Opinion Collection Meeting about Proposal in APNIC 35 Hosted by Policy-WG報告

関連記事 「P.23 APRICOT 2013/APNIC 35カンファレンス報告 アドレスポリシーに関する動向を中心に」

2013年2月7日（木）に東京・神田のJPNIC会議室で、ポリシーWGの主催により“Opinion collection meeting about proposal in APNIC 35 Hosted byPolicy-WG”と題したイベントを開催いたしました。

本イベントの目的は、日本を含んだRIRコミュニティであるAPNICのポリシーフォーラムによって、次回開催されるミーティングへの提案について、日本のコミュニティ内からのさまざまな意見を伝えるため、意見の収集を行うことでした。ミーティングでは提案内容の説明を行った上で、参加者に自由に意見を述べていただきました。参加者は関係者を除いて8名でした。

この種のイベントは、過去には「IPv4アドレスの移転」に関する提案が出たときに「臨時JPOPM（JPNIC Open Policy Meeting）」として開催したことがありますが、それ以来の実施でした。

運営準備段階では、当日の中継は予定していなかったのですが、当日開始直前にJPNIC事務局の協力でUstreamによる中継を実施できることになりました。開始時にIP-Users MLへも情報をお送りしましたが、案内が直前となったことをお詫び申し上げます。

本イベントのWebサイトは次のURLとなります。当日の説明に使った資料も掲載されておりますので、ご参照ください。

Opinion collection meeting about proposal in APNIC 35 hosted by Policy-WG
http://www.jpopf.net/Opinion%20collection%20meeting%20about%20proposal%20in%20APNIC%2035%20hosted%20by%20Policy-WG

◆ 提案とご意見について

今回のイベントでは、次の2件の提案について意見収集を行いました。

prop-105：Distribution of returned IPv4 address (Modification of prop-088)

prop-106：Restricting excessive IPv4 address transfers under the final /8 block

prop-105は、APNICへ返却されたIPv4アドレスの分配ポリシー見直しについての提案です。APNICへ返却されたアドレスは、現在は、グローバルポリシー※1によってどこかの地域インターネットレジストリ（RIR）の在庫が/9を切った後、IANAからRIRへ均等に再分配されることとなっています。prop-105では、現在IPv4アドレスを必要としている事業者への追加の分配を可能とするため、IANAからRIRへの再分配が行われた際に、すでに103/8からの分配を受けている組織が、そのアドレスブロックの中から最大/22までの分配を受けられることを提案しました。

提案に対しては、さらなるIPv4アドレスの需要に応えるために、あるいは返却されたIPv4アドレスを死蔵させないために、このような仕組みを作ることを支持する意見が複数寄せられました。

また、prop-106は、アジア太平洋地域における最後の/8ブロック※2である、103/8からのIPv4アドレスの移転を制限することを目的とした提案です。103/8からは、現在、1組織につき/22までのアドレスの分配を受けられることとなっていますが、分配を受けた後すぐに移転をしたり、逆に移転を受けてアドレスを集めたりというケースがあり、問題視されています。そうしたケースを防ぐため、

・103/8から分配を受けたアドレスは2年間移転不可とする
・103/8から分配を受ける際には10年分の維持料をデポジットとして納入し、移転した場合には返却する

の2点が具体的な提案の内容です。この提案については、問題意識に対する賛同は多く示されましたが、組織合併等、悪意のないケースもあると考えられることや、実効性に乏しいと思われることなどを理由に、提案そのものについての支持は強くなかったようです。

前述の通り、本イベントの目的は「意見を集めること」であって、日本のコミュニティとして意見を一つにまとめることではなかったため、ミーティング中でのコンセンサスの確認は行わず、賛成や反対の意見の表明は各自がAPNICのフォーラムへ参加した上で、個別に行っていただくことをイベント内でお願いしました。

参加者から集まった具体的な意見※3は、英訳した上でAPNICのオンラインフォーラムであるPolicy-SigのMLへ投稿しました。

提案についての意見収集の他、APNIC 35カンファレンスの概要説明も行いました。

● Opinion Collection Meeting about Proposal in APNIC 35 Hosted by Policy-WG会場の様子

◆ ミーティングを振り返って

アジア太平洋地域のポリシーは、日本国内のポリシーにも大きな影響を与えることになります。そのため、日本への情報伝達、国内の意見収集、意見の海外への発信といった活動は非常に重要であると考えています。今回のイベントに参加された方から「継続的な開催を期待している」というコメントをいただくことができました。今後も運営手法を改善しながら継続して実施したいと考えてます。その際には皆様の参加をお待ちしております。

今回、この種のイベントを初めて開催することができました。ご参加・ご発表いただいた皆様、運営にご協力いただいたJPNIC事務局の皆様にあらためて感謝申し上げます。今後もJPOPF（JPNIC Open Policy Forum）の活動への理解と支援をいただきますようお願い申し上げます。

（ポリシーワーキンググループ／楽天株式会社 橘俊男）

※1 インターネット用語1分解説：グローバルポリシー（global policy）、地域ポリシー（regional policy）とは
https://www.nic.ad.jp/ja/basics/terms/global-policy_regional-policy.html

※2 インターネット用語1分解説：最後の/8ブロックとは
https://www.nic.ad.jp/ja/basics/terms/final-slash8.html

※3 prop-105とprop-106に対するご意見
http://www.jpopf.net/prop-105%E3%81%A8prop-106%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E3%81%94%E6%84%8F%E8%A6%8B

APRICOT 2013/APNIC 35 カンファレンス報告

全体報告

APRICOT 2013/APNIC 35カンファレンスは、2013年2月19日（火）～3月1日（金）にシンガポールで開催されました。お隣の国、マレーシアとはバスでも行き来が可能であるなど、周辺国から比較的アクセスしやすいためでしょうか、参加者は704名で、昨年同時期のカンファレンス（APRICOT 2012/APNIC 33カンファレンス、参加者573名）より多くの方が現地に足を運んだようでした。

人口密度が世界第2位のシンガポールは、どこを見ても高層ビルばかり。高層マンションと熱帯植物が並ぶ住宅街は、どことなく千葉県の舞浜に似ていましたし、海辺に商業施設や高層オフィスビル、高級ホテル、貨物船が見える風景も、東京湾岸部を思い出させ、外国にいることをあまり意識せず過ごすことができました。

◆ APRICOT 2013/APNIC 35の構成・特徴

APRICOT 2013/APNIC 35カンファレンスのプログラム※1※2は、自身のPCを持参して実践的な演習を行うワークショップ4コマ、一つのテーマについて系統立てて知識を習得できるチュートリアル22コマ、各種最新動向や事例紹介を扱ったカンファレンス35コマなどからで構成されていました。ワークショップが満席となるなど、実践的に学べるセッションが人気である点は、JPNICが開催するイベント、Internet Weekと同じのようです。

◆ プログラムの中から注目した点

□IPv6とRPKI

今回のカンファレンスにおいて、テーマとして多く取り上げられていたのは、IPv6とリソースPKI（RPKI）※3でした。

IPv4アドレス在庫枯渇から約2年が経過し、各地域、各社ともIPv6対応が進んでいるようで、その状況を報告する発表がカンファレンス全体を通して多く見られました。香港は政府の協力を得て、中小企業や一般市民にも積極的にIPv6推進のための周知活動を行っているようで、ISOC HKのKa Ping Wong氏は「IPv6対応を始めたのは他の地域より遅かったが、今は追いついている」と胸を張っていました。

また、前回のAPNICカンファレンス 34（APNIC 34）に引き続き、モバイルネットワークのIPv6対応への関心は高い傾向にありました。特に、IPv6ネットワーク上でIPv4による接続を提供するためのIPv4アドレス共有技術である464XLAT※4の検証状況については、会場はもちろんのこと、リモートの参加者からも多くの質問が寄せられました。T-Mobile社のCameron Byrne氏は、IPv6導入が必要な理由の第一に「IPv4アドレスの在庫が枯渇したから」ではなく、「今のビジネスのニーズにIPv4はフィットしないから」を挙げていた点は、端末の増加が著しいモバイルネットワークの担当者らしいと感じました。RPKI関連の詳細な報告はP.25からの「RPKI関連の動向」に譲りますが、IRRの基本を解説したチュートリアルでもRPKIを取り上げ、公開鍵・秘密鍵など電子証明書の基本的な働きから時間を割いて丁寧に説明しているところが、私が前回、2010年に参加したAPNIC 30カンファレンスとは異なった点で、本気度がうかがわれました。

□APRICOT Opening Plenary

APRICOT 2013オープニングのセッションでは、基調講演にICANN事務総長兼CEOのFadi Chehadé氏が登場しました。「これまで我々はアジアに十分に関わって来たとは言えないが、これからはそれを変える必要があると思う」と述べた瞬間に会場から拍手が起こるなど、Chehadé氏の講演は、参加者の心をしっかりとつかんだようでした。また、シンガポールにICANNのアジアにおける拠点を設置することは、後日現地の新聞でもChehadé氏へのインタビュー付きで報じられていました。

● 基調講演を行うFadi Chehadé氏

□Asia Internet History

各地域・各団体の歴史や歴史を記録しているプロジェクトを紹介したセッションで、慶應義塾大学の村井純氏、Korea Advanced Institute of Science and Technology（KAIST）のKilnam Chon氏などが講演を行いました。Asia Internet History ProjectやKorea Internet History Projectは、書籍の出版やWebサイトでの公開など、2013年中に何らかのアウトプットがなされるようです。また、インターネット界のリーダーと言われる人たち数百人にインタビューを行ったWiWiW Projectの紹介では、インタビュー対象はどのような基準で選定したのかなど、積極的な質問が寄せられていました。

