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。

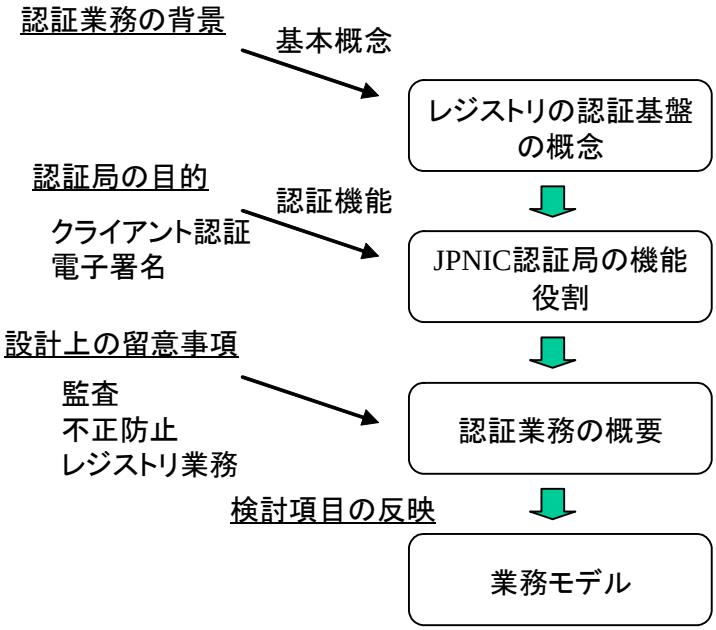

図 4-1　業務モデルの検討の流れ

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。

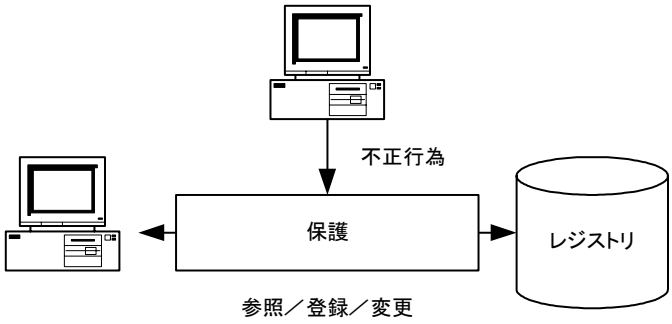

図 4-2 レジストリデータ入出力の認証

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

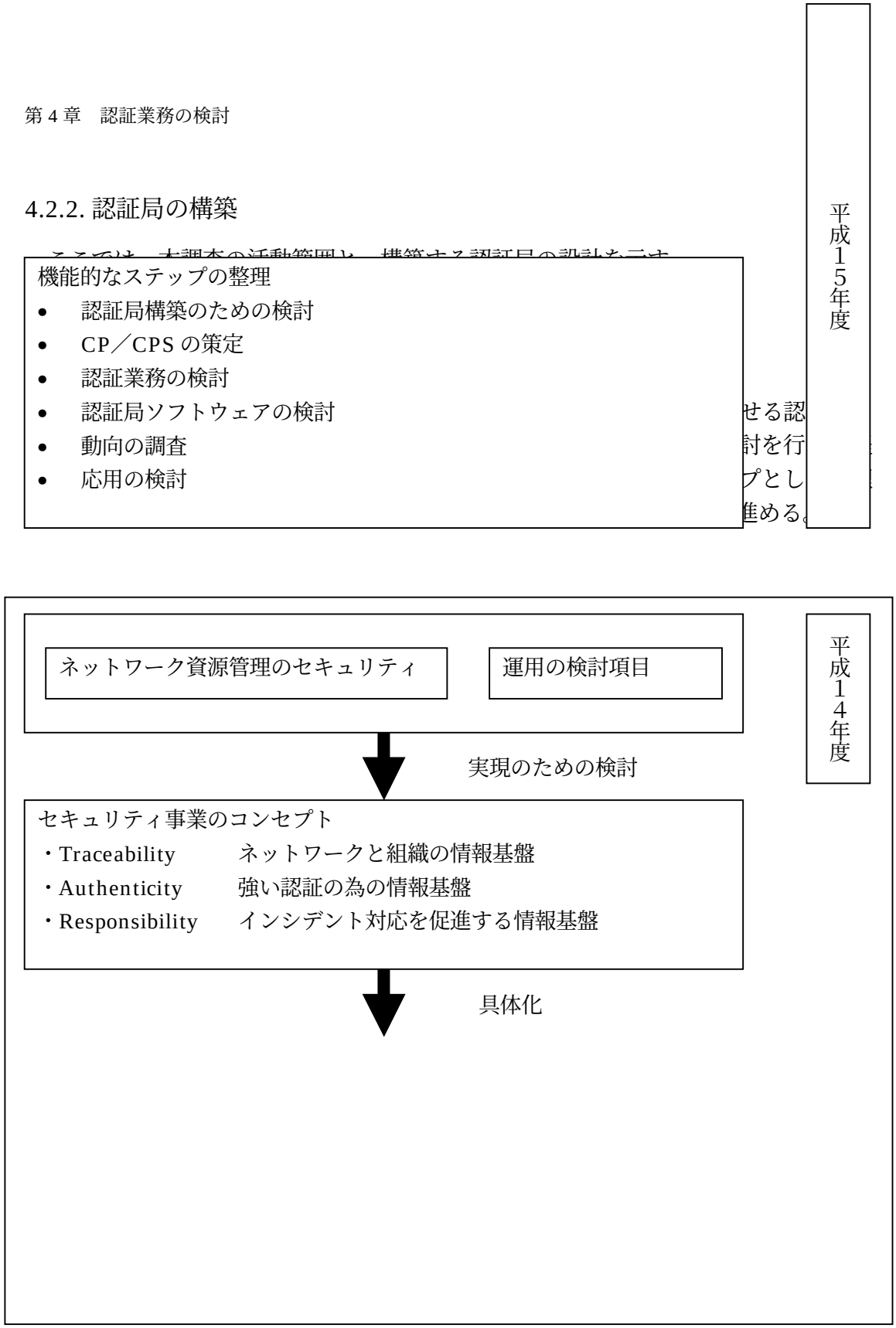

