インターネット動向紹介
INTERNET TRENDS INTRODUCTION

IPアドレストピック

❶ 2017.2.20▶3.2　ベトナム / ホーチミンシティ　APRICOT 2017/APNIC 43

❷ 2017.4.2▶4.5　米国 / ニューオーリンズ　ARIN 39ミーティング

IPアドレスに関する動向として、APRICOT 2017/APNIC 43 カンファレンスの内容を中心にご紹介します。JPNIC職員からAPNIC ECが選出されるという明るい話題もありました。また、アドレスポリシーに関する話題としてWHOIS登録情報正確性向上に関する議論の状況についても取り上げます。

APRICOT 2017/APNIC 43カンファレンスの動向

◆ カンファレンスの概要

2017年2月20日（月）～3月2日（木）にベトナムのホーチミンシティで、APRICOT 2017/APNIC 43カンファレンスが開催されました。

これまでのAPNICカンファレンスと同様に、会期を大きく二つに分けてプログラムが構成されました。会期前半のワークショップは、DNSやDNSSEC、BGPや仮想化といったトピックについて、業界の第一人者から話を聞きながら、ハンズオンなども含めた演習形式で行われました。後半は、RPSL（Routing Policy Specification Language）とRPKI（Resource Public Key Infrastructure）、DNSとDNSSEC、MPLS（Multi Protocol Label Switching）やアドレス管理といった、ネットワークの運用者にとって知っておくべき内容に関するチュートリアルのほか、「APOPS（Asia Pacific Network Operators Forum）」、「SIG（Special Interest Groups）」「BoF（Birds of a Feather）」、「AGM（APNIC Annual General Meeting; APNIC総会）」などの会議・セッションで、各種最新動向の報告やポリシーに関する議論などが行われました。

各プログラムの内容や、発表資料や質疑応答をまとめた発言録、当日の発表風景の映像・音声などは、カンファレンスのWebサイトから参照できます。

APRICOT 2017/APNIC 43 Program
https://2017.apricot.net/program


カンファレンスの様子

◆ IPv4アドレス移転に関するセッションについて

ここ数回のカンファンレンスでは、IPv4アドレス移転に関するセッションが設けられています。IPv4アドレス移転については、JPNICでも日頃から問い合わせが多く、関心が高い状態が継続しています。

今回は「Navigating the IPv4 Transfer Market」と題するセッションが設けられました。このセッションは、APNICのメンバーサービスの責任者、移転仲介事業者、IPv4アドレス移転を実際に経験した組織の担当者、IPアドレスの利用動向を調査している研究者をパネリストに迎えて、それぞれの立場からの報告と議論で構成されていました。

Making ends meet: IPv4 exhaustion and the transfer market
https://2017.apricot.net/program/schedule/#/day/10/apnic-panel---navigating-the-ipv4-transfer-market

セッションでは、IPv4アドレス移転市場に関わる人の30%は、アドレスを奪い取ることやお金を騙し取るなどの目的を持っている可能性が高いという分析があること、このような不正に対応するために、決済代金をやり取りする際に、第三者預託を行うエスクローの仕組みを利用すれば、金銭的な被害を防ぐこともできるといったことが紹介されました。現在、日本で行われているIPv4アドレス移転は、APNICやARINの契約組織からの移転が増えてきています。このセッションで紹介があった担当者自身の経験からの防衛策は、日本国内の事業者にも参考になる内容と思います。

◆ アドレスポリシーに関する議論について

APRICOT 2017/APNIC 43カンファレンスのアドレスポリシーSIGでは、3点のポリシー提案について議論が行われました。議論の結果、1点の提案について一部分がコンセンサスとなりましたが、残りはその他2点の提案ともども継続議論になりました。

提案名	「APNICにおける最後の/8相当のIPv4未割り振り在庫」の移転禁止提案（提案番号：prop-116）
提案者	藤崎智宏氏
概　要	APNICにおける最後の/8相当のIPv4未割り振り在庫」の移転を禁止する旨をポリシーに追加する。
補足事項	● 割り振り・割り当て後2年を経過しない、上記在庫からの分配済みIPv4アドレスの移転を禁止する。 ● 上記在庫からの割り振り・割り当てから2年が経過し、このIPv4アドレスが不要となった場合には、分配を受けた組織はAPNICに返却する。 ● M&A（事業移管や吸収合併など、その事実を書面などで客観的に確認できるケース）による移管で、移管先組織が上記の在庫から/22を超える割り振り・割り当てを受けることは、異なるASから経路広告を行うなど技術的な事情がある場合を除き認めない。/22を超えるアドレスについてはAPNICに返却する。
提案の詳細	http://www.apnic.net/policy/proposals/prop-116
結　果	継続議論

提案名	返却された IPv4 アドレスの管理方法と「APNIC における最後の/8 相当の IPv4 未割り振り在庫」枯渇後の分配方法についての提案（提案番号：prop-117）
提案者	藤崎智宏氏
概　要	「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」から割り振り・割り当てを行ったIPv4アドレスが返却された場合、「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」に戻す。また、「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」の枯渇後のIPv4アドレスの分配方法について定義する。
補足事項	● 「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」から割り振り・割り当てを行ったIPv4アドレスが返却された場合、「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」に戻すこととする。 ● 「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」からの割り振り・割り当てを行うことができなくなった場合、この在庫からの割り振り・割り当てを終了とする。 ● この在庫からの割り振り・割り当て終了後は、「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」を「IANAから再割り振りされたIPv4返却在庫」に一つにまとめる。 ● 一つにまとめられた「IANAから再割り振りされたIPv4返却在庫」から、1組織あたり/21の割り振り・割り当てを行う。 ● プールが一つにまとめられる以前の「/8相当の最後のAPNICにおけるIPv4未割り振り在庫」から分配を受けている組織は、「IANAから再割り振りされたIPv4返却在庫」から/22の割り振り・割り当てを受けることを可能とする。 ● 「IANAから再割り振りされたIPv4返却在庫」から割り振り・割り当てを行うことができない場合、待機者リストを作成し、そのリストに基づき割り振り・割り当てを行う
提案の詳細	http://www.apnic.net/policy/proposals/prop-117
結　果	「/8 相当の最後の APNIC における IPv4 未割り振り在庫」から割り振り・割り当てを行った IPv4 アドレスが返却された場合、「/8 相当の最後の APNIC における IPv4 未割り振り在庫」に戻すことについてはコンセンサス。その他の点については継続議論。

