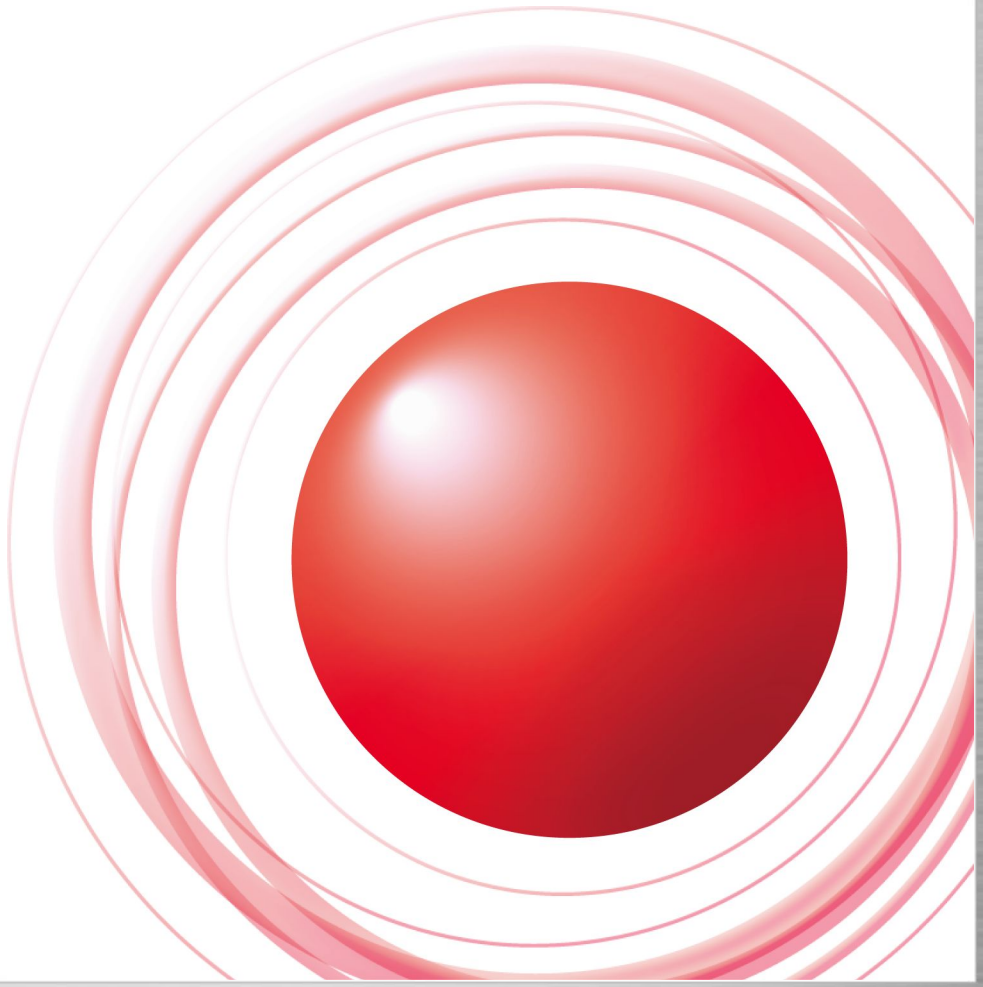
DNSの進化と研究開発での取り組みについて

IIJ
Internet Initiative Japan



株式会社 インターネットイニシアティブ
技術研究所　日比野 啓　山本 和彦

Ongoing Innovation

自己紹介

- 氏名: 日比野 啓
- 所属: IIJ 技術研究所
- 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

旧来からのDNSの仕組み

旧来からのDNSの仕組み

ドメイン名の木構造と分散配置

- ドメイン名は、
  複数のゾーンに分散されて配置されている
- ゾーンは、
  それぞれの権威サーバ群で管理される
- ドメイン名に紐付く様々なリソースレコードが保持される
  - 一般的にリソースレコードは複数(RRset)
  - タイプ A – IPv4 アドレス
  - タイプ AAAA – IPv6 アドレス
  - タイプ NS – 権威サーバの名前
  - …

