JPNIC Newsletter

Japan Network Information Center

for JPNIC Members

No.44
March 2010

【巻頭言】
インターネットコミュニティの責任
JPNIC事務局長／林 宏信

【特集1】
国際的に整備が進められるリソースPKI

【特集2】
Internet Week 2009開催報告

第3回 **IPv4枯渇 Watch**
～IPv4アドレス在庫枯渇問題についてのおさらい、現状の把握と要検討項目の再整理～

【インターネット 歴史の一幕】
国際化ドメイン名の標準化
株式会社日本レジストリサービス 米谷 嘉朗

【会員企業紹介】
さくらインターネット株式会社
代表取締役社長 田中 邦裕氏

【インターネット 10分講座】
暗号アルゴリズムの危殆化

■江崎 浩のISOC便り【第9回】

■活動報告

■インターネット・トピックス

■統計情報

JPNIC

JPNIC Newsletter for JPNIC Members

March 2010　No.044

CONTENTS

1 【巻頭言】
インターネットコミュニティの責任
JPNIC事務局長／林 宏信

2 【特集1】
国際的に整備が進められるリソースPKI

6 【特集2】
Internet Week 2009開催報告

14 【第3回】
IPv4枯渇 Watch

16 【第9回】
江崎 浩のISOC便り

17 【インターネット 歴史の一幕】
国際化ドメイン名の標準化
株式会社日本レジストリサービス 米谷 嘉朗

18 【会員企業紹介】
さくらインターネット株式会社
代表取締役社長 田中 邦裕氏

26 ■活動報告
活動カレンダー（2009年12月～2010年3月）
第39回JPNIC臨時総会報告
第17回JPNICオープンポリシーミーティング報告
第26回ICANN報告会レポート

32 ■インターネット・トピックス
APNIC28ミーティング報告
第59回RIPEミーティング報告
ICANNと米国政府との新しい関係～「責務の確認（AoC）」の締結～
ICANNソウル会議報告
第76回IETF報告

60 ■統計情報

64 【インターネット 10分講座】
暗号アルゴリズムの危殆化

69 ■会員リスト

■お問い合わせ先

巻頭言

JPNIC Newsletter for JPNIC Members

インターネットコミュニティの責任

2009年の12月にJPNIC事務局長を拝命しました。よろしくお願い申し上げます。私は、JPNIC事務局に関わるまで、インターネットコミュニティとは全く無縁の門外漢でした。

私がインターネットに初めて触れたのは、1994年になります。産業界ではトップを切って、前々職であった総合商社がPC一人一台の導入を図り、その翌年に世界各国のブランチ等との連絡を、これまで慣れ親しんできたテレックスからイントラネットに変更しました。それと同時に、個人的にもPCを購入、プロバイダと契約しました。最初の頃のメールは、テレックス文章をそのまま使っていたことが思い出されます。

その後は、ビジネスとしていくつかのクリック&モルタル型のリテイル事業やオンラインでサービスを提供する事業を新規事業として立ち上げ、経営に携わってきましたが、ビジネスでも個人でも専らユーザーの立場での関わりにしか過ぎず、インターネットの歴史も、仕組みも、技術的なことに関しても全く知識はありませんでした。

今回初めてインターネットコミュニティの中に入って感じたことは、良くも悪くも日本のインターネットの世界は、形成されてから20年も経ておらず、未成熟で発展途上だということです。この十数年間の目覚しい発展と大変革は、まさに驚きを禁じ得ませんが、それも未だ道半ばでしょう。

おおよそすべての消費マーケットにおいて、成熟してくるとイノベーションの余地は少なくなり、マーケットの主役は最終ユーザーになり、開発研究、メーカー、流通は、進化し高い選択眼を持ったユーザーのニーズに応えるべく活動することのみが、生き残るための方法となっていくと言えます。画期的イノベーションが困難なマーケットにおいては、消費者ニーズから商品開発とサービスの提供がなされ、継続的で緩やかな発展がもたらせられるのではないでしょうか。

日本のインターネットにおいては、これまでの驚異的発展を推進してきた第一世代の先人たちに敬意を抱きつつも、未だその世代が主役であり、限られた個人が発言力も有しているように思います。インターネットは、今後も画期的なイノベーションがもたらされる余地が大きく、最終的にユーザーはより賢明な消費者へと成長していくでしょう。この状況下、インターネットコミュニティの第二世代の人材が、第一世代と同じく高い志と熱い想いを持ち、ユーザーの進化とともに、より広く人類の営みを豊かにしていくことへ貢献できるように、インターネットを正しく発展させていくことへコミットしていくことが重要であると思います。

インターネットの世界での発展をめざすだけでは、インターネットが本来持っている人類の発展に寄与するポテンシャルが、充分に発揮されずに役割を終えてしまうかもしれません。既に人類にとっては、欠かせないインフラとなっていることに疑いの余地はありませんが、未だ発展段階であり、今後の大変革もあり得るだけに、今後のインターネットコミュニティに関わる人々の責任は、重大であると強く感じざるを得ません。

JPNIC事務局長
林 宏信

■プロフィール　林 宏信（はやし ひろのぶ）

1982年伊藤忠商事（株）入社、テキスタイルの国内、輸出入ビジネス、労働組合執行部などを経験。1996年以降リテイル事業を中心とした新規事業開発、M&A、外資との提携、事業会社経営などを担当する。2004年消費者視点からの事業を新規開発するベンチャーである（株）エムアウトに参画。取締役として新規事業開発、事業経営全般、組織作りに取り組む。2009年12月より現職。趣味は走ること。

特集

国際的に整備が進められるリソースPKI

2008年にリソース証明書を提供し始めたAPNICに加えて、RIPE NCCやARINでも同様の試験的な提供が始まりました。RIRでは、2011年頃と予測されているIPv4アドレスの在庫枯渇時期よりも前の2010年度に、リソース証明書のための「リソースPKI」を準備すると言われています。特集1では、このリソースPKIの国際動向をお送りします。

リソース証明書とリソースPKI

2009年、新たにRIPE NCCやARINでリソース証明書の提供が開始されました。リソース証明書は、WHOISを使わなくても、IPアドレスやAS番号がインターネットレジストリを通じて割り振られたものかどうか、端的に言えば不正に使われているIPアドレスか否かを判別するための仕組みです。リソースとは、アドレス資源、すなわちIPアドレスやAS番号のことを指しています。

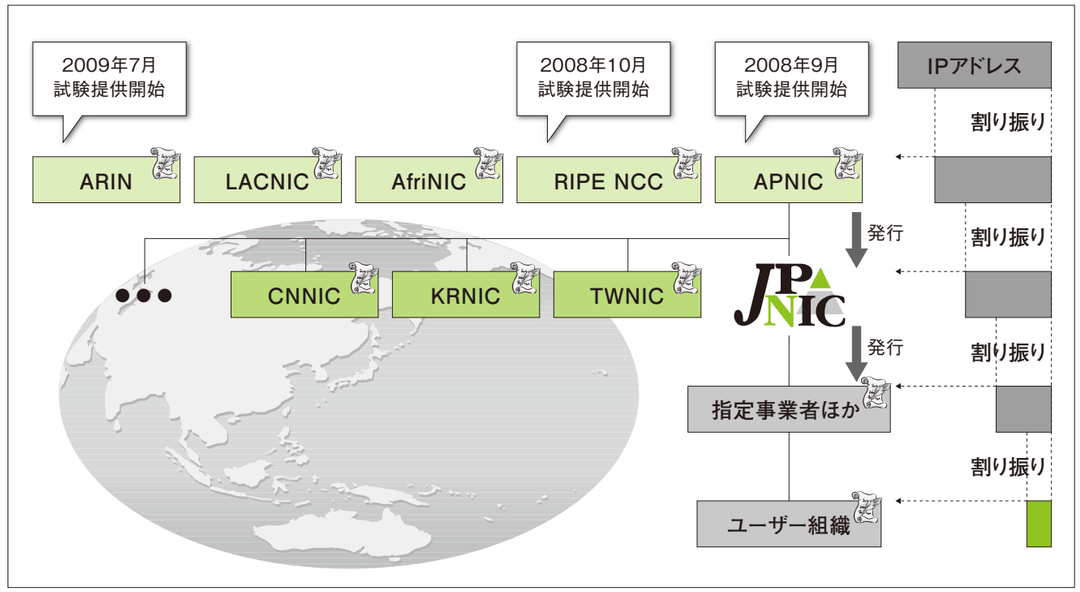
このリソース証明書を国際的に利用できるようにするため、RIRでは「リソースPKI」の整備が進んでいます。リソースPKIは、IPアドレスの割り振りや割り当ての構造に合わせてリソース認証局を設置することで、アドレス資源の利用者がリソース証明書の正しさを確認できるようにするものです。グローバルIPアドレスのリソースPKIは、図1のようにツリー構造になります。

図1の中でAPNICは2008年9月、RIPE NCCは2008年10月、ARINでは2009年7月に試験的に提供を開始しました。LACNICやAfriNICでも、リソース証明書に関する議論が行われています。

リソースPKI開発の経緯

リソースPKIのアイデアは、1997年頃、BBNテクノロジー社のStephen Kent氏、Charles Lynn氏らによって考案されました。当時研究が進められていたSecure BGP※1がそれで、IPアドレスやAS番号の正しさを担保するための仕組みです。伝搬してきたIPアドレスやAS番号を記載した情報（以下、「経路情報」と呼ぶ）のIPアドレスが正しいかどうかを確認し、不正な操作が行われている経路情報はルータで受け入れを拒否することができるメカニズムです。

図1：国際的な整備が進められるリソースPKI



BGPでは、インターネットでのIPパケットの到達性を確保するため、BGPルータ間で経路情報を交換しています。しかし、経路情報はいくつものBGPルータを経由して伝わっていくため、途中で変更が加えられていても、それを受信したBGPルータには変更が加えられたことはわかりません。また、経路情報の発信元であるBGPルータが、自組織に割り当てられていないような不正なIPアドレスを経路情報に記載していても、それが正しいかどうかを自動的に判別することは容易にはできません。

偽の経路情報を流すことができると、IPパケットの通る経路を、不正に操作することができる可能性があります。例えば、他の組織に割り当てられたIPアドレスを不正に使ったり、特定の組織のパケットを横取りして盗聴したり、目的のネットワークをインターネットに到達できないようにしたりすることが可能です※2。近年ではYouTubeのWebページが、ISPの意図的な経路広告によって閲覧できなくなった事件が有名です※3。

リソースPKIの目的

前節で述べたように、リソースPKIはもともとインターネットにおけるルーティングのセキュリティのために考案されました。リソースPKIに関連するプロトコルの策定が行われているIETFのSIDR（Secure Inter-Domain Routing）WGも、ルーティングのセキュリティ・フレームワークを作ることを目的としています※4。

しかし、リソースPKIの構築が進み始めた2007年には、別の目的についても議論されるようになりました。それが、リソースPKIを使った、アドレスリソースの利用権利の担保です。2007年7月、APNICのGeoff Huston氏により、レジストリのデータベースの正確性を保つために、IPv4アドレスの移転を認める提案が行われました※5。この頃より、リソースPKIは、移転されるようなIPアドレスの正確性を確認するための技術としても考えられ始めました。

リソース証明書が考案される以前は、IPアドレスの利用権利を表したり、保存したり、それが正しいのかどうかを電子的に検証したりできるようなデータ形式はありませんでした。IPアドレスがどこに割り振られているかという情報は、WHOISサーバにしかないため、WHOISサーバが攻撃されたり、トラフィックが不正に操作されたりすると、IPアドレスの正しさを調べられなくなってしまいます。一方、リソース証明書は電子証明書の形式であるため、記載されたIPアドレスが正しいかどうかを、WHOISサーバにアクセスせずに確認できます。

リソースPKIの普及状況

執筆時の2010年1月時点において、いくつかのRIRではリソースPKIの整備が一旦完了しており、リソース証明書の提供が始まっています。一方、WHOISサーバに対するWHOISクライアントのように、リソースPKIを利用してリソース証明書を確認するようなプログラムは、まだほとんど普及していない状況です。

以下に、RIRの動向をまとめます。

- APNIC

2008年9月、APNICのIPアドレス申請業務を行うためのポータルサイト"My APNIC"で、リソース証明書の提供が実験的に始まりました。

APNICはRIRの中でもリソースPKI関連の開発において、先導的な立場を取っているRIRです。2006年頃、他のRIRに呼びかけて、RPKIエンジンと呼ばれる主要部分の開発を行い、2007年にはユーザーインタフェースやレジストリデータベースとの連携部分の開発を行ってきました。APNICのGeoff Huston氏は、設立当初よりIETF SIDR WGのチェアを務めてきました。

- RIPE NCC

2009年2月、RIPE NCCの申請業務を行うためのポータルサイト"LIR Portal"で、リソース証明書の提供が始まりました。

RIPE NCCでは2008年10月以前から"Certtest"と呼ばれる、誰でもリソース証明書を取得できるWebページを提供しており、実際に入手してもらったり、管理Webインタフェースを使ってもらうことで、リソース証明書に関する議論を活性化する活動を行ってきました。

この他に、RIPE NCCの事務局内でリソース証明書の発行業務が可能かどうかを検証する"CertPROTO"プロジェクトや、RIPE地域のLIRが参加し、RIPEにおけるリソース証明書のあり方を議論する"Certification Task Force"が編成され

る等しました。

RIPE地域ではポリシーの提案も行われています。

2008年8月には、PAアドレスのリソース証明書に関するポリシー"2008-08: Initial Certification Policy for Provider Aggregatable Address Space Holders"が提案されました。

- ARIN

ARINでは、2009年7月にパイロットプロジェクトという位置付けでリソース証明書の提供を開始しました※6。このパイロットプロジェクトのWebページは、RIPE NCCが行っていた"Certtest"のWebページと似ており、RIPE NCCと同様にリソース証明書を試験する目的で設置されています※7。

- LACNIC

LACNICは、IETF SIDR WGにWG設立当初より積極的に参加しており、2006年以降継続して検討が行われているようです。LACNICミーティングでプレゼンテーションが行われたり、説明ビデオが製作されたりしており※8、コミュニティにおける議論の活性化が図られている模様です。

- AfriNIC

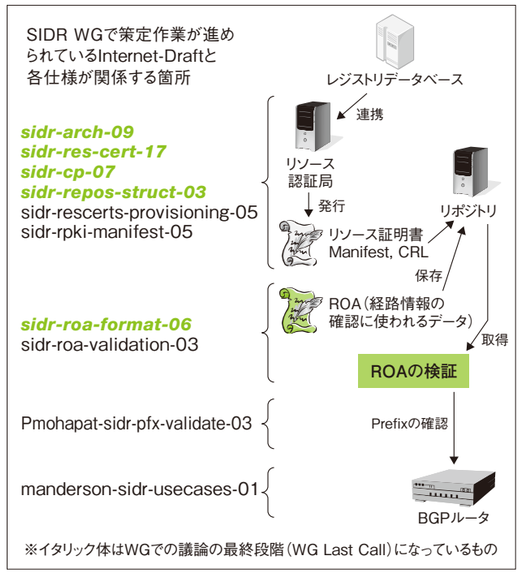
AfriNICでは、2006年頃前述のStephen Kent氏によるワークショップが開かれたり、AfriNICミーティングにおいてRandy Bush氏のプレゼンテーションが行われる等しており、情報収集の段階であるようです。しかし、AfriNICのレジストリシステムは、RIPE NCCのレジストリシステムをカスタマイズしたものであり、RIPE NCCと同様のシステムでリソース証明書を提供することは容易であると想像できます。

- IETF

IETFでは、SIDR WGにおいてリソースPKIに関わるRFCの策定が行われています。2009年11月、広島で行われたIETF-76では、WGでの議論が収束し、最終的なコメントを募集する"WG Last Call"がかけられたドキュメントが増えてきました。ドキュメントの策定状況を図2にまとめます。

図2：IETF SIDR WGにおけるドキュメント策定状況

IETF SIDR WGでは、RFC化は行われていないものの、"WG Last Call"が呼びかけられて、仕様がほぼ固まったドキュメントが増えてきた。



※イタリック体はWGでの議論の最終段階（WG Last Call）になっているもの

リソース証明書

リソース証明書の内容を図3に示します。

図3：APNICから発行されているJPNICのリソース証明書

```
Serial Number:  70092                                  ← シリアル番号
Signature Algorithm: sha256WithRSAEncryption           ← 署名アルゴリズム
Issuer:CN=APNIC Production-CVPQSgUkLy7p0XdNeVWGvnFX_0s ← 発行者
Validity                                               ← 有効期限
    Not Before:  Jan  8 17:46:11 2010 GMT              ← 開始
    Not After:  Sep 30 00:00:00 2010 GMT               ← 終了
Subject:CN=A91A7381                                    ← 発行先
X509v3 Basic Constraints: critical                     ← 認証局フラグ
    CA:TRUE
sbgp-autonomousSysNum: critical
    Autonomous System Numbers:                         ← AS番号
      2497-2528
      2554
          :
sbgp-ipAddrBlock:critical
    IPv4:                                              ← IPv4アドレス
      58.0.0.0/15
      58.3.0.0-58.5.255.255
          :
    IPv6                                               ← IPv6アドレス
      2001:240::/32
      2001:258::/32
          :
```

リソース証明書は、X.509形式［RFC5280］の電子証明書でバイナリデータです。以下のような特徴があります。

- 発行先の名称が記載されていない。
- IPアドレスやAS番号が記載されている。
- 認証局証明書として利用でき、リソース証明書の所有者は、記載されたIPアドレスの範囲内のIPアドレスが記載されたリソース証明書を発行できる。

リソース証明書には、WHOISに登録されているような連絡先情報等は記載されておらず、これだけでWHOISの代わりになるわけではありません。一方、記載されたIPアドレスがレジストリ経由で正しく割り振られたものであるかどうかは、リソース証明書を電子的に検証することで確認できるようになっています。

先に述べたルーティングセキュリティのためには、ROA（Route Origination Authorization）というデータが使われます。ROAには、経路情報として伝えられるOrigin AS番号とIPアドレスの情報が記載されています。リソース証明書を使って電子署名が行われているため、正しい経路情報であるのかどうかの確認に利用できます。ROAは、BGPのpeer（経路情報を交換するための接続）を行う前に、相手が使用しようとしているIPアドレスが正しいものであるかどうかを確認する手段としても考えられています※9。

リソースPKIとインターネットレジストリの今後

IPアドレスの管理には五つの原則（一意性・登録・経路の集約・アドレスの節約・公平性）があります。これらの原則は、インターネットの接続性とIPアドレスの持続を重要視したものと言えます。一方、リソースPKIはアドレス資源が正しいものであるかどうかを重要視するものです。これを厳密に捉えると、"正しいIPアドレスを使わなければ、インターネットにつなげられない"という考え方にもなります。今後もIPアドレス管理の原則は変わらないとは思いますが、IPv6アドレスの普及に伴って、量よりも正しさ、そしてその確認手段が重要な意味を持つようになるかもしれません。

一方、インターネットレジストリは、IPアドレスのユーザーにとって、なるべく負担が少なくなる仕組みで、IPアドレスを提供すべき組織です。IPアドレスの正しさを担保するために、ユーザーの負担が大きくなることはできるだけ避けなければなりません。

今後もRIRとIETF等における技術動向を日本のコミュニティの皆さんと共有し、インターネットレジストリのあり方について、皆さんと一緒に考えていきたいと思います。

（JPNIC インターネット推進部/技術部 木村泰司）

※1 BGP Countermeasures（Secure-BGP）
http://www.ir.bbn.com/sbgp/IETF42.ppt

※2 Revealed: The Internet's Biggest Security Hole
http://www.wired.com/threatlevel/2008/08/revealed-the-in/

※3 YouTube Hijacking: A RIPE NCC RIS case study
http://www.ripe.net/news/study-youtube-hijacking.html

※4 Secure Inter-Domain Routing（sidr）
http://www.ietf.org/dyn/wg/charter/sidr-charter.html

※5 IPv4 address transfers
http://www.apnic.net/policy/proposals/prop-050

※6 ARIN RPKI
https://www.arin.net/resources/rpki.html

※7 ARIN Resource Certification
https://rpki-pilot.arin.net/

※8 LACNIC Resource Certification
http://www.youtube.com/watch?v=wzdM_wHMXV8

※9 Certification Update（RIPE NCC）
http://www.ripe.net/ripe/meetings/ripe-59/presentations/band-certification.pdf

特集2

Internet Week 2009 開催報告

毎年恒例のJPNIC主催イベント「Internet Week」を、2009年11月末の4日間、東京・秋葉原で行いました。本稿では、イベントの全体報告とともに、最終日に行われたIP Meetingの開催レポートをお伝えします。

2009年11月24日（火）から27日（金）までの4日間、東京・秋葉原コンベンションホールにて、Internet Week 2009を開催しました。イベント準備段階では、景気の冷え込みや新型インフルエンザなどの影響から、参加者が減少するのではないかとの懸念もありましたが、おかげさまで前回より多い、延べ2,200名の方に参加いただくことができました。

Internet Week 2009では「インターネットの進化論」をイベントテーマに掲げ、インターネットの進化過程における、我々の現在の立ち位置を確認し、今後取り組むべき課題解決に向けての足掛かりを提示すべく、最新テクノロジーを扱うセッションから、今後も継続して検討が必要なインターネットの運用・技術に関わるセッションを実施しました。

具体的には、仮想化技術の解説とその実像に迫る「仮想化DAY」「クラウドの虚像と実像」、IPv4在庫枯渇問題対策/IPv6関連では、「v4枯渇時代のシステムインテグレーション」「IPv6“再”入門」「点検!IPv6のセキュリティ」、セキュリティ関連では、「インターネットセキュリティ2009」「一歩進めるインターネットルーティングセキュリティ」を行いました。また、運用に関わるセッションとして、「DNS DAY」「DNSSECチュートリアル」「運用方法論」を実施しました。その他、ドメイン名、インターネットをとりまく政策と規制、電子認証、インターネットと環境をテーマとしたセッションも行い、最終日の「IP Meeting 2009 ～インターネットの進化論～」にて、2009年のインターネットを総括する形で締めくくりました。

先のセッションのうち、「仮想化DAY」「IPv6“再”入門」「点検!IPv6のセキュリティ」「DNS DAY」は事前申し込みの時点で満席となり、特に近年注目を集めている仮想化技術や、2011年頃と迫りくるIPv4アドレスの在庫枯渇を前に、IPv6対応に関する参加者の関心の高さを感じました。その他、30歳代が参加者全体の約半数を占めるInternet Weekにおいて、20歳代の参加者が占める割合が高いプログラムとしては、「仮想化DAY」「DNSSECチュートリアル」「IPv6“再”入門」「一歩進めるインターネットルーティングセキュリティ」がありました。

また、開催初日から3日間は、夕方にInternet Week名物の一つであるBoFが行われました。今回は、おなじみのBoFに加え、「インターネットの歴史」について語り合うBoF、「ネットワークオペレーションを楽にするツール」について情報交換をしようという趣旨のBoF等、これまでなかった新しい視点の集いもあり、大勢の参加者とともに盛り上がりを見せていました。


■ 総合受付に並ぶ参加者の様子

■ 満席となった「仮想化DAY」会場内


■ ネットワークオペレーションを楽にするツールの情報交換会（BoF）の様子

セッション以外には、会場の共有スペースにて、協賛企業様による展示ブースや、新たな試みとして、メディアスポンサー様ご提供の推薦本・雑誌を、自由にご覧いただける「ライブラリーコーナー」も設置しました。参加者の皆様に楽しみながら情報収集ができる場として、ご活用いただけたなら幸いです。

◇　　◇　　◇

参加者アンケートの結果を拝見したところ、「大変役に立った」という割合が、前回の34.1%から今回は39.1%と満足度の向上が見られ、来年も「ぜひ参加したい」という方が全体の約6割弱を占めていました。また、Internet Weekへの参加動機は、やはり「セッション内容」が決め手となっていることが、フリーライティングのご意見等から読み取れました。今回このような評価をいただけたのは、参加者の関心や時代の流れともマッチした、よいセッションをご提供できたことによるのではないかと思っております。コンテンツ作りにおいては、長期間にわたり、約20名のプログラム委員の方が、幅広い知識と人脈、各々の個性を活かしながら、多種多様な意見を出し合い、一つ一つのセッションを丁寧に創り上げてくださいました。そこに込められた想いが、参加者の皆様にも届いたのではないでしょうか。

最後になりますが、今回も多くの参加者の皆様にお越しいただき誠にありがとうございました。また、Internet Week 2009にご理解と惜しみないご協力をくださいました、ご講演者様、協賛企業様、メディアスポンサー様、ご後援団体やプログラム委員の皆様、その他ご関係者様にも心より感謝申し上げます。

（JPNIC インターネット推進部 平井リサ）

■ Internet Week 2009

【会 期】2009年11月24日（火）～11月27日（金） 4日間
【会 場】秋葉原コンベンションホール
【URL】http://internetweek.jp/
【主 催】社団法人日本ネットワークインフォメーションセンター（JPNIC）
【企 画】Internet Week 2009プログラム委員会

【協 賛】NTTコミュニケーションズ株式会社
株式会社日本レジストリサービス
次世代バックボーンに関する研究開発プロジェクト
インターネットマルチフィード株式会社
株式会社SRA
シスコシステムズ合同会社
株式会社創夢
日本インターネットエクスチェンジ株式会社

【ネットワークスポンサー】
独立行政法人産業技術総合研究所（AIST）
シスコシステムズ合同会社
NECアクセステクニカ株式会社

【後援】総務省/文部科学省/経済産業省
IPv6普及・高度化推進協議会
財団法人インターネット協会（IAjapan）
仮想化インフラストラクチャ・オペレーターズグループ（VIOPS）
クライメート・セイバーズ コンピューティング・イニシアチブ（CSCI）
社団法人コンピュータソフトウェア協会（CSAJ）
一般社団法人 JPCERTコーディネーションセンター（JPCERT/CC）
社団法人情報サービス産業協会（JISA）
独立行政法人情報通信研究機構（NICT）
社団法人電子情報技術産業協会（JEITA）
社団法人日本インターネットプロバイダー協会（JAIPA）
日本DNSオペレーターズグループ（DNSOPS.JP）
財団法人日本データ通信協会（Telecom-ISAC Japan）
一般社団法人 日本電子認証協議会（JCAF）
日本ネットワーク・オペレーターズ・グループ（JANOG）
特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）
日本UNIXユーザ会（jus）
WIDEプロジェクト（WIDE）

インターネットは情報オペレーティングシステムとしては機能したが、現実社会のオペレーティングシステムとしても機能するのか?

~IP Meeting 2009 開催報告~

今回のInternet Week、そしてIP Meetingのタイトルは「インターネットの進化論」。そして、IP Meeting午後の部全体のディスカッションテーマは、「インターネットは地球規模オペレーティングシステムになりえるか?」でした。

現在のインターネットは、社会や多くのシステムがそれなしには動かないという意味において「インフラ」です。この「インフラとなったインターネット」に関わる我々は、今後、どうなっていくのかという予測を持てばいいのでしょうか、また何を見据えていけばいいのでしょうか。

今回のIP Meetingでは、このように誰も答えを持たない、ある種抽象的なテーマを選びました。これにはプログラム委員会でも賛否両論がありましたが、年に一度「IP Meeting」という場に人が集まり、それぞれの目で何かを語ることから意思が生まれていくかもしれないという期待もありました。

まず、JPNIC後藤滋樹理事長から「そもそも進化と退化とは」という話がありました。

- 「アナログ」から「デジタル」に移行すると、普通は元に戻れない。
- デジタル時代は、ブランド戦略が取りにくく、デジタルデフレでは利益の確保が難しい。
- コンピュータは、キャッシュが顕在化し、演算とストレージも分離した。インターネットは社会的認知向上を遂げた。
- 進化の点では、「電話との地位が逆転した」「動画の通信」「商用のインターネット」等が挙げられる。
- 退化の点では、「ホストカウントが減る」「通信速度の減速」「ネットワークのただ乗り論」「セキュリティ」「紛争も増加」等がある。
- 退化の原因は、技術的な運用や技術そのものではなく、すべては社会的な変動の影響や普及・成熟の結果である。
- インターネットを作ったのは人間だが、問題を起こすのはそれを「使う人」であり、インターネットがいろいろな人をカバーしているということ。
- 未来を語るということはなかなかうまくいかないが、インターネットは、政府などがビジョンを示さず発展した歴史があるので、「自分たちでビジョンを語ることも重要ではないか」と期待している。
- ただし何かを熱心に推進しようとしても、急進的な改革はうまくいかない。
- インターネットは、昔は軽かったが、今は乗る人が多すぎて飛べない。空飛ぶ絨毯は、重すぎると飛べない。
- 人間はなかなか考えが変わらない。頭はタンパク質でできているため、デジタル製品のように一晩でのダウンロード/リセットはできない。
- このように社会の変革は長丁場であるから、進化を語るには時間がかかることを考えて、健康第一で、頑張って欲しい。

その後、今回の難しいもくろみに対し、適切にテーマを投げかけてくださったのが、慶應義塾大学の斉藤賢爾さんです。「インターネットは地球規模オペレーティングシステムになりえるか?」を大前提とした、六つの切り口をパネリストに提起しました。

会場ではTwitterも利用されて(iw2009のハッシュタグの下に#evol)、議論がされました。ふたを開けてみれば、斉藤さんが提示した質問のほとんどに、それぞれの方が何らかの答えを示してくれた結果になったようにも思います。これを見て、思うところがあるか否か、また答えがあると感じるか否かは人それぞれでしょうが、ただ、どんなことでも考えてみる行為そのものが、進化にとっての第一歩であるのかもしれません。

基調講演「情報システムの進化と退化」を行うJPNIC理事長 後藤滋樹

問題提起:インターネットは地球規模オペレーティングシステムになりえるか?

