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

ICANNと米国政府の関係 ～JPA終了に向けて～

ICANN（Internet Corporation for Assigned Names and Numbers）は、米国カリフォルニア州に設立された非営利法人で、現在ドメイン名、IPアドレス、AS番号などの、インターネット資源の管理を世界規模で行っている団体です。

ICANNの設立は、1998年10月にさかのぼります。この少し前、1997年から1998年頃にかけて、DNS※1の管理権限についての議論が、インターネット関係者の間で世界規模にわたって盛んとなりました。そのような動きの中で、米国商務省（DoC, Department of Commerce）が、「インターネットの名前およびアドレスの管理（いわゆる"ホワイトペーパー"）※2」を発行し、DNSの最終的な管理権限を米国政府が持つと主張しました。その一方で、DNSの管理は民間主導で行われることが望ましいとも述べました。その結果、ICANNが設立され、1998年11月25日にはICANNと米国商務省との間で覚書（ICANN/DoC MoU※3）が締結されました。その覚書の内容は、米国政府がDNSの管理をICANNに委託するものでした。

ICANN/DoC MoUはその後6回改訂され、それを引き継ぐ形で2006年9月29日にJPA（Joint Project Agreement「共同プロジェクト合意」の意）が締結されました。JPAでは、DNSに関する技術的調整を民間に移行するというポリシー目標を達成するために、両者に以下の点を求めています。

DoCに対しては、次の4点に関連する活動の実施が規定されています。

- 透明性と説明責任の提供
- ルートサーバのセキュリティの確保
- ICANNの政府諮問委員会（GAC）への関与
- 本覚書で規定される活動実績の監視

ICANNに対しては、DNSの管理を含め、2006年9月25日にICANN理事会決議で定められた次の10点にわたる活動の実施による責務の遂行、および毎年の活動状況報告の実施を定めています。

- セキュリティと安定性の確保
- 透明性の提供
- 説明責任の提供
- ルートサーバのセキュリティおよび運営者との良好な関係の維持
- トップレベルドメインの管理
- マルチステークホルダーモデルの発展
- GACを通じた政府の役割の確保
- IPアドレス資源分配についてRIR※4との協力維持
- 組織としての責任の維持向上
- 組織管理構造の評価改善

この基本的な構造は、ICANN/DoC MoUを引き継いでいます。JPAでは、さらにこれらの実現状況を確認するため、次の2点を規定しています。

a）民間への移行についての進捗を評価するための、DoC～ICANN間での定期的な会合の開催
b）中間評価の実施

b）については、DoCの一機関である米国商務省電気通信情報局（NTIA, National Telecommunications and Information Administration）が、ICANNのパフォーマンスについて、10項目からなる意見募集を2007年10月30日より2008年2月15日まで実施しました。その結果を受け、2008年2月28日にDoCにて公聴会が開かれました。

JPAの期限は2009年9月30日までとなっており、期限満了後については特に定められていませんが、JPA期限満了に向けて、NTIAより意見募集が2009年4月27日から6月8日まで行われ、合計87件の意見が提出されました。JPNICは、民間主導によるDNSの管理運営を長年支持してきた立場から、「米国政府が最終的に、DNSの技術的調整と管理の最終権限を、現時点における唯一の適切な主体であるICANNに移管することを望む」との意見書を提出しています※5。

その理由として、意見書では次の4点を述べています。

1.インターネットの発展のためには、「安定性」「競争」「民間によるボトムアップ調整」「さまざまな観点によるインターネットステークホルダーの参加」の全ての要素が不可欠である。
2.インターネットの進歩は、これまで民間主導によって管理されてきた単一の権威ルートDNSゾーンに強く依存してきたが、ICANNはその創立以来、ルートゾーンの一意性を保証するために重要な役割を果たしてきた。
3.ICANNの創立以来、ルートサーバ管理者との関係において、DNSルートゾーンの管理に支障を来すような問題は生じていない。
4.ICANNは、各国政府との対話を実現する仕組み・場を有している。

前記は、従来のJPNICの見解を踏襲したものです。また、意見書では移管の時期については触れませんでした。

JPNIC以外から提出された意見では、JPAの継続を求めるもの、JPA終了後は同様の覚書は不要とするもの、国際的な委員会による監督を求めるもの、JPAの期限満了後の仕組みについては触れていないものなどが見受けられました。

これとは別に、意見募集終了直前の6月4日に米国下院エネルギー・商務委員会通信・技術・インターネット小委員会にて公聴会が開かれました※6。これにはNTIAとICANNに加えて、レジストリ、レジストラ、通信企業、シンクタンクより参考人がそれぞれ1人ずつ出席し、議員からの質疑応答に答えていました。質疑応答の様子から、今回のJPA期間満了をもって移管するのではなく、JPAを継続すべきという意見を持っている議員がかなりいたように思います。

その後、2009年8月上旬に、米国下院エネルギー・商務委員会および同委員会配下の通信・技術・インターネット小委員会のメンバー計10名の連名で商務長官宛に、JPAの更新や数年ごとに失効するMoUの締結ではなく、米国政府とICANNの両者が署名する恒久的な手段が必要という内容の手紙※7が送付されました。

JPAが終了する2009年9月30日、ICANNとNTIAは「責務の確認（Affirmation of Commitments; AoC）」を締結したことを発表し、翌日10月1日より発効しました。AoCはJPAと比較して、1）期限が定められていない、2）これまで定期的にICANNから報告書を提出してDoCの評価を受けていた仕組みから、ICANNの自主性を尊重した評価の仕組みに移行する、3）政府のICANNに対する関与はGACを通じて行う、4）AoCは米国政府もしくはICANN一方の当事者の意思によりいつでも終了可能、という点が異なりますが、ICANNが米国に本拠地を置く一民間非営利団体として運営される点については従来と変わりません。

ICANNは、声明でこのAoCを「民間移行に向けた大きな前進である」としています。

参考:

■インターネット用語1分解説 ～ICANNとは～
http://www.nic.ad.jp/ja/basics/terms/icann.html

■2007年度インターネット資源の管理体制と活用に関する調査研究
第1部 インターネット資源の国際的な管理体制とその在り方に関する議論の動向
第2章 インターネット資源管理体制の現状及びそれに関する議論の動向
http://www.nic.ad.jp/ja/research/200807-dom/chapter1-2.pdf

■ICANNの歴史
http://www.nic.ad.jp/ja/icann/about/history.html

■JPA全文
http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/ICANNJPA_09292006.htm

■JPA中間評価コメント・公聴会会議録へのリンク
http://www.ntia.doc.gov/ntiahome/domainname/jpamidtermreview.html

（JPNIC インターネット推進部 山崎信）

※1 DNS（Domain Name System）
インターネットに接続されたコンピュータの情報（ドメイン名とIPアドレスの対応など）を提供する仕組みです。

※2 ホワイトペーパー
1998年6月5日に発表された、インターネットの管理体系に関する提案が記述されている、米国政府による文書の通称です。1998年1月30日のグリーンペーパーに対するコメントの一部を反映してまとめられました。ドメイン名やIPアドレスの管理の調整のために非営利法人を設立するとしています。グリーンペーパー、ホワイトペーパーという流れを受けて、ICANNという新しい組織が設立されました。

※3 ICANN/DoC MoU（Memorandum of Understanding）
ICANNと米国商務省（US Department of Commerce:DoC）が、DNSの技術的管理の権限を米国政府から民間セクター（ICANN）へ移行させるために、その方法や手順を両者が共同で策定することを目的として、1998年11月に締結した覚書です。当初は、権限移行の目標期限を2年後の2000年9月末としていましたが、その後数回にわたり覚書の改正・更新が行われ、最終的に2006年9月30日まで延長されました。

