第 1 章　調査研究の背景と位置づけ

内容
- 調査研究の背景
- 調査研究の実施内容
- 調査研究の成果物

本報告書の章立て

1. 調査研究の背景と位置づけ

本章では、「電子認証フレームワークの在り方に関する調査研究」の背景と、2004 年度までに行われた IP アドレス認証局に関する調査研究との位置づけについて述べる。また本報告書の章立てについて述べる。

1.1. 調査研究の背景

当センターでは、2002 年度から 2004 年度にかけて「IP アドレス認証局」の構築に取り組んできた。IP アドレス認証局は IP アドレスというアドレス資源の管理を、国際的な連携を図りつつセキュアにするための認証局である。認証局というと、しばしば、認証の機能を一手に担うような総合的な仕組みだと思われてしまわれることがある。しかし認証局は、端的にいえば電子証明書を発行する機能でしかない。電子証明書を使って何をどのように認証するか、ということは電子証明書を使ったシステムを構築する側に任されているのである。従って、認証局がインターネットのアドレス資源（IP アドレス等）のセキュアな管理にどう生かされてくるのかは、認証局を構築、運用し、電子証明書の用途を詳細に検討する必要がある。

2004 年度までに行われた調査研究は、JPNIC におけるこの認証局の役割を明らかにする為の調査研究であった。電子証明書が誰にどのように使われるのか、それによって何がセキュアになるのか、といったことを組み立てていく作業である。2002 年度から 2004 年度の活動の結果、電子証明書を使ったユーザ認証用と、その電子証明書を発行する仕組みの構築の必要性が明らかになってきた。そこで CPS（Certificate Practice Statement：認証業務規程）の検討を行った。その結果、JPNIC に IP アドレスの情報登録を行う「IP アドレス管理指定事業者」の認証を強化し、日本国内の IP アドレスに関する登録情報の正当性を向上させる取り組みを行うこととなった。更に JPNIC で運用される複数の認証局の役割が決まり、その一部が実験的に稼動し始めた。JPNIC の認証局の構築に当たっては、CPS(Certificate Practice Statement - 認証業務規程)の策定や記述例のまとめを通じてノウハウが蓄積されてきた。

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」というタイトルで調査研究に取り組んだ。「電子認証フレームワーク」は、電子認証技術の適切な普及を図るための調査研究である。認証局を実現するための技術である PKI(Public-Key Infrastructure)は、データフォーマットや処理方法の策定は進んでいるものの、広く普及していない。PKI でないパスワードベースの電子認証は、フィッ

シングサイトによるパスワードの盗用や通信路の盗聴等、安全性が危惧されているにも関わらず多くのシステムで使われ続けている。この原因は、PKI に比べてパスワードシステムは見かけ上の使い方がわかりやすく、システム構築や初期のユーザ教育が容易であるためだと考えられる。しかし既存の多くの利用法は、システム構築を行うものの知識や意識レベルによるところが大きく、実際には安全でないこともある。すなわち安全な利用方法のノウハウを明文化して、多くの技術者に理解されやすい状態にしておくことが望ましい。いわばノウハウのデファクト・スタンダードである。この標準的で多くの技術者に確認されたノウハウをいかにドキュメント化して残していくか、その共通認識の形成の場はどんなものであるべきなのかがポイントとなる。このノウハウがあれば、パスワードを使った認証システムを安全に運用しやすくなるだけでなく、パスワードよりも安全にしやすい PKI の、適切な普及を図ることができる。

「IP アドレス認証の展開」は JPNIC の認証局の役割を発展させ、登録情報に基づく認証を具体的なアプリケーションに発展させる調査研究である。JPNIC で取り扱っている登録情報のほとんどは IP アドレスに関連付けられた情報である。IP アドレスは Web サーバや企業や家庭のパソコンを始め、電話網や家電など、様々な機器で使われており、用途が広がりつつある。IP アドレスの登録情報を使うと、これらの機器の識別やネットワークとしての所属性を調べられるため、登録情報を基にした電子認証を通じて通信の信頼性を高めることの意義は大きい。

