第 11 章　まとめ

内容

- 各章のまとめ

11. まとめ

本章では、本報告書の各章の内容をまとめる。

第 1 章「調査研究の背景と位置づけ」

本調査研究は 2004 年度までに行われた IP アドレス認証局の展開と、電子認証のノウハウとなるガイドライン策定の仕組み「電子認証フレームワーク」に関するものである。

調査研究の一環として、2004 年度までに構築した認証局を運用し、そのノウハウを電子認証フレームワークの中で利用していく。また IP アドレス認証の電子認証フレームワークにおける位置づけを明らかにすることも目指す。

第 2 章「電子認証フレームワークに関する調査研究について」

インターネットの普及と Web アプリケーションを使った身近なサービス提供によって、ID 盗用の問題が大きくなりつつある。

多くの金融機関や商用 Web サイトにおけるユーザ認証はパスワードが使われている。しかしその運用方法は提供者に任され、一定のノウハウが蓄積された状態ではない。PKI（Public-Key Infrastructure）のように電子証明書の仕組みを運用するには、PKI に共通するノウハウや、適用分野ごとに考えられるノウハウを蓄積し、利用していく必要がある。

本調査研究ではノウハウをガイドライン・ドキュメントとして策定し、蓄積している仕組みを「電子認証フレームワーク」と名づけ、その在り方について調査研究を行った。

第 3 章「IETF における電子認証とドキュメント策定プロセスの動向」

IETF（Internet Engineering Task Force）における、電子認証技術に関するプロトコル策定動向やプロトコル策定プロセスに関する動向を報告する。

IETF では、PKI の利用に関する BCP（Best Current Practice）と呼ばれるドキ

ュメントの必要性が指摘されている。これは PKI の技術をより適切に利用するために、技術そのものではなく利用方法に着目したドキュメントである。PKIX WG は PKI の技術自体に関するプロトコルの策定を目標としている為、BCP に関する情報集約や議論のできる場が少ない状況がある。

一方、IETF ではプロトコル策定プロセスを見直す動きがある。ドキュメント化のプロセスを見直し、既存のフローの効率化を図る活動とともに、プロセスの見直しの目的を明らかにし、策定されるドキュメントの質を維持する活動も始まっている。

また経路情報交換の安全性確保のために新たな WG、SIDR（Secure Inter-Domain Routing）が設立された。この WG は、インターネットにおける経路情報交換プロトコルで認証機能を実装している S-BGP や soBGP を中心に、安全な経路制御を図る仕組みの策定を目指すものである。

第 4 章「電子認証の運用に関するドキュメントの現状」

電子認証の運用に関する国内外のドキュメントについて基本調査を行った。特に共通する部分や電子認証の「保証レベル」に関するもので、認証の種別や確からしさに基づくレベル分けを示している。

日本国内においても日本 PKI フォーラムのポリシーWG において、基準となる「保証レベル」や利用方法に関する活動が行われている。

第 5 章「電子認証フレームワークの在り方」

本調査研究の一環として、PKI の専門的な知識を有しており、かつ IETF のドキュメント策定に明るい専門家によるチームを設立した。このチームではガイドライン・ドキュメントを策定する活動に関する要件について議論し、要件事項の集約を図ったものである。その結果、策定によって有用なガイドラインとなるいくつかの内容が明らかになった。その中には前節で述べた「保証レベル」が含まれている。また策定プロセスに関して、策定されたものに準拠しやすいような要件の抽出も行われた。

第 6 章「IP アドレス認証の展開に関する調査研究について」

電子認証フレームワークに関する調査研究と関連して、IP アドレス認証局を利用した認証の展開に関する調査研究を行った。IP アドレス認証局を使って実現できる電子認証は、自然人の認証と異なり、サーバやアドレスの割当先となる。これらの認証を電子認証フレームワークの中で一つの分野として位置づけ、具体的な展開を図る。

本調査研究では JPNIC の登録情報を利用して、インターネットにおける経路情報交換のプロトコルで電子認証を行う仕組みについて取り組む。

第 7 章「アドレス資源管理と経路情報の現状」

経路情報交換の仕組みの基本的な概念の解説を行う。IP アドレスの管理を行うインターネットレジストリを始め、BGP-4 やインターネットで広告されている経路情報の傾向について解説する。

第 8 章「経路制御におけるセキュリティの現状」

経路制御において交換されている情報は、必ずしも IP アドレスの割り振り情報と一貫性が保たれていない。そのため、経路ハイジャックなどの不正行為が可能である状況であり、その影響は大きい。構造上、ISP で提供しているインターネットの接続性を大規模な範囲で失わせるほどの影響が出る可能性がある。

第 9 章「経路情報交換における不正利用排除」

JPNIC の認証局を利用して、S-BGP 等の電子認証を実現するための仕組みを考察した。BGP における認証の考え方を踏まえた仕組みを紹介した。

第 10 章「インターネットの可用性と安全な経路制御の課題」

インターネットを使うネットワークアプリケーションの可用性を確保するためには、安全な経路制御を行うことが重要である。一方、既存の柔軟なネットワーク管理を維持することも必要である。前章で紹介した電子認証を運用することを考える際に必要となる検証事項をまとめた。また課題事項に関して取り組んだ、ヒアリングと実験環境の構築について述べる。

Appendix I「RFC3779 日本語訳」

S-BGP で利用される電子証明書の書式を規定した RFC3779 の日本語訳を掲載する。