術的、事務的などの全般的な問い合わせに対応する人の JPNIC ハンドル。
p.	ネームサーバ	/24 より大きなネットワークで、逆引きサーバの指定を行なう場合に記述する。詳しくは「ドメインネームサーバの設定手続きについて（http://www.nic.ad.jp/doc/jpnic-00886.html）」を参照。
y.	通知アドレス	ネットワーク情報が変更登録された場合に、通知すべき電子メールアドレス。
B.	Network-plan	新規に構築するネットワークの詳細情報をサブネット毎に記入する。
D.	Old-network	現在、割り当てを受けているアドレスで構築しているネットワークの構成をサブネット毎に記入する。
E.	審議番号	審議依頼を行ったネットワークに対する割り当て時のみ、審議申請の際に承認された審議番号を記入する。
F.	会員略称	IP アドレス管理指定事業者である場合には、JPNIC 会員情報の a.[会員略称]を記入する。

割り当て報告業務において考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい（住所などの個人情報を含んでいる）
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により割り当て報告に支障を来たし、逆引きネームサーバが登録されない

（3） 個人情報登録／変更

この申請は担当者の情報を登録または変更する手続きである。担当者の情報は、JPNIC ハンドルという識別子を利用している。

現行業務は図 2-10 のように示される。

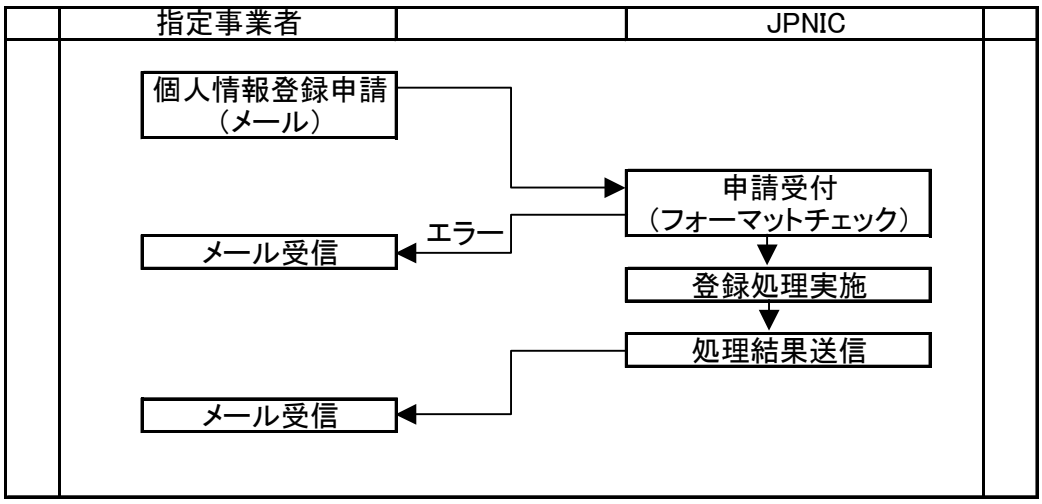


図 2-10 個人情報登録申請手続きフロー

同様に、個人情報変更に関する現行業務は図 2-11 として示される。

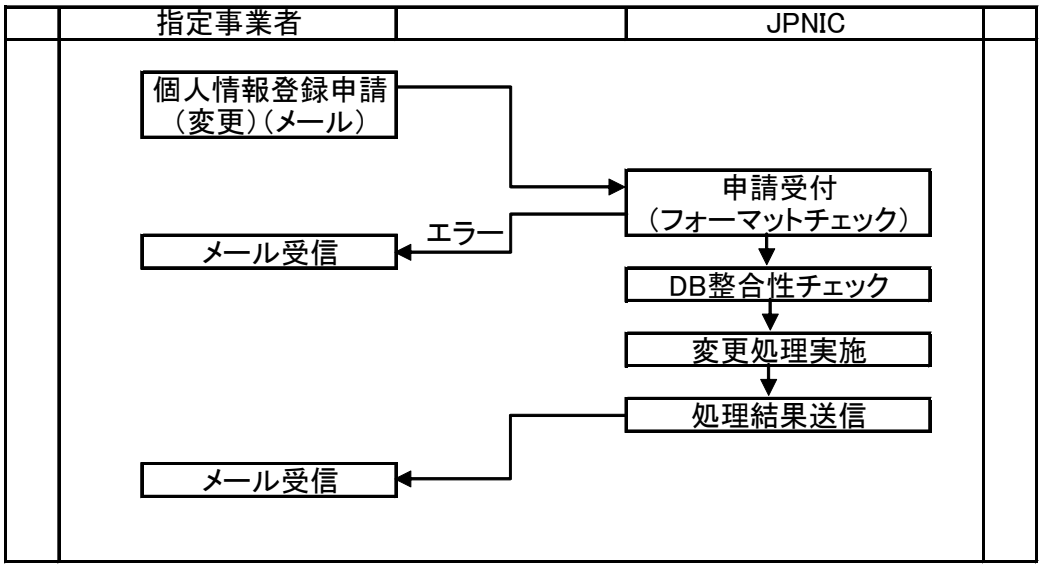


図 2-11 個人情報変更申請手続きフロー

申請フォームに記載される内容は表 2-20 のようになっている[18]。

表 2-20 個人情報登録申請フォーム

番号	項目名	概要
a.	JPNIC ハンドル	すでにデータベースに登録されている場合にはその JPNIC ハンドル、登録されていない場合には任意の数字
b.	氏名	登録する個人名
c.	Last, First	氏名のローマ字表記
d.	電子メイル	登録する個人の電子メールアドレス
f.	組織名	個人が所属する組織の正式名称
g.	Organization	組織名の英語表記
h.	郵便番号	登録する個人が所属する組織住所の郵便番号
i.	住所	登録する個人が所属する組織住所
j.	Address	住所の英語表記
k.	部署	登録する個人が所属する組織中における部署名
l.	Division	部署の英語表記
m.	肩書き	登録する個人が所属する組織中における役職名
n.	Title	肩書きの英語表記
o.	電話番号	登録する個人が所属する組織の電話番号
p.	FAX 番号	登録する個人が所属する組織の FAX 番号
y.	通知アドレス	登録する個人情報が変更された時に通知する電子メールアドレス

個人情報登録申請業務において考えられるリスクを以下に挙げる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な情報変更
- 電子メールアドレス、電話番号、FAX 番号など、連絡に必要な情報を改ざんすることで、サイトに問題が行った際に、運用責任者、技術連絡担当者に連絡をすることができないようにする。

（4） 指定事業者契約／解約

IP アドレス割り当てを行うためには、JPNIC との間に IP アドレス管理指定事業者

[18] JPNIC データベース 登録・変更ガイド：一般向け
http://www.nic.ad.jp/doc/jpnic-00869.html

契約を締結し、IP アドレス管理指定事業者とならなければならない。

この契約作業は図 2-12 のように実施される。

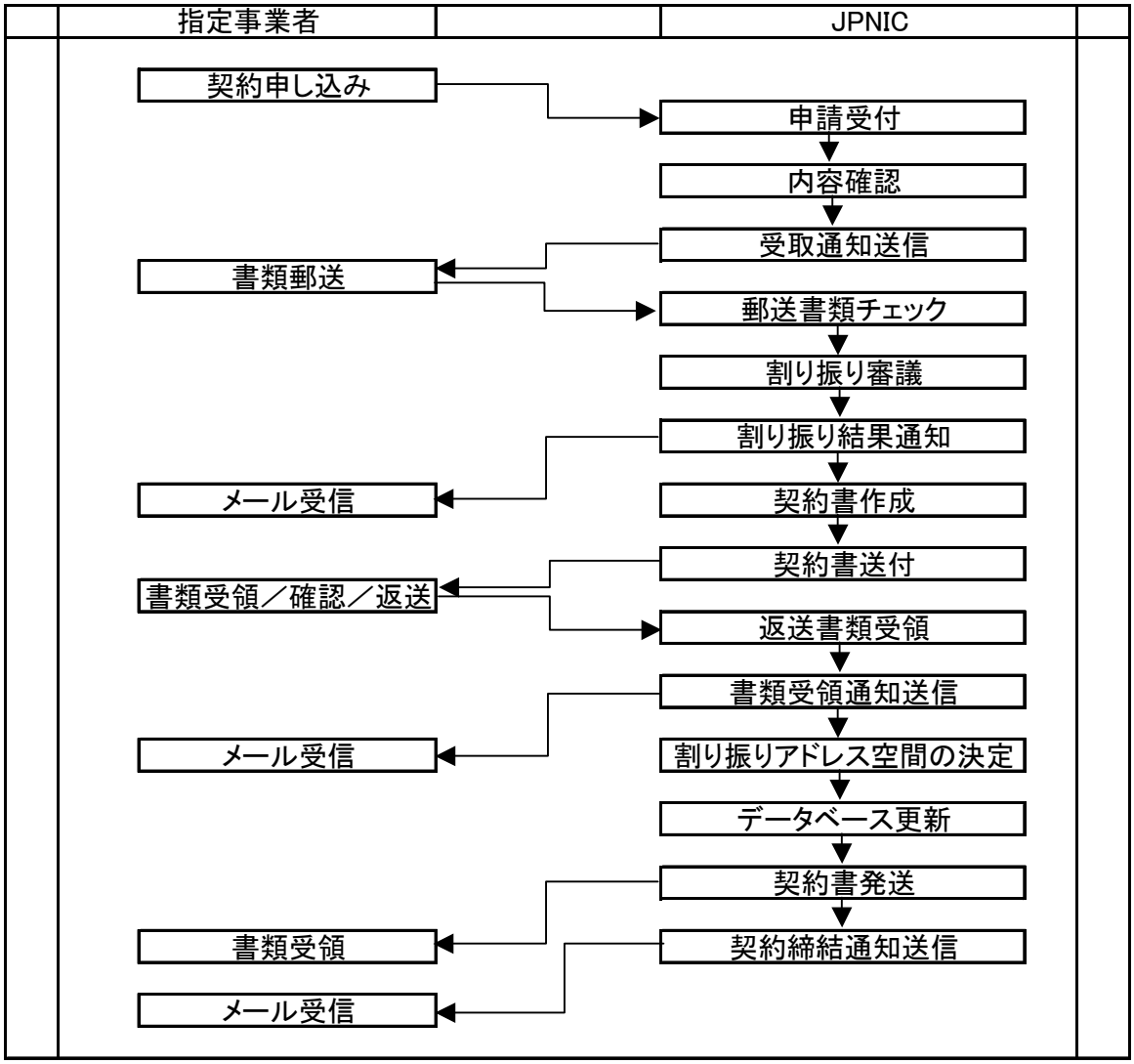


図 2-12 IP アドレス管理指定事業者契約フロー

提出書類として、表 2-21 の書類が指定されている[19]。

[19] IP アドレス管理指定事業者について
http://www.nic.ad.jp/doc/jpnic-00883.html

表 2-21 IP アドレス管理指定事業者契約提出書類

書類	提出方法
IP アドレス管理指定事業者契約申込書	電子メール
[JPNIC 会員情報](指定事業者情報)初期登録情報	電子メール
ネットワークの運用規約あるいはそれと同等のもの	電子メール
接続先確認フォーム	電子メール
初期割り振り要件確認フォーム	電子メール
法人の登記簿謄本	書面
代表者印の印鑑証明書	書面

IP アドレス管理指定事業者と JPNIC のやり取りは、郵便及び平文の電子メールで行なわれる。他の申請業務と異なっているのは、機密性（プライバシー）を有する重要な情報については書面での申請となっており、書面と電子メールを比較することで、なりすまし、改ざんなどの脅威を防止することができる点にある。

このため、考えられるリスクは次のものとなる。

- 電子メール伝達経路の盗聴による情報漏えい（初期登録情報には、申請手続き担当者電子メールアドレスなどの非公開データが含まれる）

（5） ネットワーク記載事項変更申請

ネットワーク記載事項の変更申請は「ネットワーク情報記載事項変更申請について」[20]にて示されるように、「IP アドレス割り当て後にネットワーク名、組織名、住所、運用責任者を変更する」行為である。

この操作の手続きは図 2-13 として示される。

[20] ネットワーク情報記載事項変更申請について
http://www.jpnic.jp/doc/jpnic-00407.html

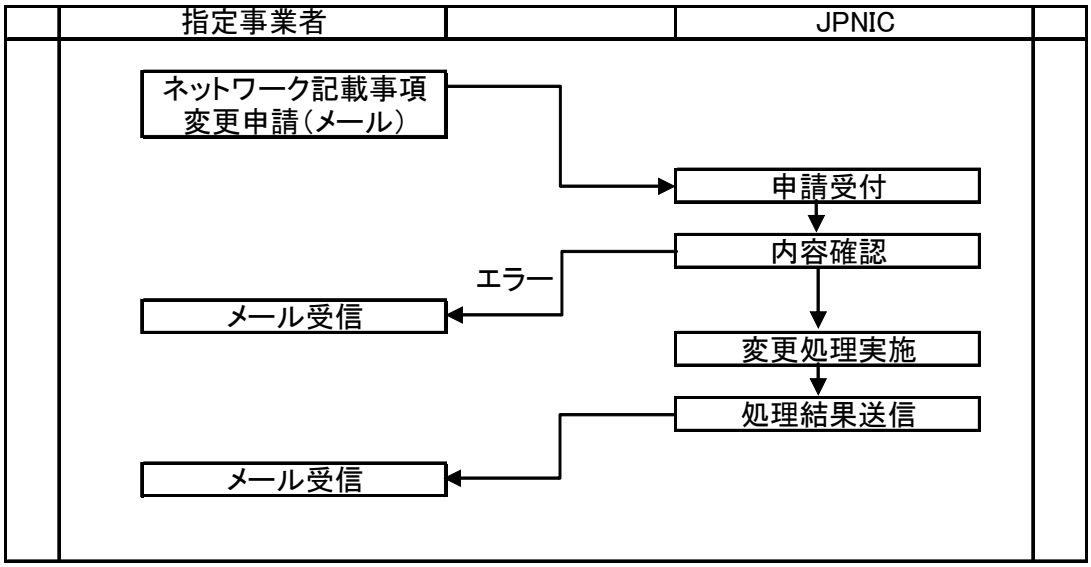


図 2-13 ネットワーク記載事項変更フロー

申請を行うフォームの記入例として表 2-22 が示される[21]

表 2-22 ネットワーク記載事項変更申請記入例

```
------------------------------------------------------------------------
# CHANGE TEMPLATE V 1.1 #
Current Network Information: [ネットワーク情報]
a. [IP ネットワークアドレス]      192.0.1.0/25
b. [ネットワーク名]               ABC-DUP-NET
f. [組織名]                       学術広帯域ネット協議会
g. [Organization]                 Academic Broadband Conference
h. [郵便番号]
i. [住所]
j. [Address]
m. [運用責任者]                   ABOOOJP
n. [技術連絡担当者]               ABOOOJP
p. [ネームサーバ]
y. [通知アドレス]                 ichiro@abc.ne.jp
```

[21] ネットワーク情報記載事項変更申請フォーム
http://www.jpnic.jp/doc/jpnic-00417.html

```
Network Information: [ネットワーク情報]
b. [ネットワーク名]
f. [組織名]
g. [Organization]
h. [郵便番号]                  101-0047
i. [住所]                      東京都　千代田区　内神田 2-3-4
j. [Address]                   2-3-4, Uchikanda, Chiyoda-ku,
                               Tokyo 101-0047, Japan
m. [運用責任者]

[変更理由]

本社移転に伴う住所変更のため。

[備考]
------------------------------------------------------------------------
```

ネットワーク記載事項変更申請の申請業務については、次のリスクが考えられる。

- 電子メール伝達経路の盗聴による情報漏えい
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な割り振り
- サービス不能攻撃により情報変更に支障を来たし、サイトに問題が行った際に、運用責任者、技術連絡担当者に連絡をすることができない

（6） IP アドレス管理指定事業者情報変更申請

この手続きについては「指定事業者情報登録ガイド[22]」に詳細が記載されている。指定事業者情報については、変更する情報種類によって申請方法が分かれている。

会員名、運用組織名、運用責任者名が変更される場合には、届出書類を作成し、名称の変更を証明する登記簿謄本等を同封した上、書面のまま JPNIC に送信する。

それ以外の情報の変更については電子メールでの変更申請が行われる。

この手続きは図 2-14 のように示される。

[22] 指定事業者情報登録ガイド
http://www.jpnic.jp/doc/jpnic-00861.html

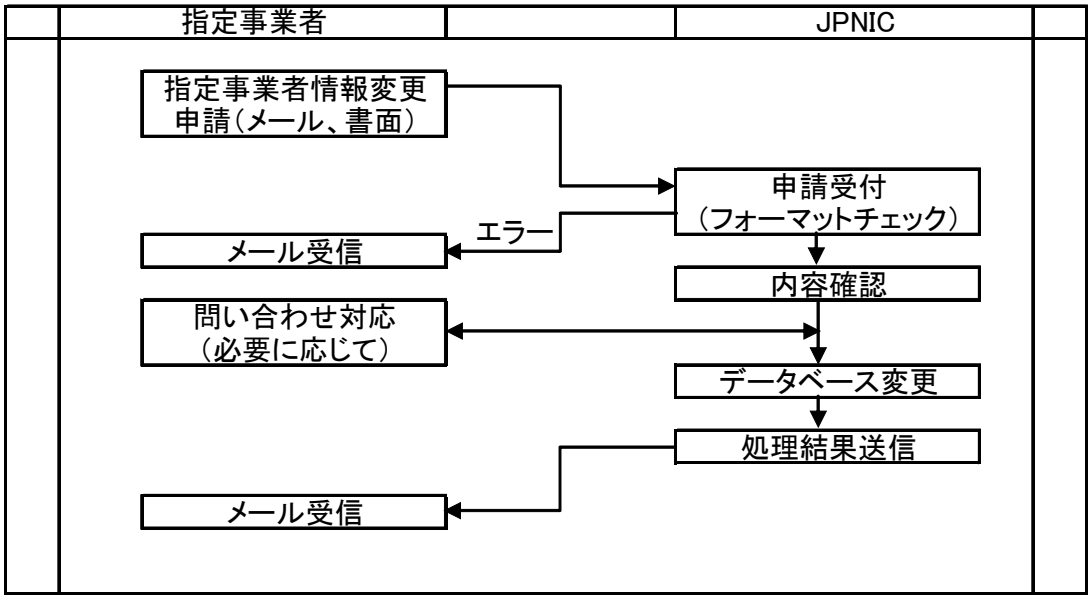


図 2-14 IP アドレス管理指定事業者情報変更申請フロー

書面での変更申請事項は郵送方法に依存した安全性になる。電子メールで変更申請される情報は表 2-23 のものとなる。

表 2-23 IP アドレス管理指定事業者情報のうち電子メールで変更申請される情報

番号	項目名	概要
a.	会員略称	指定事業者略称のこと。指定事業者を一意に識別するための符号として用いる。
g.	郵便番号	一般利用者から指定事業者に関する問い合わせを受けた場合に紹介すべき連絡先
h.	住所	同上
k.	FAX 番号	同上
l.	電子メイル連絡先	
m.	URL	指定事業者に関する情報を掲載する WWW ページの URL（RFC1738 形式）
o.	技術連絡窓口	指定事業者の技術担当者の電子メールアドレス 複数人の場合にはメーリングリストを作成することが望まれる
p.	事務連絡窓口	指定事業者の事務担当者の電子メールアドレス
q.	経理連絡窓口	指定事業者の経理担当者の電子メールアドレス
t.	DB 登録	JPNIC に対して指定事業者として申請手続きを行う担当者の電子メールアドレス
y.	通知アドレス	この情報が変更された場合に通知すべき電子メールアドレス
I.	技術連絡担当者	技術連絡担当者一名の電子メールアドレス
J.	事務連絡担当者	事務連絡担当者一名の電子メールアドレス
K.	経理担当者	経理連絡担当者一名の電子メールアドレス

これらの情報については以下のリスクが考えられる。

- 電子メール伝達経路の盗聴による情報漏えい（住所などの個人情報を含んでいる）
- 成りすましによる虚偽の申請
- 内容の改ざんによる不正な連絡担当者の変更

2.1.2.5. レジストリ間データ交換時のデータ保護

ここでは RIPE NCC と APNIC がリポジトリデータベースの同期に用いているスキームの概要を示し、安全上の問題について考察する。

はじめに RIPE NCC が用いている NRTM（Near Real Time Mirroring）について示し、次に APNIC におけるデータ同期スキームを示す。最後に whois を代替する目的で開発されている CRISP（Cross Registry Information Service Protocol）の概観

について示す。

（1） RIPE NCC における whois データベース同期スキーム（NRTM）

RIPE NCC では、レジストリ間 whois データベース同期スキームとして、NRTM が使われている[23]。RIPE NCC データベースのミラーサイトに参加するためには、NRTM によるデータベースを実施する必要がある。

NRTM は、差分更新により、データ転送量を減らす目的で作成された。その手法は、データ更新（追加、削除）のたびにシーケンス番号をインクリメントし、データ同期要求の際には、前回同期した際のシーケンス番号から、現在のシーケンス番号の間に実施された変更操作を転送するというものである。図 2-15 に、この概念が表される。

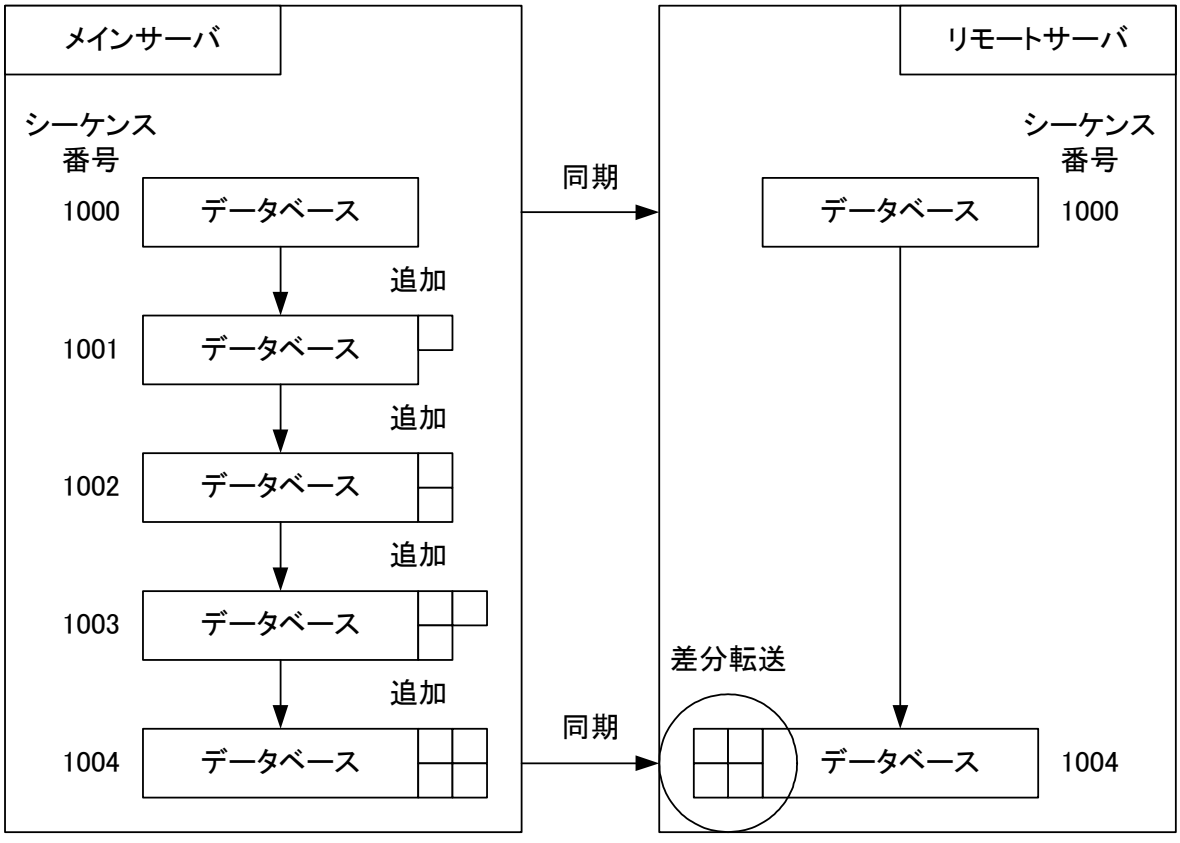


図 2-15 NRTM における差分更新概念

[23] ripe-252 RIPE Database Reference Manual
http://www.ripe.net/ripe/docs/databaseref-manual.html

NRTM では、ミラーサイトからの要求に応じて、マスターサイトからデータが送られる、プル方式を採用している。RIPE NCC のデータベースに対し、シーケンス番号 1539595 から 1539597 までのデータ転送を要求するメッセージは表 2-24 のように表される。

表 2-24 NRTM メッセージサンプル

```
%START Version: 2 RIPE:1539595-1539597
ADD

＜データオブジェクト＞

DELETE

＜データオブジェクト＞

%END RIPE
```

このプロトコル自身ではセキュリティ機能は用意されていない。このため、次のリスクが考えられる。

表 2-25 NRTM で考えられるリスク

セキュリティ機能	考えられるリスク
認証の欠如	なりすましによる認められていないミラーサイトによるデータベースの取得
機密性の欠如	データベース中のデータが、すべて無制限に公開されているわけではないため、第三者への情報漏洩が発生する
完全性の欠如	データ転送過程における改ざんの発生
可用性の欠如	過負荷によりマスターサイトがダウンする危険性がある

特に問題といえるのは第三者中継によるデータ改ざんである。NRTM では、差分方式をとっているため、いったん改ざんされたレコードの正当性が検証される機会は、プロトコル上は存在しない。このため、改ざんされたレコードが提供されつづける可能性がある。

この問題を回避するためには、データに電子署名を行う、保護されたチャンネル上で転送を実施するなどの解決策が考えられる。RIPE NCC のデータベースでは、PGP によるユーザ認証を実施しているので、この鍵を使って電子署名を実現することが考えられる。しかし、NRTM を実施している主体は RIPE NCC と他のインターネット

レジストリであり、電子署名を実施する主体のデータ所有者（ISP や EE など）に電子署名を強制する権限は無いものと考えられる。

このため、実際には転送チャンネルを保護することになるであろう。SSH や SSL/TLS といった暗号通信プロトコルを用いるのがコスト的にも適していると考えられる。ホスト同士が個別に認証を行う場合、互いの公開鍵を安全に交換することが必要になる。ミラーサイトの数が多くなった場合には PKI（Public-Key Infrastructure、公開鍵基盤）の導入を検討することになると考えられる。

（2） APNIC におけるデータ同期スキーム

APNIC では各 NIR との間で DNS の逆引きゾーンデータファイルと whois データベースを同期させている。

DNS の逆引きゾーンファイルは、それぞれの NIR の ftp サイトに次のようなディレクトリとファイルを用意することで公開されることが定められている[24]。

- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>
- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>.md5
- ftp://ftp.<nir>.net/pub/zones/<zero-padded-slash8>-<nir>.asc

実際に、APNIC の管理する逆引きゾーンファイルは ftp://ftp.apnic.net/pub/zones 以下で匿名 FTP を通じて提供されている。表 2-26 は、その一つの例である。

表 2-26 ftp://ftp.apnic.net/pub/zones/202-APNIC

```
$ORIGIN .
$TTL 172800
15.0.202.in-addr.arpa.   IN      NS      dme2.mpr.wa.gov.au.
15.0.202.in-addr.arpa.   IN      NS      karri.bs.wa.gov.au.

32.0.202.in-addr.arpa.   IN      NS      kirsty.paradise.net.nz.
32.0.202.in-addr.arpa.   IN      NS      rachel.paradise.net.nz.

33.0.202.in-addr.arpa.   IN      NS      kirsty.paradise.net.nz.
33.0.202.in-addr.arpa.   IN      NS      rachel.paradise.net.nz.
```

[24] Operational policies for National Internet Registries in the APNIC region
http://www.apnic.net/docs/policy/operational-policies-nirs.html

```
（省略）

30.12.202.in-addr.arpa.  IN      NS      ns1.nic.ad.jp.
30.12.202.in-addr.arpa.  IN      NS      ns2.nic.ad.jp.

（省略）

APNIC.202.in-addr.arpa.  IN      TXT     "Generated at 2004-03-10 06:16:57Z with
35975 NS records."
```

このデータに対する署名ファイルは表 2-27 として公開されている。

表 2-27 ftp://ftp.apnic.net/pub/zones/202-APNIC.asc

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iEYEABECAAYFAkB0stoACgkQyzQvAdFSThSC0ACfYVW30Z0FsnZfs6+Ln4wsi+CE
rloAn26KcRc+gQAkt5yPaApqT81ZnLY3
=H+Nc
-----END PGP SIGNATURE-----
```

さらにデータに対するチェックサムが表 2-28 として公開されている。

表 2-28 ftp://ftp.apnic.net/pub/zones/141-APNIC.md5

