IETF 96 報告
DNS関連

藤原 和典
fujiwara@jprs.co.jp
株式会社日本レジストリサービス (JPRS)
IETF 96 報告会, 2016年9月12日

自己紹介

- 氏名:　　藤原和典
- 個人ページ: http://member.wide.ad.jp/~fujiwara/
- 勤務先:　株式会社日本レジストリサービス (JPRS)
  技術研究部
- 業務内容:DNS関連の研究・開発
- IETFでの活動 (2004~)
  - RFC 5483 6116 (2004~2011):ENUMプロトコル
  - RFC 5504 5825 6856 6857 (2005~2013)
    - メールアドレスの国際化 (互換性部分を担当)
  - DNS関連の問題提起など
    - RFC 7719: DNS Terminology → terminology-bis
    - draft-ietf-dnsop-nsec-aggressiveuse (2015/3~)
- 個人的なIETF 96結果
  - 共著者による発表2, コメント1

DNS関連WG/BOF

- DNS関連WG/BOF
  - dnsop　　DNS運用ガイドラインの作成
  - dprive　　DNS通信路の暗号化 → 非開催
  - dane　　DNS(SEC)にTLSの証明書 → 非開催
  - dbound　　Public Suffix List の後継 → 非開催
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - homenet　　Home Networking
  - Bundled-domain-names　　Bar Bofとして開催
- IETF以外
  - IEPG

DNS関連報告の概要

概要 1

- dnsop: DNS運用ガイドラインの作成
  - RFCを多数発行中 (IETF 95から3、RFC Editor Queueに4)
  - 多数の提案の議論が進められた
  - 一つのDNSトランザクションで複数の応答を得る提案が複数
- dprive: DNS通信路の暗号化
  - RFC 7858 (DNS over TLS)が発行された
  - 残るDNS over DTLS, profileについても議論はほぼ完了し、WGLCのみのため、非開催
- dane: DNS(SEC)にTLSの証明書
  - ほとんどの議論が完了したため、非開催
  - RFC 7929 (OpenPGPKEY)がExperimentalで発行
  - SMIMEAがIESGに提出直前、残るはIPSECなど？

概要 2

- dbound: Public Suffix List の後継
  - 非開催: 遅れていて活動がみえないため、進めるか辞めるかという議論が行われる
  - 非開催だが、自分の提案を持っている人がinformalなBar Bofを開催
- dnssd: DNS-SD (RFC 6763)の拡張
  - hybrid proxyドキュメント停滞中 (expired)
  - プライバシーの議論が始まった
- homenet: Home networking
  - 新しい名前解決アーキテクチャの議論が進む
  - RFC 7788 Homenet Control Protocolで.homeと書いてしまったことの反省

概要 3

- IEPG: 運用に関する話題を扱うinformalな集まり
  - DNS (4件)とBGP (1件)、IPv6(2件)、IANAレジストリ報告の発表が行なわれた
- Root DNSSEC
  - ISOC Briefingが行なわれていた火曜の昼に、Upcoming ZSK and KSK Changes to the Root Zoneという報告が行なわれた
  - Root zoneのDNSKEY Rolloverについての報告や予定が発表された
  - KSK Rolloverの日程の発表は新規

詳細

前回の報告と同じ内容の部分

dnsop (DNS Operations) WG

- DNS運用ガイドラインを作るWG
  - DNSプロトコル拡張を作る機能も含む
  - https://tools.ietf.org/wg/dnsop/
- 振り返り: 2015年7月のIETF 93
  - TCPトランスポート, nsec-aggressiveuse, トラストアンカー管理の議論, TLD予約
- 振り返り: IETF 94でのミーティングの概要
  - TLD予約
  - 多数の新規提案: ordered-answers, maintain-ds, dns-message-checksums, message-fragments, edns-key-tag, DNAME in the Root?, NXDOMAIN
- 振り返り: IETF 95
  - 多数の案件
  - 新規: DNS over HTTP, delegation requirements, dnssec-algorithm-update, class-useless, aaaa-for-free, black-lies

dnsop (2)

