DNSに関する常識の変化

藤原和典 (JPRS)
fujiwara@jprs.co.jp

2017/7/27, JANOG 40

JANOG 15 (2005/1)
「ネームサーバは内部名で
---from JPRS---」
のアップデート

紛弾されていた資料を書いたのは私でした

JANOG 15での内部名設定の推奨について (今までを振り返る)

- 変わっていないこと
  - 内部名でグルーがあるほうが名前解決が早いのは事実である
- 書き足りなかったこと
  - サービス仕様に反してまで内部名にすることはよくない
- 資料が古いので現実に則していないこと
  - BIND 8 ってなんですか？
  - キャッシュサーバーなどといった間違った用語の使用　恥ずかしい
  - 内部名の定義が曖昧

ネームサーバ設定ガイド (2017年版)

- DNSプロバイダの指定がある場合はその通りに設定すること
  - 勝手に内部名設定にしたりはしないこと

- ネームサーバ、ゾーン情報の双方を自前で設定する場合は、内部名にしてグルーを添付すると、名前解決時間を短くできる

- ネームサーバ名を保持するドメイン名のネームサーバ名は、内部名で登録すること (DNSプロバイダ)
  - 外部名を多段で使用すると名前解決に時間がかかるため

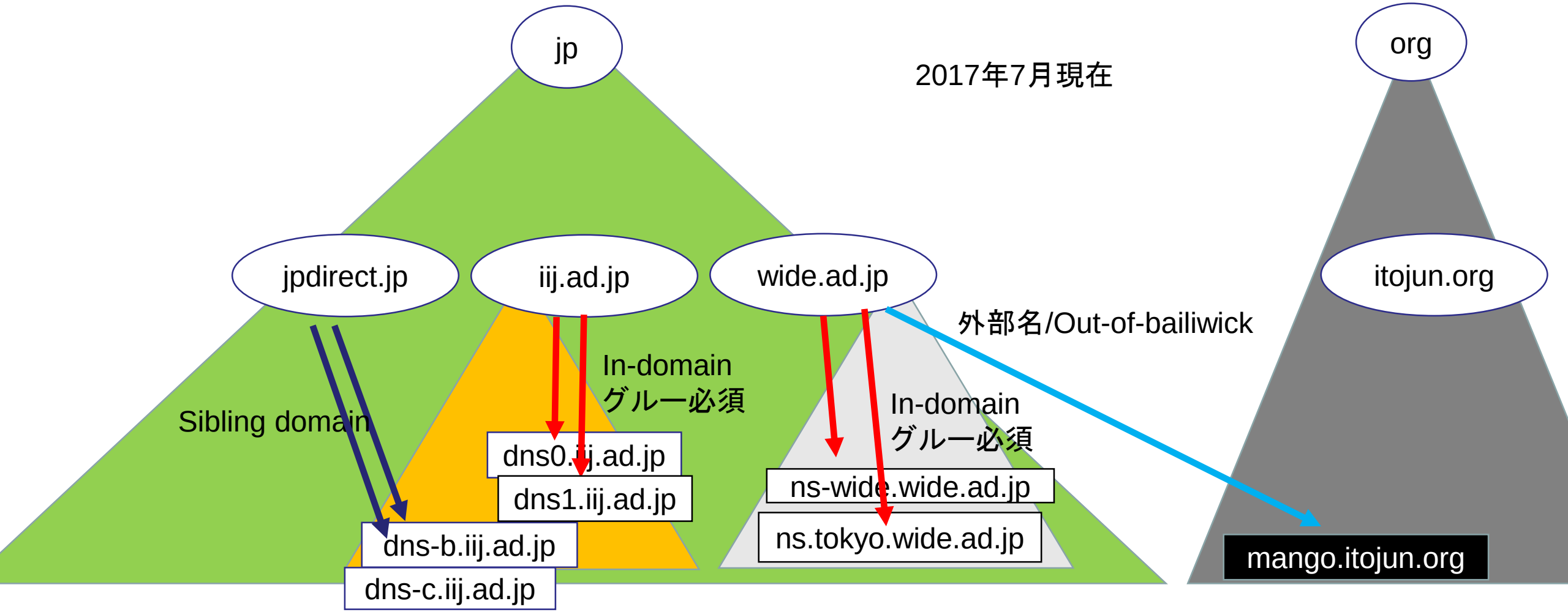
内部名、外部名という用語について

- 外部名: 委任情報を保持するドメイン名の子孫ではないドメイン名
  - JPドメイン名における外部名ネームサーバ名とは、jp以外のドメイン名
  - グルーを追加する意味がなく、捨てられる
- (広義の)内部名: 委任を保持するドメイン名の子孫のドメイン名
  - JPドメイン名での内部名ネームサーバ名とは、jpドメイン名
  - 例: jpdirect.jp. IN NS dns-b.iij.ad.jp.
  - グルーを追加してもよい
    - JPでは、他ドメイン名のネームサーバで使用されていれば追加される
- (狭義の)内部名: 委任の所有者名の子孫のドメイン名
  - ドメイン名登録時にネームサーバ情報を追加できるネームサーバ名
  - 例: iij.ad.jp. IN NS dns1.iij.ad.jp.
  - グルーを追加しないと名前解決ができない

内部名、外部名の再定義

- 内部名という用語が二つの意味で使用されているため、明確化提案中
  - RFC 7719: DNS Terminologyはもう古い
  - draft-ietf-dnsop-dns-terminology-bis-06
- Out-of-bailiwick (外部名) …委任を保持するドメイン名の子孫以外
- In-bailiwick(広義の内部名):委任を保持するドメイン名の子孫
