IETF 90 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 90 報告会, 2014年8月25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
- 活動
  - qmail IPv6対応、tcp wrapper風のものの試作(1997頃)
  - DNSSECの事前検討 (2002~2010)
  - DNS関係のトラフィック解析(root, jp, 大学)など (2005~)
  - DNSへの攻撃ツールの試作 (2005, 2014)
  - IETFでの標準化活動 (2004~)
    - DNS関連WG（dnsext, dnsop）における提案と議論
    - enum WG RFCs: 5483 6116
    - eai WG RFCs: 5504 5825 6856 6857

DNSを扱ったWG/BOF

- DNS関連WG
  - dnsop　　DNS運用ガイドラインの作成
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - dane　　DNS(SEC)にTLSの証明書を載せる
- DNSの話題があったWG
  - homenet　　家のネットワーク
- IETF以外
  - IEPG

dnsop WG (DNS Operations)

- DNS運用ガイドラインを作るWG

- ふりかえり: 3月のIETF 89
  - 特に新しい結論はなく、議論を継続することになった
  - 従来からの議題でWGLCに向けて進めるもの
    - AS112 (プライベートアドレスの逆引きなど)をDNAMEで
    - DS/NS/グルーの自動更新
  - ドメイン名に似た名前空間の話題
  - チャーター更新
    - DNSプロトコルのアップデートを追加したいという人はいる
    - 最新の更新案でDNSプロトコルの拡張が追加された
  - DNSプライバシについて取り扱う

dnsop (2)

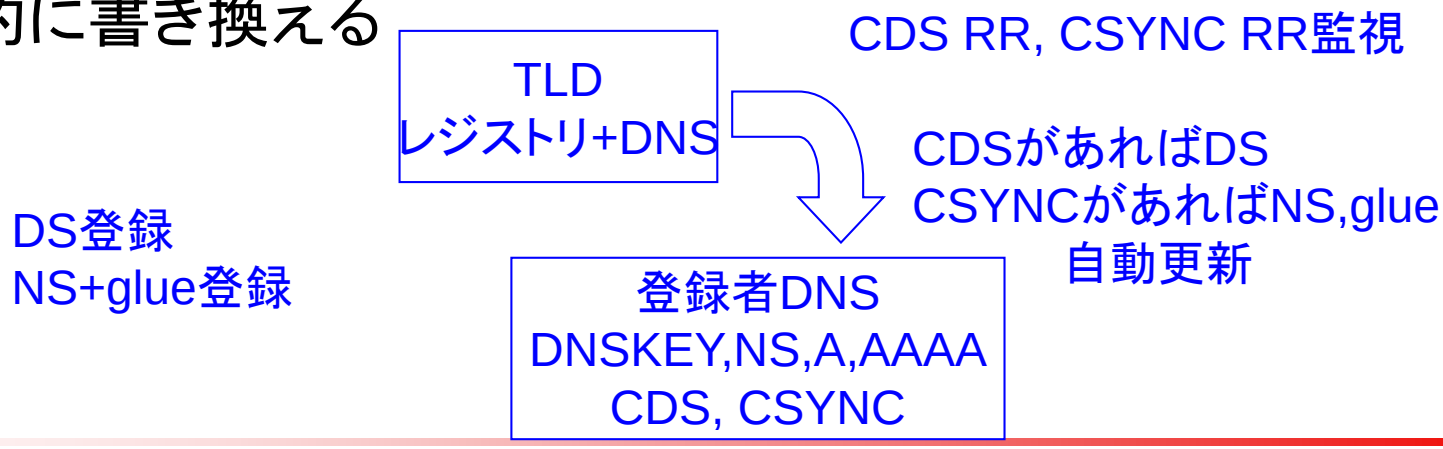
- WGミーティング運営の新提案
  - 今後、新しいInternet Draftは、メーリングリストで紹介して議論をしてから、ミーティングの時間をとるとのこと

dnsop (3)

- ステータス報告: 3月以降、完了したもの (1)
  - チャーター更新: DNSプロトコルの軽微な修正追加
    - ドメイン名に似た名前空間の予約も扱えるようになったことがチェアから指摘された
    - DNS privacy (dnse) も取り扱える
  - AS112 DNAMEとrfc6304bis (IESG処理中)
    - プライベートアドレスの逆引きを、DNAMEを使って実装
    - いまは多数のゾーンを各ノードが管理しないといけないが、empty.as112.arpaゾーンを保持するだけでよくなる
    - 10.in-addr.arpa. IN DNAME empty.as112.arpa.

dnsop (4)

- ステータス報告: 3月以降、完了したもの (2)
  - DS自動更新 (rfc editor queue)
    - 対応しているTLDなどでは、子側にCDS, CDNSKEYを書くと、親が子ゾーンを定期的にチェックし、親側のDSを自動的に書き換える
  - 親のNS/glue自動更新 (IESG処理中)
    - 対応しているTLDなどでは、子側にCSYNCを書くと、親が子ゾーンを定期的にチェックし、親側のNSとグルーを自動的に書き換える



dnsop (5)