```
MD5 (202-APNIC) = c967be9d4d8029a41e399a8a32503f41
```

このようにデータと電子署名が提供された場合、署名を検証することで作成者の正当性とともにデータの改ざんを発見することが出来る。

この場合、RIPE NCC で述べたように公開鍵を交換し合う必要がある。データを交換し合う IR の数が多くなると、鍵管理の負荷が急激に大きくなる。このため、PKI を構築することで、結果として負荷低減に寄与することとなる。

（3） CRISP のデータ認証方法

レジストリデータの公開手段として whois があることはすでに述べた。whois は単純な検索をサポートしているが、レジストリデータの数が膨大なものとなっている

現状、whois を代替する形の高度な検索プロトコルとして、Cross Registry Information Service Protocol （以下、CRISP と呼ぶ）が提案されている[25]。

このプロトコルは、分散環境への適合、情報ごとの参照権限設定、匿名アクセスからの登録者情報の保護、コンピュータで解析可能な検索・回答フォーマット規定などを実現することを目標においている。

現在は、2004 年 2 月に、「Cross Registry Internet Service Protocol (CRISP) Requirements」が RFC3707 として公開された段階にある。この RFC は、インターネットレジストリに焦点をあてたものとなっている。

今後の拡張として、クライアント認証の導入があげられているが、現時点では認証方式の指定は無く、将来の拡張に備えることだけが示されている（表 2-29）。

表 2-29 RFC3070 4. Feature Requirements より

4.1.　クライアント認証 サービスにアクセスする主体は、認証を目的として、サーバにクレデンシャルを受け渡すメカニズムを提供されなくてはならない。プロトコルは多くの認証タイプを採用でき、将来の認証タイプの拡張を受け入れるメカニズムを提供しなくてはならない。

[25] Cross Registry Information Service Protocol (crisp)
http://www.ietf.org/html.charters/crisp-charter.html

2.2. まとめ

本章では、インターネットレジストリにおけるアドレス資源管理の業務について述べ、申請データの内容、地域インターネットレジストリ（RIR）におけるメンバー、データ保護の仕組みについて述べた。アドレス資源管理における安全性は登録データの正当性が最も重要となる。そのために、申請業務におけるクライアント認証やインターネットレジストリ間の同期におけるデータ認証が必要になると考えられる。

RIR と NIR の連携したアドレス資源管理の機構によって、国際的なアドレス資源の正当性確保が可能になることもわかる。この状況を利用した認証基盤については、第 4 章で述べる。

本章で言及した RIR における認証の機能は、認証局を利用した認証システムでも実現されつつある。RIR の認証局に関しては次の第 3 章で述べる。

第3章 RIR の認証局の状況

内容

- 地域インターネットレジストリ（RIR）の認証局と証明書を使ったサービス
  - APNIC
    1. ユーザ証明書の扱い
    2. MyAPNIC
  - RIPE NCC
    1. ユーザ証明書の扱い
    2. LIR Portal
  - ARIN における議論

3. RIR の認証局の状況

3.1. はじめに

アジア太平洋地域の地域インターネットレジストリ（RIR：Regional Internet Registry）である APNIC（Asia Pacific Network Information Centre）や、ヨーロッパ地域の RIR である RIPE NCC（Réseaux IP Européens Network Coordination Centre）では、既に認証局が構築されている。これらの認証局は、各種申請の関連業務におけるクライアント認証で使われる電子証明書（以下、証明書という）の発行に利用されている。

本調査研究では、これらの認証局と証明書の利用方法について調査を行うとともに、APNIC、RIPE NCC の技術担当者との意見交換を実施した。これらの RIR の認証局の動向は、JPNIC における認証業務との連携に大きく影響するため、本章では特に APNIC と RIPE NCC の認証業務と証明書の利用について重点的に述べる。アメリカ地域の RIR である ARIN（American Registry for Internet Numbers）については、進行中である議論や動向について述べる。

従来、各 RIR においてはレジストリデータ編集の際に MAIL-FROM を用いた認証を実施していたが、かねてより強度面での脆弱さが指摘されており、CRYPT-PW、MD5、そして PGPKEY と、より強度の高い認証方式が随時、採用されてきた。

これらの認証方式として表 3-1 の方式が定義され、採用されている。

表 3-1 APNIC における mntner オブジェクトの認証方式[1]

認証方法	概要
NONE	保護されない。
MAIL-FROM	電子メールアドレスによるもの。きわめて弱い保護といえる。
CRYPT-PW	UNIX crypt 方式の暗号化パスワード。パスワード文字列長が 8 文字のため、強力とはいえない。
MD5	UNIX md5 方式の暗号化パスワード。パスワード文字列長が 65 文字に拡張され、CRYPT-PW よりも強力といえる。
PGPKEY	公開鍵証明書を示す署名識別子。公開鍵暗号による保護を提供する。

CRYPT-PW と MD5 は、ユーザパスワードを、DES 暗号を基にした Unix crypt 関数及び一方向ハッシュ関数である md5 で暗号化したものをレジストリデータに登録するものである。このことで安全性を向上させることが出来る。しかし、問題は残っ

[1] Authentication options for maintainer objects
http://www.apnic.net/db/ref/attributes/mntner/auth-mntner.html

ている。

- ユーザから RIR へ転送されるパスワードは平文で記入されるため、盗聴によりパスワードが流出する危険性がある
- 暗号化されたパスワードが whois 経由で公開されるため、パスワードが解析される危険性がある

CRYPT-PW のパスワードは 8 文字という制限があるため、現代の計算機能力を持ってすれば十分に推測可能といわれている。MD5 では、より長いパスワードが利用できるため、総当り攻撃でパスワードを推測することは困難といえる。しかし、通信経路として電子メールを使っているため、パスワード盗聴の危険性は依然として残る。

PGPKEY を使った場合には、これらの問題は解決する。更新データを含んだメッセージを事前に登録した PGPKEY を使って電子署名することで、メッセージ作成者の認証を行うとともに完全性の保証が可能となる。

現在提供されている認証方式の強度の関係は表 3-2 のように示される。

表 3-2 認証方式の強度比較

方式	強度	理由
NONE	無し	検証が行なわれない
MAIL-FROM	脆弱	なりすましの危険性がある
CRYPT-PW	弱	パスワード長が短く推測可能
MD5	中	転送中のパスワードに盗聴の危険性がある
PGPKEY	高	認証と完全性を提供できる

PGPKEY を用いることで強度的には十分な認証が実施できると考えられる。しかし、PGP は元々、個人が暗号化や電子署名を行うために開発されたものである。whois データベースの更新を電子メール経由で行う場合には十分とはいえ、拡張性、応用性を考えると難しい面がある。

ここ数年の間、各 RIR では、PGP よりも拡張性に富む PKI ベースの認証システムの配備を進めている。以降では、APNIC、RIPE NCC、ARIN における認証業務の動向について述べる。

3.2. RIR における認証局の活用

認証対象に証明書を発行し、検証を行うのが典型的な活用方法である。

本節では、PKI の活用の概要を概念的な手順で説明する。次に APNIC や RIPE NCC の認証局の活用について述べる。最後に、PKI（Public-Key Infrastructure、公開鍵基盤）の導入が進みつつある ARIN で認証方式の PKI の適性についての議論を紹介する。

3.2.1. PKI 活用の概要

PKI を利用した認証処理は、証明書の検証を通じて認証を行う検証者が、認証局（Certificate Authority、以下、CA と呼ぶ）を信頼することによってはじめて実現する。認証対象である EE は、CA から発行された証明書を検証者に提示し、検証者が EE の証明書の検証を行う。従って検証者が認証結果にもとづいてアクセス制御を実施することが出来る状況は、下記のような手順で構築される。

- 検証者による認証局の信頼
- EE による CA 証明書の組み込み
- EE による証明書の組み込み
- ユーザ（EE）管理
- 証明書の検証
  - サーバ証明書（EE が検証者となる）
  - クライアント証明書

3.2.1.1. 検証者による CA の信頼

検証者は CA の運用を兼ねているので RIR における、この手順は既に実施されている。

3.2.1.2. EE による CA 証明書の組み込み

暗号通信（SSL/TLS）を利用する場合、クライアントはサーバによる認証を受ける前に、サーバ認証を行う。その際に、サーバの提示する証明書を検証する必要があるため、CA 証明書が必要になる。EE が CA 証明書を組み込むには、検証者として CA を信頼する必要がある。この CA 証明書の組み込みと信頼の手順は、上記に述べた検証者によるものと同様である。

3.2.1.3. EE による証明書の組み込み

EE が認証手続きを受けるためには、検証者が信用する CA から証明書パスを辿る

ことができる証明書を発行されている必要がある。この手順は、EE による CA への証明書の要求と、CA による承認および発行、EE による証明書の組み込みといったもとなる。

3.2.1.4. ユーザ（EE）管理

サービスの提供者がユーザ認証に証明書を使う場合、証明書の管理すなわちユーザの管理が必要となる。クライアント証明書を使ったユーザの管理では、ユーザアカウントの無効化は証明書の失効によって行なわれる。しかし、一つのユーザアカウントに対し、複数の証明書を発行するようなモデルの場合、ユーザと証明書を管理するデータベースを用意し、該当するユーザのエントリを無効化するなどの方法となる。

ユーザアカウントが無効化されたことは、適切なタイミングで検証者に伝えられる必要がある。検証時にクライアント証明書の有効期限が切れている場合には、その情報だけでユーザアカウントが無効であることがわかる。しかし、有効期限内にユーザアカウントが無効化された場合は、CRL（Certification Revocation List）や OCSP（Online Certificate Status Protocol）といった失効情報を扱う仕組みが必要となる。

ユーザ管理は、以下のような要素によって、その形態が決まる。

- ユーザの規模
- ユーザの地理的な分散
- ユーザの権限の管理形態

ユーザの任命行為や権限の管理が地理的に分散した組織で行なわれる場合、ユーザの管理を行う管理者が分散している方が効率的な管理を行うことができる。しかし、管理者を分散して配置するとなると、運用のレベルを保つためには監視や監査といったマネジメント上の作業が発生する。

多くのユーザを管理する場合は、ユーザ登録や権限の管理といった処理にかかる負荷も大きくなる。そのため、管理部門を一箇所に集中させるよりは、社会的な権限の管理体系に合わせた構造にする必要がある。

3.2.1.5. 証明書の検証

サービス提供者が、アクセスしてきたユーザに対して、アクセス制御を行うためには、クライアント証明書の検証を行い、クライアントの認証を行う必要がある。

証明書の検証の際には、前述した証明書の失効情報を扱うとともに、アクセス制御の規則を定義したデータベースを扱う。

3.3. APNIC

ここでは、前節で述べた手順の概要に沿って APNIC（Asia Pacific Network Information Centre）における認証局の活用について述べる。

APNIC は、アジア太平洋地域を管轄とする RIR である。APNIC では、1999 年より PKI への取り組みを開始している。

1999 年には要件定義の試みとしての Scoping Project が行なわれ、認証局の運用について必要な機能及び現状の問題点がまとめられた。翌 2000 年には認証運営の試みとして Pilot Project が行なわれ、メンバ登録からオンラインでの証明書要求から発行まで詳細な議論と実証が行なわれた。これらの試験的プロジェクトの成果により、認証運営の環境が整えられたといえる。

このような環境構築の成果を受け、APNIC では、証明書ベースの認証を取り入れた、メンバの所有するデータベースオブジェクトの管理インターフェースとして MyAPNIC というウェブサービスを提供している。

以降で、MyAPNIC における PKI の利用と、認証局の運用について述べる。

3.3.1. 概要

ここでは、認証業務と MyAPNIC におけるアクセスコントロールについて述べる。

APNIC では次の目的を達成するため、独自の認証局(以下、APNIC CA と呼ぶ)を構築している。

- メンバと APNIC 間の電子メール交換を安全にする
- MyAPNIC へのアクセスを安全にする

MyAPNIC は SSL/TLS で保護された通信経路上で情報提供サービスを行なっている。（図 3-1）

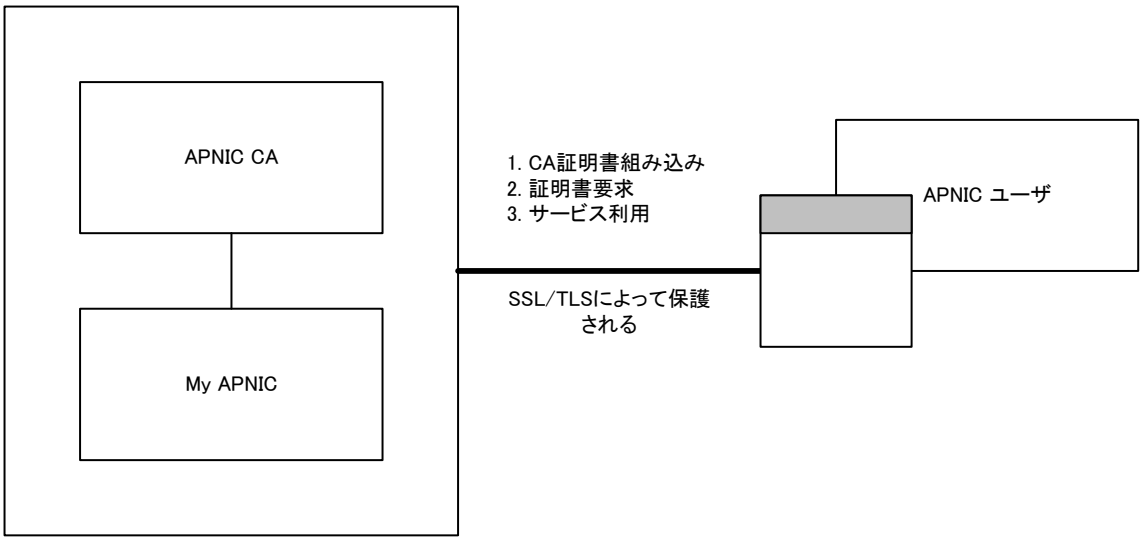


図 3-1 MyAPNIC 概要

以下では、MyAPNIC へのアクセスに用いられる証明書の運用に関して、APNIC CA の業務について述べる。

3.3.2. EE による CA 証明書の組み込み

APNIC ルート CA 証明書のロードおよびオンラインでの証明書要求申請は、ウェブインターフェース（図 3-2）を介して行なわれる。

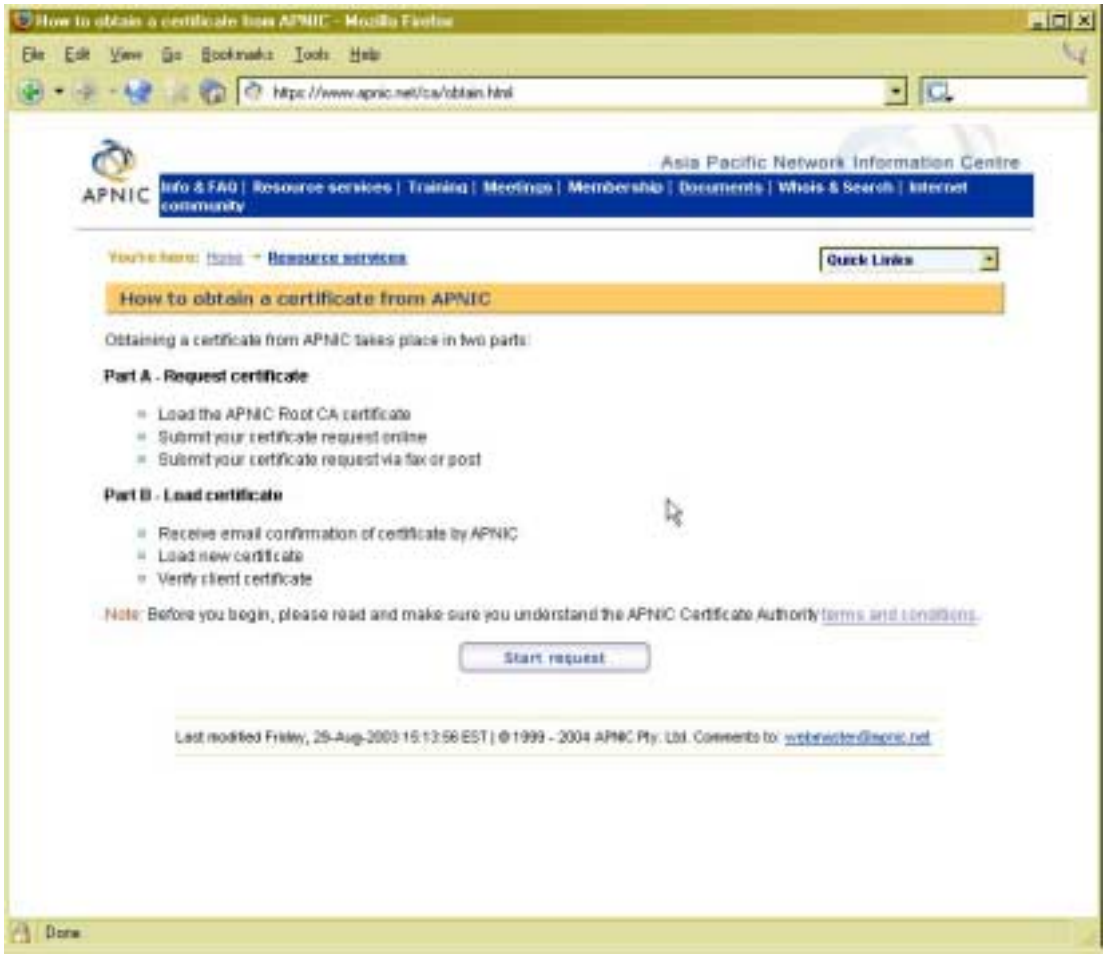


図 3-2 APNIC 認証局発行証明書の手続き[2]

このページ自体は APNIC 認証局の証明書（図 3-3）で保護された形で提供される。この証明書は、インターネットエクスプローラ及び Mozilla といった、通常使われているブラウザの CA 証明書ストアには含まれていないので、アクセス時に証明書が検証できず、受け入れるかどうかをたずねるダイアログが表示される。

[2] How to obtain a certificate from APNIC
https://www.apnic.net/ca/obtain.html

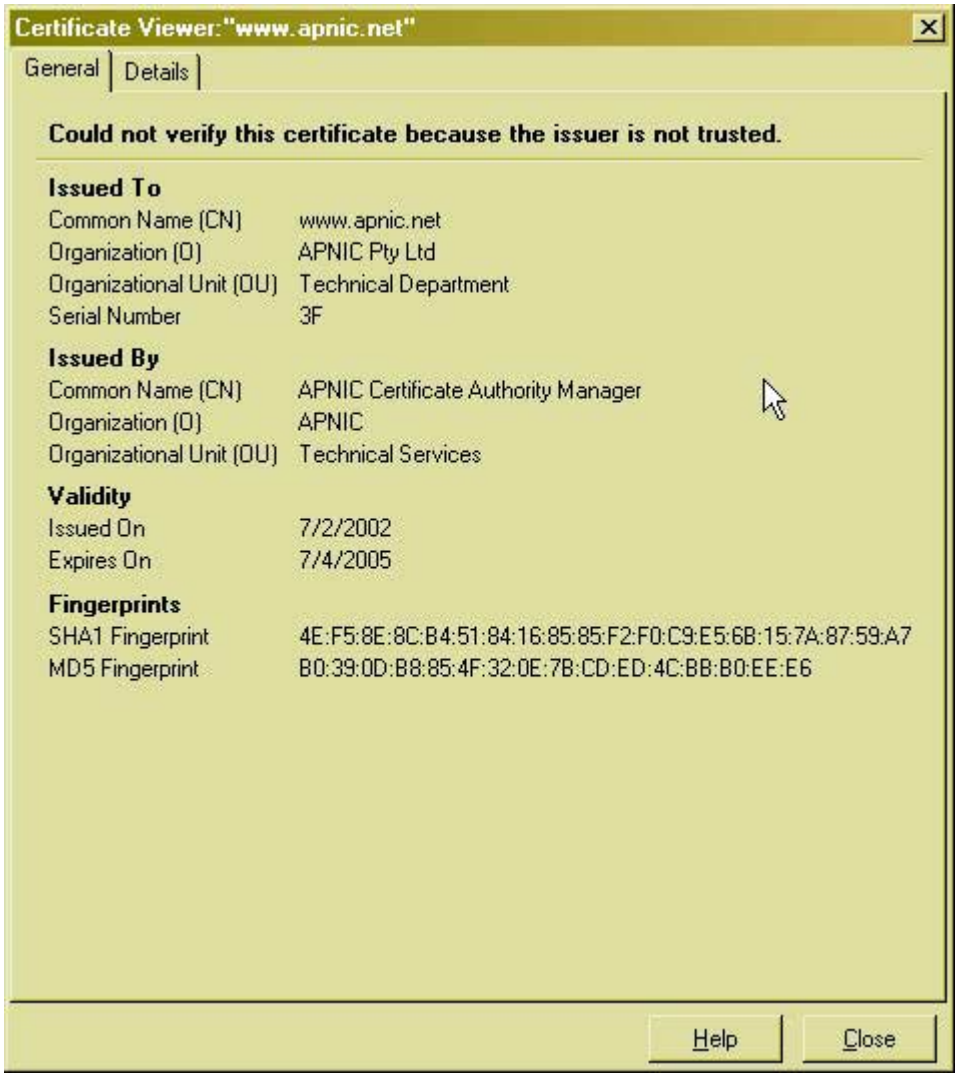


図 3-3 www.apnic.net サイトのサーバ証明書

手続きを進めると、APNIC CA 証明書をロードすることになる（図 3-4）。ここでウェブサイトの識別について、この CA を信頼することにして受け入れると、以降、APNIC ルート CA の発行する証明書が検証できるようになる。

図 3-4 APNIC CA 証明書のロード（Mozilla Firefox での実行結果）

証明書が格納されたことはブラウザから確認できる（図 3-5）。

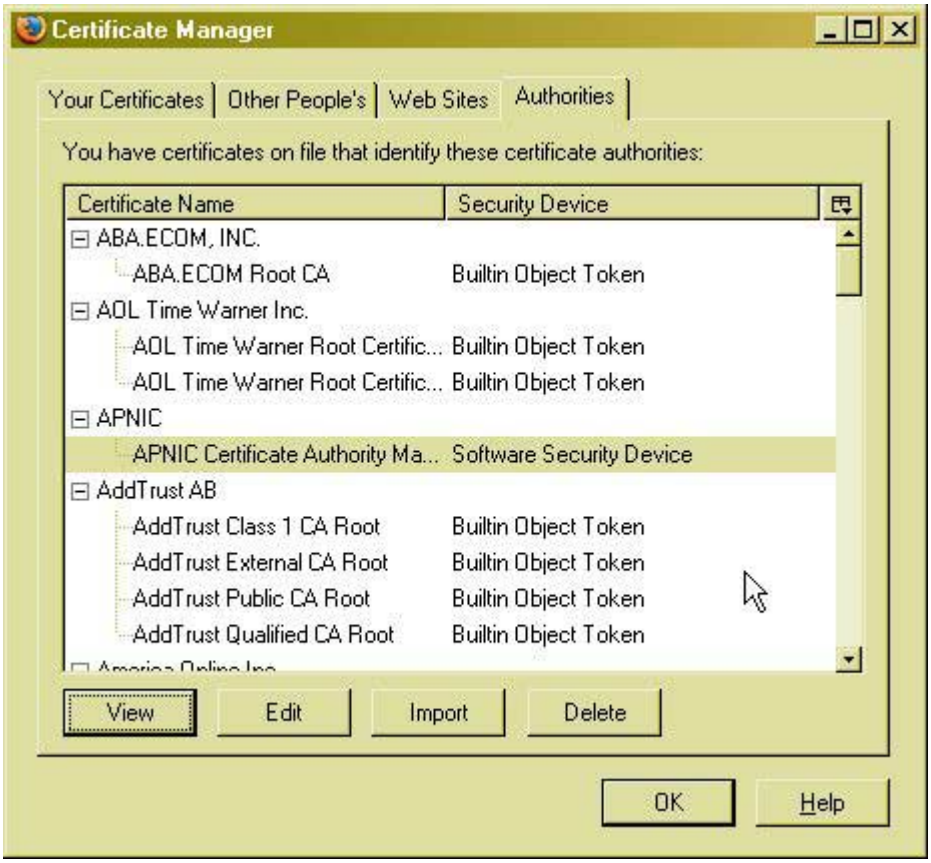


図 3-5 APNIC CA 証明書を受け入れたことの確認（Mozilla Firefox）

続けて個人証明書の発行手続きを行う。

3.3.3. EE による証明書の組み込み

ブラウザに APNIC ルート CA 証明書を組み込んだ後は、その証明書で保護された APNIC CA サイトにアクセスし、オンラインでの証明書要求申請を行う（図 3-6）。

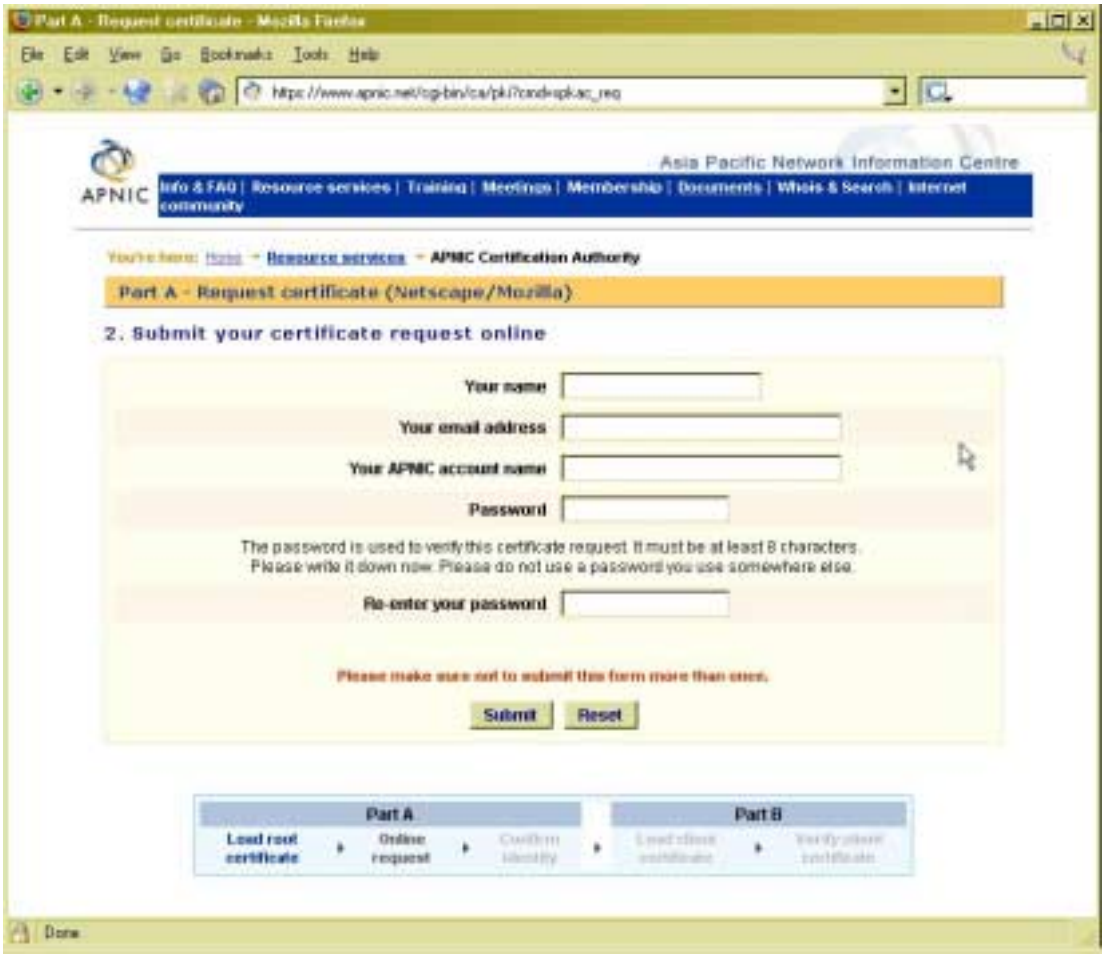


図 3-6 オンラインでの証明書要求申請

オンラインでの申請が終わりしだい、引き続き、オンラインでの申請と本人を結びつけるために、FAX または郵送で表 3-3 の内容を記載した要求申請を行う[3]。

[3] APNIC Certificate Request Form
https://www.apnic.net/ca/apnic-crf.pdf

表 3-3 紙ベースでの証明書要求申請記入内容

項目	内容
Identification document	パスポートなど写真の入った ID 文書のコピー（フォームに貼り付けるか別紙として添付する）
Your full name	オンライン申請に記入したフルネーム
Your email address	オンライン申請に記入した電子メールアドレス
The name of organization	所属する組織名
APNIC account name	APNIC アカウント名
Passwd	オンライン申請に記入したパスワード

このように、オンラインでの申請とオフラインでの申請を組み合わせることで、本人同一性の検証を行う手続きとなっている。

検証確認後は電子メールにより個人証明書の入手方法が指示される。各人は、指示に沿って、自らの環境に個人証明書を組み込むことになる。

3.3.4. ユーザ（EE）管理

APNIC CA では、RA と IA の機能を分散させることは行なってはいない。3.3.3 で述べたように、本人確認は APNIC CA 自身で行うことになる。

3.3.5. 提供されるサービス

MyAPNIC を通じて図 3-7 のサービスが提供される。

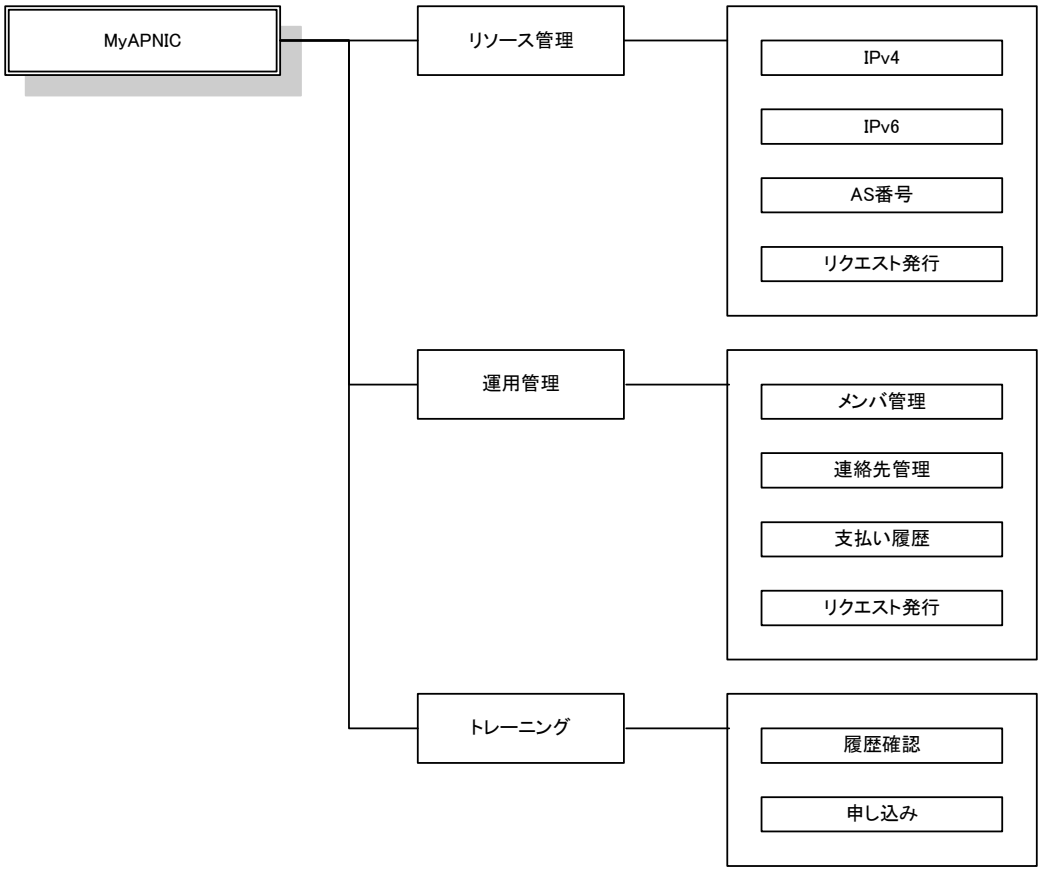


図 3-7 MyAPNIC 機能一覧

以下で、それぞれのサービスの概要を述べる。

（1） リソースマネジメント

リソースマネジメント機能では表 3-4 の機能を提供している。

表 3-4 MyAPNIC リソースマネジメント機能

機能名	機能
IPv4	保有するアドレスブロック、およびその利用率（割り当て状況）の閲覧
IPv6	同上
AS 番号	使用する AS 番号のリストと情報の閲覧
リクエスト発行	IPv4 アドレスリソース、IPv6 アドレスリソース、AS 番号に関して、APNIC ホストマスタに対する要求事項を送信し、チケット番号を受け取る機能

実際の Web インターフェースは図 3-8 のようになる（デモンストレーション）。

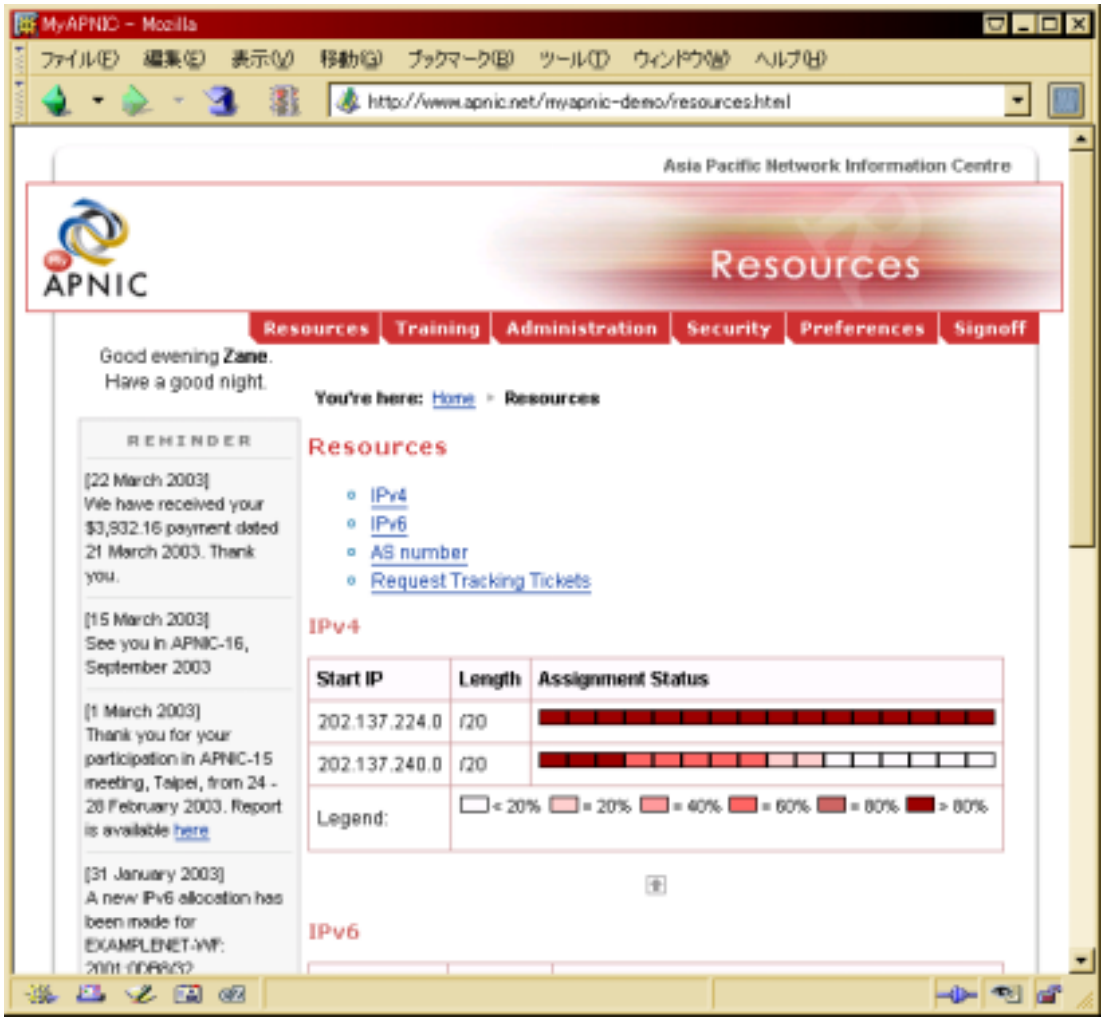


図 3-8 MyAPNIC リソース管理画面

（2） 運用管理

運用管理機能では表 3-5 の情報を管理できる。

表 3-5 MyAPNIC アカウント管理機能

機能名	機能
メンバ管理	アカウントのメンバ情報の詳細を編集することができる
連絡先管理	ホストマスタ、技術担当者、運用担当者などを追加、削除、編集することができる
支払い履歴	APNIC に対する支払い履歴を閲覧することができる
リクエスト発行	（admin@apnic.net 宛ということだが、このペインに現れる情報に関する質問、要求ということだろうか）

実際のウェブインターフェースは図 3-9 のようになる。

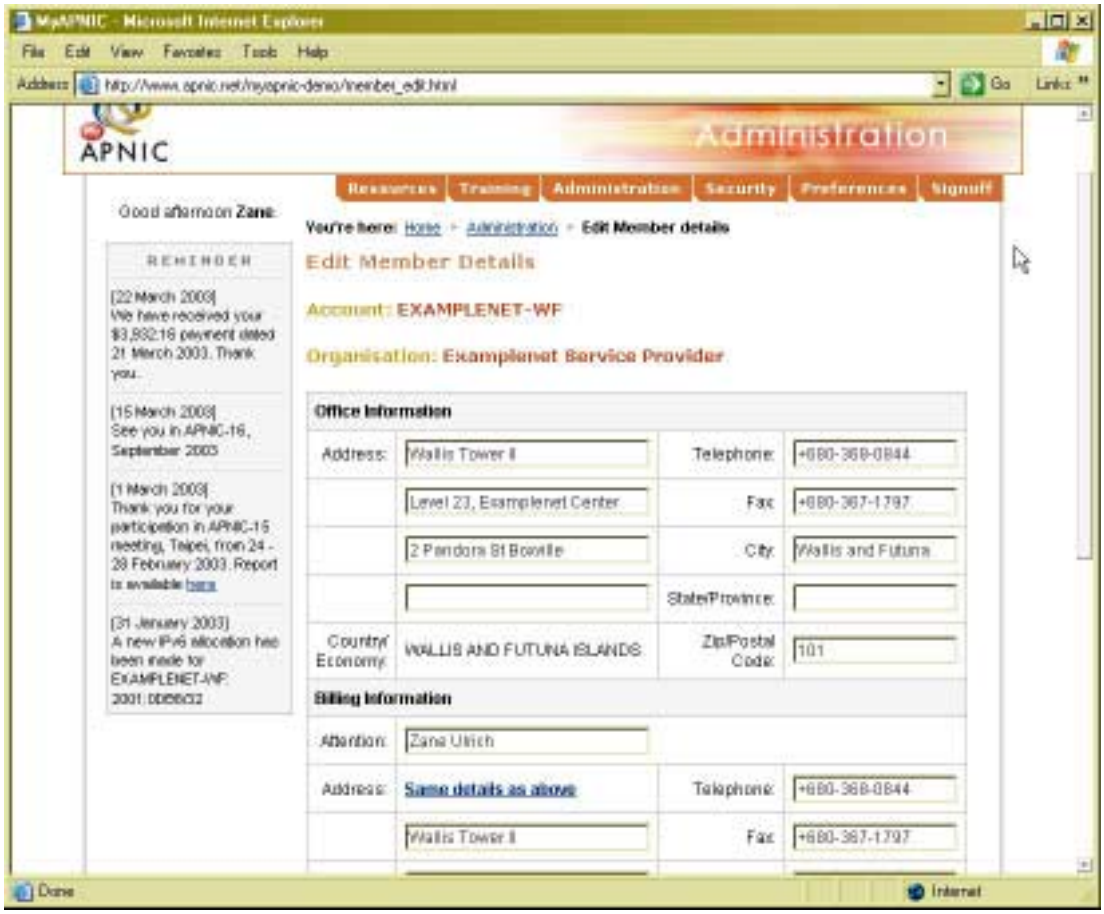


図 3-9 MyAPNIC 運用管理画面（メンバ管理）

（http://www.apnic.net/myapnic-demo/member_edit.html）

（3）　トレーニング

トレーニング機能では、表 3-6 の機能を提供している。

表 3-6 MyAPNIC トレーニング機能

機能名	機能
履歴確認	メンバの APNIC 年次総会、トレーニングなどへの参加履歴を閲覧することができる
申し込み	トレーニングの申し込みを行うことができる

実際の画面は図 3-10 のようになる。

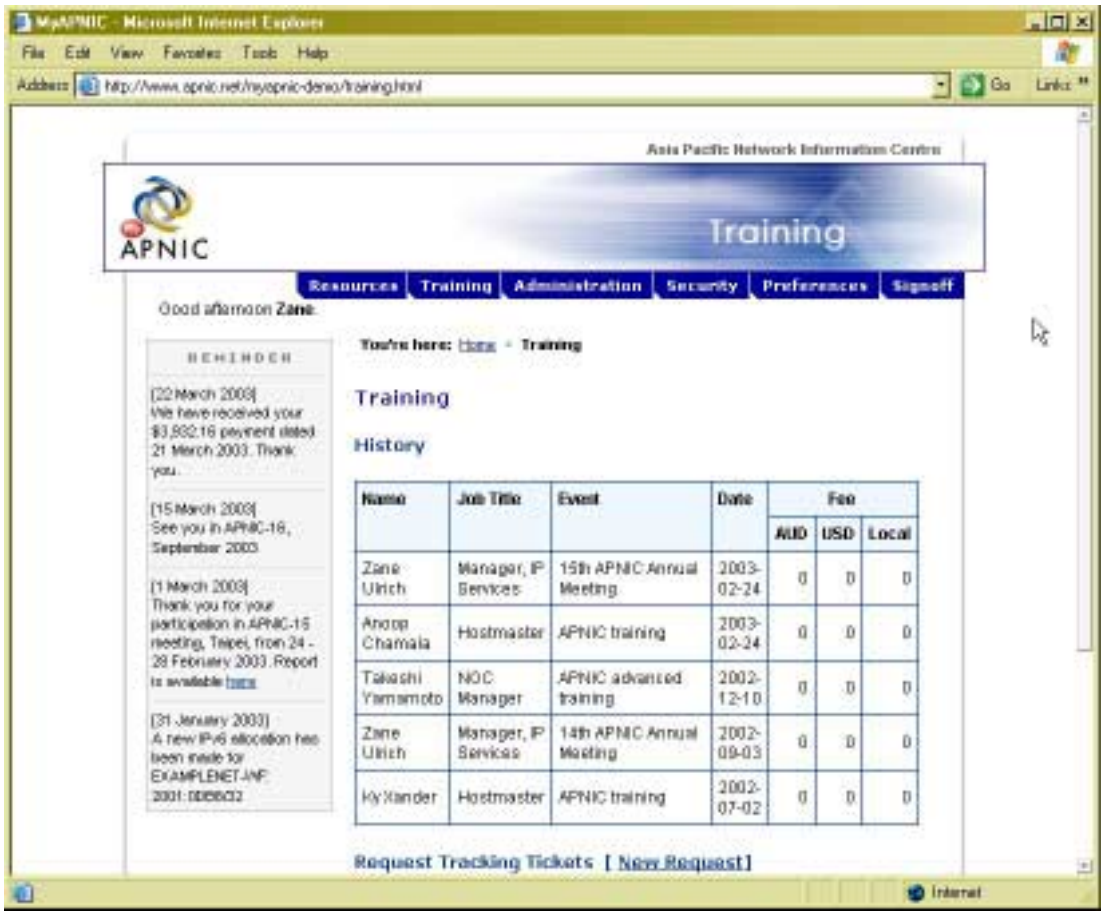


図 3-10 MyAPNIC トレーニング機能

（http://www.apnic.net/myapnic-demo/training.html）

3.3.6. 証明書の利用

ここではMyAPNICにおけるクライアント証明書を利用したアクセスコントロールについて述べる。すでに述べたようにMyAPNICでは、メンバに対し、様々な情報へのインターフェースを提供している。

これらの情報は極めてプライバシーが高いものであり、組織のメンバだからといって開示できるものばかりではない。このため、MyAPNICではメンバごとに権限を指定できるシステムを提供している。

図 3-11 は、MyAPNIC のデモンストレーション中のセキュリティ設定ページである。ここでチェックがつけられている項目は、対応するユーザ及びユーザの個人証明書が提示される際に、MyAPNIC 中で表示される情報を示している。

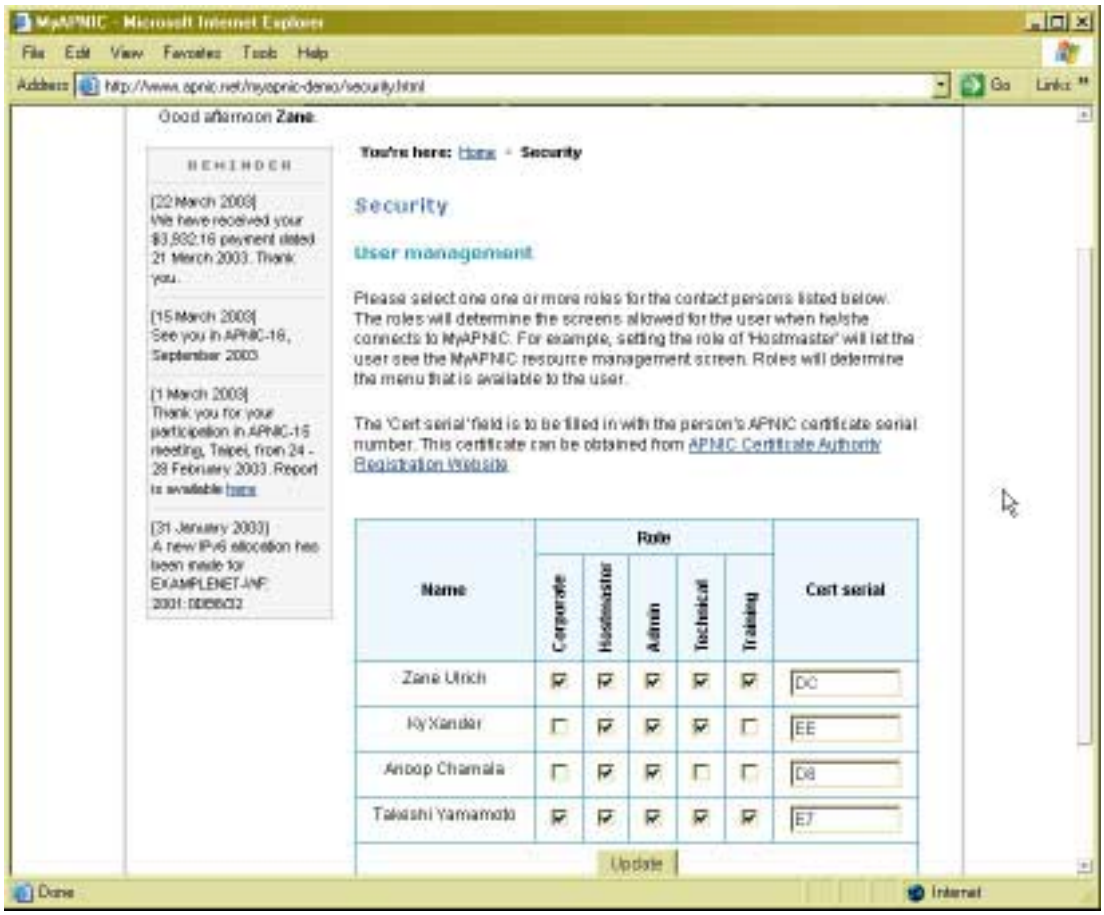


図 3-11 MyAPNIC におけるユーザアクセス権限管理

（http://www.apnic.net/myapnic-demo/security.html）

3.3.7. APNIC CA の今後

APNIC では、認証局を利用した登録情報の保護と活用について、MyAPNIC だけに留まらない検討を行なっている。APNIC の認証局の運用および技術担当者とヒアリングを行なった結果、以下のような利用方法を検討していることが判明した。

- soBGP（secure origin BGP）で使われる証明書[4]
- RIR と NIR における階層的な資源管理を踏まえたメッセージ認証の基盤構築

これらは実現可能性を検討している段階の様子ではあるが、特に soBGP の経路情報の保護を目的とする証明書は、その発行主体がインターネットレジストリであることで登録情報との同期が取りやすいというメリットがある。これはアドレスブロックの割り振り情報は、インターネットレジストリが一次情報源となると考えられるためである。

[4] Secure Origin BGP (soBGP) Certificates
http://www.ietf.org/internet-drafts/draft-weis-sobgp-certificates-01.txt

3.4. RIPE NCC

RIPE NCC（Réseaux IP Européens Network Coordination Centre）では、RIPE NCC の提供するサービスに対するインターフェースとして、SSL による保護されたウェブサイトを提供している[5]。このサイトでのサービスを LIR Portal と呼ぶ（図 3-12）。

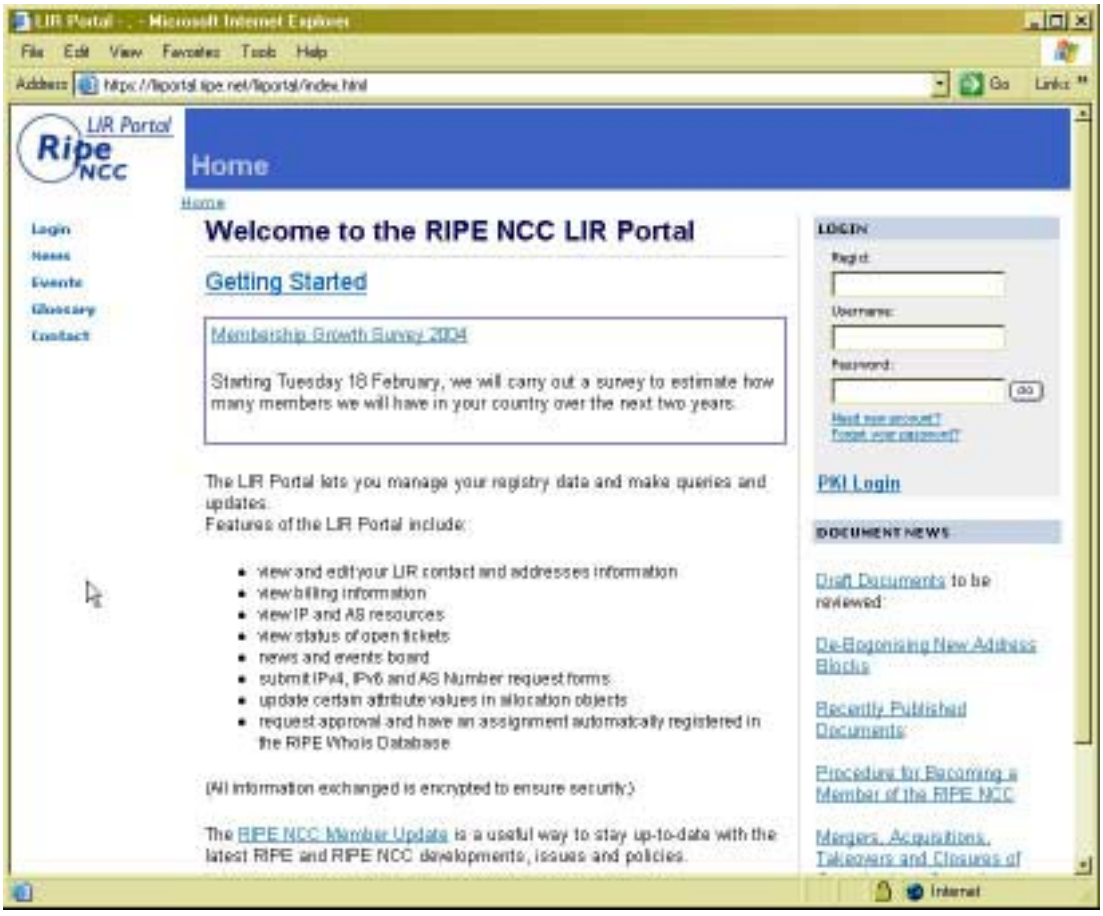


図 3-12 LIR Portal トップページ

LIR Portal では、次の各機能が実装されている。

- LIR の連絡先及び住所情報の閲覧及び編集
- 課金情報の閲覧

[5] LIR Portal
https://lirportal.ripe.net/lirportal/index.html

- IP 及び AS リソースの閲覧
- 開かれているチケット状況の閲覧
- ニュース及びイベント情報
- IPv4、IPv6 および AS 番号要求申請の提出
- 割り振りオブジェクトの属性値の更新
- 要求認可と RIPE Whois データベース中での自動的に登録された割り当て

この LIR Portal では、ウェブインターフェースによるユーザ名/パスワード認証に加え、証明書を使ったクライアント認証をサポートしている。

ここでは、クライアント認証のために発行されるクライアント証明書と認証局について説明を行う。

3.4.1. 概要

2003 年 5 月 12 日から 16 日にかけてスペインバルセロナで開催された RIPE45 でのプレゼンテーション「Improved Secure Communication System for RIPE NCC Members / Tiago Rodrigues Antao[6]」によると、RIPE NCC では、以下の目的を達成するため、安全な通信システムを実装することとなっている。

- RIPE NCC サービスへの、使いやすく、高速なインタラクション
- 統合された強力なセキュリティメカニズム
- 特権/クレデンシャル管理の支援
- ユーザにとって低い、配置及び維持コスト
- LIR にとって選択的
- 標準（X.509 PKI）のサポート

この提案では、RIPE NCC における PKI の実装は図 3-13 ように示されている。

[6] Improved Secure Communication System for RIPE NCC Members
http://www.ripe.net/ripe/meetings/ripe-45/presentations/ripe45-lir-pki/

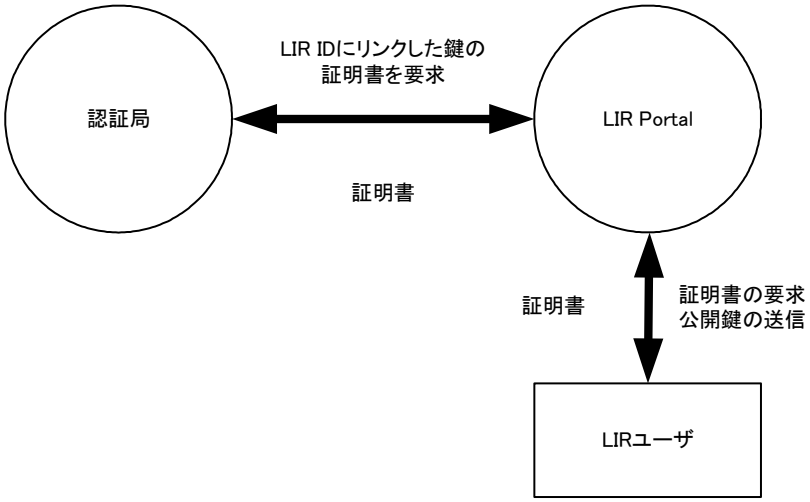


図 3-13 証明書管理サイクル[7]

以下では、RIPE NCC における PKI の活用として、LIR Portal の詳細について述べる。

3.4.2. EE による CA 証明書の組み込み

LIR Portal のサーバ証明書は、ブラウザの配布イメージに組み込まれている認証局から発行されたものであるため、明示的な組み込みは不要である。

3.4.3. EE による証明書の組み込み

ここでは LIR Portal におけるクライアント証明書の取得手順について述べる。クライアント証明書の発行に際して、本人性の確認などを行うために RA が配置される。LIR Portal では、PMS（Privilege Management System）と呼ばれる権限管理システムを導入している（図 3-14）。このシステムでは、RIPE NCC より、各 LIR に管理者権限を持つ証明書が一枚発行される。各 LIR では、この証明書を用いて、ユーザに対する証明書を発行することになる。この形態により、RA を分散配置させることが出来ている。

以下に、LIR 管理者アカウントの作成と、LIR ユーザアカウントの作成について述べる。

---

[7] certificate management cycle
http://www.ripe.net/ripe/meetings/ripe-45/presentations/ripe45-lir-pki/page9.htm

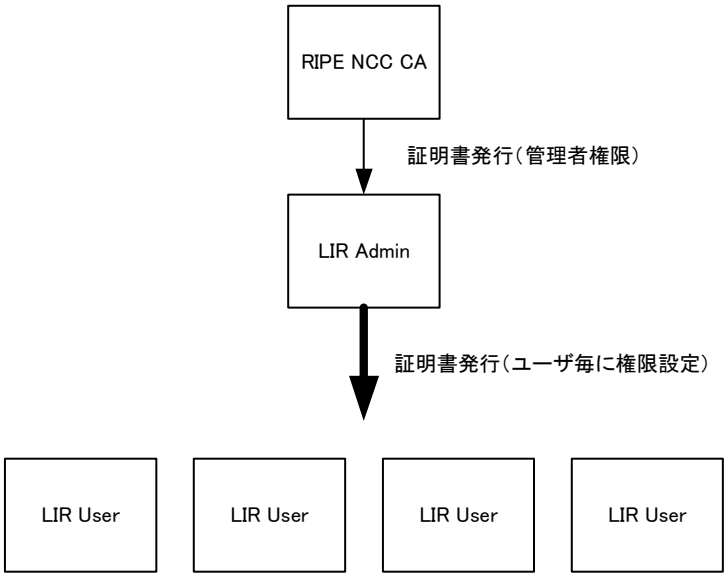


図 3-14 RIPE NCC PMS

3.4.3.1. 管理者アカウントのパスワード設定

各 LIR は管理者ユーザを一つ持つ。このアカウントはユーザアカウントを作成し、その権限を設定および修正することのできるアカウントである（その他のこと、レジストリ情報の閲覧などは出来ない）。

まず、このアカウントのパスワードを設定し、ユーザアカウントの生成を行う。この手続きは三段階に構成される。

- RegID（レジストリ識別子）、LIR への電子メールアドレスおよび FAX 番号を提供しなければならない。これは請求書を発行するために必要となる。
- LIR Portal[8]からこれらの情報が申請されると、LIR は「Fax Confirmation Number」と「E-mail Confirmation URL」が記載されたファックスを受け取ることになる。
- 「E-mail Confirmation URL」に示される URL で「Fax Confirmation Number」を与える。これによりアカウントが有効になる。

これ以降は、選択したパスワードを使って LIR Portal にログインできる。

[8] Member Services
https://lirportal.ripe.net/lirportal/activation/activation_request.html

3.4.3.2. ユーザアカウントの生成

ユーザ証明書の RA は LIR 管理者が務める。このため、LIR 管理者は、ユーザ証明書の発行及び廃棄に関する承認について責任を負うことになる。

3.4.4. ユーザ（EE）管理

前述の PMS を通じて、RA 機能の分散（階層化）が図られている（図 3-15）。RIPE NCC が RA として承認及び本人確認を行うのは LIR 辺り、一名と限られており、ユーザ証明書の発行及び管理負荷は、各 LIR に分散できる。

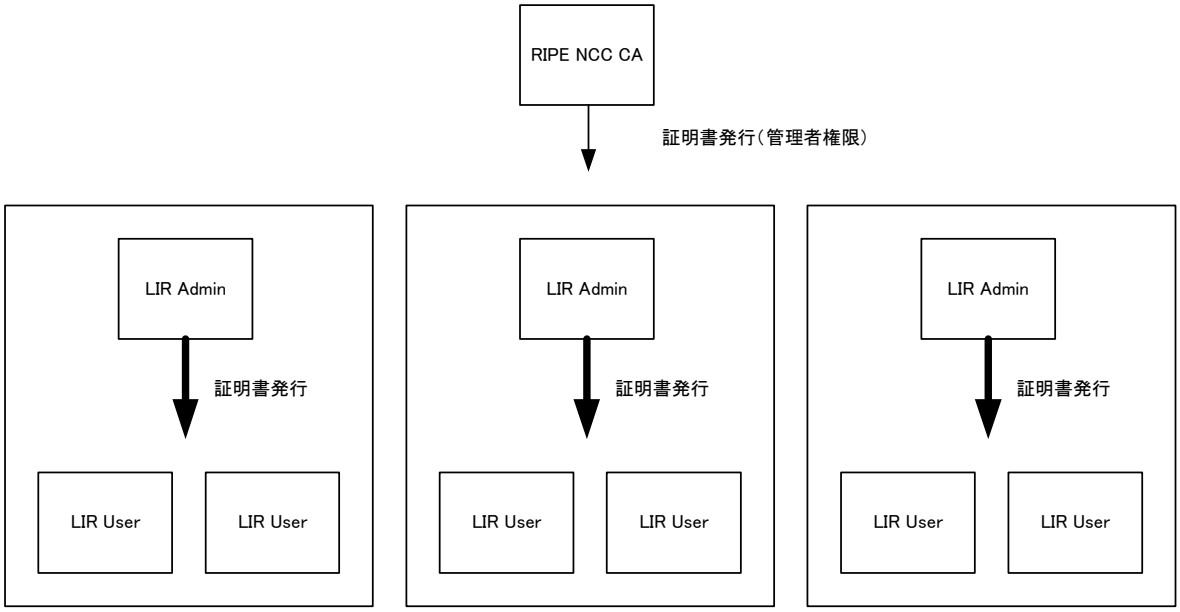


図 3-15 PMS による RA 機能の分散

各 LIR 管理者は RIPE NCC CA と安全な通信経路上で証明書発行依頼を行うことになる。

3.4.5. 認証局の利用

レジストリシステムにアクセスする通信経路には、LIR Portal だけでなく、電子メール経由のアクセスも依然として可能である。RIPE NCC では、RIPE NCC のホストマスタから LIR に送られる電子メールを安全にするため、次の選択肢から、任意のものを選択可能としている。

- PGP 署名つき電子メール（デフォルト）
- PGP 暗号電子メール
- X.509 署名の利用
- X.509 暗号の利用（LIR の公開鍵で暗号化）

また、特別に機密性の高いデータを含んだデータ通信を行う場合など、必要に応じて、より安全な通信方法を選ぶことが出来る。

3.4.6. RIPE NCC の認証局の今後

X.509 PKI インフラストラクチャの構築は、LIR と RIPE NCC サービスとの認証機構にとどまらず､サービス間の統合のためにも使われる｡この統合は主に LIR Portal を通じて行なわれると考えられる。

以下に、X.509 PKI の今後の利用可能性として、RIPE データベース、リバースデリゲーションについて述べる。

3.4.6.1. RIPE　データベースへの応用

RIPE データベースは X.509 PKI に基づいた新しい認証機構が利用可能になる。

最初の段階では、LIR Portal によって発行された証明書だけが、RIPE データベースに受け入れられる。このことは LIR ユーザでなければ、この新しい認証機構を利用することができないことを意味する。

新しい認証方法のサポートは､X.509 識別名を示す auth: 属性を追加するオプションによって行なわれる｡発行された証明書のコピーを key-cert オブジェクトに加える必要はない。

LIR ユーザはこの新しい認証を電子メールと webupdates の双方で用いることが可能となる。このことで、RIPE データベースの更新は、パスワードによる現在の認証よりも安全になるといえる。

3.4.6.2. Reverse Delegation

LIR は、リバースデリゲーション情報に対するいかなる変更も、X.509PKI によって認証されなければならないことを宣言することが可能となる。つまり、LIR からのすべての要求は、承認されるために署名されなければならないことを意味する。

さらに加えて､リバースデリゲーション情報の修正は LIR Portal においてもサポートされることになる。LIR Portal に対して適用される認証と暗号と同じものがリバー

スデリゲーションにも適用されると考えられている。

3.5. ARIN

ARIN（American Registry for Internet Numbers）では、よりよい認証方式の検討が行なわれ始めている。現段階では、PKI 配備に向けてのベータテストを行なっている段階であり、他 RIR のように、証明書組み込み、ユーザ管理といった具体的な手順については検討の段階である。このため、この節では、ここ数年における ARIN での認証に関する検討状況、および今後の計画について記述する。

3.5.1. 2002 年 ARIN X Open Policy Meeting における発表

2002 年開催された ARIN X Open Policy Meeting での Cathy Murphy 氏によるプレゼンテーション「Next Steps for the ARIN Registration Database[9]」では、認証メカニズムとして次のものが提案されていた。

- PGP 証明書の利用
- X.509 証明書の利用
- Login/SSL パスワードの利用

また、拡張された認証を必要としているプロジェクトとして次のものがあげられている。

- Web ベースのメンバーサイト
- Routing Registry 経路認証

3.5.2. 2003 年 ARIN XI Open Policy Meeting における発表

2003 年に開催された ARIN XI Open Policy Meeting での Tim Christensen 氏によるプレゼンテーション「Authentication[10]」では、最初に実装する認証方式として X.509 証明書をあげている（PGP や MD5 といった認証方式は将来の拡張）。

この理由としては次のものなどがあげられている。

- Public Policy Meeting での議論から証明書が良いという評価を得た
- PGP は公開鍵サーバが必要になる
- 他 RIR の実装を鑑みて

---

[9] ARIN X Public Policy Meeting Minutes
http://www.arin.net/library/minutes/ARIN_X/ppm.html

[10] ARIN XI Public Policy Meeting Minutes
http://www.arin.net/library/minutes/ARIN_XI/ppm_minutes_day2.html

また、X.509 証明書の用途として以下のものがあげられている。

- 電子メールテンプレートの保護（認証、暗号化）
- ウェブトランザクションの認証
- ARIN によって生成されたデータの認証

認証方式として、制御、セキュリティ、活用性のバランスが最も優れているとされている。

3.5.3. 2003 年 ARIN XII Open Policy Meeting における発表

2003 年に開催された ARIN XII Open Policy Meeting での Tim Christensen 氏によるプレゼンテーション「Cryptographic Authentication[11]」では、ARIN における暗号を利用した認証の現状について述べられている。

目標としては次のものが挙げられている。

- 受け取る電子メールの正当性の改善
- データベースの完全性の改善
- 送信される電子メールの認証の改善

要求事項としては次のものが挙げられている。

- 送信者アイデンティティの検証
- 内容が改ざんされないことを確実にする
- 顧客信頼性の改善
- 受託責任のデモンストレーション
- 適用可能な IETF RFC の遵守
- 産業の事業継続計画の追従
- 将来の拡張性

現在のプロジェクトのスコープについては次のものが挙げられている。

- テンプレートベースでの登録を安全にする
- ARIN CA の確立
  - 手続きの識別
  - ワークフローの定義
- アウトバウンド通信を安全にする
  - 電子メールの返答

[11] ARIN XII Public Policy Meeting Minute, Day 1
http://www.arin.net/library/minutes/ARIN_XII/ppm_minutes_day1.html#11

- 証明書

今後の展開として、配備及び実装への道筋が示されている。

POC（Point Of Contact）は証明書署名要求（CSR）を作成する
↓
POC は ARIN に CSR を送信する
↓
ARIN は CSR の内容を検証する
↓
ARIN は証明書を生成、データベースの更新を行ない、証明書を POC に送信する
↓
POC はテンプレートの署名に証明書を用いる
↓
ARIN は POC によって申請されたテンプレートを認証する
↓
POC は認証証明書を維持する

配備に向けてのベータテストの実施項目として次のものがあげられている。

- 識別プロセス
- テスト環境の構築
- 変更プロセスの提示
  - CSR（証明書署名要求）生成
  - ARIN 認証局の稼動
  - 署名テンプレート認可及び拒否
  - 認証失敗に対する対処

今後のタイムラインとして次のものが示されている。

- 要求事項と必要条件の確立
- 必要条件の達成
- オプションの調査
- 現存する RIR の実装の理解
- ユースケースの識別
- テストベッドの確立
- 最初に配備する手法の選択
- 変更プロセスの策定

- ベータコミュニティの形成とテスト
- 配備
- 他の手法の実装
- Mail-From の廃止

この発表が行なわれた時点では、ベータテストの第一フェーズの実施中で、ユーザによる証明書署名要求の生成と ARIN が証明書を発行することなどを評価している。

次回、ARIN XIII では、「Using X.509 Authentication with ARIN's Database」と名づけられたワークショップが開催される予定となっており、オンラインで証明書を要求するプロセスの概要が提示される予定となっている。

3.6. まとめ

APNIC や RIPE NCC では、認証局を運用すると共に、資源管理システムの認証に証明書を利用することが可能になっている。証明書の用途は Web を使った申請などに使われる https だけでなく、暗号を利用した電子メール S/MIME の活用も開始している（RIPE NCC）。サービスと認証用途の証明書は、今後活用されていくと考えられる。ヒアリングの結果、経路情報のプロトコルである BGP での情報の保護にも使う考えを持っていることもわかった。

APNIC は APNIC CA を運用し、MyAPNIC と呼ばれる Web サービスを提供している。MyAPNIC はバージョンアップを重ねており、資源管理機能はまだ実装されていないものの、Executive Council 選挙の機能や連絡先情報の変更などに対応している。APNIC CA はスタンドアローンで運用されており、ユーザが証明書を Web ブラウザに組み込む形で運用されている。CP/CPS の公開などは行なわれていない。RIPE NCC は、データベースシステムにおける証明書の活用に力を入れている。暗号を用いた認証機能では PGP が主流であったが、同様の方法で PKI を使った S/MIME が利用可能になりつつある。登録情報データベースに X.509 形式の証明書を組み込む書式も提案され、実装が進んでいる。ARIN では、証明書を利用した認証に関する議論が進んでいる段階である。ARIN の次回のミーティングでは認証機能に関するワークショップが開催される予定であり、関心の高さを伺うことができる。しかし IP アドレスといったアドレス資源ではなく、ドメイン名を基本とする証明書を利用する可能性がある。

RIR における認証局の状況の中で、JPNIC の認証局に関連することは、証明書の用途・RIR におけるデータ交換と認証方法・認証業務のレベルの 3 点であると考えられる。

- 証明書の用途
  証明書には認証用か署名用かという違いがある。RIR との連携の観点から JPNIC の認証局でも比較的運用しやすい認証用の証明書から始めるのが適切だと考えられるが、第 4 章で述べる認証基盤や RIR のデータ認証を踏まえると署名用の証明書も検討する必要があると考えられる。

- RIR とのデータ交換
  RIR においてアドレス資源の不正／浪費的な利用に関する問題が議論されることがあるが、RIR 間でのデータ同期を含めた全体的な議論は少ない。レジストリの間で登録情報を交換すると、世界規模でアドレス資源管理の情報を検証できるようになるが、その為には電子署名付きのデータがやりとりできる状態になる必要がある。EPP/CRISP といった、登録情報を扱うプロトコルの調査研究が必要となる。

・ 認証業務のレベル

　限られた相手の認証用の証明書を発行するのが RIR における認証局の状況であるが、世界規模で署名を検証するような認証局の場合は、よりセキュリティレベルの高い認証局が必要なる。RIR では認証用の証明書を発行するシンプルな構成であるが、JPNIC の認証局は認証情報の応用も検討しており、インターネットにおける基盤的な認証基盤を目標としているため、CP/CPS の策定から認証局ソフトウェアの活用など、よりセキュリティレベルの高い運用を目指す。

本調査研究で目標としているデータ認証が可能になる状況は、RIR の認証局やレジストリシステム、および認証業務と関連している。従って、今後継続して RIR の認証局について調査研究を行うとともに、IETF におけるレジストリ関連のプロトコルの策定状況の調査が必要と考えられる。

第4章 認証業務の検討

内容

- アドレス資源管理における認証基盤
- JPNIC 認証局と今年度の活動範囲
- 認証業務の検討上の留意事項
- 業務モデルについて
  - レジストリ入出力認証システムの検討

4. 認証業務の検討

JPNIC の認証業務は、インターネットレジストリにおけるレジストリデータの保護という目標に沿いつつ、一つのレジストリである JPNIC において実施されるものになる。また JPNIC における認証業務は、認証基盤の一つとして認証情報の応用することを視野に入れており、運用レベルを向上させることができなければならない。本章は、第 2 章で述べたレジストリデータの保護という大きな観点から JPNIC の認証局に観点を写し、この業務の検討を行う。

はじめにアドレス資源管理とレジストリデータの保護の観点から、JPNIC における認証システムの目指す認証モデルについて述べ、JPNIC の認証局の目的を明らかにする。次に認証業務の検討をまとめ、検討された業務モデルについて述べる。これらを下記のような項目に従ってまとめた。これらの項目の検討の流れを図 4-1 に示す。

認証業務の検討を行う際に、いくつかの留意事項をテーマとして掲げ、それぞれの考え方に則った設計を行った。ここで挙げたテーマは、監査への配慮、不正抑止・防止の確立、レジストリの業務体系の三つである。本章ではこの留意事項について重点的に述べ、その結果として作成された業務モデルを紹介する。この業務モデルは、第 5 章の認証業務規定（CP/CPS）の検討や第 6 章の認証局ソフトウェアの検討の元になっており、認証業務の検討の上で根幹となった。

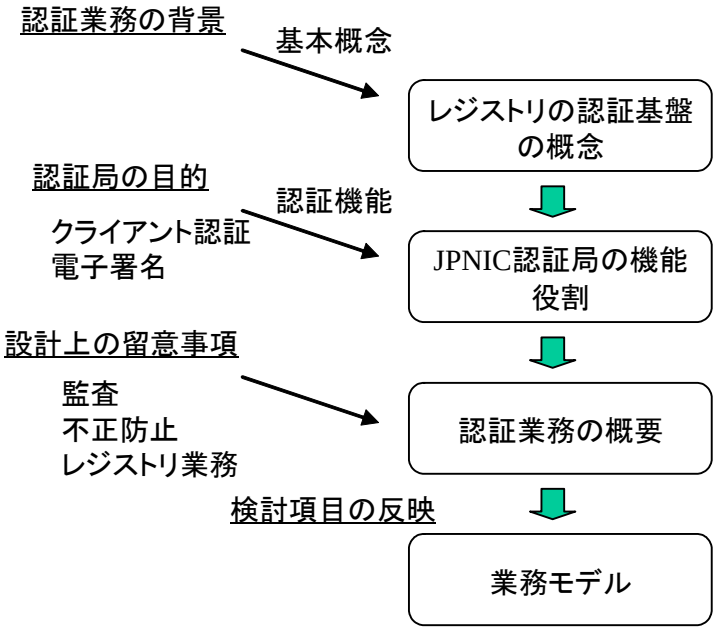


図 4-1　業務モデルの検討の流れ

4.1. アドレス資源管理における認証基盤

4.1.1. 登録情報を利用した認証

アドレス資源の登録情報の保護および活用する認証業務の検討を始めるにあたり、認証のモデルをどのように置くかということは大きな課題であった。PKI（Public-Key Infrastructure：公開鍵基盤）を用いて行なうことができる電子的な認証にはいくつかの種類があり、理想的だと思える手法は実現可能性が低いと考えられた。

2002 年度の「IP アドレス認証局のあり方に関する調査研究」では、認証モデルをトランスポートセキュリティとオブジェクトセキュリティの二種類に大別した。トランスポートセキュリティにおける認証とは、安全な通信路の確立の為の通信相手の認証を行なう手順であり、オブジェクトセキュリティにおける認証（データ認証）は特定のデータの出所と正当性が意図した通りのものであるかどうかを確認する手順である。2002 年度の調査研究の結果から、インターネットレジストリにおけるアドレス資源管理の安全性は、登録情報の正当性に最も大きく依存するものと位置づけている。従って、この正当性の確保がインターネットレジストリにおける認証局の最たる目標だとした。比較的実現が容易である登録時の安全性をトランスポートセキュリティのモデルを使って検討を進め、次に登録情報の正当性をオブジェクトセキュリティのモデルを使って検討することとした。

認証モデルの検討にあたって更に検討を要したことは、発行される証明書をどう識別するか、という問題である。IP アドレスは、インターネットにおいて通信相手を識別するアドレスである。しかしドメイン名と異なり、ユーザは多数の IP アドレスを覚えたり、IP アドレスから通信相手を連想したりすることは難しい。認証局の発行する証明書は、相手の識別子を含むことによって強力な通信相手の認証機能となりうる。しかし、この識別子にユーザが意味を読み取ることができないものを含めるときには、認証システムとして注意深く設計を行わなければならない。本調査研究では、認証業務の設計にあたり、「IP アドレス認証局」という名称から想像されるような IP アドレスを識別子として持つ証明書の利用について考えるより先に、識別子の実在物との組み合わせ（バインディング）に着目することにした。

つまり予め実在するエンティティによって登録された IP アドレスの情報を、後になってから電子的に検証できるようにするという状況を目標とした。登録者の認証と登録内容への電子署名によって、この登録情報と関連した証明書がアドレス資源の認証基盤で使われるようにするためである。

4.1.2. アドレス資源と認証基盤

第 2 章で述べたアドレス資源の管理権限の委譲モデルを実現するには、権限委譲を確認する必要がある。この権限委譲の確認の連鎖によってレジストリにおける認証基盤が構築されると考える。

レジストリは世界規模でアドレス資源の管理を行なっているため、この認証基盤は、異なる地域の IP アドレスの所属や管理主体を調べることが可能になるが、それにはレジストリの認証局の間で認証された関係が必要となる。この関係構築と検証が、IP アドレス認証局の本質である。

4.1.3. 認証基盤構築の段階

認証基盤の構築には、認証局側の連携から構築する方法と、ユーザの認証機構から構築する方法の二つが考えられる。しかし第 3 章で述べたように、他の RIR（APNIC、RIPE NCC）における認証局がユーザ認証の機能を実現することに取り組んでいることから、いきなり認証局同士の連携を検討するのは得策ではない。長期的な視点では、まずアドレス資源の情報を登録する LIR の認証を強いものにし、次に登録情報の検証環境の構築を行うという段階になると考えられる。最後にレジストリ間の情報同期、ディレクトリサービスとしての whois の連携といった段階的構築が現実的であろう。

この段階的な認証基盤の構築には、RIR における認証局の連携が始まっていない今の段階において、JPNIC 認証局による LIR の強い認証を実現し、登録情報の確実性を向上しておくことが必要になると考えられる。

4.1.4. LIR の認証

NIR は RIR によって確認された組織であり LIR は NIR によって確認された組織である。この連鎖の続く組織によってアドレス資源管理の業務が行われる。

日本では特殊な IP アドレスでない限り、LIR によって割り当て業務が行われる。登録されるアドレス資源の情報は LIR によって運用されるものであるため、アドレス資源の認証基盤を構築するには、LIR の認証が重要である。従ってアドレス資源の証明に使われる始めの IP アドレス認証局は、LIR の認証と登録情報の確実性を向上させるものと位置づける。

4.2. JPNIC 認証局

本節では、第 2 章で述べたインターネットレジストリの認証基盤の考え方に基づき、単一のレジストリにおける認証局（JPNIC 認証局）について述べる。はじめに JPNIC 認証局の意義について述べ、次にこの認証局の構築にあたって今年度の活動範囲と設計について述べる。

4.2.1. JPNIC 認証局の意義について

JPNIC 認証局はアドレス資源管理の確実性の向上という考え方に基づいた認証基盤を構成する要素になると考えられる。JPNIC 認証局の意義は、これを利用した認証システムにあるため、構築の検討を行った認証システムについて述べる。

4.2.1.1. JPNIC 認証局を用いた認証システム

はじめに登録情報の確実性向上を目指し、認証局を活用した認証システムを構築する。この認証局は、エンドユーザにクライアント証明書を発行することを目的としたものである。このクライアント証明書を用いて、システムアクセスの際にユーザを認証する。これにより、レジストリデータの編集作業をデータの所有者のみに限定することができる。

合わせてユーザの登録手続きなどを規定する。この手続きの際に本人確認を行っておく。このことで、クライアント証明書の信頼性が強固なものとなり、認証業務および登録情報の安全性向上につなげることができる。

このような、システムアクセスに認証を導入する方法は、データ保護の観点において、APNIC の CA プロジェクトや RIPE NCC の LIR Portal と類似のものといえる。

本認証システムでは、CP/CPS（Certificate Policy and Certification Practice Statement）の策定と公開を通じて、認証局の信頼性と登録情報の登録信頼性を、ユーザ一般に表明する。

この認証システムを用いることで、各種レジストリデータの保護に関する諸問題（改ざん、盗聴、正確性）を解決することができる。ここでは、次の機能を提供することを想定する。

- ユーザ認証
- 転送データの機密化
- 転送データの完全性の保証

実装としては、SSL/TLS（Secure Sockets Layer[1]／Transport Layer Security[2]）を

[1] SSL 3.0 Specification
http://wp.netscape.com/eng/ssl3/
[2] The TLS Protocol Version 1.0 (RFC2246)

想定している。図 4-2 で示されるように、レジストリへのデータ参照／登録／変更に関わる通信路を保護する。S/MIME については別途検討を行っている。

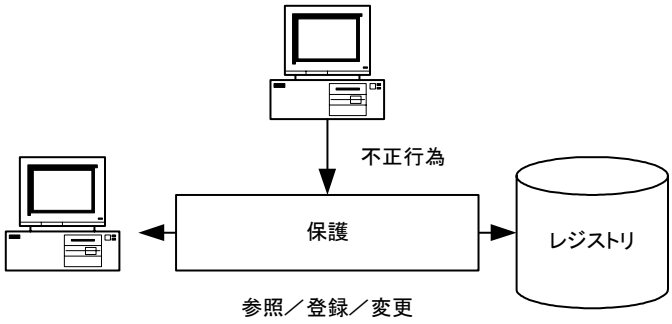


図 4-2 レジストリデータ入出力の認証

4.2.1.2. 登録情報の正当性確認機能の用意

次に登録情報の正当性を確認するための仕組みを用意する。電子署名を用いて、公開されるデータの保護を行なうことにより、Web ブラウザなどで JPNIC 認証局を信頼する設定にしているユーザが登録情報の登録正当性を検証することができるようになる。

このメカニズムを APNIC や RIPE NCC またはアジア各国の NIR と連携することができれば、世界の規模でアドレスの割り振り情報を検証する基盤を構築することが可能になる。

この目標を達成するためには、システム構築だけでなく、RIR や他 NIR とのデータ交換や通信プロトコルの標準化を踏まえた検討が必要になる。また安全性についてもデータ認証システムであるため十分な検討が必要になる。

4.2.1.3. 階層的認証局の運用

次に登録情報を証明する基盤の規模拡張性を踏まえると、LIR においても認証局が運用され、業務担当者を始め登録情報システムと連携するための認証基盤が整備されている必要がある。

LIR が発行した証明書を用いて登録情報の証明を行なうことで、登録処理を局所化することができ、より多くのデータや多種のデータを扱うことができると考えられる。

このとき、認証基盤のトラストポイントは NIR ないし RIR となる。PKI ドメインをまたがる認証については相互認証などの認証局同士の連携が必要となる。

---

http://www.ietf.org/rfc/rfc2246.txt

4.2.2. 認証局の構築

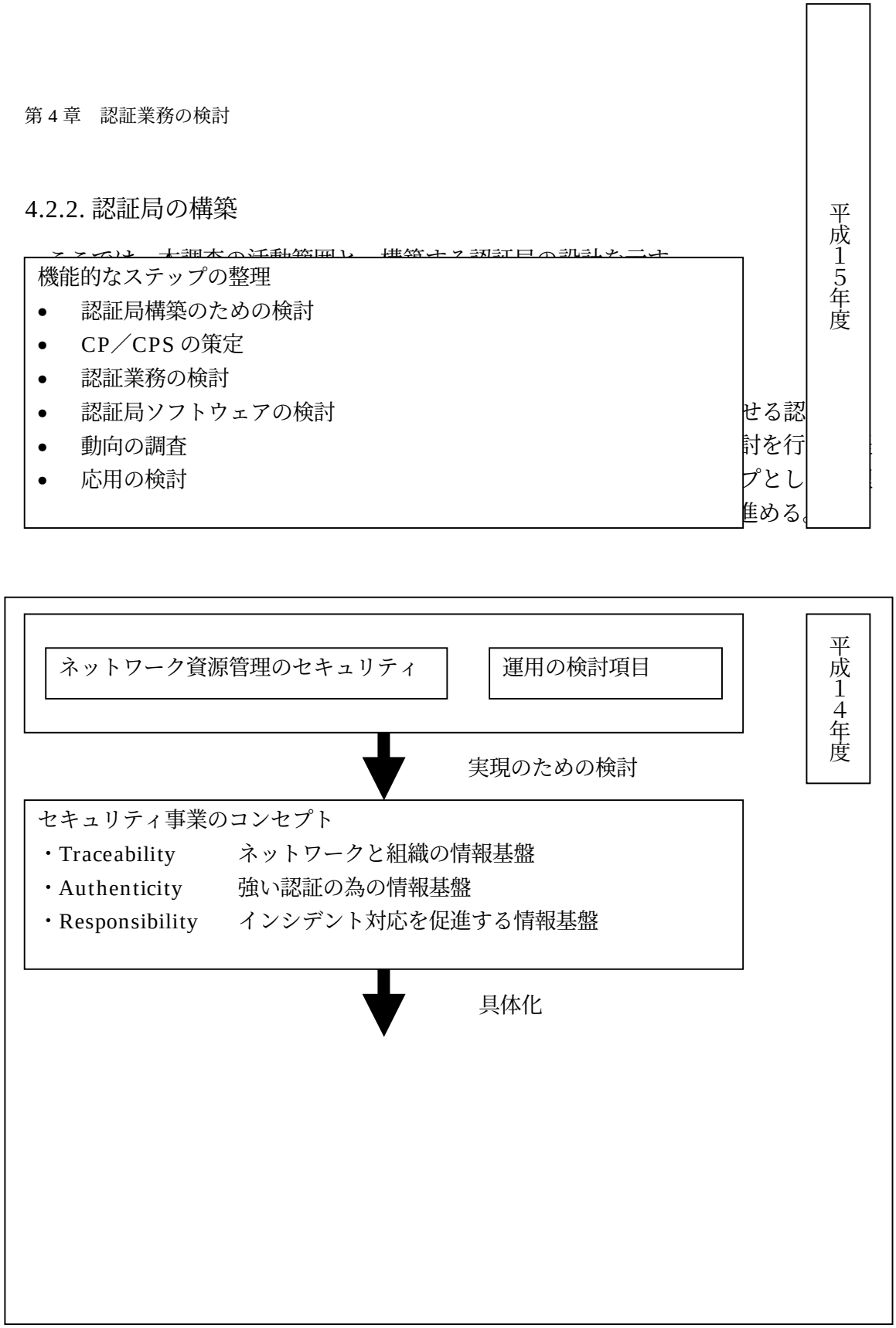


図 4-3 昨年度の活動と今年度の活動範囲

4.3. レジストリ入出力認証システムの検討

レジストリに対するデータの入出力の際に、証明書を用いたユーザ認証を行い、さらに機密、完全性を提供することで、レジストリデータの確実性を高めるシステムを検討する。

その検討方法として次のプロセスを提案し、次節以降の議論はこれに沿って行うこととした。

- 留意事項の決定
- 業務概念（モデル）図作成
- CP/CPS の項目に沿った検討
- 機能リスト作成
- ソフトウェアの検討
- 運用マニュアル作成
- システム・ネットワークの検討

また、議論を展開する際には、ある程度の品質を持った認証局を適切なコストで構築する過程を文書化し、他組織での認証局構築に参考となるよう配慮する。

4.4. 認証業務の設計上の留意事項

始めに、本調査研究における認証業務と認証システムを開発・検討するにあたり、以下の留意事項を設定した。

- 監査への配慮
- 不正抑止・防止（アクセスモデル）の確立
- レジストリの業務体系への適合性

これは将来、基盤的な認証機関となった場合に、十分な強度と信頼性を確保するためである。2003 年度の「IP アドレス認証局のあり方に関する調査報告書」の第 4 章にあるように、認証局の監査基準をどこまで準拠するか決定することよって、認証局の運用の強さが決まる。もちろん監査基準に関与せずに運用の強度を上げることは可能であるが、認証局がユーザによる信頼を得なければ運用上の意味はない。運用の強度を監査基準の強度に当てはめることで網羅的な検討や、監査による認定の意味が顕在化すると考える。

各事項の詳細を以下に記す。

4.4.1. 監査への配慮

認証業務の信頼性を図る上で、その認証業務がどのような方針を掲げてそれを実践

しているかを確認するという方法がある。実際には認証局監査を通じて実践内容の監査を受け、監査人の意見や監査報告書が利用される。本認証局は、インターネットにおける基盤的な役割を担う重要な認証業務を行う可能性があるため、2003 年度の「IP アドレス認証局のあり方に関する調査報告書」第 4 章で比較した、認証局監査基準のガイドラインを参考に要件を設定した。

本認証局が発行する証明書は、電子署名のために利用されることを視野に入れており、可能性として電子署名法の適用対象となることも考えられる。電子署名法においては、「電子署名及び認証業務に関する法律施行規則（平成 13 年総務省 法務省 経済産業省令第 2 号)」第六条第十五項（ニ）において、業務の監査に関する事項を明確かつ適切に定め、監査を適切に実施することが定められている。

また、認証業務に限らず、2003 年度より情報セキュリティ監査の普及と啓蒙を図るため、「情報セキュリティ監査制度」が制定され、情報システムに対するセキュリティ監査の実施が推奨されている。

情報セキュリティ監査を実施することで次のメリットを受けることができると考えられている。

- 外部の専門家に監査を依頼することで自らでは発見できなかったセキュリティ上の問題に気がつくことができる
- 情報セキュリティの状態を定期的にチェック、比較することで、変化の度合いを把握することが出来、早期の対応を図ることが出来る
- セキュリティの状態を専門家に保証してもらうことで対外的な信頼度の向上につなげることができる

ここで問題となるのは、誰が監査を実施するのか、監査基準は何か、といったことがらである。「情報セキュリティ監査制度」では、この要求にこたえるために、監査人の研修制度、監査機関の登録制度、監査基準の制定などを行っている。

情報システムに対する監査、検証、保証制度として、米国公認会計士協会（以下、AICPA という）とカナダ勅許会計士協会（以下、CICA という）によって以下のサービスが開発されている。

- SysTrust（システムの信頼性に関する内部統制について保証を与える）
- WebTrust（電子商取引の安全性等に関する内部統制について保証を与える）
- 電子認証局のための WebTrust（認証局のシステムの信頼性又は安全性等に関する内部統制について保証を与える）

これらの制度では、公認監査人が AICPA/CICA が作成した原則・基準に従って、対象システムを検証あるいは評価することとなっている。

この際の原則・基準として、次の文書が適用される。

表 4-1 認証基準の原則・基準文書

サービス名	文書
SysTrust	「Trust サービスの原則と規準」 (Trust Services Principles and Criteria)
WebTrust	同上
電子認証局のための WebTrust	認証局のための WebTrust の原則と規準」 (WebTrust Principles and Criteria for Certification Authorities)

検証後、問題が無いことが確認された場合に、サイトに対応する Trust マークを表示することが許される。このマークは WebTrust のサイトで保持されている監査報告書にリンクされており、ユーザはマークをクリックすることで表示される報告書を閲覧することでサイトの状況を知ることが出来、サイトを信頼する根拠とすることが出来る。

また、米国監査基準 70 号（以下、SAS70 という）に準じて、電子認証局の監査報告書を作成することが出来る。SAS70 は、外部委託サービスに関する内部統制を保証する監査制度であり、監査実施基準、報告基準を定めている。

SAS70 に基づいた報告書では、内部統制の検証または評価で発見された内部統制手続の記述が報告書に添付されるため、委託先の内部統制を理解するために利用することができる。つまり、顧客から見た場合、認証局を認証業務の委託先と考え、外部委託先が行う業務（この場合は認証業務）に関して内部統制が確立していることを保証する監査を行うのである。

実際には、外部委託先（この場合は認証局）が自らの内部統制に関する監査を独立監査法人に依頼し、監査報告書を顧客に提示するという形をとることになる。

監査の重要性については CP/CPS 策定のガイドラインとして用いられる RFC2527（2003 年 12 月に RFC3280 によって obsolete された）の「4.2.7 Compliance Audit」でも触れられている。ここでは準拠性監査について、次の要素について定義することが求められる。

- 各主体に対する準拠製監査の頻度
- 監査者の身元・資格／認定にかかる事項
- 監査者と被監査部門の関係
- 監査テーマ
- 監査指摘事項への対応
- 監査結果の通知、開示など

それぞれの要素に対する具体的な配慮については「第 5 章　CP/CPS の検討」で述べる。

現在、RFC2527 の改定版である RFC3647 が公開されている。こちらでは、準拠性監査は小項目から中項目「4.8. Compliance Audit and Other Assessment」へと扱いが変更されている。

4.4.2. 不正抑止・防止(アクセスモデル)の確立

セキュリティリスク低減のためには、抑止・防止・検出・回復の観点から管理策を検討する必要がある。

- 抑止－リスクの発生を未然に防ぐこと。主にリスクに対する意識向上、リスクを発生させる行為に対する罰則など。
- 防止－リスクが発現しないようにすること。ネットワークアクセス制御、入退出管理など。
- 検出－リスクの発生を速やかに検出できるようにすること。ログの監視、侵入検出装置など。
- 回復－リスクによる損失を回復できるように前もって準備すること。

本認証業務では、特に抑止に関して配慮した。人員の故意による不正操作を防ぐためには、教育、罰則、監視の告示といった手段が有効である。情報セキュリティを守ることが組織の維持および発展、ひいてはスタッフの利益につながるのだということを教育し、これに背くものには罰則として損害賠償請求などを行うことを示し、操作が監視されていることを周知徹底させる、といった措置により、個々人の不正行為の実施に対する心理的障壁を高いものとする。

これらの措置に加えて、認証局のように特に高いセキュリティが求められている組織では、単独の行為者によるオペレーションミス、または故意による不正行為を防ぐために、複数人の同意がなければ操作を実施することができない、デュアルコントロール（Dual Control、合議制操作）の仕組みを取り入れていることが多い。

本認証業務でも、デュアルコントロールを取り入れることとし、重要な操作に関しては承認制とする。

さらにエンドエンティティは、証明書を受領する際に PIN と参照番号を別々の手段で入手し、さらにどちらかの受け渡しの際に本人確認を行うものとしている。

4.4.2.1. 兼務マトリクスの作成

デュアルコントロールを実現する単純な方策として、すべての操作に運用責任者の承認を必要とするモデルが考えられる。必要な人員を最小限に抑えられる利点はある

が、運用責任者に掛かる負荷が相当に高くなることが予想されること、運用責任者に権限が集中すること、柔軟性にかけることなどから、このモデルの採用は望ましくない。

もうひとつの単純な方策として、すべての操作に複数人（3 人以上）の運用担当者を配置し、そのうちの複数の合議により操作を実施するモデルが考えられる。安全性の面だけを考えると良いモデルといえるが、コストを考えると現実的とはいえない。

ここでは、ある業務担当者が兼務できる業務を表形式で示す、兼務マトリクスを作成することとする。

特定業務担当者に権限が集中しないこと、負荷のバランスがとれていること、妥当な人数であることなどに配慮し、要求されるセキュリティレベルを満足するような兼務マトリクスの開発を目指す。

このマトリクスで考慮する役割には次のものがある。

- 運用責任者
  認証局の運用の責任者。以下の業務担当者の任命等を行う。
- 鍵管理者
  認証局の鍵を管理する役割。この権限は登録業務などには使われない。
- CAO（CA Operator）
  認証局の操作を行う役割。RAO の申請を受け付け証明書の発行を行う。
- RAO（RA Operator）
  認証局における操作を担当し、証明書の発行要求に対して業務を行う役割。
- ネットワーク管理者
  認証局のシステムのネットワークを管理する役割。
- ログ検査者
  認証局のログを検査する役割。
- 審査者（RAA）
  RA（EE の登録を担当する役割）の登録管理を行う役割。
  本調査研究では、ISP のメンバ管理者（RA）の登録審査を行う。
- 承認者（RAA）
  RAA の登録要求に対して、承認を行う役割。

作成された兼務マトリクスについては第 5 章で述べる。

4.4.2.2. 運用体制の検討

重要な操作については、単独で実行することを許可せず、複数人が揃って初めて操作が可能となるようなデュアルコントロールの仕組みを取り入れる。

デュアルコントロールは、n 人の操作担当者を任命し、操作に際して、そのうち m

人の同意を必要とするものが一般的である。（m < n）

このように複数人が操作に関与することで単独行為者による不正行為を防止することが可能となる。

4.4.3. レジストリの業務体系への適合性

ここでは、認証局の構成について論じる。始めに、IA（Issuing Authority）と RA（Registration Authority）の配置について、社内で行なうモデルと外部委託を活用するモデルに関して、一般的なメリット・デメリットを論じる。次に、JPNIC で認証局を構成することを前提に、事業者認証モデルと個人認証モデルのメリット・デメリットを論じ、その複合モデルを提案する。

4.4.3.1. 認証局の構成について

認証局の主要なコンポーネントは IA と RA である。この二つの主な業務は次のものである。

表 4-2 認証局の主要コンポーネント

コンポーネント	業務
IA（発行局）	RA の申請に応じて証明書を発行する。
RA（登録局）	証明書申請者の身元確認を行い、発行局に申請する。

一般的に CA には証明書発行に関するデータを格納するリポジトリが設置される。リポジトリの設置には厳しい安全基準を満たす必要がある。

物理的セキュリティの観点からはゾーンニングを行うことと、耐震、対火災性といった安全対策基準の双方を満たす必要がある。

ゾーンの区切り方としては、図 4-4 のように、一般職員のアクセスが認められる一般ゾーン、認証局のオペレータのアクセスが認められるオペレーションゾーン、IA 操作オペレータのアクセスだけが認められる IA ゾーンに分ける形態が合理的といえる。

不正なアクセスを防止するために、各ゾーンの出入りには生体認証や IC カードを用いた入出管理システムを導入する。さらに抑止対策として、監視装置を採用する。

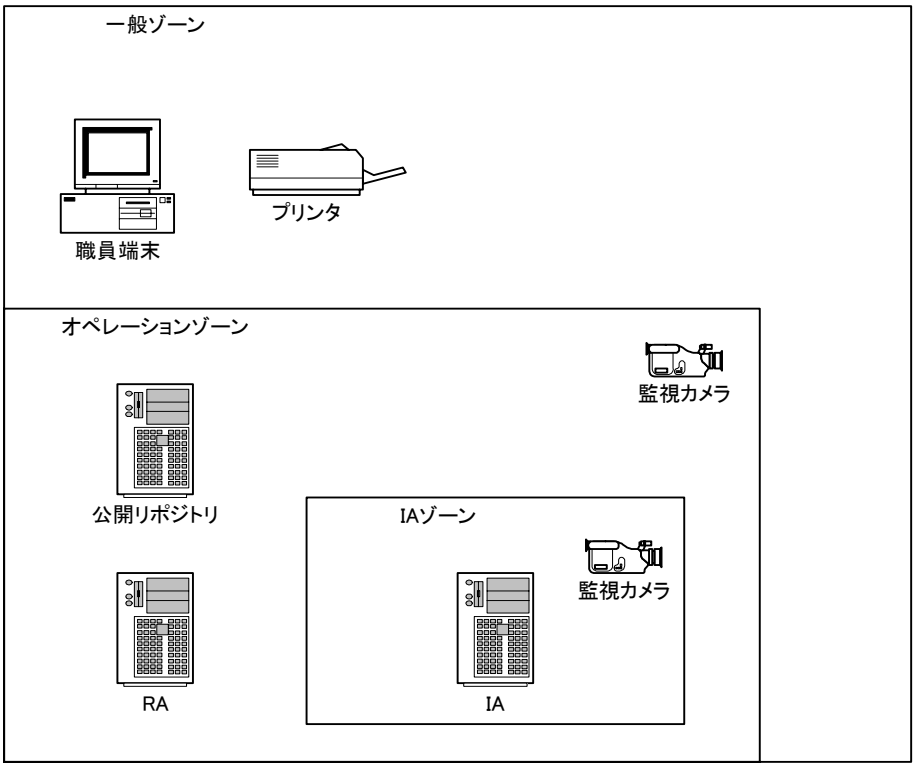


図 4-4 ゾーンニング

認証業務におけるシステムの安全基準として「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」[3]が定められている。ここでは、認証設備を設置する部屋について、次のような物理的安全対策を施すことが求められている。

- 認証設備室への入出場管理
  - 生体認証設備を備えること
  - 入室者数と退室者数が同数となるように管理すること
  - 入室装置の操作時間が通常より長い場合には警報が発せられること
  - 入室者、退室者、材質者を監視・記録する装置が設置されていること
- 災害の被害を防止する対策
  - 水害の防止のための措置が講じられていること
  - 隔壁により区画されていること

[3] 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針
http://www.meti.go.jp/policy/netsecurity/digitsign_sisin.htm

- 自動火災報知器及び消火装置が設置されていること
- 防火区画内に設置されていること
- 室内において使用される電源設備について停電に対する措置が講じられていること

- 認証設備室を設置する建築物

- 建築されている土地の地盤が地震被害のおそれの少ないものであること
- 地震に対する安全性に係る建築基準法（又はこれに基づく命令若しくは条例の規定に適合する建築物であること
- 建築基準法に規定する耐火建築物又は準耐火建築物であること

この他の物理的安全対策としては、通産省（現経済産業省）が制定した「コンピュータ施設の安全対策基準」および郵政省（現総務省）が制定した「通信設備安全基準」などを参考にすると良い。

これらの物理的安全基準を満足させるように IA を設置し、さらに保守管理を行うためには多大な運用コストがかかる。不十分な自社設備しか持たない場合には、IA をデータセンターなどに設置し、保守管理を外部委託することが考えられる。

IA と RA の運用、および証明書発行業務を考えると、次に挙げる三つのモデルを比較し、最適なモデルを選択することになる。

- 認証局の運用を含めて社内にて業務を行なうモデル
- 認証局の運用はデータセンターにて運用を行い、RA 業務を社内で行なうモデル
- 認証局と RA の業務を委託するモデル、社内では書面の管理のみ行なう

モデル間の相違は、導入から運用までのトータルコストの大小と、管理の細やかさである。

表 4-3 認証局運用モデルのコスト比較

認証局	登録局	トータルコスト	管理の細やかさ
内部	内部	大	易
外部	内部	中	
外部	外部	小	難

特に認証局の場合には、機密性、堅牢性を兼ね備えたサーバルームの設置が要求されるため、そういった部屋を持たない場合には、大きなコストが必要となる。

本認証局では、認証局とホストマスタ用 RA の運営を JPNIC 内部で行い、EE 用

RA を指定事業者に委譲するというモデルを採用する。

4.4.3.2. 事業者認証モデル・個人認証モデル

認証局の構成を、本人確認を誰が行なうのかに着目して分類すると次の二種類に大きく分けることが出来る。

- 事業者認証モデル
- 個人認証モデル

事業者認証モデルでは、IP アドレス指定事業者のみを認証する。この詳細は図 4-5 に表される。

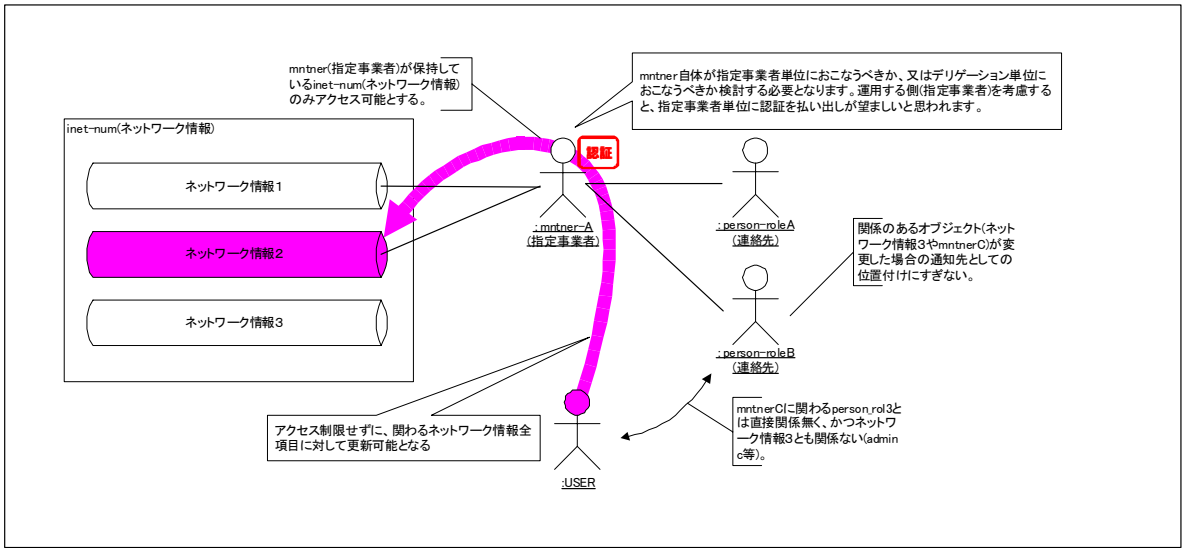


図 4-5 事業者認証モデル

この方式の最たるメリットは、管理対象が事業者のみであるため、証明書発行数が数百のオーダーに留まり、業務負荷が抑えられることにある。また、RPSL（Routing Policy Specification Language）上は指定事業者に当たる単位で認証情報を扱うため、現行の認証と枠組みとしては変わらず、IP アドレス指定事業者の混乱が避けられると考えられる。これに対しデメリットと考えられることには、エンドユーザの認証を行なわないため、現行の認証システムのセキュリティレベルの底上げにはつながらないことがあげられる。

個人認証モデルでは、エンドユーザを直接、認証する。この詳細は図 4-6 に表される。

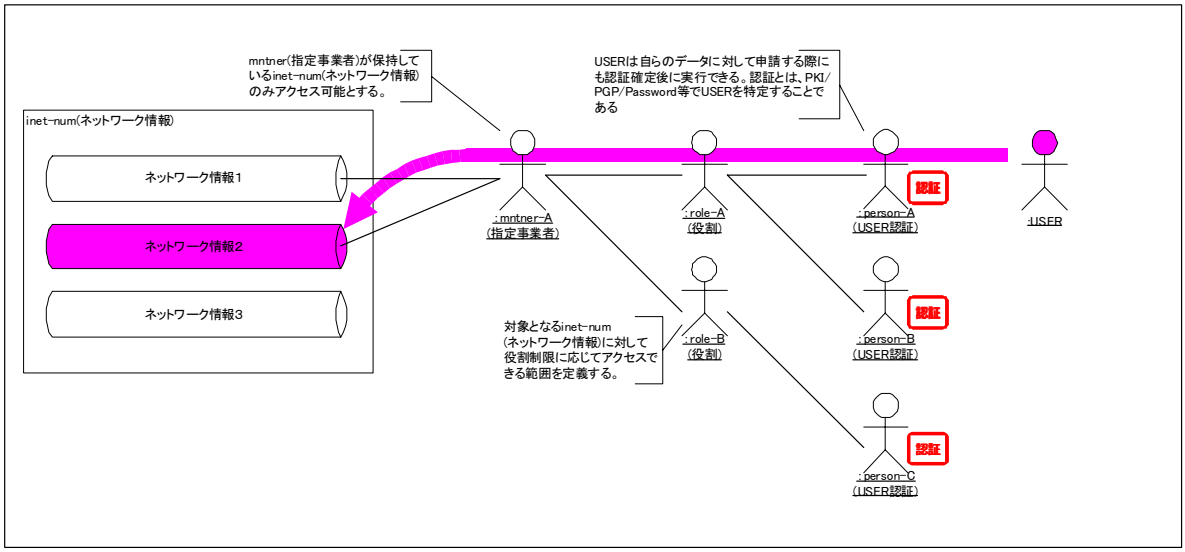


図 4-6 個人認証モデル

このモデルの最たるメリットは、個人身元認証を行なうため、情報の正当性が増すことになることが上げられる。また、あるレコードに関連する person のみがデータ管理を行なうよう制限をかけることが可能となり、データの安全性が高まる。

デメリットとしては、証明書の発行数が数万のオーダーに達するため、JPNIC だけで発行・失効といった管理業務を行うことが難しいことがあげられる。

以下に両モデルの、各種業務におけるメリット・デメリットを詳細に比較する。

（1） メリット・デメリット

- 認証発行：認証発行手続き対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
person(個人情報)に対して、個人身元確認をおこなう為に正当性が増すことになる。	大量の認証情報を保持する事になり、管理が困難である。 大量に認証発行手続きが発生し個人身元確認など、JPNIC 内での対応が困難である。	mntner(事業者)数のみとなり管理が簡略化される。	認証情報を mntner(事業者)内で周知する必要がある。

- 認証発行：再発行手続きの対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
再発行までの間に、同一 role(役割権限)に属する他の person(個人情報)より各種申請が可能である。	再発行であっても個人身元確認など、JPNIC 内での対応が困難である。	個人認証の必要がなく、JPNIC での業務量は個人よりも少ない。	再発行されるまで各種申請手続きが出来なくなる。 →JPRS 認証再発行については、再発行情報が到着(郵送)しないと、申請手続きが不可能とする運用を実施している。

- 認証問い合わせ：認証に関わる問い合わせ業務対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
事業者の認証よりも規模の小さい、本人確認手続きが適用できる。	メール・電話での認証問合せが大量に発生する。その際に JPNIC 内での対応は困難である。	mntner(事業者)単位の為に、JPNIC 対応は少量におさえられる。	問い合わせのあった事業者の確認を行なう必要がある。

- 認証失効：認証失効範囲及び管理対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
person(個人情報)単位に失効が可能となる 柔軟に認証情報の管理が出来る。	事業者内の退職者(個人)までは、JPNIC として管理が不可能であり、事業者内の正確な認証状況が把握出来ない。	mntner(事業者)単位に失効が可能となる	mntner(事業者)単位に排除し、アクセス不可能とする仕組みとなる為、事業者全体に影響する。

- 認証有効期限：継続手続き業務対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
個人単位であることのメリットはない。	person(個人情報)単位に払い出しされている為に、有効期限時の継続手続きも大量に発生する。その際に JPNIC 内での対応は困難である。 又、同一事業者内で全ての認証が有効になるまで期間が掛かると想定される。	mntner(事業者)単位の為に、JPNIC 対応は少量におさえられる。又、使用している事業者側も手続きが簡略化される。	事業者単位であることによるデメリットはない。

- アクセス制限：規定項目及びレコード制限対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