  - In-domain(狭義の内部名):委任の所有者名の子孫のドメイン名
    - 例: iij.ad.jp.　IN　NS　dns1.iij.ad.jp.
    - グルーを追加しないと名前解決ができない (TLDでホスト情報を指定できるもの)
  - Sibling domain(兄弟ドメイン名):委任を保持するドメイン名の子孫で、委任の所有者名と同じか子孫ではないもの
    - 例: jpdirect.jp. IN　NS　dns-b.iij.ad.jp.
    - グルーを追加してもよい
- ネームサーバ名を In-domain, Sibling domain, Out-of-bailiwickに分類

jpドメイン名での
外部名、内部名(in-domain, sibling domain)



In-domainの名前解決 (例: jprs.co.jp A)

1. drill -o rd @ルートのアドレス jprs.co.jp A
   → jpの委任情報 (jp IN NS a.dns.jp)
   + グルー (a.dns.jp. IN A 203.119.1.1)
2. drill -o rd @JP DNSのアドレス jprs.co.jp A
   → jprs.co.jpの委任情報(jprs.co.jp IN NS ns1.jprs.co.jp)
   + グルー (ns1.jprs.co.jp IN A 202.11.16.49)
3. drill -o rd @jprsのサーバのアドレス jprs.co.jp A
   → Aリソースレコード (jprs.co.jp. IN A 117.104.133.165)

→ DNSクエリ 3つ (ルート, JP, jprs.co.jp)

DNSサービスの名前解決 (例: jpdirect.jp A)

1. drill -o rd @ルートのアドレス jpdirect.jp A → jpの委任情報+グルー
2. drill -o rd @JP DNSのアドレス jprs.co.jp A
   → jpdirect.jpの委任情報(jpdirect.jp IN NS dns-b.iij.ad.jp)
   dns-b.iij.ad.jp A/AAAAを知らない→dns-b.iij.ad.jpの名前解決 (jp NS既知)
3. drill -o rd @JPDNSのアドレス dns-b.iij.ad.jp A →iij.ad.jp委任情報とグルー
4. drill -o rd @iij.ad.jpのサーバアドレス dns-b.iij.ad.jp
   → dns-b.iij.ad.jp Aが得られる　→　jpdirect.jp Aの解決にもどる
5. drill -o rd @dns-b.iij.ad.jpのアドレス jpdirect.jp A→jpdirect.jp Aが戻り完了