図 4-3 昨年度の活動と今年度の活動範囲

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。

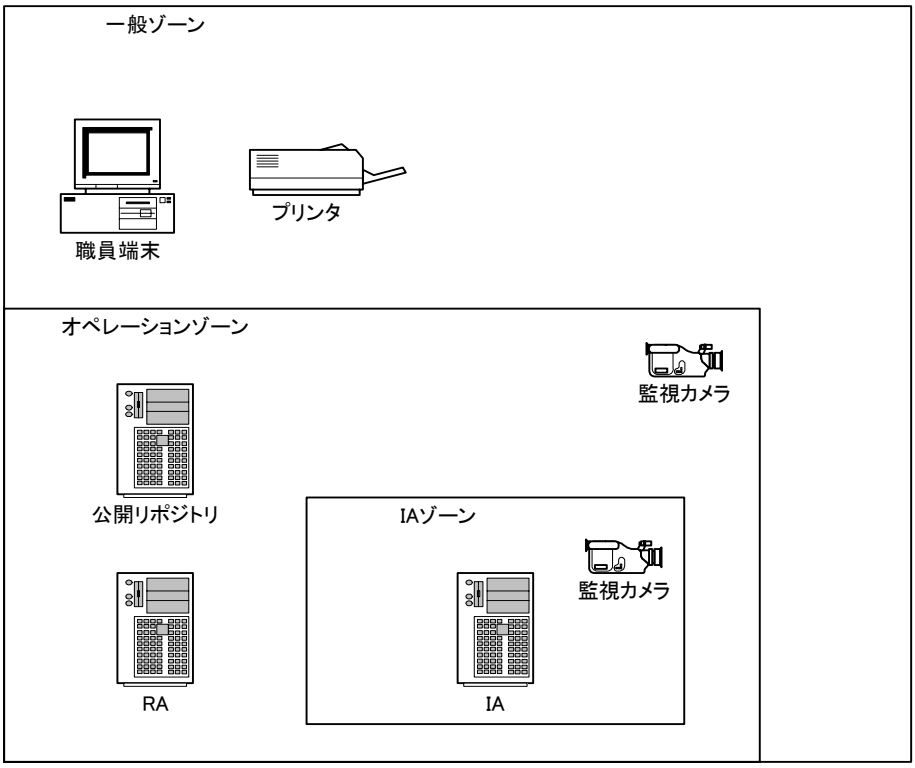

図 4-4 ゾーンニング

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。

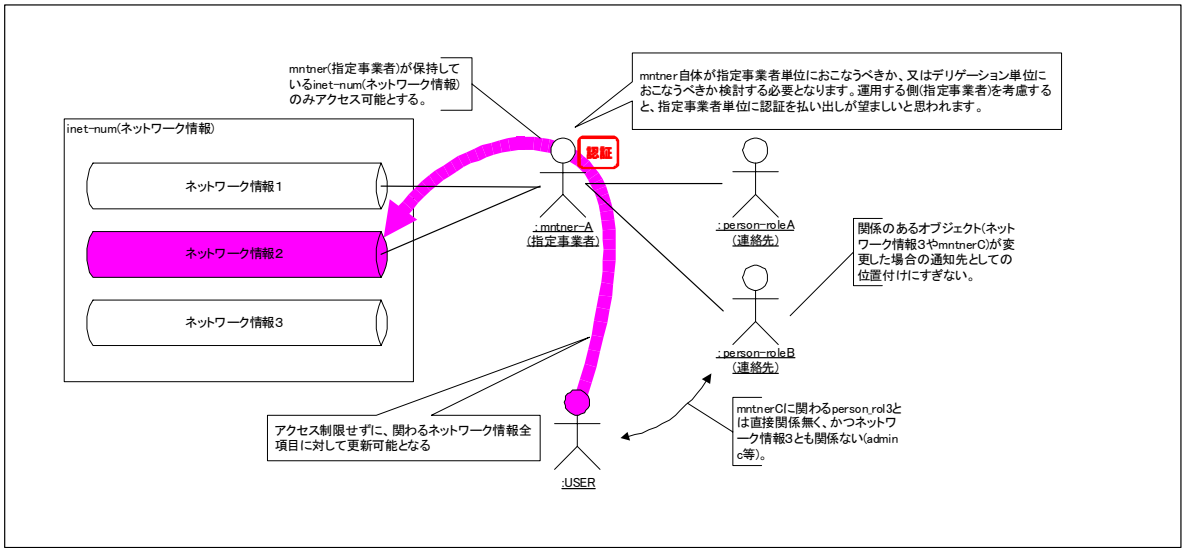

図 4-5 事業者認証モデル

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。

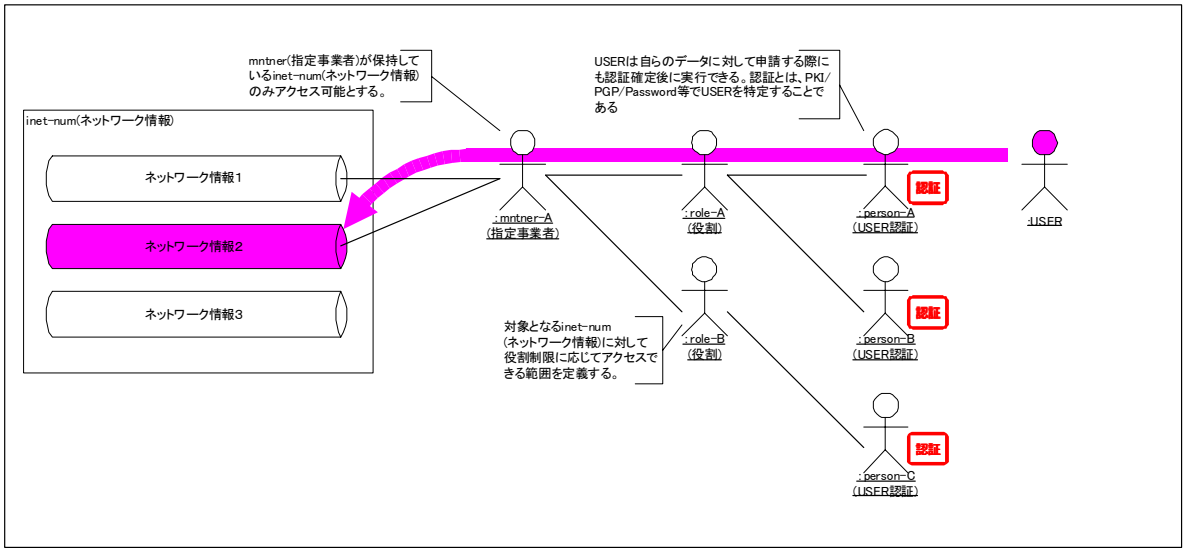

