Internet Topics
インターネット・トピックス ～関連団体の動向～

## ICANNによるルートゾーンスケーリング調査について

ルートゾーンスケーリングとは、DNSSECの導入、DNSサーバへのIPv6アドレス付与、IDN ccTLDおよび新gTLDの追加などによりルートゾーンが拡張されることによる影響を指します。

本稿では2009年にICANNによって行われた、DNSSEC[※1]や新gTLDに関連するルートゾーンスケーリング調査について、掘り下げてお伝えします。

### ◆調査の経緯

2009年2月のICANN理事会決議（2009-02-03-04）[※2]で、同月中のルートゾーンスケーリング調査に関する委任事項（Terms of Reference; ToR）の作成と、同年5月15日までの報告および勧告の提出を、理事会に対して行うことが定められました。

ToRには、主に提出物として何を記載すべきか詳細に記述されています。その中で、本調査の主要な成果物は、ルートサーバシステムの各部分がどのように関連しているのかを示す作成されたモデルであるとうたっています。このモデルを作成することで、各変数を変化させた場合にどのような結果になるかが予想できるとしており、このモデルは定量的であればあるほどよいとされています。提出物について規定している部分では、TLD数が「数百から1万まで」「1万から30万まで」「30万以上」の三つの場合に分けて、それぞれの場合における影響を推定するよう求めています。

ToRの発行は大幅に遅れ、同年5月5日付で発行されました。発行のアナウンス[※3]は5月29日付でなされ、7月31日まで意見募集に付されました。

次に、ICANNシドニー会議の一環として、6月22日に本件に関して調査チーム（Study Team）および運営グループ（Steering Group）の一部メンバーが、プレゼンテーションを行いました。

その後、9月18日付で報告書完成のアナウンス[※4]があり、11月29日まで意見募集に付されました。調査チーム名で提出されたこの報告書[※5]には、要旨にて次の2点が示されています。

- DNSSEC、新TLD、IDN、およびIPv6アドレスを同時にルートに追加することに伴うリスクは、現在のルートサーバ運用の仕組みを変えることによってのみ対処可能

- 今の仕組みを変えずに優先順位をつけて導入するとすれば、DNSSECがその他の三つに先駆けて導入されるべき

この結論を出した根拠は、ルートサーバオペレーターに作業負荷がかかり、余裕がなくなりすぎるためと説明されています。

また、モデルによる解析の結果では、モデルが十分でないため、この結果の信頼性は限定的であるとしながらも、5,000～8,000TLDを超えたあたりで、TLDの変更要求処理に要する時間が現実的でなくなる（100時間程度）可能性が示されています。

なお、上記モデル化の部分についてはTNO[※6]が担当し、別に報告書[※7]を発行しています。こちらは10月1日より11月29日までに意見募集が実施[※8]されました。

10月28日には、ICANNソウル会議にてルートゾーンスケーリング調査についてのセッションがあり、調査結果が発表されました。

### ◆本調査についての問題点

まず、理事会決議において、ToR作成および報告書／勧告提出の要請が誰に対して行われたのかは、理事会議事録を見ても直接的には明確にされていませんが、ICANN事務局による本調査についてのアナウンス[※3]によれば、セキュリティと安定性に関する諮問委員会（SSAC）ルートサーバシステム諮問委員会（RSSAC）およびスタッフに対してとなっているようです。

その結果、でき上がったToRについては、誰が作成したのか記載がありません。

また、調査チームおよび運営グループについては、前者はDNSの専門家、後者はSSACとRSSAC、およびICANNスタッフからなると、構成メンバーが公表されてはいますが、理事会決議およびToRでは明確に位置付けられていません。ICANNからのアナウンス[※4]では、コンサルティング会社であるInterisle社が調査のために選定されたとも発表されており、報告書本体には、「調査チームが運営グループのために作成した」とは記載されているものの、本当に誰が報告書を作成したのか、関係も含めて不明瞭です。

さらにはこの報告書中での、「DNSSEC、新TLD、IDN、およびIPv6アドレスを同時にルートに追加することに伴うリスクは、現在のルートサーバ運用の仕組みを変えることによってのみ対処可能」「DNSSECがその他の三つに先駆けて導入されるべき」という結論は、数字が入っていない概念図によって導かれており、モデルに基づくものではありません。調査結果および勧告の章ではモデル解析の結果は使われておらず、さまざまな箇所で技術的な解説がなされているものの、ToRが求めているものとは異なった内容となっています。

以上のことから、報告書の内容はToRが求めるものからは、かなり程遠い内容となっていると言えるでしょう。

報告書に対する意見募集で寄せられたコメントの多くは、定量的な分析が不十分であることと、ToRと報告書内容とのずれがあることを指摘しています。意見募集期間が終了してから半年以上が経ちましたが、寄せられた意見のまとめおよび分析は、本稿執筆時点ではまだ発行されていません。

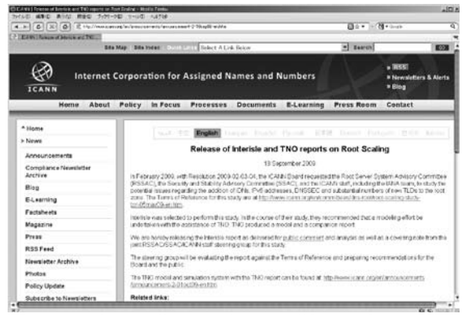
2010年2月15日に、ICANNスタッフからSSAC/RSSACからの報告を待ち望んでいるとの表明がされましたが、本稿執筆時点では両諮問委員会からの報告もなされていません。ただし、SSACからは、2009年12月17日付でルートゾーンスケーリング調査報告書およびTNO報告書へのコメント文書[※9]が公開されています。この文書においても、ToRと報告書内容との隔たりについて指摘がされています。

### ◆おわりに

ルートゾーンへのDNSSEC導入は、2009年12月より順次導入に向けて準備が進んでおり、2010年5月から6月にかけて最終判断がなされた上で、7月15日までに終わらせることになっています。また新gTLDについては、2010年中の導入をめざすとされています。

今後、本調査がモデルの改良などを盛り込んで再度なされるのか、もしくはたなざらしになるのかはわかりませんが、DNSSECおよび新gTLDのスムーズな導入のためにも改善され、誰でもモデルにより試算ができるようにしてもらえれば、と筆者は思います。

（JPNIC インターネット推進部 山崎信）




■ ICANNによるルートゾーンスケーリング調査報告書掲載のアナウンス

**※1 DNSSEC**
DNSに関するセキュリティの強化を行うための拡張機能です。DNSで提供する情報に電子署名を付加し、DNSを使って得られた情報と発信元にある情報との同一性を保証します。

**※2 ICANN 理事会決議（2009-02-03-04）**
http://www.icann.org/en/minutes/minutes-03feb09.htm

**※3 Root Server System Root Scaling Study**
http://www.icann.org/en/announcements/announcement-29may09-en.htm

**※4 “Release of Interisle and TNO reports on Root Scaling”**
http://www.icann.org/en/announcements/announcement-2-18sep09-en.htm

**※5 “Scaling the Root”**
http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf

**※6 Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek（TNO）：オランダ応用化学研究機構**
http://www.tno.nl/

**※7 “Root Scaling Study”**
http://www.icann.org/en/committees/dns-root/root-scaling-model-description-29sep09-en.pdf

**※8 “Publication of TNO Report Describing Root Scaling Model”**
http://www.icann.org/en/announcements/announcement-2-01oct09-en.htm

**※9 SAC042**
http://www.icann.org/en/committees/security/sac042.pdf

2010.3.1▶3.5

# APNIC29ミーティング報告

## ■全体報告

APNIC29は、2010年3月1日(月)～5日(金)の5日間にわたって、マレーシアのクアラルンプールで開催されました。

この時期のミーティングとして例年通りAPRICOTとの併催という形式をとり、マレーシアは国際カンファレンスの誘致に積極的なのか、過去10回のAPRICOTのうち、クアラルンプールでの開催は今回で3回目となりました。毎回政府の支援とともに、マレーシアのICT業界を代表する非営利組織であるPIKOM(Persatuan Industri Komputer dan Multimedia Malaysia)がローカルホストを務めています。

