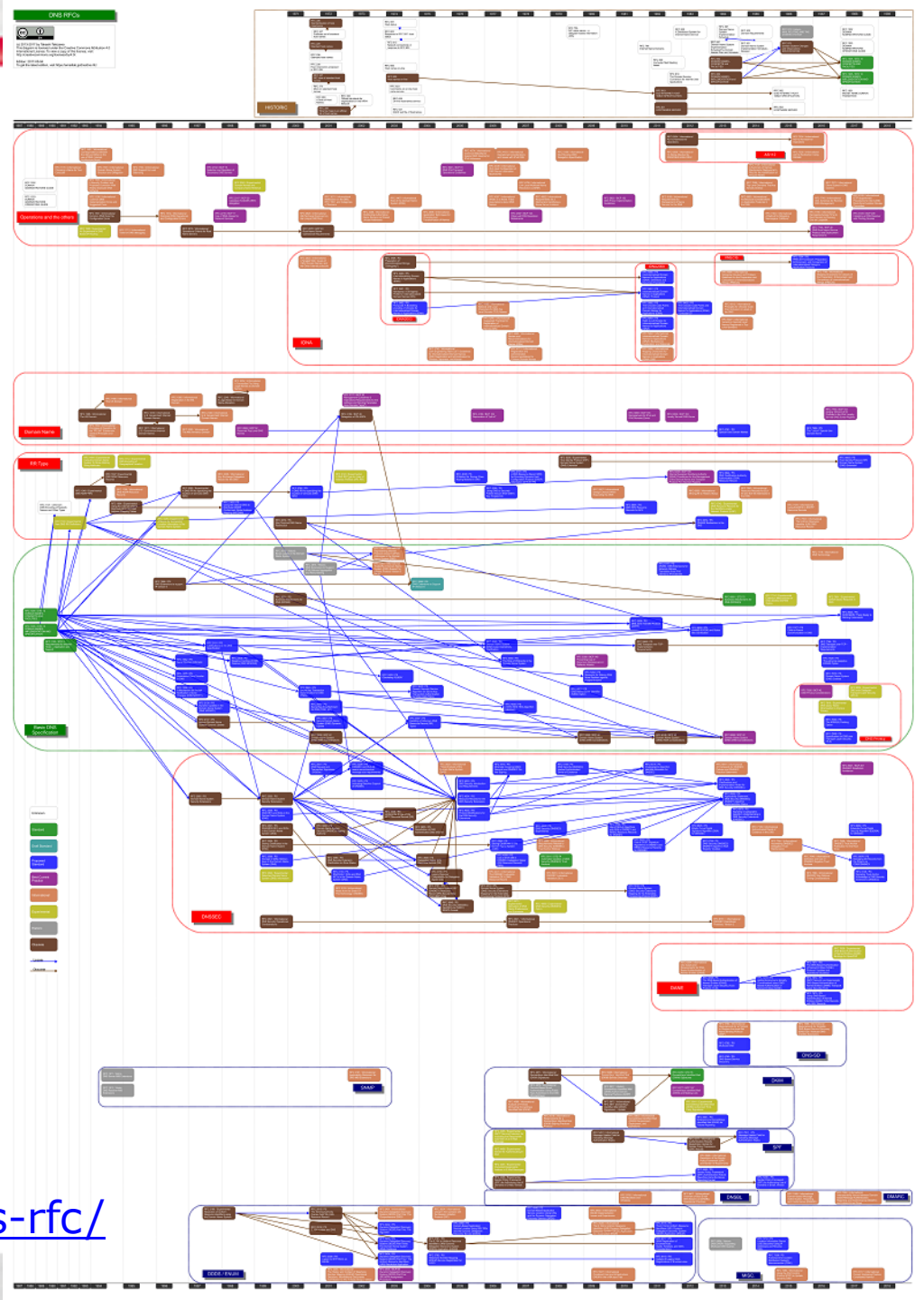
DNSに関する常識の変化
～疑問編～

山口崇徳 (インターネットイニシアティブ)

DNSの歴史

- プロトタイプ RFC882, 883 (1983)
- 現行仕様 RFC1034, 1035 (1987)
- そして長い長い仕様拡張の歴史
  - 拡張だけでなく基本部分の変更も



DNS RFC系統図
https://emaillab.jp/dns/dns-rfc/

SOA minimum フィールド(1)

- SOA レコードの数あるパラメータのうちのひとつ

```
iij.ad.jp.      86400 IN SOA bh0.iij.ad.jp. postmaster.iij.ad.jp. (
                1498493404 ; serial
                3600       ; refresh (1 hour)
                1800       ; retry (30 minutes)
                1209600    ; expire (2 weeks)
                3600       ; minimum (1 hour)
                )
```