- 着実にRFCを発行 (draft-ietf-dnsop-省略)
  - 2016/ 4/ 6　RFC 7828 edns-tcp-keepalive
  - 2016/ 5/12　RFC 7793 rfc6598-rfc6303
  - 2016/ 5/20　RFC 7871 edns-client-subnet
  - 2016/ 5/27　RFC 7873 cookies
  - 2016/ 6/21　RFC 7901 edns-chain-query
- IESGでレビュー中
  - dnssec-roadblock-avoidance-04　2016/8/23 IESGほぼ通過(enough position to pass)、コメント対応待ち
  - maintain-ds-03 2016/9/1 IESG meeting
  - nxdomain-cut-04　2016/9/15 IESG meeting

dnsop (3)

- RFC 7793, 2016/5/12発行
  - draft-ietf-dnsop-rfc6598-rfc6303, Best Current Practice
  - Add 100.64.0.0/10 prefixes to IPv4 Locally-Served DNS Zones Registry
  - グローバルなDNSに無駄なクエリが漏れるのを防ぐためにフルリゾルバに64ゾーン追加
  - {64..127}.100.in-addr.arpa
    - /10じゃなくて/8を割り当ててくれたら楽だったのに

dnsop (4)

- RFC 7871, 2016/5/20発行
  - draft-ietf-dnsop-edns-client-subnet, Informational
  - EDNS Client subnet
  - Public DNSサービスの利用者がCDNのアドレス制御を使用できるように、クライアントのサブネットアドレスを権威DNSサーバに伝えるEDNS0オプション
  - [address-family] [prefix-length] [prefix]
  - 応答にサーバの応答が対応するprefixを示すprefix-length (SCOPE prefix-length)が追加され、source prefix-lengthより長い場合は、source-prefixを長くして問い合わせ直す必要あり
    - フルリゾルバでは、Prefix + SCOPE prefix-lengthごとに応答をcacheする必要があり、実装が大変である
  - 実装済 (Public DNS, CDN, Hyper Giants)

dnsop (5)

- RFC 7901, 2016/ 6/21
  - draft-ietf-dnsop-edns-chain-query, Experimental
  - Validatingスタブリゾルバからフルリゾルバの通信で、クエリ名の検証に必要な情報をまとめて受け取るためのEDNS0オプション
  - 指定したドメイン名を検証済として、クエリ名までの検証に必要なDS, DNSKEY, RRSIGをauthority sectionに追加

dnsop (6)

- RFC 7873, 2016/ 5/27
  - draft-ietf-dnsop-cookies, Proposed Standard
  - Domain Name System (DNS) Cookies
  - DNS/UDPの攻撃耐性を上げるために、クエリ側で64ビットのCookieを添付、サーバはレスポンスにコピー
  - 送信Cookieと受信Cookieが異なると異常
  - [client-cookie 8 bytes]
    [server cookie 8 to 32 bytes]
  - 実装済 (BIND 9.10.0 sit → 9.10.3 draft対応)

dnsop (7)

- draft-ietf-dnsop-dnssec-roadblock-avoidance-05
  - Best Current Practice
  - “Host Validator”がDNSSEC検証できるかどうかを判定する
  - ホテルのネットワークやmiddle boxの悪影響を避ける目的
  - 2014/3/7 dnsop WG draft 00
  - 2016/5/26 IESG提出、9/7 IESG通過

dnsop (8)

- draft-ietf-dnsop-maintain-ds-03,
  - DNSSEC設定を、レジストリを通さずに行う提案(RFC 7477 CDS)の拡張で、DS新規追加と、DS削除を追加
    - DNSオペレータが、レジストラ・レジストリを通さずにDNSSECのDS設定をしたいという要求より
  - 新規追加の場合は、別チャネル(registrantへのメールなど)での認証してもよいし、無条件に信用してもよい
  - 2015/12/14 dnsop WG draft 00
  - 2016/6/21 IESG提出、9/15 IESG meeting予定
  - 順調にDISCUSS(異議)をつけられている
    - 9/5 4件

dnsop (9)