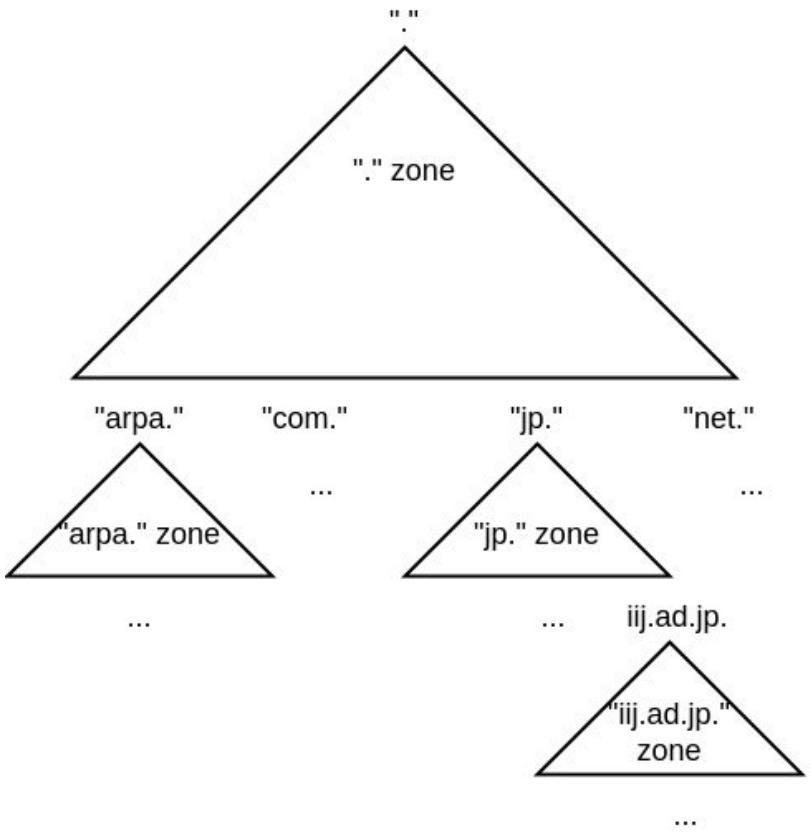


図: ゾーンに分散配置されるドメイン名

旧来からのDNSの仕組み

反復検索

- 複数ゾーンに分散配置された結果を解決する
- クライアントはフルリゾルバに検索リクエストを発行する
- フルリゾルバは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
- フルリゾルバは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
- フルリゾルバは権威サーバからの応答をキャッシュする

