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. 本調査研究の概要と位置づけ

本調査研究は、2005 年度から 2007 年度の 3 年計画で実施している調査研究の 3 年目である。また 2005 年度の調査研究に先立ち、本調査研究の背景となった、IP アドレス認証に関する調査研究が行われていた。

本章では、始めに調査研究の概要を示し、次に本調査研究の背景と 3 年計画の中の位置づけについて述べる。

1.1. 調査研究の概要

本調査研究は「電子認証フレームワークに関する調査研究」と「IP アドレス認証の展開に関する調査研究」の二本立てである。各々の調査研究の概要について述べる。

1.1.1. 電子認証フレームワークに関する調査研究の概要

調査研究の概要を図 1-1 に示す。

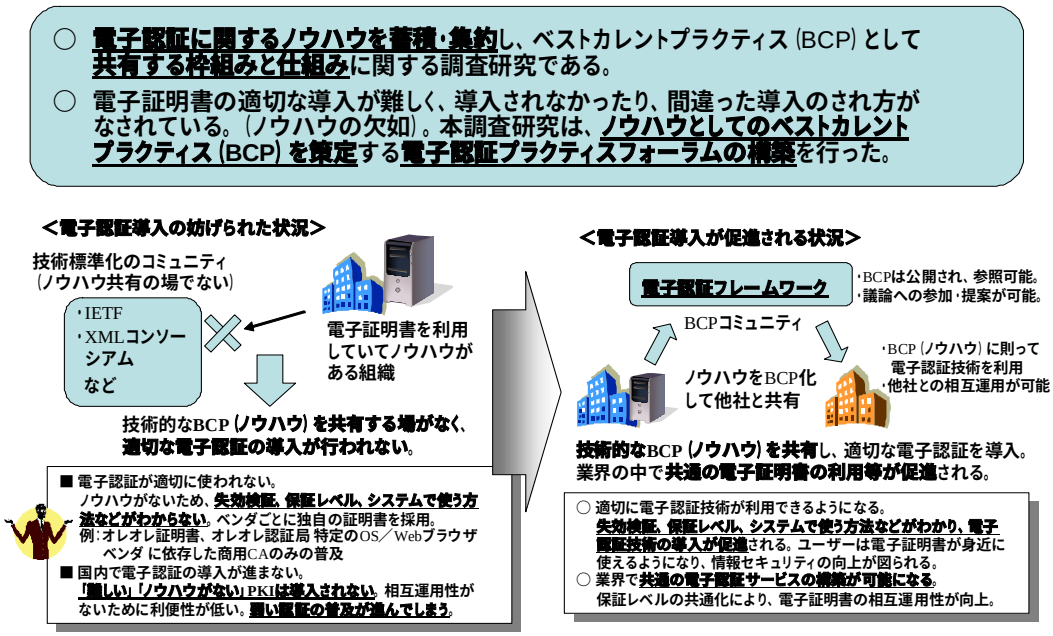

図 1-1　電子認証フレームワークに関する調査研究

電子認証に関するノウハウを蓄積・集約し、ベストカレントプラクティス（BCP）として共有する枠組みと仕組みに関する調査研究である。

電子認証技術は、利用のノウハウが得にくいため適切に使うことが難しい。例えば失効検証の適切な行い方や保証レベルの設置の仕方、システムで使う方法などのノウハウが考えられる。そのため電子認証技術は「難しい」という印象があり、また相互運用性を確保する使い方がされていないために利便性が低い。