※4 RIR（Regional Internet Registry:地域インターネットレジストリ）
特定地域内のIPアドレスの割り当て業務を行うレジストリです。現在、APNIC、ARIN、RIPE NCC、LACNIC、AfriNICの五つがあります。JPNICのIPアドレスの割り当て業務は、APNICの配下で行っています。

※5 2009年6月8日にJPNICより米国商務省へ送付したコメント全文
http://www.nic.ad.jp/ja/pressrelease/2009/20090610-01.html

※6 ICANNの監督についての公聴会映像・資料
http://energycommerce.house.gov/index.php?option=com_content&view=article&\id=1642&catid=134&Itemid=74#toc2
（このページの最下部にストリーミングおよびダウンロードリンクがあります）

※7 米国下院エネルギー・商務委員会から商務長官あての手紙
http://www.internetcommerce.org/ica-files/ICANN-Locke%20letter%20080409.pdf

2009.6.21▶6.26

ICANNシドニー会議報告

［関連記事］P.28「第25回ICANN報告会レポート」

2009年6月21日から26日まで、オーストラリアのシドニーで第35回ICANN会議が行われました。前回、2009年3月のメキシコシティ会議では、新gTLD導入が大きなトピックとして挙がりましたが、今回のシドニーでもやはり大きな話題となりました。

本稿では、この新gTLD導入に付随する動きとして、実装勧告チーム(IRT:Implementation Recommendation Team)と呼ばれる、新gTLD導入で問題となる、商標など知的財産権に関する扱いを検討するチームについて、ご報告します。

◆IRT

IRT（Implementation Recommendation Team）を直訳すると、「実装勧告チーム」となりますが、具体的には、新gTLD導入の際に必要とされる、商標保護方策を検討し勧告することが、このチームのミッションです。IRTは、ICANN理事会が2009年3月のメキシコシティ会議において議決した、GNSOの知的財産権関係者部会（IPC:Intellectual Property Constituency）に対する要請によって招集されたものです※1。IPCは決議を受けて3月中にIRTを編成し、以降2ヶ月にわたって検討を重ね、5月末にまとまった最終案が、今回のICANN会議で報告されました。


■ flickrに投稿されている最終日に開かれた理事会の様子

最終案では、以下の五つの方策が提案されています。

1）今後、多数設立されると見込まれる新たなTLDに対する、商標保護手続きの負担を軽減するための仕組み。具体的には以下の三つ。

- TLDレジストリが共通して利用し、商標に関する情報のリポジトリとして機能する「IPクリアリングハウス」
- 一定数以上の国で保護されている商標（GPM:Globally Protected Marks）を登録する「GPMリスト（GPML）」
- GPM以外の商標を取り扱う「IPクレームハウス」

2）商標悪用によるドメイン名の利用を早期に凍結する「統一早期凍結システム（URS:Uniform Rapid Suspension System）」

3）商標権をクリアして登録されたドメイン名を使って、登録後に商標保護の観点で問題のある運用がなされることを防ぐ、「登録後紛争解決メカニズム（Post-Delegation Dispute Resolution Mechanism）」

4）.comなど、登録データが一元化されず分散管理されていると、情報更新が徹底されない恐れがあることから、新たなgTLDでは全て、レジストリの一元化管理（いわゆるThick WHOIS）を行うこと

5）TLD文字列の審査において、文字列の類似性だけでなく、聞こえ方や意味も含めた類似性判別を、審査のアルゴリズムに含めること

この報告書最終案は、2009年7月に世界4都市で行われる、ICANNコンサルテーションでも紹介され、意見聴取が行われた後、秋に公開が予定されているドラフトガイドブック（新gTLD導入に関するドラフト版RFP）第3版に盛り込まれる予定です。

◆その他

GNSOでは、支持組織全体の組織改革が大詰めを迎えています。組織改革により、GNSOは現存の部会（Constituency）をベースとした組織編成から、部会を包含する四つのステークホルダーグループ（SG）をベースとする組織編成へと移行します※2。これによって、部会を新規設置する自由を確保しながら、GNSO全体として、より広い関係者の参加と、バランスの取れた方針策定をめざしています。

- GNSO評議会
  - 契約者会議（Contracted Party House）
    - レジストリ SG（RySG）
    - レジストリ部会など
    - レジストラ SG（RrSG）
    - レジストラ部会など
  - 非契約者会議（Non-contracted Party House）
    - 商用 SG（CSG）
    - ビジネス、知財権、ISP部会など
    - 非商用 SG（NCSG）
    - 非商用ユーザ部会など

各SGのチャーターと、組織改革に伴うICANN付属定款の修正案は、最終ドラフトの段階にきており、意見募集に付されています※3。

また、新gTLDの追加やIPv6やDNSSECなどの普及によって、ルートゾーンの拡大が予想されますが、これに対するスケーラビリティ確保も大きな話題の一つであり、ワークショップが持たれました※4。

ICANN会議の最終日に行われた公開理事会会合では、22に上る決議が採択されましたが、その一つとして、新たな事務総長、Rod Beckstrom氏が指名されました※5。この決議の直後に、Beckstrom氏は壇上に上がり、インターネットにおけるICANNの重要性とその使命を強調し、事務総長としての決意を表明する演説を行いました。

（JPNIC インターネット推進部 前村昌紀）


■ flickrに投稿されている、理事会で演説をする新事務総長に指名されたRod Beckstrom氏

※1 JPNIC News & Views vol.626「ICANNメキシコシティ会議報告」
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol626.html

※2 Council Organization > Structure & Composition
http://gnso.icann.org/en/improvements/structure-en.htm
Council Organization > Stakeholder Group Process
http://gnso.icann.org/en/improvements/stakeholder-process-en.htm

※3 意見募集のページ
http://www.icann.org/en/public-comment/#stakeholder
http://www.icann.org/en/public-comment/#gnso-restructure

※4 Root Zone Scaling Study Group
http://syd.icann.org/node/3806

※5 Rod Beckstrom Named ICANN CEO
http://www.icann.org/en/announcements/announcement-26jun09-en.htm

2009.7.26▶7.31

第75回IETF報告

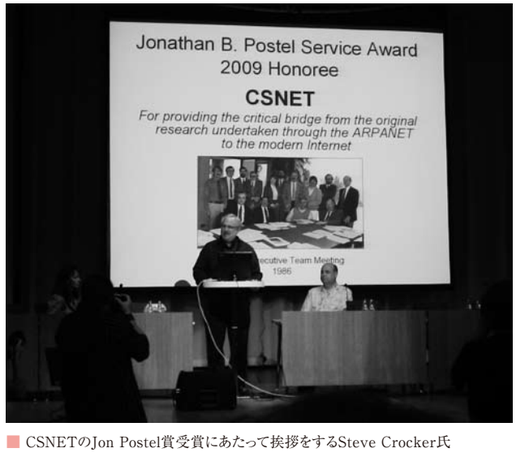
■ 全体会議報告

◆概要

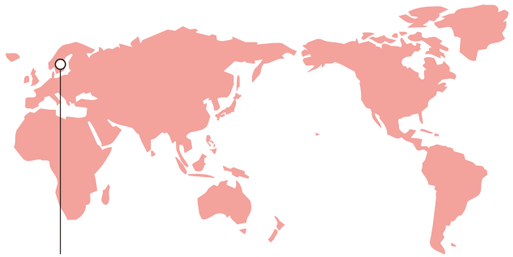
第75回IETFミーティングは、2009年7月26日（日）から31日（金）にかけて、スウェーデンのストックホルムにあるCity Conference Centreで行われました。数百名を収容できる大きなホールが二つある会議場で、ストックホルムの中心部から徒歩で10分ほどのところにあります。