斉藤 賢爾
慶應義塾大学 大学院 政策・メディア研究科

「地球規模オペレーティングシステムは何か?」と問われれば、地球をハードウェアとしたときの、オペレーティングシステム(OS)です。ハードウェアとしての地球の中には、さまざまな資源(リソース)があります。天然資源である化石燃料、水や、それ以外にも、建物、自動車、電気……また人間そのものも資源と言えるかもしれません。これらの資源を、コンピュータのOSのようにマネジメントして、ユーザーとしての人間に、アプリケーションを通じて利用させ、資源の循環がうまくいくように調整してくれる仕組みとして定義してみました。

人間が活動するにはエネルギーが必要であり、そのエネルギーを生み出すには資源が必要ですが、この資源を有効に使うためには、いくつかの側面で難しい問題があります。

化石燃料に頼ってそれを燃やすことで、温室効果ガスが出てきます。また、こういった化石燃料は有限の資源であるため、供給にはピークがあり、価格もその供給如何に左右されます。さらには、自然の循環から外れて水を消費することにより、水不足が起こることが懸念されています。

現在、実体経済活動を主として貨幣経済システムで動かしており、その情報交換手段として通信システムを用いています。しかし、この貨幣経済は、我々の社会で有効に機能しているでしょうか? 貨幣経済は情報的な経済活動です。実体的な経済活動と、情報的な経済活動の規模には、現在、大きな隔たりがあり、後者が前者を凌駕しています。

このような中で、次の問題提起をします。皆様、一緒に考えてみてください。

Q1. インターネットはエネルギーの使い方をどう変えるか?
Q2. インターネットは地域の自立をどう支援できるのか?
Q3. インターネットは貨幣を含む信頼と約束の基盤をどう変えるか?
Q4. インターネットは人間の住環境をどうプログラマブルにするのか? どうセキュアにできるのか?
Q5. インターネットは所有から共有への変化をどう起こし、持続させられるか?
Q6. インターネットは人類の活動の原資である発明・革新をどのように支援し続けられるのか?

午後のパネル「インターネットは地球規模オペレーティングシステムになりえるか?」の全景

Q1:インターネットはエネルギーの使い方をどう変えるか?
Q3:インターネットは貨幣を含む信頼と約束の基盤をどう変えるか?

秋山 卓司
日本クロストラスト株式会社

全人類の使っているエネルギーの総計は、現在15.8TWと言われています。また、人口は増えており、2050年には90億~100億人になるのではないかと言われています。こうなると、平均使用量が同じだとしたら、当然、エネルギーの使用総量も増えていきます。多くの地球上の資源は有限である中、これをどこまで使ってもいいのでしょうか。この頃、果たしてどういう世界ができていて、インターネットがどういう役割を果たしているのでしょうか。

「貨幣とは何か」を考えた場合に、「有限な資源を再配分するための道具」ということもできます。その貨幣が、社会の中で現況

特集2 Internet Week 2009開催報告

十分に機能しているかどうかと言われると、そうでもありません。そう考えると、貨幣に変わるリソース再配分の手段を見つけなくてはいけないのではないかと思います。そのツールとして、「インターネット」は十分その手段になり得るのではないでしょうか。

つまり、デジタルは有限な資源ではないということを考えると、無限のリソースの配分に、貨幣は使えません。エントロピーというものを再配分するのであれば、インターネットのような仕組みが必要で、資源の再配分においてインターネットは地球OSと言えるのではないでしょうか。

Q5: インターネットは所有から共有への変化をどう起こし、持続させられるか?

伊勢 幸一
株式会社ライブドア

2年前に事業会社としてできたライブドアの社是は、「オープンアンドシェア」です。全社員、UNIXというプラットフォームならびにインターネットというインフラの上で生きています。つまり、基本的に、ソースコードオープン、インターネットに端末をつないでリソースをシェアしています。そんな背景から、「所有から共有へ」ということを考えてみました。

所有型の生産活動では、資源や資産等の所有物を提供して対価を得ることで経済活動を行っています。一方、共有型の生産活動とは、お互いの資産を共有し、足りないところを補うことで対価を得る経済活動なのかと思っています。

このオープンとシェアによる生産活動は「共生」、つまり、互いの所有物を共有することで、全く新しい価値を創出することです。インターネットによってそれを行うことを「インターネット共生型」と言い、従来の所有物によって生産活動を行うのは「インターネット寄生型」と呼んでもいいかもしれません。このような「インターネット共生型」の例がいくつか見られるようになっていると思います。

ものすごい量の情報と交換する頻度がインターネットで生まれてきました。結果、インターネットの側でそれをコントロールするのは困難です。つまり中央でのコントロール制御では賄いきれず、情報公開に対するインテリジェンスがエンドの方に移ってきたのかなと思います。どういうことかと言うと、インターネット側では黙っていても何もしてくれません。テレビはスイッチを押せば情報が送られてきますが、インターネットはこちらからブラウザを立ち上げてアクションを起こさないと見返りはきません。ただし検索窓にワードを入れた瞬間、大量の情報がやってきます。

現在の課題・懸念は、我々の側に、情報を選別して解析する洞察力や能力が必要とされているのではないか、ということです。デジタルデバイドということが解消されて、すべての人へのコネクティビティがイコールになった次には、情報を選別して得る能力としての「リテラシー」が必要になってくるという問題が生まれてくるでしょう。

インターネットが地球規模OSとして、リソースを効率的に割り当てる基盤になるかということについて言えば、インターネット以外に、地球規模で人と人とのコミュニケーションを提供できるメディアがないのではないでしょうか。その中で、デバイドや熱やコストを考え、一つ一つをクリアしていくことが必要なことです。

最も重要なのは、変化をし続けていかないといけないのは、人類の方だということです。リテラシーを上げていかないと、その恩恵を受けることはできません。インターネットを使うことができて初めて、そのリテラシーもインテリジェンスも得ることができます。人類自らが働きかけることで、進化の種が無限に提供されます。

■ 地域とインターネットの関わりが議論されました

Q2: インターネットは地域の自立をどう支援できるのか?

曽根 秀昭
東北大学/JPNIC分野担当理事(地域・非営利)

「インターネットの進化論」という夢の話をしていますが、そういう夢のような話をしているときに「インターネットが手元にない人は、その夢から取り残されるのか」「社会活動が地球規模に広がる期待がある一方で、コミュニケーションがデバイドされている地域では、そのメリットを享受できるのか」というそもそも論から疑問を持っていました。

「インターネットは地球規模のOSになるか?」という文脈では、日本の「地方」はそのOSからはみ出ているではないでしょうか。整備が整っておらず、仮に整備されたところで、それを使いこなすリテラシーも、使いたいという意識も期待もありません。

主な問題点としては、「高齢化問題」「人口密度が低くてコストが合わない」「山間地域には引けない」など、地域それぞれの状況があると思います。また別の問題として、仮に社会活動や人的交流ができるようになったとすると、今度は逆に地域性が失われていくのではないかという懸念もあります。交通網が発達して地域性が失われた例はいくらでもあります。情報ネットワークでも同じことで、地域社会を廃れさせる可能性もあるわけです。

さらには、インターネットの都会における作用は今まで数多く語られていますが、地域においても同じ作用をもたらすのかと言えば、そうも言い切れないのではないでしょうか。

と、数多くの問題を認識しつつも、本日の議論で気づいたことがあります。

現在、手元でネットワークにつながっていないからといって、決してOSからもれているわけではなく、銀行や宅配等のシステムは既にインターネットによって動かされているということを考えると、リソースの効率的な配分の過程では、地域もOSに組み込まれていると言えるのでしょう。

また、世の中の人が、皆が皆、例えばTwitterを使わない方が、多様性という観点ではむしろ健全な社会なのではないか、ということも考え合わせると、画一的ではなくとも良いのかもしれません。逃げる先があることも重要です。地方には「都市と同じになるか、別になるかのチョイスがある」とも考えられます。

Q4: インターネットは人間の住環境をどうプログラマブルにするのか? どうセキュアにできるのか?

力武 健次
独立行政法人 情報通信研究機構 情報通信セキュリティセンター インシデント対策グループ 専攻研究員

インターネットは、電子メール・Webなどを利用し、時間が違っても、共同して働くことができるという「緩い同期」の環境をもたらしました。"eventually consistent"、つまり最終的にツジツマが合えばいい、いずれどうにかなるだろうということでインターネットは続いてきました。

ところが特に日本では真面目な国民性のせいか、とにかく周囲を気にして同じように動こうとするあまり、同期を取ることに熱心になりすぎる傾向があります。これを続けていると、自分でものを考えなくなるし、社会からの強制同期を強いられることによって、精神も肉体も疲れてきます。これが社会的な問題です。例えば、ケータイの「即時返事ルール」などが良い例でしょう。

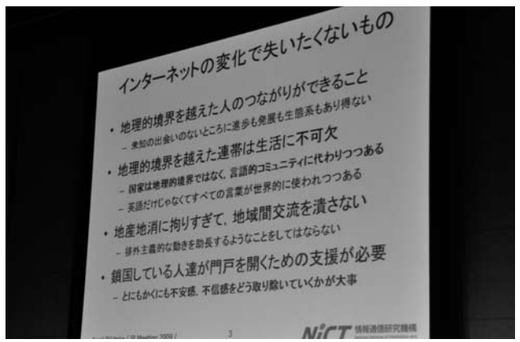
クラウドコンピューティングでデータが地球を1周するのに、約0.13秒かかります。この秒数は人間が意識できる時間であり、完全同期を取ることは難しいのではないか、というのが最近の問題意識です。つまり、地球規模で統一された社会をめざしたとしても、こういった遅延はどこにでもあるものだと、もっと人が認識していかなくてはいけない、ということです。

セキュリティについても同じことが言えます。セキュリティについては、昔は隠しておけばことが足りました。しかし、その後は「アクセス制御」というオープンでない世界に代わり、このコントロールのための集中同期にものすごいエネルギーが必要となりました。

将来、エネルギー消費を抑えることを考えると、このように強制同期を取ることはだんだん難しくなってくるのではないでしょうか。対策として、非同期で済むものは非同期にして無理にタイミングを合わせないようするなど、行動形態や社会形態を変えていかないとエネルギー消費も減りません。「コントロール」の反対の概念として「オープンネス（開放）が必要だ」と書きましたが、このオープンネスの下で本当に情報の安全性が保てるかどうかはわかりません。秘密が必要なところは通信できないかもしれないし、データはオープンでも、エンドツーエンドで暗号化をして安全性を保つなど、問題を組み替えていかないといけないかもしれません。しかし、要は、安全は守ることはできるが、安心感は心の問題であり、そういう心の醸成をどうしていくかだと思います。

インターネットがどう変わっても、個人的に失いたくないもの、それは地理的境界を超えた人のつながりです。インターネットは、良くも悪くも北から南まで情報を知らしめ、人との連携が可能になりました。これはとても重要なことで、意思交流によって、進化が生まれ、新しい生物が生まれます。未知のないところに進歩も発展もありません。

日本の社会基盤整備は、すべて官製主導でなされてきましたが、これがいつまで維持できるかは疑問です。ただ地域を突き放すのではなく、地産地消、それを前提とした関係、お金という観点にも向き合っていかないと、情報だけでやっていける時代は終わりました。すべてが分散化し、非同期という方向の中、新しい人も交え、そのときにどうセキュリティを守るか、どう動かし続けられるか、これがわかれば進化ができるのではないか、と考えています。



■ インターネットの進化で変わるべきでないものはなんでしょうか

Q6: インターネットは人類の活動の原資である発明・革新をどのように支援し続けられるのか?

江崎 浩
ISOC理事、東京大学、JPNIC副理事長

インターネットの進化や地球規模OSの話にあたり、インターネットは今後、何を経験しようとしているのでしょうか。

日本におけるGDPのうち、情報通信サービスの占める割合は13%です。これを大きいと思うか、それとも小さいと思うかは人それぞれですが、個人的には、他のパイの87%に、インターネットが影響を及ぼさなくてはいけなくなってきていると感じています。進化の上でいけば「繁栄できる種族になれるか」というところも大きなポイントであり、インターネットの進化にあたり、この分野にどう貢献できるかということが、どう進化するかということになるのではないでしょうか。

進化にあたり、いろいろと条件が変わってきています。(1)エンドユーザーの端末がパワフルになっている、(2)ずっと電源が入ってつながっている、(3)モバイルが入ってきている、(4)エンドユーザーがサービスを提供している、(5)転送、ストアとコピーのコストが小さくなった、等です。これは40年前のデザインからすると、かなり大きな進化を遂げていると言えますし、今後のアーキテクチャにとっても、大きな進化を要求されることを意味しています。また、進化の過程で「他のメディアとの戦い」や、インパクトをもたらした「ネット中立性」という問題への対峙もあります。

このような状況下、ISOCの中では、我々のゴールとして「エコシステム」という言葉を意図的に使っています。

「エコシステム」は、本来は生態学用語で「生態系」と訳され、「食物連鎖」のような垂直方向の物質やエネルギーの流れを意味します。しかしこれが、オープンソースの分野においては、「ハードウェア、ソフトウェア、開発、サービス、ユーザーの各場面にて、ソフトウェアをどのように開発、改良、利用すれば、オープンソースの世界の健全かつ安定的な発展を促進できるかという問題を解決しようとする理念」を意味し、異なるソフトウェアモデルとの共存、ユーザーの多様化への対応、商用利用への対応とコミュニティへのフィードバック、開発者の事情や動機など、水平方向のバランスをどのように調整するかに重点を置いた意味となります(※)。つまり、「エコシステム」とは「エコノミーなシステム」の意味などではなく、もっと広い観点から安定かつ健全な発展スパイラルを作るシステムの構造を指します。

エコシステムを提唱する背景としては、NGN、ビル、自動車、ファクトリーシステムなど、数多くのIPを使ったネットワークが構築される中、メモリの制約やビジネス上の理由で、IPを使っていてもネットワークをオープンにせず、敢えて閉じたネットワーク構築が増えていることが挙げられます。そういう中で、フラグメンテーションをいかに避けるか、こういうネットワークとコラボレーションできるかというのが、一番共有しているポイントであり、「エコシステム」という言葉を使う理由です。

よく「新世代のネットワークには頑丈で信頼できるものが必要だ、インターネットはぼろい」という話がされます。その意見にも一理あります。ただ、我々が心配しているのは、本当にそのネットワークにオープン性とグローバル性が担保できるのかということです。経済が悪くなると、システムやコネクティビティを囲い込むことが起こりがちです。これが「品質」そのものよりも心配するポイントになっています。一例ですが、今、国によっては、フィルターによってコンテンツが見えないということも起こっています。でも、これには「進化にとって必要なオープン性がどれだけ保たれているか」という疑問が湧き起こります。

ISOCで話している主要な戦略イニシアティブは、「トラストとアイデンティファイヤー」です。この中で唱えられるインターネットアーキテクチャとは、「マルチカルチャー」「自由と匿名性がある」「公平であり差別がない」「予測可能で、安全で、コモンズを提供して、機会を提供する」ものであるとされています。これが、次のネットワークにも求められるものであり、進化が続くためにも必要なことです。つまり、意図的にオルタナティブを提供しています。自然ではなく「意図的」が重要で、ギークな人も生かすシステムです。また、エンドツーエンドでは責任を持たないベストエフォートも、システムを安定的にする秘訣です。

僕はインターネットが良いと言っていますが、そうでない人もいます。これも健全なことです。だから、何が何でもコモンプールが良いとは言っていません。ただ、親方から弟子モデルでは、伝承はされても発展はしません。そういう意味で、自立性と自律性が必要です。また、個人の交流が減ると、健全なイノベーションが動きません。

後藤先生からも、進化には時間がかかる、進化のシナリオは、難しいという話がありました。どうなるかは僕らにもわからないところではあります。そんな中で、移行期をどうしていくのか、「どういう状況になったら、僕らはどう反応しようか」ということ、次の10年でどのように向かっていくかを、議論をし始めたところです。

（注:各講演者のコメントの内容は、当日の話をもとに編集を行ったものです。また、各講演者のタイトルは、開催当時のものです。）

（JPNIC インターネット推進部 根津智子）

■ 午後の部全体で3時間となるセッションになりました

※ http://ossipedia.ipa.go.jp/kb/%E3%82%A8%E3%82%B3%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0

IPv4枯渇 Watch

第3回

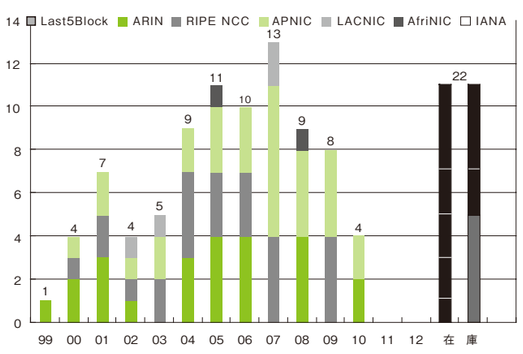
～IPv4アドレス在庫枯渇問題についてのおさらい、現状の把握と要検討項目の再整理～

JPNICとして、IPv4アドレス在庫枯渇への対応について本格的な取り組みを始めてからおおよそ3年が経ちます。この間、JPNIC会員、IPアドレス管理指定事業者の皆さんをはじめ、広くこの問題に関する認識は広まってきており、さまざまな対応策についての検討も進められている状況です。しかし、世間一般、特にIPアドレスを特に意識することなくインターネット接続サービスを利用しているユーザーレベルにまで、このIPv4アドレスの在庫枯渇が認識されている状態にはまだ至っておりません。

そこで今回の「IPv4枯渇 Watch」では、現時点で一体何が明確に分かっていて、何がまだ不明確で検討の必要性があるのか、これまでJPNICやIPv4アドレス枯渇対応タスクフォースにいただいたご意見などを踏まえ、[チェックポイント]として、一度おさらいをしていこうと思います。

■[チェックポイント1]
「IPv4アドレス在庫枯渇」の定義と、最新の分析による枯渇時期

IPv4アドレス在庫枯渇に関して、最も基本的で、最も重要なポイントは枯渇する時期が果たしていつなのか、ということです。IPv4アドレス在庫枯渇時期の予測として世界的に最も参照されている、APNICのチーフサイエンティストGeoff Huston氏の最新の予測では、IANAの在庫が枯渇する時期を2011年後半、RIRの在庫が枯渇する時期を2012年の後半としています。



上記グラフが示すように、ここ数年IANAからRIRへ、概収年間10個の/8ブロック（約1,678万個のアドレス）が分配されています。このペースは現在も衰えていない状況ですので、このまま年間10個ずつの/8ブロックが分配され続けていくとした場合、グラフの1番右側に示す在庫数22は、3年を待たずに消費されてしまう可能性が高いことが分かると思います。なお、在庫数が最後の五つの/8ブロックになった時点で、全てのRIRに一つずつ均等に分配し、IANAの在庫を払底するグローバルポリシーが既に決定していますので、実際にこれまで通り分配できる/8ブロックの数は残り19個となり、前述の通りにこれまでと消費ペースが変わらなければ、今から2年くらいでIANAの在庫が無くなり、Geoff Huston氏の予測時期とも大きくずれることはないと思われます。

一方、RIRの在庫枯渇時期はどうなるのでしょうか?Geoff Huston氏のRIR在庫枯渇予測時期は、最も早いRIRの在庫枯渇時期として2012年後半を予測しています。各RIRのアドレス分配ペースはまちまちで、それぞれの在庫が無くなる時期も異なります。JPNICとしては、当然上位組織であるAPNICの在庫がいつ底を突くのかに最も関心がありますが、Geoff Huston氏の分析では、各RIRの中でAPNICの在庫枯渇が最も早いとされており、氏の予測におけるRIR在庫枯渇時期予測は、イコールAPNICの在庫枯渇時期となっています。

ちなみに、JPNICは現在、独自の在庫は持たず、APNICと在庫を共有しているため、APNICの在庫が枯渇した時点で、JPNICも新たなアドレスの分配ができなくなることになります。

■[チェックポイント2]
近づくIPv6接続サービス提供開始時期と普及にともなうIPv6ユーザーの出現

去る2009年12月4日に、NTT東西地域会社から、次世代ネットワーク（NGN）とIPv6インターネットとの接続方式の一つである、「ネイティブ方式」で接続するための事業者選定の結果が発表されました。これにより、現時点で2011年4月と予定されている、NTT NGNを利用したIPv6インターネット接続サービス開始に向けた準備は本格化します。また、総務省の「IPv6によるインターネット利用高度化に関する研究会」における「IPv4アドレス在庫枯渇対応に関する広報戦略ワーキンググループ」に参加しているISP事業者の多くが、2011年4月のサービス開始を目標にして各種の対応を進めているということが報告されています。このような動きから、少なくとも2011年4月以降、IPv6でインターネットに接続するユーザーが、これまでより早いペースで増えていくことは確実です。

それでは、2011年4月以降、どのくらいのペースでIPv6でインターネットに接続するユーザーが増えてくるのでしょうか? 基本的に、新規にISPサービスを契約するユーザーの方には、この頃から徐々にIPv6でインターネットに接続するサービスが提供されていくことになると思いますが、既存のIPv4でインターネットに接続しているユーザーは、しばらくはそのままの状態で利用し続けることになりますので、IPv6ユーザーが急速に増加することはないでしょう。しかし、IPv6ユーザーがどの程度のペースと規模でその後増加していくか、現時点ではっきりと見極めることはできません。ただし、少数だとしても、2011年4月以降はIPv6でインターネットを利用するユーザーは確実に増加しますので、そのようなユーザーに対してどのような対応をすべきかについては、今から検討していく必要があります。

■[チェックポイント3]
分配済みIPv4アドレスの再分配の可能性と、それらの使い回しが在庫枯渇時期に与える影響

2009年11月26日に開催されたJPNICオープンポリシーミーティングにおいて、JPNIC管理下のIPv4アドレスも移転可能にする提案が行われました。ミーティングの場でもコンセンサスとなり、その後のコメント期間でも特段の意見が出されず、最終的にコンセンサスに至りました。今後JPNICでの実装に向けた慎重な検討を経て、大きな問題がなければ、ドキュメントへの反映など実装準備が進んでいきます。

それでは、このIPv4アドレスの移転が可能になると、どのようなことが起こるのでしょうか? 2009年12月に実施した第2回IPv4アドレス在庫枯渇に関するアンケートにて、このIPv4アドレス移転に関する質問を設けたところ、右記の表のような結果となりました。回答者がJPNIC会員およびIPアドレス管理指定事業者であるため、分配を受けているアドレスのほとんどが利用計画を提出して取得しているものであり、需要はあるものの、逆に余剰を提供するという事業者はほとんどないようです。

◆IPv4アドレス在庫枯渇への対応の一環として、現在禁止されている分配済みのIPv4アドレスの譲渡を認めるルールが議論されています。このIPv4アドレスの譲渡が可能となった場合、手元にあるIPv4アドレスを譲渡する、または、誰かから譲り受けますか?

N=82	回答数	%
1）現在利用していないアドレスを譲る（売る）つもりである	1	1.2%
2）譲ってくれる（売ってくれる）ところがあれば買うつもりである	26	31.7%
3）譲渡あるいは譲り受ける（売買）ことはしない	27	32.9%
4）その他	28	34.1%

このため、IPv4アドレス在庫枯渇後に余剰空間として提供されるアドレスの大半は、歴史的PIアドレスの空間からだろうと言われています。しかし、JPNICでは既に一度、全ての歴史的PIアドレス割り当て先に利用確認を行い、不要なものを返却してもらっているため、ここから出てくる量も限定的だと考えられます。

もちろん、どの程度のアドレスが譲渡の対象になるかは、実際のところ蓋を開けてみないと何とも言えないところではありますが、他者からの譲渡によってIPv4アドレスを手当てすることは、一時的には可能だとしても、継続的に安定的な量を確保することは困難だと思われます。

■[チェックポイント4]
エンドユーザーへの周知の必要性

IPv4アドレス在庫枯渇に関する周知、広報が話題になるたびに、「エンドユーザーへの周知をどうするか?」という事項も、課題となっていました。「在庫枯渇への対応にあたり、エンドユーザーへも正しい情報を伝えておくべきである」という意見がある一方で、「無闇に情報を提供することで不要な混乱を招く可能性もある」という意見もありました。これに関して「IPv6によるインターネット利用高度化に関する研究会」でも検討が行われ、やはりエンドユーザーが全く何も知らされないまま、IPv4アドレス在庫枯渇への対応策を取ることは難しく、適切な情報を適切な窓口から伝える必要があるとされています。そこで、ユーザー向けの広報は、ユーザーの「インターネットの窓口」を担うISPを通じて行うのが適切であり、これを各ISPがある程度統一的に実施するための、情報開示ガイドラインを策定することも検討されています。今後このガイドラインに沿う形で、エンドユーザーへの周知や問い合わせへの対応などがISPに求められていくと思われます。

■[チェックポイント5]
日本以外でも進むIPv4在庫枯渇への対応とIPv6導入の推進

今年、2010年の初めに、各RIRおよびその連合体であるNRO（Number Resource Organization）が、メディア向けの発表を行いました。内容としては、2010年1月にIANAからAPNICへ追加割り振りが行われたことにより、IPv4アドレスの在庫が、全IPv4アドレス空間の10%を切ったことを全世界的に周知し、IPv4アドレス在庫枯渇への対応を促進することを目的としたものです。

これまで、IPv4アドレス在庫枯渇とその対応のためのIPv6導入などを話題とするたびに、日本だけが先行し過ぎて、いわゆる「ガラパゴス化」を心配する声も聞かれました。しかし、米国や欧州連合、また中国や韓国などでもIPv4アドレス在庫枯渇への対応として、政府主導にてIPv6導入が推進されてきています。年初のRIRとNROによる広報活動は、さらにこれらの動きを促進するものだと言えます。日本国内でも、世界でのIPv6導入・推進の動きと足並みを揃えて、対応を進めていく必要があります。

第9回

江崎 浩のISOC便り

JPNIC副理事長/ISOC理事
江崎 浩

今回の会合は、理事のスケジュールを調整した結果、IETFおよびICANNとは独立して開催することになりました。開催場所は、オランダのアムステルダムで、2009年12月4日（金）～5日（土）の日程で行われました。アムステルダムでの会合場所の近くには、前ISOC議長（Daniel Karrenberg氏）が所属する、RIPE NCC（Reseaux IP Europeans Network Coordination Centre）のオフィスもあります。ちなみに、PTT（Staatsbedrijf der Posterijen, Telegrafie en Telefonie: オランダ電信電話局、現KPN社）のメインオフィスだったビルの隣にあり、夕食のレストランに向かう途中に通りがかることから、いろいろな説明をしてもらいました。

今回の会合の重要な議題は、以下の二つでした。

（1）W3Cへの財政的支援に関して

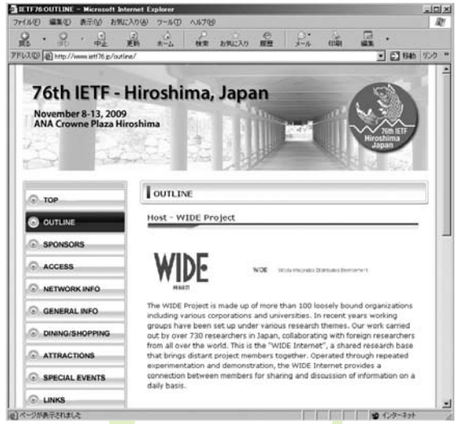
既にプレス報道が行われていますが、ISOCは、W3C[※1]と標準化活動などに関して戦略的な協調関係を構築することとし、そのために、ISOCからW3Cに対して、財政的な支援を行うことになりました。会合にはWWWの産みの親でもある、W3Cの代表であるTim Berners-Lee氏（米国MIT教授）が出席しました。氏から理事会に対して今回の提案に関する説明と、それに続いて質疑応答が行われました。W3CがIETFのように、オープンな標準化活動を推進することが可能な組織なのか、どのような協調が可能なのか、さらに、財政を健全化するためにどのような組織改革が計画されているかなどが、議論されました。議論の結果として、3年間をめどに財政的な支援をISOCがW3Cに対して行うことになったわけですが、その内容に関してはきちんと監査・評価を行い、W3Cが機敏で包括的かつ柔軟性に富んだ組織機構を展開しない場合には、3年間の確約は行わないことがコンセンサスとなりました。

（2）ISOCの財政の強化に関して

ISOCの収入の大部分がPIR[※2]からの寄与に依存していることは、常に、改善すべき課題であるとの認識があります。今回の会合では、2010年度の予算計画だけではなく、今後3年間の予算計画も議論されました。戦略的にPIR以外からの収入の増加が提案されていましたが、理事会としては、『根本的な改善案になっていない』との結論に至り、急遽、2010年1月中に電話会議を開催し、運営スタッフ側からの再提案を審議することとなりました。

本会合では、IETFの開催状況に関する報告もIAOCから行われます。2009年11月に広島で開催された、第76回IETF会合に関しての報告も行われ、ほとんどすべての会合参加者から、広島会合の成功とその努力に対する感謝と敬意が表されました。あらためまして、関係各位のご尽力とご努力に深く感謝申し上げます。2010年秋の開催が、中国（北京、ホストは清華大学）に決定したとの報告も行われ、当然のことながら、コンテンツフィルタリング（Great Firewall）への懸念などの議論が行われました。

次回の会合は、IETFが開催される米国カリフォルニア州アナハイムで、2010年3月27日から28日の開催となります。



IETF76のWebサイト

※1 W3C（World Wide Web Consortium）
WWWで用いられる技術の標準化、相互運用性の確保を目的とする団体です。HTML、URI、XML等の技術もW3Cで標準化されました。

※2 PIR（Public Interest Registry）
PIRは、ISOCによって2002年に設立された非営利企業です。PIRは.ORGトップレベルドメイン（TLD:Top Level Domain）を管理する役割を担っており、我が国における「.JP」を管理している株式会社日本レジストリサービス（JPRS）に似た組織です。

インターネット歴史の一幕

Internet History

国際化ドメイン名の標準化

株式会社日本レジストリサービス 米谷 嘉朗

国際化ドメイン名（Internationalized Domain Name、以降IDNと略記します）のRFCが発行されたのは2003年3月ですから、IDNが標準化されてもう7年近く経過したことになります。この7年間で、IDNを取り巻く状況は随分と変化しました。例えば、PC用の主要なブラウザは、全てIDNに対応したので、IDNのWebサイトへのアクセスは自然と行えるようになりましたし、さまざまなメディア上でIDNを見かけることも増えてきました。2010年中には、IDNのTLDまで登場します。

