

Copyright © 2004 Japan Network Information Center. All Rights Reserved.

著作権表示：本文書は著作権上の保護を受けています。本文所のいかなる部分も、著者の承諾を得ずに電子的・機械的に複写・複製することは禁じられています。

IP アドレス認証局のシステム構築に関する提案依頼概要

2004 年 7 月 5 日

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. 概要

1.1. 本書の目的

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）における認証局のシステムを構築するに当たり、その実現可能性を評価するのが本提案依頼書の目的です。JPNIC は、本提案依頼書（RFP）によって提案を求め、複数の提案を比較検討します。JPNIC にてその開発・構築の計画が承認された場合に調達が行われます。

1.2. システム構築に関連する活動

JPNIC は非営利の会員制組織で、日本国内のインターネットにおけるアドレス資源管理を行っています。組織の活動概要については Web ページをご覧ください。

インターネットのアドレス資源管理（IP アドレス、AS 番号）は、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ます。

JPNIC は国別インターネットレジストリ（NIR：National Internet Registry）として、アジア太平洋地域における RIR の APNIC（Asia Pacific Network Information Centre）からアドレス資源の割り振りを受け、日本における管理業務を行っています。

LIR（Local Internet Registry）は、エンドユーザにアドレス資源の割り当てを行います。JPNIC からアドレス資源の割り振りを受ける LIR は、IP アドレス管理指定事業者（以下、指定事業者と呼ぶ）と呼ばれ、JPNIC から IP アドレス管理業務を行います。

1.3. IP レジストリシステムと認証

LIR から JPNIC に対してインターネットを通じて行われる申請手続きは、主に電子

メールを利用して行われています。申請業務に関連するデータは登録情報(レジストリデータ)と呼ばれ、IP アドレスレジストリシステム(以下、IP レジストリシステムと呼ぶ)を利用して管理されています。IP レジストリシステムは、whois データベース、逆引き DNS、申請受付・処理を行っており、インターネットの運用において重要なデータを扱うシステムです。

JPNIC では、現行の IP レジストリシステムに代わる IP レジストリシステム(以下、次期 IP レジストリシステムと呼ぶ)の開発が行われています。次期 IP レジストリシステムは、証明書を利用した認証処理を扱うことができるよう仕様の検討が進んでいます。

2. 認証局の概要

開発に関連してこれまでに JPNIC で検討された事項について説明致します。

2.1. 認証局の目的

JPNIC 認証局の目的は二種類あります。

- ・ 認証局登録情報の正当性向上のため、認証機能を高める。
証明書の運用に関わる認証業務を行い、ユーザ認証、サーバ認証のための EE (End Entity: エンドエンティティ) 証明書を発行する。
- ・ アドレス資源情報と認証情報を応用した認証基盤を構築するためのテストベッドを構築する。
アドレス情報と関連した情報を含む証明書を発行する。証明書プロファイルの変更などの実験を行う環境を構築する。

