第6章 まとめ

内容

- 本報告書のまとめ
  - NIR における認証局の運用
  - 他のインターネットレジストリの活動
  - NIR の役割とセキュリティ要件
  - レジストリシステムと whois システムのセキュリティ
  - 登録情報の認証基盤の応用
  - インターネットレジストリの今後

6. まとめ

IP アドレスはインターネットにおけるネットワーク資源の一つである。インターネットの運用と、インターネットを利用した通信の信頼性の向上には、ネットワーク資源の確実な管理が必要である。この調査研究では、日本のネットワーク資源を管理する役割を担っている NIR（National Internet Registry – 国別インターネットレジストリ）における認証局のあり方に関して調査を行った。

6.1. NIR における認証局の運用

NIR は階層構造の組織関係を持つインターネットレジストリの中で、一つの国内の組織を対象としたネットワーク資源の管理を行う組織である。ネットワーク資源の管理は、経路情報の集約やアドレス資源の節約、予め登録された ISP（Internet Service Provider）へのアドレスブロックの割り振りなど、インターネットの運用上重要な役割を果たしている。アドレスブロックや AS 番号といったネットワーク資源の不正利用は、インターネットを使った大規模な不正行為を追跡不能にするなど影響が大きい。従って NIR の業務は、安全で確実に行われなければならない。

NIR における登録と割り振りの情報は、レジストリシステムとよばれるシステムで管理されている。レジストリシステムに登録された情報の一部は、ネットワーク利用組織同士が自律的な問題解決を行うことを可能にするために公開されている。従って NIR における資源管理の確実性を向上させるためには、レジストリシステムにおける登録情報の保護が必要となる。ネットワーク資源の管理権限を委譲していくインターネットレジストリの階層構造は、信頼できる第三者を見立てる認証方式を適用しやすい。そこで PKI を利用した認証システムをレジストリシステムに適用することが考えられる。

6.2. 他のインターネットレジストリの活動

APNIC や RIPE NCC といった他のインターネットレジストリでは、既にレジストリデータを保護する活動に取り組んでいる。APNIC や RIPE NCC では、登録情報の中に認証に関する情報を含め、書き換えを行うユーザの認証方法が明示されている。この一連の認証方式の中には、PKI を利用した方法は含まれていないものの、公開鍵暗号を利用した強い認証を使っているものが含まれている。更に、APNIC では CA Pilot Project の一環として認証局を構築し、X.509 形式の公開鍵証明書の利用を開始している。また RIPE NCC では、商用認証局ベンダーの証明書を使用した TLS を活用しており、PKI を利用した強い認証と利便性の両立を図っている。

6.3. NIR の役割とセキュリティ要件

NIR は国別のインターネットレジストリであり、ネットワーク資源の割り当て先に関する分類を持たない。つまり NIR が割り振ったネットワーク資源はインターネットに接続する政府、民間組織、任意団体などの様々な組織で使われる。そのため、NIR の運用はネットワーク資源の効率的な利用に貢献するだけでなく、信頼性の高い業務が行われる必要がある。特に NIR における認証業務は、各種セキュリティ要件を考慮した上に行われなければならない。

PKI を利用する認証業務は、認証局の運用を中心として行われる。本調査研究では認証局と認証業務の運用に関する、国内外の認定基準やガイドラインを調査した。具体的には、電子商取引実証推進協議会の認証局運用ガイドライン、電子署名法と施行規則および業務調査表、AICPA/CICA の WebTrust for CA の 3 基準を比較し、考察を行った。この調査を通じて、本人認証や設備、証明書の管理等、確実な認証業務の運用要件として検討されるべき項目が明確になった。また各項目についての考察を通じて、セキュリティ要件を定める為のいくつかの指針が得られた。またこの調査結果は、一般的な認証局の構築の際に参照できる詳細な基本資料になると考えられる。

6.4. レジストリシステムと whois システムのセキュリティ

インターネットレジストリにおいてネットワーク資源の管理に使われるレジストリシステムは、ユーザによる情報更新や、登録情報の一部を公開する機能を提供している。ネットワーク資源管理の確実性を向上するには、管理業務とこれらの情報サービスを提供するシステムに保護機能が必要である。

レジストリシステムに格納される情報は、データエントリー毎に、そのエントリーを書き換えることができる対象が決まっている。この条件をアクセス制御規則として定義し、強い認証が行われた上でアクセス制御の処理が実施されることで、登録情報の確実性が向上する。また whois システムが提供する情報の正当性をユーザが検証できるようにすることで、ネットワーク利用組織間の自律的な問題解決の際に、なりすましなどの安全性の問題に対策を取ることができる。

レジストリシステムと whois システムのセキュリティを、セキュリティモデルと情報モデルに基づいて検討した結果、登録情報は、本来オブジェクトセキュリティのモデルで保護機能を設計すべきであることがわかる。ただし、ユーザの利便性や PKI を利用することができるソフトウェアの実装状況を考えると、通信中のデータを保護するトランスポートセキュリティのモデルを適用する場合が考えられる。ユーザ向けのサービ

スの違いと、whois システムに適用できるプロトコル策定状況を鑑みて、今後更に検討が行われ、そして設計が行われる必要がある。

6.5. 登録情報の認証基盤の応用

ネットワーク資源の利用が確実な登録情報に基づいて行われると、その情報を用いた各種ネットワークプロトコルの、より安全な利用方法が考えられる。例えば、ある組織と、その組織がネットワークサービスの一環として提供しているゲートウェイの IP アドレスの組み合わせが正しいことを確認できる機能が考えられる。IP アドレスはインターネットの運用に直接的に関係する識別子であるため、インターネットレジストリにおける確実な管理と組み合わせることで、ネットワーク利用組織の実在性、サービスを提供するホストの IP アドレスについて、その組織の所属性を確認できる認証基盤ができる可能性がある。また識別子の組織の所属性を登録情報で証明することで、認証局の為の証明書リポジトリや証明書の確認手段を提供することも考えられる。

6.6. インターネットレジストリの今後

この調査研究を通じて、インターネットレジストリの役割が、インターネットの運用だけでなく、その安全性にも影響することが明らかになった。今後、ネットワーク資源管理の確実性が向上することで、今後インターネットの利用法の中に確実なやり取りを必要とする、クリティカルなサービスが含まれていくと考えられる。インターネットレジストリは、運用の保全と共に、ユーザ環境における利便性と安全性に関する知識を蓄積していくことが必要になると考えられる。

第 6 章　まとめ