DNSフルリゾルバの研究開発実装について

IIJ
Internet Initiative Japan

IIJ技術研究所　日比野 啓

Ongoing Innovation

自己紹介

- 日比野 啓 / @khibino
- 以　　前　はISPでRadius　認　　証　サーバを　開　　発

  2022年から DNS のフルリゾルバの研究開発実装

DNS研究開発実装

組み合わせ可能なDNSコンポーネントを目標に

DNSライブラリ
- DNSワイヤーフォーマット解釈/出力
- DNSSEC 検証機能
- 優先度付きキューによるキャッシュ
- DoH, DoT, DoQ

フルリゾルバ
- 反復検索
- DNSSEC検証機能の反復検索への組込み
  - 署名検証
  - NSEC/NSEC3検証による否定応答
- Haskellの軽量スレッドによるサーバ実装

反復検索

- クライアントからのリクエストに　応　じて複数ゾーンに分散配置された結果を解決する
- 目 的 のゾーンの 権 威 サーバが 見 つかるまで、委任情報に従って繰り返し検索を行なう
- 目　的　のゾーンの　権　威　サーバから結　果　のリソースレコード　集　合　（RRset）を取得する

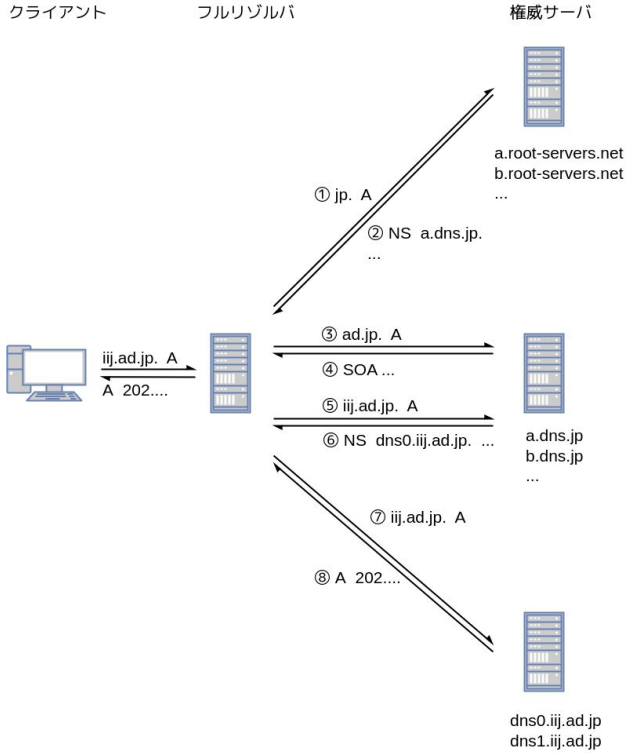


図: 反復検索
(QNAME minimization)

反復検索の委任情報

フルリゾルバは委任情報に従って権威サーバを辿る

```
;; AUTHORITY SECTION:
iij.ad.jp.              86400  IN      NS      dns0.iij.ad.jp.
iij.ad.jp.              86400  IN      NS      dns1.iij.ad.jp.

;; ADDITIONAL SECTION:
dns0.iij.ad.jp.         86400  IN      AAAA    2001:240::105
dns1.iij.ad.jp.         86400  IN      AAAA    2001:240::115
dns0.iij.ad.jp.         86400  IN      A       210.130.0.5
dns1.iij.ad.jp.         86400  IN      A       210.130.1.5
```

反復検索の委任情報（DNSSEC）

DNSSECの信頼チェーンためのレコードが付加される

```
;; AUTHORITY SECTION:
iij.ad.jp.          86400  IN    NS    dns0.iij.ad.jp.
iij.ad.jp.          86400  IN    NS    dns1.iij.ad.jp.
iij.ad.jp.          7200   IN    DS    18490 8 2
                           B354CF936F041F1E8D7E9420308AF5243E90B50A16E68AEBCB173049 54BD1AB1
iij.ad.jp.          7200   IN    RRSIG DS 8 3 7200 20231211174502 20231111174502 36861 jp.
                           SYdMfWoiAnpRapF2aImpvdS/aaalih1wYNLGHvA3S7NE6RBlxfMPh0Sd
                           RJbveCgP4gIDdJcz0EqIR05oMYwkAsibf78PVAFc7Ht6yuY4bG8ZmJ+R
                           BIYt+n8BB4pfpfSQhMfj8c/sZ5zBZM16teBfyXM1rbpvZ5OLXNwLOl4m Dy4=

;; ADDITIONAL SECTION:
dns0.iij.ad.jp.     86400  IN    AAAA  2001:240::105
dns1.iij.ad.jp.     86400  IN    AAAA  2001:240::115
dns0.iij.ad.jp.     86400  IN    A     210.130.0.5
dns1.iij.ad.jp.     86400  IN    A     210.130.1.5
```

反復検索 (DNSSEC)

