第 3 章　電子認証技術と技術文書策定に関する国際動向

内容

- IETF における技術文書の策定プロセス
- 電子認証技術の動向
- 経路制御の安全性とリソース証明書

3. 電子認証技術と技術文書策定に関する国際動向

3.1. 概要

電子認証技術、および技術文書の策定の国際動向を調査するため、IETF のミーティング、および APNIC、RIPE NCC、ARIN といった RIR（Regional Internet Registry）のミーティングに参加し、また担当者との情報交換を行った。

電子認証技術は ITU-T の X.509 にて策定された PKI（Public-Key Infrastructure）を中心に調査しているが、IETF や RIR におけるその応用的な議論は、X.509 の仕様から大きく離れ、独立した議論となっている。また IETF における技術文書の策定方法は常に見直されており、その見直しのための議論は、電子認証フレームワークの策定に必要な策定プロセスのあり方を示唆するものであった。

本章ではこれらの調査結果について、まず各 IETF ミーティングの様子をまとめ、後半で数年間のスパンで捉えた PKIX WG（Public-Key Infrastructure （X.509）WG）の動向をまとめる。

3.2. 動向調査の目的

動向調査の目的は主に 3 点である。以下では各々について述べる。

○技術文書の策定プロセス

IETF では RFC と呼ばれる技術文書を参加者のコンセンサスに基づいて策定する仕組みが運用されている。この仕組みは最新かつ多様な分野の技術者に受け入れられるアウトプットを得るという意味で、電子認証フレームワークを策定するためのプロセスのあり方に大きく影響するものであると考えられる。2006 年度は特に IETF における策定プロセスについて議論が行われた NewTrk WG の活動について調査した。

○電子認証技術の動向

電子証明書の技術である X.509 は、PKIX WG で議論が進められている仕様が多くの実装で採用されている状況がある。そこで 2006 年度および近年の PKIX WG でどのような技術が策定されているかについての最新動向を調査した。

○リソース証明書の動向

リソース証明書は IP アドレス等のアドレス資源の利用／管理権限を示す電子証明書で、主に APNIC で開発と仕様策定が行われている。APNIC は各 RIR のミーティングでデモンストレーションを行うとともに、技術的な仕様について IETF における RFC

の策定を通じて標準化を図っている。そこでリソース証明書を扱っている SIDR（Secure Inter-Domain Routing） WG に参加し、技術的な動向について調査した。

3.3. IETF における国際動向の調査

3.3.1. IETF の開催状況と注目した WG の開催状況

2006 年度、IETF におけるミーティングは第 66 回、第 67 回、第 68 回と 3 回開催された。このうち本調査研究のために第 66 回と第 67 回に参加した。

IETF はインターネットにおける通信プロトコルの標準化において注目されている団体であるが、一方でその独自の策定方式を維持するための議論や特定の国やベンダーに傾倒しないような中立性を保ち最先端の知見を IETF の活動に盛り込むための議論が行われている点でも注目に値する。

電子認証フレームワークは、IETF においてカバーされていない一方で、中立的かつ最先端の知見をドキュメント化して共有することに意義がある。従って本調査研究では、IETF における議論とドキュメント策定プロセスに注目し調査を行った。

特に注目したのは IETF における新たな策定プロセスについて議論している NewTrk WG、電子認証技術である PKI の策定を行っている PKIX WG、また電子証明書を使って IP アドレス等のアドレス資源の管理を行う技術であるリソース証明書などである。

本節ではこれらの調査の結果についてまとめる。

3.3.2. 第 66 回 IETF

2006 年 7 月 9 日(日)から 7 月 14 日(金)まで、カナダのモントリオールにて、第 66 回 IETF ミーティングが開催された。今回の IETF はカナダ・モントリオールの Palais des Congres de Montreal (モントリオール・パレ会議場)で開かれた。会場は市の中心部から徒歩 10 分程のところで、同じ規模の国際会議を同時に二つ以上は開けそうな巨大な会場である。

今回の参加登録者数は 1,257 名で、参加国は 44 ヶ国であった。米国・ダラスで行われた前回の IETF の時に、いくつかの国からの参加者が米国への入国ができず、IETF の働きかけによって急遽ビザが発行されるという出来事があったようであるが、今回はそのような事態への配慮がなされて、カナダで開催された模様である。

IETF では、WG の会議と Plenary と呼ばれる全体会議が行われる。WG の会議では

主に RFC（Request for Comments）になる前のドキュメント(Internet- Draft)に関する議論が行われる。議論は基本的に ML で進められるが、IETF 期間中にオフラインで打ち合わせることでコンセンサスを確立したり、その場で実装をしてつきあわせたりして、RFC 化が目指される。一方、Plenary は会期中 2 回だけ行われる。

“IETF Operations and Administration Plenary”は IETF の運営面の全体会議で 7 月 12 日(水)に開かれた。技術面の全体会議である Technical Plenary は 7 月 13 日(木)に開かれた。

○IETF Operations and Administration Plenary

IETF Operations and Administration Plenaryは、IETFの活動全体の運営に関する報告と議論を扱う全体会議である。今回はミーティングのホストを務めるEricsson社のプレゼンテーションとNOC(Network Operation Center)の報告、IAOC(IETF Administratire Oversight Committee)[1]やIASA(IETF Administrative Supporting Activity)、TOOLSチーム[2]といったIETFを支える活動の報告と、IETFにおける標準化プロセスの再検討に関する議論などが行われた。

はじめに IETF チェアの Brian Carpenter 氏からチェア報告があった。前回の IETF 以降、4 つの WG が新設され 13WG が終了、RFC が 138 出されたそうである。IASA 報告の中では、RFC Editor の活動報告や前回の IETF の会計報告などが行われた。RFC Editor は RFC の校正を行い、体裁を整えるチームで、2 年程前より体制を建て直し徐々に作業効率の向上を図っている。2006 年度は 2005 年度よりも RFC 編集作業のペースが 58%近く向上しているとのことである。

IETFにおける標準化プロセスの再検討は、2004 年以降、IETFチェアのBrian氏自身によって進められてきた。これに関する Internet-Draft は、draft-carpenter-newtrk-questions-00.txtである。これまでNewTrk WG[3]の会議が何回か開かれてきたが、方向性が決められず今回のPlenaryで全体の意見を聞くことになったようである。しかし会場からは再検討の議論自体に意義を見いだせないといった意見が挙げられていた。

○Technical Plenary

[1] IAOCは 2004 年初頭から行われている、IETFの運営管理体制の再編の活動の一環として作られた委員である。IETFの予算や活動計画、契約といったIAD(IETF Administrative Director)の提案に対してレビューを行い、活動の方向性を示す役割を担っている。
[2] TOOLS Team Charter
http://tools.ietf.org/charter-page
[3] New IETF Standards Track Discusion (newtrk)
http://www.ietf.org/html.charters/OLD/newtrk-charter.html

Technical PlenaryはIETFの活動の中の技術的な議論を扱う全体会議である。IRTF(Internet Research Task Force)の活動報告、IRTFのSAM RG(Scalable Adaptive Multicast Research Group) [4]の紹介、IABのチェア報告などが行われた。

IRTFは長期的な観点で技術を捉え、リサーチと議論・検討を行うグループである。必要性が認められるとIETFでの標準化作業を行う。SAM RGは前回のIETFの後に結成された。SAM RGは、複数のマルチキャスト・プロトコルの利点をそれぞれ生かし、展開・普及を図ることを目的としている。IPマルチキャストだけでなくアプリケーション層に分類されるようなものや、中間的な分類(Hybrid)に入るプロトコルも議論の対象に入っている。IPマルチキャストとして分類されるものはXCAST[5]のみである。