事業者に対して role(役割権限)を用いて、それに属する person（個人情報）で制限する。 その為、ネットワーク情報と関連する person(個人情報)のみアクセスする事によりデータの保持性が高まる。 role(役割権限)とは、レコード及び項目単位に役割に応じて制限が可能とする事である。	role(役割権限)と person(個人情報)との連結はどのようにおこなうのか不明確である。 role(役割権限)の定義は困難となり、簡略制限へ集中する可能性がある。 個々の person(個人情報)で管理する事が重要視される。	RIR が推奨する RPSL 構造に基づいて、mntner(事業者)認証で可能となった利用者は全て可能となっている。 ポリシー変更に伴うシステム内の対応が柔軟に対応できる。	変更した利用者が事業者単位の為、個人利用者まで明確にならない事になる。 ネットワーク情報に関連する利用者であるかどうか不明の為にデータの保守性が低下する。

- 不正アクセス：認証情報漏えいによる不正アクセス対応

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
person(個人情報)を特定し、認証再発行手続き実施で最小限に抑える事ができる。又、他の認証情報には影響されないものとなる。	個人単位でのデメリットはない。	事業者単位でのメリットはない。	再発行手続きする事になるが、個人まで特定できない為に再発する恐れがある。又、再発行されるまで各種申請手続きが出来なくなる。

- ダウンストリーム：二次指定事業者以降の認証発行

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
個人単位でのメリットはない。	事業者単位の方式ではあるが、認証形式として person(個人情報)まで管理する必要があり困難となる。	ダウンストリームの考え方が想定通りに実施され管理がしやすい環境になる。	事業者単位でのデメリットはない。

- そのほか：現行システムより展開する際の考え方

個人認証		事業者認証	
メリット	デメリット	メリット	デメリット
現行より強化する為に、個人認証を取り入れる方向で進められる。	person(個人情報)の指定事業者との属性や正当化の為に再度登録依頼を実施する必要がある。（全個人情報の正当化） 指定事業者など利用者に通知する必要がある。	現行移行となる為に指定業者への混乱が避けられる。	認証単位の詳細化による強化を図ることができない。

（2） 負荷試算

認証業務の付加試算を行うことは、認証業務の実現可能性を検討する上で重要である。ここでは認証情報の登録手続き（以下、認証問い合わせと呼ぶ）から発生する業務の負荷を試算し、いくつかの対応方法（認証対象のとらえ方）を検討する。検討内容は以下の通りである。

- JPNIC に登録されている個人の認証問い合わせと、事業者ごとに一人だけが認証問い合わせを行うケースを比較する。
- 同様の比較を、認証情報が効力を失う（認証失効とよぶ）場面について行う。
- 指定事業者ごとに認証対象を決めた個人認証方式（以下、提案個人認証と呼ぶ）の実現可能性を試算する。

前者の二つは、指定事業者の契約と関連のない個人を含んでいるため、実際のところは技術的に意義のある比較ではない。これは認証対象を”契約行為のあるエンティティとその関連する者”に限定するか、”認証しうるエンティティのすべてを対称にするか”という見方の違いである。この問題は、ユーザにどのような条件で認証対象になりうるかという意義の違いに影響する。JPNIC では、まず”すべてのエンティティを対象にする”方針で検討を行った。すると個人認証は明らかに不可能であるという試算ができた。

まず、JPNIC に登録されている個人を対象からの認証問い合わせと、事業者ごとに一人だけが認証問い合わせを行なうケースの比較を行なう。

ここでは各業務における負荷を試算する。各業務に要する人工時間を表現するために、スタッフ辺り、一日 8 時間勤務を行なうという前提を設ける。

以下の試算中、Ｘ人／日と表現されているのは、ある業務を何日間かかけて実施するために、一日辺りＸ人のスタッフが必要であるということを意味する。

- 認証発行

初期導入として 30000 件の認証を実施するとして計算を行なう。ひとつの認証に 15 分かかるものとし、スタッフ辺り一日に 28 件の認証を実施できるものとする（休憩時間を加味した）。必要な人員は以下の式で計算できる。

認証発行数 / (一人当たりの認証実施数 x 実施期間)

この式を認証方式にあてはめて計算すると表 4-4 となる。

表 4-4 認証発行必要人員数

	実施期間	必要人員
個人認証 person(個人情報)数： 30,000 件	1 日消化： 30 日間消化： 60 日間消化： 180 日間消化:	30,000 件÷28 件＝**1,071 人/日** 30,000 件÷(28 件×30 日)＝**35.7 人/日** 30,000 件÷(28 件×60 日)＝**17.9 人/日** 30,000 件÷(28 件×180 日)＝**5.9 人/日**
事業者認証 組織認証 指定事業者数：300 件	1 日消化： 30 日間消化： 60 日間消化： 180 日間消化:	300 件÷28 件＝**6.25 人/日** 300 件÷(28 件×30 日)＝**0.35 人/日** 300 件÷(28 件×60 日)＝**0.18 人/日** 300 件÷(28 件×180 日)＝**0.05 人/日**

スタッフの数として、他作業を鑑みると 10 人以上というのは現実的ではない。このため、個人認証を実施するとなると、30 日間消化、60 日間消化は難しいということがわかる。

しかし、一月辺りの稼動日数を 20 日とすると 180 日間というのは 9 ヶ月という長さになり、これもまた現実的ではない。このことから、個人認証を行なうのは難しいといえる。

- 認証問い合わせ

ひとつの認証問合せ対応に 20 分かかるものとし、スタッフ辺り一日に 20 件の認証を実施できるものとする（休憩時間を加味した)。また、一日に発生する問合せは全件数の 5%（1,500 件）であるとする。

これより認証問合せに必要な人員は次の式で計算される。

全件数 x 問合せ比率 / 一人当たりの処理能力

この式をそれぞれの認証に適用すると表 4-5 となる。

表 4-5 認証問合せ必要人員数

	必要人員	計算式
個人認証 person(個人情報)数： 30,000 件	75 人日	30000 x 0.05 / 20 = 75 人日
事業者認証 組織認証 指定事業者数：300 件	0.75 人日	300 x 0.05 / 20 = 0.75　人日

これは明らかに個人認証では対応できないことを示している。

- 認証失効

運用時に発生する認証失効の処理の負荷を試算する。ひとつの認証失効対応に 15 分かかるものとし、スタッフ辺り一日に 28 件の認証を実施できるものとする（休憩時間を加味した)。

認証失効発生数については次の式で求められる。

事業者辺りの平均個人情報数 x 一年辺りの平均事業者解約数

過去の実績から、一年辺りの平均事業者解約数を 15 とし、事業者辺りの平均個人情報数が 30000 / 1300 = 23 件であることから、一年辺りの認証失効数は 345 件としている。

これにより、各認証方式における認証失効の負荷は表 4-6 のように計算される。

表 4-6 認証失効必要人員数

	必要人員	計算式
個人認証 person(個人情報)数： 30,000 件	12.3 人年	345 / 28 = 12.3 人年
事業者認証 組織認証 指定事業者数：300 件	0.5 人年	15 / 28 = 0.5 人年

認証失効については想定される件数が大きなものではないので、どの認証方式でも現実的に対応可能であるといえる。

- 認証再発行

運用時に発生する認証再発行の処理の負荷を試算する。この処理は「認証失効＋認証発行」の組み合わせ処理することが想定されており、負荷の大きさは各処理の和として計算される。

- 認証継続発行

運用時に発生する認証継続発行の処理の負荷を試算する。想定では初期認証発行にある程度の期間が必要であるため、図 4-7 で示されるように、認証継続作業の発生タイミングは認証発行のタイミングと同じようなものとなる。

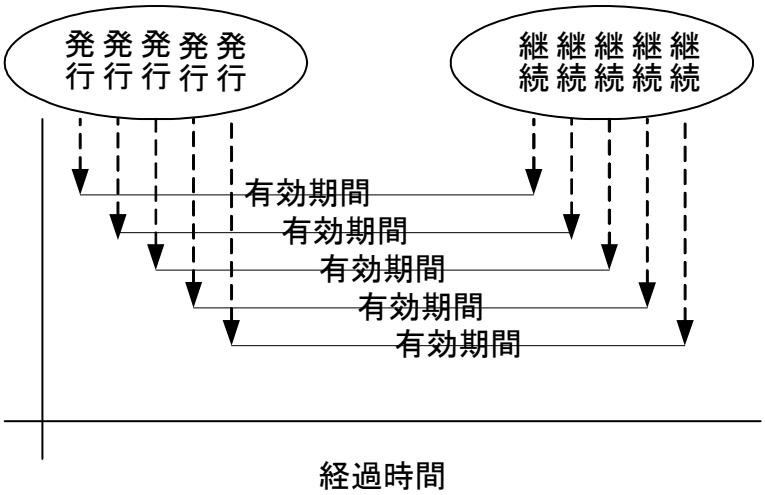


図 4-7 認証有効期間と継続の発生

従って表 4-4 と同様な人員が必要となり、個人認証方式は現実的ではないことがわかる。

4.4.3.3. リソース管理権限委譲について（提案個人認証）

これまでの議論を踏まえて、負荷として許容可能な認証方式として、個人認証と事業者認証を組み合わせた方式を提案する。

図 4-8 で示されるこの方式では、JPNIC は指定事業者の「指定事業者認証管理者」のみ認証を行う。個人認証は「指定事業者認証管理者」管理下の元で払い出させる仕組みとする。

また、この方式において、JPNIC の認証情報は、「指定事業者認証管理者」はもちろんの事、その管理下の認証情報も確保するが、「指定事業者認証管理者」管理下の本人確認や問合せには関わらないという責任範囲の提示を明確におこなうものとする。

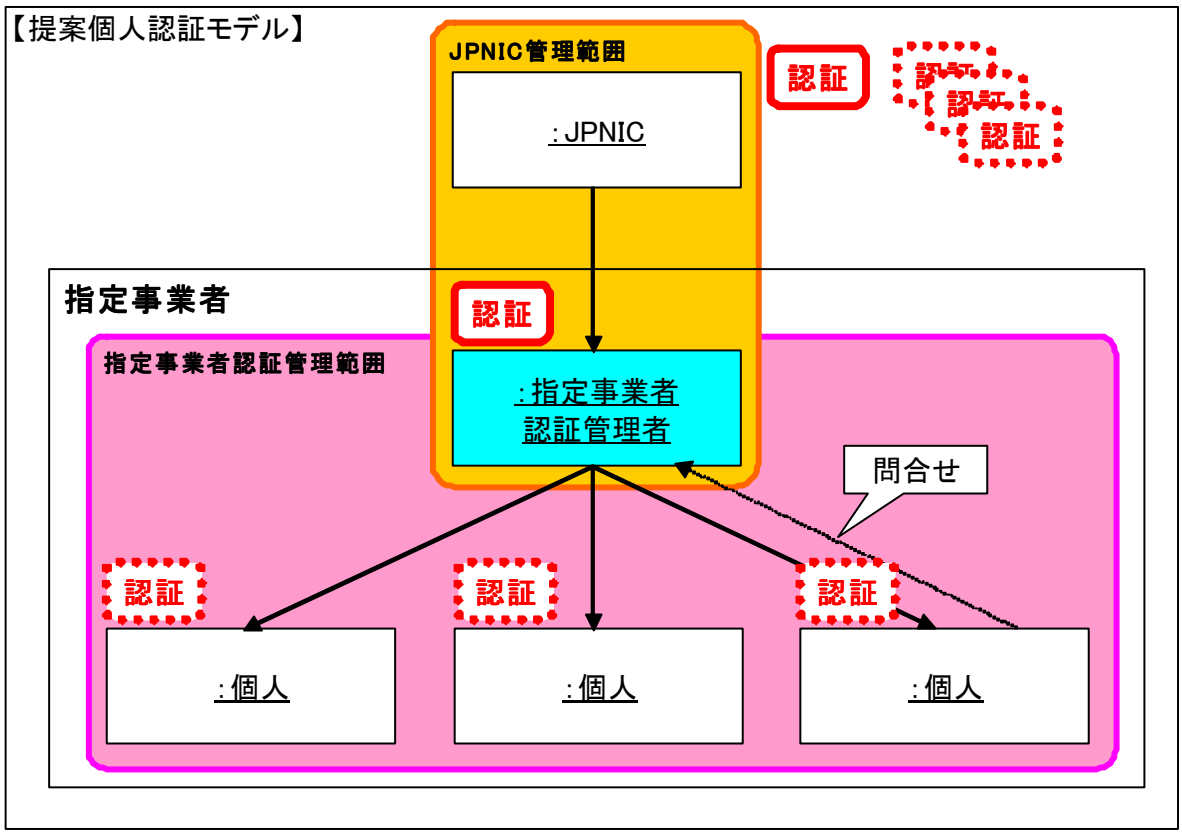


図 4-8 提案個人認証

この方式の採用により、表 4-7 に示すような業務対応の改善が考えられる。

表 4-7 提案個人認証の業務対応改善事項

認証状況	改善事項
認証発行／認証再発行	大量認証発行に伴う個人身元確認などの管理が不要となる
認証問合せ	認証問合せ対応のための専属業務が不要となる
認証失効	事業者内の退職者に対して関与が不要となる

提案される個人認証方式では、JPNIC が認証すべき対象は、事業者（mntner）となる。この構成は表 4-8 として示される

表 4-8 提案個人認証対象事業者構成

認証対象事業者	総数
指定事業者	300
PI[4]/AS 管理者	1000
合計	1300

また、事業者ごとに二人の事業者管理者が配置されると想定して、負荷試算を再度実施する。対象となる事業者総数は 1300 x 2 = 2600 件でする。

表 4-9 提案個人認証負荷試算

作業	負荷
認証発行	92.8 人/日(1 日間消化）
	3.0 人/日（30 日間消化）
	1.5 人/日（60 日間消化）
	0.51 人/日(180 日間消化）
認証問合せ	6.5 人/日
認証失効	1.07 人/年
認証継続	92.8 人/日(1 日間消化）

この中で定常的に日々発生する業務は認証問合せであり、必要な人員は 6.5 人日である。初期の認証発行業務を 30 日間かけて行なうとすると、ピーク時に必要な一日辺りの人員は 9.5 人となり、十分リーズナブルであるといえる。

[4] Provider Independent、プロバイダ非依存のことで、IP アドレス指定事業者に割り振られた空間以外から割り当てられた（IP アドレス）を意味する
http://www.nic.ad.jp/ja/basics/terms/pi-address.html

4.4.3.4. ルート認証局と IP アドレス認証局の関係

JPNIC で運用する認証局が発行する証明書の適用範囲として、ホストマスタの認証、アドレスリソースレコードの認証などが考えられている。これに加えて、将来的には様々な用途への応用を想定している。その場合には、異なる CP/CPS を持った認証局を別途、構築する必要性があると考えられる。

認証局の CP/CPS の変更を最小限に抑えるために、IP アドレス認証局の上位認証局を設置し、これをルート認証局とする。新規に構築する認証局は、IP アドレス認証局と並列に配置することで、IP アドレス認証局の CP/CPS への影響を排除することができる。

これを表したものが図 4-9 である。

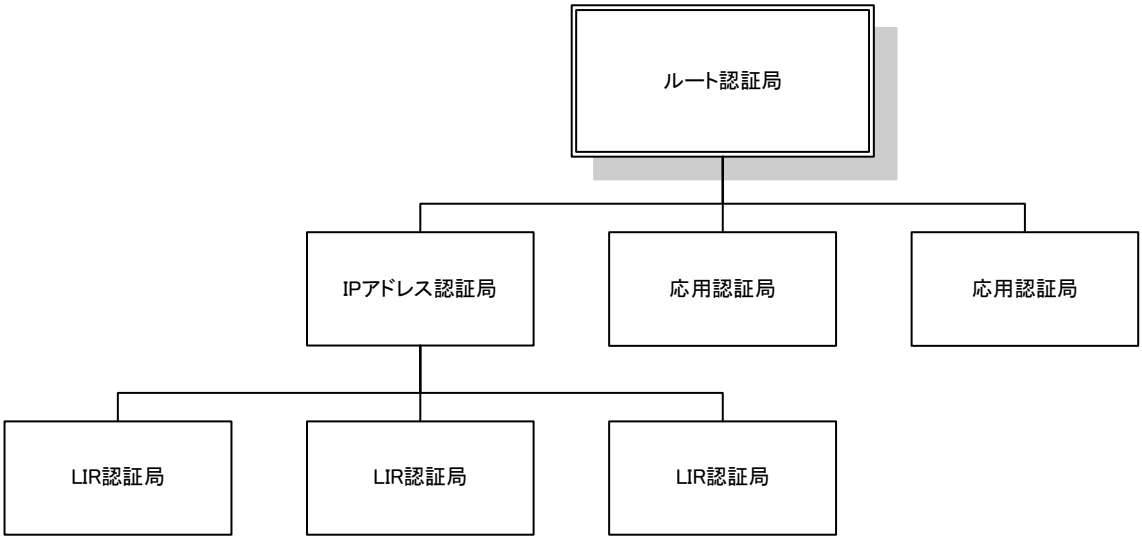


図 4-9 認証局階層構造イメージ

4.5. 業務モデルの設計

ここでは、認証業務を設計し、概念図を提示する。このために、提供する機能を示し、その機能を実現するシステムを設計する。最後にひとつの概念図にまとめる。

4.5.1. 提供する機能

認証業務は以下の機能を提供する必要がある

- IA（証明書の発行処理、証明書の失効処理、CRL の発行）
- RA（証明書発行申請の処理、証明書失効申請の管理）
- リポジトリ（証明書・失効リストの登録、証明書・失効リストの公開）

これらの機能を提供する認証局を構成するモデルについて説明する。

4.5.1.1. 一台のサーバで構成するモデル

認証局を構築するに当たって IA、RA、リポジトリ機能が必要であるが、これを一台のサーバ上で行うモデルである（図 4-10）。

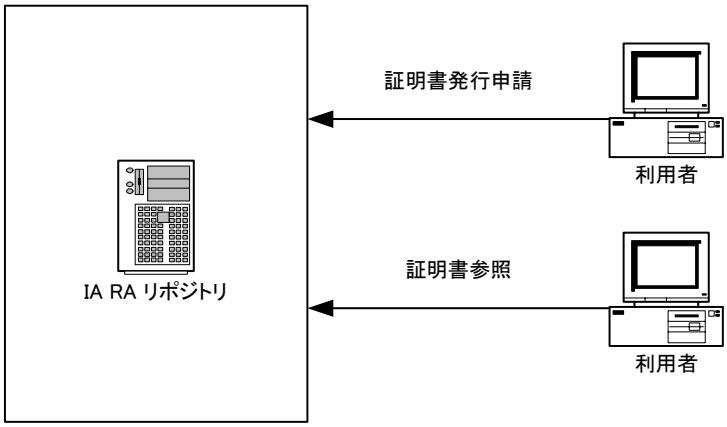


図 4-10 一台のサーバで構成するモデル

このモデルには安全性の観点から次の問題が存在する。

- 認証局では、リポジトリ部分に公開アクセスを許可する必要があることから、IA、RA 機能に対するアクセスパスを許す危険性を生むことにつながる
- 本来、操作者が別々であるべき RA と IA がひとつになっていることから、アクセス権の分離がソフトウェア（ローカルマシン）上の問題となり、CA 鍵の安全

性に悪影響を与える。

この構成では、構成が単純であることから、導入コストが低い、バックアップ／リカバリ手順が単純になる、バックアップ／リカバリ計画が立てやすいことなどのメリットも考えられるが、認証局における信頼性重要性は極めて高く、試験的な導入以外での使用は考慮すべきではない。

4.5.1.2. IA と RA を分離するモデル

次に IA と RA を分離するモデルを考える。このモデルでは、IA と RA を物理的に分離する（図 4-11）。

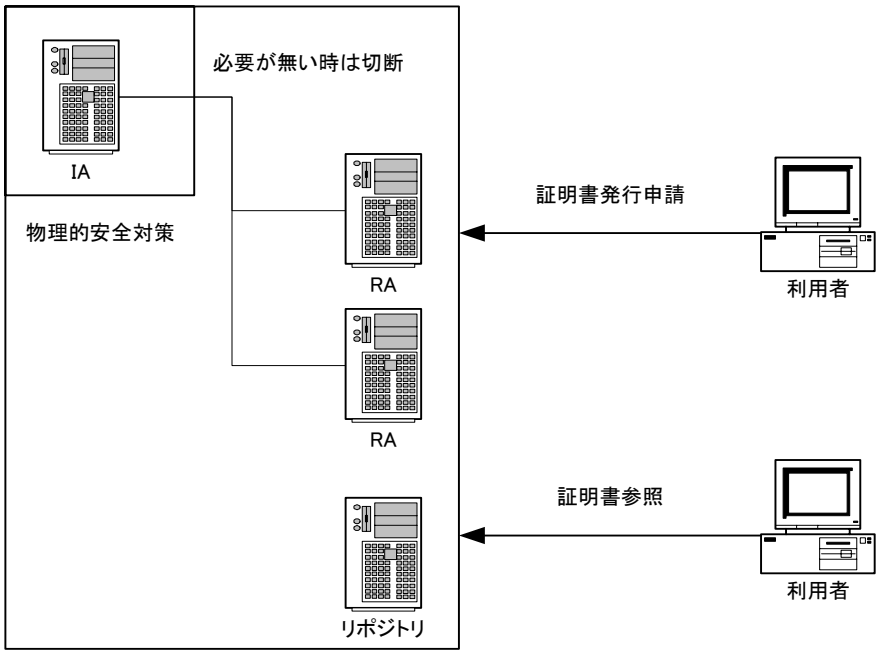


図 4-11 IA と RA を分離するモデル

IA で行うべき業務は証明書の作成と発行、廃棄リストの発行などである。いずれも認証局の鍵による署名が必要であり、オペレータがコンソールから作業を行うことになる。このためコンソールを保護することが重要となり、通常は厳重に守られたサーバルームにコンソール及び IA サーバを設置することになる。

RA の主な業務は証明書発行申請を受け取り、本人確認を行ったうえで IA に申請をフォワードすることである。証明書発行申請の受け取り方はひとつではないが、複数の組織にまたがった利用者を抱える場合には、インターネット経由で申請を受け取るのが合理的である。このため、RA では電子メールまたはウェブといったインタフェースを持つことが要求される。

RA の業務は本人性確認などのオフラインでの作業を含むため、機械的な作業ではなく、人手が要求される。一件当たりの作業時間も数分から場合によっては数日に及ぶこともあり、オペレータの数だけコンソールを用意するのが一般的である。RA のオペレータが扱う情報自体は個人情報などを含むため機密性が高いものではあるが、RA 自体は、データを一時的に保存するだけであり、IA で扱う認証局鍵ほどの重要性は持たない（表 4-10）。

表 4-10 認証局構成サーバの機密レベル

サーバ機器	機密レベル
IA	認証局鍵は最高度の機密レベルで保護される必要がある
RA	RA には申請情報などが一時的に保存されるだけであり、機密レベルは高いとはいえない
リポジトリ	公開情報であるため機密レベルは低い

このため RA コンソールは、通常のオフィスに求められる機密レベルでの運用が可能であり、IA に申請を行う際に、IA との回線を接続すればよい事になる。

このモデルでは IA だけを厳重なサーバルームに格納することが可能となり、安全性に寄与できる。

デメリットとしては管理運用コストの増大、ネットワーク機器の負担などが考えられるが、安全性の確保のためには欠かすことが出来ないといえる。

4.5.1.3. 提案モデル

本認証システムでは、JPNIC が IP 指定事業者を認証し、IP 指定事業者がエンドユーザを認証するモデルをとっているため、IA、RA、リポジトリ機能に加えて次の機能が必要となる。

- ISP 管理者申請受付サーバ
  ISP 管理者を対象とした公開鍵証明書の発行・破棄申請を行う
- ホストマスタ申請受付サーバ
  ホストマスタを対象とした公開鍵証明書の発行・破棄申請を行う
- 利用者管理サーバ
  RA および EE の申請者情報および証明書発行状態などを管理する

さらに図 4-8 で示される個人認証方式を採用することにより、指定事業者に EE 認

証用の RA が必要となる。

これらの機能を表 4-11 のようにグルーピング化する。

表 4-11 サーバのグルーピング

グループ	サーバ
JPNIC 認証局	IA RA リポジトリ
IP 事業部	ISP 管理者申請受付サーバ ホストマスタ申請受付サーバ 利用者管理サーバ
IP 指定事業者	RA

それぞれのグループの役割を説明する。

- JPNIC 認証局
  認証局として、証明書の発行（IA)、登録局（RA)、リポジトリ運用（PKC/CRL）を行なう。
- IP 事業部
  新レジストリシステムの管理を行なう。
  ホストマスタのアクセス管理を行なう。
  ISP 管理者の証明書の発行を行なう（RAA）
- IP 指定事業者
  ISP 管理者が RA となり EE の認証を行う

グループと、所有するサーバ群の関係は図 4-12 で表される。

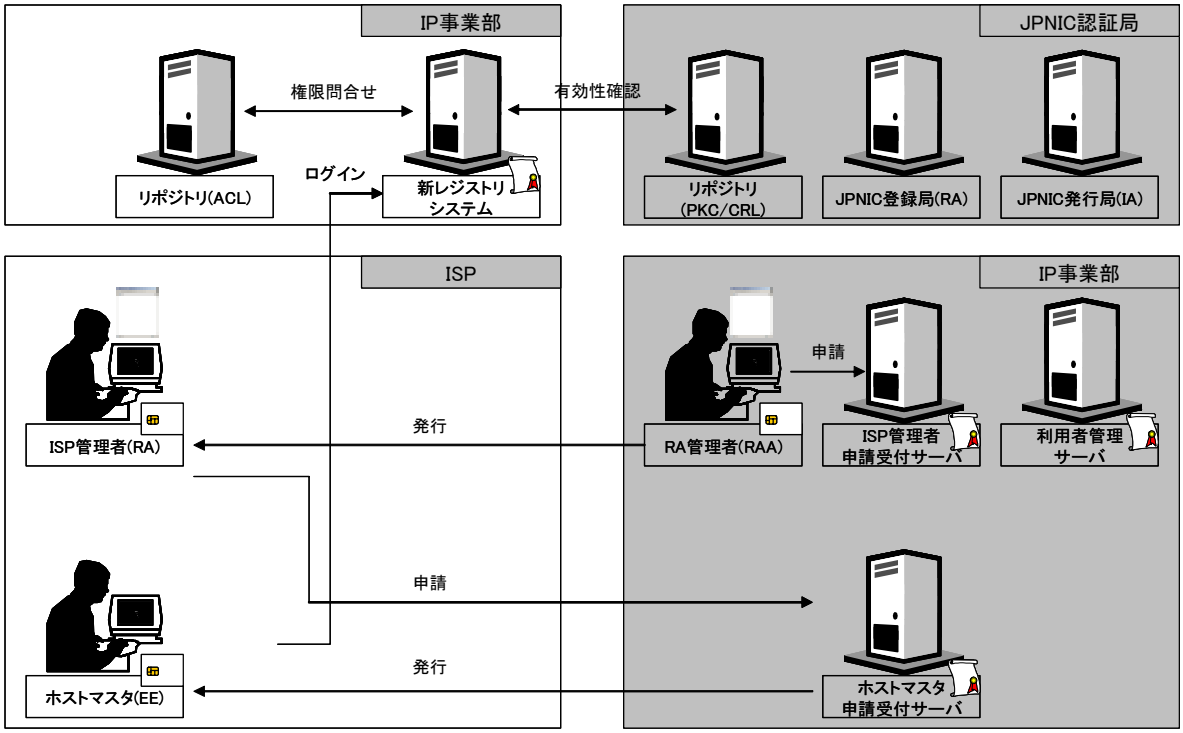


図 4-12 業務概念図

ACL（アクセスコントールリスト：Access Control List）
PKC（公開鍵証明書：Public Key Certificate）
CRL（証明書失効リスト：Certificate Revocation List）
IA（発行局：Issuance Authority）
RA（登録局：Registration Authority）
RAA（RA Authority）
RAO（登録局オフィサー：RA Officer）
EE（エンドエンティティ：End Entity）

この構成による認証局で実現される機能には次のものがある。

- IP 事業部スタッフ認証
  IP 事業部スタッフは ISP 代表者、つまり EE の RA を認証する役割を果たす。この IP 事業部スタッフには JPNIC 認証局 RA 管理者、つまり RAO による認証が行われる。
- ISP 代表者認証
  ISP 代表者には IP 事業部スタッフ RA 管理者、つまり RAA による認証が行われる。
- ホストマスタ認証
  ホストマスタ、つまり EE には、ISP 代表者、つまり RA による認証が行われる。

- ホストマスタのレジストリシステムへのログイン
  ホストマスタ、つまり EE は、データ編集のため、レジストリシステムにログインを行う。この際に、JPNIC 認証局発行の証明書を使ってユーザ認証が行われる。
- IP 事業部スタッフ失効
  IP 事業部スタッフ、つまり RAA の証明書の失効手続きである。
- ISP 代表者失効
  ISP 代表者、つまり RA の証明書の失効手続きである。
- ホストマスタ失効
  ホストマスタ、つまり EE の証明書の失効手続きである。

次節以降で、各機能の詳細について述べる。

4.5.2. IP 事業部スタッフ（RAA）認証

RAA の職務は ISP 管理者からの証明書発行申請を受付け、認証を行うことである。この RAA 自体の認証を行うのが RAO である。RAO は JPNIC 登録局の管理者として RAA の認証を行う。

RAO による RAA 認証手続きは次のように定義される。

（1） RAA から RAO へ RAA 証明書発行申請書を送付
（2） RAO から RAA 申請受付サーバへ申請を実施
（3） RAA 申請受付サーバから利用者管理サーバへ発行申請情報登録
（4） RAA 申請受付サーバから JPNIC 登録局へ申請
（5） JPNIC 登録局から RAO に対して RAA 証明書を発行
（6） RAO から RAA に対して IC カードを配布

この概念は図 4-13 に示される。

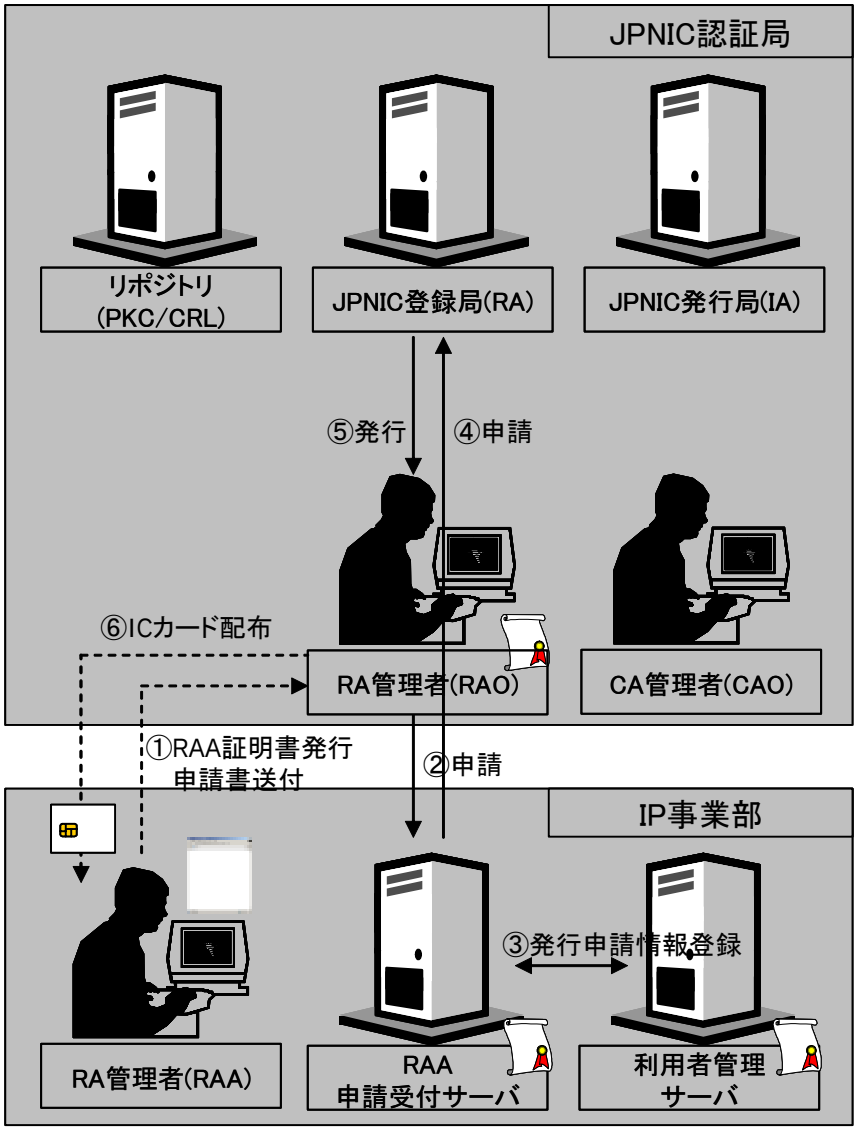


図 4-13 RAA 認証概念図

4.5.3. ISP 代表者（RA）認証

RAA 認証は RAO が行う RAA の認証について示した。ここでは RAA が ISP 代表者を認証する RA 認証について記す。

この手続きは次のように定義される。

（1） ISP 管理者から RAA に RA 証明書発行申請書が送付される
（2） 審査担当 RAA から ISP 管理者に申請受付完了通知書が送付される
（3） 審査担当 RAA が申請内容を申請し、問題がなければ ISP 管理者申請受付サーバに発行申請情報が登録される
（4） 承認担当 RAA から ISP 管理者申請受付サーバに申請が行われる

（5） ISP 管理者申請受付サーバから承認担当 RAA に証明書が発行される
（6） 審査者 RAA から ISP 管理者に IC カードが送付される

この概念は図 4-14 に示される。

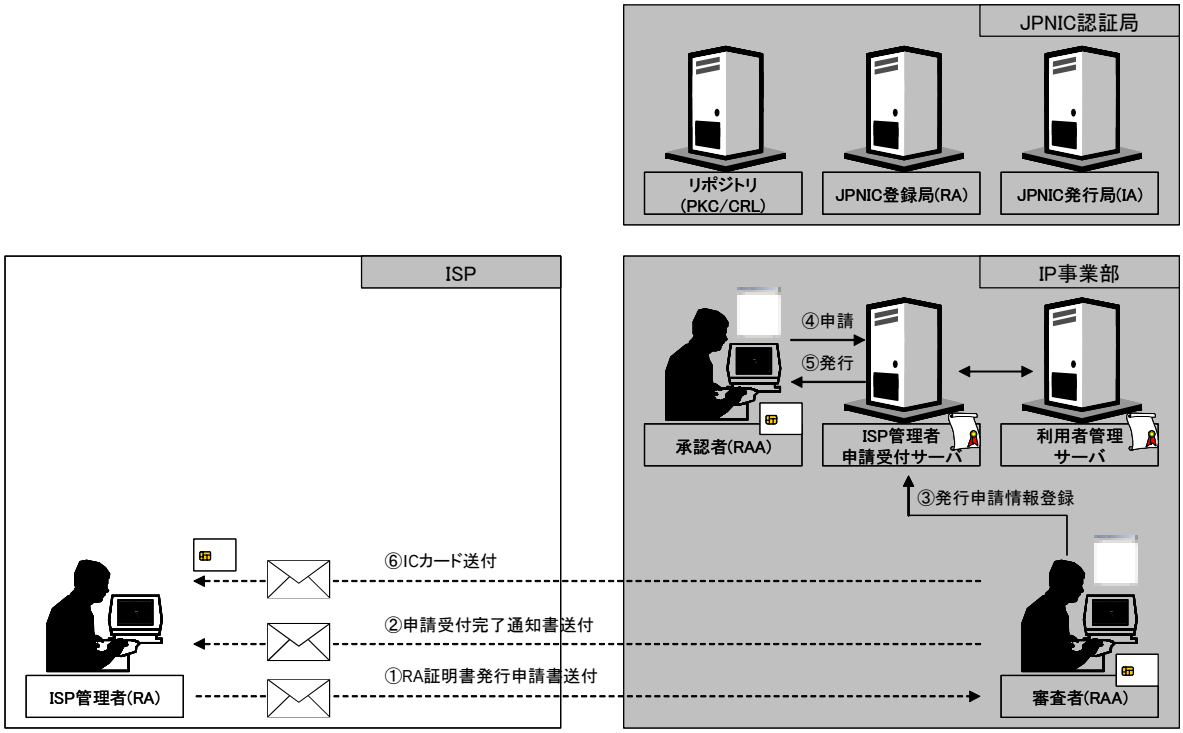


図 4-14 RA 認証概念図

4.5.4. ホストマスタ（EE）認証（センター承認モデル）

ホストマスタの認証は ISP 管理者が行う。

（1） ISP 管理者からホストマスタ申請受付サーバへ EE 証明書発行申請が送付される
（2） ホストマスタ申請受付サーバから利用者管理サーバへと発行申請情報が登録される（この際、本人確認情報と発行承認情報を生成する）
（3） ホストマスタ申請受付サーバから ISP 管理者へ本人確認情報が送付される
（4） ISP 管理者からホストマスタへ本人確認情報が配布される
（5） ホストマスタからホストマスタ申請受付サーバへ EE 証明書発行依頼が送付される
（6） 承認担当 RAA が EE 証明書発行依頼を承認する
（7） ホストマスタ申請受付サーバでは JPNIC 登録局に証明書を登録し、さらにリポジトリに証明書を公開する
（8） ホストマスタ申請受付サーバからホストマスタに公開鍵証明書が送付される

この概念は図 4-15 に示される。

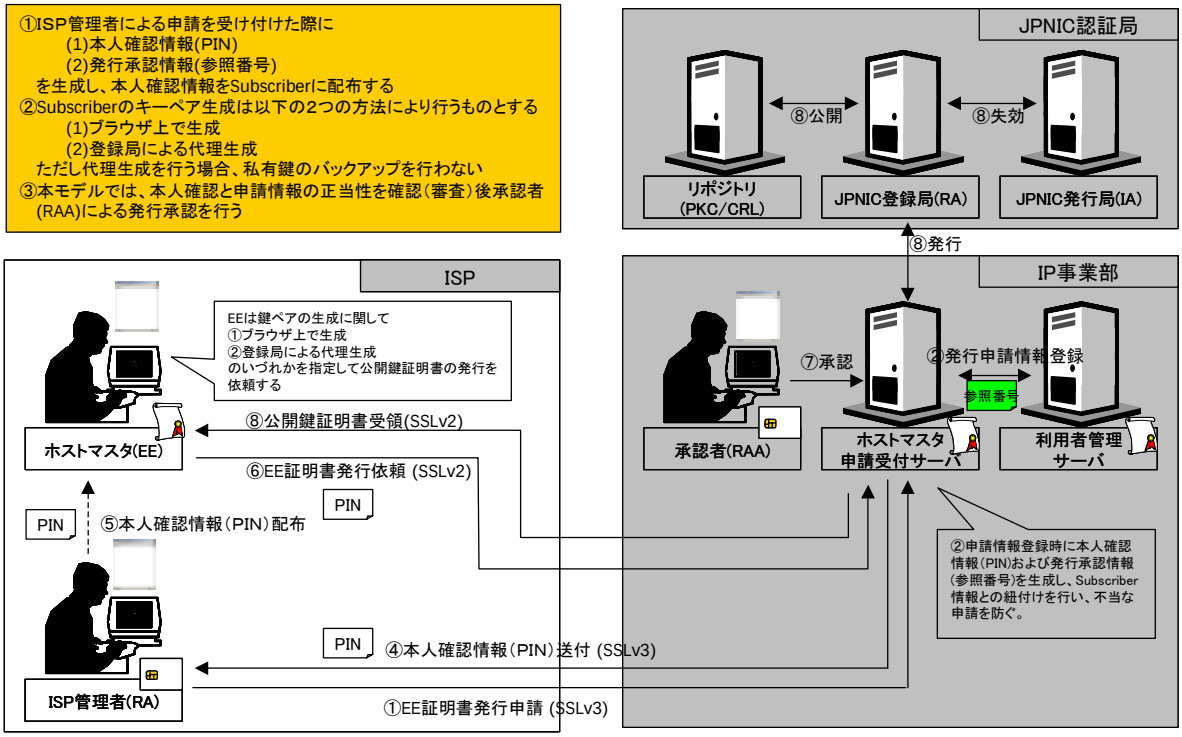


図 4-15 ホストマスタ（EE)認証概念図（センター承認モデル）

4.5.5. ホストマスタ（EE）認証(自動承認モデル)

先のセンター認証モデルでは、本人確認と申請情報の正当性を確認後に、承認担当 RAA が発行承認を行っているが、この作業を登録局が自動で行うモデルが考えられる。

この場合の手続きは以下のようになる。

（1） ISP 管理者からホストマスタ申請受付サーバへ EE 証明書発行申請が送付される
（2） ホストマスタ申請受付サーバから利用者管理サーバへと発行申請情報が登録される（この際、本人確認情報と発行承認情報を生成する）
（3） ホストマスタ申請受付サーバから ISP 管理者へ本人確認情報が送付される
（4） ISP 管理者からホストマスタへ本人確認情報が配布される
（5） ホストマスタからホストマスタ申請受付サーバへ EE 証明書発行依頼が送付される
（6） ホストマスタ申請受付サーバでは JPNIC 登録局に証明書を登録し、さらにリポジトリに証明書を公開する
（7） ホストマスタ申請受付サーバからホストマスタに公開鍵証明書が送付される

この概念は図 4-16 で示される。

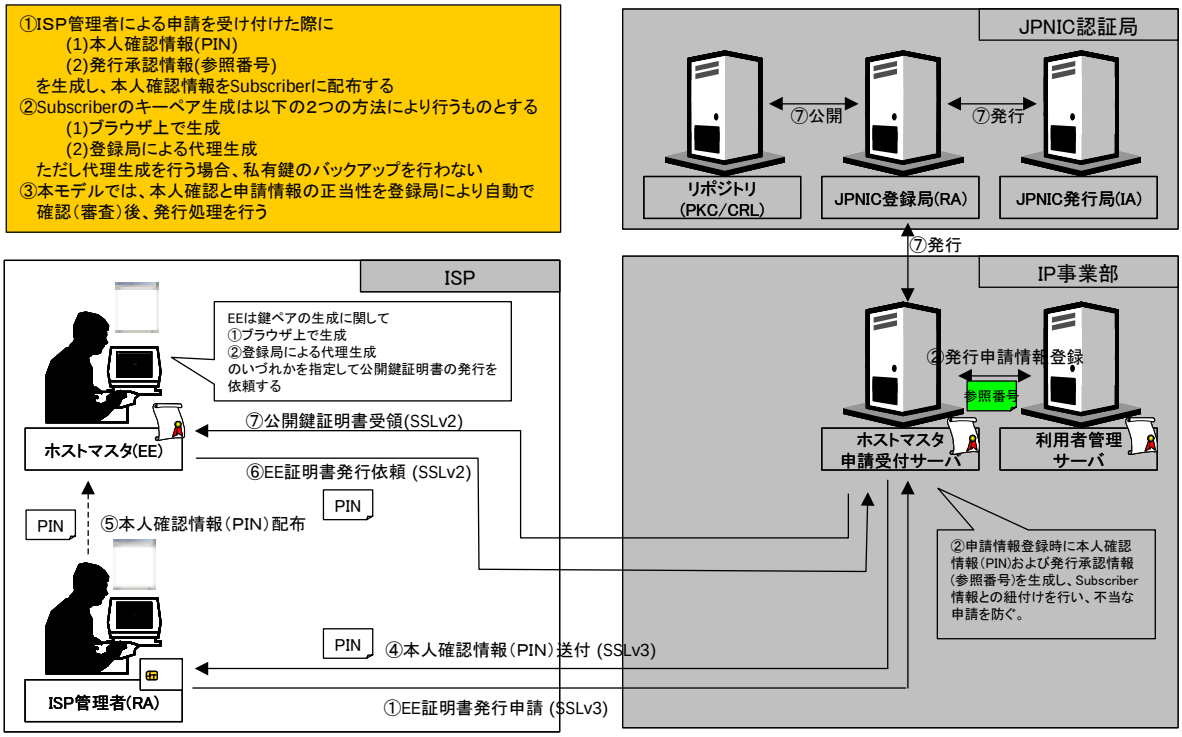


図 4-16 ホストマスタ（EE)認証概念図（自動承認モデル）

4.5.6. ホストマスタ（EE）の RS へのログイン

ホストマスタによるレジストリシステムへのログイン手続きは次のように示される。

（1） ホストマスタからレジストリシステムへログイン手続きが実施される
（2） レジストリシステムではホストマスタから提示されたログイン情報からリポジトリへオペレータ権限を問い合わせる

この概念は図 4-17 で示される。

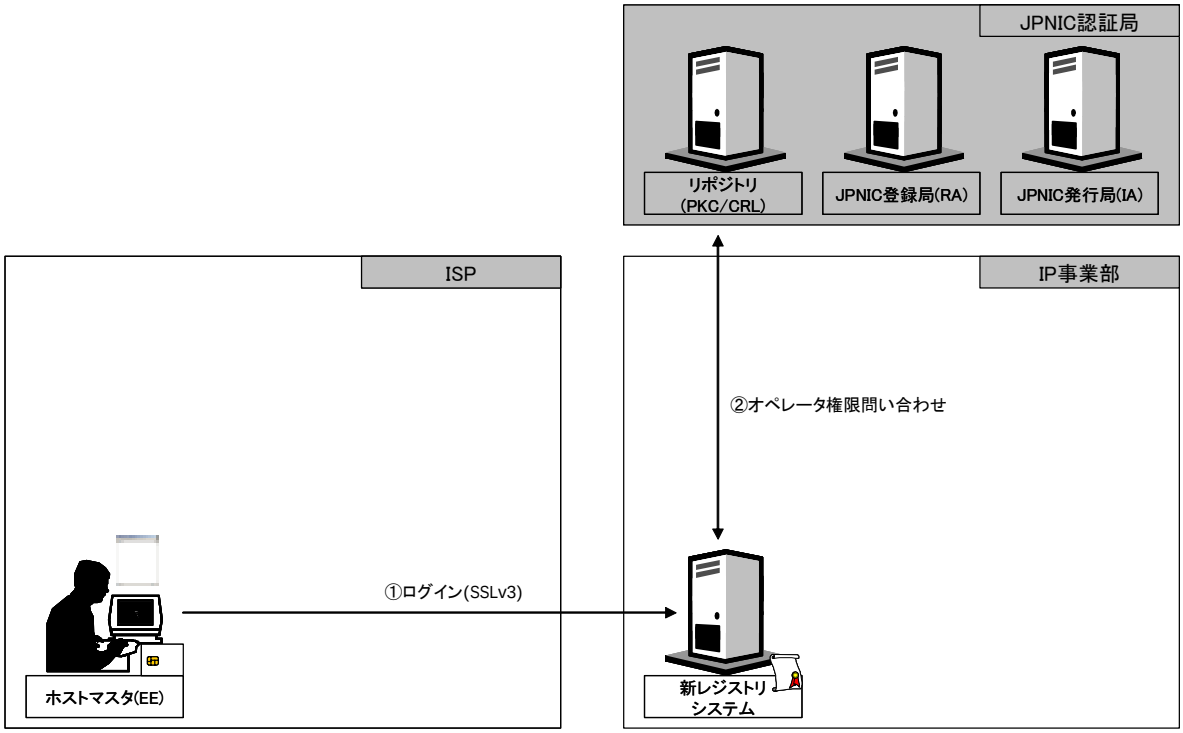


図 4-17 ホストマスタ（EE)の RS へのログイン概念図

4.5.7. IP 事業部スタッフ（RAA）失効

RAA の失効手続きは次のようになる。

（1） RAA より RAO に RAA 証明書失効申請書が送付される
（2） RAO から RAA 申請受付サーバに申請が行われる
（3） RAA 申請受付サーバから利用者管理サーバへ失効申請情報が登録される
（4） RAA 申請受付サーバから JPNIC 登録局へと失効申請が行われる
（5） JPNIC 登録局では失効作業を行った後、RAO に失効を通知する

この概念は図 4-18 で示される。

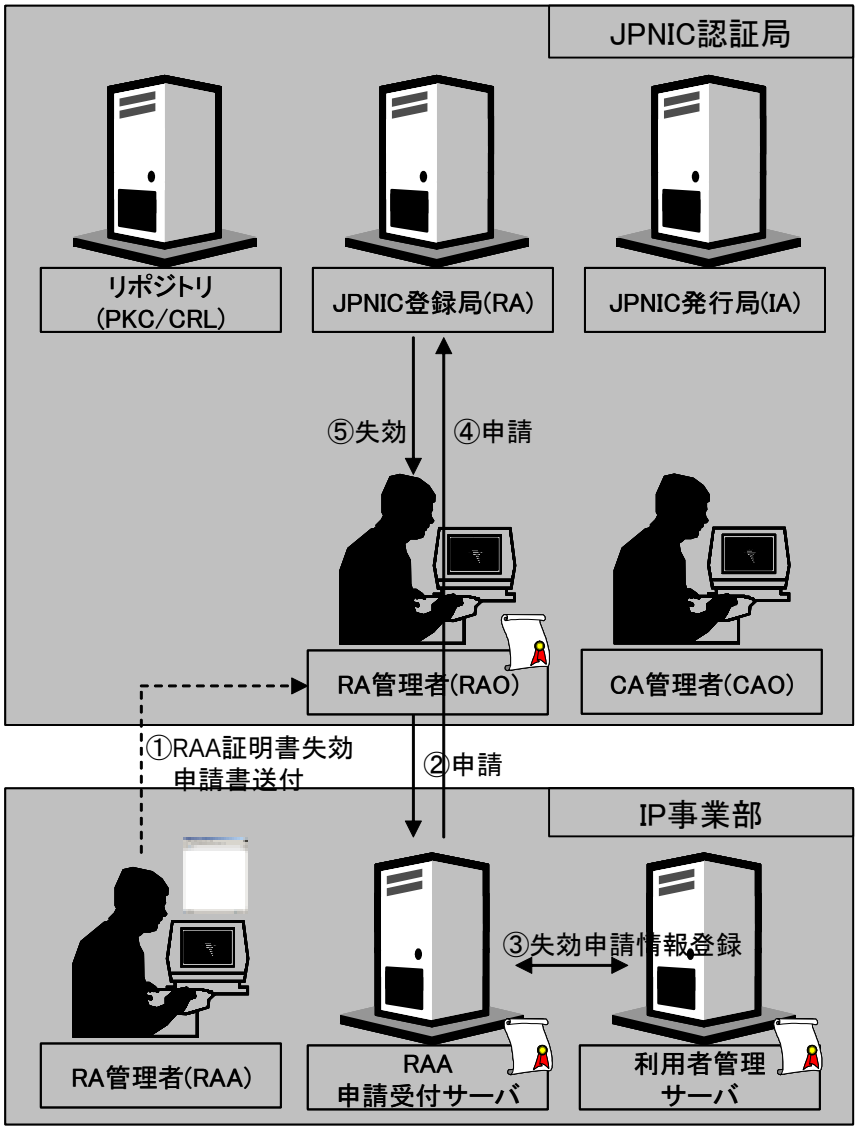


図 4-18 IP 事業部スタッフ（RAA)失効概念図

4.5.8. ISP 代表者（RA）失効

ISP 代表者の失効手続きは次のようになる。

（1） ISP 管理者から審査担当 RAA に RA 証明書失効申請書が送付される
（2） 審査担当 RAA から ISP 管理者申請受付サーバへ失効申請情報が登録される
（3） 承認担当 RAA から ISP 管理者申請受付サーバへ失効申請が送付される
（4） ISP 管理者申請受付サーバから JPNIC 登録局へ失効申請が実施される
（5） ISP 管理者申請受付サーバから承認担当 RAA に失効通知が送付される
（6） 審査担当 RAA から ISP 管理者に失効完了通知書が送付される

この概念は図 4-19 で示される。

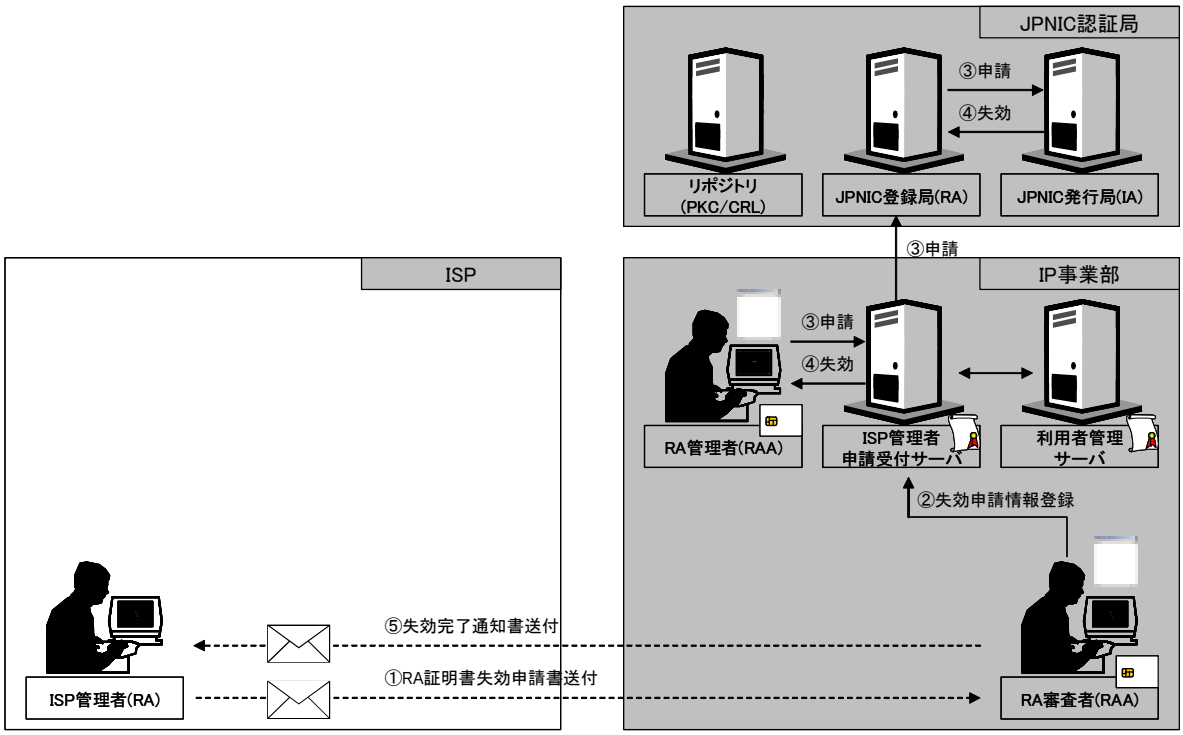


図 4-19 ISP 代表者（RA)失効概念図

4.5.9. ホストマスタ（EE）失効（センター承認モデル）

ホストマスタの失効手続きは次のようになる。

（1） ISP 管理者からホストマスタ申請受付サーバへ EE 証明書失効申請が送付される
（2） ホストマスタ申請受付サーバから利用者管理サーバへ失効申請情報が登録される
（3） ホストマスタ申請受付サーバから承認担当 RAA に失効申請通知が送付される
（4） 承認担当 RAA からホストマスタ申請受付サーバへ失効承認通知が送付される
（5） ホストマスタ申請受付サーバから JPNIC 登録局へ失効通知が送付される
（6） 承認担当 RAA から ISP 管理者へ失効完了通知が送付される
（7） ISP 管理者からホストマスタへ失効完了通知が送付される

この概念が図 4-20 で示される。

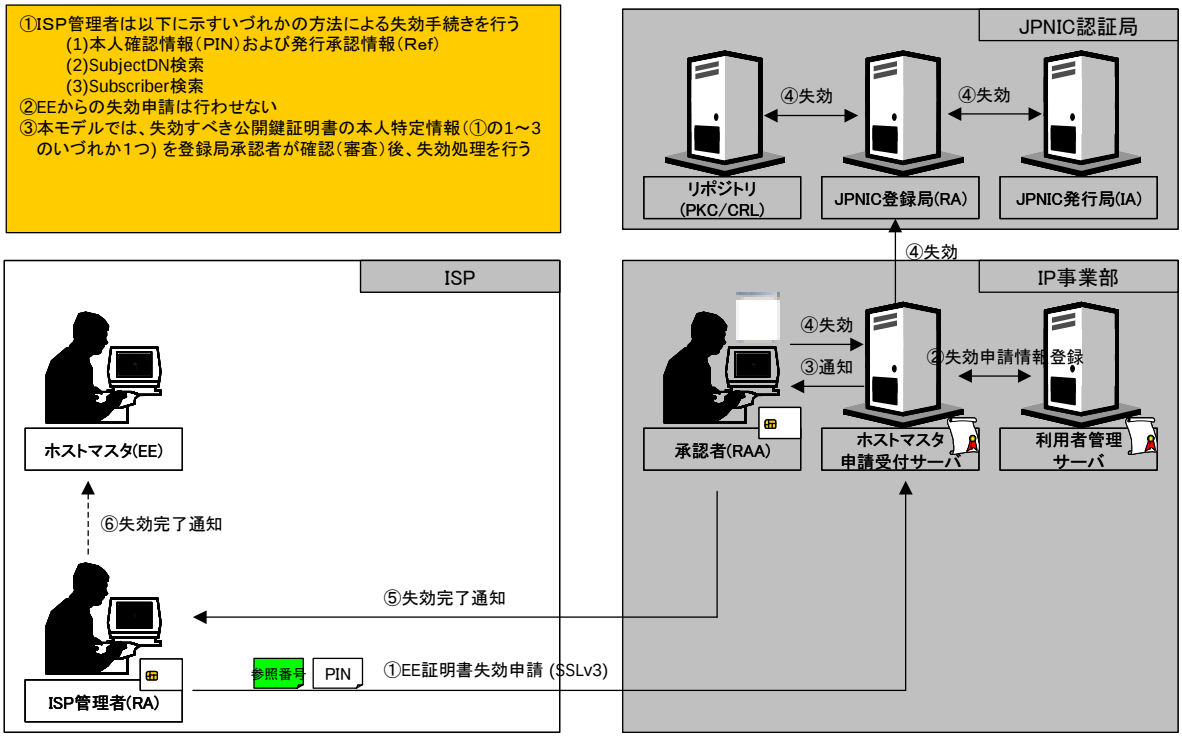


図 4-20 ホストマスタ（EE)失効概念図（センター承認モデル）

4.5.10. ホストマスタ（EE）失効（自動承認）

ホストマスタ認証と同様に、失効手続きにおいても確認作業を登録局が自動で行うモデルが考えられる。

この場合の手続きは次のようになる。

（1） ISP 管理者からホストマスタ申請受付サーバへ EE 証明書失効申請が送付される
（2） ホストマスタ申請受付サーバから利用者管理サーバへ失効申請情報が登録される
（3） ホストマスタ申請受付サーバから JPNIC 登録局へ失効通知が送付される
（4） 承認担当 RAA から ISP 管理者へ失効完了通知が送付される
（5） ISP 管理者からホストマスタへ失効完了通知が送付される

この概念は図 4-21 で示される。

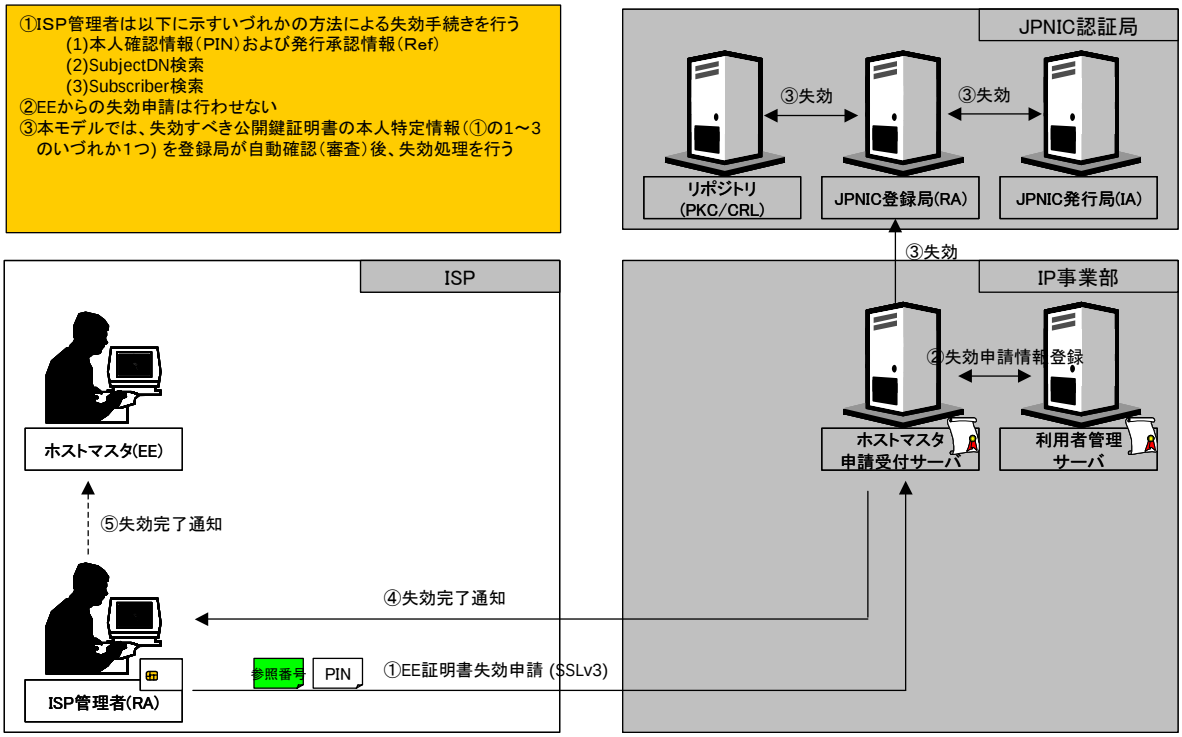


図 4-21 ホストマスタ（EE)失効概念図（自動承認モデル）

4.6. 機能リスト作成

ここでは前節で示した本認証局の各業務を実施するために必要な機能をリストアップする。その手法として、Work Breakdown Structure （作業分解図：以下、WBS と呼ぶ）を取り入れた。これは、初めに成果物を規定し、徐々に細分化して、実装すべき成果物に分解する。さらに、細分化された成果物に対する作業（以下、ワークパッケージと呼ぶ)を導出することで、プロジェクトに必要な作業を求める方式である。

ワークパッケージが求まると、それぞれの作業に対する責任者と担当者を決めることができ、プロジェクトの実施体制が出来上がる。これを Organization Breakdown Structure （以下、OBS という）と呼ぶ。

第一段階として、想定成果物の CA システムを以下の 5 つのシステムに細分化した。

- IA システム（Issuing Authority、証明書の発行業務を行なう）
- RA システム（Registration Authority、身元証明を行なう）
- リポジトリ（証明書リポジトリ、証明書と対応する公開鍵を発行する）
- 申請受付システム
- 利用者管理システム

これら 5 つのサブシステムをワークパッケージとし、さらに細分化する。この様子

は図 4-22 に示される。

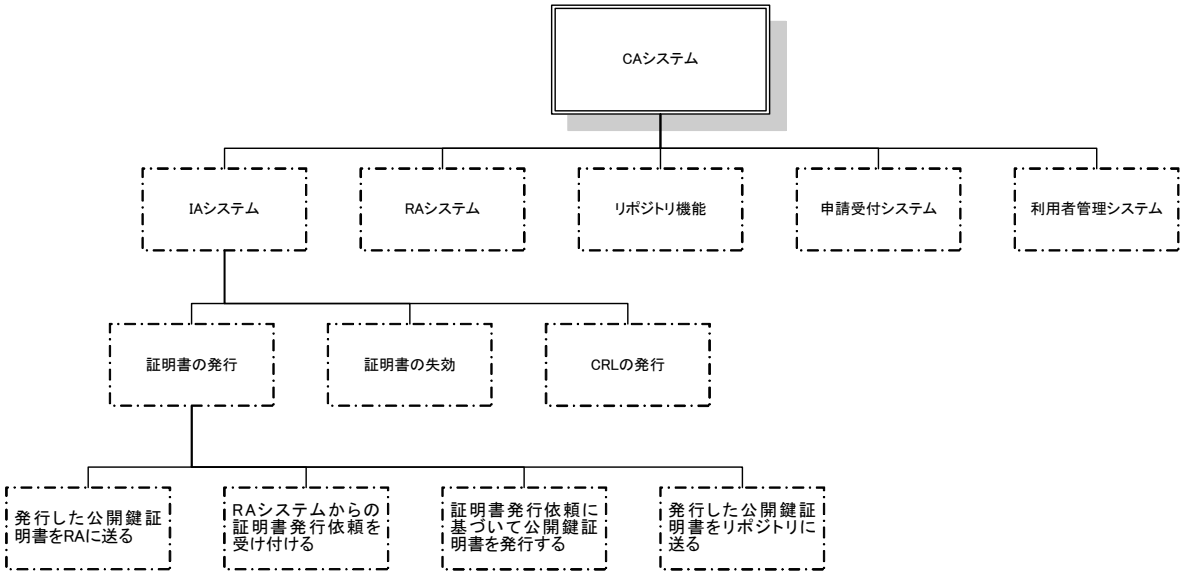


図 4-22 WBS 階層図（部分）

次節以降で、各サブシステムの詳細について述べる。

4.6.1. IA システム

IA システムの機能では、証明書の発行、証明書の失効、Certification Revocation List（証明書失効リスト：以下、CRL という）の発行を行なう。それぞれの機能について以下で説明する。

4.6.1.1. 証明書の発行

証明書の発行機能は次のように詳細化される。

- RA システムからの証明書発行依頼を受け付ける
- 証明書発行依頼に基づいて公開鍵証明書を発行する
- 発行した公開鍵証明書を RA に送る
- 発行した公開鍵証明書をリポジトリに送る

この機能は、次の手続きに対応して実施される

表 4-12 証明書の発行機能が実施される手続き

機能	対応する手続き
IP 事業部スタッフ認証	RAA 申請受付サーバから JPNIC 登録局へ申請が行われる
ISP 代表者認証	承認担当 RAA から ISP 管理者受付サーバに申請が行われる
ホストマスタ認証 （センター承認モデル）	承認担当 RAA が EE 証明書発行依頼を承認する
ホストマスタ認証 （自動承認モデル）	ホストマスタからホストマスタ申請受付サーバへ EE 証明発行依頼が送付される

4.6.1.2. 証明書の失効

証明書の失効機能は次のように詳細化される。

- RA システムからの証明書失効依頼を受け付ける
- 証明書失効依頼に基づいて失効データベースに登録する
- 失効データベースへの登録を RA システムに通知する
- 失効データベースの情報から CRL を発行する

この機能は、次の手続きに対応して実施される

表 4-13 証明書の失効機能が実施される手続き

機能	対応する手続き
IP 事業部スタッフ失効	RAA 申請受付サーバから利用者管理サーバへ失効申請情報が登録される
ISP 代表者失効	承認担当 RAA から ISP 管理者申請受付サーバへ失効申請情報が送付される
ホストマスタ失効 （センター承認モデル）	承認担当 RAA からホストマスタ申請受付サーバへ失効承認通知が送付される
ホストマスタ失効 （自動承認モデル）	ホストマスタ申請受付サーバから利用者管理サーバへ失効申請情報が登録される

4.6.1.3. CRL の発行

CRL の発行機能は次のように詳細化される。

- 発行した CRL をリポジトリに送る

この機能は、証明書の失効機能に対応して実施される。

4.6.2. RA システム

RA システムでは二つの申請、証明書発行申請及び証明書失効申請を受け付け、処理を行なう。それぞれの機能について以下で説明する。

4.6.2.1. 証明書発行申請の管理

証明書発行申請の管理機能は次のように詳細化される。

- 申請受付サーバから送られた証明書発行申請を受け付ける
- 受け付けた証明書発行申請を IA システムに送る
- IA システムから公開鍵証明書もしくはエラーステータスを受け取る
- IA システムから受け取った公開鍵証明書もしくはエラーステータスを申請受付サーバへ送る

この機能は、証明書の発行機能に対応して実施される。

4.6.2.2. 証明書失効申請の管理

証明書失効申請の管理機能は次のように詳細化される。

- 申請受付サーバから送られた証明書失効申請を受け付ける
- 受け付けた証明書失効申請を IA システムに送る
- IA システムから証明書失効完了通知もしくはエラーステータスを受け取る
- IA システムから受け取った証明書失効完了通知もしくはエラーステータスを申請受付サーバへ送る

この機能は、証明書の失効機能に対応して実施される。

4.6.3. リポジトリ

リポジトリ機能では、証明書・失効リストの登録、証明書・失効リストの公開を行なう。それぞれの機能について以下で説明する。

4.6.3.1. 証明書・失効リストの登録

証明書・失効リストの登録機能は次のように詳細化される。

- IA から送られた公開鍵証明書および CRL をリポジトリに登録する

この機能は、証明書の発行機能及び失効機能に対応して実施される。

4.6.3.2. 証明書・失効リストの公開

証明書・失効リストの公開機能は次のように詳細化される。

- 登録された証明書および CRL を公開する

この機能は、証明書・失効リストの登録機能に対応して実施されるとともに、リポジトリに対する証明書及び CRL の検索要求に応じて実施される。

4.6.4. 申請受付システム

申請受付システムの機能では、証明書・失効リストの登録、証明書・失効リストの公開を行なう。それぞれの機能について以下で説明する。

4.6.4.1. IP 事業部スタッフ（RAA)申請受付

IP 事業部スタッフ（RAA)申請受付機能は次のように詳細化される。

- RAO クライアントを認証する
- RAO クライアントからの RAA 証明書発行申請を受け付ける
- 利用者管理サーバに証明書発行申請の受け付けを通知し、ACK を受け取る
- RA システムに RAA 証明書発行申請を送る
- 利用者管理サーバに証明書発行申請の完了を通知し、ACK を受け取る
- RA システムから公開鍵証明書もしくはエラーステータスを受け取る
- RAO クライアントに対して公開鍵証明書もしくはエラーステータスを送る

この機能は、4.5.2 中の手続きに対応して実施される。

4.6.4.2. ISP 代表者（RA)申請受付

ISP 代表者（RA)申請受付機能は次のように詳細化される。

- 審査者クライアントを認証する
- 審査者クライアントから証明書発行申請における本人確認終了情報を受け取る
- 利用者管理サーバに証明書発行申請における本人確認の終了を通知し、ACK を

受け取る
- 承認者クライアントを認証する
- 承認者クライアントからの証明書発行申請を受け付ける
- 利用者管理サーバに証明書発行申請の受け付けを通知し、ACK を受け取る
- RA システムに ISP 管理者証明書発行申請を送る
- 利用者管理サーバに証明書発行申請の完了を通知し、ACK を受け取る
- RA システムから公開鍵証明書もしくはエラーステータスを受け取る
- 承認者クライアントに対して公開鍵証明書もしくはエラーステータスを送る
- 利用者管理サーバに証明書発行ステータス（完了またはエラー）を通知し、ACK を受け取る

この機能は、4.5.3 中の手続きに対応して実施される。

4.6.4.3. ホストマスタ（EE)申請受付

ホストマスタ（EE)申請受付機能は次のように詳細化される。

- ISP 管理者（RA)クライアントを認証する
- ISP 管理者クライアントから証明書発行申請を受け付ける
- 利用者管理サーバに証明書発行申請の受け付けを通知し、ACK を受け取る
- 承認者クライアントを認証する
- 承認者クライアントからの証明書発行申請を受け付ける
- 利用者管理サーバに証明書発行申請の受け付けを通知し、ACK を受け取る
- RA システムに ISP 管理者証明書発行申請を送る
- 利用者管理サーバに証明書発行申請の完了を通知し、ACK を受け取る
- RA システムから公開鍵証明書もしくはエラーステータスを受け取る
- 承認者クライアントに対して公開鍵証明書もしくはエラーステータスを送る
- 利用者管理サーバに証明書発行ステータス（完了またはエラー）を通知し、ACK を受け取る

この機能は、4.5.4 および 4.5.5 中の手続きに対応して実施される。

4.6.4.4. IP 事業部スタッフ（RAA)失効受付

IP 事業部スタッフ（RAA)失効受付は次のように詳細化される。

- RAO クライアントを認証する
- RAO クライアントからの RAA 証明書失効申請を受け付ける
- 利用者管理サーバに証明書失効申請の受け付けを通知し、ACK を受け取る
- RA システムに RAA 証明書失効申請を送る

- 利用者管理サーバに証明書失効申請の完了を通知し、ACK を受け取る
- RA システムから証明書失効終了通知もしくはエラーステータスを受け取る
- RAO クライアントに対して証明書失効通知もしくはエラーステータスを送る
- 利用者管理サーバに証明書失効完了を通知し、ACK を受け取る
- 利用者管理サーバに証明書失効ステータス（完了またはエラー）を通知し、ACK を受け取る

この機能は、4.5.7 中の手続きに対応して実施される。

4.6.4.5. ISP 代表者（RA)失効受付

ISP 代表者（RA)失効受付機能は次のように詳細化される。

- 審査者クライアントを認証する
- 審査者クライアントから証明書失効申請における本人確認終了情報を受け取る
- 利用者管理サーバに証明書失効申請における本人確認の終了を通知し、ACK を受け取る
- 承認者クライアントを認証する
- 承認者クライアントからの証明書失効申請を受け付ける
- 利用者管理サーバに証明書失効申請の受け付けを通知し、ACK を受け取る
- RA システムに ISP 管理者証明書失効申請を送る
- 利用者管理サーバに証明書失効申請の完了を通知し、ACK を受け取る
- RA システムから証明書失効完了通知もしくはエラーステータスを受け取る
- 承認者クライアントに対して証明書失効完了通知もしくはエラーステータスを送る
- 利用者管理サーバに証明書失効ステータス（完了またはエラー）を通知し、ACK を受け取る

この機能は、4.5.8 中の手続きに対応して実施される。

4.6.4.6. ホストマスタ（EE)失効受付

ホストマスタ（EE)失効受付機能は次のように詳細化される。

- ISP 管理者（RA)クライアントを認証する
- ISP 管理者クライアントから証明書失効申請を受け付ける
- 利用者管理サーバに証明書失効申請の受け付けを通知し、ACK を受け取る
- 承認者クライアントを認証する
- 承認者クライアントからの証明書失効申請を受け付ける
- 利用者管理サーバに証明書失効申請の受け付けを通知し、ACK を受け取る
- RA システムに ISP 管理者証明書失効申請を送る

- 利用者管理サーバに証明書失効申請の完了を通知し、ACK を受け取る
- RA システムから証明書失効完了通知もしくはエラーステータスを受け取る
- 承認者クライアントに対して証明書失効完了通知もしくはエラーステータスを送る
- 利用者管理サーバに証明書失効ステータス（完了またはエラー）を通知し、ACK を受け取る

この機能は、4.5.9 および 4.5.10 の手続きに対応して実施される。

4.6.5. 利用者管理システム

利用者管理システムの機能では、証明書申請ステータスの管理を行なう。それぞれの機能について以下で説明する。

4.6.5.1. 証明書申請ステータスの管理

証明書申請ステータスの管理機能は次のように詳細化される。

- 受付申請サーバから証明書申請ステータスを受け取る
- 利用者データベースに証明書ステータスを追加する
- 受付申請サーバに ACK を返す

4.7. まとめ

本章では、第 2 章で述べたレジストリにおける認証基盤の概念に基づいて、NIR における認証局（JPNIC 認証局）の設計について述べた。

設計に際して、認証局の目標・設計上の留意事項・業務モデルの検討を行い、更にその先の作業である CP/CPS の策定、ソフトウェアの検討に繋がる WBS と機能一覧の作成を行った。

本章で述べた検討方法が他の認証業務においても適用が可能であるかどうかは明言できないが、PKI を用いる新たな認証業務を検討する際の、認証業務の検討上の留意事項、運用体制の検討、業務モデルの検討といった要点について述べることができたのではないかと思われる。

本章で述べたモデルに基づく CP/CPS の策定については第 5 章で、ソフトウェアの検討については第 6 章で述べる。

第5章 CP/CPS 策定に関する検討

内容

- CP/CPS 策定の方針
  - CP/CPS の検討
  - 本検討と RFC3647 について

5. CP/CPS 策定に関する検討

5.1. 本章の目的

本章は、認証局の証明書ポリシ及び運用実施規定である CP/CPS（Certificate Policy and Certification Practice Statement）の策定を目的とし、記述すべき項目及び IP アドレス認証局の業務に則した記述内容の検討を行うものである。

5.2. 概要

IP アドレス認証局のあり方に関する調査を 2002 年度に実施し、セキュリティを考慮した運用要件の検討を進めてきたわけであるが、今回の検討では、セキュリティ要件の他に運用体制等実際の運用を考慮し検討を行った。CP/CPS の記述内容の検討、考察については 5.4.節に記述している。

本報告書上、継続検討課題としている部分も存在する。過度なセキュリティ要求とならないように考慮して検討を進めたが、更にシステムの詳細等が明らかになった時点で、CP/CPS の改善を行っていくものとする。

作成された IP アドレス認証局の CP/CPS（ドラフト版）を Appendix.1 として本報告書に添付する。また一連の検討の過程で必要とされた JPNIC ルート認証局の CP/CPS（ドラフト版）を Appendix.2 として本報告書に添付する。どちらの文書も、公開のときに利用される URL などを含めて改定される可能性がある。

5.3. RFC3647 について

RFC2527 は多くの認証局の CP/CPS 作成時のフレームワークとして利用されてきたが、今般 2003 年 11 月に RFC2527 を引き継ぐ新しい CP/CPS フレームワークとして RFC3647 が公表された。本報告書のための検討を行った時点において、RFC3647 はまだ公表されていなかったため、本報告書 5.4.節においては、RFC2527 のフレームワークにて記述している。なお、RFC2527 と RFC3647 の相違点及び追加検討事項は本報告書 5.5.節で述べるものとする。

5.4. CP/CPS の検討

本節においては、認証局の CP/CPS のフレームワークである RFC2527 の項目にそって、検討すべき項目、検討内容等を記述していく。なお、本報告書 5.4.1.項から 5.4.8.項において記述されている見出しの前の［X］、［X.X］、［X.X.X］の括弧書きの数値は RFC2527 における章、節、項の番号を示している。

5.4.1. ［1］はじめに

5.4.1.1. ［1.1］概要

CP/CPS の 1.1 節では、JPNIC IP アドレス認証局（以下、本認証局と呼ぶ）がどのような認証局であるのか（主体者、発行する証明書等）に関して、その概要を記述することとなる。また、CP/CPS が準拠する文書又は関連する文書があれば、それら文書との関係を記述することとなる。

検討項目としては、次の項目があげられる。

- どこが誰に対して、どのような証明書を発行するのか
- 本 CP/CPS が準拠又は関連する文書には、何があるか
- CP と CPS とを分離して記述するか

（1） 主体者及び発行する証明書について

本認証局における証明書の発行主体は JPNIC となる。JPNIC が、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機能を実現するための証明書を、IP アドレス管理業務をする者に対して発行するものと考えられる。また、レジストリシステムにおいてユーザがサーバの認証をするために、JPNIC は当該サーバに対してサーバ証明書を発行するものと考えられる。

このほか、JPNIC は、本認証局の運用に必要な各種の運用用証明書[1]を発行するが、当該証明書は、JPNIC で別途定める運用規則に則り、厳格な手続きのもとに発行されることから、以降、本報告書においては詳細な記述はしないこととする。

（2） 本 CP/CPS が準拠又は関連する文書について

CP/CPS を策定するうえで最初に、CP と CPS を一体のものとして記述するか、独立したものとして記述するかの検討が必要である。独立したものと記述した場合には、CP/CPS の 1.1 節において CP と CPS の位置付け及び優先関係を規定する必要がある。CP と CPS とを分離して記述するかについては、後述する本報告書 5.4.1.1.（3）にて検討を行う。

CP/CPS の記述構成としては、RFC2527 に依拠することとするのが一般的であるが、2003 年 11 月に RFC2527 を引き継ぐ新しい CP/CPS フレームワークとして RFC3647

[1]本認証局の運用上、認証業務を担う各役割（認証局管理者、登録局管理者、セキュリティ管理者、ローカル登録局管理者等）を認証するために必要な証明書として、認証局管理者(CAO)証明書、登録局管理者(RAO)証明書、セキュリティ管理者証明書、ローカル登録局(LRA)管理者証明書等がある。これら、認証業務を担う各役割については本報告書 5.2. 手続管理にて述べる。

が正式にリリースされた。今後、策定される CP/CPS は RFC3647 に準拠するケースが増えると考えられ、現段階から RFC3647 準拠としておくことが望ましいと考えられる。ただし、本報告書 5.3.節にて述べたとおり、本報告書については RFC2527 のフレームワークにて記述している。

また、RFC2527 と RFC3647 は、相互にマッピング可能であるため、検討段階では RFC2527 のフレームワークに準拠するものの、最終的な CP/CPS は RFC3647 のフレームワークに準拠することが望まれる。

次に、WebTrust 基準[2]等、本認証局が準拠すべき基準があれば、本節に記述するのが一般的である。現段階では、本認証局は所定の基準に準拠することは予定しておらず、また、「電子署名及び認証業務に関する法律」における特定認証業務の認定の適用も想定していないが、将来的には何らかの基準への準拠が要求される可能性がある。したがって、以降各所の検討においては、各種の基準が示すレベルを参考にするものとし、現段階で準拠しなければならない基準については特定せず、CP/CPS の 1.1 節に記述しないものとする。

その他、関連する文書として、証明書所有者同意書、検証者同意書、その他の契約関連規程があるのであれば、これらとの関係を記述するのが一般的である。ここで、前述した規程のうち検証者同意書の必要性について、次に検討する。

本 CP/CPS は、JPNIC と IP アドレス管理指定事業者との間のレジストリ管理業務を適用対象としており、証明書を検証する者は、証明書を発行されている者と同一範囲に限定されると考える。したがって現段階では、証明書所有者同意書の中で検証者としての事項を併せて規定すれば、検証者同意書を別途規定する必要はないと考えられる。

前述のように、証明書所有者同意書が存在し、その他の契約関連規程がないものとすると、CP/CPS 及び証明書所有者同意書の関係を記述すればよいこととなる。本認証局においては、CP/CPS と証明書所有者同意書の内容に齟齬がある場合は、現段階では、証明書所有者同意書が優先して適用されるものとする。

（3） CP と CPS とを分離して記述するか

ここでは、JPNIC が発行する証明書に関わるポリシ（CP）並びに JPNIC が適用する認証業務規定（CPS）を一体として記述するか、独立（分離）して記述するかについて検討する。

CP と CPS を独立して記述する場合、CP と CPS はその目的は異なり、別々の観点から記述することができる。認証局の設備、システム及び運用等証明書をどのように

[2] WebTrust Program for Certification Authorities V1.0（2000 年 8 月 25 日）、AICPA/CICA

発行するのかについてはCPS に記述し、どのような証明書を発行するのかに関わる規則やプロファイルについてはCP に記述することになる。

一般的に、CP と CPS は、表裏一体の関係にあり、相補的なものと言われている。したがって、CP と CPS を一体化した場合においても、十分にその両方の機能を満たす記述ができること、また効率的な作成及び管理ができること、利用者にとっても理解しやすいこと等のメリットがある。特に、発行する証明書の種類が固定的であり、かつ証明書の適用範囲及び認証局の運用体制についても固定的である場合には、一体型での記述で問題がないと考えられる。

また、本認証局の場合は、次の特徴がある。

- 本認証局が発行する証明書は、種類がほぼ固定的であり、本認証局の認証業務及びシステムの変更又は拡張も、少ないと考えられる。
- JPNIC と IP アドレス管理指定事業者等との間における適用範囲が限定されたコミュニティでの運用であり、パブリックサービスの場合と比較して、CP/CPS の改訂があったとしても利用者に及ぼす影響が少ない。

前述から、本認証局の CP/CPS は、一体型としての記述が良いのではないかと考えられる。そこで、本報告書では、CP/CPS を一体型として記述するものとして、CP/CPS の各章・節・項の検討を行うこととする。

「1.1.概要」記述案

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 アドレス認証局の認証業務に関する運用規則を定める。

JPNIC IP アドレス認証局は、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。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 RFC2527「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。

JPNIC IP アドレス認証局は、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 CP/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、本認証業務の提供にあたり、自らのポリシ、証明書所有者及び検証者の義務等を、本 CP/CPS、証明書所有者同意書によって包括的に定める。なお、本 CP/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 CP/CPS は、証明書所有者及び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）に公開される。

(1)CP/CPS

CP/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本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 CP/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。

5.4.1.2. ［1.2］識別

CP/CPS の 1.2.節では、CP/CPS の正式名称及び証明書ポリシ（CP）のオブジェクト識別子（OID）を記述することとなる。これは、証明書拡張の CertificatePolicies 属性において、OID による制御を行う場合等に重要な意味を持つ。その他、CP の OID に限らず、関連する OID があれば本節に記述することとなる。

検討項目としては、次があげられる。

- 発行する証明書に割り当てられる OID について
- その他、関連する OID について

（1） 発行する証明書に割り当てられる OID

OID は、組織や文書等一つ一つのオブジェクトを区別するために、各オブジェクトに一意になるよう割り振られた識別子であり、階層構造で管理される。

本認証局の場合、証明書の発行組織である JPNIC の他、本 CP/CPS 並びに本 CP/CPS に基づいて発行される EE 証明書（ホストマスタ証明書及びサーバ証明書）のポリシに対して OID を割り当てることができる。本節では、このように割り当てた OID を列記するのが一般的である。

また、証明書拡張の CertificatePolicies 属性において、CP の OID を記述することで、その証明書がどの CP に基づいて発行されたかを示すことができる。証明書に CP の OID を含めるべきか否かであるが、OID を含める場合には、証明書の利用を OID

によってきめ細かに制御することが可能となる一方、検証アプリケーション側での実装が必要となるという問題がある。

本認証局の場合、証明書の利用に際し、次の特徴がある。

- 証明書の利用用途が主に SSL/TLS 及び S/MIME での利用と想定されていること。
- サーバ側では、識別名（DN：Distinguished Name）[3]によるアクセスコントロールが可能であること。
- 原則として、EE 間でのやり取りは発生しないとしていること。

前述から、本 CP/CPS に基づき発行される証明書内には、OID を含める必要性は必ずしもないと考えられる。

（2） その他、関連する OID

JPNIC 以外の主要なインターネットレジストリ（APNIC、RIPE NCC、ARIN 等）のうち、APNIC、RIPE NCC においては既に認証局運用に関するプロジェクトが開始しており、その他のインターネットレジストリにおいても、今後、レジストリシステムのセキュリティ確保のために認証局を構築する動きがでてくるものと思われる。その際、本認証局と、他の認証局との相互接続が検討され、本 CP/CPS にて相互認証証明書ポリシ等の OID を記述することになると考えられる。しかし当面、本認証局に APNIC 等との相互接続が予定されていないことから、現段階では、他の認証局に関連する OID の記述はせず、他の認証局との相互接続が決まった段階で、関連する OID の記述を検討するものとする。

「1.2.識別」記述案

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 JPNIC IP アドレス認証局に関連するオブジェクト識別子を､次に示す。

1.2.392.00200175　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

1.2.392.00200175.2.（OID は決定後に記述される） JPNIC IP アドレス認証局 認証業務規程（CP/CPS）

[3]識別名（DN：Distinguished Name）については、本報告書 5.4.3.1. 新規発行時での利用者の本人確認方法を参照のこと。

1.2.392.00200175.2.（OID は決定後に記述される） EE 証明書ポリシ

5.4.1.3. ［1.3］コミュニティと適用性

CP/CPS の 1.3 節では、証明書の利用目的、制限事項、利用環境、適用範囲、発行対象等を記述する。

CP/CPS 1.3 節の記述は、本認証局が発行する証明書をどのような目的で、どのような組織、人、物に対して流通させるのかという重要な要素を含んでいる。流通させる適用範囲が明確でないと、本人認証手段、証明書の検証手続きき等にも影響する。また、適用範囲、使用目的が明らかでないと、証明書に関する事故、訴訟への発展も危惧されるので十分な検討が必要と思われる。

検討項目としては、次があげられる。

- 証明書の流通するコミュニティ（組織、人、物）
- 証明書の適用範囲
- 証明書が適合する又は使用が制限されるアプリケーション
- 証明書の使用が禁止される用途
- 証明書の相互運用性

（1） 証明書の流通するコミュニティ（組織、人、物）

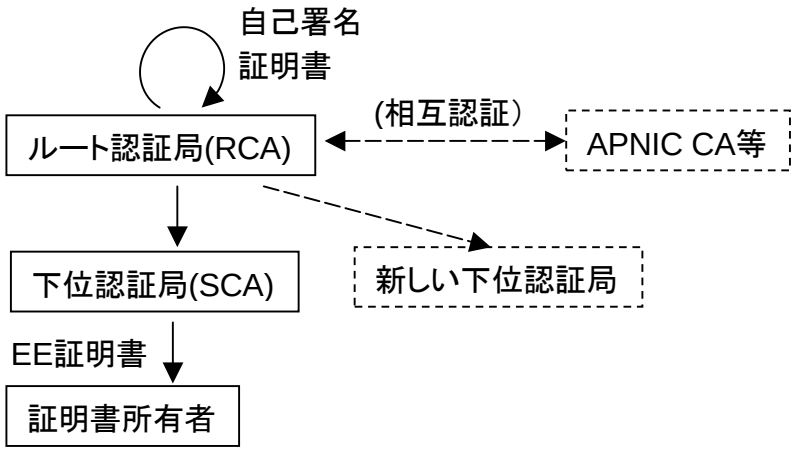
証明書の流通するコミュニティを検討する前に、本認証局を単独の認証局とするか、階層構造を持った複数の認証局の一部（下位認証局）とするかの検討が必要である。各々のメリット・デメリットを表 5-1 に示す。

表 5-1 認証局の構成比較

ケース	メリット	デメリット
単独型認証局	認証局構築・運用コストの低減が図ることができる。	システムの拡張性・応用性が制限される。他の認証局と接続する場合、要件により認証局を再構築する必要がある。
階層型認証局	新たな用途のための認証局追加が比較的容易、かつ既存の認証局に影響を与えない。また、ルート認証局の相互認証により、他との信頼関係の確立が容易となる。	複数の認証局を運営するための、運用負荷・コストが増加する。※ただし、製品の仕様及びライセンス体系に依存する。

本認証局の場合、当面、証明書の適用範囲として、レジストリシステムにおけるメ

ッセージ認証及びクライアント認証を想定しているが、将来的には、インターネットを通じて接続を受け付けるためのゲートウェイを認証する等、証明書の多面的な応用を検討している。その際、新しい用途の認証局を構築することが想定されるため、階層型認証局の構成を取っておくことが望ましいと考えられる（図 5-1)。この場合、新たに追加する下位認証局についてもルート認証局の認証を受けることで、互いの認証局ドメイン間での信頼関係確立が容易となる。また、APNIC CA 等との相互接続はルート認証局だけが行うことで、相互認証が可能となる。ただし、相互認証を行う場合には、相互認証証明書のプロファイルについて調整を行わなければならないと思われる。



RCA: Root Certification Authority, SCA: Subordinate Certification Authority

図 5-1　階層型認証局

次に、コミュニティを構成する認証局、EE 等の登場者の基本的な関係を図 5-2 に示す。JPNIC IP アドレス認証局は、登録局（RA)、発行局（IA）及びリポジトリから構成されるとして扱うのが一般的である。

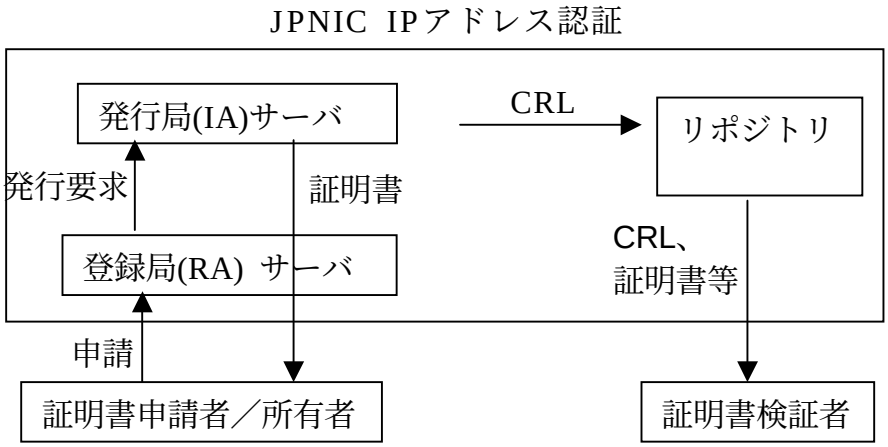


図 5-2　認証局、EE 等の登場者の関係

ここで、主たる証明書所有者は IP アドレス管理指定事業者に所属するホストマスタとなるが、JPNIC が個々のホストマスタに対して証明書の発行業務をすることは、人的業務量が膨大となり非現実的である。そこで、JPNIC は、JPNIC との契約において関連付けられた日本国内の IP アドレス管理指定事業者（以下、LRA[4]と呼ぶ）の管理者（以下、LRA 管理者と呼ぶ）のみを認証し、LRA 管理者が個々のホストマスタ個人を認証する仕組みとする（図 5-3）。

[4] LRA: Local Registration Authority

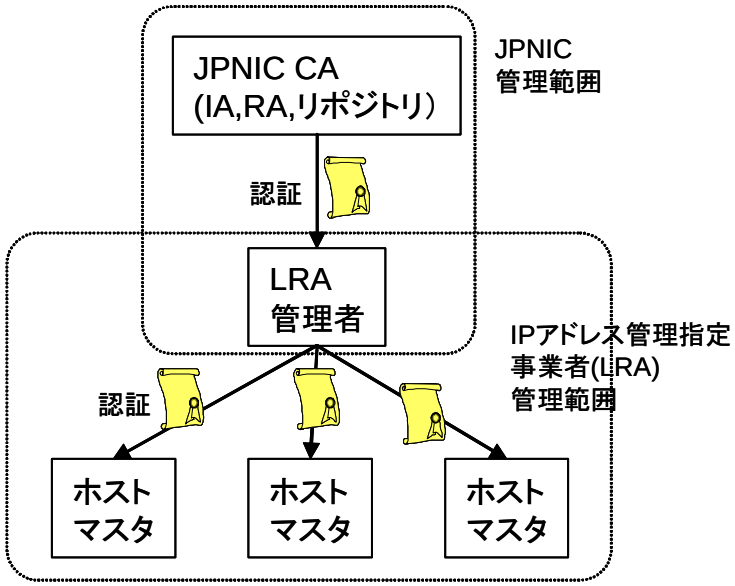


図 5-3　LRA による個人認証モデル

CP/CPS 1.3 節においては、前述したような、証明書の流通するコミュニティに関係する登場者と役割をまとめて記述するのが一般的である（表 5-2）。

表 5-2　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
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	申請者	EE 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 CP/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 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 登録局	JPNIC RA	証明書発行の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。
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（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。

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 の約款に従って運営される。
ローカル登録局	LRA	証明書を発行する組織とは異なる別組織であり、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。
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。

（2） 証明書の適用範囲

ここでは、発行する証明書の用途について記述することとなる。本認証局の発行する証明書は、JPNIC の行う IP アドレス管理業務における各種申請、連絡等に使用するものであり、IP アドレス管理業務に関係しない使用、特に商取引での使用等には利用できないとするのが妥当である。

具体的には、前述した目的のもと、EE 証明書（サーバ証明書及びホストマスタ証明書）は、レジストリシステムにおけるサーバ及びクライアント（ユーザ）間の相互認証並びにメッセージ認証に用いる。また、本証明書の否認防止目的での使用は想定しないものと考えられる。

（3） 証明書が適合する又は使用が制限されるアプリケーション

ここでは、発行する証明書が適合するアプリケーション及び使用が制限されるアプリケーションがあれば、該当するアプリケーションの一覧を記述することとなる。

本認証局で発行する証明書は、主に SSL/TLS 及び S/MIME での利用を想定している。ただし、現段階では、適合する具体的なアプリケーションについては絞り込めていない状況である。また、既存の CP/CPS においても、適合するアプリケーションについて明記していないのが一般的であるため、本 CP/CPS においても現段階では、記述しないものとする。一方、使用を制限するアプリケーションについても現段階では特に該当するものがないため、記述しないものとする。

（4） 証明書の使用が禁止される用途

ここでは、本認証局の発行する証明書の使用を禁止すべき用途があれば、記述することとなる。

本認証局の発行する証明書は、JPNIC の行う IP アドレス管理業務における各種申請、連絡等に使用するものである。したがって、IP アドレス管理業務に関係しない使用、とりわけ商取引での使用等については禁止することが妥当と思われる。

また、IP アドレス管理業務における各種申請及び連絡等は、JPNIC と IP アドレス管理指定事業者のホストマスタ等との間でなされるものであるから、JPNIC を介さないホストマスタ間での連絡等への使用は、証明書の適用範囲からは外れるものと考えられる。しかし JPNIC として、当該証明書のホストマスタ間での使用を禁止するというのは行き過ぎであると思われ、CP/CPS 上は、ホストマスタ間での証明書使用を禁ずるものではないが、JPNIC が責任を持たないこととするのが妥当であると考える。

（5） 証明書の相互運用性

ここでは、本認証局が発行する証明書の相互運用性等について記述するか否かについて検討する。

本認証局では、前述のとおり、階層型認証局での運用を想定しているが、現段階では他認証局との相互接続等は具体的には予定されていない。ただし将来的には、APNIC CA 等との相互接続が考えられるため、CP/CPS 上は、「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」といった記述にとどめることとする。

「1.3. コミュニティと適用性」記述案

（1） コミュニティにおける登場者と役割

本認証局が発行する証明書の流通するコミュニティには、表 5-2 に示す複数の登場者が含まれる。

（表 5-2 が記述される）

（2） 証明書の適用範囲

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。

（3） 証明書が適合する又は使用が制限されるアプリケーション

規定しない。

（4） 証明書の使用が禁止される用途

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。

（5） 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。

5.4.1.4. ［1.4］連絡先

CP/CPS 1.4 節では、本 CP/CPS の登録、維持管理及び解釈に責任を負う機関の名前と住所を記述することとなる。また、本 CP/CPS に関する連絡先の担当者の名前、電子メールアドレス 電話番号、FAX 番号を記述することとなる。

各種基準では、認証局の管理組織の連絡先として組織名、責任者、住所、電話番号、FAX 番号、電子メールアドレスの明確化及び開示を求めている。

また通常、連絡先の情報として、住所、担当窓口名、電話番号、FAX 番号、電子メールアドレスを記載する他、問い合わせ受付時間を営業時間に限定する場合には、営業日及び営業時間も明記するのが一般的である。

一方で、認証局の所在地等を詳細に開示することが、セキュリティ上の問題を引き起こすとも考えられるため、詳細な連絡先を記述しないこともある。

JPNIC の場合、IP アドレス管理業務の重要性及び認証局のセキュリティを重視して、所在地等の明示は行わないことが望ましいと考えられる。ただし、一定の情報公開の責任はあるため、必要最小限の連絡窓口情報は記述するのが妥当である。

「1.4.連絡先」記述案

本 CP/CPS に関する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］用語

CP/CPS 1.5 節では、本 CP/CPS の内容を正しく理解するうえで必要となる用語の解説を記述することとなる。

用語の解説については、RFC2527 及び各種基準ともに、記述することを要求していないが、CP/CPS の理解を容易にするために、一般的な用語については解説しておくことが望ましいと思われる。ただし、本 CP/CPS 1.3 節において、本認証局に関係する登場者について記述するため、登場者等に関する別途ここでの解説は不要であると考える。そこで、CP/CPS 1.5 節では表 5-3 に示すような、CP/CPS にて記述される一般的な用語についてのみ、解説するものとする。なお、解説する用語が多数となる場合、本節に記述するのではなく、CP/CPS の最後に別章を設けて記述する場合もある。

表 5-3 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 CP/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 CP/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。
RFC2527		Request For Comments 2527 認証局 や PKI のための CP/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	OID	Object Identifier 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。秘密鍵と呼ぶこともある。
証明書発行要求	CSR	Certificate Signing Request 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。

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取消された 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。

「1.5.用語」記述案

（表 5-3 が記述される）

5.4.2. ［2］一般条項

5.4.2.1. ［2.1］義務

［2.1.1］JPNIC 発行局の義務

CP/CPS 2.1.1 項では、主に発行局が発行局自身やリポジトリの信頼性と安全性を確保するための義務を規定する。

その他の検討項目として、次のものがあげられている。

- 発行した証明書の申請者への発行通知
- 申請者以外への発行通知
- 証明書失効後の所有者への失効通知又は停止された証明書の所有者への通知
- 証明書失効後の所有者以外への失効通知又は停止した証明書の所有者以外への通知

JPNIC 発行局自身やリポジトリの信頼性・安全性確保や、所有者・検証者に対する適切な情報提供を保証するために、JPNIC 発行局が JPNIC 登録局や発行する証明書やリポジトリに対して負う義務を検討しなければならないと思われる。

その一つとして、JPNIC 発行局から発行された証明書であることを証明するための JPNIC 発行局の証明書署名鍵を安全に生成し、確実な管理を行うことや、問題がないことを証明する情報を公表する義務があると考えられる。なぜなら、この署名鍵が改ざん又は漏えいすることがあれば、JPNIC 発行局が発行した全ての証明書の信頼性が損なわれるからである。

また JPNIC 登録局からの申請を正確に受付け、正確な処理が行われるよう JPNIC 発行局のシステム稼動を監視し、正常な動作を保つ義務があると考える。

今回の検討では、認証局が EE に対して証明書の発行に必要な情報を送付し、EE 自身が鍵ペアを生成し、証明書の発行に必要な情報とともに認証局システムへアクセスすることにより、証明書をその場で受け取ることができる仕組みを想定している。ゆえに、EE は証明書の発行操作時点で証明書が発行されたことを認識できる。また、リポジトリにおいても確認ができるので、発行した証明書の申請者への発行通知は不要と考える。

申請者以外への発行通知に関しては、一般的には特に申請者以外に知らせる必要はないと思われる。証明書失効後の所有者への失効通知又は停止された証明書の所有者への通知に関しては、JPNIC が必要と考える特別な事情のもとで強制的に失効させることがない限り、所有者又は LRA 担当者からの失効申請に基づいて失効が行われ、CRL へ反映されるため、これをもって所有者への通知と考えられる。また、JPNIC の決定のもとで EE の証明書が失効させられた場合には、所有者への通知を直接又は LRA を介して行う義務があると考える。JPNIC 認証局では証明書の停止を行わない

ため、これに関する義務はないと考える。

証明書失効後の所有者以外への失効通知又は停止した証明書の所有者以外への通知に関しては、一般的には特に申請者以外に知らせる必要はないと思われる。証明書の失効に関する情報は、CRL に開示することで通知されているものと考えることとした。ただし、CRL をいつでも確認できるようにリポジトリを維持管理する義務が発生する。ここで、これらの義務の詳細な検討については JPNIC 発行局のサービスレベルによって大きく影響されるため、特に具体的な数値や可用性、規定すべき内容の表現等は JPNIC 発行局のサービスレベル決定後に再度検討する必要がある。

前述の検討内容を踏まえた CP/CPS 記述案を次に示すが、最低限必要であると思われる一般的な規定内容を示す。

「2.1.1.JPNIC 発行局の義務」記述案

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
- 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

［2.1.2］JPNIC 登録局の義務

CP/CPS 2.1.2 項では、登録局が発行局・LRA・申請者等に対して負う義務を規定する。

JPNIC が JPNIC 登録局自身の信頼性・安全性確保を保証するために、JPNIC 登録局が JPNIC 発行局･LRA･申請者に負う義務として次のようなことが考えられる。

- JPNIC 登録局の端末を不正に操作され、不正な証明書の発行・失効が行われるということがない環境の構築や、端末の運用
