World IPv6 Dayありました。

◆ はじめに

技術者というのは新しい技術を実際に見て触って、動かしてみることが大事だなぁと思っていたのですが、実はこれ、技術者に限らずいろいろな分野でも同じではないかと考え始めています。例えば、彼女のお母さんに、「結婚前に一緒に暮らして、きちんとやって行けるかどうかトライアルしてみなさい」とアドバイスされました。IPv6の導入は技術者のみならず、いろんな人が関わってきます。新たな技術の導入という変化を、みんなが注意を払って見ることで、これまでに気が付かなかった視点や課題、利用方法が見えてくるのではないかと思っています。

◆ World IPv6 Dayとは

日本時間の2011年6月8日（水）朝9:00から、主にコンテンツ提供者が24時間のIPv6トライアルを行う「World IPv6 Day」が行われました。World IPv6 Dayは24時間だけWebサイトをIPv6対応にしてみるトライアルイベントです。この取り組みは、IPv4の在庫枯渇がいよいよ差し迫った2010年に企画されました。サイトがIPv6対応した際の影響や課題を明らかにするために、コンテンツ事業者が協調して大規模なトライアルを行うことが計画されたのです。

プロジェクトのWebサイトはInternet Society（ISOC）が協力を申し出て、ホストをしてもらえることになりました。日取りはIANAの在庫が枯渇した後で、みんなが準備できそうな日ということで、6月8日が選ばれました。日本語での情報も欲しいということになったので、専用ページを開設して情報提供をしました。

□ World IPv6 Day
http://isoc.org/wp/worldipv6day/

□ 日本でのWorld IPv6 Day
http://www.attn.jp/worldipv6day/

この取り組みに賛同した他のコンテンツ事業者やWebサイト管理者が、次々に参加者リストへ名を連ねていきました。しかしここで少し残念なのが、既に何年も前にIPv6対応を終わらせて、日常的に運用している人達でした。既に対応を終えているために、当初は参加者リストに名を載せるわけにもいかず、何だか楽しそうなイベントをやるのに参加できなかったのです。そのため、このようなサイトは既にIPv6対応済みのサイトとして、日本語のプロジェクトページで紹介することにしました。ついでに言うと、いまだ世の中に大規模なIPv6の利用実績が無く、World IPv6 Dayのようなイベントが、現状ではインパクトのあるイベントだという事実も哀しいのですが。

しかし、せっかくのイベントであるため、いろいろと有意義なものにしたいと考えました。インターネットは広く普及してしまったが故に、さまざまな端末や接続環境があります。無数の組み合わせで問題が無いかを検証していく必要があり、多くの人が検証に携わることで、より多くの環境を調べることができます。事前の調査で分かったのは、IPv6対応サイトへのアクセスで問題が発生する場合もありますが、世界的に見て、どうもそれは特定バージョン、特定環境、特定条件等とても限定的で小さな問題が多い、言わばロングテールの様相を呈しているということでした。つまり誰かがどこかで頑張れば解決するわけではなく、問題のあるそれぞれの環境を直す必要がありそうだということです。

● World IPv6 Dayに関する情報提供を行った筆者作成のWebサイト

◆ 日本におけるIPv6通信の問題点と対策

日本ではNTT東西の提供する光サービスでIPv6閉域網が採用されていることもあり、IPv6→IPv4のフォールバック※1が数多く発生する環境にあります。既に何年も前から知られている事実であり、NTT東西の光サービスではIPv6閉域網側にユーザーからの接続要求があった場合には、フォールバックの速度を速めるためにTCP RSTを返信しています。それでもフォールバックのため1秒程度の時間がかかったり、実装によっては期待したフォールバックを行わない場合もあります。ユーザーにIPv6のインターネット接続が提供できていれば、IPv6でアクセスできるためにこうした問題は発生しないのですが、NTT NGNを利用したIPv6接続サービスはサービス開始が遅れているために、問題が大きくなっています。

では、このような状況下でインターネット接続サービス提供者としてはどのような対策を採る必要があるのでしょうか。

1）IPv6接続の提供
2）ポリシーテーブルの変更推奨（ユーザーサポート）
3）AAAA filter
4）問題ない実装への移行推奨（ユーザーサポート）

1）の「IPv6接続の提供」は、安定したIPv6インターネット接続をユーザーに提供してしまうという方針です。現状ではIPv4/IPv6のデュアルスタック接続を提供するのが妥当です。IPv6対応ということで将来へつながる取り組みになるので、とても前向きです。ただし、6to4等の自動トンネリング技術は品質が悪く、ユーザーへ提供するサービスとしては不適切であるため、できればきちんと品質を担保できる接続サービスを提供することが好ましいです。

2）における「ポリシーテーブル」とは、端末が通信に利用するIPアドレスを選択する際に、参照するルールテーブルです。詳細はRFC3484等を参照してください。IPv6対応の端末であればサポートしているはずです。これを利用すれば、IPv6閉域網からIPv6アドレスが払い出されても、それはIPv6閉域網と通信する時にのみ利用するようになり、不要なフォールバックが発生しなくなります。もちろん、別途インターネット側からIPv6アドレスが割り当てられれば、インターネットにアクセスする際にはそのIPアドレスを利用しますので、悪影響もありません。ただ、ユーザーに端末の設定を変更してもらう必要があります。これを簡単に設定できるツールを提供できるように関係各所と調整を行いました。

http://www.attn.jp/maz/p/i/policy-table/

3）の「AAAA filter」は、インターネット接続サービス提供者が、これら無用なIPv6→IPv4のフォールバックが発生すると分かっているユーザー向けのキャッシュDNSサーバでAAAAレコード、つまりIPv6アドレスを応答しなくする方策です。これにより、ユーザーからIPv6のインターネットを隠し、無用なIPv6→IPv4のフォールバックの発生を避けることができます。BIND9.7以降など、既にこの機能を搭載しているDNS実装もあります。この実装ではAAAAレコードのみ、つまりIPv6のみで提供されているホスト名であればIPv6を応答するため、万が一ユーザー側で独自にIPv6の接続性を確保していた場合には、IPv6のみのサイトにアクセスできます。なお、IPv6での接続サービス向けには、これまで通りのAAAA filterを適用しないキャッシュDNSサーバを維持しなければならないため、サーバ運用の手間は少しかかってしまいます。

