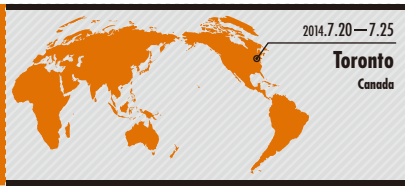
第90回IETF報告



全体会議報告

2014年7月20日(日)から25日(金)まで、第90回IETFミーティングがカナダで開催されました。オンタリオ湖、北西のトロントにある、フェアモント・ロイヤルヨークホテルが会場です。本稿では、このIETFミーティングのレポートをお届けします。

◆ 開催規模

第90回IETFミーティングの参加人数は、1,175名でした※1。ここ数回と大きくは変わらず、日本からの参加人数は、以前のように具体的な数字が公表されていないものの、IETFチェアの報告資料では、100名前後で推移しているようです。ワーキンググループ(WG)のリスト※2にあるWG議長の中には、日本人の名前が見られますので、日本人はミーティングに参加しているだけではなく、IETFにおける活動の中で活躍されていることがわかります。

IETFには、120ほどのWGがあります。WGでは、技術の仕様や課題に関する検討結果などを、RFCとして取りまとめて公開するための活動が行われています。RFCの編集を行うグループであるRFCエディターによると、2006年以降、RFCが公開された数は毎年300前後とされています。2014年は、7月の時点でRFC化に向けて提出された文書が200ほどと多く、想定されていた作業量を超えています※3。

◆ ジョン・ポステル賞

今回は、2014年のジョン・ポステル賞の発表があるIETFミーティングでした。今年のジョン・ポステル賞は、ネパールにおける無線LANのネットワーク敷設に尽力した、Mahabir Pun氏に贈られました※4。

● 今年のジョン・ポステル賞はMahabir Pun氏が受賞しました

◆ 第90回IETFのBoFに見られる新たな活動

IETFでは、新たな技術や議題が出てきた時や、WGを作成する必要があるかどうかがわからない状態の時には、Birds of a Feather(BoF)というミーティングが開かれて議論されることがあります。IETFにおいて、新たに立ち上がりつつある活動の動向を見ていくには、BoFのミーティングに参加するのが手っ取り早いと言えます。BoFの中には、発案者を中心として少人数で行われる非公式のBoFもあり、正しい数はわからないながらも、今回のIETFでは10ほどのBoFが開かれました※5。ここでは、そのうちのいくつかを紹介します。

○UCAN(Use Cases for Autonomic Networking)
ネットワークの設定や最適化、障害からの復旧といった運用が、自動的に行われる自動ネットワーク(Automatic Networking)の技術に関するBoFです。その用語や概念は、IRTFのNetwork Management Research Group(NMRG)で検討されてきました。

Autonomic Networking - Definitions and Design Goals
http://tools.ietf.org/html/draft-irtf-nmrg-autonomic-network-definitions
BoF開催の背景となる文書
- Autonomic Networking - Definitions and Design Goals
  http://tools.ietf.org/html/draft-irtf-nmrg-autonomic-network-definitions-02

○TCPINC(TCP Increased Security)
TCPの拡張(extensions)を利用して、TCPで転送されるデータを暗号化したり、その完全性を確認できるようにする技術のBoFです。第88回IETFミーティングで大きく取り上げられた、大規模なネットワークの盗聴(pervasive monitoring)への対策技術として位置付けられています。

BoF開催の背景となる文書
- Gap Analysis for Autonomic Networking
  http://tools.ietf.org/html/draft-irtf-nmrg-an-gap-analysis-00

※1 IETF 90 Administrative Plenary, IETF 90
http://www.ietf.org/proceedings/90/slides/slides-90-iesg-opsplenary-7.pdf
※2 Active IETF Working Groups
http://datatracker.ietf.org/wg/
※3 RFC Editor Report, IETF 90
http://www.ietf.org/proceedings/90/slides/slides-90-iesg-opsplenary-0.pdf
※4 Mahabir Pun Receives 2014 Jonathan B. Postel Service Award
http://www.internetsociety.org/news/mahabir-pun-receives-2014-jonathan-b-postel-service-award

○IANAPLAN（IANA Plan）
米国商務省電気通信情報局（National Telecommunications and Information Administration：NTIA）の発表したIANA機能の監督権限移管について、IETFにおける対応を検討するためのBoFです。IANA機能について言及されているRFCの更新が必要なことがわかっており、WG設立の方向になっています。

メーリングリストの情報
- http://www.iab.org/mailman/listinfo/internetgovtech

○VNFPOOL（Virtual Network Function Pool）
ファイアウォールやロードバランサーといった、ネットワーク機能を仮想化するVirtualized Network Function（VNF）を使ったネットワークにおいて、ソフトウェア障害などに対する信頼性を向上させる仕組みを検討しているグループのBoFです。第89回IETFミーティングでもBoFが開かれていました。WG設立の方向で検討されているようです。

WG設置前のWebページ
- https://datatracker.ietf.org/wg/vnfpool/charter/

これらの他に、BoFのWikiには下記のBoFに関する最新情報が掲載されています。

Birds of a Feather Meetings（IETF Pre-WG Efforts）
http://trac.tools.ietf.org/bof/trac/wiki/WikiStart
- Application Enabled Collaborative Network（AECON）
- Transport Independent OAM in Multi-Layer network Entity（TIME）
- Network Function Virtualisation Configuration（NFVCon）
- Abstraction and Control of Transport Networks（ACTN）
- Delay Tolerant Networking Working Group（DTNWG）
- Transport Services（TAPS）
- Application-based Policy for Network Functions（APONF）
- RFC Format Update（RFCFORMAT）

◆ IETFの活動のための、ネットワークやアプリケーションの活用

IETFチェアのレポートによると、Webページ「http://www.ietf.org/」の、コンテンツ・デリバリー・ネットワーク（CDN）を使った提供が始まりました。その結果、東京からアクセスした時のページの読み込み時間は、3.2秒から0.8秒に短縮されたとのことです。

IETFミーティングでは、SNSやさまざまなツールも活用されています。Twitterアカウント@IETF※6では、#IETFというハッシュタグで全体会議（プレナリー）のアナウンスや中継の情報などが流されています。#IETF90というハッシュタグは1,186ツイートで使われ、新たにフォロワーが578増えました。技術に関する全体会議（テクニカル・プレナリー）は、YouTubeで中継されており、301アクセスがありました。なお、初めて中継が行われて、“Hardening The Internet”というセッションが話題となった第88回IETFミーティングのテクニカル・プレナリーは、11,000回以上再生されたと報告されていますが、それ以降は300ほどであるようです。