7月のストックホルムは、午後9時頃になってからようやく夕暮れが訪れるほどに、日照時間が長い時期です。スウェーデンの代表的な料理であるスモーガスボード（日本で言うバイキング）は素晴らしく、また気温は摂氏15度から20度前後と快適であるため、午後7時半頃にミーティングを終えるIETF参加者には、魅力的な街であるという印象を残したに違いありません。

今回の参加登録者数は、若干少なめの1,084名（プレナリでの発表時）で、参加国数は50ヶ国でした。国別の内訳は、第1位がアメリカ（37%）、第2位が中国（9%）、第3位が日本（8%）、第4位がスウェーデン（8%）でした。隣の国のフィンランドは4%（40名）でした。



■ CSNETのJon Postel賞受賞にあたって挨拶をするSteve Crocker氏



Stockholm, Sweden

◆Operations and Administration Plenary

IETFの運営等に関する全体会議であるOperations and Administration Plenaryが、4日目の7月29日（水）に行われました。はじめに.SEのホスト・プレゼンテーションが行われ、続いてJon Postel賞の発表、IETFチェアによる活動報告等があり、最後に会場の座席側に設置されたマイクを使って意見交換を行う、オープンマイクロホンが行われました。

.SEは、スウェーデンの政府機関であるNational Post and Telecom Agencyを監督官庁とする非営利組織で、スウェーデンにおけるccTLD（.se）レジストリです。ホスト・プレゼンテーションでは、2003年以降急激に増加し2009年に88万に達しているSEドメイン名の登録状況や、5万ドメインへの導入を目標にDNSSECを推進するという、2009年の活動が紹介されました。IETFのローカルホストを務める理由として、DNSSECの機運を高めることや、スウェーデンの若い人がIETFに参加しやすいようにする、といった点が挙げられました。

2009年のJon Postel賞は、米国のthe Computer Science Network（CSNET）が受賞しました。CSNETは、1981年に、米国NSFの資金により設立され、その間に165の学術組織や政府組織をARPANET※に接続しました。当時、5万人以上の研究者や学生が利用したとされています。CSNETは、当初NSFの研究ネットワークという位置付けであったARPANETについて、CSNET自らが運営する形にすることをNSFと合意しました。表彰の理由は、オープンなネットワークを学術コミュニティにもたらすとともに、ARPANETを現代のインターネットに変容させていくことに貢献したこと、とされています。

IETFチェアによる活動報告では、IETFの概況などが報告されました。現在112のWGがあり、前回のIETF-74以降90のRFCが出ました。新たなInternet-Draftは517作成されました。次回のミーティングについては、当センターの理事でもある村井純氏より広島について紹介がありました。

この他の主な報告事項を以下にまとめます。

- RFCにおけるAbstract（概要）を入れる位置の変更

以前はCopyright Notice（著作権について）の後だったAbstractが、Titleの直後に変更されました。これにより、最初のページにAbstractが来るようになります。

- IETFのトップページ

IETF Webトップページ<http://www.ietf.org/>のデザインが変わりました。詳細なメニューがトップページから利用できるようになりました。

- DNSSECの導入

ietf.org、iesg.org、iab.org、irtf.orgにDNSSECが導入されました。

- Nomcom（Nomination Committee）ドキュメントの更新

前回、第74回IETFのPlenaryでの議論を受けて、Nomcomに関するドキュメントが更新されました。

■ 第75回IETFの会場となったCity Conference Centre

draft-dawkins-nomcom-dont-wait-04（IESG承認済み）には、その年最初のIETFミーティングから、4週間後にNomcom Chairが決まっていない場合には、IETF Executive Directorが、IESGとIABの候補者を伝える役割を担うことなどが加わりました。

またdraft-dawkins-nomcom-openlist-05（コンセンサス確認中）では、IESGとIABの候補者のリストを公表することで、ロビー活動が行われてしまう現状と、懸念をまとめた節が設けられました。

最後に、2009年6月3日に他界した、IETF最初のExecutive DirectorであるSteve Coya氏に対して、黙とうが捧げられました。オープンマイクロホンでは、ドキュメントのレビュープロセスや、IETF-announceメーリングリストで流すべきメールの種類に関して議論が行われました。

◆Technical Plenary

技術的な議論を行う全体会議のTechnical Plenaryは、7月30日（木）に行われました。はじめにIRTFとIABのチェアから活動報告があり、続いて“Network Neutrality”、すなわちネットワークの中立性に関する議論が行われました。最後にオープンマイクロホンが行われました。

IRTFでは、Public Key Next-Generation Research Group（PKNG）という新たなリサーチグループが設立されました。新たな証明書フォーマットやセマンティクスを検討しており、PKIXに代わる公開鍵サービスのリサーチを行うようです。Paul Hoffman氏がチェアを務めます。この他に、現在活動中のHost Identity Protocol（HIP）と、Internet Congestion Control Research Group（ICCRG）について紹介されました。

IABの活動報告では、ドキュメント化活動の状況が報告されました。以下にまとめます。

- RFC化されたもの

  - Principles of Internet Host Configuration（RFC5505）
  - Design Choices When Expanding DNS（RFC5507）

- 議論を進めているもの

  - IAB thoughts on IPv6 Network Address Translation, draft-iab-ipv6-nat-00

- P2P Architectures
  draft-iab-p2p-archs-02
- Defining the Role and Function of IETF Protocol Parameter Registry Operators
  draft-iab-iana-04
- Evolution of the IP model
  draft-iab-ip-model-evolution-01

ネットワークの中立性に関する議論は、問題のないコンテンツやアプリケーションが制限されることを避けるために、IETFとして技術的にできることは何か、という観点で行われました。

QoS（Quality of Service）、DoS（Denial of Service） attack、ウイルス、スパム、輻輳（congestion）が挙げられ、ネットワークの拡張に伴って必要になる"制限するための機能"によって、インターネットというアーキテクチャが備えている、自由な通信プラットホームであるという側面や、アプリケーションを作り直さなくてもコミュニケーションの範囲を広げられるという思想、そのコミュニケーションによって醸成される文化やエコノミクスが失われかねないといった危機感が指摘されました。

一方、SIGCOMM 2002に投稿されたDavid Clark氏らによる論文"Tussle in Cyberspace"では、「Tussle（奪い合い）を内包することはネットワークの発展に不可欠である」と述べられている点についても議論されました。プロトコルを使って通信サービスを実現する過程で、通信業者同士のTussleを吸収するために、元々は無かった機能が検討され標準化されていった事例が紹介されました。


■ Plenary（全体会議）の様子

会場では、インターネットにおいて、通信路は高度な処理をするのではなく、通信データの伝送に徹するべきであるが、DoSの回避は重要であるといった点が確認されたり、遅延や再送をエンドユーザーがわかりやすいように可視化してはどうか、といった意見が出されたりしていました。引き続くIABオープンマイクロホンでは、逆にIABとして何ができるか、という疑問が投げかけられ、同時にTussleに関する認識を共有しやすいよう、より読みやすくすべきだといった意見が挙げられていました。

◆IETFミーティングに合わせて行われたイベント

ミーティング期間に合わせて、以下のイベントが行われました。DNSSECに関するイベントが二つあり、SEのDNSSECを推進したいという意向が感じられました。

- ISOC Panel: "Securing the DNS" - 7月28日（火）

会場近くのClarion Sign Hotelで7月28日（火）に行われたISOC主催のイベントで、前DNSEXT WGチェアのOlaf Kolkman氏（NLnet Labs）らをパネリストに迎えてパネルディスカッションが行われました。モデレーターはISOCのLeslie Daigle氏が務めました。