- 証明書の発行・失効申請において、JPNIC 発行局へその正確な申請を行うこと
- 失効申請があった場合は、証明書有効性と関わりがあるため、速やかに正確

な失効申請処理を行うこと
等

ここで、JPNIC 登録局にて証明書の発行・失効申請を受付ける時間帯を限定するか 24 時間とするかを検討する必要があると思われる。特に失効申請受付時間帯に関しては証明書有効の確実性と関わりがあるため、この時間帯を明確にし、JPNIC 登録局がこの決定に沿った運用を行うことが義務になると考えられる。ただし、受付時間については、運用体制やコストに大きく影響するため、次のような検討を行った。

証明書の発行・失効申請を受け付ける時間帯を限定せず 24 時間対応とすれば、緊急の失効申請に対しても受付可能であるため、証明書の信頼性が高くなる一方、時間外に受付要員を配置する必要があり、運用体制及び人件費コスト等の問題が生じる。

一般的に証明書の失効処理が即時に行えるということは、証明書の信頼性を高めることになると考えられるため、極力 24 時間の受付を行うことが望ましい。このためには要員の対応だけでなく、システム面での 24 時間対応の検討も必要である。24 時間対応としない場合には、時間外に失効申請が受付けられない際に生じる損害を考慮しつつ、受付時間帯を検討しなければならない。しかし現段階では、詳細な検討ができず、後述の記述案においては、JPNIC 登録局の受付時間に関する義務は規定しないものとする。

前述の検討内容及び一般的な CP/CPS の例を踏まえ CP/CPS 記述案を次に示すが、CP/CPS への記載内容は JPNIC 登録局のサービスレベルや運用手順によって大きく影響されるため、実際の利用組織である IP アドレス管理指定事業者と協議を行ったうえで再度規定内容を検討する必要があると思われる。

「2.1.2.JPNIC 登録局の義務」記述案

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

［2.1.3］ローカル登録局の義務

CP/CPS 2.1.3 項では、LRA が登録局・申請者・所有者等に対して負う義務を規定する。

主な検討項目として次のものが考えられる。

- 証明書発行申請を行う前に確実な本人確認の実施
- 申請情報の登録局への正確な伝達

その他にも、LRA 自身の信頼性や安全性確保を保証するための義務を規定する。

前述の各検討項目に対応した LRA の義務を次のように検討した。

証明書発行申請を行う前に確実な本人確認の実施に関しては、申請者が証明書申請書類上の本人であることを LRA 管理者が確実に認証し、JPNIC 登録局へ LRA 管理者が正確に発行申請する義務があると考える。

申請情報の登録局への正確な伝達に関しては、申請者から提出され、審査が終了した申請書類の情報に基づいて LRA 管理者がそれらを正確に JPNIC 登録局へ伝達する義務があると考える。

LRA 自身の信頼性や安全性確保を保証するために、LRA が JPNIC 登録局や申請者や所有者に負う義務を検討しなければならないと思われる。

その一つとして、LRA には、JPNIC との間で取り交わされた契約に基づいてその業務を行う義務があると考えられる。なぜなら、その契約の中で JPNIC 認証局と LRA のそれぞれの業務における責任の所在を明確に分離するために、責任について詳細な規定が行われると考えられるからである。

また LRA には、証明書利用上の注意事項に関して、ホストマスタに徹底させる義務があると考えられる。なぜなら、ホストマスタは LRA 業務を行う IP アドレス管理指定事業者の一員であるため、各 LRA にて所属するホストマスタへの教育を行うべきであると考えられるからである。

現段階では、JPNIC と IP アドレス管理指定事業者との間で行われる契約や義務等に関する協議が行われていないので、協議後に改めて規定内容を検討する必要がある。よって、CP/CPS の記載内容として最低限必要と思われる記述案を次に示す。

「2.1.3.ローカル登録局の義務」記述案

LRA は LRA 業務を遂行するにあたり次の義務を負う。

- 申請書類上の所有者と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
- 証明書利用におけるホストマスタの教育
- 正当な申請者への確実な証明書配布（鍵ペアの受渡しについては生成システムに依存するため、後日の要検討内容）
- 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

［2.1.4］証明書所有者の義務

CP/CPS 2.1.4 項では、所有者が LRA や各自の証明書等に対して負う義務を規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 証明書アプリケーションを用いた証明書記載内容正確性の確認
- 各自の私有鍵の防護
- 私有鍵と証明書使用についての制限厳守
- 私有鍵改ざんについての LRA への通知

前述の各検討項目に対応する JPNIC 認証局が発行する証明書の所有者の義務を次のように検討した。

証明書アプリケーションを用いた証明書記載内容正確性の確認に関しては、JPNIC 発行局から発行された証明書に記載されている内容が、自らの申請内容と同一であることを確認する義務があると考えられる。また記載内容に誤りがある場合には、速やかに LRA へ申告する義務もあると考えられる。

各自の私有鍵の防護に関しては、他人への貸与を行わないことや他人によって不正に使用されないよう管理する義務があると考えられる。もし CP/CPS に規定された証明書の失効申請を行うべき条件に該当する事象が生じた場合には、速やかに LRA へ失効申請を行う義務もあると考えられる。

私有鍵と証明書使用についての制限厳守に関しては、所有者は CP/CPS に規定されている内容を理解し、所有者本人による使用であっても CP/CPS に規定された利用範囲を超えて使用しないことを厳守する義務があると考えられる。

私有鍵改ざんについての LRA への通知に関しては、所有者の私有鍵が改ざんされた場合又はそのおそれがある場合には、速やかに LRA へ失効申請を行うこと義務があると考えられる。同様に私有鍵が漏えいした場合又はそのおそれがある場合にも、速やかに LRA へ失効申請を行う義務があると考えられる。

その他にも証明書申請時の所有者による正確な情報の提示等を保証するために JPNIC が所有者に課す義務を検討しなければならないと思われる。

ただし、これらの義務に関しては CP/CPS 上で詳細に記載するのではなく、別途“ 証明書所有者同意書 ” を作成しその中で詳細に規定することも考えられる。公開する CP/CPS 上にて所有者の義務の詳細な記述を行うことは困難であっても、証明書所有者同意書として別途、所有者の義務や責任を詳細に記述し、申請者から証明書所有に関する詳細な同意を得ることが可能である。また CP/CPS 上に記載するより内容の改

定手続きが容易となると考えられる。

一方、証明書所有者同意書を作成すると、管理すべき書類（同意書の改版や同意後の書類等）の増加や、申請者との間での同意書授受処理を行う必要が生じると考えられる。

一般的に、CP/CPS 上には基本的な方針を記載するべきであって、詳細な規定を記述するべきではないと思われる。JPNIC 認証局運営における、所有者義務内容の変更に留意し、証明書所有者同意書のような規定を別途作成し、証明書所有者に対して理解と承諾を求めることが望ましい。

前述の検討内容を踏まえた記述案を次に示すが、詳細な規定内容は所有者同意書に記述されることを前提として、一般的な規定内容を示す。

「2.1.4.証明書所有者の義務」記述案

所有者は証明書所有にあたって、次の義務を負うものとする。

- 本 CP/CPS 及び（証明書所有者同意書以外にも必要な書類があれば記載する）の理解と承諾
- 証明書所有者同意書の理解と、証明書所有者同意書への署名
- 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
- 利用目的の確認と利用目的内での利用
- 証明書申請内容の正確な提示
- 私有鍵の秘匿管理や私有鍵と公開鍵の対応管理

［2.1.5］証明書検証者の義務

CP/CPS 2.1.5 項では、検証者が証明書を信頼するにあたって証明書に対して負う義務を規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 証明書が使用される目的確認と承諾
- 署名検証
- 失効と停止の確認

前述の各検討項目に対応して JPNIC 認証局が発行する証明書の検証者の義務を次に検討する。

証明書が使用される目的確認と承諾に関しては、検証者がその証明書を信頼するに先立って証明書の使用目的を理解し、その内容に承諾していることを認識する義務があると考えられる。

署名検証に関しては、検証者がその証明書を信頼する根拠として、JPNIC 認証局による有効期限以内の有効な署名が付与されていることを確認する義務があると考えられる。

失効と停止の確認に関しては、検証者がその証明書を信頼する根拠として、CRL 上に当該証明書の登録が存在しないことを確認する義務があると考えられる。

その他にも検証者による証明書の適切な利用を保証するために、JPNIC が検証者に課す義務を検討しなければならないと考えられる。

その一つは、証明書を信頼する根拠として前述の義務以外に、証明書の有効期限と記載項目の確認を確実に行う義務があると考えられる。当該証明書が CRL に記載されていないとしても、証明書生成時に設定された有効期限を過ぎていることが考えられる。

「2.1.5.証明書検証者の義務」

検証者は証明書を信頼するにあたって次の義務を負わなければならない。

- 証明書を信頼する時点で、本 CP/CPS の理解と承諾
- 証明書の利用目的と自己の利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

［2.1.6］リポジトリの義務

CP/CPS 2.1.6 項では、リポジトリが検証者等に対して負う義務を規定する。

RFC2527 では、主な検討項目として次のものがあげられている。

- 証明書と失効情報の適時な公表

JPNIC 発行局によってリポジトリに登録された証明書の失効情報が、遅滞なく検証者による参照を可能とする義務がリポジトリにはあると考えられる

その他にも証明書利用目的や方法を踏まえてリポジトリの利用可能時間を検討する必要があると考え、次の検討を行った。

証明書有効性検証等のためのリポジトリ参照の利用可能期間を、JPNIC 認証局運営費用の削減等の理由により限定するなら、リポジトリの通常運用時間に関して次の点を検討する必要がある。

- 1 日の何時から何時まで運用するか
- 1 週間の何曜日に運用するか
- 1 年間を通して特別に運用を停止する時（年末年始等）があるか

しかし、一般的には任意のタイミングでリポジトリへのアクセスを許容するため、リポジトリの 24 時間サービス提供が原則と考えられる。24 時間のリポジトリサービス提供を行う場合は、24 時間提供することを明記するかどうかを検討しなければならないと思われる。明記することで、サービス利用者にサービスに対する信頼感を与えることができる一方、24 時間運用が義務化されるためにシステムの冗長化及び運用体制の強化等を行う必要がある。

ここで、既存の CP/CPS の多くはリポジトリの常時利用可能を前提条件としているが、「24 時間のリポジトリサービスを目指す。ただし、保守・緊急対応の必要性が発生した場合は除く。」といった柔軟な対応を許容する規定が一般的であり、これと同様な記述をすることが適当であると思われる。

「2.1.6.リポジトリの義務」記述案

JPNIC はリポジトリ運用を次のように行う。

- 所有者証明書やサーバ証明書の失効があった場合、直ちに当該証明書失効の公表をリポジトリにて行う
- CRL 等の必要情報を常時確認可能とする。ただし、保守・緊急対応の必要性等が発生した場合は除く

5.4.2.2. ［2.2］責任

CP/CPS 2.2 節中の各項では、発行局・登録局・LRA が取るべき責任について規定する。

RFC2527 では検討項目として次のものがあげられている。

- 権利と権利についての限度
- 補償される被害の種類と適用除外者
- 証明書ごと、若しくはトランザクションごとの賠償限度
- 天災や他の主体が負うべき責任等の例外事項

前述の各項目に基づいて JPNIC 発行局・JPNIC 登録局・LRA が他に対して取るべき責任を規定しなければならない。ただし、この責任の節は CP/CPS の義務及び賠償の節と重複する内容が多いため簡素な記述にまとめられることもある。

今回の検討では、前述の賠償限度、適用除外等の賠償、補償に関わる事項は CP/CPS 2.3 節に記述する。

［2.2.1］JPNIC 発行局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.1.JPNIC 発行局の責任」記述案

JPNIC 発行局は本 CP/CPS 2.1.1 項に従った運用及び 2.1.6 項に示されたリポジトリに関する管理に責任を負う。

［2.2.2］JPNIC 登録局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.2.JPNIC 登録局の責任」記述案

JPNIC 登録局は本 CP/CPS 2.1.2 項に従った運用を行う責任を負う。

［2.2.3］ローカル登録局の責任

本報告書 5.4.2.2.を踏まえた記述案を次に示す。

「2.2.3.ローカル登録局の責任」記述案

LRA は本 CP/CPS 2.1.3 項に従った運用を行う責任を負う。

5.4.2.3. ［2.3］財務上の責任

CP/CPS 2.3 節中の項では、認証局の責任を遂行するための財務上の責任について規定する。

RFC2527 では主な検討項目として次のものがあげられている。

- 補償の範囲
- 補償時の原資の調達先又は企業賠償責任保険への加入
- 補償金額上限

ここで、CP/CPS では JPNIC 認証局が発行する証明書の商用利用を目的としておらず、かつ閉じた領域で使用されるため、CP/CPS 2.2 節の責任に対する賠償の必要性があるかどうかを検討する必要がある。その検討結果として賠償する必要がないと結論付けられるなら、前述の各検討項目について考慮する必要はないと思われる。

一般的に損害賠償責任について、CP/CPS 上に明確に記述されることは少ない。よって、この項では、保証内容及び免責内容について検討した。

JPNIC によって管理し得ない原因によって生じる損害を免責内容とするのがよいと思われる。具体的に免責内容とすることが妥当と思われる状況を次に示す。

- 緊急的な保守時（リポジトリの停止等）
- 火災・停電等の発生時
- 自然災害発生時
- 戦争、テロリズム等の人的災害発生時
- 予想を超えた暗号解読技術の向上時
- LRA の責で生じた時

更にこれらの免責事項に該当しない場合でも、JPNIC は発生した損害の直接的な部分のみを賠償するとし、次に示す損害は免責内容とするのが良いと思われる。

- 間接損害
- 特別損害
- 付随的損害
- 派生的損害

「2.3.賠償」記述案

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、LRA との契約における該当条項に従う。

［2.3.1］依存する主体による賠償

ここでは、証明書検証者が適切に失効情報を調べることなく行った証明書の使用、又は認証局の許可の範囲外の目的での証明書の使用により、認証局が被った損失について証明書検証者が認証局に対し賠償する義務があることを定める協定を認証局が使用する旨定めることができる。

「2.3.1.依存する主体による賠償」記述案

規定しない。

［2.3.2］様々な主体との間の受託関係

CP/CPS 2.3.2 項では、様々な主体との間の受託関係についてその有無を規定する。

JPNIC に他との受託関係や親子関係等がないのであれば規定する必要性はないと考えられる。

「2.3.2.様々な主体との間の受託関係」記述案

規定しない。

［2.3.3］管理的手続き

CP/CPS 2.3.3 項では、課金や監査等の管理的手続きについて規定する。

この項の規定がある CP/CPS では企業会計原則等が記述されていることがある。一般的には特に記述不要と考えられる。

「2.3.3.管理的手続き」記述案

規定しない。

5.4.2.4. ［2.4］解釈及び執行

［2.4.1］適用される法律

CP/CPS の 2.4.1 項では、適用対象となる CP/CPS 又は協定の解釈と執行を一定の司法権 に属する法に準拠する旨の記述及び関係者が適用法を遵守する要件、例えば、

輸出規制の適用を受ける暗号ハードウェア及びソフトウェアに関連する法律等、に関して規定をすることができる。

今回の CP/CPS においては、本認証局の所在地は日本国であり、かつ証明書の発行対象となる EE は、JPNIC との契約において関連付けられた日本国内の IP アドレス管理指定事業者の組織から任命された者及び JPNIC 内で使用されるサーバであるため、日本国の法令を適用する旨の記述が妥当と考えられる。また、輸出規制や関連する法律を遵守する旨を記述する。

「2.4.1.適用される法律」記述案

本認証局を含む JPNIC 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 CP/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。また、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。

［2.4.2］分割、存続、合併及び通知

CP/CPS の 2.4.2 項では、CP/CPS、協定等の可分性、効力の継続性、サービスの統合等により CP/CPS に変更が発生する場合に対する方針を記述する。

一般的な記述としては、認証局の示す CP/CPS や協定等の一部の条項について、法律等により有効でないとされた場合においても、その他の条項については、有効性が存続する旨の記述がなされる。また、サービスの統合等により CP/CPS に変更が発生する場合の方針については、統合前の合意事項に責任を持ち続けることに最善を尽くす又は責任を持ち続ける旨の記述がなされる。

「2.4.2.分割、存続、合併及び通知」記述案

本 CP/CPS 及び本認証局より示す協定等において、その一部の条項が有効でないと判断された場合においても、他の条項については有効に存続するものとする。

また、本認証局は、サービスの統合等により CP/CPS に変更が発生する場合においても、統合前の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。

［2.4.3］紛争解決の手続き

CP/CPS の 2.4.3 項では、本認証局が行う証明書発行に関わる紛争について、訴訟、仲裁における手続きについての記述を行う。

「2.4.3.紛争解決の手続き」記述案

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、CP/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。

5.4.2.5. ［2.5］料金

CP/CPS の 2.5 節では、認証局、リポジトリ又は登録局によって課される料金に関して規定する。例えば、証明書の発行又は更新料、証明書へのアクセス料金、失効又はステータス情報へのアクセス料金、関連する CP/CPS へのアクセスを提供するといったその他のサービスに対する料金、払戻しに関する方針について記述することとなる。

本認証局の場合、一般個人、法人に証明書を発行する商用認証局とは異なるので、公開する CP/CPS 上に料金等を示さないのが一般的と思われる。また、今回の検討においては、料金等に関し検討は行われていないため、次のような記述案とする。

「2.5.料金」記述案

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、別途定められるものとし、事前に関係者に周知されるものとする。

5.4.2.6. ［2.6］情報の公表とリポジトリ

［2.6.1］認証局情報の公表

CP/CPS 2.6.1 項では、リポジトリに公表する認証局情報に関して記述する。

公表する情報としては、

- 自己署名証明書
- リンク証明書
- 相互認証証明書
- 下位認証局証明書
- EE 証明書

- CRL/ARL
- CP/CPS
- 証明書所有者/検証者同意書

等が考えられる。

認証局の構成、リポジトリの構成により発行する若しくは公表する証明書は異なるものとなるが、今回の検討においては、JPNIC ルート認証局と下位認証局である JPNIC IP アドレス認証局の構成とし、リポジトリに関しては、ルート認証局と下位認証局は同一のリポジトリを使用するものとして記述を行う。

検討項目として、CP/CPS、EE 証明書を公開するか否かがあげられる。

今回のような適用範囲が限定された利用においては、CP/CPS、EE 証明書を公開しない場合もありうる。

認証局は、関係者に対して義務等の周知及び認証局自体を紛争から守る意味での認証局の要件の周知を CP/CPS、契約書等にて行う必要がある。周知の一般的な方法として、CP/CPS をリポジトリに公開することが妥当と思われる。

EE 証明書については、リポジトリ上に公開することにより、証明書上の個人情報が広く知られることとなり、好ましくない場合もありうる。適用範囲が限定された利用においては、お互いの証明書を交換することが可能であり、証明書をリポジトリに公開しないで PKI を利用することが可能となる。継続的な検討課題として、EE 証明書をリポジトリに公開するか否かについては、今回の PKI 利用に関係する組織と業務上の利便性や個人情報保護の考え方等を踏まえ、更に検討するものとする。

「2.6.1.認証局情報の公表」記述案

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）
- 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、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）

［2.6.2］公表の頻度

CP/CPS 2.6.2 項では、公表する情報の公表頻度、時期について記述を行う。

CRL/ARL の公表時期、頻度については、認証局の運用形態、システムにより左右されるが、24 時間以内での更新が一般的と思われる。

「2.6.2.公表の頻度」記述案

（1） CP/CPS の公表については、本 CP/CPS 8 章にて規定される。

（2） 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する。

（3） CRL については、24 時間以内に定期的に更新が行われ、証明書の失効が行われた場合は即時に更新が行われる。

（4） 認証局に関する重要情報若しくはその他情報は、JPNIC 認証局の判断により適宜更新が行われる。

（5） EE 証明書については、発行及び更新の都度公表される。＊公表時のみ

［2.6.3］アクセスコントロール

CP/CPS 2.6.3 項では、CP/CPS、証明書のステータス及び失効リストを含む公開情報へのアクセス管理について記述する。

「2.6.3.アクセスコントロール」記述案

本認証局を含む JPNIC 認証局は、公表情報に関して、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。

［2.6.4］リポジトリ

CP/CPS 2.6.4 項では、認証局又は他の独立主体によって運用されているリポジトリの利用に関する要件について記述する。

「2.6.4.リポジトリ」記述案

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。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。

5.4.2.7. ［2.7］準拠性監査

［2.7.1］各主体に対する準拠性監査の頻度

CP/CPS 2.7.1 項では、CP/CPS に基づいて、評価されるべき個々のエンティティに対する準拠性監査又は他の評価を行う頻度又は評価を行うきっかけとなる状況について記述することとなる。

準拠性監査は、一般的に最低でも毎年実施することが必要と思われる。また、定期的な監査のほかに、運営責任者や運営委員会が必要と判断した場合は、即時に行われることが必要と考える。

「2.7.1.各主体に対する準拠性監査の頻度」記述案

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。

［2.7.2］監査者の身元・資格／認定にかかる事項

CP/CPS 2.7.2 項では、監査又は他の評価を行う担当者の身元、資格について記述を行う。

ここでは、

- 外部監査とするか
- 内部監査とする場合、内部監査組織は存在するか若しくは組織するか
- 監査する者の身元、資格を規定するか

等の検討が必要となる。

認証局の監査については、一般的な情報システム監査のほかに認証局特有の注意点（認証局鍵管理、暗号アルゴリズム、厳密性等）があり、認証業務に精通した監査者が望まれる。

現状、JPNIC の組織において、システム監査に関する内部監査組織は組織されておらず、また、現段階での検討においては、内部監査組織を組織化するのか又は外部監査の利用するのかについて定まっていないため、CP/CPS の記述上、運営委員会が指定する認証業務に精通した監査者により行われる旨の記述にとどめることとした。

「2.7.2.監査者の身元・資格／認定にかかる事項」記述案

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。

［2.7.3］監査者と被監査部門の関係

CP/CPS 2.7.3 項では、監査者の独立性の程度、監査者と被監査部門との関係を記述することとなる。

監査者は、監査する業務を客観的に評価する必要があり、被監査部門から独立していることが望まれる。

「2.7.3. 監査者と被監査部門の関係」記述案

JPNIC は、監査者を本認証局を含む JPNIC 認証局の認証業務に関わる要員以外から選定する。

［2.7.4］監査テーマ

CP/CPS 2.7.4 項では、評価又は評価を行うために使用された評価方法に関する事項に関して記述する。

認証局の準拠性監査は、認証局の運営が CP/CPS を遵守して運営されているかを確認するものである。監査項目としては、

- 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

等が考えられる。

また、運営委員会が必要と認めた監査目的による監査の実施も必要と考えられる。

「2.7.4.監査テーマ」記述案

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 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。

主な監査項目として、

- 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

等の監査を行う。

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。

［2.7.5］監査指摘事項への対応

CP/CPS 2.7.5 項では、監査において発見された不備等の指摘事項への対応について記述する。例としては、指摘事項が改められるまでの運用の一時的な停止、不正な証明書の失効、人事の変更、特別な調査の実施又は準拠性監査周期の変更及び不正を起こした要員に対する損害賠償請求等があげられる。

指摘事項に対する詳細な対応事項をもれなく列挙するのは難しく、損害賠償請求、証明書の失効等の詳細な記述はせず、認証局として、どのような方針で対応するのかの概要を示すことにとどめる。

「2.7.5.監査指摘事項への対応」記述案

本認証局を含む JPNIC 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。

［2.7.6］監査結果の通知、開示等

CP/CPS 2.7.6 項では、監査結果を誰が、誰に、どのように通知若しくは開示するのかを記述する。

検討点として、

- 公開文書とするのか
- 関連組織である LRA の要求があった場合、開示するか
- 開示する場合の手続きは

が、考えられる。

監査報告は、認証局の運用状態等が把握でき、セキュリティ上公開文書とするのは好ましくないと考えられる。また、内容によっては認証局としての信頼性の低下を引き起こす可能性のあるセンシティブな情報を含むことがあり、原則は、外部への開示は行わないとすることが良いと思われる。

「2.7.6.監査結果の通知、開示等」記述案

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。本認証局を含む JPNIC 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、監査報告書は、JPNIC 認証局運営責任者により最低 5 年間保管管理される。

5.4.2.8. ［2.8］秘密保護ポリシ

［2.8.1］秘密扱いとする情報

CP/CPS 2.8.1 項では、秘密扱いとする情報について記述する。

秘密扱いとする情報については、

- 申請に関わる情報
- 証明書の発行申請記録、失効申請記録、開示申請記録
- 監査ログを含む各種トランザクションの記録
- 監査の記録、監査報告書
- 不測の事態に対応する計画、災害時の復旧計画
- 認証局運用業務のセキュリティ対策
- 業務に関する、規定、手順書、マニュアル等
- 業務に関する記録

等が考えられる。

記述方法として、詳細にそれぞれの情報を記述するのか又は前述の CP/CPS 2.6 で公表すると定めた情報以外と記述するかの選択がある。今回の記述においては、公表すると定めた情報以外については、秘密情報として扱うこととする。

「2.8.1.秘密扱いとする情報」記述案

本認証局を含む JPNIC 認証局が保持する情報は、本 CP/CPS 2.6 節で公表すると定めた情報、本 CP/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を除き、秘密扱いとする。JPNIC 認証局は、本 CP/CPS 2.8.3 項から 2.8.7 項に定められた方法を除いてこれらの情報を開示しない。

証明書所有者の私有鍵は、その所有者によって秘密扱いとされる情報とする。

なお、個人情報の保護に関する取扱は、本 CP/CPS 2.10 節に定める。

［2.8.2］秘密扱いとしない情報

CP/CPS 2.8.2 項では、秘密扱いとしない情報について記述する。

前述の CP/CPS 2.8.1 項以外に、次のような情報が考えられる。

- 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、組織により承認を得ている情報

ここでは、JPNIC 認証局の範囲ではなく、JPNIC においての情報として範囲を広げて記述を行うこととした。

「2.8.2.秘密扱いとしない情報」記述案

本 CP/CPS で公表すると定めた情報、本 CP/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、組織により承認を得ている情報

［2.8.3］証明書失効及び停止情報の開示

CP/CPS 2.8.3 項では、証明書の失効及び停止情報に関する取扱いに関して記述する。

なお、JPNIC 認証局では、業務の煩雑さ等を考慮し、停止は行わないこととした。

「2.8.3.証明書失効及び停止情報の開示」記述案

本認証局を含む JPNIC 認証局は、証明書を失効する場合、その証明書の発行者である認証局情報、失効日時を含む CRL を開示する。失効理由及び失効に関するその他の詳細情報は原則として開示しない。

［2.8.4］法的執行機関への情報開示

CP/CPS 2.8.4 項では、法執行機関からの命令による情報開示への対応を記述する。

本検討では、法的な権限に基づく開示請求については、開示できる旨の記述を基本とした。

「2.8.4.法的執行機関への情報開示」記述案

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。

［2.8.5］民法上の要求にともなう開示

CPS 2.8.5 項では、調停、訴訟、仲裁、裁判上行政手続きにおける開示請求に対する対応を記述する。

「2.8.5.民法上の要求にともなう開示」記述案

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きの過程において、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。

［2.8.6］加入者からの要求に基づく開示

CP/CPS 2.8.6 項では、加入者（一般的には証明書所有者）から、加入者に関する登録情報の開示要求があった場合の対応を記述する。

本認証局の場合、サーバ証明書を除き、JPNIC と利用契約を結んだ、LRA が属する組織から任命された個人に証明書を発行する形態であり、加入者は JPNIC と利用契約を結んだ組織と考えられる。また、その組織は、LRA 管理者に対し、その組織で利用する証明書の管理する権限を与えていると考えられる。ゆえに、開示要求者は証明書にて証明された証明書所有者個人ではなく、LRA 管理者であると考える。

「2.8.6.加入者からの要求に基づく開示」記述案

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。

［2.8.7］その他の理由に基づく開示

CP/CPS 2.8.7 項では、前述で示した以外の理由による開示要件を記述する。

一般的には、CP/CPS 2.8.4 項～2.8.7 項で示す要件以外の開示はしない旨の記述又は規定していない場合が多い。

「2.8.7.その他の理由に基づく開示」記述案

本認証局を含む JPNIC 認証局は、証明書検証者からの証明書所有者情報開示要求には、本 CP/CPS 2.8.4 項、2.8.5 項に規定する場合を除いて、応じない。

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。

5.4.2.9. ［2.9］知的財産権

CP/CPS 2.9 節では、CP/CPS、証明書、名前、ライセンス若しくは関係者からのライセンスの対象となる著作権、特許、商標又は企業秘密等の知的財産権について記述する。

「2.9.知的財産権」記述案

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 に帰属する財産である
- 本 CP/CPS は JPNIC に帰属する財産である
- JPNIC 認証局の私有鍵及び公開鍵は JPNIC に帰属する財産である
- 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 に帰属する財産である

5.4.2.10. ［2.10］個人情報保護方針

RFC2527 において、個人情報保護方針を記述項目としていないが、個人情報保護法の制定、個人情報保護に関する関心の高まりにより、個人情報保護方針について、追

加的に記述する場合が増えている。今回の検討においても個人情報保護方針について記述することが望ましいと考え、JPNIC 認証局における個人情報保護方針として、検討及び記述を行うこととした。

ここでは、

- 個人情報をどのように取扱うのか

を検討することとなる。

日本の場合、個人情報保護法において、個人情報取扱事業者に課せられる個人情報保護義務が定められている。これは、「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告」の 8 原則（いわゆる OECD8 原則）[5]を考慮したものであり、JPNIC 認証局においても、本法の保護義務を遵守することが望ましい。

現在、JPNIC では、IP アドレスに関連する個人情報の取扱いに関するポリシとして、「JPNIC におけるドメイン名情報および IP アドレスの取扱いについてのポリシー」、「ドメイン名情報および IP アドレス情報の取扱い等に関する規則」、「IP アドレス割り当て等に関する規則」第 18 条を規定している。しかし、JPNIC 認証局においては業務の種類と目的が異なるため、既存のポリシとは別に新たなポリシを規定する必要があると思われる。

ただし、JPNIC 全体におけるプライバシポリシは統一して決められている必要がある。

「2.10.個人情報保護方針」記述案

本認証局を含む JPNIC 認証局は個人情報保護の重要性を認識し、個人情報を次のように取扱う。

（1） 管理責任者を置き、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上で、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、本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

[5]OECD8 原則と個人情報取扱事業者の義務規定の対応
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/pdfs/03.pdf

（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責任を持ち、これに努めている。

（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、認証局業務に従事する職員に対して個人情報保護の教育啓蒙活動を実施する。

（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。

5.4.3. ［3］識別と認証

5.4.3.1. ［3.1］新規発行時での利用者の本人確認方法

［3.1.1］サブジェクトに割り当てられた名前の形式

CP/CPS 3.1.1 項では、X.500 識別名、RFC-822 名前（インターネットメールアドレス）及び X.400 名前（X.400 形式のアドレス）といった、サブジェクトに割り当てられた名前の形式について記述する。ITU-T によって証明書の規格として標準化された X.509 では、エンティティを識別するために X.500 に基づいた名前空間（X.500 識別名）を利用する。したがって、証明書形式として X.509 を利用する場合は、X.500 の識別名の規定に従う旨を記述する。ちなみに X.509 は、S/MIME や SSL/TLS 等の多くのセキュリティプロトコルで利用されており、デファクトスタンダードとなっている。

「3.1.1.サブジェクトに割り当てられた名前の形式」記述案

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］名前が意味を持つ必要があるか否か

CP/CPS 3.1.2 項では個人名・組織名に意味を持たせる必要性の検討を行う。また、利用者は匿名又は仮名を用いることができるかどうか、そして、もしできるならいかなる名前が匿名希望の利用者に割り当てられ、使用されうるのかを検討する。

証明書の用途が JPNIC のアドレス資源管理業務におけるホストマスタの認証であるため、証明書に記載される名前はホストマスタ個人名及び所属組織名をあらわすものである必要があると思われる。なお、具体的に X.500 識別名の各属性値をどのような値とするかについては、CP/CPS 7 章にて記述するため、本項では大まかな記述にとどめる。

「3.1.2.名前が意味を持つ必要があるか否か」記述案

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である。

［3.1.3］様々な名前の形式を解釈するルール

CP/CPS 3.1.3 項では、様々な名前の形式を解釈するルールについて記述する。CP/CPS 3.1.1 項及び CP/CPS 3.1.2 項では名前の形式及びその意味について規定しており、ここではそれらに従って解釈する旨を記述する。

「3.1.3.様々な名前の形式を解釈するルール」記述案

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。

［3.1.4］名前が一意である必要があるか否か

CP/CPS 3.1.4 項では、名前が一意である必要性について検討を行い、一意とするか否かを記述する。

一意であるとする場合は、名前が一意である範囲を予め規定しておくことが望ましい。一意とする範囲は、例えば、認証局の発行する全証明書内、認証局の発行する同一ポリシの全証明書内、といったように規定する。今回の場合は、一意とする範囲を「本認証局が発行する同一ポリシの証明書内」と規定することが適当と思われる。

また、同一組織の同姓同名の申請者に対して証明書を発行する場合や、証明書更新時に同一主体者に対して新旧の証明書が存在する場合等を想定して、名前を一意とする方法を検討する必要がある。名前を一意とする方法としては、末端の相対識別名（RDN[6]）に EE の名前（commonName）だけでなく、serialNumber 属性を使用して LRA によって一意に管理されるシーケンシャルな番号を追加することが考えられる。

「3.1.4.名前が一意である必要があるか否か」記述案

証明書に記される名前は、本認証局が発行する同一ポリシの証明書において一意とする。

［3.1.5］所有者の名前を決定する際の紛争解決手続き

CP/CPS 3.1.5 項では、証明書に記載される名前に関して認証局が責任を持つのか、また、証明書所有者間で紛争が発生した場合に認証局が関与するのか及び紛争解決の手続きについて検討を行う。

[6] RDN: Relative Distinguished Name

紛争に関しては、認証局は関与せず当事者間で解決するよう規定するのが一般的である。ただし、発行業務を円滑に進めるうえで次のような規定を設けることが必要と思われる。

- 最終的な名前の決定権は認証局が持つこと
- 認証局は紛争を理由に申請を却下できること

また、証明書上の名前は、サイバー空間上で用いられる登録制の名前という点でドメイン名と同様の性格を持つことから、JPNIC の定めるドメイン名紛争処理方針（JP-DRP）[7]に準ずると規定してもよいと思われる。

「3.1.5.所有者の名前を決定する際の紛争解決手続き」記述案

本認証局が発行する証明書に記される主体者名に関する異議申し立てについては、本認証局の責めに帰すべき事由がない場合、本認証局は全ての決定を行う権利を留保する。また、主体者相互間の紛争発生時には、まず当事者間での解決を図るものとし、これにより解決できない場合、本認証局が最終決定者となる。紛争の当事者はこの裁定に拘束される。

［3.1.6］商標の認識・認証・役割

CP/CPS 3.1.6 項では、商標の取扱いについて記述する。なお、日本法において、名前に含まれる可能性のある知的財産権として、商標のほか、商号、ドメイン名等もあり、これらについても本項での記述対象となると思われる。

JPNIC 認証局の場合、想定している証明書の用途においては、名前の誤認混同等の損害による紛争発生の恐れはないと思われる。したがって、本項については規定する必要はないと考える。

「3.1.6.商標の認識・認証・役割」記述案

規定しない。

［3.1.7］公開鍵に対応する私有鍵の所有を証明する方法

CP/CPS 3.1.7 項では、証明書主体者が登録された公開鍵に対応する私有鍵を所持し

[7] JP ドメイン名紛争処理方針
http://www.nic.ad.jp/ja/drp/index.html

ていることを証明しなければならない場合とその方法を記述する。

申請者は、公開鍵に対応する私有鍵を所持していることを、証明書が生成される前に証明しなければならない。私有鍵の所持を証明する方法については、次の点を考慮のうえで検討を行う。

- 鍵ペア生成を行う主体は申請者と認証局のどちらか又は第三者機関を利用するのか
- 証明書の生成はオンラインかオフラインか

鍵ペアを申請者側で生成する場合には、例えば PKCS[8]#10 形式の電子署名が付された証明書リクエストを申請者が送付する方法がある。また、鍵ペアを認証局側で生成する場合には、例えば暗号化された証明書及び私有鍵を PKCS#12 形式で認証局が送付する方法がある。

なお、今回の検討においては、鍵ペアの生成は申請者側で行うこととした。

オンラインで証明書の発行を行う場合は、SSL/TLS 等のセキュアな通信方式を用いる必要がある。オフラインで証明書の発行を行う場合は、上記ファイルを送付するにあたって、本人限定受取郵便等の安全・確実な送付手段の検討が必要である。

「3.1.7.公開鍵に対応する私有鍵の所有を証明する方法」記述案

本認証局は、証明書申請者が私有鍵を所有していることを、PKCS#10 に従った電子署名のされた証明書リクエストの利用、その他本認証局が認めた方法を通じて、確認する。

［3.1.8］サブジェクトの組織（法人）としての識別のための認証要件

CP/CPS 3.1.8 項では、組織の認証を行うための要件を記述する。

組織の認証の例として、設立登記、法的にサインされた会社の決議、社印、その他正式なものと証明された文書がある。また、日本国内の場合には、代表者の印鑑証明がある。

LRA を設置する場合は、LRA の組織認証を行う必要があると思われる。

[8] PKCS: Public-Key Cryptography Standards, http://www.rsa.com/rsalabs/pkcs/index.html

「3.1.8.サブジェクトの組織（法人）としての識別のための認証要件」記述案

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。

［3.1.9］個人の認証要件

CP/CPS 3.1.9 項では、証明書発行時における、個人の本人確認の要件を記述する。

RFC2527 では、検討ポイントとして次の項目をあげている。

- 要求される識別証の数
- どのように認証局若しくは登録局が提供された識別証を認証するか
- 個人は本人認証を行う認証局若しくは登録局に出頭しなければならないか
- どのように個人が組織の一員として本人確認されるか

個人の本人確認を行う目的は、次の 2 点を確認することであるといえる。

- 申請書に記載された名前と一致する個人が実在するか
- その個人が存在するとして、申請者はその個人本人か

したがって、個人の本人確認要件は、架空の人物をでっちあげた不正な申請や、なりすましによる不正な申請を見分けられるものである必要がある。

個人の本人確認の方法には様々なものがあるが、例えば次のようなものがある。

- 認証局（登録局）への出頭並びに 1 種類の写真付き証明書若しくは複数種類の身分証明書の提示を求める
- 1 種類若しくは複数種類の身分証明書を郵送等にて受付け、証明書記載住所に確認書類を送付する
- 個人信用情報機関のような個人情報を収集する組織のデータベースと比較する
- 証明書の申込みをした本人しか知らない機密情報（PIN 等）を提示させる
- メールアドレスを確認する

身元確認に利用することができる身分証明書としては、次のものが考えられる。

- 住民票
- 戸籍謄本
- パスポート

- 運転免許証
- 健康保険証
- 組織（法人）が発行する ID バッヂ

ここで、ID バッヂは社員証のような本人を確認できるものであるとする。

なお、どの程度の要件を規定するかについては、証明書とビジネスモデルに要求される厳密性のレベルを考慮のうえ、適切な要件を検討する必要がある。例えば FBCA では、証明書の保証レベルごとに次の要件が規定されている。

- 初期： 電子メールアドレス
- 基本： データベースとの照合、監督者又は本人による身分証明
- 中位： 登録局又は代理店への出頭及び身分証の提示
- 高位： 登録局又は代理店への出頭及び政府発行の識別書類を最低 2 種類提示（少なくとも 1 種類は写真つきの身分証であること）

LRA を設置する場合、個人の本人確認を LRA にて実施することにより認証局の業務量を削減することが可能である。この場合、LRA における本人確認要件を認証局側で規定するかどうかを検討する必要がある。

本人確認の要件を認証局側で規定する場合、本人確認に関して一定の厳密性を確保することが可能である。ただし、その要件は各 LRA の運営内容を考慮したものである必要がある。また、要件が守られていることを何らかの形で確認する必要があると思われる。一方、本人確認の要件を LRA に任せる場合、各 LRA の実情に合わせた運用が可能となるが、本人確認の厳密性は各 LRA に依存することになるので、本人確認に関して LRA が責任を持つことを規定する必要があると思われる。

ここで、本認証局が本人確認を行うべき申請者数の検討を行う。IP アドレス管理指定事業者ごとに LRA 管理者を 1 名ないし 2 名設置した場合、IP アドレス管理指定事業者の数が 300 程度であることから、LRA 管理者の数は 300 人～600 人である。一方、ホストマスタの人数は 1000 人程度であり、仮にホストマスタについても本認証局が本人確認するとした場合、対象となる人数が 1300 人～1600 人となるため、本人確認に関わる業務量は 3～4 倍になる。業務量の観点から言えば、ホストマスタの本人確認は LRA 業務に関する契約を結ぶ IP アドレス管理指定事業者にて実施することが望ましい。

発行される証明書は、本認証局と IP アドレス管理指定事業者間での申請業務に使われる、クローズドな利用を前提としたものである。証明書の発行対象であるホストマスタは、LRA 組織である IP アドレス管理指定事業者が任命する者であり、その本人確認は IP アドレス管理指定事業者において確実に行うことができると考えられる。したがって、ホストマスタの本人確認を LRA 業務に関する契約を結ぶ IP アドレス管理

指定事業者にて実施するとしても、本人確認における厳密性が損なわれることはないと考えられる。

ホストマスタの本人確認要件については、完全に LRA に任せるのではなく、JPNIC 側で最低限の規定を設けることは必要と思われる。

なお、LRA が行った本人確認及び発行申請等の証明書の管理に関する LRA の責任は、LRA との間で結ばれる契約書に記述されるものと考える。

「3.1.9.個人の認証要件」記述案

LRA 管理者は、証明書発行対象者の証明書発行登録に際し、人事情報 DB、雇用契約等本人を特定できる情報の確認を行う必要がある。また、証明書発行対象者が、LRA 責任者より許可された証明書の発行の許可を受けているものであるかの確認を行う必要がある。

5.4.3.2. ［3.2］通常の更新

CP/CPS 3.2 節では、通常の鍵更新時における本人性確認及び認証に対する要件について述べる。ここで検討すべきポイントは次の 2 点である。

- 本人性確認及び認証の必要性
- 新規発行時の認証要件との違い

証明書の更新を要求できる者は、証明書の新規発行を要求できる者と同様、原則として証明書の所有者本人に限定するべきであると思われる。したがって、第三者による不正な更新要求を排除するために、本人性確認及び認証を行う必要がある。

本人性確認及び認証の要件としては、CP/CPS 3.1.9 項にて規定した要件のほかに、次のようなものがあげられる。

- 証明書中の公開鍵に対応する私有鍵による署名
- 証明書発行時に通知された PIN の提示
- 予め登録しておいた符丁（キーワード等）の使用

私有鍵に危殆化のおそれがないならば、私有鍵による署名ができるのは証明書所有者本人だけであるため、私有鍵による署名付きのメール等により本人性確認を行うことができる。また、証明書発行時に認証局より通知された PIN は、証明書所有者本人だけしか知り得ない情報であるため、PIN の提示により本人性確認をできるものと思われる。また、証明書の申請時等に符丁（キーワード等）を認証局に登録しておき、

証明書所有者が更新要求を行うときにこの符丁を使用して本人性確認を行う方法も考えられる。

上述した 3 つの要件は、いずれも証明書所有者本人だけが、私有鍵、PIN、符丁といった秘密情報を保持していることを前提としている。3 つの要件の中から複数を組み合わせた場合も同様である。万一、これら秘密情報が第三者に知られてしまった場合は、不正に証明書更新が行われるおそれがあるため、これら秘密情報の管理は厳密に行われなければならない。

本認証局においては、証明書は 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 が指定した者に発行されるものである。したがって、証明書の発行要求は、IP アドレス申請業務の業務担当者としての任命に基づくものであり、発行対象者である証明書所有者自身の判断によるものではない。ゆえに、あくまでも、LRA である IP アドレス管理指定事業者から IP アドレス申請業務の業務担当者としての任命又は任命継続が必要であり、新規発行時と同様な手続きが必要と考えられる。

「3.2.通常の更新」記述案

新規発行手続きと同様とする。

5.4.3.3. ［3.3］失効後の更新－鍵が危殆化していない場合

CP/CPS 3.3 節では、証明書失効後の鍵更新における本人性確認と認証に対する要件について述べる。ここで検討すべきポイントは次の 2 点である。

- 本人性確認及び認証の必要性
- 新規発行時の認証要件との違い

証明書の更新を要求できる者は、証明書の新規発行を要求できる者と同様、原則として証明書の所有者本人に限定するべきであると思われる。したがって、第三者による不正な更新要求を排除するために、本人性確認及び認証を行う必要がある。

証明書が失効した以上、公開鍵が証明書所有者のものであることを保証しうるものは存在しないことになるため、たとえ危殆化していなかったとしてもその公開鍵に対応する私有鍵が証明書所有者のものであることは保証できない。したがって、本人性確認及び認証の要件としては、CP/CPS 3.1.9 項にて記述される新規発行時の本人確認及び認証の要件と同様とすることが良いと思われる。

本認証局においては、本報告書 5.4.3.1.で検討したように、ホストマスタの認証は LRA にて実施することが望ましく、本認証局ではホストマスタの本人確認等は行わない。この場合、本認証局がホストマスタを認証する手段は証明書以外に存在しないた

め、証明書が失効したならば、新規発行時と同様な手続きが必要と考えられる。

「3.3.失効後の更新－鍵が危殆化していない場合」記述案

新規発行手続きと同様とする。

5.4.3.4. ［3.4］証明書の失効申請

CP/CPS 3.4 節では、失効申請時の申請者本人の認証方法について述べる。

本認証局では、ホストマスタの本人認証を LRA にて実施する。したがって、詳細な手続きは LRA ごとに相違していることが予想される。しかし、本認証局としてのホストマスタの認証方法についての基本方針を記述する必要があると思われる。なお、LRA 管理者から本認証局への EE 証明書若しくは LRA 管理者証明書の失効登録の際には、LRA 管理者証明書による本人確認が行われる必要がある。

「3.4.証明書の失効申請」記述案

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。なお、LRA 管理者の本人確認は本認証局により、LRA 管理者証明書をもって確認される。

5.4.4. ［4］運用上の要件

CP/CPS の 4 章では、様々な運用要件に関して、認証局、証明書所有者に課せられる要件について記述する。

本認証局では、EE 証明書としてホストマスタ証明書とサーバ証明書の 2 種類を発行する。ホストマスタ証明書に関しては、その申請、発行、受理及び失効の各手続きについて CP/CPS 上に明確な規定を行う必要がある。

サーバ証明書に関しては、発行対象となるサーバが JPNIC 内部のものであり、関係者は JPNIC 内部に限定される。したがって、発行に係わる手続きの詳細は JPNIC 内部で検討するものとし、CP/CPS 上では簡潔な記述にとどめるものとする。

なお、LRA 管理者証明書に関しては、運用証明書の一つとして位置づけられるものであるから、本報告書 5.4.1.3.で述べたように JPNIC の運用規定に則って管理・運用されるものとし、CP/CPS 上には運用上の要件を記述しないものとする。

5.4.4.1. ［4.1］証明書の申請

CP/CPS の 4.1 節では、証明書申請を提出することができる者、例えば、証明書のサブジェクト又は認証局等について記述する。

本報告書 5.4.1.3.で述べたように、本認証業務における主たる証明書所有者は IP アドレス管理指定事業者に所属するホストマスタとなるが、本認証局が個々のホストマスタに対して証明書の発行業務をすることは、人的業務量が膨大となり非現実的である。そこで、本認証局においては、ホストマスタ証明書の発行に関する審査、登録及び証明書管理等の業務を各 LRA にて実施することが妥当と思われる。

ホストマスタ証明書の申請を行う者は、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 が指定した者である。彼らは、IP アドレス申請業務の業務担当者への任命に基づいて、LRA 管理者に対して証明書の発行申請を行う。このように、証明書の申請に関わる手続きは、各 LRA において組織的な管理のもと実施されるものである。したがって、証明書の申請に関わる要件は、本認証局が一律に規定するという性格のものではなく、各 LRA においてその業務の実態に即した形で定められるべきものであると考える。

ただし、次にあげる要件は証明書申請における最低限の要件として規定する必要があると思われる。

- 証明書申請者が CP/CPS の内容を承諾していること
- 申請者がアドレス申請業務担当者に任命されていることに関して LRA 管理者が確認を行うこと

LRA 管理者証明書に関しては、LRA 組織の責任者より LRA 管理者として任命された者が、本認証局に対して発行申請を行うものと考えられる。本認証局において、申請を受付けるにあたって確認すべき要件としては、次の項目が考えられる。

- 申請者が組織若しくは団体の責任者より LRA 管理者として任命されていること
- 本人からの申請であること
- 申請内容に虚偽がないこと

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して発行申請を行い、申請を受けたレジストリシステム責任者が本認証局に対してあらためて発行申請を行う、という手順が考えられる。

「4.1.証明書の申請」記述案

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、証明書の発行申請を行う。申請者は、証明書の発行申請を行うにあたり、本 CP/CPS の内容を承諾しているものとする。申請者の本人確認及び証明書にて証明される者の各種申請業務担当者としての資格確認審査は LRA 管理者により実施される。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者を通じて本認証局に対し発行申請を行うものとする。

5.4.4.2. ［4.2］証明書の発行

CP/CPS の 4.2 節では、証明書の発行と、申請者への発行通知に関する要件を記述する。

前項で述べたとおり、本認証局が、LRA 組織に所属するホストマスタ等に対して証明書を発行する場合には、LRA 管理者からの申請登録に基づき証明書を発行するものとする。証明書所有者の本人確認等は LRA 管理者の責任において実施されるものとし、本認証局では本人確認等は行わないこととする。

ここで、証明書の発行対象としては、役割に対するものと個人に対するものの 2 通りが考えられる。

証明書を役割に対して発行する場合には、担当者が変わっても引き続き証明書を利用することが可能であり、LRA にとってはコストを低く抑えることができる。ただし、鍵ペア生成者と証明書使用者が異なるため、LRA 管理者と担当者との間での権限分離

があいまいになるおそれがある。また、LRA 管理者が全ての証明書を管理することが予想されるため、LRA 管理者が EE 証明書を使用できないことを確実にする仕組みが必要である。また、証明書の不正使用があった場合に、使用した個人を特定するため、証明書使用記録を詳細に記録しておく必要があると思われる。

証明書を個人に対して発行する場合には、担当者が変更になる都度、証明書を申請しなおす必要があり、LRA にとっては発行コストの増加を招くこととなる。しかし、鍵ペア生成者と証明書使用者が同一であるため、LRA 管理者と担当者との間での権限分離を確実に行うことができる。ただしこの場合、LRA 管理者は担当者に対し、私有鍵の管理義務を徹底させる必要がある。証明書の不正使用に対しては、個人と証明書とが 1 対 1 で対応するため個人の特定が容易である。

本認証局においては、証明書所有者の個人特定が容易である点、また、LRA 管理者と証明書使用者との間の権限分離が確実に実施できる点から、証明書は個人に対して発行すべきであると思われる。

また、鍵ペアの生成主体としては、本認証局、LRA 管理者、申請者の三者が考えられるが、本認証局に課せられる業務量、また私有鍵の秘匿性の観点から、申請者自身が鍵ペアを生成することが良いと思われる。

これらの検討に基づき、一連の証明書発行手順（証明書の申請、発行及び受領）の一例を図 5-4 に示す。

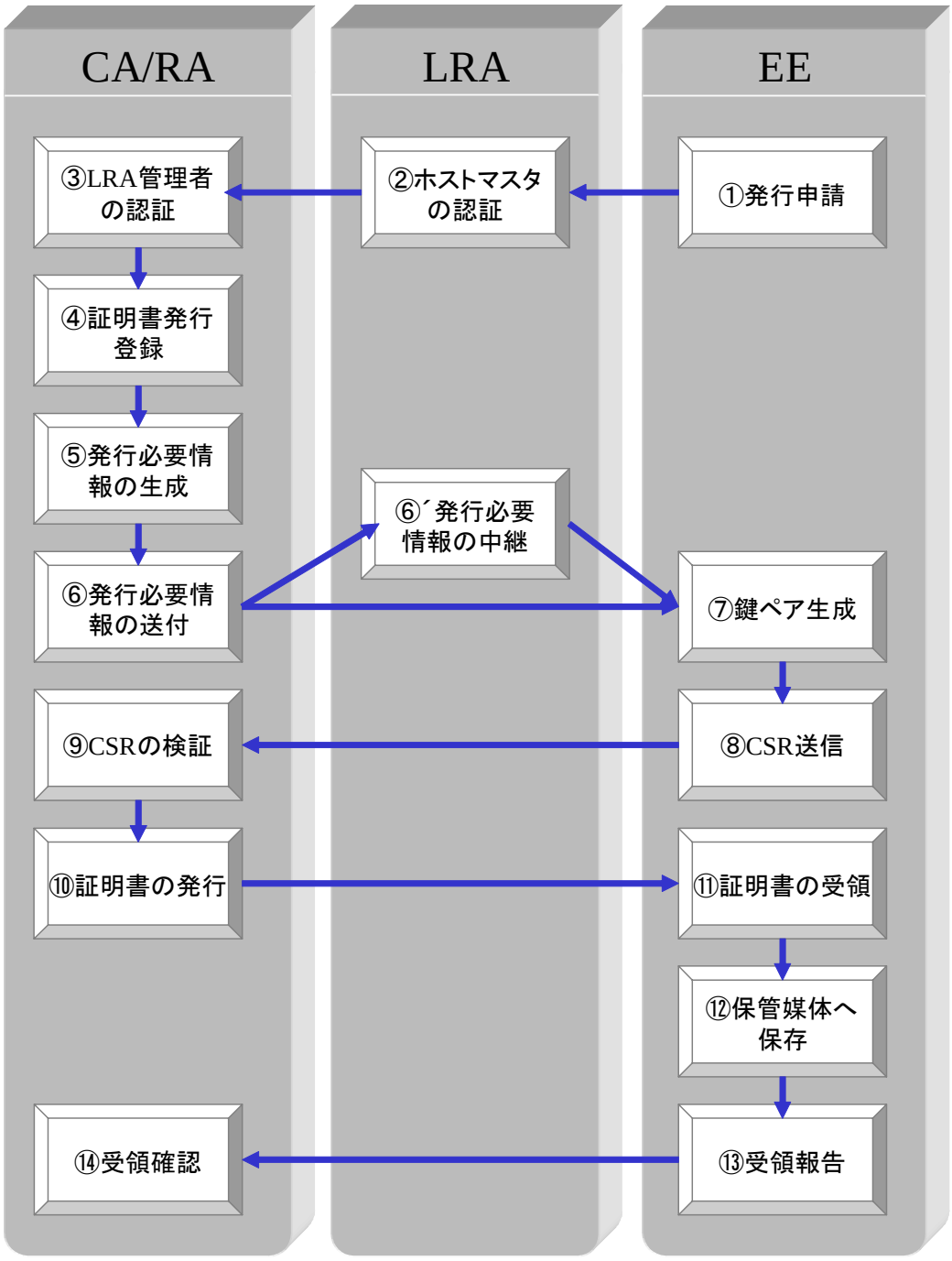


図 5-4　ホストマスタ証明書の発行手順

手順①：ホストマスタは、LRA 管理者に対してホストマスタ証明書の発行申請を行う。

手順②：LRA 管理者は、CP/CPS 3 章で定める個人の認証要件に基づき、ホストマ

スタの本人確認を行い、本認証局に対して証明書の発行申請登録を行う。

手順③：本認証局は、発行申請登録を行った者が真正な LRA 管理者であることの確認を行う。

手順④：本認証局は申請された証明書の発行登録を行う。

手順⑤：本認証局は、証明書の発行要求を受付ける際にホストマスタを識別するための情報を生成する。

手順⑥、⑥´：本認証局は、生成した発行対象者識別情報をホストマスタに送付する。このとき、必要な情報を 2 種類用意し、1 つは直接ホストマスタに、もう 1 つは LRA 管理者経由とすれば、安全かつ確実に情報を渡すことができる。

手順⑦：発行対象者識別情報を受け取ったホストマスタは鍵ペアを生成する。

手順⑧:ホストマスタは、発行必要情報と CSR を本認証局に対して送信する。なお、証明書に記載される情報は、この前の段階で決められている。

手順⑨：本認証局は CSR の検証を行う。

手順⑩：本認証局が証明書を発行する。

手順⑪：ホストマスタが発行された証明書を受領する。

手順⑫：ホストマスタは証明書及び生成した鍵を保管媒体に保存する。

手順⑬：ホストマスタは証明書の内容を確認した後、本認証局に対して受領報告を行う。

手順⑭：本認証局は、申請者からの受領報告をもって証明書の受領を確認する。

上述した一連の手続きは、本認証局側の手続きをシステムによって自動化することにより、証明書の申請から発行、受領までを一貫してオンラインで実施することが可能である。またこの場合、証明書のダウンロードをもって申請者は証明書の受領を完了したとみなすことができ、図 5-4 における手順⑬の受領報告及び手順⑭の受領確認は不要である。

したがって、本認証局側の手続きはシステムによる自動化が望ましいが、詳細はシステム、運用要件の決定によって定められるものである。このため、CP/CPS の記述上は、手作業、システムによる自動処理のどちらになったとしても、問題ない程度の記述内容とする。

LRA 管理者証明書に関しては、本報告書 5.4.4.1.で述べたような要件を確認した後、発行手続きを行う。証明書の発行方式としては、オンラインとオフラインが考えられる。オンラインで発行する場合は、ホストマスタ証明書と同様な発行手続きが考えら

れる。オフラインで発行する場合は、認証局にて鍵ペアを生成し、暗号化された証明書及び私有鍵を PKCS#12 形式でフロッピーに格納するか、若しくは IC カード等の媒体に格納するかして、申請者に送付する方法が考えられる。

サーバ証明書に関しては、レジストリシステム責任者からの発行申請を受けて、本認証局がサーバ管理者に対し証明書を発行するものとする。

「4.2.証明書の発行」記述案

LRA 管理者は、本 CP/CPS 3.1.9 項に基づいて申請者の本人確認及び審査を行い、本認証局に対し申請登録を行う。本認証局は、申請登録を行った LRA 管理者の本人確認を行った後、鍵ペア生成及び証明書発行に必要な 2 種類の情報を生成し、2 系統の経路で申請者へ通知する。証明書はセキュアな通信プロトコルを使用し発行される。

サーバ証明書に関しては、レジストリシステム責任者からの発行申請を受けて、本認証局がサーバ管理者に対し証明書を発行するものとする。

5.4.4.3. ［4.3］証明書の受理

CP/CPS の 4.3 節では、発行された証明書の受領に関する要件を記述することとなる。

証明書の信頼性を確保するために、証明書の受理の際には受領確認を行うことが望ましい。ECOM ガイドライン[9]でも、証明書の送付に関して、受取りの確認ができる手段を利用することを推奨している。また、受領確認がない場合には、証明書を失効させる等の手続きを検討する必要がある。

証明書をサーバからダウンロードする形式であれば、ダウンロードした時点で受領したものとみなすこととができると考えられる。証明書をフロッピーディスク等の記録媒体に格納して送付する場合は、受領確認のメールや証明書の使用をもって受領したとみなすことが可能である。なお、送付の手段としては、開封が検知できる手段を講じたうえで、本人限定受取確認郵便等の確実に申請者本人が受け取ることのできるサービスを利用することが望ましい。

なお、今回の検討では、サーバ証明書を除く EE 証明書の発行はオンラインによる方法を想定している。

一方、申請者は、証明書の受理の際に内容の検証を行うべきである。内容に不備がある場合は直ちに本認証局に通知することが望ましい。

---

9 「認証局運用ガイドライン V1.0 版」、電子商取引実証推進協議会（ECOM）、平成 10 年 3 月

LRA 管理者証明書の場合も同様である。

サーバ証明書の受領確認方法については、上述の検討を踏まえ、証明書の発行方法（オンラインかオフラインか）に応じて適切な方法を別途検討する。

「4.3.証明書の受理」記述案

本認証局は申請者に対し証明書発行に必要な情報を送付する。申請者は送付された証明書発行に必要な情報を用いて、本認証局とセキュアなオンライン通信を行う。本認証局はセキュアなオンライン通信を介して証明書を発行する。申請者がその証明書を受け取った時点で、その証明書を受領したものとする。

なお、申請者は証明書ファイルが自身の PKI 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。

サーバ証明書に関しては、サーバ管理者から本認証局への報告をもって、受領の確認を行うものとする。

5.4.4.4. ［4.4］証明書の停止と失効

CP/CPS の 4.4 節では､証明書の停止及び失効に関する運用要件について記述する。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- 証明書が失効される理由
- 証明書の失効要求の主体者
- 証明書失効要求の手続き
- 失効要求の有効期間
- 証明書の停止理由
- 証明書の停止要求の主体者
- 証明書の停止要求の手続き
- 停止が継続する期間
- CRL の発行頻度
- 検証者における CRL をチェックする要件
- オンラインの失効／ステータスチェックの利用可能性
- 検証者におけるオンラインの失効／ステータスチェックを行う要件
- 利用可能なほかの形態の失効情報
- 検証者におけるほかの形態の失効情報をチェック要件
- 鍵の危殆化に関する特別な要件

上述した各々の要素について、記述すべき内容の検討を行う。

なお、サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して失効申請を行い、申請を受けたレジストリシステム責任者が認証局に対してあらためて失効申請を行うものとする。

［4.4.1］証明書が失効される理由

CP/CPS の 4.4.1 項では、証明書が失効される状況として、証明書を失効させることができる場合及び証明書を失効させなければならない場合について記述することとなる。証明書が失効される状況として、例えば、加入者の雇用期間の終了、暗号トークンの紛失又は私有鍵危殆化のおそれ等の場合がある。

証明書の信頼性を保つために、私有鍵が危殆化した場合、証明書記載事項に変更が生じた場合、虚偽の申請が発覚した場合等は証明書を失効させるべきである。一般的には、次のような失効事由が定められる。

- 証明書所有者の私有鍵が危殆化した（またはそのおそれがある）場合
- 証明書所有者本人の請求があった場合
- 証明書所有者が使用を停止する場合
- 証明書所有者が CP/CPS、その他契約、規則、法律に従わない場合
- 証明書の記載事項が事実と異なる又は変更がある場合
- 認証局の私有鍵が危殆化した（またはそのおそれがある）場合
- 認証局がサービスを停止する場合
- 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
- LRA が JPNIC 認証局との契約における義務を果たさなかった場合

また、証明書をサーバからダウンロードさせる場合は、申請者による証明書ダウンロードの失敗も失効事由として検討する必要がある。

LRA 管理者証明書に関しても、同様な要件が該当すると思われる。

サーバ証明書に関しては、次のような失効事由が考えられる。

- 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（またはそのおそれがある）場合
- サーバ管理者の請求があった場合
- サーバ管理者が CP/CPS、その他契約、規則、法律に従わない場合
- 証明書の記載事項が事実と異なる又は変更がある場合
- 認証局の私有鍵が危殆化した（またはそのおそれがある）場合
- 認証局がサービスを停止する場合

「4.4.1.証明書が失効される理由」記述案

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。

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ほかに、次の項目に該当すると認めた場合、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

サーバ証明書に関しては、サーバ管理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（またはそのおそれがある）場合

また、本認証局は、サーバ管理者からの失効申請のほかに、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
- サーバ管理者が本 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
- その他本認証局が失効の必要があると判断した場合

［4.4.2］証明書の失効要求の主体者

CP/CPS の 4.4.2 項では、誰が証明書の失効を要求することができるかについて記

述する。失効要求の主体者は、一般に、証明書所有者本人と証明書を発行する認証局である。証明書が役割に対して発行される場合等においては、発行対象の組織の人事部等の場合がある。また、申請者及び証明書所有者が個人で証明書の発行を受けている場合においては、証明書所有者が死亡した場合等において、第三者による申請を受付ける必要がある。ただしこの場合は、失効申請を行う法律上の正式な代理人に対して、事由を明示する書類（死亡届等）の提出を義務付ける等の検討が必要であると思われる。

