第 6 章　電子認証フレームワークと IP アドレス認証の今後

内容

- IP アドレス認証と電子認証フレームワーク
- 今後のレジストリセキュリティ

6. 電子認証フレームワークと IP アドレス認証展開の今後

2006 年度の調査報告書の第 6 章で、本調査研究の将来像について述べた。2007 年度でもその将来像は大きく変わらないが、ここではより近い将来について述べたい。

まず電子認証フレームワークの今後について述べ、次に IP アドレス認証の展開の今後について述べたい。

6.1. 電子認証フレームワークの今後

電子認証フレームワークの調査研究の一環として立ち上げた、電子認証プラクティスフォーラムは、今後、まず、各分野に共通の電子認証リスクの回避に役立つようなノウハウの集約が図られると考えられる（図 6-1）。

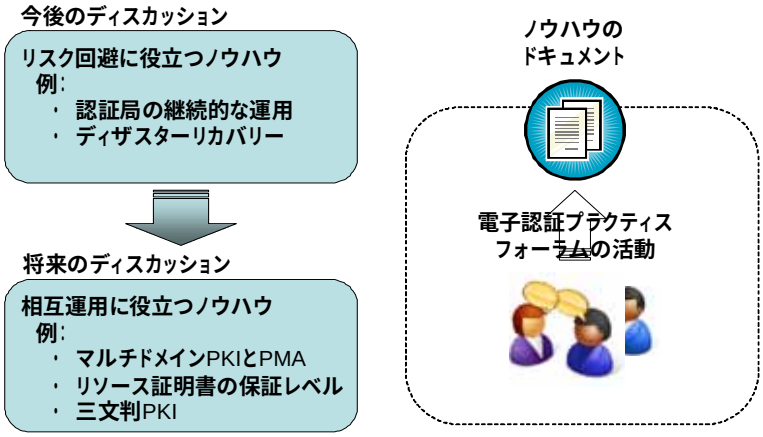

図 6-1　今後のディスカッションの傾向

これは現代、暗号アルゴリズムの変更可能性に関する議論や電子署名法をめぐる議論など、日本国内の認証局のビジネス環境に変化が起こっているためである。その中で、富士ゼロックスの横田氏が行ったような PKI アプリケーションの挙動の違いに関する調査結果と、例えば問題が起こりにくいキーロールオーバーの方法に関する情報が貴重である。

更にその先には、相互運用に役立つノウハウの提案やディスカッションが行われると考えられる。これはセコム株式会社の島岡氏や JPNIC の木村がアイディアとして提案したもので、複数の PKI ドメインを超えるような電子証明書の利用のために役立つようなノウハウである。

6.2. IP アドレス認証展開の今後

IP アドレス認証展開に関する調査研究の一環で開発した経路情報の登録機構は、今後、実験を継続し、IRR（Internet Routing Registry）の登録者増を図ると共に本機構の利用者増を図る。

本機構の今後は、すでに第 4 章で述べた ISP との連携である（図 6-2)。国内 ISP における正常な経路制御のために、JPIRR に蓄積された経路の情報が利用されることを示している。JPIRR は「正しい経路台帳」の役割を果たす。

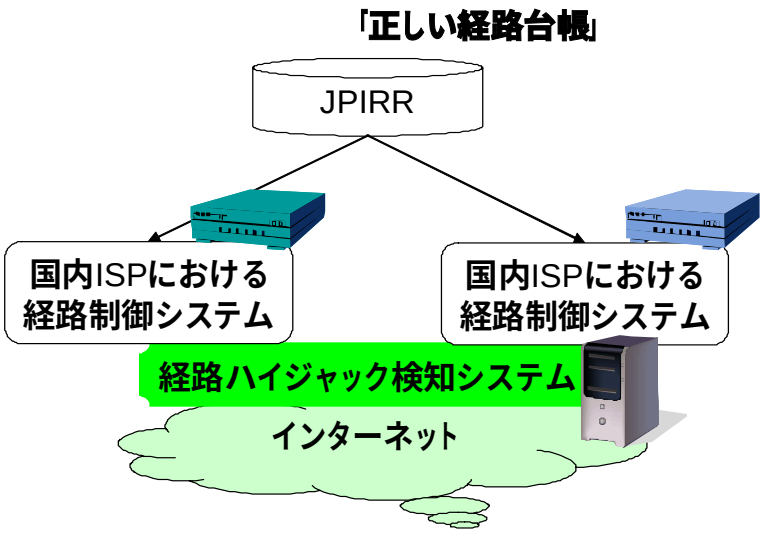

図 6-2　経路情報の登録機構の今後

IPv4 アドレスの枯渇に伴い、自組織の IPv4 アドレスが無断で使われてしまう問題が起きる可能性が高まると考えられる。これを避けるためには不正な経路情報を検知し回避することが重要である。今後、本機構の利用によって蓄積された正しい経路台帳を有効に活用し、広範囲のネットワークで役立つような普及を図ることが重要であり、また課題でもある。

もう一つ、将来像として考えられることはリソース証明書の発行である。第 5 章の RIPE NCC の CA-TF の調査の際に、APNIC の技術者が NIR の動向として provisioning に関する活動を行っていると紹介していた。この指摘が経路情報の登録機構に関する調査研究を指しているかどうか定かではないが、本機構がリソース証明書の発行インターフェースの一部として利用できる。

リソース証明書を発行する段階になると、電子認証プラクティスフォーラムにおける活動との連携が必要になる。リソース証明書の相互運用には、各レジストリや LIR によって発行される証明書の相互運用性が必須である。電子証明書の相互運用性は、プロフ

ァイルとしての相互運用性よりも、保証レベルとしての相互運用性の方が問題になりやすい。電子認証プラクティスフォーラムにて、相互運用が可能なリソース証明書を発行するための認証業務や CP をドキュメント化し、リソース証明書を検証するシステム開発者がそれを参照するような状況になることが望ましい。

6.3. 今後の課題と活動

前節で述べた今後の活動のためには、二つの調査研究で取り組んできたフォーラムおよびシステムの利用実験について、以下の課題があると考えられる。

- 電子認証プラクティスフォーラムの継続と発展
  2007 年度はドキュメント策定のプロセスを実験的に行ったが、今後は実際のノウハウを蓄積するための活動として継続する必要がある。そのために認知度を上げることや、コンテンツの充実、ノウハウの活用などを図る必要があると考えられる。

- 経路情報の登録機構の利用者の増加と普及
  経路情報の登録機構は、一部の希望者によって使われているだけでは効果が薄い。日本国内の IP アドレスの安全性を高めるという意味では、多くの ISP に利用され、またできれば IP アドレス管理業務の一環として組み入れるられる必要があると思われる。

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、およびインターネットセキュリティの向上を図りたい。