APRICOTも含めたカンファレンス全体の参加者は、733名と2009年よりも100名程度多い結果となりました。日本からの参加者も全体の約1割を占めており、これは国別の参加者としては高い比率と言えます。

### ◆今回のミーティングの特徴

アドレスポリシーに関する議論では、在庫枯渇後の対応として大きな注目を集めていたIPv4アドレスの移転が既に2010年2月に施行されたこともあり、今回大きく紛糾する議論や特筆すべき決定はありませんでした。

一方、参加者が議論を行う「コミュニティコンサルテーション」と呼ばれるセッションが開催され、ITU(国際電気通信連合:International Telecommunication Union)で議論が行われているアドレスの分配方式について、IPアドレスコミュニティとしての意見が取りまとめられました。こういったガバナンスをテーマとして参加者が議論を行うセッションは初の試みでしたが、Plenaryと同程度の参加者が会場に集まり、地域外の参加者もITUに向けたIPアドレスコミュニティとしての意見を述べるとの意識で議論に参加し、関心も高かったようです。

本稿では、(1)ITU IPv6 GroupへのIPアドレスコミュニティとしての声明文、(2)APNIC29においてコンセンサスの得られたアドレスポリシー提案3点、(3)EC選挙の結果を中心にご紹介します。


### (1)コミュニティコンサルテーション

ITU IPv6 Groupが2010年3月15日～16日に初の会合を開き、ITUを介した国ベースのIPv6アドレス分配方式について議論が行われる状況を受け、その会合に向けアドレスコミュニティとしての意見を取りまとめるべく、セッションが開催されました。

IPv6 Groupは、「IPv4アドレスの分配が先進国に偏っており、IPv6でも同様の現象が起きるとの懸念が、一部の発展途上国から表明されている」とのITUの見解のもと、対策検討のために立ち上げられたグループです。その検討の一環として、ITUをインターネットレジストリとし、国ベースに設置するCIR(Country-based Internet Registries)を介したIPv6アドレスの分配方式も視野に入れ、その実現性と妥当性の調査を専門家に依頼していました。

その調査結果として、NAv6※のSureswaran Ramadass氏により、ITUがRIRと並行してIANAからIPv6アドレスの割り振りを受け、CIRに分配する方式とそれに対する分析がペーパーとしてまとめられ、本セッションでもその概要が紹介されました。

パネリストを交えた議論(当初90分の予定が、90分延長されて180分となりました)では、問題対処方法としてITUで検証されている分配方式の必要性への疑問や、施行に伴うリスクに関する質問が中心に表明されました。

セッションの終わりに、本セッションでの議論をまとめた文書が共有され、ITU IPv6 Groupへ提示するコミュニティからの意見として、コンセンサスが得られました。その後、2010年3月5日に、次のコミュニティ声明文がITU IPv6 Groupに提出されています。

※National IPv6 Centre Of Excellence(NAv6)
http://www.nav6.usm.my/index.php

□ITU IPv6 Groupへのコミュニティ声明文
http://www.apricot2010.net/__data/assets/text_file/0005/18923/Kuala-Lumpur_Community-Statement.txt

1. 現行と並列した別のアドレス分配方式の施行は大きなリスクを伴うにも関わらず、NAv6から提示されている文書では、施行に伴う詳細なリスク分析、その他必要な情報が不足している。ITU IPv6 Groupでの検討材料としては十分でないと考える。
2. ITUにおける懸念がIPv6アドレスの枯渇であるように見受けられるため、この点に関するさらなる調査を推奨する。
3. ITU IPv6 Group において必要な文書を公開し、(会員に限定しない)マルチステークホルダー方式の対応を求める。

### (2)アドレスポリシー提案の結果

今回は、6点のアドレスポリシー提案のうち、3点の提案でコンセンサスが得られましたが、国内のアドレスの分配管理に大きな影響を及ぼす決定はありませんでした。

施行されれば影響を及ぼすものとして、APNICにおける最後の/8の在庫からの分配方法を変更する提案も2点行われましたが、「現在の最後の/8からの分配要件を変更する必要はない」として、どちらも支持されず、否決されています。

コンセンサスの得られた提案については、2010年5月3日まで引き続きメーリングリストでの意見も受け付けています。

□コンセンサスの得られた提案

・prop-079:abuse-cの新設
abuse対応効率化のため、WHOIS上で提供される連絡窓口として、abuse専門窓口の登録を義務付けた提案です。国内の施行については別途JPOPM(JPNICオープンポリシーミーティング)での提案が必要となります。

・prop-080:IPv4プリフィクス交換ポリシーの撤廃
日本国内では施行していないため、影響はありません。

APNICでは連続しない複数プリフィクスを、それに相当するサイズの単一プリフィクスと交換するポリシーを施行しています。しかし、在庫枯渇に伴い、当該プリフィクスの確保を保障できなくなるため、これを撤廃する提案です。

・prop-082:IPv6初回割り振りにおける経路集約要件の撤廃
日本国内のアドレスフォーラム運用を行っている機関である、ポリシーWGのメンバーから行われた提案です。

現在のIPv6の初回割り振り要件の中で、割り振りアドレスの経路集約を義務付けた要件を撤廃する提案です。経路集約は、要件として規制するのではなく、運用者の判断に委ねることが適切とし、ポリシーでは推奨に留める表現に変更となります。現在もポリシー上、定義はされていますが、APNIC/JPNICへの申請における影響はありません。

□コンセンサスの得られなかった提案

・prop-078:APNIC最後の/8在庫からの分配に対するIPv6実装要件
・prop-081:APNIC最後の/8からの割り当て資格
・prop-083:IPv6追加割り振りにおける別要件の新設

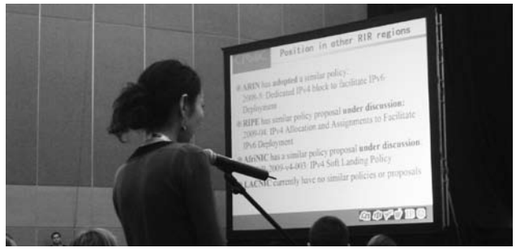
□参考:APNICフォーラムにおけるポリシー提案一覧
http://www.apnic.net/community/policy/proposals

### (3)EC選挙

今回は3名の現職ECの任期満了に伴う選挙が行われ、JPNICの前村昌紀を含めた現職ECが3名とも再選されました。

・Ma Yan (CERNET、中国)
・前村 昌紀 (JPNIC、日本)
・Che-Hoo Cheng (The Chinese University of Hong Kong、香港)

APNIC総会中、第三者による開票の立ち会い資格をめぐって、立候補者の関係者と、選挙運営を務めるECとの間に認識の不一致があり、開票作業が一時中断する事態も生じましたが、運営方針を共有し、総会参加者へ今後の対応の理解も得た上で、開票作業を再開しました。選挙結果自体に影響を及ぼすものでないことは確認されています。




■ JPNICからは、筆者をはじめ6名が参加しました

### ◆ミーティングを振り返って

APNIC29に特化した報告は上記の通りですが、今年は特にAPRICOTとAPNICミーティングとの垣根をなくす方向でWebサイトが統合され、参加者もプログラムの区別を強く意識することなく参加できる構成となっていたように思います。

全体としては、IPv6、DNS、ルーティングやインターネット計測等、インターネット基盤の運営にあたって必要な分野がカバーされ、数年前と比べて随分技術的なセッションも充実してきている印象です。

オペレーショナルなセッションにおいても、APNICに2010年1月に新たに割り振られた1.0.0.0/8の経路到達実験や、レジストリが発行するアドレス証明書を利用したルーティングセキュリティの実装等、アドレス管理に関わる発表も数点見受けられました。これらのトピックスについては、次の記事以降をご覧ください。

### ◆次回のAPNICミーティング

次回のAPNICミーティングは、2010年8月23日～27日まで、タイのバンコクで開催されます。

http://www.apnic.net/events/whats-on/meetings/calendar/events/2010/apnic-30

（JPNIC IP事業部 奥谷泉）

□APNIC29
http://meetings.apnic.net/29

□Meeting Report
http://www.apricot2010.net/report

## ■ APNICにおけるリソースPKIの動向

本稿では、APNIC29ミーティング報告の中での発表を元に、APNICにおけるリソースPKI（RPKI）の動向について報告します。

前回のAPNIC28ミーティングで行われたメンバーミーティング（AMM）で、会場から意見があったためか、今回のAPNICミーティングでは、リソースPKIの情報共有とディスカッションを行うセッション「RPKI BoF」が開かれました。またAPNICとAP地域のNIRが集まって行われる「NIRテクニカルワークショップ」と、通常セッションである「ルーティングセキュリティ」のセッションでもリソースPKIが取り上げられました。