本調査研究では、ノウハウをドキュメント化し、会議を通じて継続的に「ベストカレントプラクティス（BCP）」を策定する電子認証プラクティスフォーラムの構築を行った。

1.1.2. IP アドレス認証の展開に関する調査研究の概要

調査研究の概要を図 1-2 に示す。

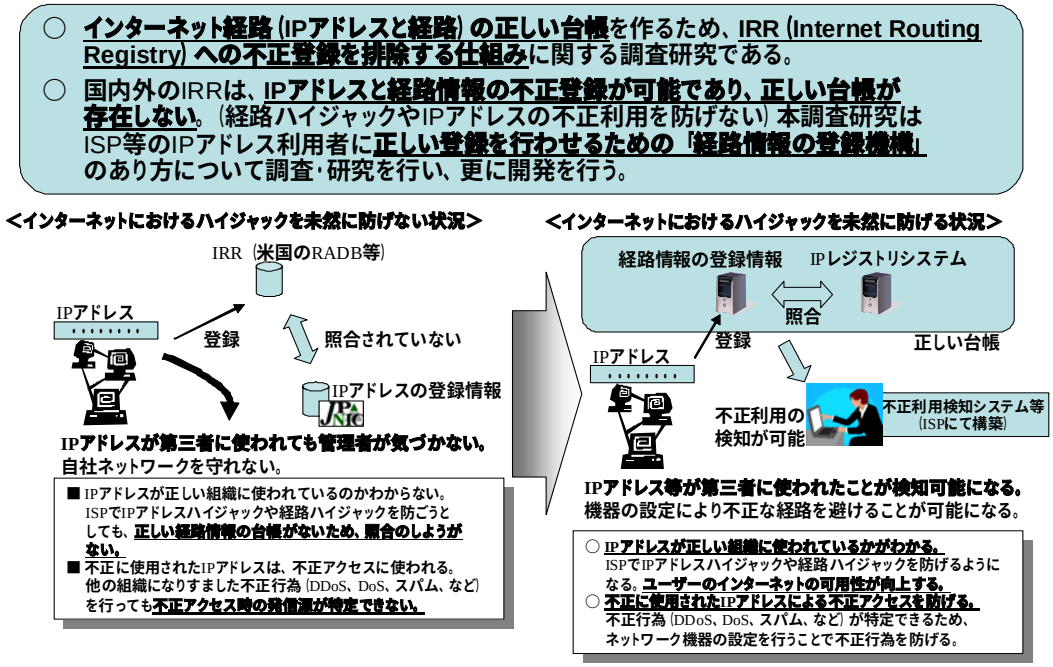

図 1-2　IP アドレス認証の展開に関する調査研究

インターネット経路（IP アドレスと経路）の正しい台帳を作るため、IRR（Internet Routing Registry）への不正登録を排除する仕組みに関する調査研究である。

IP アドレスの登録情報と経路情報のデータベースが異なり、いわば正しい経路情報の台帳が存在しない。そのため IP アドレスが正しい組織によって使われているのかどうかが本質的にはわからない。なお経路ハイジャックが行われているようなときには、不正アクセスの発信源を特定できない。

本調査研究では、ISP 等の IP アドレス利用者に正しい登録を行わせるための 「経路情報の登録機構」のあり方について調査・研究を行い、更に開発を行った。

1.2. 調査研究の背景

2005 年度より以前、当センターでは「IP アドレス認証局」と呼ばれる認証局に関する調査研究を行っていた。これは IP アドレスのレジストリである JPNIC において認証

局を運用し、インターネットセキュリティの向上に役立てることを目的とした調査研究である。

IP アドレス認証局の調査研究の結果、独自の認証局を構築し、更に IP アドレスに関する登録情報を守るためのユーザ認証用の認証局を構築することとなった。JPNIC 独自の認証局が構築した理由は、IP アドレスやインターネットのアドレッシングに関する「信頼点」として機能する authority を確立し、その認証局を当センターで運用することで登録情報を各種ネットワークサービスに役立てようという考え方に至ったためである。

このような背景から、認証局の構築あたっては、CP（Certificate Policy - 証明書ポリシー）や CPS（Certification Practice Statement – 認証業務規程）の策定や運用のレベル、業務モデルに関する検討を一から行い、同時に IETF PKIX WG などの最新の国際動向の調査を行ってきた。また電子認証技術に関する利用者へのヒアリング等も行ってきた。