提案名	APNIC地域のIPv4アドレス移転時における要件緩和についての提案（提案番号：prop-118）
提案者	David Hilario氏
概　要	APNIC契約組織間のIPv4アドレス移転は、利用計画の提出なしにすべて受け入れることとする。また、移転先組織に利用計画の提出を義務付けている地域からのIPv4アドレス移転は、移転後5年以内に移転を受けたアドレスの50%を利用する計画を示すこととする。
提案の詳細	http://www.apnic.net/policy/proposals/prop-116
結　果	継続議論

継続議論となった提案については、引き続き、アドレスポリシーSIGのメーリングリストで議論が行われます。

メーリングリストにはどなたでも参加可能です。また、アーカイブが公開されているので、興味のある方はご自身で議論の動向を追ってみてはいかがでしょうか。メーリングリストでの議論を経て、次回のAPNIC 44カンファレンスにおいても議論される予定です。

Mailing list archive: sig-policy
http://mailman.apnic.net/mailing-lists/sig-policy/index.shtml

◆ 技術セッションについて

APRICOT 2017/APNIC 43カンファレンスで4日間にわたり開催された技術セッションのうち、IPv6・NTP（Network Time Protocol）・IoT（Internet of Things）についてご紹介します。その他の話題については、次のURLに報告を掲載しておりますので、あわせてご参照ください。

JPNIC News & Views vol.1485
APRICOT 2017/APNIC 43カンファレンス報告
[第4弾] 技術動向報告（1）
～ピアリング、ネットワークオペレーション、IPv6～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1485.html

JPNIC News & Views vol.1486
APRICOT 2017/APNIC 43カンファレンス報告
[第5弾] 技術動向報告（2）
～ルーティング、NTP、IoT～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1486.html

◎ IPv6 Deployment

IPv6 Deploymentセッションでは、NAT64/DNS64の動向、設定の注意点と試験ツールの紹介、バングラデシュ、スーダンおよびベトナムの固定電話系通信事業者であるFPT Telecom社から、展開事例の紹介が行われました。

ISOCのJan Zorz氏によるNAT64/DNS64についてのセッションでは、T-Mobile社などのオペレーターではNAT64/DNS64技術および464XLATの利用によるIPv6の展開が進んでいる一方、Web製作者やコンテンツ事業者などにはツールや試験環境などが整っていないことが問題として挙げられ、DNS64を設定する上での注意点の紹介や、試験を容易にするために設置されたGo6labのPublicテストベッドの紹介がありました。これは、四つのNAT64ソリューションを誰でも利用できるように設置されたテスト環境となっており、次のWebサイトに利用可能な設定内容が記載されています。

NAT64/DNS64 public test
https://go6lab.si/current-ipv6-tests/nat64dns64-public-test/

また、WebサイトのNAT64への対応状況をチェックできるWebサイトも紹介されています。

NAT64 Check
https://nat64check.go6lab.si/v6score/

◎ Fukuoka University Public NTP Service Deployment Use Case

福岡大学の藤村丞氏から、福岡大学で運用しているNTP公開サービスについての状況報告がありました。福岡大学では1993年からNTP公開サービスを行っており、普段は8MbpsのQoS（Quality of Service）によるトラフィック制限を行っていたそうです。しかし、2014年にネットワーク障害が起こった際には、大量のNTPのリトライパケットが流入し、ファイアウォールの過負荷やネットワーク接続性の低下、またQoSを設定していたBGPルータの停止が起きたそうです。この際には、BGPルータによるソフトウェアベースのQoSから、別途接続したL2スイッチによる、ハードウェアベースのQoSへ変更することで対応したという報告がありました。この障害時のトラフィック流入は二つの接続先ASからあり、一つのASは135Mbps、もう一つのASからは900Mbpsのトラフィックが発生したそうです。現在では、ネットワーク構成の変更やサーバの増強等で、NTPトラフィックに対応しているとのことです。

発表の後半では、大量のNTP問い合わせが発生する原因についての調査報告がありました。そこでは、世界各国の各種ネットワーク機器のマニュアルや、無線AP等のデフォルト設定に、福岡大学のNTPサーバが記述されていることが紹介されました。そのため藤村氏から「NTP公開サーバおよび福岡大学のネットワークへの負荷軽減のため、そうした記述や設定は行わないようにしていただきたい」と呼びかけがありました。

◎ IoT - Next Wave of DDoS?

ARBOR NETWORKS社のCF Chui氏から、最近のDDoS（Distributed Denial of Service）の状況、また2016年に発生した、Dyn社へのDDoSについての調査報告がありました。

はじめに、最近のDDoSの全体的な発生状況に関する紹介がありました。近年において、DDoSのトラフィック量、発生回数等については増加傾向にあり、DDoSによるトラフィックのピークが2010年には100Gbpsだったものが、2013年には309Gbps、2016年には800Gbpsの攻撃が観測されたそうです。回数においても、2016年は2015年と比較して、100Gbpsを超える攻撃が223回から558回まで増加し、200Gbpsを超える攻撃は16回から87回になったそうです。攻撃対象についても、オンラインゲームに関するサービスや、WikiLeaks等の政治的なサービス、金融機関のサイトなどが多く対象となっていることが紹介されました。

最近のDDoSの攻撃元についてはIoTデバイスが多く、理由としては一般ユーザーが購入後簡単に接続できること、しばしばセキュリティ対策が弱いこと、ファームウェアのアップデートができない、あるいはされないことが多いことなどが理由として挙げられ、その結果DDoSの踏み台とされることなどが紹介されました。

Dyn社へのDDoSの攻撃元、いわゆるMirai botnetについても報告がありました。インターネットに接続されたWebカメラやセットトップボックスなどには、容易にログイン画面へアクセス可能なものがあり、デフォルトのIDとパスワードでログインできてしまうことで侵入され、Mirai botnetへと組み込まれてしまうということが紹介されました。また、Mirai botnetの持つ攻撃方法についても紹介があり、そこではDNSによるものだけではなく、SYN-floodやACK-flooding、HTTP GET/POSTなどを用いた攻撃もできるとのことでした。さらに、日々プログラムもアップデートされており、将来異なった攻撃もできるようになるだろうとの予測も紹介されました。

◆ APNIC ECにJPNIC奥谷泉が就任

APNICカンファレンスの最終日には、APNIC Annual General Meeting（AGM）が開催されます。AGMでは、APNICの活動内容に関する報告、APNICカンファレンス期間中に開催されたSIGや各種セッションの報告、次回APNICカンファレンスの紹介などが行われます。また、春に開催されるAPNICカンファレンスでは、APNIC理事会メンバー（EC）を選出するための選挙がAGMの間に行われます。今回は4名の改選があり、JPNICの職員である奥谷泉が立候補し、16名の立候補者のうち現職3名に続く4位の得票で当選いたしました。任期は2017年3月2日から2019年3月までとなります。APNIC ECは、会員の代表として、APNICの予算の承認や、IPアドレス管理のルール（ポリシー）の受諾などのAPNIC事務局の運営管理と、法人としてのAPNICの経営責任という重役を担います。