Verisign社のMatt Larson氏は、DNSSECが.eduに導入済みであることを述べた後、.netは2010年末に、.comは2011年初頭に導入する計画を発表しました。またルートゾーンへは、2009年中に導入するべく活動することを発表しました。

- OpenDNSSEC technical preview release party - 7月30日（木）

OpenDNSSECは、.SEやNLnet Labs等が参画しているOpenDNSSEC Projectによって開発されている、DNSSEC対応用のソフトウェアです。UnboundやBIND9に合わせて使うことができるソフトウェアで、BSDライセンスで配布されています。

これは技術的なプレビューリリースを記念したパーティーで、7月30日（木）の20時より、市内にあるカフェバーの一部を借り切って行われました。

- RIPE NCC Routing Registry Training Course - 7月31日（金）

RIPE NCCによる、ルーティングレジストリ（IRR）のチュートリアルです。最終日の7月31日（金）、会場近くのRadisson SUS Royal Viking Hotelで、9時から17時半まで行われました。通常、RIPE NCCのメンバーであるLIRしか参加できないトレーニングコースですが、今回はIETF参加者にもアナウンスされ、登録無しで参加することができました。

チュートリアルには、ルーティングセキュリティの権威であるSandra Murphy氏をはじめ、SIDR WGで活発なRoque Galiano氏（LACNIC）や、AfriNICの技術者が参加していました。コースの合間には、IPレジストリのルーティングセキュリティへの関与に対する考え方や、Randy Bush氏が行っている実験の経路情報への影響、IRRの登録のセキュリティに関するディスカッションで盛り上がり、主催者と参加者の両方にとって貴重な時間となりました。

◇　　◇　　◇

次回の第76回IETFミーティングは、広島で行われる予定です。

IETFは、単にプロトコルを策定する会議であると考えられがちです。しかし、その背景には国際的情報通信ネットワークの技術的な在り方を議論によって導き出し、ドキュメント化していくという素晴らしい文化があります。この文化こそがインターネット技術を発展させる礎であると思います。

WGチェアの指示に従って行われる、ラフで、しかし論理的なディスカッションは、英語でのディスカッションに慣れていない方にとっては、ついていくことが難しいと感じられるものかもしれません。

しかしひとたび飛び込めば、私達の検討や考察にさまざまな国から集まった人々が耳を傾け、もっともな意見であれば共感し、文書化して残していこうとするグループであることに気づくと思います。ビジネスがグローバル化したと言われる現代の、特に若い技術者にとっては、こういった経験は貴重なものではないでしょうか。

業務や研究に関係のあるWGの趣意書やドキュメントをご覧になり、実際に会場に足を運んで国際的に活動しているインターネット技術者の文化に触れていただければと思います。

□第76回IETFミーティング

日時:2009年11月8日（日）～13日（金）
場所:広島県広島市 ANAクラウンプラザホテル広島
ホスト:WIDEプロジェクト

□IETFに関する情報

- The Internet Engineering Task Force （IETF）
  http://www.ietf.org/

- Working Group Charters （WGの趣意書）
  http://www.ietf.org/dyn/wg/charter.html

- IETF Meetings
  http://www.ietf.org/meeting/
  "Register"から参加登録できます。

（JPNIC 技術部/インターネット推進部 木村泰司）

※ **ARPANet（Advanced Research Projects Agency Network）**
1969年にアメリカ国防総省高等研究計画局（ARPA）が開始した、コンピュータのネットワークです。この研究から生まれた「UNIXコンピュータ同士をTCP/IPで相互接続する」という形態は現在のインターネットの原型となりました。

■ DNS関連WG報告

◆dnsop WG（Domain Name System Operations WG）報告

dnsop WGの会合は、月曜日の朝一番の時間帯にて開催されました（2009年7月27日）。会合の冒頭では、いつも通りInternet-Draftの状態確認が行われ、今までのInternet-Draftには特に大きな進展はないことが確認されました。

まず、draft-morris-dnsop-dnssec-key-timing-00に関する報告と議論がなされました。このInternet-Draftは、RFC4641を拡張したものであり、主にDNSSECにおける鍵更新のタイミングについて、より詳しく提案したものです。前回のIETFにおいても発表されたInternet-Draftであり、WG draftとするかどうか、議論が行われました。結果、数式が多く読みにくいという意見も出され、新たなバージョンが発行されるのを待つことになりました。

次に、draft-wijngaards-dnsop-trust-history-00について、発表と議論がなされました。これは、DNSSECで検証を行う際の起点となるTrust Anchorを更新するにあたって、期限切れとなったTrust Anchorを、DNSのプロトコルを用いて更新する仕組みを提案したものです。発表後の議論では、RFC5011との違いが取り上げられ、鍵やDNSの更新がどのぐらいの頻度で行われるか、過去の鍵情報はどの程度まで保存しておけばよいのか等、議論されました。過去の鍵を保存する方法のみに特化した方がよいのでは、という意見も出され、メーリングリストでの議論が続けられることとなりました。

さらに、draft-livingood-dns-redirect-00について発表がなされました。これは、DNSの応答を用いて、ユーザーを別のWebページに誘導するような仕組みについて、そのガイドラインを述べた文章です。DNSによる誘導は、DNSSECとの相性や、存在しない名前を入力した場合にもNXDOMAINが返らない等、セキュリティ上の問題を抱えるため、推奨すべきではないとの意見も出されました。このInternet-Draftも、引き続きメーリングリストにて議論が行われることとなりました。

他に特筆すべきものとしては、draft-ljunggren-dps-framework-00です。これは、DNSSECを用いてTLDゾーンを署名するにあたって、レジストリが担う役割を明記した文章です。会場からは、有用でありWG draftとすべきだとの意見が出ました。次の更新を待って議論が続けられることとなりました。

今回の会合は、DNSSECに関連するInternet-Draftの議論が多く、あらためてDNSSECが導入されつつあるという現状がうかがえました。

◆dnsext WG（DNS Extensions WG）報告

dnsext WGの会合では、主にforgery resilience※に関する議論と、EDNS0に関する議論、ならびに毎度のことになりますが、WGのチャーターに関する議論が行われました。

まずforgery resilienceに関する議論では、今までの議論の経緯がまとめられ、現在出ている提案が列挙されました。DNSへの詐称攻撃を防ぐために、ポート番号やクエリID等のランダム性を増加させる手法としては、DNS Pingやdns0x20、RTT Bandingといった手法が提案されています。また、DNSリゾルバサーバの挙動としては、キャッシュの上書き防止や、CNAME/DNAME連鎖の確認、TCPによる再問い合わせ等が提案されています。これらをまとめたものとして、draft-barwood-dnsext-fr-resolver-mitigations-08とdraft-wijngaards-dnsext-resolver-side-mitigation-01が提案されており、議論の最後に、どちらの提案をWG draftとして採用するかの決がとられました。結果として、両方の提案をマージして一つのWG draftとする方がよい、という意見が多数を占め、著者と調整することとなりました。ただし、会場の雰囲気としては、これらの手法は少なからずDNSの既存実装に手を入れる必要があるため、それほど積極的にやらなくてもよいのではないか、という意見もかなり出ていました。