IABのチェア報告では、IAB主催のBoFやワークショップの紹介とRFC Editor[6]のあり方の検討に関する発表があった。これまで 2005 年 10 月のNANOG[7]や 2006 年 3 月のAPRICOT[8]で開いてきたIPv6 Multicast BoFが、2006 年 4 月に行われたRIPE Meeting[9]でも行われたようである。またRouting and Addressingワークショップ（IABではRAWSと呼ばれている）の告知があった。このワークショップのようなIABが主催するオープンなミーティングについての情報は、下記のWebページにまとめられている。

□ IAB-Sponsored Open Meetings (IAB 主催のオープンミーティング)
http://www.iab.org/documents/open-mtgs/

IAB では今後 30 年という長期的な視点で、RFC Editor のあり方について検討してい

[4] SAM Research Group
http://www.samrg.org/
[5] XCAST
http://www.xcast.jp/
[6] RFC-Editor Webpage
http://www.rfc-editor.org/
[7] NANOGはThe North American Network Operators' Groupの略で、主に北アメリカ地域のインターネット関連のネットワーク運用管理担当者（ネットワークオペレータ）を対象にしたグループ。MLや 1 年に 3 回開催されるミーティングを通じて、主に技術的な議論や知見の共有、相互の普及・啓発活動が行われている。
http://www.nanog.org/
[8] Asia Pacific Regional Internet Conference on Operational Technologiesの略で、アジア太平洋地域のインターネットインフラストラクチャーを発展させるため、技術者に必要な知識や技術を向上させることを目的として開催される非営利のフォーラムである。1996 年の設立以来、毎年 1 回アジア太平洋地域のさまざまな都市で開催され技術者の人材養成、実用的な技術と知識の習得を目指したプログラムが行われている。
http://www.apricot.net/
[9] ヨーロッパ地域のRIRであるRIPEが主催して行われるミーティングである。APNICやARINと同様に、IPアドレスに関するポリシーやインターネットの運用に関する議論が行われる。

る。(ちなみに最初の RFC である RFC1 が出たのは 1969 年 4 月 7 日で、今年で 37 年経ったことになる)特に RFC Editor のプロセスの中で IAB や IAOC（IETF Administrative Oversight Committee）、そして IETF がどのように関わっているべきかといったことを議論しており、そのために RFC の目的やミッション、RFC 化の役割分担についての整理を試みている。また IAB では IAOC と共に RFC Editor の RFP(Request for Proposal - 提案依頼書)の作成を進めているようである。会場からは RFC Editor に関する議論に対して時間をかけ過ぎているといった意見が出ていたが、ドキュメント(Internet-Draft)の著者の主旨を正確に組み入れ、かつ RFC 化の作業がコミュニティの必要に応えるようなスピードで行われるための効率化を図るため、慎重な検討が進められている様子がうかがわれた。

この他に、IDN(Internationalized Domain Names)と IDNA(Internationalizing Domain Names in Applications)を組み合わせて使うことの問題点、例えば類似する文字で spoofing(だます行為)が行われてしまうこと等について、DNS のアーキテクチャの中で取り組む考え方などについて紹介されていた。

○セキュリティエリアにおける電子認証関連 WG

第 66 回 IETF では、セキュリティエリアのセッションが 18 行われた。BoF は Network Endpoint Assesment BoF と Handover and Application Keying and Pre-authentication BoF の 2 つである。また PKIX WG と前回 WG になった SIDR WG とのジョイントセッションが行われた。

本節では、PKIX WG と SIDR WG、及びインターネットの経路制御における電子証明書の動向について報告する。また末尾で BoF について紹介する。

○SIDR WG (Secure Inter-Domain Routing WG)

第 64 回および第 65 回の IETF で BoF が開かれていた SIDR が、2006 年 4 月 18 日に WG になった。今回の IETF で行われるミーティングが WG として行われる初めてのミーティングである。

SIDR は Secure Inter-Domain Routing の略で、ネットワーク・ドメイン間の経路制御におけるセキュリティメカニズムを開発することを目標としている。RPSEC WG で議論されてきたセキュリティの要件に則り、利用や展開(deployment)を含めて検討を行う。

今回の WG セッションでは、IP アドレスや AS 番号が入った"リソース証明書"の実験を行っている APNIC の Geoff Huston、George Michaelson 両氏による、2 つのドキュメントプレゼンテーションが行われた。また経路制御プロトコルをより安全に利用するためのトランスポート層(TCP)のセキュリティに関するドキュメントプレゼンテーショ

ンが行われた。リソース証明書に関するプレゼンテーションは以下の 2 つである。

□ "A Profile for X.509 PKIX Resource Certificates"
draft-huston-sidr-res-certs-01.txt
IP アドレスと AS 番号の利用権を検証するための電子証明書のプロファイルを定めたもの。この証明書はリソース証明書と呼ばれる。

□ "A Profile for Resource Certificate Repository Structure"
draft-huston-sidr-repos-struct-00.txt
リソース証明書を保持するリポジトリの構造を定めたもの。Subject Key Identifier(SKI)や Authority Key Identifier(AKI)を使って電子証明書を検索できるようにするため、Subject にそれらのハッシュ値を含めた名前を使う。

APNIC ではこれらの仕様を前提として実装を進めているようである。主な論点はリソース証明書の Subject とトラストポイント(信頼点、またはトラストアンカーと呼ばれる)の 2 つである。SKI のハッシュ値を Subject に含めるのは、リソース証明書の証明書パスにおける一意性を維持することを意図している。本来、Subject は電子証明書の発行対象の識別子を入れるために使われるが、証明書を識別しやすくするために特殊な使われ方がされているようである。

またリソース証明書に想定されるツリー構造の頂点をどうするか、トラストポイントをどう想定するか、といった点については議論が収束していない様子である。IP アドレスと AS 番号の管理を行っているインターネットレジストリの構造からすると、直感的には IANA が頂点となる認証局を運用し、RIR の認証局がその下位認証局となって、IANA の認証局を多くの利用者がトラストポイントと位置づけることが考えられる。しかし RIR の中にはその認証局の運用可能性に疑問を持っているところが多いようである。これは IANA に比べて RIR（もしくは RIR の連合体である NRO）が、IP アドレス及び AS 番号の割り振り／割り当て業務の大半を実施している現状を鑑みたものと思われる。

標準技術的な観点では、絶対的な頂点の存在を規程することよりも Relying Party(証明書検証者)が、トラストポイントを使って必要十分なリソース証明書の検証ができるか、という点が重要である。そのため、頂点の認証局については、今のところは先に延ばせる議論である。

トランスポート層のセキュリティについては以下のドキュメントに関するプレゼンテーションが行われた。

□ "Key Change Strategies for TCP-MD5"
draft-bellovin-keyroll2385-00.txt
BGP のような長期的な TCP セッションにおける、MD5 オプションのための鍵変更の方式である。既存の方式と互換性がありながら、片方のエンドだけで実施できるようになっている。

□ "Authentication for TCP-based Routing and Management Protocols"
draft-bonica-tcp-auth-04.txt
MD5 に代わる、より強度の高い暗号アルゴリズムを使った TCP オプションの取り決めである。

□ "Automated key selection extension for the TCP Authentication Option"
draft-weis-tcp-auth-auto-ks-01.txt
TCP の Extended Authentication オプションのためのセッションキーの交換方式と、そのためのノンス(暗号文を変化させるためのランダム値)を使ったメッセージ認証の方式の取り決めである。