- これまで何度か意味が変わっている

SOA minimum フィールド(2)

- RFC1035 (1987)
  - そのゾーン内のレコードの最小 TTL
  - が、RFC2308 曰く「実際にこの意味で使われたことはない」
- RFC1912 (1996)
  - 「RFC1035 には最小 TTL って書いてるけど、みんなデフォルト TTL として実装してるみたいだね」
    - この RFC によって定義が変わったのではなく、現状を追認しただけ
- RFC2308 (1998)
  - ネガティブキャッシュの TTL
  - 現在の意味はこれ

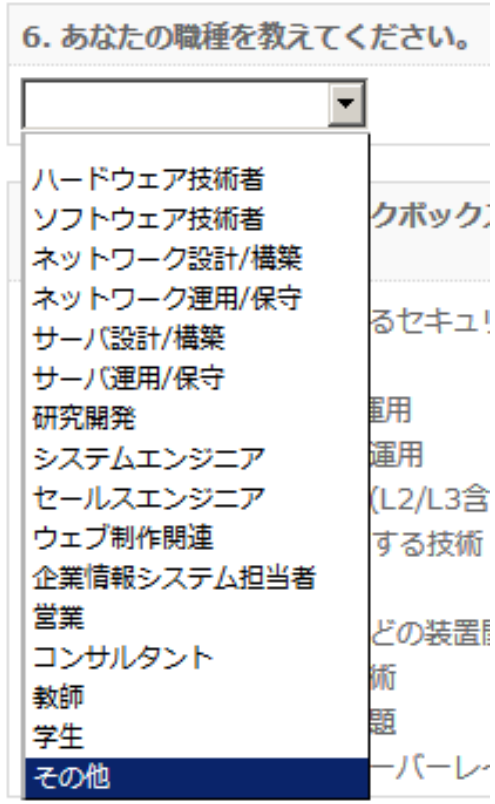
変わりゆく Best Current Practices

- BCP はあくまでその当時における最善策
- 時代の変化に合わせてプロトコルの修正・拡張がおこなわれるだけでなく、運用における BCP も時代とともに廃れて historical practices になってゆく

- 本セッションは、そんな DNS の温故知新がテーマです

話者の紹介

- 藤原和典
  - JPRSの技術研究部
  - JANOG 11: DNS正引きの実態
  - JANOG 12: ENUMの野望
  - JANOG 15:ネームサーバは内部名で---from JPRS---
  - JANOG 25:メールアドレスの国際化 ～ASCIIではないメールアドレスがやってくる～
  - JANOG 31:メールアドレスの国際化(JANOG25からの変更点)
  - JANOG 37.5: DNS-OARCワークショップ報告 (Root Zone ZSKサイズの変更)
- 山口崇徳
  - IIJ で「その他」をやってる人



ネームサーバは内部名で?