4）の「問題ない実装への移行推奨」は、問題があると分かっているソフトウェアのバージョンアップやパッチの適用、他のソフトウェアへの移行をユーザーに推奨するものです。ユーザーには最低限、サイトがIPv6対応してもびっくりして固まってしまわないソフトウェアを利用してもらわないと、今後のインターネット利用が不便になってしまいます。また、できれば新しめのソフトウェアを利用してもらった方が比較的フォールバックの実装が良かったり、セキュリティ上の問題も解消されていたりして良いこともあるのですが、一方でユーザー側にもそのソフトウェアを利用しなければならない理由があるかもしれないため、一概に移行して問題ないと言い切れるわけではないのが難しいところです。

● World IPv6 Day開催を知らせるISOCのWebサイト

◆ World IPv6 Dayを終えて

事前にはさまざまな懸念や心配事がありましたが、当日は想定した程の混乱は無かったように見えました。さまざまな立場で関わったみなさん、あれこれありがとうございました。個人的には、「ふぅ」という安堵とともに、何かもっとうまくやれたんじゃないかという忸怩たる思いがあります。で

もってこの先、注力していかなきゃいけない方向も見えてきたので、静かに頑張ろうって決意しているところです。

World IPv6 Dayに際し、多くの方々が影響を検討し、それによる混乱を最小限に抑えるために議論や検証を重ねました。これまでにもIPv6導入のための検証は行われており、そうした知見も広く共有されました。NTT東西の提供する光サービスで使われているIPv6閉域網のIPv6アドレスがユーザー端末に割り当てられていると、IPv4/IPv6対応したサイトにアクセスする際に、IPv6→IPv4のフォールバックが発生してしまいます。この環境を想定していないアプリケーションでは、接続に問題が出ることが予想されました。全般に古いバージョンに問題があるようで、知見が生かされた最近のバージョンではうまく問題を回避するようになっています。古いバージョンに関してもみんなで開発元に修正をお願いするなどしてきましたが、すべてに修正版が提供される状況ではありませんでした。

各ISPでは、NTT東西の光サービスを利用しているユーザー向けにAAAA filterの準備を進めました。これはIPv6トライアルという観点から見ると主旨に逆行しているようにも見えますが、修正版が提供されない場合がある現状でユーザーを混乱から救うには、しょうがない選択だろうと考えています。弊社（IIJ）でも想定以上の混乱が生じた際に備えて、AAAA filterの事前検証と導入準備は進めておきました。NTT東西は、光サービスで利用しているIPv6閉域網にインターネット向けのTCP SYNが送信された際に、フォールバックを素早く実施できるようにTCP RSTをユーザーに返しています。World IPv6 Dayでは当然このアクセス要求も増加することが予想されたため、TCP RSTを応答する機能の増強をお願いしておきました。

World IPv6 Dayでは日本時間の午前9時にAAAAを設定することになっていました。事前にAAAAレコードを設定しちゃう、おおらかな参加者もいましたが、多くのユーザーが参照するような著名なサイトは概ね予定の時刻通りに設定を行っていたようです。世界のISPや参加者がIRC（Internet Relay Chat）を使って、それぞれの地域でどんな状況かといった情報を交換しながらイベントは進みました。IIJでは特に顧客からの申告も無く推移していたため、AAAAfilterの導入は見送りました。世界的に見ても大きな混乱は無く、むしろDNSに登録するレコードを間違ったり、サーバの設定で問題があったりする場合が多かったです。これらの問題はすぐさまIRCで情報交換され、問題解決に向けて対応されていました。

今回、各ISPにはユーザーからの障害申告はほとんど無かったようですが、ユーザー側で全く問題が無かったわけでもなく、TwitterでIPv6→IPv4フォールバックの影響を受けていると思われるユーザーも散見されました。実は接続に問題のあるユーザーは日常的に相当数いるため、どれほどがWorld IPv6 Dayの影響か分かりません。当日、見つけられる限りコンタクトを試みたところ、そのうち1名の方から、ポリシーテーブルの変更で問題無くアクセスできるようになったと報告がありました。当日はIPv6のトラフィックも増加しました。特に着実に計画を進めてIPv6対応のユーザーを増やしていた接続事業者では、Gbps単位でIPv6のトラフィックが増えたと聞いています。一部コンテンツは当日のトライアルが終了してもAAAAレコードを残したままにしているので、その後もIPv6のトラフィックは以前よりは増えた状況が続いています。

今後、インターネットではIPv6対応のコンテンツやサービスが増えていくでしょう。今回の経験を通じて言えば、今後もユーザーが楽しくインターネットを利用するには、それぞれのユーザーが適切な利用環境を整備することが重要です。例えば、一番お勧めなのはIPv6接続の導入です。知見が生かされた最新版のアプリケーションに更新するのはセキュリティ対策の面からもお勧めです。今年はさまざまな事業者がコンシューマー向けのIPv6接続サービスを提供し始めました。ISPとしては、ユーザーがうまく選べて、適切な接続環境を整えられるようにサービス提供や情報提供を行っていく必要があるだろうなあと考えています。