DNSSEC の信頼チェーン

- **DS は委任先ゾーンの SEP(SECURE ENTRY POINT) DNSKEYのハッシュ**
- **委任先ゾーンではSEP DNSKEYでDNSKEY の RRset に対する RRSIG(署名)が検証可能**
- **ゾーン内では DNSKEY で、それぞれのRRset に対するRRSIG(署名) が検証可能**
  - **次の委任先への DS RRset に対するRRSIG(署名)も検証可能**

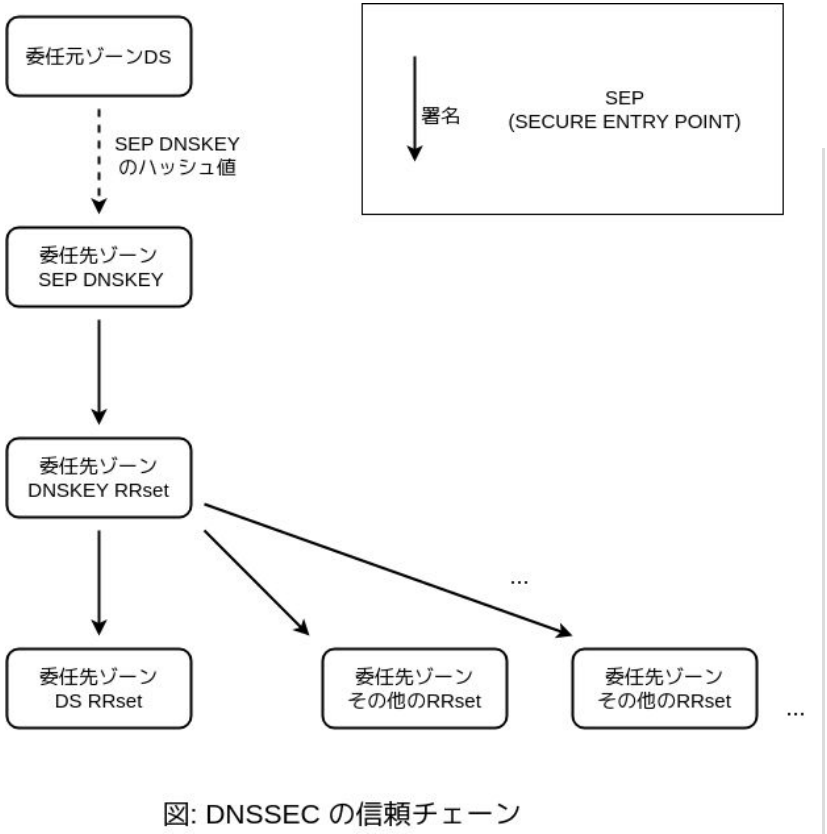
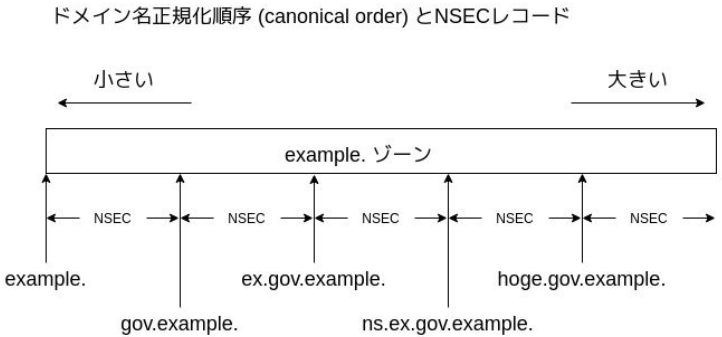
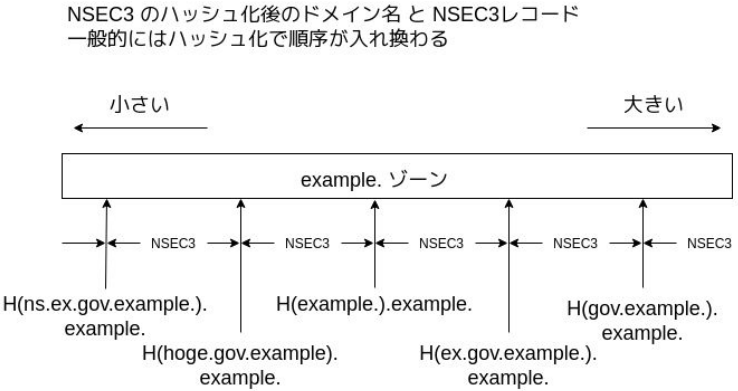


図: DNSSEC の信頼チェーン

DNSSECでの否定応答

- NSEC/NSEC3
  - 存在するドメインの範囲情報
  - 間のドメインの不存在
  - NSEC/NSEC3 のレコードのRRSIGが検証される
- NSEC
  - ゾーンをドメイン正規化順序による範囲情報で分割
- NSEC3
  - 隠蔽目的でドメイン名のハッシュ値を再度ドメイン名とする
    - ハッシュ値を取ることで順序は入れ換わる
    - 入れ替わった順序でも、範囲情報によりゾーンが分割される性質は変わらない
  - ハッシュ値はBase32Hexで文字列化
    - 順序関係を変化させない