◇　◇　◇

一部講演については、当日の模様を収録したビデオやトランスクリプトが公開されています。冒頭でご紹介したAPRICOT 2013/APNIC 35カンファレンスのプログラムページからたどることができますので、興味を持たれた方は、一度ご覧になってみてはいかがでしょうか。

◆ APNIC20周年に向けて

2013年8月には、中国・西安でAPNIC 36カンファレンスが単独開催されます※5。APNIC 35カンファレンスが閉幕したばかりですので、まだ詳細は明らかになっていませんが、現在公開されている情報を見ると、20周年を祝う「何か」が行われると思われます。

会場で出会った中国からの参加者は皆、「次のAPNICカンファレンスは絶対に素晴らしいものになるから」と話していたことが印象的でした。2年後の2015年、APRICOT/APNICカンファレンスは日本で開催されます。私も同じことを言えるようになりたいなと思い、シンガポールを後にしました。

◇　◇　◇

次回のAPNIC 36カンファレンスは、2013年8月20日（火）～30日（金）、中国・西安で開催されます。また、次回APROCOTとの共催となるAPROCOT 2014/APNIC 37カンファレンスは、2014年2月18日（火）～28日（金）にタイ・バンコクでの開催が予定されています。

（JPNIC IP事業部／インターネット推進部 坂口康子）

※1 Program - APRICOT2013
http://www.apricot2013.net/program

※2 Program - APNIC35
http://conference.apnic.net/35/program

※3 インターネット用語１分解説「リソースPKIとは」
https://www.nic.ad.jp/ja/basics/terms/resource-pki.html
※4 464XLAT: Combination of Stateful and Stateless Translation
http://tools.ietf.org/html/rfc6877
※5 Home - APNIC 36
http://conference.apnic.net/36/

技術動向報告

APOPSは「The Asia Pacific OPeratorS forum」の略称で、環太平洋地域のインターネット運用者を対象とする、情報交換と交流のコミュニティです。APOPSのPlenaryセッションは、毎回のAPNIC/APRICOTカンファレンスにおいて開幕直後に設定されていて、年間の動向や注目すべきテクノロジーについて共有と報告がなされます。

今回のAPOPSは、2013年2月25日（月）、26日（火）の2日間に、APOPS Plenary1～2の二つのセッションによって構成され、開催されました。

本稿では、APOPSで紹介されたプレゼンテーションのうち、DNS関連のものについて詳しくご報告します。

◆ オープンリゾルバに関する話題

Cloudflare社のTom Paseka氏から、“The curse of the Open Recursor（オープンリゾルバのもたらす災厄について）”という演題で、オープンリゾルバに関する発表がありました。

オープンリゾルバとは、どのDNSクライアントからの再帰的な名前解決に対しても応答する状態になっている、キャッシュDNSサーバのことです。Google社、OpenDNS社、Level3社などの事業者は、特にセキュリティに配慮した上でそのようなキャッシュDNSサーバをサービスとして公開していますが、インターネットに存在しているキャッシュDNSサーバには、セキュリティへの対策が不十分なものが多数あり、DNSリフレクション攻撃と呼ばれる攻撃の踏み台となってしまう場合がある旨が述べられていました。

Cloudflare社では実際にそのような攻撃を観測しており、詳細について発表されていました。

DNSリフレクション攻撃は下記の特徴を持っています。

・UDPを使う
・送信元アドレスは、攻撃対象のホストのものに偽装する（これにより、キャッシュDNSサーバが該当の送信元アドレスに対してパケットを返すようになる）
・攻撃者は、ripe.netやisc.orgのanyレコードのように、クエリのパケットサイズは小さいが、応答パケットサイズは大きくなるような名前解決を問い合わせる（これにより、パケットサイズが増幅されて攻撃対象へ送信される）

Cloudflare社の調査により攻撃元を確認したところ、APNIC地域となる56の国と地域の中からは、27の国と地域から攻撃が行われていました。傾向としては、より人口の多い国と地域から、より多くの攻撃が観測されるようです。確認されたオープンリゾルバとなっているサーバの数について報告されていましたが、1位が日本の4,625となっていました。

オープンリゾルバを利用したDNS攻撃への対策については、下記の方法が紹介されていました。

・アドレスの詐称を防ぐために、BCP 38で規定されるような、送信元アドレスのフィルタリングを実施する（送信元アドレスがネットワークに割り当てたアドレスのものかどうかを確認し、割り当てたアドレスであればパケットを転送し、そうでないものは拒否する）。※1
・キャッシュDNSサーバ側で、名前解決を受け付けるDNSクライアントを必要な範囲に限定する
・権威DNSサーバ側で、再帰的な名前解決を不必要に受け付けないようにする。

◆ DNSの応答レート制限に関する話題

株式会社インターネットイニシアティブ（IIJ）のRandy Bush氏から、“DNS Rate Limiting（DNSの応答レート制限について）”という演題で、DNSの応答に一定の制限をかける技術について発表がありました。

発表は、下記の流れに沿って、DNSリフレクション攻撃の実例とその対策について述べられていました。

・Bush氏の管理しているDNSサーバが、急に外部向けトラフィックを大量に流すようになった
・DNSサーバ宛のパケットをキャプチャしたところ、DNSリフレクション攻撃に遭っていることがわかった
・しかし、該当のDNSサーバはキャッシュDNSサーバではなく、ccTLDのゾーンを管理している権威DNSサーバである（いわゆるオープンリゾルバではない）
・攻撃の分析を進めたところ、DNSSEC関連のレコードを利用した攻撃であることがわかった
・今回は、スイスのccTLDである.chドメイン名のDNSSEC付きレコードの大量問い合わせがあったが、個々の問い合わせのパケットサイズは小さくとも、署名の付いた.chドメイン名の応答は1KB以上のサイズに増幅される
・攻撃者は送信元アドレスを詐称したUDPパケットを送信していた
・対処として、DNSサーバのソフトウェアに、同一送信元アドレスからの単位時間あたりの応答に制限をかけたところ、問題は解消した
・Bush氏のDNSサーバのソフトウェアはBINDであったが、NSDについても対策のあることを確認した

上記二つの発表はJANOGのメーリングリストでも紹介され、日本のオペレーターの間でも議論が交わされていました（[janog:11575]参照）※2。

◆ その他のセッション

上記のセッション以外にも、次のようなトピックでさまざまなセッションが開催されていました。発表のビデオとスライドが公開されていますので、興味のある方は以下のURLをご参照ください。

・IPv6関連（Asia Pacific IPv6 Task Forceなど）
・ルーティング関連（Peering Forum、Routing Securityなど）
・SDN関連（Software Defined Networking Panelなど）

http://www.apricot2013.net/program/presentations/

（JPNIC 技術部 澁谷晃）

※1 インターネット用語１分解説「イングレスフィルタリングとは」
https://www.nic.ad.jp/ja/basics/terms/ingress-filtering.html
※2 JANOGのMLに参加すれば、アーカイブで過去の投稿記事も読むことができます。
http://www.janog.gr.jp/

アドレスポリシーに関する動向を中心に

関連記事 「P.19 Opinion Collection Meeting about Proposal in APNIC 35 Hosted by Policy-WG報告」

今回のAPNIC 35カンファレンスにおけるアドレス等のポリシー関連動向について、アドレスポリシーSIGでの発表内容を中心にお届けします。

◆ SIGについて

特定の話題について議論を行うために、APNICではSIG（Special Interest Group）という仕組みが設けられています。

現在、IPアドレスやAS番号のポリシーに関連する話題について議論を行うアドレスポリシーSIGと、JPNICのような国別インターネットレジストリ（NIR）に関連する話題について議論を行うNIR SIGの二つが設けられています。メーリングリスト（ML）上での議論を中心として、年に2回開催されるAPNICカンファレンスでは顔を合わせての議論を行います。最近では、ストリーミングによる議論の中継や、発言をリアルタイムに画面やスクリーン上に映し出すトランスクリプト、チャットによるコメント受け付けなど、会場以外からミーティングに参加するための手段も多く設けられています。

◆ IPアドレスポリシー提案の結果について

アドレスポリシーSIGでは２点の提案について議論が行われました。アドレスポリシーSIG開催前のMLや会場での議論の結果、１点はMLでの継続議論、もう１点は棄却となり、コンセンサスに至った提案はありませんでした。

アドレスポリシーSIGでの提案の内容と結果をご紹介します。

（1）「Distribution of returned IPv4 address（Modification of prop-088）」（提案番号：prop-105）	
提案者	藤崎智宏氏（JP IPv4 ADDRESS ALLOCATION DISCUSSION TEAM）
概　要	APNICにおける最後の/8ブロックである103/8からの分配（1組織当たり最大/22）に加えて、IANAからの再割り振りやAPNIC会員からの返却により分配可能となったIPv4アドレスを、1組織当たり最大/22まで分配する。
結　果	アドレスポリシーSIG MLでの継続議論

提案者から、第22回JPNICオープンポリシーミーティングでの議論をきっかけとして結成された「JP IPv4 ADDRESS ALLOCATION DISCUSSION TEAM」が実施した、日本国内およびAPNIC地域を対象としたアンケート結果を紹介し、提案の背景を会場の参加者と共有しながら発表が進みました。アンケート結果の解説は割愛しますが、アンケートに回答した150組織の約7割が、APNICにおける最後の/8ブロックである103/8からの分配以外にも、新たなIPv4アドレスの分配を希望していることが明らかになりました。APNIC/JPNICにおけるIPv4アドレス在庫が枯渇して約2年が経過する現在においてもなお、IPv4アドレスの需要は残っていることを感じました。

議論では、APNICの分配可能な在庫を有効活用して、APNIC会員に再配分することに反対する意見は表明されませんでした。その一方で、分配サイズおよび分配方法について多くの時間が割かれました。主な意見は次のようなものでした。