今回は、IPv6対応する際の問題点を浮き彫りにすることを一つの目的にしていました。この点は文句無く世界的に大成功です。これまでになく多くの環境で検証が行われ、問題点の共有と開発元へのフィードバック、対応策の検討が行われました。関係者の方々による事前の尽力もあって、当日も大きな混乱も無く終えることができました。報告書には載らないでしょうが、あちこちで淡々と頑張ってくれていた方々はいっぱいいます。勝手に心から感謝します。今後も楽しく頑張っていきましょう。

（株式会社インターネットイニシアティブ 松崎吉伸）

※1 IPv6→IPv4のフォールバック
IPv6とIPv4の双方が利用可能な状態（デュアルスタック）の環境において、何らかの要因でIPv6による通信ができない場合に、それを諦めてIPv4での通信に切り替える動作、もしくはその逆の、IPv4での通信からIPv6での通信に切り替える動作を指します。

第81回IETF報告

全体報告

2011年2回目のIETF会合が、7月24日（日）から7月29日（金）の間、カナダのケベックシティにて、RIM（Research In Motion）社のホストで開催されました。市内の旧市街地はユネスコの世界遺産に登録されており、ヨーロッパ風の城郭や建物を眺めることができます。そんな旧市街地を離れ、丘の上の新市街地に会場となったケベック・コンベンション・センターはありました。急な坂の上に位置しているためか、ケベックは坂の多い町という印象を持って帰ってきました。

ここでは、「Operation and Administration Plenary」と「Technical Plenary」の、二つの全体会合についてご報告します。

Operation and Administration Plenaryは、IETFの運用と管理についての報告を中心とした会合で、7月27日（水）に行われました。Operation and Administration Plenaryの中で表彰される、Jon B. Postel Awardは、受賞者が参加できなかったため延期となった旨の報告がありました。IETFチェアであるRuss Housley氏からは、今回のIETF81会合の運営状況について46ヶ国1,057人の参加者があったこと、前回の会合からのアップデートとして五つのWGが活動を終了し、五つのWGが新設され、合計121のWGが現在活動中であることや、149もの文書がRFCとして発行されたことなどが報告されています。

7月25日（月）に行われたTechnical Plenaryは、“Report from World IPv6 Day”と“The Web Privacy Tussle”という二つの技術トピックスでのパネルディスカッションをメインとして、IRTF（Internet Research Task Force）のリサーチ報告、IAB（Internet Architecture Board）の活動報告、RSOC（RFC Series Oversight Committee）の報告など技術系の報告がされました。

IRTFのチェアのLars Eggart氏からは、12のリサーチグループの活動状況報告があり、DTNRG（Delay Tolerant Networking Research Group）の活動が活発でたくさんの文書が提出されている状況が伝えられました。その一方で活動が活性化していないものとして、VNRG（Virtual Network Research Group）やP2PRG（P2P Research Group）が挙げられていました。TMRG（Transport Modeling Research Group）は、ICCRG（Internet Congestion Control Research Group）にマージされることが報告されました。


● 会場となったQuebec Convention Centre（公式Webサイトより引用）

今回からIRTFの活動に貢献し、実際に研究成果を実用化させた人を讃えるApplied Networking Research Prize（ANRPと略するそうです）の授与がされることになりました。1回目の受賞者は、Mattia Rossi氏とBeichuan Zhang氏の2名で、それぞれBGPの研究とトラフィック制御にかかる省電力化に対して評価がされました。賞金500ドルとIETFミーティング参加にかかる費用などが副賞として贈呈されると同時に、会期中に行われるIRTFミーティングへの招待がされ、研究内容に関するスピーチが行われたとのことです。次のIETF82でも表彰を予定しており、ノミネートの受付が開始されています。ノミネートは、IRTFのWebページ（http://irtf.org/anrp/）から行えます。

IABチェアのBernard Aboba氏からは、新しいWebサイト（http://www.iab.org/）の紹介がありました。IABの活動内容もI-Dの形で文書化されますが、沢山の文書が投稿され、RFC化されている状況が報告されました。IABではインターネットの他団体とも連携した活動を行っており、プライバシーや多言語化などのアクティビティの紹介がされました。プライバシーに関する活動の一環で、このプレナリでのパネルディスカッションが企画されています。

RSOCチェアのFred Baker氏からは、RFC文書の発行を行う実務者の活動と予算の管理について、実務者採用基準

の明確化の状況報告がされました。

続く、World IPv6 Dayの開催意義に関するパネルディスカッションでは、Google社、Facebook社、Yahoo!社、Microsoft社などコンテンツサイト側での計測とその分析結果、ユーザーサイドからみたWorld IPv6 Dayの観測結果などが報告されました。このパネルディスカッションでは日本企業からの正式な報告はなかったのですが、Google社の発表の中で、KDDI社のIPv6ネイティブサービスが良いサービス例として取り上げられました。しかしその一方で、KDDI社以外のサービスでは問題も見られたという指摘もされていました。Google社が日本の通信事情に興味を持っているのは、他国に比べるとIPv6接続といってもいろいろな方式が展開されているからなのではないかと思いました。

まとめると、World IPv6 Dayの開催目的の一つであるWebサイトを含む業界内のIPv6対応のモチベーションを上げることに関しては、世界各国から多くの関心が寄せられ、1,000サイトにも上るイベント参加者もあったことが報告されました。3分の2の参加者がイベント後もIPv6対応を継続しており、IPv6のトラフィックも順調に伸びているそうです。IPv6対応サイトが増えることで問題点やDDoS攻撃が増加するという不安がありましたが、そういった観測はなく成功裏に終わったようです。

