第 6 章　IP アドレス認証の展開に関する調査研究について

内容

- IP アドレス認証局の役割と構成
- 安全な経路制御の為の電子認証

6. IP アドレス認証の展開に関する調査研究について

本章では、2004 年度までに構築された IP アドレス認証局の展開に関して述べる。IP アドレス認証局は JPNIC で構築された認証局の一部で、他の認証局が発行する電子証明書と組み合わせ、また登録情報に基づいた電子証明書の発行を行うことで、様々な展開方法が考えられる。

2005 年度の調査研究では、インターネットにおける経路情報交換のプロトコルである BGP の安全な運用に着目し、調査研究を行った。

本章ははじめに IP アドレス認証の考え方と IP アドレス認証局の構成について述べ、次に BGP の安全な運用のために考えられる電子認証の利用方法について紹介する。

6.1. 概要

「IP アドレス認証」とは 2004 年度までに JPNIC で構築が進められた IP アドレス認証局を使った電子認証を意味する言葉である。特に IP アドレスが入った電子証明書を意味しているわけではない。

JPNIC の「IP アドレス認証局」は主に二つの考え方に則って構想が検討された。一つは登録情報の正当性確保である。これは JPNIC に情報登録を行う IP アドレス管理指定事業者に対して電子認証技術を使った認証を行い、不正な情報登録を防ぐという考え方である。この認証強化によって JPNIC が WHOIS サービス等で提供する情報の信頼性が向上するだけでなく、IP アドレス管理指定事業者に割り振られたアドレス資源の情報が、第三者によって不正に書き換えられ、ISP 事業に支障が出ることを防ぐというメリットが考えられる。もう一つの考え方は、登録情報に基づく電子認証の提供である。正当な手続きを踏んで登録された情報は、登録されたユーザやサーバの間の認証に使うことができる有効な情報源になると考えられる。そこで登録情報に基づいて電子証明書の発行を行えば、登録された者同士が SSL や IPsec などの暗号プロトコルを利用するためにその電子証明書を利用することができるようになる。

この二つの考え方は、電子認証の導入における二つの段階でもある。一つ目は JPNIC による登録者の認証であるため、認証する者は必ず JPNIC となる。認証に使われる電子証明書の検証を行う者が JPNIC 自身であるため、電子証明書に入れる内容や保証のレベルを決定しやすい。また電子証明書の発行を行う認証局の信頼性について、外部から担保されるための体制を整える必要がなく、運用を開始しやすい。二つ目は、JPNIC

でない証明書ユーザ同士の認証である。証明書ユーザにとって JPNIC が第三者となるため、PKI の本来の適用方法に近い。発行される電子証明書はユーザの利用環境や、ユーザの挙動を想定して設計される必要がある。また証明書ユーザに対して認証局の信頼性を示す必要がある。JPNIC の認証業務の信頼性は、一つ目の情報登録のための認証が基本となる。

2004 年度までに行われた調査研究では、一つ目の役割を持つ認証局として「IP アドレス認証局（認証）」が、二つ目の役割を持つ認証局として「IP アドレス認証局（証明）」が構築された。

