IETF 報告会
DNS 関連 WG

東京大学 情報基盤センター
関谷 勇司

東京大学
THE UNIVERSITY OF TOKYO

自己紹介

- 本職
  - 東京大学 情報基盤センター
  - 学内基幹ネットワークの設計・運用
  - ネットワークを中心とした実践的な研究活動
- 研究活動
  - WIDE Project ボードメンバー
  - 運用と研究を兼ねた活動
- その他活動
  - Interop Tokyo NOC ジェネラリスト (2010 〜 現在)
  - Interop Tokyo 会場ネットワークの統括責任者

東京大学 THE UNIVERSITY OF TOKYO

DNS 関連 WG

- そんなにありません
  - dnsext (DNS Extensions)
  - dnsop (Domain Name System Operations)
  - dane (DNS-based Authentication of Named Entities)

DNS 関連 WG

- そんなにありません
  - **dnsext (DNS Extensions)**
  - **dnsop (Domain Name System Operations)**
  - dane (DNS-based Authentication of Named Entities)

東京大学 THE UNIVERSITY OF TOKYO

dnsext WG

- Charter
  - The DNS has a large installed base and repertoire of protocol specifications. The DNSEXT working group will actively advance DNS protocol-related RFCs on the standards track while thoroughly reviewing further proposed extensions. The scope of the DNSEXT WG is **confined to the DNS protocol, particularly changes that affect DNS protocols "on the wire"** or **the internal processing of DNS data**. DNS operations are out of scope for the WG.

dnsext WG working items

- DNSSEC and TSIG/TKEY algorithm maintenance
- Mechanisms that complement, or are alternatives to, TSIG and SIG(0)
- Hardening DNS protocol and providing guidance to implementers
- Advancing existing DNS-related Proposed Standard RFCs to Draft/Full Standard
- Obsoleting DNS-related RFCs
- Improving DNS zone synchronization mechanisms
- Examining transport protocols, possibly adding new ones
- Mechanisms to alias DNS trees or parts thereof

東京大学 THE UNIVERSITY OF TOKYO

Active WG drafts (dnsext)

- draft-ietf-dnsext-dnssec-algo-imp-status-04
  - Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status
  - in RFC Editor Queue
- draft-ietf-dnsext-dnssec-algo-signal-10
  - Signaling Cryptographic Algorithm Understanding in DNSSEC
  - in IESG Evaluation

東京大学 THE UNIVERSITY OF TOKYO

最近の RFC (dnsext)

- RFC6895
  - Domain Name System (DNS) IANA Considerations
- RFC6891
  - Extension Mechanisms for DNS (EDNS(0))
- RFC6840
  - Clarifications and Implementation Notes for DNS Security (DNSSEC)
- RFC6725
  - DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates
- RFC6672
  - DNAME Redirection in the DNS
- RFC6605
  - Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
- RFC6604
  - xNAME RCODE and Status Bits Clarification

最近の dnsext WG

- もう特段の事情がなければ会合は開催されない
  - IETF80 にてこの方針が発表され、その後 IETF83 で一度だけ会合が開催されたのが最後
- WG shutdown の段階に向かっている
  - 予定では May 2013 となっているが。。。
- Mailing List 上では散発的に議論が起こっている

RFC6891

- Extension Mechanisms for DNS (EDNS(0))
- Changes since RFCs 2671 and 2673
  - Support for the OPT record is now mandatory.
  - Extended label types remain available, but their use is discouraged as a general solution due to observed difficulties in their deployment on the Internet, as illustrated by the work with the "Binary Labels" type.
  - RFC 2673, which defined the "Binary Labels" type and is currently Experimental, is requested to be moved to Historic.
  - Made changes in how EDNS buffer sizes are selected, and provided recommendations on how to select them.

東京大学 THE UNIVERSITY OF TOKYO

RFC6672

- DNAME Redirection in the DNS
  - The DNAME record provides redirection for a subtree of the domain name tree in the DNS. That is, all names that end with a particular suffix are redirected to another part of the DNS.
  - This document obsoletes the original specification in RFC 2672 as well as updates the document on representing IPv6 addresses in DNS (RFC 3363).
- Changes from RFC 2672
  - The EDNS option to signal DNAME understanding and compression has never been specified, and this document clarifies that there is no signaling method (Section 2.5).
  - Recursive caching servers MUST perform CNAME synthesis on behalf of clients (Section 3.4).
  - Rules for dynamic update messages adding a DNAME or CNAME RR to a zone where a CNAME or DNAME already exists are detailed in Section 5.2.