□ "The TCP Simple Authentication Option"
draft-touch-tcpm-tcp-simple-auth-01.txt
MD5 オプションに代わる認証のための TCP オプションである。IPsec のように別途の SA (Security Association)を確立する方式を提案している。

TCP における認証方式の改善は、強度と運用の容易さ、既存の TCP との互換性といった様々な要素が関係している。ネットワーク・セキュリティの大家である Steven Bellovin 氏を中心に慎重に検討が進められている。

○PKIX (Public-Key Infrastructure (X.509)) WG

PKIX WG は 7 月 10 日(月)の 17 時 40 分～21 時に行われた。18 時 50 分からは SIDR WG とのジョイントミーティングであった。約 50 名の参加があった。

第 65 回 IETF(2006 年 3 月)以降、AC Policies Extension(RFC4476)と GOST Cryptographic Algorithms(RFC4491)の 2 つが RFC になった。RFC3280 の部分的な変更である DirectoryString の UTF-8 の処理に関するドキュメントは、RFC3280 の改定作業とは独立して、RFC Editor's queue に入っており、RFC になる直前の段階にある。

SIM(Subject Identification Method)、SCVP(Server-based Certificate Validation Protocol)、Lightweight OCSP の 3 つが WG Last Call を終え、Area Director のレビュ

ー中である(8 月 17 日現在、SIM は IESG レビューを終え、RFC Editor's queue に入っている。)。SCVP の S は以前 Simple であったが、Server-based に変わった。

SIM は元々韓国の Jong-Wook 氏から出されたドキュメントであったが、Tim Polk 氏が引き継ぎ、現在 IESG からのコメントに対応中である。SCVP は 27 版になり、いよいよ IESG によるレビューの段階に入った。前回の IETF 以降、編集上の変更や定義づけに関する追記といった比較的軽微な変更がなされた模様である。

Lightweight OCSP は、オンラインで証明書検証処理を依頼するためのプロトコルの OCSP を改良したものである。大量のやりとりに適するよう、メッセージサイズを小さくしたり、返答結果のキャッシングを行うことができたりするようになっている。

X.509v3 形式の電子証明書の基本的なプロファイルを記述した RFC3280 の後継となるドキュメント、通称 3280bis については nameConstraints フィールドのエンコーディングに関する追記が行われている。また CRL Distribution Points や AIA(Authority Information Access)/SIA(Subject Information Access)といったフィールドで、https を使用することに関する注意事項の追記が行われた。電子証明書の検証のために https が使われると、その処理のために更に電子証明書の検証が必要になり、場合によっては本来の検証処理が終わらなかったり、状態が複雑になりすぎたりする。これを避けるための注意喚起のための追記が行われたようである。他にも議論が収束していない点が残っている。しかし部分的にドキュメントを分割して、3280bis の対象外とするなどして整理を進められる模様である。

○Joint PKIX/SIDR Meeting

PKIX WG の 2 セッション目に、PKIX WG と SIDR WG のジョイントミーティングが行われた。内容は Secure BGP(S-BGP)の提案者である Stephen Kent 氏による"A PKI for Internet Address Space"というプレゼンテーションである。PKIX WG の参加者に加えて、SIDR WG のチェアである Sandra Murphy 氏らが加わった形で意見交換が行われた。

Stephen Kent 氏は、IP アドレスと AS 番号の使用権を示す電子証明書を使ってインターネットのルーティングプロトコルである BGP(Border Gateway Protocol) の安全性の向上を図る仕組み"S-BGP"の提案をしている。これは、RFC3779 に記述されている電子証明書の拡張フィールドを使って IP アドレスの割り振りと AS 番号の割り当てを証明し、経路情報として広告された prefix が、所有者(利用者)によって正しく使われていることを検証できるようにする仕組みである。インターネットにおける経路情報の中で、誤った IP アドレスと AS 番号が使われると、経路ハイジャックと呼ばれる大規模な利用不能攻撃が可能になる。S-BGP がうまく利用されると、このような攻撃を未然に防ぐことができると考えられている。

このセッションでは、RIRが運営する認証局を使ってこの電子証明書の発行を行うモ

デルが紹介された。電子証明書の入手にはrsync[10]が使われることとなっている。

ここでもトラストポイントに関する議論も行われた。APNIC や RIPE NCC からの参加者の間では、RIR が運用する認証局がトラストポイントとなることを想定して議論が行われている。しかし本来、トラストポイントとはプロトコルの提案者が決めるものではなく、電子証明書の検証を行う者、正確には証明書の検証結果に依存した処理を行う方針を持つもの(Relying Party)が決めるものである。そこで筆者は Address Space PKI の構造に含まれるとされる JPNIC でも、トラストポイントとして利用されることを想定した認証局を運用していることから、RIR の認証局だけがトラストポイントになるわけではないことを会場で確認した。これは、例えば日本国内の ISP の間で経路情報の交換を行う場合に、APNIC や RIPE NCC の認証局を利用する必要はないと考えられるためである。

会場では、この他に割り振りを受けたアドレスブロックを使ったまま地域を移動し、割り振り元を別の RIR に変更するケースの扱い方などについて議論が行われた。

IETF の会場で APNIC の方々と情報交換することでわかってきたことであるが、APNIC では、Address Space PKI に関する開発プロジェクトが 2006 年末の終了を目標として進んでいることがわかった。既に IP アドレスと AS 番号が入った電子証明書の発行やリポジトリの設置が実験的に行われていた。今後、MyAPNIC という申請業務用の Web システムに組み込まれることが考えられており、実用化に向けた活動が今後も引き続いて行われていくことが考えられる。

第 66 回 IETF で新たに行われた BoF を以下に示す。

□ Network Endpoint Assessment (NEA) (Porposed NEA WG Charter)
http://www3.ietf.org/proceedings/06jul/agenda/nea.txt
NEA は、ネットワークに接続するエンドポイント(ホスト等)の OS やパッチの適用状況に関する情報(posture)を交換し、エンドポイントの安全性が確認された場合にのみ会社のネットワークへの接続を許可するといった仕組み構築の為に利用できる。

□ Handover and Application Keying and Pre-authentication (HOAKEY)
モバイルネットワークにおけるハンドオーバーの為の、認証情報を交換する仕組みに関する BoF である。第 65 回 IETF に続いて 2 回目である。

[10] rsync （遠隔のファイルやディレクトリを同期するソフトウェア）
http://rsync.samba.org/

○第 67 回 IETF

第 67 回 IETF は 2006 年 11 月 5 日～10 日、アメリカ・サンディエゴにある Sheraton San Diego Hotel & Marina で開かれた。会場の Sheraton Hotel はダウンタウンから車で 15 分ほど離れた所にある。サンディエゴ空港とヨットハーバーに隣接していて眺めは良いが、ショッピングセンターや飲食店はほとんど無く、また鉄道の駅が近くにない。そのためか IETF 開催中の夕方頃から夜にかけて、会場の裏手とダウンタウンの中心地にある Gaslamp 地区との間で参加者のためにチャーターされたバスが臨時運行されていた。

オンラインのサービスには、前回と同様にミーティング参加者向けのメーリングリストが提供されていた。更に今回は参加者が情報交換を行うためのブログと Wiki が設置されていた。メーリングリストでは Sheraton Hotel のゲストルームにあるインターネット接続機器の不具合や、会場の無線 LAN に関する情報交換が行われていた。

今回の IETF の参加登録者は 1,199 名で、41 ヶ国からの参加があった。日本からの参加者は全体の 10%強で、55%近くを占めるアメリカに次いで 2 番目の参加者数である。全体の人数はここ 3 回程では大きな変化はないようである。