次にEDNS0に関する議論が行われました。

draft-ietf-dnsext-rfc2671bis-edns0-02ならびにdraft-gudmundsson-dnsext-setting-ends0-do-bit-00が取り上げられていました。前者は主にEDNS0のバッファサイズとMTUに関する問題点を取り上げた文書であり、後者はDNSSECにおけるペイロード増大に関して、DNSバッファサイズとの関連を述べた文章です。draft-ietf-dnsext-rfc2671bis-edns0-02では、EDNS0によって通知されるバッファサイズが、必ずしもMTU値と一致していないため、経路途中にPMTUができないルータ等が存在すると、UDPパケットのフラグメントが行われず、結果としてEDNS0のパケットが届かない、という問題を指摘しています。これに対して、DNSバッファサイズを減らして再試行するようEDNS0の仕様を変更するという提案を行っています。

draft-gudmundsson-dnsext-setting-ends0-do-bit-00では、リゾルバサーバが扱うことのできるDNSバッファサイズが1,220Bytesより小さい場合には、DO（DNSSEC OK bit）を有効にしないよう推奨する提案を行っています。これらに関しては、引き続き議論が行われることとなりました。

その他には、behave WGのinternet-draftである、draft-ietf-behave-dns64-00におけるDNSSECの扱いに関する報告や、DNSSECにて利用される、新たな暗号アルゴリズムに関するinternet-draftの紹介がありました。dnsop WGと同様に、DNSSECに関連する議論が、時間の多くを占める結果となりました。

（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）

■ City Conference Centre内の様子

※ **forgery resilience**
RFC5452にて述べられている、DNSへの詐称パケット攻撃に対する対策。

■ IPv6関連WG報告

スウェーデンの首都ストックホルムにて、2009年7月26日から31日まで、第75回のIETFが開催されました。世界的な景気の低迷、および米国以外での開催ということで、今回も参加人数の減少が懸念されていましたが、前回のサンフランシスコとほぼ同数の1,124名の参加となりました。また、国別の参加人数は、日本を抜いて中国が第2位となっています。会議中も多くのワーキンググループ（WG）で、中国の方がプロトコルの提案をしたり、活発に意見を述べる等、目立っている印象がありました。

本稿では、IPv6に特化した内容を議論するWGでの話題を中心に紹介します。

◆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、水曜日の午後最初のコマにて開催されました。

まずは、いつもの通り、チェアより今回のミーティング議題の確認および、WGで取り組み中の四つの文書（フラグメント重複問題、ノード要求仕様、アドレス選択解法、IPv6サブネットモデル）に関する状況紹介がありました。また、このうち、ノード要求仕様、アドレス選択解法の二つについては、議論も実施しました。

今回のミーティングでは、

1.ノード要求仕様文書に関する議論
（draft-ietf-6man-node-req-bis）
2.ルータ広告メッセージにおける回線識別子
（draft-krishnan-6man-rs-mark）
ノード広告メッセージにおける回線識別子
（draft-li-6man-ns-mark）
3.IPv6アドレスのテキスト表記方法
（draft-kawamura-ipv6-text-representation）
4.UDPのトンネルトランスポートモード
（draft-fairhurst-6man-tsvwg-udptt）
5.アドレス選択問題について
アドレス選択ポリシー間の矛盾解決
（draft-arifumi-6man-addr-select-conflict）
6.アドレス選択デザインチーム議論報告
（draft-chown-addr-select-considerations）

といった内容が議論されています。

上記のうち、1、2、3、5につき、簡単に紹介します。

1.ノード要求仕様文書に関する議論

RFC4294として発行されている、IPv6ノードの要求仕様文書に関する改版提案に対する議論です。しばらく議論が止まっていましたが、近頃、再開されています。CPEルータのような、ルータとしてもホストとしても動作するノードをどう扱うかといった問題や、MIPv6の経路最適化を「SHOULD（すべき）」としている現在のRFCの記述は、経路最適化の実装が少ないことなどから適切でない、といった意見が出されました。また、この文書の位置付け（ステータス）に関する議論も実施されています。元のRFC4294は「Informational」というステータスですが、これをより強いものにすべきではという意見がある一方、他のRFCで規定されている以上の制限を付けるべきではないという意見もあり、内容とは独立して議論を実施することになっています。

2.ルータ広告メッセージにおける回線識別子／ノード広告メッセージにおける回線識別子

一部のADSL等では同じセグメント上に複数の顧客が存在することがあり、顧客ごとに別の広告メッセージを返答することができないため、メッセージを識別するための回線識別子オプションを新設しようという提案です。これに対し、ユニキャストの広告メッセージは使えないのか、CPEルータを設置してDHCPv6-PDを使用すべきだといった意見や、そもそも同じセグメント上に複数の顧客が存在するようなモデルがおかしいのであり、VLANで顧客ごとにセグメントを分けるトンネルリンクを使用するといった手法を採るべきだ、という環境自体に対する意見等、提案に否定的な意見が多く出されました。

3.IPv6アドレスのテキスト表記方法

IPv6アドレスの表記方法はRFC4291で規定されていますが、現在の規定では、同じアドレスが複数の別表記で記述可能となっています。このためテキストデータやアドレス管理表から特定のアドレスを検索する場合や、電話サポート等でアドレスを知らせる場合に誤解が起こる可能性があるため、表記方法を統一しようという提案です。2009年7月に開催されたJANOG24や、JPOPM16でもプレゼンテーションがありました。趣旨に同意する意見が多く、会場ではWGとして取り扱うべきだという意見が多数を占めました。そのため、MLにて、WG文書として扱うべきかの合意を確認することになりました（2009年8月10日現在、ML上で数名の賛同が得られています。）

5.アドレス選択問題について（アドレス選択ポリシー間の矛盾解決）

前回、前々回のIETFに引き続き、IPv6ホストがアドレスを複数持っている場合の、アドレス選択のあり方について、その検討状況の報告がありました。今回は特に、複数の上流から矛盾するアドレス選択ポリシーが配布された場合に、そのポリシーをどうマージするかに特化した提案が実施されました。時間の関係で、議論はそれほどできませんでした。こちらの提案についてもチェアから参加者に対して、WGとして取り組む必要のある内容かとの問いかけがありましたが、提案ドラフトを読んでいる人の数が多くなかったため、MLにて確認をすることになりました。

□6man WG
http://www.ietf.org/dyn/wg/charter/6man-charter.html

□第75回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/75/agenda/6man.html

◆v6ops WG（IPv6 Operations WG）

v6ops WG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。以前のダブリンでのIETFから、移行技術の標準化についての議論はbehave WGで実施されることになり、内容が薄くなるかと思われました。しかし、今回は火曜日の午後全ての時間（3コマ）を埋めるほどの提案があり、引き続き活発な議論が実施されました。

今回の議論内容は、次のようになっています。

1コマ目:ディプロイメントに関する問題
- Internet Exchange（IXP）でのIPv6ディプロイメント（draft-ietf-v6ops-v6inixp）
- IPv6サービスとIPv6/IPv4間通信を実現するハイブリッドISPフレームワーク（draft-xu-v6ops-hybrid-framework）
- IPv6移行のための段階的キャリアグレードNAT（CGN）導入（draft-jiang-v6ops-incremental-cgn）
- Teredoクライアントに対するICMPv6エコー応答生成（draft-denis-icmpv6-generation-for-teredo）
- 非決定的なIPv6トンネルの弊害（draft-vandevelde-v6ops-harmful-tunnels）
- IPv4サービスプロバイダネットワークでのIPv6提供（draft-townsley-ipv6-6rd）

2コマ目:CPEルータに関する問題
- 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）
- IPv6 CPEルータのユースケースと要求仕様（draft-donley-ipv6-cpe-rtr-use-cases-and-reqs）
- IPv6 CPEルータ推奨機能（draft-ietf-v6ops-ipv6-cpe-router）

3コマ目:その他の問題
- IPv4とIPv6のGreynets（draft-baker-v6ops-greynet）
- IPv6エニーキャストを利用した負荷分散と疑似モビリティ（draft-luo-v6ops-6man-shim6-lbam）