東京大学 THE UNIVERSITY OF TOKYO

RFC6604

- xNAME RCODE and Status Bits Clarification
  - The Domain Name System (DNS) has long provided means, such as the CNAME (Canonical Name), whereby a DNS query can be redirected to a different name. A DNS response header has an RCODE (Response Code) field, used for indicating errors, and response status bits. This document clarifies, in the case of such redirected queries, how the RCODE and status bits correspond to the initial query cycle (where the CNAME or the like was detected) and subsequent or final query cycles.

draft-jabley-dnsext-eui48-eui64-rrtypes

- 48-bit Extended Unique Identifiers (EUI-48) and 64-bit Extended Unique Identifiers (EUI-64) are address formats specified by the IEEE for use in various layer-2 networks, e.g. ethernet. This document defines **two new DNS resource record** types, **EUI48** and **EUI64**, for encoding ethernet addresses in the DNS.
- ここ数日 ML 上で議論になっている draft
  - 何のために？
  - ホスト名に対する EUI48 or EUI64
  - 手続きにのっとって new RR を申請しているから問題ない

東京大学 THE UNIVERSITY OF TOKYO

dnsop WG

- Charter
  - The DNS Operations Working Group will **develop guidelines for the operation of DNS software servers and the administration of DNS zone files**. These guidelines will provide technical information relating to the implementation of the DNS protocol by the operators and administrators of DNS zones.

dnsop WG working items

1. Define the processes by which **Domain Name System (DNS) software may be efficiently and correctly administered, configured, and operated** on Internet networks. This will include root zone name servers, gTLD name servers, name servers for other DNS zones, iterative DNS resolvers, and recursive DNS resolvers. As part of this effort, the group will produce documents explaining to the general Internet community what processes and mechanisms should be employed for the effective management and operation of DNS software.
2. Publish documents concerning **DNSSEC operational procedures**.
3. Publish documents concerning the **IPv6 DNS operational procedures** and DNS-related **IPv6 transition and coexistence issues**.
4. Publish documents concerning the operations of the **root and TLD services, and DNS resolvers**.

東京大学 THE UNIVERSITY OF TOKYO

Active drafts (dnsop)

- NO WG drafts

- Related drafts
  - draft-andrews-dnsop-rfc6598-rfc6303-02
  - draft-gersch-dnsop-revdns-cidr-04
  - draft-jabley-dnsop-anycast-mapping-01
  - draft-licanhuang-dnsop-distributeddns-13
  - draft-wkumari-dnsop-omniscient-as112-02

最近の RFC (dnsop)

- RFC6841
  - A Framework for DNSSEC Policies and DNSSEC Practice Statements
- RFC6781
  - DNSSEC Operational Practices, Version 2
- RFC6305
  - I'm Being Attacked by PRISONER.IANA.ORG!
- RFC6304
  - AS112 Nameserver Operations
- RFC6303
  - Locally Served DNS Zones
- RFC6168
  - Requirements for Management of Name Servers for the DNS

draft-wkumari-dnsop-omniscient-as112

- AS112 に新たなゾーンを加えるのは難しい
  - 管理組織が分散されているから
- “empty” zone という概念を導入し、どのようなゾーンでも AS112 に導入できるようにしては？
- 上位のゾーンから “empty” zone に委譲すると自動的に AS112 サーバの管轄となる

RFC6303

- Locally Served DNS Zones
  - Experience with the Domain Name System (DNS) has shown that there are a number of DNS zones that all iterative resolvers and recursive nameservers should automatically serve, unless configured otherwise. RFC 4193 specifies that this should occur for D.F.IP6.ARPA. This document extends the practice to cover the IN-ADDR.ARPA zones for RFC 1918 address space and other well-known zones with similar characteristics.

IETF86 での会合 (dnsop)

1. DNS in JSON
   - draft-bortzmeyer-dns-json-00
   - 既にいくつかの場面で使われ始めている。Web を通じての DNS データやりとりとか。そのために標準化をしようという動き。
   - この WG でやるのが正しいのか？JSON WG？
   - 標準化すること自体は賛成

IETF86 での会合 (dnsop)

2. Negative Trust Anchors
   - zone の鍵が有効期限切れになっていたり、DNSSEC 的な設定に問題があると名前が引けなくなる。
   - Resolver サーバの管理者はどうにもできない。でもユーザからのクレームは来る。
   - 一時的に DNSSEC の検証を無効にするドメインを指定できれば。

IETF86 での会合 (dnsop)

3. Automating DNSSEC delegation
   - KSK rollover を簡単にしよう
   - 現在は DS レコードを親ゾーンに送付して公開してもらうことで信頼の連鎖を形成
   - CDS (Child DS) レコードの導入
   - 子ゾーンにて CDS を発行し、それを親ゾーンの管理者が既に存在する DS レコードと置き換えることで更新
   - 手法としては有効に機能する
     - レジストラの既存のビジネスモデルを壊す？