# 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。

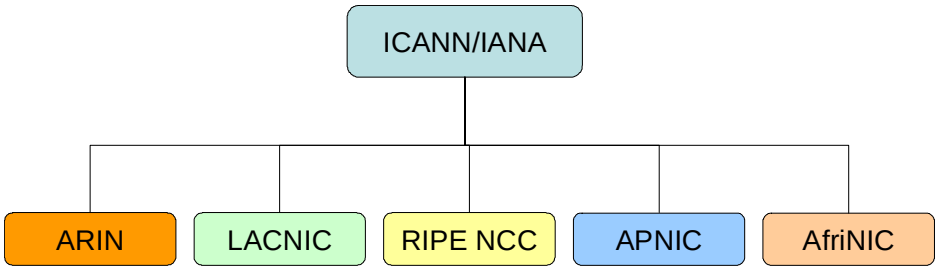


**図 8-1　ICANN/IANA と RIR の構造**

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。

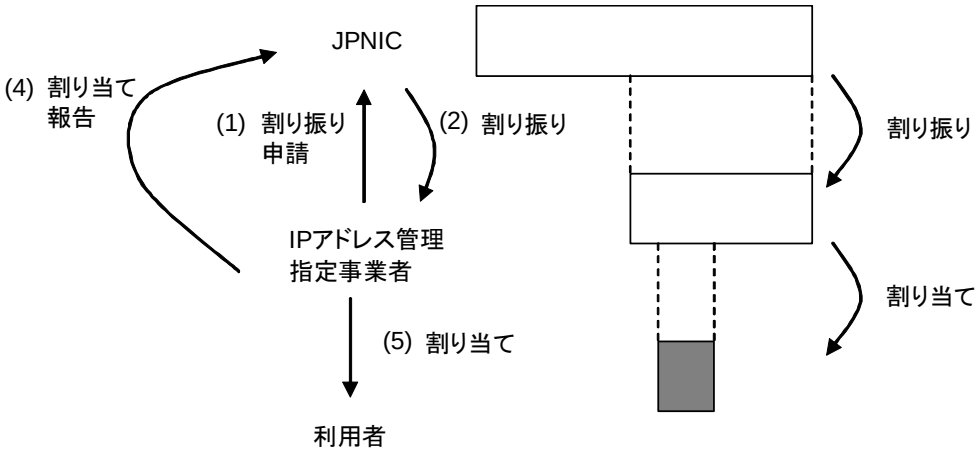


**図 8-2　JPNIC における割り振り、割り当て概念図**