初日の 11 月 5 日(日)に各種チュートリアルとレセプションが、11 月 6 日(月)～11 月 10 日(金)に WG と BoF が、8 日(水)と 9 日(木)の夜に Plenary(全体会議)が行われた。

○IETF Operations and Administration Plenary

IETF Operations and Administration Plenary は、IETF の運営全般に関する報告と議論が行われる全体会議である。この Plenary では、NOC(Network Operation Center)リポートやホストプレゼンテーション、IETF チェアの報告などが行われた。

NOC リポートでは IETF 会場のネットワークの利用状況などについて報告された。会場では毎回無線 LAN を使ったインターネットへの接続サービスが提供されており、最近では無線チャンネルの有効利用と効率化のために、802.11a の利用が推奨されている。IETF 期間中に 802.11a を利用していた端末は全体の 25%程で、前回に比べて徐々にその数が増えつつあるようである。

IETF チェアの Brian Charpenter 氏からは、IASA（ETF Administrative Support Activity）と IAD（IETF Administrative Director）の活動報告が行われた。前回の第 66 回 IETF 以降二つの WG が設立され、12 の WG がクローズ、現在 120 程の WG が活動しているとのことである。RFC は 99 出され、新規の Internet-Draft は 440 程作成されたとのことである。ちなみに去年の同じ期間には 100 程度の RFC が出され、新しい Internet-Draft は 435 作成されていたので、昨年と比べると若干少なかった模様である。

また今回はJon Postel賞[11]の受賞者の発表があった。Jon Postel賞はRFCの編纂やIANAとしてIPアドレスの管理などに貢献したJonathan B. Postel氏にちなんで1999年に設けられたもので、技術的な貢献やリーダーシップの発揮といったコミュニティに対する継続的な貢献のあった人物に対して贈られる。受賞者は毎年選ばれ、クリスタルグローブと賞金2万ドルが贈られる。

今年の受賞者は、南カリフォルニア大学のISI(Information Sciences Institute)におけるRFC Editorのco-leaderであったJoyce K. Reynolds氏と、Bob Braden氏であった。Joh Postel氏より引き継いでRFCの編纂にあたり、RFCの品質向上や現在に至るRFCの認知度向上に対する貢献が称えられた。

会場での参加者の発言に基づいて議論を行うオープンマイクの時間には、主にIETFで提供されているツールに関して議論が行われていた。IETFによるツールの提供は、IETFの予算の中で行われているにも関わらず、開発の際に参加者が意見を出す機会が設けられていない、という指摘から議論が始まった。これについて、オープンソースにすることでノウハウがたまりやすくなる(と同時に多くの人の考えを反映できる)、ツールの位置付けを知っているところでないと開発が難しいことから、事務局の契約が特定の会社に結びつきやすいのではないか、といった意見が挙げられていた。その他に、IETFの音声中継は参加者でなくても聞くことができるが著作権の提示がないといった指摘が挙げられていた。この件についてはIPR(Intellectual Property Rights) WG[12]で議論されていく模様である。

○Technical Plenary

Technical Plenaryは、IETF全体に関係した技術に関する議論を行う全体会議である。IABのチェアレポート、IRTFの活動報告、テクニカルプレゼンテーションなどが行われた。

IABのチェアレポートはIABチェアのLeslie Daigle氏によって行われた。IABではインターネットのアーキテクチャの観点で、WGとは独立したドキュメント作成を行っており、中にはRFCになっているものがある。最近作成されたドキュメントは以下の三つである。

□ draft-iab-iwout-report-00.txt
"Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"

[11] Postel Awards
http://www.isoc.org/awards/
[12] Intellectual Property Rights (ipr)
http://www.ietf.org/html.charters/ipr-charter.html

□ draft-iab-multilink-subnet-issues-00.txt
"Multilink Subnet Issues"

□ draft-iab-net-transparent-00.txt
"Reflections on Internet Transparency"

はじめの Internet-Draft は、2006 年 3 月に行われた"IAB Unwanted Traffic Workshop"の報告である。Technical Plenary の後半でサマリー報告も行われた。質疑応答の際の Leslie Daigle 氏の補足によると、このワークショップは主に(コミュニティの)意識向上を図ることが目的であったようである。

インターネットの利用者に対する脅威は Code Red や Blaster ワームが流行した 2001 年～2003 年頃に比べて深刻になりつつある。ワークショップでは"アンダーグランドエコノミーの発展"を主な要因と位置づけ、現状の問題を明文化して今後の活動の方向性を探るための議論が行われた模様である。

ある Web サイトではクレジットカード情報や銀行口座に加えて、ISP で稼動しているルータのアカウントやボットネットが売り買いされている。このような経済活動の結果、スパムメールや DDoS 攻撃といった Unwanted Traffic を生み出す基盤が維持され、またマルウェア(不正な挙動をするソフトウェア)の発達を促すような競争が行われている、と言われている。一方でさまざまなデータが全て HTTP の中でやりとりされていたり不正行為を隠すための IP アドレスの詐称や、インターネットの経路広告の交換をハイジャックできたりしてしまうことなど、Unwanted Traffic を止められない現状が指摘されている。

これに対して、中長期的な対策と短期的にできる活動が挙げられた。中長期的には、まずルーティングのセキュリティ向上を図る点が挙げられた。そのため、IRR(Internet Routing Registry)の登録情報をクリーンアップして、経路情報の検証ができるようにすることが必要だと指摘された。次にボットネットを止めること、そして TCP の MD5 オプションやパットフィルタリングの BCP(Best Current Practice)といった既存の技術の普及を図ること、といった提案がなされた。

短期的にできることとしては、既にRFCになっているhost requirement、route requirement、ingress filteringに関するドキュメントを更新することや、IABによる啓発活動、IRTFにおける効果的な対策に関する調査などが挙げられた。Security Area DirectorのSam Hartman氏によると、このワークショップのリポート[13]は興味深く、一読することが薦められていた。

Technical Plenaryの後半では、IABのInternet-Draftである"Reflections on Internet

[13] "Report from the IAB workshop on Unwanted Traffic March 9-10, 2006"
http://www.ietf.org/internet-drafts/draft-iab-iwout-report-00.txt

Transparency"[14]とIAB Routing and Addressing Workshopの報告が行われた。

このドキュメントはインターネットの原則的な考え方である「透過性」に関するもので、これまでの IAB の見解を見直し、新たな透過性の考え方に関する議論を紹介したものである。プレゼンテーションでは TCP/IP の階層モデルの中で、様々なプロトコルが透過性に影響する要素を持っているという点が紹介されていた。

IAB Routing and Addressing Workshop[15]は、2006 年 10 月 18 日にオランダのアムステルダムで開かれたもので、近年の経路情報の増大にどのように対処すべきかについて、主にバックボーンオペレーターを対象として行われたものである。現在、Tier-1 レベルのISPでは交換されている経路情報が 20 万経路に達しているという報告がある。もし現在のままIPv6 とのdual stack(IPv4 とIPv6 を同時に使える構成)にすると 50 万経路に達するという予測が立っており、インターネットのアーキテクチャとしては規模拡張性に欠けるのではないか、と指摘されている。会場では現在最も普及しているBGPにこだわらず、この問題を解決するための議論を行うBoFを今後開くことの提案があった。試しに会場で挙手をしてもらったところ、多くの人が賛成に手を挙げていた。その他にIPv6 は今後様子を見ながら検証すべき、(ルーティングにおける)セキュリティに関する議論も必要である、といった意見が挙げられていた。

このワークショップは第 53 回 RIPE ミーティングの後、同じアムステルダムで行われていた。今後も、ISP のコミュニティと IETF のコミュニティの情報交換が進んでいくと考えられる。