- draft-ietf-dnsop-nxdomain-cut
  - あるドメイン名がNXDOMAIN(名前不存在)の場合、その子孫をすべてNXDOMAINとして扱うという提案
    - あるドメイン名の名前不存在がキャッシュされている場合、有効期間内には、その子孫をすべてNXDOMAIN扱いする
  - Updates RFC 1034, 2308 (-04で追加)
  - 2016/5/26 – 6/10 WGLC
  - 2016/7/1 IESG提出
  - 2016/9/15 IESGミーティング議題

dnsop (10)

- IETF 96ミーティングの概要
  - IETF 95からの提案とその後の新規提案を進めるための議論が行なわれた。
  - 継続提案
    - terminology-bis
    - nsec-aggressiveuse
    - Special Names (TLD予約)
    - TLS-TCP-DNS implementation
  - 新規提案
    - session-signal
    - multiple responses/queries: 盛り上がる
    - bulk-rr
    - その他はタイムアウト

dnsop (11)

- draft-ietf-dnsop-nsec-aggressiveuse
  - DNSSECの不存在証明の活用
  - 可能なケースに対応 (NSEC, NSEC3, ドメイン名空間全体)
  - 部分的な実装も考慮
  - draft-wkumari-dnsop-cheese-shop をマージ
    - ルートサーバからの応答に限定
  - 著者にWarren Kumari氏を追加
    - Native speaker, 有識者(対抗ドラフトの著者)
  - Google Public DNSで、rootに適用した結果を発表
    - Googleではもうonにしたらしい

dnsop (12)

- draft-bellis-dnsop-session-signal
  - DNSにsessionの概念を追加する提案
  - dnssd WGのPUSH提案を複数の提案に分割、DNSへの変更が大きいsessionをdnsop WGで行う提案
  - sessionとは、長生きで双方向通信
    - DNS over TCP, DNS over TLSを想定 (UDP除外)
  - 新Opcode SESSION
  - Format
    - 16bit message ID
    - 16bit: QR, Opcode, Z, Rcode
    - そのあとに、TLV-DATA (QDCOUNTなどなし)
  - Call for adoption 7/22-8/12
    - 合意され、8/14付けでWG draft
    - draft-ietf-dnsop-session-signal

dnsop (13)

- draft-wkumari-dnsop-multiple-responses
  - 一つのクエリに対して、サーバがAdditional sectionに応答を追加する
  - BIND 9が、MXやSRVなどのクエリに、A, AAAAなどを勝手に追加することを、明確なプロトコルにしようという提案
  - www IN EXTRA 10 A images
    - DNSサーバに対して、www.$ORIGIN　Aのクエリに対して、images.$ORIGIN A を追加する応答を指示するEXTRA RR

dnsop (14)

- draft-bellis-dnsext-multi-qtypes
  - 一つのクエリ名で、複数のクエリタイプのクエリを同時に発行するEDNSオプションの提案
  - A, AAAAなどの組み合わせを同時に問い合わせる
  - 類似提案: draft-yao-dnsop-accompanying-questions
    - Paul Vixie + CNNIC
    - エレガントだけど複雑
  - ミーティング後に、複数応答・複数クエリをどう扱うかメールで議論が行なわれ、しばらくは決めないという考えが強かった。議論は継続する。

dnsop (15)

- draft-woodworth-bulk-rr
  - BIND 9の$GENERATEの拡張がほしい
  - IPv4逆引きでの$GENERATE例
    - 0/26 NS ns.example.jp.
    - $GENERATE 0-63 $ CNAME $.0/26.2.0.192.in-addr.arpa.
    - 64行のCNAMEを生成する → メモリを使用
  - IPv6の逆引きを書けるもの
    - $GENERATEだと事前展開なのでメモリを使用する
    - 事前展開しないで、動的な生成 → 正規表現
    - * 86400 IN BULK PTR ([0-f].[0-f].[0-f].[0-f].[0-f].[0-f].[0-f].[0-f]pool-W-${1}-${2}.${3}-${4}.${5}-${6}.${7}-${8}.example.com.)
  - DNSSECのon the fly signingが必要といったコメントや、例のwildcard labelがよくないといったコメントあり
  - (knot DNS にはその機能が実装されているが、開発者はコメントしていない)

dnsop (16)

