# DNSSEC.jp プロトコル理解SWG
# RFC 5074

# Abstract

- DNSSEC Lookaside Validation (DLV)
- DNS委任連鎖の外側でDNSSECを使う
- トラストアンカーの提供

# Table of Contents

# 1. Introduction

- バリデータが署名済みゾーンを検証するには
  トラストアンカーの設定が必要
- ルートゾーンや多くのTLDでは未署名
- 複数のトラストアンカーを設定しなければならない

- 本文書ではトラストアンカーの提供と
  トラストアンカーの外部管理について定義

# 2. Architecture

- バリデータが署名を検証する時
  1. トラストアンカーが設定されているとき
  2. 1で認証した親ゾーンにDSレコードが設定されているとき
- DLVでは3つ目のメカニズムを提供
  3. DLVドメインが設定されているとき

- DLVドメインの提供
  - 署名済みゾーンのセット
  - DSレコードが登録可能

# 3. DLV Domains

- あるゾーンのトラストアンカーを提供するDLVドメインをターゲットゾーンと呼ぶ
- 「trustbroker.example.com」を.orgゾーンに見立てたり、「bar.example.com」をルートゾーンとして扱うことが可能
- 例えばDLVドメインでは「example.org」を「example.trustbroker.example.com」として扱われる
- 同様にルードゾーンでは「org.bar.example.com」として扱われる
- DLVドメインではDLVレコード以外の情報は含まない
- 積極的にネガティブキャッシュし、最小構成のNSECレコードやNSEC3レコードを最小限の扱いにするべきでない（SHOULD NOT）

# 4. Overview of Validator Behavior

- 最初にDLV以外のトラストアンカーを使用するべきである（SHOULD）
  - クエリの応答時間、DLVドメインの負荷削減
- DLVドメインをトラストアンカーとする時は、DLVドメイン以下のレスポンスを検証するべきである（SHOLD）
- バリデータはDLV RRsetを検索し、RFC4035のセクション5の手順通りDS RRsetを返す
- 複数のDLVドメインが設定されているとき、どのDLVドメインを選択するかについては、[INI1999-19]を参照

# 5. Details of Validator Behavior

- 応答時間に限らずDLVドメインのサーバ負荷削減のためにも、最初にDLV以外のトラストアンカーを検証するべき（SHOULD）
- バリデータは設定されている全てのDLV RRset問い合わせてQNAMEを捜すが、問い合わせの前にキャッシュを確認するべき（SHOULD）
- 見つからなかったときは不在証明を検証するべき（MUST）
- 検証の結果Insecureであれば使用してはならないし（MUST）、レスポンスはInsecureであることを返すべき（SHOULD）
- Insecureの時は他のDLVドメインを検証するべきではない（SHOULD　NOT）

# 6. Aggressive Negative Caching

- 権威サーバの負荷削減のために、バリデータは積極的にネガティブキャッシュするべきである（SHOULD）
  - 権威サーバに問い合わせる前にキャッシュにNSECレコードが存在するか確認
  - バリデータはNSECレコードのキャッシュがあり、CDビットが無ければ常に否定的な応答を返す

# 6.1. Implementation Notes

- 積極的にネガティブキャッシュを行うときは、NSECレコードを効率よく扱う必要がある
  - NSECレコードのデータ構造を保持
  - キャッシュの内容を返すわけではない点に注意

# 7. Overlapping DLV Domains

- DLVドメインは複数登録可能
- 複数のDLVドメインを登録しているとき、どのDLVドメインから問い合わせるかオプションとして実装するべき（SHUOLD）
  - 優先順位のつけかた
  1. 登録順に全てのDLVドメインから検索し、見つかるまで繰り返す
  2. 各DLVドメインに重みを設定して検索
  3. 全てのDLVドメインから検索し、最も重みが高いDLVレコードを採用
  4. それらを含めて選定する為のシステムを作るべき（例えば最初に同じものが2つ現れたら採用）
- 上記は一例なので、詳しくは[INI1999-19]を参照

# 8. Optimization

- 権威サーバは見つかった全てのDLV RRsetを Additional sectionに含むべき（SHOULD）
- バリデータは得られた情報を（検証後）キャッシュしてもよい（MAY）
- DLVドメインへ再び問い合わせするのは避けるべき

# 9. Security Considerations

- 検証に失敗したときはDLVドメインを使用してはならない（MUST NOT）
- ネガティブキャッシュをするとき、NSECレコードのnext nameフィールドを保持しなければならない（MUST）
  - NSECを偽装される恐れ（行き過ぎたNSEC）
  - ワイルドカードレコード
- RRSIGやDNSKEY RRset単体で検証してはならない（MUST）
  - ダウングレード攻撃を受ける恐れ
- DS RRのセキュリティに関する考慮点はDLV RRsetにも適応できる。
  - DS RRの鍵タグからDNSKEYを特定できるがユニークではない

# 10. IANA Considerations

- DLVでは、[RFC4431]でアサイン済みの
  DLVリソースレコード(RR type 32769)を使用