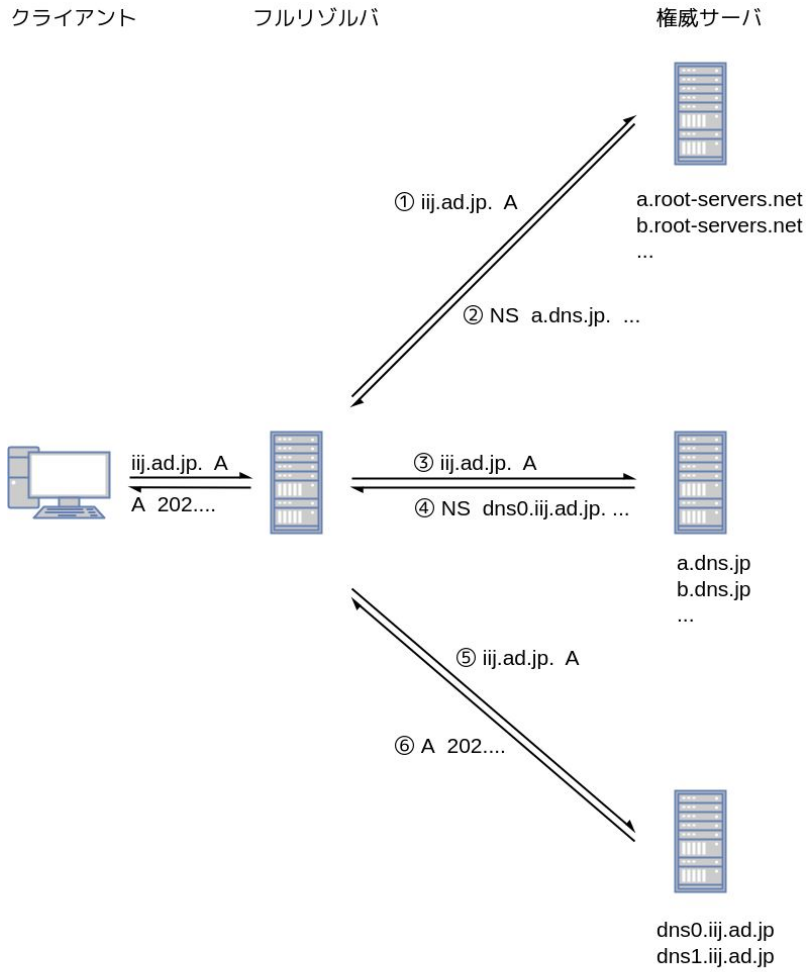


図: 反復検索

DNSの進化

DNSの進化

DNS over X

クライアント、フルリゾルバ間で暗号化した通信路を利用する

- DNS over HTTPS (DoH)
- DNS over TLS (DoT)
- DNS over QUIC (DoQ)