IDNの標準化に関わった一人として、この広がりを大変に嬉しく思っています。

IDNの標準化を通じて学んだことは、以下の5点です。

（1）国外に仲間を作る

国際標準を作るということは、相当の力が必要であり、独力で成し得るのは困難です。また、世界中の人が利用するものですから、特定の地域や国の都合が感じられる提案は、受け入れられるのも困難です。そのため、国内はもとより国外にも一緒に提案をしていく仲間を作ることが、標準化組織の場で合意を得るためには重要です。

具体的にIDNの標準化においてやったことですが、中国・日本・韓国・台湾のccTLDで共同技術チーム（Joint Engineering Team、以降JETと略記します）を編成して技術的な検証や提案を共同で行ったり、IETFでの経験が豊富で影響力がある人にドキュメントの共著者となってもらったりしました。個別にJETの会合を開き、時には12時間以上にも及ぶ激しい議論を繰り返しながら4者の意見を集約し、それをIETFで提案することで説得力を持たせ、標準化を進めることができました。

（2）実装を作る

IDNの標準化過程では、文字列正規化の方式やASCII互換表現（ASCII Compatible Encoding、以降ACEと略記します）への変換アルゴリズムに複数の提案が行われました。それら提案が、想定したシナリオ通りに動作するか、相互接続性を持つか、そもそも実装可能かということを検証するために、JPNICでmDNkitおよびidnkitという参照実装を開発し（私もこの開発には深く関わりました）、オープンソースのツールキットとして公開しました。提案が実際に動くことを示すことは、標準化の方式を決定していく上で非常に大きな説得力を持ちました。

また、idnkitは緩やかなライセンスのツールキットとして開発したため、ブラウザベンダーやDNSソフトウェアベンダーなどに採用を働きかけ、早期のIDN環境整備に役立てることができました。

（3）対立提案を評価する

前述の通り、IDNの標準化過程では多くのACE変換アルゴリズムが提案されました。そのため、どのアルゴリズムを採用するのが適切なのかを判断しなければならず、具体的な評価に基づく比較が必要でした。そこで、JETで既に登録された多数のIDN（試験登録を含む）をサンプルに、各ACEアルゴリズムを評価し、それぞれのccTLDの観点（韓国ではハングル、中国・台湾では漢字、日本では漢字と仮名の混合など）から優れたACEを導き出しました。その結果を合同で「適切と思われるACE」としてIETFで提案し、結論として合意されました。

（4）プロトコルと運用を分ける

中国語文化圏では、台湾などで使われている繁体字と中国などで使われている簡体字は、例えば「國」と「国」など由来が同じであれば同じ文字とみなしたいという要求が強くあります。そのため、IDNの標準化過程において、アルファベットの大文字と小文字を区別しないのと同様に、それをプロトコルレベルで取り入れるべきという主張が続いていました。しかし、それは前述のように特定の地域や国の都合であるため受け入れられず、一時期平行線をたどっていました。

IDNの標準化が達成されないことは誰にとっても望まれないことであったため、長い議論の末、JETの中でプロトコルでは別の文字として扱うが、運用では同じ文字として扱うという方針が合意され、そのための運用ガイドライン作成を行いました。

この運用ガイドラインはRFC3743として発行され、IDN登録と運用に関する重要なモデルとなっています。

（5）標準化はゴールではなく、スタートである

標準化は、グローバルなサービスを提供するために必要なツールの一つです。標準化しその標準に準拠することよって、同じ機能を持つサービスや製品を異なる人が実装しても相互接続性が保証されるのです。

ところで、それらサービスや製品の実装者は、標準と需要があって初めて実装を開始します。一方、利用者はアプリケーションなどの実装があって初めてサービスを利用するため、往々にして鶏と卵問題を引き起こします。

IDNの場合は、ブラウザのIDN対応がブレイクスルーでしたが、それも、IDNの標準化が行われたからこそです。

◇　◇　◇

IDNが標準化され、IDN登録サービスが始まり、IDN対応アプリケーションが普及したことにより、IDNの利用が増加しました。それに伴って新たな課題が見つかっています。例えば、見かけが文字に良く似た記号を使って、著名ドメイン名との誤解を招くようなドメイン名を登録できてしまう問題の解決などです。運用対処だけでは困難なこともあるため、現在、IDNの標準そのものの改訂作業が行われています。改訂作業も最終段階にあり、今年中には新しいRFCが発行される見込みです。

プロトコルが見直され、改訂されていくということは、それがグローバルに使われていることの証左であると言えるでしょう。IDNがホットトピックとなりそうな今年、IDNの歴史を振り返って見るということは、なかなか興味深いのではないかと思います。

JPNIC 会員企業紹介

「会員企業紹介」は、JPNIC会員の、興味深い事業内容・サービス・人物などを紹介するコーナーです。

さくらインターネット株式会社を訪問しました。同社はホスティングサービスの分野で月額125円のレンタルサーバを提供し、またラックへのサーバ収容効率の高さなどで注目されていますが、それに託した社長の想いを存分に伺いました。

さくらインターネット株式会社

住　　所：大阪府大阪市中央区南本町1丁目8番14号（本社）
東京都新宿区西新宿7-20-1
住友不動産西新宿ビル33F（東京支社）
設　　立：1999年8月17日（サービス開始:1996年12月23日）
資 本 金：8億9,530万円（2008年9月末時点）
代表取締役社長：田中邦裕
U　R　L：http://www.sakura.ad.jp/
従業員数：168名（2009年9月末時点）
事業内容：1.インターネットでのサーバの設置およびその管理業務
2.電気通信事業法に基づく電気通信事業
3.インターネットに関するコンサルティング
4.コンピュータおよびその周辺機器の製作および販売・保守

インターネットで実現したい“夢”とは

お話しいただいた方:
さくらインターネット株式会社
代表取締役社長　田中 邦裕氏

1996年に国立舞鶴工業高等専門学校在学中にさくらインターネットを創業し、当時国内ではまだ珍しかった共有ホスティングサービス（さくらウェブ）を開始。高専卒業後に有限会社インフォレストを設立し事業を継承、代表取締役へ就任。1999年にはさくらインターネット株式会社を設立し、月額125円から始められる低価格レンタルサーバ「さくらのレンタルサーバ」の開発に自ら携わる。インターネット業界発展のため、各種団体に理事や委員として多数参画。

コストパフォーマンスの高いサービスを提供できる理由 ～全体を見渡した最適化～

■まずは、現在の事業内容についてお聞かせください。

提供しているのは、データセンター分野のサービスです。細かく言うと、コロケーションとホスティングの二つで、ホスティングは、サーバをまるごとお貸しする専用サーバと、複数のお客様でリソースを共有するレンタルサーバに分かれます。

金額で言うと、月何百円のサービスから何千万円というかなり大きな範囲で表すことができます。下から上までレンジが広いのが強みです。今の大口顧客でも、最初は月500円から始めた人もいるんですよ。幅広く柔軟性が高いサービスを提供しています。

特筆すべきは、自社でインターネットバックボーンを持ち、データセンターを構築し、サーバの設計までやるという、自社で全体を最適化しながら、比較的コストパフォーマンスの高いサービスを提供しているという点でしょうか。

■ユーザーのレンジが広いということですが、割合はどうなっているのでしょうか？　また、どういうスキルレベルのユーザーが多いのですか？

ユーザーに占める法人と個人の割合は、3：2で法人が高いです。

年齢層としては20歳代以降ですね。以前はプロシューマー（生産消費者）が多かったのですが、現況は、ブログの開設などにとどまらず、もう少し深くチャレンジをしたいという初心者も多いように見受けられます。

■どのサービスの売れ行きが良く、業績はどのようになっていますか?

件数だけで言えば、20万以上のユーザーを抱える共有レンタルサーバです。ただ、売り上げで言うと、それは十数%程度に過ぎません。専用サーバやハウジングなどのサービスが売り上げの多数を占めていますね。

2008年度が71億円の売上高で経常利益3億5千万円弱。今期は、売上高77億円、経常利益4億円弱の予定です。

不景気の影響で、サーバを社外に出す人が多くなっており、専用サーバは好調です。逆にサーバ持ち込みのハウジングの場合は、お客さんの事業縮小や撤退もあるので、トントンというところでしょうか。

ただ、コロケーション・ハウジングよりも専用サーバ、専用サーバよりレンタルサーバの方が利益率が高いので、売り上げ自体は厳しくても、利益は確保できています。ここにきて、利益の質の変容が起こっていると感じています。

■貴社の業績好調の要因をどう分析しますか?

創業以来の、運用とサービスに根付いた組織、人員体制ですね。奇しくも世の中では「クラウド」というサービスが流行っていますが、SIerのように設計やコンサルティングで稼ぐよりも、運用で稼ぐモデルにシフトしています。もともと弊社はそういう体制、つまりは、ITが「所有」じゃなくて「利用」となった、今の時代にマッチした陣容であると思います。

また、世の中的に中間業者を通さずにダイレクトに商売することが多くなってきましたが、もともと弊社はそういう商売です。例えば大多数の申し込みもオンラインサインアップ経由です。払うべきコストが少なく、他者と比べて低価格化を実現しやすいですね。

月額125円は市場を広げこそするが、破壊するものではない

■低価格と言えば、月額125円のレンタルサーバサービスは、業界的にも衝撃的でした。125円は何がセットになって125円なのでしょうか。

「さくらのレンタルサーバ」のライトプランですね。POP、IMAPでメールが使えて、HTTP経由でアクセスできる領域があります。ディスク容量は500MB、CGIを動かせますし、RubyやPerl、Pythonも使えます。FTPもできるし、コントロールパネルで設定も可能で、ブログも付いています。

ただ、一番多いのはこのプランのユーザーではなく、500円のスタンダードプランのユーザーです。125円ですとシェルログインができず、PHPも使えませんので、500円ぐらいなら最初からこちらでというお客さんが多いですね。

■ものすごくリーズナブルですね。「この値段で行ける!」という直感があったのでしょうか。

そうですね。普通はデータを分析すると思いますが、びっくりするほど成長し、かつ非常にニッチな市場なので、データ分析はできませんでした。

当時の客単価は1,000円超程度でしたが、ユーザーは9,000ぐらいいました。これなら、単価を下げても、10倍の8～9万ユーザーぐらいいればいけるんじゃないかと考えたのです。

この10倍の顧客獲得は、びっくりするぐらいすんなり行きましたね。初日で2,000～3,000件の申し込みがあって、オンラインサインアップ用のサーバが落ちました。その後、初年度で2万5,000件の申し込みがあり、2～3年で当初の目標値を超えました。昨年には

20万ユーザーを抱え、損益分岐点をかなり超えている状況です。また、付帯するドメイン名ビジネスでも登録してくれるユーザーが多く、この手数料収入も大きいです。とても成功したサービスだと感じていますね。

■そんなに値段を下げて、その後の価格競争について、先を見越した懸念はなかったのでしょうか?

ホスティングは、以前は価格的にハードルが高いものでした。しかし、値段を下げたことで、ユーザーの層自体が、かなり分厚くなったと感じています。

つまり、ホスティングは家庭用の日用品を売っているのとは違います。業界の市場や、売り上げは拡大している状況にあり、業界にとってそれほど悪影響ではないですね。

この価格については、追随する他社の方が大変なのではないかと考えています。今でも125円と騒がれていますが、実は、125円で始めたのは、5年以上前なんです。そこから定価を下げておらず、キャンペーンもほとんどしていません。「定価」をモットーに「市場の値段は我々が最初に決める」というスタンスです。「こういうユーザーが必ずいるはずだ」という確信のもと、値付けを行っています。

弊社単独で見れば、その価格を印象付けられます。印象が付かない値段競争は、どんどんと値段を下げるものになります。幸いなことにそういった競争にはなっていませんね。

■ オフィス玄関先にて

サーバ集積の工夫に見る、誰にも真似のできない全体最適化と汎用化のバランス

■また、御社はラックへのサーバ集積率が高いということで有名ですが、サーバやラックの自社での開発について、教えてください。

二つの利点があります。コストが下げられるという点と、他の会社よりもアグレッシブなサービスを作ることができるという点です。サービスの幅が非常に広がりますね。

ITは「モジュラー化した産業」と言われますが、しかし、それがかなりのオーバーヘッドを生んでいることも事実です。例えば、通常のサーバをラックに詰め込むと廃熱で設置に制限がかかりますし、メモリなんてスロットが8本もあったりします。

一方、弊社のサーバはラックと一体であり、まずサービスありきで作っています。ラック、空調、サーバ、ネットワークをトータルで設計した上で、サービスを提供しています。他のデータセンターに持っていくと熱暴走するかもしれないくらい余剰がほとんどありません。これで、全体最適化が図れています。前後にマウント、1ラックに最大で160台収容できます。

ちなみにデータセンターは、通信キャリアさんと全く同じスペックであり、サービスを比べても劣りません。かつ、メモリも1本当たり4〜5時間かけて全数検査しています。つまり、他社より質も悪くない。質が高くて、かつ他者より安い。これが強みです。

■モジュール化はモジュール以外のことを知らなくても生きていけるのが強みですが、全部を知って、無駄を詰めることも重要なんですよね。その結果、今があるということでしょうか。

そうですね。ただ、摺り合わせ型、全体最適型の一番ダメなところは、コストがかかり過ぎることです。汎用化もコストを下げるために重要なのです。全体最適化をしつつ、汎用化するというバランスが一番必要ですね。

例えば、ケース、マザーボード、ハードディスクもパーツは全て市販品を使っています。Googleだって、かつて自社でマザーボードの設計をして失敗しました。汎用品をいかに組み合わせて全体最適化を図るかがノウハウです。結果的には、それが一番安いのです。

■御社の注文品が、市場で汎用品となることもあると聞きましたが。

はい。例えば、ラックもメッシュの開口率も弊社が指定していて、これが、河村電器産業の標準品になっています。つまりは、弊社のノウハウが他社に取り入れられた結果です。

結果的にはそれが一番安いし、他社が何をしても、その時は弊社はもう次のステップに行っています。だから、ある意味オープンソース的な考え方でノウハウを公開しています。弊社として占有はできませんが、それでサービスの質も高まりますし、自分でやっているからこそわかる運用の能力やノウハウが貯まっていきます。真似をして他社が弊社より安くできるんだったら、弊社はそれを買いますし(笑)。

サーバ技術やOS、コントロールパネル、スケールメリット、ブランディングなどなどどれも、単独では切り出せません。全てが一体となって弊社ができています。その代わり、ルータもスイッチも既製品ですし、ISPと違い、細かいネットワークを組んでいません。帯域はたくさん取れても、細かいシェーピングはできない仕様になっています。ただ、こうしてQoSを切り捨てることで、コストがすごく下げられる。広い帯域を確保してトラフィックを流し放題でも別にいいんじゃないかという独自のやり方です。

■しかし、それでは法人向けには、通用しないのではないですか? また、ネットワークはどのようになっているのでしょうか。

そうですね。法人向けには実は、この集積度の高いラックとは別の、もっとレガシーなラックを使っています。

ネットワークは、今は対外接続で200Gbpsを超えています。フリーピアをしておらず、1ホップで到達できないところはトランジットを買っており、それ以外はほとんど10Gbpsプライベートピアリングです。スループットが非常に良いです。東京-大阪で10Gbpsを2本引いているところはそうそうないでしょう。ネットワーク的にも強いと思います。

世界につながる感動を得た運命の日 〜創業のきっかけ〜

■創業時のいきさつを教えてください。

始めたのは13年前の12月。舞鶴高専の学生の時でした。現時点でも若いですねとよく言われますが、もう創業13年で、実は結構長くやっています。

当時、自分でサーバを運用し、Apacheに関する情報発信をしていたのですが、学校の設備を利用して自由に情報発信するには、学校側の対応がかなり厳しいことがあり、また、外でサーバを借りようにもディスク容量が少なく、CGIはダメなどいろいろと制約がありました。

当時、「世界中につながる」と、知識としてわかっても、体感はできていませんでした。しかし、ある日、秋葉原のお店のパソコンから自分のWebページを見て、とても感動しました。そこからもう離れられなくなりましたね。

そこで、地元舞鶴のISPに持ち込んで、儲けの一部を渡す代わりに、サーバを置かせてもらったのがそもそもの始まりです。その時に社長であった梅木氏が協力してくれたおかげで、ホスティングサービスが実現できました。梅木社長には、今も弊社の監査役をしてもらっていますが、当時「よくわからないけど、面白そうだ」と理解を示してくれたのです。

■社名の由来は?

「わかりやすいドメイン名じゃないとダメだ」と思っていました。ちょうど1996年12月、JPNICのルールが変わり、第2レベルが違えば、第3レベルが一緒の文字列でも登録がOKとなり、また「NE.JPドメイン名」ができました。これがいいきっかけになりました。

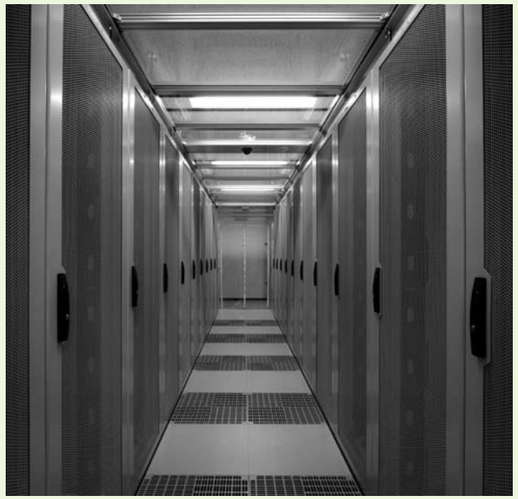
つまり、それまでは、「sakura.co.jp」を当時さくら銀行が登録していて、他の属性でも「sakura」の文字が登録できませんでしたが、ここで開放されたため、「sakura.ne.jp」が取れることになったのです。

当時は「さくらWeb」というサービスをしており、創業時はさくらインターネットとは呼んでいなかったのですが、年が明けて1月か2月に、さくらウェブの名前とドメイン名から「さくらインターネットサービス」と社名を付けました。

■そこから全てが始まっていったのですね。

はい。PC-9801にFreeBSDを入れたことから始まります。サーバが足りなくなったので、大阪の日本橋でフルタワーのPentium Pro 150MHzのサーバを2台買って始めました。かなり大きなサーバでしたね。

ホスティングを個人向けにサービスしはじめると、トラフィックが増え、業界では1・2番目になりますが、12年前にはデータセンターにサーバを入れました。



■ さくらインターネットのデータセンター

そうなると、今度はラックに何台入るかがポイントになってきます。最初は6台とか8台を入れていたのですが、ラック代がもったいないということになり、1997年に、書類ケースみたいなものに電源をぶら下げたものでしたけれども、初めて自社でサーバを作り、それを25台ぐらい入れていました。その後もNLXのケースを台湾から輸入したりして、ついには2000年頃からケースから板金して作るようになりました。

また1999年、ラック自体も、データセンターが郊外にあって不便なので、自分達でデータセンターも作ろうと、最初は大阪と東京の事務所に15ラック程度を置きました。オーソドックスなサーバでしたが、積み上げると6台目ぐらいからズレてましたね（笑）。それが初めてデータセンターを作った10年前です。当時はIXにつなぐのはハードルが高く、また1次プロバイダも2次プロバイダも値段の高い時代でした。

同じく1999年には、バックボーンをBGPでやりはじめました。当時は求められる品質が今ほど高くなかったため、UPSさえあれば、事務所の端のデータセンターでも許された時代だったんですね。その後、ネットバブルがやってきて出資したいという人も多くいて、そういう幸運も重なって、2001年頃、次の新しいデータセンターを構築できました。

他のデータセンターと弊社が明らかに違うのは、あくまでも弊社のサービスを入れるために、自社のデータセンターとして始めた経緯があるという点です。あくまでもホスティングが主目的であって、コロケーションは、スケールを出すための手段でした。そこが他社と違うところです。

顧客の夢を実現する手段を提供するために常に行動を忘れない ～経営者として～

■話は変わりますが、ご自身のことを経営者としてはどう思いますか?

正直、自分はでき上がった会社の社長には不向きだと思います。今まで3社ぐらい起業し、経営者の中でも起業家タイプなんでしょうね。事業を興すのが好きで、アーリーステージが得意です。従って、今のようなステージになると、今までとは違うスキルも要求されており、他の役員を頼りながらチームとして経営しているイメージですね。

■経営者として心がけていらっしゃる信条はありますか?

「行動は早く」です。私は、さくらインターネットを3日で始めました。まあ、3日はちょっとやり過ぎだとは思いますが（笑）。

Googleがすごいところは、アイデア自体ではなく、そのアイデアを即座に実行するところです。アイデアだけでは意味がありません。常に行動することが重要ですね。

また、最近は自らのミッションを強く意識しないといけないと考えています。

どういうことかと言うと、よくISPだと接続する権利を売っている、ホスティングだとサーバを貸している感覚になってしまいます。でもこれは間違いで、ユーザーはその中で、動画配信をしたりしているわけで、「自分らはその手段を提供している」と考えなくてはなりません。

ユーザーの立場で考えると、サーバが故障したら必死になります。しかし、サーバを貸している感覚のままだと、「サーバは壊れるものでしょ」となってしまいます。

「顧客が夢を実現する、その手段を提供している」と言っている割には、今までは、しっかりできていなかった部分もあるのではないかと思っています。ユーザーが増え、またTwitterやブログ等でレスポンスが早くなったこともあり、ユーザー視点で考えることの重要性を痛感しています。

■今後の目標というのはありますか?

一つは、「組織変革」です。今を第二創業期と考えて、社内を変えていきたいですね。今までは、ホスティングは成長する市場でしたので、流れに沿えば勝手に成長しました。これからは社員が成長させようと思わないと成長しない時代です。だから、組織力を上げ、イノベーティブな組織を作らないといけません。イノベーティブな人だけがいてもダメですけれどね。

また、顧客の視点を持つ社風も必要です。安いだけじゃダメです。昔のイメージを引きずらないことも必要です。

もう一つは、日本のITは他国に比べて遅れているように言われますが、その意識を改めたいですね。

例えば、データセンターも日本は高いと言われていますが、東京や大阪に置いていれば当たり前です。お客さんにコンピューティングリソースを提供するのが目的なら、別に田舎でも良い訳ですし、アメリカと同じようなデータセンターを作れなくもありません。エクセレントなファシリティを作りたいという夢があります。先週も地方3ヶ所に見学に行きました。サーバの集積度ももっと上げたいですね。今は1ラックに400台入るサーバを考えていますよ。まだ、笑い話レベルなんですけれども。

「AmazonやGoogleには勝てない」と思い込んでいませんか ～日本の誇りを取り戻したい～

■将来の夢について、伺わせてください。

端的に言うと、先の話の通り、世界で日本のITが認められるようにしたいですね。本当はもっと輸出できるはずなのに、日本はITは輸入過多です。日本はすごいんだと、これからそういう風に発信したいですね。

回線も、日本のキャリアは海外の線を「コスト」と考えているようです。これ以上、海外投資をしたくない、それどころかGoogleやYouTubeが日本まで送ってくれるんならそれでいいじゃないかと、そんな考えになっています。そのため、最近は回線、特にインターネットトラフィックという意味では増設されていません。

この意味では、IPv6に変わる時はターニングポイントだと思っています。弊社がヨーロッパに進出できるかはわかりませんが、米国には拠点を持ちたいですね。グローバルTear1の末席には行きたいなと。ネットワークについての夢もあります。

バックボーンネットワーク、サーバ、データセンター、サービスを、一から全体最適を取り全部自社設計にすれば、AmazonやGoogleに勝つとは言わなくとも、負けないサービスはできると思っています。多くの日本企業は、AmazonやGoogleには勝てないと思っています。でも、最初から負けるつもりはよくありません。

日本にあれば10msecとか20msecとか、いったん海を渡ってから戻ってこない分、速いわけです。勝っていなくても負けていなければ、非関税障壁でも日本が勝つことができるわけです。アメリカにも勝てると思いますよ。

弊社としては、何かを実現する人の手助けになるような、手軽にインターネットサービスを出せるような環境を作っていきたいです。具体的には、もっと海外に通用するようなサービスを作っていきたいですね。サーバをもっと使いやすい値段で提供するとか、いろいろ組み合わせて、気軽に高級なネットワークを利用できるように柔軟性を高くすることなどを始めていきたいですね。

また、今年は、ちゃんとしたパブリッククラウドを提供したいと考えています。

■その「正統派クラウド」については、構想はどのようなものなのでしょうか?

容量を気軽に追加できるように、まずはストレージです。また、ネットワークももっとフレキシブルにします。例えば社内のサーバと専用のプラットフォームを連携できるなど、その辺りを手がけはじめています。その次にくるのはプロセッサの仮想化。EC2の領域ですね。この辺りを研究所と開発で取り組んでいます。

■研究所を作っていらっしゃるんですね。

サービスだけで言うなら3年後は考えません。3ヶ月、もしくはせいぜい半年です。しかし、「事業」という視点なら3年後も考えます。研究所は、このように中長期的な視点で考えるところとして設けています。

仮想化の話で言えば、XenやVMwareじゃなくて最近はKVMも試しています。また、データの効率的な分散を支えるKVS（キー・バリュー・ストア）が流行り始めていますので、国内での関連プロジェクトと連携も進めています。

過去、さくらのレンタルサーバを僕自身がコーディングまでしている時代がありましたが、それだと「次のサービスができるのか?」という話になってきます。やれないことはないのでしょうが、新たな広がりはありません。1人ではなくて、こういうことをできる人が、増えていかないと進歩がありません。サービスを買ってきてレバレッジを利かすという方法もありますが、組織として、自然に拡大できなくては、本質ではありません。

我々のビジネスは地味なビジネスですが、気軽に使えるものをイノベーションを通じて生み出し、その上でさらに大きなイノベーションを生み出していきたいですね。

「自由」と「夢」をインターネットで提供する

■そういう「イノベーション」の観点から、御社で行っている中国でのビジネスについて思うところはありますか?

中国では、インターネットが厳しく悪くなる方向に行っています。現状だと中国でのこれ以上の展開は難しいかなと考えています。

私は、「誰もが同じ機会を与えられること」、そして「自由であること」がとても重要だと考えています。日本でも昔、インフラは高かったですが、今は弊社のものを使えば誰でもインターネットに参入できます。そういうところで、インターネットの発展に寄与できたかなと考えています。

しかし、中国ではサーバを自由に貸していたらIPアドレスをブロックされたとか、ドメイン名を登録する人は顔写真が必要になるとか、とにかく規制、規制です。そういう考えは、弊社の理念に合いません。

「自由」という意味をどう捉えるかの違いだと思うんです。匿名で好き放題できるとか、そういった自由の話はしていません。インターネットを自由に使えるかどうか、利用機会が平等であるかどうかが重要なのです。法とマナーに触れない限りは何でもやっていいはずです。

中国にはそれがありません。政府を批判してはいけないというのは、法律でもマナーでもありません。インターネットに通じる自由すら奪うというやり方に、データセンターやコンテンツプロバイダも加担しないといけないのが嫌ですね。

■この業界で働く人に向けてメッセージはありますか。

もっと誇りを持って良いと思います。「インターネット土方」なんて揶揄がありますが、日こそ当たりにくくても、ラックやサーバを構築することは、ものすごく面白い仕事です。インフラの重要性を知ればさらに面白くなります。「Webサイトを作ることだけが面白いこと」なんてことはありません。誇りを持って楽しんで仕事をすればいいと思います。

逆に、コンテンツ側の人に言いたいのは、インフラをコストと見過ぎだということですね。そうではなくて投資なんだと。そういう意識を持って、上位レイヤの人には取り組んで欲しいです。GoogleやAmazonは、インフラは投資だと考えていますよ。コストではなく、新たなビジネスチャンスのための投資なんです。そこが、明らかに日米コンテンツ事業者の差異となって現れてきています。

日本のコンテンツ事業者は本当に狭い範囲しかやっていません。しかし、人口があるのでそこそこ儲かり、今は、どんどんインフラへの投資を削っています。でもここで効果的な投資をすると国力も上がるし、自らのサービスレベルも上がると心から思います。

■そんな貴社では、どのような人材を採用しているのでしょうか。

スキルではなく、人柄を見ています。もちろん、技術は大切にしているし、尊重されるべきものですが、企業としての技術力が重要なのであって、個人個人の技術が、特別に尊重されるべきものではないと考えています。つまり、「誰は技術があるから」ではなく、個人は平等に尊重されるべきです。テクニカルハラスメントという言葉もありますが、技術力があるからといって強く出たりするような人は採用しません。

最近は、派遣社員や契約社員が、正社員になるというパターンが多いですね。1年もあれば、できる人とできない人に分かれます。やる気があればBGP4、ドメイン名、Linuxだってわかります。我々の世代はロストジェネレーションなどと言われていますが、そういう人達に機会を与えるという、社会的な意義もあると思っています。

■あなたにとってインターネットとは?