奥谷泉からのAPNIC EC就任にあたってのコメント


演説をするJPNIC奥谷泉

この度のAPNIC理事選挙は4席に対して、16名の候補者が名乗りを上げた非常に厳しい選挙でしたが、国内外の多くの皆さまの協力のおかげで当選することができました。
当選という結果だけではなく、現地そしてリモートで多くの方々のサポート、仲間達との協力を実感することができた点がなによりも喜ばしく、心強かった選挙でした。特に国内のAPNIC会員の皆さまに多大なるお力添えをいただきまして、心から感謝申し上げます。

今後は、
・APNICと多くの共通分野を持つJPNICにおける活動、および資源管理を軸とした国内外のインターネットコミュニティでの国際調整に15年以上携わってきた経験
・ICANN、ISOC等での活動を通し、外からAPNICコミュニティを見ている経験
の二つの視点を活かし、APNICにおける円滑な資源管理サービス・その他活動の向上につなげ、アジア太平洋地域全体、そして国内のAPNIC会員の皆さまにとって、よりよいAPNICとなるよう、貢献してまいります。

◆ 次回以降のAPNICカンファレンスについて

次回のAPNIC 44カンファレンスは、2017年9月7日（木）～14日（木）に、台湾・台中で開催されます。また、APRICOTとの共催となるAPRICOT 2018/APNIC 45カンファレンスは、SANOG 31カンファレンスとも共催となり、2018年2月20日（火）～3月2日（金）に、ネパール・カトマンズでの開催が予定されています。

APNIC44カンファレンス
https://conference.apnic.net/44/

SANOG（South Asian Network Operators Group）
http://www.sanog.org/

WHOIS登録情報正確性向上に関する議論の状況について

米国連邦捜査局（FBI）や各国の警察といった法執行機関より、サイバー犯罪対応のために、WHOIS登録情報正確性向上の議論がが始まっていることについて、前号で取り上げました。各RIRと法執行機関が連携し説明を行った上で、2017年春にポリシー提案を提出するというスケジュール予定でしたが、APNIC 43カンファレンスではポリシー提案や、関連するセッション等は行われませんでした。APNIC地域においては、APNIC事務局が議論の進め方を検討する予定とのことで、今後のカンファレンスでの動向が注目されます。

一方、2017年4月2日（日）～5日（水）に米国・ルイジアナ州ニューオーリンズで開催されたARIN 39ミーティングでは、WHOIS登録情報正確性向上に関する「Draft Policy ARIN-2017-3: Update to NPRM 3.6: Annual Whois POC Validation（年間を通じた連絡先情報の妥当性検証）」というポリシー提案が行われました。提案の概要は、データベースに登録されたすべての連絡先に対して電子メールを送信し、送信から60日以内に受信者から応答がない場合にはその旨をWHOISに登録し、そこから90日後までの間にさらに連絡が取れない場合、登録情報を削除し、逆引きゾーンの委任を停止するという内容です。この委任停止の影響への懸念等の意見があり、継続議論となっています。JPNICでは、引き続き状況を注視し、最新の情報をお知らせしてまいります。

ARIN 39 Meeting
https://www.arin.net/vault/participate/meetings/reports/ARIN_39/

Draft Policy ARIN-2017-3: Update to NPRM 3.6: Annual Whois POC Validation
https://www.arin.net/policy/proposals/2017_3.html

IPアドレスの申請手続きに関する情報提供やご相談に関する取り組み

JPNICでは、IPアドレス管理指定事業者の方向けにIPアドレス管理業務の理解を深めていただくための説明会（年3回程度）や、お申し込みに応じて随時実施するJPNIC担当者との個別相談会を設けています。

IPアドレス関連のミーティング・コミュニケーション
https://www.nic.ad.jp/ja/ip/event/

その他、JANOG39ミーティングでは、ローカルスポンサーとして出展し、IPアドレスの申請担当者（ホストマスター）が疑問・質問にお答えするIPアドレス特別相談会を実施しました。

IPアドレス相談会 in 金沢 開催中です!
https://blog.nic.ad.jp/blog/janog39-exhibition2/

今後もこのような機会を設け、IPアドレスに関して、みなさまからご質問・ご相談を受けやすい場の提供に努めてまいります。また、JPNICブログを活用し、IPアドレスの申請のやり方を解説した記事の投稿も行っています。このような情報提供も継続して取り組んでまいります。

IPv4割り振り申請の手続きを解説します!
https://blog.nic.ad.jp/blog/ipv4-allocation/

簡単にできる!IPv6アドレス割り振り手続き
https://blog.nic.ad.jp/blog/ipv6-allocation/

ドメイン名・ガバナンス

③ 2017.3.11▶3.16 デンマーク/コペンハーゲン 第58回ICANN会議

④ 2017.4.20 日本 / 東京 第48回ICANN報告会

本稿では、2017年2月～5月にかけての、ICANN（The Internet Corporation for Assigned Names and Numbers）やIGF（Internet Governance Forum）などの情報を中心に、ドメイン名およびインターネットガバナンスに関する動向をご紹介します。

ICANN関連の動向

◆ 第58回ICANNコペンハーゲン会議

2017年3月11日（土）より16日（木）まで、デンマークの首都コペンハーゲンにて第58回ICANN会議が開催されました。今回は会議A（Community Forum）に分類される中規模なもので、参加者数は2,086名でした。

今回の会議の特徴は、新gTLDに関する議論が引き続き盛り上がりを見せたことと、WHOIS/RDS登録データディレクトリサービス（RDS）関連のセッションが複数開催されたことです。以下、それぞれの動向を簡単にご紹介します。

◎次回新gTLD募集手続き開始に向けた動き

今回は、次回新gTLD募集手続きに関連するポリシーを策定する作業部会（GNSO New gTLD Subsequent Procedures PDP Working Group）に関するセッションが複数開催されました。同WGでは、次のラウンドに向けた改善点について意見募集の準備を行ってきており、コペンハーゲン会議で開催されたセッションでは、主にその意見募集（Community Comment 2, CC2）の内容について議論されました。一般からの意見募集※1を行った後、2017年12月に暫定報告書を、2018年9月には最終報告書をそれぞれ提出する予定となっています。

◎WHOIS/RDS関連

WHOIS/RDS関連では、GNSO RDSポリシー策定プロセス（PDP）作業部会（WG）のセッションが複数開催されました。同WGの目的は、gTLD登録データの収集、保守、アクセス提供に関する目的を定義し、データ保護のためのセーフガードを検討することです。WGでは、まずは「Thin data ※2」およびデータ収集に関する重要コンセプトに焦点を絞って検討が進められています。