### ◆RPKI BoF

RPKI BoFでは、APNICによるリソースPKIへの取り組みと今後のプランに関するプレゼンテーションが行われました。本BoFのアジェンダを以下に示します。

RPKI BoF アジェンダ
（1）リソースPKIの標準化動向
（2）NROロードマップ
（3）リソース証明書のCPS
（4）MyAPNICにおける対応状況
（5）リソース証明書検証ツール

はじめに（1）で、IETF SIDR WGにおける標準化動向について簡単に説明があり、次に（2）で、国際的にリソースPKIを適用していくロードマップについてプレゼンテーションがありました。APNICでは、今後の1年間で、次の四つのフェーズを経て実施していくプランが立てられています。

・フェーズ1－Pilot
リソース証明書に記載されているIPアドレスやAS番号が、他RIRのリソース証明書の記載と重複することを許容した状態で開始。アドレスの移転が起こった場合のリソース証明書の処理を、手動でできるようにする。

・フェーズ2－Initial Production
五つのRIRにおいて、外部トラストアンカーを利用開始。外部トラストアンカーとは、SSL/TLS等で用いる電子証明書を発行する認証局のことで、RIR毎に立ち上げられる。この段階で、リソース証明書に記載されたIPアドレスやAS番号が、他のRIRで発行されたものと重複しないようにする。

・フェーズ3－Global Consistency
RIR間のリソースの移転を、自動で処理できるようにする。

・フェーズ4－Single TA
単一のトラストアンカーを確立して、RIR間の移転を処理できるようにする。

（3）では、APNICにおけるリソース証明書発行のためのCPS（Certification Practice Statement）案が紹介されました。CPSとは認証局の業務実施内容を、情報公開用にまとめたものです。APNICにおける準備が本格化している様子がうかがわれます。

（4）では、MyAPNICのリソース証明書発行画面が紹介されました。経路情報の検証に使われるROA（Route Origination Authorization）も発行できるようになっています。

（5）では、ユーザーが手元でリソース証明書を検証できるようなツールを、今後APNICが開発することについてプレゼンテーションが行われました。リソース証明書を印刷する機能についても考えられています。

### ◆NIRテクニカルワークショップ

NIRテクニカルワークショップのアジェンダを、以下に示します。

アジェンダと内容
（1）RPKIプロジェクト
国際的に唯一のトラストアンカーを設けることに向けた活動プラン
（2）DNSSECプロジェクト
APNICの割り振りゾーンにDNSSECを導入するプロジェクト
（3）DNS APIプロジェクト
DNSSECが使われる場合にゾーンデータを更新できるAPIの説明
（4）High Availabilityプロジェクト
APNICのWHOISなどのサービス向上を目的とした、災害復旧計画などの検討状況
（5）IPv6 Fast Track
自動的にIPv6を割り振る仕組み。NIRのWebポータルでも利用可能

APNICでは、NROのECG（Engineering Coordination Group）に働きかけ、これまで五つのRIRが個々にトラストアンカーの認証局を立ち上げることになっていた状況を変えて、トラストアンカーの認証局を単一（いわゆるルート証明機関）にするべく活動を行っています。

先のBoFの項で述べたように、今後1年以内に調整がつくと、よりシンプルなリソースPKIができあがることになります。ただ、トラストアンカーの認証局をどこが運用するのかという具体的なことは、まだ決まっていない模様です。

### ◆ルーティングセキュリティセッション

APNICミーティングの「ルーティングセキュリティ」セッションでは、三つのプレゼンテーションが行われました。

・RPKI and Internet Routing Security
川村 聖一氏（NECビッグローブ株式会社）

ISPの観点でルーティングのための正しい情報源の必要性と、リソースPKIが普及すると、オペレーターはリソース証明書とROAを管理しなければならない点などを指摘しています。

・The RPKI & Origin Validation
Randy Bush氏（株式会社インターネットイニシアティブ）

2008年に、YouTubeの経路情報が不正にインターネットに流れるという事件が起こりました。こうした経路ハイジャックを防ぐために、BGPの経路情報のOriginを確認する必要性を指摘した上で、BGPルータにおいてリソース証明書とROAを処理することで、Originの確認が行えることを実装を交えて示しています。

・Local Trust Anchor Management for the RPKI
Stephen Kent氏（BBN Technologies社）

プライベートアドレスや、その経路制御を扱うことを踏まえた、ローカルの証明書検証用の“Relying Party”を用いる提案です。

以上のように、APNICミーティングでは、リソースPKIの話題が積極的に取り上げられています。実験的ではありますが、RIPE NCCやARINでもリソース証明書の提供を開始しており、また今回Randy Bush氏が発表していたように、リソースPKIを利用して経路情報のセキュリティに役立てるプログラムが現れてきています。

しかしAPNIC配下のNIRの中で、リソースPKIを積極的に調査し、技術的な検証を行っているようなところはほとんどないようです。AP地域のNIRが、今後どのようにリソースPKIに取り組んでいくのか、ひいてはルーティングセキュリティにどう関わっていくのか、動きが見えない状況が続いています。

（JPNIC 技術部/インターネット推進部 木村泰司）

## ■ ルーティングセッション

本稿では、ルーティングセッションの内容を、1.0.0.0/8に関する問題を中心にご紹介します。

### ◆ルーティングセッションの概要

ルーティングセッションでは、三つのプレゼンテーションが行われました。今回のレポートでは、筆者が特に注目していた、1.0.0.0/8のIPアドレスブロックに関する経路到達性を複数視点で分析したプログラムである、“1.0.0.0/8 Routability Issues”について詳細を報告します。

### ◆1.0.0.0/8 Routability Issues

2010年1月に、IANAからAPNICへ、1.0.0.0/8の割り振りが行われました。通常、IANAからAPNICへ新規のIPアドレスブロックが割り振られた場合、RIPE NCCが実施するdebogonプロジェクト※を利用して、新規アドレスブロックの経路到達性をAPNICが確認してから、NIRやLIRへの実際の割り振りが行われます。

しかしながら、1.0.0.0/8はそのIPアドレス自体が持つ特徴のため、機器の設定例として使われていたり、テスト用の設定をインターネットへ経路広告してしまったりと、過去に複数回、異常な経路広告がされたことがわかっています。

本プログラムでは、APNICは、このような過去の経緯を持つIPアドレスブロックである1.0.0.0/8を、通常の割り振りブロックとして利用しても問題無いかどうかについて、慎重に調査していることが発表されました。

debogonプロジェクトでは通常、/8のアドレスブロックごとに単一のアドレスブロックを切り出して、到達性の確認を行います。今回の1.0.0.0/8では、過去に異常な経路として経路広告された複数のアドレスブロックを用いて、到達性の確認が継続して行われています。また、追加で複数の協力ASから経路広告を実施し、通常よりも広範囲のASで、到達性の確認が実施されていることが会場へ伝えられました。

セッションの後半では、RIPE NCCから1.0.0.0/8の過去の経緯について報告が行われました。1.0.0.0/8は過去に、14AS、26種類のアドレスブロックが経路広告されたことが観測されているとのことです。また、実際に1.0.0.0/8のアドレスブロックから一部のアドレスブロックを経路広告すると、ある一定量のパケットが経路広告を行ったASへ向かってくる状況であり、そのほとんどの宛先が1.1.1.1や1.2.3.4などの特徴的なIPアドレスであることが伝えられました。

このことは、1.1.1.1や1.2.3.4を含むアドレスブロックの割り振りを受けたASは、このようなIPアドレスにやってくる異常なトラフィックに晒されることを意味しています。この事実は、今後レジストリがアドレスを割り振る際に、特徴のあるIPアドレスを含むアドレスブロックの取り扱いをどうするかという点で影響してきます（本プログラムの前日に開催された、NIRテクニカルワークショップでは、このようなIPアドレスブロックからは割り振りは行わないと、APNICスタッフが発言していました）。

