経済産業省委託調査

IP アドレス認証局の
マネジメントに関する
調査報告書

2004 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

平成 15 年度 情報セキュリティ基盤整備
IP アドレス認証局のマネジメントに関する調査研究　概要

背景と目的

IP アドレスはインターネットに接続する際に必ず必要になるアドレスである。世界各国で使われる IP アドレスはアドレス資源として位置づけられ、ICANN/IANA を頂点とするインターネットレジストリ（以下、レジストリと呼ぶ）によって割り振り業務が行われている。その際、レジストリは利用されているアドレス資源と利用組織を登録し、連絡先などを適宜公開することでネットワークの自律的な運用を支えている。従って、レジストリの保持する登録情報はインターネットにおける台帳の意味を持つ。

前年度に実施した IP アドレス認証局に関する調査研究から、アドレス資源管理と公開鍵基盤（PKI：Public Key Infrastructure）を利用した登録情報の保護および活用（電子証明書の利用）が有効であることが判明した。これはアドレス資源の登録管理を行うレジストリが認証局を運用し、アドレス資源の利用に関して電子的に検証可能な登録情報を持つことで、インターネットにおける基盤的な認証基盤の構築が可能なためである。国際的にアドレス資源管理を行っている APNIC（Asia Pacific Network Information Centre）や RIPE NCC（Réseaux IP Européens Network Coordination Centre）でも認証局を利用した登録情報の保護機能を実現する為の取り組みが進められ、既に運用が開始されている。どちらのシステムもその有効性が評価されており、特に昨年度から今年度にわたって機能拡張や技術開発の動きが見られている。

これらの状況を鑑み、本調査研究は、日本におけるアドレス資源の登録機関である JPNIC において認証局の構築を行い、アドレス資源の利用に関する登録情報の保護と活用の検討を行うものである。この調査研究は下記の柱を軸に実施される予定である。

- レジストリにおいて認証局を運用することにより、アドレス資源に関する登録情報の確実性を高める。
- 登録情報の確実性に基づいた証明書を発行することにより、インターネットを利用するアプリケーションにおいて応用可能な認証基盤の基礎を作る。

前者は、認証局における認証業務の構築を通じて登録情報の保護を行い、アドレス資源管理の確実性の向上を図る。後者は、アドレス資源管理の確実性に基づく証明書の利用とネットワークへの応用性について検討を行う。

実施内容

前述の通り、登録情報の保護に関してはAPNICやRIPE NCCにおいても検討が行われているが、これらはJPNICが目標としている強固な認証基盤とは異なり、CP/CPSの策定を伴うような認証業務については世界のレジストリにおいて前例がない。従って、認証業務の要件、方針といった検討から始め、認証業務の検討に繋げるという実施方法を取る。平成15年度までの活動内容を図 a に示す。