2005 年度の本調査研究を開始する段階になると、JPNIC に電子認証に関する知見が得られる人的環境が整ってきたが、すると電子認証技術が持つ課題や、普及のカギが欠けている現状が見えてきた。それが次に述べる電子認証フレームワークと IP アドレス認証の展開の調査研究を行うことになった背景である。本調査研究のテーマが「電子認証フレームワーク」と「IP アドレス認証の展開」の二つになったのには、各々に背景がある。ここで各々の調査研究の背景について述べる。

1.3. 電子認証フレームワークの背景

インターネットを通じて提供されている、様々な個人向けまたは企業向けサービスにおいて、その電子的すなわちオンラインでの認証方法はパスワードが主流である。中には強い電子認証技術を使うような IC カード（Felica とは異なる、耐タンパ性を持った IC カード）を採用しているサービスはあるが、一般のサーバ構築の場面で簡単に利用できるような状況にはなっていない。当センターの認証局および関連サーバを構築した際に改めてわかったことであるが、電子認証技術、特に PKI（Public-Key Infrastructure）の採用に抵抗を感じる開発業者は多い。

しかし、本当に危惧すべきことは、ID／パスワードで十分、もしくはそれしか運用可能な方式がないと考えて採用してしまうという現状である。実際には、パスワードが複数のユーザに共有されていて、漏洩に気づきにくいことになっていたり、パスワードが何年も変更されず、簡単に破られてしまうようなシステムが存在している。本来であれば、一定期間毎にパスワードを変更したり、推測が難しく全ての可能性を試されるような攻撃にも耐えられるように十分に長い文字列を使う必要があったりする。しかしそれではユーザにかける負担が大きく、実際に行われている事例はほとんど聞いたことがな

い。暗号技術を使った電子認証技術であれば、その必要性は低く、ユーザへの負担は軽いはずである。しかも今日の多くの Web ブラウザには PKI を使った電子認証技術が実装されている。

なぜ、電子認証技術は難しいという印象をぬぐえないのか。本調査研究では、この疑問に答えるためのカギとして、国際会議などで言われているプラクティスと呼ばれる、「実用的なノウハウ」に着目した。プラクティスを蓄積し共有すれば、システム構築を行う者の障壁を下げることができると共に、電子認証の相互運用性を高める効果も期待できる。相互運用性の高い電子認証がインターネットで使われるようになれば、より安全で安心できるネットワークサービスを、一般ユーザに提供しやすくなる。

1.4. 2007 年度の位置づけ

電子認証フレームワークは、各業界に共通して役立つような電子認証に関するフレームワークを意味している。元来、定義のある言葉ではなく、調査研究を通じてあり方を明らかにしてきた。2005 年度の調査の結果から、本調査研究におけるプラクティスの蓄積と共有の為の仕組みを指し、ノウハウを広く共有できるような仕組みをさすこととなった。2005 年度から 2007 年度までの調査研究の実施内容と成果を表 1-1 に示す。

表 1-1　2005 年度から 2007 年度までの実施内容と成果

年度と実施内容	成果
2005年度 ・電子認証フレームワーク ・各国の策定プロセス調査 ・必要性とIETFの状況調査	○電子認証フレームワークにおける策定プロセス に関する調査結果の結果 ・各国のベストプラクティスにあたるドキュメント策定について調査した結果 ・BCPの策定プロセスの要件
2006年度 ・電子認証フレームワーク ・策定プロセス案作成 ・プラクティスドキュメント例作成	○電子認証フレームワークの策定プロセス案とドキュメントの例など ・策定プロセス案の作成とベストプラクティスドキュメント例 ・議論のためのML、Web等
2007年度 ・電子認証フレームワーク ・策定プロセスの試験実施 ・体制の評価	○電子認証フレームワークで策定されたBCP ・策定プロセスに則って策定されたBCP ・レビュー結果