本認証局の場合、JPNIC に対して各種申請業務を行う役割を LRA 組織が個人に対して任命するものであり、失効申請をできるものは証明書にて証明された個人とは限らないと思われる。LRA 組織が任命しているので LRA 組織の責任者からの指示により、LRA 管理者が失効登録するということも考えられる。今回の検討では、LRA 組織の業務を画一的に決定できないため、CP/CPS 上ではホストマスタ証明書の失効要求は、証明書所有者が LRA 管理者に失効要求を行い、要求を受けた LRA 管理者が、本認証局に対し当該証明書の失効申請登録を行う若しくは LRA 責任者の指示に基づき LRA 管理者が、本認証局に対し当該証明書の失効申請登録を行うものとする。

この他に、前項で述べたとおり、CP/CPS 4.4.1 項に基づいて、本認証局は失効要求を行うことができる。

LRA 管理者証明書に関しては、LRA 管理者本人、組織の責任者、本認証局が失効要求可能な者として想定される。

サーバ証明書に関しては、サーバ管理者と本認証局が失効要求可能なものとして想定される。

「4.4.2.証明書の失効要求の主体者」記述案

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

サーバ証明書に関しては、サーバ管理者と本認証局が失効要求を行うことができるものとする。

［4.4.3］証明書失効要求の手続き

CP/CPS の 4.4.3 項では、証明書失効要求に使用される手続きについて記述する。

検討すべきポイントは、次の点である。

- 失効の申請先
- 失効の申請手段

ホストマスタがホストマスタ証明書の失効申請を行う申請先として、LRA 管理者と本認証局とが考えられる。申請先を LRA 管理者とする場合、LRA 管理者から本認証局に対してあらためて失効申請を行う必要があり、本認証局にて失効処理を開始するまでに遅れが生じる。しかし、失効申請者の本人確認を LRA にて実施するため、本認証局における業務負担は少なく、失効処理そのものは迅速に行うことができる。LRA 管理者の本人確認をシステム化することにより、本認証局における失効処理を自動化することも可能である。一方、申請先を本認証局とする場合、LRA 管理者が不在等のケースでも失効処理を開始することが可能であるが、本認証局において申請者の本人確認を行う必要があり、認証局側の業務負担は大きいものとなる。

証明書の新規発行及び更新時のホストマスタの本人確認を LRA にて実施するならば、失効時におけるホストマスタの本人確認も LRA にて実施することが妥当であり、ホストマスタの失効申請先は LRA 管理者とするべきである。また、本認証局における業務量の観点からも、LRA 管理者を失効申請先とすることが望ましい。

失効申請の手段は、その要求が正当な人物によってなされたものであることを確認できる必要がある。失効の要求を行う手段としては、一般に、署名付きメール、書面、FAX、電話といった手段が考えられる。

次に、これらの手段について検討を行う。

【署名付きメール】

署名検証の結果問題がなければ、本人確認を行う必要なく、失効処理を行ってよいと考えられる。なぜなら、署名ができるのは私有鍵の所有者だけであるから、要求を行っているのは所有者本人であると推定されるからである。仮に第三者が所有者の私有鍵を使って失効要求をしてきたのであれば、第三者が使用している時点で既に鍵は危殆化しているといえるので、本人確認を行うまでもなく当然失効させなければならない。

【書面】

本人確認を行う必要がある。証明書の発行申請時に提出した個人認証情報、若しくはそれと同等な情報の提出を求めなければならない。

【FAX】

失効申請を行う際に、証明書の発行申請時に提出した個人認証情報を同時に送信する等、本人確認を実施できるよう要件を課す必要がある。

【電話】

本人確認が困難であるため、失効要求の手段としては原則不可とするべきと思われる。電話による失効要求を認める場合は、パスワードやキーワードを事前に設定する、コールバックを行う等、何らかの形で本人確認ができる運用を検討する必要がある。

本認証局においては、ホストマスタの失効申請先は LRA 管理者であることが望ましく、したがって、失効申請の手段は、各 LRA において適切な手段を検討するよう規定することが妥当であると思われる。また、本認証局が必要と認める場合には本認証局の判断により失効処理ができる旨を規定することが必要であると思われる。

LRA 管理者証明書に関しては、失効申請先は本認証局となる。申請手段については上述の検討内容と同様なことがいえる。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者に対して失効申請を行い、申請を受けたレジストリシステム責任者が本認証局に対してあらためて失効申請を行う、という手順が考えられる。

「4.4.3.証明書失効要求の手続き」記述案

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きによって、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。

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。

サーバ証明書に関しては、サーバ管理者がレジストリシステム責任者を通じて本認証局に対し失効申請を行うものとする。

なお、サーバ証明書に関しても、「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。

［4.4.4］失効要求の有効期間

CP/CPS の 4.4.4 項では、サブジェクトにとって利用可能な失効要求の有効期間について記述する。

一般に、CP/CPS 4.4.1 項で定めた証明書の失効事由に該当することがわかった場合、証明書の信頼性を保つために、CP/CPS 4.4.3 項で定める手続きにより、可及的速やかに失効要求を送信するべきであると考えられる。

LRA 管理者証明書、サーバ証明書に関しても同様である。

また、失効要求を受付けた認証局においても要求を受付けてから処理を完了するまでの時間は、できる限り短いことが望まれる。しかし、処理可能な時間についてはシステム及び運用体制等に依存するものであり、現状では具体的な処理時間が確定しないため、「速やかに失効処理を行う」旨の記述が妥当であると考えられる。運用体制等の確定後、別途、処理可能な時間について定めることとする。

「4.4.4.失効要求の有効期間」記述案

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。また、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、速やかに（[決定後に記述される] 時間以内に）行われる。失効処理の結果は CRL に反映される。

サーバ証明書に関しても、同様である。

［4.4.5］証明書の停止理由

CP/CPS の 4.4.5 項では、証明書が停止される状況について記述する。

認証局において証明書の停止をサポートするメリットとしては、EE の私有鍵に危殆化のおそれがある場合、逡巡することなく証明書を停止することができるため、鍵の危殆化への速やかな対応が可能となる。一方、デメリットとしては、失効手続きとは別に、停止業務及び停止解除業務が発生し、これにともなうシステムの拡張が必要であり、業務量及びコストの増大となる。

本認証局では、JPNIC における業務量増大及びシステム対応を考慮し、証明書の停止はサポートしないこととする。

「4.4.5.証明書の停止理由」記述案

本認証局は、発行した証明書の一時停止を行わない。

［4.4.6］証明書の停止要求の主体者

CP/CPS の 4.4.6 項では、誰が証明書の停止を要求することができるかについて記述する。証明書の一時停止を申請することができる者には、例えば、所有者、LRA 管理者又は本認証局等が考えられる。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.6.証明書の停止要求の主体者」記述案

規定しない。

［4.4.7］証明書の停止要求の手続き

CP/CPS の 4.4.7 項では、証明書停止を要求するための手続きについて記述する。停止要求手続きには、例えば、所有者若しくは認証局からの署名付メッセージ、又は認証局からの電話等がある。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.7.証明書の停止要求の手続き」記述案

規定しない。

［4.4.8］停止が継続する期間

CP/CPS の 4.4.8 項では、証明書の停止が継続する期間について記述する。

CP/CPS 4.4.5 項で定めたとおり、本認証局では証明書の一時停止を行わないため、本項は規定しないものとする。

「4.4.8.停止が継続する期間」記述案

規定しない。

［4.4.9］CRL の発行頻度

CP/CPS の 4.4.9 項では、CRL の発行頻度について記述する。

各種の基準によると、ECOM ガイドライン、電子署名法、WebTrust いずれも、CRL を定期的に発行することを要求しており、週次、日次というように定期的に発行することが望ましい。また、発行間隔はより短い方が、検証者にとって安全性が高いと思

われる。更に、定期的な CRL 発行のほか、証明書の失効が発生した場合には、即時に CRL を更新することが望まれる。

CRL の発行間隔の規定例としては、証明書の種類によらず、全証明書一律 24 時間以内と規定する場合、FBCA-CP における規定のように、証明書の保証レベル別に規定する場合（規定なし、週に 1 度、1 日に 1 度、12 時間に 1 度）等がある。

本認証局においては、発行する証明書の保証レベルは単一であるため、CRL 発行の時間間隔としては適当な時間間隔を 1 種類規定すればよいと思われる。

「4.4.9.CRL の発行頻度」記述案

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、失効手続きが完了した時点で更新される。

［4.4.10］検証者における CRL をチェックする要件

CP/CPS の 4.4.10 項では、検証者における CRL をチェックする要件について記述する。

証明書の検証を正確に実施するために､検証者に常に最新の CRL を参照するよう要求する必要があると思われる。また、CRL に関する検討事項として、CRL の公開場所をどこに記載するか、また有効期限の切れた証明書を含めるか、といったことがある。後者については、有効期間内に署名された証明書が、検証者のもとに届いたときには期限が切れていた、といった事態が起こりうるため、有効期限の切れた証明書の失効情報についても、CRL に残しておくこと望ましいと思われる。ただし、これはシステムの容量、機能等により別途、決定されるものと考える。したがって本項では、有効期限の切れた失効情報の CRL 上の扱いについては記述せず、下記のとおり、一般的な記述にとどめることとする。

「4.4.10.検証者における CRL をチェックする要件」記述案

本認証局は、CRL を定期的に更新し、証明書に記載されたリポジトリに公開する。検証者は、証明書の有効性を確認するにあたって、最新の CRL を参照し、当該証明書の失効処理が行われているか否かを確認しなければならない。

［4.4.11］オンラインの失効／ステータスチェックの利用可能性

CP/CPS の 4.4.11 項では、オンラインの失効／ステータスチェックの利用可能性に

ついて記述する。この手段として、例えば、ステータスについての問い合わせを受けられる OCSP（オンライン証明書状態確認プロトコル）等がある。

本認証局では、現段階において OCSP 等の利用を想定していない。このため、次のような記述案とする。

「4.4.11.オンラインの失効／ステータスチェックの利用可能性」記述案

OCSP 等のオンラインの失効／ステータスチェックの機能はサポートしない。

［4.4.12］検証者におけるオンラインの失効／ステータスチェックを行う要件

CP/CPS の 4.4.12 項では、オンラインでの失効／ステータス確認を行うために検証者に課せられる要件について記述することとなる。

しかし、CP/CPS 4.4.11 項で定めたとおり、本認証局においては OCSP 等の機能はサポートしないため、本項は規定しないものとする。

「4.4.12.検証者におけるオンラインの失効／ステータスチェックを行う要件」記述案

規定しない。

［4.4.13］利用可能な他の形態の失効情報

CP/CPS の 4.4.13 項では、利用可能な失効通知の他の形式があれば、その失効通知形式について記述することとなる。

一般的に、CRL、OCSP 以外の形式による失効情報の通知手段としては、証明書検証サーバがある。本サーバの導入には、コスト面及び技術的負担面での検討が必要であり、現段階では導入の予定がされていない。したがって、本項では特に規定しないものとする。

「4.4.13.利用可能な他の形態の失効情報」記述案

規定しない。

［4.4.14］検証者における他の形態の失効情報をチェック要件

CP/CPS の 4.4.14 項では、検証者における他の形態の失効情報をチェックする要件について記述することとなる。

しかし、CP/CPS 4.4.13 項で定めたとおり、現段階では本認証局においては証明書検証サーバ等の利用は想定していないため、規定しないものとする。

「4.4.14.検証者における他の形態の失効情報をチェック要件」記述案

規定しない。

［4.4.15］鍵の危殆化に関する特別な要件

CP/CPS の 4.4.15 項では、証明書の一時停止又は失効が、私有鍵の危殆化によって生じた場合の CP/CPS 4.4 節の規定に関する変更について、一時停止又は失効が他の理由で生じた場合と対比して記述することとなる。

認証局私有鍵の危殆化に関する検討項目として、次の項目があげられる。

- 危殆化時に認証局は何を行うか
- 危殆化のおそれに対して何を行うか
- 危殆化時の通知を、誰が、誰に、いつ、どのように行うのか

本認証局の私有鍵が危殆化した場合は、本認証局が発行した全証明書の信頼性が確保できなくなるため、直ちに全証明書を失効させ、CRL を発行すべきと思われる。

本認証局の私有鍵の危殆化のおそれに対しては、JPNIC 認証局内に専門チームを設置し、対策を検討するよう規定することが望まれる。

JPNIC 認証局以外の関係者が本認証局の私有鍵の危殆化に気づいた場合は、直ちに、JPNIC 認証局に通知するよう義務付けることが望まれる。

なお、相互認証を行う場合には、相手認証局が JPNIC 認証局に対して発行する証明書を無効にしてもらうよう相手認証局に要請する旨の記述が必要となると思われるが、今回は相互認証を行わないため、記述は不要とする。

「4.4.15.鍵の危殆化に関する特別な要件」記述案

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。

5.4.4.5. ［4.5］セキュリティ監査の手続き

CP/CPS の 4.5 節では、認証局のセキュアな環境を維持するために実装されるイベント記録と監査システム及びセキュリティ監査に関して記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- 記録されるイベントの種類
- 監査ログが処理、若しくは監査される頻度
- 監査ログの保存期間
- 監査ログの保護
- 監査ログのバックアップ手続き
- 監査ログの収集システム
- 監査イベントを引き起こした者への監査活動の通知
- セキュリティ対策の見直し（脆弱性評価）

次に、前述の各々の要素について、記述すべき内容を検討する。

［4.5.1］記録されるイベントの種類

CP/CPS の 4.5.1 項では、セキュリティ監査のために記録されるイベントの種類を記述することとなる。

本項は、認証局の完全性を証明するために必要な項目であり、本来であれば取得可能な全てのログを記録することを規定することが望ましいが、認証局のレベルに応じて、妥当なイベントを選択することが必要である。

既存の CP/CPS では、記録するイベントの種類の記述に大きな格差がある。最多のものは FBCA-CP[10]である。FBCA-CP では、4 種の保証レベルごとに、記録すべき具体的なイベントを規定しており、初期レベルの保証レベルでは 14 種類のイベントを記録するとしているが、高位の保証レベルでは、52 種類ものイベントを記録することとしている。ただし、実際に記録できるイベントの種類は認証局システムに依存する場合が多いため、CP/CPS 上は具体的なイベントを記述するのではなく、多少幅をもたせ、「認証局私有鍵の操作、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/ARL の発行等の操作ログを記録する」程度に記述するのが妥当と考えられる。本考察では一般的な記述にとどめ、認証局システムが明確になった時点で特記すべきイベントがあれば、記録すべきイベントを取

[10]連邦ブリッジ認証機関（Federal PKI BCA）X.509 CP V1.3R

捨選択のうえ、CP/CPS の中で明示することが望まれる。

「4.5.1.記録されるイベントの種類」記述案

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

［4.5.2］監査ログが処理、若しくは監査される頻度

CP/CPS の 4.5.2 項では、4.5.1 項で記録することを定めたイベント、つまり監査ログをどの程度の頻度で処理又は監査するかについて記述することとなる。

監査ログの処理頻度については、CP/CPS の記述上は必須とはいえないが、実際の運用上は具体的に定めるべきである。運用体制及び運用コスト等に影響されるため、運用体制及び運用コストを検討のうえ、最終決定するものとして、本考察では一般的な記述にとどめる。

FBCA-CP においては、証明書の保証レベルごとに少なくとも 1 週間に一度又は 1 ヶ月に一度を検査頻度としている。その他の、CP/CPS では、「セキュリティ監査は少なくとも毎月行われる」、あるいは「監査ログを定期的に精査する」といった記述もある。

この例のように、監査ログの監査頻度を少なくとも 1 ヶ月に一度というように定めることが望ましいが、検査の頻度は、運用体制又は運用コスト等により左右され

CP/CPS 上で明確に記述するのは困難である。当面、具体的な期間を記述するのではなく、定期的に行うとするのが妥当であると考える。具体的な処理頻度については、運用上の総合的な検討のうえ、後日の決定とする。

「4.5.2.監査ログが処理、若しくは監査される頻度」記述案

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。

［4.5.3］監査ログの保存期間

CP/CPS の 4.5.3 項では、4.5.1 項で記録することを定めたイベントを、オンサイト若しくはオフサイトにて、どの程度の期間、保存しておくのかに関して記述することとなる。

オンサイト／オフサイト各々の保管方法と保管期間を適切に定める必要がある。

- 各種基準においては、明確な保管方法・保管期間について要求していない。
- PKI Assessment Guidelines[11] （以下、PAG と呼ぶ）においては、運用体制の特性にもよるが、数ヶ月から数年間は監査ログがいずれかの場所で保存されるのが適当だとしている。
- FBCA-CP では、「監査ログは、少なくとも 2 ヶ月間オンサイトで保有される」としている。
- その他、既存の CP/CPS では「監査ログは、最低 6 週間は認証局サーバ内に保持され、その後、外部記憶媒体に最低 10 年間は保持される。」程度の記述もある。

前述のように、オンサイト保管としてサーバ内に 1～2 ヶ月程度、オフサイト保管として外部記録媒体に数年～10 年程度は保管するとするのが望ましいと考えられる。

監査ログは、誤操作、不正操作の検知、記録のほかに、運用の正当性を証明する記録とも考えられるので、帳簿等の重要書類と同様な取扱が必要と思われる。したがって、電子署名法が要求する帳簿の保管期間と同様に 10 年間（オフサイト保管）は保存しておくこと望ましい。ただし、保管地、保管環境、コスト等によって、再度の検討が必要と思われるため、本考察では、一般的な記述にとどめることとする。

[11] PKI Assessment Guidelines, PAG v0.30,Public Draft for Comment,June 18,2001,American Bar Association

「4.5.3.監査ログの保存期間」記述案

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。

［4.5.4］監査ログの保護

CP/CPS の 4.5.4 項では、記録した監査ログの保護に関して記述する。具体的には、監査ログにアクセスすることが出来る者、並びに監査ログの削除や改ざんができないようにするための要件等を記述することが望ましい。

検討項目としては、次のものがある。

- 誰が監査ログを見ることができるか
- 監査ログの改ざんに対する防護
- 監査ログの削除に対する防護

ECOM ガイドラインでは「監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の改ざん、消去、漏えい等に対して保護し、必要に応じ適正な期間内に提供可能な状態で保管しておく必要がある。」としている。

WebTrust では、「3.10.12 システム監査ツールへのアクセスは、不正使用や誤用を防ぐように防御する。」としている。

ある民間認証局では、「漏えい、改ざん、滅失及び毀損等の防止処置を施し、監査証跡を保管管理する。」としている。

本認証局の場合も、監査ログのアクセスについては一定の制限を設けるべきである。また、監査ログの改ざん及び削除に対する保護方法について、具体的に規定することが望ましいが、本認証局に係わる施設設備の検討及び決定がされていないので詳細を規定することはできない。したがって、現段階では前述の基準及び CP/CPS 記述例にあるような、一般的な記述にとどめることとする。

「4.5.4.監査ログの保護」記述案

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。監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。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。

［4.5.5］監査ログのバックアップ手続き

CP/CPS の 4.5.5 項では、バックアップが必要な監査ログがある場合、そのバックアップ手続きを記述することとなる。具体的には、バックアップの手順と保管場所に関して、いつ、何に対してバックアップを取り、どこに保管するか、を記述することが望ましい。通常の認証局では、監査ログは、定期的に外部記憶媒体に対してバックアップをとり、安全な施設に保管するとするのが一般的である。また、詳細なバックアップ手続きについて CP/CPS 上に規定できない場合は、バックアップ手順を別途定めて、それに従う旨を記述することでも良いと考えられる。

「4.5.5.監査ログのバックアップ手続き」記述案

監査ログは、認証局サーバのデータベースとともに、事前に定められた手続きに従い、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。

［4.5.6］監査ログの収集システム

CP/CPS の 4.5.6 項では、監査ログの収集システムが、認証局システムの内部のものであるか、外部のものであるかについて記述することとなる。監査ログは、認証局システムで行われた操作との一貫性が保証されなければならない。監査ログの収集は、認証局システム内にあった方がシステム全体として一貫した収集が可能であり、より安全であるといえる。したがって、監査ログの収集システムは、認証局システムに内在している事が望ましい。しかし、監査ログの収集機能は認証局システムに依存し、前述のように内在させる事ができない場合もあるため、認証局システム構成の決定時点で、再度見直すこととする。

「4.5.6.監査ログの収集システム」記述案

監査ログの収集機能は認証局システムの一機能とて内在しているものとし、セキュリティに関する重要な事象を監査ログとして収集する。

［4.5.7］監査イベントを引き起こした人への監査活動の通知

CP/CPS の 4.5.7 項では、監査イベントの記録に際し、イベントを引き起こした者に対して警告等の通知をするか否かについて記述することとなる。

何らかの操作イベントを引き起こした者に対して、その操作を中止させ、あるいは抑制をさせる必要があるのであれば、何らかの通知を行うための方針を記述することとなる。

しかし、監査イベントを記録していることはセキュアな認証局システムにおいては当然のことと考えられ、あえて監査イベントを記録し保存していることを特別に通知する必要性はないものと思われる。また、全ての監査イベントについて、引き起こした者へ通知することはシステム的対応が困難であり、CP/CPS 上、明確に記述することは難しい。更に、何らかの通知方針を CP/CPS に記述することは、どのような場合に監査ログが記録されるかを外部の攻撃者に知らせることとなり、セキュリティ上も好ましくないと考えられる。前述から、監査イベントを引き起こした者に対して通知しないと記述するのが妥当であり、かつ一般的な記述であると思われる。

「4.5.7.監査イベントを引き起こした人への監査活動の通知」記述案

本認証局では、監査ログの収集を、事象を発生させた人、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。

［4.5.8］セキュリティ対策の見直し（脆弱性評価）

CP/CPS の 4.5.8 項では、本認証局関連システムの脆弱性及び脅威の評価について記述することとなる。

認証局システムでは、そのセキュリティを確保するために定期的に、運用面及びシステム面におけるセキュリティ上の脆弱性を評価して、必要に応じて関連システムの更新並びに CP/CPS 及び関連する文書の見直しを行うことが望ましい。

しかし、CP/CPS のような開示文書上に、脆弱性の評価内容を具体的かつ詳細に記述することは、外部の攻撃者に対して関連システムの脆弱性の評価方法を詳細に知らせることとなり、セキュリティ上は好ましくないと考えられる。したがって、詳細な記述はすることなく、適宜、関連システムの脆弱性評価と見直しを行う旨の記述にとどめるのが妥当であると考えられる。

「4.5.8.セキュリティ対策の見直し（脆弱性評価）」記述案

本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。

5.4.4.6. ［4.6］記録の保管

CP/CPS の 4.6 節では、認証局における一般的な記録の保管・保持のポリシについて記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- アーカイブ記録の種類
- アーカイブの保存期間
- アーカイブの保護
- アーカイブのバックアップ手順
- 記録に対するタイムスタンプを付ける要件
- アーカイブの収集システム
- アーカイブ情報の入手、検証の手続き

次に、上に示した各要素について、記述すべき内容を検討する。

［4.6.1］アーカイブ記録の種類

CP/CPS の 4.6.1 項では、アーカイブされる記録の種類、例えば、全ての監査データ、証明書申請情報及び証明書申請を補う書類等について記述することとなる。

アーカイブする記録の種類は、主に認証局システムで生成され、電子データとして保存されるもの及び紙媒体（書類）として保存されるものに分類される。電子署名法対応の認証局の場合では、記録されるアーカイブの情報には次のような物が網羅されると考えられる。また、記録の保存にあたっては、情報の漏えい、改ざん、滅失の防止措置を施し、紙媒体については原本を保存するものとする。

- 発行された全ての証明書及び CRL（電子データ）
- CP/CPS、証明書所有者規程及びその変更に関する記録（電子データ、紙媒体）
- 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（電子データ、紙媒体）
- 証明書の発行、失効時に提出を受ける申請書（電子データ、紙媒体）
- 利用者の真偽の確認のために提出を受けた書類（電子データ、紙媒体）
- 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（電子データ、紙媒体）
- 証明書の発行、失効申請の扱いに際し認証局で記録される電子データ
- 認証業務の手順に関して記載した書類。またその変更に関する記録（電子データ、紙媒体）

- 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（紙媒体）
- セキュリティ監査対象イベント（CP/CPS 4.5 節）（電子データ）
- 監査の実施結果に関する記録及び監査報告書（電子データ、紙媒体）
- 手続き的管理（CP/CPS 5 章）で規定する権限付与等の記録（電子データ、紙媒体）
- 認証業務用設備の維持管理に関する記録（電子データ、紙媒体）
- 認証業務における、事故に関する記録（電子データ、紙媒体）
- 帳簿書類の利用及び破棄に関する記録（電子データ、紙媒体）

本認証局の場合、電子署名法対応等所定の基準へ準拠することが求められていないため、上に示したほど CP/CPS 上、詳細にアーカイブ記録を定める必要はないものと考えられる。また一方、前述の情報が電子データで記録されるか、紙媒体で記録されるかは、認証局関連のシステム構成に依存する。現段階では、システム構成が決まっていないため、システム構成決定後に、前述のアーカイブ情報を参考にし、どの情報を記録するのか及び各々の情報を電子データ又は紙媒体として記録するのかについて確定していく必要がある。現段階の記述案では、一般的にどのような記録がアーカイブされるのかについて記述する。

「4.6.1.アーカイブ記録の種類」記述案

本 CP/CPS 4.5.1 項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】

- 認証局の署名用鍵ペアの生成
- システムからの加入者の追加や削除
- 証明書の発行や取消を含めた鍵の変更
- RA 担当者権限の追加や変更、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）
- 利用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）

［4.6.2］アーカイブの保存期間

CP/CPS の 4.6.2 項では、アーカイブされる記録の保存期間について記述することとなる。アーカイブの保存期間の目安として、FBCA-CP では、証明書の保証レベルごとに最低限、次の保存期間を設けることとしている。

- 初期（Rudimentary）レベル　　：7 年 6 ヶ月
- 基本（Basic）レベル　　：10 年 6 ヶ月
- 中位（Medium）レベル　　：20 年 6 ヶ月

本認証局の場合、1 つの証明書保証レベルでの運用を検討しており、証明書の保証レベルごとにアーカイブの保存期間を設定する必要はないと考えられる。

もう一つの目安として、電子署名法における帳簿書類の保存期間が法定されており、証明書申請者本人の署名等のある書類等の原本を、証明の有効期間終了後 10 年間保存しなければならないとしている。

前述から、アーカイブの保存期間については、電子署名法及び FBCA-CP の基本（Basic）レベルを意識して、10 年程度としておくのが妥当であると考えられる。

一方で、個々のアーカイブの種類ごとに、保存期間（起点、終点）に差異を設けるかどうかを検討する必要がある。通常、証明書のライフサイクルに関する記録のアーカイブについては、証明書の有効期間満了日を起点とし最低 10 年間とするのが一般的である。また、監査関連のアーカイブについては、監査終了後から次回の監査日までとするのが一般的である。

本項の記述方針としては、個々のアーカイブ対象の保存期間を明示するために、CP/CPS 4.6.1 項において、アーカイブ対象物を規定すると同時に各々の保存期間を記述するのが望ましい。

アーカイブの保存期間については、保存に要するシステムの容量及び運用コスト等との兼ね合いも問題となる。今後、関連システムの構成等の決定後に、システム容量及びコスト等を勘案のうえ、アーカイブ期間を決定することとする。

「4.6.2.アーカイブの保存期間」記述案

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は、最低 10 年は保存される。紙媒体及び外部記憶媒体の保存期間に関しては本 CP/CPS 4.6.1 項のとおりである。

［4.6.3］アーカイブ記録の保護

CP/CPS の 4.6.3 項では、アーカイブ記録の保護のために、アーカイブを見ることができる者、アーカイブの変更・削除に対する防止策及びアーカイブが保存される媒体の品質低下に対する防止策等について記述することとなる。

監査ログの保護については、CP/CPS 4.5.4 項にて検討したとおりである。その他のアーカイブ記録に対しても、記録へのアクセスについては一定の制限を設けるべきであり、また、アーカイブの改ざん防止及び削除防止の方法について具体的に規定することが望ましい。しかし、現段階では、本認証局に係わる施設設備の検討及び決定がされていないため、詳細な規定することはできない。したがって、現段階では次のとおり、一般的な記述にとどめることとする。

「4.6.3.アーカイブ記録の保護」記述案

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。アーカイブデータのバックアップは、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以外の者がアクセスできないように、制限された施設に保存される。また、その施設は、温度、湿度、磁気等の環境上の脅威からも保護される。

［4.6.4］アーカイブのバックアップ手順

CP/CPS の 4.6.4 項では、アーカイブのバックアップ手順について記述することとなる。具体的には、アーカイブのバックアップ間隔、バックアップ先、紙等の保管手続きについて記述することが望ましい。

通常、アーカイブのバックアップは日次／週次／月次等、定期的な間隔で、外部記憶媒体に格納されるとするのが一般的である。

また、紙媒体のアーカイブバックアップについては、書類のコピーを施設外の災害復旧施設において保管することが望ましいが、運用上の負荷が極めて高くなるため、CP/CPS 上の記述をしないことも考えられる。ただしこの場合、紙媒体の原本保管を厳重に行う必要があると考えられる。

「4.6.4.アーカイブのバックアップ手順」記述案

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。

［4.6.5］記録に対するタイムスタンプを付ける要件

CP/CPS の 4.6.5 項では、アーカイブされる種々のデータに対してタイムスタンプを付ける要件について記述することとなる。

認証局においては、例えば、いつ証明書の失効申請が行われたのか、いつ証明書が失効されたのか等の、正確な時刻を記録する必要がある。このため、記録する種々のデータに対し、レコード単位でそのイベントが起きた正確な時刻を記録することが望まれる。また、アーカイブに限定されないが、情報に記録される時間に差異があった場合、情報の整合性が損なわれるので、認証局関連システムの時計は、正確に記録するため時刻の同期化を行う必要があると思われる。そのためには少なくとも、認証局システムの時計は何らかの時刻源から時刻を取得し、各種サーバ間にて時刻の同期化を行う必要がある。更に厳格な時間管理が必要となる場合、又は対外的に法的な時刻証明を必要とする場合は、時刻認証局（TSA：タイムスタンプ局）の利用も考えられる。

現段階では、本認証局において、時刻認証局を利用した時刻証明を行うかどうかの結論はでていない。また、JPNIC におけるレジストリ関連業務においては、トランザクションの前後を厳密に争うことはないと考えられる。したがって、GPS 等を時刻源として、NTP により認証局サーバ等全てのシステム間の時刻を同期させれば十分であると考えられる。将来的に、各種ログデータの原本性保証の要求がある場合には、時刻認証局（TSA）の利用も検討すべきである。

本考察では、次の記述案にとどめ、時刻認証局の利用又は GPS を時刻源としたシステムの構成等が決定された時点で、再度見直しをかけるものとする。

「4.6.5.記録に対するタイムスタンプを付ける要件」記述案

本認証局において使用される認証局システムは、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。

［4.6.6］アーカイブの収集システム

CP/CPS の 4.6.6 項では、CP/CPS 4.6.1 項に規定するアーカイブ記録の収集システムを内部的にするか（システムに内在しているか）、又は外部的にするか及び自動収集できるアーカイブは何かについて記述することとなる。

監査ログに対する収集システムについて、CP/CPS 4.5.6 項にて記述したのと同様に、アーカイブの収集についても、監査ログの収集との一貫性を保持するために、認証局サーバシステムに内在していることが望ましい。ただし、自動収集機能に関してはシステム構成に依存すると考えられるため、システム構成決定後に再度見直すものとする。現段階では、監査ログの収集システムと同等の記述をするものとして、次に記述案を示す。

「4.6.6.アーカイブの収集システム」記述案

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 CP/CPS 4.5.6 項に記述のとおりである。

［4.6.7］アーカイブ情報の入手、検証の手続き

CP/CPS の 4.6.7 項では、アーカイブの情報を入手し、検証する手続きについて記述することとなる。

本認証局においても、適切な権限者がアーカイブを入手し、定期的に可読性の検証を行うことが必要と考えられる。この検証間隔については、可能であれば「年 1 回」というように具体的に定めることが望ましいが、認証局の運用の詳細が確定していない段階では「定期的に」とのみ記述するのが妥当である。

「4.6.7.アーカイブ情報の入手、検証の手続き」記述案

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。保管期間の過ぎた古い媒体は破棄する。

5.4.4.7. ［4.7］鍵の更新（切り替え）

CP/CPS の 4.7 節では、認証局による鍵更新にともなって、認証局の利用者に対して新しい公開鍵を提供する手続きについて記述することとなる。これらの手続きは、現在の鍵を提供した手続きと同じものにすることができる。また、新しい鍵を、古い鍵を使用して署名された証明書の中で認証することもできる。

本認証局の場合、新しい認証局公開鍵は、JPNIC ルート認証局から証明書の発行を受け、次のいずれかの方法により利用者へ提供するものと考えられる。

- セキュアなプロトコルを使って広く公開する方法（Web サイト又はその他のリポジトリにより公開）
- オフラインによる利用者への送付（フロッピーディスクその他の記録媒体に格納し、LRA 管理者経由での手渡）
- オンラインによる利用者への送付（電子メール等への添付）

新しい認証局公開鍵の提供方法を決めるうえで、次の考慮が必要であると考えられる。

- リポジトリ等への公開の場合、証明書の改ざん防止措置等を検討しなければならないこと
- 本認証局の場合、認証局公開鍵の更新は現状 8 年[12]間隔程度と予想され、頻繁に配布するものではないこと
- 今回の認証業務が、適用範囲の限定された環境での運用であることを考慮すると、新しい公開鍵をフロッピーディスク等の外部記憶媒体に格納し、アウト・オブ・バンドで直接配布するのが便利、かつ安全であること

前述の点を考慮すると、本認証局においては、新しい公開鍵は、リポジトリ等上で公開せずに、記録媒体に格納して、LRA 管理者経由で配布することが適当であると考えられる。

ただし、鍵の更新については、認証システム及び利用ユーザのアプリケーションに依存するものと思われる。システムによっては、認証局の鍵の更新を意識せずに利用することも可能である。システム的な対応がない場合は、新規発行時における認証局の公開鍵の提供と同様な手続きになると思われるため、現段階では新規発行時の提供方法と同様の手続きとし、システム構成等の決定後に、再度見直すこととする。

---

[12] 認証局鍵ペアは、その有効期間（10 年）より、EE 証明書の有効期間（2 年）の分だけ前に、更新するのが一般的である。

「4.7.鍵の更新（切り替え）」記述案

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 CP/CPS 6 章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 CP/CPS 6.1.4 項に定めた方法と同様に配布を行う。

5.4.4.8. ［4.8］危殆化と災害からの復旧

CP/CPS の 4.8 節では、危殆化又は災害が起きた際の通知及び復旧手続きに関連する要件について記述することとなる。RFC2527 によると、本節で記述されるべき要素には次のものがある。

- 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の対処
- 証明書を失効しなければならない場合の対処
- 私有鍵が危殆化した場合の対処
- 災害等発生時の設備の確保

次に、上に示した各々の要素について、記述すべき内容を検討する。

［4.8.1］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の対処

CP/CPS の 4.8.1 項では、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、あるいは破損のおそれがある場合に用いられる復旧手続きについて記述することとなる。

本項では、認証局システムに係わる事故の際の報告先、担当窓口及び手続き等を規定することが望ましいが、一般的に、これら事故時の対応については、CP/CPS 上、詳細な記述をすることが困難と考えられる。JPNIC における前述したような事故の際の体制及び詳細な手続き等については別途、検討するものとして、ここでは一般的な記述案をあげる。

「4.8.1.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の対処」記述案

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。

［4.8.2］証明書を失効する場合の対処

CP/CPS の 4.8.2 項では、EE の公開鍵が失効された場合に使用される復旧手続きについて記述することとなる。

本項では、EE の公開鍵が失効された場合の復旧手続きとして、具体的に、どのように安全な環境が再構築されるのか、どのように新しい公開鍵が EE に提供されるのか、どのように EE は再認証されるのか、について記述することが望ましい。現段階では、EE の証明書を失効した場合に、再度証明書を発行する場合には、初期発行時と同様の手続きをとるとするのが、妥当な対処と考えられる。本考察では、証明書を失効し再発行する場合の一般的な記述案にとどめることとする

「4.8.2.証明書を失効する場合の対処」記述案

発行した証明書の失効処理にあたっては、その失効の取消は行わない。証明書を失効した証明書所有者に対し、再度証明書を発行する場合は、あらためて発行手続きを行う。

［4.8.3］私有鍵が危殆化した場合の対処

CP/CPS の 4.8.3 項では、エンティティの鍵が危殆化された場合に用いられる復旧手続きについて記述することとなる。

本項では、主体の私有鍵が危殆化した場合の復旧手続きとして、前項と同様に、安全な環境がどのように再構築されるのか、サブジェクトはどのように再認証されるのか、等について記述することが望ましい。

認証局の私有鍵が危殆化した場合は、発行した各種証明書の失効手続き、認証局私有鍵の再生成及び各種証明書の再発行手続きをとるのが一般的である。

一方、EE の私有鍵が危殆化した場合は、CP/CPS 4.4 節で定めた手続きをとるのが一般的である。

「4.8.3.私有鍵が危殆化した場合の対処」記述案

認証局私有鍵が危殆化した場合は、予め定めた計画に基づいて認証業務を停止し、次の手続きを行う。

- ホストマスタ証明書、サーバ証明書等の失効手続き
- 認証局私有鍵の廃棄及び再生成手続き
- ホストマスタ証明書、サーバ証明書等の再発行手続き

また、証明書所有者の私有鍵が危殆化した場合は、本 CP/CPS 4.4 節において定める手続きに基づき、証明書の失効手続きを行う。

［4.8.4］災害等発生時の設備の確保

CP/CPS の 4.8.4 項では、自然災害又はその他の災害後、事業継続を保証するエンティティの能力について記述することとなる。

一般の基準によると、WebTrust では、事業継続計画の定期的レビュー及びテスト、バックアップ装置及びバックアップデータの遠隔地保管等を実施することとしている。

本認証局においても、証明書の重要性、補償レベル等に応じて事業継続計画を策定し、バックアップ機器、バックアップデータの遠隔地保管等を考慮する必要があると思われる。しかし、現段階では、事業継続計画及び災害復旧サイトの詳細検討までには至っておらず、詳細確定後に CP/CPS に改善を加えるものとする。

本考察では、本認証局に関連する全てのデータのバックアップを維持し、災害等発生時には予備機等を確保して、事業の継続に努めるものとして、次に記述案を示す。

「4.8.4.災害等発生時の設備の確保」記述案

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。

5.4.4.9. ［4.9］認証局の終了

CP/CPS の 4.9 節では、認証局、登録局の終了と終了の通知のための手続きに関する要件について記述することとなる。

各種基準によると、ECOM ガイドラインでは、認証業務を終了する場合には、そのスケジュールと手続きを決め、その内容を利用者等直接その影響を受けるものに通知する必要があるとしている。利用者への通知スケジュールに関して、署名法では、認証業務終了の 60 日前までに行う必要があるとしている。

本認証局においても、認証業務の終了に際しては、周到な準備と相応の期間が必要であることを認識しておくべきであり、業務終了より相応の期間前までに、関係者に通知することを記述すべきと思われる。

「4.9.認証局の終了」記述案

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、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検証者に告知し、所定の業務終了手続きを行う。

5.4.5. ［5］建物・関連設備、運用、要員のセキュリティ管理

CP/CPS 5 章では、認証業務を遂行するために必要とされる非技術的なセキュリティ統制を規定する。非技術的なセキュリティ統制とは、物理的・手続き的・人物的なセキュリティ統制のことである。

これらの規定の検討を行う際に ECOM 作成の認証局運用ガイドライン V1.0、特定認証業務の認定に係る調査表[13]（以下、調査表と呼ぶ）、WebTrust for CA（これらを以下、CP/CPS 策定参考文書と呼ぶ）を参考にする。

なお現段階では、JPNIC 認証局の設置場所等が決まっておらず、また CP/CPS 上に詳細な要件を記述することはセキュリティ上好ましくないため、本報告書上の記述案は、最低限必要と思われる基本的内容についてのみ記述するものとする。

5.4.5.1. ［5.1］建物及び関連設備管理

CP/CPS 5.1 節の各項中では、認証局に要求される物理的な管理に関連することが規定される。

［5.1.1］施設の位置と建物構造

CP/CPS 5.1.1 項では、認証局を設置する建物の立地条件や認証局を設置する区画の条件を物理的なセキュリティの面から規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 建物の立地条件としては、周辺の火災、電磁界、水害、落雷、空気汚染の自然災害等を受けにくい場所であること
- 建物の条件としては、（準）耐火構造、耐震構造であること
- 認証局を設置する区画条件としては、障壁による区分け、区画への入場資格確認等が行われていること

その他、調査表の中では次のことも規定されている。

- 認証局の所在を公開又はそれを示唆する情報を提示しないこと

前述の内容は、重要な電子計算機設備が設置される建物・区画に関する記述であり、最低でもその概要を記述する必要があると考えられる。

---

[13] 電子署名及び認証業務に関する施行規則及び指定調査機関による特定認証業務調査表

「5.1.1.施設の位置と建物構造」記述案

本認証局に係わる重要な設備については、周辺の火災、電磁界、水害、落雷、空気汚染の自然災害、地震等の影響を受けにくい建物内に設置し、本認証局の設備は、障壁により区画され、入場資格確認等が可能な収納システムの表示のない室に設置する。

［5.1.2］入退管理

CP/CPS 5.1.2 項では、認証局が設置されている区画への入退出を管理・監視するために整備する必要がある環境を規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 許可された者のみが入室可能となる入退出管理を行うこと
- 認証設備室が無人になる場合にセンサ・カメラによる監視を行うこと
- 窓、扉には防犯装置を講ずること
- 入退出に関する管理規定を整備し、管理責任者を決定すること
- 部外者の認証局区画内への入退出は権限を有する複数名による同行とその日時の記録を行うこと

その他、ECOM ガイドラインや調査表では次の項目も要件として規定されている。

- 2 名以上の生体認証によって入室が可能となること
- 不正な入出操作が行われた際に警報が発せられること
- 監視カメラは死角が出来ないように設置すること
- 装置、情報、ソフトウェアは許可なしで持ち出し出来ないこと

また次のような要件をあげている CP/CPS もある。

- 認証設備室は、天井から床まで設置された 2 重若しくは 3 重の隔壁を持ち、窓がない又は窓に効果的な安全対策が施されている領域に構築すること

「5.1.2.入退管理」記述案

本認証局の認証設備室は、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が行われ、監視カメラによる記録が行われる。また認証設備室への立入は、入室権限を有する複数人が同時に操作することにより行われる。

［5.1.3］電源及び空調設備

CP/CPS 5.1.3 項では、認証局運用に必要な電源確保と空調設備設置の要件を検討する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 停電対策（UPS、自家発電設備、その他技術的方法から選択）を講じること
- 適切な室内空調を安定して提供できること

その他、ECOM ガイドラインには次の項目が規定されている。

- 電圧、周波数等の安定した電力供給が可能なこと

JPNIC 認証局においても、停電による電力断絶や空調不良によるシステムの温度上昇は業務の停止、システムの故障を起こす要因となるため対策が必要である。

「5.1.3.電源及び空調設備」記述案

JPNIC 認証局における設備は、停電に対する対策を行う。また空調設備は、各種使用する機器に悪影響を与えないよう維持管理される。

［5.1.4］水害及び地震対策

CP/CPS 5.1.4 項では、認証業務を妨げないように水害対策と地震対策の要件を検討する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 認証局システムの停止が生じないよう対策が講じられていること
- 災害への対策を規定した文書が作成されていること
- 通常想定される規模の地震によるシステムの転倒及び構成部品の脱落等を防止するための耐震措置が講じられていること

その他、調査表では、水害の防止措置として、直上階からの漏水対策等についても記述されている。

「5.1.4.水害及び地震対策」記述案

漏水等水害に対する措置を講ずる。また地震等により JPNIC 認証局システム等の

機器が転倒、脱落を起こさないように措置を講ずる。

［5.1.5］防火設備

CP/CPS 5.1.5 項では、認証局に設置すべき防火設備の要件について検討する。

ECOM ガイドラインや調査表では次の項目が要件としてあげられている。

- 電源設備や空調設備の防火措置を講ずること
- 認証設備室は防火区画内に設置されること

その他、一般的な CP/CPS では、次のような規定内容も記述されている。

- 自動火災報知器及び消化装置が設置されていること

JPNIC 認証局では前述した項目に従って対策を講じることを CP/CPS 上に規定すれば、一般的な要件レベルを満たしていると考えられる。

「5.1.5.防火設備」記述案

JPNIC 認証局の設備は、防火壁によって区画された防火区画内に設置される。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、火災報知器や消火設備の設置を行う。

［5.1.6］記録媒体の保存

CP/CPS 5.1.6 項では、記録媒体の安全な保管方法を検討する。

調査表で規定されている主な内容として次の項目があげられている。

- 加入者の真偽確認に際して知り得た情報の目的外使用の禁止及び帳簿書類の記載内容の漏えい、滅失又は毀損の防止措置を講じていること

帳簿書類の記載内容の漏えい、滅失又は毀損の防止措置に関しては、紙書類にて保存する情報と電子媒体にて保存する情報を選別・決定し、その保存方法・利用手続きに関してなんらかの規定書上に記載しなければならないと思われる。また電子媒体にて保存される場合には、適切な媒体を検討しなければならないと思われる。

また CP/CPS 上に詳細を記載するかどうかは別として、記録媒体の保管場所を検討しなければならないと思われる。

複製した記録媒体を認証局設備が設置されている場所以外の遠隔地にて保管する場合には、稼動している認証局の所在地にて大規模な災害が発生しても情報の滅失は最小限に抑えられる一方、稼動している認証局から遠隔の保管場所までの安全な輸送方式を確保する必要があり、そのための輸送費用と保管場所確保のためのコストが発生する。

一方、遠隔地保管を行わない場合には、複製した記録媒体の確実な保護のために、各種災害にも耐えられる堅牢な保管設備が必要である。堅牢な保管設備を確保したとしても、稼動している認証局の所在地にて大規模な災害が発生した場合には情報が滅失する可能性があると思われる。そのため、認証局の復旧が困難となり、その結果業務停止となる可能性がある。

稼動している認証局が設置されている場所での記録媒体の保管以外に、稼動している認証局が設置されている地域以外の場所にも保管する方が、災害発生後の復旧を保証する可能性が高くなると考えられる。

「5.1.6.記録媒体の保存」記述案

アーカイブデータ、バックアップデータを含む認証業務を行う上で必要な情報は、適切な入退管理が行われた室内の保管庫に保存されるものとする。

［5.1.7］廃棄物の処理

CP/CPS 5.1.7 項では、情報や設備を破棄する場合の方法を検討する。

WebTrust では、次の項目があげられている。

- 破棄前に機密情報の有無を確認すること
- 機密情報を含む記録媒体は破棄前に完全初期化又は物理的破壊を行うこと

廃棄物からの情報漏えいを防ぐために、前述の項目に対して具体的な対応方法を手順書等に明確に定めておく必要があると思われる。ただし、詳細な対応方法については、公開されることが前提である CP/CPS に記載する必要はないと考えられる。認証局の私有鍵に関する事項は、CP/CPS 6.2.9 項に従うものとする。

「5.1.7.廃棄物の処理」記述案

機密扱いとする情報を含む書類・記録媒体の廃棄については、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がなされる。

［5.1.8］オフサイト・バックアップ

CP/CPS 策定参考文書の中では、CP/CPS 5.1.8 項に関して特に詳細な規定は行われていない。ただし、サービスレベルを高めるためにはオフサイト・バックアップを用意することが望ましいため、その要件を検討する。なお、記録媒体のオフサイト・バックアップについては前述の CP/CPS 5.1.6 項にて記述している。

オフサイト・バックアップを行うには相当のコストが要求されるため、事業内容を踏まえてその必要性を検討する必要があると思われる。オフサイト・バックアップを行う場合には、稼動している認証局で障害が発生してもオフサイトで引き続きサービス提供を行うことが可能である一方、設備維持や管理要員のコストが増大し、また、サイト間のデータ転送時のセキュリティ対策を厳格に行う必要もある。

一方、オフサイト・バックアップを行わない場合には、特別なコストは要しないものの、稼動している認証局で障害が発生した場合には、復旧完了までサービスを提供することができないという問題が発生する。

コストの点を考慮しないとすると、JPNIC 認証局業務の継続性を保証するためにオフサイト・バックアップを行うことが望ましいと思われる。ここで、オフサイト・バックアップの準備レベルとして次の 3 種があると思われる。

- コールドサイト

JPNIC 認証局の代理運用を可能とする施設のみを事前に確保しておく状態である。代理運用に必要な機器は代理運用が必要となった時点で調達を行うと共に、バックアップからのデータ復旧を行うことによって代理運用可能となる。

- コールドスタンバイ

バックアップからのデータ復旧によって、JPNIC 認証局の代理運用を行うことが可能なだけの設備が整えられている状態である。

- ホットスタンバイ

コールドスタンバイの状態に加え、電源が既に投入されており、バックアップからのデータ投入によっていつでも代理運用可能な状態である。又は JPNIC 認証局システム以外の情報はリアルタイムに更新が行われ、JPNIC 認証局の鍵及び JPNIC 認証局システムの復旧のみによって JPNIC 認証局の代理運用が可能となる状態である。

JPNIC が提供するサービスレベルと許容されるコストをもとに、どの方法を採用するか継続検討課題とし、現段階では規定しないこととする。

「5.1.8.オフサイト・バックアップ」記述案

規定しない。

5.4.5.2. ［5.2］手続き管理

CP/CPS 5.2 節では、認証局を運営するにあたって業務実施上の手続き方法を検討する。

一般的な CP/CPS では、主な規定として次の項目があげられている。

- 認証業務の手順の細目を明確に事務取扱要領に規定し、実施していること
- 業務内容、手順等の変更に伴う事務取扱要領の改訂に関する手順等を明確に規定し、実施していること

またより詳細な規定内容として考えられる項目が、ECOM ガイドラインや WebTrust にて次のように規定されている。

- 役割に応じたアクセスコントロールが行われていること
- 重要な情報にアクセス可能な部署は他から隔離されること
- アクセス権限は定期的にレビューすること
- 事故を予防するために内部牽制が行われること
- 部署外からの監査等のチェック機能が働くこと
- 事故発生時にはその発生源が特定できること

［5.2.1］信頼される役割

CP/CPS 5.2.1 項では、認証業務を担う各役割の決定と要件を規定する。

CP/CPS 策定参考文書によると、次の項目が主な要件としてあげられている。

- 認証局の安全性と信頼性を長期的に確保すること
- 情報セキュリティ技術やシステム監査等の専門家を配置しておくこと
- 指揮命令系統、責任及び権限が文書に明確に定められ、それに従って業務が実施されること
- 全ての就業者の役割に応じて教育・訓練計画等が策定され、それに従って実施されること
- 指揮命令系統、責任及び権限に変更がある場合、規定等の変更手順等が明確に定められ、それに従って変更が行われ、変更に係る教育・訓練が実施されること

一般的にはこの節ではどのような役割があるかについて検討され、教育・訓練については CP/CPS 5.3 節以降で述べられている。ここで、各役割を定めるにあたってセキュアな運用を保証するために、各役割に認められる権限を保有する者を確実に分離する必要がある。権限分離の考慮点としては次のものがある。

- システム操作の承認権限と承認に基づくシステム操作権限を持つ者の分離
- システム管理操作権限と発行・失効操作権限を持つ者の分離
- 運用に携わる権限の付与者と被付与者の分離

前述 3 項目を考慮した役割案を表 5-4 に示す。

表 5-4 名称とその役割

			役割名称又は用語	役割又は用語の説明
			運営委員会	・監査報告確認、承認 ・認証局運営責任者への監査指摘事項対応指示 ・JPNIC 認証局の運営方針の決定 ・証明書ポリシ、運用ポリシ及び運用ポリシ変更の最終承認 ・認証局運営責任者の任命・解任等 ・その他、重要な事項の協議及び決議
運営組織			認証局運営責任者	・サービス及び運用組織の統括 ・監査指摘事項への対応統括 ・運用管理者の任命・解任 ・システム変更及び運用ポリシ変更の承認 ・非常時対応等の指揮、監督
	運用組織		運用管理者	運用組織の統括 ・運用担当者の任命・解任 ・運用担当者の教育計画策定、実施 ・運用担当者の入室権限付与 ・運用担当者の作業報告確認 ・認証局私有鍵の活性化操作、非活性化操作の立会い（生成、削除操作ではない） ・非常時の対応指示 ・作業報告書、貸出簿等、運用記録の保管・管理等 ・その他運用全般の管理 （認証局の運用で使用するパスワード、PIN の管理等を含む。）
		運用担当者	ログ検査者	・監査ログ、入退室ログ等の検査
			鍵管理者	・キーセレモニ時の認証局鍵生成作業立会い ・認証局鍵廃棄時の立会い ・バックアップ私有鍵の管理
			セキュリティ管理者	・認証局システムのセキュリティ設定、変更 ・キーセレモニ時の RAO の登録、発行
			認証局管理者	・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
			登録局管理者	・証明書発行、失効の登録作業 ・登録局の管理運営

			審査者	・証明書（LRA 管理者証明書）発行申請の受付け ・証明書発行にかかる審査 ・承認者への、LRA 管理者証明書の発行依頼
			承認者	・審査結果の承認 ・発行登録作業承認
			保守員	ネットワーク技術者、システム技術者及び監視技術者の総称 ・ネットワークの設定、維持管理等 ・システム技術サポート（認証局システム、RA システム等）、サーバの設定・維持管理等 ・監視（不正侵入検知連絡、システム状況監視等）
			ベンダー保守員	・各種機器の故障等の対応
	ローカル登録局		ローカル登録局	・証明書を発行する組織とは異なる別組織であり、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
			ローカル登録局責任者	・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	・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

前述の役割の位置付け案を図 5-5 に示す。

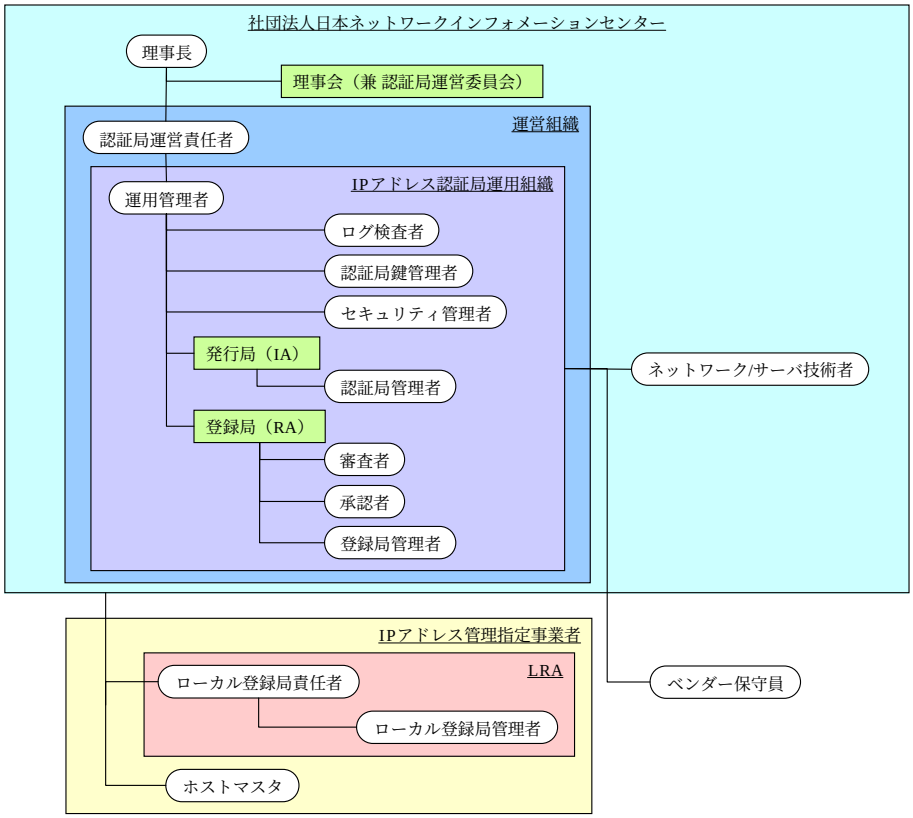


図 5-5　各役割の位置付け

前述の役割の中で兼務可能と考えられる役割について次のように検討した。

- ログ検査者

運用管理者にシステム操作権が認められていないため、ログ検査者は運用管理者と兼務可能と思われる。

- セキュリティ管理者

キーセレモニ時以外はほとんど作業が発生しないため、JPNIC 認証局システムや入退室管理システムによっては複数人操作を前提に、運用管理者と CAO 又は RAO による合同操作にて兼務を可能と思われる。

- 審査者

RAO に申請の承認権がないため、審査者と承認者が兼務されない場合に限って審査者は RAO と兼務可能と思われる。

- 承認者

運用管理者にシステム操作権が認められていないため、承認者がシステム操作を伴わない場合に限って運用管理者と兼務を可能と思われる。

「5.2.1.信頼される役割」記述案

次の表 5-4 に JPNIC 認証局の運営、運用上の役割を示す。

（表 5-4 が記述される）

［5.2.2］必要とされる人数

CP/CPS 5.2.2 項では、各業務において業務を遂行するために必要な要員数に関して規定する。

調査表では各役割の必要要員数を次の視点で検討している。

- 業務遂行上に必要な知識・経験を有している技術者を認証業務に必要数配置する
- 認証設備室への入室が許可される者の指定と登録及び複数人による入室を実施する

また認証業務における重要操作は、複数人で行われるのが通例であると思われる。

これらを考慮した具体的な要員数の構成案を次に示す。

案 1：

- 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
- 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、JPNIC 認証局システムサーバの設置室へ入室権限者以外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
- JPNIC 登録局の端末を用いた発行・失効操作等は、複数人の RAO によって行う

案 2：

- JPNIC 認証局システムサーバの操作は、複数人の CAO 又は運用管理者立会いのもとで CAO が行う
- 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、

JPNIC 認証局システムサーバの設置室へ入室権限者以外が入室する必要がある場合は、必ず入室権限者が立会いを必要とする

- JPNIC 登録局の端末による発行・失効操作等は、複数人の RAO 又は運用管理者の立会いのもとで RAO が行う

調査表にて認証設備室への立入には複数人を要求しているように、認証局での端末操作のような情報へアクセスする操作に関しても、信頼性を確保するために複数人による相互牽制が可能な人員配置を行う必要があると考えられる。次に、これらの検討をふまえ、各役割の必要要員数を検討した。

案 1 に基づき、兼務を行わない場合と行う場合の必要要員数を考慮すると、次の二つが考えられる。

表 5-5　案 1 に基づいて兼務を行わない場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	2 名	正・副各 1 名。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	2 名	正・副各 1 名。
CAO	3 名	正 2 名、副 1 名。
RAO	3 名	正 2 名、副 1 名。
審査者	2 名	正・副各 1 名。
承認者	2 名	正・副各 1 名。
人数合計	18 名（正 10 名・副 8 名）	

表 5-6　案 1 に基づいて兼務を行う場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	0 名	運用管理者が兼務。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	0 名	運用管理者と CAO 又は RAO との合議により行う。
CAO	3 名	正 2 名、副 1 名。
RAO	3 名	正 2 名、副 1 名。
審査者	0 名	RAO が兼務。

承認者	0 名	運用管理者が兼務。
人数合計	10 名（正 6 名・副 4 名）	

案 2 に基づき、兼務を行わない場合と行う場合の必要要員数を同様に考慮すると、次の二つのように考えられる。

表 5-7　案 2 に基づいて兼務を行わない場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	2 名	正・副各 1 名。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	2 名	正・副各 1 名。
CAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
RAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
審査者	2 名	正・副各 1 名。
承認者	2 名	正・副各 1 名。
人数合計	16 名（正 8 名・副 8 名）	

表 5-8　案 2 に基づいて兼務を行う場合の必要要員数

役職	人数	備考
運用管理者	2 名	正・副各 1 名。
ログ検査者	0 名	運用管理者が兼務。
鍵管理者	2 名	正・副各 1 名。 鍵生成等は CAO、RAO との合議により行う。
セキュリティ管理者	0 名	運用管理者と CAO 又は RAO との合議により行う。
CAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
RAO	2 名	正・副各 1 名。 合議操作は運用管理者との合議により行う。
審査者	0 名	RAO が兼務。
承認者	0 名	運用管理者が兼務。
人数合計	8 名（正 4 名・副 4 名）	

権限分離や複数人制御は、いかに誤用・不正を抑制するかを目的としていると考えられる。できる限り詳細に、権限の分離、操作の複数人制御を行うことが望ましいが、システムのアクセスコントロール設定機能、入退室管理システム機能等により左右される要素が多く、論理的セキュリティや物理的セキュリティと共に検討を行った上で運用体制の決定を行う必要があると思われる。

今回の検討では、一連の業務が単独で行えないことを基本とし、承認者と操作者の分離、権限付与者と付与対象者の分離、役割ごとの操作権限の分離、重要操作の複数人制御を行うものとした。今後も、厳しい条件である案 1 をベースに詳細な運用体制、役割の検討を進める必要があると考えられる。

「5.2.2.必要とされる人数」記述案

- 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
- 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、JPNIC 認証局システムサーバの設置室へ入室権限者以外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
- JPNIC 登録局の端末を用いた発行・失効操作等は、複数人の RAO によって行う

［5.2.3］役割ごとの識別と本人認証

CP/CPS 5.2.3 項では、認証局設備にアクセスする者の識別条件と権限の確認条件について規定する。

調査表では、主な規定項目として次のものがあげられている。

- 認証局設備を操作する権限を操作者ごとに設定可能であること
- 認証局設備を操作するにあたって操作者と必要権限を確認可能であること

JPNIC 認証局の設備に対するアクセス権のセキュリティ基準を文書化することは必須要件であるが、一般的に CP/CPS 上は詳細な記述がされていないことから、本考察においても詳細な記述は行わず、方針レベルの記述案にとどめることとした。

「5.2.3.役割ごとの識別と本人認証」記述案

JPNIC 認証局の設備へのアクセス管理は、役割ごとの操作権限を操作者ごとに設定できるものとする。また JPNIC 認証局の設備へのアクセス時において、操作者と

必要権限を識別可能とする。

5.4.5.3. ［5.3］要員のセキュリティ統制

［5.3.1］JPNIC 認証局における人事上のセキュリティ管理