2.2. 認証局の構成と位置づけ

認証局は図 1 のようなツリー構造を想定しています。

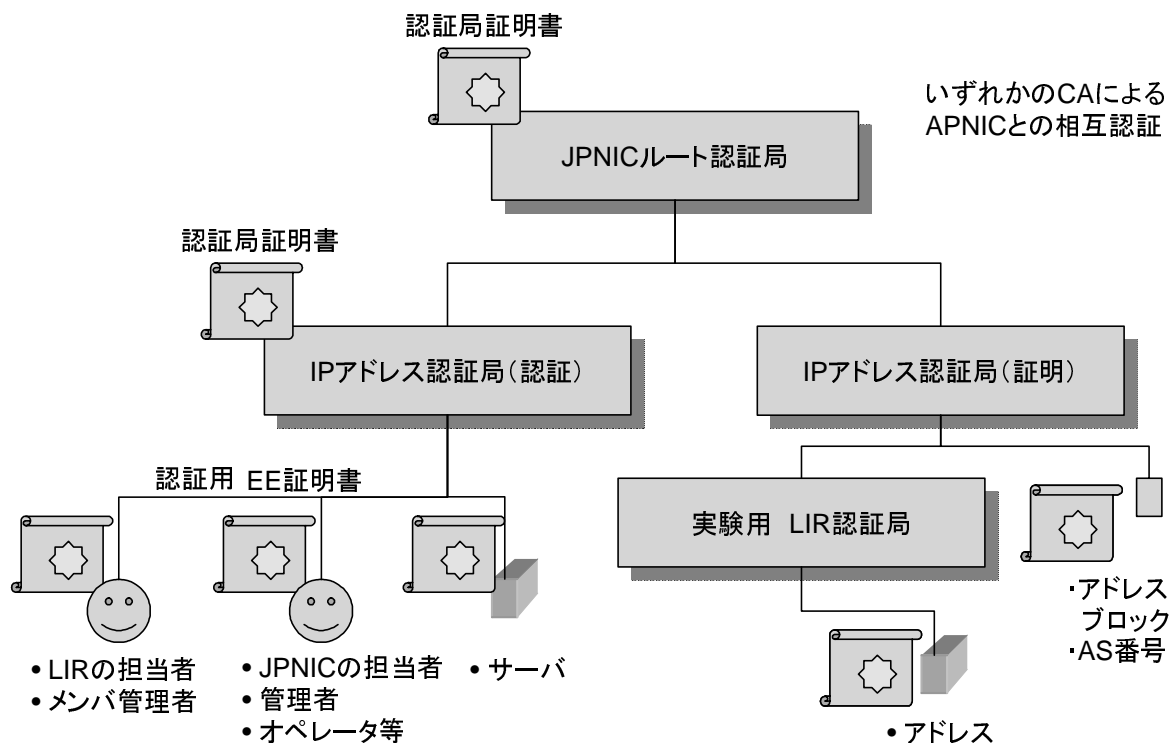


図 1 認証局と証明書のツリー

JPNIC ルート認証局は、認証局に対する認証業務を主な目的としており、JPNIC におけるすべての認証局はこの下位認証局になります。

IP アドレス認証局（認証）はアドレス資源管理の業務に関わる認証業務を行うための認証局です。この認証局は EE（End Entity：エンドエンティティ）証明書の発行を行います。EE 証明書は、まずクライアント認証、サーバ認証のために使われます。将来的に署名用の証明書が発行されることを視野に入れていきます。

IP アドレス認証局（証明）は、JPNIC ルート認証局の下位認証局に位置づけられ、LIR 認証局の認証局証明書やアドレスブロック、AS 番号の証明書の発行を行います。LIR 認証局は LIR（一般的に ISP と呼ばれる組織です）において運用される認証局で、IP アドレス認証局（証明）の下位認証局に位置づけられます。IP アドレス認証局（証明）と LIR 認証局は実験運用を想定しています。

3. システム構築における要求事項

本構築でいう”構築”とはシステムの開発と共に、認証業務の運用を踏まえたドキュメンテーションを含んでいます。”ドキュメンテーション”は業務手順書や操作マニュアルの作成を想定しています。認証業務規程（CP/CPS）の策定は含まれません。

3.1. PKI を利用したアドレス資源管理

認証に関わる業務の整理と、適切なコストでの認証局の運用を通じて、アドレス資源管理における認証処理をよりセキュアなものにします。また、アドレス資源に関わる証明を目的とした認証局を構築し、LIR 等と連携した運用実験と認証基盤構築の検討を行う環境を整えます。

シンプルな構成を持ち、柔軟かつコンパクトな運用規模と費用で PKI の利用を行います。

4. 提案手続きについて

4.1. 調達と説明会について

調達は原則として JPNIC の公募に対する業者（複数）の応募を比較検討し、選ばれた業者から行います。

提案依頼書についての説明会を、下記に述べるスケジュールで行います。提案依頼書は説明会の際に公示されます。

4.1.1. 提案依頼スケジュール

2004 年 7 月 5 日（月）	公募開始
2004 年 7 月 8 日（木）	説明会申し込み期限
2004 年 7 月 12 日（月）	RFP 提示日および説明会
2004 年 7 月 23 日（金）	提案書提出期限
2004 年 7 月 30 日（金）	業者選定結果内示

4.2. 参加資格条件

同規模の認証局システム開発経験を持ち、ネットワーク系に通じたシステム開発に関する実績を持つベンダーが望まれます。