2005 年度は、電子認証フレームワークのための基礎的な調査を行った。各国のプラク

ティスと呼べるドキュメント（特に電子認証における保証レベルという概念にフォーカスした）について調査を行うと共に、ノウハウをドキュメント（文書）として集約するような社会的な仕組みについて調査を行った。ドキュメントを集約する仕組みとして、IETF や RIR（Regional Internet Registry – 世界に 5 つある地域インターネットレジストリ）のポリシーミーティングがある。IETF は技術的なプロトコル策定の会議体であり、RIR のミーティングは IP アドレスに関するポリシー文書を策定するための会議であるが、別の見方をすると、参加者のドキュメント化の提案を受け付け、よりよいドキュメントを策定していく社会的な仕組みであると捉えることができる。調査研究ではこれらのドキュメントの策定プロセスに着目し、またルール設計の部分についても意識しながら現地調査を行った。

2006 年度は、IETF 等の調査でわかってきたコミュニティの仕組みを構築するため準備の年度であった。まず情報公開や議論の基本的な機能となる、Web サーバやメーリングリストサーバを構築・準備した。またベストプラクティスという、他の種類のドキュメントとの境目が曖昧な話題を扱うことに対する各種の考察を行った。例えば、電子認証技術があるベンダーのシステムに限定されるようなノウハウが公開されると、特定のベンダーの製品の利用を促進するようなことになってしまう。すると電子認証技術自体の発展とは活動主旨が異なってしまう恐れがある。また相互運用性の確保も難しくなることが想像される。2006 年度は、これらの検討結果を踏まえたドキュメントの基本的な書式やドキュメント化プロセスの明文化などを行った。

2007 年度は、いよいよ実験的に会議体「電子認証プラクティスフォーラム」を運営する段階である。2006 年度に構築したシステムに加えて、本フォーラムへの参加に際しての、参加者の同意事項を整備するなどした。本フォーラムの一環としてオンライン活動（Web ページを使ったドキュメント管理やメーリングリストを使ったディスカッション）とオフライン活動（会議）を実施した。更に、そこで策定されたドキュメントとフォーラム活動に対するレビューを行った。この実験的なフォーラムの実施を通じたアウトプットが、本調査研究の成果になると考えられる。

1.5. IP アドレス認証展開の背景

本調査研究の二つ目のテーマである「IP アドレス認証の展開」は、2004 年度までの IP アドレス認証に関する調査研究の応用編である。IP アドレス認証とは、IP アドレスなどの登録情報に関する、またはそれを利用した電子認証といった意味であるが、2004 年度の段階では登録者の認証の為の各種の仕組みを構築するに留まっていた。これでも登録情報の保護には十分に役立つ仕組みであるが、ユーザ数の拡大やそれに伴う電子認証事業の確立の意味で、ユーザに利便があるような仕組み作りが必要であった。これは電子署名・電子認証技術一般に言われることであるが、既に行われているような業務手続きに対して、安全性を向上させるだけではユーザへの訴求度は低い。利用することで、

それに見合う恩恵を得られるような仕組みが必要である。例えば当センターであれば、IP アドレスの不正な利用を検知できるようになる、インターネットを顧客に安全に提供できるようになる、といった、利用に見合う恩恵が与えられなければならない。本調査研究は、インターネットセキュリティに資するような仕組みの調査研究を行うこととなった。

1.6. 2007 年度の位置づけ

IP アドレス認証の展開は、2004 年度までに構築した ISP 等の IP アドレスの割り振り先の認証を応用し、インターネットセキュリティに資する仕組みを構築する調査研究である。しかしインターネットの運用に関しては、IETF の RFC（Request for Comments）や、国際的なネットワーク運用者のコミュニティにおいて常識になっている文化や理念が存在し、新たに構築した IP アドレスに関連するシステムや業務が簡単に受け入れられるとは考えにくい。一方で、インターネット経路制御の分野では IP アドレスの登録情報を使った不正利用排除のニーズが高まりつつある。2005 年度から 2007 年度までの調査研究の実施内容と成果を表 1-2 に示す。