クライアントのプライバシーを守る

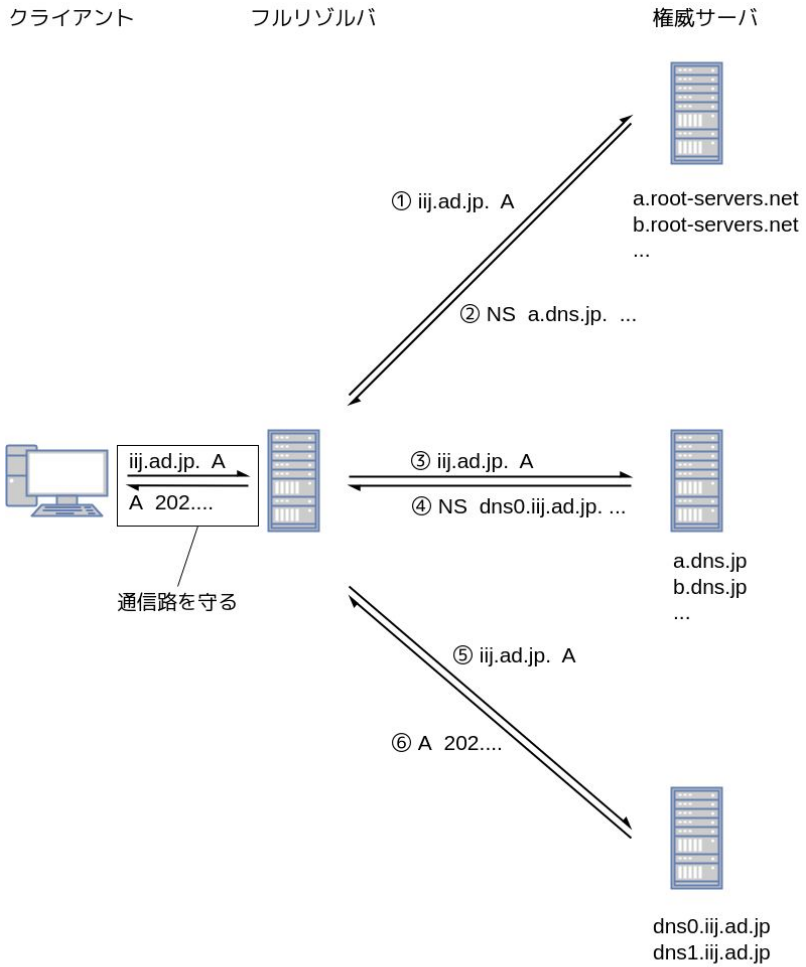


図: クライアント、
フルリゾルバ間を守る

DNSの進化

反復検索と QNAME minimization

QNAME minimization

- フルリゾルバ、権威サーバ間の検索ドメイン名を切り詰める
- クライアント側のプライバシーを守る

※反復検索の検索回数は若干増加する

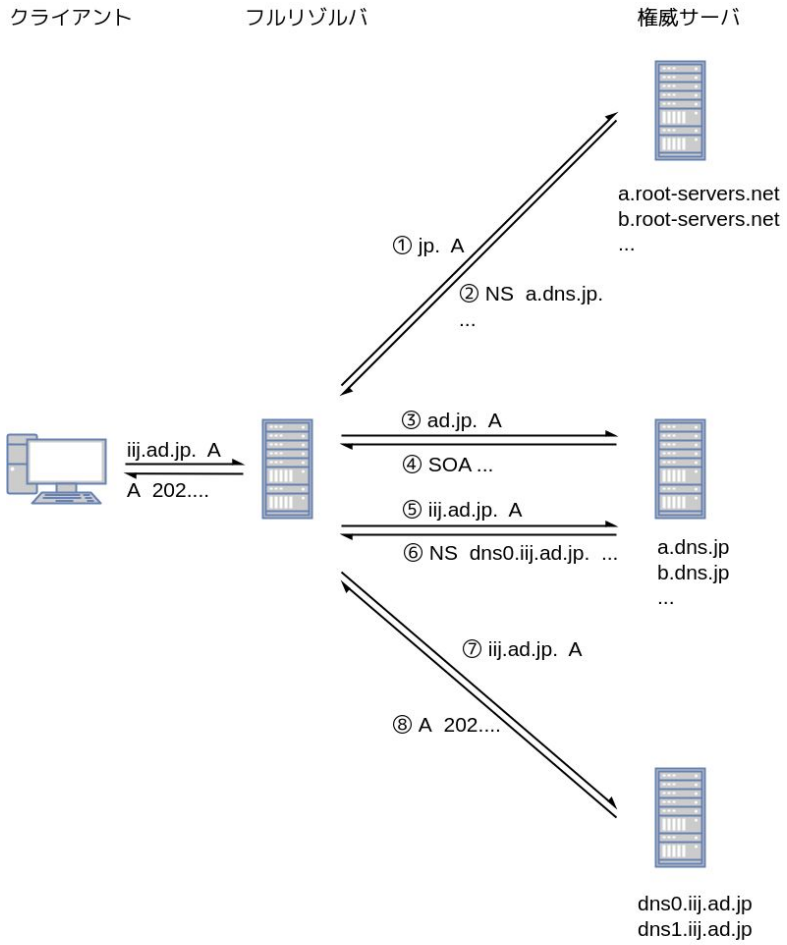


図: 反復検索
(QNAME minimization)