2011年頃からAppleのApp Storeで配布されている「IETFers※7」は、iPhone用アプリケーションで、PCを広げなくてもWGのミーティングの参加に必要な発表資料などが閲覧できるようになっています。

◆ テクニカルトピック ～ネットワーク・トポロジーと地理的な情報～

技術に関する全体会議であるテクニカル・プレナリーでは、最新のホットな話題や技術的なインターネットの仕組みのあり方が議論できるような話題が、テクニカルトピックとしてプレゼンテーションされます。今回のトピックは、「Network topology and geography（ネットワーク・トポロジーと地理的な情報）」と題して、三つのプレゼンテーションが行われました。

○IXmaps.ca
カナダでIX（Internet Exchange）の位置情報を可視化している、IXmapsプロジェクトの紹介です。データセンターにあるルータの位置情報を、オペレーターの協力の下に集積して、Google Mapsなどを使って可視化しています。カナダの国際トラフィックはアメリカ国内を通ることがわかっており、アメリカ国家安全保障局（NSA）による通信傍受の対象となっているかどうかを調べられるといった用途の紹介もありました。

○Internet Exchange Point（IXP） - Global Development Work
IXPの設置についての情報提供など、国際的に協力してIXPの発展を支えている、ISOCのWebサイト「IXP Toolkit&Portal」の紹介です。

- IXP Toolkit
  http://www.internetsociety.org/ixptoolkitguide
- IXP Portal
  http://www.ixptoolkit.org

○CAIDA Tools, Data and Research on Internet Topology and Geography
カリフォルニア大学にある、インターネットトラフィックの分析を行っているグループのCAIDA（Center for Applied Internet Data Analysis）による、地理的な情報を含めた計測プロジェクトArchipelagoの紹介です。小型で安価なコンピューターであるRaspberry Piを使って、計測ノードを実現しています。

- Archipelago Measurement Infrastructure
  http://www.caida.org/projects/ark/

会場では、「利用者の観点では、地理的な場所よりもIXPがどれほど混んでいるのか、すなわち、トラフィック量に興味を持たれるのではないか」「発展途上国では、IXPの遅延やコストを知るために、（地理的な計測は）効率的だと思う」といったコメントが寄せられていました。

◇　　◇　　◇

次回の第91回IETFミーティングは、2014年11月9日から14日まで、アメリカ合衆国ハワイ州オアフ島、ホノルルで行われます。

（JPNIC 技術部／インターネット推進部 木村泰司）

IPv6関連WG報告

第90回IETFのWorking Group（WG）のうち、筆者が会合に参加したIPv6に関連するWGの中からv6ops WGとhomenet WGについて、主な議論の概要をご紹介したいと思います。なお、今回のIETFでは、6man WG（IPv6 Maintenance WG）は開催されませんでした。

◆ v6ops WG（IPv6 Operations WG）

v6ops WGは、IPv6を全世界に展開するにあたっての緊急の課題、特に運用上の課題に対処することに焦点を当てたWGです。また、新しいネットワークや既存のIPv4ネットワークにIPv6を導入するためのガイドラインや、IPv4/IPv6共存ネットワークの運用ガイドラインを作成することも目的としています。

今回のv6ops WGでは、2014年7月17日（木）～18日（金）に香川県高松市で開催された、JANOG34で行われたIPv6 ULA（Unique Local Address）に関する実験※1の結果について、NTTコミュニケーションズ株式会社の小原泰弘氏が発表を行いました。

IPv6 ULA（fc00::/7）は、IPv4におけるプライベートアドレス※2に相当するアドレスです。ただし、下記2点のような違いがあり、IPv4におけるプライベートアドレスと完全に一致しているわけではありません。

- IPv6では一つのIFがULA（Unique Local Address）とGUA（Global Unicast Address）の両方のアドレスを持てる点
- ランダムに生成することが推奨されている40bitのフィールドをprefixに含んでいることから、実質上はグローバルにユニークであることが期待されている点

当初、IPv6におけるプライベートネットワーク用としてはsite-local addresses（fec0::/10）が予約されていましたが、定義が曖昧だったことから非推奨となり、代わりにIPv6 ULAが、2005年にRFC4193※3において定義されました。

IPv6 ULAの利用シーンとしてさまざまな構成が考えられるため、それぞれの構成の利点と欠点を明確にするためのドラフト（draft-ietf-v6ops-ula-usage-recommendations-02）が提出されており、v6ops WGのメーリングリスト（ML）では、このドラフトについて現在も活発に議論がされています。

JANOG34では、ドラフトに記載されている利用シーンのうち、以下の二つのシチュエーションを構築して実験を行いました。

- ULA along with GUA: IPv6 ULA + GUAで構成したネットワーク（IPv4アドレスはあり）。IPv6サイトへはGUA（またはULA+NPTv6）、IPv4サイトへはNAT44で通信を行う。
- ULA-only Deployment: IPv6 ULAのみで構成したネットワーク（IPv4アドレスは無し）。IPv6サイトへはNPTv6、IPv4サイトへはNAT64/DNS64で通信を行う。

前者のケースでは、さまざまなアプリケーションで通信にまったく問題が無かったこと、ソースアドレスとしてULAを選択した通信が発生しなかったこと（Neighbor DiscoveryとmDNS通信を除く）が報告されました。また、後者のケースでも、IPv4アドレスが無いと動作しないSkypeを除き、ほとんどのアプリケーションで問題が無かったことが報告されました。

会場からは、実験内容の詳細について尋ねる質問が多かったですが、マイクに立った質問者全員が、コメントの冒頭で、貴重な実験結果を共有したことに対しての感謝の意を述べていました。

今回の実験では、ほとんどの場合で通信に影響が無いという良好な結果でしたが、アプリケーションに依存して、または、端末のソースアドレスセレクションのルールに依存して、通信への影響が発生することが想定されるため、「次はもっとア

※5 IETF-90 BoFs
http://www.ietf.org/blog/2014/06/ietf-90-bofs/
※6 @IETF on Twitter
https://twitter.com/ietf
※7 IETFers
http://www.itunes.com/app/ietfers
※1 JANOG34 Meeting - ネットワーク
http://www.janog.gr.jp/meeting/janog34/network/
※2 RFC1918“Address Allocation for Private Internets”
http://tools.ietf.org/rfc/rfc1918.txt
※3 RFC4193“Unique Local IPv6 Unicast Addresses”
http://tools.ietf.org/rfc/rfc4193.txt