3.4. 電子認証フレームワークに関連する動向

本節では、2006 年度に限らずに IETF の活動の中で電子認証フレームワークに関連すると考えられる話題について述べる。

○NewTrk WG における策定プロセスの議論

NewTrk は” New IETF Standards Track”の略で、IETF における標準化プロセスを見直すことを目的とした WG である。電子認証フレームワークを策定する活動は、IETF と同様かまたは「ノウハウの文書化と蓄積」に適する策定プロセスを持つことが考えられるため、IETF における NewTrk の議論の内容は参考になると考えられる。

[14] Reflections on Internet Transparency
http://www.ietf.org/internet-drafts/draft-iab-net-transparent-01.txt
[15] The IAB Workshop on Routing and Addressing
http://www.iab.org/about/workshops/routingandaddressing/index.html

この WG は 2003 年 11 月中旬に行われた第 58 回 IETF で最初の BoF が開かれ、その後 2005 年 7 月末の第 63 回 IETF までに 4 回の WG ミーティングが開かれた。

NewTrk BoF では、既存の標準化プロセスを変更する必要性が確認された。当時上がっていた論点を以下に示す。

- 既存のように一つの段階ではなく複数の段階を設けること
- WG 内での状態も文書として認めること
- 明確さの裏づけとなる複数の実装が確認できる段階の新設
- 著作権に関する確認の段階を設けること

また、以下の団体における標準化プロセスと比較が行われた。

- W3C
- ISO
- GGF
- Open Group
- ITU-T
- 3GPP

後に ISD（Internet Standards Documentation）と呼ばれる新しい策定プロセスが提案された。しかしドキュメントのグループ化に関する詳細ルールについて WG 内で意見が分かれた記録が残っている。

本 WG は、電子認証フレームワークの為のドキュメントの策定プロセスを検討する際、以下の点で参考になることがわかる。

○ドキュメント策定の段階の設計

IETF の策定プロセスでは、WG Last Call、IETF Last Call のようにコミュニティの大きさに応じた確認が行われている。段階を設けることで、一つの話題ないしドキュメントについて各段階でチェックすべき事項が明らかにできる。先の段階に進んだときに、当該の内容を見直す必要が出た場合には、適宜戻ってくることができる。

○ドキュメントのグルーピング

IETF の策定プロセスでは、ドキュメントのグルーピングは行われておらず、RFC の中で関連するドキュメント（RFC）の番号が参考文献として引用されているにとどまっている。閲覧する側の立場では、関連した内容のドキュメントがグループ化されている方がドキュメントを参照しやすいと考えられる。しかしすべてのドキュメントがグルー

プ化される必要はなく、その判断が著者に委ねられた場合にグループ化自体の品質が変化する可能性がある。

結果として、NewTrk WG は現行の策定プロセスをすぐに変更するまでの提案には至っていないが、既存の策定プロセスがもつ問題点とあるべき姿が明らかになった点は大きな成果であるといえる。電子認証フレームワークを作るための策定プロセスでは、特に著作権の扱いと各ドキュメントに対する確認方法について検討する必要があると考えられる。

3.5. PKIX WG における電子認証技術の動向

PKIX WG は” Public-Key Infrastructure (X.509)” WG の略で、ITU-T の X.509 として策定された公開鍵基盤を、インターネットの観点で標準化することを目的とした WG である。

本節では、PKIX WG の動向をわかりやすくするため、4～5 年と 1 年程度の二つのスパンでまとめる。

○PKIX WG の近年（4～5 年）の動向

4～5 年のスパンで見ると、PKIX WG では図にまとめたような話題が議論されている（本節で示す以下の図は、説明の為に作成したものである）

図 3-1　PKIX WG の動向

4,5 年程の中期的な動向としては、”Certificate and CRL Profile”、応用的な証明書に関する RFC、オンラインの証明書検証プロトコルの 3 点がポイントとして挙げられる。

“Certificate and CRL Profile”は、電子証明書の形式と CRL（Certificate Revocation List – 証明書失効リスト）の形式を定めたものである。応用的な証明書は、電子証明書を使ってアプリケーションで電子認証を行うための標準化である。

オンラインの証明書検証プロトコルは、電子証明書の検証処理がある程度の計算機資源やネットワーク資源を使うことから、軽量な処理を行うための機器（例えば PDA や

携帯電話など）で、電子証明書の処理ができるようにするためのプロトコルである。

１年程の短期的な動向としては、”Hash Algorithm Agility”、”リソース証明書”の２点が挙げられる。以降では、各々の動向の内容について述べる。

“Certificate and CRL Profile”は、数年来に渡って改訂が進められてきた（図 3-2）。改定に伴い、詳細な標準化が必要であると考えられる機能や処理内容については別の RFC としてまとめ直されるなどしている。図 3-2 ではこれらを「派生」と呼んでいる。

図 3-2　Certificate and CRL Profile の動向

RFC2459 は日本国内における PKI の普及の始まりの頃に出された RFC で、2006 年現在では RFC3280 に置き換わっている。RFC3280 を置き換える次のバージョンはいくつかの詳細化と追記が行われ、WG Last Call の段階にある。記述の詳細化が行われたのは、電子証明書に入れられる名前形式のセマンティクス（形式）、証明書拡張（extension）の要件に関する記述、CRL バージョン 2 の書式、電子証明書の発行関係を確認するパス検証などについてである。また RFC3280 の作成に伴い、いくつかのドキュメントが派生した。rfc3647：Certificate Policy（電子証明書の発行状況や管理に対する想定を記載したもの）、rfc4158：Path Building（電子証明書の検証のために、発行した認証局を辿っていくルールなど）、rfc4325：CRL AiA（CRL を発行した認証局の証明書を得るための情報）である。RFC4325 は今後 RFC3280 の後継バージョンに統合される予定となっている。

通信相手の認証を行う為のプロトコルとして使ったり、電子証明書の書式を使ってアプリケーション機能を実現したりするような、応用的な証明書の RFC の作成が進められている（図 3-3）。

図 3-3　応用的な証明書に関する RFC のリスト

「PPP and WLAN（rfc4334）」はパソコンを ISP や企業に接続する際などに使われている Point-to-Point Protocol や WLAN（Wireless LAN – 無線 LAN）における電子認証のために電子証明書を使うための電子証明書の扱い方を策定したものである。

「Proxy Certificate（rfc3820）」は、様々な理由で本人性確認のための証明書よりも代理で権限を行使できるようなアクセスを実現するための証明書の書式を策定したものである。

「IP address and AS Identifiers（rfc3779）」は電子証明書の中に IP アドレスや AS 番号を入れ、それらのアドレス資源の利用権限や管理権限を示す電子証明書の書式を策定したものである。APNIC において実験が進められているリソース証明書で使われている書式である。

「Logotypes（rfc3709）」は電子証明書の中に画像のデータを入れ、ユーザが電子証明書を識別しやすくするための書式を策定したものである。

これらの電子証明書を応用するための書式の出現によって、電子証明書を利用する場面が増えると共に、電子証明書が持つ意味も多様化しつつある。特に「IP address and AS Identifiers（rfc3779）」は個々の電子証明書をユーザの識別ではなく、アドレス資源の

利用権限の確認に使われるため、電子証明書に含まれる値の扱い方が、人による識別よりもプログラムによる識別に重点を置いたものになっている。

電子証明書の利用場面が増えると、電子証明書を処理するプログラムが必ずしも計算機資源を豊富に持つ環境で実行されない場合を想定する必要がでてくる。例えば PDA や携帯電話のように、通信帯域が限られていたり計算能力のために電力を多く消費しない方がよい計算機環境がある。電子証明書の内容に応じて処理結果を変化させるようなプログラムで処理されることは重要であるが、計算処理や通信帯域を要する電子証明書の処理を他のコンピューターに任せ、その結果のみを利用するという考え方もある。この処理を実現するのが「オンラインの証明書検証プロトコル」である（図 3-4）。