内部名と外部名

- あるドメインのネームサーバがそのドメインのサブドメインなら内部名

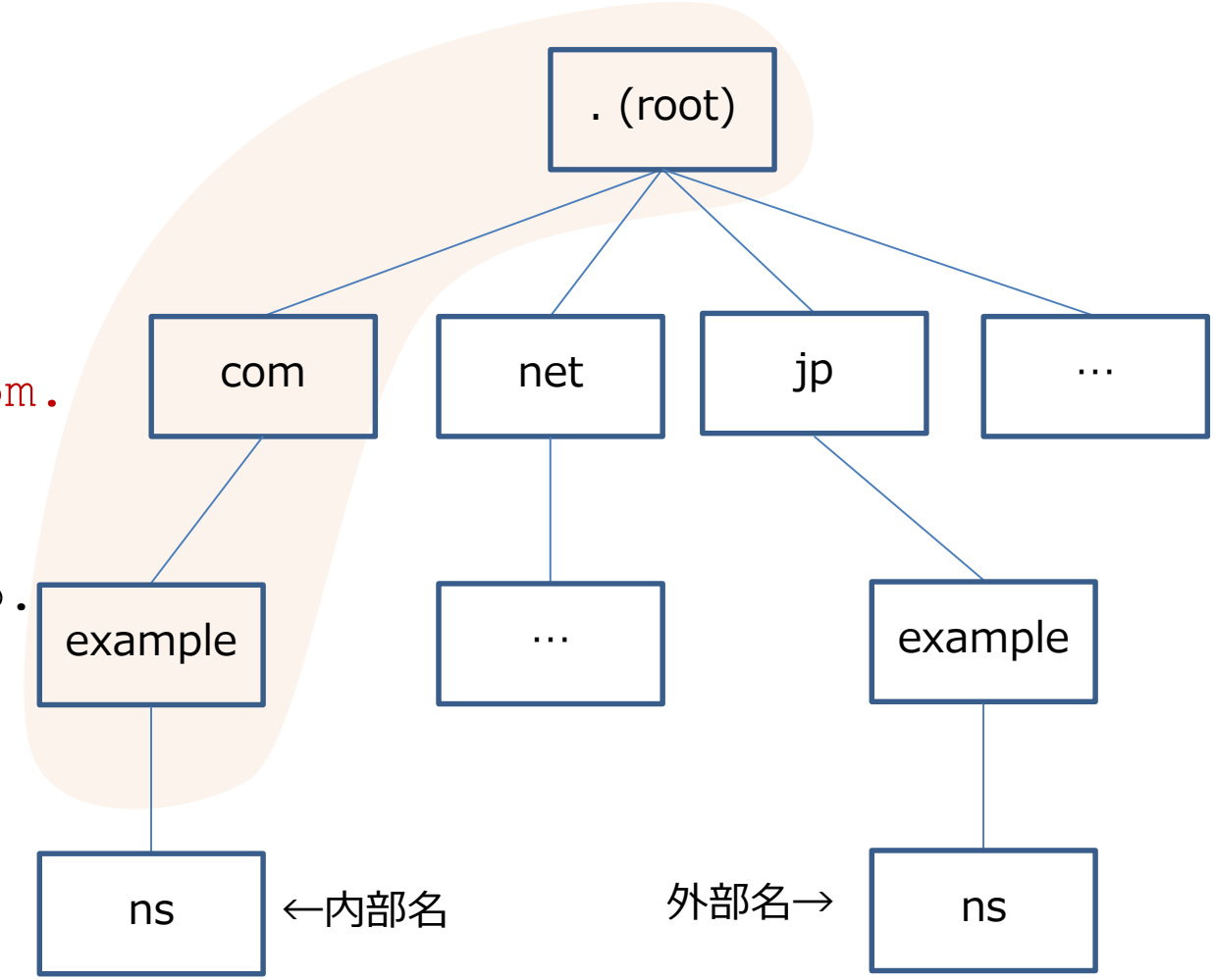
```
example.com. IN NS ns.example.com.
```

- 別ドメインならば外部名

```
example.com. IN NS ns.example.jp.
```

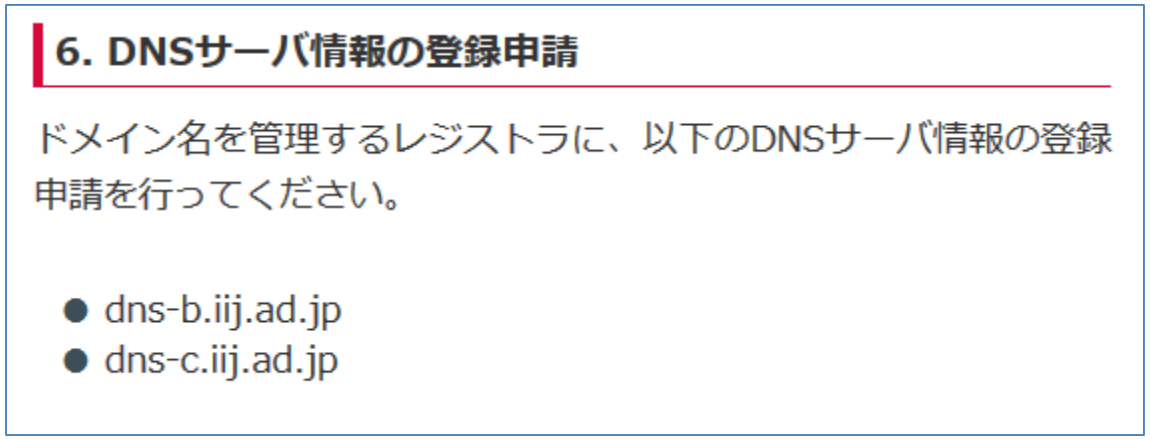
- 内部名の場合のみ、上位ゾーンに glue が必要

```
ns.example.com. IN A 192.0.2.1
```



ネームサーバは外部名で

- IIJ の DNS サービスでは、外部名を登録するようにマニュアルに記載
  - 他社サービスもほとんどそう



- 理由: もしサーバの IP アドレス変更が必要になったとき、
  - 外部名: 該当サーバの A/AAAA レコード変更で終わり
    - サービス提供者が1回作業すればよい
  - 内部名: 収容している顧客ドメインすべての glue 変更
    - 顧客それぞれがレジストラに変更申請しなければならない
    - 実質不可能