プリケーションと端末のバリエーションを増やして実験をして欲しい」というコメントが、大勢を占めていました。

今回の発表は、JANOG34の会場ネットワークでULAに関する実験を発案した、シスコシステムズ合同会社の土屋師子生氏が、v6ops WGのMLに実験内容について投稿したことがきっかけで実現しました。IETFでは現在、IETFの上位組織であるISOC（Internet Society）におけるDeploy360※4という取り組みの中で、運用者の意見をプロトコルの標準化に積極的に取り込んでいこうという試み「Operators And The IETF」※5を行っています。日本の運用者の意見が集約されるJANOGから、IETFの場に意見をインプットしていくことは非常に重要であり、今後も継続していくべきと感じました。

v6ops WGでは他にも、次のような注目すべき発表が行われました。

- DHCPv6/SLAAC Address Configuration Interaction Problem Statement（DHCPv6/SLAACアドレス構成対応問題に関するステートメント）
（draft-ietf-v6ops-dhcpv6-slaac-problem）

JPNIC News & Views vol.1153※6で「DHCPv6/SLAACアドレス構成対応問題」として取り上げられているので、詳細はこちらをご参照ください。今回の進捗としては、文章の細かい修正を経て、内容に技術的な間違いが無いことが確認されたため、WGLC（Last Call）をすべきかの採決が行われ、賛成多数となりました。

- Close encounters of the ICMP type 2 kind（near misses with ICMPv6 PTB）（ICMP type2 パケットとの遭遇（ICMPv6 Packet-Too-Big パケットのニアミス問題））
（draft-jaeggli-v6ops-pmtud-ecmp-problem）

ロードバランサやAnycastを用いている環境で、サーバからサイズの大きいパケットを送った際に、ICMPv6 type 2"Packet Too Big"（PTB）メッセージ応答が、元のサーバに返らない問題をドラフト化したものです。Fastly社のJoel Jaeggli氏が発表を行いましたが、この問題は日本国内では既に指摘されている事象です。特定の状況で起こる事象ですが、v6ops WGとして解決すべき問題という位置付けとするかどうかの採決が行われ、賛成が多い結果となりました。今後、WGドラフトとなるための協力を求むとして、発表は終わりました。ちなみに、この一風変わったドラフトタイトルは、「未知との遭遇」（原題:Close Encounters of the Third Kind）をもじったものです。

- Power consumption due to IPv6 multicast on WiFi devices（Wi-Fiデバイスにおける IPv6マルチキャストパケットによる電池消費）
（draft-desmouceaux-ipv6-mcast-wifi-power-usage）

IPv6のWi-Fiに接続した時に、マルチキャストパケットによって端末の電池の消耗が早くなってしまう可能性について、実測した結果について述べた発表です。同じ発表が、intarea WG（Internet Area WG）においても行われました。実験結果から、IPv6のWi-Fiネットワークに所属しただけで、少なくとも4パケット、可能性としては20パケット以上のマルチキャストパケットが発生するなど、興味深い知見が得られています。v6ops WGの反応としては、電池の消耗を比較するのであれば、他の場合と慎重に比較すべきだ、との意見がありました。

- IPv4 Address Literal in URL（URLにおけるIPv4アドレス表記）
（draft-osamu-v6ops-ipv4-literal-in-url）

NAT64/DNS64環境においては、通常では"http://192.0.2.10/index.html"のような、IPv4リテラル表記が含まれるURLを持つIPv4サイトには到達することができません。これは、IPv4アドレスをマッピングしたIPv6アドレスを通じて、外部のIPv4サイトと接続する必要があるためです。このようなIPv6マッピングアドレスを得るために、「<ipv4-address-literal>.TLD」をDNSに登録（あるいはホストに登録）する手法について、奈良先端科学技術大学院大学の櫨山寛章氏が発表を行いました。また、IPv4リテラルに自動的にsuffixを付与し、名前として解釈するGoogle Chromeのplug-inを開発し、問題なく動作したことが紹介されました。

チェアであるFred Baker氏は、このことは解決すべき問題であると会場に対し表明し、賛同を得ました。しかし、TLD（Top Level Domain）を使うアプローチであることから、他の実装との干渉を心配する会場の声も多く、標準化にあたっては注意深く手順を踏んで欲しいという意見が、参加者から複数ありました。

◆ homenet WG

homenet WGは、家庭内が複数のセグメントに分かれ、複数の上流ISPを持つ（来るべき）状況を想定し、ルーティング（Interior Gateway Protocol; IGP）、アドレス選択、DNSキャッシュサーバ選択、セキュリティ、境界検出（border discovery）、それらの自動設定に関する問題の解決を目的としたWGです。

今回は、ルーティングプロトコルをどのように標準化するかについて、時間を20分取ってじっくりと議論が行われました。チェアの1人であるMark Townsley氏のスライドにおいて、IETF 89で示された三つの方向性についての再確認が行われました。

1）ルーティングプロトコル無しで実装する（HNCP（Home Networking Control Protocol）フォールバックを用いる）
2）一つのルーティングプロトコルを選択する（OSPF（Open Shortest Path First）、IS-IS（Intermediate System to Intermediate System）、etc..）
3）二つ以上のルーティングプロトコルを選択する

これまでの議論をまとめると、1）、2）に対しては賛成多数であるが、3）に対しては賛成少数という状況です。チェアは、ルーティングプロトコルを一つに絞りきれなければ、Coin-flip（コイントス）による決定も考えていると表明しました。会場からは、1）と2）の意見が半々といった状況でした。既存のルーティングプロトコルに依存せずに1）で進めたい意見がある一方、1）では結局homenet WGで新しいルーティングプロトコルを生み出すことが必要となり、難しいのではないかという反対派もおり、結局何も決まらないままタイムアップとなってしまいました。

続いて、IS-IS Implementation Reportでは、ルーティングプロトコルとしてIS-ISを用いたhomenetの実装（送信元/先のアドレスの組を用いたルーティング）の報告が行われました。現在、homenetにおいて利用可能なルーティングプロトコルとして、IS-IS、OSPF、Babelの三つの実装が存在することとなりました。

その他、下記を含む多岐にわたる提案が、十分な議論の時間が取れないまま大量に行われました。最終日である金曜日の午前に行われたため、一部参加者のフライトスケジュールに配慮した都合によって、時間を巻いて行われたという側面もあります。