- Special Names
  - プロトコルで使用するTLDを予約する話
  - IETF 95 arching BoFで専用WGを作るという話があったが停滞している様子 (話が出ない)
  - 問題点の指摘、改善案などのドキュメントをdnsop WGのドキュメントとすることが提案された程度
  - ipv4only.arpaの予約が追加で提案された
  - 時間もなく、それほどの議論は行われなかったが、Interim meetingを行うことが示された
    - まだ決まっていない

dnsop (17)

- WGLC前という状態で議論されなかったもの多数
  - 大量生産体制?: What's next in the WGLC pipeline
  - draft-ietf-dnsop-resolver-priming
    - 2016/8/4-8/19 WGLC, IESG提出見込み
    - リゾルバがRoot DNSサーバの情報をアップデートする動作について定めたもの (従来から実装されていたこと)
    - WGLCコメントでSecurity Considerationにon-path attackerからの攻撃について追記 (DNSSECで防御)
  - draft-ietf-dnsop-refuse-any
    - タイプANYクエリを拒否したいがRFC 1035違反
    - ANYに対して大きな応答を返さないことに変更
    - すべてではなく何かを返せばよい (any != all)

dnsop (18)

- 議論されなかったもの (続き)
  - draft-ietf-dnsop-edns-key-tag
    - DNSSEC validatorが、自分のtrust anchorを権威DNSサーバに伝えるEDNSオプション
  - draft-ietf-dnsop-rfc2317bis
    - ClasslessなIPv4逆引きのアップデート
    - 1 CNAME 1.0/25.2.0.192.in-addr.arpa
    - ただし expired
  - draft-ietf-dnsop-attrleaf
    - _udp, _tcp, _domainkeys, _sip, _sips, _443 など、プロトコルで使用される_で始まる特殊ラベルが増えたため、一括管理する仕組みの提案

dnsop (19)

- 議論されなかったもの(3)
  - DNS over HTTP: draft-song-dns-wireformat-http
    - DNSのbinary dataをそのままHTTPで伝達
    - DNSをブロックされた時にport 80/443を使いたい？
    - 2016/7/11~7/25 Call for adoption
    - 躊躇する意見がそれなりにあり、Candidateのまま
    - HTTP的に問題ないか懸念: httpbis WGで確認すること
  - draft-hoffman-dns-in-json のほうが好まれる？
    - 2014年の提案
    - DNSのbinary dataをJSONにしてHTTPで伝達
    - 9/3からdnsop mailing listで議論開始
      - Binary dataの表現方法(¥000など)の議論

dprive WG

- DNS PRIVate Exchange (dprive) WG
- スタブリゾルバとフルリゾルバの間の通信を暗号化するプロトコルを策定するWG

- 振り返り: IETF 91 2014年10月17日に設立
- 振り返り: IETF 92: 別ポート案とSTARTTLS案
- 振り返り: IETF 93: DTLS, EDNS Padding新規
- 振り返り: IETF 94: TLS,padding ほぼ完了
- 振り返り: IETF 95: 完了が見え、1時間と短め
  - DNS over DTLS, TLS/DTLS Profile, TLS 1.3 の議論
  - 2016/5/17 RFC 7858 (DNS over TLS) 発行
- IETF 96では非開催 (dnsopで実装報告)

dprive (2)

- RFC 7858, 2016/5/17発行
  - Proposed Standard
  - draft-ietf-drprive-over-tls
  - TCP port 853 で待ちうけ、(httpsのように)TLS処理
  - DNS over TCP のデータをTLS上に流す
    - 2オクテットのデータ長 + UDP DNSパケットと同じもの
  - サーバ認証プロファイルとしてOpportunistic(認証しない)と 事前設定
  - RFC発行により、正式に実装、使用できるようになった
- RFC 7830, 2016/5/10発行
  - Proposed Standard
  - draft-ietf-dprive-edns0-padding
  - 暗号データを守るためのEDNS0 Padding optionの追加

dprive (3)