また関連して、WGメンバーからの提案により、データプライバシー保護の専門家に質問をぶつけるという「データ保護機関とのコミュニティ横断セッション」が開催されました。参加者からはさまざまな意見が出されましたが、中にはICANNにプライバシーオフィスを作ることを求める声もありました。


コペンハーゲン会議の様子

Cross-Community Discussion with Data Protection Commissioners
https://icann58copenhagen2017.sched.com/event/9nnl/cross-community-discussion-with-data-protection-commissioners

◎GNSOポリシー策定関連

・全gTLDにおけるすべての権利保護メカニズム（RPM）評価WG

検討を2段階に分け、フェーズ1で2012年の新gTLD募集に併せ導入されたRPMについて評価し、フェーズ2でUDRP（統一ドメイン名紛争処理方針）の見直しを行うことになっています。現状はフェーズ1で、事前にレジストリやレジストラが参照するデータベースへ登録することで商標保護を受けられる、Trademark Clearinghouse（TMCH）に関する構造とスコープのレビューを継続しています。完了次第、優先登録および商標と一致する文字列が登録された場合の通知（Trademark Claims）について検討予定となっています。フェーズ1は2017年末～2018年初頭に終了することが目標となっていて、その後フェーズ2が開始予定となっています。

・IGO/INGO事後権利保護PDP WG

国際政府間機関（IGO）-国際非政府機関（INGO）向けの権利保護メカニズムについては、2014年4月に理事会で決議され、現在ICANN事務局で実装中のドメイン名登録前のRPMとは別に、事後RPMとしてのUDRPおよびURS（Uniform Rapid Suspension）をIGO/INGOのニーズに合わせて変更するかどうかを、IGO/INGO事後権利保護PDP WGで検討しています。暫定報告書ではどちらも変えず、新たなプロセスも設けないという内容の勧告となっています。これに関しては、政府諮問委員会（GAC）が、ゼロもしくはわずかな費用で事後RPMを利用可能にするようにと反対していますが、WG内での支持は得られていないようです。

・新gTLDオークション収入

文字列競合が発生した際のオークションによるICANNの収入が莫大なものとなったことから、その使い道を検討するためのコミュニティ横断WG（CCWG）が設立され、2017年1月より検討が開始されています。WGでは作業計画を作成すると同時に、今後のブリーフィングで必要となる項目を確認中です。今回の会合では、主にICANN事務局から法的な制約などについての説明と、それに対する質疑応答がなされました。

・TLDとしての国および地域名の利用

2文字TLDは現状通りccTLDのみとし、3文字ccTLDの導入可否については検討したものの、コンセンサスは得られませんでした。国および地域名のフル名称をそのままccTLDとすることについては、検討が進んでいない状況です。このような状況のため、基本的にはCCWGを閉じることとし、今後の方向性については検討中となっています。

会議では主要言語による同時通訳が提供されています

◎技術面での特筆すべき発表

・Moving Towards a data-driven ICANN
（データ駆動のICANNに向けて）

競争、消費者からの信頼、消費者の選択肢（CCT）評価チームが発行した暫定報告書中の勧告で、ドメイン名マーケットとポリシー実装の成果に対し、データ収集活動を正式化するよう求めたことに対応して開催されたセッションです。データ収集対象、収集されたデータの利用などについて議論され、ICANNによるオープンデータイニシアティブについても紹介されました。

・Root Zone KSK Rollover
（ルートゾーン鍵署名鍵の更新について）

現在、DNSSECプロトコルで使われている鍵署名鍵（KSK）は2010年に署名されたものですが、2017年10月11日にルートゾーンの鍵署名鍵が更新されます。更新への対応が必要になる可能性があるということで、更新に関して周知啓発するためのセッションが開催されました。

◎Emerging Identifiers Technology

（新たな識別子技術について）

新たに出現したインターネットの識別子技術として、次の三つが紹介されました。

- Namecoin：ブロックチェーン技術を利用した識別子登録および更新技術
- Frogans：アプリケーション層で動作する識別子技術
- Digital Object Architecture（DOA）：デジタル図書館のために考案された技術を基に開発された、インターネット上で動作する分散情報保存、特定および検索識別子技術

◎その他の話題

・説明責任についてのコミュニティ横断作業部会（CCWG- Accountability）

ICANNの説明責任強化に向けての検討は、IANA監督権限移管後も継続しています。次のサブグループより進捗報告が行われました。

- スタッフの説明責任について
- 支持組織（SO）および諮問委員会（AC）の説明責任について
- SO/AC/配下もしくは横断グループのダイバーシティについて
- 独立評価パネル（IRP）実装監督チームの状況
- ICANNの法管轄（Jurisdiction）について（具体的にはICANNが米国にあることについて）

・GNSOスタッフ退任

GNSOの事務局を長らく担当されたICANNスタッフ、Glen de Saint Gery氏が今回を持って退任しました。それに合わせ、今回はGNSOの歴史に関する炉辺談話（GNSO History Fireside Chats）と名付けられた、彼女を囲むセッションが行われたほか、GNSO評議会会合および理事会会合では、それぞれ彼女に対する感謝決議がなされました。

◎第48回ICANN報告会

本コペンハーゲン会議に関する報告会を、JPNICと一般財団法人インターネット協会（IAjapan）の共催にて、2017年4月20日に東京・神田のJPNIC会議室で開催しました。


ICANN報告会の様子

※1 JPNICブログ
「新gTLD、次の申請ラウンドに向けた意見募集」
https://blog.nic.ad.jp/blog/newgtld_next_round_cc2/

※2 Thin data
Thin WHOISで表示される情報である、レジストラ情報、登録状態、登録日および登録終了日、ネームサーバ情報、WHOIS更新日時、レジストラのWHOISサービスURLを指します。

当日のプログラムは次の通りです。

1. ICANNコペンハーゲン会議概要報告
2. 国コードドメイン名支持組織(ccNSO)関連報告
3. ICANN政府諮問委員会(GAC)報告
4. ICANN理事からの報告
5. アドレス領域の報告
6. 技術領域の報告
7. レジストリ・レジストラ関連状況報告
8. 次期新gTLD募集手続き検討状況報告

本報告会のレポートをメールマガジンにて発行していますので、詳細については次のURLからバックナンバーをご覧ください。

JPNIC News & Views vol.1502
「第48回ICANN報告会レポート」
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1502.html

◎次回のICANN会議

第59回ICANN会議は、南アフリカ・ヨハネスブルグで、2017年6月26日(月)から29日(木)の開催です。本ヨハネスブルグ会議の報告は、2017年11月発行の次号67号で取り上げる予定です。