- 上流ISPから割り当てられたアドレスを、自動的にhomenet内の複数セグメントにfloodingする方法の提案（draft-pfister-homenet-prefix-assignment）
- homenet内のノードの名前解決をインターネット上のサードパーティーDNSにアウトソースする方法の提案（draft-mglt-homenet-front-end-naming-delegation）
- homenetに適したPCP（Port Control Protocol） proxyの実装の提案（draft-stenberg-homenet-minimalist-pcp-proxy-00）など

homenet WGは、家庭内に小規模なマルチホームネットワークを丸ごと作ることを課題設定としているため、必然的に他のエリアやWGに関わる提案が多くなります。ルーティングエリアとのコンフリクトを懸念したり、チェアや参加者から他のWGでも議論するよう求められたりと、標準化における難しいプロセスを、これから先、いくつもクリアしていく必要がありそうです。

（NTTコミュニケーションズ株式会社 西塚要）


● 会場となったFairmont Royal York

暗号技術に関する動向

第88回IETF※1で大きく注目された「Pervasive Surveillance（大規模な盗聴行為）」を受けて、IETF参加者の間で暗号技術への注目が集まっています。暗号技術の議論が、セキュリティエリアのWG以外でも行われているため、本稿では、セキュリティエリアのWGかどうかにこだわらずに取り上げ、最新の動向を報告したいと思います。第90回IETFのさまざまなセッションで議論された、楕円曲線に関する話題や、共通鍵暗号アルゴリズムの動向を取り上げます。

◆ 新しい楕円曲線の選定

第88回IETFのプレナリーでPervasive Surveillanceが取り上げられて以降、IETFでは、インターネットで標準的に使われる暗号をどう決めていくべきか、具体的には多くの候補の中からどういうプロセスを踏んで選んでいくべきなのかが、重要な論点になってきています。プロセスが不透明であると、国家によって盗聴可能な暗号がインターネットの標準の中に入れ込まれるのではないか、といった懸念も挙げられています。

Webブラウザなどで利用されている鍵交換アルゴリズムである、ECDH（Elliptic Curve Diffie-Hellman key exchange）などで利用されている楕円曲線として、米国国立標準技術研究所（National Institute of Standards and Technology; NIST）が規定している楕円曲線（以降、NIST曲線とする）が有名です。しかし、楕円曲線のパラメータを決定するプロセスが不透明などの理由で、NIST曲線への懸念を持っている人たちを中心に、NIST曲線

※4 Deploy360 Programme
http://www.internetsociety.org/deploy360/
※5 Operators And The IETF
http://www.internetsociety.org/deploy360/projects/operators-and-the-ietf/
※6 JPNIC News & Views vol.1153「第88回IETF報告［第2弾］IPv6関連WG報告 ～6man WG、v6ops WGについて～」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1153.html
※1 JPNIC News & Views vol.1152「第88回IETF報告 [第1弾] 全体会議報告」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2013/vol1152.html

以外をIETFとして選択しようという動きを受けて、2013年後半から徐々に議論が継続して行われています。

今回のIETFで行われた議論の中から、次に示す二つの項目について、情報を共有します。

1. 新しい楕円曲線を選定する上での要件

TLS（Transport Layer Security）WGは、Webなどで使われているSSL/TLSの標準化を行っているWGです。SSL/TLSで使われる暗号もTLS WGで決定されます。インターネットに関連する技術やプロトコルを中長期的な観点で研究を推進している、IRTF（Internet Research Task Force）にある暗号のグループであるCFRG（Crypto Forum Research Group）では、新しい楕円曲線を選定する際の要件を検討してほしいというTLS WGからの要請を受けて、

・NUMS Curves（Nothing Up My Sleeve Curves - バックドアのない楕円曲線）
・高速化が期待できるCurve25519、Curve41417、E-512といった楕円曲線に関する提案
・楕円曲線の基本的な安全性に関する考え方

に関する発表がありました。

これらの議論を受けて、TLS WGへの回答としてCFRG co-chairから、安全な楕円曲線が満たすべき要件が示されました。その要件は以下の通りです。

・暗号装置の動作状況をさまざまな物理的手段で観察することにより、装置内部のセンシティブな情報を取得しようとする攻撃である、サイドチャネル攻撃に対する耐性があること
・必須ではないが、Twist securityを有することが望ましい
・ECDHE、ECDSA（Elliptic Curve Digital Signature Algorithm）などの、楕円曲線暗号である既存のアルゴリズムをサポートできること
・信頼できる曲線の決定プロセスに基づいて選択された楕円曲線であること
・楕円曲線の形式について、Weierstrassのみの形式ではなく、その他の形式（Montgomery/Edwards/twisted Edwards）へ切り替え可能なこと

□ 楕円曲線関連の発表資料
- Deterministic Generation of Elliptic Curves（NUMS Curves）の発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-cfrg-5.pdf
- Curve25519、Curve41417、E-521の発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-cfrg-4.pdf
- Elliptic-curve cryptographyの発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-cfrg-3.pdf
- CFRG reporting back to TLS WG
http://www.ietf.org/proceedings/90/slides/slides-90-tls-6.pdf

2. TLSプロトコルにおける楕円曲線の取り扱い

現在、TLSプロトコルで楕円曲線暗号の利用を規定している、RFC4492※2があります。このRFCのステータスがInformationalではあるものの、現状の利用状況を踏まえてStandards TrackでのRFCを発行し、今後利用するTLSプロトコルでの、実装が必須であることを意味するMandatory To Implement（MTI）としてのCiphersuite※3の中に、楕円曲線暗号を加えることについてコンセンサスが取られました。

□ 楕円曲線関連の発表資料
- ECC to Standards Trackの発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-tls-3.pdf

◆ 新しい共通鍵暗号アルゴリズムの検討

現在のIETFでは、ChaCha20というストリーム暗号アルゴリズムと、使い捨て認証符号（One-time Message Authentication Code）であるPoly1305を組み合わせて、AEAD（Authenticated Encryption with Associated Data）を構成する暗号技術が提案されています。今回のIETFでは、CFRG、TLS WG、UTA（Using TLS in Applications）WGで、ChaCha20+Poly1305に関して提案されており、CFRGやTLS WGにおいて提案者から、ChaCha20+Poly1305は、以下のような利点があるとアピールされていました。

・OMAP 4460やSnapDragon S4 Proといった、タブレットやスマートフォンに搭載されているモバイル向けCPUにおいて、AES-GCMと比較してパフォーマンスが3倍程度優れている
・サイドチャネル攻撃の一種である、タイミング攻撃に対する対策が容易である