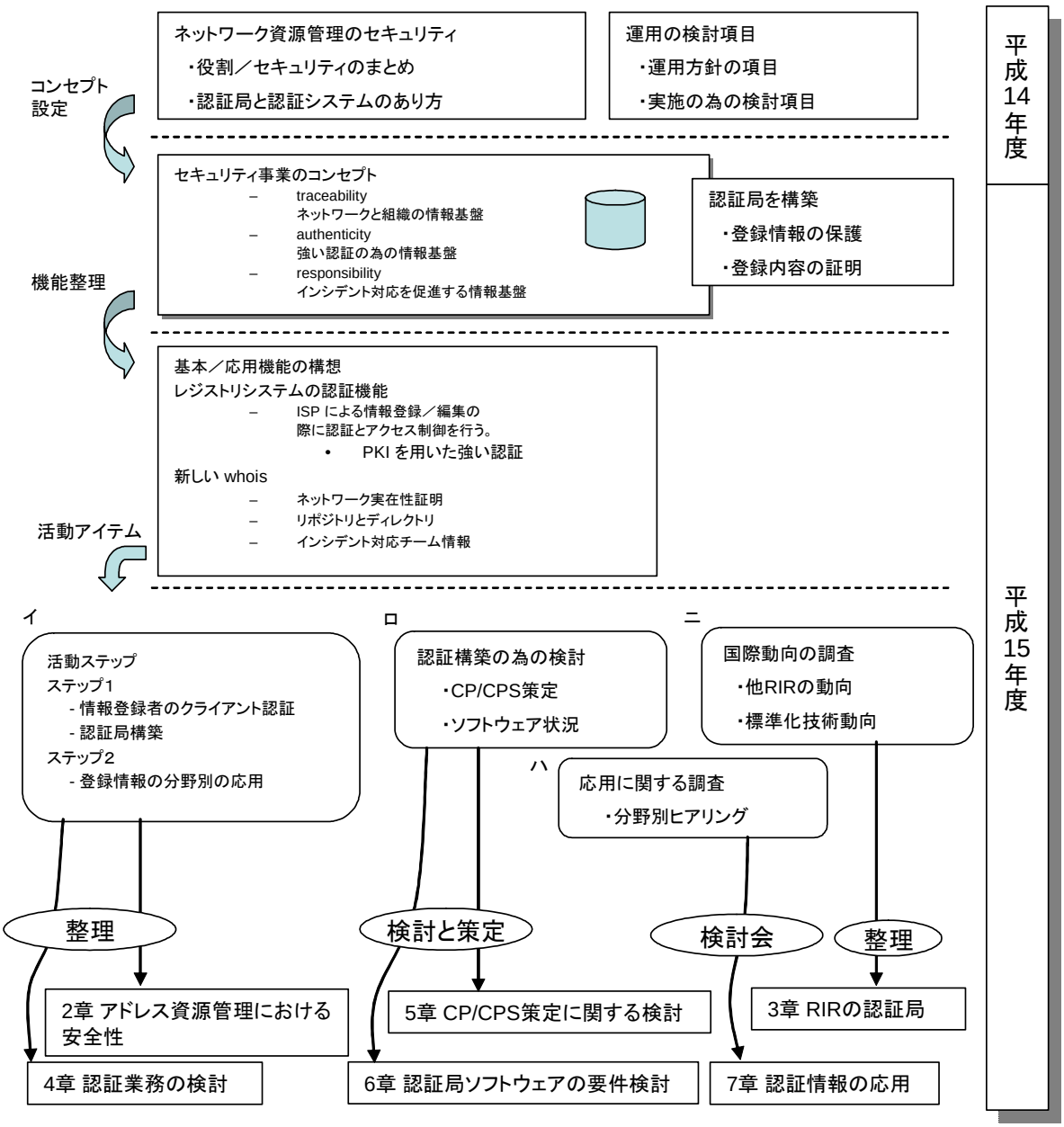

図 a　活動内容と本報告書の関連

はじめにインターネットにおける、認証技術利用の観点から、認証基盤の事業の考え方をまとめる。これが、traceability（ネットワークと組織の情報基盤）、authenticity（強い認証の為の情報基盤）、responsibility（インシデント対応を促進する情報基盤）の 3 つである。同時に、強い認証基盤と認証局の運用に関する調査研究を進め、JPNIC における認証局の機能を整理する。この認証機能実現のための構築／マネジメントのための検討活動をイ、ロ、ハ、ニのアイテムに分ける。これらは平成 15 年度に実施され、その後、開発・運用体制の確立・応用アプリケーションの検討などに繋げていく。

活動アイテム（イ）では、アドレス資源管理における安全性に関する調査を行い、レジストリにおける認証業務の検討を行う。この段階で業務モデルを設計する。これらの検討については報告書の 2 章と 4 章にまとめる。（イ）の調査および検討の結果を基に認証業務の為の検討（ロ）を行う。（ロ）では運用の要素（役割）と技術（ソフトウェア）の要素に分けて検討を進める。運用の要素は、（ロ）の認証業務規程（CP/CPS）の策定に反映し、技術の要素は認証局ソフトウェアの要件の検討を通じて行う。これらは報告書の 5 章と 6 章にまとめる。

これらの検討に並行して、RIR の認証局の動向調査および標準化技術の動向調査（ニ）を実施し、RIR における認証技術の利用や将来的な連携可能性等についての情報収集を行っておく。これは報告書の 3 章にまとめる。