→ DNSクエリ 5 (Root, JP, JP, iij.ad.jp, jpdirect.jp)
   in-domainの場合(3)の二倍程度

NSとネームサーバ名のTTL値を大きくすると、キャッシュにより、1,2,3,4を減らせる → キャッシュが有効な間はin-domainの場合と同じコストにできる

現状把握

- 現在の状況を知るため、NSの設定内容（In-domainかそれ以外か）とDNS設定のエラー率の関係について評価した
- 調査対象は、JPドメイン名及びtop 1mリスト
  - http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
- 判定の詳細
  - in-domainか、それ以外か、混在かに分類
  - 各ドメイン名がエラーかどうかを、APEX SOA RRを問い合わせて調査、SOA RRが得られたか、CNAMEが戻ったものを正常とした

JP及びtop 1mの調査結果

- JPドメイン名
  - すべてIn-domainのもの 1%、そのうちエラー11.5%
  - すべてIn-domain以外 97%、そのうちエラー　5.5%
  - 混在のもの 2%、そのうちエラー 10%
  - jpでは、いわゆる外部名設定が97%で、内部名設定のほうが設定ミスが多い(倍)
- top 1m
  - top 1mですべてIn-domainのもの 5%、そのうちエラー 1.2%
  - top 1mですべてIn-domain以外 93.6%、そのうちエラー 0.3%
  - top 1mのうち混在のもの 1.4%、そのうちエラー0.3%
  - top 1mでは、いわゆる外部名設定が93.6%で、エラー率は内部名の1/4
- JPドメイン名は使われていないものも多いためエラーが多いが、top 1mは使われているものだけのはずなのでエラーが少ない

ネームサーバ設定についての注意

- 複数のネームサーバを設定すると、すべて対等に参照される
  - 参照する側からはマスター(プライマリ)とスレーブ(セカンダリ)の区別はない
- ネームサーバのIPアドレスや、ネームサーバ名を第三者に奪われると、第三者にドメイン名(の管理権限)を奪われる
  - 奪ったネームサーバのアドレスで偽サーバを設定する
  - ネームサーバのドメイン名が失効して、第三者に登録されると、ネームサーバ設定しているドメイン名の管理権限を奪われることとなる

ネームサーバ名についてのまとめ

- DNSプロバイダを使用する場合は、指定されたサーバ名を使うこと
- 世の中では外部名の設定がほとんど (97%, 93.6%)
- 正しく設定した外部名を使う設定なら、名前解決コストを2倍程度におさえることができ、キャッシュで隠蔽できる
- 外部名のほうが、エラー率が少ない
  - おそらく運用サービスなので正しく運用されている
  - 一般の登録者はDNSプロバイダに任せると間違いが少ない
- DNSプロバイダを運用する場合は内部名で設定すること

TTL値について

JANOG 19での長いTTL値の推奨について (今までを振り返る)

- 変わっていないこと
  - 低頻度攻撃ではTTL値が大きいほうが攻撃成功確率が下がる
  - TTL値を小さくするとDNSサーバのクエリ数が増大する
- 書き足りなかったこと
  - CDNの普及により、小さなTTL値の使用が主流になっている
  - NSレコードや、ネームサーバ名、CNAMEのTTL値を大きくしておく
- 現実に則していないこと
  - Kaminsky/Müller攻撃ではTTL値が小さくても攻撃を受けること