本調査研究の初年度である 2005 年度は主にインターネットのルーティングの安全性向上を図るための電子認証に取り組んだ。インターネットにおけるルーティングは、インターネットの IP パケットの伝送網を支える最も重要な仕組みである。インターネットを利用する全てのアプリケーションに共通して利用される、基盤的な仕組みである。ルーティングの安全性の向上を図らずに、インターネットアプリケーションの可用性向上を図ることは考えにくい。しかしインターネットのような分散環境におけるルーティングは、中央集権的な役割を設けず、各ネットワークの自律的な運用を原則としている。この状況で、ルーティングを安全にするために JPNIC の認証局が提供する電子認証をどのように適用するのかがポイントとなる。

2005 年度は 3 年度計画の初年度であるため、調査研究の方向性を探ることに多くの時間を費やした。本報告書では、調査研究の過程で見出されてきた「電子認証フレームワークのあり方」や「IP アドレス認証の展開のあり方」を様々な情報交換や検討の経緯を交えて報告したい。

1.2. 調査研究の実施内容

本調査研究は、二つのテーマについて取り組む。どちらのテーマも国際会議を通じた情報交換と、専門家による検討を重ねて実施することとなった。

電子認証フレームワークに関する調査研究では、PKI の専門家で、かつ IETF 等の標準的なドキュメント策定の会議に詳しいメンバーでチームを構成して、現在の電子認証の普及に必要な仕組み（フレームワーク）に関する議論を繰り返して行った。その結果、電子認証の適用に関するベストプラクティス・ドキュメントが必要であることが分かってきた。ベストプラクティスとは、IETF で使われている用語である Best Current Practice の意味を示している。これは現在わかっている最善の実践方法という意味で、技術を利用または運用するにあたって判明している、いわばノウハウである。またこのノウハウとして現在必要とされているものを調査するため、電子認証の「保証レベル」やドキュメント策定プロセスに関する基本調査を実施した。

IP アドレス認証の展開に関する調査研究では、IETF 等国際会議を通じた情報交換や JANOG(Japan Network Operator's Group)での意見収集、ISP へのヒアリング等を実施した。その結果、IP アドレス認証の展開の仕組みとして許可リストと呼ばれる仕組みを提案することとなった。この仕組みは、インターネットにおける経路制御（ルーティング）のセキュア化のため、IP アドレスと AS 番号（Autonomous System 番号）の正当な組み合わせを作り出していくためのものである。

1.3. 調査研究の成果物

本調査研究は、IP アドレス認証の展開のあり方、および電子認証フレームワークのあり方を明らかにする調査研究であり調査検討の結果が成果物となる。本報告書では、検討のために使用した発表資料を始め関連性が強い技術標準、ガイドラインに関する基本調査資料などを交えて調査結果を報告する。

1.4. 本報告書の章立て

本報告書の章立てについて述べる。第 2 章では本調査研究のテーマのひとつである電子認証フレームワークの意義と IP アドレス認証局との関係について述べる。第 3 章では IETF における電子認証技術とドキュメント策定プロセスの動向について報告する。IETF では参加者主体のプロトコル策定活動を行っており、電子認証フレームワークのガイドライン策定プロセスを構築するに当たって参考になる活動である。第 4 章では電子認証フレームワークの要件を検討するにあたって調査した、電子認証の運用に関するドキュメントやその策定プロセスについて述べる。第 5 章では第 4 章の調査結果を受け、電子認証フレームワークの在り方について述べる。第 6 章では IP アドレス認証局とその認証の展開について概説する。第 7 章では、IP アドレス認証の展開を行う分野であるインターネットのアドレス資源管理と経路情報の現状について述べる。第 8 章で経路情報におけるセキュリティの現状について述べ、第 9 章で主に電子認証技術を利用した不正利用排除の仕組みについて述べる。第 10 章ではインターネットの可用性維持の為の、安全な経路情報の交換の課題について述べる。第 11 章では本調査研究をまとめ、今後の活動の方向性について述べる。