・IANAからの再割り振りやAPNIC会員からの返却により/10（約400万アドレス）程度のIPv4アドレスが分配可能であることが明らかになっているが、現在のAPNIC会員の増加傾向から考えた場合には、すべての組織に/22の分配を行うことは難しいのではないか
・上記のIPv4アドレス以外にも、新たなIANAからの再割り振りやAPNIC会員からの返却により分配可能アドレスが発生した場合、再度分配を受けることができるのかどうか

議論の結果、今後も継続してアドレスポリシー SIG ML上での議論と検討を行うことになりました。

● 提案内容を説明する藤崎氏

⑵「Restricting excessive IPv4 address transfers under the final /8 block」（提案番号：prop-106）	
提案者	白畑真氏、藤崎智宏氏
概　要	APNICにおける最後の/8ブロックである103/8から分配されたIPv4アドレスについて、最後の/8ブロックの分配に対する考え方と一致しない移転であることが確認された場合、APNICまたはNIRはその移転承諾を保障しない場合があることを運用ガイドライン文書に明記する。
結　果	棄却

APNIC 35カンファレンス開催前のアドレスポリシーSIG MLでは、APNICでの移転履歴をもとに提案者がまとめたAPNICにおける最後の/8ブロックから分配されたアドレスに関する移転状況の紹介や、現在のIPv4 アドレス移転に関するポリシーの考え方に関する再確認など、活発な議論が続きました。

議論の過程において、APNICにおける最後の/8ブロックからの分配アドレスを移転した場合の移転禁止やデポジットの徴収を「ポリシー文書に明記する」、という当初の提案内容から、「運用ガイドライン文書に明記する」という内容に変更することとなりました。

アドレスポリシー SIG当日の議論では、変更後のポリシー提案の内容に基づき議論が行われ、

・申請処理を行うAPNIC担当者が正しく判断することが難しいのではないか
・提案者が懸念しており現在起きている問題への対応が必要かどうか

についてが争点となりました。議論の結果、今後も状況の把握が必要なことは確認されましたが、提案はコンセンサスに至らず、棄却となりました。

これら2点の提案に関して、日本ではポリシーワーキンググループが2013年2月7日に「Opinion Collection Meeting about Proposal in APNIC 35 Hostedby Policy-WG」という意見収集のイベントを開催し、この場で集まったご意見をアドレスポリシーSIGのMLに報告しました。この意見収集のイベントの模様や寄せられたご意見などについては、P.19の「Opinion Collection Meeting about Proposal in APNIC 35 Hosted by Policy-WG報告」をご覧ください。

◆ その他のポリシー関連の動向について

アドレスポリシー SIGでは、提案に対する議論以外にもアドレスポリシーの話題について情報提供が行われることがあります。

実際に、APNICでは、管理する資源（IPv4アドレス、IPv6アドレス、AS番号）別に資源の取り扱いの方針をまとめたポリシー文書を制定していますが、今回これらのポリシー文書の再構成に関する検討内容がAPNIC事務局から紹介されました。

また、APNICが制定するポリシー策定プロセス、他の文書および実際の運用との相違点が提示され、アドレスポリシーSIG参加者から広く意見を収集するための発表も行われました。

アドレスポリシー SIGではこのほかにも、興味深い発表が行われています。発表内容や議論の内容は、アドレスポリシーSIGのページ※1から確認することが可能です。興味を持たれた方はぜひご覧ください。

◆ APNIC Member Meetingについて

APNIC 35カンファレンスの最終日にはAPNIC Member Meeting（AMM）が開催されました。AMMでは主にAPNICの活動内容に関する報告、APNIC 35カンファレンス期間中に開催されたSIGや各種セッションの報告、次回のAPNIC 36カンファレンスの紹介が行われました。

これらの報告と併せて、APNIC理事会メンバーを選出するための選挙が行われました。候補者のプロフィールは事前にAPNICのWebサイト※2で公開され、その内容を参考にして、APNIC会員の多くは前日までに会員向けポータルサイトからオンライン投票を済ませます。AMM当日は、候補者自身で抱負を述べる機会が設けられますので、その内容を確認して投票用紙での投票を行う組織もあるようです。

今回は5名の候補者の中から、次の4名がAPNIC理事会メンバー（EC）として選出されました。この4名に加えて、今回の改選対象には含まれない3名、およびAPNIC事務局長Paul Wilson氏の合計8名で、新APNIC理事会の体制がスタートすることになります。

・Gaurab Raj Upadhaya氏（Limelight Networks）
・Wei Zhao氏（CNNIC）
・Kenny Huang氏（TWNIC）
・James Spenceley氏（Vocus Communications Limited）

● AMMにてECとしての抱負を述べるKenny Huang氏

◆ まとめ

APNICにおけるIPv4アドレスの在庫枯渇から約2年が経過し、IPv4アドレスの分配に関わる提案は少なくなりました。アドレスポリシー SIGでの議論は、どのようにAPNICの在庫を効率よく分配するか、という点に集中してきていると感じます。返却されたアドレス等を含めた、IPv4アドレスの分配に関わる話題は継続して議論が行われる可能性が高く、今後の動向が注目されます。

また、ポリシー策定プロセスに関する情報提供や議論に多くの時間が割かれている点が印象的でした。APNICカンファレンスでの議論は、APNICと同様のポリシー策定プロセスを持つ日本のコミュニティにおいても参考になると考えられますので、今後も情報収集を続けていきたいと考えています。

（JPNIC IP事業部 川端宏生）

※1 Policy - APNIC35
http://conference.apnic.net/35/policy/

※2 2013 APNIC EC Elections
http://conference.apnic.net/35/elections/

RPKI関連の動向

関連記事「P.12 ルーティングセキュリティに関する取り組みの強化 RPKIハッカソン開催について」

本稿では、APNIC 35カンファレンスにおけるRPKI（Resource PKI - リソースPKI）の動向を報告いたします。

今回のカンファレンスでは、「RPKI CA hackathon」とそのBoFである「RPKI in AP-Region BoF」が行われました。このミーティングに先立つ2013年2月に開催されたJANOG（JApan Network Operators' Group）ミーティングでは、“RPKIルーティングを試す会”によってハッカソンが行われました。その様子は、P.12の「RPKIハッカソン開催について」でご紹介しています。

今回の「RPKI CA hackathon」は、その国別インターネットレジストリ（NIR）版として企画されたものです。また、APOPS（The Asia Pacific OPerator Sforum）の中でも、Routing Security Sessionと呼ばれる、RPKIに注目したセッションが開かれました。

◆ RPKI CA hackathonとその背景

今回のRPKI CA hackathonは、アジア太平洋地域のNIRでも検討が進められているRPKIのCA（認証局:Certification Authority）について、参加者自身が実装を動かしてみることで、今後の情報交換と意義のあるディスカッションにつなげていくことを目的とし、行われました。

・日　時：2013年2月26日（火） 17:45-18:20
・場　所：APNIC 35カンファレンス会場 Island Jurong
・参加者：13名（二つのNIRが参加）
・ＵＲＬ：http://conference.apnic.net/35/program/rpki-hackathon/

アジア太平洋地域には、NIRが七つあり、各国のIPアドレスとAS番号のレジストリを担っています。RPKIは、このIPアドレスとAS番号の割り振りと割り当ての構造に従って、電子証明書が発行される仕組みであるため、アジア太平洋地域におけるRPKIの普及には、NIRにおけるRPKIの導入が、鍵の一つになってくると言えます。

2013年になって、JANOGのRPKIハッカソンで確認されつつあるように、BGPルータにおけるRPKIの実装は進んできており、ルーティングの運用で使われる可能性があります。すでにRIPE NCCやLACNICでも、RPKIを使ったWebサービスが試験的に立ち上がっており、インターネットに流れる経路情報のIPアドレスが正しく割り振られたものなのか、また本来のASから広告されているのかが視覚的にわかりやすく確認できるようにする試みが行われています※1※2。

このように、他の地域におけるRPKI導入に向けた動きが活発になる中、アジア太平洋地域ではどのように取り組んでいけばよいのか、技術的にはどのような構成になっていくのかをディスカッションしていく試みとして、RPKI CA hackathon開催につながったのです。

◆ RPKI CA hackathonの経過

RPKI CA hackathonのセッションは、2月26日（火）に設けられていました。しかし実際にはこの時間よりも、その後の打ち合わせスペースなどでの活動の方が活発に行われることになりました。その経過を簡単に報告したいと思います。

APNICカンファレンスでは、これまでにもRPKIに関する技術的な発表は多数行われていました。しかしNIRからの参加者の間では特に話題に上ることはなく、導入を検討するような段階とは程遠い状況でした。そんな中で、本セッションの時間は設けられたのですが、当日は参加者が20名ほどしか集まりませんでした。

個別に話を伺ってみると、RPKIには興味をもってはいるものの、担当者自身の興味であり、NIRとして組織的に取り組んでいるところは少ない様子でした。この状況でAP地域のRPKIについてディスカッションを進めていくにはどうしたらいいのか。そこで、セッションのように一堂に集まるのではなく、休憩コーナーなどでRPKIの情報共有を進めつつ、RPKI CA hackathonを行うというやり方で進めることになったのです。

その結果、APNIC 35カンファレンスの終了時点で、TWNICとKRNICの方がJPNICで用意していた仮想マシンを使い、NIRとしてのCAを体験されました。VNNICはRPKIの実験に必要な、APNICから割り振られたIPアドレスの確認などの作業を行いました。APNIC 35カンファレンスの終了後、TWNICは、TWNICで用意されたサーバに移設して実験を継続しています。CNNICは、BBNのツール[※3]を用いた技術検証を行っており、後述するBoFでの論点の一つであるIPアドレスの移転をどのように扱うのか、といった議論に参加しています。