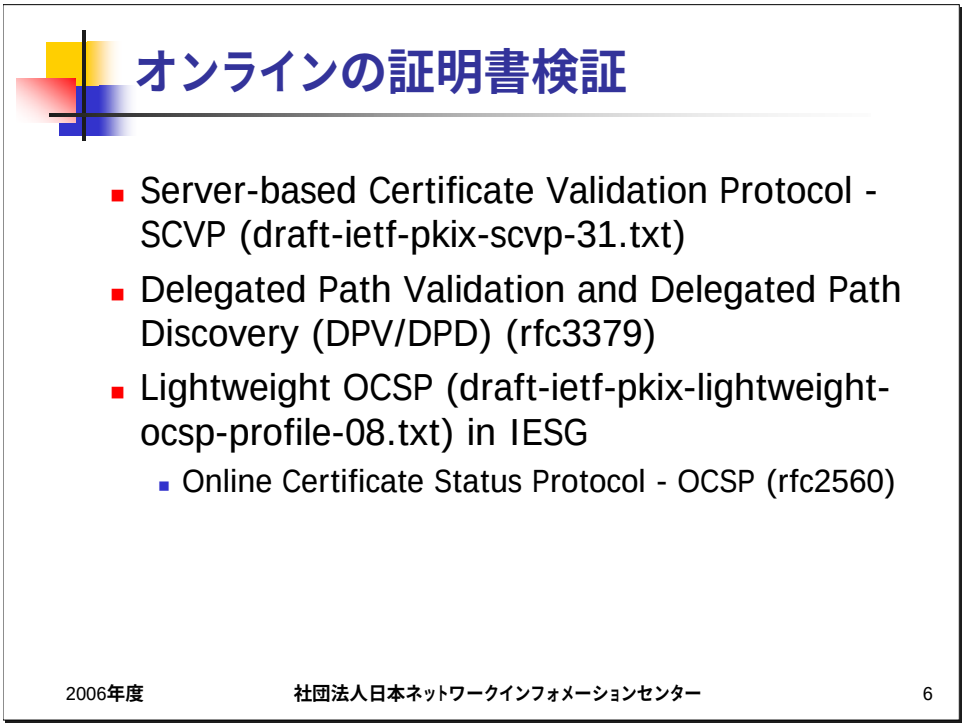

図 3-4　オンラインの証明書検証プロトコル

オンラインの証明書検証プロトコルは、大きな処理能力を持たない PDA や携帯電話などの機器でも電子証明書を扱えるようにするものである。「Server-based Certificate Validation Protocol – SCVP」は電子証明書の検証を検証専用のサーバに任せてしまうプロトコルである。証明書を検証するための情報の入手などもサーバに任せてしまうため、クライアントは電子証明書を処理する必要がない。

「Delegated Path Validation and Delegated Path Discovery (DPV/DPD)」は、パス検証（Path Validation）とパス構築（Path Discovery）をサーバに任せるもので、電子証明書の検証方針などをクライアント側が持つことができるプロトコルである。パス検証やパス構築といった計算能力や、通信帯域を要する処理をサーバに任せることができる。

「Lightweight OCSP」は Online Certificate Status Protocol の軽量版で、メッセージサイズを小さくするなどの工夫がなされたものである。サーバが証明書の検証した結果に対して、クライアントが検証を行うため、このほかのプロトコルよりもクライアント側に処理能力が必要とされるが、メッセージサイズなどの工夫によって一度に大量の処理ができるような効果が期待できる。

○PKIX WG の近年（ここ１年）の動向

SHA-1 などの一方向性ハッシュアルゴリズムを弱体化する攻撃方法が実証されたことを受け、PKIX WG ではこのアルゴリズムの代替手段が検討されてきた。

新たなアルゴリズムをはじめから検討することは、IETF のプロトコル策定の場ではなく研究の分野で行われるべきであるという考え方から、PKIX WG では既存のプロトコルに対して「Hash Algorithm Agility」と呼ばれる考え方を導入することとしている。これはアルゴリズムを代替できるようにするもので、単に書式として変えられるようにするだけでなく、例えば電子証明書を検証する側の処理がしやすいように、扱うことができるアルゴリズムの一覧を事前に伝達できるような工夫が行われることが考慮されている。一方、代替手段となるアルゴリズムを選択する作業は米国の NIST（National Institute of Standards and Technology）にて行われている。

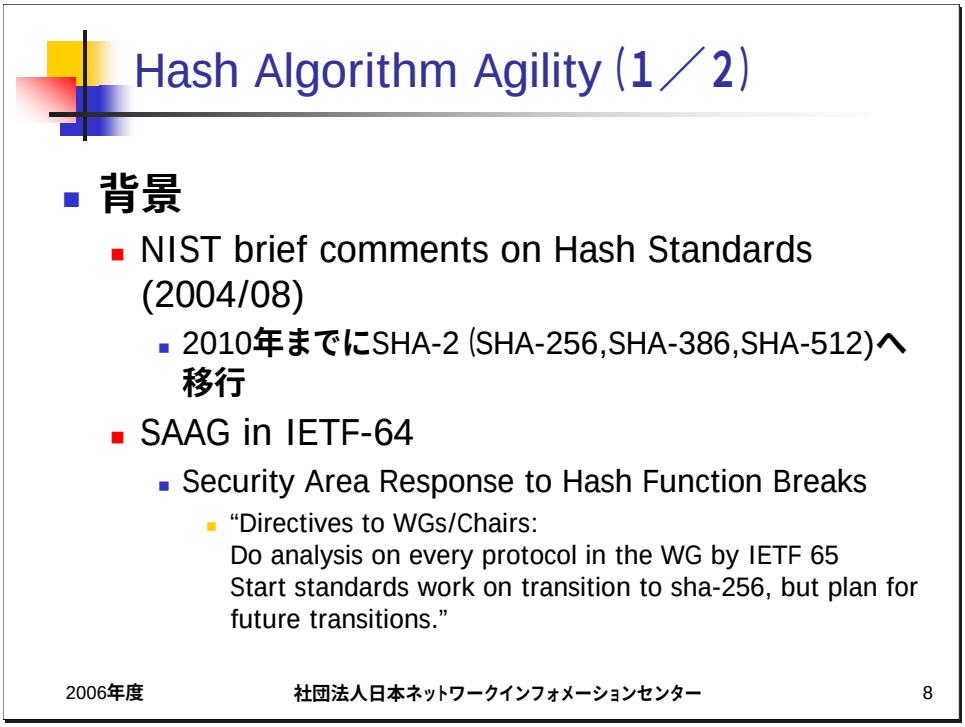

図 3-5　IETF における Hash Algorithm Agility の動向

多くのベンダーによる認証局の実装に、共通のアルゴリズムを導入させるためには、指

針となる期限やアルゴリズムの候補が必要であるという考え方から、NIST では 2010 年までに SHA-2 シリーズのアルゴリズムを実装するというコメントを発表している。また IETF でも既に第 64 回 IETF で SHA-256（SHA-2 シリーズのアルゴリズムの一つ）を使ったプロトコルへ移行する方針を打ち出した（図 3-5）。