表 1-2　2005 年度から 2007 年度までの実施内容と成果

年度と実施内容	成果
2005年度 ・IPアドレス認証の展開 ・ISPへのヒアリング ・RIRの状況調査	○経路情報の登録機構の要件調査の結果 ・ISP等へのヒアリングを通じて、正しい台帳を作るシステムの要件
2006年度 ・IPアドレス認証の展開 ・経路情報の登録機構 設計と実装 ・RIRの登録機構調査	○経路情報の登録機構（プロトタイプシステム） ・本機構の設計と実装
2007年度 ・IPアドレス認証の展開 ・ISPとASにおける試験運用 ・RIRの今後の取り組み調査	○経路情報の登録機構（プロトタイプシステム） ・実験的にサービス ・フィードバック ・国内・海外でのディスカッションの結果

2005 年度は ISP へのヒアリングや、RIR の状況調査などの基本的な調査を行った。RIR では認証局がすでに構築されており、また IP アドレスに関する登録情報を IRR

（Internet Routing Registry）と連携させる等の仕組みを有している。2005 年度の調査の結果、日本国内において経路情報に関する正しい台帳を持つことの重要性と、その要件が明らかになった。

2006 年度は 2005 年度に明らかになった要件を元に「経路情報の登録機構」の設計と開発を行った。また RIR における IP アドレスのルーティングに対する authorize（認可）の仕組みの詳細について調査を行った。活動の結果、経路情報の登録機構のプロトタイプシステムが完成した。

2007 年度は経路情報の登録機構を実験運用し、実際に ISP の担当者に使ってもらえるようにするための活動を行った。対象となるユーザは ISP の IP アドレスに関する申請業務担当者と、AS の登録情報を管理しているメンテナーの登録担当者である。活動の結果、実験サービスを行い、ユーザからのフィードバックを得た。またフィードバックを元に経路情報の登録機構を改修するなどした。

1.7. 本報告書の内容について

本調査研究に関する本報告書でのまとめかたについて述べる。

- **電子認証フレームワークに関する調査研究（第 2 章）**
  調査研究の一環として「電子認証プラクティスフォーラム」と呼ばれる会議体を運営し、電子認証技術に関わるノウハウのドキュメント化活動を行った。この活動と活動のレビュー、および活動成果であるドキュメントについて述べる。

- **電子認証技術の動向に関する調査（第 3 章）**
  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。2007 年度は第 69 回 IETF ミーティングと第 70 回 IETF ミーティングに参加した。PKIX WG の動向を中心にまとめる。

- **IP アドレス認証の展開に関する調査研究（第 4 章）**
  調査研究の一環として経路情報の登録機構の実験運用を行った。実際に ISP の担当者に利用してもらいフィードバックを得ると共に、国内および海外の会議でプレゼンテーションを行い、RIR コミュニティの技術的な見地での意見交換を行うなどした。

- **経路制御のための電子認証技術に関する国際動向（第 5 章）**
  経路情報の登録機構は、インターネット経路制御のために役立つ仕組みである。一方、RIR の中には本機構に似た役割を持つ仕組みが適用されていたり、全く別のアプローチであるリソース証明書と呼ばれる電子証明書のシステムが開発されていたりする。そこで IETF や RIR のミーティングに参加し、具体的な

開発動向等について調査を行った。

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 Appendix として、経路情報の登録機構のユーザインターフェースを解説したものと、JPIRR 認証局の CPS、およびその英語訳を掲載した。

RIR や IETF および IEPG 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が高いと感じる場面がたびたびあった。そこで英語圏の技術者に対しても JPNIC 認証局に関する情報提供ができるよう、経路情報の登録機構と連携する JPIRR 認証局の CPS の英語訳を作成した。

第 1 章　本調査研究の概要と位置づけ