逆引きゾーン

- 外部名で書かざるを得ない…

```
2.0.192.in-addr.arpa. IN NS ns.example.com.
2.0.192.in-addr.arpa. IN NS ns.2.0.192.in-addr.arpa.
```

  - DNS の仕様上できないわけではないが、NIR/LIR/RIR が受け付けてくれないので実質不可

- なのに…

https://www.janog.gr.jp/meeting/janog15/data/12-dns-fujiwara.pdf

ネームサーバは内部名で

--- from JPRS---

JANOG15
2005年1月21日
株式会社日本レジストリサービス
藤原和典 <fujiwara@jprs.co.jp>

BINDキャッシュサーバの動作

https://www.janog.gr.jp/meeting/janog15/data/12-dns-fujiwara.pdf

- グルーがない参照が2段続くとBIND 8.2キャッシュサーバからは検索不能
  - www.bad2.co.dnslab.jp の A の検索
    isp.ne.dnslab.jp, isp.ad.dnslab.jpを使い上記を再現
- BIND 8.3で修正され、引けるようになったが、時間がかかる
  - ネームサーバのアドレスがキャッシュに入ると速い
  - 二度目のクリックで読めるようなこともある
- BIND 9では問題なし、時間も短い
- 検索できたりできなかったりする名前がある場合、ネームサーバの設定を確認しましょう

ネームサーバは内部名で?

- 外部名のネームサーバはほんとにやっちゃダメなの?
- 外部名で指定しろって言ってる DNS サービスは滅ぶべきなの?
  - っていうか、サービス提供側からすると、勝手に内部名で登録してるお客さんマジ困るんですけど…

短いTTLって危険なの?

柔軟な運用

- 昨今のサービス運用で求められること
  - 可用性、柔軟性、拡張性、…
  - 必要なときに迅速にサーバ構成を変更できて当たり前
- そのためには、DNS の TTL はあまり長くしたくない
  - いまの世の中、構成変更に丸1日かかるとかありえない
- CDN を利用する場合、CNAME の先の A/AAAA は CDN 事業者が握っていて、利用者自身で TTL を指定できない
  - で、CDN 事業者は短い TTL を設定している

```
www.example.com.          86400 IN CNAME  hoge.cdn-provider.tld.
hoge.cdn-provider.tld.       30 IN A      192.0.2.1
```

https://www.janog.gr.jp/meeting/janog19/files/DNS_Minda.pdf

これでいいのかTTL

短いDNS TTLのリスクを考える

2007年1月26日

民田雅人
株式会社日本レジストリサービス

JANOG 19@沖縄県那覇市

誕生日攻撃による毒入れ

https://www.janog.gr.jp/meeting/janog19/files/DNS_Minda.pdf

- 各DNS RR(リソースレコード)のTTLが短いと
  キャッシュサーバの問合せ頻度は高くなる
  - TTLが86400秒 → 1日に**1**回 問い合わせ
  - TTLが30秒 → 1日に**2880**回 問い合わせ
- 気長に嘘のDNS応答をキャッシュサーバに
  送り続ければ、**そのうち**当たる

「そのうち」が**意外に短い**

Kaminsky Attack

- 従来のキャッシュポイズニングは、攻撃対象の名前がキャッシュされていないことが前提だった
  - TTLが短いほどキャッシュから消えやすい = 毒入れリスクが大きい
- 2008年、Kaminsky / Müller が攻撃対象と異なる名前を使ってポイズニングする手法を発見
  - キャッシュされていない名前は無数にある
  - TTL に関係なく攻撃できるように
- Kaminsky 以降、TTL の値に関係なく毒入れリスクは同じ
- …のはず

DNSはデータの更新に冷たい

- 「このデータは更新されたから、キャッシュに残っていても新しいのに替えてね」と伝える機能がない
- データの更新前にTTLを短くしておく必要あり
  - 緊急に更新したい場合には対応できない
- 「じゃ、TTLを常に短くしておけばいいんじゃね?」
  - 某CDNなど
- しかし、常にTTLを短くすることはリスクを伴う
  - 参考:これでいいのかTTL
    ―短いDNS TTLのリスクを考える―
    - http://www.janog.gr.jp/meeting/janog19/files/DNS_Minda.pdf
  - DNSの系全体の負荷も増える
    - 権威DNSサーバー（自分の負荷）
    - キャッシュDNSサーバー（他人の負荷）

https://www.slideshare.net/OrangeMorishita/20111029-part1dnsdis

短い TTL って危険なの?

- Kaminsky 以後、2011年の資料でも短い TTL のリスクを肯定してるような…?
- 短い TTL ってほんとに危険なの? やっちゃいけないの?