図 4-6 個人認証モデル

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。

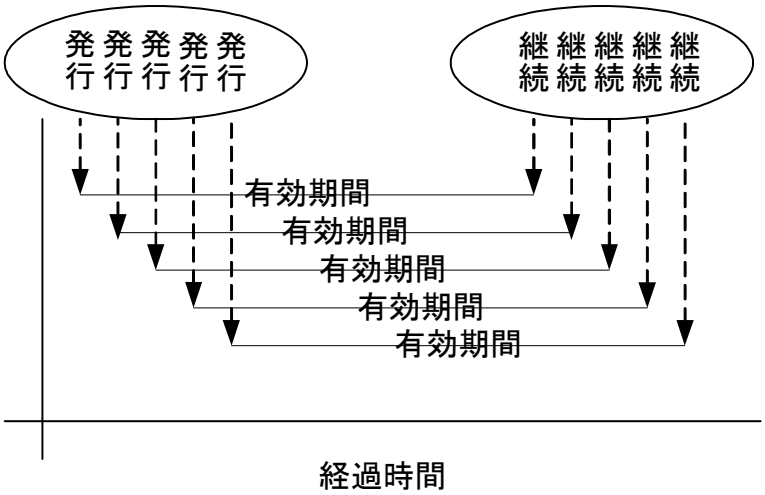

図 4-7 認証有効期間と継続の発生

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。

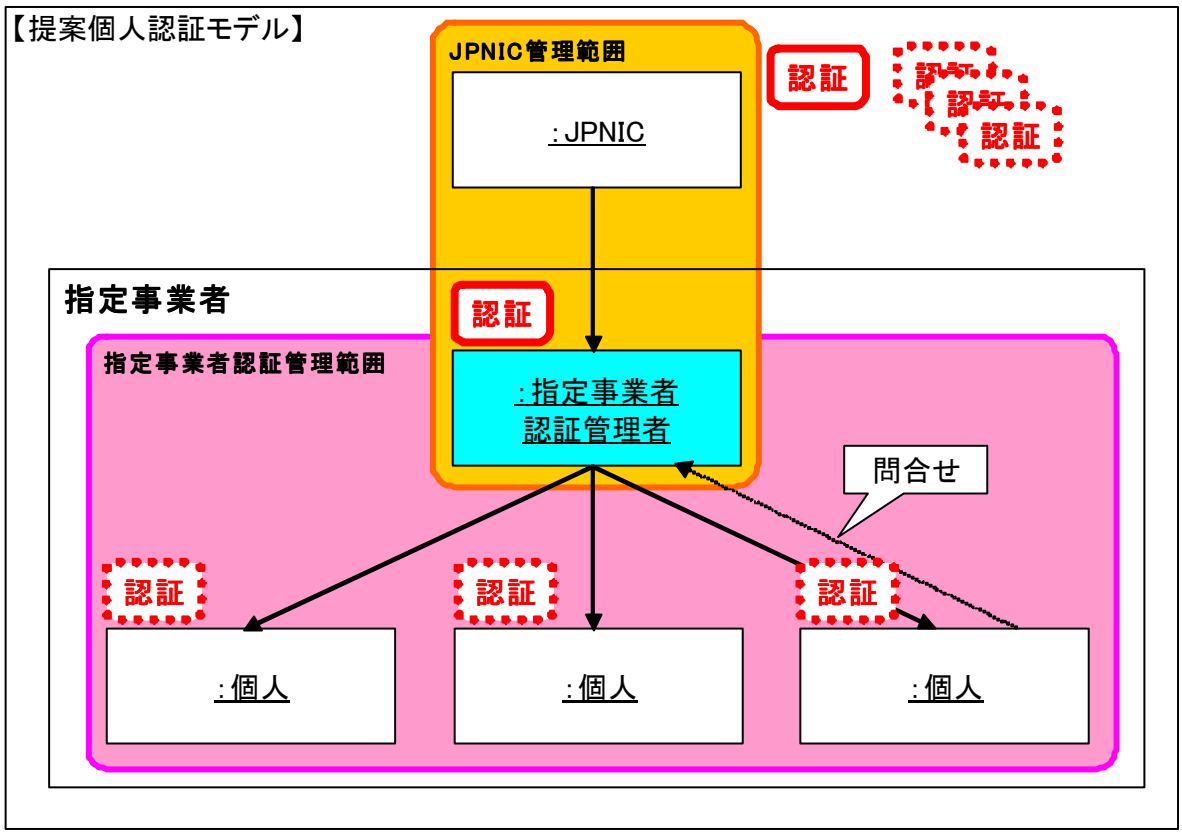

図 4-8 提案個人認証

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。

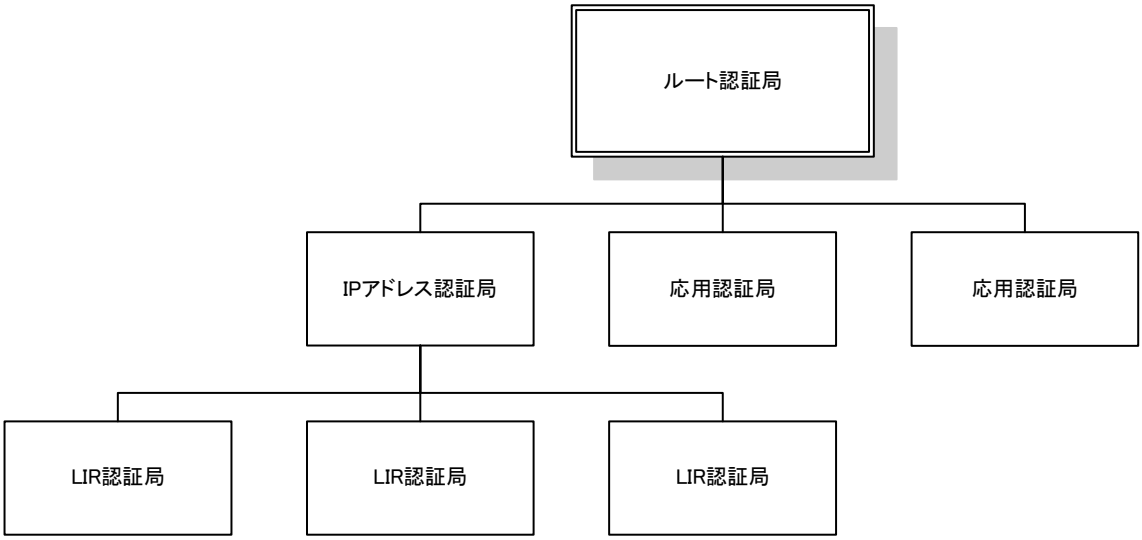

