

経済産業省委託調査

IP アドレス
認証局のあり方に関する
調査報告書

2003 年 3 月

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

はじめに

インターネットは、かつてはネットワークの相互接続のための実験ネットワークであった。しかしその実用性と規模拡張性の恩恵により、現在では商業組織・学校・政府組織・任意団体・個人等様々な目的の多様なネットワークサービスがインターネットを用いて運用されるに至っている。企業間の取引や e-Japan 戦略に代表される政府の取り組み、インターネットを利用したソフトウェアの開発など、我々の生活に欠かせないインフラストラクチャ（生活基盤）の側面を持つネットワークになりつつある。

水道、電気、ガスといった既存のインフラストラクチャで共有される「資源」が存在するように、インターネットにはネットワーク資源と呼ばれる資源が存在する。ネットワーク資源とは、IP アドレスや経路情報の交換に使われる AS 番号、ドメイン名といった識別子で、インターネットレジストリによって管理されている。ネットワーク資源の管理は、インターネットの運用だけでなくインターネットを利用する通信サービスにも影響する。例えば、他の組織が登録したネットワーク資源を使って不正な通信サービスが提供された場合、本来、登録されていた組織が不正行為を行ったとみなされる可能性がある。

一方、APNIC や RIPE NCC といったインターネットレジストリでは、登録情報の保護をすでに実施している。ネットワーク資源を利用する組織は、登録内容だけでなく登録情報を書き換える際の認証情報を登録する。そこで使われる認証方式は、電子メールの送信者といった偽造可能な情報をもとにしたものではなく、公開鍵暗号を用いた強い方式である。

他のインターネットレジストリの状況を鑑みても、インターネットレジストリにおける登録情報の保護、延いてはネットワーク資源の不正利用を防止する方策を検討することは急務である。

この報告書では、日本のインターネットレジストリである JPNIC の役割を述べ、登録情報の利用上の脅威について述べる。セキュリティの機能には PKI (Public-Key Infrastructure - 公開鍵基盤) を適用し、安全性が要求される業務の運用要件について述べる。また PKI は登録情報の応用の可能性を広げるため、その可能性についても述べる。

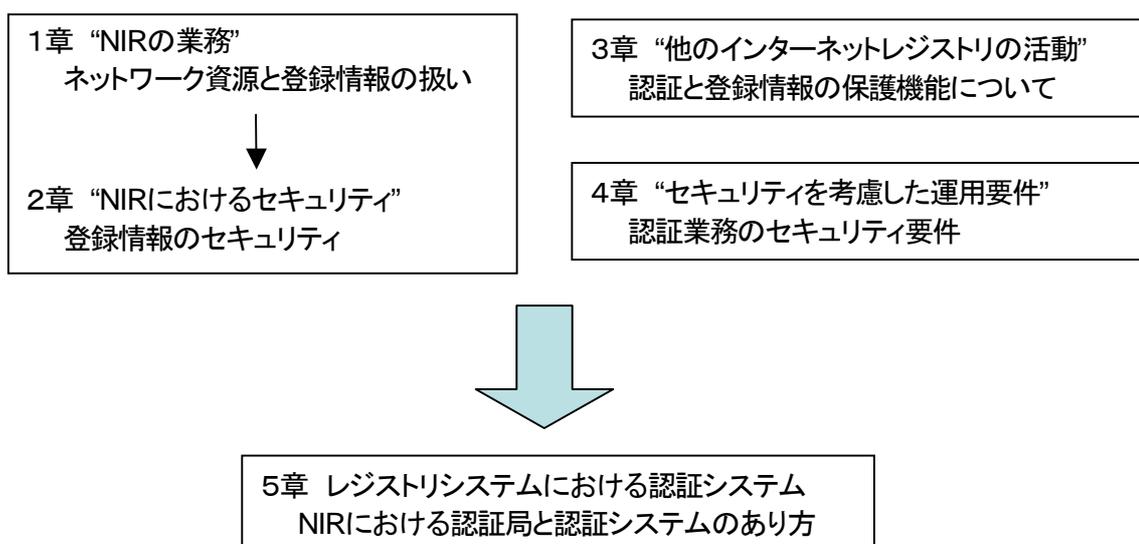
本年度の調査研究は、来年度以降に行う認証業務立ち上げのための基本調査である。来年度以降では、この調査結果を元に認証業務の具体的な要件事項を取り決め、事業を立ち上げるための活動を行う予定である。

本研究では、日本のインターネットレジストリにおける認証局のあり方について調査を行った。認証局のあり方を考慮するにあたり、以下の調査項目を挙げた。

- NIR におけるネットワーク資源と登録情報の扱い
- 登録情報を扱う際のセキュリティ要件
- 他のインターネットレジストリの認証および登録情報の保護機能
- セキュリティを考慮した運用要件
- レジストリシステムにおける認証システム

これらの項目の調査を通じて、機能的要件とセキュリティ要件の二つの面から、NIR における IP アドレス認証局のあり方を明らかにする。最後に IP アドレス認証局のあり方を元に、得られた知見と今後どのような活動が行われるべきかを述べる。

各章の関係を以下に示す。



第1章および第2章で、NIRの登録情報の扱いとその安全性について述べる。第3章では他のインターネットレジストリにおける認証や登録情報の保護について述べ、第4章では認証業務の運用要件として、認証業務の認定基準を基にした調査結果を述べる。第5章では各章の調査結果を受けて、NIRにおける認証局と認証システムのあり方についてまとめる。最後の第6章にて本報告書の内容をまとめる。