また、本プログラム開催日の早朝から、AS36561（YouTube）が1.2.3.0/24のIPアドレスブロックについて経路広告を開始したため、本プログラムで共有される内容を知らなかった筆者は、複数のIRRやWHOISを検索してもこの経路の真贋についてわからず、一時戸惑ってしまいました。この件については、NANOGメーリングリストに詳細が記録されていますので、興味をお持ちの方はどうぞご参照ください（NANOGメーリングリスト“Subject: 1.0.0.0/8 route from MERIT?”で始まるスレッドにおいて、一連の流れが参照可能です）。

■ 会場の様子

今回のルーティングセッションに限る話ではありませんが、ルーティングセキュリティセッションなどへの参加を通じて、レジストリとして、IRRやRPKIといったIPアドレス一意性の確認手段を、今後どのようにAS運用者などのオペレーターに対して提供するかを、継続してリサーチする必要性を感じました。今後もJPNICとして、このようなミーティングへの参加やコミュニティとの交流を通じて、情報交換を密にしていきたいと考えます。

（JPNIC 技術部 岡田雅之）

※ **debogon プロジェクト**
RIPE NCC が実施するプロジェクトの一つです。IANA から RIR へ新しく割り振られたアドレスは、bogon フィルタ等が原因となって、経路広告を行っても到達しない AS が複数存在することがわかっています。このような問題を低減するため、debogon プロジェクトでは、RIR から NIR や LIR へ割り振りを行う前に、到達性を確認し、旧来の IP アドレスと同程度まで到達する AS を増やす試みを実施しています。

## ■ APNIC EC再選にあたって

2010年3月5日に行われたAPNIC総会（AMM:APNIC Member Meeting）で、EC（Executive Council:理事会）選挙が行われました。私は2000年10月の臨時選挙でECに初当選して以来、5期を務めましたが、今回の選挙においても、JPNICから推薦を受け出馬しました。結果として1,528票をいただき、トップ当選を果たすことができました。これはまさに皆様からの温かいご支援の賜物であり、感謝の念に堪えません。

APNIC ECが持つ責任は、10年前に比べ数段重いものになっています。最近の大きい仕事の一つは、料金制度の改定だったと思います。

2007年に、米国ドルで設定されていた会費を豪州ドルに変更しました。これによって、事業に対する為替変動による影響を最小限に留め、事業運営の安定化を図りました。これを皮切りに、APNIC ECでは外部コンサルタントとともに、より抜本的な料金改定の検討に着手し、2009年4月に新しい料金制度を施行しました。

料金制度の改定に際しては、会員の皆様からAPNIC事業運営全体に対して、大きな関心が寄せられました。会員の皆様にご負担いただく会費を変えるということで、会費が事業にどう活かされているかに関心が集まることは当然と言えますが、オーストラリアのブリスベンにオフィスを構えて10年が経ち、その間に事業規模は5倍になる中、会員の皆様のAPNIC事業運営に対する関心は、日増しに高まってきていることを感じます。

その中でAPNIC ECは、会員を代表してAPNIC事務局の事業運営を監督する立場として、会員の皆様に対する説明責任を果たすことがより一層強く求められています。適切なガバナンスを維持するために、定款を今一度読み込んで、APNIC ECの行動規範を明確化したのも、2007年から3年間の仕事でした。

今後2年間の任期中にも、課題が山積みです。

2007年からの3年間は、IPアドレス移転制度が初めて提案され、施行に至る3年間でもありました。現在JPNICでもアドレス移転制度の施行に向けた検討を行っていますが、NIRとAPNICとの間の移転、あるいはRIR間の移転に取り組まなければなりません。この実現にはアドレスポリシーとともに、レジストリ間のトランザクションを規定する必要があり、簡単ではありません。

2年後の2012年には、RIRにおけるIPv4アドレス在庫が枯渇するとされていますので、今後2年間の任期の内に、本格的に、IPv4アドレス在庫枯渇後の事業運営指針を立てなければなりません。ITU IPv6 Groupの議論※やIGF（Internet Governance Forum）など、インターネットガバナンスに関する議論も重要です。

今までの任期以上に、気を引き締めて取り組まなければなりません。

私自身、2009年4月のインターネット推進部への異動によって、JPNICのIPアドレス事業からは離れましたが、代わりにICANNの動向を追うことが私の仕事の一つとなりました。これまでとは違う視点からAPNICを眺めることができるようになったことは、APNIC ECの仕事にも寄与してくれると思います。

この任期中、皆様からいただいたご信託に応えるよう、頑張ってまいります。引き続きのご支援を、よろしくお願いいたします。

（JPNIC インターネット推進部 前村昌紀）

※ ITUがRIRと同じレベルでのレジストリとなって分配を受け、Country-based Internet Registryと呼ばれる国別の機構を通じて、IPv6アドレスを分配する案が議論されています。詳しくは、P.22からの全体報告をご覧ください。

2010.3.20▶3.26

# 第77回IETF報告

## ■ IPv6関連WG報告

2010年3月20日から26日まで、米国アナハイムにて第77回のIETFミーティングが開催されました。春先の温暖なカリフォルニア、また、景気の回復基調を反映してか、初めての参加者173名を含む1,192名の参加がありました。参加者の内訳では、米国からの参加者数が過半数を占め第1位、続いて日本、中国がほぼ同数で続いています。

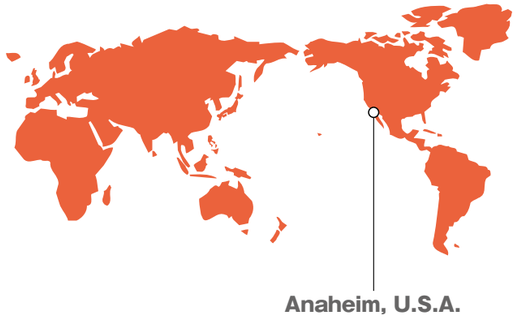
本稿では、会期中に議論されたIPv6に関連したトピックスのうち、IPv6に特化した内容を議論するワーキンググループ(WG)での話題を中心に紹介します。余談ですが今回、IPv6関連のWGは、mif WGとv6ops WG、6man WGとsoftwire WG等、セッションが並列で同時に実施され、参加者も戸惑っていました。

### ◆v6ops WG (IPv6 Operations WG)

v6opsはIPv6に関するオペレーション技術や、移行技術に関する議論を実施するWGです。今回は、3月22日(月)、26日(金)の朝一番のコマにて実施されました。v6ops WGでは、IPv6とIPv4の相互変換技術に関する議論を他WG(behave WG)に移行した後、議論内容が少なくなるのかと思ったのですが、昨今のIPv4アドレス在庫枯渇、IPv6導入の流れを受けてか、継続議論のみでなく、数々の新提案もあり、内容も多岐にわたりました。特に、2010年3月上旬に、サンフランシスコにて開催された3GPPとIETFのジョイントミーティングにおいて、IETFが3GPPでのIPv6利用について、プロトコル制定の面でサポートをする方向になったことを受けてか、3GPPでのIPv6利用に関する提案、議論もいくつか実施されています。

今回、次の議論がアジェンダとして挙げられていました。

〈3月22日(月)〉
- RFC5006(DNS設定のためのRAオプション)の実装と普及に関する議論
- 家庭向けIPv6インターネットサービス提供用CPEにおける簡易セキュリティ推奨機能
  draft-ietf-v6ops-cpe-simple-security
- IPトンネリングにおけるセキュリティの懸念
  draft-ietf-v6ops-tunnel-security-concerns




- IPv6 CPEに関する高機能セキュリティ
  draft-vyncke-advanced-ipv6-security
- 3G拡張パケットシステムでのIPv6
  draft-korhonen-v6ops-3gpp-eps
- モバイルネットワークでのIPv6導入検討
  draft-koodli-ipv6-in-mobile-networks
- ステートレスIPv6プリフィクス委譲
  draft-savolainen-stateless-pd
- ISATAPと6to4における経路ループ: 問題提起と解決案
  draft-nakibly-v6ops-tunnel-loops