◆ その他ICANN関連の話題

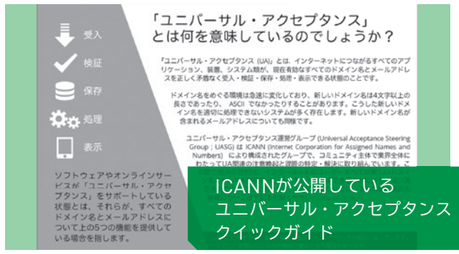
◎ユニバーサル・アクセプタンス クイックガイド

2003年10月に開始された新gTLDプログラムによって、gTLDの数が飛躍的に増加し、2017年5月時点では1,200を超えるほどとなっています。これにより、5文字以上の英数字からなるドメイン名や、国際化ドメイン名(IDN)など、従来では見慣れないドメイン名が増加することになりました。このようなドメイン名が増加するに従って、これらがICANNによる正式に登録されたものであるにも関わらず、例えばドメイン名や電子メールアドレスの入力チェックシステムで従来のTLDのみを許可する設定になっているといったことが原因で、システム上うまく扱えない現象などが見られるようになってきました。

ICANNでは、新たに追加された多様なドメイン名があまねく利用できるようにするために、「TLD ユニバーサル・アクセプタンス」というコンセプトを打ち出して、状況の改善に努めています。そのような活動の一環として、システム上どういった点に配慮すればユニバーサル・アクセプタンスを実現できるのかをまとめたクイックガイドを、ICANNが小冊子形式にて公開しています。各国語版があり、日本語版も用意されています。

ユニバーサル・ アクセプタンス クイックガイド (PDF)
https://uasg.tech/wp-content/uploads/2016/05/UASG005-20170127-jp-quickguide-digital.pdf

このクイックガイドでは、ドメイン名や電子メールアドレスをシステム上受け入れて、それが正しいかどうか検証し、システム内で適切に保存・処理した上でユーザーインタフェース上に表示する一連の流れにて、それぞれ確認するべき項目を挙げています。受入、



検証、保存、処理、表示について各1ページで記述されているため、ユニバーサル・アクセプタンスの観点から注意すべきことをクイックに確認することができます。

ドメイン名や電子メールアドレスに関係するシステムに従事する方々は、この機会にぜひご一読ください。本クイックガイドについては、JPNICブログの記事としてもご紹介しています。

ドメイン名や電子メールアドレスを扱う技術者の皆様へ
～ユニバーサル・ アクセプタンス クイックガイド
日本語訳公開～
https://blog.nic.ad.jp/blog/ua-qucik-guide-jp

◎ICANNに関連したJPNICによる情報発信のご紹介

本ニュースレターをはじめ、WebやメールマガジンNews & Viewsなど、JPNICではさまざまな媒体でICANN関連の情報を発信しています。あまりに多岐にわたるため、すべてを把握されていない方も多いかと思います。そこで、JPNICによるICANN関連の情報発信の一覧を簡単にご紹介したいと思います。

新しい情報があり次第、随時更新されるもの
・ICANNによるアナウンスメントの一覧 ・gTLDの追加情報およびICANN理事会の決議概要
ICANN会議ごとに更新されるもの
・ICANNによる会議情報や理事会の決議内容、JPNICによる報告記事などの一覧 ・ICANN報告会の資料および動画
その他
・理事会や各委員会・支持組織等の概要などの情報 ・定款などのICANN主要文書 ・統一ドメイン名紛争処理方針(UDRP)などのポリシー文書 ・ICANNの歴史や新gTLDなどの参考情報 ・ICANN関連の用語集解説

それぞれの情報発信に関する詳しい説明を、JPNICブログの記事としても公開しています。こちらもぜひ併せてご覧になってください。

ICANNに関する情報提供のいろいろ
https://blog.nic.ad.jp/blog/icann-info-provision

IGF関連の話題

◆ IPv6 Best Practices Forumのご紹介

国連が主催するInternet Governance Forum (IGF)では、特定テーマに関する最適な運用を成果文書として取りまとめる、「Best Practices Forum」と呼ばれる活動が行われています。毎年四～五つの特定テーマを選び、その年のIGF会議が開催される半年以上前からメーリングリストと定期的なテレカンファレンスにより議論を積み重ね、さらにIGF会議でも対面で議論が行われます。そうしてまとまった最終的な文書が、国連IGFのWebサイトに公開されます。このような活動の元、2015年と2016年には、IPv6に関する成果文書が公開されています。

IPv6に関する検討が行われた理由ですが、昨今グローバルなインターネットガバナンスの場では、「(途上国への) アクセス提供」と「セキュリティ」が注目を集めています。そのような状況の中で、IGFでは途上国へのアクセス提供という観点から、2015年より「次の10億人への接続提供」をIGF共通のテーマとして掲げました。この目的を達成するために、既に余剰のないIPv4ではなく、今後インターネットへ接続する機器やユーザーに対して分配が行えるインターネットの重要資源として、IPv6が2015年および2016年のIGFにおけるBest Practicesのテーマの一つに選定されました。

2015年はIPv6導入に向けた政府、コミュニティ主導のタスクフォース、事業者等、さまざまな関係者の役割や事例を紹介し、2016年は経済的な要素に基づくインセンティブに重点を置きました。これは、個々の取り組みに入る前に、IPv6導入のインセンティブを共有することが大切だとのインプットが、2015年のIGFで行われたことに対応したものです。2016年のIPv6に関するBest Practices Forum(IPv6-BPF)は、CoordinatorをJPNICの奥谷泉が、バングラデシュのBDNOG BoardのChairであるSumon Ahmed Sabir氏と務め、地域インターネットレジストリ(RIR)コミュニティメンバーの協力を得ながら、文書策定・公開に至りました。

本文書は、政府のインフラ基盤整備等に関わっている政策担当者や、企業の幹部を読み手として想定しているため、内容としては運用者やIPv6の導入促進に取り組んできた事業者にとって目新しいものではありません。RIRコミュニティが本文書を策定するにあたって運用者はむしろ、IPv6導入に向けた取り組みについて知見を持つ立場として内容を充実させるなど、中心的な役割を果たしています。日本からも、文書中の事例紹介に国内の事例を提供するなどの形で貢献しました。

IGF IPv6 BPF活動に関する情報、メキシコで開催されたIGF 2016会議でのIPv6-BPFセッションの動画、IPv6-BPF成果文書については、以下のURLより参照可能です。

IGF2016 IPv6-BPFページ：
BPF IPv6 - Understanding the commercial and economic incentives behind a successful IPv6 deployment
http://www.intgovforum.org/multilingual/content/bpf-ipv6