- DNS over DTLS, draft-ietf-dprive-dnsodtls
  - UDP port 853を使用し、DTLSのデータとしてDNSを運ぶプロトコル
  - Mailing listでのreviewが進む
  - Working Group Last Call: 2016/8/16-8/30
    - 現在は細かい書き方の修正のみ (8/26)

dprive (4)

- 今後の提案 (DNS over DTLSの後)
  - draft-ietf-dprive-dtls-and-tls-profiles を進める
    - 2016/1/27にWG draftとして採択
    - DNS over (D)TLSの使い方を規定するもの
  - draft-bortzmeyer-dprive-step-2-00, 2016/7/16
    - フルリゾルバと権威サーバの間もTLSにする提案
  - IETF 97 (2016/11) にてBoFスタイルで議論を行なうという提案あり

dane WG

- DNS-based Authentication of Named Entities WG
- DNSにTLSの証明書を載せるWG
- Status
  - 2015/10/14にRFC 7671 (Updates), RFC 7672 (DANE SMTP), RFC 7673 (DANE SRV) 発行
  - 残件: SMIMEAなど
- 振り返り: IETF 92, 2015/3
  - OPENPGPKEY: WGLC完了→2015/5/23にIESGに提出
  - hex(先頭28バイト(sha256(tolower(localpart)))) ._openpgpkey.dom
- 振り返り: IETF 93, 2015/7
  - OPENPGPKEY変更案: base32(localpart)._openpgpkey.dom
- IETF 94, IETF 95, IETF 96: ミーティング非開催

dane (2)

- RFC 7929, 2016/8/5発行, Experimental
  - draft-ietf-dane-openpgpkey
  - 2015/5/23にIESGに提出 (-03)
  - メールアドレスで迷走
    - 問題点が多いため、実験に変更　(Status: Experimental)
    - ローカルパートの正規化 (CFWS, “.”の削除, Unicode NFC)
    - hex(先頭28バイト(sha256(localpart)))._openpgpkey.dom
      ↑ tolower小文字化が削除
    - アスキーの大文字小文字などのVariantは別の所有者名

dane (3)

- 残るドキュメント: draft-ietf-dane-smime-12
  - 2016/7/9-25 WGLC
  - OPENPGPKEYのIESG Reviewを受け、SMIMEも同じように変更
    - 実験に変更　(Status: Experimental)
    - ローカルパートの正規化 (CFWS, “.”の削除, Unicode NFC)
    - hex(先頭28バイト(sha256(localpart)))._openpgpkey.dom
      ↑ tolower小文字化が削除
    - アスキーの大文字小文字などのVariantは別の所有者名
  - IESG提出の見込み

dane (4)

- dane WGの今後: Milestone
  - Aug 2015 - Advance DANE operational guidance/errata document to IESG
  - Sep 2015 - Advance DANE SMIME document to IESG
  - Dec 2015 - Advance DANE IPSEC document to IESG
  - Dec 2015 - Advance DANE reverse binding (server to client) document to IESG
  - Oct 2016 - Recharter or close down

dbound WG

- Domain Boundaries WG
- Public Suffix List (PSL)の後継を考えるWG
- Public Suffix List
  - Cookieの取り扱い判定などで使用されている
  - 巨大なテキストの順序付きリスト
  - Mozilla Foundationがメインテナンス
  - https://publicsuffix.org/
- 振り返り
  - IETF 91:WG設立の合意
  - IETF 93:主な議題はDefine the problemで結論出ず
  - IETF 94:何を解決したいかがあいまいであり、結論出ず
  - IETF 95:非開催　2016/3/21に担当ADから進捗が見られないので進め方を提案するようにという厳しいメール

dbound (2)