DNSの進化

UDP送信ポートのランダム化

フルリゾルバへ偽の応答を送信する攻撃

- フルリゾルバのキャッシュを汚染させる
- フルリゾルバの送信アドレスに向けて攻撃
- UDP送信ポートをランダム化することで防御

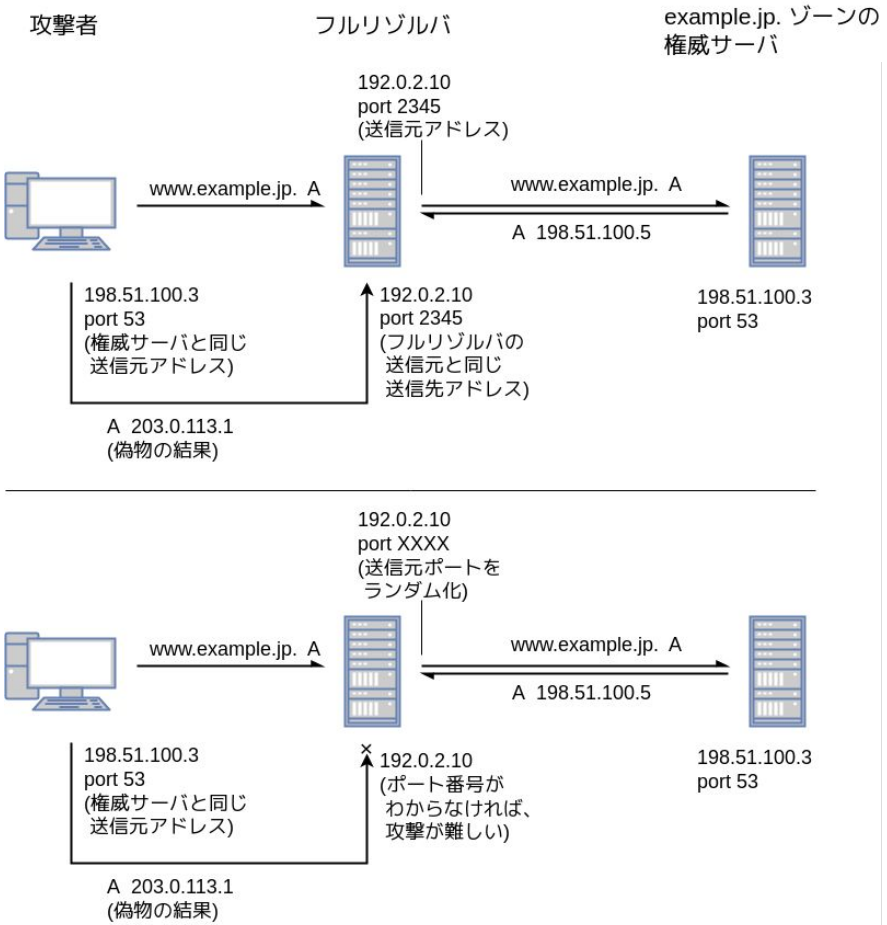


図: 送信ポートのランダム化

DNSの進化

DNSSEC

権　威　サーバから　返　答　されるレコードの正当性を守る

- 署名を検証
- DNSSEC 用のタイプを追加
  - DS:　委任先のSEP　DNSKEY のハッシュ値
  - DNSKEY: 署名検証用の鍵
  - RRSIG: RRset の署名値
  - NSEC/NSEC3: 否定応答用の範囲情報