- その他の議題
  - Root Scaling (ルートの規模増大への対応)
  - DNSSEC Validator requirements
  - 変なフルリゾルバの避け方 (ホテルとか)
  - 鍵と署名ポリシー
  - キャッシュポイズニング対策再び
  - IPv6の逆引き再び
  - マルチキャストアドレスの逆引きをどうするか

dnsop:Scaling root zone

- 新しい話題

- ルートサーバへの負荷増大への対策
  - フルリゾルバにルートゾーンを配布して、ルートサーバへのクエリを減らす
    - draft-wkumari-dnsop-dist-root
  - ルートサーバを増やせるようにする
    - draft-lee-dnsop-scalingroot

draft-wkumari-dnsop-dist-root

- ルートゾーンを配布するという提案
- フルリゾルバがルートゾーンを持てば、ルートサーバの負荷が軽くなり、応答速度が向上する
- 遅滞なく大規模に配布することは困難
- いまでも、rootゾーンを持つことは可能
  - f.root-servers.netからのゾーン転送
  - ICANNゾーン転送サービス
    - http://www.dns.icann.org/services/axfr/
- アイデアには合意する人が多いが、配布方法についていろいろ議論が出た
- Requirementsからやることになりそうである

draft-lee-dnsop-scalingroot

- 著者
  - Xiaodong Lee (CNNIC CEO兼CTO)
  - Paul Vixie
  - Zhiwei Yan (CNNIC)
- ルートゾーンはICANN/IANA管理
- ルートサーバの名前・アドレスをAnycastアドレスの組に改組して、階層的に配置するという提案
  - 国ごととか、地域ごとなど
  - いまのroot serversをつぶして作り直そうという提案
  - 完全に再割り当てと、一部のルートを変更するという2案
- よく考えられてはいるが、、、不評
  - 政治的意図を感じた人が多かった？

キャッシュポイズニング対策再び

- draft-fujiwara-dnsop-poisoning-measures-00
  - “キャッシュポイズニングの検知と対策について” 提案しました
- 検知
  - 送っていないクエリに対する応答を検知
  - 攻撃者が注入しようとしている情報を通知 (NS, A, AAAAなど)
  - ただし、数が多いとログがあふれるので集約が必要
- 対策
  - TCPクエリで注入がほぼ困難になる
  - TCPのSequence numberは32bitで、最低2つ連続して注入しないと入らない (ACK+最初のデータ)
- 具体的な提案は、検知で得たドメイン名関連クエリをTCPで問い合わせしなおす/しばらくTCPで問い合わせる
- 反応
  - 他にも対策があるという指摘、メーリングリストで継続という指示

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

- ふりかえり: 3月のIETF 89
  - Requirementsはほぼ合意された
  - 最初の候補を考える時期になってきた
    - mDNSのブリッジ
    - 通常のDNSとマルチキャストDNSの複合プロキシー
      - 検索時は、DNSとmDNSの両方を検索
      - mDNSで登録された名前をDNSにどう展開するか
    - 家電機器などの情報をDNSに出すことへの懸念
    - 複雑さを増すことへの懸念など
    - WG参加者の理解は深まった

dnssd (2)

- Requirementsは完了
  - マルチキャストの電力消費の話を追記
- セキュリティモデルの話題
  - 最初の話題提供
- プロトコルの実装はハイブリッドプロキシーになりそう
  - 既存のDNSとmDNSをプロキシーする
  - 例: lb._dns-sd._udp.meeting.ietf.org. ptr
  - 例: _pdl-datastream._tcp.meeting.ietf.org. ptr
  - 例: term-printer._pdl-datastream._tcp.meeting.ietf.org srv

dane WG

- DNSにTLSの証明書を載せるWG

- ふりかえり: 3月のIETF 89
  - WGの今後: プロトコルが完成したら閉じるか？
  - SMTP, SIP, XMPPなどへの適用した場合の深い話が議論された
  - OpenPGPへの適用について

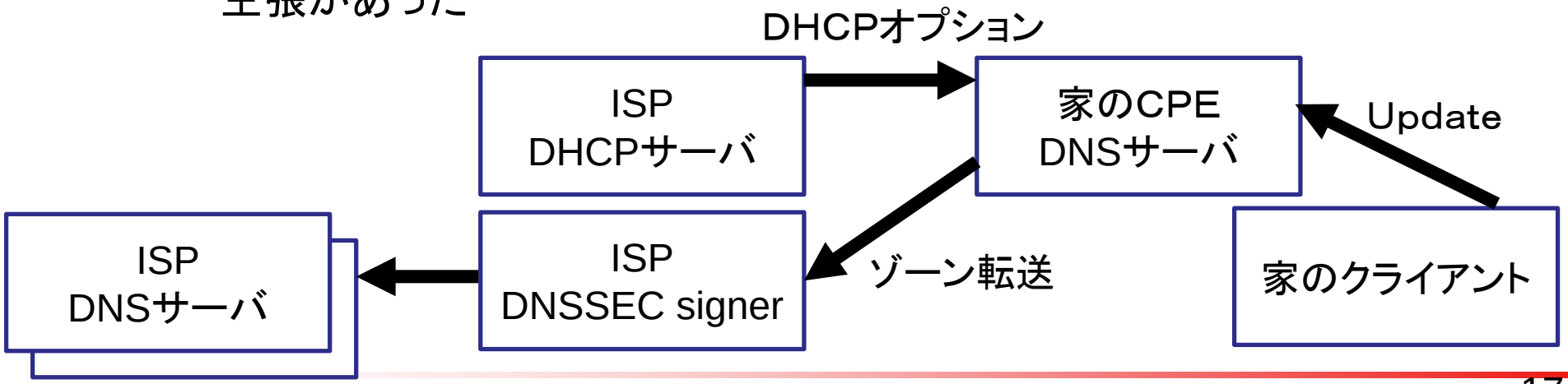
dane (2)