更に JPNIC 認証局の持つ認証情報を応用するネットワークアプリケーションについての調査研究を行う（ハ）。これは各種ネットワーク利用分野（家電メーカー、グループウェアベンダ、通信事業者など）の専門家にヒアリングを行った上で、検討会を通じた意見交換を行いアイディアの集約を行う。その後は、集約されたアイディアを基に実現方法と課題の解決方法について検討を行っていく。

これらの検討を通じて、アドレス資源の登録業務を行う国内のレジストリ（JPNIC）による、強固な認証基盤の構築と、RIR との協調（認証基盤の国際化）、ネットワークを使うアプリケーションのための認証機能の基盤作りを進めていく。

調査結果

- アドレス資源管理における安全性の調査

  レジストリにおけるアドレス資源管理と登録管理業務の安全性について調査した。登録管理業務の安全性は登録データの安全性に依存しており、登録データの不正利用におけるリスクを検討すると、レジストリのシステムには登録時の強力な認証機能が必要であることが判明した。この認証機能は、アドレス資源管理の構造に則ってアドレス資源の割り振りを受けた組織によって利用される。更に電子署名を使ったデータ認証を行う仕組みができれば RIR との連携の際の安全性を向上させることが可能であり、世界規模の証明の基盤が構築可能であることも示された。

- 認証業務の為の検討調査

  CP/CPS の策定の為に、認証業務の検討、認証モデルの構築などを行なった。レジストリにおける担当者の権限管理に合わせ、様々な要因を検討した。認証業務の検討には、RFC3280 などのフレームワークが存在するが、業務モデルの構築と役割の検討を基に多数の資料を用意し、適切な業務負荷と運用を導いた。この検討資料は、他の認証業務の検討の場合にも参考情報になりうる内容を含んでいるため、できる限り多くの資料を報告書にまとめた。

- 国際動向（RIR の認証局と標準化技術）の調査

  RIR（Regional Internet Registry：地域インターネットレジストリ）の APNIC や RIPE NCC では既に認証局を構築し、ユーザ認証の為の証明書の発行を行なっている。ユーザ認証は主に Web サービスで利用され、資源管理機能の実現を目標に活動が行われている。認証局の運用形態は、スタンドアローンで認証局証明書はユーザが各自で組み込む形態である。

  一方、APNIC および RIPE NCC の技術担当者の間では、電子署名を用いた認証基盤の構築に関してもアイディアが議論されていた。

  また IETF においてレジストリにおける登録情報の扱いに関連したプロトコル（CRISP と EPP）の策定が進んでいる。

  これらのことから IP アドレス認証局は、まず登録者の認証機能を実現し、次に電子署名の仕組みを構築した上で RIR との連携を図ることでインターネット全体のアドレス資源管理に則った認証基盤の構築が可能であることが考察された。ただし、CP/CPS を策定し運用レベルの高い業務を構築することで、インターネットにおける基盤的な認証局の構築が可能と考えられる。

- 認証情報の応用に関する調査

  認証情報の応用に関しては、アドレス資源と属性情報の証明という考え方を基本に、様々なアイディアを集約した。アドレスブロックを用いた証明書の発行をはじめ組織属性の検証、地域属性の検証、用途属性の検証など、様々な用途が考えられることが示された。

結論と今後の活動

今年度の調査研究を通じて、レジストリと ISP によるアドレス資源管理の業務体系にあわせた認証業務について調査研究を行った。またアドレス資源の登録情報に属性情報を付加することにより、IP アドレス認証局が安全な IP ネットワークの構築に利用できることが示された。

IP アドレス認証局は、レジストリのアドレス管理業務にともなって運用されることにより、基盤的かつ世界規模の認証基盤となりうる。インターネットにおける認証基盤を構築するにあたり、レジストリのような登録機関がアドレスと実体との対応付けを証明し、また属性情報を付加することで、応用性の高い認証基盤となる。

今後、IP アドレス認証局の構築を進めると共に認証情報を応用するアプリケーションの実現に向けた検討を継続して行う。