◆ RPKI in AP-Region BoF

RPKI in AP-Region BoF（AP地域におけるRPKI BoF）は、hackathonそのものについて意見交換を行うと共に、前述のhackathon開催を受けて、AP地域におけるRPKIの普及に関する論点を洗い出すことを目的としたBoFで、今回初めて行われました。

● RPKI in AP-Region BoFにてプレゼンテーションを行う筆者

・RPKI in AP-Region BoF
・日　時：2013年2月27日（水）　17:45-18:20
・場　所：APNIC 35カンファレンス会場 Island Tanglin
・参加者：約20名
・ＵＲＬ：http://conference.apnic.net/35/program/rpki-in-ap-region-bof/

議事を簡単に紹介します。

- CNNIC Update, Di Ma氏, CNNIC

CNNICでは、BBN社のRahtheon氏が開発したRPSTIRやNIST SRx quaggaを利用したテストベッドを運用しています。テストベッドでは、“アドレスの移転”、“3階層モデルのCAの運用”、“セキュアBGPの普及”の三つの観点に注目し、RPKIのオペレーションを検証しています。このプレゼンテーションは、アメリカ・ボストンにいるDi Ma氏によって、Skypeを使って行われました。

- Hackathon Update, 木村泰司, JPNIC

筆者は、RPKI CA Hackathonの経過を報告しました。この時にはKRNICとCNNICの方が設定を開始していたため、その様子を報告しました。RPKI CA Hakathonでは、NIRのCAを設定するためにJPNICが構築した実験用のAPNICのCAを構築してNIRのCAと連携させています。今後は、実際のAPNICのCAを利用した実験に発展させていく必要があります。

- ディスカッション

ディスカッションの時間には、AP地域でのRPKIの導入を検討するために考えられる論点の洗い出しを行いました。挙げられた論点を次に示します。

a. APNICのRPKIシステムとの連携

NIRのRPKIシステムとAPNICのシステムとの連携をどのように動作検証していくのかという点です。この後、APNICでは動作試験用のサーバを１ヶ月以内に用意するという連絡がありました。

b. Publication Point

AP地域におけるリソース証明書とRPKIの配布サーバをどのように配置するかという点です。NIR自身が一次配布サーバを運用することになりますが、APNICにも配布サーバがあり、どのような全体構成にしていくのかを議論していく必要があります。

c. RIRとNIRの間の動作検証

NIRの間での動作検証をどのように行うのか、技術的なテスト環境をどこにどのように用意するかといったテストベッドの話題です。

d. ソフトウェア開発

APNICにおけるRPKIのCAと、NIRにおけるCAの開発をどのように進めていくのか、という話題です。基本的に各々のNIRが取り組んでいくことではありますが、システム構成、特に配布サーバの設置方法について情報共有を図っていくことが考えられます。

◆ APNIC 35カンファレンスにおけるRPKIの話題を振り返って

APNIC 35カンファレンスでは、RPKI CA hackathonとRPKI in AP-Region BoFを通じて、NIRの方を交えたトライアルを始めることができました。CNNICではBGPにおける応用を視野に入れた技術検証を始めていることがわかり、さらにAPNICからはNIRが試験できるようにテスト環境を用意してくれることになりました。AP地域でもRPKIへの注目が高まってきていると思われます。

今後は、前述の論点を踏まえて、IPアドレスの移転をRPKIでどのように実現できるのか、RPKIのCAの構造はどのようになっていくのかなどの具体的な議論が進んでいくと思われます。

RPKIは、その技術の性質上、インターネットを特定の組織が制御するような構造になってしまったり、逆に、導入そのものが目的になってしまって、使われなくなってしまったりする恐れのある技術だと思います。RPKIが本当に役立つ仕組みとして導入されていくためには、NIRなど、関係する方々によって、どういうものなのかの理解が得られ、国を超えたインターネットにおいて、うまく機能する形にしていくためにディスカッションしていくことが重要です。

そのために、とりわけAPNIC 35カンファレンスにおけるRPKI関連のディスカッションには、実際に動作するプログラムと動作させる環境が不可欠でした。RPKI Toolsを簡単に試せるようにするための洞察とさまざまな改良作業をいただいたRob Austein氏とRandy Bush氏、そしてRPKIを試すことのできるBGPルータを実験用に提供してくださったインターネットマルチフィード株式会社の方々にこの場を借りて感謝したいと思います。またHakachonの形態はJANOGのRPKIルーティングを試す会の関係者各位の考案によりますことを申し添えます。

今後も、RPKIが技術的に簡単で便利なものになるよう、活動していきたいと考えています。

（JPNIC 技術部／インターネット推進部 木村泰司）

※1 Public RIPE NCC Validator
http://rpki01.fra2.de.euro-transit.net:8080/

※2 RPKI Origin Validation Looking Glass
http://www.labs.lacnic.net/rpkitools/looking_glass/

※3 RPSTIR - Relying Party Security Technology for Internet Routing
http://sourceforge.net/projects/rpstir/

第86回IETF報告

全体会議報告

第86回IETF Meetingは2013年3月10日（日）から3月15日（金）の間、米国フロリダ州オーランドにて、米国のCATV会社コムキャスト社と、子会社でメディア企業のNBCユニバーサル社のホストで開催されました。

フロリダといえば、1年中暖かでTシャツで過ごせるような印象でいましたが、滞在中は1日の寒暖差が10度くらいあり、朝晩は東京と同じくらい寒く、雨のそぼ降る寒い日もありました。

ディズニーワールドやユニバーサルスタジオもバスなどで行ける距離にあり、合間に楽しんだ人も多いようでした。個人的にはスギ花粉から逃れられると喜んでいたのですが、開催地でも別の種類の花粉が飛んでいたようで、かゆみや鼻炎に悩まされました。

さて、全体報告ですが、前回は「One Plenary」として１回にまとめる試みがされていましたが、今回は従来通りの「IETF Operation and Administration Plenary」と「Technical Plenary」に戻して開催されました。その両Plenaryについて、簡単にご報告します。

◆ Technical Plenary

3月11日（月）の夕方から2時間の枠で開催されました。IRTF、IABチェアレポートに続いて、テクニカルトピック二つ、RFC編集者レポート、新規のIABメンバの紹介、最後に会場から自由に意見や質問を述べるオープンマイクという流れで議事進行がされました。

- IRTFチェアレポート

IRTFチェアレポートでは、11ある研究グループの状況報告がありました。

（1）ASRG:Anti-Spam Research Group
（2）CFRG:Crypto Forum Research Group
（3）DTNRG:Delay-Tolerant Networking Research Group
（4）ICCRG:Internet Congestion Control Research Group
（5）ICNRG:Information-Centric Networking Research Group
（6）NCRG:Network Complexity Research Group
（7）NMRG:Network Management Research Group
（8）P2PRG:Peer-to-Peer Research Group
（9）RRG:Routing Research Group
（10）SAMRG:Scalable Adaptive Multicast Research Group
（11）SDNRG:Software-Defined Networking Research Group

P2PRGは活動終了し、ASRGとSAMRGの二つが活動終了に向けて動いていること、NCRG、NMRG、RRGの3グループはあまり活動がなく、CFRG、DTNRG、ICCRG、ICNRG、SDNRGは活発に活動されているとのことです。Applied Networking Research Prize（ANRP）という研究活動に対する賞の受賞者の1人であるGonca Gursun氏のスピーチが、第86回開期中のIRTFオープンミーティングでされることが告知されました。2014年のノミネーションは、2013年の秋に行われるそうです。筆者は今回久しぶりのIETFへの参加で、IRTFの活動に疎かったため、SDN（Software Defined Network）について、IETFの中では調査段階にあるということを新鮮に感じました。

- IABチェアレポート

IABチェアレポートでは、第86回開期中に行われるITU-Tの状況について総括する“The World Conference on International Telecommunications（WCIT）2012: What Happened, What's Next?”の予告や、IAB内の活動の進捗報告の他にIABメンバーの交代の話がありました。

これまでIETFチェアだったRuss Housley氏が次期IABチェアとなります。また、David Kessens氏、Danny McPherson氏、Jon Peterson氏の3人が退任し、新しくEliot Lear氏、Xing Li氏、Andrew Sullivan氏が加わります。また、Bernard Aboba氏、Jari Arkko氏、Marc Blanchet氏、Ross Callon氏、Alissa Cooper氏、Spencer Dawkins氏、Joel Halpern氏、Dave Thaler氏、Hannes Tschofenig氏の9人は、残留です。

既にIABのWebページは更新されており、IABメンバーの経歴などは詳しく紹介されています。

- http://www.iab.org/about/iab-members/

IABは、IETF内の監督業務のほかに、対外組織との連携業務など内外に活動をしていますが、取り扱う内容がWCITのようなガバナンスや、プライバシー考慮など高次の内容になり、多様化しているとあらためて感じました。また、IABはwikiなどのWebベースのツールを持っていますが、今後の活動予定に「IPv6 for IAB internal website」というのが挙がっていて、これからIPv6対応するというのも意外でした。

- テクニカルトピックI

テクニカルトピックIでは、“The End of Plain Old Telephone Service（POTS）”と題して、前回85回ミーティングのプレナリで計測についての話者の1人だった、FCC（米国連邦通信委員会）チーフテクニカルオフィサーのHenning Schulzrinne氏が今回も登壇しました。

米国では、2018年に電話網（日本でいうところの加入者電話回線網）を引退させることが予定されており、それに向けた整備が行われています。Schulzrinne氏によると、「それはtechnical + economics + policyの問題である」ということで、多面的に現状分析と問題点が話されました。FCCでは、タスクフォースを作って取り組んでいますが、携帯電話とその技術の登場によって固定電話の役割は終焉を迎えても良い状況になっています。3段階の移行が考えられており、「copper → fiber, wired →wireless, circuit → packet」と表現されていました。