図 4-9 認証局階層構造イメージ

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）。

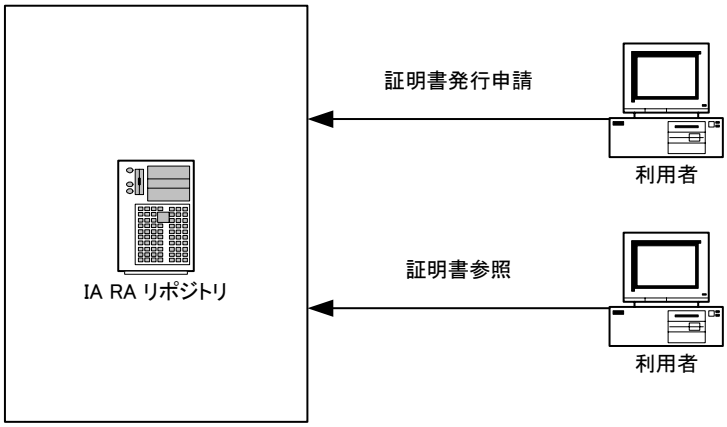

図 4-10 一台のサーバで構成するモデル

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）。

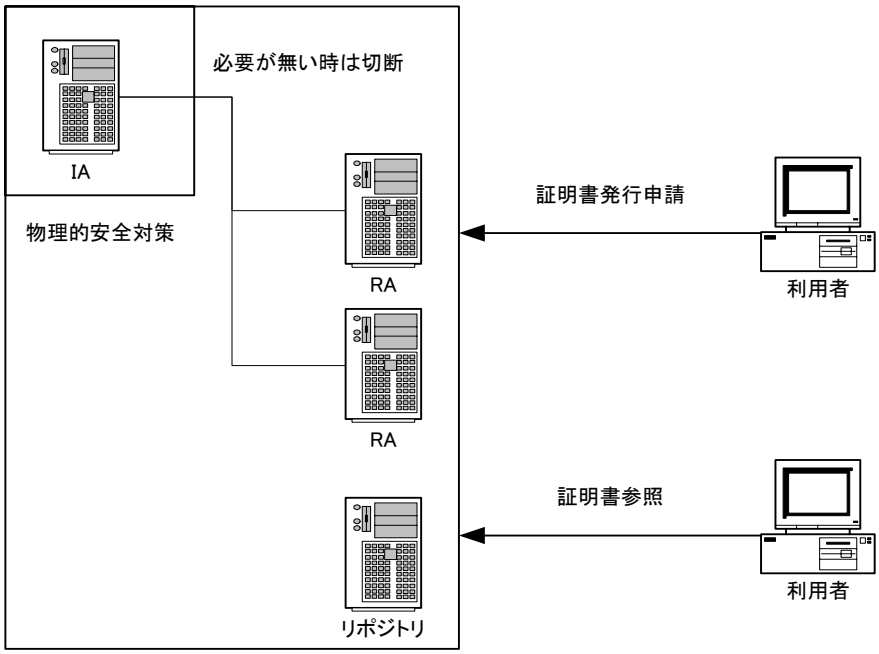

図 4-11 IA と RA を分離するモデル

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。