またIPv6導入に関する問題点として、“Brokenness”と総称して呼ばれる6to4などの移行技術を使ったアクセスの問題点や、OSやブラウザの実装に関する不具合点が指摘されていましたが、イベントの前後で観測される問題数に大きな変化はないようです。むしろ問題点の一部に関しては減ってきている状況という報告がされました。実際Yahoo!へのアクセス全体における“Broken User”は、0.078%から0.022%に落ちたそうです。一般的にWebサイトのIPv6対応は、サイト運営者が個別に進めるものですが、6月8日というターゲットに向けて取り組んでみると、期限があると強い動機づけになること、実験イベントというスタイルであったためユーザーにも説明がしやすかったこと、テストによって準備してきたことが間違っていないことを確かめられたことなどが、今回のイベントのメリットが報告される一方で、世界中に理解を求めることの難しさも挙げられていました。いずれにしても、WebサイトがIPv6対応するにあたって障壁と考えられていたようなことは大きな問題ではないことが分かり、今後はIPv6対応が進むと考えられます。

プライバシーに関するパネルディスカッションでは、3人の専門家から発表がされました。プライバシーの認識と行動の関係をもとにプライバシーに配慮したWebサイトのデザインが可能であることや、実際にどのような原則でWebサイトを構築すると良いか、利用に気をつける技術としてCSSやGeolocationがあること、User Trackingに関して一つのWebサービスの背後にある何十、何百の情報連携の現実など興味深い内容が提示されました。これらを踏まえ、IABのプライバシープログラムの成果として、実装開発やモデル化など研究開発のいろいろな段階で参照できる文書がまとめられます。

次回IETF82は、2011年11月13日（日）から18日（金）にかけて、台湾で開催されます。

（株式会社インテック 廣海緑里）

IPv6関連WG報告

2011年7月24日（日）から7月29日（金）まで、カナダのケベックシティにて第81回IETFミーティングが開催されました。同時期、日本は非常に暑かったとのことですが、ケベックシティは涼しく、過ごしやすい気候でした。

今回の参加人数ですが、46ヶ国より1,057名（新規参加133名）と、プレナリにて発表されています。最近、参加人数は増加傾向だったのですが、今回は減少しています。国別の参加人数内訳では、米国、中国、日本、カナダ、フランスという順番でした。前回に引き続き、日本からの参加者が少なかったように感じられました。

本稿では、IPv6に特化した内容を議論するワーキンググループ（WG）での、会期中における議論内容を中心に紹介します。

● 会合ではWikiによる情報提供も行われています

◆ 6man WG（IPv6 Maintenance WG）

6man WGは、IPv6のプロトコル自体のメンテナンスを実施するWGです。今回は、7月26日（火）の夕刻に開催されました。

まずは、チェアによるアジェンダ確認、および6man WGで取り組み中である以下の文書についてステータス報告がありました。

- IPv6フローラベル仕様に関するドラフト群
  →IESGレビュー中
  draft-ietf-6man-flow-3697bis：
  改版ドラフトが必要とのコメント。
  draft-ietf-6man-flow-{ecmp,update}：
  エリアディレクター（AD）フォローアップ中。

- IPv6ノードの要求仕様改版（draft-ietf-6man-node-req-bis）
  →ADレビュー中、執筆者の対応待ち。

- UDPの0チェックサム（draft-ietf-6man-udpzero）
  →WGラストコールへ。

- UDPチェックサムに関する問題提起
  （draft-ietf-6man-udpchecksums）
  →WGラストコール前に、改版ドラフトが必要とのコメントあり。

- RPL（低電力高損失ネットワーク向けIPv6ルーティングプロトコル）用のデータ転送オプション
  （draft-ietf-6man-rpl-option/draft-ietf-6man-rpl-routing-header）
  →ADレビュー中、改版ドラフトが必要とのコメントあり。

- 回線IDオプション（draft-ietf-6man-lineid）
  →WGラストコール準備完了。後述する、ルータ要請ベースのアクセス制御の問題（draft-dec-6man-rs-access-harmful）ドラフトの議論待ち。

今回は、以下のテーマが議論されました。

- IPv6拡張ヘッダの統一フォーマット
  draft-ietf-6man-exthdr

- 近隣探索におけるIPv6拡張ヘッダに起因するセキュリティ問題
  draft-gont-6man-nd-extension-headers

- RFC3484 IPv6デフォルトアドレス選択機構の更新
  draft-ietf-6man-rfc3484-revise
  draft-ietf-6man-addr-select-opt

- DADプロキシ
  draft-ietf-6man-dad-proxy

- 近隣探索の問題と拡張
  draft-gashinsky-v6nd-enhance

- 近隣到達不可能解析の問題点
  draft-nordmark-6man-impatient-nud

- IPv6近隣探索の省エネルギー対応
  draft-chakrabarti-nordmark-energy-aware-nd

- MS/TPネットワーク上でのIPv6転送
  draft-lynn-6man-6lobac

- ルータ要請ベースのアクセス制御の問題
  draft-dec-6man-rs-access-harmful

これらのトピックスの中から、いくつかをご紹介します。

1．IPv6拡張ヘッダの統一フォーマット
draft-ietf-6man-exthdr

前回に引き続き、議論が続いている、IPv6拡張ヘッダの標準フォーマットを決める提案に関する議論です。WGラストコールのコメントを反映、挙げられた問題点について対応し終えたことについて報告がありました。会場から、IPv6を拡張する場合、終点オプションの利用を強く推奨しているが、経路途中すべての中継点での処理（従来、中継点ごとオプションヘッダ（hop-by-hopoptions header））をしたい場合にはどうするのか、などの質問があり、そのような拡張はこの文書の範囲外であることなどの返答がありました。RFC化に向け、IESGに送ることになりました。