「夢」ですかね。全てがかなう。「夢と感動」かもしれません。

ネットワークがつながっているという説明を頭では理解していても、実際につながった時の感動を、今でも忘れません。今までの人生で一番感動したかもしれません。このように、初めてアクセスした時の感動があるから、インターネットに夢が見られるのかもしれません。

青春時代にインターネットに触れたこと、それが自分の中のベースになっていますし、インターネットは常に自分と一緒にあるものだと思っています。

JPNIC 活動報告

Activity Report

活動カレンダー（2009年12月～2010年3月）

■12月

4日	第39回JPNIC臨時総会（東京、富士ソフト アキバプラザ） 第75回臨時理事会（東京、富士ソフト アキバプラザ）
8日	電子証明書を用いた認証方式に関する説明会（東京、JPNIC会議室）
17日	第26回ICANN報告会（東京、JPNIC会議室）

■1月

15日	IPアドレス管理指定事業者定例説明会（東京、JPNIC会議室） 電子証明書を用いた認証方式に関する説明会（東京、JPNIC会議室）
20日	JPNICオープンポリシーミーティングショーケース3（新潟、新潟市民プラザ）
27日	第76回通常理事会（東京、JPNIC会議室）

■3月

4日	HOSTING-PRO 2010（東京、KFC Hall）［後援］
12日	第40回通常総会（東京、東京ステーションコンファレンス） 第77回臨時理事会（東京、東京ステーションコンファレンス）
19日	IPアドレス管理指定者定例説明会

■ 第39回JPNIC臨時総会報告

2009年12月4日（金）に、第39回JPNIC総会（臨時総会）を、東京都千代田区の富士ソフト アキバプラザにて開催いたしました。今回の総会では、導入準備が進められているIDN ccTLDである「.日本」に関する報告が1件、また審議事項としては2009年度補正予算案の1議案について、会員の皆様にお諮りしました。以下、本総会の議案等について、簡単にご報告します。

◇理事長挨拶

総会開会に先立って後藤滋樹理事長から、出席会員へ挨拶が行われました。その中で、JPNIC事務局長の交代に関する報告が行われました。

■ JPNIC後藤滋樹理事長より、開会に先立ち挨拶がありました

2001年以来事務局長として運営を担ってきた成田伸一に代わり、2009年12月1日付けで新事務局長として林宏信が就任したことが会員の皆様に伝えられました。なお成田は当面、事務局長補佐として、JPNICの運営に関わることも報告されました。

◆報告事項:IDN ccTLD「.日本」について

2009年7月10日に開催された総務省の情報通信審議会において、「21世紀におけるインターネット政策の在り方（平成13年情報通信審議会諮問第3号）～新たなトップレベルドメイン名の導入に向けて～」という答申が行われました。この答申を踏まえ、日本国内におけるインターネット関連団体が共同して「日本インターネットドメイン名協議会」[※1]を設立し、活動を開始しています。この協議会で検討を進めている「.日本」について、JPNICの関わり方を含めたこれまでの経緯等を、成田事務局長補佐より報告いたしました。

■ 第39回JPNIC臨時総会会場の様子

◆第1号議案:2009年度補正予算案承認の件

本議案は、2009年3月19日に開催された第37回通常総会[※2]にて承認された、2009年度収支予算に変更が生じたため作成した、補正予算案についてお諮りしたものです。

主な補正の要素は、

・インターネット基盤整備基金資産運用収入の減額補正
・2008年度決算値を反映させた前期繰越収支額の増額補正

等で、その他の増減する収支予算項目も併せて、林事務局長が説明を行いました。本議案は、原案の通り承認可決されました。

この第39回臨時総会の資料、議事録等は、JPNIC Webサイトにて公開しております。

社団法人日本ネットワークインフォメーションセンター
第39回臨時総会
http://www.nic.ad.jp/ja/materials/general-meeting/20091204/

◇　◇　◇

総会に引き続き、講演会を行いました。今回は、当センターの前村昌紀インターネット推進部部長より、「ICANNの最新動向」と題した講演をお送りしました。講演では、ICANNの役割、組織構造や、新gTLD、IDN ccTLDに関する最新動向について説明いたしました。

■ 総会後の講演会では、JPNICインターネット推進部部長の前村昌紀よりICANNの最新動向についてご説明いたしました

次回の第40回通常総会（2010年度事業計画・収支予算）は、2010年3月12日（金）に開催予定です。

（JPNIC 総務部 佐藤俊也）

※1 日本インターネットドメイン名協議会
http://jidnc.jp/

※2 社団法人日本ネットワークインフォメーションセンター 第37回総会（通常総会）
http://www.nic.ad.jp/ja/materials/general-meeting/20090319/

Activity Report

■ 第17回JPNICオープンポリシーミーティング報告

［関連記事］P.32「APNIC28ミーティング報告」

2009年11月26日（木）に、秋葉原コンベンションホールにて、第17回JPNICオープンポリシーミーティング（JPOPM）を開催いたしました。Internet Week 2009の会期中、同会場での開催です。

今回のミーティングには、64名の方々（関係者を除く）にご参加いただきました。NTTスマートコネクト株式会社様、JPNICの協力により、今回も映像ストリーミング、Jabberチャットによるリモート参加環境を提供いたしました。試験的に、Twitterによる情報提供も実施しました。リモート参加者は、100名（うち16%はIPv6経由）でした。皆様、ありがとうございました。

JPOPMは、日本におけるインターネット資源（IPアドレスおよびAS番号）の管理に関するポリシーを検討・調整し、日本のコミュニティにおけるコンセンサスを形成するための議論の場です。開催は年2回で、JPNICとは独立した組織であるポリシーワーキンググループ（ポリシーWG）が主催しています。ミーティングのプログラムは、ご応募いただいたポリシー提案や情報提供プレゼンテーションから構成します。今回は、提案3件および情報提供プレゼンテーション7件の応募をいただきました。

◆提案に関する議論

今回の提案は、2件がAPNICで決まったポリシーを日本国内でも実施することに関するもので、もう1件がポリシー策定プロセスの変更提案でした。提案の概略、およびミーティングでの議論結果について紹介します。

1.IPv6申請手続き簡素化提案への対応について
http://venus.gr.jp/opf-jp/opm17/p017-01.html

APNIC28にて決まった、IPv6アドレス割り振りポリシーの簡素化提案です。APNICからIPv4アドレスの割り振りを受けている組織は、IPv6アドレスの割り振りを受ける際に、現状では他組織への割り当て予定の提示等、いくつかの要件を満たさなければなりません。これを、既存IPv4アドレスホルダーに対してはIPv6アドレスが必要という意思表示のみで配布するようにしよう、というものです。ミーティングでは、日本におけるこのポリシーの必要性に懐疑的な意見もありましたが、特に強い反対もなく、コンセンサスとなっています。

2.RIRで施行されたポリシーをNIRで実装する為の手続きの変更について
http://venus.gr.jp/opf-jp/opm17/p017-02.html

このポリシーは、「JPNIC管理下にあるIPv4アドレスの移転」のポリシーを、JPOPM17に提案するために、ポリシーWGから提案したものです。現在のポリシー策定プロセスでは、APNICミーティングで成立したポリシーのうち、NIRで施行の是非を判断できるポリシーについては、JPNICがJPOPMにて提案する、となっています。しかしながら、JPNIC内の業務プロセスの都合で、APNICミーティング直後のJPOPMへの提案が間に合わなかった場合に、国内でのポリシー施行が遅れてしまう、という問題点がありました。

この提案では、APNICでの決定事項は、誰でも国内JPOPMに提案できるようにすることで、この問題の解決を図っています。これに対し、APNICミーティングで決まったポリシーのうち国内で提案されないものが出てきてしまうのでは、といった懸念や、JPNICが必ず次のJPOPMで提案するというように変更する方がよいのでは、といった意見が出されました。前者については、JPNICとポリシーWGで、そのようなことがないように運用すること、後者については、組織の運用に絡む話でもあり、今後継続して検討することとし、本ポリシーはコンセンサスとしています。

3.JPNIC 管理下にあるIPv4アドレスの移転提案
http://venus.gr.jp/opf-jp/opm17/p017-03.html

以前より議論が続いていたIPv4アドレスの移転提案ですが、直前にAPNICにて施行が決定しています。本提案は、同様の移転提案を、国内でも実施するというものです。大勢は移転提案実施に賛成でしたが、移転を許し、IPv4アドレスが売買された場合に、組織が保有するIPv4アドレスが資産として課税される可能性があるという理由から、提案に反対する意見もありました。ミーティングではコンセンサスとなっています。

今回の1～3の提案は、ミーティングでは全てコンセンサスとなりましたが、「3」の提案は、「2」の提案の成立を前提とするという条件付きとなっています。今後、それぞれの提案について、ip-usersメーリングリストで最終コンセンサス確認実施後、JPNICに対して実装勧告をすることになります。

◆情報提供プレゼンテーション

その他、過去のポリシー提案に関するJPNICでの検討状況、APNICミーティング紹介などの通例の情報提供プレゼンテーションに加え、APNICより来日いただいた藤井美和氏に、最近のAPNICでの取り組み、特にAPNICにおける「人的」資源の割り当ての現状について発表していただきました。APNICにおけるプライオリティの高い活動として、インターネット資源、インターネットインフラに関するR&D活動が挙げられました。また、アジア太平洋地域におけるネットワークエンジニアリング教育、トレーニングやIPv6の普及推進に力を入れていることの紹介、APNICミーティングへのオンサイト、リモートを含む積極的な参加の依頼がありました。

なお、以下のURLより、当日の発表資料、議事録がご確認いただけますので、ご参照ください。

□第17回 JPNICオープンポリシーミーティングプログラム
http://venus.gr.jp/opf-jp/opm17/opm17-program.html

◆ミーティングを振り返って

IPv4アドレス在庫枯渇への対策の一つとして、IPv4アドレス移転提案がAPNICでもコンセンサスとなり、日本国内でも実施の方向となっております。IPv4の延命、IPv6への移行もいろいろな観点から議論されており、アドレスポリシーとしての提案も今後まだまだ増えてくることが予想されます。今後の議論にご注目ください。

ミーティング中に、藤井氏よりご紹介がありましたが、次のAPNICミーティングは2010年3月に、マレーシアで開催されます。今回はAPRICOTミーティング中での開催となります。リモート参加環境も非常に充実していますので、ご興味のある方は、ぜひともご利用ください。ミーティングの詳細については、下記のURLでご覧になれます。

□APNIC 29 - Kuala Lumpur 1 - 5 March 2010
http://meetings.apnic.net/29

最後になりますが、オンサイト、リモートともに議論にご参加いただいた皆様、発表にご応募いただいた皆様、ありがとうございました。次回のJPNICオープンポリシーミーティングは、2010年7月上旬に開催、提案募集開始は6月初頭頃を予定しています。アドレスポリシーに関してご意見をお持ちの方のご応募をお待ちしています。また、今回ご参加いただけなかった方も、ぜひご参加ください。

（ポリシーワーキンググループ/
NTT情報流通プラットフォーム研究所 藤崎智宏）

■ 会場の様子

■ まずはじめに、本ミーティングでコンセンサスとして確認したい項目の説明が行われました

■ APNICの藤井美和氏に発表いただきました

■ 第26回ICANN報告会レポート

［関連記事］P.45「ICANNソウル会議報告」

2009年12月17日（木）にJPNIC会議室（東京都千代田区）にて、JPNICと財団法人インターネット協会（IAjapan）の共催により第26回ICANN報告会を開催しました。本報告会は、韓国のソウルで開催された第36回ICANN会議（2009年10月25日～30日）についてご紹介したものです。今回50名近い参加申し込みをいただき、当初の締め切りより早く受け付け終了となるほどの盛況となりました。以下、その模様をご紹介します。

◆新たな報告会構成

今回はICANN会議の会場がお隣の韓国と比較的近く、日本から多数の参加があったこともあり、新たに4名の方（計8名）より講演していただくことができました。そのため、第1部（ICANN支持組織・諮問委員会についての報告）／第2部（新gTLD関連トピック）という、2部構成とすることができ、最も関心が高まっていると思われる新gTLDについて深く掘り下げることができました。

◆第1部（ICANN支持組織・諮問委員会についての報告）

○ICANNソウル会議概要報告

JPNICの前村昌紀より、ICANNソウル会議の全体概要について報告しました。AoC[※1]、新gTLD、IDN ccTLDなどについて網羅しています。詳細については、P.45からの「ICANNソウル会議報告」をご覧ください。

○国コードドメイン名支持組織（ccNSO）報告

株式会社日本レジストリサービス（JPRS）の堀田博文氏からは国コードドメイン名支持組織（ccNSO）会合での議論のうち、以下の3点について、主にご報告いただきました。

- DNSSECワークショップでの各TLDおよびルートでのDNSSEC対応状況
- レジストリにおけるIPv6準備状況
- IDN ccTLDファストトラックおよび関連する議論

○ICANN政府諮問委員会（GAC）報告

総務省の中沢淳一氏より、ICANN政府諮問委員会（GAC）会合で話し合われた議題のうち、IDN ccTLD（国コードトップレベルドメインの多国文字表記）、新gTLD（分野別トップレベルドメイン）の導入、AoCの3点を主にご報告いただきました。

○GNSO評議会報告

東京大学のラフィク・ダンマク氏より、GNSO評議会について、主にGNSO組織改編およびGNSOが現在抱える課題についてご報告いただきました。氏は新たにGNSO評議員に選出され、ソウル会議より職務を開始されています。

■ GNSO評議員のラフィク・ダンマク氏

◆第2部（新gTLD関連トピック）

○レジストリ／レジストラ分離問題

株式会社インターリンクの才門功作氏より、レジストリ／レジストラ分離問題（新gTLD募集にあたり、レジストリがレジストラを運営すること、あるいはその逆について認めるかどうか）についてご報告いただきました。ソウル会議での論点は、レジストラが資本関係にあるレジストリのTLDを扱うことを認めるか否かというものでした。

○新gTLD Expression of Interest WG動向

GMOドメインレジストリ株式会社の大東洋克氏より、新gTLD応募に関する関心表明（Expression of Interest; EoI）ワーキンググループ（WG）の動向についてご報告いただきました。

EoIとは新gTLD申請の前段階として、申請文字列および申請者に関する情報を申請者より提出してもらい、参加した人のみが新gTLDの本申請に参加できるという仕組みです。最初は新gTLD利害関係者がソウル会議会期中に集まって今後の新gTLDについて議論したのがきっかけで、その後公開フォーラムへの提案後、理事会よりEoIとしてスタッフに検討を指示する旨の決議がありました。

この後、新gTLD利害関係者の集まりはEoI WGと呼ばれることになりました。検討中の案によれば、EoIの申請者は申請文字列と申請者についての情報を提供することになり、ICANNはこれらの情報を公開することになっています。

■ GMOドメインレジストリ株式会社大東洋克氏にEoI WGの動向についてご報告いただきました

○新gTLDにおけるRight Protection Mechanismについて

株式会社ブライツコンサルティングのヘレン・ケンニョン氏より、新gTLDによる商標権の侵害を防ぐための仕組みである、Right Protection Mechanism（商標保護措置）の検討状況についてご報告いただきました。

主な商標保護措置としては、次の3点が想定されています。

- 登録開始前に利用されることになる商標データベースであるTrademark Clearinghouse
- 登録開始後に利用されることになる、商標権侵害時の迅速な対応手段であるUniform Rapid Suspension（URS）
- TLD利用開始後に利用されることになる、レジストリに対する異議申し立て手段であるPost Delegation Dispute Resolution Mechanism（PDDRM）

■ 株式会社ブライツコンサルティングのヘレン・ケンニョン氏にご講演いただきました

○新gTLD申請における文字列競合・オークションについて

JPNIC理事の丸山直昌より、新gTLD申請の際、複数の申請者より提出された同一または類似の文字列が競合する際の解決プロセスについて、例示および考察についての報告がありました。それによれば、競合がある場合はまずICANNがその事実を公表した上で、コミュニティ優先評価を行い、合格したところのみが残ります。合格した事業者が複数あればオークションとなり、競合がなくなるまでオークションを繰り返すことになります。参加者の利害関係について考察したところ、申請者間での個別調整が行われるのではないか、とのことでした。

最後に、IAjapanの高橋副理事長からご挨拶をいただき、本報告会を閉会しました。なお、次回第37回ICANN会議は、ケニアのナイロビにて開催される予定です。

◇　　◇　　◇

なお、本報告会の発表資料は、JPNIC Webサイトで後日公開いたします。また、動画も後日公開予定ですので、ぜひそちらもご覧ください。

（JPNIC インターネット推進部 山崎信）

■ 会場の様子

※1 AoC（Affirmation of Commitments: 責務の確認）
米国商務省とICANNとの間の文書で、インターネットの資源管理に関して、両者が果たすべき責務について記載されています。前身の文書であるJPAが2009年9月30日に失効したのに伴い、同日、米国商務省電気通信情報局とICANNの双方により公開され、翌10月1日から発行しました。

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

2009.8.25▶8.28

APNIC28ミーティング報告

■ アドレスポリシー動向

［関連記事］P.28「第17回JPNICオープンポリシーミーティング報告」

今回北京で行われたAPNIC28ミーティングは、中国のNIRであるCNNICがローカルホストを務め、2009年8月25日（火）～28日（金）の4日間で開催されました。

会場となったホテル、Grand Hyatt Beijingは、天安門広場から徒歩15分ほどの街の中心にあり、会議に参加しながらも短い観光ができ、街の雰囲気を味わうことのできる環境となっていました。

参加者は51組織、272名（APNIC26では70組織、237名）と、昨年の単独開催（APRICOTとの併催型でなかったAPNIC26）と比較した場合、組織単位での参加者数が昨年よりも多かったことが特徴です。

数年前まではAPNICミーティングというと、アドレスポリシーの提案について議論を行うカンファレンスとのイメージが強くありましたが、現在はAPOPSやIPv4アドレスの在庫枯渇/IPv6の実装などをテーマにしたテクニカルセッションも主なプログラムとして組み込まれ、地域内でオペレーショナルな情報を共有/議論できる構成になっています。

□Program Highlights

トレーニング、APOPS、各種プレナリー、ポリシーSIG（およびNIR SIG）、APNIC総会、レセプション/懇親会
http://meetings.apnic.net/28/program/

今回はやはり地元である中国からの発表が普段よりも多く、オペレーション面では、4バイトAS番号の対応に向けた情報提供や、IPv6の実装について具体的な事例紹介、また、時事ネタとして2009年7月のDDoS攻撃の事例が紹介されていました。

本稿ではアドレスポリシー提案の結果を中心にお伝えします。オペレーション面での内容については、P.35の「APOPSにおけるオペレーター向けの話題」をご覧ください。

◆APNIC28でコンセンサスの得られたポリシー提案

前回までの流れから見ると、IPv4アドレス在庫枯渇に向けた対応、IPv6アドレスの取得における障壁に向けたポリシー面での対応は一段落したと考えていたので、あまり多くの提案が提出されないことが予測されていました。

しかし、結果としては今回のミーティングでは、ポリシーSIGにて7点の提案が提出されました。そのうち、コンセンサス※1の得られた提案は、次の4点です。

テーマとしてはIPv4アドレスの移転、IPv4保有者に対するIPv6の分配手続きの簡素化が注目され、残り2点のAS番号に関する提案も、現状の2バイトAS番号の利用状況を見据えて必要な施策として支持されました。

コンセンサスの得られた提案

prop-050：IPv4アドレスの移転
http://www.apnic.net/policy/proposals/prop-050
（＊）提案の背景については、JPNIC News & Views vol.623※2の特集記事内、「prop-050 IPv4アドレス移転の提案」を参照ください。

移転元、移転先、両者の合意があれば、以下の要件でAPNICから直接分配を受けているIPv4アドレスの移転（最小移転単位/24）を認める。
（1）移転元は、移転後12ヶ月はAPNICへ追加のアドレス申請を行うことができない。ただし正当な事情があることを証明すれば、当該期間内の申請も可能。
（2）APNICのIPv4アドレス在庫枯渇前は移転時に利用状況の審議を行う。枯渇後は、審議は行わない。

prop-073：現IPv4保有者を対象としたIPv6アドレス申請手続きの簡素化
http://www.apnic.net/policy/proposals/prop-073
（＊）旧題:IPv4アドレス保有者へのIPv6の自動的な割り振り/割り当て

IPv4アドレスの分配をAPNICから直接受けている組織は、IPv6においても同じく分配対象と想定されており、当該組織が分配を必要とする意思表明をすれば、それ以上の審査をすることなく、以下のIPv6の分配を行う。
（1）IPv4の割り振りを受けている場合:IPv6/32を割り振る。
（2）IPv4の割り当てを受けている場合（＊）:IPv6/48を割り当てる。
（＊）歴史的PIは対象外

prop-074：4バイトAS番号の分配に関するIANAからRIRへのAS番号割り振りポリシー
http://www.apnic.net/policy/proposals/prop-074

IANAからRIRへ2バイトから4バイトを区別してAS番号を割り振る期間を2009年12月31日→2010年12月31日に1年間延長する。
グローバルポリシーとして全RIRにて提案中。

prop-075：歴史的経緯を持つAS番号の有効利用
http://www.apnic.net/policy/proposals/prop-075

経路広告されておらず、利用意思の確認できない歴史的経緯を持つAS番号を回収する。歴史的PIアドレスの回収と基本的に同じ手続きとする。

◆ポリシー提案の結果について

今回のミーティングにあたって参加者が最も気にかけていたのは、2007年から議論を行っているIPv4アドレス移転の提案に対する結果でした。

また、「prop-073 現IPv4保有者を対象としたIPv6アドレス申請手続きの簡素化」提案も当初は懸念の方が強かったものの、コミュニティメンバーの意見を反映した形で提案内容が見直され、コンセンサスが得られる結果となりました。

移転提案については、前回のAPNIC27（マニラ）では、ミーティングのコンセンサスは得られたものの、その後のメーリングリストでの議論により、最終的な結論としては「継続議論」となり今回に持ち越されたため、提案者も、前回のミーティングで提案を支持していた参加者も、今回こそは正式な決定に至りたい、という気持ちがあったと思います。

事前に行われていたメーリングリスト上での議論の争点は、IPv4アドレス在庫枯渇前の、移転目的でのAPNIC在庫消費/再移転を目的とした移転アドレスの取得防止に向けた要件設定でした。意見の異なるコミュニティメンバーが自主的に調整し、合意できる要件を見つけられたため、ミーティング当日は大きな反論もなくスムーズに参加者のコンセンサスが得られる結果となりました。

国内での施行については、2009年11月26日（木）開催のJPNICオープンポリシーミーティングで議論をいたしました。議論の詳細については、P.28の「第17回JPNICオープンポリシーミーティング報告」をご覧ください。

また、prop-073に基づき、IPv6の割り振り申請手続きが簡素化されることにより、これまでよりも申請時の負荷が軽減されると考えられます。国内においては、具体的にIPv6の実装を予定している組織であれば、既存の要件でIPv6アドレスを取得済みであるケースが多いと考えられ、具体的な障壁となっているとの意見はありませんで

■ 会場となったGrand Hyatt Beijing

■ Opening PlenaryでスピーチをするAPNICのPaul Willson氏

した。しかしながら、まずはアドレスを取得しようと考えている組織にとっては、これまでよりも申請が行いやすくなるのかもしれません。

◆ミーティング後のプロセス

8週間のメーリングリストでのコメント期間中に、特筆すべき懸念が表明されなかったため、定義されたプロセス※3に従って、これらの提案はAPNICにおいて正式に承認されました。

◆次回のAPNICミーティング

次回はAPRICOTカンファレンスプログラムの一部として、2010年3月にマレーシアのクアラルンプールで行われる予定です。

□APNIC29 kuala Lumpur
http://meetings.apnic.net/29

◆参考情報

□APNIC28 -Beijing 2009
http://meetings.apnic.net/28

□その他APNIC28におけるポリシー提案

継続議論となった提案：

prop-076：IPv6追加割り振り申請時における経路集約の要件追加
http://www.apnic.net/policy/proposals/prop-076
JPOPM16でのコンセンサスに基づいた提案。

http://venus.gr.jp/opf-jp/opm16/jpopm16-p1-v1.pdf
IPv6追加割り振り申請時にも、初回申請時と同じく、ポリシー上、割り振りIPv6アドレスを単一の経路に集約することを求める。

提案者へ差し戻しとなった提案：

prop-077：歴史的経緯を持つPIアドレスにおける移転に関する移転要件の補完
http://www.apnic.net/policy/proposals/prop-077
APNICと契約/費用支払い関係にない歴史的PIは、LIR管理下に移転することが認められている。当該アドレスの移転要件もprop-050と統一することをめざしている。なお、JPNIC管理下の歴史的PIは、すべて合意書締結済みのため対象外。

prop-078：IPv6の実装を前提として分配するIPv4アドレスのための/10 IPv4アドレス空間の確保
http://www.apnic.net/policy/proposals/prop-078
IPv6の実装を前提としたIPv4アドレスの分配専用に、APNICの最後の/8在庫のうち、/10を別途リザーブする。

（JPNIC IP事業部 奥谷泉）


■ NIR SIGでは、chairに筆者（写真右端）が、co-chairにWei Zhao氏（写真中央）が選ばれました

※1 コンセンサス
JPNICやAPNICのポリシーフォーラムにおける「コンセンサス」とは、特定の提案事項に対するコミュニティの「総意」を意味します。そして、コンセンサスに至った提案はJPNICやAPNICのポリシー、またはIPアドレス登録管理業務に反映、施行されます。

※2 JPNIC News & Views vol.623
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol623.html

※3 APNIC地域におけるポリシー策定プロセス
http://www.apnic.net/community/policy/process

■ APOPSにおけるオペレーター向けの話題

本稿では、APNIC28ミーティングの中で開かれた、The Asia Pacific OperatorS Forum（APOPS）※1について報告します。APOPSは、AP地域のインターネット・オペレーターを対象とした技術的な話題を扱うフォーラムで、APNICミーティングで開催されるプログラムの一つとして開催されています。APNIC28ミーティングでは、2日目の2009年8月26日（水）午前11時から15時半にかけて開催され、約90名が参加しました。

今回のAPOPSは、特にテーマが限られておらず、NAT、IPv6、AS番号、DNSSEC、DDoSといったさまざまな話題のプレゼンテーションが行われました。日本からは、川村聖一氏（NECビッグローブ株式会社）、芦田宏之氏（イッツ・コミュニケーションズ株式会社）、外山勝保氏（インターネットマルチフィード株式会社）の3名が、プレゼンテーションをされていました。

APOPSの議題

（午前の部）

- “DNSSEC deployment in New Zealand”
  Andy Linton氏（Victoria University of Wellington）
- “IPv6 representation”
  川村聖一氏（NECビッグローブ株式会社）
- “Careful planning is needed for introducing NAT”
  芦田宏之氏（イッツ・コミュニケーションズ株式会社）
- “Challenges in Large IP network deployment”
  Echo Liu氏（WANDL社）
- “The strategic value of introducing IPv6”
  Cancan Huang氏（China Telecom社）

（午後の部）

- “APIX Update”
  外山勝保氏（インターネットマルチフィード株式会社）
- “AS number report”
  Geoff Huston氏（APNIC）
- “DITL”
  George Michaelson氏（APNIC）
- “7.7 DDoS cyber attack in Korea”
  Ji-Young Lee氏（KRNIC/KISA）
- “The Emperor's New Cloud: An Analysis of the July 2009 RoK/USA DDoS Attacks”
  Roland Dobbins氏（Arbor Networks社）

本稿では、これらのプレゼンテーションのうち、DNSに関するトピックを二つとセキュリティに関するトピックを一つ、合計三つについて報告します。

◆DNSSEC deployment in New Zealand

Andy Linton氏から、ニュージーランドのccTLDである、.nzにおけるDNSSECの取り組みについて紹介がありました。はじめに、.nzは2009年中もしくは2010年早々に、DNSSECのサービス開始をする予定であり、それに向けて準備をしている段階だという話がありました。続いて、DNSSECでサービスを開始するにはさまざまな課題があり、その解決が必須であることも紹介されました。DNSSECサービス開始のためにDNSソフトウェアの整備が必要であることや、DNSSECが加わったときのドメイン名登録手続きに関わる作業の変化、鍵の管理、レジストリやレジストラの責任など、多数の検討項目が挙げられました。

◆DITL

APNICのGeorge Michaelson氏により、DNSの状況を調査するDITL（Day In The Life）というプロジェクトについて紹介がありました。DITLは毎年ある期間、世界中のDNSサーバにおけるクエリ状況を調査するもので、2009年も3月29日から4月2日まで行われました。37組織190ノードのDNSサーバが対象となってデータが収集され、そのデータの総計は4TBにもなったそうです。


■ 会場内のロビーの様子

APNICのDNSサーバもそのうちの一つであり、この発表ではAPNICが管理するサーバの統計が紹介されました。問い合わせ元のIPアドレスについて、2008年のものと2009年のものを比較すると1/3が一致せず、流動的なアドレスが比較的多数を占めること、ごく少数のホストが大量に問い合わせを行っていること、2008年と比較してIPv6トランスポートでの問い合わせが増えていること、毎日午前4時頃に日本から大量の問い合わせがくることなど、APNIC DNSの挙動について興味深い紹介がありました。

◆7.7 DDoS cyber attack in Korea

KRNICのJi-Young Lee氏からは、2009年7月7日頃に韓国および米国で起こったDDoS（Distributed Denial of Services）事件について報告されました。DDoS攻撃は、最初のうちは米国のホワイトハウスを対象としていましたが、時間の経過とともに、韓国内のポータルサイトや新聞社のWebサーバへの攻撃に変わっていったことがわかっています。zombie PC※2となったホスト数を集計した結果、韓国内ではその台数が77,875台にのぼりました。

KRNICでは、ISPとしての対策が取れるように、DDoSに利用されたzombie PCのIPアドレスを該当するISPに通知したり、主要なポータルサイトにワクチンを載せるための連携を図ったりしました。それらの活動を通じて、WHOISの情報を正確に保つことの重要性をあらためて学んだ、とのことです。会場からは、DDoSが起こった時間的経緯に関する質問がありましたが、技術的な経緯のわかる詳細な情報は、KRNICには来ていなかったようです。他には、DDoS攻撃のあった時間帯にBGPのupdateメッセージが多くなったという情報が寄せられました。

■ 会場のそばの王府井大街

当日のプレゼンテーション資料などは、以下のWebページに載せられています。

□APNIC28 / Program / APOPS
http://meetings.apnic.net/28/program/apops

◇　　◇　　◇

APOPSでは、日本からの参加者も活躍していました。チェアを務める吉田友哉氏（NTTコミュニケーションズ株式会社）の活躍をはじめ、日本の事業者の方々が内容の濃い発表をされていることが印象的でした。

今回のAPOPSは、APNICミーティング全体に比べると参加人数が少なく、また会場での質疑応答は多くありませんでしたが、各発表の内容の良さがより多くの人に知られることで、今後この状況は変わっていくかもしれません。