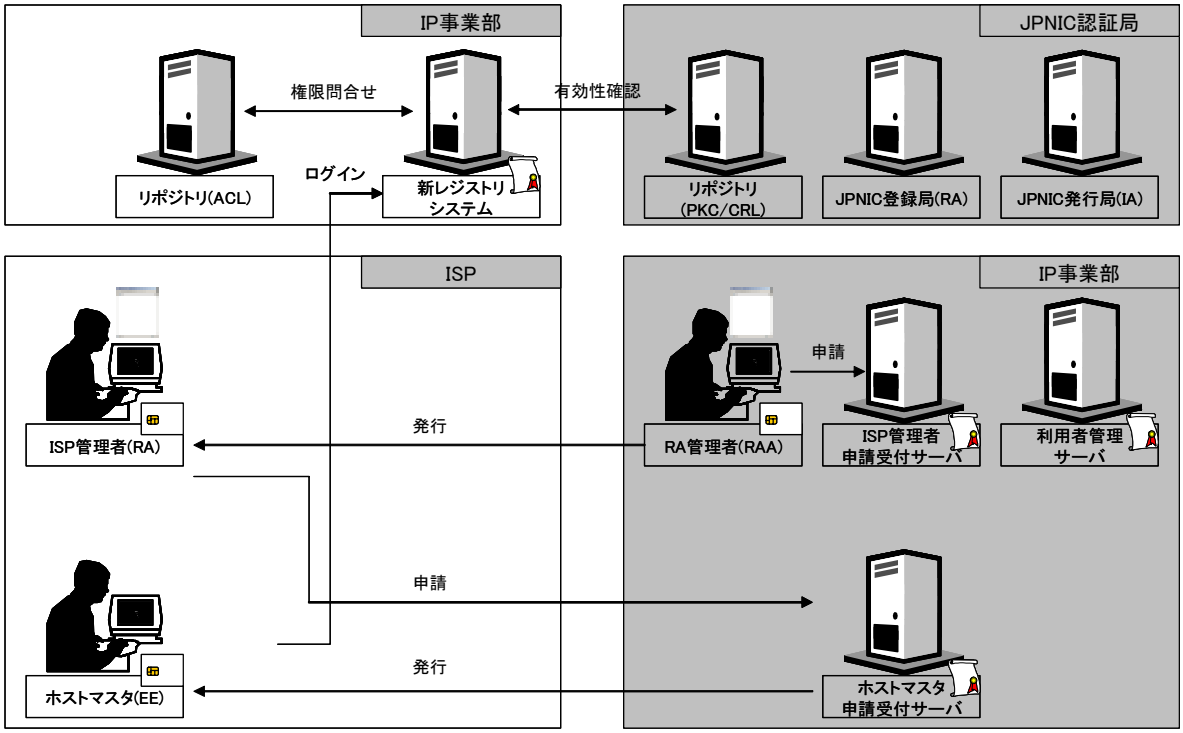

図 4-12 業務概念図

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。

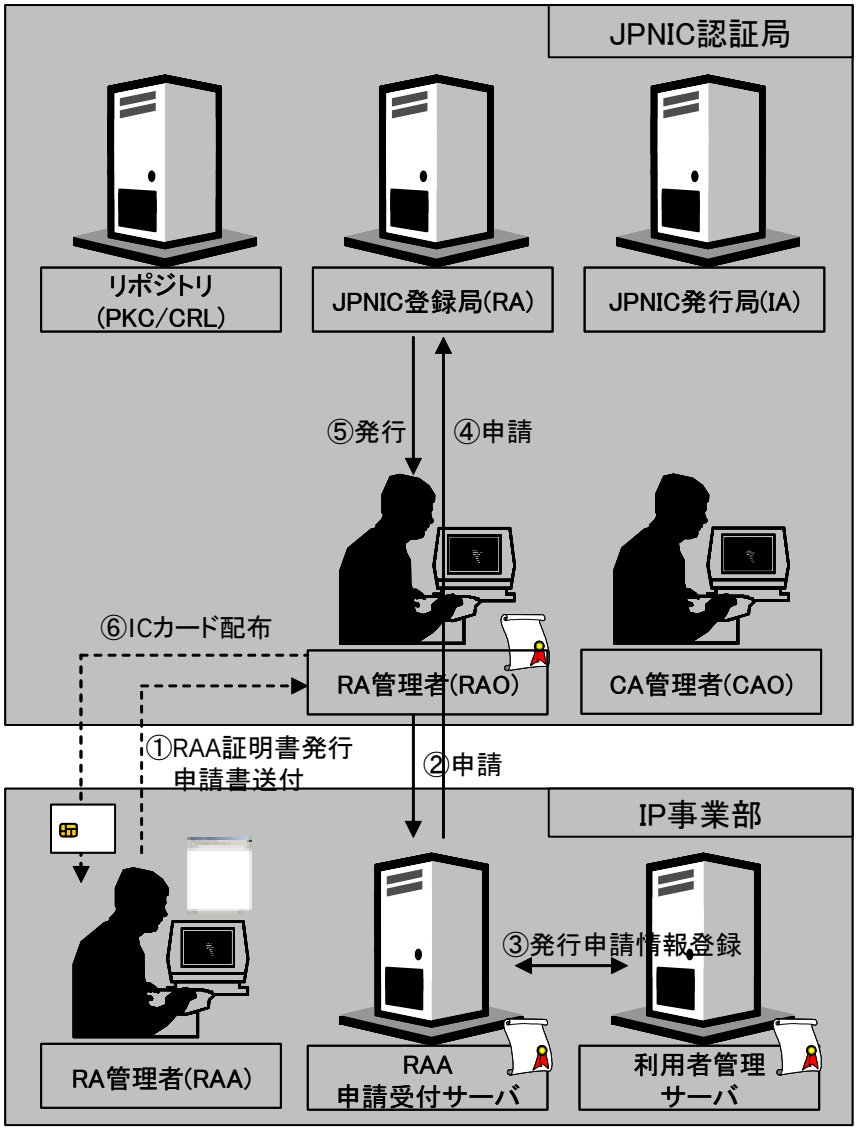

図 4-13 RAA 認証概念図

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。

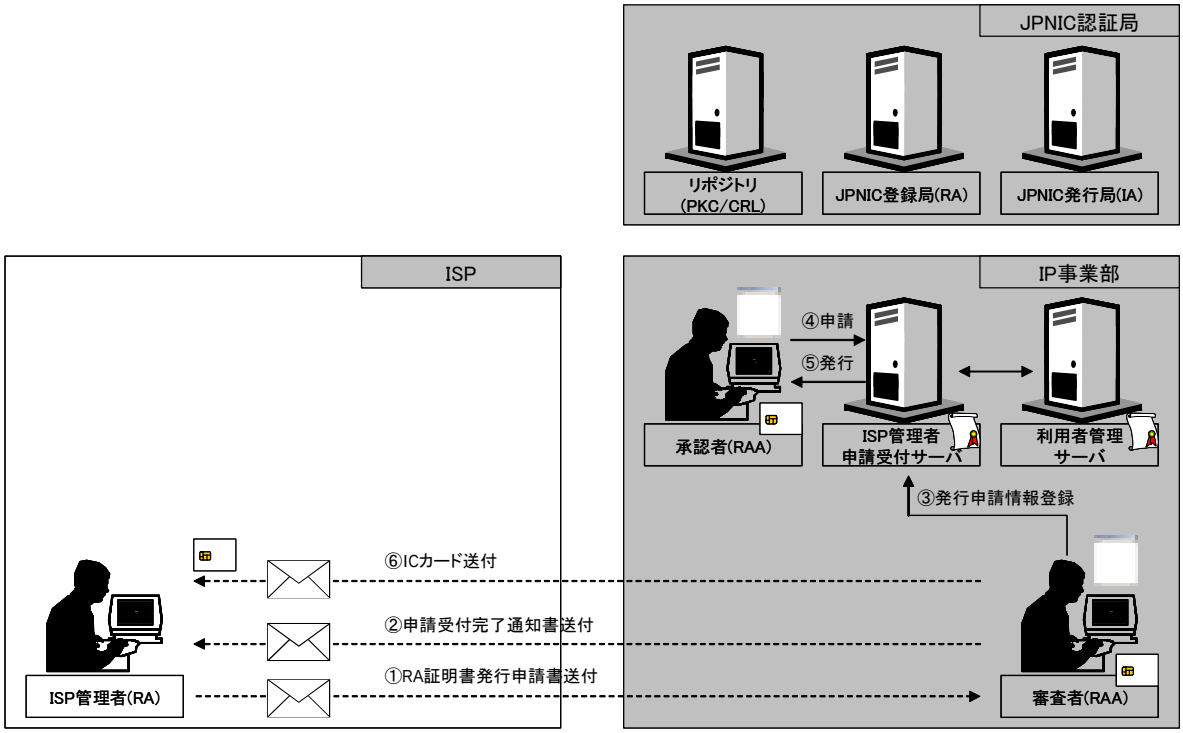

図 4-14 RA 認証概念図

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。