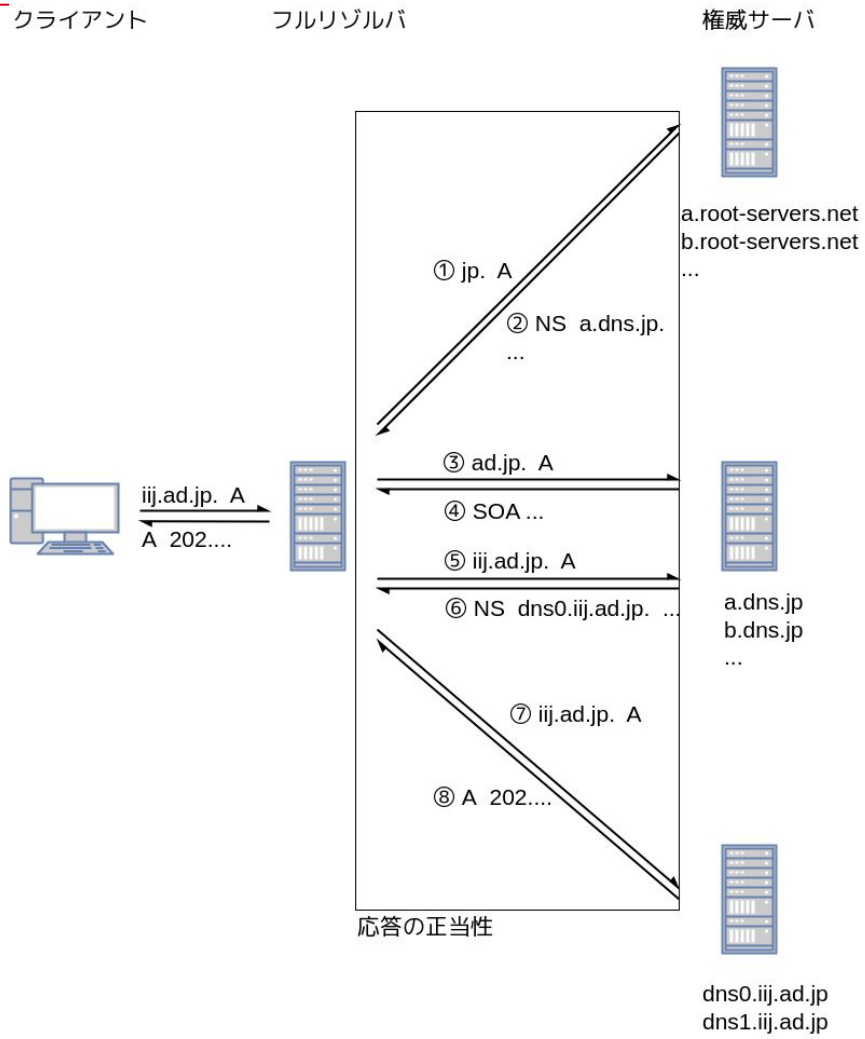


図: 権威サーバからの応答の正当性を守る

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

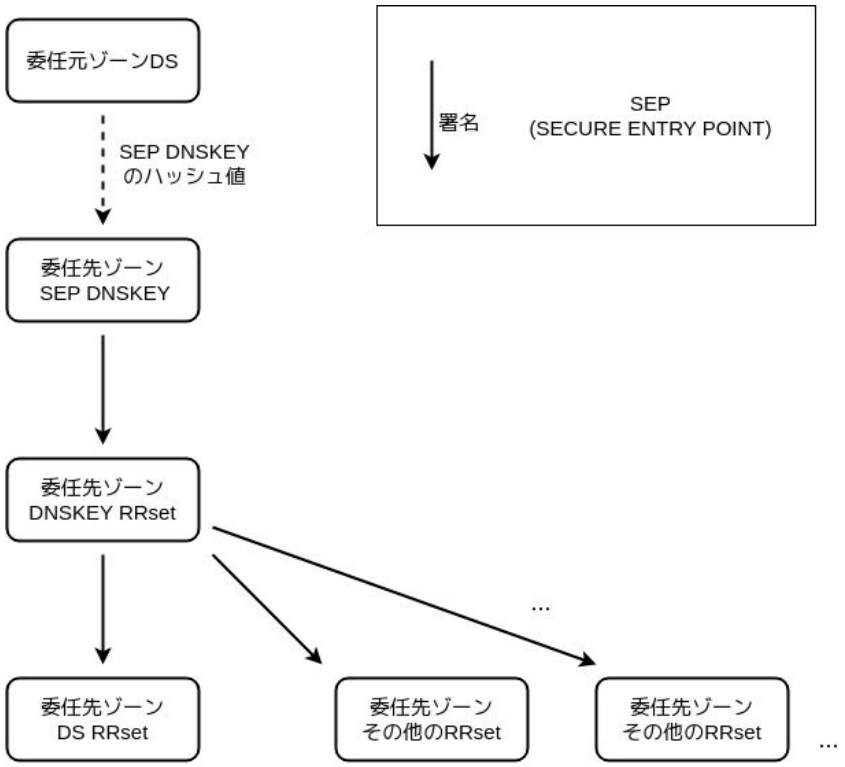
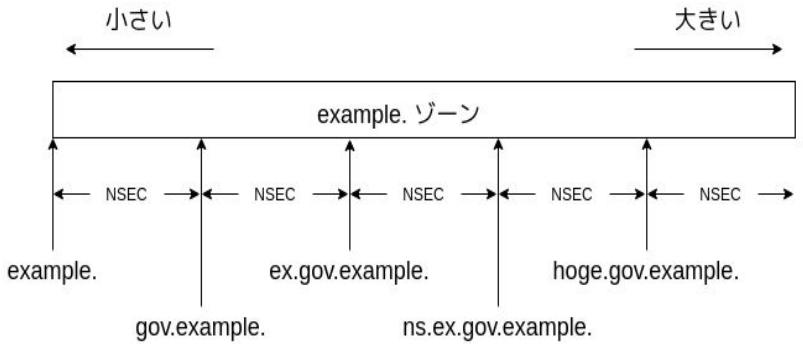


図: DNSSEC の信頼チェーン

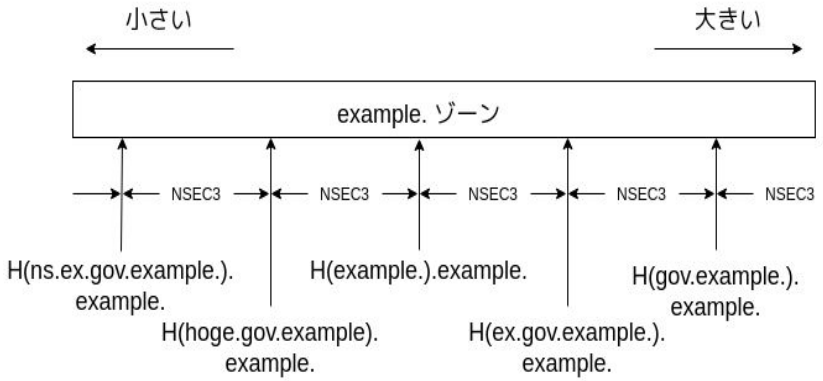
DNSSEC 否定応答の証明

- 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
  - 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
    - 入れ換わった順序でも、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
    - この変換は順序関係を変化させない