しかし、固定電話には悪い部分（品質やビデオ送信などができないことやセキュリティ）もありましたが、良い部分（緊急時の通話や可用性や低コストやグローバルな接続性）もあり、特にユニバーサルな展開の維持などを携帯電話で行うことに課題があるとしています。また、これまでの電話網における番号体系が、IPベースでは変更になることから、番号の問題も取り上げられていました。

IPアドレスは通信先の特定以外にもIDとして利用されたり、名前体系と紐付けられたりといった運用がされています。一方、電話番号には、地域コード（局番）などの管理階層があります。IPアドレスと電話番号それぞれの管理体系を踏まえた移行計画が必要そうです。今回の発表を受けて、IETF内でも電話網の終焉に関係した必要技術の提案が増えていきそうです。

- テクニカルトピックII

テクニカルトピックIIでは、IEEE Registration Authority CommitteeチェアのGlenn Parsons氏より、“IEEE 802 Proposed OUI Registry Restructuring”と題して、イーサネット技術で利用される番号であるOrganizationally Unique Identifiers（OUI）の拡張について話がありました。

OUIをはじめとするイーサネット技術で利用される番号は、IEEEのRAC（Registration Authority Committee）が登録管理をしています。昨今のスマートフォンの増加などで物理デバイスが急増したことによるOUIの枯渇問題があり、拡張せざるを得ない状況になってきたことを受けた管理機構の改訂に向けた発表でした。既存のOUIとOUI-36は維持しつつ、MACアドレスなどに使われるEUI-48の管理体系を新設し、MACアドレスとは分離した企業IDを登録すること、新設する企業IDを使った仮想マシンのアドレスを作るようにすることなどが提案されています。2014年には登録開始したい意向のようで、2013年半ばまで意見を募集するそうです。この再編については、draft-ieee-rac-oui-restructuring-00.txtとしてドラフト文書が提出されています。

- RFC編集者レポートとオープンマイク

RFC編集者レポートでは、RFC文書のフォーマット変更の準備作業状況報告がありました。現在のRFC文書のフォーマットはRFC2223で規定されていますが、規定への変更要望が、“RFC Series Format Requirements and Future Development”（draft-iab-rfcformatreq-03.txt）というドラフト文書にまとめられています。この文書はまもなくRFCとして発行する承認過程に入るようで、2013年はドキュメントに従った文書フォーマットの変更作業に入るそうです。

会期の始まりだからか、テクニカルトピックの発表が終わると徐々に人が減っていき、最後のオープンマイクの頃にはかなり人が減ってしまい、オープンマイクの質問もそれほどなく終了しました。


● Technical plenary 会場の様子

◆ IETF Operation and Administration Plenary

こちらは、3月13日（水）の夕方から2時間半の枠で開催されました。従来通り、ホスト企業のプレゼンテーションから始まり、IETFチェア、IAOCチェア、IETFトラストチェア、Nomcomチェアからのレポート、IAOCオープンマイク、IESGオープンマイクという流れで議事進行されました。今回、IETFチェアをはじめ、IAB／IAOC／IESGメンバーの交代の時期で、新しいチェアやメンバーの紹介が合間に議事として行われました。テクニカルプレナリに比べると、発表資料にも面白い画像が入っていたり、くだけた感じで進められました。

- IETF チェアレポート

2013年3月でチェアがJari Arkko氏に交代することが決まっているため、Russ Housley氏による最後のチェアレポートとなりました。第86回の参加者は、51の国と地域から1,071人の参加となり、前回から20人ほど減少しています。新規参加者は182人と、全体の1割は新規参加者で新しい参加者層の取り込みがされているようです。国別の参加者数は、1位米国、2位日本、3位中国で、これは前回と変わらない状況でした。

IETFに投稿するドキュメントの記述のために提供されている、xml2rfcツールのバージョンアップの告知がありました。1月からベータテストが開始され、いくつかの発見されたバグ修正版が3月からダウンロード可能となったそうです。古いバージョンのツールも半年間はダウンロード可能ということです。

また、IETFのミーティングのホストについて、シスコ社とジュニパーネットワークス社の両社と「Multi-year Host Agreement」という契約を結び、今後の9年間で開催されるミーティングのうちそれぞれ3回ずつについてホストとなることが決定したそうです。シスコ社はホストのほか、会議システムや無線LANのシステム提供も行うそうです。

- IAOCチェア、IAD、IETFトラストチェアレポート

IAOCチェアand IADレポートは、IAOCチェアのBob Hinden氏から行われました（ちなみにIADチェアは、Ray Pelletier氏です）。今回は、報告の前に、IETFチェア交代にあたりRuss Housley氏の功績を面白おかしく紹介し、IABメンバーから一言ずつ贈る言葉があり、メンバーのBert Wijnen氏からはオランダ語と思われる歌まで披露されました。意味はわかりませんでしたが、栄誉を称えるような勇敢な曲調の歌でした。その後、記念品が授与されていました。

その後、2012年の収支報告や2013年の予算（詳細は、http://iaoc.ietf.org/budget.html）やチェアの選挙の結果報告として、IAOCチェアにはBob Hinden氏が選出され、IETF TrustチェアにChris Griffiths氏が選出されたことが報告されました。

- Nomcomチェアレポート、IAOCオープンマイク、IESGオープンマイク

Nomcomチェアからは、IAOC 2名、IAB 7名、IESG 7名の選出結果発表がありました。引き続き、Russ Houstley氏から「Passing The Baton To Jari」(Jariにバトンを渡します) という発表があり、これに応える形でJari Arkko氏からは「Accepting the Baton from Russ」(Russからバトンを受け取ります) という発表がありました。Russ氏は記念品として授与されたサッシュをつけてスピーチをしていました。Jari氏からは、「今日はちゃんとジャケットを着るよ」という発言があり、新しいIETFチェアとして、IETFのこれまでの活動の良い所は伸ばし、悪い所 (結論がでるまでに時間がかかるケースがある等) を改善していくといった表明がありました。

この後はIAOCのオープンマイクとIABのオープンマイクですが、この段になると一層リラックスした雰囲気になり、IAOCのオープンマイクの際には、Bob Hinden氏は、「フリースタイルで」といいながら、長いマントを羽織って登場しました (今回のソーシャルイベントがユニバーサルスタジオのハリーポッターのアトラクションを貸し切って行われることに引っ掛けたようです)。

しかし、IABのオープンマイクでは雰囲気は一転し、会場からはリーダーシップやダイバーシティの問題、マイノリティや英語を母国語としない人へのケア、若手などへのメンターの提案など多くの参加者で円滑に運営していくための話し合いが時間いっぱいされました。今回のオープンマイクでは、非常に多数の女性がマイクに立って発言をしており、一層今までにない雰囲気となっていました。ダイバーシティに関してはその後もIETFの全体メーリングリストで活発なやり取りが続いていますが、今回あったような話は簡単に結論が出るものでもなく、継続してなされていくと思われます。

◇　　◇　　◇

次回のIETF Meetingは、2013年7月28日(日) から8月2日(金)にかけてドイツのベルリンにて開催されます。

◆ リンク

第86回IETFミーティング議題・資料
- https://datatracker.ietf.org/meeting/86/agenda.html

第87回ミーティング
- https://www.ietf.org/meeting/upcoming.html

(株式会社インテック 廣海緑里)


● 第86回IETFの会場となったCaribe Royale

DNS関連WG報告

今回のIETF 86は、米国フロリダ州のオーランドで開催されました。ディズニーワールドの近くであり、カンファレンスセンターはリゾート気分満載でした。DNS関連WGとしては、dnsop WGが会合を開催しました。dnsop WGの会合での議論と、dnsop WG、dnsext WGそれぞれのメーリングリストでの議論を元に、DNS関連WG報告をします。

◆ dnsop WG報告

dnsop WGの会合は、1時間の枠で開催されました。主な議題は、

(1) DNS in JSON
(2) Negative Trust Anchors
(3) Automating DNSSEC delegation

の三つでした。

これらに先立ち、会合の冒頭に、チェアからドラフトの状況に関する報告がありました。前回のIETF 85から現在までに、draft-ietf-dnsop-rfc4641bis がRFC6781 と し て、draft-ietf-dnsop-dnssec-dps-framework がRFC6841 と し て発行されたとの報告がありました。RFC6781はDNSSEC Operational Practicesの更新版であり、DNSSECに用いる鍵の生成からゾーンの署名、鍵の管理等、DNSSEC一連の運用に関してガイドラインを示した文章となっています。また、RFC6841はトップレベルドメインやセカンドレベルドメインの管理者が、DNSSECの導入や運用に関しての文章を作成するにあたってのフレームワークを提供する文章となっています。ドラフトの確認後、アジェンダとして予定されていた議題に移りました。

まず、(1)のDNS in JSON (JavaScript Object Notation) では、DNSの問い合わせや応答のフォーマットを、現在のバイナリ形式のワイヤーフォーマット以外にも定義し、アプリケーション間でDNSデータのやり取りをしやすくしようという意図から提案されました。具体的には、DNS Looking Glassなどからデータを抽出したり、HTTPを用いてDNSデータを交換したりする場合を想定しているようです。JSON WGでやるべきでは、との意見も出されましたが、JSONフォーマットを定義すること自体には大きな反対も無く、議論は続けられることとなりました。