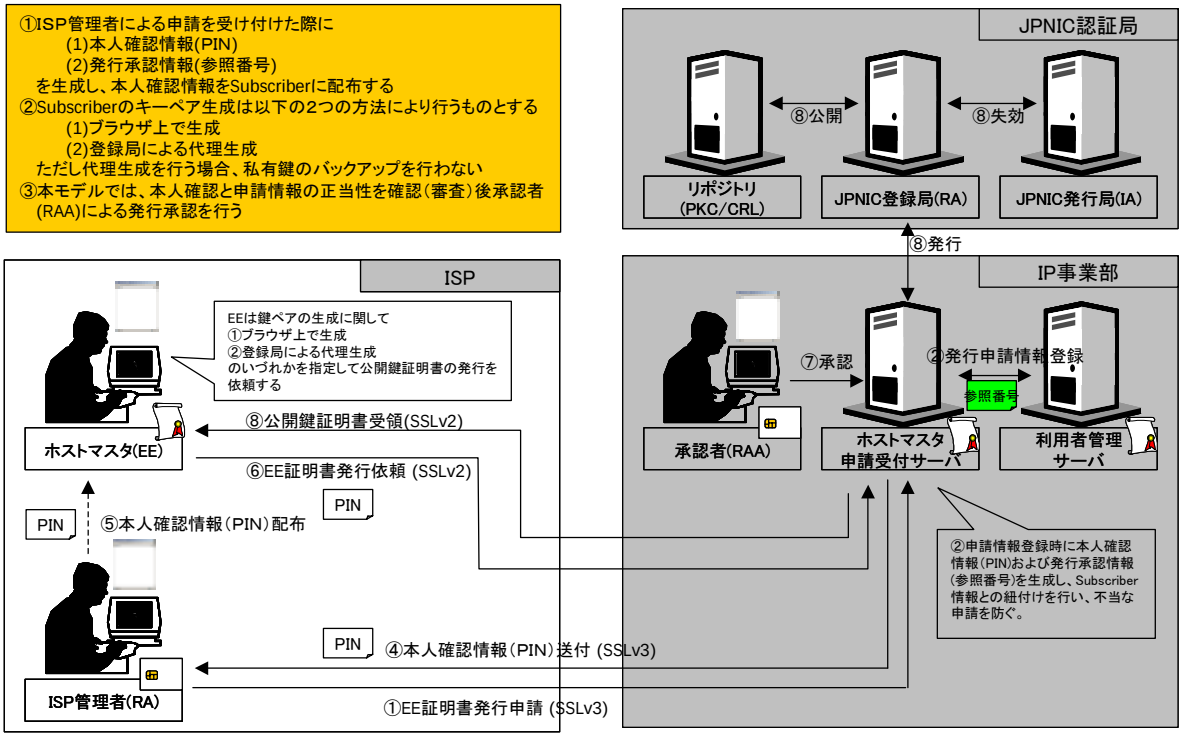

図 4-15 ホストマスタ（EE)認証概念図（センター承認モデル）

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。

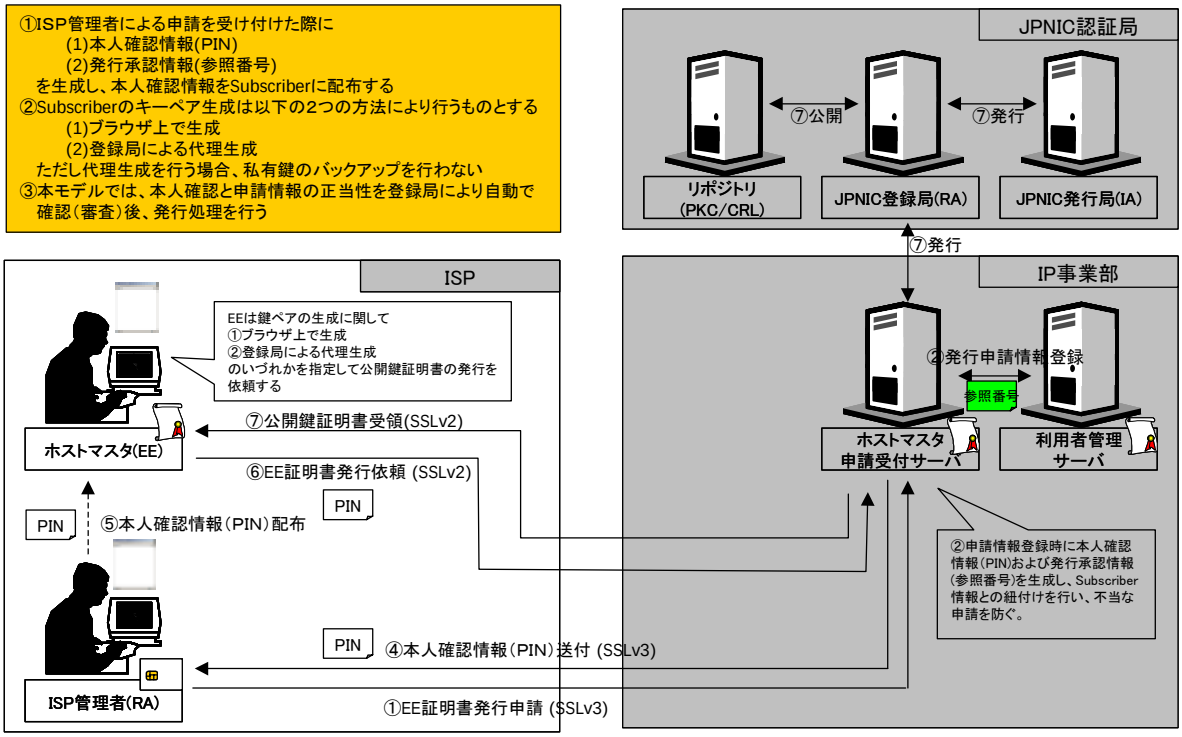

図 4-16 ホストマスタ（EE)認証概念図（自動承認モデル）

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。

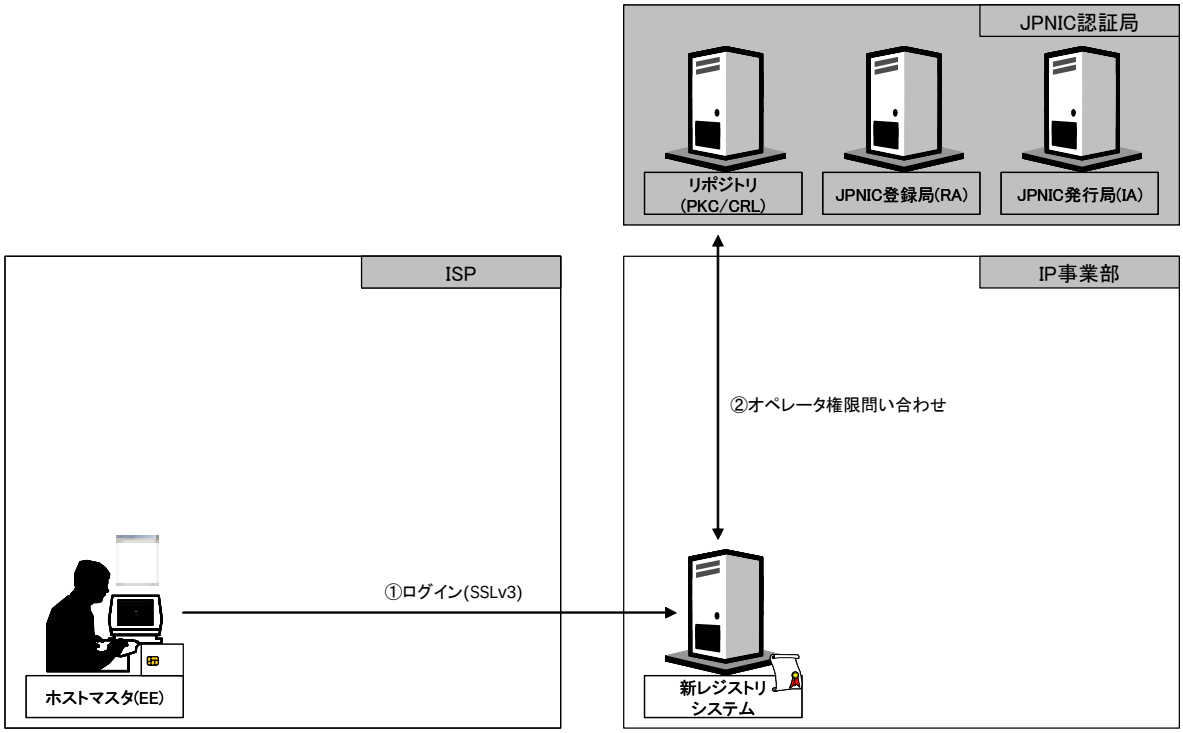

図 4-17 ホストマスタ（EE)の RS へのログイン概念図