上記に示した利点や、Google ChromeおよびGoogle社の運用するサーバにおいて実装され、稼働していることがアピールされており、TLSプロトコルやIPsecプロトコルで、ChaCha20+Poly1305を利用するための標準化活動が精力的に行われているので、今後の動向に注目が必要だと思います。

□ TLS WGにおけるChaCha20+Poly1305の発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-tls-2.pdf

※2 RFC4492"Elliptic Curve Cryptography（ECC）Cipher Suites for Transport Layer Security（TLS）"
http://www.ietf.org/rfc/rfc4492.txt

※3 Ciphersuite
SSL/TLSプロトコルで使用される、鍵交換、暗号化、メッセージ認証符号のそれぞれのアルゴリズムの組み合わせ

□ CFRGにおけるChaCha20+Poly1305の発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-cfrg-0.pdf

◆ Pervasive Surveillance（大規模な盗聴行為）への技術的なアプローチ

大規模な盗聴行為への対策技術として、TLSプロトコルなどを用いたエンドツーエンドの暗号化や、「（Perfect）Forward Secrecy」といった、秘密鍵の情報が漏えいしたとしても、影響範囲をその鍵が利用されたセッションだけに限定する技術が検討されています。大規模な盗聴行為が行われると、暗号化された通信データを逐次解読することはできなくても、蓄積された通信データを解析することで、将来解読されてしまうリスクがあると言われているためです。

今回のIETFから、新たにTCPINC（TCP Increased Security）WGという、TCP通信のデータ暗号化や完全性を提供するための、TCP拡張を検討する会合が開催されました。このWGは、多くのTCP通信が暗号化されていないため大規模な盗聴行為に対して対策されていないところに注目し、TCP通信の暗号化をするということが検討されました。実現されると、今後の大規模な盗聴行為に対して、大きな効果を持つ技術になることが予想されます。以下に、tcpcryptの目的などを含めた発表資料のリンクを示しますので、参照いただけたらと思います。

□ tcpcryptの発表資料
http://www.ietf.org/proceedings/90/slides/slides-90-tcpinc-2.pdf

◇　◇　◇

最後になりますが、今後のIETFにおいて、暗号技術を用いたプロトコルが多く検討され、重要性が今以上に増加することが予想されます。このような状況において、プロトコル自体の仕様を策定する段階で脆弱性を排除する手法などを検討する必要が、今後は出てくることが予想されます。最近の事例を挙げれば、暗号プロトコルとして広く利用されているSSL/TLSにおいて、仕様に起因する脆弱性が発見されて、実社会に与える影響が大きかったことからも、RFCの発行前に暗号プロトコルの安全性を評価する取り組みは、必要だと感じています。

（NTTソフトウェア株式会社 菅野哲）


● IETF90の様子

DNS関連WG報告

本稿では、IETF 90におけるDNS関連の動きとして、dnsop WG、dane WG、dnssd WGの概要を報告します。dane WGについては、今回初めて取り上げています。

◆ dnsop WG（Domain Name System Operations WG）

dnsop WGの会合は、7月22日（火）の午前中に開催されました。今回は多くの議題があり、時間いっぱい議論が行われ、まず、I-D（Internet Draft）の状態確認が行われました。

draft-ietf-dnsop-dnssec-key-timingについての報告が行われ、一つ前の版である、03版が公開されたのが2年前であり、今回久しぶりに更新されて04版として公開されました。2012年8月にWGラストコールまでは行われていましたが、その後何も動きがなく今日に至っていました。多くの編集が行われましたが、中身は基本的に変わりはなく、再度WGラストコールを行うことが確認されました。

次に、draft-ietf-dnsop-dnssec-roadblock-avoidanceに関する議論が行われました。このI-Dは、DNSSECを導入するにあたって、障害となるインフラ上やネットワーク上の問題点に関して、注意事項を述べた文章となっています。ファイアウォールやブロードバンドルータなどのミドルボックス、EDNS0や最大UDPパケットサイズによるパケットフラグメント問題等、DNSSECを導入する際に起こりがちな問題について述べています。問題発見とともに、どう対処するかの議論が行われ、少し発散気味になりました。

今回、最も長い時間をとって議論されたのが、Root DNSサーバの分散に関する議題です。draft-wkumari-dnsop-dist-rootとdraft-lee-dnsop-scalingrootがこの議題に関連する発表でした。

draft-wkumari-dnsop-dist-rootは、Recursive DNSサーバにRoot zoneのキャッシュを持たせることで、Root DNSサーバに不必要な問い合わせが行くことを防ぎ、Root DNSサーバの規模性を確保しようという提案です。また、キャッシュとして保持するRoot zoneはDNSSECで署名されているため、リソースレコードの偽装はできないからRecursive DNSサーバがキャッシュを

保持しても問題ない、という主張です。

次に、draft-lee-dnsop-scalingrootは、現在13あるRoot DNSサーバそのものを増やそうというものです。IPv4 UDPメッセージの最大サイズである512バイトは、IPv6が普及するにつれ問題にならなくなるため、IPv6パケットのMinimum MTUである1280バイトから考えれば、20個のRoot DNSサーバアドレスをUDP 1パケット中に入れることができる、という試算です。そして新たに追加するアドレスはすべてエニーキャストアドレスとして扱えば、より多くのRoot DNSサーバを世界中に展開できるという提案でした。

その他にも、draft-mekking-dnsop-kasp、draft-fujiwara-dnsop-poisoning-measures、draft-howard-dnsop-ip6rdns、draft-jabley-multicast-ptrの発表が行われました。Root DNS分散の議論が終わった時点で、会合の残り時間が少なくなっていたため、議論はメーリングリストに持ち越されました。

◆ dane WG
(DNS-based Authentication of Named Entities WG)

daneは、DNS-based Authentication of Named Entitiesの略で、2011年3月のIETF 80から活動を開始しているWGとなります。アプリケーションやトランスポートレイヤーが認証や暗号化に用いる証明書に関連する情報を、DNSを用いて配布する仕組みを標準化するためのWGです。本IETF DNS関連WG紹介で取り上げるのは初めてですが、最近活発に議論が行われているWGとなっています。

今回のIETF 90では、このdaneについても、7月22日（火）の夕方に、2時間の会合が開催されました。まず始めに、SRVレコードとSMTP通信へのDANE TLSA DNSレコードの適用に関する、I-Dの状況確認が行われました。I-Dとしては、draft-ietf-dane-srv、draft-ietf-dane-smtp-with-daneとなります。どちらもWGラストコールに入る前の修正段階であることが確認されました。