国連IGFでのIPv6-BPFセッション(動画)：
BPF on IPv6 workshop at the 11th IGF meeting (7 December 2016, Guadalajara, Mexico)
https://youtu.be/g9EmjZXpscA

成果文書：
IGF 2016 Best Practice Forum on IPv6
http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3407/458

IPv6 Best Practices Forumの活動について、より詳しい内容をJPNICブログでご紹介していますので、ぜひこちらも併せてご覧ください。

国連IGFにおけるIPv6 Best Practices Forumのご紹介 (その1)
https://blog.nic.ad.jp/blog/igf2016ipv6-bpf/

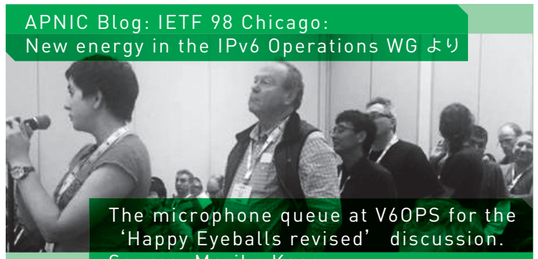
IGF 2016の
メインセッションの様子

技術トピック

5 2017.3.26▶3.31
米国 / シカゴ
第98回IETFミーティング

技術関連動向として、第98回IETFミーティングの主な内容と、ルートゾーンKSK（鍵署名鍵）更新の話題についてご紹介します。

全体会議



第98回IETFミーティング(IETF 98)は、米国・シカゴのスイスホテルで行われました。米国での政権交代に伴い、入国制限の波紋が広がる中での開催となりました。米国への入国制限および入国時の情報収集については、IETFミーティング開催地の選定に関する問題として、今回のIETFにおいて度々議論になりました。

主に中近東の国からのフライトについて、PCなどの電子機器の機内持ち込みが制限されるといった話、ビザの発行に時間を要した、または発行されなかったなどの理由で参加できなかった人がいたとの話がありました。こういった話は、将来のIETFミーティング開催地を選定する際に大きな影響を及ぼします。出身国によってIETFミーティングに参加できないということは、オープンなインターネットの仕様を定めるIETFの理念に一致しないからです。

Meeting Venue WG (MTGVENUE WG)では、開催地に求められる基準について議論されました。IETFミーティングは年に3回ですが、春開催は北米地域、夏開催は欧米地域、秋開催はアジア・パシフィック地域という慣例があります。しかし、会場やネットワークなどのファシリティの問題だけでなく、入国制限の問題や法制度の問題など、すべての問題がクリアな開催地を探すのは大変困難です。WGではどの基準を必須とするか、どのように優先順位をつけるかという、現実的な落とし所について議論が進められました。

技術全体会議(Tech plenary)では、「プロトコルと人権」というテーマのプレゼンテーションが行われました。

一つ目のプレゼンテーションでは、IRTF (Internet Research Task Force)のHuman Rights Protocol Considerations Research Group (HRPC RG)での議論が総括して紹介されました。「中立的な技術は存在しない」という立脚点から、プライバシーや表現の自由が阻害されるような、人権問題が存在することの理解から始めようというメッセージが伝えられました。現在IETFにはシステムデザインにおける倫理的規定や社会的責任についての文章やガイドラインといったものは無いため、策定の議論をすべき時機がきたのではないか、と投げかけて発表を終えました。

二つ目のプレゼンテーションでは、サイバースペースでの争い(Tussle in Cyberspace) ※1という著名な論文を執筆した、マサチューセッツ工科大学(MIT)コンピュータ科学研究所のDavid Clark氏が登壇しました。

彼は、IETFにおけるプロトコル設計について、ゲームに例えて次のようにわかりやすく語りました。「ゲームの結果をデザインしているのではなく、ゲームのフィールドを設計しているのだ。なので、フィールドを傾けることもできる」

実は、IETFでは過去(1999年頃)、法執行機関がネット上の通信を傍受するのを容易にするプロトコルを開発する必要があるかどうかについて、熱く議論された時期がありました。結果として、IETFは傍受をプロトコル設計時の考慮事項に入れることに対して“NO”と結論を下しました。その顛末は、RFC2804:傍受に関するIETFのポリシー(IETF Policy on Wiretapping)※2にまとまっています。

対して、3GPP (Third Generation Partnership Project)では、SA WG3(Security)サブWGにて、合法的傍受の要件を満たす仕様を定めるとしています。これらの過去の経緯を踏まえ、彼は人権をプロトコル設計における基本的な考慮事項に入れることを強く推奨すると同時に、バランスよく適切にフィールドを設計することの難しさを指摘しました。

そのほか、全体会議に関するトピックの詳細については次のURLをご参照ください。

JPNIC News & Views vol.1492【定期号】
第98回IETF報告 [第1弾] 全体会議報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1492.html

※1 Tussle in Cyberspace: Defining Tomorrow's Internet
http://david.choffnes.com/classes/cs4700fa14/papers/tussle.pdf

※2 RFC2804: IETF Policy on Wiretapping
https://www.ietf.org/rfc/rfc2804.txt

トランスポートエリア

QUIC WGの目的は、低遅延かつセキュアな通信を実現するトランスポートプロトコルである「QUIC」の策定です。今日のWebサービスでは、体感品質(UX)の向上、特にネットワーク遅延を含む、あらゆる遅延を可能な限り抑えることが求められています。QUICでは、バイトストリーム型トランスポート、すなわちTCPに起因するヘッドオブラインブロッキング(HoL)の回避によって遅延を抑制します。

QUICの特徴としては、

・上位アプリケーションにHTTP/2を想定
・マルチストリームに対応
・デフォルトでTLS 1.3の機能を利用する
・UDPベースのセキュアなトランスポート

が挙げられます。

IETF 98では、QUICの仕様が記述された四つのWG文書のアップデートについて発表が行われました。はじめにトランスポートコアに関する発表がありました。ヘッダ形式、コネクションID、バージョン番号のルール、トランスポートパラメータをTLS拡張として扱う、などの修正が行われました。

次に、TLS 1.3へのマッピングに関する発表がありました。TLSハンドシェイクの非暗号化、QUICヘッダの整合性、TLS 1.3以上を必須とする、などの修正が行われました。

三つ目に損失検出と輻輳制御に関する発表がありました。損失検出と早期再送、ハンドシェイク時の損失回復、RTT計算方法に関する修正が説明されました。

最後にHTTP/2のマッピングに関する発表がありました。特定番号のストリームマッピングの変更、HTTP/2ヘッダ圧縮方式の変更、設定情報交換のフレーム形式の違いなどが説明されました。