〈3月26日(金)〉
- IPv6ディプロイメントに関するサービスプロバイダシナリオ
  draft-carpenter-v6ops-isp-scenarios
- IPv6移行技術の利用に関するガイドライン
  draft-arkko-ipv6-transition-guidelines
- IPv6マルチキャストメッセージのユニキャスト転送
  draft-gundavelli-v6ops-l2-unicast
- 近隣探索プロトコルにおける近隣キャッシュの保護
  draft-jiang-v6ops-nc-protection
- セルラーネットワークにおけるIPv6移行ツールとしてのDHCPv6プリフィクス委譲
  draft-sarikaya-v6ops-prefix-delegation
- ステートレス自動IPv6 over IPv4トンネル: 仕様
  draft-matsuhira-sa46t-spec
- IPv6 CPEルータ拡張推奨機能
  draft-wbeebee-v6ops-ipv6-cpe-router-bis
- Softwire-liteのためのステートレスアドレスマッピング(SAM)
  draft-despres-softwire-sam

次ページより、いくつかの内容について、簡単に紹介します。

### ◎RFC5006(DNS設定のためのRAオプション)の実装と普及に関する議論

当初、この項目はアジェンダにはありませんでしたが、v6opsメーリングリストで大きな議論を呼び、進め方についての確認を実施するために急遽追加されました。IPv6ではPC等の端末にDNSサーバのアドレスを配布する方法がかなり議論され(RFC4339に議論がまとめられています)、その結果、DHCPv6を利用した方法(RFC3646)が標準となり、一般的に利用されています。当時、ルータ広告(RA)を利用した方法も検討されましたが、"Experimental"(実験的)のステータスとして、RFC5006が出版されるにとどまっており、実装もあまりされませんでした。これに対し、RAでの配布も標準にして欲しい、という要望があがり、RFC5006を"Standard"(標準)のステータスにするかどうか再議論となりました。事前のメーリングリストでの議論で、標準とする方向で議論はほぼ固まっており、ミーティングでも、現在のスペックをほぼそのまま標準とすべきである、という意見があった程度で反対はありませんでした。ドラフトを6man WGに提出、標準化を進めていくことになりました。

### ◎IPv6ディプロイメントに関するサービスプロバイダシナリオ

世界的に、IPv6の導入は徐々に進んでおり、対応を進めているサービスプロバイダも増えてきました。このドラフトでは、実際に導入を進めているISPに導入方法、導入時に発生した問題、必要だと思う機能等のアンケートを実施し、その結果をまとめています(JANOGでも昨年末に、アンケートの案内が流れています)。ミーティングでは、「これは中間報告であり、またISPの数もそれほど多くない(ミーティング時点では30程度)ため内容には偏りがある可能性がある」という前提のもと、現状の集計結果の報告がありました。

興味深い結果としては、IPv6サービスの導入時期について、もっとも遅いISPで2013年としていること、IPv6トラフィックが50%を占めるようになる時期は、「2015年」という回答が一番多かったこと、対応が不十分だと思われる機器としてCPEの指摘が多かったこと、ほとんどのISPでIPv4/IPv6のIP層での何らかの相互通信(トランスレーション、デュアルスタック等)が必要だと考えていること等があります。結果は、
http://www.ietf.org/proceedings/10mar/slides/v6ops-0.pdf
にまとめられています。このドラフトの今後ですが、RFCとして発行することに対する反対意見はあったものの、まずは文書としての構成を見直して整理する方向となっています。

### ◎近隣探索プロトコルにおける近隣キャッシュの保護

IPv4のARPキャッシュにあたる、近隣キャッシュの保護に関する提案です。近隣要請メッセージを多数送るというDoSアタックにより、ノードの近隣キャッシュが溢れてしまうという攻撃を防ぐために、近隣要請メッセージを送ってきたノードに対して、問い合わせを実施し、返答が得られた場合に近隣キャッシュに登録するとしています。これに対し、問題点は共有されたものの、提案されている解決手法に対しては、返答要求メッセージの処理でまた同じ問題が発生すること、問題の一部の解に過ぎないこと(遠隔からの問い合わせでも同じ問題は発生する可能性があるが、それには対応できない)等の指摘がありました。提起された近隣キャッシュを保護するという問題に対して、メーリングリスト上で議論を継続することになりました。

### ◎IPv6 CPEルータ拡張推奨機能

IPv6対応のCPEルータが持つべき機能に関する提案です。WANとLANの設定、基本的なルータ機能、基本セキュリティ機能のみを基本部分として分離した基本機能ドラフトは別途RFC化に向けて進んでいます。そのドラフトから切り出した検討事項が多い部分(マルチキャスト、DNS、プリフィクスの再委譲、IPv6移行機能、パケットフィルタ、QoS等)に関して、今後の進め方に関する議論がありました。現在、別のWGとしてホームルータの機能を議論するhomegate WGが構成されようとしており(2010年4月末に中間ミーティング実施予定)、棲み分けをどうするか、が主な論点でしたが、homegate WGとは連携をするが、現状まだhomegate WGでの議論動向がはっきりしないことおよび、homegate WGでカバーされない部分に取り組む必要があることから、v6ops WGで継続的に議論をしていくことになっています。

□v6ops WG
https://datatracker.ietf.org/wg/v6ops/

□第77回 IETF v6ops のアジェンダ
http://www.ietf.org/proceedings/77/agenda/v6ops

### ◆6man WG (IPv6 Maintenance WG)

6man WGは、IPv6のプロトコル自体のメンテナンスを実施するWGです。今回のミーティングは、3月24日(水)の午後の2コマ(13:00-16:10)にて開催されました。途中、2コマ目はDS-Liteや6rdを扱っているWGとして最近注目を集めているsoftwire WGと時間帯が重なってしまったため、多くの参加者が途中退出する様子も見受けられました。

まず、6man WGで取り組み中である、以下の文書のステータス確認が行われました。

・経路制御ヘッダー（RFC出版準備中）
・IPv6サブネットモデル（IESGレビュー中）
・IPv6推奨アドレス表記（IESGレビュー中）
・フラグメント重複問題（RFCとして出版）

アジェンダには下記のアイテム/テーマが掲載されていました。

・ノード要求仕様の更新
　draft-ietf-6man-node-req-bis
・RFC5006（RAでのDNS情報配布）をStandard Trackへ
・UDPゼロチェックサム
　draft-fairhurst-tsvwg-6man-udpzero
・IPv6フローラベルの使用法に関して
・IPv6フローラベルを用いたECMP（Equal-Cost Multi-Path）
　draft-carpenter-flow-ecmp
・IPv6フローラベル仕様の更新
　draft-carpenter-6man-flow-update
・IPv6フローラベルを用いたトランスポート層シグナリング
　draft-donley-6man-flowlabel-transport-sig
・DHCPv6経路情報オプション
　draft-dec-dhcpv6-route-option
・ユニークIPv4射影アドレス
　draft-thaler-6man-unique-v4mapped
・ルータ間リンクでの127ビットプリフィクス
　draft-kohno-ipv6-prefixlen-p2p
・アドレス選択
　draft-ietf-6man-addr-select-considerations
　draft-ietf-6man-addr-select-sol
・データプレーンデータグラムにおいてRPL情報を伝達するためのRPLオプション
　draft-hui-6man-rpl-option
・近隣探索ベンダー固有オプション
　draft-gundavelli-6man-ipv6-nd-vendor-spec-options
・RS（ルータ要請）のマーキング
　draft-krishnan-6man-rs-mark

この中で、DHCPv6経路情報オプションについては、既に行われたmif WGのセッションにおいて、mif WGで扱われることがほぼ確定したため、本セッションでの発表はありませんでした。これらのアジェンダの中から、いくつかのトピックについてご紹介します。

### ◎RFC5006（RAでのDNS情報配布）をStandard Trackへ

RFC5006で定められた、RAを用いたDNS情報配布オプションを、これまでのExperimental（実験的）のステータスから、Standard Track（標準としての提案）に変更しようというテーマについての議論が行われました。このアイテムについては、月曜日に行われたv6ops WGのセッションや、v6ops WGのメーリングリスト上で、支持者が大勢を占めるという状況になっており、標準化を進めることについての合意はほぼ形成されていましたが、6man WGが実際のプロトコル策定を行うWGということもあり、ここでも再度発表が行われました。