次に、OpenPGPとS/MIMEへのDANE TLSA DNSレコードの適用に関するI-Dの状況が確認されました。draft-ietf-dane-openpgp、draft-ietf-dane-openpgpkey-usage、draft-ietf-dane-smimeの三つのI-Dとなります。実際の普及や使用例も含めた文章となっているため、その辺りを増強するとともに、文章をまとめるかどうかの議論がなされました。引き続きメーリングリストで議論が行われます。

さらに、DANEbis and operational guidance（draft-ietf-dane-ops）に関する発表と議論が行われました。DANEとPKIX（Public Key Infrastructure WG）との関連性や使い分け、RFC6698（The DNA-Based Authentication of Named Entities Transport Layer Security Protocol : TLSA）の更新に関する議論が主であり、PKIXとDANEの管理モデルの違いやそれぞれの使い分け、もしくはPKIXにDANEを付加的に用いる方法等が議論されていました。

他にも、TLSA Raw Keys（draft-ietf-dane-rawkeys）に関する議論が行われました。これは、TLSAリソースレコードに直接公開鍵を入れてしまう手法を提案したものです。これによって、アプリケーションやプロトコル毎にTLSAをどう使うかを定義せずとも、利用することが可能になります。この提案に関しては、TLS以外の用途にも適用可能なので、TLSAとは別のレコードにした方が良いのではないか等の議論が行われました。

◆ dnssd WG
(Extensions for Scalable DNS Service Discovery WG)

dnssd WGの会合は、7月24日（木）の午後に開催されました。まず、draft-ietf-dnssd-requirementsに関する議論が行われました。WGラストコールが完了し、寄せられた質問やコメントに基づく回答が行われました。VPNを用いた場合のサービス発見等、WGチャーターにも関連する部分の指摘があり、引き続き改訂が行われる模様です。

次に、draft-rafiee-dnssd-mdns-threatmodelに関する議論が行われました。dnssdを用いた場合のセキュリティ的な懸念に関して述べた文章であり、requirements文章とは別に作成されることが確認されました。

さらに、ULAs for scaling DNS-SDに関する議論が行われました。DNS-SDに用いるアドレスにIPv6 ULAを用いることで、ファイアウォールの設定もしやすくなるため、セキュリティの向上やPrivacy Extensionによるグローバル IPv6アドレス変更にも対応できるという提案です。IPv6のみの対応となるため、引き続きメーリングリストでの議論となりました。

他にも、draft-cheshire-dnssd-hybridに関する議論が行われました。オンリンクでのサービス発見に用いられているMulticast DNSの名前解決を、通常の名前解決に用いられているUnicast DNSがProxy動作することで、外部からも解決できるようにするという提案です。実際に動く実装の提案として、WGドラフトとして引き続き議論していくことが合意されました。

（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）

● Bits-N-Bitesの様子

IGFイスタンブール会合（IGF 2014）報告およびMAGによるプログラム選定について

Internet Governance Forum（IGF）は、インターネットガバナンスに関する対話の場として2006年から毎年開催されている、国際連合主催の会議です。誰でもが自由に参加でき、今年2014年は9月2日（火）から5日（金）の4日間、トルコのイスタンブールにて開催されました。本稿では、前村昌紀からIGFイスタンブール会合の様子をご紹介します。また、会合の報告に先立ち、IGFのプログラムの選考を行うMultistakeholder Advisory Group（MAG）によってどのようにIGFのプログラムが選ばれているのか、2014年のMAGメンバーに選ばれた奥谷泉から、その選考過程についても詳しくご紹介したいと思います。

IGFの特徴とイスタンブール会合のプログラムについて

◆ IGFとは

IGFの正式名称は、Internet Governance Forumです。国際連合主催の会合で、その名の通り、インターネットガバナンスに関する課題について、参加者間で議論を行うカンファレンスです。

大きな特徴は、誰もが自由に参加できることで、IGFは何らかの決定を行う場ではないとし、対話を重視している点です。つまり、インターネットに関与する、異なる立場のステークホルダー（政府関係者、技術者、学者、市民社会、企業など）に対して、相互対話の場を与えるものとして設定し、政策の策定や執行が必要な場合は、IGFでの検討を経た上で、それぞれのステークホルダーの権能に従って行われるものとしています。

2006年の第1回からこれまでに至る、IGFの詳しい経緯に興味のある方は、「インターネットガバナンスとは何か」※1をご覧ください。

◆ MAGによるプログラムの選考

プログラムの選考は、MAG（Multistakeholder Advisory Group、マルチステークホルダーの立場でアドバイスをするグループ）が行います。MAGは、ステークホルダーグループ（政府、学術、市民社会、企業、技術コミュニティ）や性別、地域などのバランスを考慮して国連事務局により選任され、約50名のメンバーにより構成されています※2。 筆者も、ISOC（Internet Society）の推薦を受け、技術コミュニティーのメンバーとしてこのMAGに参画しています。

MAGの中で、存在感を示しているのは米国です。国別では最多となる7名のメンバーが選出されており、Google社、Microsoft社といった企業や、米国商務省電気通信情報局（NTIA）のベテラン担当官が参加し、官民ともにコミットしていることが感じられます。

今年は合計208件の応募があり、これを約半数までに絞るようMAGメンバーが選考を行いました※3。選定基準は内容だけではなく、途上国からの応募、初応募といった要素も加味された上で採点されます。地域別に見ると、東アジアは相対的に応募数が少ない中、中国が今回積極的に提案を提出し、一部のMAGメンバーの中で着目されていました。

プログラムの検討にあたり、MAGでの議論を知りたい場合、MAGメンバー以外でも状況が追えるようになっています。例えば、対面でのMAG会議では、オンサイト・リモートいずれの方法で誰もが参加し、コメントを行うことが可能です。ただし、プログラムの選定はMAGメンバーのみが行います。また、メーリングリストのアーカイブと会議記録も、誰もが参照できるようにIGFのWebサイトで公開※4されています。

◆ プログラムの見どころ

セッションの目的に応じて、セッションの検討と選定方法が異なり、内容も多様なセッションが開催されることは、IGFのプログラムの特徴でもあります。

MAGメンバーが、サブテーマに基づき企画するメインセッションは、今年のインターネットガバナンスにおける主な課題と、異なる立場からの意見を確認する上で、お勧めです。前項で紹介した通り、公募に基づき選定されるワークショップは、多くの場合、メインセッションよりも、応募者の視点で個々の課題に踏み込んで議論をするので、特に興味があるトピックスがあれば、議論を聴いたり、意見を述べやすいのではないかと思います。

