第 2 章　各章の概要

内容

- 第 1 章から第 7 章までの概要

第2章 各章の概要

本章では、今年度の調査研究の内容を簡単に把握できるよう、各章のポイントをピックアップする。詳細に関しては適宜各章の該当部分を参照されたい。

第 1 章　IP アドレス認証局に関する調査研究について

今年度の調査研究の位置づけや、活動内容と各章との関連について述べた。

第 2 章　各章の概要

各章の概要を 1 パラグラフ程度にまとめたものである。

第 3 章　認証技術とセキュリティに関する国内外の動向

電子認証の技術的な最新動向を調査するため、IETF の PKIX WG を中心に情報収集を行った。PKIX WG では IP アドレスと AS 番号の情報を X.509 形式の証明書（以下、証明書とよぶ）に含める RFC3779 の標準化がされ、また CRISP（Cross Registry Service Protocol）WG では AREG の RFC 化の最終段階に入った。RPSEC WG では S-BGP（Secure BGP）の議論が行われており、RIR が発行する RFC3779 形式の証明書の利用が想定されている。IETF では認証技術の実践的な議論や技術の標準化の必要性が指摘されており、EasyCert を始めとする新たな WG や BoF が始まっている。

ネットワークオペレータの会議である NANOG では、ルーティング技術を利用したバックボーンのセキュリティ技術に関する議題が多かった。国内では JANOG でもルーティングのセキュリティに関する議論が始まっており、JPNIC の IRR 企画策定専門家チームでは IRR の経路情報を使ったインターネットのセキュリティが活動の柱の一つとして位置づけられている。JNSA（日本ネットワークセキュリティ協会）ではセキュリティの複雑な機能をミドルウェアで吸収しその認証のセキュリティインフラ運用を各種認証局が行っていくというモデルについて議論が行われていた。

第 4 章　RIR の認証局とセキュリティの動向

RIR のうち、APNIC や RIPE NCC、ARIN ではすでに認証局を構築している。これらの認証局はすべて電子証明書使ったユーザ認証の為に利用されている。APNIC CA は HSM（Hardware Security Module）の導入を行ない、また証明書を利用する Web アプリケーションの MyAPNIC の機能拡張が徐々に進んでいる状況である。証明書の発行数は二年間で 1000 を超え順調にユーザを増やしている。RIPE NCC は Webupdates といった Web での認証だけでなく、S/MIME を使った申請にも証明書が使えるようになった。RIPE NCC に発行された証明書は自動的に Database に登録さ

れるようになって利便性が上がり、証明書の発行数は 700 を超えた。RIPE NCC では別途登録された証明書を認証に用いることが可能だがその数は除いている。ARIN は S/MIME を使った申請者の認証にのみ証明書を利用している。

APNIC を中心に RFC3779 形式の証明書を RIR で運用する際の課題抽出や方向性の確認が行われはじめている。この証明書は割り振りと割り当ての証明に使われ、現在 S-BGP で利用することが想定されている。

第 5 章　IP アドレス認証局のマネジメントに関する検討と構築

IP アドレス認証局の実験的な業務を想定した業務フローと認証局システムの設計を行った。業務のモデルは 2003 年度の調査研究の一環として行った専門家チームによる検討結果を活用した。認証業務は、既存のインターネットレジストリにおける登録者の扱いを踏襲し、またアクセスコントロールも既存のルールに近くなるようにした。

第 6 章　認証業務規程 CPS 策定の更新

2003 年度のドラフト版を元に、第 5 章で設定を行った認証局システムの運用に合った記述を行った。認証局システムは安全上の要点を押さえつつ費用を押さえたものになった。一方 CPS の記述については全章にわたって改編が行われ、より実際の運用に即した規程となった。

第 7 章　IP アドレス認証局の応用

NIR における認証局の応用として、具体的なプロトコルと事例についてまとめた。一つ目は経路情報の安全性で、インターネットバックボーンの保護に利用される構想である。二つ目は登録情報の効率的かつ安全なやり取りを実現する Web トランザクションである。登録申請業務の自動化だけではなく IP アドレス認証局が上位認証局となるような状況では、登録情報をオンラインで迅速にやり取りできる必要がある。三点目はオーストリアにおける ENUM（tElephone Number Mapping）の登録における認証の事例である。レジストリの情報登録に使われる証明書と認証のスキームが直接利用される。

Appendix.1

認証業務と方針の検討の結果、更新を行った CPS ドラフト版を添付する。

Appendix.2

前年度の CPS との差異を表にまとめた。