WG文書のアップデートに関する発表の後、さまざまな検討課題について議論が行われましたが、最後は時間切れとなり、多くの課題が次回のInterim（中間）会合(フランス・パリ、2017年6月)に持ち越されました。

その他、QUICと関係が深い話題として、TCPM(TCP Maintenance and Minor Extensions) WGでタイマーベースの損失検出アルゴリズムRACKについて、IRTF(Internet Research Task Force) ICCRG (Internet Congestion Control RG)でBBR輻輳制御アルゴリズムについて発表がありました。前者のRACKは、重複確認応答だけでは(しきい値に達せず)判定できない損失を、送信側がタイマーによって早期に判定する方式で、QUICにも採り入れられる見込みです。後者のBBR輻輳制御アルゴリズムは、経路上のボトルネックに起因する遅延を抑えつつ高いスループットを実現する方式ですが、これがGoogle QUICに実装されていることが示されました。ちなみに、実装と異なり標準文書では、BBRのように標準化されていない方式を参照することはできないので、QUICは輻輳制御方式として(標準化中の)CUBICおよびRenoが参照されています。

そのほか、トランスポートエリアに関するトピックの詳細については以下をご参照ください。

JPNIC News & Views vol.1493【臨時号】
第98回IETF報告 [第2弾] トランスポートエリア関連報告
～IETF QUIC プロトコル標準化とその周辺～
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1493.html

IPv6

IPv6に関するトピックスとしては、IPv6の仕様に関する議論や、IPv6の運用に関する諸問題を取り上げます。

◆ 6man WG (IPv6 Maintenance WG)

6man WG (IPv6 Maintenance WG)では、基本プロトコル仕様のInternet Standardへの格上げに関する議論が行われました。その中で、特に基本プロトコル仕様のRFC2460と、アドレスアーキテクチャを規定するRFC4291が激しい議論を引き起こしています。

RFC2460については、パケットの送信ノード以外はIPv6の拡張ヘッダをパケットに挿入できないとする仮定を、文面として明記するかどうかで意見が分かれています。これは、RFC2460の策定時、暗黙的に認めていた仮定のため、RFCでは「挿入」という言葉が明示的に使われていませんでした。

これに対し、Segment Routing (SR)というプロトコルの一部実装では、パケットを転送するルータが拡張ヘッダを挿入する挙動になっています。RFC2460の格上げにあたって本来の仮定を明記してあいまいさを解消しようとしたのですが、SRを実装、運用するベンダーやオペレーターから強い反対が示されました。WGの議論およびIETFでのラストコールを経て、あいまいさを解消する文面を提案されましたが、ミーティング参加者からの強い抗議もあり、IESGの承認プロセスに入っているものの、今後どうなるかはやや不透明な状況です。

RFC4291については、現状使われているグローバルアドレスのサブネット長およびインタフェースID長を64ビットに固定するという記述を、残すか緩めるかについて対立しています。

アドレスもサブネット長も変更することが多いISP運用者を中心に、固定するのは実運用を無意味に規定違反とするだけで、有害だとする意見があります。一方、一部のホスト実装者は、事実上無限と言えるだけのID空間を取ることによる将来的な拡張の可能性や、簡潔に実装できるなどの点で、現状の仕様のままとすべきだと主張しています。結局、両者の意見の隔たりが大きく、時期尚早だとして議論はWGに差し戻されました。

◆ v6ops WG (IPv6 Operations WG)

v6ops WGでは、IPv6の運用に関する諸問題を議論しています。ここでは、特に注目を集めた発表を二つご紹介します。

◎ On the Dynamic/Automatic Configuration of IPv6 Hosts

IPv6ホストが、DNSサーバアドレスやドメイン名サーチリストなどの設定情報を取得するためのプロトコルとしては、現在、DHCPv6による方法とルータ通知(Router Advertisement、RA)による方法があります。これらのプロトコルの実装状況は、ホストやルータによってまちまちであり、任意のホストが任意のネットワークで設定情報を自動取得できるとは限らないという状況が続いています。これを両方のプロトコルに対応するように求めるよう提案がありました。

しかし、この問題が難しいのは、これが単なる実装の不備ではなく、IPv6ネットワーク運用の考え方についての、根本的な見解の相違に根付いているというところです。一方では、DHCPv6は柔軟さに欠ける劣ったプロトコルだとして実装を拒否するグループがあり、他方ではIPv4からの継続性や、より集中的な管理のためにDHCPv6以外での運用を拒否するグループがあります。そのため、どちらかの方式の実装を“MUST”として強制したり、両方の実装を要求したりするといった提案が、合意に至る見込みが立っていません。

今回のミーティングでも、いつものように議論は平行線気味で、結局ドラフトもWGドキュメントとして採択されるには至らず、MLでの継続議論ということになりました。

◎ An Update to Happy Eyeballs

米Apple社のDavid Schinazi氏による、iOSの開発・運用経を元にしたHappy Eyeballs (HE)アルゴリズムに対する改善提案です。RFC6555で規定されるHEは、IPv6/IPv4のデュアルスタックホストにおいて、TCPコネクション接続先の候補が複数ある場合に、複数候補についてある程度並行してコネクション確立を試みることで、特定のアドレスへの接続性が悪くても長いタイムアウトを待たずに済むようにするというアルゴリズムです。RFCで規定されるアルゴリズムでは、TCPコネクション確立に先立って、IPv6とIPv4アドレスの双方についてDNSによる名前解決(それぞれAAAAとAレコードの取得)を完了させるのが前提になっています。このドラフトでは、DNSの名前解決においても、AAAAまたはAの一方の問い合わせだけに長い時間がかかる場合がしばしばあるとして、名前解決を非同期にする(どちらかの問い合わせが完了した時点で、他方の応答を待ちつつコネクション確立を開始する)必要があるとしています。

ミーティングでの発表においては、iOSデバイスで取得した統計情報を元にこうした事情が説明されており、説得力がありました。また、こうした実際の運用データを元にした細かなタイムアウト値の計算方法なども示されていて、興味深い発表でした。実際、この発表には参加者から多くのコメントがありました。IETFの発表では、特に議論を呼ぶような発表に対してコメントする人がマイクの前に長い列を作るという光景がときどき見られますが、この発表に対する反応はその典型的なケースでした。APNICのブログ※3に、その様子を撮った写真が掲載されています。

コメントは、従来の「同期的」名前解決に対する考え方、TCP SYNのタイムアウトに対する考察、APIの標準化に関する助言、あるいはそもそもHEは問題を隠蔽するもので推奨すべきでないとの意見など、多岐にわたりましたが、全体としてはおおむね肯定的でした。本稿執筆時点で、RFC6555の後継とするためのWGドラフトとして採択されています。