この中で、1コマ目、2コマ目の議論内容について紹介します。

1コマ目の「ディプロイメントに関する問題」セッションでは、IPv6導入モデルに関する提案、移行プロトコルや移行技術に関する提案／問題が議論されました。

IXPにおけるIPv6導入モデルでは構築例として、/47相当の空間を取得し、片方の/48をグローバルインターネットに経路広告せずに、IXP内部的に利用する方法に関しての議論等がありました。IXP文書はレビュー後、WGラストコールが実施される予定です。また、ISPにおけるIPv6導入手法として、IPv4/IPv6変換の導入や、CGNの導入とIPv4上でIPv6をトンネルで提供する手法から、IPv6上でIPv4を提供するモデルへの移行といったモデルの提案等が実施されました。現在、変換プロトコルはbehave WGで、トンネルプロトコルはsoftwire WGで議論されていることもあり、この文書をv6ops WGで扱うべきかという議論になりましたが、WGの文書として議論を継続することになっています。

■ 会場内に設置された次回IETF(広島開催)のブース

Teredoに関する問題提起では、Teredoは通信確認にICMPv6を利用しており、IPv4/IPv6トランスレータが入った環境や、ファイアウォール等でICMPv6が落ちた場合に通信できなくなるため、その改善提案が行われました。これに対しては、Teredo通信より、IPv4通信を優先するべきである等の意見が出され、ML上で継続議論になりました。また、Teredoのようなトンネルを用いてIPv6通信を実現している場合に、そのトンネルが複数のプロバイダをまたいだりする際、通信品質の担保ができなくなる等の問題があるため、このような非決定的（non-deterministic）なIPv6トンネルは問題であるという提案も実施されています。この提案に対し、問題はわかるが、6to4などは既に広くディプロイしており、利用を停止することは困難であるという意見や、そもそも「非決定的（non-deterministic）」の定義はどうなのか、といった議論となりました。

2コマ目の「CPEルータに関する問題」では、CPEの要求仕様や、CPEに載せるべきセキュリティ機能の議論が実施されました。CPEの要求仕様に関する議論では、上流からDHCPv6-PDで受け取ったプリフィクスを下流に委譲する手法や、経路の設定等が議論になりました。セキュリティ機能の提案では、IPv4と同じセキュリティ概念をIPv6に持ち込むことの是非や、CPEルータがどのような機能をどの程度持つべきか、といったことが長時間議論されました。特に、ドラフトで機能要件として挙げている、トンネルパケットの扱いについては激しい議論になり、MLで継続議論となりました。IPv6 CPEルータ推奨機能の議論では、同様の議論をブロードバンドフォーラムや、ケーブルLab、3GPP等でも実施しているため、他団体の筆者を加え、内容をアップデートする方向で調整することになりました。

□v6ops WG
http://www.ietf.org/dyn/wg/charter/v6ops-charter.html
http://www.6bone.net/v6ops/

□第75回 IETF v6ops のアジェンダ
http://www.ietf.org/proceedings/75/agenda/v6ops

◆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の高さからIPv6/IPv4変換についての議論も行われています。今回は、そのIPv6/IPv4変換を中心にさまざまな提案がなされた関係で、二つのスロットにわたってセッションが行われました。

- draft-ietf-behave-v6v4-framework-00
- draft-ietf-behave-v6v4-xlate-00
- draft-ietf-behave-v6v4-xlate-stateful-01
- draft-ietf-behave-dns64-00

IPv6/IPv4変換に関するトピックとしては、上記Internet-Draftに関する議論が行われ、前回からの検討状況のアップデートについて報告がありました。

この一連のInternet-Draftについての目新しい変更点としては、前回ご紹介した※1NAT66と呼ばれるIPv6からIPv6へのNATの提案でも触れられていた、checksum neutralityについての言及があったことが挙げられます。checksum neutralityとは、アドレス変換の前後で上位層（主にトランスポート層）のヘッダーで利用されるチェックサムの値に影響を与えないようにする、というものです。これは変更前後のアドレス対をうまく選ぶことで実現が可能です。例えば16ビットのCRCチェックサムを利用しているTCPでは、変換後のアドレスのうち16ビットをうまく選ぶことで、チェックサムを不変にしたままNATをすることができます。

このchecksum neutralityによるメリットとしては、今後新たなトランスポート層プロトコルが出現した際にも、同じチェックサム計算方式を使ってさえいれば、NAT装置をその新プロトコルに対応させる必要なく利用できる、ということがあります。しかし、IPv6/IPv4変換の場合は、IPv6とIPv4でUDPチェックサムの扱いが異なる、つまりIPv6ではUDPチェックサムが必須となったことから、結局再計算をせざるを得ないケースが出る、等の議論が行われました。

- draft-thaler-behave-translator-addressing-00

また、behaveのチェアを務めるDave Thaler氏からは、IPv6/IPv4変換の際に用いるダミーアドレスとして、どのようなアドレスが望ましいか、という検討の発表がありました。

IPv6からIPv4変換を行う際のダミーアドレスには、ダミーIPv6アドレスの、どの部分にIPv4を埋め込むべきか、またダミーアドレスとして用いるアドレスは、各サイトで取得したアドレスを使用するべきか、それともwell-knownなプリフィクスを定義すべきか、またプリフィクス長はどの程度必要か、といったさまざまな角度から、またそれぞれのIPv6/IPv4変換シナリオについて分析した結果が報告されました。

その他にも、LSN（Large Scale NAT）と呼ばれるISP等でNATを行う方式や、そのNAT装置の信頼性をより高めるための方式、そしてNATが介在している場合でも、アプリケーションが通信相手を正しく認識するための方式等、さまざまな提案があり、議論が行われました。

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

□第75回 IETF behave WGのアジェンダ
http://www.ietf.org/proceedings/75/agenda/behave.html

◆softwire WG（Softwires WG）

softwire WGでは、トンネルを用いてIPv4 over IPv6、またはIPv6 over IPv4通信を実現する方式を検討するWGです。基本的にはDS-lite（Dual stack lite）と呼ばれる方式にまとまりつつあるのですが、今回は6rd（もともとはIPv6 Rapid Deploymentの意）という、IPv6 over IPv4通信を実現する方式についての議論も行われました。

- draft-townsley-ipv6-6rd-00

簡単に説明すると、6to4というIPv4グローバルアドレスを保持しているサイトにIPv6アドレスを自動割り当てし、IPv6接続性を自動的に提供する方式があるのですが、これを特定のサイト内で完結させ、管理性を高めた方式がこの6rdとなっています。実際にもともとの提案者のRemi Despres氏は、FREE TelecomというフランスのISPにおいて、商用のIPv6接続サービスを提供するための方式として使用しているとのことです。

ここ最近、IPv6の普及度を調査したレポートなどにおいて、IPv6の通信品質の悪さが取りざたされており、その原因が6to4やTeredo等の、IPv4ネットワーク上で提供されるIPv6トンネル接続方式にあるとされています。そこで、6to4やTeredoといったプロトコルを廃止しよう、またはより信頼性を向上させようという提案がなされています。本方式はこういったIPv6への移行のためのプロトコルではなく、より管理性と品質の高いIPv6接続サービスを提供するための方式として提案されています。こういった背景から、6rdは比較的大勢のサポート獲得に成功しており、WGアイテムとなる予定ですが、まずその前にWGのチャーターを変更する必要があり、それを待ってWGアイテムとして公開される予定になっています。

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

□第75回 IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/75/agenda/softwire

◆homegate bar-BoF

ホームネットワークにフォーカスし、ユーザーエクスペリエンスの向上、セキュリティの維持、新機能の導入、という三つのテーマを扱うhomegate WGの設立をめざす動きがあります。今回は、公式なBoFとしてスロットを申請していたのですが、主にスコープに不明確な部分があるとの理由から、開催には至りませんでした。そこで、bar bof、すなわち非公式BoFという形で、有志によりIETFミーティングの設定時間外にミーティングが行われました。