※1 インターネットガバナンスとは何か
https://www.nic.ad.jp/ja/governance/about.html

※2 About the MAG
http://www.intgovforum.org/cms/magabout

※3 応募されたセッションと選考結果
http://www.intgovforum.org/cms/147-igf-2014/1851-igf-2014-workshop-status

※4 MAGのメーリングリスト
http://mail.intgovforum.org/pipermail/igfmaglist_intgovforum.org/

メインセッションの中で、特に今年らしいものは、以下の3セッションです。

・IANA機能の監督権限移管
  - NTIAの発表を受け、IGFでも議論
・ネットワークの中立性（Network Neutrality）
  - NETmundialでは結論が出ませんでしたが、重要なトピックとしてIGFのメインセッションとして採択
・インターネットガバナンスの今後のあり方・IGFの役割
  - WSISから10年が経過し、その成果の見直しが進められている中、IGFの継続や改善も含めて、継続課題にどう取り組んでいくべきかを議論

また、今年の新たな試みとして開催される「Best Practices Forum」は、MAGで検討したそれぞれのテーマごとの最適事例を紹介し、文書化するというセッションでした。事前に、テーマごとにメーリングリストで議論をし、関心のあるトピックがあれば、適切な事例が反映されるよう議論に参加することが重要になってきます。トピックスとしては、詳細は次項で説明しますが、ネットワーク運用にも関わりのあるテーマも挙げられました※5。

◆ IGFの改善に向けた取り組み：議論の文書化・関係者への配布

IGFの改善に向けたMAGでの議論を踏まえ、議長のJanis Karklins氏が提示した取り組みを、簡単にご紹介します。

◇ Best Practices Forumの開催

次の五つのトピックスにおいて開催、各セッションのまとめを文書化して配布物とし、これにより実践的な参考情報を提供することをめざしました。

1.マルチステークホルダーによる意義のある参加メカニズムの構築
2.spam等望まれていない通信への規制や回避策
3.コンピュータ緊急対応チーム（Computer Emergency Response Team; CERT）の設立と支援
4.ローカルコンテンツの策定を実現するための環境
5.オンライン上での児童保護における最適な事例

トピックスごとに最適な事例の公募を経て、IGFでのセッションの議論と併せて、外部の専門家が文書の取りまとめを実施しました。トピックスごとのメーリングリストは、誰でも参加登録が可能であり、IGF開催後も継続して運用されています※6。

◇ IGFの有効事例の募集

MAG議長の名の下で、有益な政策や取り組みにつながった事例を募集し、取りまとめた結果がIGFで発表されました。

◇ IGFでの議論結果の取りまとめと改善への取り組み

今回のIGFでは、メインセッションのテーマにおける設問、合意事項、合意されなかった事項をまとめ、結果をより明確な形で提示することになりました。議長より、Way Forwardとして推奨をまとめ、地域や国レベルのrIGFやnational IGFにも参考として共有される予定です。また、地域・国レベルでの取り組みを翌年のグローバルIGFで共有することも検討されています。

◇ 議論結果の能動的な共有

イスタンブール会合における議論の結果は、政府間組織（IGO）、非政府間国際機構（INGO）、I*（アイスター）等の技術コミュニティの団体、主な市民社会団体などへ共有されます。そのために、それぞれのコミュニティへの周知を依頼することになりました。

基本的には、主なセッションでの議論を文書に取りまとめ、さまざまな立場の関係機関に配布することで、それぞれの立場から、対策を検討する上での参考としてもらえることを、念頭に置いています。

なお、今回のIGFは終了しましたが、Best Practices Forumについては、引き続き議論のためのメーリングリストが運用されています。アーカイブも参照できますので、興味のあるトピックスがありましたら、ご覧になってみてください。

（JPNIC インターネット推進部／IP事業部 奥谷泉）

● IGFイスタンブールにおけるBest Practice Forumの一つ。右から2番目が筆者

※5 Draft Programme（執筆時は基本構成のみ公開、公募セッション未掲載）
http://www.igf2014.org.tr/programme.html

※6 IGF2014Best Practices Forums
http://www.intgovforum.org/cms/open-call-to-join-igf-best-practices-forums-preparatory-process

※7 IGF 2014 Chair's Summary
http://www.intgovforum.org/cms/documents/igf-meeting/igf-2014-istanbul/246-chairs-summary-igf-2014/file

IGFイスタンブール会合（IGF 2014）報告

◆ IGF 2014の概要

IGF 2014の会場は、Lutfi Kirdar International Conference and Exhibition Center（ICEC）というところでした。イスタンブール市内で、アジアとヨーロッパを隔てるボスポラス海峡のヨーロッパ側にある丘の上に位置し、会場入り口からはボスポラス海峡の向こうにアジア側を見渡すことができる、眺めの良い場所でした。既にWebで入手できる速報版の会議報告書※7（前ページ）によると、会場での参加者は2,374名とのことです。世界各地からさまざまな関係者が集まるため、会場の中は、服装や肌の色がさまざまで、まさに、世界の多様性を体現した場だという印象を受けました。

今年は、「Connecting Continents for Enhanced Multistakeholder Internet Governance（マルチステークホルダーによる協力の拡張に向けて大陸をつなげる）」が、メインテーマとして選ばれました。これには、インターネットガバナンスについて、議論が行われているさまざまな場をつなげていく、という意味合いが込められています。

メインホールの他に、10を数えるワークショップルームが設定され、同時並行で会議が進み、参加者は自身の関心に合わせて、参加するセッションを選びました。メインホールでは、前述のMAGが設定したサブテーマに沿ったメインセッションが行われました。メインセッションは、テーマに関して見識があるパネリストがホール前方にコの字に配置された席に着席し、後方を埋め尽くす参加者とパネリスト席の間にはセッションモデレータが立ち、会場からの意見も取り入れながら進んでいきました。今年のサブテーマは、以下の八つです。

- アクセスライン政策
- コンテンツの制作・配布・利用
- 成長と発展のためのインターネット
- IGFとインターネットエコシステムの未来
- デジタルコミュニケーションにおける信頼の強化
- インターネットと人権
- 重要インターネット資源
- 最新課題

また、これ以外に、インターネットの諸課題への対処に関する実践例をドキュメントに残すことを目的とする前述のBPF、諸団体の活動をIGFの場でオープンに話し合うOpen Forumなどが開催されました。また、開会式の前日となる月曜日には、Day 0として、関連イベントが催されました。