2．近隣探索におけるIPv6拡張ヘッダに起因するセキュリティ問題
draft-gont-6man-nd-extension-headers

近隣探索の際に、拡張ヘッダの利用について明確には考慮されていないため、実装間の不整合、SAVI、RA Guardなどの機能での不具合や、セキュリティ上の問題が発生する可能性がある、という指摘です。解決策として、近隣探索時の拡張ヘッダを禁止するなどが提案されています。会場より、近隣探索のセキュリティ機構であるSEND（SEcure Neighbor Discovery）では、証明書のやりとりのために拡張ヘッダの一つである断片化ヘッダが多用される、との指摘がありました。SENDに関する考察を含めて、ドラフトの詳細化を実施し、メーリングリストで議論を継続することとなりました。

3. RFC3484 IPv6デフォルトアドレス選択の更新
draft-ietf-6man-rfc3484-revise
draft-ietf-6man-addr-select-opt

IPv6ノード、および、通信相手が複数のアドレスを持つ場合に、通信に使うアドレスペアを選択する仕様である、RFC3484に関する改版提案です。RFC3484の改訂については、残りの課題である、サイトローカルアドレスなどの廃止されたアドレス空間の扱い、プライバシー拡張アドレスの扱い、アドレスの有効期限の扱いについて議論を実施、その結果を反映したドラフトでWGラストコールを実施することになりました。アドレス選択のDHCPオプションについては、dhc WGにレビューを依頼、その後にWGラストコールを実施することになりました。

今回のWGでは、IPv6の各種機能（近隣探索、近隣到達不可能解析など）に関する実利用上の問題点の指摘と、解決策の提案が多く実施されました。実際に、IPv6が利用され始めていることを受けてのことだと思われます。

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

□ 第81回 IETF 6man WGのアジェンダ
http://www.ietf.org/proceedings/81/agenda/6man.html

◆ v6ops WG（IPv6 Operations WG）

v6opsは、IPv6に関するオペレーション技術、および、共存・移行技術に関する議論を実施するWGです。今回も、合計24件と議題が非常に多く、当初は7月26日（火）午前、28日（木）午後2コマの計3コマで議論する予定でしたが、直前になって29日（金）に2コマ追加され、合計5コマでの実施となりました。参加者も非常に多く、26日（火）、28日（木）のセッションではそれぞれ200名程度が参加していたと思います。

前回、チェアより、ミーティング内でアジェンダとして取り上げる議題を厳選する提案が挙がっていましたが、結局のところ、今回は提案議題をほぼすべて議論するような形になっていたようです。議論を有効にするために、v6opsミーティング自体とは別に、提案内容について個別にチェアに相談する時間・部屋が用意されていました。実際に幾人かが相談に行っていました。

● Jabber、WebEx、Meetechoなどを使ってリモート参加ができるWGもあります

今回、当初のアジェンダは、

1. World IPv6 Dayセッション
2. Old Businessセッション
3. New Ideasセッション

という形で構成されていましたが、議論時間を多く取るために、追加された29日（金）のセッションにアイテムを回す調整が実施されました。「28日（木）のセッションでの発表の場合には1人3分の持ち時間だが、29日（金）に回ればより多くの時間を割り当てる」という形での募集で、アジェンダの順番がいくつか入れ替わりました。しかしながら実際のところ、29日（金）のv6opsセッションは参加者も半減し、それほど議論も活発には実施されませんでした。

以下では、議論されたいくつかのトピックについて、簡単に紹介します。

1）World IPv6 Dayセッション

「World IPv6 Day」は2011年6月8日（水）に実施されたイベントで、この日に多くのWebサイトがIPv6化されました。終了後、元通りIPv4のみに戻したサイトがほとんどでしたが、いくつかのサイトは継続してIPv6対応をしています。

今回の会議におけるv6opsの当セッションでは、実際にIPv6対応した組織からの状況報告や、World IPv6 Day当日のトラフィックなどの様子を観測した結果が報告されました。自社のサーバをIPv6対応にしたマイクロソフト社では、実際にIPv6でアクセスしてきたユーザーは非常に少なかったこと（0.5%程度）、IPv6によるアクセスの9割方はネイティブIPv6でのアクセスであったこと、7%のユーザーがWindows XPを利用していることなどが報告されました。特に、Windows XPのユーザーが多かったことは、Windows XPでは意識的にインストールしないとIPv6に対応しないため、驚くべき数値だとのコメントがありました。概ね問題点はなかったとのことですが、IPv6ではIPアドレスによる位置情報検索サービスがサードパーティーより提供されていないことを課題の一つとして挙げていました。その他、RIPE NCC、Hurricane Electric社、Comcast社などが報告を実施しています。このセッションとは別に、25日（月）夜に実施されたテクニカルプレナリでもWorld IPv6 Dayセッションが開催されており、こちらでは、Google社、Facebook社、Yahoo!社などが報告を実施しています。

報告の後、関連議題として、以下が議論されました。これらは、継続的に議論になっているアイテムでもあります。

2）World IPv6 Day参加招集（World IPv6 Day Call to Arms）について
draft-chown-v6ops-call-to-arms

World IPv6 Dayに向けて有用な内容でしたが、終了後、RFC化は必要ないと著者が判断したようです。内容を他のドラフトにて取り込むとのことです。

3）Happy Eyeballs：デュアルスタックホストにおいて通信を成功させるために
draft-ietf-v6ops-happy-eyeballs

Happy Eyeballsの仕様について、メーリングリストの議論を反映し、アルゴリズムの詳細を削除、要求条件に絞ったとの著者からの報告があり、賛同の意見がありました。Happy Eyeballsに類似する仕組みは、現在、ChromeやFirefoxの最新版に実装されているそうです。