CP/CPS 5.3.1 項では、本来、要員の資格、経験及び身分証明の要件を記述することとなっているが、JPNIC 認証局の信頼性を損なわないために、JPNIC 認証局運用に関わる要員の信頼性を保証するための要件を規定することとした。

ECOM ガイドラインでは、規定内容として次の項目があげられている。

- 認証局の役割任命において適切な審査を行うこと
- 運用要員のメンタルヘルス・健康管理・適正な処遇等における継続した人事管理を行うこと

また WebTrust では、規定内容として次の項目があげられている。

- 認証局運用要員は任命時に守秘義務契約に署名すること
- 各役割の要員に欠格事項がないかどうかを継続して定期的に検査すること

CP/CPS 上では基本的な方針を示すべきであり、詳細なセキュリティ管理手順は管理手順書等を別途作成し、これに記載することが適切であると考えられる。よって、本報告書での記述案も基本方針を示す程度とした。

「5.3.1.JPNIC 認証局における人事上のセキュリティ管理」記述案

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。日常業務においては、メンタルヘルス・健康管理・適正な処遇等における継続した人事管理を行う。また任命前までには、任命者と守秘義務契約を結び、情報の適切な管理を行う。

［5.3.2］背景調査

CP/CPS 5.3.2 項では、認証局運用要員及び認証局以外の関連する従業員（警備員等）を採用する際に行う人物確認の要件を規定する。

人物確認方法として、本人による書類提出が一般的であると考えられる。ここで提出する書類としては次のものが考えられる。

- 最終学歴を証明する書類
- 職歴を表す書類
- 賞罰が記載された書類

これらの書類に基づいて人物確認を行う場合は、その書類の記載内容の真偽及び背景を確認する必要があると考えられる。また採用にあたっては JPNIC 認証局運用要員と同様に、JPNIC 認証局の運用要員以外の者とも守秘義務契約を結ぶことが望ましいと考えられる。

「5.3.2.背景調査」記述案

JPNIC 認証局業務と関連する者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］トレーニング要求

CP/CPS 5.3.3 項では、認証局を適切に運用し続けるために運用要員の役割に応じて行うトレーニングの要件を規定する。

調査表では、規定内容として次の項目があげられている。

- 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・訓練を実施すること
- 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・訓練を実施すること

また一般的な CP/CPS では、主な規定内容として次の項目もあげられている。

- 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こと

教育・訓練について具体的内容を CP/CPS に記載する必要はなく、教育・訓練の方針を記載するべきであると考えられる。通常時と変更が生じた時の教育・訓練を最低限必要なものとして実施概要を規定するのであれば、前述の項目のようなトレーニング方針を記載することで十分であると考えられる。

「5.3.3.トレーニング要求」記述案

JPNIC 認証局は、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］再トレーニング期間と手続き

CP/CPS 5.3.4 項では、JPNIC 認証局の要員に対する再トレーニングの周期、手続きに関する要件を規定する。

「5.3.4.再トレーニング期間と手続き」記述案

JPNIC は定期的に JPNIC 認証局の要員に対して再トレーニングを行う。また、必要に応じて適時再トレーニングを行う。

［5.3.5］ジョブローテーションの頻度と順序

CP/CPS 5.3.5 項では、各役割間でのジョブローテーションの頻度と順序に関する要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 業務運用及びセキュリティが損なわれないよう、職員の退職・解任時には適切な対応を行うこと

「5.3.5.ジョブローテーションの頻度と順序」記述案

JPNIC は、JPNIC 認証局運営が損なわれないよう職員の退職・解任に備えて適切な対策・対応を行う。

［5.3.6］認可されていない行為に対する制裁

CP/CPS 5.3.6 項では、認可されていない行為・認証局の使用・システムの使用についての職員に対する制裁要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 許可のない操作、許可のない認証局利用、許可のないシステム利用に対しては制裁規定に従って制裁を実施すること

一般的には CP/CPS 上に具体的な制裁規定が記載されることはなく、別途制裁規定に従って制裁が実施されることを、CP/CPS 上に規定していることが多い。

「5.3.6.認可されていない行為に対する制裁」記述案

JPNIC は、JPNIC 認証局の職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）に従って制裁を与える。

［5.3.7］契約要員に関する要件

CP/CPS 5.3.7 項では、委託契約を行う際の実施事項について規定する。

調査表では、規定内容として次の項目があげられている。

- 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委託者の指示の遵守及び責任分担、保証、違反時の罰則等について明確にすること
- 委託契約において、受託者と守秘義務契約を結ぶこと
- 受託者の業務が適切に行われているかどうかを監督し管理すること

JPNIC の規則上、外部と契約を行う場合に必要な手続き等が前述の項目以外にあるならば併せて規定することが良いと考えられる。

「5.3.7.契約要員に関する要件」記述案

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かどうかを監督し管理する。

［5.3.8］要員に提供されるべき文書

CP/CPS 5.3.8 項では、要員に提供されるべき文書に関する要件を規定する。

WebTrust では、規定内容として次の項目があげられている。

- 認証局運営組織によって決定した（CP/CPS、情報セキュリティポリシ、個人情報保護ポリシ、その他認証局の規定等）は全ての運用要員に開示し通知すること

JPNIC 認証局では、各要員に対して要員の役割に応じた義務やセキュリティポリシに関する文書を開示することは、CP/CPS に準拠した認証局運営を行うために必須であると考えられる。またその他、開示する必要があると考えられる文書があるならば併せて開示することが望ましいと思われる。

「5.3.8.要員に提供されるべき文書」記述案

JPNIC 認証局は次の文書を運用要員に開示し、周知する。

- CP/CPS
- 認証局運用に関する諸規程、手続き書、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
- （その他に決定された文書）

5.4.6. ［6］技術的なセキュリティ管理

5.4.6.1. ［6.1］鍵ペアの生成と実装

［6.1.1］鍵ペアの生成主体

各エンティティの鍵ペア生成を誰が行うのか等を記述する。次の項目について検討を行う。

- 誰が鍵ペアの生成を行うのか
- 作業は何人で行われるのか
- どのようなコントロールのもとで生成するのか
- 要件としてどのような基準（ISO 15782-1/FIPS 140-1 又は FIPS 140-2 レベル等）を採用するのか

通常、主に認証局の鍵ペアの生成について記述され、EE 等の鍵ペア生成については、認証局として一定の方法を要求する場合にのみ記述を行うのが一般的であると言える。本認証局では EE 鍵ペアは EE 自身に生成させ、また使用するクライアントアプリケーションを制限しないため、認証局の鍵ペアについてのみ記述する。

認証局の鍵ペア生成は、責任ある役割の者の立会いのもと、適切な権限の与えられた複数名の作業者によって、不正のなされないようなコントロール下で行われることが望ましい。また、高い信頼を得たい場合には、認証局鍵ペアの漏えい、複製等が行われないよう、FIPS 140-1 又は FIPS 140-2 レベル 3 認定若しくはそれ相当の暗号装置の使用が必要と考える。基準を明確に定めない、暗号装置を使用しない場合等においては、CP/CPS 上は誰が、どのように行うのかのコントロールのみを記述することでよいと考える。

本報告書の CP/CPS 記述案では、認証局の鍵ペア生成に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することを前提とし、要件とする標準については規定しないこととする。

「6.1.1.鍵ペアの生成主体」記述案

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、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。

［6.1.2］利用者への私有鍵の送付方法

利用者の鍵ペアを利用者自身で生成しない場合の私有鍵の受渡し方法についての検討を行う。利用者自身が鍵ペア生成を行う場合は規定しない。一般的な検討内容として、

- 私有鍵、証明書の受渡し方法（ダウンロード、私有鍵及び証明書の郵送、認証局窓口での手渡し等）
- 私有鍵利用のための PIN の受渡し方法（簡易書留、2 種類のコードの 2 系統配布等）

が考えられる。

本認証局では EE 鍵ペアの生成を行わず、ホストマスタの鍵ペアはホストマスタ自身が、サーバの鍵ペアは当該サーバの管理者が生成を行うため本項の規定は行わない。

「6.1.2.利用者への私有鍵の送付方法」記述案

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］認証局への利用者の公開鍵の送付方法

認証局へ利用者の公開鍵をどのような方法で送付するかを記述する。オフラインで送付する場合には、送付に使用する媒体、送付方法等を記述し、オンラインで送付する場合には通信の保護、改ざん防止の仕組み等を記述する。

運用組織への負荷の軽減、証明書発行までの時間的問題を考慮し、認証局システムによって提供される、オンラインによる署名付証明書発行要求の送付の仕組みを使用することが望ましいと考える。

「6.1.3.認証局への利用者の公開鍵の送付方法」記述案

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］利用者への認証局公開鍵の配布

認証局の証明書を利用者へ送付する方法や、改ざんを防止するための仕組み等を検討する。

- セキュアなプロトコルを使用して広く公開する

- オフラインで利用者への送付する
- Web ブラウザへの組み込み

等の方法が考えられる。

本認証局ではオンラインで公開する方法と、オフラインで配付する方法の 2 つの方法を用意し、EE に応じてどちらかより適切な方法を使用することとする。

また、オンラインにて公開する場合には、認証局の証明書フィンガープリントを異なるサーバ上に公開する等置換攻撃への対策を施す必要があると考える。

「6.1.4.利用者への認証局公開鍵の配布」記述案

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。

- 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。EE 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。EE 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。

［6.1.5］鍵のサイズ

使用する鍵のサイズに関する要件を記述する。

認証局の鍵ペアは RSA 公開鍵暗号方式の 2048 ビット、EE 鍵ペアは RSA 公開鍵暗号方式の 1024 ビットが一般的であると考えられ、またもっとも多くのアプリケーションで利用可能であると考える。

「6.1.5.鍵のサイズ」記述案

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］公開鍵パラメータの生成主体

公開鍵を生成するためのパラメータに関する要件を記述する。

通常、公開鍵パラメータの生成は鍵ペアの生成で使用する暗号装置若しくは安全性の高い暗号化モジュールを含むソフトウェアにより行われる。

今回の検討においては、鍵ペア生成に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するとしているので、本項の記述案においてもソフトウェアの使用を前提として記述する。

「6.1.6.公開鍵パラメータの生成主体」記述案

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 と呼ぶ）を用いて生成される。

［6.1.7］パラメータ品質の検査方法

公開鍵パラメータの品質チェックに関する要件を記述する。

鍵ペアの生成で使用する暗号装置がどのような規格に合致しているのかを記述することになる。

今回の検討においては、要件とする標準については規定しないものとしているので、本項は規定しないものとする。

「6.1.7.パラメータ品質の検査方法」記述案

規定しない。

［6.1.8］ハードウェア又はソフトウェアによる鍵ペア生成

鍵ペアがハードウェアで生成されるのか若しくはソフトウェアで生成されるかを記述する。

本項の内容は CP/CPS 6.1.1 項にて記述するものとする。

「6.1.8.ハードウェア又はソフトウェアによる鍵ペア生成」記述案

本 CP/CPS 6.1.1 項にて記述する。

［6.1.9］鍵の使用目的

鍵の利用目的や鍵の使用の制限について記述する。またそれらの利用目的が証明書の keyUsage 拡張にどのようにマップされているかを記述する。

「6.1.9.鍵の使用目的」記述案

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、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 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こと。

サーバ証明書の keyUsage は digitalSignature、keyEncipherment を使用する。SSL/TLS サーバ証明書としてのみ使用すること。

5.4.6.2. ［6.2］私有鍵の保護

［6.2.1］暗号化モジュールに関する標準

認証局で使用する暗号化モジュールに要求する標準について検討する。

暗号化モジュールに関する標準として、ISO 15782-1、FIPS 140-1 又は FIPS 140-2、ANSI X9.66 があげられる。

本認証局の私有鍵については、私有鍵の管理、安全性等を優先的に考慮する場合には、一般的に安全性が高いと言われている FIPS 140-1 又は FIPS 140-2 のレベル 3 以上の認定製品であるハードウェアセキュリティモジュール（以下、HSM と呼ぶ）の使用が妥当と考えられる。

本報告書の CP/CPS 記述案では、要件とする標準については規定しないこととする。

「6.2.1.暗号化モジュールに関する標準」記述案

規定しない。

［6.2.2］複数人による私有鍵の管理

認証局の私有鍵は一般的に厳重に管理するものとされており、どのように管理するかを記述する。

認証局の私有鍵の管理として、権限を複数に分散させ、複数人によって行うことが考えられる。また、権限を有する者のうち、事前に定める人数以上が揃わなければ私有鍵を取り出すことはできないものとすることも考えられる。

「6.2.2.複数人による私有鍵の管理」記述案

本認証局の私有鍵の管理は、複数の CAO に権限を付与し、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

認証局及び EE の私有鍵の第三者へのエスクローについて記述する。エスクローをする場合には、エスクローする機関、形態等について記述する。

一般的には認証局の私有鍵は認証局自身で厳重に管理されるものと考える。EE の私有鍵は、暗号用として使用される場合は、その用途から認証局におけるエスクローが必要な場合もあると考えられる。ただし、今回の検討においては、認証用として使用することを前提としていることから不要と考える。

なお、エスクローする場合は、次の主たる項目について十分に検討することが必要であると考えられる。

- エスクローする機関
- エスクローする形態（どのような保管をするか等）
- セキュリティ管理
- 責務
- 賠償責任

「6.2.3.私有鍵のエスクロー」記述案

本認証局の私有鍵を第三者に対して委託しない。

EE の私有鍵は EE 自身が生成及び管理する。

［6.2.4］私有鍵のバックアップ

認証局及び EE の私有鍵のバックアップについて、バックアップの方法、管理等について記述する。

障害等に備え、認証局の私有鍵のバックアップは必要と考える。災害等による施設への被害等も考慮し、認証局の私有鍵は稼動中の認証局システムが設置されている場所とは別地に保管することが望ましい。

認証局の私有鍵のバックアップは、複数人の操作を必要とし、鍵管理者の立会い及び複数の CAO による操作を行う必要があると思われる。

私有鍵を管理するソフトウェア若しくはハードウェアにより、バックアップ形態は依存すると考えられることから詳細は決定後記述されるものとする。

また、EE の私有鍵は EE 自身が生成及び管理を行うことから、認証局ではバックアップを行う必要はないと考えられる。

「6.2.4.私有鍵のバックアップ」記述案

本認証局私有鍵は、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。

また、そのバックアップは予め定める保管場所に保管される。

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

認証局及び EE の私有鍵について、アーカイブを行うか否かを記述する。

一般的には認証局の私有鍵のアーカイブは行われていないことが多いと思われる。

アーカイブを行う場合には、認証局の私有鍵はソフトウェア若しくはハードウェアで生成及び管理されることから、ソフトウェアの場合はアーカイブした記録媒体、ハードウェアの場合はそのハードウェアの管理を行うこととなると考えられる。

また、EE の私有鍵は EE 自身が生成及び管理を行うことから、認証局ではアーカイブを行う必要はないと考えられる。

「6.2.5.私有鍵のアーカイブ」記述案

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］暗号化モジュールへの私有鍵の格納

認証局及び EE の私有鍵の暗号化モジュールへの格納に関して記述する。

暗号化モジュールへの格納は、認証局の私有鍵を取り扱うことのできる権限を付与された者が複数で行うことが必要と考える。

EE の私有鍵は EE 自身が鍵ペアの生成を行うため、EE 自身が格納を行うものと考えられる。

「6.2.6.暗号化モジュールへの私有鍵の格納」記述案

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そのモジュールに介入することはない。

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。

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］私有鍵の活性化方法

認証局の私有鍵の活性化に関して記述する。

認証局の私有鍵を利用可能状態にする操作は、複数人で行うことが必要と思われる。

「6.2.7.私有鍵の活性化方法」記述案

本認証局の活性化は、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。

［6.2.8］私有鍵の非活性化方法

認証局の私有鍵の非活性化に関して記述する。

認証局の私有鍵を利用不可能状態にする操作は、複数人で行うことが必要と思われる。

「6.2.8.私有鍵の非活性化方法」記述案

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。

［6.2.9］私有鍵の破棄方法

認証局及び EE の私有鍵の破棄方法に関して記述する。

認証局の私有鍵の使用終了時には、物理的な破壊、完全な初期化等を行うことが必要と考えられる。その操作は［6.2.7］と同様に複数人によって行われ、私有鍵が復元できないことを確認する。バックアップ、アーカイブを行った私有鍵についても同様な操作が必要と思われる。

EE の私有鍵は、EE 自身で確実に破棄することが必要と考える。

「6.2.9.私有鍵の破棄方法」記述案

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きによって破棄する。

EE の私有鍵は、EE 自身で確実に破棄するものとする。

5.4.6.3. ［6.3］鍵ペア管理に関するその他の面

［6.3.1］公開鍵の保存

公開鍵の保存が必要かどうか、またどのように公開鍵の有効性を確保するかを検討する。

検証者による署名検証の可用性を確保するためには、公開鍵のアーカイブを行うことが必要である。また公開鍵の有効性を確保するため、アーカイブは暗号化し改ざん防止措置をとることが望ましい。

「6.3.1.公開鍵の保存」記述案

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。

［6.3.2］私有鍵と公開鍵の有効期間

私有鍵、公開鍵の使用可能期限について検討する。

私有鍵については、暗号化された文書の復号を行うため、有効期間を規定しないことが一般的である。

公開鍵については、有効期間の短いほうがより安全性が高いと言われているが、暗号解読技術の進展等を踏まえた変更が必要になると思われる。

「6.3.2.私有鍵と公開鍵の有効期間」記述案

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。

5.4.6.4. ［6.4］活性化データ

［6.4.1］活性化データの生成と組み込み

暗号化モジュールの起動時に要求される活性化用データについて記述する。

暗号化モジュールの起動時に要求される活性化用データを保護する方法として、パスワードや PIN を使用することが考えられる。

パスワードや PIN に用いる文字及びその長さは、容易に推測できてはならず、十分な長さを使用することで推測を困難なものにすることが可能と考える。

使用する文字は、英大文字、英小文字、数字を全て含むこととし、8 文字以上の長さが妥当であると思われる。

「6.4.1.活性化データの生成と組み込み」記述案

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 文字以上の長さを使用する。

［6.4.2］活性化データの保護

暗号化モジュールの活性化データの保護について記述する。

使用するパスワードや PIN を長期間同一のものを使用することは、悪意のある第三者に対して推測する時間を与えるだけであり、解読されてしまう危険性がともなうことが考えられる。

パスワードや PIN を定期的に変更することが必要と考える。

また、パスワードや PIN の管理及び変更は、事前に権限を付与された者が行う必要があると考える。

「6.4.2.活性化データの保護」記述案

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。

5.4.6.5. ［6.5］コンピュータのセキュリティ管理

［6.5.1］信頼されるコンピューティング基本コンセプト

システムのセキュリティに関する要件及びその対策を記述する。

記述する内容として、

- OS の要塞化
- アクセスコントロール
- パスワードの管理方法
- リソースの常時監視

等が考えられる。

具体的な対策については、実際のシステム構成や使用する OS、ソフトウェアが決定した後に詳細な検討を行わなければならない。記述案では、一般的にどういった項目について対策をとるのかについて記述する。

「6.5.1.信頼されるコンピューティング基本コンセプト」記述案

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われるものとする。システムに対して行われた重要な操作は、全てログが残るよう設定されている。システム

にアクセスするためのパスワードは、全て適切な管理が行われる。本認証局のサーバシステムは、常時リソース監視が行われ、システムの異常や不正運用を検知し、速やかに適切な対策が行われる。

［6.5.2］コンピュータセキュリティ評価

使用するハードウェア、ソフトウェア及び CP/CPS 6.5.1 項で記述している対策への評価をどのように行うのか検討する。また評価に使用する基準があれば、その基準について記述を行う。

記述内容として、

- クラッキングテスト等を行う
- ISO/IEC15408-3:1999 の EAL4 等の認定を取った製品を使用する

等が考えられる。

具体的な内容については、実際に使用するハードウェア、ソフトウェアを検討する際に採用した基準や運用テストについて記述を行うことが望ましい。

「6.5.2.コンピュータセキュリティ評価」記述案

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。

5.4.6.6. ［6.6］ライフサイクルのセキュリティ管理

［6.6.1］システム開発管理

システム開発時における管理について記述する。

システム開発管理においては、一般的なシステム開発時における管理（セキュリティも含む)、成果物のレビュー、導入時の受け入れ試験等を実施し、障害発生率を抑えるとともにセキュリティを保つ必要があると考えられる。

「6.6.1.システム開発管理」記述案

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］セキュリティ管理統制

セキュリティ運用管理に関して記述する。

国際標準規格である「ISO/IEC 17799:2000（JIS X 5080:2002）」、「ISMS」、経済産業省が推進している「情報セキュリティ管理基準」を参考に、システム開発時にはセキュリティを十分に配慮した管理が必要であると思われる。

検討項目として必要があると考えられるものを次に記す。

- 入退室管理、要員管理（教育を含む）、権限管理等の運用管理の実施及び運用改善
- 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の改善等の実施

「6.6.2.セキュリティ管理統制」記述案

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の実施を行うものとする。

［6.6.3］ライフサイクル評価

［6.6.1］、［6.6.2］で記述した管理について、評価を行う。評価結果をもとに分析を行い、管理方法を見直すことも必要である。

また、導入を行ったシステムに関して、最新のセキュリティ上における脆弱性等の情報収集を行い、最新の動向を考慮したシステムへの評価、改善を行うことが必要と考えられる。

「6.6.3.ライフサイクル評価」記述案

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、改善を行う。

5.4.6.7. ［6.7］ネットワークのセキュリティ管理

ネットワークセキュリティを確保するための対策について記述する。

検討内容としては、

- 利用可能なプロトコルの制限
- ファイアウォールや IDS（Intrusion Detection System）の導入
- ネットワークアタックテストの実施

等が考えられる。

具体的な対策については、実際のネットワーク構成や使用する機器等が決まった後に詳細な検討を行わなければならない。記述案では、一般的にどういった項目について対策をとるのかについて記述する。

「6.7.ネットワークのセキュリティ管理」記述案

本認証局の存在するネットワーク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は必要最低限のプロトコルに制限され、またアクセス可能なホストも限定される。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

5.4.6.8. ［6.8］暗号化モジュールの技術管理

［6.2］と同様であるため、省略する。

5.4.7. ［7］証明書と失効リストのプロファイル

CP/CPS 7 章では、その CP/CPS に従って発行される証明書及び CRL のフォーマット、拡張領域を含む各領域の値について記述する。

証明書及び CRL のプロファイルを検討するうえで、次の項目を前提とした。

- ホストマスタ証明書は S/MIME 及び SSL/TLS、サーバ証明書は SSL/TLS で使用される。
- 可能な限り多くのアプリケーションで使用できるよう、シンプルなプロファイルにする。あるアプリケーションでは使用できないことが判明している拡張領域や値がある場合には極力使用せず、使用する場合には non-critical とする。
- 本認証局が発行する証明書だけでなく、JPNIC ルート認証局が発行する証明書のプロファイルも同時に策定する。
- 可能な限り RFC3280 準拠とする。

また、次の 2 項目については、個別に検討を行った。

- certificatePolicies 拡張の使用について
- 証明書中の DirectoryString のエンコードについて

certificatePolicies 拡張について、RFC3280 準拠とすると critical でなければならないが、一部アプリケーションではこの拡張を解釈できずに証明書の検証に失敗してしまうものがあるため、non-critical で発行することとした。

また、もし証明書ポリシのない PKI ドメインと相互認証を行うことになった場合には、有効なポリシツリーが辿れなくなるおそれがあるため、相互認証相手のドメインより発行される相互認証証明書中の policyIdentifier の値として anyPolicy を入れて発行してもらう等、相互認証証明書のプロファイルについて調整を行わなければならないと思われる。

DirectoryString のエンコードについて、 RFC3280 には「2003 年 12 月 31 日より後に発行する証明書中の DirectoryString は UTF8String でエンコードしなければならない」と記述されているが、PKI で使用する際のエンコードの異なる DirectoryString の一致規則が明確化されておらず、また一部のアプリケーションでは DN が UTF8String でエンコードされている証明書が使用できない等の理由から、DirectoryString のエンコードには PrintableString を使用することとした。実際、第 58 回 IETF ミーティングにおいても UTF8String の導入は先送りされることとなり、PKIX WG にて UTF8String を使用した際の一致規則について仕様を策定することに

なっている。

表 5-9、表 5-10 に本認証局が発行する証明書及び CRL のプロファイル案を記す。

表 5-9　JPNIC IP アドレス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	c		
digitalSignature		1	1
nonRepudiation		0	0
keyEncipherment		1	1
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

表 5-10　JPNIC IP アドレス認証局が発行する 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

また、本認証局の CP/CPS には記載されない JPNIC ルート認証局が発行する証明書及び CRL のプロファイル案を表 5-11、表 5-12、表 5-13 に記す。

表 5-11　JPNIC IP アドレス認証局の証明書と JPNIC ルート認証局の証明書プロファイル

Field	critical flag	JPNIC IPアドレス認証局 証明書	JPNIC ルート認証局 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*4	PrintableString*4
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		notBeforeの時刻より10年後	notBeforeの時刻より20年後
subject	NA		
		PrintableString*1	PrintableString*4
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		JPNIC IPアドレス認証局 公開鍵のBIT STRING	JPNIC ルート認証局 公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 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	JPNIC IPアドレス認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		本CPのOID	使用しない
policyQualifiers			
policyQualifierId		CPSUri	使用しない
qualifier		本CP/CPSを公開するURI	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	使用しない
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

表 5-12　JPNIC ルート認証局リンク証明書プロファイル

Field	critical flag	JPNIC IPルート認証局リンク証明書OldwithNew	JPNIC ルート認証局リンク証明書NewwithOld
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString*4	PrintableString*4
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime 古い自己署名証明書の notAfter	UTCTime 古い自己署名証明書の notAfter
subject	NA		
		PrintableString*4	PrintableString*4
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		古いJPNIC ルート認証局公開鍵のBIT STRING	新しいJPNIC ルート認証局
authorityKeyIdentifier	n		
keyIdentifier		新しいJPNIC ルート認証局 公開鍵の160bit	古いJPNIC ルート認証局 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	古いJPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	新しいJPNIC ルート認証局 公開鍵の160bit
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		anyPolicy	anyPolicy
policyQualifiers			
policyQualifierId		使用しない	使用しない
qualifier		使用しない	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	JPNIC ルート認証局が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

表 5-13　JPNIC ルート認証局が発行する 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[*4]
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより1年後
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 ルート認証局 公開鍵の160bit SHA-1ハッシュ値

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

※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）

※3　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, OU=Resource Management System, CN=（証明書発行対象サーバの FQDN）

※ 4　C=JP, O=Japan Network Information Center, OU=JPNIC Root Certification Authority

5.4.8. ［8］仕様の管理

5.4.8.1. ［8.1］改訂手続き

CP/CPS の 8.1 節では、CP/CPS の改訂に関する手続きを記述することとなる。

検討項目として、

- どのようなときに改訂を行うのか
- 大幅な仕様変更時の扱い
- 改訂に関する関係者の合意
- 改訂にともなう関係機関に確認承認が必要な場合の手続き

について検討を行う。

どのようなときに行うのかについては、認証局の運用、手続きの変更等において、CP/CPS の改訂の最終承認を行う運営委員会が証明書ポリシ及びその履行の保証に著しく影響を与えないと判断した場合に、CP/CPS の改訂を行うものと考えられる。

証明書ポリシ及びその履行の保証、利用者の義務に変更が行われ、証明書を利用する者、検証する者に著しく影響を与える変更等の大幅な仕様変更時の扱いとしては、本来、同一の証明書ポリシでよいのかという検討が必要になる。CP/CPS の最終承認組織である運営委員会は、前述の検討を行ったうえで、CP/CPS の改訂承認、若しくは別の証明書ポリシの策定を指示することが望まれる。

改訂に関する関係者の合意については、改訂が有効になるまでの間に関係者より申出がない場合は合意が得られたと解釈する場合が一般的と思われる。合意が得られず、関係者より申出があった場合の対応であるが、本認証局の場合、LRA との契約を前提としており、本考察では一般的な記述にとどめ、契約関係が明確になった時点で変更を行うものとする。

改訂にともなう関係機関に対する、確認又は承認が必要な場合の手続きについては、今回の JPNIC 認証局は特別な関係機関からの認定等を想定していないので、関係機関に対する確認、承認依頼は不要であると考える。

「8.1.改訂手続き」記述案

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 CP/CPS 変更の必要性が生じた場合、利用者又は検証者に事前の承諾なしに、随時 CP/CPS の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利用を中止するものとする。

5.4.8.2. ［8.2］公表と通知の手続き

CP/CPS の 8.2 節では、CP/CPS の公表と通知に関する手続きを記述することとなる。

検討項目として、

- 公表、通知の時期、公表頻度
- 公表、通知の方法（公表先、公表場所、通知方法等）
- 変更履歴を公表するか否か

について検討を行う。

公表、通知の時期については、関係者の確認期間を考慮し、その改訂が有効になる一定期間以前に公表、通知が必要と思われる。また公表頻度は常時公表とするのが一般的である。

公表の方法については、認証局のホームページ及びリポジトリへの開示が一般的と考えられる。

通知の方法については、利用者への通知方法を定めている場合はその方法により行うこととなると思われるが、通知業務の負荷等を考え特段の通知方法を定めない場合、ホームページ等への公表をもって通知とすることも一般的な記述として考えられる。

公表先については、証明書の適用範囲を限定している証明書の利用の場合は広く一般には公開せず、証明書の利用者及び関係者等に限定して開示する場合がある。本認証局においても、IP レジストリ業務における利用を前提としており、公表先を一部に限定することも考えられるが、適用範囲外の者からの問い合わせ等を考慮し、広く一般に公開を行うものとする。

変更履歴の公表については、最新の CP/CPS 及び変更履歴についての公表を行うことが一般的であり、変更履歴についても公表を行うものとする。

「8.2.公表と通知の手続き」記述案

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、変更履歴とともに本認証局ホームページに掲載することにより、利用者及び関係者に改訂の通知を行うものとする。

5.4.8.3. ［8.3］承認手続き

CP/CPS の 8.3 節では、CP/CPS の承認に関する手続きを記述することとなる。

一般的な CP/CPS においては、どのような承認が行われるのかが記述される。また、関係者との合意についての記述がなされる場合がある。本報告書では、関係者との合意については、本報告書 5.4.8.1.にて記述しているので、承認者又は承認機関についての記述のみとする。

「8.3.承認手続き」記述案

本規定の改訂は、社団法人日本インターネットインフォメーションセンターの認証業務に関する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。

5.5. RFC3647 との相違点及び追加検討事項

5.5.1. RFC2527 と RFC3647 の相違点の概要

新しい CP/CPS のフレームワークである RFC3647 は、RFC2527 においてわかりにくかった説明や内容的に重複している項目に対して補足説明及び整理統合が行われ利用しやすいものとなっている。RFC3647 は RFC2527 に比べ構成の変更及び若干の項目追加が行われているが、記述すべき項目及び内容において、RFC2527 との著しい変更は行われていない。RFC2527 に比べ CP/CPS を検討する者にとって評価できる内容となっていると思われる。

RFC3647 において追加されている項目については、「5.5.2.RFC3647 にて追加された項目及び記述方針」にて述べるものとする。

5.5.2. RFC3647 にて追加された項目及び記述方針

（1） RFC3647　1.3.5 その他関係者

本認証局では、証明書一括発行期間、リポジトリサービス等外部組織の利用を想定しておらず、規定しないと記述するものとする。

（2） RFC3647　1.6.定義と略語

本検討上、RFC2527 のフレームワークにおいても、定義と略語は必要と考え RFC2527 の章構成の 1.5 節に追加記述している。

（3） RFC3647　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

証明書の使用者等からの失効申請に対し、認証局が失効を完了させなければならな

い期間の記述をすることとなる。

完了する期間の定めは、休日、夜間の対応等認証局の運用体制に大きく影響するため、実際の認証局の運用体制が定まってから再度検討する必要がある。若しくは、運用によらずシステム的に自動化する等の対応の検討が必要となる。本項については継続的に検討を行うものとし、当初の記述方針とし、

- 証明書の使用者が申請した時点からの完了期間ではなく、申請確認を行った後、完了するまでの期間を記述する
- 完了期間は、速やかに実施するという表現にとどめる

こととする。

（4） RFC3647　4.11.加入の終了

ここでは、加入者が認証局のサービスの登録を終了する場合の手続きを定める。

検討点として、サービスの利用終了と証明書の関係を明確にする。

本認証局で発行する証明書は IP アドレスの管理に関する各種申請業務に使用することを前提にしており、本認証局のサービスの加入者は IP アドレス管理指定事業者となる。IP アドレス管理指定事業者が本認証局のサービスの登録を終了するということは、JPNIC に対する IP アドレスの管理に関する各種申請業務を終了するということになり、継続的に証明書を使用する必要性がなくなる。ゆえに、加入者が本認証局のサービスの利用登録を終了する場合は、加入者に対して発行した証明書を全て失効する旨の内容を記述方針とする。

（5） RFC3647　6.8.タイムスタンプ

タイムスタンプに関する検討は、本報告書の 5.4.4.6.の RFC2527 の文書構成上の「4.6.5.記録に対するタイムスタンプを付ける要件」において記述している。

（6） RFC3647　7.3.1.OCSP プロファイル、7.3.2.OCSP バージョン、7.3.3.OCSP 拡張

OCSP サーバ等を利用する場合、プロファイル、プロトコルのバージョン、拡張の内容を記述する箇所であるが、本認証局では OCSP によるサービスを提供しないこととしているので、記述方針としては、各項目に「OCSP は使用しない。」若しくは「規定しない。」と記述するものとする。

（7） RFC3647　9.4.1.プライバシポリシ

ここでは、関係者の活動に適用されるプライバシポリシの明示及び公開を記述することとなる。

RFC3647 上ではプライバシプランとなっているが、プライバシポリシとして記述する。

JPNIC においては、プライバシポリシをホームページ上で公開しており、JPNIC が扱う個人情報をプライバシポリシの対象としている。本認証局において、この公開されているプライバシポリシを適用するのか、公開されているプライバシポリシを改訂の上使用するのか、新たに認証局のサービスにおけるプライバシポリシを作成するのか等の JPNIC 全体での検討が必要となる。

今回の検討においては、個人情報保護の高まりを考慮し、RFC2527 の追加事項として、RFC2527 の文書構成上の 2.10 節に記述を行っている。

（8） RFC3647　9.4.5.個人情報の使用に関する個人への通知及び承諾

（7）の検討と同様。

（9） RFC3647　9.6.5.他の関係者の表明保証

（1）の検討と同様。

（10） RFC3647　9.10.1.有効期間

ここでは、CP/CPS、契約書、協定等の文書の有効期間について記述することができる。

RFC3647 の説明自体曖昧な感があるが、各種文書は正当な承認手続きにて発行され、正当な承認手続きにて改訂されるまでの間、有効である旨の表記になると考えられる。

（11） RFC3647　9.10.2.終了

ここでは、CP/CPS、契約書、協定等の文書の全部又は一部、若しくは特定の関係者に対して有効でなくなる場合について記述することができる。

RFC3647 の説明自体曖昧な感があるが、各種文書の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、その該当部分についてのみ終了の効果が及ぶといった旨の表記をするものと考えられる。この項においては、「9.10.3.終了の

効果と効果継続」と重複感があり、記述内容について、再度調査を行うものとする。

（12） RFC3647　9.16.2.権利譲渡条項

ここでは、相手方当事者との契約等に基づく自己の権利の譲渡や義務の履行の委任についての制限等を記述することができる。

現時点では各種関係者との契約的な協議は行われておらず、継続検討課題とする。

（13） RFC3647　9.17.その他の条項

ここでは、RFC3647 のフレームワークにあてはまらない追加的な責任等を記述することができる。

この項は、RFC3647 のフレームワーク以外で、特に記述しておきたい事項の記述となるが、現時点では各種関係者との契約的な協議は行われておらず、継続検討課題とする。

第6章 認証局ソフトウェアの要件検討

内容

- 機能分離の実現
- 権限分離の実現
- ユーザ環境の対応状況
- 業務システムとの連携

6. 認証局ソフトウェアの要件検討

6.1. はじめに

本調査研究の一環として認証局の検討を行うにあたり、運用とシステムの両面の検討を行うことに留意した。これは安全性の確保を目的としたシステムは、SI ベンダに構築の一切を任せるような手法が向いていないと考えたためである。例えば、戦国時代に活動拠点となる城を構築することを考える。運用を行う主体が、敵の侵入を遅くする、跳ね上げ橋や入り組んだ道路といった基本的な知識を持たずに、城を持つことは危険ではないだろうか。運用者が、設計者のいう通りに構築をして、城を維持し敵から身を守ることができるだろうか。また、城は防衛と同時に活動拠点でもあるため、城を守る武士は何名いるのか、何を目的とする城なのかといった要件を意識して構築しなければならない。認証局の構築においても、構築を人任せにすることで運用レベルが想定していたものと著しく異なるか、非現実的な運用コストを発生させてしまう恐れがある。

そこで本調査研究では、認証局のシステムの根幹である認証局ソフトウェアに関して、国内外のベンダ 6 社に協力を依頼し、評価・検討を行った。認証局ソフトウェアを実際に試験導入することで、そのソフトウェアが想定している環境や運用形態を理解するためである。その結果判明してきたことは、価格とともに、利用形態、想定する環境などがソフトウェアごとに様々だということである。価格が高い製品であれば適用可能性が広がるかといえば、そうではない。逆に自社の環境に適合する製品を導入すれば、開発部分を最小化させ、場合によっては設定変更だけで導入が可能になる場合があると考えられる。

本章では、認証局ソフトウェアがどのような運用や環境を想定しているのか、認証局ソフトウェアを選ぶ際のポイント、また運用の想定のために検討しておくべき点について、下記の項目に重点をおいて述べる。

- 機能分離の実現
- 権限分離の実現
- ユーザ環境の対応状況
- 業務システムとの連携

特に二番目の権限分離の実現は、安全な認証局の重点だと考えられるため、JPNIC における検討方法をまじえて説明する。また PKI の適切な普及を考えた場合に、業務システムとの連携は認証局ソフトウェアにとっての課題だと考えられるため、考察事項を交えて述べる。

また本章の最後に、一部のソフトウェアベンダに対して回答を依頼した質問表を掲載する。この質問表は CP/CPS 策定の際に作成した業務モデルを元に、ソフトウェアの構成要素ごとの質問を集めたものである。評価に先立ってこのような質問表を用意したことで、ソフトウェアの概要把握に役立った。

6.2. 機能分離の実現

認証局ソフトウェアにおける機能分離とは、概念的な認証局の機能をシステムの中で分離させることである。概念的な機能は、ITU-T の X.509 や IETF の RFC3280 における定義に加えて、慣例的な概念も使われている。

認証局の機能を分別していくとそれぞれの機能に要される安全性の要素が異なることがわかる(表 6-1)。

表 6-1 認証局の概念上の機能

機能体	役割	安全性の要素
RA	EE の登録と発行申請を受け付ける。	申請者の本人性(個人とは限らない)や申請内容に対する適切な方針の適用が要求される。受け付け機能のサービルレベルに影響する。
IA	RA によって受け付けられた発行申請を受け取り、適切なフィールドを持つ証明書の発行を行う。狭義に CA と呼ばれることがある。	恣意性を排除して証明書発行のポリシに従うことが要求される。秘密鍵の保護を担う。
PA	証明書や CRL を公開する。リポジトリとも呼ばれる。検証者や公開鍵を得ようとする EE の要求に応じて動作する。	サービスレベルに応じた公開機能の維持が要求される。CRL の配布が遅れると、失効情報の伝達が遅れ、無効な証明書を無効だと判断できない恐れがある。
VA	検証者の要求に応じて証明書の有効性を判定する。	サービスレベルに応じた検証機能の維持が要求される。検証結果に署名を行うため、鍵の管理等が必要となり、PA よりもサービスレベルの向上を図りにくい。

簡略に書くと、RA は要求をきちんと受け付けることができるか、IA は認証局の信頼に足る発行を行うことができるか、PA と VA はサービスを維持し続けることができるかといった要件を持つ、ということになる。

これらの機能の分離が、運用を検討している認証局にどこまで必要であるのかを決定する必要がある。機能の分離によって、RA は受け付け業務に専念し、IA は鍵の保護に専念するといった、保護機能の専門化を行うことができる。例えば IA はハードウェアセキュリティモジュール（以下、HSM と呼ぶ）のような特殊な機器を使って鍵を保護し、暗号鍵の漏洩やそれによる不慮の証明書発行が起こらないようにする。

一方、機能を分離しないことで生まれるメリットもある。管理の容易さ・管理人員の削減・機器の維持にかかる費用の削減といったものである。社内利用のように閉じた環境で認証局を運用したり、迅速な発行処理が必要とされたりする場合に有効である。

商用認証局ソフトウェアのうち、比較的高価なものはより細かい機能の分離を実現することが出来る。逆に比較的安価なソフトウェアは機能が一体化しているという傾向がある。

6.2.1. 機能分離の影響

認証局ソフトウェアの検討にあたり、機能分離は運用と技術の面で下記の二つの点に影響する。

- 機能を機器(または仮想的なクライアント)ごとに分離しているかどうか
- 機能間の通信プロトコルに何を利用しているか

6.2.1.1. 機能の機器ごとの分離

「機能の機器ごとの分離」は、認証局ソフトウェアの運用に影響する。運用形態を分類すると表 6-2 のようになる。

表 6-2 認証局ソフトウェア運用形態の分類

運用形態	概要
一体型	認証局が持つ全ての機能を単一のソフトウェアや機器で実現するもの。
RA-CA 型	EE の登録管理を RA で行い、特殊で高価な機器を利用する CA を分離するタイプ。
RA-IA-PA 型	RA-CA 型に加えて PA(リポジトリ)を別途に管理するタイプである。
RA-IA-PA-VA 型	VA を設けて、失効情報の伝達遅延を短縮させたり、利用者端末の単純化を図ったりしたものである。

一体型では、発行する証明書の種類の変更や証明書の状態管理に関して小回りが利く運用が可能である。技術的に複雑な設定や開発を行う必要がある場合には、一体型が向いている場合が多い。一方、登録業務と発行業務の分離といった、安全性のレベルを上げる運用には向かない。発行対象に関する情報管理や利用者ごとの発行要求の管理は別のソフトウェアで行うような場合に向いている。

次に機器の分離の型と特徴を述べる。

- RA-CA 型
  RA-CA 型では、登録管理業務を一般のオフィスで行い、HSM を利用した CA をセキュアデータセンターで管理する、といった運用形態である。
  認証局の運用を EE の登録管理であると捉え、IA や PA といった運用要件の厳しい機能を専門業者に委託するような場合にも該当すると考えられる。
  ソフトウェアの中には単一の RA で複数の CA に接続することができ、少数の管理者が複数の認証局を管理することができるものがある。

- RA-IA-PA 型
  RA-IA-PA 型では、リポジトリを別途管理することで、利用者のメンバ管理に PA を用いることができる。商用認証局ソフトウェアの典型的な型である。PA で LDAP を利用し、証明書以外の情報も一緒に管理することで社員名簿や連絡簿、社内システムのユーザデータベースとして応用することが考えられる。
  PA の運用は可用性(availability)の確保が重要である。特に失効処理の遅延に影響する。しかし、実際の運用の場では運用者の主体的な可用性の確保よりも現実的な検討が行われることが多い。つまり利用者に対して提示したサービスレベルを如何に適切なコストで維持するか、という検討方法である。このことは、次の RA-IA-PA-VA 型にも当てはまる。

- RA-IA-PA-VA 型
  RA-IA-PA-VA 型は、証明書の検証者が複雑な検証処理を行わずに、VA に任せる場合に使われる。商用認証局ソフトウェアに VA が付属していることは少なく、他製品の購入が必要なることが多い。しかし大量の証明書を発行するような大規模な運用の場面では、VA を設けるよりも PA を使った CRL の配布の方がサービス停止を避けやすく、かつ失効情報の伝達遅延が短いことがある。
  証明書検証を一手に担う VA は、求められるサービスレベルが高くなりがちである。例えば証明書検証者が 24 時間 365 日アクセス可能なサーバを用意することは容易ではない。

機器の機能ごとの分離に関する要件検討のポイントは、まず要求されるサービスレベルから認証局の型を想定し、その型で運用が可能な認証局ソフトウェアを利用することである。

6.2.1.2. 機能間の通信プロトコルの採用方法

後者の「機能間の通信プロトコルの採用方法」は、それぞれの機能がどのようなプロトコルを使って通信を行うか、という点である。

RA-IA 間でどのようなプロトコルが使われているのか、PA はどのプロトコルを利

用可能か、といったことを事前に調べておくことは、業務に合わせた認証局ソフトウェアを採用する際に有効である。

RA-IA が標準的なプロトコルを用いていると、RA に機能を付加して社内システムと連携するような開発を行うことが比較的容易にできる。RA-IA 間で使われる代表的なプロトコルに CMP(Certificate Management Protocol)がある。CMP のように、証明書の管理に適したプロトコルが利用できると RA 端末の開発が行いやすい。証明書のバルク発行のために、RA 端末プログラムが開発されていることがある。商用認証局ソフトウェアでは CMP が利用されることが多い。

PA は一般的に LDAP を用いることが多い。PA で LDAP のような標準化されたプロトコルを用いることで、オープンソフトウェアの利用など、ソフトウェアの選択の幅ができる。LDAP の他に HTTP や FTP などが利用されることもある。一方、LDAP でデータの格納に使われるオブジェクトクラスは、ベンダごとに違いがあることがある。オブジェクトクラスとは、一塊のデータが持つ値の種類を定義したものである。LDAP ではアクセスする際にオブジェクトクラスを指定して検索やデータの格納を行うため、プログラム間で共通したオブジェクトクラスを想定していないと、データの交換ができない。利用者のエントリ person 等についてはソフトウェア毎に共通している事が多い。

Web ブラウザやメールソフトの中には、電話帳のような共有データベースのために LDAP を使うことがある。Web ブラウザなどのクライアントプログラムから PA へのアクセスがある場合には、クライアントプログラムがどのようなオブジェクトクラスを想定しているのか、調査しておく必要がある。

機能間の通信プロトコルに関する要件検討のポイントは、まず RA システムや証明書発行システムの開発を行う必要があるかどうかを決めることである。開発の必要がない場合にはあまり重点をおいて検討を行う必要はない。証明書発行システムや RA にある程度の機能を実装する必要がある場合には、標準的なプロトコルを採用していて、かつその開発環境を用意できることが望ましい。

6.3. 権限分離の実現

認証局ソフトウェアの中には、証明書の管理するための権限や、認証局のシステム管理のための権限といった、権限分離の仕組みを実装しているものがある。例えば認証局のシステム管理の権限ではシステムの起動や終了等の操作しか行うことができず、証明書の発行ができない。逆に証明書の発行を承認する権限だけでは、他の操作、例えば認証局の設定が行えないなどである。変更同一内容の権限でも、複数のオペレータが揃わないと操作できない、といった合議制操作のための権限を実現したものもある。

権限の分離によって、不正の抑止／防止といった認証局の運用レベルの向上を図ることができるが、管理に要する人員が増えるなどのデメリットがある。認証局ソフトウェアがどのような権限分離に対応しているのか、それが必要十分であるかを予め調べておくことが有効である。いくつかの認証局ソフトウェアが実装している操作の権限分離機構では、下記のような役割が存在している。

- **システムの起動と終了**

  認証局システムの起動に必要な権限と、証明書の操作に必要な権限とが異なっているようなケースである。RA と PA などのサーバ毎に異なるパスワードを設定することができるものもあり、実質的に管理の分担を行うことが可能である。

- **RA 業務**

  証明書の発行や失効など、RA 業務を行う権限が設けられるケースである。

  単一の RA 端末で複数の RA 業務を行うことができるソフトウェアの場合、RA サーバが RA 端末の接続時に認証と権限の確認が行われる。

  複数の認証局の RA 業務を、単一の部署で担当し、その代わりに IA の鍵の保護をセキュアデータセンターで行うといったことが可能である。

- **監査**

  記録の監査のみを行うことができる権限が設けられるケースである。

  監査権限だけでは、RA 業務も認証局システムの設定変更を行うこともできない。認証業務の外部監査を受ける場合などに、監査人に対して監査権限のみを与えるといったことが可能である。

- **バックアップ**

  認証局の運用に関連するファイルのバックアップのみを行うことができる権限が設けられているケースである。

  バックアップの権限だけでは、RA 業務やシステムの起動や終了を行うことができない。データの遠隔地保管を行う場合など、認証業務の担当とは異なる部署でデータを

扱う必要があるときに有効である。

これらの機能の中で、運用を検討している認証局が必要としているものは何かという検討が必要である。操作の機能分離は、認証局ソフトウェアの基本的な設計方針に依存している場合が多く、特殊な役割を増やしたり操作を単純化する変更を行ったりすることは難しい。

権限分離の機能を利用するには、ソフトウェアの設定を行う前に、実際の担当者の役割を決めておく必要がある。本調査研究では下記のような手順で担当者の役割を検討した。

1. **運用レベルを決める**

   自然人の認証を可能にする認証局なのか、Web を使った商取引に利用する認証局なのか、社内で利用するローカルな認証局なのか、といった運用のレベルを決める。

   運用レベルの検討には、2002 年度の「IP アドレス認証局のあり方に関する調査研究報告書」の第 4 章が参考になる。WebTrust for CA、ECOM の認証局運用ガイドライン、特定認証業務のガイドラインを RFC2457 の目次に揃えて比較している。

2. **役割を列挙する**

   運用責任者、鍵管理者、オペレータ、監査者などの役割を列挙する。過度に詳細な役割を設けると、業務負荷が増大するだけでなく、担当者が自分の役割を忘れてしまうことがある。

   認証業務の運用にどのような役割があるかは、本報告書の第 5 章が参考になる。

   認証局ソフトウェアが規定値として設定している役割を参考にすることは有効な方法である。

3. **兼務の可能性を検討する**

   兼務ができない排他的な役割は存在するが、兼務を検討することでトレーニングコストを下げたり役割を自覚できたりするような円滑な運用を図ることができる。

   担当する部署の、具体的な人員を当てはめると検討しやすい。

   JPNIC において検討した、構成人数や兼務の可能性については本報告書の第 5 章で述べた。

4. **担当者の役割と操作体制を決定する**

   各担当者に割り当てられた役割に応じて、認証局ソフトウェアの操作の体制を決める。決定された体制に従って、権限を持つユーザをそれぞれ登録する。

以上の手法はあらゆる場面で適用可能であるとは考えにくいが、認証業務を始めるにあたって業務配分の際に参考になるものではないかと考える。

権限分離の実現に関する要件検討のポイントは、認証局の運用レベルよって異なっている。比較的高い安全性を要求される認証局の場合は、まず前述したような方法で運用体制を想定しておき、その体制を実現できるソフトウェアを利用する。限定的な発行対象しか持たない認証局の場合は、むしろ認証局ソフトウェアで実現可能な権限の分離方法を調査した方が早い。認証局ソフトウェアの中には、OS の機能等を利用してより細かい操作の権限分離ができるものがあるためである。

6.4. ユーザ環境の対応状況

高価な認証局ソフトウェアを使って発行した証明書でも、ユーザ環境で効果的に利用できなければ意味がない。想定しているユーザ環境で利用できる証明書や CRL を、認証局ソフトウェアを使って発行することができるのかどうかを、検討しておくことは重要である。

ここでいう証明書の効果的な利用とは、利用環境に適したセキュリティトークンに証明書を格納できるか、そしてアプリケーションが証明書を解釈できるか、ということである。ここでは特にユーザ環境に関係するセキュリティトークンについて述べる。

セキュリティトークンには、ハードウェアトークンとソフトウェアトークンがある。これらは実現方法がハードウェアか、ソフトウェアかという違いにとどまらず、認証局ソフトウェアに必要とされる機能が異なってくる。認証業務の形態を交えながら、違いについて述べる。

ハードウェアトークンは IC カードに代表される小型の機器である。FIPS140-1 等の安全要件を満たす製品の場合、一度 IC カードに保存された秘密鍵を外部から読み出すことが非常に難しい。証明書を IC カードという機器に結び付けて捉えることができるため、証明書と鍵ペアのコピーが作られてしまう危険を避けることができ、また鍵ペアを紛失したことを物品である IC カードの紛失によって知ることができる。

ハードウェアトークンを利用するには、鍵ペアをどこで生成し、認証局によって発行された証明書をどこで格納するかという検討を行う必要がある。社員証や学生証のような認証に用いる証明書の場合には、認証局側で IC カードを管理し配布する"センター発行モデル"が考えられる。この場合は、認証局ソフトウェアが IC カードを使った鍵生成や、IC カードにエンコードするためのデータイメージを作成することができればよい。商用の認証局ソフトウェアのいくつかは、このどちらの用途にも対応している。

ユーザ側で鍵ペアの生成を行う必要がある場合には、そのハードウェアトークンの受け渡しに留意する必要がある。ユーザ側で鍵の生成を行った後にネットワークを利用して認証局側から証明書を転送し、ハードウェアトークンに書き込む方法があるが、この方法では、ユーザが本当にハードウェアトークンを利用しているのかどうかを、認証局側から確認することができない。

遠隔地のユーザと本人確認の上でハードウェアトークンを受け渡しするには、本人確認書類と共に IC カードを持参してもらうか、本人特定郵便などを利用して、ユーザ本人が IC カードを利用する状況を作る必要がある。

ソフトウェアトークンはハードウェアトークンの機能をソフトウェアで実現したもので、SSL/TLS に対応した Web ブラウザで"証明書ストア"などと呼ばれているもの

である。予め設定したパスフレーズを入力しないと格納された鍵ペアを利用できないなど、利用方法はハードウェアトークンに似ている。しかしソフトウェアで実現されているため、データのコピーが可能であり、また認証局側から"秘密鍵をエクスポートできない"といった設定を強制することができない。

一方、ソフトウェアトークンはハードウェアトークンの利用に必要なカードリーダといった機器やドライバソフトウェアが必要ないため、多くの種類のユーザ環境で利用できる。導入コストが低く Web ブラウザを使った鍵生成と証明書の格納に対応しているため、Web インターフェースを持つ認証局ソフトウェアと通信を行って証明書の利用に使われることが多い。

Web ブラウザを使った鍵生成と証明書の格納には、認証局ソフトウェアがそのための Web サービスを提供できる必要がある。Web ブラウザ毎に対応方法が異なるため、ユーザ環境で使われる Web ブラウザに対応した認証局ソフトウェアが必要になる。

ユーザ環境の対応状況に関する要件検討のポイントは、ユーザの利用環境の中で、鍵ペアの生成と管理をどう行うか決めることである。ユーザに鍵生成をさせるか、生成された鍵はどこに保存されるか、証明書の上書きは可能か、オフラインでの受け渡しを実現する業務体制を持つかなどを決定しておくことで、どのタイプのセキュリティトークンを使用するかなどが必然的に決定されるようになる。

6.5. RA の業務システムとの連携

認証局がユーザとの接点を持つ業務は、RA 業務である。ユーザサービスの向上や業務効率の向上を考えると、RA 業務でユーザ登録や既存のユーザ情報の参照などが行われることが考えられる。つまり既存の業務システムにあるユーザ情報と認証局の持つ証明書の情報を一元的に扱う場面が、今後現れてくると考えられる。

既にグループウェアの中にはユーザ情報と証明書を連動させたものがあり、また証明書が格納された IC カードを使った社員証の発行サービスがある。

今後、PKI がより一般化するに従い業務システムと融合し、業務システムにおける認証情報の一つとして、透過的な形態で証明書を利用する場面が現れると考えられる。

本調査研究で検討したクライアント認証用の証明書は、RA 業務とアドレス資源管理業務が連携したシステムで管理することを検討している。このようなシステムを検討するには、RA と業務システムがどのようなインターフェースで連携をするのかを定めることが重要である。ここでは、RA 業務と業務システムの連携の例として、ユーザグループの扱いについて述べる。

6.5.1. ユーザグループの扱い

業務システムにおいて、あるユーザ（例えば人事課の担当者）が他のユーザ（例えば総務課の社員）のユーザ情報を作成する場面は一般的である。グループ企業の中で転勤ないし異動があれば、両企業の人事担当者が所属変更の手続きを行い、異動したユーザの業務システムにおける扱い（認証情報）を変更する。

これは、システム管理者による一元的なユーザ情報の管理とは形態が異なる。ユーザ情報の変更が人事担当者によって申請され、システム管理者によって処理されることは考えられるが、システム管理者が本人確認を行っているわけではない。

認証局における認証業務の観点でみると、これは人事課の担当者が RA 業務を行っていることになる。一つの認証局に対して複数の RA が設けられた状態である。しかしこの RA は、他の RA の担当であるグループのユーザ情報を変更することはできない。

このように、ユーザのグルーピングが行われた場面で PKI を活用するには、認証局による一つのユーザ管理ではなく、複数の RA によるグループ毎のユーザ管理が行われる必要がある。

6.5.2. 業務システムと認証局のインターフェース

証明書を業務システムにおける認証情報として利用することを考えると、証明書の発行がユーザ情報の作成であり、証明書の失効がユーザ情報の削除という意味になる。

これを実現するには、業務システムにおけるユーザ管理のユーザインターフェースにおいて RA 業務が行えるような工夫が必要である。単なる RA 端末のカスタマイズではなく、役職や担当、連絡先といった属性と共に管理できるような透過的な連携が必要である。

多くの認証局ソフトウェアは、業務システムとの連携の面で課題を持っている。グループウェアや業務システムのミドルウェアにおいて PKI を統合的に利用できるようなれば、強固な認証機能を利用した社内業務システムや、関連企業との取引に使われるシステムにおいて広範囲に普及すると考える。

認証局ソフトウェアの中には、いくつかの試みを行っているものがあり、企業ユーザによるフィードバックによって、より適切なコストの PKI が普及していくことが望まれる。

6.6. 要件検討のポイント

