

第 1 章 本調査研究の背景と位置づけ

内容

- 調査研究の位置づけ
- 調査研究の活動と本報告書の内容

1. 本調査研究の背景と位置づけ

本調査研究は 2005 年度から 3 年度の計画で実施している「電子認証フレームワークと IP アドレス認証の展開に関する調査研究」の 2 年目である。「電子認証フレームワーク」とは電子認証に役立つ BCP (Best Current Practice) によって電子認証の分類やレベルを整理する枠組みを意味する。また「IP アドレス認証」は 2005 年度までに JPNIC において構築されてきた「IP アドレス認証局」を中心とする認証基盤を使った電子認証のことで、IP アドレスに関する登録情報を使った電子証明書を利用する点に特徴がある。この 2 つは一見別々のテーマのように見えるが、本質的には密に関連するテーマである。

本章では、本調査研究の進め方、重点、年度ごとの活動について述べ、最後に本報告書の章立てについて述べる。

1.1. 2006 年度の調査研究の位置づけ

本調査研究は、インターネットレジストリである JPNIC における認証基盤の構築と電子認証の適切な普及に必要な BCP を策定する仕組み作りの 2 つのアプローチを行う調査研究である。本調査研究のポイントは 2 つある。一つは IP アドレス認証の展開と電子認証フレームワークの各々を確立することである。もう一つは IP アドレス認証の展開によって構築された認証業務を電子認証フレームワークの中で整理し、ノウハウをドキュメント化して残していくことである。本調査研究の進め方は、はじめに各々を別個に進め、最終的にドキュメントにまとめるような形となる。

本調査研究は次に述べるような進め方で実施している。はじめに諸外国におけるドキュメント策定プロセスを調査し、電子認証フレームワークの要件を調査する。次にこのフレームワーク自体をドキュメントとして策定するための仕組み「電子認証プラクティスフォーラム」の試験的な設置を行い、専門家による議論を通じてノウハウとなるドキュメントの策定を行う。一方、「IP アドレス認証の展開」は次のように進める。はじめにインターネットレジストリにおける登録情報を利用した電子認証の役立つ分野について調査する。次に必要とされる認証局や関連システムを構築し、実験的な運用を行う。最後にこれらの電子認証の有効性が確認し本運用に向けた検討を行う。

2005 年度は、電子認証フレームワークと IP アドレス認証の展開の両方のあり方について調査研究を行った。電子認証フレームワークについては諸外国における BCP に近いドキュメントの策定プロセスについて調査を行い、日本国内での BCP の策定に対する要求事項などについてまとめた。IP アドレス認証の展開については、インターネットにおけるルーティングの安全性向上に役立つ電子証明書とルーティングプロトコルについて調査を行った。

第 1 章 本調査研究の背景と位置づけ

2006 年度は、電子認証フレームワークに関する活動よりも IP アドレス認証の展開を先行させ「経路情報の登録機構」の開発を行った。これは本機構の実験運用を先行させることで、JPNIC 内での電子認証に関するノウハウの蓄積が早まると考えられたためである。電子認証フレームワークについては専門家との議論を進め、フレームワークを策定するためのオープンなフォーラムである「電子認証プラクティスフォーラム」の具体化を進めた。

1.2. 調査研究の活動と本報告書の内容について

2006 年度はドキュメント策定プロセスに関する調査と電子認証技術の動向、RIR における IP アドレスに関する登録情報のセキュリティなどについて調査研究を実施した。本節では、それぞれの活動とテーマの関連性と、本報告書でのまとめ方について述べる。

- **RIR における登録情報データベースの動向調査**

2006 年度、APNIC、RIPE NCC、ARIN といった主要な RIR では本調査研究と時期を同じくして IP アドレスの経路制御に対する認可に関する議論が行われていた。主要な RIR のミーティングと IETF の関連する WG に参加し、現地の職員と情報交換を行うなどして詳細の調査を行った。調査の結果を第 2 章にまとめた。

- **ドキュメント策定プロセスについての調査**

国外では主に IETF のミーティングに参加し、また国内では JANOG や JPOPM といったミーティングに参加し、オープンなミーティングやコミュニティでのドキュメント策定プロセスについて調査を行った。2006 年度は次に述べる「経路情報の登録機構」の開発に重点を置いたため、この調査は技術最新動向に関する調査の一環として行う程度に留まった。主に IETF での議論について第 3 章にまとめた。

- **電子認証技術の動向に関する調査**

主に IETF のミーティングに参加し、電子認証技術の最新動向について調査した。また近年の状況をわかりやすくするため、4.5 年前以降からの動向とここ 1 年の動向という形でまとめなおし、電子認証技術の標準化で取り組まれている技術分野の変化などについて第 3 章にまとめた。

- **「経路情報の登録機構」の設計と開発**

RIR におけるアドレス資源の認可機構、および APNIC におけるリソース証明書動向を受け、IP アドレス認証の展開の為に「経路情報の登録機構」の開発を行った。認証局システムの開発を伴うため、2006 年度はこの活動に重点を置いた。詳細を第 4 章にまとめた。

- **電子認証フレームワークの定義と仕組みの検討**

国内外での電子認証の普及状況を鑑み、専門家との議論を通じて整理が進んだ電子認証フレームワークの定義や仕組みについてまとめた。フレームワークを策定する活動「電子認証プラクティスフォーラム」と、フォーラムの活動を実現するための要件とシステム構築について第 5 章にまとめた。

第 6 章では、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の関わり方について整理し、調査研究の方向性を交えてまとめた。

また RIR や IETF での情報交換のなかで、JPNIC の認証局や本調査研究に対する関心は高いと感じる場面がたびたびあった。そこで JPNIC 認証局に関する情報提供のため、JPNIC の資源管理認証局（前 IP アドレス認証局（認証））の CPS（Certification Practice Statement）と、認証局証明書利用規約を英訳した。これらは Appendix として本報告書の最後に掲載する。

第 1 章 本調査研究の背景と位置づけ