PKIX WG では初めに OCSP を取り上げ、Hash Algorithm Agility への対応が進められることになっている（図 3-6）。

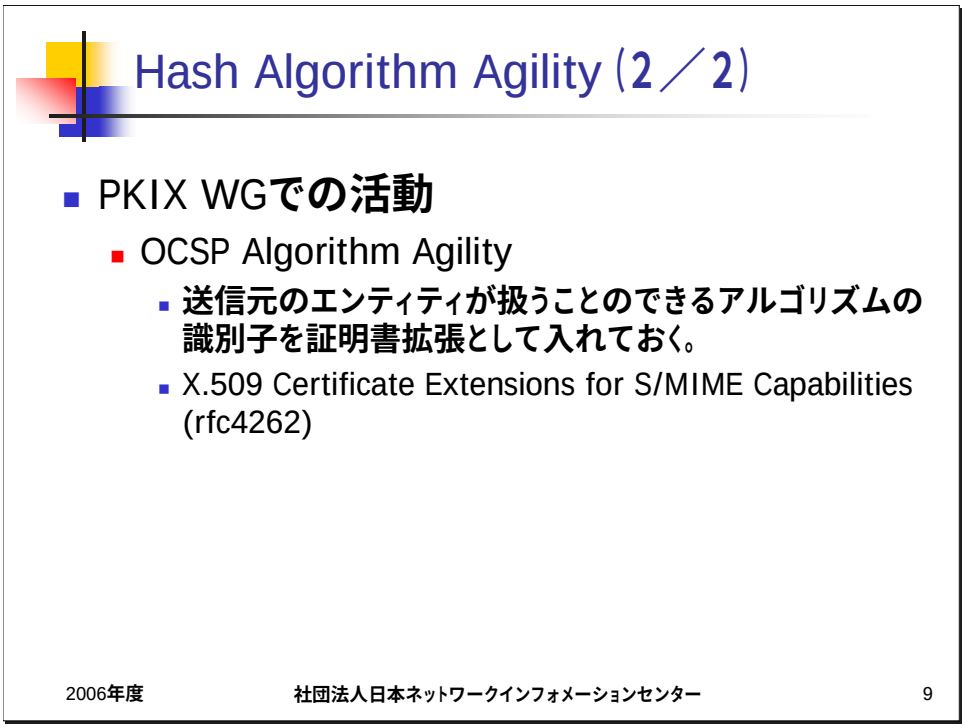

図 3-6　PKIX WG における Hash Algorithm Agility への対応

OCSP ではリクエスト側（証明書検証を依頼するクライアント）がレスポンダー側（証明書検証の依頼を受け付けるサーバ側）の返答につけられた署名検証を行う必要がある。そこでリクエスト側が、レスポンダー側が使う可能性がある一方向性ハッシュアルゴリズムを知っておくことができれば、リクエストを行う前にレスポンダーに証明書検証の依頼を出すべきかどうかを判断できる。この機能は電子メールにおける電子署名機能の標準である S/MIME でも同様であり、すでに rfc4262：X.509 Certificate Extensions for S/MIME Capabilities でドキュメント化されている。

○リソース証明書の動向

電子証明書を用いて IP アドレス等のアドレス資源の管理を安全にする仕組みであるリソース証明書は、主に SIDR （Secure Inter-Domain Routing）WG で議論されている。SIDR WG は APNIC の Geoff Huston 氏と SPARTA 社の Sandra Murphy 氏がチ

ェアを務めている WG で、第 65 回 IETF から第 68 回 IETF にかけて 4 回のミーティングが行われている。RPSEC（Routing Protocol Security）WG と異なり、新たなセキュリティの仕組みを提案し策定することを目的としており、そこで検討に使われるセキュリティ要件は RPSEC WG での議論に基づいて行われるものとされている。

第 65 回 IETF で BoF として行われた SIDR のミーティングでは、リソース証明書を中心とする電子証明書を基本とする新たなルーティングセキュリティの仕組みと、BGP（Border Gateway Protocol）における安全性の強化の 2 つの仕組みに関する RFC の策定に取り組むこととなった（）。しかし第 66 回 IETF 以降の WG となって以降のミーティングでは、主に前者の電子証明書の議論が主に取り上げられている。

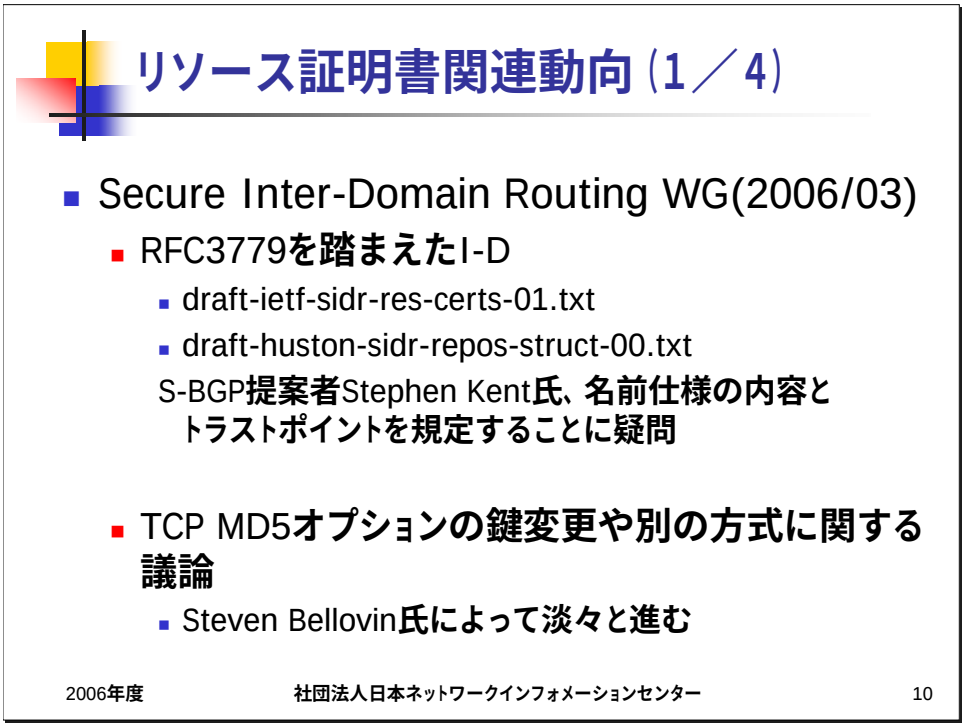

図 3-7　SIDR WG におけるリソース証明書の動向

SIDR WG における議論によって、RIR によるリソース証明書の管理運用と、BBN 社の Stephen Kent 氏が提案した S-BGP（Secure BGP）によるリソース証明書の利用という構造が作られつつある。PKI の概念を踏襲するという考え方によるためか、PKIX WG との JOINT ミーティング（合同ミーティング）が開かれることがあり、いくつかの課題について PKI の概念を使うことで解決を図っている（図 3-8）。