今回の検討を通じて得られた要件検討のポイントを項目ごとにまとめると、下記のようになる。

- 機器の機能ごとの分離
  　要求されるサービスレベルから認証局の型を想定し、その型で運用が可能な認証局ソフトウェアを利用する。

- 機能間の通信プロトコル
  　RA システムなどの開発を行う必要がない場合は、VA や PA、RA の設置に関する条件がない限り、重点をおいて検討する必要はない。RA システムや証明書発行システムの開発の必要がある場合には、標準的なプロトコルを利用しているかどうかを調べ、またその開発環境が用意できることを確認する。

- 権限分離の実現
  　高い安全性が要求される認証局の場合は、まず運用体制を想定する。その体制を実現できるソフトウェアを利用する。限られた発行対象を持つ認証局の場合は、認証局ソフトウェアで実現可能な権限の分離方法を調べ、それに合わせた運用体制を検討する。

- ユーザ環境の対応状況
  　鍵ペアの生成と管理をどこで、どのように行う必要があるかを決める。オフラインでの受け渡しがある場合には、その業務体制が確保できるかを検討する。

6.7. 質問表について

　認証局ソフトウェアの機能概要を調査するため、機能ごとの状況をたずねた質問表を作成した。これは第 4 章で述べた業務モデルに基づいて作成されており、想定した業務に適合する認証局ソフトウェアを検討するために有効であった。

　質問表は、対象別と観点別の二種類が作られた。参考のため、ここに掲載する。

評価観点別の質問表

評価の観点	大項目	中項目	評価対象
役割分担が明確なシステム構成をとりやすいか	システム構成	ポンチ図に相当するサーバ機能を開発なしに そろえられるか? (IA, RA, リポジトリ、申請受付サーバ、利用者管理 サーバ)	システム構成要素
		ポンチ図に相当するRA用ツールを開発なしに そろえられるか? (RA管理インタフェース、RAA申請インタフェース、RA 申請インタフェース)	各種RA用インタフェース
	オペレータの権限設定	RAAはRAのみの証明書申請ができるように 設定できるか?	RAサーバ or 申請受付サーバ
		RAはEEのみの証明書申請ができるように設定できる	RAサーバ or 申請受付サーバ
		RAAはRAのみの証明書失効ができるように 設定にできるか?	RAサーバ or IA(CA)サーバ
		RAは自分が申請したEEのみの証明書失効が できるように設定できるか?	RAサーバ or IA(CA)サーバ
		RAによるEE証明書申請数について上限を設定できるか?	申請受付サーバ?
		EEの鍵対のバックアップをとる場合、バックアップデータ へアクセスできるオペレータを指定できるか?	RAサーバ or IA(CA)サーバ
		複数名のRAO, RAAの認証が完了しないと証明書発行ができないように設定できるか?	RAサーバ
		CAサーバ、RAサーバのログ閲覧のみができる インタフェースの提供と設定ができるか?	RAサーバ or IA(CA)サーバ
	オペレータのアクセス	RAOからRAサーバへのアクセス制限方法としてユーザ	RAサーバ
		RAAから申請受付サーバへのアクセス制限方法として	申請受付サーバ
		RAから申請受付サーバへのアクセス制限方法として ユーザ認証以外の方法をサポートしているか?	申請受付サーバ
オペレータ以外からの不正アクセス対策が 充実しているか?	サーバ管理権限の設定	CAOを複数人とし、複数人集まらないとIA(CA)サーバの 設定を変えられないようにできるか?	IA(CA)サーバ
		RAOを複数人とし、複数人集まらないとRAサーバの 設定を変えられないようにできるか?	RAサーバ
		RAAを複数人とし、複数人集まらないと申請受付サーバ	申請受付サーバ
		?	利用者管理サーバ
		?	リポジトリ
	サーバ間の通信保護	IA(CA)サーバとRAサーバ間の通信保護を考慮した プロトコルが採用されているか?	IA(CA)サーバ、RAサーバ
		RAサーバと申請受付サーバ間の通信保護を考慮した プロトコルが採用されているか?	RAサーバ、申請受付サーバ
	不正アクセス対策の前提となる機能	JPNIC認証局の設備である、IA(CA)サーバ、RAサーバ、 リポジトリへの不正アクセスを防ぐための機能がある	IA(CA)サーバ、RAサーバ、 リポジトリ
		IP事業者の設備である、申請受付サーバ、利用者管理 サーバへの不正アクセスを防ぐための機能があるか?	申請受付サーバ、 利用者管理サーバ
	サーバ管理ログ	RAサーバの作業記録に、RAO, RAA, RAの区別があるか?	RAサーバ
		申請受付サーバの作業記録に、RAA, RAの区別があるか?	利用者管理サーバ
		IA(CA)サーバの作業記録をCAOにメールで送る機能が	IA(CA)サーバ
		RAサーバの作業記録をRAOにメールで送る機能があるか?	RAサーバ
		申請受付サーバの作業記録をRAAにメールで送る機能	申請受付サーバ
RA(ISP)にとって導入しやすいか?	インタフェース導入	RA申請インタフェースの動作プラットフォームは、Windows	RA申請インタフェース
		RA申請インタフェースの動作プラットフォームは、UNIXに	RA申請インタフェース
		RA申請インタフェースの動作プラットフォームは、Macに	RA申請インタフェース
	インタフェースの使いやすさ	RA申請インタフェースのカスタマイズが 簡単にできるか?	RA申請インタフェース
事業部にとって導入しやすいか?	インタフェース導入	RAA申請インタフェースの動作プラットフォームは、Windows xxに対応しているか?	RAA申請インタフェース
		RAA申請インタフェースの動作プラットフォームは、UNIXに対応しているか?	RAA申請インタフェース
		RAA申請インタフェースの動作プラットフォームは、Macに対応しているか?	RAA申請インタフェース

その他、認証局の機能が充実して	アルゴリズムの設定	鍵対作成時、鍵長設定を証明書の種別ごとに変えられるか?	IA(CA)サーバ
	データベース保護	証明書データベースの保護を考慮した方式が採用されて	IA(CA)サーバ
		作業記録にディジタル署名をつけられるか?	IA(CA)サーバ、利用者管理サーバ
		作業記録にタイムスタンプをつけられるか?	IA(CA)サーバ、利用者管理サーバ
	証明書プロファイルの設定	証明書プロファイルの xxx 拡張フィールドをサポートしているか?	IA(CA)サーバ
	証明書のスムーズな発行	EE証明書をバルクで発行できるか?	IA(CA)サーバ
	ライフサイクル管理対応	CAの鍵対変更(Rekey)を想定したリンク証明書を発行する機能があるか?	IA(CA)サーバ
		EE証明書を更新(Update)する機能があるか?(同一DNの証明書発行を許容するか?)	IA(CA)サーバ
		EE証明書を更新する機能があるとき、EEから直接申請するインタフェースを開発なしに用意できるか?	IA(CA)サーバ? 申請受付サーバ?
		EEから直接申請するインタフェースがあるが不要となった	IA(CA)サーバ? 申請受付サーバ?
	トークン対応	ICカードに対応しているか?	IA(CA)サーバ? RAサーバ? RAA申請インタフェース?
		USBキーに対応しているか?	IA(CA)サーバ? RAサーバ? RAA申請インタフェース?
	CRL	CRL発行後、リポジトリへの登録が自動化できるか?	IA(CA)サーバ、リポジトリ
		CRL発行の自動化ができるか?	IA(CA)サーバ
	秘密鍵管理レベル	IA(CA)の秘密鍵をHSM内で作成して管理できるか?	IA(CA)サーバ
		IA(CA)の秘密鍵はUpdateを含め最長xx年使い続けられるか?(ソフトとしての制限ではなく、HSMとしての制限があるか?)	IA(CA)サーバ
		HSMはFIPS140-1レベル3認定であるか?	IA(CA)サーバ
		HSM管理のために複数人認証をサポートしているか?	IA(CA)サーバ
		HSM管理のために複数方式による認証をサポートしているか?(パスワード+物理トークンなど)	IA(CA)サーバ
		HSMで秘密鍵の分割バックアップをサポートしている	IA(CA)サーバ
		HSMで秘密鍵の暗号化バックアップをサポートしているか?	IA(CA)サーバ
		HSMで秘密鍵のバックアップ媒体として安全な媒体が利用可能であるか?	IA(CA)サーバ
	一般	公開鍵の重複チェック機能があるか?	IA(CA)サーバ
	管理権限		
	ログ	証明書の累計発行枚数表示機能があるか?	IA(CA)サーバ
	発行承認		
	インタフェース		
	プロトコル		

評価対象別の質問表

評価対象	大項目	中項目	その他の観点
IA(CA)サーバ	サーバ管理権限の設定	CAOを複数人とし、複数人集まらないとIA(CA)サーバの	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	IA(CA)サーバの作業記録をCAOにメールで送る機能が	
	アルゴリズムの設定	鍵対作成時、鍵長設定を証明書の種別ごとに変えられるか?	その他、認証局の機能の充実
	データベース保護	証明書データベースの保護を考慮した方式が採用されて	
	証明書プロファイルの設定	証明書プロファイルの拡張フィールドをサポート状況は？	
	証明書のスムーズな発行	EE証明書をバルクで発行できるか?	
	ライフサイクル管理対応	CAの鍵対変更(Rekey)を想定したリンク証明書を発行	
		EE証明書を更新(Update)する機能があるか?（同一DNの証明書発行を許容するか?）	
	CRL	CRL発行の自動化ができるか?	
	秘密鍵管理レベル	IA(CA)の秘密鍵をHSM内で作成して管理できるか?	
		IA(CA)の秘密鍵はUpdateを含め最長xx年使い続けられるか? (ソフトとしての制限ではなく、HSMとして	
		HSMはFIPS140-1レベル3認定であるか?	
		HSM管理のために複数人認証をサポートしているか?	
		HSM管理のために複数方式による認証をサポートしているか? (パスワード+物理トークンなど)	
		HSMで秘密鍵の分割バックアップをサポートしている	
		HSMで秘密鍵の暗号化バックアップをサポートしているか?	
		HSMで秘密鍵のバックアップ媒体として安全な媒体が	
	一般	公開鍵の重複チェック機能があるか?	
	ログ	証明書の累計発行枚数表示機能があるか?	
IA(CA)サーバ、リポジトリ	CRL	CRL発行後、リポジトリへの登録が自動化できるか?	その他、認証局の機能の充実
IA(CA)サーバ、利用者管理サーバ	データベース保護	作業記録にディジタル署名をつけられるか?	その他、認証局の機能の充実
		作業記録にタイムスタンプをつけられるか?	
IA(CA)サーバ、RAサーバ	サーバ間の通信保護	IA(CA)サーバとRAサーバ間の通信保護を考慮したプロトコルが採用されているか?	オペレータ以外からの不正アクセス対策が充実しているか?
IA(CA)サーバ、RAサーバ、リポジトリ	不正アクセス対策の前提となる機能	JPNIC認証局の設備である、IA(CA)サーバ、RAサーバ、リポジトリへの不正アクセスを防ぐための機能がある	オペレータ以外からの不正アクセス対策が充実しているか?
IA(CA)サーバ・RAサーバ・RAA申請インタフェース	トークン対応	ICカードに対応しているか?	その他、認証局の機能の充実
		USBキーに対応しているか?	その他、認証局の機能の充実
IA(CA)サーバ・申請受付サーバ	ライフサイクル管理対応	EE証明書を更新する機能があるとき、EEから直接申請するインタフェースを開発なしに用意できるか?	その他、認証局の機能の充実
		EEから直接申請するインタフェースがあるが不要となった	その他、認証局の機能の充実
RAA申請インタフェース	インタフェース導入	RAA申請インタフェースの動作プラットフォームは、Windows xxに対応しているか?	導入／開発のしやすさ
		RAA申請インタフェースの動作プラットフォームは、UNIXに対応しているか?	
		RAA申請インタフェースの動作プラットフォームは、Macに対応しているか?	
RAサーバ	オペレータの権限設定	複数名のRAO, RAAの認証が完了しないと証明書発行ができないように設定できるか?	役割分担が明確なシステム構成をとりやすいか
	オペレータのアクセス	RAOからRAサーバへのアクセス制限方法としてユーザ	役割分担が明確なシステム構成をとりやすいか
	サーバ管理権限の設定	RAOを複数人とし、複数人集まらないとRAサーバの設定を変えられないようにできるか?	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	RAサーバの作業記録に、RAO, RAA, RAの区別があるか?	
		RAサーバの作業記録をRAOにメールで送る機能があるか?	
RAサーバ or IA(CA)サーバ	オペレータの権限設定	RAAはRAのみの証明書失効ができるように設定にできるか?	役割分担が明確なシステム構成をとりやすいか
		RAは自分が申請したEEのみの証明書失効ができるように設定できるか?	
		EEの鍵対のバックアップをとる場合、バックアップデータへアクセスできるオペレータを指定できるか?	
RAサーバ or IA(CA)サーバ	オペレータの権限設定	CAサーバ、RAサーバのログ閲覧のみができるインタフェースの提供と設定ができるか?	役割分担が明確なシステム構成をとりやすいか
RAサーバ or 申請受付サーバ	オペレータの権限設定	RAAはRAのみの証明書申請ができるように設定できるか?	役割分担が明確なシステム構成をとりやすいか
		RAはEEのみの証明書申請ができるように設定できるか?	
RAサーバ、申請受付サーバ	サーバ間の通信保護	RAサーバと申請受付サーバ間の通信保護を考慮した	オペレータ以外からの不正アクセス対策が充実しているか?

RA申請インタフェース	インタフェース導入	RA申請インタフェースの動作プラットフォームは、Windows	RA(ISP)にとっての導入しやすさ
		RA申請インタフェースの動作プラットフォームは、UNIXに	
		RA申請インタフェースの動作プラットフォームは、Macに	
	インタフェースの使いやすさ	RA申請インタフェースのカスタマイズが簡単にできるか?	RA(ISP)にとっての導入しやすさ
各種RA用インタフェース	システム構成	ポンチ図に相当するRA用ツールを開発なしにそろえられるか? (RA管理インタフェース、RAA申請インタフェース、RA申請インタフェース)	役割分担が明確なシステム構成をとりやすいか
システム構成要素	システム構成	ポンチ図に相当するサーバ機能を開発なしにそろえられるか? (IA, RA, リポジトリ、申請受付サーバ、利用者管理サーバ)	役割分担が明確なシステム構成をとりやすいか
申請受付サーバ	オペレータのアクセス制限	RAAから申請受付サーバへのアクセス制限方法として	役割分担が明確なシステム構成をとりやすいか
		RAから申請受付サーバへのアクセス制限方法としてユーザ認証以外の方法をサポートしているか?	
	サーバ管理権限の設定	RAAを複数人とし、複数人集まらないと申請受付サーバ	オペレータ以外からの不正アクセス対策が充実しているか?
	サーバ管理ログ	申請受付サーバの作業記録をRAAにメールで送る機能	
申請受付サーバ、利用者管理サーバ	不正アクセス対策の前提となる機能	IP事業者の設備である、申請受付サーバ、利用者管理 サーバへの不正アクセスを防ぐための機能がある	オペレータ以外からの不正アクセス対策の充実
申請受付サーバ?	オペレータの権限設定	RAによるEE証明書申請数について上限を設定できるか?	役割分担が明確なシステム構成をとりやすいか
リポジトリ	サーバ管理権限の設定		オペレータ以外からの不正アクセス対策の充実
利用者管理サーバ	サーバ管理権限の設定		オペレータ以外からの不正アクセス対策の充実
利用者管理サーバ	サーバ管理ログ	申請受付サーバの作業記録に、RAA, RAの区別があるか?	オペレータ以外からの不正アクセス対策の充実
その他	管理権限 発行承認 インタフェース プロトコル		その他、認証局の機能の充実

第7章 認証情報の応用

内容

- IP アドレスの認証で可能となるサービス
- IP 指定事業者と認証
- 応用サービス、ビジネス例

7. IP アドレス認証の応用

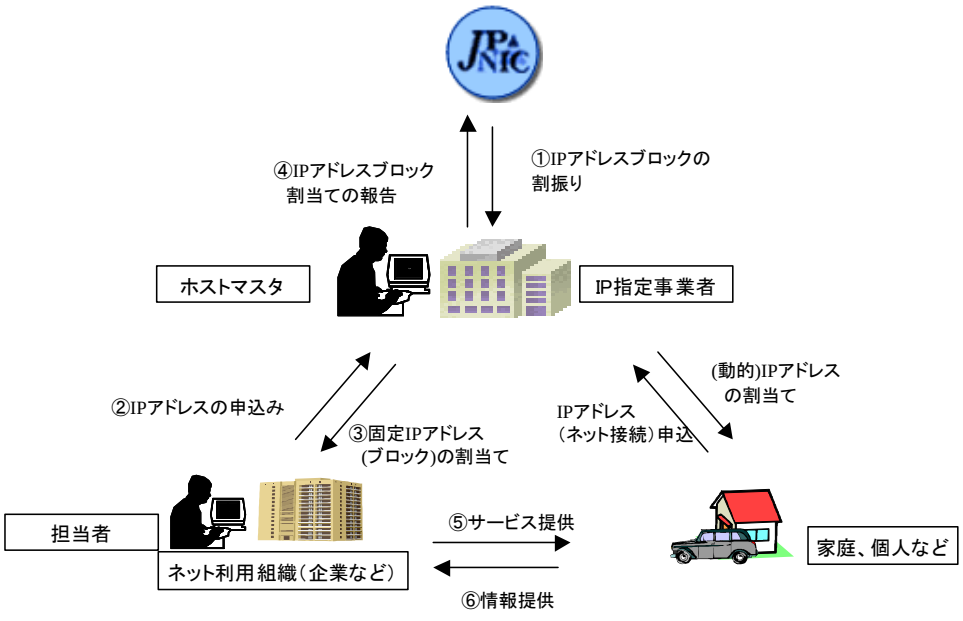
本章では、IP アドレスを認証することにより展開できる可能性のあるサービスを考え、そのサービスを応用したビジネスや事業のイメージを示す。なお、今回提示するビジネスや事業は、採算性や法や社会制度的な実現上の課題、制約等については考慮せずに考えたものである。

7.1　IP アドレスの認証で可能となるサービス

7.1.1.　現行の IP アドレス申請のプロセスと課題

企業（組織）や個人が所有する情報通信機器をインターネットに接続し、ネットワークサービスを提供（あるいは享受）したい場合、インターネットに接続する機器に特定の IP アドレスを設定しなければならない。

この IP アドレスは各人が勝手に設定するのではなく、一般には接続する ISP を通じてアドレス値を入手することになる。国内では、特定の IP アドレスが得られるまでの流れは図 7-1 のようになっている。



参考：JPNICホームページ：IPアドレスの申請
（http://jpnic.jp/ja/ip/ipguide-u.html#o1）

図 7-1　現行の IP アドレスに関わるプロセス

インターネットを利用するサービスのニーズは年々高まっており、それに応じて IP アドレスの申請も膨大な件数となっている。

このため、図 7-1 に示された各プロセスでは、作業量や利便性の点で IP アドレスの申請や承認に関する重要な情報をインターネットを通じてやりとり（送受信）されていることが多い。

ところで、現行の手続きでは、この申請や発行に関する情報の送受信を通常の電子メールシステムを通じて行っており、送信者の詐称などのリスクが残っている。このため、業務運用やシステム技術でこのリスクに対応していくことが必要である。

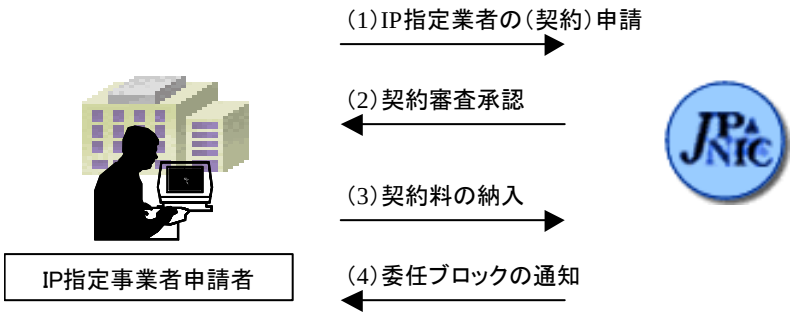
本節では、図 7-1 の中の各 2 者間で行われる情報のやりとり（プロセス）をさらに詳細に分析し、その中で判明した課題について、現行のセキュリティ上の課題と電子認証技術を使用することによって解消可能か考察する。

合わせてそうした課題が解消されることにより、これまで実施できなかったサービス（またはこれから実施可能となるサービス）について示してみたい。

7.1.2.　JPNIC と IP 指定事業者間における課題と認証

図 7-1 の①および④で示したように、JPNIC と IP 指定事業者間では、IP アドレスブロックの割り振り時、また自社やネット利用組織（ユーザ）に IP アドレスを割り当てた際に IP アドレス情報のやりとりが発生する。

「IP アドレスブロックの割振り」は IP 指定事業者になろうとする事業者（申請者）が JPNIC と契約した時点で初めて行われるものである。契約締結までの主な情報の流れは図 7-2 のようになる。



参考:JPNICホームページ:IPアドレス管理指定事業者について
（http://jpnic.jp/doc/jpnic-00117.html）

図 7-2　IP アドレス指定事業者となるまでのプロセス

現行の方式では、図 7-2 の（1）の過程で、IP 指定事業者になろうとする申請者は JPNIC に必要な文書（表 7-1）を電子メールおよび書面（郵送）で提出する。なお、この過程では対面確認までは必要とされていない。

直接の対面がないため、申請を行った者が本当にその組織の者と安易に判断することは危険ではあるが、2 章の表 2-21 中の 6、7 などその組織でないと入手が困難な文書があり、かつ契約料の納入がブロック割振りよりも先であるため、契約時点で IP 指定事業者が詐称されることは考えにくい。

ところが契約が済んだあとに、割り当て報告や登録内容の変更を通知する場合でも、現行の手続きでは電子メールベースで情報を交換している。

この過程で、悪意をもった者が IP 指定事業者の送信者を詐称し、内容の変更と偽って技術連絡窓口、事務連絡窓口等を通知してくるようなことがないとも限らない。仮にこの通知の段階で不正が発見できなかった場合、以後、詐称した者により虚偽の IP アドレスの割り当て情報が JPNIC に通知されてしまうリスクがある。

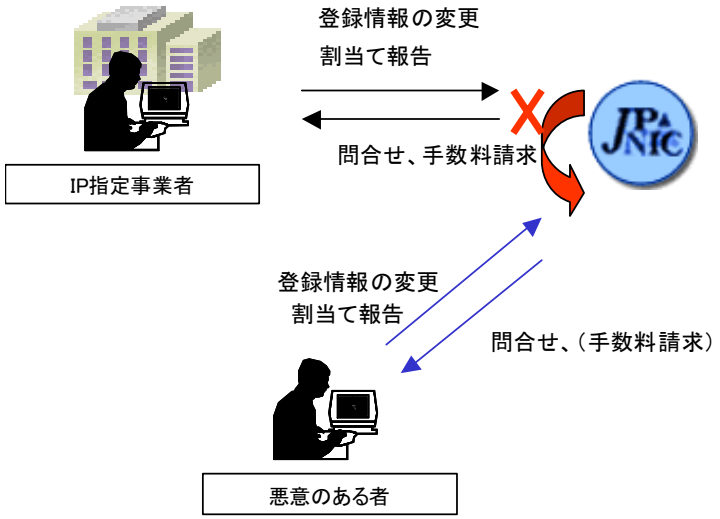


図 7-2　IP 指定事業者の詐称

こうした事態を回避するためには、JPNIC に割り当て報告や変更の連絡を行なう IP 指定事業者の担当者（以下、ホストマスタと呼ぶ）が確かにその本人であり、また連絡の文書が確実にその組織に割り当てられた IP アドレスが設定された情報通信機器から配信されたものであることを確実に示せる（確認できる）仕組みが必要である。

具体的には図 7-3 のようなホストマスタとその組織の情報通信機器（クライアント）を認証する方式が考えられる。

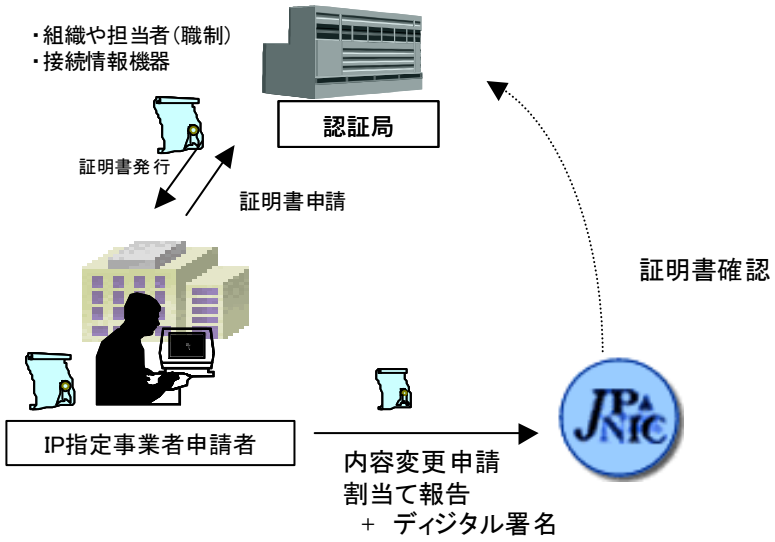


図 7-3　IP 指定事業者の認証方式

この方式が実現すると、次のようなネットワークサービスが可能となる。

- IP 指定事業者、または情報通信機器との安全なメッセージ交換サービス
- IP 指定事業者（ホストマスタ）の実在性や IP アドレス使用の真正についての一般または特定者への通知サービス

ただし、この方式では送信するメッセージ（文書、コンテンツ）の内容の真正性までは判断できない。つまり、ホストマスタが故意やミスにより割り当て情報を本来と異なる内容で記述してしまった場合などでも内容は誤ったままの状態で JPNIC には通知されてしまうことになる。これを回避するためには、割り当てた先の組織（企業等）からも割り当てについて確認が得られるような仕組みを考える必要がある。これについては 7.1.3 で示したい。

7.1.3.　IP 指定事業者とネット利用組織間の認証

図 7-1 の②および③で示したように、IP 指定事業者とインターネットを利用してサービスを実施しようとする組織（企業）との間でも接続の申込みや割り当てた IP アドレスに関する情報のやりとりが発生する。

IP 指定事業者は、図 7-4 のように通常は申込を受けた後、自社のネットワーク設備と申込者のネットワーク設備とを接続するため、申込者に出向き作業を実施する。これにより申込者が実在することや接続するルータ等は確認できる。

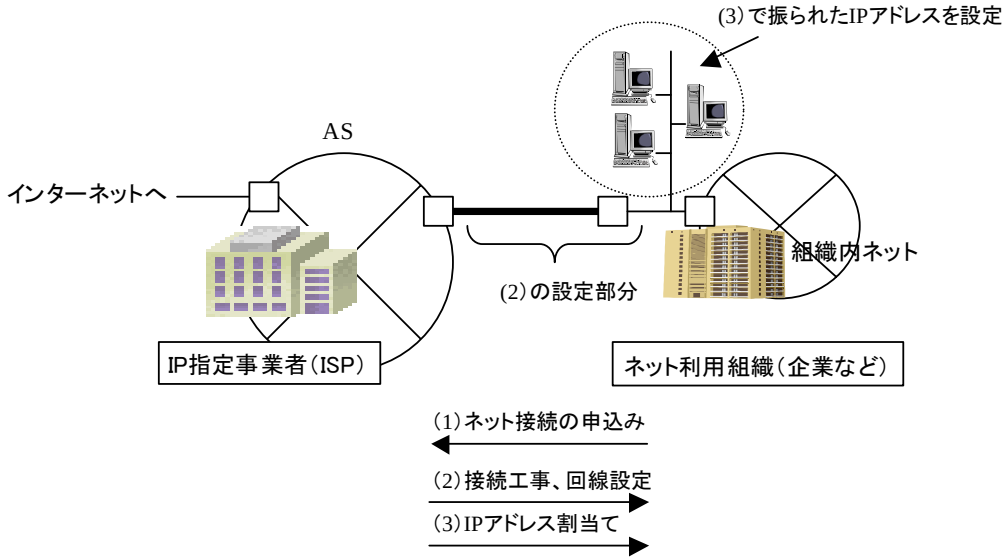


図 7-4　IP アドレス割り当ての一般フロー

ところで、ネット利用組織の IP アドレスの割り当て情報は図 7-1 の④のように IP 指定事業者が JPNIC にネットを通して報告するようになっている。④の情報は、電子メールのテキストで送信されており、ネット利用組織がその情報を確認したかは受信側（JPNIC）では不明である。このため、前述したようにホストマスタのミスや故意によって間違った割り当て情報が報告され、データベースに登録され、whois システム等を通じて外部に公開されてしまうようなリスクがある。

この事態を回避するためには、IP 指定事業者から JPNIC へ IP アドレス割り当て情報が報告される際に、申込みを行った組織（企業）による内容の承認（保証）も合わせて行われればよい。

認証技術を使用してこれを実現する例を図 7-5 に示す。IP 指定事業者は申込みを行った組織から割り当て内容が正しいことを承認するディジタル（電子）署名付きの文書をもらい、JPNIC に更に自らの署名を付与して割り当て報告を行なうというものである。

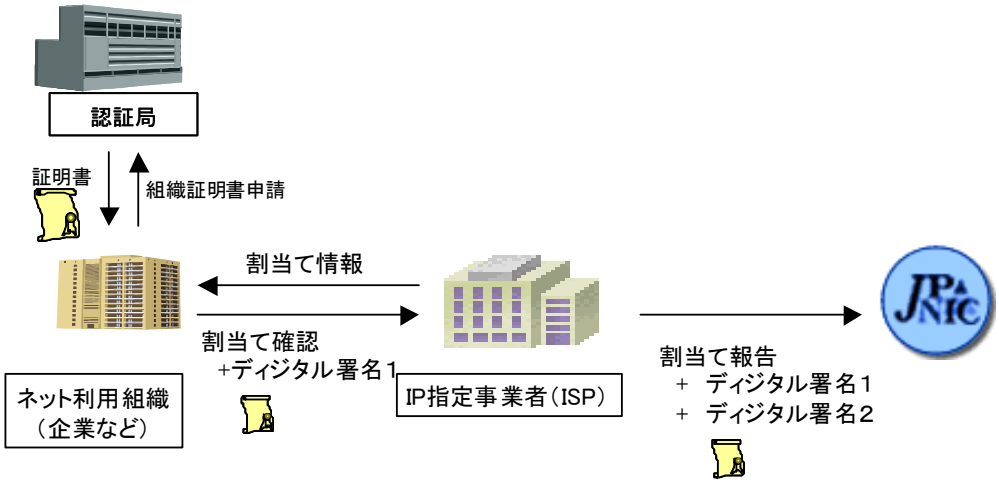


図 7-5　ネット利用組織（ユーザ）の認証方式

この認証の方式をとることにより、IP 指定事業者が配信するネット利用組織の IP アドレス割り当てに関する情報は非常に信頼性の高いものになり、以下のようなネットワークサービスが可能になる。

・割り当て先（ネット利用組織）またはその情報通信機器との安全なメッセージ交換サービス

・割り当て先（ネット利用組織）やユーザネットワークの実在性についての一般または特定者への通知サービス

ところで、現行では、IP アドレスブロックの割り当て時に IP 指定事業者が JPNIC に報告する内容は 2 章表 2-6 に示した事項となっている。

JPNIC の「IP アドレス割り当て報告申請フォーム（ユーザネットワーク用）」（http://jpnic.jp/doc/jpnic-00889.html）によれば、表 7.2 中のうち、b. [ネットワーク名]、B. [network-plan]については表 7-1 のような内容を記述することになっている。

表 7-1　割り当て時に行なう報告項目詳細

b. [ネットワーク名]	このネットワークを表す、意味のある任意の文字列を記入する。 ネットワーク名には、ネットワークが割り当てられる組織に関連のある名前を指定する。 また、英大文字，数字，"-" (ハイフン) のみを用いて 12 文字以内で記述する。複数のネットワークアドレスが同じネットワーク名を持つことも可能。 ネットワーク名は、インターネットレジストリの整合性チェックなど、主として管理目的に使用される。
B. [network-plan]	新規に構築するネットワークの詳細情報をサブネット毎に以下のフォーマットで記入する。ただし、プライベートアドレスを用いて構築する部分については記入しない。 address : ネットワークアドレス 申請時に割り当てるアドレスが確定していない場合には、 代わりに 10.0.0.0 からを使用して記入する。 mask : サブネットマスク connect : YES、NO または PART YES : インターネット接続する NO : インターネット接続しない PART: パートタイム接続(たとえばダイヤルアップ接続など)の場合 n0 : そのサブネットの直後のホスト数 n1 : そのサブネットの 6 カ月後のホスト数 n2 : そのサブネットの 1 年後のホスト数 remark : ネットワークの使用組織、用途(目的)を記入する。 日本語(全角)、英語(半角)表記が可能。 例) ・division：経理、総務、開発、販売、情報システム、 計算機センター、東京 NOC、大阪 AP HQ,Branch,R&D,Marketing,Sales support-group,customer-svc ・purpose ：バックボーン、サーバ、ダイヤルアップ LAN、WAN、ネットワーク R&D-network,HQ-net dial-up,dialup-ports,servers,point-to-point

このようにネット利用組織は、現行でも IP 指定事業者および JPNIC に対しては、割り当て先の組織や IP アドレスが振られるネットワークの用途（目的）について、ある程度の情報を示すことになっており、その一部は一般向けにも公開されている。(B. [network-plan]の情報は公開対象外)

ただし、以下の項目についてこの情報の中には含まれておらず、JPNIC や IP 指定事業者を含め、ネットワーク利用組織以外の者がこうした情報を得たい場合は、直接組織の担当者等と交渉の上で入手するしかない。

・割り当てた各 IP アドレスに情報通信機器が接続されアクティブな状態であるか（あるいは予備としてプールされているか）

・割り当てた各 IP アドレスに接続した情報通信機器の内容（用途やサービス）

・割り当てた各 IP アドレス接続先の情報通信機器の設置場所、位置

今後、ネットワークサービスがより高度化、複雑化する中で、B. [network-plan]を含め、上記のような情報を組織外に示す必要が出ることは十分に考えられる。担当者の手を逐一煩わすことなく、ネットワークを通じて信頼性の高い情報を示せるような仕組みがあれば、これまで実現できなかったような新しいネットワークサービスやビジネスに多いに利用されるのではないだろうか。

認証技術を利用する仕組みとしては図 7-6 のように図 7-5 の手順で登録する内容(項目）を拡張して、前述した情報を含めて認証を取る方式が考えられる。

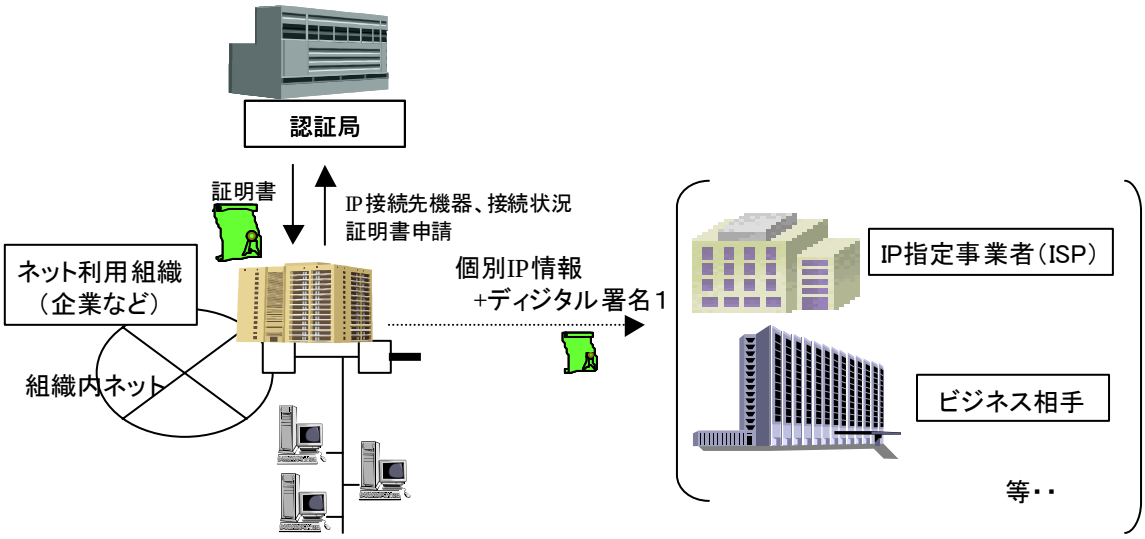


図 7-6　IP アドレス利用先の認証

この認証の方式をとることにより、前述したサービスに加え、以下のようなネットワークサービスが可能になる。

・割り当て先（ネット利用組織）のインターネット接続ネットワークの利用（計画）所についての一般または特定者への通知サービス

・割り当て先（ネット利用組織）の IP アドレス接続先機器の内容、設置場所についての一般または特定者への通知サービス

・割り当て先（ネット利用組織）の IP アドレス利用状況（使用、未使用）についての一般または特定者への通知サービス

7.1.4.　ユーザネットワークにおける IP アドレスの割り当てルールの新設

7.1.3 に示したように、ネット利用組織に割り当てられた IP アドレスの利用についての情報を必要に応じて外部者が入手できることで新しいネットワークサービスが出現する可能性がある。

ところで、この仕組みを利用して、特定の目的・用途や地域に割り当てられた IP アドレスに向けたネットワークサービスを行なうこと考えると、サービス提供者は IP アドレスの利用内容（証明）を確認するのに図 7-6 に示した認証局と通信を行なう必要がでてくる。もし、サービスが大規模な処理を必要とするような場合、逐一通信を行なうようなことでは機能として成り立たないことになる。このため、IP アドレス自体に特定の用途や接続場所等の意味が込められているようにする必要がある。

現行の IP アドレスの割り振り方式には、特定のアドレスブロックについて接続する情報通信機器の用途等を限定するルールはない。もし、ユーザネットワークで情報通信機器に IP アドレスを割り当てる際に、ユーザ共通の割り当てルールがあり、ルールに則った割り当てが一斉に行われ、加えて 7.1.3 の認証も行うことが可能となるならば、更に特定の IP アドレス（接続情報通信機器）に向けたネットワークサービスが可能となろう。

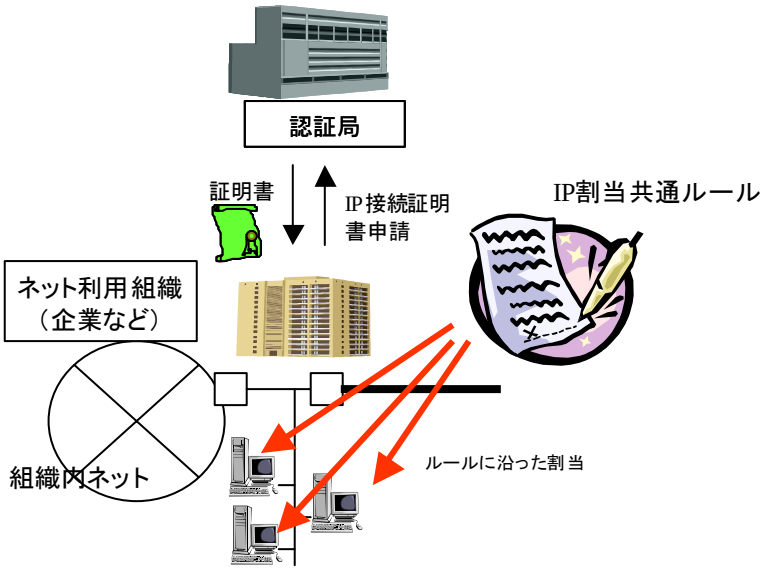


図 7-6　IP アドレスの利用別割り当て

7.1.5.　認証の対象と実現できるサービス

これまでの記述により、IP アドレスの付与や利用に関し、認証技術を用いることで既存の課題を解消したり、新たに出現する可能性のあるサービスがあることがわかる。

これまで挙げた認証の方式と可能性のあるサービスを表 7-2 に整理した。

表 7-2　IP アドレス認証により可能となるサービス例

No.	認証対象	可能になるネットワークサービス
A	IP 指定事業者担当者（ホストマスタ）およびクライアント	・IP 指定事業者、または情報通信機器との安全なメッセージ交換サービス ・IP 指定事業者（ホストマスタ）の実在性や IP アドレス使用の真正についての一般または特定者への通知サービス
B	ネット利用組織（担当者）	・割り当て先（ネット利用組織）またはその情報通信機器との安全なメッセージ交換サービス ・割り当て先（ネット利用組織）やユーザネットワークの実在性についての一般または特定者への通知サービス
C	ネット利用組織の IP アドレス接続機器の用途等	・割り当て先（ネット利用組織）のインターネット接続ネットワークの利用（計画）についての一般または特定者への通知サービス ・割り当て先（ネット利用組織）の IP アドレス接続先機器の用途、サービス内容、設置場所（地域）等の情報を一般または特定者へ通知するサービス ・割り当て先（ネット利用組織）の IP アドレス利用状況（使用、未使用）についての一般または特定者への通知サービス
D	割り当てルールに基づき設定した接続機器	（基本的にはCと同様）

次節では、こうしたサービスの組み合わせや応用により展開できる可能性のある応用サービスやビジネスの例を示し、実現に向けての要件や課題を考察してみたい。

7.2.　IP アドレス認証による応用サービス、ビジネス例

本節では IP アドレスを認証することにより新たに可能となるサービスやビジネスのアイデア例や実現に向けての課題点を表７-3 のように分類して示してみたい。

表 7-3　IP アドレス認証により可能となるサービス例

サービスタイプ	内容
既存通信事業補完型	現行の情報通信技術を使用して、安全性に課題のある既存のビジネス、サービスの部分を解決し、全体の信頼性を向上させるサービス。
高セキュア通信機能型	ISP などの通信事業者が、顧客のネットワークの安全を維持するために、通過するパケットに対するルートやフィルタリング機能を顧客のニーズや環境を考慮してより安全に高めるサービス。
新通信インフラ提案型	IP アドレスのブロック域に特定用途の意味を持たせることを前提に、実現できる可能性がある新しい通信サービス。

7.2.1.　既存通信事業補完型

ここでは、表 7-2 に示したＡ、Ｂを中心に JPNIC、IP 指定事業者、ネット利用組織間で認証技術によりインターネットを介して交換する情報の信頼が高まることを前提とした応用サービス、ビジネスを挙げてみたい。

7.2.1.1.　ネットワーク接続関連情報照会

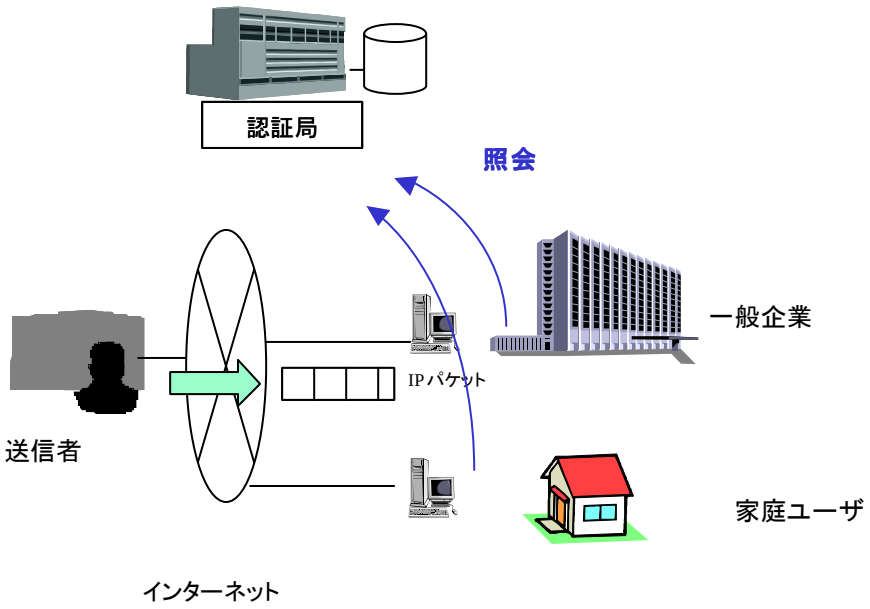


図 7-7　送信者（パケット）の確認イメージ

現在、インターネットを通じて通信を行なう際、相手先の IP アドレス（あるいはドメイン名）が正規に割り当てられた相手であるか、またその相手が信頼できる事業者なのかを確認するのは簡単ではない。現行で可能な一般的な手段は JPNIC が提供する whois システムにより IP アドレスの割り当て先を確認し、そこで得られた割り当て先の企業名等から必要に応じて別の信用調査機関（帝国データバンク等）が調査したその企業の事業に関する情報を参考にするというものである。ただし、前述したように現行の whois システム内に搭載されている情報は、信頼性と網羅性の点で十分ではない。また、ネットワーク事業の内容を調べるのに、わざわざ別の信用調査機関のサービスを利用するというのは業務上無理がある。

そこで、表 7-4 の A、B のサービスを応用し、IP アドレス割り当て範囲やその用途、またその組織自体に関する信頼性の高い（第三者により証明された）情報を必要に応じて企業や一般ユーザに提供するサービスが考えられる。

このサービスは、ネット利用組織から直接情報が得られる IP 指定事業者が手がけやすいと思われる。ただし、各事業者が保有している情報は自社の顧客のみであるため、そのままでは提供できる情報は限定されてしまう。そのため、全 IP 指定事業者から情報を集約する機関や、あるいは IP 指定事業者間で必要に応じて情報を提供し合えるようなシステムがあれば、利用者は 1 つの IP アドレス情報からワンストップで必要な情報を得ることができるようになるだろう。

7.2.1.2.　通信相手確認サービス

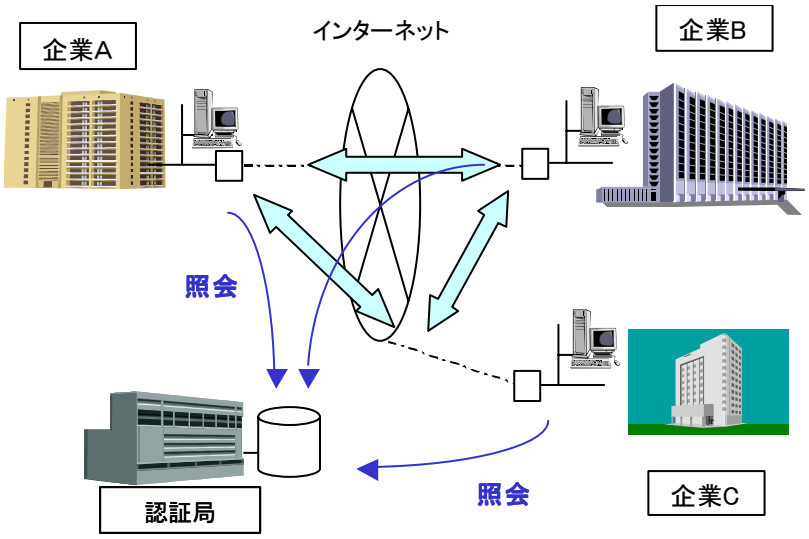


図 7-8　企業間通信サービスにおける相手先の確認イメージ

現在、異なる企業サイトのネットワークを安全に接続する方式として VPN（Virtual Private Network）が使用されることが多い。この場合、通信相手間では IP アドレスを含む使用する機器の環境を交換し、ルータやサーバに設定する必要がある。

企業内で事業所間を接続する場合や日頃付き合いの深い企業間の場合は、接続情報について信頼の高いものを得られるが、今後のネットワークビジネスの中で、多数の企業間を VPN のような形で結ぶような場合、相手先のネットワーク接続についてより信頼性の高い情報を簡易な方法で入手できることが求められる。

7.2.2.　高セキュア通信機能型

ここでは、表 7-4 の C を中心に認証技術を利用して、ネット利用組織がネット上で自組織に割り当てられた IP アドレス（接続された情報通信機器）の利用に関する情報を特定者または一般に通知できる、また特定のルールに則ってインターネットに接続する情報通信機器に IP アドレスが振られることを前提とした応用サービス、ビジネスを挙げてみたい。

7.2.2.1.　ネット利用組織の IP アドレス利用状況を考慮したルーティング

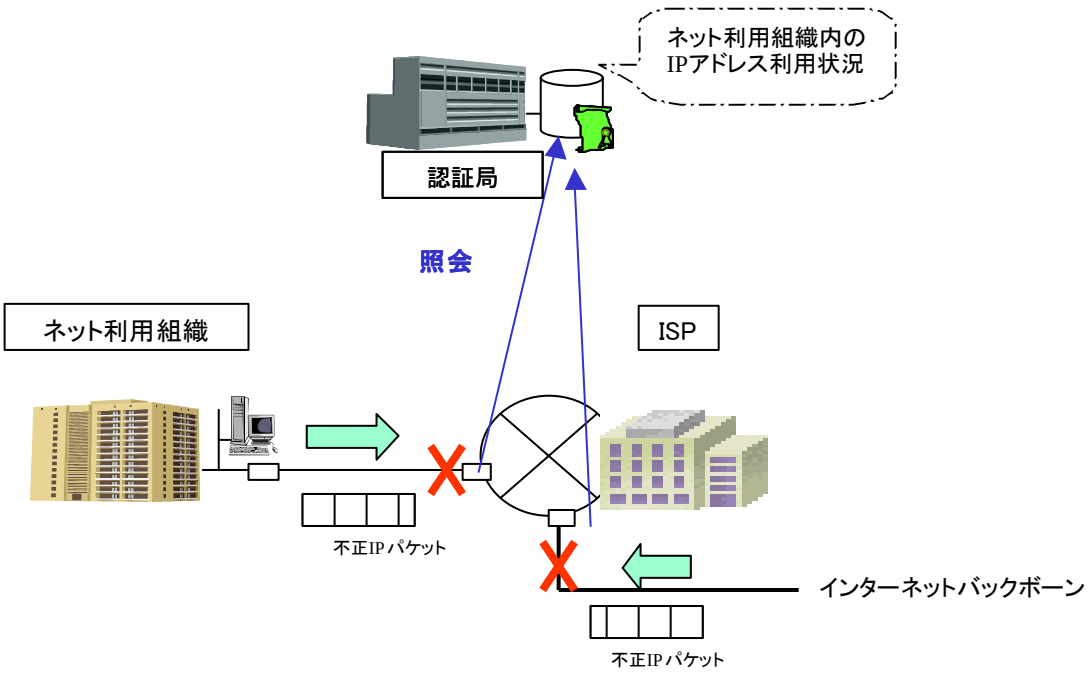


図 7-9　未使用 IP アドレスのパケットをブロックする

ネット利用組織から IP アドレス利用状況を確認できることにより、ISP では、ネット利用組織から AS に届くパケットのうち未使用であるはずの IP アドレスから発信されたものを選別（フィルタリング）できるようになる。また、ネット利用組織へ送信するパケットについても未使用 IP アドレスへ送信しているパケットを選出して IDS などに応用することが考えられる。

7.2.2.2.　特定用途割り当てを考慮したルーティング

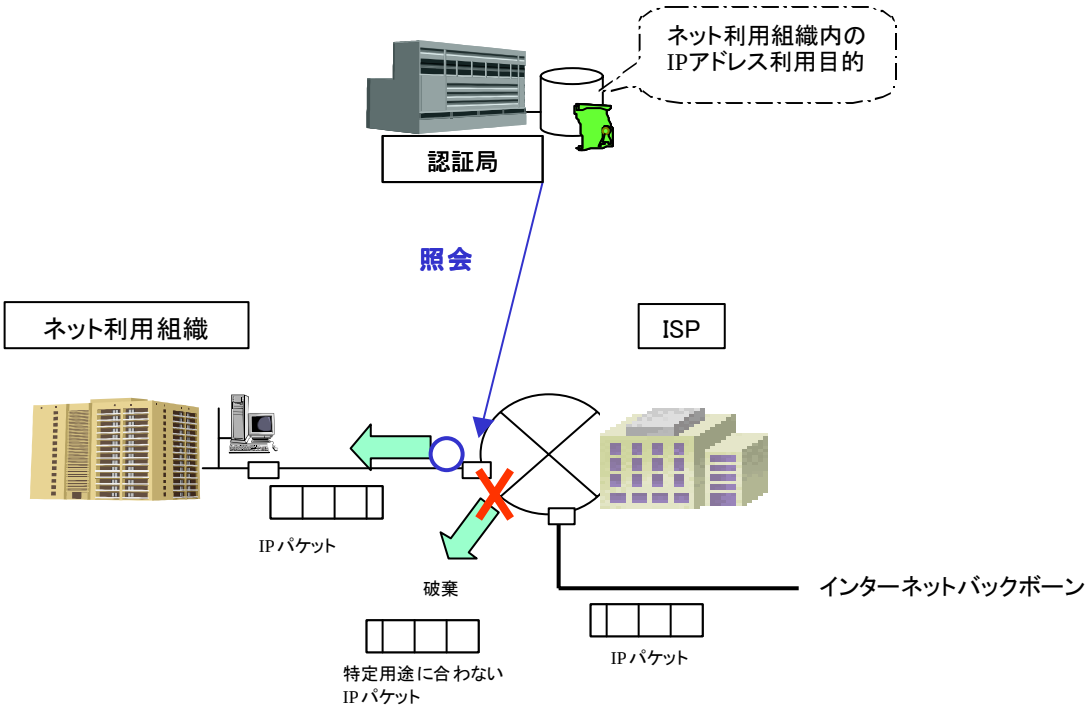


図 7-10　特定用途にマッチしない IP パケットのフィルタリング

ネット利用組織から使用する IP アドレスの接続機器の用途や場所を確認できることにより、ISP は、ルータを通過させるパケットについてその用途毎にポリシーを定めることが可能となり、新たなルーティングサービスを付加することが可能となる。

例えばネット利用組織向けに送信されたパケットについて、未使用の IP アドレスに送信された IP パケットや認証局に登録されていない IP パケットの場合は自動的に破棄する（通過させない）、パケット送信元と送信先の特定用途がマッチしている場合のみ通過させる、などが実施可能になる。

7.2.3.　新通信インフラ提案型

ここでは、表 7-4 の C、D を中心に、IP アドレスのあるブロック域を特定用途に割り当てるルールが確立され、ネット利用者が使用されている IP アドレスに接続されている機器の用途や場所が簡単に確認できるようになることを前提として、特定用途かつ不特定多数の IP アドレス先を対象とするネットワークサービスのアイデアを挙げる。

特定用途として地理的条件や利用者（年代、職業）等、様々な対象（セグメント）が考えられるが、ここでは次のように分類、整理を行なった。

（ア）学校・教育

（イ）街・地域

（ウ）家庭

（エ）公共・メディア

（オ）社会インフラ

（カ）医療

（キ）その他

なお、本アイデアの多くは JPNIC 内で組織されている「認証情報の応用専門家チーム」で検討の中から挙がったもので、現行の社会生活の中で不便、不安に感じる事象を中心に、ネットワーク社会の中で IP アドレスが認証できることにより社内生活が便利、安心になるようなサービスが示されている。なお、今回の検討については、あえて法制度や規制などによる実現難度は考慮していない。

次ページより、分類ごとに挙げられたアイデアを具体的に示してみたい。

7.2.3.1.　学校・教育

（1）　登下校時間通知サービス

【概要】

学童の交通事故を予防するためには、登下校の時間帯は車両よりも歩行者を優先する交通制御や車両への事前の情報提供が有効と思われる。小中学校などでは、行事や地域事情（天候や災害）により通常と異なる時間帯に登下校することがある。こうした場合に、通学地域内の IP アドレスを振られた情報通信機器向けに学校から登下校時間情報を配信すれば、情報を受けた各機器は以下のようなアクションを起こすことが可能となる。

-信号機

通学路の進行方向を優先（青の時間帯を長くする）する。

-車（カーナビ）

スクールゾーンを赤色等で強調表示し、多数の児童・生徒が通る可能性を警告する。

-携帯電話（メール、着メロ）

周辺注意のメールを受信する。また、専用の着信音で通知を行う。

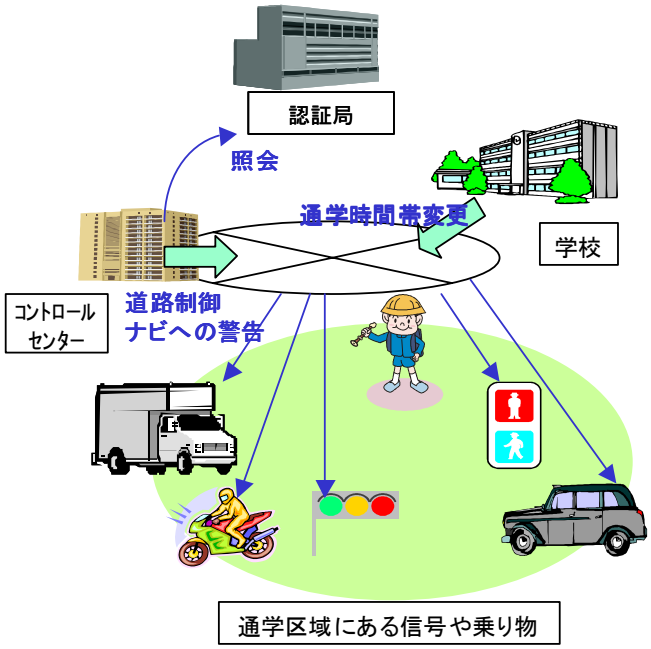


図 7-11　登下校時間通知サービス

【サービス対象者・ニーズ】

サービス提供元：

学校、自治体　[登下校の時間帯変更の注意を促したい]

サービス提供先：

家庭　[登下校の安全を高めたい]

【アプリケーションの機能・実現方式】

- 各種 GIS データへの通学路の設定機能
- 登下校時間帯入力（変更）機能
- 登下校変更時間の一斉配信機能

【認証方式・技術】

- 送信者が確実に学校からであることを確認する。
- 送信先を当該地域に限定する。

7.2.3.2.　街・地域

（1）　災害時の地域一斉連絡

【概要】

局所的な災害などが生じた場合、地域毎に、より細かな即時性の高い情報（ニュース）が配信される必要がある。地域向けの連絡手段としては現在 CATV による地域放送があるが、加入者は限られており、地域全域に情報を行き届けるための基盤となっているとは言いがたい。もし、情報通信機器の IP アドレスや認証情報の中に特定の地域に設置（接続）されていることを示す情報を含めることができれば、その地域の機器向けに一斉に緊急情報（信号）を配信することが可能となる。情報（信号）をキャッチした後の警告等の表示の仕方については情報通信機器ごとのアプリケーション仕様となるが、例えば次のようなことも可能となる。

-地域内の公園、商店街等のスピーカーによる緊急連絡

緊急情報を音声により周辺に伝える。

-家庭内の情報家電による緊急連絡

モニタによる文字や映像表示により住人に注意喚起を行なう。

-携帯電話、車等の通信機器による緊急連絡

音声や振動により、搭乗者へ注意喚起行なう。またモニタで詳細情報を表示する。

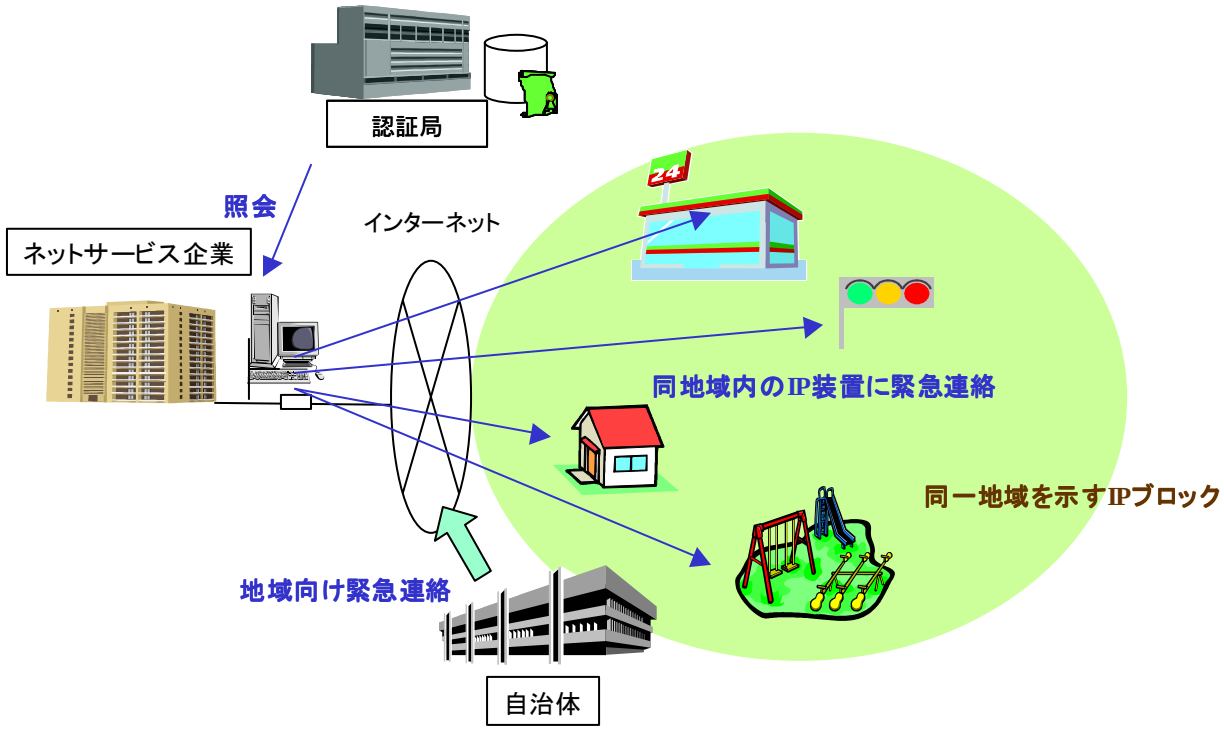


図 7-12　災害時の地域一斉連絡

【サービス対象者】

サービス提供元：

自治体、自治会　[災害時に正確な情報を迅速に地域に伝えたい]

サービス提供先：

住民　[災害時に多様な手段で情報を得たい、正確な情報を知りたい]

【アプリケーションの機能・実現方式】

・送信対象機器範囲確認機能

・対象機器向け情報一斉配信機能

・パケット経路変更、地域外パケットフィルタリング機能

【認証方式・技術】

・ 配信先の機器が該当地域に設置されたものであるか、IP アドレスブロック域や認証機関に登録された属性情報により確認する。

（2） 福祉用の地域連絡

【概要】

幼児や徘徊癖ある老人が自宅からいなくなってしまった際などに周辺地域に容姿や服装、連絡先などの情報を一斉配信し、支援を求めるサービス。また、1 人暮らしの人が近所への緊急の通知手段として使用するなど、様々な連絡用として応用できる可能性がある。

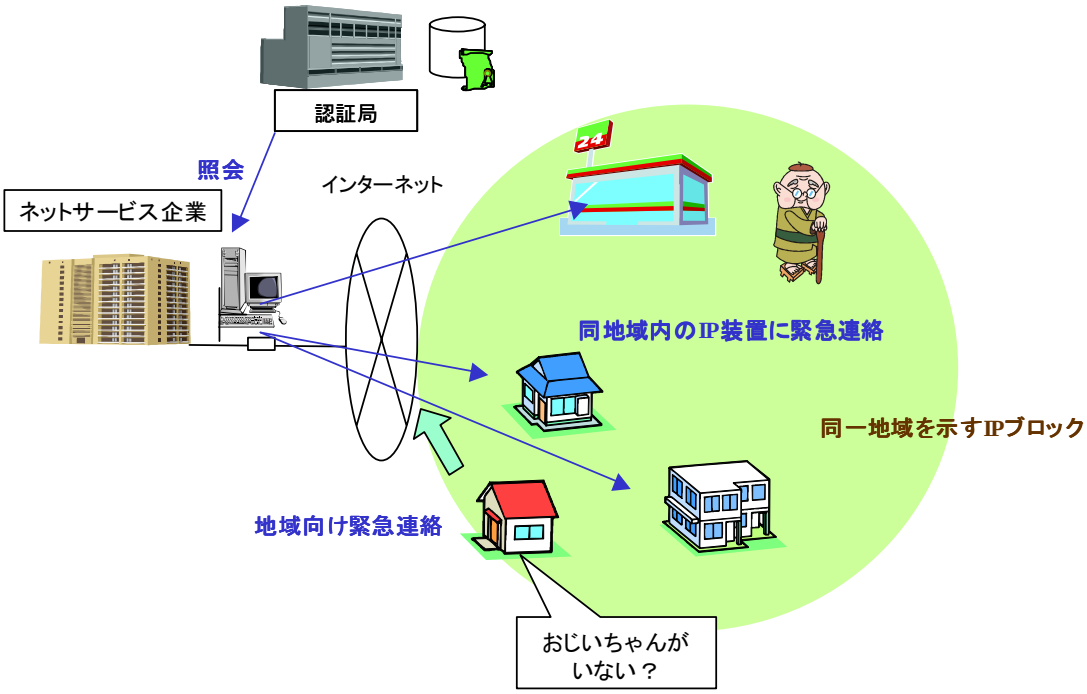


図 7-13　福祉用地域連絡

【サービス対象者・ニーズ】

サービス提供元：

自治体、自治会　[住民が安心して暮らせるサービスを提供したい]

サービス提供先：

介護の必要な家庭　[徘徊者を早く探し出したい]

【アプリケーションの機能・実現方式】

・送信対象機器範囲確認機能

・対象機器向け（警告）情報一斉配信機能

・パケット経路変更、地域外パケットフィルタリング機能

【認証方式・技術】

・ 配信先の機器が該当地域に設置されたものであるか、IP アドレスブロック域や認証機関に登録された属性情報により確認する。

7.2.3.3.　家庭

（1）　ペット認証サービス

【概要】

ペット（犬、猫等）の首輪などに小型情報通信機器を取り付け、ネットワークを通じてペットとの通信を可能にする、飼主や自治体（保健所）などによって実施するサービスである。IP アドレスブロックの中にペット用のアドレスブロックも用意する。

具体的なサービスとしては、以下のようなことが考えられる。

-GPS や地域に設置されたセンサーと組み合わせ、ネット上で猫などのペットの現在位置を確認する。また、他のペットの位置も確認できることより、ペットの集まりやすい場所や行動（なわばり）範囲などをネットから確認することができる。

-狂犬病の予防注射時期などを該当時期に保健所がペット向けに通知する。受信した小型情報通信機器にそれに合わせて発光する等の機能をつけると第三者にも認識が可能になる。

-小型情報通信機器を通じて音声や特殊音等により餌や注意の情報をペットに伝える。

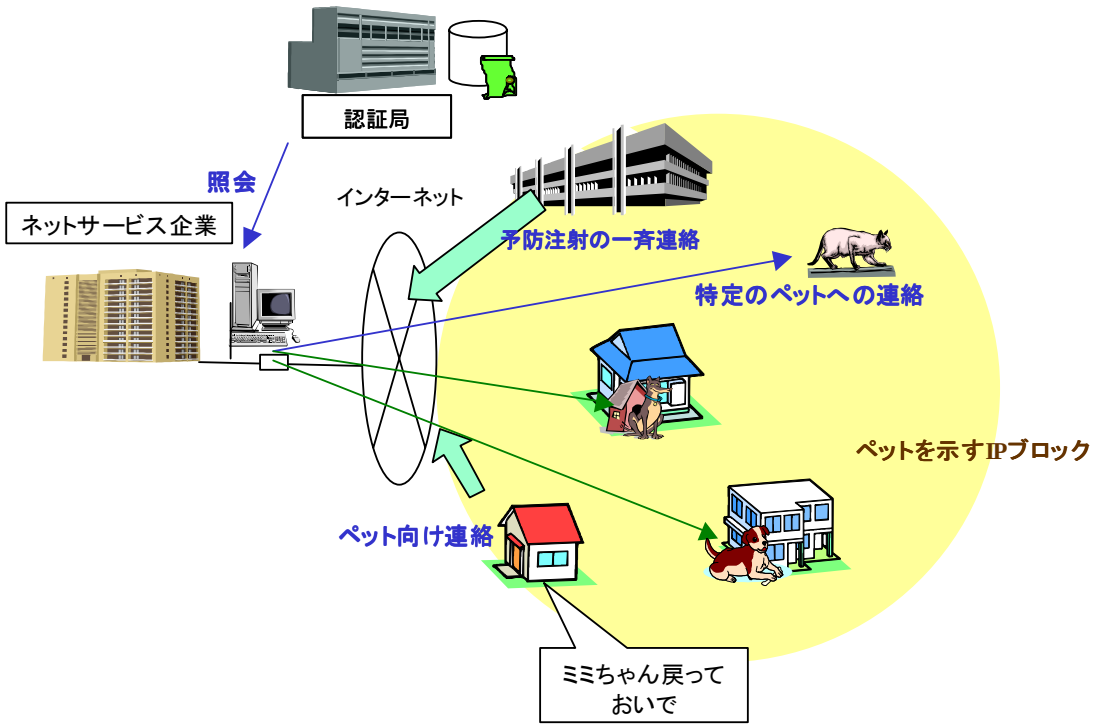


図 7-14　ペット用 IP アドレスブロックとその利用

【サービス対象者・ニーズ】

サービス提供元：

保健所、警備会社

[住民が安心して暮らせるサービスを提供したい、ペット飼主に注意を促したい]

サービス提供先：

ペットの飼主　[ペットの行動を把握したい、コミュニケーションを上げたい]

【アプリケーションの機能・実現方式】

・ペット位置確認機能

・飼主との通信機能

・アラート情報表示（光、音声）機能

【認証方式・技術】

・ ペット用の IP アドレスブロック域を使用する。認証機関に登録されたペットに関する情報より、飼育環境（飼主）を確認する。

（2）　（家庭外からの）家庭内機器・装置の遠隔サービス

【概要】

現在、身近な家電製品の中には、ネットワークに接続して家の外から遠隔で家電の操作を行なえるもの（ネット家電）が現れている。今後の家庭では、このような家電以外にも様々な電気機器や装置のネットワーク化が進んでいくと思われる。例えば、以下のような装置がネットワークに接続することにより、留守中でも通常と同じように家事が行えたり、家の中を警備するようなサービスが可能となる。

- 留守中に庭の植物へ天候の状況を見ながら散水を行なう、またペットへの餌の量をモニタ映像を見ながら調節する。
- 部屋内で侵入があった場合に、監視カメラ映像を警備会社や警察に転送する。また、モニタを見ながら遠隔で防犯インクなどを侵入者に噴射する。
- 車から降りずに車庫のシャッター操作（開閉）を行なう。また、旅行先などで遠隔で天窓を開閉し、部屋内の空気を入れ替える。

なお、こうしたサービスを行なうには、プライバシー保護の点からサービス提供範囲が限定され、確実に利用対象者だけの操作を受け付ける仕組みが必要である。

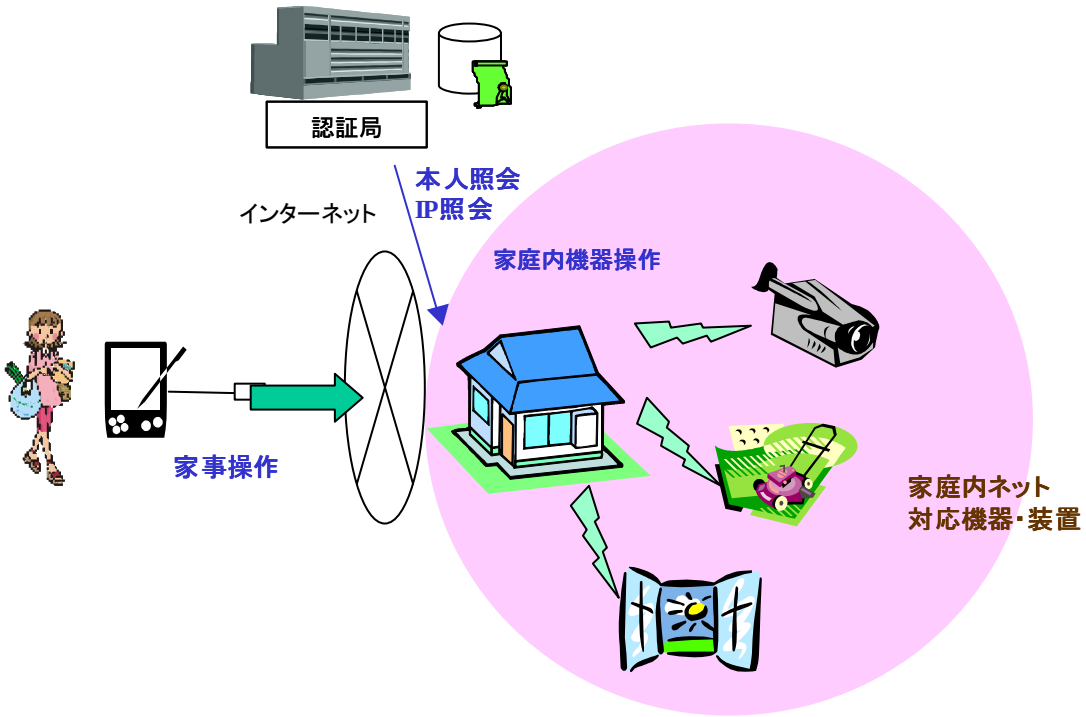


図 7-15　家庭内機器・装置の遠隔サービス

【サービス対象者・ニーズ】

サービス提供元：

警備会社、ハウジングメーカー

[住民が安心して暮らせるサービスを提供したい、付加価値の高い家を提案したい]

サービス提供先：

住人　[安心して旅行に出かけたい、生活をより一層快適にしたい]

【アプリケーションの機能・実現方式】

・遠隔操作者確認機能

・動作終了（状態）通知機能

【認証方式・技術】

・ 操作者自身の認証の他、操作先の情報通信機器が操作を許可する IP アドレスになっているか等、複数の認証により判定を行なう。

（3）　ネット家電を通じての緊急情報発信サービス

【概要】

住宅火災を防止するため、アイロンや電気ストーブなど発熱する家電について標準使用時間を大幅に越えてスイッチが入った状態になっている場合に、家人が不在やなんらかのトラブルがあったとみなしてマンションの管理人や隣の世帯、製造メーカーの保守部門などにネットを通じて警告情報を通知するようなサービスである。

また、逆に普段使用するはずの機器が一定時間全く使用されていないことを警告するようなサービスも考えられる。例えば、家族が別々に暮らしている場合や、老親と子供の世帯が別の場合などでは、直接電話などで連絡を取り合うのが億劫となる場合もある。この場合、遠隔で相手方の家庭内の機器利用がわかれば、普段通り生活していると推測でき、また、通常使用されるはずの機器が暫くの期間使用されていないような場合は、なんら異常があるとみなして関係者に通知を行なうようにすることも可能である。

こうしたサービスでも機器間や特定の相手の通信で確実に通信したい相手か確認できる必要があり IP アドレス認証の仕組みが活用できるものと思われる。

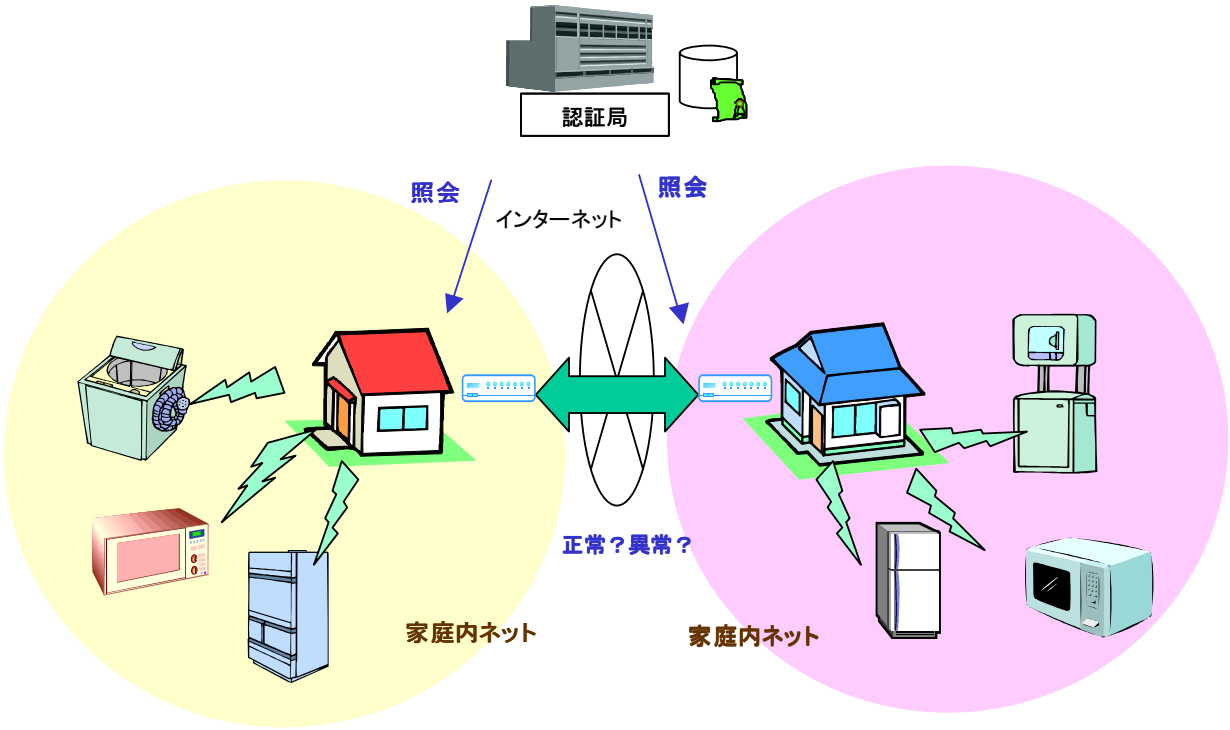


図 7-16　家庭内機器を通した家庭間緊急連絡サービス

【サービス対象者・ニーズ】

サービス提供元：

家電メーカー、警備会社、自治会

[住民が安心して暮らせるサービスを提供したい、付加価値の高い製品を販売したい]

サービス提供先：

住人（マンション等）[安心して外出したい、離れた家族の様子を知りたい]

【アプリケーションの機能・実現方式】

・送信相手登録機能

・送信条件設定（異常、正常）機能

・異常時リモート対応機能（スイッチオフ等）

【認証方式・技術】

・ 通信し合う機器自体の認証、また異常時の緊急措置を実行できる権限があるか判定を行なう。

（4）　幼児・児童玩具向け通信サービス

【概要】

今後、幼児・児童を対象とした玩具でもインターネットに接続機能を備えるものが急増してくると思われる。こうした玩具からアクセス要求があった場合、幼児・児童からということが予め認識できれば、不適切なサイトへのアクセスやコンテンツの受信を ISP 側で止めることができる。

このサービスの実現には、玩具に割り当てる IP アドレスブロックの中に幼児・児童用の機器ということがわかるような仕組みがあるとよいだろう。

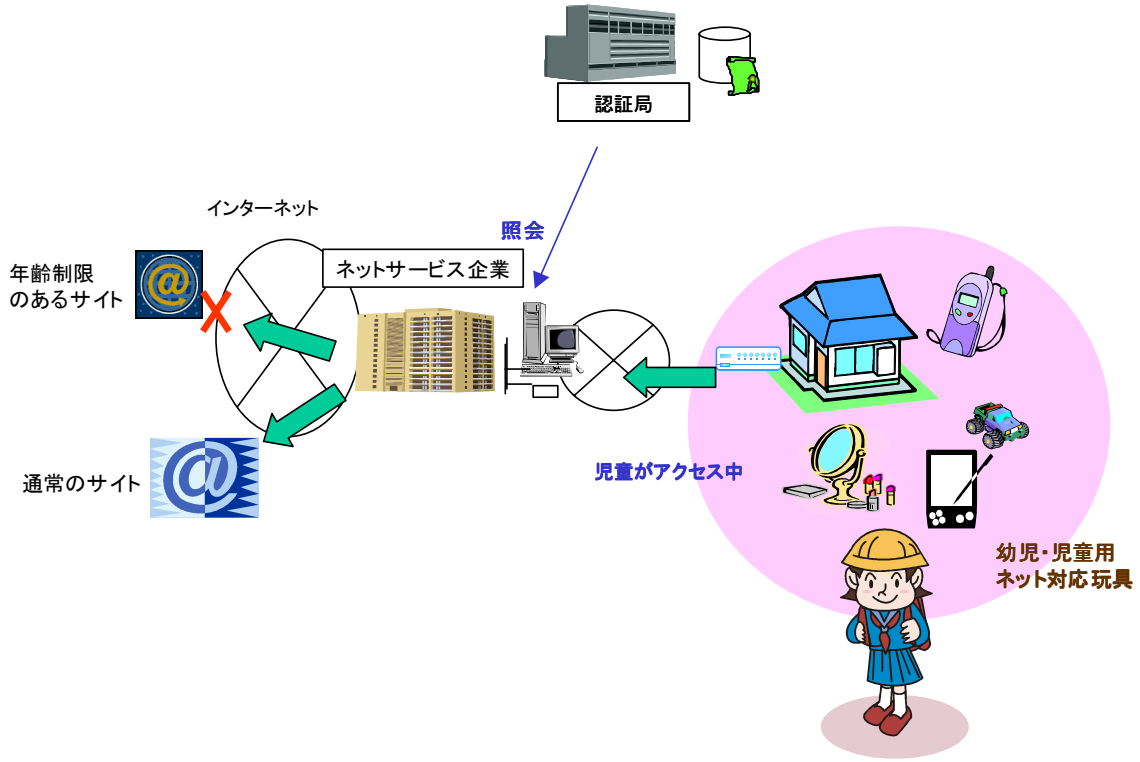


図 7-17　幼児・児童向け通信サービス

【サービス対象者・ニーズ】

サービス提供元：

ＩＳＰ、ＷＥＢサイト　[資格のある利用者のみアクセスを受け付けたい]

サービス提供先：

玩具メーカー、家庭　[子供に年齢制限のあるサイトにアクセスさせたくない]

【アプリケーションの機能・実現方式】

・送信先機器属性判定機能

・条件外パケットフィルタリング機能

【認証方式・技術】

・ 玩具に割り振られた IP アドレスブロック等により機器を操作する者の年代を判定する

7.2.3.4.　公共メディア

（1）　電子書籍への閲覧制限サービス

【概要】

公共や学校図書館ではスペースの関係で蔵書を大幅に増やすのは難しい状況にあり、電子書籍に対する関心が高まっている。ただし、電子書籍を購入した場合、現在、貸し出しの扱いは難しい。電子的なコピーが自由にできるのでは著作権上問題であり、また公共図書館内など特定の場所に設置された PC でしか閲覧できないのでは利用しづらく普及は見込めないだろう。インターネットを通じた利用方法についても大きな課題である。

もし、購入する際にその電子書籍が利用できる範囲を予め特定でき、利用する PC がその条件にマッチしていることが認証できればこの課題を解決することができる。

例えば、学校図書館の場合は、利用された PC がその学校内に設置された PC または生徒（児童）の携帯型 PC であれば、閲覧期限付きで電子書籍のコピーや閲覧が可能になるといったものである。同様に公共図書館の場合は地域住人の家に設置された PC または地域住人が常時使用する PC であるかが認証できれば、同じく閲覧期限付きで電子書籍のコピーや閲覧を可能とする。

これらの仕組みを実現するのに IP アドレスに地域ブロックや学校ブロックを割り当てや IP アドレス認証は効果のあるものと思われる。

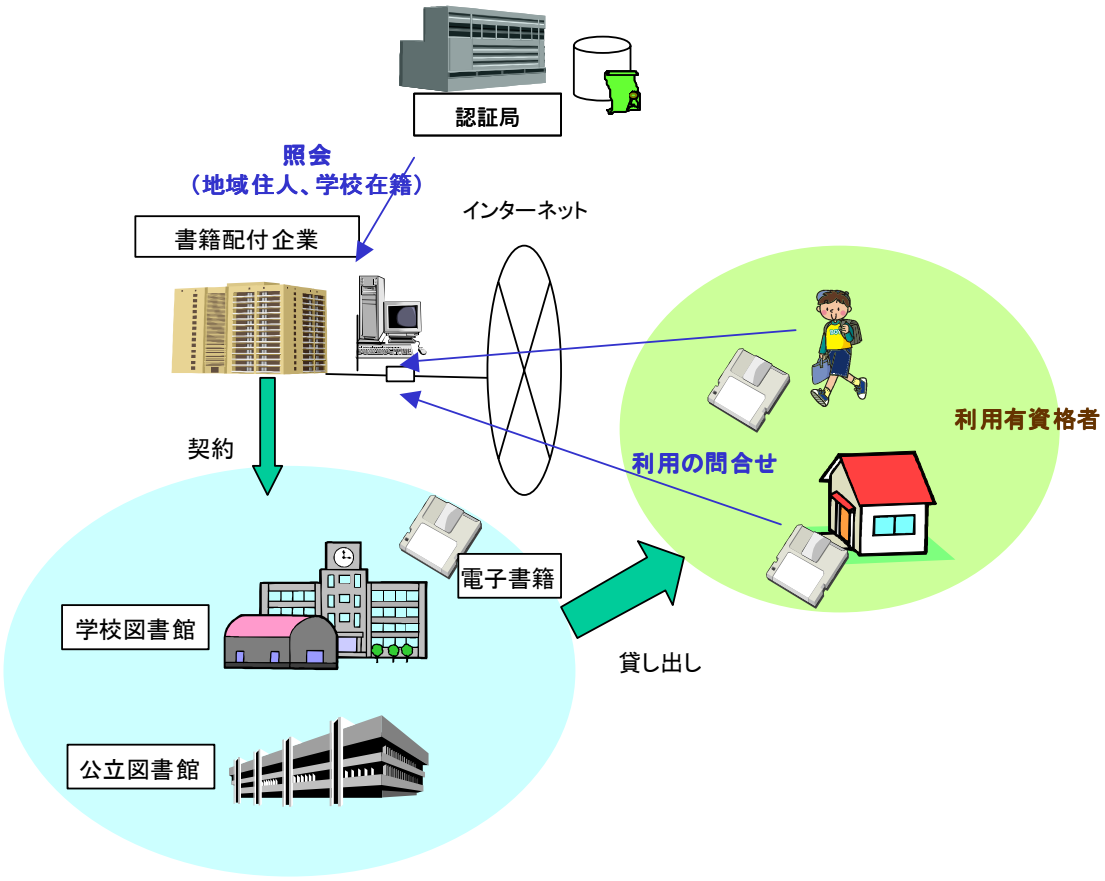


図 7-18　電子書籍の利用者認証サービス

【サービス対象者・ニーズ】

サービス提供元：

学校図書館、公共図書館　[蔵書数を増やしたい、管理費を下げたい]

サービス提供先：

（学校）生徒、地域住民　[最新の書籍を読みたい、書籍を持ち歩きたくない]

【アプリケーションの機能・実現方式】

・電子書籍利用資格確認機能

・電子書籍使用期限設定機能

・不正閲覧（資格外、期限外）防止機能

【認証方式・技術】

- 電子書籍使用時に、割り振られた IP アドレスから設置場所（地域）、施設（学校、図書館）の利用資格を判断する。
- 電子書籍使用時に、ネットワークを通じて IP アドレス認証局に登録されている利用者の情報（住所、所属先）から使用資格を判断する。

（2）　ネット投票サービス

【概要】

現行の選挙や住民投票は、投票場所や投票の時間帯が限られているため、当日の急な都合によっては投票に行くことが難しい場合がある。また、障害を持つ人が投票場に出向くことも現実的には難しい問題が多い。

もし、ネットワークを通じた安全な投票の仕組みがあれば、出先や投票場に行きにくい住民でも手軽に投票することが可能になる。安価なコストでネット投票が実現できれば、これまでの投票に加え、アンケート調査も兼ねた各種の投票サービスが登場する可能性がある。

ネット投票の仕組みとしては、投票時に個人やその属性の認証に加え、投票する機器の設置場所や形態、発信する IP アドレス等を予め特定させるようにすれば、なりすまし等不正を防ぐ手立てを増やすことができよう。

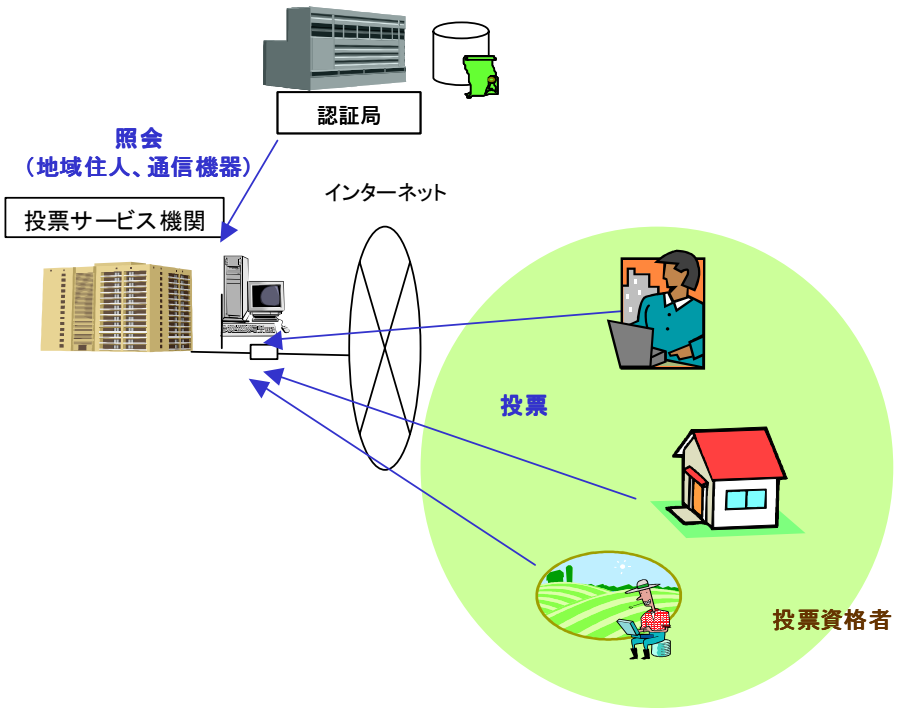


図 7-19　ネット投票サービス

【サービス対象者・ニーズ】

サービス提供元：

自治体　[投票コストを下げたい、民意を知る機会を多くしたい]

サービス提供先：

住民（選挙人）　[投票手段を増やしたい]

【アプリケーションの機能・実現方式】

・投票資格確認機能

・ネット投票機能

・投票結果分離機能（投票者と投じた内容を切り離す機能）

・集計結果提示機能

【認証方式・技術】

・ 投票時に、個人の認証他、投票機器に割り振られた IP アドレスから設置場所（地域)、形態（PC、携帯電話、キオスク端末、等）などからその投票に対する資格の有無や投票集団属性を判断する。

7.2.3.5.　社会インフラ

（1）　緊急時交通制御サービス

【概要】

緊急車両（パトカー、救急車、消防車等）は発進時に道路を優先的に通過できることになっているが、通行車両はサイレンの音や光により緊急車両の存在を認知するため、両端への待避などの行動は遅れがちとなる。また、緊急車両は信号が赤の場合でも交差点を通過するが、非常に危険を伴うためできるだけ緊急車両の動きに合わせて信号制御がされる方が望ましいといえる。

現在車両や交通インフラの IT 化が急速に進展しており、情報通信環境が十分に整い車両間や周辺の交通インフラと通信できるようになる日も遠くないと思われる。このような環境が整備された場合、車両や交通インフラへの IP アドレスの特定域の割り当て、認証は非常に重要になると思われる。前述の緊急車両の場合、GPS 技術と組み合わせることにより、通過道路の信号などの制御装置の IP アドレスブロックに対して進行意思（情報）を一斉配信することができる。各信号はその情報を受取り、適切に点灯時間をコントロールし、緊急車両を安全かつ短時間で現場に誘導することが可能となる。また同時に、周辺の車両（IP アドレスブロック）に対し、通過の意思を一斉配信することで、カーナビゲーションシステムや携帯電話などを通して、緊急車両が近づくことを早い時期に周辺に知らせることが可能となる。

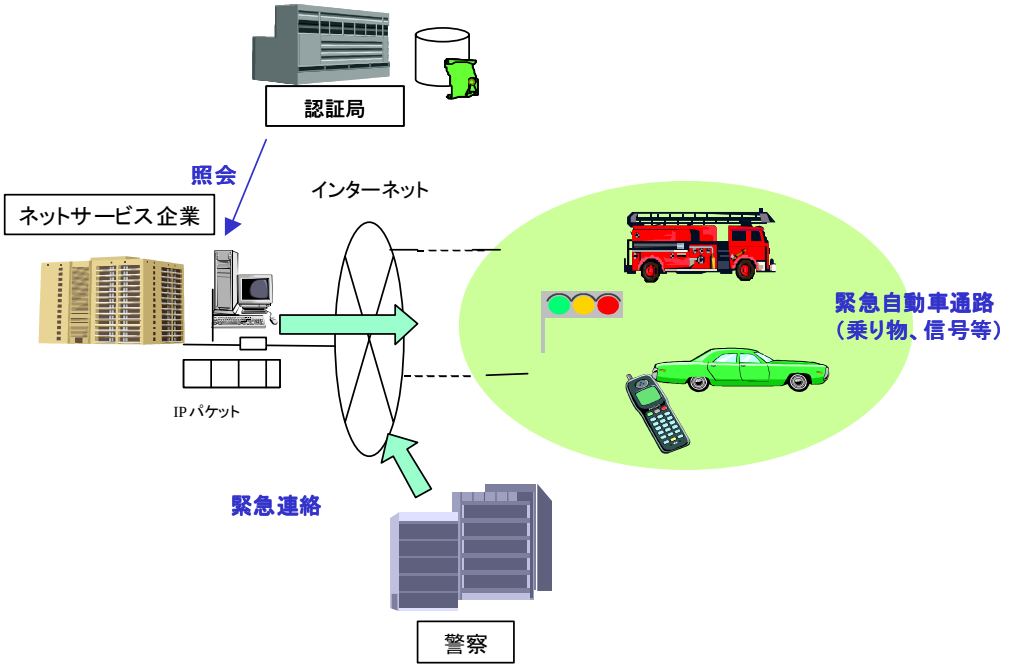


図 7-20　緊急時交通制御サービス

【サービス対象者・ニーズ】

サービス提供元：

公共基盤　[緊急情報を早く、確実に周辺に伝えたい]

サービス提供先：

警察・消防署（緊急車両）　[現場に早く、安全に到着したい]

【アプリケーションの機能・実現方式】

・緊急情報適正範囲ブロードキャスト機能

・緊急情報発信者確認（認証）機能

・緊急情報受信（表示）機能

【認証方式・技術】

- 緊急情報受信側で、発信者が確かに緊急情報を発信できる相手かどうかを IP により確認（認証）する。
- 発信側では、車両用として割り振られ、かつ自分から半径 200 メートル以内などに限定した IP アドレス域に緊急情報を一斉に配信する。

7.2.3.6.　医療

（2）　医療用 IP 閉域サービス

【概要】

医療用の情報は、当事者や許可のある者以外には絶対に渡ることがない仕組みが必要である。特にネットワークを通じた医療情報の交換には十分な配慮が必要がある。

こうした機密性を要するネットワークのセキュリティを高めるのに専用の IP アドレスブロックを設け、同時に認証を実施するのは効果的な方法である。例えば、医療用に使用される情報通信機器に特定の IP アドレスブロックが割り当てられた場合、ＩＳＰなどがパケットをチェックし、データ域が暗号化されていない場合は通過させない、というようなサービスが可能になる。また、通信相手について IP アドレスブロックや認証情報から不適切な相手かどうかを判別するようなサービスも考えられる。また、適切な送信相手に対しては、経路や優先度により同じ IP アドレスブロック内で閉域のネットワーク化が期待でき、レントゲン情報などは非常に大量のデータ容量を必要とするような場面での高速通信サービスが期待できる。

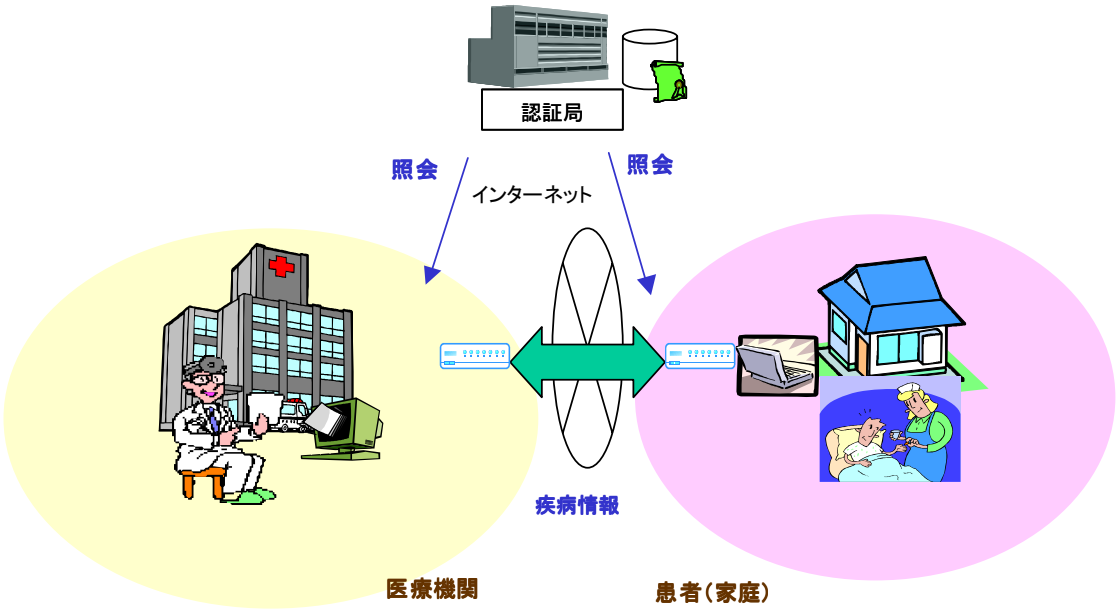


図 7-21　医療用 IP 閉域サービス

【サービス対象者・ニーズ】

サービス提供元：

ISP　[送受信相手が適切な所であるか確認したい]

サービス提供先：

医療機関　[医療情報を安全に送受信したい、大量の情報を高速に送りたい]

【アプリケーションの機能・実現方式】

・送受信先（属性）確認機能

・パケット暗号化確認機能

・医療機関閉域ネット（一種の VPN）構成機能

【認証方式・技術】

・ 医療情報の送信先、受信先について正規の相手かどうかを IP アドレス認証により確認する。また、送信先を特定の IP アドレスブロック域が振られた相手のみに限定し、不必要な発信を回避する。

（3）　家庭医療機器のネット対応

【概要】

高齢化社会を迎える中、家庭内で疾病を予防し、また病状を早期発見することは今後益々求められていくことになろう。近年では体温計、血圧計などの家庭用医療機器もディジタル化、高機能化が進んでおり、本人や家族が計測した場合でも信頼あるデータ値が得られるようになっている。

今後、これらの家庭内医療機器においても通信機能が標準装備されるようになった場合、地域の医療機関と連携して、複数の医療機器を定期的な自己計測することにより、リアルタイムで自分の健康度合いのチェックや医療機関からの助言が受けられるサービスが可能となる。また、老人や健康不安を持つ人には、一定の計測を越えたり、一定期間の入力がない、等の条件により自動的に医療センターに通知が行き、生存確保や急病対処の連絡を行なうようなサービスも考えられる。

このようなサービスにおいては、送信データが確かにその患者のものであり、指定された機器が正常な動作状態の下で送ったことを確認する仕組みが必要になる。

IP アドレス認証と特定ブロック域の割り当てはこのような場面においても有効な方法であると思われる。

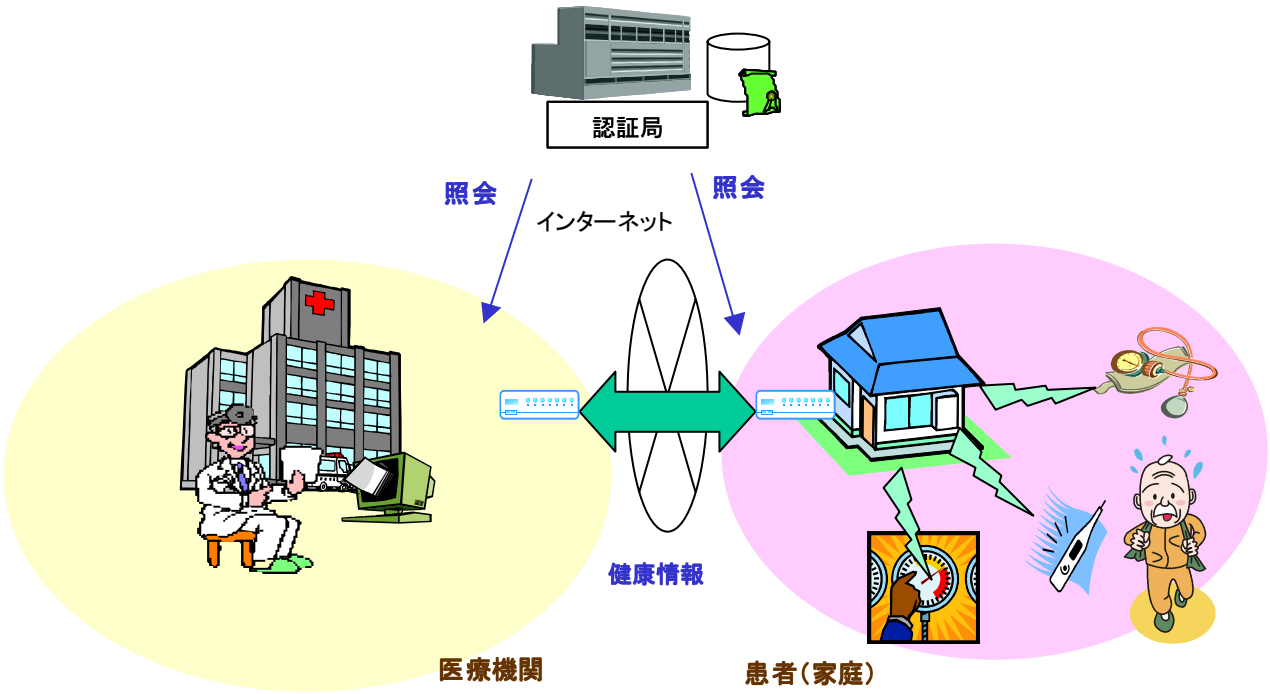


図 7-22　家庭用医療機器のネット対応イメージ

【サービス対象者・ニーズ】

サービス提供元：

医療機関、家庭医療機器メーカー[患者の最新の健康状態を総合的に知りたい]

サービス提供先：

住民（高齢者、病人など）　[健康状態を知りたい、担当医に現状を通知したい]

【アプリケーションの機能・実現方式】

・家庭内医療機器情報登録機能（初期および正常状態の登録）

・計測データ送信機能

・計測データ受信（相手先確認）機能

【認証方式・技術】

・ 計測データの送信先、受信先について正規の相手かどうかを IP アドレス認証により確認する。また、送信先を特定の IP アドレスブロック域が振られた相手のみに限定し、不必要な発信を回避する。

7.2.3.7.　その他

（1）　ライフスタイル集計サービス

【概要】

一般者の行動や購買活動を調べる方法として様々なマーケティング手法があるが、これは携帯型の情報通信機器を利用して行なうサービスである。携帯型の情報通信機器を街中に設置されたセンサーで認証し、特定のセグメント（年代や性別）の人の行動を集計、分析するものである。収集の段階では、IP アドレス情報自体は渡されず　IP アドレス認証用として付随登録されている年代や性別などのみがカウントされる。参加者は、情報通信機器だけを持ち歩くだけで、報酬（調査謝礼）を得ることができる。

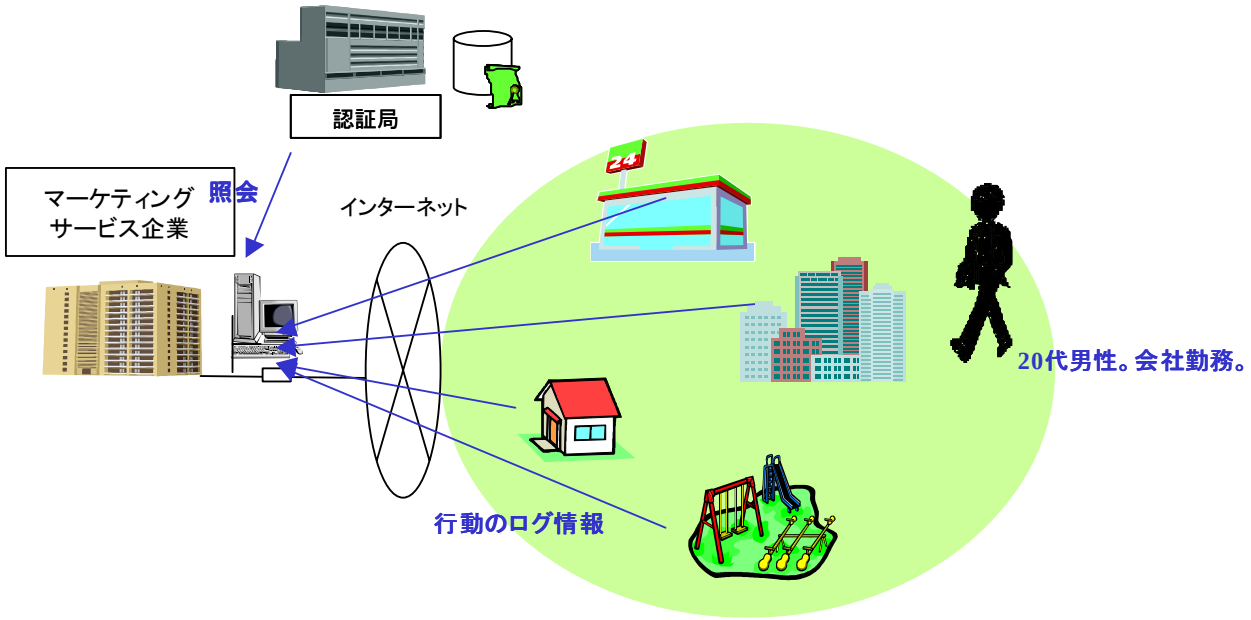


図 7-23　ライフスタイル集計サービス

【サービス対象者・ニーズ】

サービス提供元：

マーケティング会社、大手メーカー　[消費者行動をより正確に知りたい]

サービス提供先：

一般消費者　[労せず報酬を得たい]

【アプリケーションの機能・実現方式】

・携帯機器情報登録機能（初期および正常状態の登録）

・受信 IP 機器の利用者情報確認機能

・セグメント別行動情報集計・分析機能

【認証方式・技術】

・　センサーにより認識された IP アドレスをもとにその機器の利用者のマーケティングに関係するセグメント情報（年代や性別等）を確認する。

（2）　特定移動体向け情報配信サービス

IP アドレスの認証や IP アドレスブロックから移動体が判別できるようになることで次のようなサービスが実施できる可能性がある。

・安全情報についての車体間およびパトロールセンターへの通信（前後方の運転手の異常予測）
・別の移動体への自分の位置の通知
（電車が近づいていることを車側が事前に確認できるなど）

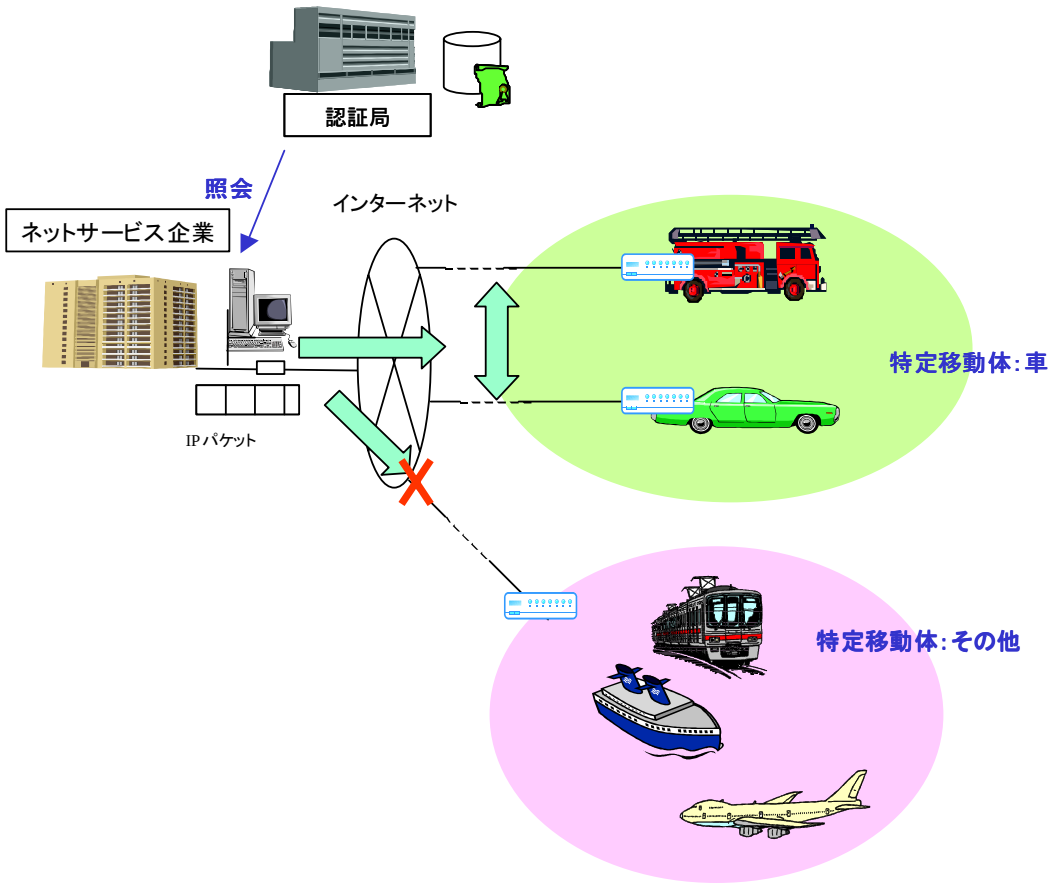


図 7-24　特定移動体向け情報配信サービス

【サービス対象者・ニーズ】

サービス提供元：

交通センター、警察　[最新の交通情報を提供し、安全性を高めたい]

サービス提供先：

各種移動体　[安全に通行したい、事故を防ぎたい]

【アプリケーションの機能・実現方式】

・通信相手（送信、受信）選別（認証）機能

・情報送信機能

【認証方式・技術】

・ IP アドレスブロックや自分の場所の情報をもとに、周辺の同じ移動体からの情報や地域特有の情報を認識する。

7.3.　まとめ

本章では、IP アドレスを認証することにより新たに展開できる可能がある情報通信サービスやビジネスのアイデアを探り、既存通信事業補完型、高セキュア通信機能型、新通信インフラ提案型に分類し、整理を行なった。本章に挙げたようなアイデアを実際に実現するには、技術的な問題から社会法制度の改正まで様々な障壁があるが、いずれも公共性の高いサービスであり、いくつかのアイデアについては実現に向けて今後詳細検討する価値があるものと思われる。

アイデアを検討する中で、現在の業務の中のセキュリティ面が弱い部分を補完するようなビジネス、サービスの展開はもちろんのこと、IP アドレス自体に特定の用途を持たせることができれば、従来では技術上やコスト上で実現が難しかったビジネス、サービスが短期、低コストで実現できる可能性がある。

実際に認証局を設立して、サービスを具現化する際には本章で挙げたようなビジネス、サービスをいずれ行なえるようにすることも視野に入れ、各種技術仕様を検討していくとよいであろう。

第8章 まとめ

内容

- 本報告書の位置づけ
- 各章のまとめ

8. まとめ

本調査研究は、IP アドレス認証局というインターネットレジストリにおいて運用される認証局に関する調査研究である。調査研究は IP アドレス認証局のあり方を求めることから始まり、認証局のマネジメントについて調査し、構築と応用に関する調査及び実施を行うという網羅的な内容である。IP アドレス認証局に関するプロジェクトは 3 年度計画で進められており、2003 年度はマネジメントに関する調査研究を行う 2 年目である。

2003 年度の調査研究はマネジメントに関する調査研究で、RIR（Regional Internet Registry：地域インターネットレジストリ）の認証局の調査をはじめ、アドレス資源管理業務における認証の必要性や適用方法、認証業務の検討、運用方針を含む CP/CPS（認証業務規定）の策定、認証情報の応用といった活動を行った。認証局のマネジメントにおける、要件、ポリシーとしての運用面、技術面、応用面の検討を進めたという位置づけになる。

今後は、今年度に検討を行った認証業務の立ち上げやシステムの構築、応用面の技術的検討を進め、本格的な運用に向けた活動が行われることになる。国内 ISP（Internet Service Provider：プロバイダ）や RIR との調整も重要になってくると考えられる。

本章では、本格的な運用に先立って今年度の調査研究の内容を参照しやすくするため、各章のポイントとなる内容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 アドレス認証局のマネジメントに関する調査研究について

本章では、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られた。今年度は、マネジメントに関する調査研究の為、特に認証業務に着目し、業務の検討や CP/CPS の策定に重点を置いている。このほかに RIR の認証局の調査や IP アドレス認証局と認証情報の応用に関する調査を行っており、それぞれを章を分けてまとめた。

第 2 章　アドレス資源管理における安全性

第 2 章は IP アドレス認証局の運用目的と設立の位置づけに関する調査の結果から要点をまとめたものである。

インターネットレジストリにおける登録業務の安全性は、登録データの安全性に依存する。登録時の認証機能に加え、電子署名を使ったデータ認証を行なえる仕組みができると基盤的認証基盤となる。RIR においても登録データの安全性の向上の為、認証局を用いた認証機能が実装されつつある。

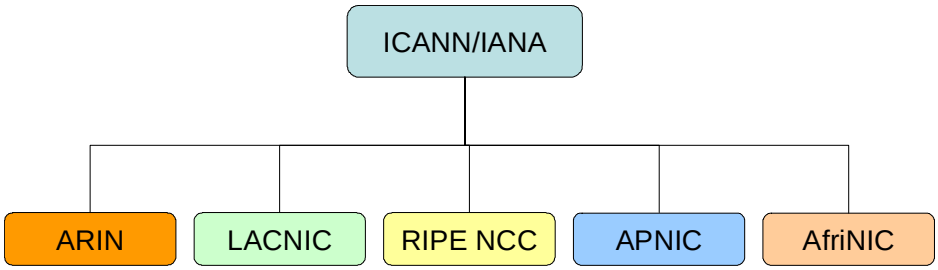


図 8-1　ICANN/IANA と RIR の構造

インターネットレジストリは、アドレス資源の割り振りを下位レジストリに対して行い、全体的に一意となるアドレス資源の管理を行っている。RIR（Regional Internet Registry：地域インターネットレジストリ）は NIR（National Internet Registry）や LIR（Local Internet Registry）を登録し、割り振りを行ってアドレス資源の情報を維持している。

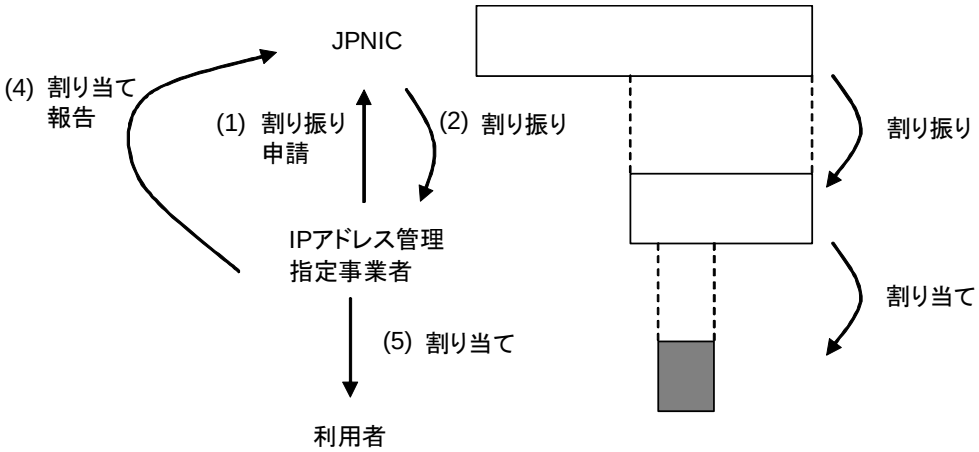


図 8-2　JPNIC における割り振り、割り当て概念図

アドレス資源の割り振りは、各種申請を通じて行われる。その際に登録される情報はアドレス資源管理に利用され、またその一部は、ネットワークの自律的運用の為に公開される。したがって登録時のデータ安全性や登録者の認証が必要となる。

第 3 章　RIR の認証局の状況

RIR のうち、APNIC や RIPE NCC ではすでに認証局を構築し、電子証明書（以下、証明書とよぶ）をユーザ認証の為に利用している（図 8-3、図 8-4）。これらの認証局とユーザ認証機能を利用した Web サービス（APNIC における MyAPNIC、RIPE NCC における LIR Portal）は現在も機能拡張が進んでいる（資源管理機能は未実装）。ヒアリングの結果、経路情報の保護に応用することが検討されている。IETF の CRISP（Cross Registry Service Protocol）WG における活動も見られる。今後、特に CRISP と RIR における認証局の応用に関して、継続して動向調査を行っていく必要があると考えられる。

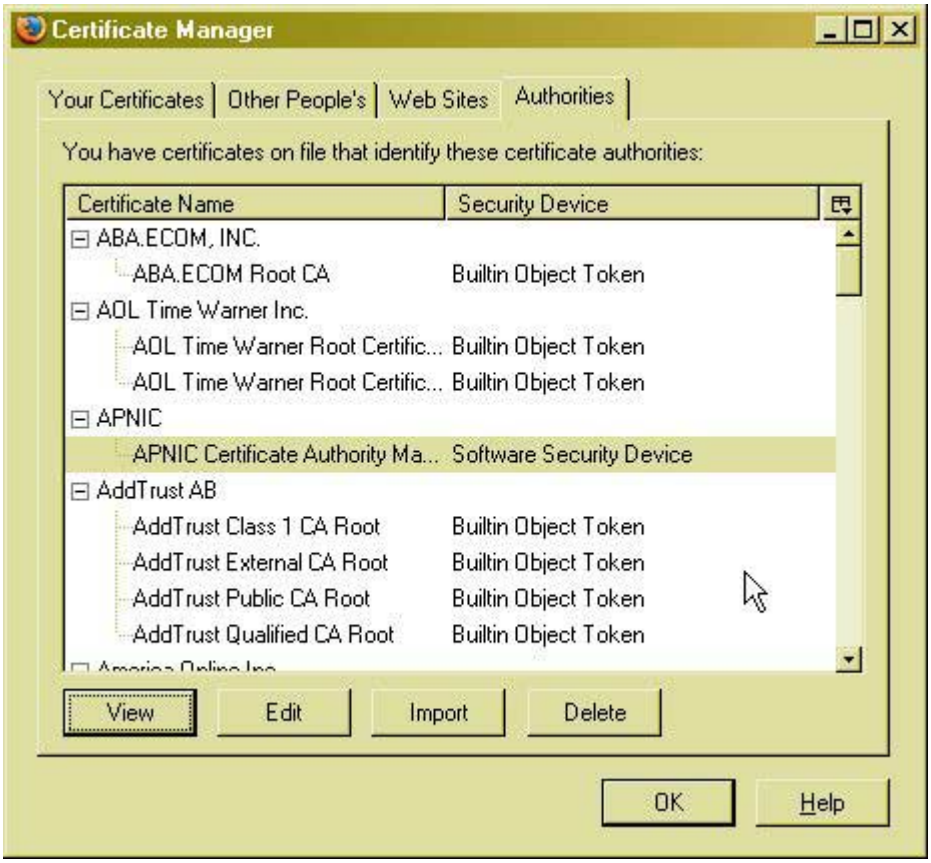


図 8-3　Web ブラウザに組み込まれた APNIC CA 証明書

資源管理の実装が進みつつある Web インターフェース MyAPNIC は https を利用しており、クライアント認証が利用できる。認証局はスタンドアローンで運用され、認証局証明書はユーザが各自に組み込む。クライアント証明書はパスポートのコピーを送付する等、業務担当者の個人認証を行なって発行業務が行われる。

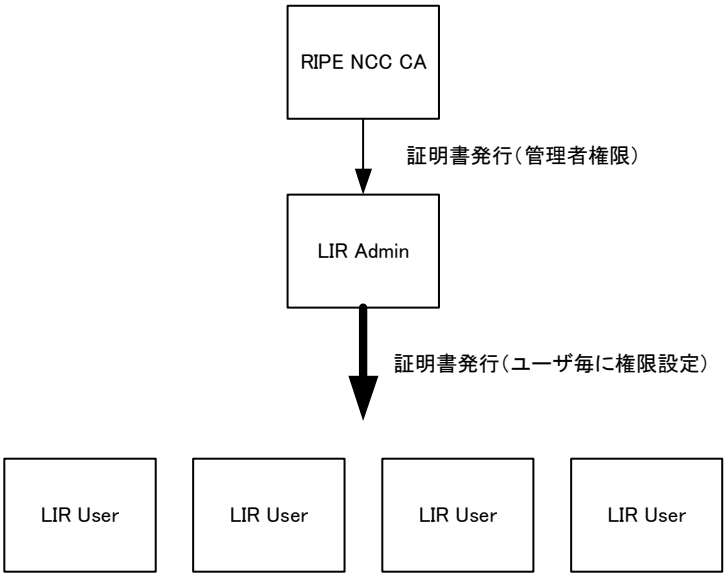


図 8-4　RIPE NCC における PMS（Privilege Management System）

RIPE NCC では、証明書の発行対象に権限を持たせ、LIR（Local Internet Registry、日本のプロバイダにあたる）における業務担当者の任命といった権限管理を行っている。IP アドレス認証局の登録業務の検討の結果、日本の ISP においてもこの構造と同様のモデルが適切であることが判明している（第 4 章にて詳説される）。JPNIC の場合には、このほかにユーザ証明書の発行における不正防止／監査可能となる認証手続きの設計、CP/CPS の策定などを行なっている。

第 4 章　認証業務の検討

JPNIC における認証局の運用を検討するにあたり、その業務（認証業務）の検討が必要である。IP アドレス認証局は、アドレス資源管理の業務構造に合わせ、かつ業務の確実性を確保する必要がある。その為、検討の際には下記のような留意事項を設けた。

・監査への配慮
・不正抑止・防止のモデル
・レジストリの業務体系に合わせる

本章では、各留意事項を考慮しながら行った検討と業務モデルについて述べた。モデル図を図 8-5 に示す。この業務モデルは、第 5 章で述べられる CP/CPS 策定の検討に使われ、また第 6 章で述べられる認証局ソフトウェアの要件検討にも使われた。

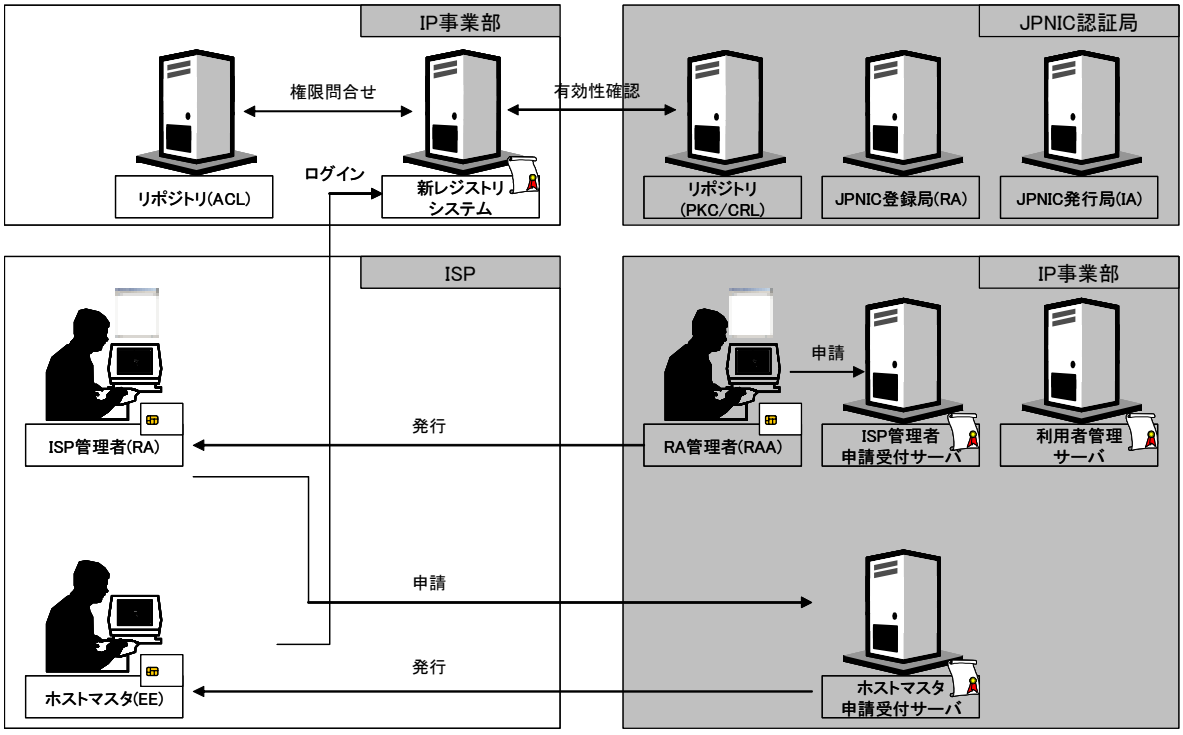


図 8-5 業務モデル

ISP における IP 管理担当者（ホストマスタ）の業務と LRA（Local Registration Authority）との分離を行い、権限の分離を図る。アドレス資源管理には、証明書を使った認証を用いる。

第 5 章　CP/CPS 策定の為の検討

認証業務の信頼性を確保する為、CP/CPS（認証業務規程）策定を行った。CP/CPS の策定には既存のフレームワーク（RFC2527）のみならず、既存の認証局運用にもとづく多くの検討材料が必要である。今回は国内の認証局に関わる専門家と専門の業者を行ったため、今後、国内における CP/CPS 策定活動の参考資料になるように、検討資料と記述例をまとめた。

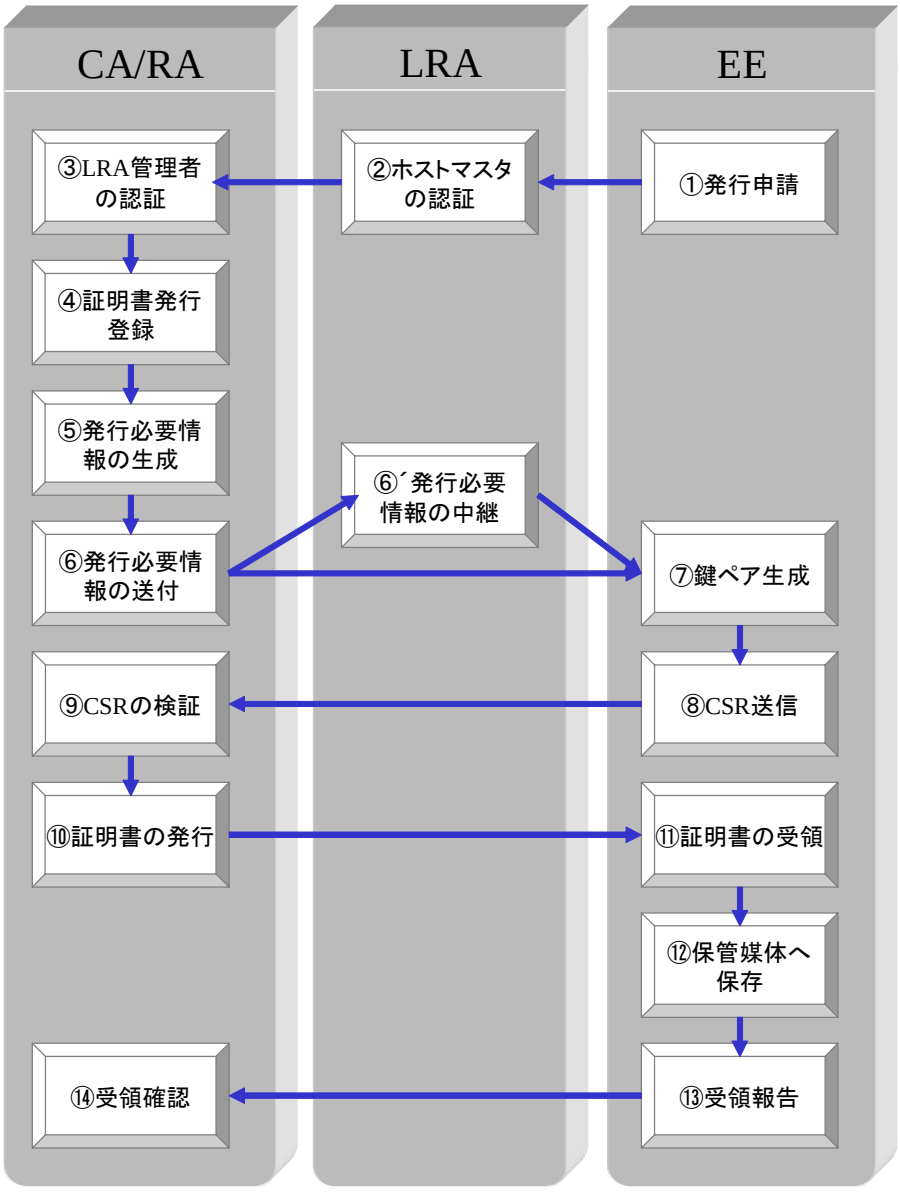


図 8-6 ホストマスタ証明書の発行手順

資源管理業務を行うホストマスタの証明書を発行する手順。この他に設備・組織の要件や証明書プロファイルなどの検討を行った。

第 6 章　認証局ソフトウェアの要件検討

認証業務は、認証局のシステムによって支えられ遂行される。認証局ソフトウェアは高価なケースがあるが、適切な検討を行うことで業務システムの認証システムとして活用が可能だと考えられる。そこで認証局スフとウェアを利用した実験環境を構築し、認証局ソフトウェアの検討の留意点や要件についてまとめた。

-

第 7 章　認証情報の応用に関する検討

アドレス資源管理を行っているインターネットレジストリで認証情報を持つことにより、インターネットを利用するアプリケーションで PKI を用いた認証基盤を構築することが可能だと考えられる。認証情報を応用することで、どのようなアプリケーションが考えられるようになるのか、ヒアリングや検討会を通じて検討を行った。ここでは自由な発想を元にアイディアを集約し分類してまとめておく。今後、実現性の検討を行っていく題材とする。

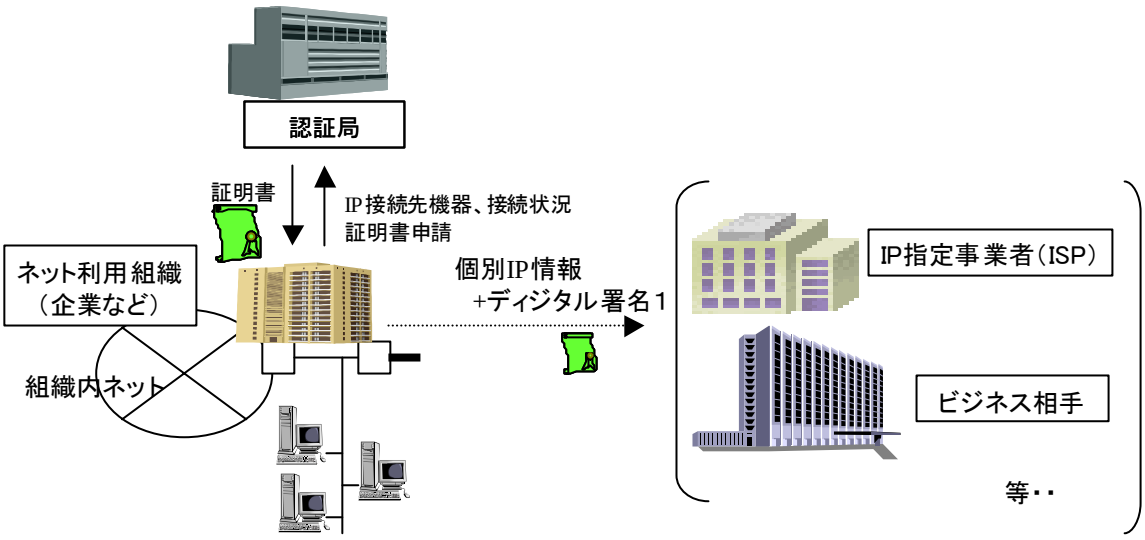


図 8-7　IP アドレス利用先の認証

アドレス資源の利用の登録を証明する基盤として、登録されたアドレス資源の所属性を検証する。IP アドレスが判明すると、アクセスコントロールに利用することができる。

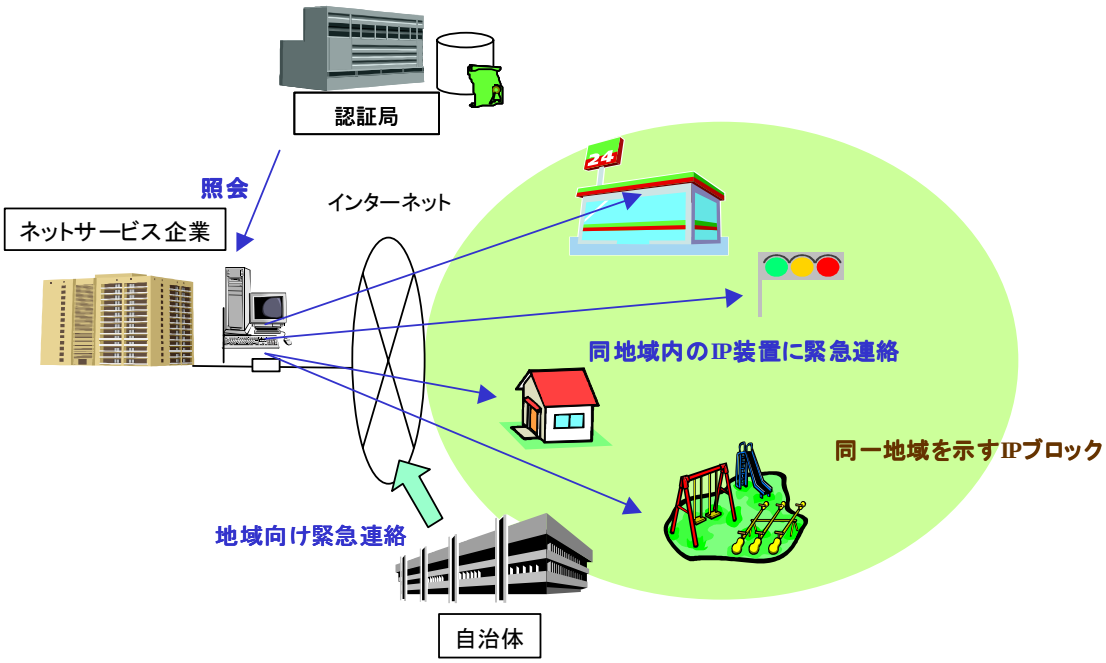


図 8-8　災害時の地域一斉連絡

ネットワークに接続されたノードを有効利用するためには、そのノードの属性を確認したり、通信する際の認証を行ったりすることが重要となる。特にインフラ設備、緊急の設備では IP のネットワークから安全性を考慮した設計を行なう必要がある。ここでは、IP アドレスの属性を証明する認証局があり、その証明書を検証することでどの分野のノードであるのかを確認することができる。また Web などに利用されるインターネットと区別したファイアウォール／ネットワーク機器によるアクセスコントロールも考えられる。

Appendix.1 および 2

　認証業務と方針の検討結果である CP/CPS のドラフト版を添付する。その際に、IP アドレス認証局と認証業務の拡張性を持つために設置した JPNIC ルート認証局の CP/CPS を添付する。

おわりに