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。

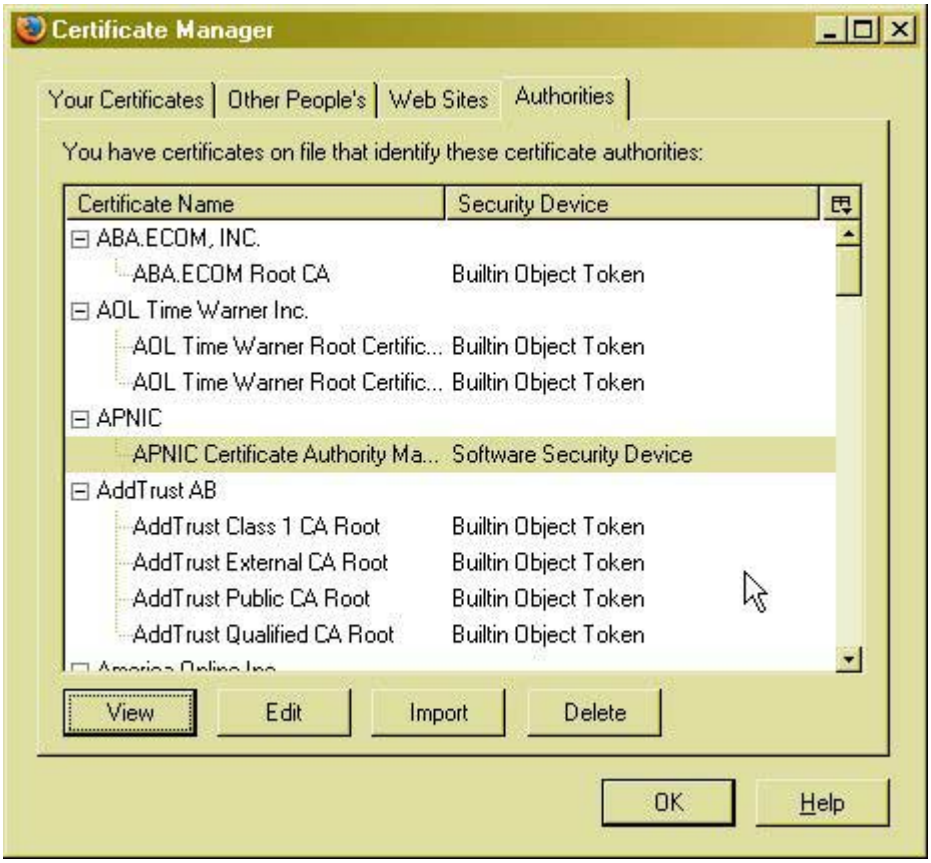


**図 8-3　Web ブラウザに組み込まれた APNIC CA 証明書**

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。

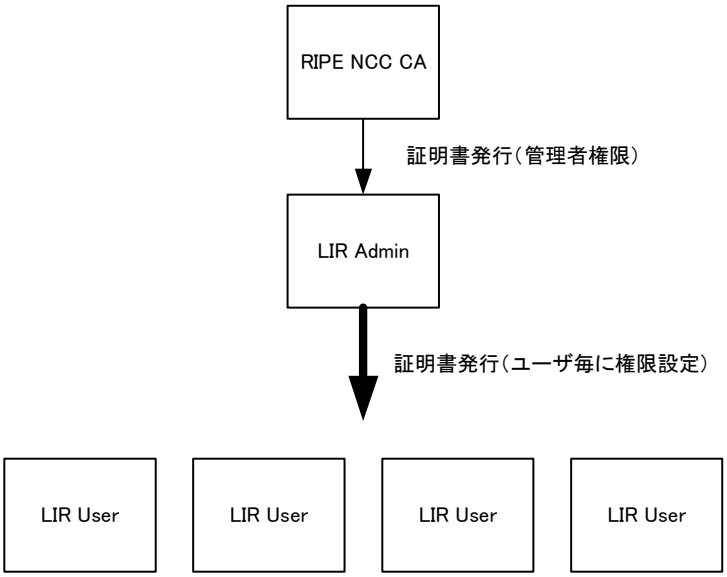


**図 8-4　RIPE NCC における PMS（Privilege Management