- ある解決案の提案者が非公式に集まろうと提案
  - 提案をすすめたいとのこと
  - あきらめられない人はいる
  - やらないといけないことは残っているのは事実
  - メーリングリストでの議論は続く見込み

dnssd WG

- Extensions for Scalable DNS Service Discovery
- DNSを使ったサービスディスカバリを作るWG
  - DNS-SD (RFC 6763)をベースに、複数ネットワークセグメントに対応したものを標準化する
- 振り返り: IETF 91
  - Long Lived Queries,脅威モデル
  - ハイブリッドプロキシー
- 振り返り: IETF 92
  - DNS Push: LLQの代わりに Update
- 振り返り: IETF 93: 基本的には継続した議論
- 振り返り: IETF 94: 継続した議論だが若干減速気味
- 振り返り: IETF 95
  - Hybrid ProxyをIESGに提出見込み (→まだ出てない)
  - DNSSD Privacy, DNS Push

dnssd (2)

- draft-ietf-dnssd-hybrid (dnssdのコアプロトコル)
  - dnssdをmDNSとDNSのHybrid proxyとして実装
  - リンクごとにドメイン名を設定、ルータなどでproxyを動かす
    - 例: link1.example.com, link2.example.com, …
  - Proxy: <name>.local ⇔ <name>.link1.example.com
    - <name>.link1.example.com PTRクエリを受け取ると、<name>.local PTRクエリをmDNSで送り、応答を書き換えて返す
  - Browse設定を管理者が行なう
    - b._dns-sd._udp.example.comPTR link1.example.com
PTR link2.example.com
…
  - IETF 95前のコメントが反映されていないため、進めるように指示があったが、現在はexpired
  - dnssdの時間に、"Homenet vs DNSSD Hybrid proxy"という発表があり、Homenetの要求とdnssdの違いが示された
  - homenet WGではUnicast DNSとmDNSのhybridとして、正引き逆引きゾーンを持ち、mDNSデータについてはlinkごとにcacheを持つ

dnssd (3)

- draft-ietf-dnssd-push-07
  - DNS Push Notifications
  - DNS/TCPで名前管理サーバに接続し、ゾーン名を指定してSUBSCRIBE (rcode 6)メッセージを送るとSUBSCRIBE
  - 名前管理サーバは、DNS UPDATEのフォーマットでクライアントにゾーン情報の変化を送る
    - 最初は全情報？
  - Session定義をdnsopに委任
- draft-huitema-dnssd-privacy-00
  - Privacy Extensions for DNS-SD
  - プライバシーのために、ホスト名をランダムに、ID類を64bitのハッシュにするという提案
  - 許可したペア間だけで名前解決できるアクセス制限や、encodedな名前を使うことなどが提案された
  - 興味がある人は多そうで、call for adoptionがかかる見込み

Homenet WG

- Home Networking
- (IETF Chairの)家のネットワーク

- 振り返り: IETF 93 (2015/7), IETF 94 (2015/11)
  - Homenetでの名前解決にはdnssdのhybrid proxy使用
  - 家の情報をDNSに出す仕組みが提案されているが停滞
  - draft-ietf-homenet-front-end-naming-delegation
    - 家でhidden masterを動かし、ISPにゾーン転送してDNSSEC署名してISPのDNSサーバで公開
  - draft-ietf-homenet-naming-architecture-dhc-options
    - DHCPにhybrid proxyなどのオプションを追加する提案
- 振り返り: IETF 95 (2016/4)
  - homenetでの名前解決の新提案
    - dnssd hybrid proxyは使えないので、DNS Update + mDNS snoop
  - Name spaceの議論: Global, Local, Guest (客向け)

homenet (2)

- RFC 7788 Home Networking Control Protocol
  - Errata指摘
    - 2016/4/23に発行されたRFC 7788に ”.home” TLDをdefaultで使用すると書かれていた
    - ただし、正式な予約手続きは書かれていない
    - 2016/4/26にErrataとして”.home”のところを削除する訂正案をdnsop chairが投稿
  - IETF 96では、RFC 7788の扱いが議論された
    - . home, .homenetなどを予約するという案も存在
    - .homeを削除した新しいRFCを出すなどの案があったが、現在のままなにもしないという案が好まれた

homenet (3)

- draft-lemon-homenet-naming-architecture
  - homenet naming architecture
  - Homenet Naming Databaseで情報管理
    - mDNS browse, snoopで情報収集
    - UPDATEで明示的に登録
  - 複数のname space
    - Global, Local (.homenet想定), Guest
  - dnssd hybrid proxyの問題点の指摘
    - リンク名をだれかが設定する必要がある
    - リンク間の名前衝突問題が起きる
    - 名前衝突を伝えることができない