次に、(2) のNegative Trust Anchorsに関する議論が行われました。この提案は、DNSSECを導入したドメインで、ゾーン管理者の設定ミスや管理のミスにより、ゾーン全体が無効になってしまうなどの事故が発生しても、ユーザーへの被害を最小限にするための手法です。過去にも、ZSK (Zone Signing Key) やKSK (Key Signing Key) が有効期限切れとなり、ゾーン全体が無効となってしまう事故が発生しています。この場合、DNSSECによる検証を有効にしたリゾルバを使っているユーザーは、そのゾーン全体を検索することができなくなってしまいます。これがISPや企業のリゾルバサーバであれば、ユーザーはそのゾーンが検索できないことに対するクレームを出し、結局リゾルバサーバ管理者は、そのリゾルバサーバのDNSSEC検証を無効にせざるを得ない事態となります。このような場合にも、このNegative Trust Anchorにより一時的にDNSSEC検証を無効にするドメインを指定することができれば、リゾルバサーバの管理者側で一時的な対応ができることになります。今のところ、企業やISPのDNSリゾルバサーバは全体的にDNSSECを使うか、使わないかという二つの選択肢しかありませんが、この提案は、DNSSECを使うかどうかをドメインごとに指定できることを目的としています。この提案に対しては前向きな意見が多く、レビューメンバーが募られ、引き続き議論が続けられることとなりました。

最後に、(3) のAutomating DNSSEC delegationの議論が行われました。これは、DNSSECのKSK rolloverをより簡単にする手法の提案です。現在のDNSSECでは、子ゾーンの管理者はDSレコードを作成し、それを親ゾーンに対して送付することで、信頼の連鎖を形成しています。一方、この提案では、現在親ゾーンに存在しているDSレコードを、CDS (Child DS) レコードで置き換えることでDSレコードの更新をほぼ自動化しています。CDSレコードはDNSKEYで署名されたレコードであり、子ゾーンの中のレコードとして発行されます。つまり、子ゾーンの管理者が自身のタイミングで自由に設定し、発行することが可能となっています。親ゾーンの管理者は、それを定期的に検証等することで、CDSが更新されていたらそれを検証し、親ゾーンに存在するDSレコードと置き換えることで、DSレコードの更新を行います。これによって、子ゾーンのKSKの更新時に、新たなDSレコードを親ゾーンに送付し、KSKをrolloverするという手順が簡略化されます。

この提案に対して、既存のツールが子ゾーンのDSレコードを親ゾーンに送付するという形での署名に対応したものとなっていたり、レジストラのビジネスモデルが既に存在したりすること等から、導入は難しいとの意見が出されました。その一方で、技術的には必要であるとの意見も出されました。結果として、レビューメンバーが募られ、引き続き議論が行われることとなりました。

◆ dnsext WG報告

dnsext WGは、特段の事情が無ければIETFにて会合を開催しないことが合意されているため、今回も会合は開催されませんでした。ドラフトもdraft-ietf-dnsext-dnssec-algo-signalがIESG Last Callの段階であり、draft-ietf-dnsext-dnssec-algo-imp-status、draft-ietf-dnsext-rfc2671bis-edns0、draft-ietf-dnsext-rfc6195bisの三つのドラフトがRFCエディタ待ちになっているという状況で、これ以外にActive WGドラフトは存在しません。着実にWGをクローズする段階に入っていると言えます。メーリングリスト上では、前回のIETF 85から、draft-ietf-dnsext-dnssec-algo-signalとdraft-ietf-dnsext-dnssec-algo-imp-statusの議論、RFC5155の修正点に関する議論が行われた他は、散発的な議論が行われるのみでした。RFC5155の修正点に関しては、いくつかの指摘がなされ、用語的な指摘と、より間違いの無い定義をめざした文章への変更でした。どれも新たな提案ではなく、大きな議論も発生しませんでした。

(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)


● 参加者同士の交流の場、Bits-N-Bitesは大盛況でした

IPv6関連WG報告

米国オーランドにて開催された第86回IETFのWorking Group（WG）の中で、筆者が会合に参加したIPv6に関連するWGの中から6man WG、v6ops WG、softwire WG、sunset4 WG、homenet WGについて、議論の概要をご紹介したいと思います。

◆ 6man WG（IPv6 Maintenance WG）

6man WGは、IPv6プロトコルのメンテナンスを目的としたWGです。今回は会期最終日となる2013年3月15日（金）のタイムスロットで行われたため、発表者のフライトの都合を考慮し、WGアイテム、メーリングリスト（ML）で活発に議論されているドラフト、その他のドラフトという順番に入れ替えて、プレゼンテーションが行われました。

今回は6man WGのチャーター変更に関する議論が行われ、インタフェースIDのU/Gビットにおける問題や、フラグメントおよび拡張ヘッダに関する取り組み、IPv6 over Foo（何らかの仕組み上でIPv6を使用）に関する取り組みが追加アイテムとして挙げられ、その他にもいくつか検討すべき追加アイテムの案が挙げられました。WGチェアとしては、検討アイテム以外にもコミュニティが必要としているものがあれば、これらの検討アイテムはそれを妨げるものではないとの考えを示しており、既に活動中のWGにおいては、チャーター変更はWGの活動に大きな影響を与えるものではないと感じました。

今回のセッションで議論が行われた、いくつかのトピックについてお伝えします。

1. Transmission of IPv6 Extension Headers（IPv6拡張ヘッダの転送）
draft-carpenter-6man-ext-transmit-02

現在のインターネットにおいては、IPv6拡張ヘッダがトランスペアレントに取り扱われているとは言えず、将来の拡張用に定義されたTLV形式の拡張ヘッダフォーマット（RFC 6564）を解釈できないルータやFirewallも多数存在しています。このような現状において、中間ノードであるそれらの装置が拡張ヘッダをどのように取り扱うべきかを明文化することで、問題を少しでも減らしたいというのがこの提案のモチベーションになっています。

この提案ではいかなる拡張ヘッダも転送すべきであり、Firewallなどのノードでは新規の拡張ヘッダも識別して、default設定では定義されているすべての拡張ヘッダを許容すべきとされています。またホップバイホップオプションについては、高性能ルータなどでは破棄されたり、スローパスとして扱われたりすることが想定される旨の記載が含まれています。

プレゼンテーションの最後に本提案をWGアイテムとして採択すべきかハミングが行われ、賛同者が多かったため、ML上で最終的なコンセンサス確認が行われることになりました。

※ その後、ML上でのコンセンサス確認の結果、2013年3月30日（土）にWGアイテムとして正式に採択されています。

2. The U and G bits in IPv6 Interface Identifiers（IPv6インタフェースIDにおけるU/Gビットの取り扱い）
draft-carpenter-6man-ug-01

RFC 4291にて定義されているU/Gビットは、主にModified EUI-64フォーマット生成時に用いられており、その他にはPrivacy Extensions for SLAAC（RFC 4941）、CGA（RFC 3972）、HBA（RFC 5535）、4rd（draft-ietf-softwire-4rd）などで定義されているものの、意味を成す値として用いられていません。また、それぞれの定義においても一貫性が無く、あいまいな情報として現状取り扱われているため、混乱を避けるためにU/Gビットの定義を明確に記述しようというのが本提案です。U/Gビットの有用性としては、インタフェースIDがModified EUI-64フォーマットで生成されている場合に、MACアドレス情報に変換できることから運用面で故障診断の助けになったり、U/Gビットを考慮したインタフェースID生成を行っている方式であれば、インタフェースID重複の可能性を低減させることができたりすることなどが挙げられます。

会場からは、Modified EUI-64フォーマットについて明確に記述した方がよいという意見や、IPv6 Addressing of IPv4/IPv6 Translators（RFC 6052）もU/Gビットを考慮しているので参照した方がよいといった意見がありました。

なお、その後のプレゼンテーションでは、6man WGチェアであるBob Hinden氏より6man WGのMLで行われた多くの議論の結果として、インタフェースIDには特別な意味を持つビットは無く、いかなる文書もインタフェースIDに意味を持たせるべきではないとの結論に至ったことが説明されました。

ISATAP（RFC 5214）などはインタフェースIDに独自の定義を行っているという会場からの意見に対しては、各ドキュメントで独自の定義を行うことは構わないが、それ自体は何ら保障が無いものである（例えばインタフェースIDの競合は無いと想定することはできない）と発言されました。

本提案をWGアイテムとして採択すべきかどうかは、ML上でコンセンサス確認が行われることになりました。

※ その後、ML上でのコンセンサス確認の結果、2013年3月30日（土）にWGアイテムとして正式に採択されています。

3. Updates to the IPv6 Multicast Addressing Architecture（IPv6マルチキャストアドレス体系の更新）
draft-boucadair-6man-multicast-addr-arch-update-00

本提案は、Unicast-Prefix-based IPv6 Multicast Addresses（RFC 3306）や、Embedding the Rendezvous Point（RP）Address in an IPv6 Multicast Address（RFC 3956）にてreservedとして定義されている領域（17-20ビット）を、すべてのIPv6マルチキャストアドレスで汎用的に使用可能なフラグとして定義しようというものです。この新しいマルチキャストアドレスのフォーマットの定義により、あいまいなフラグの解釈を明確にしつつ、将来の拡張も容易にしていこうというものです。本提案では、これを実現するために分離されているビットを、フラグビットとして取り扱うことをMUST要件としています。

会場からは、マルチキャストのフィルタリングを行う際にこのフラグビットが影響を与えるかもしれないので、このビットを独立したビットとして扱うか、あるいはビットのグループとして扱うかを明確にする必要があるとのコメントがありました。提案者からは、これはIPv6マルチキャストが広く普及する前に定義を変更する、最後のチャンスであるとの考えが示されました。

プレゼンテーションの最後に本提案をWGアイテムとして採択すべきかハミングが行われ、賛同者が多かったため、ML上で最終的なコンセンサス確認が行われることになりました。

※ その後、ML上でのコンセンサス確認の結果、2013年3月30日（土）にWGアイテムとして正式に採択されています。

□6man WG
http://tools.ietf.org/wg/6man/

□第86回IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/86/agenda/agenda-86-6man