ドメイン名正規化順序 (canonical order) とNSECレコード



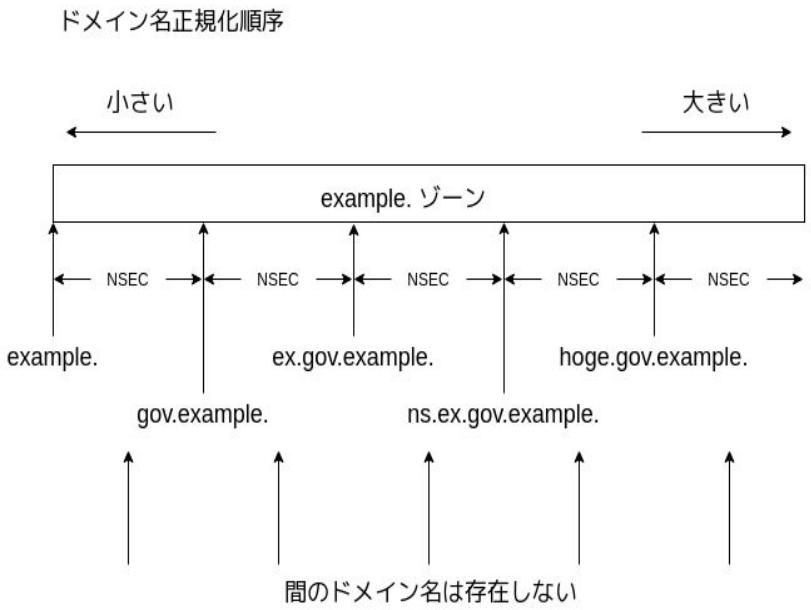
NSEC3 のハッシュ化後のドメイン名 と NSEC3レコード
一般的にはハッシュ化で順序が入れ換わる



ランダムサブドメイン攻撃の対策

ランダムに 生　成 したサブドメイン 検　索 する、権威サーバへの攻撃への対策

- RFC 8198 Aggressive Use of DNSSEC-Validated Cache
  - 存 在 するドメイン 名 の 範 囲 情 報 (NSEC/NSEC3) を利用して、不要なリクエストから権威サーバを守る
- RFC 8806 Running a Root Server Local to a Resolver
  - フルリゾルバにルートゾーンのコピーを持 つことで、存在しないドメインへのクエリからルートサーバを守る



研究開発実装と今後の課題

研究開発実装と今後の課題

DNS研究開発実装

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/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
- 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

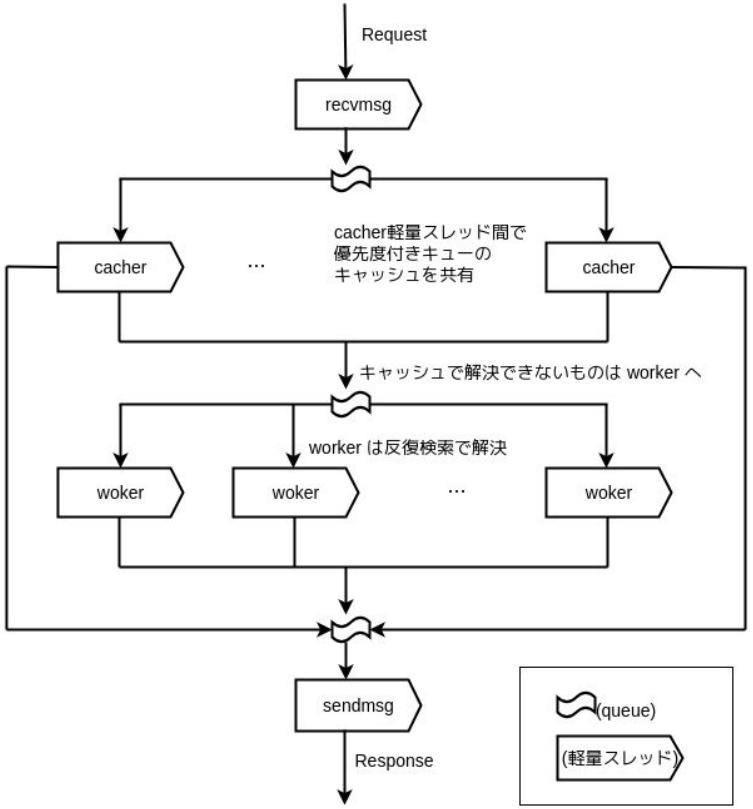


図: 軽量スレッドによるフルリゾルバの構成

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
  - 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）
- 組み合わせ可能なDNSコンポーネントの拡充

レポジトリ

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

ありがとうございました