Bundled-domain-names BoF

- draft-yao-bundled-name-problem-statement
- draft-yao-dnsext-bname
- 水曜日の昼休みに開催 (Bar Bofのため)
- 異なるゾーンを同じものとして扱いたいという提案
  - DNAMEではOwner nameを変換できないため
  - 例: 簡体字と繁体字を同一として扱う: .中国 と .中國
  - 同じとするにはrootにDNAME: 中國 IN DNAME 中国
    - example.中國は、example.中国に変換
  - 中國 zoneにDNAMEを大量に書く
    - example.中國 IN DNAME example.中国
    - ただし、example.中國 そのものは変換されない
  - あるいは、DNAME+CNAME == BNAME を標準化
- problem statementから始めるべきという意見が多い

IEPG

- 運用に関する話題を扱うinformalな集まり
- 9件の発表 (DNS関連 4)
  - Roa Misconceptions - Randy Bush
  - Yeti Status Update - Davey Song, Shane Kerr
  - DNS Privacy - Sara Dickinson, Allison Mankin
  - Cryptech Update - Lief Johansson
  - There's Gold in the Data Stream - Daniel Karrenberg
  - IANA Registry Updates - Sabrina Tanamal
  - IPv6 Deployment Survey - Jordi Palet Martinez
  - IPv6 Performance - Geoff Huston
  - DNSSEC Encryption Algorithm Agility - Dan York

IEPG (2)

- Yeti Status Update - Davey Song, Shane Kerr
  - Status
    - 3箇所でIANA root zoneからYeti root zoneを生成
    - 25 Yeti root servers (soon 26)
    - 14 Yeti root operators (soon 15)
    - 400以上のIPアドレスがYeti rootを検索
    - 30以上のリゾルバ、100qps以下
  - 実験
    - 複数のゾーン生成箇所で、別々のKey使用
    - 2048bit ZSK実験
    - KSK Rollover実験
    - うまくいったようで、レポートが出るらしい
  - IETF 97の前の日、土曜にWorkshop

IEPG (3)

- DNS Privacy実装報告
  - UnboundがDNS over TLSを実装済
  - Qname minimisation: Unbound, Knot実装済
  - Stubではgetdns apiがすべて実装済
- There is Gold in that Stream
  - RIPE Atlasで、DNSサーバへのping, traceroute, DNSクエリを行え、研究できる
- DNSSEC Encryption Algorithm Agility
  - RSAではなくECDSAを使いたいという話
  - RCDSAのほうが鍵長を短くできるため

Root DNSSEC key rollover関連

- Increasing the Root Zone ZSK Size
  - 2016/10/1にRoot zone ZSK sizeを1024bitから2048bitに変更する計画
  - Daune Wessels @ Verisign = Root zone operator
  - 政府的に1024bit RSAの使用を継続しにくいと推定
- Rolling the Root Key
  - 元VerisignのMatt Larson氏がICANNのVP of Researchという立場で発表
  - DNSSECのRoot trust anchorを変更する話
  - RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors で自動更新すること
  - 資料 https://www.icann.org/kskroll

Root DNSSECスケジュール

- https://www.icann.org/en/system/files/files/ksk-rollover-at-a-glance-22jul16-en.pdf
- 2016年10月: ZSKサイズを2048ビットに変更
- 2016年10月: 新しいTrust Anchorを生成
- 2017年2月: ICANN Web siteで公開
- 2017年7月: Root zoneに公開
- 2017年10月: 新KSKで署名開始
- 2018年1月: 古いKSKの無効化開始/revocation
- 2018年3月: 完了
  - このときまでにTrust anchorを更新しないとエラー

参考

- www.ietf.org
  - 過去のIETFミーティングの資料、議事録あり
- www.rfc-editor.org
  - RFC
- www.iepg.org
  - IEPGミーティングの資料
- https://www.icann.org/resources/pages/ksk-rollover