今後も特筆すべき事項がありましたら、本稿のような形で報告していきたいと思います。

（JPNIC 技術部 小山祐司／木村泰司）


■ 手前の東長安街通りの先には天安門広場があります

※1 The Asia Pacific OperatorS Forum
http://www.apops.net/

※2 zombie PC
DDoS攻撃のパケットを送出するために利用されたホスト

2009.10.5▶10.9

第59回RIPEミーティング報告

■ 全体会議報告

ポルトガルの首都リスボンは、ゴツゴツとした石畳と明るいクリーム色の建物が印象的な歴史ある街です。夕食のために旧市街に出かけると、情緒あるケーブルカーが急な斜面を登っていくのを目にしました。

◆RIPE59ミーティングの概要

第59回RIPEミーティングは、リスボンにあるCorinthia Hotelで行われました。

開催期間：2009年10月5日（月）～9日（金）
参加者数：300名（登録者数355名） ※2009年10月9日時点
参加国数：36ヶ国
参加者の多い国：イギリス（36名）、オランダ（34名）、ドイツ（34名）、米国（33名）、ポルトガル（28名）（日本からの参加者は9名）

初日と2日目は全体会議であるPlenaryが行われ、後半は各WGのミーティングが行われました。2009年10月現在、活動していないWGを除くと、RIPEには11のWGがあります。

□RIPE Working Groups
http://www.ripe.net/ripe/wg/

◆Plenary

全体会議であるPlenaryは、以下のような内容で行われました。

Plenary 1 - 4バイトAS番号やMPLS、CPE（Customer Premises Equipment: カスタマー構内設備）等

Plenary 2 - IPv6のディプロイメント

Plenary 3 - RIR/NRO等関連団体の活動報告

Plenary 4 - RIPE NCCのトピック

Plenary 5 - 主にDNSSEC関連のトピック

Plenaryのアジェンダと資料は、次のURLから見ることができます。


Lisbon, Portuguese Republic

□“Agendas RIPE 59 Lisbon, 5-9 October 2009”
http://www.ripe.net/ripe/meetings/ripe-59/agendas.php?wg=plenaries

以降、主にPlenaryでの議論を中心に報告いたします。

◆IPv6関連

IPv6のディプロイメントについては、2日目のPlenary 2で四つのプレゼンテーションがありました。簡単に内容を紹介します。


■ Plenaryの様子

- France Telecom's IPv6 Strategy

フランスの大手通信会社であるフランステレコム社の、インターネット接続サービスにおけるIPv6導入の中間発表です。CPEとNATを併用する方式や、IPv6でIPv4のプライベートアドレスをカプセル化する、Dual-Stack Lite方式などのいくつかの収容方法が検討されています。フランステレコム社では、2010年末までにグループ会社全体でIPv6が使えるように整備が進められています。

- A Strategic Approach to IPv6

HEARNET社では既にIPv6の導入が済んでいますが、今後IPv6のみのサービスネットワークを提供するという課題に直面しています。IPv4アドレスの在庫枯渇時期と予測されている、2011年に向けたマイルストーンが示されています。

- IPv6 in Real Life

DNSを使ったIPv6導入に関する国別統計を、2、3年前と比較しています。100ヶ国程度を調査した結果、AAAAが返ってくるドメイン名は3～4倍に増えていますが、中にはリンクローカルのアドレスが返ってくるなど、設定が適切ではないところがあったようです。

- IPv6 in the Citizens with Special Needs' Network

ポルトガルの学術関連ネットワークにおけるIPv6導入状況の紹介です。IPv6の通信を行っているノードは約120見つかっているそうです。

◆RIPE Labs

RIPE NCCでは、正式サービスになる前の実験サービスや開発途中のプログラムを公開し、RIPEコミュニティにおける議論の活性化を目的とした「RIPE Labs」と呼ばれる活動が始められました。これは、RIPE NCCのRobert Kisteleki氏の考案によるものです。会場では、IPv4アドレスの/8の割り振りを自動車レースになぞらえたアニメーションが紹介されていました。この他に以下のようなアプリケーションやデータベースが開発されています。

- REX - the Resource Explainer

割り振り済みIPアドレスの利用状況を、経路情報やDNS･ブラックリストに載っているIPアドレスといった複数の観点で見られるWebのツールです。ISPやRIPE NCCのIPアドレス担当者がIPアドレスの利用状況を確認できるほか、IPアドレスの移転が行われる場合にもIPアドレスの情報を確認できるようになっています。

- The Internet Number Resource Database（INRDB）

RIPE NCCのRISやIANA、他RIRの情報を集約したデータベースで、RIPE Labsの各アプリケーションやコマンドラインプログラムで使えるような出力インタフェースを持っています。

- RIPE 59 Meeting Plan for Google Calendar

これは厳密には「開発」とは呼べませんが、Google CalendarでRIPE59ミーティングの予定が見られるようにメンテナンスされているようです。

- 16-bit ASN Exhaustion - some data

2バイトAS番号の在庫枯渇状況をわかりやすく見えるようにするツールで、会場では在庫枯渇のグラフが紹介されていました。

- NetSense - next generation Information Services

1990年にIPアドレスが割り当てられたホスト数の統計を求める「hostcount」がRIPEコミュニティで始まって以降、RIPE NCCではRIS（Routing Information Service）、TTM（Test Traffic Measurements）、DNSMON（DNS Monitoring Services）といった統計データを取り、それを視覚化するさまざまなツールが開発されました。

NetSenseは、これらを簡単に見られるようにするためのWebアプリケーションで、詳しい情報を表示しつつも全体概要を捉えやすいようなツールになるように設計されています。

RIPE Labsのこれらのツールは、同Webサイトで紹介されつつ、リンクも張られています。

□RIPE Labs
http://labs.ripe.net/

◆DNSSEC

2日目のPlenary 5では、DNSSECについて三つのプレゼンテーションがありました。

- DNSSEC in .pt

ポルトガル国内で行われたDNSSECの必要性に関するアンケート結果などについての報告です。

- Scaling the Root

ICANN理事会の要請により行われている調査活動で、DNSSECや国際化TLD、新gTLDを視野に入れた、ルートゾーンのサイズと変更頻度の増加に関する調査の途中経過です。今後、ソウルで開催されるICANN会議やパブリックコメントの募集が行われるようです。

- DNSSEC for the Root Zone

ICANNとVeriSign社による、ルートゾーンへのDNSSECの導入に関する発表です。Transparency（業務の透明性）、Audited（ISO/IEC 27002:2005認定）、High Security（NIST SP800-53相当）といったキーワードを使って取り組みが紹介されていました。PKIでいうCPS（Certification Practice Statement）と似た構成のDPS（DNSSEC Policy & Practice Statement）を作成するなど、堅牢性に留意したシステムが検討されています。

このうち3番目のプレゼンテーションで、今後のルートゾーンへの署名スケジュールが発表されました。

December 1, 2009
　ルートゾーンへの署名
　ICANNとVeriSign社によるKSR（Key Signing Request）の処理

January - July 2010
　署名付きルートゾーンの提供

July 1, 2010
　トラストアンカー提供とKSK運用
　署名付きルートの提供完了

会場では、KSK（Key Signing Key）の鍵長が1,024bitでは短かすぎるのではないか、provisioning systemの準備が遅れているのではないか、実際にKSKがITAR（Interim Trust Anchor Repository）などに置かれるのはいつなのかが重要である、といったコメントが挙がりましたが、スケジュールを公開しながら進めることに関する評判はよかったようです。

これを受けてRIPEのDNS WGでは、ICANNによるルートゾーンへのDNSSEC導入の発表を歓迎するとともに、今後も計画を公開しながら進めるよう要請する声明を出すことになりました。

◆RPKI関連

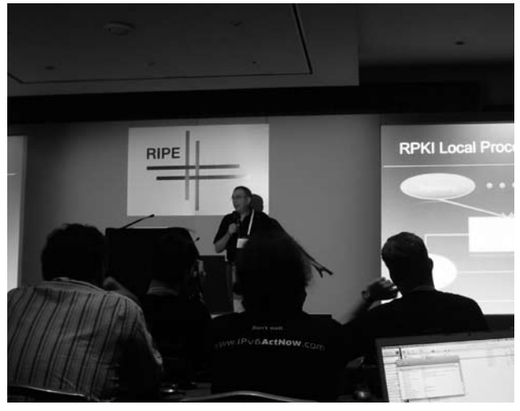
RPKI（Resource PKI）証明書については、Address Policy WGで議論が行われました。NCC Service WGでもプレゼンテーションが行われました。RIPE NCCでは、リソース証明書を発行し利用していくまでに、大きく分けて四つの課題があると考えられています。

（1）RIPE NCCにおける契約との関連性

（2）政府による要望や命令に従って証明書を失効すべきかどうか

（3）紛争の対象となっているアドレスの扱い

（4）業務ミスやプログラムエラーへの対応



■ RPKIに関するプレゼンテーションを行うStephen Kent氏

この中で特に議論されたのは、(2)のリソース証明書の失効についてです。失効とは、有効期限内に電子証明書を無効化することで、リソース証明書を発行しているRIPE NCCは、技術的には証明書保持者の意図に反してリソース証明書を失効させることができます。例えば、RIPE NCCの事務局があるオランダの政府当局によって、特定のネットワークのIPアドレスを無効化させるような要請や命令があった場合に、どのような対処をし、問題の整理を行えばよいのか、といったことが議論されました。

会場では、ISPで経路制御のためにリソース証明書を使い、自動的に制御されるような状況をすぐに実現させるべきではないといった意見や、レジストリはインターネット経路制御に関与しないという背景を受けて、リソース証明書の失効は割り振り情報の削除と同様に、インターネット経路制御に影響しないようにすべきといった意見が挙げられました。

今後、Certification Task Forceが中心となって、Address Policy WGでリソース証明書のためのCPSの作成が行われることになりました。RIPE NCCでは、全てのRIRで正式サービス化されると言われている2011年1月1日までに正式サービス化する、としています。

◇　　◇　　◇

次回の第60回RIPEミーティングは、2010年5月3日～7日にチェコのプラハで行われる予定です。

（JPNIC 技術部／インターネット推進部 木村泰司）

■ RIPE地域におけるアドレス分配ポリシーの動向

2009年10月5日から9日に行われた第59回RIPEミーティングのうち、本稿では、アドレス分配ポリシーの動向をお伝えします。

今回のミーティングでのアドレス分配ポリシーにおいて特筆すべきトピックは、やはりIPv4アドレス在庫枯渇後の対応です。

これに関わる提案としては、「RIPE NCCでのIPv4在庫の分配方法」や「返却されたアドレスの世界的な管理・再分配方法」が挙げられます。そして、在庫枯渇後は重要性が増すと考えられている、アドレス資源の利用権利を担保する仕組みとしてのRPKI（Resource PKI）の提供について、RIPE NCCでの検討状況も紹介されていました。

また、ドイツ国防省による省内のネットワークにおける他に類を見ないアドレス利用の事例紹介も行われ、そのような情報提供を公式のミーティングで堂々と発表していることも含めて新鮮でした。

RPKIの検討については前号でご紹介しましたので、ここではIPv4アドレスの在庫枯渇に向けたポリシー提案について、どのような議論が行われていたのかを簡単にご報告します。

◆IPv4アドレスの在庫枯渇に向けたポリシー提案

今回議論された主な提案の目的は、以下の二つに整理することができます。

1.RIPE NCCの最後のIPv4アドレス在庫をどう分配していくかを定義したもの:2008-06、2009-04、2009-03

■ 会場のCorinthia Hotel

2.返却されたIPv4アドレスを、世界的にどう管理・再分配していくかを定義したもの:2009-01

個々の提案の概要は、以下の通りです。

◎RIPE地域における最後の/8の分配方法について

［提案］2008-06：Use of Final/8
2009-04：IPv4 Allocation and Assignments to Facilitate IPv6 Deployment

2008-06
- RIPE NCCの最後の/8在庫は1組織につき/22（1,024アドレス）の分配に限定し、同じ/8空間の中から/16を予期せぬ用途のために確保することを提案しています。
- 内容、提案者ともに、2009年2月からAPNICで施行したポリシーと同じです。

2009-04
- 2008-06の代案として同じ/8の空間を、IPv6の実装を前提としたネットワークに分配先を限定することにより、IPv6移行へのインセンティブとするものです。ARIN地域では、これと同じ趣旨の提案が施行されています。

どちらの提案もIPv4在庫枯渇後の状況に備えて、RIPE NCCにおける最後の/8アドレス在庫を別途リザーブし、この空間からのアドレスの分配はこれまでの基準と分けて定義していることが共通しています。

Policy WGセッションでの議論では、IPv4アドレス在庫枯渇まで時間的な制約もあることから、多くの要素は盛り込まず、最低限必要な対応と考えられる2008-06をベースに、継続議論を行うことになりました。この提案が施行された場合は、新規・既存の事業者ともに、/22の分配を必ず受けることができるため、一定数のIPv4アドレスの分配が最後に保障されることを前提として、在庫枯渇後の状況に備えることが可能となります。

◎在庫枯渇時期に応じた“公平”なIPv4アドレスの分配について

［提案］2009-03：Run Out Fairly

これは前項で紹介した提案と若干アプローチが異なり、より多くの申請者に機会を与えるために、枯渇時期が近づくにつれ、段階的に分配量を縮小していく（例:2010年7月:9ヶ月分の需要を分配→2011年1月:6ヶ月分の需要を分配等）というものです。大きなISPが一度に大量のアドレス申請を行うことにより、その後に申請を行ったISPが分配を受けられなくなる事態を避けることが、提案者の目的です。

会場では分配量を調整するタイミングの定義について、参加者の一人からは懸念が表明されましたが、基本的には好意的に受け止められました。現行の提案を施行する方向で、継続議論を行うことになっています。

◎IPv4在庫枯渇に向けたIANAからRIRへのIPv4割り振りに関するグローバルポリシー

［提案］2009-01：Global Policy for the allocation of IPv4 blocks to RIRs

現在、RIRへ返却されたIPv4アドレスは各RIR単位で在庫管理・再分配が行われています。しかし、アドレスの返却が特定のRIRに集中し、IANA在庫枯渇後に再分配できるアドレスが、RIR地域によって偏ることも想定されます。

そこで、この提案では返却されたアドレスを、IANAが世界共通の在庫として管理・再分配を行うことを定義しています。施行にあたっては、全RIRフォーラムにおけるコンセンサス（提案への賛同）とICANN理事による承認が必要となり、現在はAfriNIC、APNIC、LACNICの3 RIRフォーラムにてコンセンサスが得られています。

Policy WGセッションでは、ARIN地域ではIANAへの返却を必須ではなく「任意」に変更して提案されており、本提案の有効性が薄れること、また、全RIRに対して共通に適用されるグローバルポリシーとして機能しないことが問題提起されていました。

結論としては、参加者からARINの対応について懸念が表明されていたものの、基本的には他のRIRにおける対応であるため、RIPEのアドレスフォーラムとしてはARINでの結論を待った上で、議論を再開することになりました。

■ RIPE NCCの新サービスNetSenceを紹介するパンフレット

◆その他の特筆すべき提案

アジア太平洋地域のAPNICフォーラムとも共通するテーマを取り扱った提案としては、以下2点がありました。

2009-06 Routing Requirements

・本提案により、RIPE地域においては、IPv6初回割り振り申請時に割り振りを受けたアドレスに対する、経路集約を求める要件が撤廃され※1、ミーティング期間中の10月8日に施行されました。

・ポリシーの要件とはしないものの、経路集約は促進するため、IPv6における経路広告に関するガイドラインをどう文書化していくかについて、ルーティングWGにて別途議論が行われました。

・APNIC28（2009年8月25日～28日）ではこれと逆行し、初回に加え、追加割り振り申請時にも経路集約を求める提案が行われましたが、支持されませんでした（詳しくはP.32からの「APNIC28ミーティング報告」をご覧ください）。今後は、RIPEと同じ対応を行う方向で検討する可能性が濃厚です。

2008-07:Ensuring Efficient Use of Historical IPv4 Resources

・追加割り振り申請時に、申請者が分配を受けている歴史的PIアドレスも含めて、分配済みアドレスの効率的な利用の確認を行うとする提案です。

・RIPEでは一部要件見直しの上、継続議論となりました。APNICでは2009年2月より施行されています。

■ 会場周辺のリスボン市街の様子

※1 IPv6アドレスポリシーではIPv6アドレス初回申請時の要件の一つとして、割り振りを受けたIPv6アドレスの経路広告は単一に集成して行うことを求めています（例：/32の割り振りを受けた場合は/32で経路広告を行い、複数の/36等に分割しない）。RIPE地域では、アドレスポリシーで経路広告を定義することは適切ではないとして撤廃されました。

◆今後の議論の動向を知りたい方は

RIPEのポリシーフォーラムでは、IETFに比較的近いポリシー決定プロセスが採用されており、提案に対してミーティングで議論は行いますが、決議はとらず、メーリングリストでの議論も踏まえて、WGのチェアが施行の判断を行います。

今後のRIPE地域におけるポリシー提案の動向が気になる方は、“address-policy-wg@ripe.net”に下記URLよりご登録ください。提案の議論や施行の発表を追うことができます。

□address-policy-wg MLへの登録サイト
http://www.ripe.net/mailman/listinfo/address-policy-wg#subscribers

◆参考

第59回RIPEミーティング　アジェンダ・発表資料
http://www.ripe.net/ripe/meetings/ripe-59/agendas.php?wg=address-policy

第59回RIPEミーティング　トランスクリプト・映像（Policy WGは「Wednesday」および「Thursday」に開催）
http://www.ripe.net/ripe/meetings/ripe-59/archives.php

RIPE地域にて議論中のポリシー提案一覧
http://www.ripe.net/ripe/policies/proposals/

（JPNIC IP事業部 奥谷泉）

2009.9.11▶9.12

ICANNと米国政府との新しい関係

■ ～「責務の確認（AoC）」の締結～

2009年6月15日発行のJPNIC News & Views vol.646※1にて、インターネットの資源管理の頂点に立つICANNと米国政府の関係について述べ、両者が締結し終了を間近に控えたJPA（Joint Project Agreement「共同プロジェクト合意」の意）※2について解説しました。その際、「JPA満了後の枠組みや、ICANNと米国政府の関係がどのようになるのか興味深い」と記しましたが、2009年10月1日に、JPAに代わる「責務の確認（Affirmation of Commitments; AoC）」と呼ばれる新しい文書が発効しました。本稿では、このAoCの解説と、これまでの背景についてお伝えします。

◆背景

今回、AoCの締結に至った背景は、AoCの前身であるJPA、さらにその前身となるMoU（Memorandum of Understanding）※3の締結にまで遡れます。ICANNと米国商務省（Department of Commerce; DoC）との間でのMoUの締結は、「ドメイン名の一元的管理を含むDNSの管理権限は米国政府が持っている」とする米国政府の主張に基づいて、1998年11月に行われました。この主張はいわゆるホワイトペーパー※4の中で主張されたものですが、同文書は「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、ICANNが設立された際にMoUを結び、DNSの管理をICANNに委託することになりました。MoUはその後何回か改訂された後、3年の期限付きであるJPAとなりました。

JPA終了が近づいた2009年5月、NTIAはJPAに関して意見募集を行いました。また、同時期に米国議会もこの問題に興味を示し、公聴会を開いてICANNおよびNTIAより参考人を招致しました。これらの動きを背景に、NTIAとICANNとの間でJPA終了後の取り決めについて交渉がなされたと思われます。

ICANNがWebページで公開している内容によりますと、2009年9月11日から12日にかけて理事合宿を行っています。正式な理事会ではないため議事録は公開されていませんが、主な議題を列挙している中にAoCが含まれています。そして、AoCがICANN理事会で正式に承認されたのは、JPA終了期限ぎりぎりの2009年9月30日となっています。

◆AoCとは

AoCとは、DoCとICANNとが、それぞれが果たすべき責務を記載した文書です。その前身であるJPAが2009年9月30日に終了したのに伴い、同日DoCの一機関である米国商務省電気通信情報局（National Telecommunications and Information Administration; NTIA）およびICANNがそれぞれ公開し、翌10月1日より発効しました。

AoCに書かれている責務は多岐にわたりますが、ICANNに関する主なものは次の通りです。

a）公益のための、DNSのグローバルな技術的調整
b）DNSのセキュリティ、安定性、回復性の維持
c）競争、消費者の信頼、DNS市場での消費者による選択の自由の促進
d）DNSの技術的調整における国際的な参画の促進

これに対し、DoCの責務としては主に次のものを挙げています。

e）グローバルなインターネットユーザーのメリットを代表するDNSの技術的調整において、マルチステークホルダー、民間セクターが率いる、かつボトムアップなポリシー策定モデルへの関与

前身であるJPAとAoCを比べた場合の主な違いは、以下の4点となります。

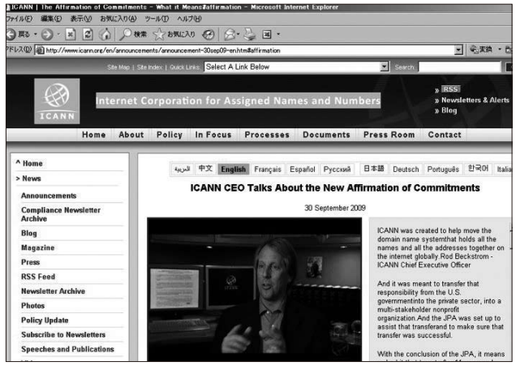
1）期限が定められていない
2）これまで定期的にICANNからDoCに報告書を提出して評価を受けていた仕組みから、ICANNの自主性を尊重した評価の仕組み※5に移行する
3）米国政府のICANNに対する関与は、米国以外の各国政府同様にGAC（Governmental Advisory Committee:政府諮問委員会）※6を通じて行う
4）AoCは、米国政府もしくはICANNのどちらか一方の当事者が、意思を表明することにより、いつでも終了となる

これに対し、JPAの頃から一貫して変わらない点は、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ことです。

◆AoCが示すもの

では、JPAからAoCになったことで、DNSの管理運営が民間主導となったと言えるのでしょうか。これについては、前述したAoCとJPAの相違点の4番目である「AoCは、米国政府もしくはICANNのどちらか一方の当事者が意思を表明することにより、いつでも終了となる」という条項により、必ずしもそうとは言えないと解釈することが可能です。つまり、AoCが終了すればICANNはDNSの管理権限を持たなくなるため、DoCはICANNに対してAoCの終了通告を行うことで、引き続きいざというときの関与を可能としているということです。ただし、通常時における米国政府の関与は、他国の政府と等しいGAC経由の関与とされているため、この点だけが注目されて、ICANNが米国政府の管理下より独立したという見方がされているようです。

AoCの締結後に、ICANNに寄せられたコメントは公開されており、米国の連邦議員からのものも含め、歓迎する内容のものばかりです。米国政府が前述の「相違点4）」という担保を残している点では、JPAとそれほど変わらないのでは、という見方も可能なAoCですが、ICANNが米国政府の管理から独立することを望んでいたと思われる国々も歓迎している理由は、上記、相違点4）が発動されない限りにおいて、全ての政府はGACを通じてICANNに関与することになっており、同等の権利を有するからです。今後、ICANNの評価委員会がスムーズに立ち上がり、ICANNの評価内容が肯定的なものとなれば、AoCおよびそれに付随した体制が成功したということになるのかもしれません。



■「ICANNのCEOが語る新しい『責務の確認』」が掲載されているICANNのWebサイト

■ ICANNと米国商務省間のDNS管理に関する「責務の確認」契約締結に対するJPNICのコメント

◆参考

Affirmation of Commitments（原文）
http://www.icann.org/en/announcements/announcement-30sep09-en.htm#affirmation

（JPNIC インターネット推進部 山崎信）

※1 JPNIC News & Views vol.646
ICANNと米国政府の関係 ～JPA終了に向けて～
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol646.html

※2 JPA（Joint Project Agreement:共同プロジェクト合意）
米国商務省（DoC, Department of Commerce）とICANNの間で、2006年9月に結ばれた覚書のことを指します。1998年11月にICANNと米国商務省との間の覚書（ICANN/DoC MoU）として締結されて以来、明確にJPAと称されるようになった2006年9月に至るまで6回更新され、2009年9月30日に期限満了を迎えました。

※3 ICANN/DoC MoU（Memorandum of Understanding）
ICANNと米国商務省（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。1998年11月25日に締結され、2006年9月30日まで延長された後、JPAへと引き継がれました。

※4 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。

※5 AoCでのICANN評価の仕組み
AoCでは、GAC議長、ICANN理事長または事務総長、DoC情報通信担当次官補、ICANNの各諮問委員会（Advisory Committee; AC）および各支持組織（Supporting Organization; SO）の代表、および独立した専門家からなる評価委員会を設置する、としています。

※6 GAC（Governmental Advisory Committee:政府諮問委員会）
ICANNの諮問委員会の一つで、各国政府の代表などで構成されています。各国政府の立場からICANNの理事会に対して助言を行っています。

2009.10.25▶10.30

ICANNソウル会議報告

2009年10月25日（日）から30日（金）まで、韓国のソウルで第36回ICANN会議が開催されました。今回の会議で最も大きく取り上げられたのはIDN ccTLDですが、新gTLDに関する議論も盛りだくさんでした。

◆IDN ccTLD導入に関する進捗

前回シドニー会議では、2009年5月31日に公開された“Draft Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス実装計画案）”の第3版※1に従って議論されましたが、これを反映した“Proposed Final Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス最終実装計画案）（以下Prop Final）”※2が9月30日に公開され、これが理事会審議に掛かることになりました。2日目の10月26日（月）に行われたIDN ccTLD Fast Track Workshopでは、このProp Finalの説明がなされました。バリアント（異体字）やコミュニティサポートなどに関する質問が出ましたが、Prop Finalの大枠を左右する議論はありませんでした。

同日夕刻のレセプションは“IDN Reception”と名付けられ、TLDにおけるIDNの導入という大きな節目に際して、関係者の労をねぎらうような趣向で、TLDに限らずIDNの標準化、サービス開始に関与した関係者が壇上で挨拶しました。

Prop Finalは、最終日の10月30日（金）に開かれた理事会の議案に上がり、無事承認されました。この承認によって、Prop Finalでの記述通りに、2009年11月16日からFast Trackの申請受け付けが開始されることが正式に決定しました。この議決は、歴史的なものであるとして、理事会の聴衆からスタンディングオベーションによって迎え入れられ、また、事務総長Rod Beckstrom氏は壇上からリアルタイムで、この議決をTwitterでも全世界に向けて伝えていました。その後、11月16日から予定通りIDN ccTLDの登録受け付けが開始され、中国などいくつかの国から申請が行われています。

◆新gTLD導入に関する進捗

新gTLDに関しては、ICANN会議以外にもコンサルテーションセッションを開催しながら検討が進められた結果、ソウル会議の直前である10月2日に、“Draft Applicant Guidebook（ドラフト版申請ガイドブック）”の第3版（以下DAGv3）※3が発表されました。ソウル会議では、新gTLDに関する総括的セッションである“New gTLD Program Overview”以外に、商標保護やレジストリ・レジストラ分割など、関連するテーマ毎に分けられたセッションが複数開催されました。

商標保護に関するセッション“Trademark Protection and new gTLDs”においては、商標保護に関するメカニズム - トレードマーク・クリアリングハウス（IPクリアリングハウスから改称）、URS（Uniform Rapid Suspension）、PDDRP（PostDelegation Dispute Resolution Process）に関して、DAGv3において変更された点と、議論中のポイントが提示されました。

「レジストリ・レジストラ分離」のセッションでは、理事会議長であるPeter Dengate Thresh氏のモデレーションの下、分離支持派と分離反対派の計2名のパネリストが壇上で発表する形で、ディスカッションが展開されました。セッションの最後には参加者の発声によって、双方に対する支持が測られ、若干ながら分離支持に対する賛

■ 会場となったロッテホテル

成が多かったものの、際立った違いはありませんでした。

また、理事会の席上、AOB（Any Other Business：「その他」）の部で「新gTLDに対する関心表明（Expression of Interest）を行った場合に起こり得る影響を調査し、理事会における検討計画案を、リスク分析を伴う実施オプションとともに12月の理事会で提示することを、ICANN事務局に指示する」という決議が承認されました。

新gTLDに関してこのような関心表明が議論となったのはこれが初めてですが、関心表明のプロセスが新gTLD追加のプログラムに付け加えられる見通しであることが、この決議で明らかになりました。また、ここで挙げた商標保護、レジストリ・レジストラ分離を含む六つのポイントなどが、継続議論のアイテムとして残されており、これらの準備が整って新gTLDが募集されるまでには、今しばらく時間が掛かるという印象を持ちました。

◆その他

前号の「ICANNシドニー会議報告[※4]」でも報告した、GNSOの組織改正はそのプロセスを終え、今回のソウル会議では、二院制の組織構造になってから初めての評議会が開催されました。これに加え、新たな事務総長Rod Beckstrom氏が2009年7月に就任して以降初のICANN会議でもあり、ICANNと米国商務省の間の覚書、JPA（Joint Project Agreement:共同プロジェクト合意）[※5]が満了し、AoC（Affirmation of Commitments: 責務の確認）[※6]が発効してからも初のICANN会議と、IDN ccTLD以外にも「初めて」尽くしのICANN会議となりました。

（JPNIC インターネット推進部 前村昌紀）

■ GNSO評議会の様子

■ 理事会でIDN ccTLD Fast Track Processの最終実装計画案が承認されると、会場ではスタンディングオベーションが起こりました

※1 “IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス実装計画案 第3版）”
http://www.icann.org/en/announcements/announcement-31may09-en.htm（英語）

※2 “Proposed Final Implementation Plan for the IDN ccTLD Fast Track Process（IDN ccTLD ファスト・トラック プロセス最終実装計画案）”
http://www.icann.org/en/announcements/announcement-2-30sep09-en.htm（英語）
http://www.icann.org/ja/announcements/announcement-2-30sep09-ja.htm（日本語）

※3 “Draft Applicant Guidebook（ドラフト版申請ガイドブック）”
http://www.icann.org/en/topics/new-gtlds/dag-en.htm

※4 JPNIC News & Views vol.654
ICANNシドニー会議報告
http://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol654.html