◆ v6ops WG（IPv6 Operations WG）

v6ops WGは、IPv6運用上の問題解決のための議論を第一優先として、その他にはIPv6普及に向けた運用上のガイドラインなども取り扱うWGです。2013年3月11日（月）と13日（水）の二つのタイムスロットで実施されましたが、いずれのタイムスロットでも、予定していた時間よりかなり早く終了するという状況でした。

今回のセッションで議論が行われた、いくつかのトピックの概要についてお伝えします。

1. NAT64 Deployment Considerations（NAT64使用時の考慮事項）
draft-ietf-v6ops-nat64-experience-01

本ドキュメントは、NAT64の展開シナリオと運用上の経験について記載されたもので、Working Group Last Call（WGLC）を終えた段階にあります。今回のプレゼンテーションは、WGLC中に寄せられたコメントとしてStateless NAT64に関する記述を含めるかどうかと、今後の進め方について確認を求めるものでした。また、WGLC中のコメントなどフィードバックが少なかったため、このまま標準化を進めるべきかどうか提案者としては懸念している、という発言がありました。

会場からは、タイトルがExperienceからConsiderationsに変更された点について、ドキュメントは提案者の経験に基づき記述されており、より一般的な情報として参照できるレベルとは言えないので、Experienceに戻すべきだという指摘がありました。また、Google社がWebページの表示を高速化する目的で開発したSPDYのような、持続性のあるセッションを扱うプロトコルの存在が、NATデバイスに与える影響についての知見が不足しているので、Experienceに戻すべきだとの意見もありました。今後の進め方として、タイトルをExperienceに戻して、かつ現在のコメントを反映した版で再度WGLCが行われることになりました。

2. Extending an IPv6 /64 Prefix from a 3GPP Mobile Interface to a LAN（/64プリフィクスを3GPPモバイルインタフェースからLANへ拡張する方法）
draft-ietf-v6ops-64share-03

本提案では、3GPPネットワークにおいて、DHCPv6-PDが利用できない環境下について取り扱っており、User Equipment（UE）の3GPPモバイルインタフェースがモバイル網からRAで/64のプリフィクスを取得した際に、同じプリフィクスをLANでも使用可能にするための、次の三つのユースケースについて提案しているものです。

（1）UE上にグローバルアドレスを一切保持しないケース

（2）グローバルアドレスをLAN側だけに割り当てるケース

（3）同じグローバルアドレスをエニーキャストアドレスとして3GPPモバイルインタフェースとLAN側の両方に割り当てるケース

なお、別の手法として既にRFC 4389として標準化されているND Proxyがありますが Experimental Statusであり、またループ回避に関する制限事項があることが、本提案の動機になっています。

会場からは、おのおののユースケースにおいて、ローカルアプリケーションに与える影響についても考慮すべきとのコメントがありました。WGLCを行うかどうかについての確認では1/4程度の賛同は得られたものの、ML上での議論を継続して判断することとなりました。

その後すぐにML上で議論が開始され、IETF会期後半まで非常に多くの議論が行われました。3GPP standardに違反しないのかとか、USBドングルやdriverの存在により想定外の挙動になったりしないのかとか、短期/中期解として本方式を使うのではなく、やはりDHCPv6-PDを使うべきではないかなど多くの提案やコメントが寄せられました。

3. Balanced Security for IPv6 CPE
（IPv6 CPEのためのバランスの良いセキュリティ）
draft-v6ops-vyncke-balanced-ipv6-security-00

本提案は、スイスのSwisscom社が展開しているIPv6 CPEのセキュリティ要件を参考例として、セキュリティレベルとEnd to Endの接続性を適度にバランスしたポリシーを提供することを目的としたものです。実際、マーケティング部門はセキュリティを重要視するのに対し、多くのエンジニアはEnd to Endの接続性を重要視しているので、良い落としどころを見つけて情報提供することがこの提案の主旨であると言えます。

これまでの標準化の議論では、Recommended Simple Security Capabilities in CPE for Providing Residential IPv6 Internet Service（RFC 6092）がすべてのInbound Trafficをブロックするか許容するかの2択としているのに対して、Advanced Security for IPv6 CPE（draft-vyncke-advanced-ipv6-security-03）[Expire]では、IPSやReputation Databaseなどを必要とするなどハードルがかなり上がっているため、ほどよくバランスされたセキュリティポリシーを必要としているという背景事情があります。

会場からは、新しいアプリケーションやインシデントなどの事情によりポリシー変更を伴う場合に、どのようにしてドキュメントを更新していくのかといった質問や、このセキュリティポリシーにより実際にどの程度のインシデントが抑制されているのかなど、運用上のフィードバックがより必要であるとの発言がありました。提案者によると、Swisscom社は2012年からIPv6 CPEを展開しているが、今のところインシデント報告はされていないとのことでした。

その後、本提案をWGアイテムとして採択すべきかハミングが行われましたが、賛成／反対が半数ずつに分かれたため、ML上で継続して議論を行うことになりました。

4. Guidance of Using Unique Local Addresses
（ULA 使用に関するガイド）
draft-liu-v6ops-ula-usage-analysis-05

本ドキュメントでは、Unique Local IPv6 Unicast Addresses（RFC 4193）自体のメリット／デメリットの分析とともに、ULAの使用が推奨されるユースケースのガイドとして記述されています。なお、推奨されるユースケースとしては、次の3点が記述されています。

（1）インターネット接続から独立した、いわゆる閉域ネットワークでULAのみを利用
（2）ULAとGUA（グローバルユニキャストアドレス）の両方を利用
（3）特別なユースケースとして、B2Bのようなプライベートネットワーク間の接続における利用や、NAT64プリフィクスとしての利用、上位レイヤにおける識別子としての利用

なお、ULA + Proxyや、ULA + NPTv6は、取り得るユースケースとしては分析されていますが、推奨されるユースケースには含まれていません。

会場からは、ULAとGUAの両方を利用する場合、大規模ネットワークでは誰がそれを実際にやってるのか疑問だという意見があり、小規模での適用なら同意できるとコメントされました。また、特別なユースケースは、おのおのPros/Consがあるはずで推奨されるユースケースではないので、ユースケースの整理はより明確に記述すべきといったコメントがありました。その他のコメントとしては、ULAの境界ルータではどのように振る舞うべきかといった事項が記述されておらず、明確な記述が必要だとするコメントもありました。

その後、本提案をWGアイテムとして採択すべきかハミングが行われましたが、少数の賛成と、反対はほぼ無しという結果だったため結論は出さず、ML上で継続して議論しつつ、方向性を決定していくことになりました。

※ **会期終了後から本稿執筆時に至るまで、ML上で数多くの議論が行われていますが、ULAの運用経験がまだまだ少ないことから、ドキュメントのカテゴリはBCP（Best Current Practice）ではなく、Informationalとして進めようという意見が大多数となっている状況ではあるものの、まだ結論は出ていません。**

□v6ops WG
http://tools.ietf.org/wg/v6ops/

□第86回IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/86/agenda/agenda-86-v6ops

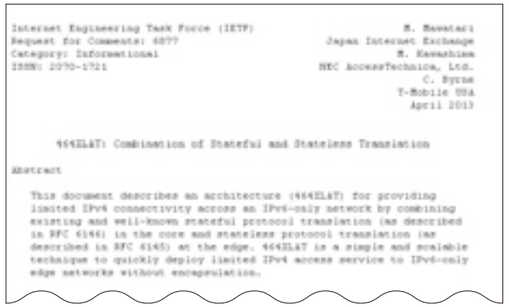
［おまけ］draft-ietf-v6ops-464xlatに関して

筆者が共著者の1人として、v6ops WGに提案していた464XLAT: Combination of Stateful and Stateless Translation（draft-ietf-v6ops-464xlat）ですが、IETFの会期直前にRFC Editor Process（AUTH48 status）に進むことができたため、本セッションでプレゼンテーションを行うことはありませんでした。

なお、本提案は2013年4月3日（水）にRFC 6877として正式に発行されました。

（参考URL）http://www.necat.co.jp/press/2013/pre_01.html

この場をお借りしまして、464XLATの提案をご支援いただきました関係者の皆さまにお礼を申し上げたいと思います。さまざまなアドバイスやご支援をいただきまして、本当にありがとうございました。


Internet Engineering Task Force (IETF)
Request for Comments: 6877
Category: Informational
ISSN: 2070-1721

M. Mawatari
Japan Internet Exchange
M. Kawashima
NEC AccessTechnica, Ltd.
C. Byrne
T-Mobile USA
April 2013

464XLAT: Combination of Stateful and Stateless Translation

Abstract

This document describes an architecture (464XLAT) for providing limited IPv6 connectivity across an IPv6-only network by combining existing and well-known stateful protocol translation (as described in RFC 6146) in the core and stateless protocol translation (as described in RFC 6145) at the edge. 464XLAT is a simple and scalable technique to quickly deploy limited IPv4 access service to IPv6-only edge networks without encapsulation.