Kaminsky/Müller攻撃

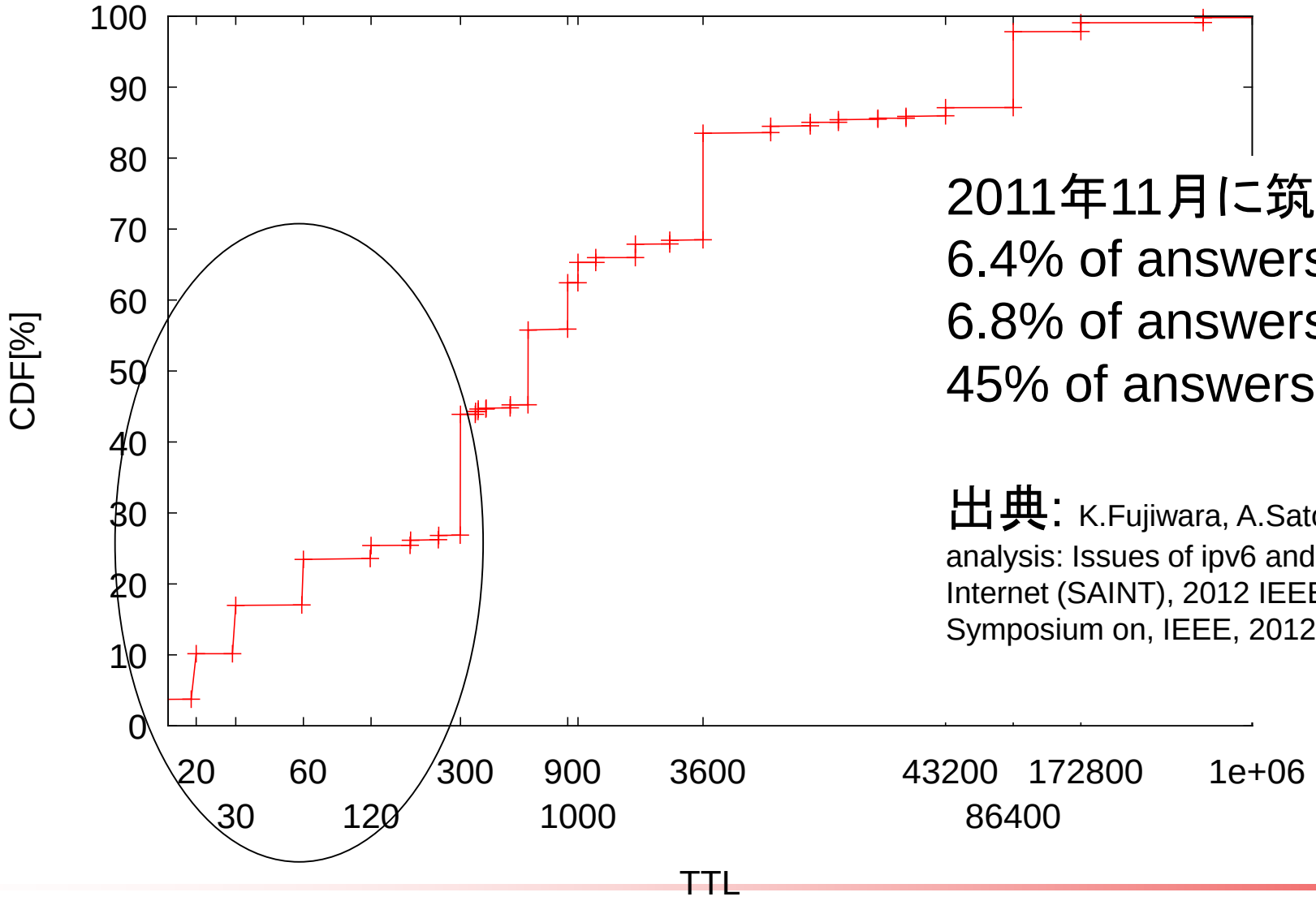
- 任意のZone cutではないところにNS RRを注入できる
  - 例: www.janog.gr.jp NSを注入
- A RRなどがすでにキャッシュされていても注入できる
- キャッシュされていた正しいRRのTTLが0になり、キャッシュから消えた後でNS RRが有効になる
  - 例: www.janog.gr.jp Aが消えたあとでwww.janog.gr.jp NSが有効になる
- 委任先のネームサーバを用意しておくと、任意のA, AAAAを注入可
- 注入しようとするRRのTTL値が小さいほうが早く効果を得られるが、待つだけで注入できるので、TTL値はなんでもよい
- ただし、Kaminsky/Müller型攻撃では、大量の偽装応答を送り込まれるため、トラフィックの変化を見るだけでばれてしまう

