第 6 章　電子認証フレームワークと IP アドレス認証の展開の今後

内容

- IP アドレス認証と電子認証フレームワーク
- 今後の電子認証の相互運用

6. 電子認証フレームワークと IP アドレス認証の展開の今後

2005 年度および 2006 年度の調査研究の中で、「電子認証フレームワーク」と「IP アドレス認証の展開」を 2 つのテーマとして別々に扱ってきたが、実際にはこの二つは電子認証の適切な普及のために連携して進めることが必要な研究プロジェクトである。本章では、今後図られるべき連携について述べる。

6.1. これまでの IP アドレス認証と電子認証フレームワーク

本調査研究のテーマの一つである「IP アドレス認証の展開」は、日本国内の IP アドレスを管理している NIR における電子認証の実践を主な活動内容として取り組まれてきた。

具体的には JPNIC に登録された IP アドレスに関する情報を、登録・編集・削除する日本国内の ISP（以下、IP 指定事業者とよぶ）のクライアント認証を推進し、またその為にローカル RA といった利用環境の向上を図ってきた（図 6-1）。

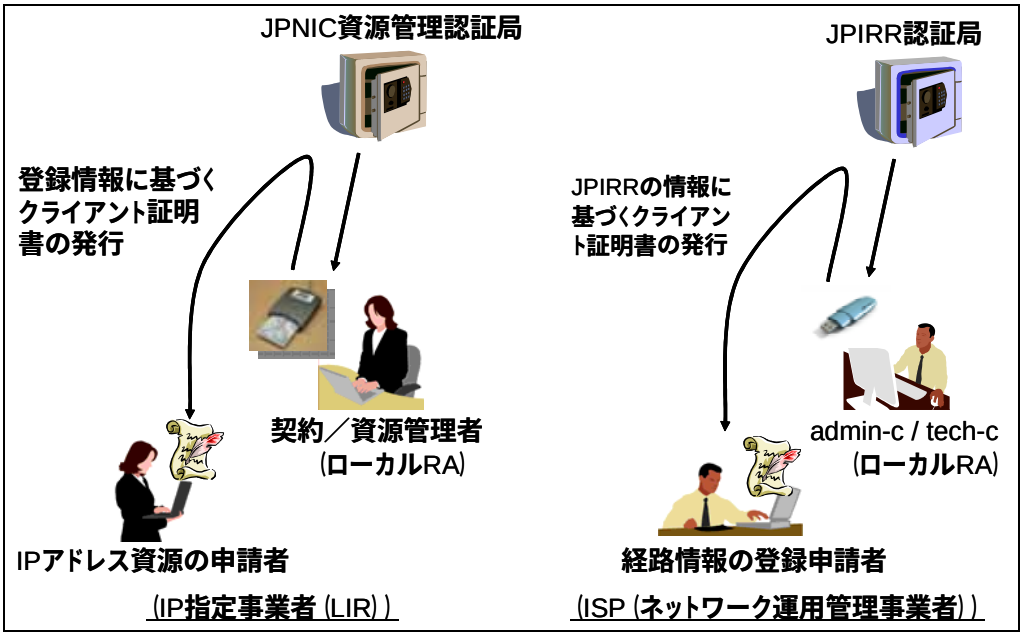

図 6-1　管理しやすいクライアント証明書の環境整備

IP 指定事業者と JPIRR のユーザ認証は、ユーザに対する電子証明書をローカル RA が管理できる仕組みで実現したものであり、証明書の発行対象は人である。この段階で電子認証フレームワークが関連することは、これらの電子認証の保証レベルである。

IP 指定事業者や JPIRR のユーザに発行された電子証明書は、組織内で本人確認手続

きが行われた、三文判的な電子証明書に位置づけることができる。これらの電子証明書はほぼ同一の保証レベルを持っているため、今後 ISP 業界やルーティングの業界で担当者同士が連絡をとり、暗号化もしくは電子署名を行う場合に、担当者印としての位置づけを持たせることが可能だと考えられる（図 6-2）。

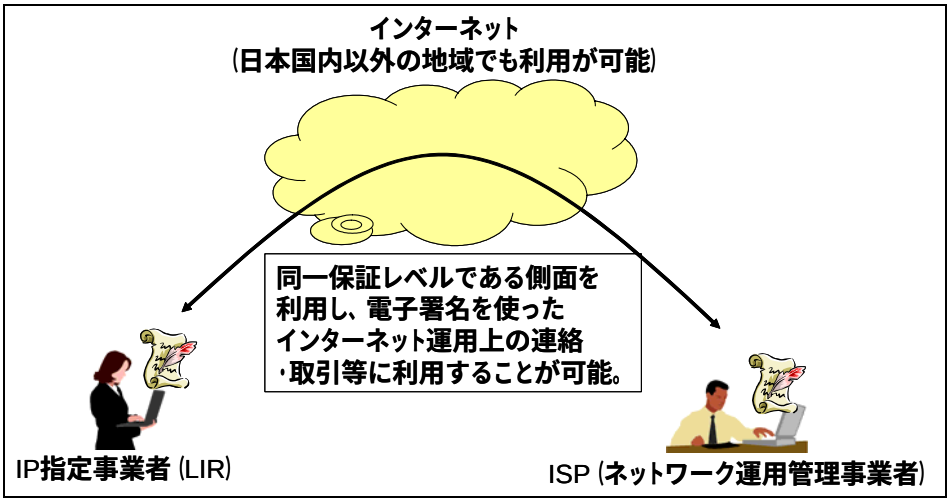

図 6-2　JPNIC 認証局の電子証明書を使った三文判的な PKI

また、これらはクライアント証明書の管理のしやすさを図った仕組みである一方、IP アドレスに関する登録情報に基づく認証情報の取り扱いを行う仕組みでもあった。ローカル RA モデルの構築によって、IP アドレスの管理者の電子証明書を使って、IP アドレスを割り当てられたホストのような人でないエンティティに対する電子証明書の管理体制を作ることができる（図 6-3）。