6.2. IP アドレス認証局の役割と構成

JPNIC の認証局である IP アドレス認証局の構成を図 6-1 に示す。

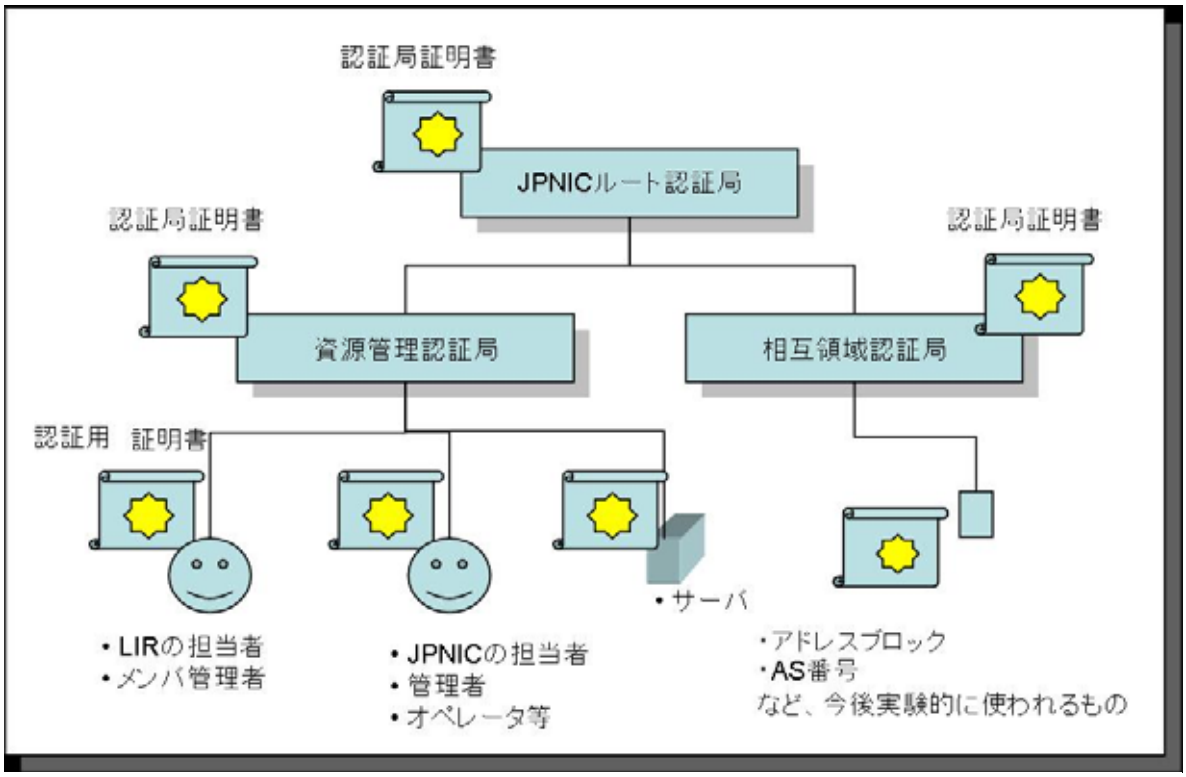

図 6-1　JPNIC の認証局の構成

JPNIC の認証局の中で、すべての認証局の上位認証局となるのが「JPNIC ルート認証局」である。この認証局は、JPNIC における認証業務の信頼点（Trust Point）を提供するためにあり、証明書の検証を行う者は必ずこの「JPNIC ルート認証局」の証明

書を正しい方法で入手する必要がある。2005 年の時点の、この認証局の CN（Common Name）は「JPNIC Primary Root Certification Authority S1」である。

「IP アドレス認証局（認証）」は「資源管理認証局」として示されている。この認証局は、登録情報の正当性向上のための PKI を使った認証機能の提供を目的としている。2005 年の時点のこの認証局の CN は「JPNIC Resource Service Certification Authority」である。

「IP アドレス認証局（証明）」は「相互領域認証局」として示されている。この認証局は、登録情報に基づいた電子証明書の発行を行い、アドレスブロック、AS 番号等における電子認証ために設置されている。2005 年の時点の CN は「JPNIC Interauth Certification Authority」である。

前節で述べた二つの段階は、「資源管理認証局」の構築と「相互領域認証局」の構築の二つにそれぞれ当てはまる。

6.3. 安全な経路制御のための電子認証

JPNIC における登録情報は、主に IP アドレスに関する情報である。この登録情報は、IANA を頂点とするインターネットレジストリの階層構造に則って割り振られた IP アドレスに関するもので、IP アドレスの一意性や地域性を正しく反映したものとなる。一方、IP アドレス管理指定事業者に対する割り振り情報は、インターネットの経路情報に対する原本となる情報であり非常に重要な意味を持つ。インターネットでは、原則的として、この割り振られた IP アドレスの範囲に則って経路情報が決定されているためである。そこで 2005 年度は経路情報の交換を安全に行うための電子認証に注目し、調査研究を行った。

インターネットにおける経路情報の交換は、自律分散システムの技術が使われており、専門的な分野である。また経路情報を交換するシステムは、1970 年代より運用されており歴史が長い。従ってこの分野における電子認証の適用には、経路情報の交換（ルーティング）における歴史的背景や常識的な運用形態に関する理解が必要となる。

そこで次章以降には、ルーティングの分野の専門家に協力を得て、基本的な技術情報から近年の動向にかけて重点的に情報をまとめた。