そこで検討されたトピックとしては、DNSSEC、IPv6/DHCPv6、ECN/RED、Multicast、Security、Firmware更新、ゼロコンフィグ、デバイスの管理方法、複数サブネット、といった項目がありました。

それぞれのトピックについて、興味を持っている人がどれぐらいいるかについて確認していくという形で進められましたが、どのトピックも扱う必要が無いと感じている人は少数で、どれもこれも扱うという流れになってしまったようです。

また、さらにはWG化された場合のアウトプットとして、ホームゲートウェイの要求仕様書などのようなものができた場合には、v6ops等のIETF内の他のWGで既に部分的に行われている活動とはどうすみ分けがされるのか、またIETF以外にもさまざまなSDO（Standards Developing Organization）で取り扱われている仕様書との関係はどうなるのか、といった方向に話は発散する一方となってしまい、なかなかWGのスコープを明確に定めるのには至らないという様子でした。

homegateのセッションのスライド等はIETFのWebサイトから取得できるようにはなっていませんが、メーリングリストが開設されており、依然活発な議論が行われているようです。次のURLから参加できますので、ご興味のある方はぜひご参加ください。

□homegate ML
https://www.ietf.org/mailman/listinfo/homegate

第75回IETFミーティングの各種情報は、以下のURLより参照可能です（議事録も今後掲載される予定です）。

□全体プログラム、WGアジェンダ、発表資料
https://datatracker.ietf.org/meeting/75/materials.html

□録音
ftp://videolab.uoregon.edu/pub/videolab/media/ietf75/

（NTT情報流通プラットフォーム研究所 藤崎智宏）
（NTT情報流通プラットフォーム研究所 松本存史）

※1 JPNIC News & Views vol.637
第74回IETF報告 [第5弾] IPv6関連WG報告 ～v6ops WG、6ai BoFについて～
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol637.html

■ セキュリティ関連WG報告

第75回のIETFは、スウェーデンのストックホルムにて、2009年7月26日から31日まで開催されました。今回の参加者は、50ヶ国1,084人でした。これは、直近のヨーロッパで開催された第72回IETF(48ヶ国1,183人)と比較すると、2ヶ国増99人減という結果です。

毎回IETFでは、セキュリティに関連した話題が多くのWG(今回は15セッション)で議論されており、幅広い領域のセッションが開催されているため、全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Security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WGでの話題を中心に紹介します。

◆krb WG(Kerberos WG)

krb WGは、認証方式の一つである、マサチューセッツ工科大学(MIT)が開発したKerberosについて、新規仕様や実装のための検討を行うWGです。

今回のミーティングは、2009年7月31日に開催され、参加者は30人程度でした。最初にチェアから、WG文書のステータスおよび本ミーティングのアジェンダについて報告がありました。

■ IETF会場近くのホテルで行われたRIPE NCCのRouting Registry Training Course

今回のミーティングで発表された提案は、次の通りです。

・Preauth framework
・Kerberos hash Update
・DHCPv6 Kerberos option
・IA-Kerb Update

上記の四つの中から報告者が注目した提案について簡単にご紹介します。

「Kerberos hash Update」は、MIT Kerberos ConsortiumのTom Yu氏により発表が行われました。

概要としては、Kerberosで使用しているハッシュ関数に対する危殆化対策(暗号技術の世代交代)として、現在主に利用されているハッシュ関数から、より安全とされているSHA-2へ移行しようという提案でした。危殆化の流れとして、ハッシュ関数だけではなく共通鍵アルゴリズムについても、今後検討が行われるのではないかと予想されます。

また、今回のkrb WGでは「DHCPv6 Kerberos option」について、横河電機株式会社の坂根昌一氏から提案があり、ミーティングにおいて活発な議論が行われていました。

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

□第75回IETF krb WGのアジェンダ
http://www3.ietf.org/proceedings/75/agenda/krb-wg.txt

◆tls WG(Transport Layer Security WG)

tls WGは、インターネット上で情報を暗号化して送受信するためのプロトコルであるTLS(Transport Layer Security)について、仕様の拡張や新規Cipher suiteの検討を行うWGです。

今回のミーティングは、2009年7月31日に開催され、参加者は40人程度でした。本ミーティングにおいて、冒頭でチェアから、WG文書のステータスおよびアジェンダについて報告がありました。

今回のミーティングで発表された提案は、以下の通りです。

・TLS Cached Info
・DTLS Heartbeat
・TLS -IBE
・XMPP TLS Multiplexing

上記の四つの中から、報告者が注目した提案について簡単にご紹介します。

「TLS -IBE」は、Huawei Symantec Technologies社のMin Huang氏により、発表が行われました。

IBEとはID Based Encryptionの略であり、近年、暗号業界で話題になっている基本的な暗号技術です。この提案は、IBEを利用してTLS通信を行おうというものでした。ミーティング会場では参加者同士の議論が活発に行われ、IBEをTLS通信に適用した時の課題等が多く洗い出されました。

また、第72回IETFで提案された、国産暗号のCamellia cipher suite(rfc4132bis)について、IETF期間中にInternet-Draftのステータスが、ID-ExistからAD Evaluationに変更されました。

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

□第75回IETF tls WGのアジェンダ
http://www3.ietf.org/proceedings/75/agenda/tls.txt

(NTTソフトウェア株式会社 菅野哲)

◆SIDR WG(Secure Inter-Domain Routing WG)

SIDR WGは、インターネットにおける経路制御のセキュリティ・アーキテクチャについて検討を行っているWGです。まだRFCになったドキュメントはなく、Internet-Draftの議論が続いています。第75回IETFでは、5日目(7月30日)の午前9時から2時間半ほどミーティングが行われました。約80名が参加しました。

更新された五つのInternet-Draftのうち四つについては、多くの議論はありませんでした。最後の一つについては、二つのプレゼンテーションがありました。

－ ROA Format - draft-ietf-sidr-roa-format-04
IPアドレスのprefixに対する経路広告元を指定(authorize)するデータ、Route Origination Authorization(ROA)の形式を定めるものです。

会場での確認の結果、ROAにおける署名アルゴリズムはdraft-ietf-sidr-cp-06ではなく、本ドキュメントにまとめて記述されることになりました。

－ RPKI Architecture - draft-ietf-sidr-arch-07
リソースPKI(RPKI)の全体像を述べたものです。

会場では、収束していない論点はなく著者としても書き足りないことはないことが説明され、WGメンバーにレビューが依頼されました。

－ Certificate Policy - draft-ietf-sidr-cp-06
リソース証明書の発行要件やCPSについて書かれています。

会場では、RFCの分類としてSTD(Internet Standards)ではなく、BCP(Best Current Practice)としてRFC化を目指すことが確認されました。RIPE NCCのAndrei氏がRIRで本ドキュメントのレビューを働きかけたため、あらためてNumber Resource Organization(NRO)に確認する必要がなくなりました。

－ RPSL with RPKI Signatures - draft-ietf-sidr-rpsl-sig-01
リソース証明書を使ってRPSLオブジェクトに電子署名を施す形式を定めるものです。

会場では、RPSLのオブジェクトに記述されたコンタクト先の情報が電子署名で担保されるわけではないなど、不明瞭な点があるという指摘がありました。Routing Policy Specification Security (RPSS)との関係を記述すべき、という指摘がAPNICのGeoff Huston氏(リモート参加)からありました。

