# DNS権威サーバclove



2026.11.26

(株)インターネットイニシアティブ
山本和彦



bowline
(もやい結び)
フルリゾルバ



clove
(巻き結び)
権威サーバ

# 権威サーバにニッチはあるか？

- 2025年12月 JPRSのみなさんとミーティング
  - 森下さん「権威サーバにニッチはない」
    - ルート・サーバ (ひたすら正しく応答を返す)
    - TLD (委任が多い)
    - ホスティング (多数のゾーンを管理)
- 2025年12月 IIJ運用チームとミーティング
  - 「こういうのがあれば使いたい」
- 2026年1月 権威サーバの実装を開始
  - まずはプロトコルを理解するところから

「独学できる？無理です。」

Geminiに聞く

kazu:「DNSのauthority sectionに
入る可能性のあるRRは何ですか？」

kazu:「それを定めているのはどのRFCですか？」

DNSに関しては正しく答える

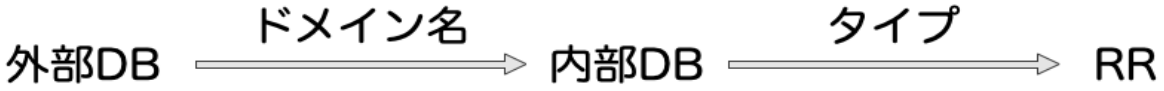
# データ構造

- 最初は一段のkey value store (辞書)として実装




  - 問題：Empty Non-Terminalが実現できない

- 二段のkey value storeへ変更




  - 問題：ワイルドカードを完全には表現できない

- ラベル単位のtrieで実装
  - ドメイン名の木構造を素直に表現

DNSの次はDNSSEC

DNSSECに関してはGeminiがウソをつく

同じ質問を2回続けてすると真逆の答え

DNSSECの肯定応答は納得できる
DNSSECの否定応答は絶望的

知見をブログへ

「哀しみの果てのNSEC」
「哀しみの果てのNSEC3」

# フィールドテスト

ns1.mew.org
プライマリ



ns2.mew.org
セカンダリ




- テストサイト
  - dnsviz.net
  - zonemaster.net
  - dnscheck.jp

# AIを使った開発

- 2026年9月15日よりClaude Codeの利用を開始
- 問題点と脆弱性
  - kazu:「このディレクトリのコードを読んで
    問題点を指摘してください」
  - 気が遠くなるような大量の問題点を指摘され修正を指示
- 設計書
  - kazu:「コードを読んで設計書を書き起こしてください。
    理想を書きます。問題点はissueにします。」
  - https://github.com/iijlab/dnsext/tree/main/dnsext-bowline/clove/design

# ZSKのロールオーバー

| | RFC6781<br>二重署名 | RFC6781<br>事前公開 | RFC6781<br>簡略化<br>事前公開 | clove |
|---|---|---|---|---|
| 増えるもの | すべての<br>RRSIGが2倍 | DNSKEYが<br>2つ | DNSKEYが<br>2つ | DNSKEYが<br>3つ |
| 状態数 | 2 | 3 | 2 | 1 |

- 詳しくは設計書のZSK.mdを参照

# 壊れた世界の模倣

- 「奇妙なDNS設定例」を模倣したい
  - https://www.e-ontap.com/dns/samples.html
- cloveに"`--insecure`"オプションを追加
  - 検査を外す
    - CNAMEと他のRRの共存を許す
    - CNAMEを複数書くことを許す
  - 偽装を許す
    - 実在するのにNXDOMAINを返す
    - 偽のグルーを付ける
    - 他にもたくさん
  - 24個の奇妙な設定例のうち、21個を実現
- bowline
  - 意図通りに振る舞うことを確認