※5 JPA（Joint Project Agreement:共同プロジェクト合意）
米国商務省（DoC, Department of Commerce）とICANNの間で、2006年9月に結ばれた覚書のことを指します。1998年11月にICANNと米国商務省との間の覚書（ICANN/DoC MoU）として締結されて以来、明確にJPAと称されるようになった2006年9月に至るまで6回更新され、2009年9月30日に期限満了を迎えました。

※6 AoC（Affirmation of Commitments: 責務の確認）
インターネットの資源管理に関して米国商務省とICANN、それぞれが果たすべき責務について記載した文書です。前身の文書であるJPAが2009年9月30日に失効したことに伴い、同日公開され、翌10月1日より発効しました。詳しくはP.43「ICANNと米国政府との新しい関係 ～「責務の確認（AoC）」の締結～」をご覧ください。

2009.11.8▶11.13

第76回IETF報告

■ 全体会議報告

◆概要

山陽新幹線の改札口を出ると、正面に立っている看板「Welcome -76th IETF Meeting Hiroshima」の文字が目に入ってきました。ホテルに向かう途中のアーケードには、IETFミーティング開催の横断幕がかかっています。市内のこのような掲示は、私が参加したことのあるIETFミーティングでは見たことがありませんでした。IETFが日本の広島で開催されるという実感とともに、ホストであるWIDEプロジェクトの力の入れように驚き始めた開催前夜でした。

第76回IETFミーティングの開催概要は以下の通りです。

開催期間：2009年11月8日（日）～13日（金）
会　　場：ANAクラウンプラザホテル広島
参加登録者数：1,155名
参加国数：44ヶ国
参 加 費：635USD（早期割引料金）、785USD（通常料金）、200USD（一日料金）
ホ ス ト：WIDEプロジェクト


■ Plenaryの様子

全体会議（Plenary）での発表によると、日本からの参加人数は363名と最も多く、全体の34%を占めていました。米国は304名で27%、中国は99名で9%、続いてフランス4%、韓国4%という内訳でした（2009年11月10日時点）。

初日の11月8日（日）はチュートリアルとレセプションが開かれ、2日目から最終日にかけて、各WGのミーティングとBoFが開かれました。

◆Operations and Administration Plenary概要

Operations and Administration Plenaryは、IETFの運営などに関する全体会議です。4日目の11月11日（水）16:30から3時間程行われました。ホストであるWIDEプロジェクトのプレゼンテーションと、新設されたItojun Service Awardの発表、NOCレポート、IETFチェアの活動報告などが行われました。

○WIDEプロジェクトのホストプレゼンテーション

WIDEプロジェクトのプレゼンテーションでは、WIDEプロジェクト代表で、JPNICの理事でもある村井純氏によって広島市内の広告や、第76回IETFのロゴやTシャツのデザイン、RFID（Radio Frequency Identification）の利用実験などについて説明が行われました。

会場のホテルが面している平和大通りでは、数多くのイルミネーションが飾られるイベント「ひろしまドリミネーション」が毎年行われていますが、今回はIETFの開催期間に合わせ、イベントの開始が例年よりも早められたとのことでした。また、ロゴとIETFで恒例となっているTシャツは、広島市立大学の及川久男教授によってデザインされたそうです。

RFIDは、以下の二つの実験で使われました。

- 発言者の情報表示システム

マイクの前に立って発言する際、マイクスタンドにかかっているRFIDリーダーにタグをかざすと、発言者の氏名などがスクリーンに表示されます。タグは、首から下げる名札入れに入っているため、人によってはマイクに近づくだけでタグが認識されます。議論中に発言者の名前を確認できる他、Jabberや議事メモの作成に役立っていました。

- E-bluesheet

ブルーシート（Bluesheet）とは、WGなどで参加者自身が記入する形式の参加者リストです。今回のIETFでは、ブルーシートに加えてRFIDリーダーが座席にまわってきました。タグをRFIDリーダーにかざすだけでよいため、紙に氏名やメールアドレスを記入するよりも楽になっています。

RFIDタグは、1,121名中、889名によって使用されました（2009年11月10日時点）。RFIDの利用実験で印象的だったのは、その運用とサポートです。RFIDタグは、ユーザーが登録しなければ有効にならないオプトインの形で配布され、また意図せずに他人に読み取られるのを防ぐ、“スキミングプロテクション”カードも一緒に配布されていました。会場にはヘルプデスクが設けられ、常時スタッフが対応できるようになっていました。

この他に、ソーシャルイベントの参加者向けに、「PASPY」と呼ばれるFelicaカードが配布されていました。PASPYは広島市内の交通機関で使えるだけでなく、平和記念資料館の入場などにも使うことができます。

■ 発言者のRFIDを読み取るためにマイクスタンドに設置されたRFIDリーダー

○Itojun Service Award

Itojun Service Awardは、KAMEの実装などで知られる萩野純一郎氏の功績をたたえ、萩野氏の家族と有志の寄付を基にして設置された賞です。この賞は、インターネットに関わる開発や運用などの技術的貢献を行った人に贈られます。

第1回のItojun Service Awardは、Google社のLorenzo Colitti氏とErik Kline氏に贈られました。両氏は、GoogleのWebサービスを、IPv6を使って利用できるように尽力したことが認められ、受賞に至りました。

□The KAME project
http://www.kame.net/

□Internet Society（ISOC）- Itojun Service Award
http://www.isoc.org/itojun/

○NOCレポート

NOCレポートは、IETFのために設置されたネットワークに関する、ネットワークオペレーションチームからの報告です。WIDEプロジェクトのメンバーでもある東京大学の加藤朗氏によって行われました。概要は以下の通りです。

- ネットワークのデザイン

“Simple but robust”という原則の下、どのネットワークでもIPv4とIPv6が使えるようになっていました。


■ 萩野氏のご家族と、Itojun Service Awardの最初の受賞者になったGoogle社のLorenzo Colitti氏とErik Kline氏（右端の二人）

会場のみならず、会場以外の五つのホテルでもIETFのネットワークが提供されました。一般の宿泊客も使えるようになっており、ボトルネックになると考えられるNATが介在しない、高速なネットワークが提供されました。

- ネットワーク回線

会場のANAクラウンプラザホテル広島は1Gbps、他のホテルは100MbpsでNTT西日本の回線に接続され、その先はSINET、JGN2+、NSPIXP3、JPNAPに各々1Gbpsで接続されました。主にAlaxala社とCisco社の機器が使われました。NSPIXP3とJPNAPから先では、NTTコミュニケーションズ、KDDI、IIJの3社によって接続サービスが提供されました。

- 無線LAN

これまでのIETFと同様に複数の規格で提供されました。クライアント数を以下に示します（2009年11月11日時点）。最大で854クライアントが接続しました。

802.11g: 324　802.11n: 255
802.11a: 149　802.11b: 10

会場1階のレストランでは、ガラス張りのワインセラーの中に基地局が設置され、カバー範囲を広げるとともに、NOCチームのユーモアが現れていました。

- IPv6

総トラフィックのうち約7%がIPv6でした。これにはGoogleのDNSサーバで、WebサーバのAAAAレコードが返されるような設定変更が会期中に行われたことが影響したようです。

今回のネットワークは、特に障害が発生せず大変安定していたことから、IETF参加者のメーリングリストでNOCチームに感謝する旨のメールが数多く飛び交っていました。

○IETFチェア報告など

IETFチェアのRuss Housley氏からは、RFCの公開状況などについて報告がありました。

- RFCの作成状況

前回（IETF-75）以降、RFCは104公開されました。合計で約3,077ページあるそうです。

- Code Sprint

ミーティングの前日に、IETFのWebページなどのプログラミングを行うセッション“Code Sprint”が今回も行われました。今回は、IETFのコンテンツ管理に使われている、Djangoの1.1へのバージョンアップが行われました。

IAOC（IETF Administrative Oversight Committee）とIAD（IETF Administrative Director）のレポートは、Bob Hinden氏とRay Pelletir氏によって行われました。

- 2009年度のIETF運営状況

今のところ参加者数は計画の範囲内ではあるものの、当初予算に比べて収入が減りました。一方、会議費における飲料費の低減化を図るなどし、支出も減りました。ISOCからの追加補助は不要である見込みです。

- 2010年度の予算

2010年度の予算が承認されました。IETFミーティングの参加費は635ドルに据え置かれる予定です。


■ ReceptionでスピーチをするWIDEプロジェクト代表の村井純氏

◆Technical Plenary概要

Technical Plenaryは、ミーティング参加者全体で技術的な議論を行う全体会議（Plenary）です。11月12日（木）の16:30から3時間ほど行われました。

- IRTF（Internet Research Task Force） Chair's report

二つのResearch Group（RG）の紹介が行われました。Anti-Spam Research Group（ASRG）は、スパム対策のRGで、現在はブラックリスト管理に関するドラフトの作成が行われています。Scalable, Adaptive Multicast Research Group（SAMRG）は、複数の方式のマルチキャストに関するRGで、“ハイブリッドマルチキャスト”と呼ばれる複数の方式が組み合わされたマルチキャストの、テストベッドの構築が行われています。

- IAB（Internet Architecture Board） Chair's report

逆引きに使われるTLDである「.ARPA」における署名レコードの提供が計画されています。2009年第4四半期に一時的なセットアップが行われ、2010年第2四半期にルートゾーンを管理するためのアーキテクチャへの組み込みが行われるスケジュールとなっています。

○ドメイン名や識別子の国際化に関する議論

今回のTechnical Plenaryにおける議論のテーマは、ドメイン名や識別子の国際化（Internationalization in Names and Other Identifiers）です。はじめに、アルファベット以外の文字列がドメイン名やパス名で使われるケースを紹介し、文字列同士の比較やマッピングなどの処理が持つ複雑さが説明されました。

IABでは、ドメイン名と文字列のエンコーディングに関する考察の結果をドキュメントにまとめる作業が行われています。

会場では、複数のコード体系がある中でbackward compatibility（後方互換性）を保つにはどうすればいいのかといった疑問が投げかけられたり、誤認しやすいURLを使ったフィッシングを防ぐためにどうすればいいのか、といった議論が行われました。

□IAB Thoughts on Encodings for Internationalized Domain Names
http://tools.ietf.org/html/draft-iab-idn-encoding-01

◆IETFミーティングに合わせて行われたイベント

今回のIETFでは、会期中以下のイベントがありました。いずれもランチの時間を使ったセッションで、会場のホテルで行われました。

- ISOC Briefing Panel: “Internet Bandwidth Growth: Dealing with Reality” - 11月10日（火）

近年のさらなる広帯域化の影響と広帯域アプリケーションの影響などについて、トラフィックの統計を取っている研究者などによるパネルディスカッションが行われました。

- Challenges to the Future in WIDE Project - 11月12日（木）

ホストであるWIDEプロジェクトによる最新動向の紹介が行われました。同プロジェクトの村井純氏、江崎浩氏に加え、パナソニック電工株式会社と日本放送協会のスピーカーによる、さまざまなIPの適用場面について発表が行われました。

◆今回のIETFについて

■「Chanllenges to the Future in WIDE Project（2009年11月12日）」の案内板

今回、ミーティング参加者用のMLのやりとりが、とても活発でした。通常は“本MLは稼動していますか?”といった質問が投げられることがあるほど静かなMLですが、今回は、広島への行き方に始まり、市内のサッカー/フットサル場や、空手道場がどこにあるかといった質問、さらに広島という地名の由来、RFIDの活用法など、さまざまな情報交換に使われました。質問には、WIDEプロジェクトのメンバーが、一つ一つに丁寧に対応していたのが印象的でした。

◇　　◇　　◇

次回の第77回IETFは、2010年3月21日～26日、米国のアナハイムで開催される予定です。

（JPNIC 技術部/インターネット推進部 木村泰司）

■ DNS関連WG報告

◆dnsext WG

今回のdnsext WG会合では、TCPによるDNS問い合わせに関する話題が多くとりあげられました。これは、DNSSECの導入によりクエリサイズが大きくなることを解決する方法としての、TCPクエリの利用を想定した議論となっています。

draft-ietf-dnsext-dns-tcp-requirementsの発表では、RFC1123においてTCPによるDNSクエリ応答のサポートがSHOULDと明記されており、それをMUSTに変える必要があるのではないかと提案がありました。またEDNS0といった提案もあり、いまだUDPによるDNSクエリが一般的ではあるが、DNS実装としてはTCPを必須項目にするべきだ、と提案がなされました。しかしこの提案に対して、CPEといった小型の機器に内蔵されるDNS Proxy等はTCPをサポートしていないものが多く、EDNS0とTCPどちらもまだ、必ず機能するというものではないため、対策が必要であるとの認識がなされました。

次に、“TCP for DNS security consideration”という発表が行われました。これは、TCPに発見されているセキュリティ問題（draft-ietf-tcpm-tcp-security）に対して、DNSとしてどう対応すべきかという提案です。HTTP Keep Aliveと同じように、永続的にDNSサーバ間でTCPコネクションを保つような仕組みが必要になるかもしれないので、DNSクライアントは積極的にTCP active closeを行うべきだという提案がなされました。DNSクエリにTCPが本格導入されるにあたっての注意点を提起する発表となりました。


■ 会場の様子

また、APNICのGeoff Huston氏から、“An Experiment in Implementing a Stateless TCP DNS Server”という発表が行われました。これはDNSクエリ応答のために簡略化されたTCPを用いるという提案です。もっとも、本人はこの提案を“Really a Bad Idea!”と言っており、本気で提案したわけではないのですが、思いついて実験してみたらできてしまったので紹介した、というもののようです。ユーザーランドでTCPによるDNSクエリを受け取って、DNSサーバに仲介するというDNS Proxyモデルです。

以上のような、TCPによるDNSクエリに関する話題が会合の中心となりました。DNSSECの導入をにらんだ、現実的な提案が行われていたように思われます。

◆dnsop WG

dnsop WG会合では、DNSSEC鍵更新に関する話題、ならびにDNSSECのトラストアンカーに関する話題に多くの時間が割かれました。

まずdraft-morris-dnsop-dnssec-key-timingについての発表が行われ、DNSSECのZSK、KSKの鍵更新を行うタイミングに関して提案がなされました。発表後の質疑応答では、署名アルゴリズムの導入や削除に関する記述がもっと必要との提案がありました。ゾーンの署名サービスを提供しているOpenDNSSECも、この提案に基づいて鍵更新を行っているそうです。引き続き議論が行われます。

また、draft-ljunggren-dps-frameworkに関する発表も行われました。これは、ドメイン名レジストリに対して.seにおけるDNSSEC署名の経験を踏まえた提案を行っている文章です。署名されたゾーンの生成や更新、鍵の更新時における処理等を提案した文章となっています。

他には、CNNICの方がIDN TLDに関する発表を行いました。日本よりも漢字のバラエティが多い中国では、“bank.中国”と“bank.中國”の扱いをどうするのか、等大きな議論になっているようです。

◆Root DNSSEC Presentation with Q&A

IETF76において、公式なBoFではないのですが、オープンな会合として“Root DNSSEC Presentation with Q&A”という会合が開催されました。これは、Root DNSオペレーターやレジストリ、ICANNの有志からなるRoot DNSSECデザインチームによる、Rootゾーンの署名計画の報告と質疑応答が行われた会合です。まずRootゾーンの署名時期や、鍵管理の仕組みについて報告がありました。そして鍵の所有者を明確に定義し、VeriSign社が行う

ゾーン署名のシステム説明とその流れが報告されました。その後の質疑応答では、鍵が盗まれた際の緊急処理やゾーンの緊急再署名に関する話題を中心として、活発な議論が行われました。

署名されたRootゾーンの提供は、2010年7月までに行われる予定となっており、DNSSECの導入が急速に始まろうとしている感がうかがえました。

（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）

■ IPv6関連WG報告

本稿では、第76回IETFミーティングの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WGでの話題を中心に紹介します。

◆6man WG（IPv6 Maintenance WG）

6manワーキンググループは、IPv6プロトコルのマイナーなメンテナンスを実施しているWGです。今回のミーティングは、11月10日（火）の午前最初のコマにて、開催されました。

会議は、前回と同様、チェアよりのミーティングの議題確認および、WGで取り組み中である文書のステータスについての報告から始まりました。現在、6man WGにて正式に取り組み中の文書（WG document）は、

・フラグメント重複問題（IESG※1 review中）
・ノード要求仕様（メーリングリストで議論中、アジェンダからは落ちました）
・アドレス選択（今回、議論されました）
・IPv6推奨アドレス表記（今回、議論されました）
・IPv6サブネットモデル（ワーキンググループラストコール中:ラストコールは最終合意のこと。以下、Working Group Last Callを略してWGLCと表記。）※2009年11月14日に終了
・経路制御ヘッダ（WGドラフト化）

の六つとなっています。

今回のミーティングの議題は、

・IPv6アドレスのテキスト表記方法（draft-ietf-6man-text-addr-representation）
・6LoWPANでの近隣探索（draft-ietf-6lowpan-nd）
・アドレス選択に関する次へのステップ
  - アドレス選択ポリシー間の矛盾解決（draft-arifumi-6man-addr-select-conflict）
  - アドレス選択デザインチーム議論報告（draft-ietf-6man-addr-select-considerations）
・近隣探索キャッシュの更新について（draft-kitamura-ipv6-neighbor-cache-update）
・P2Pリンクでの/127プリフィクス長の利用（draft-kohno-ipv6-prefixlen-p2p）
・ノード要求仕様文書に関する議論（draft-ietf-6man-node-req-bis）
・IPv6のUDPチェックサムついて（draft-fairhurst-tsvwg-6man-udpzero）

となっています（上記の通り、ノード要求仕様については簡単なコメントのみで議論されませんでした）。このうち、いくつかについて簡単に紹介します。

・IPv6アドレスのテキスト表記方法

前回のミーティング、およびその後のメーリングリスト（ML）での議論で、6man WGとして取り組んでいくことに合意し、今回のミーティングの前にWGLCが終わっていました。ミーティングでは、IETF75からの変更点について簡単に解説がありました。会場からのコメントも、文章表現についての簡単なもので、RFC化に向けて進めることになっています。

・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）

今回も引き続き、IPv6サイト/ホストがアドレスプリフィクスを複数持った場合の、アドレス選択のあり方の検討状況報告がありました。前回は、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の、コンフリクトの解消（ポリシーのマージ）についての提案・議論がありましたが、今回は、主にポリシーを配布するプロトコルについての議論がありました。プロトコルとして、ルータ広告、DHCPv6、もしくは経路制御プロトコルのオプションを利用する場合の利点、欠点の検討紹介について、どれか一つに決めるべきである、DHCPv6でも情報をアップデートは可能、といったコメントがありました（その後、MLでも手法についての議論が延々と続いています）。提案文書について、より多くのコメントが欲しい、とのことです。

・P2Pリンクでの/127プリフィクス長の利用

現在、アドレスのプリフィクス長に/127を利用することはIPv6の仕様的に問題があるとされており、/127のプリフィクスを使用することの問題点を記述した文書（RFC3627）も出版されています。これに対して、特にオペレーションの観点から、P2Pリンクにて/127より短いプリフィクスを利用することの問題点を提示し、P2Pリンクでの/127の利用を明示的に可能とすることについての提案です。リンクローカルアドレスに関する問題等仕様上の注意点が指摘はされましたが、賛成も多く、今後WGとして継続して議論することになると思われます。

・IPv6のUDPチェックサムついて

ここしばらくIETFで議論されている、UDPにおけるチェックサム計算をしなくてもよいことにする提案に関する議論です。IPv6では、IPv6ヘッダにチェックサムがないため、IPv4と違ってUDPにおけるチェックサムの計算を必須としています。しかしながら、UDPを利用したトンネルの際に、トンネルの中を通るパケットレベルで相当のチェックをしている場合には、外側のUDPでのチェックサム計算が必要ない、途中のルータでトンネルリンクにパケットをフォワードする際に、UDPチェックサムを計算するコストが高くなってしまう、などが問題とされていました。今回は、計算コストに関する議論、チェックサムを廃止した場合の影響が検討され、ミーティング中の議論では、UDPのチェックサム処理への変更は実施しない方向となっています。

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

□第76回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/76/agenda/6man.html

◆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、11月10日（火）、11月12日（木）午後最初の、合計2コマにて議論が実施されています。今回も、数々の新提案があり、内容も多岐にわたっていました。

議論内容は以下の通りです。

11月10日（火）
・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）（アジェンダから消されました）
・IPv6 CPEに関する高機能セキュリティ（draft-vyncke-advanced-ipv6-security）
・BitTorrentネットワークでのIPv6トラフィック測定（draft-defeche-ipv6-traffic-in-p2p-networks）
・IPv6 CPEルータ推奨機能（draft-ietf-v6ops-ipv6-cpe-router）
・IPv6 CPEルータ拡張推奨機能（draft-wbeebee-v6ops-ipv6-cpe-router-bis）
・IPv4/IPv6共存フレームワーク（PET）（draft-cui-softwire-pet）
・PETでのIPv6からIPv4への通信（draft-cui-softwire-pet64）
・Internet Exchange（IXP）でのIPv6ディプロイメント（draft-ietf-v6ops-v6inixp）

11月12日（木）
・ICPに対するISPのIPv6移行サービスのプロビジョンに関する推奨（draft-qin-v6ops-icp-transition）
・IPv6ディプロイメントに関する新サービスプロバイダシナリオ（draft-carpenter-v6ops-isp-scenarios）
・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）
・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）
・Teredoの拡張（draft-thaler-v6ops-teredo-extensions）
・IPv4サーバにアクセスするIPv6アプリケーションの構築（draft-wing-v6ops-v6app-v4server）

■ 会場となったANAクラウンプラザホテル広島

いくつかの内容について、簡単に紹介します。

・IPv6 CPEに関する高機能セキュリティ

IPv6 CPEに関する高機能セキュリティは、現在議論中である「簡易セキュリティ推奨機能」（当初、議題には挙がっていましたが、議論はされませんでした）に対する、より高度なセキュリティモデルとしての提案です。IPv6ネットワークは、IPv4グローバルアドレスを内部にも使っている企業ネットワークと同等であり、セキュリティポリシーを考える際に、企業で利用しているポリシーが参考にできると考えて、七つのホームネットワーク用セキュリティポリシーを提案しています。特に、CPEデバイスを外部から動的にアップデートすることで、より強固なセキュリティを担保できるようにすることの必要性を強調していました。提案に対する賛成意見もありましたが、一方で、これはIPv6に特化したものであるのか、また、動的アップデートには標準等は必要ないため、IETFでなく、ブロードバンドフォーラム等で議論すべき内容ではないかとの反対意見もあり、提案に対する賛成、反対も含め、MLで継続議論となりました（火曜日のセッション終了後、継続議論されています）。

・IPv6 CPEルータ推奨機能、IPv6 CPEルータ拡張推奨機能

ここ数回のIETFで議論を続けている、IPv6対応のCPEルータが持つべき機能に関する提案です。今回から、検討事項が多い部分を拡張機能として別ドラフト（フェーズ2ドラフト）に切り出し、WANとLANの設定や、基本的なルータ機能、セキュリティ機能のみを基本部分として分離しています。基本部分のドラフトについては、MLにて意見を集め、それを反映後にWGLCを実施することとなりました。フェーズ2ドラフトの議論項目としては、マルチキャスト、DNS、プレフィックスの再委譲、IPv6移行機能、パケットフィルタ、QoS等が挙げられており、議論を継続していくこととなりました。

・Internet Exchange（IXP）でのIPv6ディプロイメント

IXPにおけるIPv6導入モデルは、3度目の発表となります。今回は、AMS-IXで導入されている、余計なARPトラフィックを減少させるための仕組みであるARPスポンジと同等の機能を、IPv6で実装する方法についての検討報告がありました。ARPスポンジは、多くのIXPで導入されているそうです。IPv6では、近隣探索プロトコルへの対応となりますが、アドレス長の違い、利用されていないアドレスが広大なことによる必要資源の増加等が問題となるようです。会場からは、この問題はIXPに特有でなく一般的な問題である、利用されていないアドレス対策が必要なら、/64より長いプリフィクスを使ったらどうか、といった質問がありました。コメントを反映して改版後、WGLCに進むことになりました。

・ICPに対するISPのIPv6移行サービスのプロビジョンに関する推奨

ICPをどのようにIPv6対応にしていくべきかをまとめようとしている提案です。利用できる移行機構（デュアルスタック、NAT64、IVI）を列挙し、利用できるツール等をまとめることを目的としています。会場からは、重要な観点であり、利用可能な技術を集めて情報共有をすることは意味がある、という意見や、重要ではあるが、多くのプロトコルは現状、標準化中であったり、どれがよい、と選べるものではなかったりと、まとめ方には注意が必要だ、といった意見がありました。今後デザインチームを作って、各機構、ツールの利点、欠点、ユースケース等を議論することになっています。

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

□第76回 IETF v6ops のアジェンダ
http://www.ietf.org/proceedings/76/agenda/v6ops

◆softwire WG（Softwires WG）

softwire WG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。現在扱っている方式は三つあります。一つはWGタイトルそのままのsoftwireと呼ばれる、IPv4 over IPv6またはIPv6over IPv4の汎用的なトンネル方式です。他にはDS-Lite（Dual Stack Lite）と呼ばれる、softwireのIPv4 over IPv6方式にCGN（Carrier Grade NAT）の機能を加味することで、IPv4アドレス在庫枯渇対策も含めたもの、そして6rd（IPv6 Rapid Deployment）と呼ばれる、IPv6アドレスの自動割り当ても含むIPv6 over IPv4トンネル方式があります。

これら三つの方式はいずれもまだ標準化が完了していませんが、それぞれが競合しているわけではなく、適用領域が異なっているとして、並行して標準化が進められています。

今回のセッションでは6rd、DS-Liteそれぞれについての標準化の進捗が報告され、いくつかの子細な部分に関する議論が行われました。6rdに関する議論では、Dave Thaler氏より6to4プロトコルで得られたNUD（Neighbor Unreachability Detection）の扱いや、routing loop問題への対策などの知見を盛り込むこと、また複数のBR（Border Router）を扱えるようにしてはどうか、といった提案がなされました。

DS-Lite方式の進捗に関しては、用語の変更などがあり、これまでCGNと呼ばれていたNAT装置を、AFTR（Address Family Translation Router）と呼ぶとの説明がありました。DS-Liteでも6rdと同様に、トンネル終端装置であるAFTR を二重化する話が議論され、6rdと違ってDS-LiteではAFTRがクライアント装置毎にstateを持つ必要があるため、より実現が困難であり、引き続き検討が必要であるということになりました。

その他、6rd over UDPといった、6rdに対する拡張の提案などがありましたが、根本的な仕様変更を伴う提案であったため、まずはベースとなる6rdの標準化が完了してから検討すべきであるとの結論に至りました。

6rdは今回の議論を反映した改訂版を作成し、すぐにでもWGLCに進む予定になっています。DS-Liteに関しては、AFTRの二重化に関する議論が終わればWGLCに進むものと思われます。

□第76回 IETF softwire WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/softwire.txt

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

◆aplusp BoF

IETFではIPv4アドレス在庫枯渇の対策として、ISP内でNAT装置（CGN）を用いる方法と、ユーザーにグローバルIPv4アドレスを割り当てつつ、利用できるポート番号の範囲を限定する、というA+P方式の二つが主に議論されてきました。今回のBoF（WG設立前のミーティング）では、このA+P方式全般というよりはさらにフォーカスをしぼって、DS-Liteのトンネル上でこのA+Pを行うという方式についての議論が行われました。

A+P方式の利点としては、ポート範囲が限定されてはいるものの、ユーザーに直接グローバルIPv4アドレスを配布できるため、NATに阻害されずに通信が可能であるということが挙げられます。欠点としては、ホストやルータに対する影響が大きいことなどが挙げられます。このDS-Liteのトンネル上でA+Pを行うことで、トンネル終端装置以外の装置（中継ルータなど）への影響を最小限に留める、といった狙いがあると思われます。

今回のBoFのゴールは、IETFがこの方式を扱うかどうかを決定すること、ということで、新たなWGを設立するか、既存のWGのアイテムとなるかといった選択肢が示されました。

セッションでは、まずA+Pの概要説明後、モバイル環境への適用についての提案、そしてA+Pに関する懸念事項、そしてフリーディスカッションの後に、今後の方針について決定する、という流れで検討が行われました。

フリーディスカッションでは多くの意見が交わされましたが、結局Dave Thaler氏によるA+P方式のTCP/IPプロトコルスタックへの微小な修正が、多大な影響をもたらすものであり、またそれはNATの導入とは質の異なる根本的な変化であるとの指摘に同意する人が多かったのか、WGの設立はおろか、本提案についてIETFで取り組むべきではないと感じる聴衆が大半を占めるに至りました。これらの意見はIESGにインプットされ、A+P提案が他のWGで扱われるか、などの決定がなされることになっています。

□第76回 IETF aplups BoFのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/aplusp.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。今回も、そのIPv6-IPv4変換の議論や、その他のNATに関する議論など、多数のトピックがありました。

まず、チェアからWGの状況についての報告があり、IPv6-IPv4変換に関する提案については、Interim Meeting（IETFミーティング期間以外での中間ミーティング）を経て、当初最重要であるとした問題ケースを解決する提案として、ほぼ仕様策定が完了したとの報告がありました。次の五つの提案について、2009年12月にはWGLCを行うとし、5人のレビュアーが必要であるということで、ボランティアを募りました。

- Address Format
  draft-ietf-behave-address-format-01
- Framework for IPv4/IPv6 Translation
  draft-ietf-behave-v6v4-framework-03
- IPv6/IPv4 Translation

draft-ietf-behave-v6v4-xlate-03
- Stateful IPv6/IPv4 Translation
draft-ietf-behave-v6v4-xlate-stateful-02
- DNS64
draft-ietf-behave-dns64-02

その後、これらのそれぞれの提案について、変更点の報告などが行われました。Address Formatの提案では、Well Known Prefixのフォーマットについての議論や、またTranslationの提案では、パケットのフラグメントの扱いに関する詳細議論が行われましたが、特に大きな変更が必要となるような意見は出ず、今後もInterim Meetingを行いながら迅速に標準化を進めていくということになりました。