System）**

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。

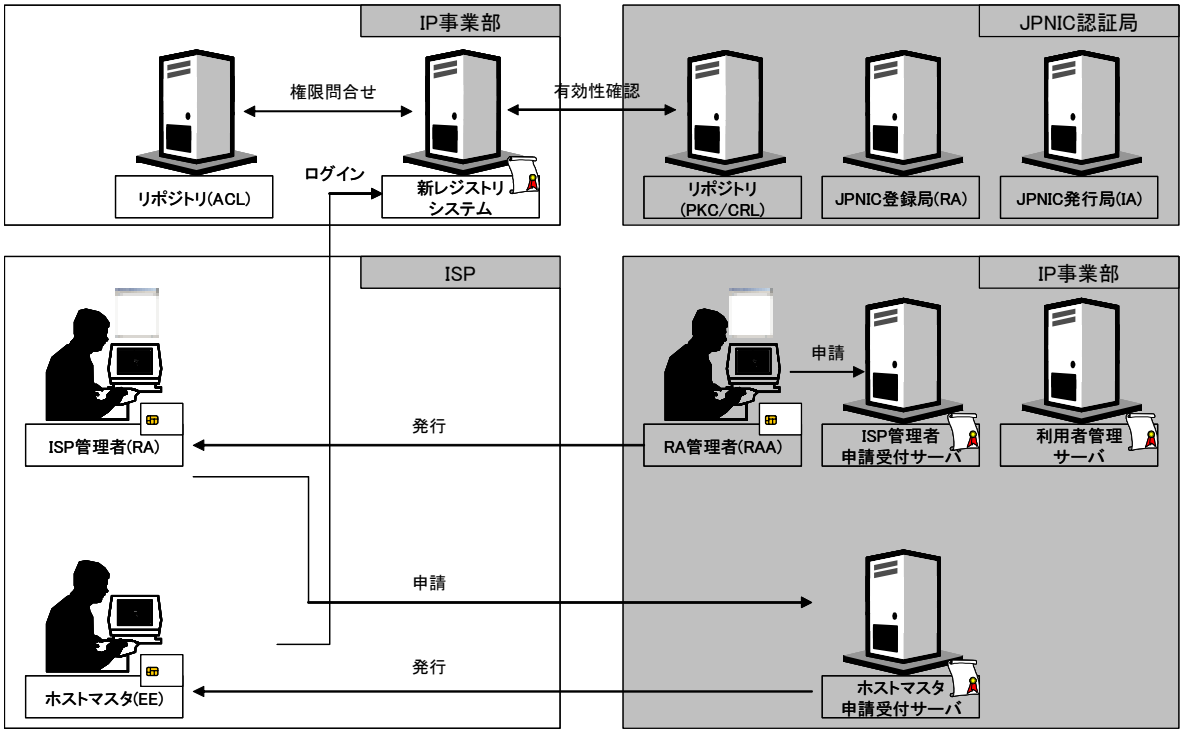


**図 8-5 業務モデル**

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。

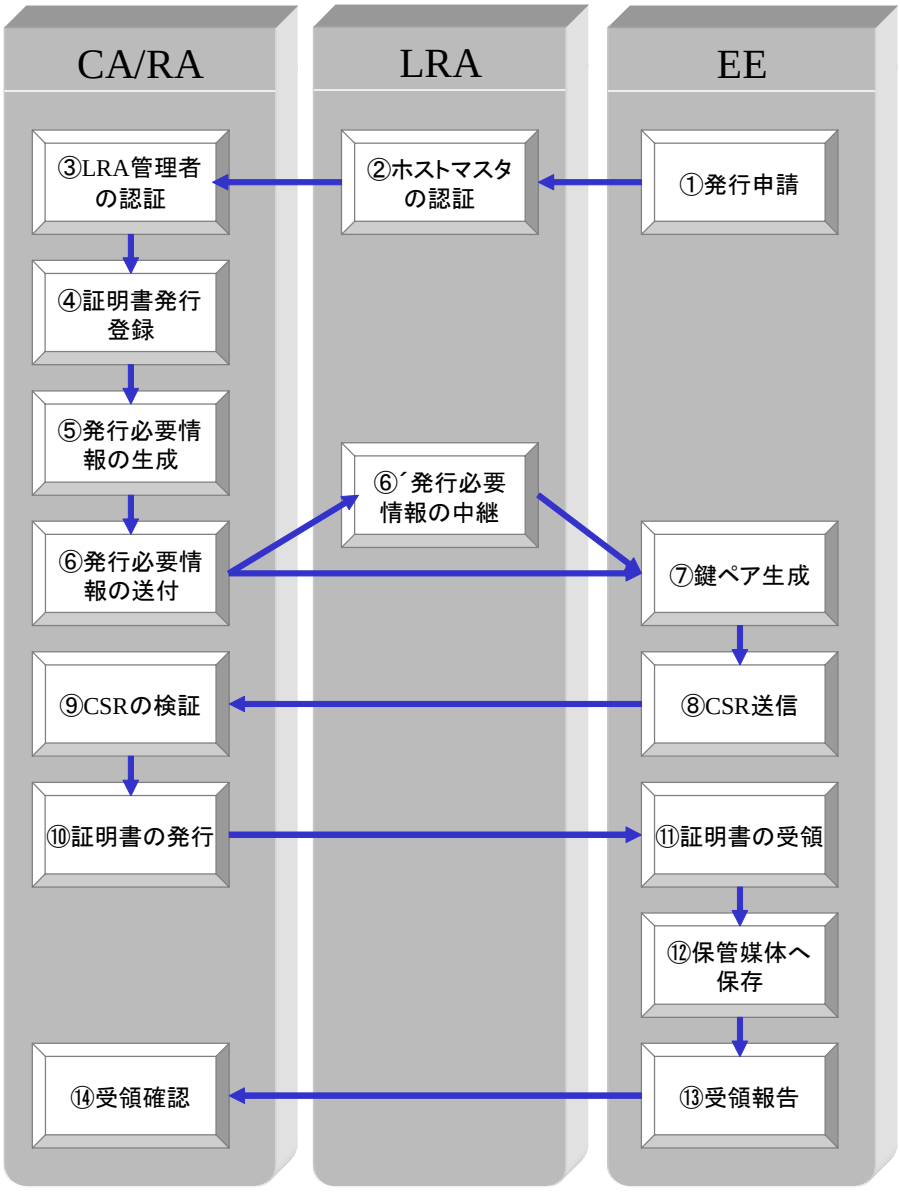


**図 8-6 ホストマスタ証明書の発行手順**

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。