4）DNSホワイトリストによるIPv6 AAAAの返答
draft-ietf-v6ops-v6-aaaa-whitelisting-implications

IESGからのコメントを受け、改版したことに対する著者からの意見照会がありました。DNSのホワイトリスティングは推奨すべきでない、という立場から、このドラフトをRFC化すべきかどうかも議論になりました。改版後、dnsop WGに意見照会をする予定です。

5）6to4を「歴史的」ステータスに変更する提案
draft-ietf-v6ops-6to4-to-historic

6to4を廃止したときの影響について、議論がありました。製品に関してはあまりインパクトはないこと、廃止に関する広告の範囲（6to4リレーのオペレーター向けなど）について、議論がありました。

6）IPv6のカスタマーエッジルータに対する高度な要件
draft-ietf-v6ops-ipv6-cpe-router-bis

RFC化されたカスタマーエッジルータに対する要件として、追加すべき高度な要件に関する議論です。PCP（Port Contorol Protocol）を、要件として取り込むことに関する議論や、今回から、新たに組織されたhomenet WGとのすみ分けが主な議論になりました。homenet WGの様子を見ながら、議論を進めることになっています。

□ v6ops WG
http://datatracker.ietf.org/wg/v6ops/charter/

□ 第81回IETF v6ops WGのアジェンダ
http://www.ietf.org/proceedings/81/agenda/v6ops.html

（NTT情報流通プラットフォーム研究所 藤崎智宏）

セキュリティ関連WG報告 ～KRB-WG、SAAG、暗号アルゴリズムの危殆化対応の動向について～

第81回IETFは、カナダのケベックシティにて、2011年7月24日（日）から7月29日（金）の期間に開催されました。IETFでは、インターネットに関するさまざまな議論が行われ、情報セキュリティに関する議論もその中に含まれます。IETFには、セキュリティに関係するWGとして、13のWGが存在しています。今回のIETF会合では、13WGのうち11WGのミーティングが開催され、さらにBoF（Birds of a Feather）として、CICM（Common Interface to Cryptographic Modules）とWOES（Web Object Encryption and Signing）が開催されたため、計13のセキュリティに関するセッションが開催されました。

このように、セキュリティ関連のWGが扱う領域は多岐にわたります。今回の報告でも、毎回お伝えしている認証や、セキュア通信に特化した内容を議論するWGである、KRB-WG（Kerberos WG）の動向を報告します。また、それら二つのWGの報告に加え、セキュリティ全般に関して横断的にディスカッションを行うSAAG（Security Area Advisory Group）において、現在アメリカ国立標準技術研究所（NIST; National Institute of Standards and Technology）が選

定を行っている、SHA-3※1に関する発表がありましたので報告します。その上で、今後重要な問題であると考えられている、暗号アルゴリズムの危殆化対応※2（暗号アルゴリズムの世代交代）に関するメールが、会期中にCFRGのメーリングリスト（ML）に投稿されましたので、それについても報告します。

● IRTFのWebサイトではApplied Networking Research Prizeのノミネートを受け付けています

◆ KRB-WG（Kerberos WG）

KRB-WGは、マサチューセッツ工科大学（MIT）が考案した認証方式の一つである、Kerberosプロトコルに関する新規仕様や機能拡張について、検討を行うWGです。このミーティングは、2011年7月28日（木）の午前9時から2時間半程度開催され、参加者は30人程度でした。

ミーティングの構成として、以下のような議題で進行されました。なお、このWGがKerberosに関するものであるためか、MIT Kerberos Consortium（http://www.kerberos.org/）のメンバーたちが主導的に議論を行っていました。

1）ドキュメントステータスおよび確認
2）技術的な議論
3）可能性のある新規項目

この三つの議題について、議論のポイントを報告します。

1）ドキュメントステータスおよび確認

前回の会合から今回の会合までの期間にRFCとして発行されたドキュメントは、4本あったことが報告されました。そのドキュメントのカテゴリーの内訳は、Standards Trackが3本、Informationalが1本でした。

- RFC 6111 Additional Kerberos Naming Constraints
  - この規約は、よく知られているKerberosに関するprincipal nameとrealm nameについてのname constraintsを定義しています。

- RFC 6112 Anonymity Support for Kerberos
  - この規約は、identityやKerberos realm以上の情報を暴くことなく、Kerberosアプリケーションサービスで安全に通信するための拡張を定義しています。

- RFC 6113 A Generalized Framework for Kerberos Pre-Authentication
  - この規約は、Kerberos事前認証に関して、より形式的なモデルを記述したものです。

- RFC 6251 Using Kerberos Version 5 over the Transport Layer Security（TLS）Protocol
  - この規約は、TLS通信を用いたKerberosクライアントとKey Distribution Centers（KDCs）との間での、通信について記述しています。

また、WG itemとして扱われている9本のドキュメントについて、ステータスの報告がありました。その中で個人的に興味を持ったドキュメントは、Deprecate DES support for Kerberos（draft-lha-des-die-die-die-05）です。このドキュメントは、危殆化した暗号アルゴリズムであるDESの利用を廃止することを目的にしています。この危殆化アルゴリズムであるDESは、Kerberos V5で利用可能な暗号アルゴリズムの一つとして定義されているので、仕様として利用できる状況になっています。ドキュメントの状況としては、Expireしてしまっている状況でありますが、暗号アルゴリズムの危殆化対策の観点からも、危殆化した暗号アルゴリズムを、標準化活動において無効化するための対応としての、ケーススタディとして重要なものと位置づけられると考えられるため、更新版の投稿が望まれていると思われます。

2）技術的な議論

技術的な議論の対象として扱われたのは、次の二つのドキュメントについてです。

- A Generalized PAC for Kerberos V5（draft-sorce-krbwg-general-pac-02）
  - このドキュメントは、Keberos V5における汎用的な認証の仕組みを記述することを目的としています。