これまでに行われてきたアドレス資源管理は、インターネットという自律的なネットワークの集合体で、アドレスが健全に利用されることを目指したものである。アドレスブロックを適切な範囲で割り振ることによって、アドレス資源の適切な利用や経路情報の最適化が図られる。この役割の必要性は問うまでもないだろう。

本調査研究で研究対象としてきた IP アドレス認証局は、このアドレス資源の健全な利用に、ネットワークの安全性の観点を取り入れたものである。インターネットが、単に匿名性のあるネットワークを作り出すだけでなく、緊急通報や重要な商取引をも実現するネットワークだとしたら、認証基盤は必要不可欠になる。

本報告書の「はじめに」で問いかけた、インターネットにおけるアドレスと実在性との関係は、おそらく様々な属性に応じて構築されていくと考えられる。商取引の属性、教育の属性、医療の属性など、通信を行うもの同士で相手を認める仕組みが使われると考えられる。

IP アドレス認証局は、今の段階では、様々な属性を付加する前のアドレス資源の管理のために利用される認証局である。このプロジェクトが、通信相手の属性を確認し、安心してやりとりができるような環境作りに繋がるよう、今後も調査研究を継続し、構築を進めたいと考えている。

Appendix 1

IP アドレス認証局

認証業務規定（CP/CPS）

ドラフト版

<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 5 章で述べる。
  - 本 CP/CPS は RFC3647 のフレームワークに則って記述されている。
  - URL などを含め、公開が行われる前に一部改定されることが想定されている。

目次

1. はじめに

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 CP/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 CP/CPS、証明書所有者同意書によって包括的に定める。なお、本 CP/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 CP/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)CP/CPS

CP/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 CP/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 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	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	1.2.392.00200175
JPNIC IP アドレス認証局 認証業務規程（CP/CPS）	1.2.392.00200175.2 （OID は決定後に記述される）
EE 証明書ポリシ	1.2.392.00200175.2 （OID 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
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

登場者	略称	役割、説明
証明書申請者	申請者	EE 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 CP/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 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 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（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。

登場者	略称	役割、説明
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。
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。

1.4. 証明書の使用方法

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 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。

1.4.3. 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 CP/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. 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。

1.5.3. CP/CPS 承認手続

本 CP/CPS の改訂は、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 CP/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 CP/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 CP/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。

用語	略称	説明
RFC 3647 （ Request For Comments 3647）		認証局 や PKI のための CP/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。
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。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

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）
- 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、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。

- CP/CPS については、改訂の都度、本 CP/CPS「9.12.2.通知方法及び期間」で定める時期に公表される。
- 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 CP/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、JPNIC 認証局の判断により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。＊公表時のみ

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. 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。

3.1.4. 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。

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. 個人的本人性の認証

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行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確認する。

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、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。

3.2.6. 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 CP/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 CP/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

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。

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

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。

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

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送付する。

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 CP/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

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。

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

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。

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。

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

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。

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。

サーバ証明書に関しては、本認証局は、本 CP/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、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。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 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。

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

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。

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

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。

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 PKI 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

本認証局を含む JPNIC 認証局は、本 CP/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 CP/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。

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 CP/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 CP/CPS「4.7.証明書の鍵更新」に定める手続とする。

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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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

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。

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

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ほかに、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 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
- 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、LRA 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

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。

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。

4.9.6. 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。

4.10. 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 CP/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 CP/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 CP/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。

EE は私有鍵を EE 自身で生成及び管理する。

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、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。

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。

5.1.3. 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。

5.1.5. 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、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。

5.1.7. 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 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。

表 5-1 名称とその役割

			役割名称	役割の説明
			運営委員会	・ 監査報告の確認及び承認 ・ 認証局運営責任者への監査指摘事項対応指示 ・ JPNIC 認証局の運営方針の決定 ・ 証明書ポリシ、運用ポリシ及び運用ポリシ変更の最終承認 ・ 認証局運営責任者の任命・解任等 ・ その他、重要な事項の協議及び決議

			役割名称	役割の説明
運営組織			認証局運営責任者	・ 認証サービス及び運用組織の統括 ・ 監査指摘事項への対応統括 ・ 運用管理者の任命・解任 ・ システム変更及び運用ポリシ変更の承認 ・ 非常時対応等の指揮、監督
	運用組織		運用管理者	運用組織の統括 ・ 運用担当者の任命・解任 ・ 運用担当者の教育計画策定及び実施 ・ 運用担当者の入室権限付与 ・ 運用担当者の作業報告確認 ・ 認証局私有鍵の活性化操作、非活性化操作の立会い ・ 非常時の対応指示 ・ 作業報告書、貸出簿等、運用記録の保管・管理等 ・ その他、運用全般の管理
		運用担当者	ログ検査者	・ 監査ログ、入退室ログ等の検査
			鍵管理者	・ キーセレモニ時の認証局鍵生成作業立会い ・ 認証局鍵廃棄時の立会い ・ バックアップ私有鍵の管理
			セキュリティ管理者	・ 認証局システムのセキュリティ設定及び変更 ・ キーセレモニ時の RAO の登録、発行
			認証局管理者	・ 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
			登録局管理者	・ 証明書発行、失効の登録作業 ・ 登録局の管理運営
			審査者	・ LRA 管理者証明書発行申請の受付 ・ 証明書発行に係る審査 ・ 承認者への LRA 管理者証明書の発行依頼
			承認者	・ 審査結果の承認 ・ 発行登録作業の承認
			保守員	ネットワーク技術者、システム技術者及び監視技術者の総称 ・ ネットワークの設定、維持管理等 ・ システム技術サポート、サーバの設定・維持管理等 ・ 不正侵入及びシステム状況等の監視
			ベンダー保守員	・ 各種機器の故障等の対応

			役割名称	役割の説明
	ローカル登録局		ローカル登録局	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、登録局業務において、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。
			ローカル登録局責任者	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 管理者の任命及び解任
			ローカル登録局管理者	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。

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

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

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. 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. 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

JPNIC 認証局は、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 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。

5.3.5. 仕事のローテーションの頻度及び順序

JPNIC は、JPNIC 認証局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。

5.3.7. 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

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. 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
- 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

5.4.2. 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。

5.4.4. 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。監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。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、認証局サーバ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 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

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、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、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。

5.5.6. 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 CP/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 CP/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 CP/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 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。

5.7.4. 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（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. 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、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。

6.1.2. 所有者に対する私有鍵の交付

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

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。

6.1.5. 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 と呼ぶ）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 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 CP/CPS「4.12.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。

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。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。

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。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。

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。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

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 CP/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、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。

7.1.2.4. 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 CP/CPS「7.1.6.証明書ポリシ OID」、policyQualifiers の値は本 CP/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 CP/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、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。

7.1.7. 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 CP/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 IP アドレス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	c		
digitalSignature		1	1
nonRepudiation		0	0
keyEncipherment		1	1
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 Services, OU=JPNIC Resource Service Certification Authority

※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）

※3　C=JP, O=Japan Network Information Center, OU=Internet Resource Services, 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 IP アドレス認証局が発行する 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 Services, OU=JPNIC Resource Service Certification Authority

7.3. OCSP プロファイル

OCSP は使用しない。

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。

8.2. 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。

8.5. 不備の結果としてとられる処置

本認証局を含む JPNIC 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。本認証局を含む JPNIC 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

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. 情報の秘密性

9.3.1. 秘密情報の範囲

本認証局を含む JPNIC 認証局が保持する情報は、本 CP/CPS「2.2.証明情報の公開」で公表すると定めた情報、本 CP/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 CP/CPS で公表すると定めた情報、本 CP/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。

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 CP/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

本認証局を含む JPNIC 認証局は個人情報保護の重要性を認識し、個人情報を本 CP/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啓蒙活動を実施する。

（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。

9.5. 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 CP/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
- （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
- 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

9.6.2. 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。

- 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
- 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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 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。

9.12.3. 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 CP/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

本認証局を含む JPNIC 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 CP/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 CP/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 CP/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。

Appendix 2

JPNIC ルート認証局

認証業務規定（CP/CPS）

ドラフト版

<添付資料 2 について >

- この資料は、JPNIC ルート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 5 章で述べる。
  - 本 CP/CPS は RFC3647 のフレームワークに則って記述されている。
  - URL などを含め、公開が行われる前に一部改定されることが想定されている。

目次

1. はじめに

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）における JPNIC ルート認証局（以下、本認証局と呼ぶ）の認証業務に関する運用規則を規定した文書である。

本認証局は、JPNIC が運営する公開鍵基盤において、認証階層経路の最上位に位置するルート認証局であり、本 CP/CPS に基づいて、JPNIC の下位認証局に対して証明書を発行する等の認証サービスを提供する。

JPNIC は、認証サービスの提供にあたり、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CP/CPSによって定める。本CP/CPSにおける証明書所有者とは、証明書発行申請を行い、自ら鍵ペアを生成し、本認証局により証明書の発行を受ける、JPNIC の下位認証局をいう。

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CP/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。

本 CP/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。

1.2. 文書の名前と識別

本 CP/CPS の正式名称は「JPNIC ルート認証局 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 ルート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	1.2.392.00200175
JPNIC ルート認証局 認証業務規程（CP/CPS）	1.2.392.00200175 （OID は決定後に記述される）
下位認証局証明書ポリシ	（下位認証局の CP/CPS にて規定されるサービス毎に異なる OID が記述される）

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
証明書申請者		JPNIC の運営する下位認証局の証明書の発行申請をする者
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、本認証局により証明書の発行を受ける主体を表す。本 CP/CPS では、JPNIC の下位認証局をいう。
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 ルート認証局内の発行局及び JPNIC 下位認証局内の発行局の総称。JPNIC ルート認証局及び JPNIC 下位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 登録局		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。証明書所有者の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 の認証業務に関する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。

登場者	略称	役割、説明
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の証明書に電子署名を行う。
JPNIC 下位認証局		JPNIC ルート認証局により証明書の発行を受ける、JPNIC の運営する下位認証局
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 下位認証局、JPNIC 登録局及びリポジトリから構成される。
下位認証局証明書		JPNIC ルート認証局が、JPNIC 下位認証局に対して発行する証明書
EE 証明書		JPNIC 下位認証局がエンドエンティティに対して発行する証明書

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 CP/CPS に基づき発行される下位認証局証明書は、当該認証局の発行する公開鍵証明書の検証のために使われるものとする。JPNIC 下位認証局を信頼して利用する者は、当該証明書の信頼性を本認証局の公開鍵証明書によって検証することができる。

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、本 CP/CPS「1.4.1.適切な証明書の使用」に規定する目的で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。

1.4.3. 証明書の相互運用性

本認証局を含む JPNIC 認証局は、予め定められた方法により、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 CP/CPS を管理する組織及び問合せ先を次に定める。

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. 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運営委員会が行う。

1.5.3. CP/CPS 承認手続

本 CP/CPS の改訂は、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 CP/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 CP/CPS では、特に断らない限り JPNIC 下位認証局の証明書、自己署名証明書及びリンク証明書を総称して「証明書」と呼ぶ。

用語	略称	説明
認証局		証明書の発行・更新・失効、認証局等私有鍵の生成・保護及び証明書所有者の登録を行う機関。本CP/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 CP/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。
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。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

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）
- 下位認証局証明書（JPNIC ルート認証局）
- JPNIC 下位認証局が発行する EE 証明書（JPNIC 下位認証局）＊公表時のみ
- CRL（JPNIC ルート認証局、JPNIC 下位認証局）
- CP/CPS（JPNIC ルート認証局、JPNIC 下位認証局）

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、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。

- CP/CPS については、改訂の都度、本 CP/CPS「9.12.2.通知方法及び期間」で定める時期に公表される。
- 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 CP/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、JPNIC 認証局の判断により適宜更新が行われる。
- JPNIC 下位認証局が発行する EE 証明書については、発行及び更新の都度公表される。＊公表時のみ

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. 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、認証局の運営に係わる組織名に適切な範囲で関連したものでなければならない。

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。

3.1.4. 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、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. 組織的本人性の認証

証明書申請者は、運営委員会において、組織の認証として、下位認証局証明書の発行申請の許可を受けていることを証する書類、組織情報等を提出し、本認証局による審査を受けなければならない。

3.2.3. 個人的本人性の認証

本認証局は、証明書申請者が運営委員会により承認された下位認証局の正当な権限者であることを確認する。

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、証明書申請者が、下位認証局の組織に関する情報の申請を行うための正当な権限を有していることを確認する。

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 CP/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 CP/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

本認証局は、証明書の失効申請を受付けた場合、下位認証局の組織に関して提供された情報をもとに、正当な失効要求であることを確認する。

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

証明書の発行申請を行うことができる者は、運営委員会から承認を受けた下位認証局の組織から任命された者とする。

4.1.2. 登録手続及び責任

証明書申請者は、証明書を申請するにあたって、本認証局に次の情報を提供するものとする。

- 証明書発行申請書
- 運営委員会による承認を受けていることを示す情報
- CSR

また、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 CP/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

本認証局は、本 CP/CPS「3.2.初回の本人性確認」に基づき、証明書申請者の本人確認及び組織確認を行う。

4.2.2. 証明書申請の承認又は却下

本認証局は、証明書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。申請を受理するにあたっては、運営委員会の承認の確認を行うものとする。

4.2.3. 証明書申請の処理時間

本認証局は、本 CP/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、証明書申請者から提出された CSR の公開鍵に対し、本 CP/CPS「7.1. 証明書プロファイル」に準じた内容で、本認証局の署名を付した証明書を発行する。

4.3.2. 認証局の所有者に対する証明書発行通知

本認証局は、発行した証明書をフロッピーディスク等の外部記憶媒体に保管し、証明書申請者に手渡しすることにより発行通知を行ったものとする。

4.4. 証明書の受領確認

4.4.1. 証明書の受領確認の行為

証明書申請者は、本認証局の認証局管理者立会いのもと、証明書の内容確認を行うものとする。

4.4.2. 認証局による証明書の公開

本認証局を含む JPNIC 認証局は、本 CP/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

本認証局が発行する証明書の用途は、証明書の発行対象である組織が提供するサービス又は製品に定められている用途に制限されるものとする。

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
- 利用目的の確認と利用目的内での利用
- 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 CP/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 CP/CPS「4.7.証明書の鍵更新」に定める手続をとる。

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書申請を行うことができる者

本 CP/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 CP/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 CP/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 CP/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 CP/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 CP/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 CP/CPS「4.7.2.新しい公開鍵の証明書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 CP/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 CP/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 CP/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 CP/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 CP/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

証明書所有者は、次の場合に、本認証局に対し証明書の失効申請を行わなければならない。

- 証明書記載事項に変更があった場合
- 私有鍵が危殆化、若しくはそのおそれがある場合
- 証明書の内容、利用目的が正しくない場合
- 証明書の利用を中止する場合

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、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
- 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

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
- 本認証局
- その他 JPNIC が指定した者

4.9.3. 失効申請手続

証明書の失効申請を行う者は、証明書失効に関する必要な情報を手交にて提出することにより、本認証局に証明書の失効申請を行う。

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。

4.9.6. 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かかわらず、［期間決定後に記述される］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により、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

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 CP/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 CP/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 CP/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、本認証局は当該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。

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い、また監視カメラによる記録を行う。認証設備室へは、入室権限を有する複数人が同時に立ち入る必要がある。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。

5.1.3. 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。また本認証局は、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、適切な入退室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、別地の適切な入退室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 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。

表 5-1 名称とその役割

			役割名称	役割の説明
			運営委員会	・ 監査報告の確認及び承認 ・ 認証局運営責任者への監査指摘事項対応指示 ・ JPNIC 認証局の運営方針の決定 ・ 証明書ポリシ、運用ポリシ及び運用ポリシ変更の最終承認 ・ 認証局運営責任者の任命・解任等 ・ その他、重要な事項の協議及び決議

			役割名称	役割の説明
運営組織			認証局運営責任者	・ 認証サービス及び運用組織の統括 ・ 監査指摘事項への対応統括 ・ 運用管理者の任命・解任 ・ システム変更及び運用ポリシ変更の承認 ・ 非常時対応等の指揮、監督
	運用組織		運用管理者	運用組織の統括 ・ 運用担当者の任命・解任 ・ 運用担当者の教育計画策定及び実施 ・ 運用担当者の入室権限付与 ・ 運用担当者の作業報告確認 ・ 認証局私有鍵の活性化操作、非活性化操作の立会い ・ 非常時の対応指示 ・ 作業報告書、貸出簿等、運用記録の保管・管理等 ・ その他、運用全般の管理
		運用担当者	ログ検査者	・ 監査ログ、入退室ログ等の検査
			鍵管理者	・ キーセレモニ時の認証局鍵生成作業立会い ・ 認証局鍵廃棄時の立会い ・ バックアップ私有鍵の管理
			セキュリティ管理者	・ 認証局システムのセキュリティ設定及び変更 ・ キーセレモニ時の RAO の登録、発行
			認証局管理者	・ 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
			登録局管理者	・ 証明書発行、失効の登録作業 ・ 登録局の管理運営
			審査者	・ 下位認証局証明書の発行申請の受付 ・ 下位認証局証明書の発行に係る審査 ・ 承認者への下位認証局証明書の発行依頼
			承認者	・ 審査結果の承認 ・ 発行登録作業の承認
			保守員	ネットワーク技術者、システム技術者及び監視技術者の総称 ・ ネットワークの設定、維持管理等 ・ システム技術サポート、サーバの設定・維持管理等 ・ 不正侵入及びシステム状況等の監視
			ベンダー保守員	・ 各種機器の故障等の対応

5.2.2. 職務毎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

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、操作者毎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

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. 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. 経歴の調査手続

JPNIC 認証局業務に係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

JPNIC 認証局は、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 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。

5.3.5. 仕事のローテーションの頻度及び順序

JPNIC は、JPNIC 認証局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。

5.3.7. 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

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. 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
- 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

5.4.2. 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。

5.4.4. 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。監査ログは、改ざん防止対策を施し、かつ改ざん検出を可能とする。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、認証局サーバ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 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の記録を維持、管理する。

（ ）内は保管期間

- 本 CP/CPS 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を確認する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

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、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の重要なデータ及び監査ログを、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、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。

5.5.6. 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ものとする。監査ログファイル用の履歴収集システムについては、本 CP/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。保管期間の過ぎた古い媒体は破棄する。

5.6. 鍵の切替

本認証局の私有鍵の有効期間は 20 年とし、10 年毎に鍵ペアの更新を行う。JPNIC 下位認証局の私有鍵の有効期間は 10 年とし、8 年毎に鍵ペアの更新を行う。本認証局の鍵ペア更新時には、古い公開鍵と新しい公開鍵の認証パスを構築するリンク証明書を発行し、リポジトリ上で公表する。新たな公開鍵は、本 CP/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

本認証局の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

本認証局の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。

- 下位認証局証明書等の失効手続
- 私有鍵の廃棄及び再生成手続
- 下位認証局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.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（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. 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、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。

6.1.2. 所有者に対する私有鍵の交付

本認証局は JPNIC 下位認証局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

JPNIC 下位認証局の公開鍵は、本 CP/CPS「3.2.1.私有鍵の所持を証明する方法」に定める手続により検証され、その受渡しはオフラインで行う。

6.1.4. 検証者に対する認証局の公開鍵の交付

本認証局の公開鍵の配布は、本認証局の登録局管理者が、下位認証局証明書の管理者に対して、手渡しによって行う。検証者に対する本認証局の公開鍵の配布は、安全かつ確実な手段により行う。

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。JPNIC 下位認証局については、2048 ビットの 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 と呼ぶ）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

本認証局の私有鍵は、発行する証明書及び CRL への署名に使用する。証明書の keyUsage は keyCertSign、cRLSign のビットを使用する。

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 CP/CPS「4.12.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、JPNIC 下位認証局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。

JPNIC 下位認証局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。

JPNIC 下位認証局の私有鍵は、当該認証局自身が私有鍵の生成を行い、当該認証局自身で格納を行う。

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。

JPNIC 下位認証局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。

JPNIC 下位認証局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場合には、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。

JPNIC 下位認証局の私有鍵は、当該認証局自身で確実に破棄するものとする。

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。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。

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 20 年、私有鍵の有効期間は 10 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。

下位認証局証明書の有効期間は 10 年とする。

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。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

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 CP/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

本認証局が発行する証明書は全て keyCertSign と cRLSign のみを使用する。この拡張は critical である。

7.1.2.4. certificatePolicies

下位認証局証明書は certificatePolicies 拡張を使用する。policyIdentifier の値は本 CP/CPS「7.1.6.証明書ポリシ OID」、policyQualifiers の値は本 CP/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。

自己署名証明書は certificatePolicies 拡張を使用しない。

7.1.2.5. cRLDistributionPoints

下位認証局証明書及びリンク証明書は、cRLDistributionPoints 拡張を使用する。distributionPoint として、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 CP/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

下位認証局証明書は、本 CP/CPS「1.2.文書の名前と識別」に定める下位認証局証明書ポリシの 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

下位認証局証明書は、ポリシ修飾子の値として本 CP/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(1) JPNIC ルート認証局が発行する証明書プロファイル（1）

Field	critical flag	JPNIC 下位認証局 証明書	JPNIC ルート認証局 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*2	PrintableString*2
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		notBeforeの時刻より10年後	notBeforeの時刻より20年後
subject	NA		
		PrintableString*1	PrintableString*2
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		JPNIC 下位認証局 公開鍵のBIT STRING	JPNIC ルート認証局 公開鍵のBIT STRING
authorityKeyIdentifier	n		
keyIdentifier		JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 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	JPNIC 下位認証局 公開鍵の160bit SHA-1ハッシュ値	JPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		本CPのOID	使用しない
policyQualifiers			
policyQualifierId		CPSUri	使用しない
qualifier		本CP/CPSを公開するURI	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	使用しない
reasons		使用しない	使用しない
cRLIssuer		使用しない	使用しない

表 7-2(2) JPNIC ルート認証局が発行する証明書プロファイル（2）

Field	critical flag	JPNIC IPルート認証局リンク証明書OldwithNew	JPNIC ルート認証局リンク証明書NewwithOld
version	NA	2	2
serialNumber	NA	non-negative integer	non-negative integer
signature	NA		
algorithm		sha1withRSAEncryption	sha1withRSAEncryption
parameters		null	null
issuer	NA		
		PrintableString*2	PrintableString*2
validity	NA		
notBefore		UTCTime	UTCTime
notAfter		UTCTime 古い自己署名証明書の notAfter	UTCTime 古い自己署名証明書の notAfter
subject	NA		
		PrintableString*2	PrintableString*2
subjectPublicKeyInfo	NA		
algorithm		rsaEncryption	rsaEncryption
parameters		null	null
subjectPublicKey		古いJPNIC ルート認証局公開鍵のBIT STRING	新しいJPNIC ルート認証局
authorityKeyIdentifier	n		
keyIdentifier		新しいJPNIC ルート認証局 公開鍵の160bit	古いJPNIC ルート認証局 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	古いJPNIC ルート認証局 公開鍵の160bit SHA-1ハッシュ値	新しいJPNIC ルート認証局 公開鍵の160bit
keyUsage	c		
		keyCertSign	keyCertSign
		cRLSign	cRLSign
certificatePolicies	n		
policyIdentifier		anyPolicy	anyPolicy
policyQualifiers			
policyQualifierId		使用しない	使用しない
qualifier		使用しない	使用しない
basicConstraints	c		
cA		TRUE	TRUE
cRLDistributionPoints	n		
DistributionPoint			
distributionPoint		JPNIC ルート認証局がCRLを公開するURI	JPNIC ルート認証局が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　JPNIC 下位認証局の識別名

※ 2　C=JP, O=Japan Network Information Center, OU=JPNIC Root Certification Authority

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 7-3 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 7-3 JPNIC ルート認証局が発行する 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1年後
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 ルート認証局 公開鍵の160bit SHA-1ハッシュ値

※ 1　C=JP, O=Japan Network Information Center, OU=JPNIC Root 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。

8.2. 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、本認証局を含む JPNIC 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
- 認証局の私有鍵の管理
- 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。

8.5. 不備の結果としてとられる処置

本認証局を含む JPNIC 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。本認証局を含む JPNIC 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 認証局の運営責任者が最低 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

JPNIC は、本 CP/CPS に規定した内容を遵守して認証サービスを提供し、本 CP/CPS の範囲内で、本認証局の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 は、JPNIC 認証局の運営を維持し、かつその義務を履行するために十分な財務的基盤を維持するものとする。

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 CP/CPS「2.2.証明情報の公開」で公表すると定めた情報、本 CP/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 CP/CPS で公表すると定めた情報、本 CP/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。

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 CP/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

本認証局を含む JPNIC 認証局は個人情報保護の重要性を認識し、個人情報を本 CP/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啓蒙活動を実施する。

（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 CP/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 CP/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
- （本 CP/CPS、本認証局の自己署名証明書、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
- JPNIC の判断によって下位認証局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

9.6.2. 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. 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 CP/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 CP/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

9.6.4. 検証者の表明保証

証明書検証者は、本 CP/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。

9.6.5. 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 CP/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 CP/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、JPNIC は次の場合に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
- 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
- 証明書所有者が利用する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

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 CP/CPS 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 CP/CPS の全部又は一部、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 CP/CPS 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、本 CP/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 CP/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 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。

9.12.3. 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 CP/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

本認証局を含む JPNIC 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 CP/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 CP/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 CP/CPS 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。