このセッションでは、DNS関連のオプションとしてはDomain Search Pathオプション等も存在するが、これらは必要ではないのか、という疑問に対して、Domain Searh Pathは通信のために必須ではないが、DNSサーバアドレス情報は通信のために必須であるから、RAに含めるべきだ、といった意見が出されました。

また、他にもlifetimeオプションは有用ではないか、Domain Nameオプションはあった方がいい、といった意見は出されましたが、このアイテムについて標準化を進めることはほぼ合意が取れていることが確認されました。

### ◎IPv6フローラベルの使用法に関して

IPv6ヘッダー中にフローラベルという20ビットのフィールドがあり、RFC3697でこの使用法について規定されています。しかし、現在このフィールドは広く利用されているとは言えず、RFC3697で定められた、途中のルータでこのフィールドを変更してはならない、といった規定がその利用を制限しているため、これを緩和しようという提案がなされました。

提案内容としては、現在のフローラベルの1ビット目が1にセットされていた場合に、それ以降の19ビットはRFC3697の規定が適用されず、サイト等のローカルドメインで利用してよい、というものです。

また、フローラベルの具体的な利用法についても提案があり、ECMP（Equal-Cost Multi-Path）というトラフィックの負荷分散や、QoS（Quality of Service）の実現等が提案されました。これらの利用例は、上記のフローラベルの規定が変更されなければ実現が難しく、現在の規定の制限を受けているものとして説明されました。

この発表に関する議論としては、実際にフローラベルがどの程度、どのように利用されているのかという疑問が投げかけられ、それを調査してから仕様変更に着手するべきである、といった慎重な意見も出されました。また、実際にフローラベルが使われている例についても紹介がありました。仕様を変更することで、ローカルドメインにおける新たな使用法が可能になるため、ぜひ仕様を変更するべきであるという意見と、それによってこれまでの使用法が不可能になってしまうという意見があり、議論は平行線となりました。

### ◎ルータ間リンクでの127ビットプリフィクス

ルータ間に付与するアドレスとして、パケットのループ（ping-pong）や、近隣探索キャッシュ溢れ等の問題の発生を防ぐために、127ビットのプリフィクスを用いることが有用です。しかし、IPv6ではサブネットエニーキャストアドレスが存在するため、これを利用することができないという問題が提起され、ルータ間リンクではこのアドレスを無効にしようという提案がなされました。

Point-to-Pointリンクが利用できるのではないか、また、ホームゲートウェイのWAN側でも利用できるようにするのか、といった議論が行われ、WGアイテムとしての採用はこれらの議論を行ってから、ということになりました。

### ◎アドレス選択

IPv6のアドレス選択方式については、複数の送信元アドレスと送信先アドレスのペアが存在するときに、短時間で一斉にこれらのペアについて通信を試みる、アグレッシブモードと呼ぶ方式と、従来方式との棲み分けについての提案がなされました。提案内容としては、どちらの方式を採用した場合でも、サイトのポリシーを適用することは必要であり、このポリシーを配布し適用する方法については、アグレッシブモードと従来方式とで、別々に分けて議論を行うことが可能であり、そのように進めようというものでした。

その後の議論では、アグレッシブモードの有用性が思ったほど大きくない研究結果の紹介があったり、アグレッシブモードについては後で検討を進めれば良いといった意見が出されたりしました。また実際のポリシー配布の方法については、実際の配布する情報の選定がまだ議論が十分し尽くされていないという意見があり、メーリングリストで引き続き検討を行うということになっています。

□6man WG
　https://datatracker.ietf.org/wg/6man/

□第77回 IETF 6man WGのアジェンダ
　http://www.ietf.org/proceedings/77/agenda/6man.html

### ◆behave WG（Behavior Engineering for Hindrance Avoidance WG）

behaveは主にNATの挙動に関して扱うWGですが、その技術的な関連性からIPv6-IPv4変換についての議論も行われています。今回は、3月25日（木）と26日（金）に合わせて5時間以上ものスロットを用いて、現在のWGアイテムのステータス紹介と、今後のアクションアイテムの選定が行われました。

IPv6-IPv4変換の基本方式については、以下の文書がIESG（Area Director）のレビュー段階となっており、Transport AreaのArea Directorである、Magnus Westerlund氏からいくつかのコメントや質問が行われました。なお、この基本方式では、IPv6ホストからIPv4ホストへの通信は1対多の変換、逆にIPv4ホストからIPv6ホストへの通信は1対1の変換について定めたものとなっています。

　draft-ietf-behave-address-format-04
　draft-ietf-behave-dns64-07
　draft-ietf-behave-v6v4-framework-07
　draft-ietf-behave-v6v4-xlate-stateful-09
　draft-ietf-behave-v6v4-xlate-10

上位層のプロトコルの扱いに関して、トランスレータが上位層のプロトコルに対応していない場合に、そのパケット転送を必須（MUST）とするかどうかという質問が行われました。会場からの反応としては、ステートフルモードでは転送はできない、MUSTではなくSHOULDにするべきだ、等の意見がありました。またIPv4ヘッダーのIP IDフィールドの扱いについて明記することが必要であるとの意見が述べられました。

続いて、behave WGの今後のアクションアイテム選定と、マイルストーンの設定をするべく、さまざまな方式提案の発表が行われました。主に以下のテーマについて議論が行われました。

・IPv4ネットワークから、IPv6インターネットへの通信（シナリオ3）
・IPv4インターネットから、IPv6ネットワークへの通信（シナリオ4）
・マルチキャストパケットのIPv6/IPv4変換
・IPv6-onlyホストでのIPv4アドレスの扱い

・デュアルスタックホストでのNAT64利用を避けるための方式
・NATのハイアベイラビリティ、負荷分散方式
・ラージスケールNAT

これらのうち、いくつかのトピックについて概況をご紹介します。

### ◎IPv4ネットワークから、IPv6インターネットへの通信（シナリオ3）
### ◎IPv4インターネットから、IPv6ネットワークへの通信（シナリオ4）

IPv4からIPv6への変換については、トランスレータをIPv6サーバ側に設置してIPv4クライアントからのIPv4での通信をIPv6に変換するシナリオ4と、IPv4クライアント側に設置してIPv4クライアントがIPv6インターネットに接続できるようにするシナリオ3とが既にチャーターに掲載されています。しかし、これらの方式はDNSへの依存度の高さ等、以前廃止されたNAT-PTでの問題点をクリアすることが難しく、WGでの標準化マイルストーンも設定されていないという状況になっています。

今回も中国勢をはじめ、両方のシナリオについてさまざまな提案がなされました。シナリオ4については、IPv4-IPv6変換にIPv4アドレスのポート部分を用いてアルゴリズミックに行うことでステートレスに近づけたもの、シナリオ3については、NAT-PTのIPv4-IPv6変換方式そのままのもの、BIS（Bump In the Stack）と呼ばれるホスト内で変換を行うもの、等が提案され活発な議論が行われました。

NAT-PTでの問題の多くが解決されていなかったとしても、移行にはトランスレータが必要であり、これらの技術が必要である等の肯定的な意見も複数あり、またこれらのシナリオは緊急性がそれほど高くはなく、必要になってから議論すべきだ、との意見も出されました。これらの議論を踏まえて、次のステップについてはチェアとAD（Area Director）との協議で決定することになりました。

### ◎NATのハイアベイラビリティ、負荷分散方式

NATのハイアベイラビリティや、負荷分散方式については、これまでの議論のサマリー等が提示され、これら方式の標準化の是非について、議論が行われました。ベンダーからの意見と利用者（キャリア）からの意見が大きく異なっており、マルチベンダー環境でも使えるようにすべく、標準化が必要だというキャリアからの意見と、L2スイッチ等でもベンダー独自方式でやっているように、こういった技術については標準化は難しくベンダーでの独自方式で進めるべきだとのベンダーの意見で対立した状況となりました。

### ◎ラージスケールNAT

ISP等においてNATを行う、ラージスケールNATについても発表がありました。ラージスケールNATに関連する各文書の位置づけや、改訂内容について説明があった後、数名から支持を表明するコメントがありました。特に反対意見や質問等は挙げられなかったため、今後behaveのWGアイテムとして標準化が進むものと思われます。