- Kerberos number registry to IANA（draft-lha-krb-wg-some-numbers-to-iana-00）
  - このドキュメントは、Kerberosプロトコルを定義する多くの数値について整理し、それらの管理をIANAに移管することを目的としています。

ここでは、A Generalized PAC for Kerberos V5について、議論の要点および今後の方針を報告します。この議題は、krb-wgのMLに投稿されたコメント※3をベースに議論が行われました。コメントは、一般的なものから仕様に踏み込んだものまで多岐にわたっており、それぞれのコメントについて議論を行った結果を、次版のドキュメントに反映することで、WG itemとして採択されました。今後の課題として、さまざまなサービス間での相互運用性を実現するために、fieldの記述を詳細化することが求められています。

3）可能性のある新規項目

KRB-WGとしてWG itemにするかどうか検討するために、Camellia Encryption for Kerberos 5（draft-hudson-krbwg-camellia-cts-02）に関する議論が行われました。このドキュメントは、Kerberos V5における利用可能な暗号アルゴリズムとしてCamelliaの追加およびチェックサムとしてCipher-based MAC（CMAC）を追加することを目的としています。これまでKerberosで仕様化されていないアルゴリズムのため、WGの将来的な議論として取り上げられています。

議論の流れとしては、AES以外の共通鍵暗号として追加される暗号アルゴリズムの安全性に関する議論（例えば、暗号に関する研究成果など）や、新たに暗号アルゴリズムを追加した際に、さらに暗号アルゴリズムの追加要望が出るのではないか？ などについても議論されました。

なお、enc-typeの追加に関しては、新たにCamelliaをKerberos V5に追加するかどうかを、2010年3月から議論を行っていますが、ミーティング参加者における賛同者は増加しています。WG itemとしてCamelliaに関するDraftの採択に関しては、KRB-WG Chairが検討することになり、次回以降のミーティングで決定されるものと考えられます。

□ KRB-WG
http://datatracker.ietf.org/wg/krb-wg/charter/

□ 第81回IETF KRB WGのアジェンダ
http://www.ietf.org/proceedings/81/agenda/krb-wg.html

◆ SAAG（Security Area Advisory Group）

SAAGでは、IETFにおけるSecurity Areaの総括やセキュリティ全般に関した横断的な議論が行われ、Security Areaの各WGやBoF、セキュリティが関係するWG等の確認が行われます。また、招待講演で勉強会も開催されるため、Security Areaの横断的な状況や、注目のトピックスについて情報を得たい場合に有意義な場です。このミーティングは、2011年7月28日（木）の午後1時から2時間程度開催され、多くのセキュリティ関係者が参加していました。

今回のトピックスは以下の通りです。ここでは、SHA-3に関する報告を行います。

- IETFにおけるプロトコルや実装でのSHA-3のサポート
- 安全保護のためのIdentifier Comparison
- IEEE 802.15における鍵管理プロトコル

今回のミーティングでSHA-3に関する報告された点は次の通りです。

- IETFで標準化されたプロトコルに対するインパクト
  - プロトコルとしてハッシュ関数が代替可能であるならば、SHA-2からSHA-3への乗り換えが容易に行える
  - しかしながら、SHA-2に対応していない場合、SHA-3への移行についてはバッファサイズなどの検討が必要かもしれない

- NISTとしては、SHA-3決定後にSHA-2を取りやめたり、SHA-3を推すことはなく、SHA-2とSHA-3を共存させる

- 今後のSHA-3に関するスケジュール
  - 2012年3月22日 Final SHA-3 Candidate Conference
  - 2012年夏 最終選考結果をアナウンス
  IETFとしては、最終選考結果を受けて標準化を実施可能

なお、このSHA-3に関する詳しい情報を確認したい場合は、次の発表資料をご覧ください。

http://www.ietf.org/proceedings/81/slides/saag-3.pdf

また、Security AreaのWGの動向については、WGとしての役割を終えて、DKIM（Domain Keys Identified Mail）、MSEC（Multicast Security）、ISMS（Integrated Security Model for SNMP）がクローズされる予定です。WGとして扱う新規検討項目が発生しなかった場合、IPSECME（IP Security Maintenance and Extensions）は、2012年2月にクローズされると報告されていました。

□ 第81回IETF SAAGのアジェンダ
http://www.ietf.org/proceedings/81/slides/saag-0.pdf

◆ 暗号アルゴリズムの危殆化対応（暗号アルゴリズムの世代交代）に関する最新動向

会期中、CFRG（Crypto Forum Research Group）のMLに、IETFに存在するInternet-Draftに関して、危殆化した暗号アルゴリズムであるMD5を利用しているものを抽出したリストが共有されました※4。このメールは、更新されたMD5に関するSecurity ConsiderationsのRFC※5を参照することを勧めることで、ハッシュ関数の正しい利用を推進することを目的としています。Security Areaが中心となって、IETFにおける暗号アルゴリズムの危殆化対策を行っていることを、垣間見ることができる一例だと思います。

● 新しくなったIABのWebサイト

◆ 最後に

インターネットの標準化活動に触れる機会としては、台湾（台北）で開催が予定されている、次回の会合が大きなチャンスだと考えられます。今後のIETFにおいては、これ以降アジア地域での開催がしばらく予定されていません。なお、会合の開催日程は2011年11月13日（日）から11月18日（金）です。インターネットの標準化活動に興味がある方は、ぜひ参加を考えてみてはどうでしょうか？