DNSSEC 署名検証時の TTL の復元

RRSIG にある original TTL で復元する

```
 % dig @a.dns.jp. jp. SOA +dnssec
jp.             86400 IN    SOA   z.dns.jp. root.dns.jp. 1700124302 3600 900 1814400 900
jp.             86400 IN    RRSIG SOA 8 1 86400 20231211174502 20231111174502 36861 jp.
                            mp4Xu9fl…

% dig @a.dns.jp. does-not-exist.jp. A +dnssec
jp.             900   IN    SOA   z.dns.jp. root.dns.jp. 1700124302 3600 900 1814400 900
jp.             900   IN    RRSIG SOA 8 1 86400 20231211174502 20231111174502 36861 jp.
mp4Xu9fleEhK0pCPn6ckzD5MdhDXjVb/WMGaz2+uZGWFNV4cEiOozJvr
TgCy18CS0XinqdS8zCOZEAZ0D5ip8yJEF/S2BnSG4rJh8cKvoy7CRXjj
KJ8MU2R5uiEJ6fJpu62UYRSf1xgWC4chEnRnpNREd3Ht5/79tGKTzmv3 0/Y
```

例外的な振舞い

Empty Non-Terminal に対するNXDOMAIN

QNAME minimization で問題

- **委任情報が無い場合(NoErr)と同様に扱った方が無難**
- **RFC8020 (NXDOMAIN 下には何も無い)に対応すると引けなくなる**

```
## 実例

 % dig danuoyi.alicdn.com. NS +short
danuoyinewns1.gds.alicdn.com.
...
 % dig @danuoyinewns1.gds.alicdn.com.
\sc02.alicdn.com.danuoyi.alicdn.com.  A
... status: NOERROR, ...
sc02.alicdn.com.danuoyi.alicdn.com. 60 IN A ...
...
 % dig @danuoyinewns1.gds.alicdn.com.
\alicdn.com.danuoyi.alicdn.com.  A
... status: NXDOMAIN, ...
 % dig @danuoyinewns1.gds.alicdn.com.
\com.danuoyi.alicdn.com.  A
... status: NXDOMAIN, ...
```

例外的な振舞い

ゾーンの親子同居

- 委任元と委任先が同じ権威サーバ
- 委任情報を直接得る方法が無い
- DNSSECの場合もDSが取れない
    - DSを補うためのクエリ

反復検索に親子同居のためのロジックが必要

フルリゾルバの構成とキャッシュ

- Haskellの軽量スレッドによるサーバ実装
- 優先度付きキューによるキャッシュ/ネガティブキャッシュ
  - キャッシュ破棄時刻を優先度に設定（現在時刻 + TTL ≡ 破棄時刻）

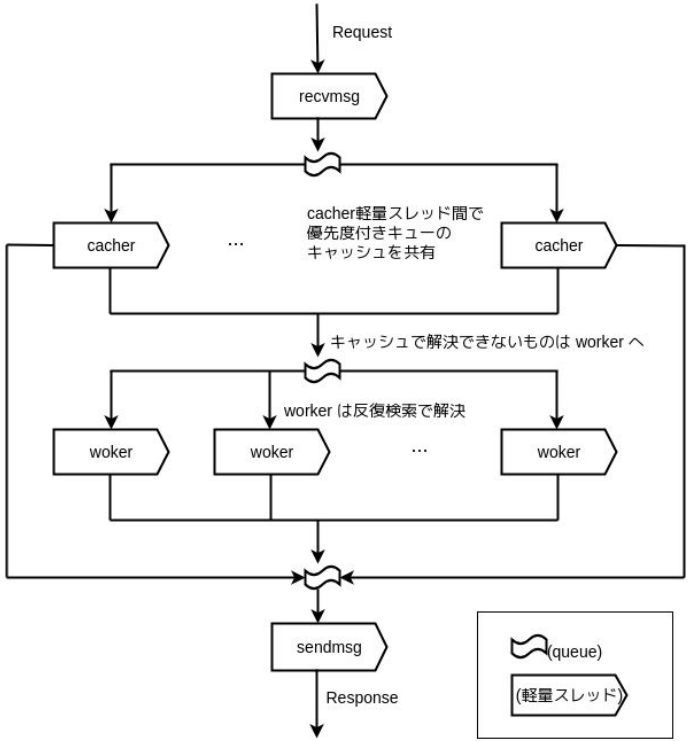


図: 軽量スレッドによるフルリゾルバの構成

デモ

今後の課題

パフォーマンスチューニング

- キャッシュが無い状況でのスループット向上

機能追加

- 攻撃に対する耐性
  - NSEC/NSEC3範囲情報による否定応答キャッシュ (RFC8198)
  - ルートゾーンのコピーを持つ (RFC8806)

レポジトリ

- https://github.com/kazu-yamamoto/dnsext

ありがとうございました