また、前述以外のトピックとして、今回IETF77の会場ネットワークで運用されていたNAT64トランスレータの実験について報告がありました。カナダのVIAGENIE社のオープンソース実装を用いた実験で、専用のSSIDを用いて実験が行われていました。実験の参加ホスト数は34と、あまり多くはなかったものの、いくつかのバグや、各種OSやソフトウェアの問題等が発見され、有意義な実験となったようです。

□behave WG
https://datatracker.ietf.org/wg/behave/

□第77回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/77/agenda/behave.html

（NTT情報流通プラットフォーム研究所 藤崎智宏／松本存史）

■ 会場となったHilton Anaheim（ホテルのWebサイトより転載）

## ■ DNS関連WG報告

### ◆dnsext WG

dnsext WGでは、前回のIETF76での会合から今回のIETF77での会合までに、一度会合が開催されていました。これは、どこかの会場にて開催されるいわゆるinterim meetingではなく、WebExを利用した遠隔会議として行われ、virtual interim meetingと呼ばれました。

WebExは、最近のIETFにおいてもいくつかのWG会合に導入されており、従来の音声中継に加えて、遠隔からの双方向参加を実現するツールとして利用され始めています。

今回のdnsext WGの会合では、まず“Name equivalences”に関する議論が行われました。これはinterim meetingにて話し合われた議題で、DNSに完全なaliasの機能を導入しようという動きです。現在利用されているCNAMEやDNAMEといった機能では、RR（Resource Record）単位もしくはzone単位のredirectionが提供されますが、NS（Name Server）やMX（Mail Exchange）を含めたすべてのRRに完全なredirection（alias）は提供されません。

これは、もともとはIDN（Internationalized Domain Name: 国際化ドメイン名）に関連する要求として上がってきた機能です。IDNの場合、その文字上の表記は異なっていても、同じドメイン名として扱いたいという場合が発生します。例えば日本語でのIDNの場合、“慶応義塾大学.日本”というドメイン名と、“慶應義塾大学.日本”というドメイン名を、DNS的に全く同じものとして扱いたい、という要求が出てくるかもしれません。日本語TLDでこのような機能が導入されるかは全くわかりませんが、中国語TLDではこのような要求があることが、以前のIETF会合にて報告されています。

この機能の提案に関して、会場では活発な議論が行われました。Paul Vixie氏は“CLONE RR”という新たなRRを導入して解決することを提案しました。発表の中で例として挙げられていたのは、“vix.com”というドメイン名を、“vixie.com”ならびに“vixie.sf.ca.us”というドメイン名にaliasする例です。BINDのzone表記に従うと、以下のように定義します。

```
$ORIGIN vix.com
  @ IN CLONE vixie.com.
  @ IN CLONE vixie.sf.ca.us.
```

このようにTLDから異なるドメイン名に関しても完全なaliasを提供することを提案しています。もちろん、まだ単なる提案レベルであり、セキュリティ的な問題やaliasのループ等、気をつけるべき多くのことがあるとも報告されました。会場の雰囲気としては、あまり導入に前向きとは言えず、まだ多くの慎重な議論が必要である、という方向性になりました。

その他の議題としては、draft-ietf-dnsext-dnssec-bis-updates-10に関する報告が行われました。09との差分が報告され、DNSSECでの応答に関してもDO bitを設定することや、CD bitが設定された問い合わせに対しては、CD bitを設定した応答をすることが必須とされました。

さらに、2009年12月16日に発生した、in-addr.arpa zoneに対するDNSKEY問い合わせの増大に関する報告も行われました。これは、Fedora OSにあらかじめ設定されていたDNSKEYが有効期限切れになったことに起因して、世界中のFedora OSを利用したDNSリゾルバサーバから一斉に、in-addr.arpa zoneに対するDNSKEYの問い合わせが増大したという現象です。現在は収まりつつあることが報告されましたが、BINDへの改善要求も出され、DNSSEC導入に向けての一つの教訓となりました。

### ◆dnsop WG

dnsop WGの会合では、通常通りWG draftの状況報告や、関連draftの報告が行われました。まず、draft-ietf-dnsop-dnssec-dps-framework-01に関する報告が行われました。.SE TLDは、このフレームワークに従い、OpenDNSSEC[※1]を用いた運用を開始したと紹介されました。また、Root zoneの署名に関する事項も追記されています。

次に、draft-ietf-dnsop-dnssec-trust-history-01ならびに、draft-ietf-dnsop-rfc4641bis-02に関する報告が、Olaf M. Kolkman氏から行われました。これらの報告に関しては、多くの質問がなされ、本当に提案したものを検証しているのか、また変更の意図は何なのか等の質問が出されました。会場の雰囲気としては、あまり説得されていない感触で、さらなる検討を求める声が複数出された上で、より実践的な提案が求められる結果となりました。

その他のDNSSEC関連では、draft-morris-dnsop-dnssec-key-timing-02の報告も行われました。このdraftに関しては、いくつかの質問が出ましたが、特に大きな反論も無く、WG draftとして採用されました。

WG draft以外としては、draft-howard-isp-ip6rdns-03ならびにNSEC3 Hash Performance、IPv6 & recursive resolversに関する報告が行われました。

IPv6の逆引きに関するdraftでは、主にCPEの場合におけるIPv6逆引きに関する事項が変更されたとの報告がありました。会場からはあまり反応も無く、引き続き議論が行われる運びとなりました。

NSEC3 Hash Performanceでは、NSEC3が導入されたzoneにおいて、DNSSECのvalidatorやAuthoritativeサーバにどの程度負荷が増えるのかの評価結果が報告されました。結果として、validatorは鍵長が増えることが、iteration（反復）の回数が増えることよりも負荷に影響を与えることがわかり、Authoritativeサーバは鍵長に影響されず、iterationの回数のみに負荷が影響されることがわかったと報告されました。

IPv6 & recursive resolversでは、Yahoo!社のIPv6リゾルバに関する提案が行われました。これは、サーバにAAAAアドレスを付加した場合、クライアント側のIPv6環境が適切でなければ、IPv6 timeoutによるIPv4 fallbackが頻発するという問題に対する提起です。ISPのDNSリゾルバサーバが、クライアントからの要求に対してAAAAを返答するにあたって、そのクライアントが適切なIPv6環境にあるかどうか、すなわちIPv6の到達性があるかどうかを判断してからAAAAを返すようにしたらどうか、という提案です。BINDでは、9.7.0b2から導入されたdisable-aaaa-on-v4-transportというオプションによって、IPv6トランスポートによるDNS問い合わせの場合のみAAAAを返すという機能が追加されています。この提案に関しては、AAAAを返す場合が非常に限定される形となるため、やはりさまざまな意見が出されました。残念ながら時間が押していたため、議論に多くの時間を取ることができず、メーリングリストでの議論継続となりました。

### ◆その他のDNS関連活動と雑感

その他のDNSに関連した活動としては、DNSSEC ROOT Q+A BoFが開催されました。このBoFでは、Root zoneがDURZ（Deliberately Unvalidatable Root Zone）[※2]によって署名され、いくつかのRoot DNSサーバが署名されたRoot zoneを提供開始したため、その影響や各Root DNSサーバでの計測結果が報告されました。TCPによる問い合わせの増加や、UDPにおけるパケットサイズの増大が見て取れる結果となりました。

今回のIETFはアナハイムで開催され、近くにディズニーリゾートがあったため、多くの参加者はディズニーリゾートに入園もしくはダウンタウンディズニーにて食事したのではないかと思われます。普段は一人で来ている人が、子供を連れて来ている様子も見受けられました。

IETFの会合自体は、金曜日の午後まで埋められており、以前に比べて会合の数が増えてきた印象を受けます。また、"Bar BoF"と呼ばれる、時間外に企画される簡易的なBoFが多く行われ始めています。これはもともとホテルのBarにて、夜に関係者だけが集まって話を行う形態で行われていたものですが、最近は昼食の時間帯に部屋を取り、気軽なミーティング形式で行われるものも"Bar BoF"と呼ばれています。これに関しては賛否両論あるようで、IETFメーリングリスト上でも議論が行われました。できるだけ通常のBoFとして行い、早めに事前アナウンスを行った方が参加者にとってもうれしい、という議論がなされました。次回以降も、"Bar BoF"形式は継続されると思われます。