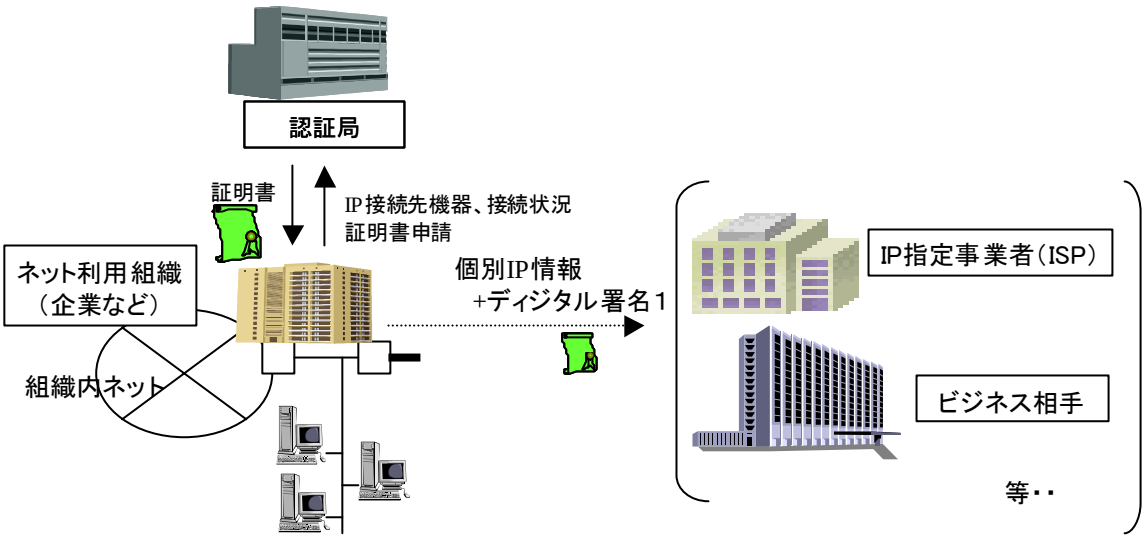


**図 8-7　IP アドレス利用先の認証**

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。

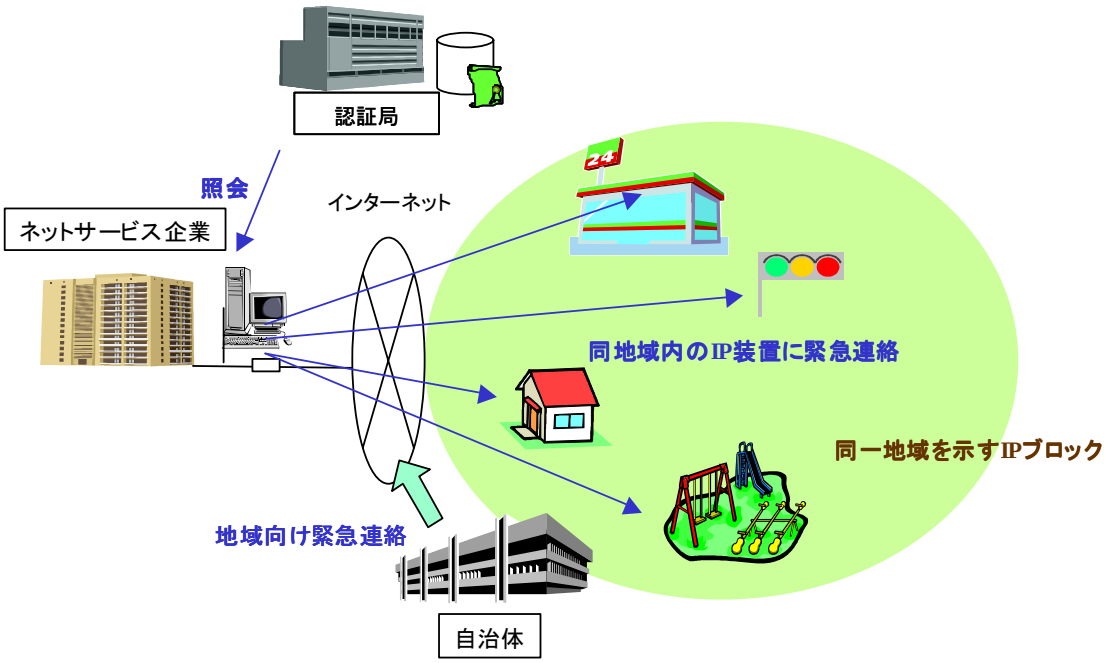


**図 8-8　災害時の地域一斉連絡**

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。