- DANE SMTP, DANE SRVはほぼ議論完了
  - EximとPostfixで実装された
- DANE OpenPGP, S/MIME
  - 個人の鍵をDNSに載せる
  - XXXX._openpgpkey.example.com
  - まだまとまらず、継続
- Raw key format: draft-ietf-dane-rawkeys-00
  - TLSA RRでRaw Public Keysを扱えるようにする拡張
    - Certificate Usage 3 (DANE-EE)
    - Selector 1 (SubjectPublicKeyInfo - "SPKI")
    - Match 0 (Full public key)
  - 長い議論であったが、議論を継続するようにみえる
- draft-ietf-dane-ops
  - BCPからStandards trackに変更
- 今後: DANEbisとOps、残務を行う

homenet WG

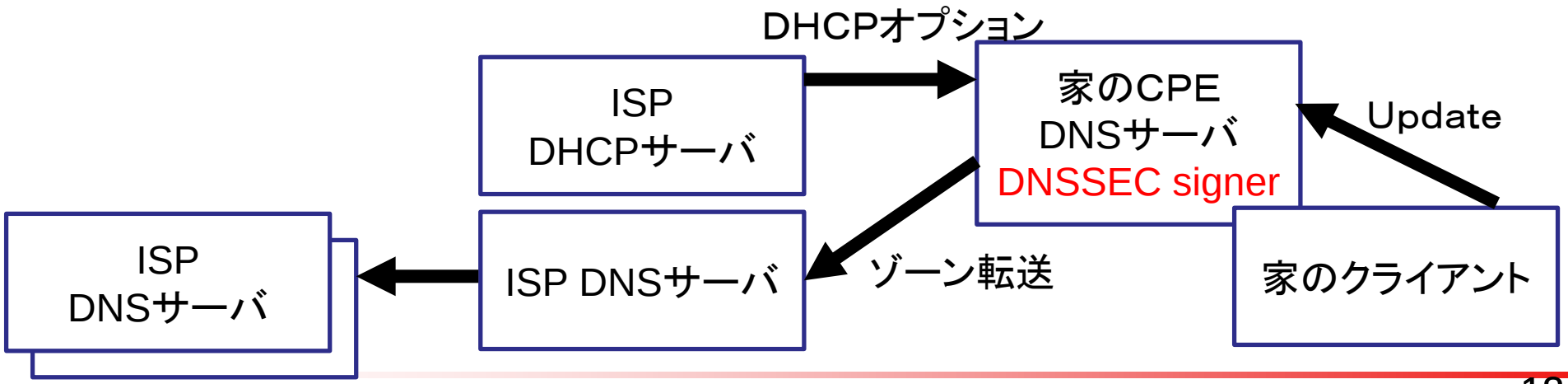
- 家の(IPv6)ネットワーク

- ふりかえり: 3月のIETF 89
  - draft-mglt-homenet-dnssec-validator-dhc-options-01
    - 要求: 宅内のホスト情報をインターネットに出したい
    - 提案: 家庭のCPEがhidden masterで、ISPのDNSサーバに転送してDNSSEC署名し、ISPが権威DNSサーバを動かすという提案
    - マルチホームのときにどうするかという質問や、
    - 家のゾーンは自分のものだから、自分でDNSSEC署名したいという主張があった



homenet (2)

- draft-mglt-homenet-dnssec-validator-dhc-options-04
  - 家のゾーンの署名はCPEが行い、それをISPに転送するという提案になった



IEPG meeting

- DNS: What If Everyone Did It?, Geoff Huston
  - DNSSECが及ぼす悪影響の話
  - DNSSEC検証の普及度を調べたら、検証しないものが80%
  - DNSSEC検証で200~500msほど名前解決が遅くなる
  - DNSSECでDNSトラフィックは7.5倍
- Redirecting the target domain's nameserver cache poisoning attacks
  - NSを注入する攻撃について藤原が紹介したが、IEPG参加者には当たり前レベルの話だったようで、あまり興味を引かなかった

参考

  - 過去のIETFミーティングの資料、議事録あり
- http://www.iepg.org/
  - IEPGミーティングの資料