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。

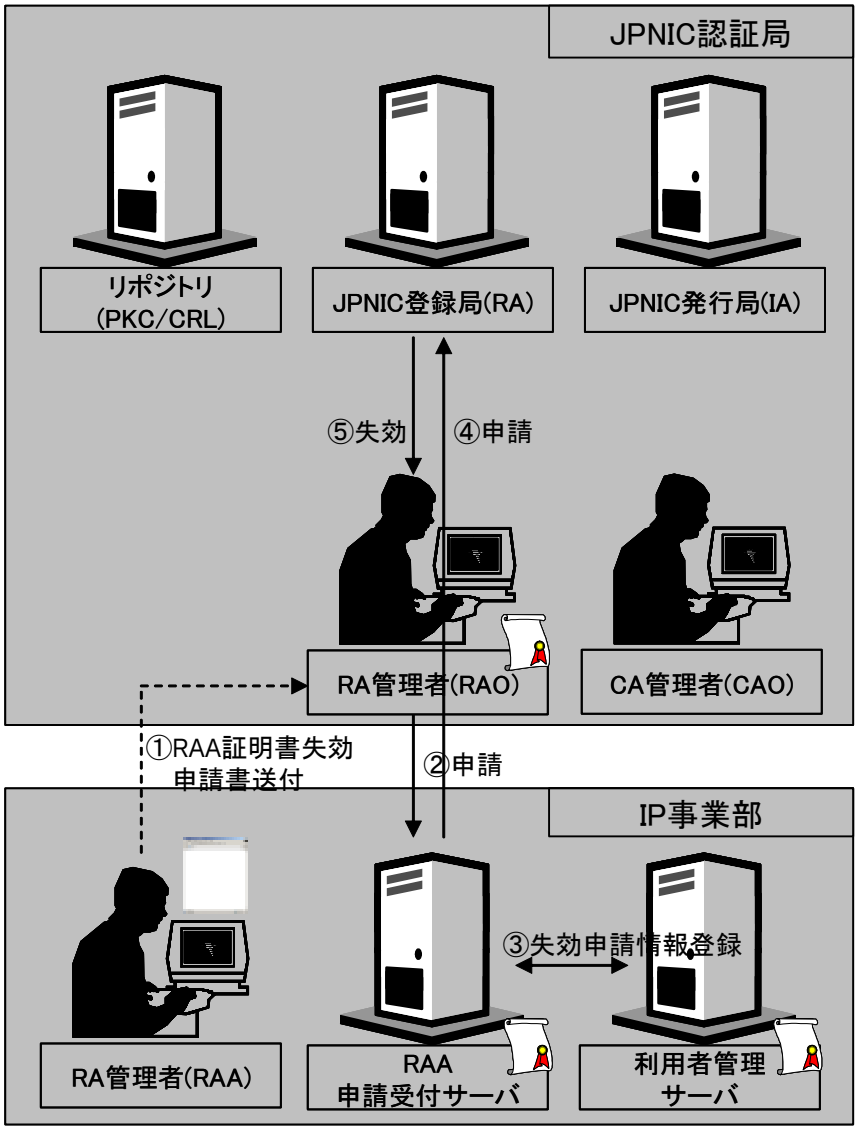

図 4-18 IP 事業部スタッフ（RAA)失効概念図

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。

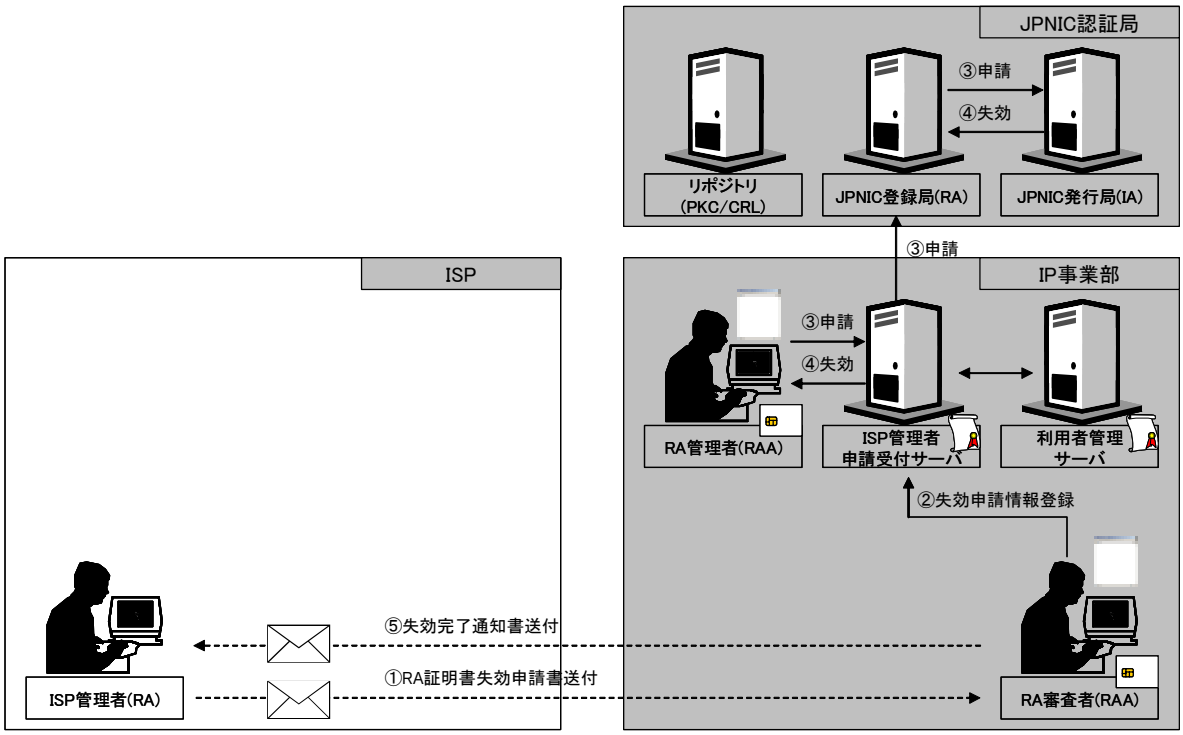

図 4-19 ISP 代表者（RA)失効概念図

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。

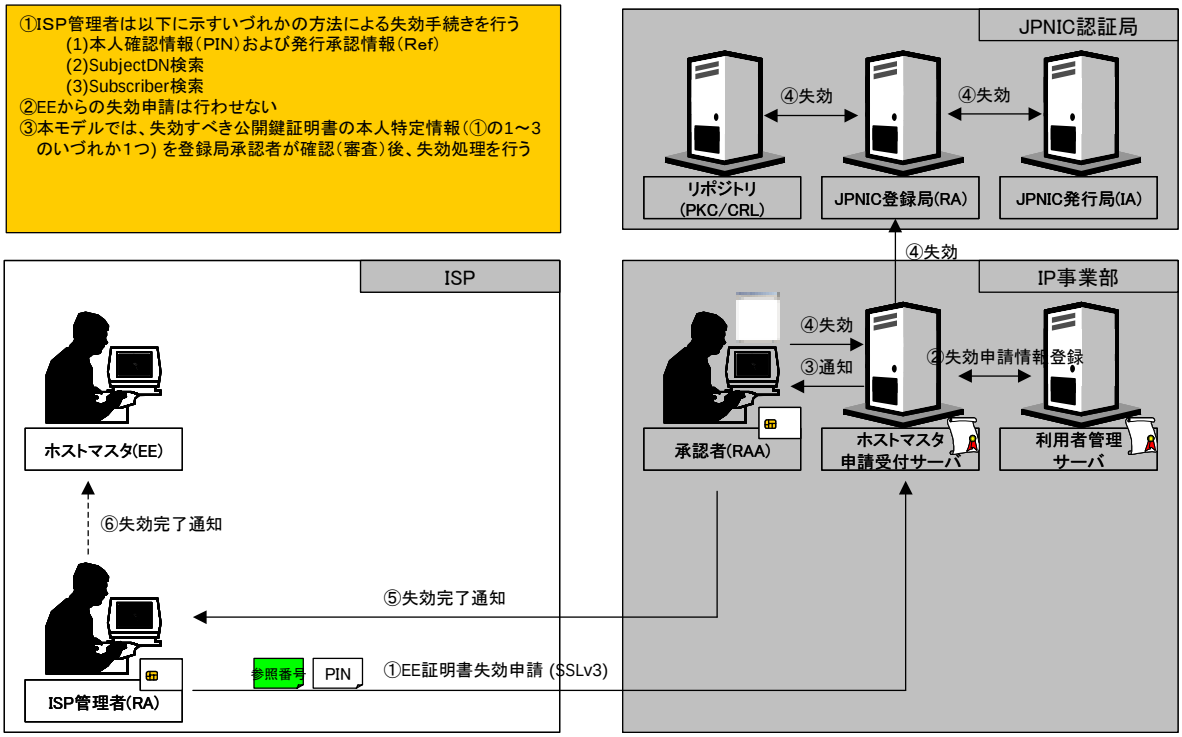