（NTTソフトウェア株式会社 菅野哲）

※1 Hash Competition
http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

※2 暗号アルゴリズムの危殆化
簡単に言えば、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指します。詳しくは次のURLをご覧ください。
JPNIC Newsletter No.44 インターネット10分講座
「暗号アルゴリズムの危殆化」
http://www.nic.ad.jp/ja/newsletter/No44/0800.html

※3 Comments on adopting draft-sorce-krbwg-general-pad as a work item
https://lists.anl.gov/pipermail/ietf-krb-wg/2011-July/009342.html

※4 meeting at IETF 81 to discuss review of MD5 uses,
http://www.ietf.org/mail-archive/web/cfrg/current/msg03012.html

※5 Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms,
http://tools.ietf.org/rfc/rfc6151.txt

DNS関連WG報告

2011年7月24日（日）から7月29日（金）まで開催された第81回IETFケベックシティ会合のうち、本稿では、DNSに関連した内容を議論するワーキンググループ（WG）である、dnsop WG（Domain Name System Operations WG）と、dnsext WG（DNS Extensions WG）における議論の様子をご紹介します。

◆ dnsop WG報告

今回のDNS WGの会合では、主に現状のドラフトの確認と、AS112ならびにDNSSEC鍵更新に関する議論が行われました。

まず、Internet-Draftの確認に関しては、draft-ietf-dnsop-dnsesec-dps-framework、draft-ietf-dnsop-dnssec-key-timingについてIETFラストコールを行うことが確認されました。また、draft-ietf-dnsop-respsizeについては、2年前にWGラストコールが行われたまま放置されていたため、次回IETFまでに再度WGラストコールを行うことが確認されました。WGドラフトに関しては、主要なものは既にRFCになっており、DNSSECに関するいくつかのドラフトが残っているのみという状態に見えます。そのため、会場での議論も落ち着た雰囲気で行われている印象を受けました。

● ホストによる第81回IETFのWebサイト

新たな話題としては、draft-michaelson-as112-ipv6ならびにdraft-sotomayor-as112-ipv4-cullに関する発表と議論がありました。draft-michaelson-as112-ipv6とdraft-sotomayor-as112-ipv4-cullは、共にAS112のネームサーバにおいて、逆引きゾーンを追加する提案を行ったドラフトですが、追加する内容が異なります。

draft-michaelson-as112-ipv6は、AS112のネームサーバにおいて、IPv6のリンクローカルアドレスや、未定義アドレスについての逆引きゾーンも提供することを提案したドラフトです。どの逆引きゾーンを提供するかに関していくつかコメントが出されましたが、提案自体に関しては特に反論も無く、AS112の運用者たちの意見を集めて連携を取っていくことが重要、との認識が確認されました。

draft-sotomayor-as112-ipv4-cullは、AS112が提供しているIPv4逆引きゾーンに、さらにいくつかの逆引きゾーンを追加する提案を行ったドラフトです。IPv4 loopbackネットワークや、IPv4 Testネットワーク、ブロードキャストネットワークに関する逆引きゾーンの追加です。このドラフトに関しても、大きな反対意見は無く、AS112運用者と連携して、新たなゾーンの追加を行う必要があることが確認されました。

次に、draft-mekking-dnsop-dnssec-key-timing-bisに関する議論が行われました。このドラフトは、draft-ietf-dnsop-dnssec-key-timingを更新する目的で提案されたものであり、アルゴリズム変更を含めた鍵更新の手続きに関して述べられたものです。複雑なことを述べ過ぎているという意見や、アルゴリズム変更を含めた鍵更新は当然必要なのだから、bis（別名のドラフト）ではなく元のドラフトに含めた方がいいといった意見が出されました。結果として、まだ元のドラフトがRFCになっていないので、そちらを先にRFCにすべきだという意見が多く出されました。

最後に、dnsop WGの今後について話し合いが持たれました。WGドラフトも少なくなってきたため、WGを解散することも含めて方向性を問う議論が行われました。このWGは運用的な問題を扱うため、プロトコルの現実性についてのチェックや性能に関する評価についてまだ行うことがあるのではという意見や、他のWGでDNSに関連するものを扱っていくべきという意見が出されました。しかし、WGを継続する大きな原動力は今のところ見つからないため、現在のドラフトや新しいドラフトの提案状況を見て今後を考える、という認識がなされました。

◆ dnsext WG報告

dnsext WGは、今回のIETF81において会合を開催しませんでした。そのため、メーリングリストにて行われた議論を中心に、前回のIETFから今回までにあった動きに関して報告します。主に、次のドラフトに関する議論が行われました。

- draft-ietf-dnsext-ecdsa
- draft-ietf-dnsext-dnssec-algo-signal
- draft-ietf-dnsext-rfc2672bis-dname
- draft-ietf-dnsext-dnssec-algo-signal
- draft-eastlake-dnsext-xnamercode
- draft-ietf-dnsext-dnssec-registry-fixes
- draft-ah-dnsext-rfc1995bis-ixfr
- draft-ietf-dnsext-rfc2671bis-edns0
- draft-ietf-dnsext-dnssec-bis-updates

これらのうち、draft-ietf-dnsext-ecdsa、draft-ietf-dnsext-dnssec-algo-signal、draft-ietf-dnsext-rfc2671bis-edns0、draft-eastlake-dnsext-xnamercodeはWGラストコールが行われ、メーリングリスト（ML）上にてコメントが寄せられていました。RFCとなるためには、まだ更新が繰り返されると思われます。

一方、draft-ietf-dnsext-rfc2672bis-dnameは24版まで更新されているため、ほぼコメントも出尽くした感があります。近くRFCになると思われます。

MLでの議論は、主に既存のドラフトの更新やコメントに関する投稿が主であり、新しい提案等は行われませんでした。そのため、直接顔を合わせて話し合うべき問題が存在せず、会合が開催されませんでした。

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