また、これらの提案以外に、ホスト自身でIPv6-IPv4変換を行うといった提案や、A+Pの考え方をIPv4からIPv6への変換方式に組み込むことで、IPv6ホストにIPv4グローバルアドレスを付与するといった提案など、さまざまなIPv6-IPv4変換に関する変更や拡張の提案がなされました。しかしながら、これらの提案は、現在注力している上記の方式の標準化が終わってから着手するべきであるとか、また他のWGで進められている技術と同一目的であるのでそこで議論するべきである、という意見が多数となっていました。

IPv6-IPv4変換だけでなく、IPv4-IPv4変換の議論も行われ、CGN装置の信頼性向上のための冗長化の議論、また複数のユーザーで同一のIPv4アドレスを共有するという観点から問題点、対策をまとめた文書などの発表がありました。これらの議論も継続して進めることになっています。

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

□第76回 IETF behave WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/behave.html

（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 Internet Engineering Steering Group（IESG）
IETFの活動と標準化プロセスの、技術的な側面についての責任を担っているグループです。IESGのメンバーは、IETFの複数のWGで文書のレビューを行ったり、WGの方向性について助言を行っているArea Directorで構成されています。IESGはInternet-Draftの標準化プロセスを進めるかどうかを決定し、IESGによって承認されるとRFC番号が割り振られ、RFCとしてIETFのサーバで公開されます。

■ セキュリティ関連WG報告

第76回IETFは、日本の広島にて、2009年11月8日から13日まで開催されました。2002年横浜以来の7年ぶりとなる日本での開催であることから、全参加者1,155名中363名と、日本人が一番多い結果となりました。また、会場のあちこちで積極的に議論に参加しているNew Comer（初参加者）を多く見ることができました。

毎回IETFでは、セキュリティに関連したWG（今回は13セッション）が開催され、世界中からいろいろな背景を持った参加者によって議論されています。幅広い領域において、WG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セキュリティに関連したセッションのうち、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※1について、新規仕様の検討や実装のための検討を行うWGです。このミーティングは、11月11日（水）に開催され、参加者は20名程度でした。最初にチェアから、WG文書のステータスおよび今回のミーティングのアジェンダについて説明が行われました。

今回の会議は、FAST Negotiationに関する問題と、KDC（Key Distribution Center）のデータモデルにおけるEncryption typeについて技術的な議論を行うことを目的としており、それらについて会議の参加者たちが活発に発言していました。

前回の会議では、危殆化対策（暗号技術の世代交代）や新規アルゴリズムに関する議論が行われたので、今回の会議でも引き続き議論されることを期待していたのですが、それらについて議論されなかったので残念でした。

■ New comer's orientationで日本語のチュートリアルを行う江崎浩氏

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

□第76回 IETF krb WGのアジェンダ
http://www.ietf.org/proceedings/09nov/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、11月12日（木）に開催され、参加者は100名程度でした。

最初にチェアから、WG文書のステータスおよび今回のミーティングの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議論の対象となった提案は、以下の通りです。

・TLS Cached Info
・Additional PRF Input
・TLS Renegotiation Vulnerability

今回のミーティングでは、ミーティング時間の大半を使って、2009年11月に発見されたTLS Renegotiationにおける脆弱性に関する議論が中心に行われました。この脆弱性について詳細を知りたい場合には、本ミーティングの発表資料やInternet-Draftをご参照ください。

◇TLS Renegotiation Vulnerability

・発表資料
http://tools.ietf.org/agenda/76/slides/tls-7.pdf
・Internet-Draft:Transport Layer Security（TLS）Renegotiation Indication Extension
http://tools.ietf.org/html/draft-rescorla-tls-renegotiation-00

また、今回発見された脆弱性は、他のプロトコル（例えば、IMAP、LDAP、XMPP、SIP、SMTPなど）も同様に起こり得るかもしれないとの指摘がされていました。

ミーティングで議論された内容として、技術的な内容の他にTLSプロトコル実装者への影響などを考慮して、今後のマイルストーンや進め方について、入念に議論が行われていました。

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

□第76回 IETF tls WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/tls.txt

◆ipsecme WG（IP Security Maintenance and Extensions WG）

ipsecme WGは、2005年にクローズされたIPsec WGの後継WGであり、IPsec WGがクローズされてから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。このミーティングは、11月12日（木）に開催され、参加者は40名程度でした。会場となった部屋が比較的に狭かったため、立ち見が出るような状況でした。

ミーティングの流れとしては、今回のアジェンダについて説明が行われ、参加者からコメントがなかったため予定通り会議が開始されました。

ipsecme WGとしての初めてのRFC（RFC 5685 IKEv2 Redirect）が発行されたことが周知され、多くの参加者から拍手が送られました。また、TAHI Projectから、The 10th TAHI Test Eventが2010年1月25日～29日に千葉で開催されることが周知されました。

今回、発表された議題は以下の通りです。

・A Childless Initiation of the IKE SA
・Labeled IPsec
・EAP-Only Authentication in IKEv2
・Secure Pre-Shared Key Authentication for IKE
・A Quick Crash Discovery Method for IKEv2
・WESP Extensions
・IPsec High Availability

今回、実験的な試みとして、Labeled IPsecでは、発表者がリモートから音声によるプレゼンテーションを行いました。実際に参加した感想としては、音声もクリアで聞き取りやすく成功だったのではないかと思いました。このような仕組みが本格化することで、今まで参加できなかったような人たちにも、IETFで発表するチャンスを与えられるのではないかと考えました。

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

□第76回 IETF ipsecme WGのアジェンダ
http://www.ietf.org/proceedings/09nov/agenda/ipsecme.txt

（NTTソフトウェア株式会社 菅野哲）
（NTTソフトウェア株式会社 小林千夏）

◆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。WG Last Call（WGLC）となるInternet-Draft（I-D）が出揃ってきました。WGLCとは、WG内でドキュメントを変更する必要性がないかどうか、一定の期間を取り最終確認をすることです。第76回IETFでは、SIDR WGのミーティングが2日目（11月9日）の午前9時から1時間半程行われました。参加者は80名程でした。

SIDR WGでWGLCの状態になっているI-Dを、以下に示します。

- An Infrastructure to Support Secure Internet Routing
  draft-ietf-sidr-arch-09
  RPKIの全体構造や概念を述べたドキュメントです。

- Certificate Policy（CP）for the Resource PKI（RPKI）
  draft-ietf-sidr-cp-07
  リソース証明書の発行条件を定義したドキュメントです。RIPE NCCのAndrei氏のコメントを受けた修正が終わりました。

- A Profile for Route Origin Authorizations（ROAs）
  draft-ietf-sidr-roa-format-06
  ROAの書式を定義したドキュメントです。

- A Profile for Resource Certificate Repository Structure
  draft-ietf-sidr-repos-struct-03
  リソース証明書などの格納や公開の仕方を定義したドキュメントです。公開サーバと登録オブジェクトの命名方法に関する提案がなされています。

- A Profile for X.509 PKIX Resource Certificates
  draft-ietf-sidr-res-certs-17
  リソース証明書の各フィールドの内容を定義したドキュメントです。

これらは、ほぼ議論が終わっており、大きな変更はない見込みです。ただ、RPKIで使われる暗号アルゴリズムの記述をまとめた次のドキュメントが新たに作成されたため、これらのドキュメントでは、各々記述を持つのではなく、これを参照する形に変更されました。

- A Profile for Algorithms and Key Sizes for use in the Resource Public Key Infrastructure
  draft-ietf-sidr-rpki-algs-00
  RPKIで使われる暗号アルゴリズム、ハッシュアルゴリズム、鍵長などについてまとめたドキュメントです。デフォルトではSHA-256と2,048bitのRSAが使われることになっています。

SIDR WGのアジェンダの最後で、2009年9月にISOC主催で行われた会議「RPKI Operators Roundtable Report and Discussion」の報告がありました。この会議は、RPKIに関するルーティング・オペレーターのニーズを確認するために開かれたもので、米国、日本、ヨーロッパのISPでルーティングに携わっている技術者を中心に、参加者が構成されました。SIDR WGでドキュメント策定に関わっている主要なメンバーは招待されなかった模様です。

下記のレポートには、以下のようなポイントがまとめられています。

- 参加者の間で確認された、RPKIに対するニーズ
  - ・RPKIにおいてはIPv4とIPv6のサポートが必要である。
  - ・IPアドレスの一意性の担保は必要である。
  - ・IPv6のデータ（登録情報）をきれいにする必要がある。（IPv4は難しいので後にする）
  - ・リソースホルダーの認証（レジストリごとの対応）が必要である。
- 参加者間における認識の違い
  - ・IRR（RADB）とWHOISとでどちらがクリーンか。
  - ・単一のルート（例えばIANAやNRO）は必要か。
  - ・BGP（プロトコル）を変えずにpath validationはできるか。
  - ・リージョンごとにIPアドレスやルーティングの正しさに関する認識や状況は異なる。
- 参加者が共通に認識している課題。
  - ・RPKIに関する共通のツール開発が必要である。
  - ・Origin Validationの仕組み（draft-ymbk-rpki-rtrprotocol）。

□"Securing Routing Information - Findings from an Internet Society Roundtable", September 2009
http://www.isoc.org/educpillar/resources/docs/routingroundtable_200909.pdf

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

PKIX WGは、インターネットのための、PKI技術の策定に取り組んでいるWGです。ミーティングは、3日目の11月10日（火）午後1時から2時間程、行われました。参加者は30名程でした。

新たに以下のドキュメントがRFC化されました。

- Elliptic Curve Cryptography Subject Public Key Information（RFC 5480）
  電子証明書発行先の公開鍵暗号として、楕円暗号のアルゴリズムを使うためのアルゴリズムIDと構造を定義したドキュメントです。以下のアルゴリズムを使うことができます。

  - Elliptic Curve Digital Signature Algorithm（ECDSA）
  - Elliptic Curve Diffie-Hellman（ECDH）family schemes
  - Elliptic Curve Menezes-Qu-Vanstone（ECMQV）family schemes

WGで作業中となっている主なドキュメントの状況を、以下にまとめます。

- Trust Anchor Management（TAM）関連
  PC以外の機器を含むPKIアプリケーションで、トラストアンカーのデータを管理するためのプロトコルなどのドキュメントです。Trust Anchor Formatに関するドキュメントdraft-ietf-pkix-ta-format-04はIESGのレビューが行われている状態で、プロトコルを定義したdraft-ietf-pkix-tamp-04は今後WGLCがかけられる見込みです。

- OCSP Algorithm Agility
  OCSPで使われる暗号アルゴリズムを、複数候補から選べるようにする仕組みの提案です。議論は特になく、今後WGLCがかけられる見込みです。

- Certificate image
  証明書の証明内容や発行元、発行先のイメージデータを入れる提案です。PDF（Portable Document Format）とSVG（Scalable Vector Graphic image）が入れられるようになっています。議論は特になく、今後WGLCがかけられる見込みです。

PKIの仕様に関係して行われた、主なプレゼンテーションを次にまとめます。

- RFC 5280 Implementation Report, 発表者 Tim Polk氏
  RFC 5657に基づく実装の調査報告です。実装が存在することを提示することで、RFC5280をProposed Standard（PS）からDraft Standard（DS）にする（格上げする）活動として行われています。

  PKIX WGのMLに投げられたS/MIMEメッセージを収集し、米国NISTのPublic Key Interoperability Test Suite（PKITS）を使って検証が行われました。国際化対応については、確認が行われませんでした。

  今後、RFC5280にはErrataの修正を行った上で、調査報告書を添えてDraft Standardをめざすようです。

- Certificate information expression, 発表者 Stefan Santesson氏
  電子証明書のフィールドに、EUで進められているSTORKプロジェクト※2で使われる「マッピングの情報」を含める提案です。STORKプロジェクトで課題となっている、EU内の各国間で、発行されている証明書を対応付けるマッピングの必要性についてプレゼンテーションが行われていました。

この他に、ホスティングサーバの間で行われるXMPP連携で使われる属性証明書の必要性や、Digital Right Management（DRM）のためのProxyアーキテクチャの提案、TLSでサービスごとに異なる識別子に関する共通ルールの提案などが行われました。

◇　　◇　　◇

日本での開催とあって、会場では多くの日本人を見かけましたが、SIDR WGやPKIX WGの議論でアクティブなのは相変わらずの常連メンバーでした。この二つのWGは、他のWGでも活躍しているIETFの常連メンバーによって成り立っている側面があり仕方がないことではあるのですが、日本からも抽象度の高いハイレベルな議論に参加していきたいとあらためて感じました。

（JPNIC 技術部 木村泰司）

※1 Kerberos認証
共通鍵暗号を用いるネットワーク認証方式の一つです。

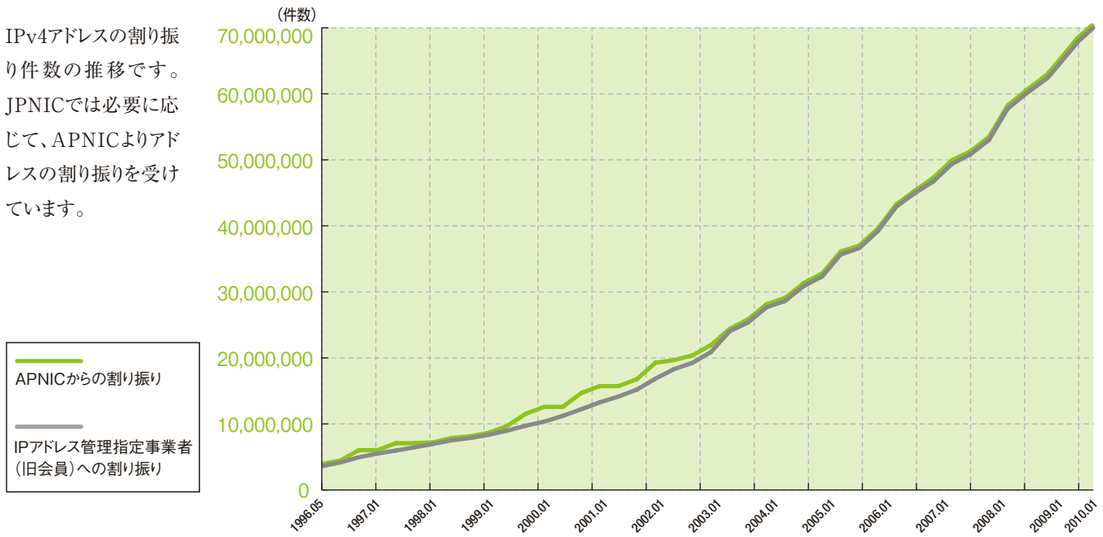
※2 STORK（Secure idenTity acrOss boRders linKed）プロジェクト
http://www.eid-stork.eu/

統計情報

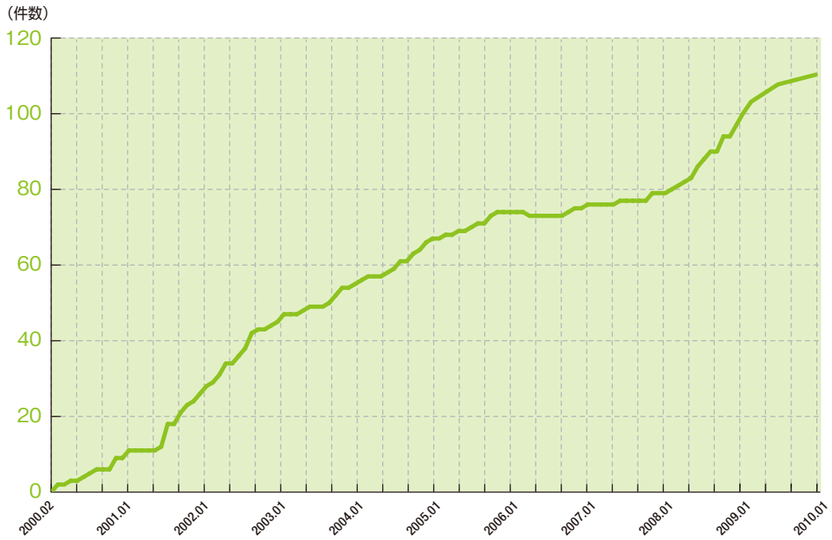
Statistics Information

■ IPv4アドレス割り振り件数の推移

IPv4アドレスの割り振り件数の推移です。JPNICでは必要に応じて、APNICよりアドレスの割り振りを受けています。



■ IPv6アドレス割り振り件数の推移

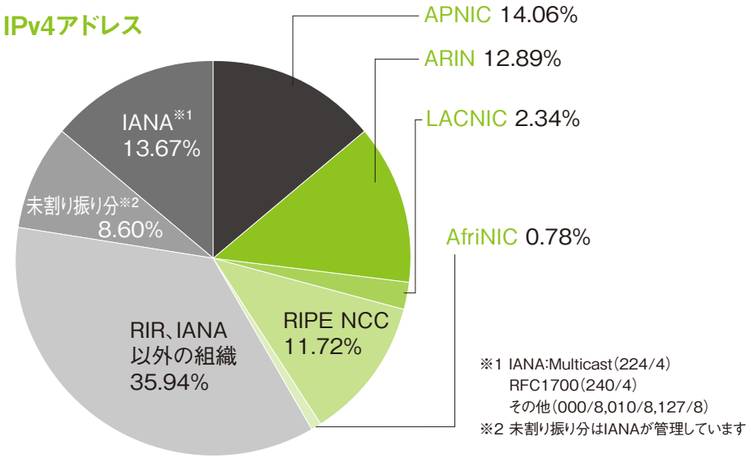


JPNICでは、これまでAPNICで行う割り振りの取り次ぎサービスを行っていましたが、2005年5月16日より、IPアドレス管理指定事業者を対象にIPv6アドレスの割り振りを行っています。

■ 地域インターネットレジストリ(RIR)ごとのIPv4アドレス、IPv6アドレス、AS番号配分状況

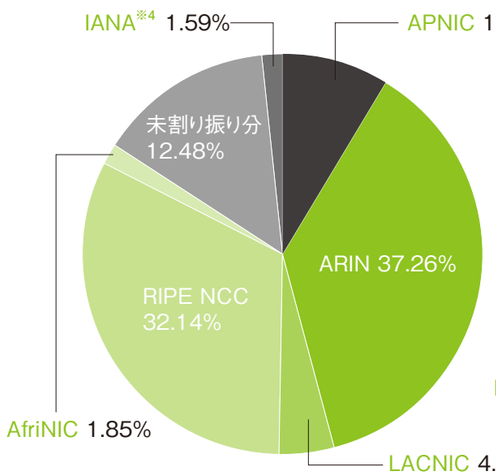
各地域レジストリごとのIPv4、IPv6、AS番号の割り振り状況です。APNICはアジア太平洋地域、ARINは主に北米地域、RIPE NCCは欧州地域、AfriNICはアフリカ地域、LACNICは中南米地域を受け持っています。(2010年2月11日現在)

● IPv4アドレス



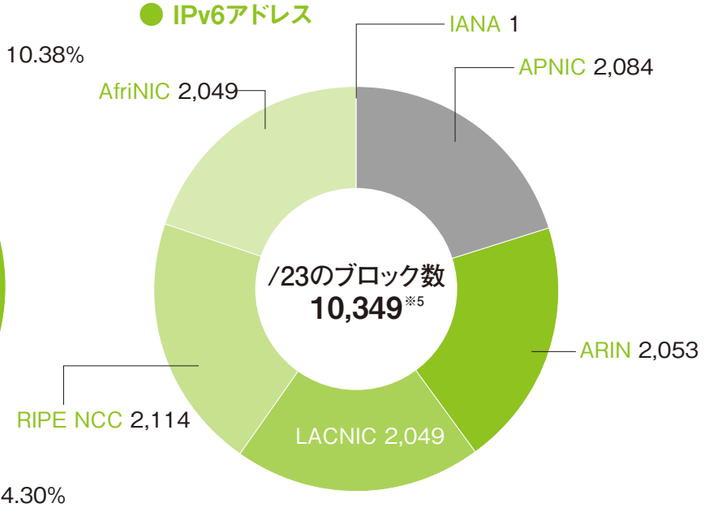
※1 IANA:Multicast(224/4)
RFC1700(240/4)
その他(000/8,010/8,127/8)
※2 未割り振り分はIANAが管理しています

● 2バイトAS番号※3



※3 上文の他に、IANAから各RIRに対して1,024個の4バイトAS番号の割り振りが行われています
※4 IANA:AS番号 0,23456,64512-65535

● IPv6アドレス



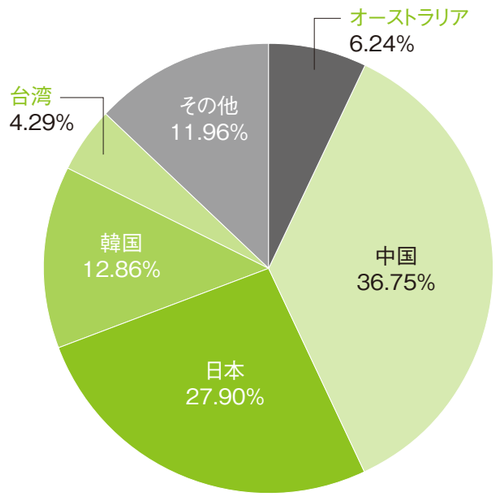
※5 IANAからRIRに割り振られた/23のブロック数は10,349

統計情報

Statistics Information

■ アジア太平洋地域の国別IPv4アドレス配分状況

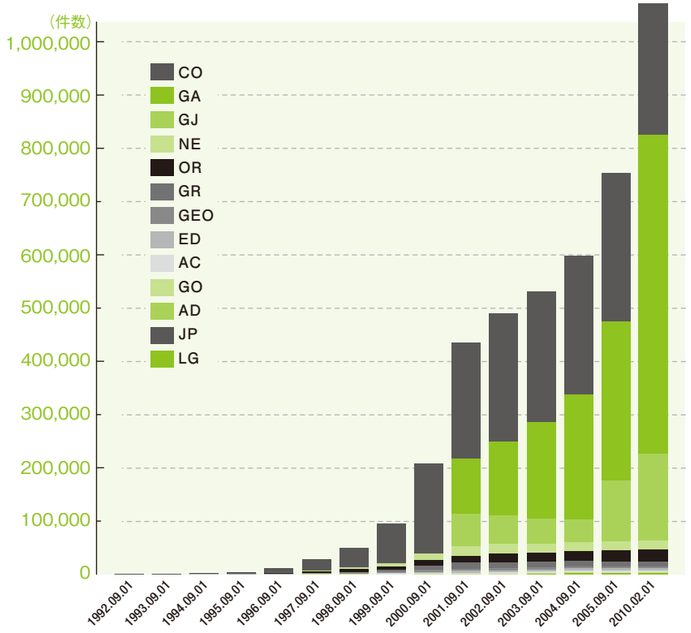
APNICからローカルインターネットレジストリ（LIR）へ割り振られたホスト数と、APNICから直接割り当てられたホスト数の合計を国別に示しています。（2010年1月31日現在）



■ JPドメイン名登録の推移

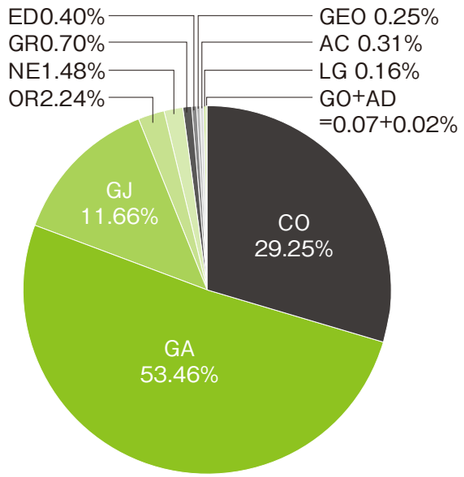
JPドメイン名の登録件数は、2001年の汎用JPドメイン名登録開始により大幅な増加を示し、2003年1月1日時点で50万件を超えました。
その後も登録数は増え続けており、2008年3月1日時点で100万件を突破、2010年2月現在で約114万件となっています。

属性型・地域型JPドメイン名	JP	属性なし
	AD	JPNIC会員
	AC	大学等教育機関
	CO	一般企業
	GO	政府機関
	OR	会社以外の法人
	NE	ネットワークサービス
	GR	任意団体
	ED	小・中・高校
	GEO	地域型
	LG	地方公共団体
汎用JPドメイン名	GA	ASCII（英数字）
	GJ	日本語



■ 属性ごとの登録JPドメイン名の割合

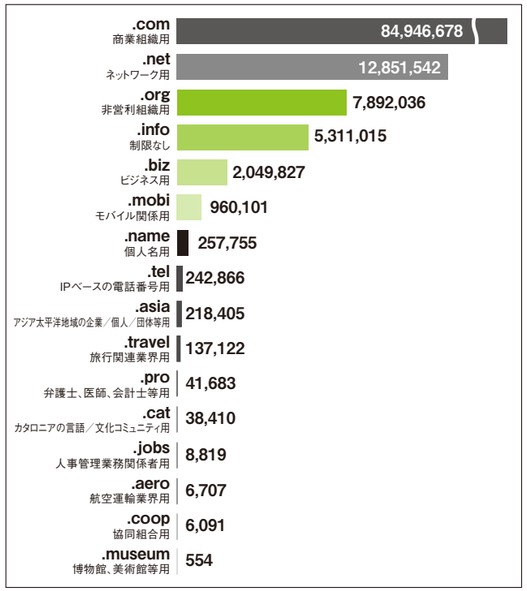
2010年2月1日現在の登録ドメイン名を属性別で円グラフにしたものです。最も多い属性は、汎用JPドメイン名（GA）で53.46%、次いでCO、汎用JPドメイン名（GJ）、OR、NEの順となります。



■ gTLDの種類別登録件数

分野別トップレベルドメイン（gTLD: generic TLD）の登録件数です（2009年10月現在）。データの公表されていない、.edu, .gov, .mil, .intは除きます。

※下記のデータは、各gTLDレジストリ（またはスポンサー組織）がICANNに提出する月間報告書に基づいています



■ JPドメイン名紛争処理件数

JPNICはJPドメイン名紛争処理方針（不正の目的によるドメイン名の登録・使用があった場合に、権利者からの申立に基づいて速やかにそのドメイン名の取消または移転をしようとするもの）の策定と関連する業務を行っています。この方針に基づき実際に申し立てられた件数を示します。（2010年2月現在）

※申立の詳細については下記Webページをご覧ください
http://www.nic.ad.jp/ja/drp/list/

2000年	2件	移　転　1件・取下げ　1件
2001年	11件	移　転　9件・取下げ　2件
2002年	6件	移　転　5件・取　消　1件
2003年	7件	移　転　4件・取　消　3件
2004年	4件	移　転　3件・棄　却　1件
2005年	11件	移　転　10件・取下げ　1件
2006年	8件	移　転　7件・棄　却　1件
2007年	10件	移　転　9件・棄　却　1件
2008年	3件	移　転　2件・棄　却　1件
2009年	9件	移　転　3件・取　消　2件・棄　却　2件・手続終了　1件・係属中　1件
2010年	1件	係属中　1件

※取下げ：裁定が下されるまでの間に、申立人が申立を取り下げること
移　転：ドメイン名登録者（申し立てられた側）から申立人にドメイン名登録が移ること
取　消：ドメイン名登録が取り消されること
棄　却：申立を排斥すること
係属中：裁定結果が出ていない状態のこと
手続終了：当事者間の和解成立などにより紛争処理手続が終了すること

Internet インターネット 10分講座

暗号アルゴリズムの危殆化

今回のインターネット10分講座では、インターネットに関する技術に対して比較的影響が大きい、暗号アルゴリズムの危殆化について解説します。

1. はじめに

既にご存じの方も多いと思いますが、2010年1月7日に、複数の欧州の研究機関とNTTで構成される研究グループによって、768ビット（10進232桁）のRSAモジュラスである合成数の素因数分解に成功したという発表がありました（[1,2]）。RSAモジュラスとは二つの素数の積の形をした合成数です。素因数分解問題の困難性、言い換えますと、大きな桁数の合成数の素因数分解が難しいということが、多くの暗号プロトコル、および、暗号アルゴリズムの安全性を担保しているというのが、最も基本的な事項の一つです。

今回の記録達成は、現在多くのアプリケーションで使用されている、例えば1024ビットのRSAモジュラスなどの、より大きな桁数の合成数から見れば一つの通過点に過ぎませんが、素因数分解の困難性が有する安全性の評価のみならず、暗号アルゴリズムに関するパラメータ設定の移行時期、および、使用期限を予測する上で非常に重要な通過点です。

2. 暗号アルゴリズムの危殆化とは

簡単に言えば、暗号アルゴリズムの危殆化とは、暗号アルゴリズムの安全性のレベルが低下した状況、または、その影響により暗号アルゴリズムが組み込まれているシステムなどの安全性が脅かされる状況を言います。普通は、暗号アルゴリズムが破られたとか、解読されたとか言われますが、どの程度暗号アルゴリズムが破られたのか、解読されたのかが説明されないと詳しいことは分かりません。暗号アルゴリズムに対する解析方法は数多くあり、しかも、解析結果には非常に大きな幅があるので、専門家による解説がなければ一般の人には分かりません。

例えば、大雑把な分類として、

(1) 暗号アルゴリズムに問題点が見つかっていない。
(2) 暗号アルゴリズムの一部分に、ある欠陥が見つかっただけで、暗号アルゴリズムの全体の問題ではない。
(3) 暗号アルゴリズムの全体にまで解析が及んでいるが、解読するためのコストが現実的な量ではない。
(4) 暗号アルゴリズムの全体にまで解析が及んでおり、解読するためのコストが現実的な量である。