◆ IGF 2014の特徴

IGF 2014の特徴は、例年よりもアウトプットを重視している点です。

IGFは、対話を重視し、交渉の場としないことから決議を採らないとしていますが、これに対して、「IGFは言いっ放しで終わっている」、「課題への具体的な成果につながらない」、といった批判を一部から受けてきました。

今年2014年は、世界情報社会サミット（WSIS）の開催から10年を経て、その成果を振り返る「WSIS+10」※8や、インターネットガバナンスにおける原則を文書化したNETmundial※9が開催されたこともあり、IGFに対して、より具体的なアウトプットへの期待が、一部の関係者から寄せられています。IGFのプログラム検討を行っているMAGにおいても、IGFの成果をもっと具体的に見せる改善の必要性が、多くのメンバーから表明されています。

このような背景から、今年は、対話を重視するIGFの特性は維持しながらも、議論の内容を具体的に提示し、政府間組織（IGO）、非政府間国際機構（INGO）、I*（アイスター）諸団体※10、企業や市民社会を代表する団体など、各関係者の立場から活動する各種機関に対して、文書として配布する取り組みが、いくつか行われます。

● プレナリホール。トルコの大臣が登壇中

◆ NETmundialの振り返り

NETmundialは、2014年4月にブラジル・サンパウロで開催されたイベントで、正式名称は「今後のインターネットガバナンスに関するグローバルマルチステークホルダー会合（Global Multistakeholder Meeting on the Future of Internet Governance）」です。インターネットガバナンスの原則とロードマップに関す

※8 WSIS+10 High-Level Event Outcomes
http://www.itu.int/wsis/review/2014.html

※9 NETmundial（ネットムンディアル）とは
https://www.nic.ad.jp/ja/basics/terms/NETmundial.html

※10 I*（アイスター）
インターネットの技術基盤の調整に責任を持つ諸団体です。

※11 JPNIC News & Views vol.1196「NETmundial報告」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2014/vol1196.html

る成果文書を作成することを目的に開催されました。詳しくはJPNIC News & Views vol.1196の、特集「NETmundial報告」をご覧ください※11(前ページ)。

Day 0では、「NETmundial: Looking Back, Learning Lessons and Mapping the Road Ahead」と題された振り返りイベントが終日開催され、いろいろな角度からNETmundialを振り返り、今後のインターネットガバナンスにどう活かすのかに関して話し合われました※12。

NETmundialは、多方面からの参照に堪えうる成果文書の内容とともに、その取りまとめのプロセスが、マルチステークホルダーによる合意形成の好例として、各所で高く評価されています。このセッションでは、肯定的な部分に対しても更なる分析がなされ、ネットワーク中立性のように意見が対立する課題の扱い方や、成果文書作成プロセスにおける問題点など、否定的な部分にも議論が及び、4ヶ月前となる成果に対して冷静な振り返りがなされたのが印象的でした。

◆ Best Practices Forum(BPF)

一方、IGFは、チュニスアジェンダ※13において「拘束力を持たない対話の場」と定められており、前回会合までは、議長によるミーティングレポートを除いて、合意文書の類いが作成されたことはありませんでした。この点に関して、課題解決への寄与が少ないのではないかとして、何らかの対処を求める声もありました。このような声に対応したのが前述の「IGFの改善に向けた取り組み」で紹介したBPFです。

BPFの多くは、スパム対策やCERT設立など、極めて実践的な内容でしたが、「マルチステークホルダーによる意義のある参加メカニズムの構築」というテーマに関しては、実践というより体制論の意味合いが強い印象でした。具体的な実践例にとどまらない、考え方や方針を含むものが文書として残ることになると、今までのIGFの「対話の場」としての性質を変えていくことにもなりかねず、今後の動向に注意が必要です。

◆ その他

IANA機能の監督権限移管、ICANNの説明責任強化など、基盤運営の領域においても、体制論に関する検討が進みつつあり、これらに関するセッションも持たれました。体制の検討においては、「マルチステークホルダーモデルの固持」「対等な立場での参加」といった原則論が叫ばれる一方で、議論のための議論に陥らず、課題に有効に対応していく実践性も重要で、しばしば原則論と実践性は対立します。今回のIGFでは、このような考え方が対立する議論においても、相手の考え方を理解し、その上で自分の考え方を上手に表現して主張しているな、と感じることが度々ありました。今回が9回目のIGFとなりますが、年を経て、議論の仕方が進歩している印象を受けます。

◆ 2015年の年限延長に向けて

IGFは、2006年に5年の活動年限によって始められ、現在は2011年に延長された年限の4年目にあたり、来年、再び年限延長を検討する段階にあります。IGFが対話の場に徹するあまり、成果が少ないのではという懸念も聞かれる一方で、参加している政府からはIGFの年限延長を支持する発言が目立ちました。

◆ 最後に

IGFは、各国政府を含むあらゆるインターネットの関係者が集まる場所で、その動きは、ITU(国際電気通信連合)をはじめとする国連の会議体にも影響を及ぼし得ます。JPNICでは、引き続き奥谷がMAGメンバーとしてこれに関わることをはじめとして、情報収集と適切な対応を進めて参ります。これらに関しては、Webやメールマガジンなどで適宜お知らせいたします。

また、国内において情報交換・議論を行う場として、「日本インターネットガバナンス会議(IGCJ)」が発足し、定期的に会合を開催しています。各会合の資料およびレポートはWebで公開しています。参加者間で情報共有を行うメーリングリストも設置されていますので、ぜひご登録ください。このIGCJの会合でも、IGFに関する情報は適宜ご紹介してまいります。

日本インターネットガバナンス会議(IGCJ)
https://www.nic.ad.jp/ja/materials/igconf/

日本インターネットガバナンス会議(IGCJ)のメーリングリスト
https://www.nic.ad.jp/ja/governance/igconf/mailing-list.html

(JPNIC インターネット推進部 前村昌紀)

● メインホールの様子

※12 IGF 2014 Pre-Event: NETmundial: Looking Back, Learning Lessons and Mapping the Road Ahead(including a book launch - Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem)
http://www.intgovforum.org/cms/igf-2014/pre-events/1879-igf-2014-pre-event-event-on-netmundial-book-release-beyond-netmundial-the-roadmap-for-institutional-improvements-to-the-global-internet

※13 チュニスアジェンダ
正式名称は「情報社会に関するチュニスアジェンダ(Tunis Agenda for the Information Society)」です。 国連のサミットとして2005年にチュニジア・チュニスでITU(国際電気通信連合)が開催した、WSIS(世界情報社会サミット)チュニス会合で採択された文書です。