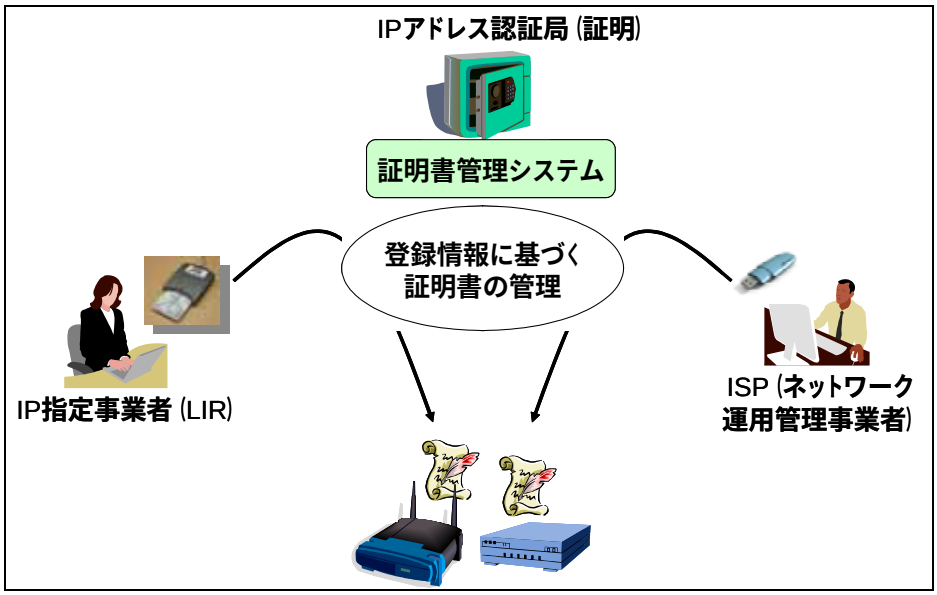

図 6-3　ローカル RA モデルの IP アドレス証明書の管理体制

6.2. IP アドレス認証の今後と電子認証フレームワーク

IP アドレス認証は今後、「経路情報の登録機構」に基づいた RFC3779 形式のリソース証明書への発展が可能である。また「経路情報の登録機構」や「JPNIC 資源管理認証局」は現在 IP レジストリシステムとの連携が行われていることから、「割り振り情報／割り当て情報」に基づくルーティング用の電子証明書や IPsec 用の電子証明書の発行なども検討可能な状態となった。

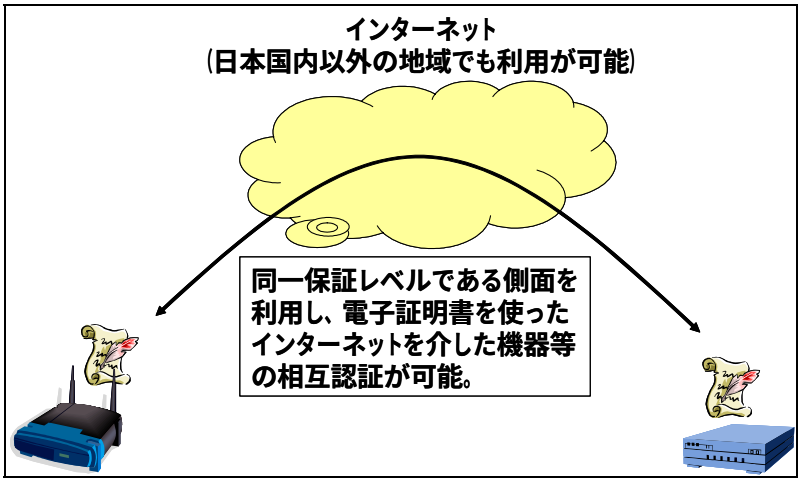

図 6-4　保証レベルに基づく人でない電子証明書の相互利用

今後、ユーザでない機器などのエンティティに対する電子証明書の位置づけを電子認証フレームワークの中で明らかにすることで、国際的に認知された電子証明書の相互利用を進めることが可能になると考えられる（図 6-5）。

図 6-5　ユーザ／IP 機器 向けの電子証明書の相互運用のイメージ

6.3. 今後の課題と活動

前節では、ユーザやインターネットに接続された IP 機器の相互認証の将来的なイメージについて述べたが、それには本調査研究で取り組んでいるノウハウの整理がある程度ついている必要がある。

今後、将来的な電子認証の相互運用を進めるためには、以下のような活動が必要になってくると考えられる。

- 電子認証の相互運用実験
  実際に電子認証技術の運用を行い課題点の抽出を行っていく必要がある。得られた課題点が技術上の問題なのか運用上の問題なのかを整理し、ユーザにとってわかりやすい解決策を提示していく必要がある。
- 電子認証・電子署名技術に関する最新動向の調査
  電子認証技術の問題点を整理するにあたり、技術の発展の方向性を把握しておく。例えば一方向性ハッシュアルゴリズムの代替性のように、標準化技術に変化があると運用面への影響が大きいと考えられる。
- 技術的なノウハウの整理
  ノウハウを蓄積するだけでなく、文書化することでより広いユーザやサービス提供者と情報共有ができ、また運用上の問題を解決しやすくなると考えられる。

今後これらの活動に取り組み、より適切な電子認証技術の利用と普及を進める必要がある。