図 4-20 ホストマスタ（EE)失効概念図（センター承認モデル）

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。

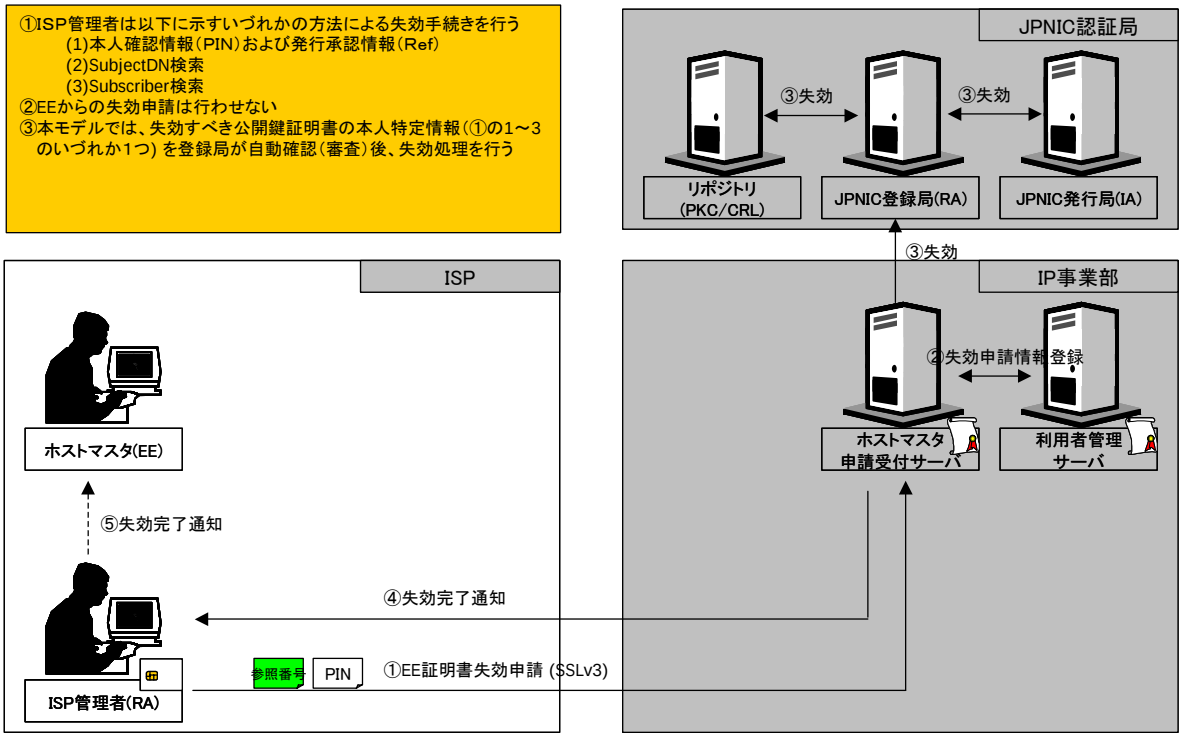

図 4-21 ホストマスタ（EE)失効概念図（自動承認モデル）

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。

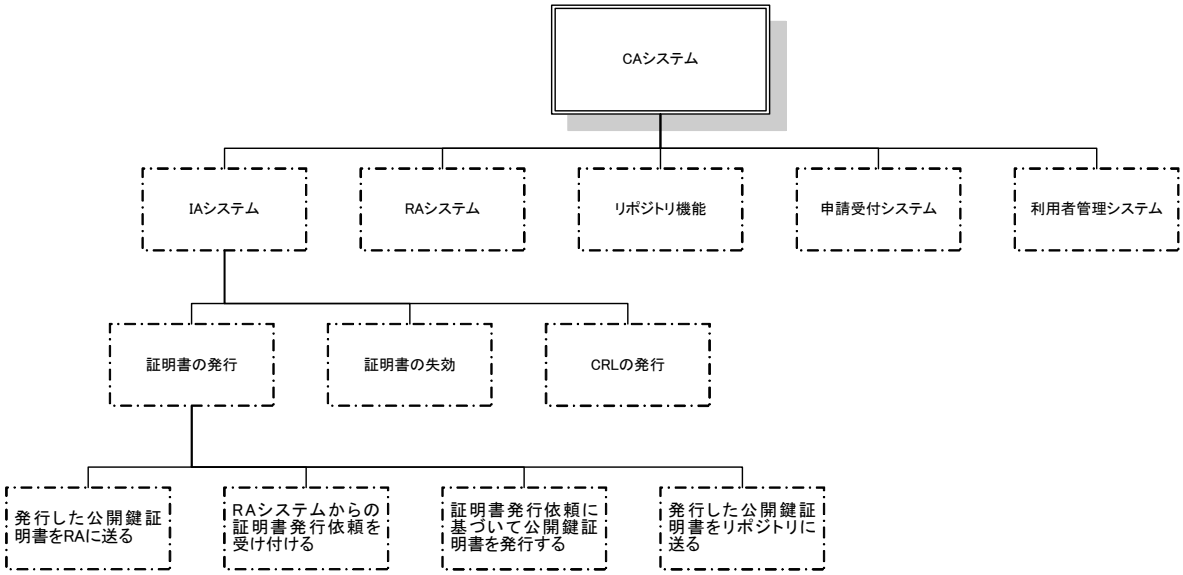

図 4-22 WBS 階層図（部分）

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。