小さなTTL値

- 需要・要求があるため、悪いとはいえない
- 権威DNSサーバへのクエリが増加する
  - CDNで小さなTTL値を設定するものは、最終的なサーバのA, AAAA

    例: e10474.b.akamaiedge.net. 20 IN A など
  - 頻繁(毎秒など)に検索されるドメイン名のTTLを3600から20にすると、180倍 → 一時間に一度から20秒に一度
  - Content Delivery Networkは、強力な権威DNSサーバを用意しているので問題なし → フルリゾルバの負荷も上がるが、、、
  - NS, CNAME, ネームサーバ名のTTL値を大きくしておくこと
- Kaminsky/Müller攻撃ではTTLによる影響はないが、従来の低頻度攻撃ではTTL値が大きいほうが攻撃成功確率が下がる

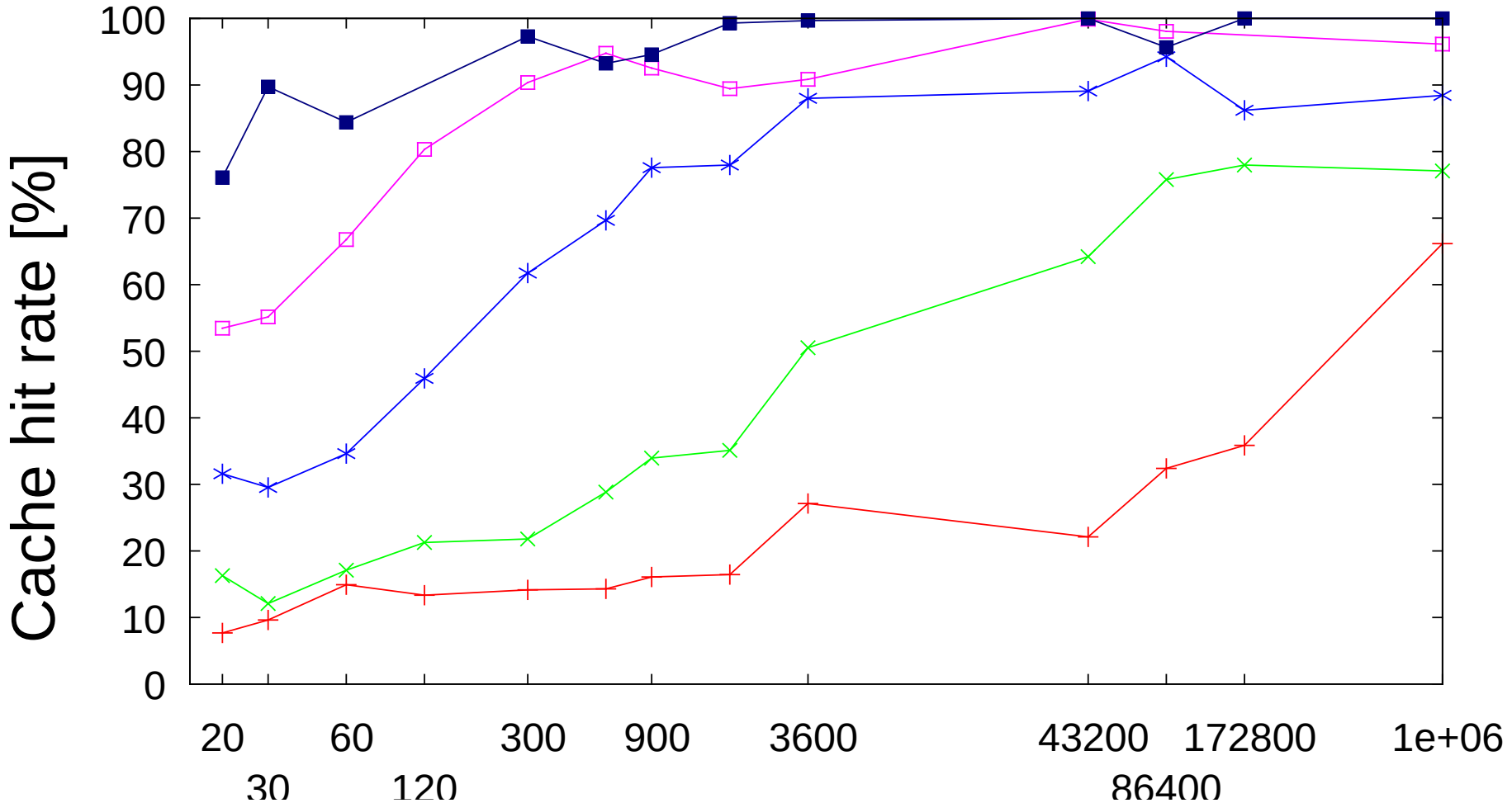
小さなTTL値の普及
クライアントからのクエリに対応するTTL値の分布



2011年11月に筑波大学でとったデータ
6.4% of answers have TTL 20
6.8% of answers have TTL 30
45% of answers have TTL ≦ 300

出典: K.Fujiwara, A.Sato, and K.Yoshida, `Dns traffic analysis: Issues of ipv6 and cdn,' in Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on, IEEE, 2012, pp. 129-137.

キャッシュヒット率とTTL値、アクセス頻度



Over 3/min
- 3/min~
- 1/min
- 1/min~
- 1/hour
- 1/hour~
- 1/day
- 1/day or less

小さなTTL 値を使用すると権威DNSサーバへのクエリが増加するが、アクセス数が大きい場合はキャッシュにより、隠蔽される
アクセス頻度 = クエリ名・タイプごとのクエリ数 / 期間(30日)

出典: K.Fujiwara, A.Sato, and K.Yoshida, `Dns traffic analysis: Issues of ipv6 and cdn,' in Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on, IEEE, 2012, pp. 129-137.