（JPNIC DNS運用健全化タスクフォースメンバー/
東京大学 情報基盤センター 関谷勇司）


■ IETFには、WebExを利用して遠隔からの会議参加が可能なWGもあります

※1 OpenDNSSEC
http://www.opendnssec.org/

※2 Deliberately Unvalidatable Root Zone（DURZ）
意図的に検証不可能としたルートゾーン、またはDNSSECの検証をできないようにするため、意図的に入れられたダミーの署名データのことを指します。

## ■ セキュリティ関連WG報告

セキュリティ領域においては、数多くのWGが開催されているため、それらすべてのセッションの内容を把握することが困難な状況です。そこで本稿では、会期中に議論されたセキュリティに関連したセッションの中から、認証や通信に特化した内容を議論するWGでの話題を中心に紹介することとして、IPSECME WG（IP Security Maintenance and Extensions WG）およびKRB WG（Kerberos WG）の動向について報告します。

### ◆IPSECME WG（IP Security Maintenance and Extensions WG）

IPSEC WGの後継として、2005年に同WGがクローズした後、必要になった拡張や既存ドキュメントの明確化などの議論を行うためのWGです。今回このミーティングは、2010年3月22日の午前9時から1時間半程度開催されました。参加者は、50人程度でした。

IPSECME WGにおいて、今回のIETFまでにRFCとして発行されたドキュメントや、RFCとして発行される直前のドキュメントを示します。

**＜RFCとして発行されたドキュメント＞**

**RFC 5658: Redirect Mechanism for the Internet Key Exchange Protocol Version 2（IKEv2）**
ノードからIPsecでの接続を他ノードへリダイレクトするための、IKEv2における拡張仕様を規定するドキュメントです。

**RFC 5723: Internet Key Exchange Protocol Version 2（IKEv2）Session Resumption**
現状のIKEv2では、VPN接続をサスペンドした後に、その接続を再開する際、IKEv2ネゴシエーションを再度実行する必要があり、ノードやVPNゲートウェイの負荷を増加させてしまう問題がありました。この問題を解決するために、最初のIKEv2認証完了時にチケットを発行することで再接続を簡略化するための拡張仕様を規定するドキュメントです。

**RFC 5739: IPv6 Configuration in Internet Key Exchange Protocol Version 2（IKEv2）**
RFC 4306では、IPv4のためのConfiguration payloadは規定されていますが、IPv6での機能を利用するまでには至りませんでした。このドキュメントでは、IPv6のために新規でConfiguration attributeを規定しています。

**＜RFCとして発行される直前のドキュメント＞**

- **Wrapped ESP for Traffic Visibility（draft-ietf-ipsecme-traffic-visibility-12）**
  Wrapped Encapsulating Security Payload（WESP）プロトコルを定義したドキュメントです。なお、Internet-Draft（I-D）のステータスは、RFC Editor queueです。

- **Heuristics for Detecting ESP-NULL packets（draft-ietf-ipsecme-esp-null-heuristics-07）**
  暗号化されたESPパケットからESP-NULLパケットを識別するための、ヒューリスティックについて記述したドキュメントです。I-Dのステータスは、IESG reviewです。

また、今回議論された検討項目は、以下の通りです。

- **IPsec High Availability and Load Sharing Problem Statement（略称:IPsec HA）**
- **An Extension for EAP-Only Authentication in IKEv2（略称:EAP-only authentication）**
- **Secure Failure Detection**
- **Password-Based Authentication in IKEv2: Selection Criteria and Comparison（略称:PAKE authentication）**

今回のミーティングにおいて、現在WGとして扱っている検討項目がRFC化され、完了フェーズに入りました。そのため、新規の項目として今回議論された中から、IPsec HA、EAP-only authentication、PAKE authentication の3項目がWGとしての検討項目に選定され、IPSECME WGのマイルストーンへ反映されました。

なお、詳細な情報やI-Dなどについてご興味がありましたら、以下のURLをご参照ください。

□IPSECME WG
http://www.ietf.org/dyn/wg/charter/ipsecme-charter.html

□第77回IETF IPSECME WGのアジェンダ
http://www.ietf.org/proceedings/10mar/agenda/ipsecme.txt

### ◆KRB WG（Kerberos WG）

KRB WGは、マサチューセッツ工科大学（MIT）が考案した、認証方式の一つであるKerberosプロトコルに関する新規仕様や機能拡張について、検討を行うWGです。このミーティングは、2010年3月24日の午後1時から2時間程度開催されました。なお、参加者は、30人程度でした。

**＜検討項目に関するドキュメントの状況＞**

KRB WGでの検討項目に関するドキュメントの状況は、次の通りです。

- **Problem statement on the cross-realm operation of Kerberos**
  IESGによって承認され、Editor's queueのステータスになりました。

- **A Generalized Framework for Kerberos Pre-Authentication**
  2010年4月8日に、IESG Telechatを実施することになりました。

・Using Kerberos V5 over the Transport Layer Security (TLS) protocol
IESG reviewというステータスです。

・Initial and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB)
数ヶ月前にWGとしてのLast Callが完了しました。

＜失効ステータスI-D＞

・Additional Kerberos Naming Constraints
・Anonymity Support for Kerberos

上記のI-Dについては、どちらもKRB WGでの検討項目ですが、失効しているステータスです。これらのような失効しているI-Dも、新たに更新版をアップロードすることで、ドキュメントのステータスをアクティブな状態に変更することができ、これにより他の議題と同様に議論を行うことができます。

Additional Kerberos Naming Constraintsについては、ドキュメントに存在している問題は解決されているため、最新版の投稿が行われるのを待つという状態であり、また、Anonymity Support for Kerberosは、いくつかの修正が残っている状況です。

＜Last Call中の検討項目＞

KRB WGでLast Callを行っている検討項目として、次の項目がありました。

・An information model for Kerberos version 5

複数のrealm（realmとは、ここではKerberosを使用したネットワークのこと）において、Kerberosを使用して認証できるユーザーやサービス固有の名前であるprincipalが、複数の名前を持ってしまうかもしれないことについて議論されていました。

＜新規の検討項目＞

KRB WGにおける新規の検討項目として、以下の議題について議論を行いました。

・Kerberos ticket extensions
・Deprecate DES support for Kerberos
・Kerberos Option for DHCPv6

この検討項目の中で、個人的に注目しているのは、Deprecate DES support for Kerberosです。その理由としては、暗号アルゴリズムの危殆化対策（暗号技術の世代交代）の対象アルゴリズムである、DES暗号の利用停止を行うために、WGとして検討が行われていることが挙げられます。暗号アルゴリズムを利用するプロトコルの危殆化対策を推進していくことは、プロトコルが利用している暗号アルゴリズムの安全性について強く意識することであり、利用者や実装者への注意喚起を促すのに良い機会にもなります。そのため、このような検討は多くのセキュリティ関連のプロトコルでも、積極的に行われてほしいと考えています。

＜今後の検討項目＞

今後のKRB WGとしての検討項目について議論しました。議題は、以下の通りです。

・Kerberos number registry to IANA
・KDC Schema
・Camellia Encryption for Kerberos 5

ここでは、上記の中から議論が盛り上がった話題について報告します。それは、NTT社とMIT Kerberos Consortiumの共同により提案が行われた「Kerberos 5 プロトコルにおいて、日本で開発されたCamellia暗号をCTS（Cipher Text Stealing）モードで利用するための仕様提案」についてです。現状のKRB WGにおいて、新規暗号アルゴリズムを追加することが、検討項目になっていないため、本提案をどのように扱うべきか議論が行われました。

結果的には、KRB WGにおける検討項目にはなりませんでしたが、Individual draftとして有識者のレビューを行うことになりました。この議論に関係した話題として、Kerberos 5プロトコルで利用する暗号モードとして、GCMモード（Galois Counter Mode）やCCM（Counter with CBC-MAC）モードに関する話題も検討される流れになっていました。

□KRB WG
http://www.ietf.org/dyn/wg/charter/krb-wg-charter.html

□第77回 IETF KRB WGのアジェンダ
http://www.ietf.org/proceedings/10mar/agenda/krb-wg.txt

（NTTソフトウェア株式会社 菅野哲）