のような区別を付けることが考えられます。

また、コストについては、

(5) 時間的なコスト
(6) 金額的なコスト

の二つの量に分けられます。

本稿では例として、RSA暗号（素因数分解問題）、ハッシュ関数MD5とSHA-1の三つのケースを挙げて、もう少し詳細について見ていきます。

2.1 RSA暗号（素因数分解問題）の場合

素因数分解問題とは、二つの相異なる素数p,qの積である合成数Nが与えられた時に、Nだけからその素因数p,qを求める問題です。そして、RSA暗号は、1978年にリベスト（Rivest）、シャミア（Shamir）、エイドルマン（Adleman）の3人によって公表された公開鍵暗号の一つで、その安全性は素因数分解問題の困難性に依存しています。一般によく使われているRSA守秘やRSA署名もその一種です。公開されている公開鍵から秘密鍵が解かれてしまえば、暗号文の復号も、署名の偽造も可能になってしまいますから、RSAモジュラスの選択において、素因数分解問題の困難性は非常に重要な位置を占めています。

1990年頃になって、ポラード（Pollard）らの数学者によって一般数体ふるい法（General Number Field Sieve, GNFS）が提案されてからは、徐々に分解される合成数のサイズが大きくなってきました。一般数体ふるい法は、非自明な関係式

$$x^2 \equiv y^2 \pmod N$$

を見つけて、最大公約数GCD（x±y,N）を計算することにより、Nの素因数を見つけ出すアルゴリズムで、

(1) 多項式選択
(2) 関係式収集
(3) フィルタリング
(4) 線形代数計算
(5) 平方根計算

の五つのステップからなり、(2) 関係式収集、および、(4) 線形代数計算の二つのステップが計算量の大半を占めます。現在知られている解法アルゴリズムの中では最速ですが、最適化のためのパラメータ設定が複雑なのが特徴です。表1が分解記録リストです。

表1：一般数体ふるい法による近年の分解記録

合成数	サイズ	公表年月
RSA-768	232桁（768ビット）	2010年1月
RSA-200	200桁（663ビット）	2005年9月
RSA-640	193桁（640ビット）	2005年11月
$11^{281}+1$の約数	176桁（582ビット）	2005年4月
RSA-576	174桁（576ビット）	2003年12月
$21^{826}+1$の約数	164桁（545ビット）	2003年12月
RSA-160	160桁（530ビット）	2004年4月
$2^{953}+1$の約数	158桁（524ビット）	2002年1月
RSA-155	155桁（512ビット）	1999年8月
RSA-140	140桁（463ビット）	1999年2月
RSA-130	130桁（430ビット）	1996年3月

実は、一般数体ふるい法の計算量は、以下のような漸近的な評価が与えられているのでおおよその推定は可能ですが、正確な計算量の予測にはあまり適していません。

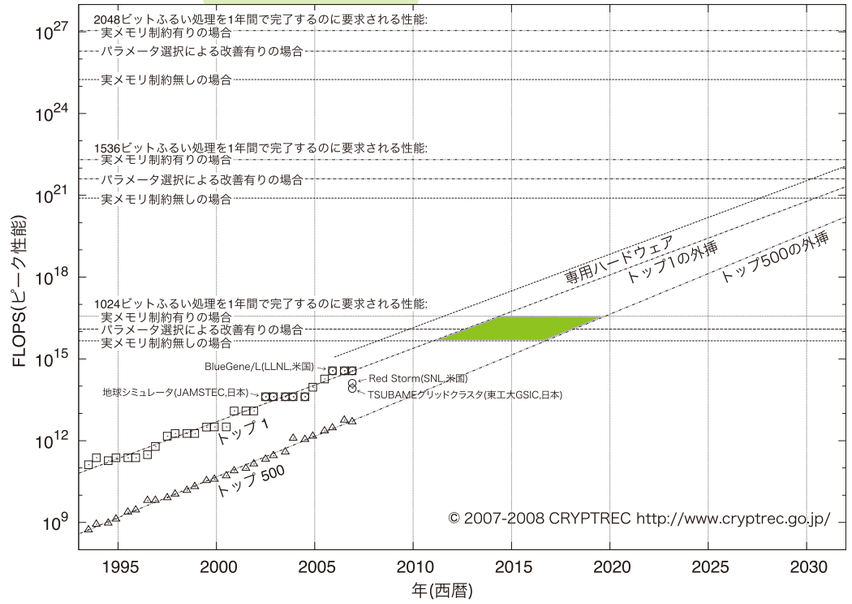
$$L_N\left[\frac{1}{3}, \left(\frac{64}{9}\right)^{\frac{1}{3}} + O(1)\right], \qquad \left(\frac{64}{9}\right)^{\frac{1}{3}} = 1.9229994\cdots$$

ただし、

$$L_N[S,C] = exp\left(C(\log N)^S(\log\log N)^{1-S}\right)$$

そこで、関係式収集ステップの計算量を部分的な実験結果から推定する方法を用いて、CRYPTREC※1では素因数分解問題に関する評価結果を2006年度に公表しています※2。

図1：1年間で関係式収集ステップを完了するのに要求されるコンピュータの処理性能予測（[3]からの引用）



この評価結果から、分解にかけるコストに依存するものの、1024ビットのRSAモジュラスの素因数分解はおおよそ2015年～2020年頃から分解の可能性が高まってくるということが読み取れます。従って、今後、新規にシステムを構築する場合には、1024ビットよりも長いサイズのRSAモジュラスを選択することが望ましいものと考えられます。

移行に際してまずはじめに問題となるのは、次にどのビットサイズを用いるのかということです。PC環境においては2048ビットへ変更するのは比較的容易であっても、ICカードや携帯電話など記憶容量や計算能力といったリソースに制限がある場合には難しいことが考えられます。また、1024ビットの使用をいつまで認めるべきかという、使用期限の観点についても問題となってきます。

2.2 ハッシュ関数MD5の場合

MD5はリベストによって1991年に提案された、ブロック長が512ビット、ハッシュ長が128ビットであるハッシュ関数です。提案されてから数年後には、MD5の一部分に問題点が指摘され、MD5の仕様に変更を加えたハッシュ関数に対して、衝突を探索する攻撃アルゴリズムが発見されました。しかしその時はオリジナルのMD5の衝突発見までには至っていませんでした。

説明が前後しますが、一般にハッシュ関数Hの安全性には大きく分けて、以下の三つがあります。

(1)衝突発見困難性 ― ハッシュ値が一致する、すなわち、H(M_1)= H(M_2)となるようなメッセージM_1とM_2を探索することが困難なこと。

(2)第2原像計算困難性 ― ある既知のメッセージMとそれに対するハッシュ値が与えられた時に、ハッシュ値が一致する、すなわち、H(M)= H(M')となるような別のメッセージM'を探索することが困難なこと。

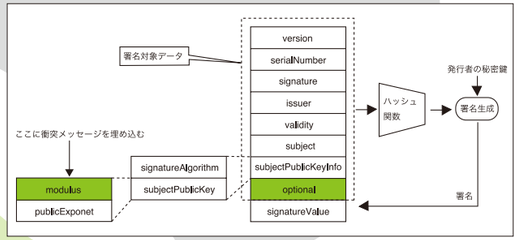
(3)原像計算困難性 ― ある未知のメッセージMに対するハッシュ値が与えられた時に、ハッシュ値が一致する、すなわち、H(M)= H(M')となるようなメッセージM'を探索することが困難なこと。

ようやく、2004年になってワン(Wang)らによってMD5の衝突を効率的に探索するアルゴリズムが提案されました。ワンらは入力ブロックの一つ目と二つ目に差分を加え、それぞれのブロック、および、関数内部の内部変数に制約条件を与えることで、衝突探索の効率を著しく高めることに成功しています。

探索で計算されるメッセージのペアはランダムなデータなので、それ自体では意味をなすような文書になる確率は低いものです。つまり、普通のテキストファイルのような文書の範囲で、衝突を起こすようなメッセージのペアを見つけることは困難です。しかしながら、バイナリなメッセージを文書中に埋め込んでも文書フォーマットとして正当であるような場合には、衝突を起こすような文書を作成することが原理的には可能となります。

その顕著な例が、公開鍵暗号基盤(Public Key Infrastructure, PKI)の公開鍵証明書のメッセージフォーマットとして利用されているX.509証明書です。レンストラ(Lenstra)らはワンらがMD5の衝突探索アルゴリズムを提案してすぐさま2005年に、X.509証明書の衝突探索手法を提案しています。つまり、はじめは探索で計算された衝突メッセージを「modulus」フィールドに埋め込むことで衝突を起こすX.509証明書のペアを計算する手法でした。

図2：2005年時点のX.509証明書の衝突手法のあらまし



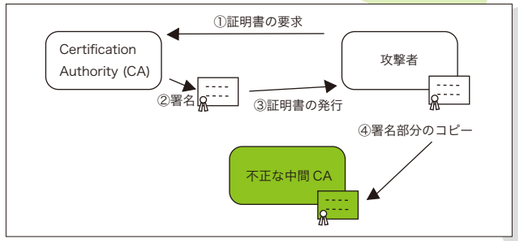
ところが、その後探索手法の研究の進展によって、レンストラらの研究チームは偽造したX.509証明書を商用のCA(Certification Authority)に実際に署名させることにより、中間CA証明書の偽造に成功するまでに至っています([4])。ここで重要なことは、前述の(1)～(3)とは異なる、新たな、

(4)Chosen-Prefix衝突発見困難性 ― 既知のメッセージP_1とP_2が与えられたときに、ハッシュ値が一致する、すなわち、H(P_1 || S_1) = H(P_2 || S_2)となるようなメッセージS_1とS_2を計算することが困難なこと。

という探索アルゴリズムが提案されていることです。第2原像計算困難性を有していたとしても、この探索アルゴリズムのおかげで、より現実の状況に沿ったX.509証明書の偽造が可能になっています。また、探索で計算された衝突メッセージを埋め込む場所は図2における「optional」フィールドで、署名検証側にとって無意味な場合には読み飛ばす場所を利用しています。

この発表を受けて、ベリサイン社が2009年初めにMD5の証明書発行の停止を発表するなど、証明書発行ベンダー側での対応も早速なされています([5])。

図3：2008年時点のX.509証明書偽造の様子



2.3 ハッシュ関数SHA-1の場合

SHA-1は米国の国立標準技術研究所(National Institute of Standards and Technology, NIST)によって1995年に制定されたブロック長が512ビット、ハッシュ長が160ビットのハッシュ関数です。提案されてから10年近くの間、深刻な問題点が発見されていませんでしたが、MD5の衝突と同じ、ワンらによって2005年に衝突探索アルゴリズムが提案されています。

ワンらが提案した2005年頃の評価では、衝突探索に関する計算量は2^{63}～2^{69}の範囲でしたが、最近になってSHA-1の衝突探索アルゴリズムの計算量がさらに2^{52}まで低下しているとの報告がなされています([6])。

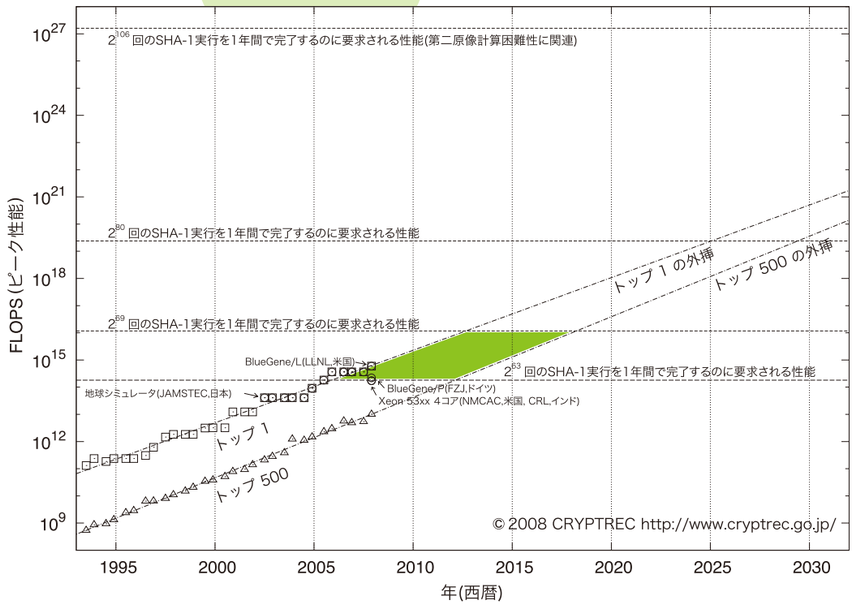
論文などにおいて公表されている、SHA-1の衝突探索に関する計算量をまとめると表2のようになります。

表2：MD5とSHA-1の衝突探索計算量低下の時間的流れ([4]からの引用)

Year	MD5		SHA-1	
	identical-prefix	chosen-prefix	identical-prefix	chosen-prefix
pe-2004	2^{64}	2^{64}		2^{80}
2004	2^{40}			
2005	2^{37}		2^{69} 2^{63}	
2006	2^{32}	2^{49}		$2^{80-\varepsilon}$
2007	2^{25}		2^{61}	
2008	2^{21}			
2009	2^{16}	2^{39}	2^{52}	

使用しているデータが古く、最新のデータをプロットしていませんが、CRYPTRECではSHA-1に関する評価結果を公表しています。

図4：1年間で衝突を探索するのに要求されるコンピュータの処理性能予測([7]からの引用)



計算量が2^{52}まで低下しますと、SHA-1の衝突メッセージがいつ世界で初めて算出されても、現在のコンピュータの性能からいっておかしくはありませんが、本原稿の執筆時点においてはまだ発見されていません。なお、SHA-1については、MD5においてサーバ証明書を偽造することが容易になるほど、衝突探索アルゴリズムの効率は向上していませんが、そうでなくてもコンピュータの性能向上により安全性は徐々に低下していきますから、今後の動向には細心の注意が必要です。

3. 危殆化に係る問題点

暗号アルゴリズムはそもそも単体で用いられるものではなく、ソフトウェア、または、ハードウェアとして実現され、システムなどに組み込まれて初めて使われるものです。もう少し詳しく見ると、暗号アルゴリズムはソフトウェア、または、ハードウェアとして実現され、暗号モジュールを構成し、暗号モジュールは暗号プロトコルなどに組み込まれます。最後に、システムは実現したい要件に従って、暗号プロトコルなどを選択して自身に組み込んでいます。

問題になるのは、システムで使用しているある暗号アルゴリズムに危殆化が生じたとして、暗号アルゴリズムを交換したり、あるいは、暗号アルゴリズムのパラメータの設定を変更したりすることがはたして可能なのかということです。

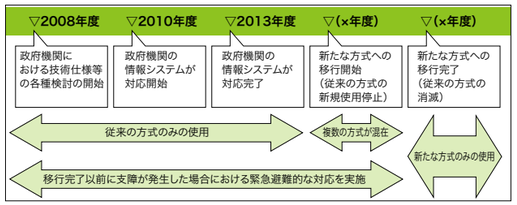
残念なことに、暗号アルゴリズムの変更を考慮に入れてシステム構築がなされていることが非常に少ないのが現状です。

4. 移行スケジュールの策定の必要性

暗号アルゴリズムの変更を考慮に入れていない情報システムが多い中で、暗号アルゴリズムの移行指針とそのロードマップについて検討することは非常に重要です。

CRYPTRECにおいて2006年度に公表された、RSA1024ビットが有する素因数分解の困難性、および、SHA-1の衝突発見困難性に関する評価結果を受けて、政府機関の情報システムに関する情報セキュリティ対策を立案・遂行する機関である、内閣官房情報セキュリティセンター(National Information Security Center, NISC)は、政府機関の情報システムにおいて使用されているSHA-1、および、RSA1024ビットに係る移行指針を策定しています([8])。そこでは、政府認証基盤(Government Public Key Infrastructure, GPKI)などの電子政府システムにおいて、情報システムのライフサイクルに合わせて、SHA-256、および、RSA2048ビットが選択可能なように今後、システム設計をする旨、政府統一的な対応策が取られています。

図5：移行指針に基づく暗号方式の移行スケジュール概念図



5. まとめ

本稿では、暗号アルゴリズムの危殆化の概要について駆け足で見てきました。海外の動向など他にもご紹介すべき点がたくさんあるのですが、紙面の都合で割愛せざるを得ませんでした。この場を借りてお詫びしたいと思います。最後に政府機関における移行指針について紹介しましたが、すべての民間企業においてコンセンサスが得られているわけではありません。重要なことは、それぞれの所属するコミュニティにおいて、主体的に暗号アルゴリズムの移行について検討することです。その中で、他のコミュニティとの調整が必要となってくる場合もあると思います。

(独立行政法人情報通信研究機構(NICT)/黒川貴司)

参考文献

[1] Kleinjung,Aoki,Franke,Lenstra,Thomé,Bos,Gaudry,Kruppa,Montgomery,Osvik,te Riele,Timofeev,Zimmermann, "Factorization of a 768-bit RSA modulus" http://eprint.iacr.org/2010/006

[2] NTTニュースリリース「公開鍵暗号の安全性の根拠である「素因数分解問題」で世界記録を更新～768ビット合成数を一般数体篩法にて完全分解に成功～」 http://www.ntt.co.jp/news/news10/1001/100108a.html

[3] CRYPTREC,「CRYPTREC Report 2006」 http://www2.nict.go.jp/y/y213/cryptrec_publicity/c06_wat_final.pdf

[4] Stevens,Sotirov,Appelbaum,Lenstra,Molnar,Osvik,Wegner ,"Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate" http://eprint.iacr.org/2009/111

[5] ベリサイン,「MD5アルゴリズムへの衝突攻撃によるSSLサーバ証明書の偽造に関する報道について」 https://www.verisign.co.jp/ssl/about/20090106.html

[6] McDonald,Hawkes,Pieprzyk, "Differential Path for SHA-1 with complexity O(2^{50})" http://eprint.iacr.org/2009/259

[7] 総務省・法務省・経済産業省,「電子署名及び認証業務に関する法律の施行状況に係る検討会」報告書 http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html

[8] 内閣官房情報セキュリティセンター,「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1及びRSA1024に係る移行指針」 http://www.nisc.go.jp/active/general/res_niscrypt.html

※1 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省、経済産業省、独立行政法人情報通信研究機構、独立行政法人情報処理推進機構が事務局を運営している。

※2 参考文献[2]によると、ふるい処理の計算量はAMD Opteron 2.2GHz換算で1500年と見積もられています。これは[3]の予測値の35%増であって、おおよそ予想の範囲内にあるものと考えられます。

会員リスト

■ 2010年1月19日現

S 会員

株式会社インターネットイニシアティブ
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社日本レジストリサービス

A 会員

富士通株式会社

B 会員

株式会社エヌ・ティ・ティ・ドコモ
株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ
KDDI 株式会社
メディアエクスチェンジ株式会社

C 会員

e- まちタウン株式会社
NEC ビッグローブ株式会社
関西マルチメディアサービス株式会社
株式会社日立情報システムズ
株式会社 UCOM

会員リスト

■2010年1月19日現在

D会員

アイコムティ株式会社
株式会社アイテックジャパン
アイテック阪急阪神株式会社
株式会社朝日ネット
株式会社アット東京
株式会社アドミラルシステム
アルファ総合研究所株式会社
株式会社イージェーワークス
株式会社イオンビスティー
イッツ・コミュニケーションズ株式会社
インターナップ・ジャパン株式会社
インターネットエーアールシー株式会社
インターネットマルチフィード株式会社
株式会社インテック
株式会社エアネット
AT&Tジャパン株式会社
株式会社SRA
株式会社STNet
株式会社SBR
エヌ・アール・アイ・ネットワークコミュニケーションズ株式会社
株式会社エヌアイエスプラス

エヌ・ティ・ティ・スマートコネクト株式会社
株式会社エヌ・ティ・ティ・データ
株式会社エヌ・ティ・ティ・データ三洋システム
株式会社エネルギア・コミュニケーションズ
株式会社オージス総研
株式会社オービック
大分ケーブルテレコム株式会社
株式会社大垣ケーブルテレビ
株式会社大塚商会
沖電気工業株式会社
沖縄通信ネットワーク株式会社
オンキヨーエンターテイメントテクノロジー株式会社
関電システムソリューションズ株式会社
株式会社キッズウェイ
キヤノンITソリューションズ株式会社
株式会社キューデンインフォコム
九州通信ネットワーク株式会社
京都リサーチパーク株式会社
共同印刷ビジネスソリューションズ株式会社
近畿コンピュータサービス株式会社
近鉄ケーブルネットワーク株式会社

株式会社倉敷ケーブルテレビ
株式会社クララオンライン
株式会社グッドコミュニケーションズ
KVH株式会社
株式会社ケーブルテレビ可児
ケーブルテレビ徳島株式会社
株式会社ケイ・オプティコム
株式会社KDDIウェブコミュニケーションズ
KDDI沖縄株式会社
株式会社コミュニティネットワークセンター
彩ネット株式会社
株式会社サイバーリンクス
さくらインターネット株式会社
株式会社サンフィールド・インターネット
株式会社シー・アール
株式会社シーイーシー
株式会社CSK-ITマネジメント
システム・アルファ株式会社
シャープ株式会社
GMOインターネット株式会社
ジャパンケーブルネット株式会社

スターネット株式会社
株式会社ZTV
全日空システム企画株式会社
ソネットエンタテインメント株式会社
ソフトバンクテレコム株式会社
ソフトバンクテレコム株式会社　サービス開発本部
知多メディアスネットワーク株式会社
中部テレコミュニケーション株式会社
株式会社つくばマルチメディア
ティアイエス株式会社
有限会社ティ・エイ・エム
株式会社テクノロジーネットワークス
鉄道情報システム株式会社
株式会社ディーネット
株式会社ディジティミニミ
株式会社電算
東京ケーブルネットワーク株式会社
東芝ドキュメンツ株式会社
東北インテリジェント通信株式会社
豊橋ケーブルネットワーク株式会社
株式会社ドリーム・トレイン・インターネット
株式会社長崎ケーブルメディア

株式会社新潟通信サービス
ニフティ株式会社
日本インターネットエクスチェンジ株式会社
株式会社日本経済新聞社
日本情報通信株式会社
株式会社ネクサス
株式会社ネクストアイ
ネクストウェブ株式会社
株式会社ネスク
パックネットサービス・ジャパン株式会社
株式会社ビークル
株式会社ビットアイル
株式会社PFU
ファーストサーバ株式会社
株式会社フイズ
富士通エフ・アイ・ピー株式会社
富士通関西中部ネットテック株式会社
株式会社富士通システムソリューションズ
株式会社フジミック
株式会社フューチャリズムワークス
フリービット株式会社
株式会社ブロードバンドセキュリティ

株式会社ブロードバンドタワー
ブロックスシステムデザイン株式会社
ベライゾンジャパン合同会社
北陸通信ネットワーク株式会社
北海道総合通信網株式会社
松阪ケーブルテレビ・ステーション株式会社
ミクスネットワーク株式会社
三菱電機情報ネットワーク株式会社
株式会社南東京ケーブルテレビ
武蔵野三鷹ケーブルテレビ株式会社
株式会社メイテツコム
株式会社MECHA
株式会社メディアウォーズ
山口ケーブルビジョン株式会社
株式会社USEN
ユニアデックス株式会社
リコーテクノシステムズ株式会社
株式会社リンク
株式会社ワイズ
株式会社ワダックス

会員リスト

推薦個人正会員（希望者のみ掲載しております）

歌代　和正	高田　寛	山口　二郎
小林　努	冨田　良	
佐藤　秀和	三膳　孝通	

非営利会員

財団法人京都高度技術研究所	財団法人地方自治情報センター	北海道地域ネットワーク協議会
国立情報学研究所	東北学術研究インターネットコミュニティ	WIDE インターネット
サイバー関西プロジェクト	農林水産省研究ネットワーク	
塩尻市	広島県	

賛助会員

株式会社アドバンスコープ	株式会社コム	日本インターネットアクセス株式会社
株式会社アンネット	サイバー・ネット・コミュニケーションズ株式会社	株式会社ネット・コミュニケーションズ
株式会社Eストアー	株式会社サイプレス	BAN−BANテレビ株式会社
株式会社イーツ	株式会社さくらケーシーエス	姫路ケーブルテレビ株式会社
伊賀上野ケーブルテレビ株式会社	三洋コンピュータ株式会社	ファーストライディングテクノロジー株式会社
イクストライド株式会社	株式会社 JWAY	株式会社富士通鹿児島インフォネット
伊藤忠テクノソリューションズ株式会社	セコムトラストシステムズ株式会社	フュージョン・コミュニケーションズ株式会社
株式会社エーアイエーサービス	ソニーグローバルソリューションズ株式会社	株式会社平和情報センター
株式会社カイクリエイツ	ソニーブロードバンドソリューション株式会社	株式会社ヴェクタント
株式会社キャッチボール・トゥエンティワン・インターネット・コンサルティング	テクノブレスト株式会社	株式会社マークアイ
グローバルコモンズ株式会社	デジタルテクノロジー株式会社	株式会社ミッドランド
株式会社ケーブルネット鈴鹿	虹ネット株式会社	宮城ネットワーク株式会社
株式会社ケイアンドケイコーポレーション	日本商工株式会社	株式会社悠紀エンタープライズ

JPNIC CONTACT INFO

お問い合わせ先

JPNICでは、各項目に関する問い合わせを以下の電子メールアドレスにて受け付けております。

JPNIC Q&A　http://www.nic.ad.jp/ja/question/

よくあるお問い合わせは、Q&Aのページでご紹介しております。

一般的な質問	query@nic.ad.jp
事務局への問い合わせ	secretariat@nic.ad.jp
会員関連の問い合わせ	member@nic.ad.jp
JPドメイン名※1	info@jprs.jp
JP以外のドメイン名	domain-query@nic.ad.jp
JPドメイン名紛争	domain-query@nic.ad.jp
IPアドレス	ip-service@nir.nic.ad.jp
取材関係受付	press@nic.ad.jp

※1 2002年4月以降、JPドメイン名登録管理業務が（株）日本レジストリサービス（JPRS）へ移管されたことに伴い、JPドメイン名のサービスに関するお問い合わせは、JPRSの問い合わせ先であるinfo@jprs.jpまでお願いいたします。

JPNICニュースレターについて

- JPNICニュースレターのバックナンバーをご希望の方には、一部900円（消費税・送料込み）にて実費頒布しております。
  現在までに1号から43号までご用意しております。
  ただし在庫切れの号に関してはコピー版の送付となりますので、あらかじめご了承ください。
- ご希望の方は、希望号・部数・送付先・氏名・電話番号をFAXもしくは電子メールにてお送りください。
  折り返し請求書をお送りいたします。ご入金確認後、ニュースレターを送付いたします。
  宛先　FAX:03-5297-2312　電子メール:jpnic-news@nic.ad.jp
- なお、JPNICニュースレターの内容に関するお問い合わせ、ご意見は **jpnic-news@nic.ad.jp** 宛にお寄せください。

JPNICニュースレター●第44号
2010年3月12日発行

発　行　人　後藤滋樹
編集責任者　佐野　晋
発　　行　社団法人日本ネットワークインフォメーションセンター（JPNIC）
住　　所　〒101-0047
東京都千代田区内神田2丁目3番地4号
国際興業神田ビル6F
T　e　l　03-5297-2311
F　a　x　03-5297-2312

制作・印刷　凸版印刷株式会社

ISBN 978-4-902460-19-3

JPNIC認証局に関する情報公開

JPNICプライマリルート認証局
（JPNIC Primary Root Certification Authority S1）のフィンガープリント
SHA-1:07:B6:67:E7:73:04:0F:71:84:DB:0A:E7:B2:90:A3:38:D4:18:60:74
MD5:DF:A6:2B:6B:CD:C6:D3:00:18:D5:67:2E:BE:76:D7:E9

JPNIC認証局のページ
http://jpnic-ca.nic.ad.jp/

初めてでも、ビジネスでも使える さくらのレンタルサーバ！

サービス利用件数20万件の実績！

すでに20万人以上のお客様にご愛用いただいている「さくらのレンタルサーバ」では、お気軽にお使いいただける「ライト」プランから、法人用途に最適な「ビジネスプロ」まで、豊富なラインナップを取り揃えております。もちろん、どのプランもオンラインサインアップが可能。すぐに利用できて、しかも2週間の無料お試し期間付きです。
あらゆる用途に対応可能なプランを備え、データセンターとして培ってきた長年の技術とノウハウでお客様の大切なデータをお守りいたします。さくらインターネットが自信を持ってお届けするレンタルサーバサービスをぜひお試しください。

- 2week FREE!!! 2週間の無料お試し期間!
- .jp .org .com .biz .info .net 独自ドメインに対応!
- メールアドレス無制限!
- ウイルスチェック無料!
- ブログ標準提供!
- サインアップで即利用可!

		個人のお客様向け			法人のお客様向け	
		ライト	スタンダード	プレミアム	ビジネス	ビジネスプロ
ディスク容量		500MB	3GB	10GB	20GB	40GB
利用料金	月額料金	125円※	500円	1,000円	2,500円	4,500円
	初期費用	1,000円	1,000円	1,000円	5,000円	5,000円
マルチドメイン		20個	20個	30個	40個	40個
ウイルスチェック ／ 迷惑メールフィルタ		○	○	○	○	○
無料サポート（フリーコール／メール／サポートサイト）		○	○	○	○	○
Webアプリケーションファイアウォール		-	○	○	○	○
SSL	共有SSL	-	○	○	○	○
	独自SSL	-	-	-	-	○
データベース（MySQL4／MySQL5）		-	1個	1個	2個	3個
複数ユーザでの管理 ／ 複数ユーザでのFTP転送		-	-	-	○	○
メール自動応答 ／ メール振り分け転送		-	-	-	○	○

※月額換算料金で、お支払い方法は年間一括払い（1,500円）のみとなります。

SAKURA Internet

さくらインターネット株式会社
本　社／〒541-0054 大阪府大阪市中央区南本町1-8-14　堺筋本町ビル9F
東京支社／〒160-0023 東京都新宿区西新宿7-20-1 住友不動産西新宿ビル33F
フリーコール 0120-775664 受付時間：平日10:00~18:00（土日・祝祭日を除く）
E-MAIL support@sakura.ad.jp
さくらインターネット Webサイト www.sakura.ad.jp

ICMS-SR0063/JISQ27001:2006 10821461(02)

社団法人 日本ネットワークインフォメーションセンター
〒101-0047 東京都千代田区内神田2丁目3番地4号 国際興業神田ビル6F
Tel 03-5297-2311 Fax 03-5297-2312