19

短いTTL値を設定する場合には

- フルリゾルバから権威DNSサーバへのクエリ数が増大することを意識する
- NS, CNAME, ネームサーバ名のTTL値は小さくしない
  - 小さくすると、エンドノードからのクエリのたびにTLDから委任情報を取得することとなるため、TLDへのクエリも増大してインターネットを不安定にする
- ゾーンファイル先頭に $TTL 60 と書かず、必要なものだけ小さくすること
- CDNを使う場合のTTL値の設定は事業者に任せてください
  - CNAMEのTTL値を小さくする必要xはありません、その先のAで制御します

例

$TTL 86400

example.jp.　(86400)　IN　NS　ns.example.jp.←NS,SOAのTTL値を大きく

www.example.jp.　7200 IN CNAME www.example.jp.CDN.example.←TTL値を大きく

www.example.jp.CDN.example. 60 IN　A　192.0.2.1←CDNがTTL値を設定

TTLに関する他の資料

- https://jprs.jp/tech/security/2014-05-30-poisoning-countermeasure-auth-1.pdf
  - pp.13-16
  - A/AAAAは短くなる傾向にあるけどリスクを把握した上で運用を
  - NSのTTLが短すぎるのは無意味かつ危険
- https://blog.cloudflare.com/tld-glue-sticks-around-too-long/
  - DDoS を受けている IP アドレスはブラックホールして、別アドレスでサービスを継続したい
  - そのためには TLD に登録している glue A の TTL を短くしてほしい

過去の資料について

大昔のJANOG発表資料について

- JANOG 11: DNS正引きの実態 ← 14年前
- JANOG 12: ENUMの野望 ← ENUMは使われなかったプロトコル
- JANOG 15:ネームサーバは内部名で ← 12年前, 誤解を生んだ
- JANOG 25:メールアドレスの国際化 ← 7年前, まだ流行ってない

- JANOGの資料を参照して社内資料を作られたかたはいらっしゃいますか？　更新していますか？
- 古い資料を見てしまって困った経験、恥ずかしい経験などがあれば聞きたいです。

まとめ

- 古い資料はあてにならないこともある
- 新しい知識を仕入れよう