以下は、RPKIに関するBGPルータの実装に関する二つのプレゼンテーションです。

－ BGP Protocol Geekiness
- http://archive.psg.com/090730.sidr-rpki.pdf
BGPルータにおけるRPKIを使ったOrigin ASの検証方式を検討した結果に関するプレゼンテーションです。

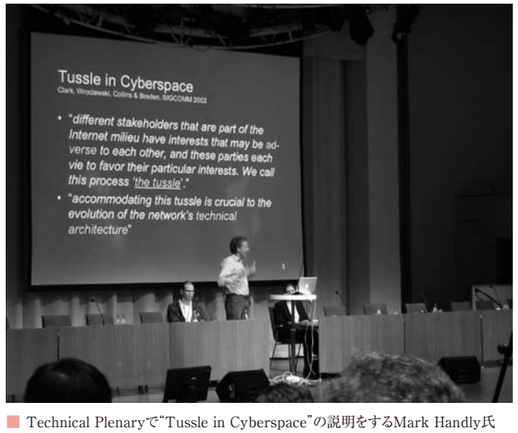
－ BGP Prefix Origin Validation
- draft-pmohapat-sidr-pfx-validate-01

BGPルータにおけるROAを使ったOrigin Validationの経路表への適用方法に関するプレゼンテーションです。

ルータベンダーやISPを交えてレビューが行われています。別のInternet-Draft（draft-ymbk-rpki-rtr-protocol-04）に基づいてプロトタイプの実装が行われていることなどが報告されました。WGのInternet-Draftにするかどうかはmlで議論することとなりました。

前回のIETF以降、RPKIとROAの用途を明文化するためのInternet-Draft、“Use Case”がICANNのTerry Manderson氏によって作成されました。このドキュメントはROAを使って、（BGPでいうところの）Originを検証する利用ケースを集めたものです。MLに引き続いて、BGPではOriginの検証よりもPathの検証の方が効果的ではないか、という議論がありました。しかし、SIDR WGとしては、Originの検証なしにはPathの検証に意味がないとされ、WGとしてはこれまで通りOriginの検証について取り組むことが確認されました。

最後に新たなトピックとして、BBNのStephen Kent氏が“Trust Anchor Management”についてプレゼンテーションされました。これはRPKIやROAを検証するRelying Party（RP;電子証明受け取り側）において、トラストアンカーとなる認証局の処理を工夫し、プライベートアドレスのプリフィクスやプライベートネットワークでもRPKIを使えるようにする提案です。アドレスの全域をカバーする、IANAにあたるトラストアンカーの証明書を生成し、その証明書の配下に有効な証明書を配置していくという内容となっていました。



■ Technical Plenaryで“Tussle in Cyberspace”の説明をするMark Handly氏

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

PKIX WGは、インターネットのためのPKI技術策定に取り組んでいるWGです。ミーティングは、4日目の7月29日（水）午後1時から1時間程行われました。参加者は30名程でした。

前回のIETF以降、RFCになったドキュメントはなく、三つのドキュメントがIESGのレビュー中です。

- Update for RSAES-OAEP Algorithm Parameters
  http://tools.ietf.org/id/draft-ietf-pkix-rfc4055-update-02.txt

Optimal Asymmetric Encryption Paddingという手法を用いたRSAの暗号化方式を証明書でサポートするためのRFC4055のアップデート版です。

- Attribute Certificate Profile - 3281bis
  http://tools.ietf.org/id/draft-ietf-pkix-3281update-05.txt

属性証明書（Attribute Certificate）を定めたRFC3281の修正版です。

策定内容に主だった変更はないものの、参照先のRFCの番号をアップデートするなどのerrata（誤字）を修正しました。

- Traceable Anonymous Certificate
  http://tools.ietf.org/id/draft-ietf-pkix-tac-04.txt

証明書のSubject欄に匿名の識別子を入れる方式で、匿名の識別子を作成する役割を証明書とは別にすることで、特殊な場合でなければ実際のIDと匿名の証明書とのマッピングができない仕組みを提案したドキュメントです。

WGで議論することになっているInternet-Draftは九つあります。このうち七つのInternet-Draftについてプレゼンテーションが行われました。

Trust Anchor Management（TAM）は、トラストアンカーである認証局証明書をオンラインで管理できるようにする仕組みで、三つのInternet-Draftが出されています。それぞれWG Last Callに近づいています。実装も行われており、WindowsのCAPIを使ったアプリケーション用のインタフェースを備えたプログラムを、SourceForgeにて公開する予定とのことです。

- 本プロトコルの要件
  http://tools.ietf.org/id/draft-ietf-pkix-ta-mgmt-reqs-03.txt
- トラストアンカーストア（格納場所）を転送するプロトコル
  http://tools.ietf.org/id/draft-ietf-pkix-tamp-03.txt
- トラストアンカーの表現形式
  http://tools.ietf.org/id/draft-ietf-pkix-ta-format-03.txt

OCSP Agility（draft-ietf-pkix-ocspagility-01）は、証明書検証用のオンラインプロトコルであるOCSPで、SHA-1以外のハッシュアルゴリズムを使えるようにする提案です。特に議論はなく、何かある場合にはMLで議論されることになりました。

Time Stamp Protocol 3161 update（draft-ietf-pkix-rfc3161bis-01）は、ESSCertIDv2のオプションを追加するための書き直しを行ったものです。RFC3161bis（RFC3161の後継）とするには、用語を大幅に書き換える必要があり、それは適切ではないため、本ドキュメントは先に進めないことになりました。

Certificate Image（draft-ietf-pkix-certimage-00.txt）は、証明書の中に画像データを入れられるようにする拡張フィールドの提案です。何の証明書であるのか、発行元（Issuer）、発行対象（Subject）を示す画像データを入れることができ、画像の形式はPDF（Portable Document Format）、SVG（Scalable Vector Graphics）、PNG（Portable Network Graphics）の三つが提案されています。

最後に、毎回恒例の“Related specifications and Liaison Presentations”（関連する標準と関連団体のプレゼンテーション）として二つのプレゼンテーションが行われました。

- Certificate Information Expression, Stefan Santesson

EUでは、PEPS（ID提供機能の代理機能）において、証明書のID情報をマッピングする仕組みがあります。認証処理ならばこれで認証情報の交換が適切にできますが、電子署名を検証する処理の場合は交換できません。ETSI（欧州電気通信標準化機構）のESI（電子署名および基盤に関する技術評議委員会）で、証明書にID情報を含める提案が承認されたため、テクニカルレポートの作成を2009年秋に開始予定です。

- Local Management of Trust Anchor for RPKI, Steve Kent

SIDR WGでも提案されている、RPKIのためのRelying PartyにおけるトラストアンカーのRP処理方式です。全ての範囲が入ったIANAのリソース証明書に代わるRPの証明書を作る方式が提案されています。

会場では、BGPを使った相互接続に関係して、RP毎に証明書のツリーが変わってしまい、有効とみなされるプリフィクスが異なる可能性がある、といった懸念が出ていました。

◇　　◇　　◇

5日目のTechnical Plenaryで行われたIRTF報告で、Public Key Next-Generation Research Group（PKNG）という新しいリサーチグループが設置されたことが報告されました。PKIXに代わる公開鍵暗号を使った新たな公開鍵サービスを検討しており、証明書フォーマットやセマンティクスを検討しているようです。チェアは、古参で、セキュリティエリアのWGで鋭い洞察力を発揮しているPaul Hoffman氏です。どのような議論が行われていくのかが楽しみです。

Public Key Next-Generation Research Group
http://www.irtf.org/charter?gtype=rg&group=pkng

（JPNIC 技術部 木村泰司）


■ ストックホルム湾から見た街並みの様子