そのほか、IPv6に関するトピックの詳細については以下をご参照ください。

JPNIC News & Views vol.1495【臨時号】
第98回IETF報告 [第3弾] IPv6関連WG報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1495.html

セキュリティ

IETF 98で唯一開催された、セキュリティエリアでのBoF※4である、TEEPについてご紹介します。

□ セキュリティエリアでのBoF：TEEP

TEEPの目標は、動的な信頼できる実行環境を実現するための、プロトコル標準化です。産業界では、アプリケーション層のセキュリティプロトコルの開発を進めてきています。このプロトコルを利用することで、いつでも信頼できる実行環境(Trusted Execution Environment；TEE)上で動作する、セキュリティクレデンシャル(認証情報)と、ソフトウェアの設定が許可されます。現在のTEEとしては、家庭用ルータ、セットトップボックス、スマートフォン、タブレット、ウェアラブル端末などがありますが、これらの環境では独自プロトコルが利用されています。このBoFでは、このようにTEEごとに検討されているプロトコルの標準化をめざしています。具体的なプロトコルとしては、The OpenTrust Protocol (OTrP)※5がInternet-Draftとして投稿されています。

このセッションは、大別して三つの話題が取り扱われました。一つ目として、TEEPが何を想定しているのか？という概観に関する共有。二つ目は、異なる二つの信頼できる実行環境プラットフォームとして、ARM社とIntel社の製品紹介。三つ目は、TEEPで実現できるユースケースです。モバイルで注目を集めているPaymentやBYOD (Bring Your Own Device)により、企業内で利用された機器に対するインストール、アップデートなど、OEM先に依存しない信頼されたソフトウェア管理方法およびアーキテクチャとして、OTrPに関する紹介が行われました。BoFの最後に問題設定について理解したか、WGを発足する必要性について、ハミングによって確認が行われました。その結果、20人前後の賛同者がありましたが、引き続きメーリングリスト上での議論を継続することが、セキュリティエリアディレクターから告げられました。

TEEP BoF Overview
https://www.ietf.org/proceedings/98/slides/slides-98-teep-teep-overview-00.pdf

TEEP BoF Minutes
https://www.ietf.org/proceedings/98/minutes/minutes-98-teep-00.txt

そのほか、セキュリティエリアでのトピックの詳細については、以下をご参照ください。

JPNIC News & Views vol.1498【臨時号】
第98回IETF報告 [第4弾]
セキュリティエリア関連報告
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2017/vol1498.html

ルートゾーンKSKロールオーバーが実施されます

ルートゾーンを管理するICANNは、2016年10月から2018年3月にかけて、ルートゾーンKSK (Key Signing Key; 鍵署名鍵)ロールオーバーを実施しています。

KSKのロールオーバーは、DNSSEC (Domain Name System Security Extensions) におけるトラストアンカーであるルートゾーンのKSKを更新し、同時にインターネット上のDNSSEC検証を行っているキャッシュサーバ(フルリゾルバ)や各種DNSソフトウェアに新しいKSKの公開鍵を設定することです。

◆ 対応が求められる対象と内容

ルートゾーンKSKロールオーバーの実施にあたり、DNS運用者に対応が求められます。対象は大きく分けて以下の3者になります。

(1) キャッシュサーバ(フルリゾルバ)の運用者
(2) 権威サーバの運用者
(3) 顧客のネットワークを運用しているシステムインテグレーター

◎ (1)キャッシュサーバ(フルリゾルバ)の運用者

KSKロールオーバーの実施期間中、鍵や署名の追加などにより応答パケットが巨大化するため、IPフラグメントが発生する可能性があります。応答パケットの大きさが変化する主な日付と、応答パケットの大きさは次の通りです。IPフラグメントが発生し、パケットが欠落するなどすると、DNSSEC検証の有効・無効を問わず、名前解決ができなくなります。ルートゾーンに対して名前解決ができないと、結果としてDNS全体の名前解決ができなくなるため、キャッシュサーバに名前解決を依存しているサーバやユーザーなどに影響が出ることになります。

2017年 7月11日	新KSK(KSK-2017)の公開	1139bytes
2017年 9月19日	新ZSKの公開 (ZSKもKSKロールオーバーと独立して3ヶ月ごとの更新が行われています)	1414bytes
2017年 10月11日	KSK-2017を用いた署名の開始	1139bytes
2017年 12月20日	新ZSKの公開	1414bytes
2018年 1月11日	古いKSK(KSK-2010)の失効	1424bytes
2018年 3月22日	KSK-2010の削除	1139bytes

IPフラグメントの有無は、以下のサイトやコマンドで確認できます。

・Webでの確認方法
http://keysizetest.verisignlabs.com/
(このWebでチェックをし、チェックボックスの四つ目まで緑だったらOK)

・コマンドラインでの確認方法
dig +bufsize=4096 +short rs.dns-oarc.net txt

DNSSEC検証を有効にしている場合は、できるだけ最新のDNSサーバソフトウェアにしておくことが大切です。特に、トラストアンカーの自動更新機能であるRFC5011に対応したバージョンかどうか、自動更新の設定を有効にしているかどうかを確認しておく必要があります。RFC5011に対応していないソフトウェアの場合は、手動や他の方法でのトラストアンカー更新が必要になります。新しく生成されたトラストアンカー(KSK-2017)はすでにIANAのWebサイト※6で公開されていますので、早めの更新が推奨されます。

◎ (2)権威サーバの運用者

ルートゾーンのKSKロールオーバーが失敗した場合、自組織の権威サーバが正常に運用されているにも限らず、ユーザーが名前解決ができなくなる可能性があります。ユーザーからの問い合わせに対応が必要になる場合がありますので、あらかじめ準備しておくことが推奨されます。

◎ (3)システムインテグレーター(SIer)

顧客のネットワークやサーバの設計・構築・運用を請け負うSIerは、顧客のシステム内のDNSサーバやネットワーク機器の設定、運用状況を確認しておく必要があります。対応としては上記(1)(2)と同様です。

◆ 参考情報

DNSSECバリデーションにおけるルートゾーンKSKロールオーバーに関する重要なお知らせ
https://www.nic.ad.jp/ja/topics/2017/20170531-02.html

※3 IETF 98 Chicago: New energy in the IPv6 Operations WG
https://blog.apnic.net/2017/03/31/ietf-98-chicago-new-energy-ipv6-operations-wg/

※4 Birds of a Feather Meetings
https://trac.tools.ietf.org/bof/trac/#TimeframeIETF98Chicago

※5 The Open Trust Protocol (OTrP)
draft-pei-opentrustprotocol-03
https://tools.ietf.org/html/draft-pei-opentrustprotocol

※6 IANA - DNSSEC Key Signing Key
https://www.iana.org/dnssec/files