● RFC 6877 冒頭部分（http://tools.ietf.org/rfc/rfc6877.txt より）

◆ softwire WG（Softwires WG）

softwire WGは、IPトンネリングを用いてアクセス網などのネットワークを構成する手法を取り扱っていますが、ここ数年は特にIPv4アドレス在庫枯渇対策技術にフォーカスした議論が行われています。現在のチャーターでは、6rd、DS-Liteに加え、MAP-E等のステートレスソリューションが対象となっています。

今回議論された中で筆者が特に興味を持ったのは、Unified IPv4-in-Softwire CPE（draft-ietf-softwire-unified-cpe-00）の提案でした。この提案は、一つのCPEがDS-Lite、Lw4o6（Lightweight 4over6）、MAP-Eなどの複数のIPv4 over IPv6機能を有する場合に、このようなCPEはどのように振る舞うべきか、またおのおのの方式でどのようなパラメータが必要で、どのような方法でプロビジョニングを行うのかといった内容が記述されています。会場からは、各方式のパラメータを取得する具体的な方法や、MAP-Tなど他の方式の扱いはどうするのかなどについて、コメントや意見が寄せられました。

その他には、MAP-EのWorking Group Last Call（WGLC）に向けた最終確認、Lw4o6のupdate（前述のUnified CPEとの関連を説明）、DS-Lite MIB、Softwire Mesh MIB、MAP-E MIBなどの各種MIB（Management Information Base）定義の提案、DS-Liteの障害検知や冗長化方法に関する提案などが行われました。

※ **Lw4o6はML上でのコンセンサス確認の結果、2013年4月5日（金）にWGアイテムとして正式に採択されています。なお、MAP-Eは現在WGLC中です（2013年4月9日現在）。**

今回、softwire WGは、2013年3月11日（月）と13日（水）の二つのタイムスロットで実施されましたが、v6ops WGと同様にいずれのタイムスロットでも、予定していた時間よりかなり早く終了するという状況でした。これまで長らく続けられてきた、IPv4アドレス在庫枯渇対策技術の乱立による激しい議論は、ようやく収束したと言えそうです。

□softwire WG
http://tools.ietf.org/wg/softwire/

□第86回IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/86/agenda/agenda-86-softwire

（NECアクセステクニカ株式会社 川島正伸）

ルーティングセキュリティとPKI関連の動向

本稿では、セキュリティ関連関連の話題の中で、インターネットのルーティングセキュリティに関するSIDR WG（Secure Inter-Domain Routing WG）とPKI（Public-KeyInfrastructure）の動向について報告します。

◆ SIDR WG

SIDR WGは、インターネットにおける経路制御のための、PKI技術を使ったセキュリティの仕組みを検討しているWGです。

第86回IETFでは、WGの会合が二つのタイムスロットで行われました。議題からも検討内容が多いことがうかがわれます。50名から60名が参加しており、2年前にも見かけた常連の参加者によって議論が進められている様子でした。

○ Origin Validationに関わるRFC化が進む

SIDR WGでは、大きく分けて2段階の仕組みが検討されて

います。一つはOrigin Validationと呼ばれ、インターネットのルーティングにおいて他のネットワークのIPアドレスが使われた場合に、不正な経路情報を検知する技術です。

筆者が参加した、2年前の第79回IETFミーティングのときにはまだドラフト段階であった、Origin Validationのドキュメントのほとんどがすでになっていました。主なRFCを挙げます。

- **An Infrastructure to Support Secure Internet Routing (RFC6480)**
  http://tools.ietf.org/html/rfc6480
  PKIを使ったセキュアなルーティングの全体像を記述したRFC

- **A Profile for X.509 PKIX Resource Certificates**
  http://tools.ietf.org/html/rfc6487
  セキュアなルーティングのための証明書の書式を規定するRFC

- **Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations(ROAs)**
  http://tools.ietf.org/html/rfc6483
  経路情報を確認するための署名検証の考え方を記述したRFC

またSIDR WGでは、ここ2年ほど、もう一つの仕組みのPath Validationに関する検討が行われています。Path Validationとはインターネットの経路を意図的に変えてしまうような、不正なASパス情報を検知する技術で、Origin Validationの使用を前提としています。両方を合わせた仕組みはBGPSECと呼ばれています[※1]。

今回のミーティングでは、このBGPSECの中核となるプロトコルと、その実現に必要な鍵管理の仕組みの文書がアジェンダとして取り上げられましたが、会場での議論はほとんどなく、引き続きメーリングリストで議論されることになりました。

○ IPアドレス移転への対応で議論を呼んだAPNICのRPKI

前述のOrigin Validationには、IPアドレスが記載されたリソース証明書が使われます。IPアドレスが移転される場合、リソース証明書は、移転元で失効され、移転先で新たに発行されるという手続きが必要になってきます。

APNICでは、RIR間でIPアドレスが移転されるときの、リース証明書の失効と発行の実験を行っていますが、他のRIRにはない特殊な仕組みが導入されました。他のRIRから移転されたIPアドレスのリソース証明書をAPNICにおいて扱いやすくするため、移転元がRIPE NCCである場合の認証局や移転元がARINである場合の認証局が立ち上げられているのです。つまり、APNICにおいて五つのRIRの認証局が立ち上がることになります。

この仕組みに関して、SIDR WGでは多くの意見と質問が挙げられ、ミーティングの半分くらいの時間が割かれることになりました。例えば、筆者は国際移転が複雑になり過ぎてしまう点を指摘しました。NIRへの移転を視野に入れるとAPNICにおける五つのRIRの認証局とNIRの認証局がどのようなつながりを持つのかを整理しなければなりません。

さらに会場からは、特定のサイズ(/16以上)のアドレスブロックがNIRに移転されたときに、適切にリソース証明書を発行できない点などが指摘されました。発表者のGeorge Michaelson氏はこの議論を進めるのではなく、この場ではコメントを受けるに留めました。

このほかにSIDR WGでは、ROA配布の性能や冗長性に関する議論が行われました。

- **IETF-86 sidr agenda**
  http://tools.ietf.org/wg/sidr/agenda?item=agenda-86-sidr.html

◆ PKIに関する話題

第86回IETFでは、PKIの仕様を策定してきたPKIX WGのミーティングが最終回とされていたことに加え、現在のWebにおけるPKIのモデルを整理して見直す、WPKOPS WG(Web PKI Operations WG)が始まったり、新しいPKIのモデルを検討する非公式のBoFが開かれたりしました。

○ 最終回として開かれたPKIX WGミーティング

PKIX WGは、インターネットのためのPKI技術の仕様を検討しているWGです。40名程が参加しており、40分程度の短いミーティングでした。はじめに、セキュリティエリアディレクターのSean Turner氏から、1995年に始まったPKIX WGはいまクローズの方向にあり、今回のミーティングを最終回にしたいという連絡がありました。WGでは次が議題になりましたが、特に多くの議論は行われませんでした。

- **Enrollment over Secure Transport**
  http://tools.ietf.org/html/draft-pritikin-est-02/
  クライアント証明書などの証明書入手のためのプロトコル

- **Authentication Context Extension**
  http://aaa-sec.com/_temp/draft-santesson-auth-context-extension-04.txt
  認証連携の際にユーザー証明書に付随する情報を伝えるための証明書拡張

今後、PKIに関する仕様の更新が必要になったときに議論のできるWGがあるのかどうか、先の見えない状況です。

○ WebにおけるPKIモデルのドキュメント化活動 - WPKOPS WG

WPKOPS WG(Web PKI OPS)は、World Wide Webで使われているPKIの実装の多くが、どのような動作をしているのかをモデル化するなどして整理するWGです。2013年2月にWGが設置されてから初めての会合です。

WGでは、Webにおけるサーバ認証やクライアント認証の基本的なPKIの信頼モデルを図式化したり、証明書の失効が、SSL/TLSの接続を確立するかどうかの判別に対してどのような意味を持っているのかという議論の下地作りとして、CRL(Certificate Revocation List)やOCSP(Online Certificate Status Protocol)の基本的な役割の確認が行われたりしていました。

WebブラウザやWebサーバが、明文化されていないモデルに基づいて実装されていることで、本来PKIでできることが実現していなかったり、実装によって違いが出てきてしまったりしているのではないか、という観点が興味深いWGです。

□Wpkops Status Pages
http://tools.ietf.org/wg/wpkops/charters

○ Alternative PKI model - 新たなPKIのモデルに関する非公式のBoF

最後に非公式に行われたBoFを紹介します。新たなPKIのモデルや仕組みを考えるAlternative PKI modelと題されたBoFです。BoF自体は人気のBits-N-Bitesの時間と重なっていたり、議題や資料がなかったりしたため、参加者約20名が現在のPKIのモデルについてさまざまな意見を交わすだけで終わりました。

次はBoFの進行と今後の議論のために会場でまとめたものですが、このBoFでPKIについて再検討の余地あり、という意見が出た点を紹介します。

a. エンドユーザーから見た認証局の透明性
　エンドユーザーの視点では認証局の証明書が正しいものであることが分かりにくいため、不正な証明書の検知に役立ったCertificate Transparency(CT)のような新たな仕組みの必要性の指摘です。

Certificate Transparency
http://www.certificate-transparency.org/

b. 認証局とその監査費用のコストモデル
　Webブラウザにインストールされている証明書の認証局は、毎年、監査を受けるとともに、その高額な費用を支払っています。一方で、エンドユーザーにおけるセキュリティの恩恵に対して支払われる対価(証明書の費用)は、その認証局監査の負担とのバランスが取りにくい、と言われています。持続的なPKIのためには再検討が必要だ、という指摘です。

c. PKIにおけるインシデント対応
　不正な証明書が発行されたようなときに、認証局におけるインシデント対応の整備が不十分であるという指摘です。

2011年から2012年にかけて、認証局やPKIを構成する技術に関するさまざまな攻撃とインシデントの報告がありました。Alternative PKI modelの参加者のみならず、会場で話をした他のIETF参加者からも、現在のままのPKIではなく何かを変えていく必要があるのではないか、という危機感に似たものを感じました。

(JPNIC 技術部／インターネット推進部 木村泰司)

※1 7. インターネット経路制御のセキュリティに関する動向 - BGPSEC
http://www.ipa.go.jp/security/fy23/reports/tech1-tg/b_07.html

● 2013年4月18日(木)に、ISOC-JPとの共催によりIETF報告会(86thオーランド)を開催しました