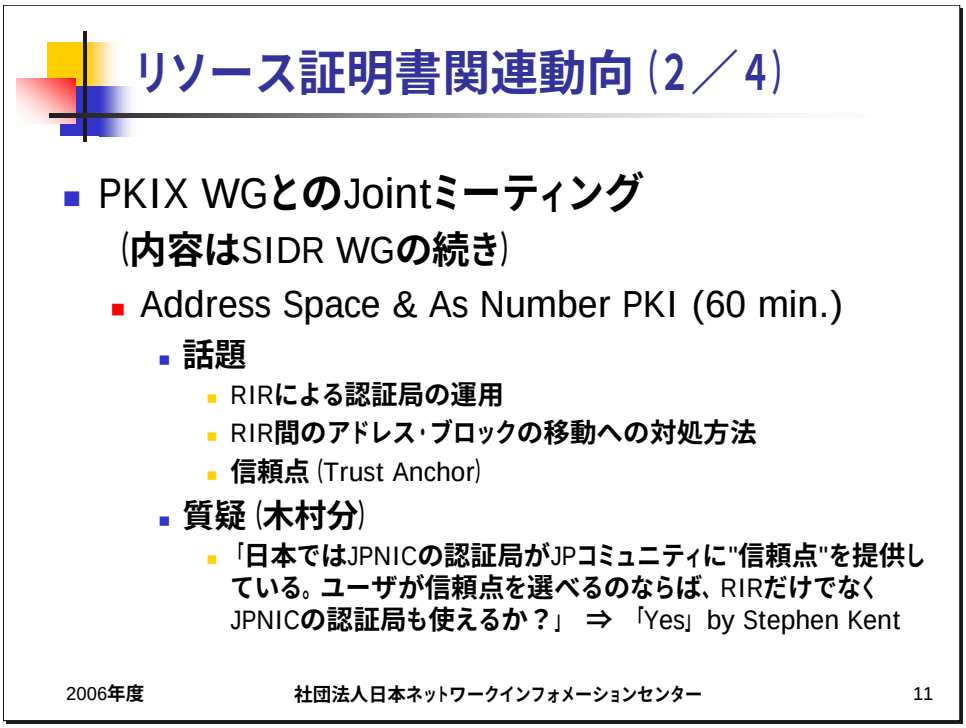

図 3-8　リソース証明書に関する Joint ミーティング

しかし、リソース証明書は「アドレス資源の利用／管理権限」を表す証明書であって管理者の認証のために利用されるものではないという考え方から、証明書リポジトリのアクセス方法や証明書の発行先を示す Subject フィールドの値が独自の形式を持っている。これらの独自の形式は APNIC におけるリソース証明書プロジェクトを通じて考案されたもので、主にチェアの Geoff Huston 氏によって提案されている。

APNIC ではリソース証明書のプロジェクトを 2006 年 4 月頃から開始しており、2007 年末にプロジェクトが一旦終了し、APNIC から IP アドレスの割り振りを受けているメンバー向けの Web ページ MyAPNIC で利用のためのインターフェースが実験的に提供される予定になっている（図 3-9）。

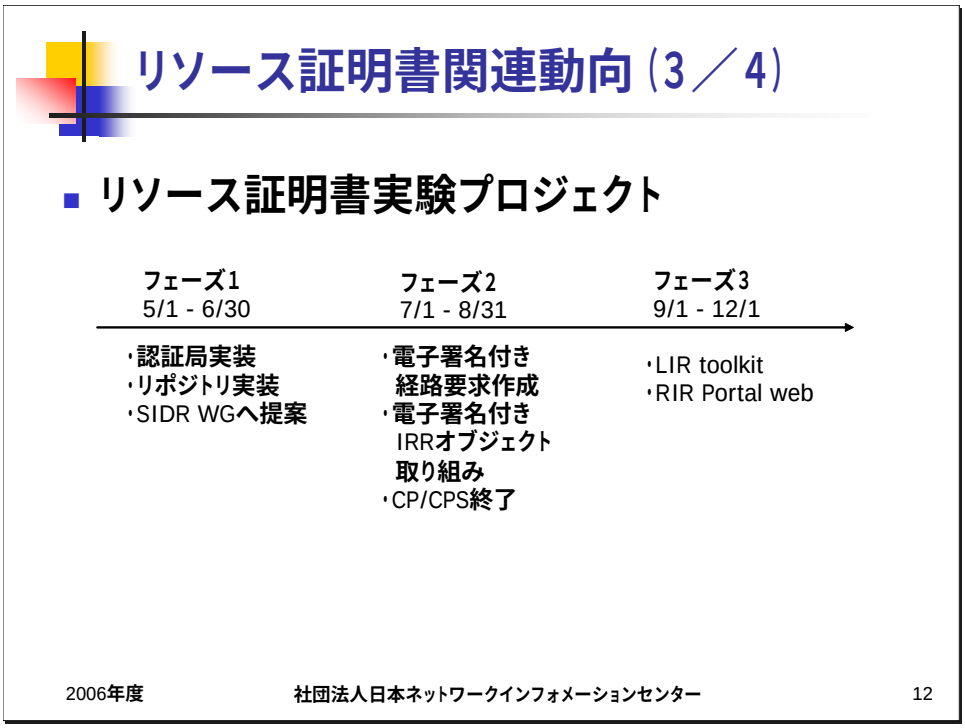

図 3-9　APNIC のリソース証明書プロジェクト

○リソース証明書における課題

リソース証明書は PKI を用いてアドレス資源の利用／管理権限を示す電子証明書のことで、APNIC ではアドレス資源のより厳密な管理のために資する有効な手段だと位置づけられていると言える。一方、提唱されているリソース証明書には技術的な課題がある。一つはアドレス資源の移管のサポートとアドレス資源管理の実効性である。

RIPE NCCにおけるERXプロジェクト[16]のように、アドレス資源はRIRの間で移管が行われることがある。これは頻繁に起こることではないが技術的に対応できなければ実施ができなくなってしまう。APNICでは移管が起こりうる状況でもRIR同士で齟齬のないリソース証明書が発行できるようにするため、各々のRIRに移管用の認証局を設け、移管されたアドレス資源の証明書はその認証局によって収容されるものを提案している。これにより各RIRは他のRIRに管理されているアドレス資源のリソース証明書を発行することができなくなる一方、認証局の構造の複雑さと管理負荷が上がるという課題がある。

またリソース証明書の実効性については、割り振り情報／割り当て情報の正確性を向上させるわけではないことから、本来有効かどうかがわからない証明書が普及してしまうという懸念がある。その場合、リソース証明書が無効になった場合に、割り振り先組織への割り振りを停止してよいかどうかわからない事態に陥り、結果的にリソース証明

[16] Early Registration Transfer [ERX] Project
http://www.ripe.net/projects/erx/index.html

書を導入する意味がなくなってしまう。

RIPE NCCはAPNICのリソース証明書の開発プロジェクトに協力しつつも、これらの課題に対して静観しておりその効果を評価するプロジェクトを立ち上げている[17]。

3.6. まとめ

本章では主に IETF への参加を通じて調査した、ドキュメント策定プロセスと電子認証技術、およびリソース証明書に関して述べた。IETF では RFC の策定プロセス自体に対する議論も盛んに行われており、RFC を効果的に策定し、また理念に即した形で議論できるような基盤が再確認された。

電子認証フレームワークの策定は、IETF と異なり技術自体ではなくノウハウの蓄積を目的とするものであるが、活動の中立性およびオープンさの維持、新技術をいち早く取り入れる意味では、IETF における段階定義や簡便な提案手続き、オープンな情報公開などは参考になる手法であると考えられる。

PKIX WG では近年、電子証明書技術の派生的および応用的な RFC が策定されつつあり、また携帯電話や PDA といった処理能力が小さい端末をサポートできるようなサーバを使った電子証明書の検証プロトコルが策定されつつある。また一方向性ハッシュアルゴリズムの攻撃可能性の向上に伴い、SHA-2 への対応方針が取られ、実施されつつある。

SIDR WG では、RIR におけるリソース証明書プロジェクトと連携する形でリソース証明書関連の RFC の策定が進められている。リソース証明書にはいくつかの技術的な課題があり、RIPE NCC などの RIR では採用に慎重な姿勢を保っている。

RIPE NCC 等の RIR ではリソース証明書の有効性に関する議論が行われつつあり、今後も注目していく必要があると考えられる。

[17] RIPE Certification Task Force
http://www.ripe.net/ripe/tf/certification/index.html

第３章　電子認証技術と技術文書策定に関する国際動向