

DNSトリビア（出張版）

2011年11月30日
DNSOPS.JP BoF

森下 泰宏

@OrangeMorishita

「DNSトリビア」とは

- 私が**個人的に**twitterでやっている企画
- DNSについて意外に知られていなさそうなことや、知っていると思える(かも知れない?)ことを不定期にツイート
- 気分転換したい時の頭の体操と**自己満足**
 - 140文字以内にまとめる
 - 最初は大抵はみ出している

「DNSトリビア」とは(続き)

- 現在までに22項目をツイート
- 50項目ぐらいまではツイートしたい
- 100項目ツイートできたら書籍にでも(無理w)

- 今日はそのうちの5つを簡単にご紹介します

その7:日本のむかしばなし: ネームサーバー3系列

- かつて日本のネームサーバーにはA、B、Cの3系列が存在していた。系列Aで海外と接続可能な、系列Bで国内すべてのJPドメイン名をそれぞれ管理し、系列Cで海外に接続可能な国内組織向けに、通常のDNSツリーと系列Bを参照(マージ)する形で運用されていた。
- 系列A: 海外向け(海外からのみ参照)
- 系列B: 国内向け(海外到達性がない国内組織)
- 系列C: マージ(海外到達性がある国内組織)
 - jpゾーンの下を系列Bのものに差し替え
 - 今で言う「Split DNS」を国全体で運用

その7:日本のむかしばなし: ネームサーバー3系列

- 背景: 海外に到達できないネットワークの存在
 - AUPによるフィルタリング
 - 日本-米国-日本という経路を避けたい、などの事情
- 1995年5月16日に廃止
- 今のJP DNSは「**系列A**」の子孫
- 海外向けとして、当時海外回線を保持していたネットワークに、当時のJPNICがセカンダリサーバーを依頼
 - プライマリ: JPNIC
 - アカデミック(ABC順): JOIN(後に廃止)、SINET、WIDE
 - 商用(ABC順): IIJ、Spin(後に廃止)

その10:AS112で実験された IP Anycast

- DNSサービスにおけるIP Anycastの利用はAS112プロジェクトにおいて実験され、その嚆矢(こうし)となった。それにより得られた運用経験はルートサーバーをはじめとする、その後の広域DNSサービスへのIP Anycast導入に役立てられた。
- AS112:プライベートアドレスの逆引きゾーン
- トラブっても致命傷にならない(はず)
 - その割に**色々とあった**ようですが...
- 仮に困った人がいても「そもそもそんな問い合わせをインターネットに出すんじゃない(RFC 6303)」と**冷たく言い放つ**ことができた
 - もちろん実際には冷たく言い放ってはいません...

その11:イギリスのむかしばなし: 逆順だった.uk

- 1980年代、英国は既に独自の名前解決サービス(NRS)を使っており、自国はUKでかつuser@UK.AC.SITEのように、表記がDNSとは逆であった。DNSへの移行時に.gbへの切り替えが併せて計画されたが実施されず、.ukが継続使用された。
- 英国のゲートウェイサーバーで外国(から|へ)の電子メールアドレスを書き換え、**相互変換**していた
 - 英国から日本に出す場合、使うゲートウェイの仕様により指定するアドレスが異なる場合があった → **混乱**のもと
 - user%u-tokyo.ac.jp@uk.ac.ucl.cs.nss
 - user%jp.ac.u-tokyo@uk.ac.earn-relay
- 1990年代前半までに他国と同じ順番に変更された
- でも**DNSプリフェッチ**のことを考えると、実は**逆順のほうがよかった**のかもしれない...

その13:DNSSECの署名は有効期限ではなく「有効期間」

- DNSSECの署名 (RRSIGレコード)には、開始時刻と満了時刻の双方が存在する。そのため厳密には「有効期限」ではなく「有効期間 (validity period)」と表現される。
- 当時「クレジットカードとは違う」とツイートしたところ、@tss_0101さんから「**ダイナースのクレジットカード**には開始も書かれている、というご指摘をいただきました。感謝いたします



確かに2つある！

その18:許されるCNAMEの段数は 実装依存

- CNAMEの連鎖(CNAMEの先がまたCNAME)はたどられるべきであるとRFC 1034には記述されている。ただし、CNAMEの連鎖を何段まで許すのかは決められておらず、実装依存である。
- Google Public DNSはCNAMEの連鎖が**数十段あっても**名前を引けるらしい
- (**事後資料で追加**)@ioaiaさんの実験結果によると、Google Public DNSではCNAMEの連鎖を**182段**まで処理可能だったそうです
- (**事後資料で追加**)いろいろな意味ですごいです…

ありがとうございました！

今後ともよろしくお願いいたします

<http://twitter.com/OrangeMorishita>