権威DNSサービス調査報告

～beyond the DNSサービス申し込みBoot Camp!～

2021年7月16日(金)
長崎県立大学 岡田雅之･古賀大雅
DNSOPS.JP幹事会 米谷嘉朗･石田慶樹

はじめに

- DNSOPS.JP(日本DNSオペレーターズグループ)は、2020年4月から国内外で提供されている代表的な権威DNSサービスの機能調査を「市井の一ユーザとして」実施しています(絶賛継続中です！)
- 1年間の準備～調査実施、報告会およびDNSOPS.JPコミュニティからのフィードバックを通じて、サービス調査そのものの知見が溜まってきました
- それはDNSに限定されるものではなく、他のネットワークサービスにも通じる部分があると感じ、JANOGコミュニティからもフィードバックをいただければよりよい調査に成長させられると考えました
- 本日は、JANOGコミュニティのみなさんが気にかけているDNS設定項目やサービス契約時の評価項目について、議論させてください

調査の背景

- 前提
  - インターネットサービスの多様化により、サービス情報を提供する汎用データベースとしてDNSの役割が増加している
  - それにともない新しいリソース レコードの定義や、既存リソースレコード(特にTXTレコード)のユースケース追加などが行われている
- 認識
  - 一般的な組織の権威DNSサーバ運用者(ゾーン管理者)はDNSプロトコルや新しいインターネットサービスの専門家ではないため、すべてのリソースレコードを理解し正しく設定できることは期待できない
  - 現代においては、権威DNSサーバの自前運用は設定ミスや大量クエリによるサービス障害の原因となり得るため、一般的な組織においても推奨されない

調査の目的

- 組織のシステム管理部門やサービス提供部門が、それぞれの目的に沿って適切な権威DNS(自ゾーン)を運用可能とするため、国内外で提供されている代表的な権威DNSサービスの機能一覧作成が望まれる
- 本調査の目的は、そのような機能一覧となることである

機能の優劣をつけることや、
特定のサービスを推奨することは目的ではありません。

調査項目

- 組織におけるDNSの利用目的に沿って適切な権威DNSサービスを容易に選択できるようになることを念頭に、以下の観点で権威DNSサービスの機能を調査する

項目	概要
機密性	サービスコンソールログインが多要素認証、ロールベース認証、ゾーン転送にTSIGが利用可能、サブドメイン名ハイジャック対策
可用性	権威DNSサーバの地域冗長性、レスポンスレートリミット、他権威DNSサービスとのセカンダリ連携、地域指定可能、SLA規定、更新処理のDR化
完全性	バックアップ有無・頻度、DNSSEC対応
利便性	専門知識を有しないユーザが目的の設定を容易に行えること、大量のリソースレコードを一括登録できることなど
リソースレコード	最低でもA/AAAA/CNAME/MX/NS/TXT/SRVに対応していること、CAAやDNSSECに対応していることなど
サポート	運用レポートが作成されること、問い合わせが可能で時間帯が明確であることなど
コスト・契約	課金体系が明確であること、契約期間や解除方法が明確であることなど

調査しながら整理中

調査項目

- 組織におけるDNSの利用目的に沿って適切な権威DNSサービスを容易に選択できるようになることを念頭に、以下の観点で権威DNSサービスの機能を調査する

項目	概要
機密性	サービスコンソールログインが多要素認証、ロールベース認証、ゾーン転送にTSIGが利用可能、サブドメイン名ハイジャック対策
可用性	権威DNSサーバの地域冗長性、レスポンスレートリミット、他権威DNSサービスとのセカンダリ連携、地域指定可能、SLA規定、更新処理のDR化
完全性	
利	
リ ド	
サポート	ポートが作成されること、問い合わせが可能で時間帯が明確であることなど
コスト・契約	課金体系が明確であること、契約期間や解除方法が明確であることなど

この実体験、まさにBoot Camp!
運用経験も蓄積してきました

調査しながら整理中

本日の進め方

- 調査レポート(2021年4月9日版)の概要紹介
  - 詳細は調査結果詳細シートに記載
- その後の更新情報紹介
  - 得られる定期運用レポート、追加で調査した権威DNSサービスなど
- DNSOPS.JPコミュニティから得られたフィードバックの概要紹介
- 議論
  - 対象とすべき調査項目、サービス契約時の評価項目など
- まとめ

DNSOPS.JPコミュニティから得られたフィードバック概要紹介(1/2)

- 報告会でのフィードバック(代表的なものを抜粋)
  - サービスの説明に標準的な用語を使用しているか
  - ローカルIPアドレスの逆引きゾーンを設定できるか
  - 登録時にドメイン名のオーナーであることを確認しているか
  - サブドメインの親子同居や兄弟同居の制約はあるか
  - 権威DNSサービスプロバイダ移転(特にDNSSEC有効時)に協力的か
  - NSに設定できるネームサーバ名に制約はあるか
  - Lame Delegationチェックを実施しているか
  - 請求書払い・振込払いが可能か
  - 新しい機能の導入に積極的か

DNSOPS.JPコミュニティから得られたフィードバック概要紹介(2/2)

- ユーザ側フォームからのフィードバック(代表的なものを抜粋)
  - UIを通じたレコード操作の可用性(利便性)は高いか
  - APIはあるか、ある場合は単位時間当たりの利用制限があるか
  - ゾーン(レコード)のエクスポートが可能か
  - OctoDNSに対応しているか
  - ユーザ認証の仕組みとして外部IdP(SAML/OAuthなど)に対応しているか
  - 請求書の送付先を変更可能か
- 事業者側フォームからのフィードバック(代表的なものを抜粋)
  - セカンダリとなる場合、DNSSECの署名サーバとして運用可能か
  - 運用レポート作成やドリルダウン可能なダッシュボードを用意しているか

参加者のみなさまへのお願い

- 調査に対するフィードバックにご協力ください
- 以下の2種類(ユーザー用・事業者用)がありますので、ご自身にとって適切と思われる方を選んでご回答ください

権威DNSサービスユーザー用

権威DNSサービス事業者用

調査費用(実費)はDNS Summer Day 2020および**2021**に
協賛いただいた費用の一部を使用しております。
協賛をいただいた各社様にこの場を借りてお礼申し上げます。

DNSOPS.jp
DNS Operators Group, Japan

議論

DNSOPS.jp
DNS Operators Group, Japan

まとめ