JP DNS ソフトウェアダイバーシティ導入の裏側(LT)

2024年11月26日 Internet Week 2024

DNSOPS.JP BoF

株式会社日本レジストリサービス(JPRS)

池田和樹

自己紹介

名前

- 池田　和樹

所属

- 株式会社日本レジストリサービス(JPRS)

経歴

- 2018年 JPRS新卒入社 システム部に配属
- 2020年～現在 同部 大阪オフィス配属

業務内容

- JP DNS/JP レジストリシステム等のサーバ・ネットワークの管理・運用
- 対外系はDNSOPS.JP 事務局、Internet Week プログラム委員

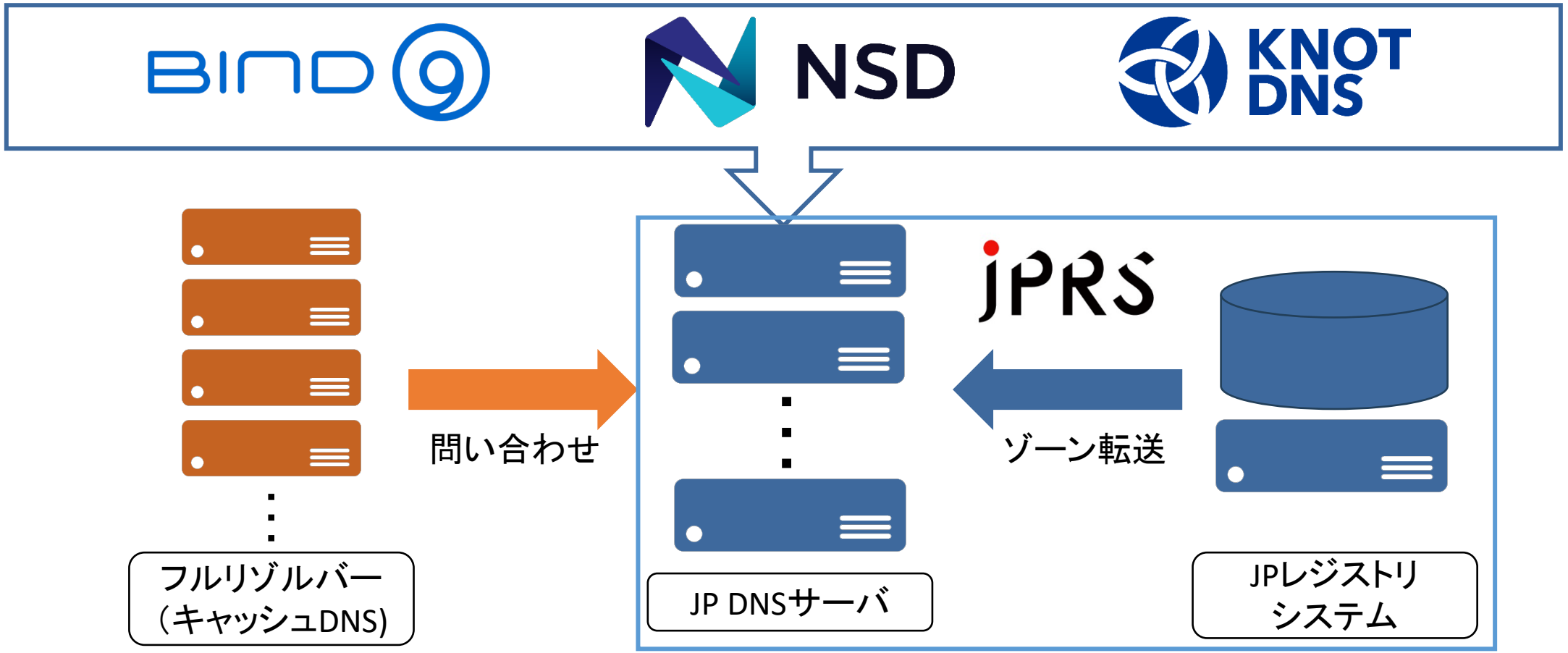
目次

- DNSソフトウェアダイバーシティ確保の振り返り
- 導入時の評価結果の一覧
- クエリ応答比較の詳細
- 3種類のソフトウェアを同時運用することで変わったこと
- 活動全体の所感
- まとめ

JP DNS Updateより再掲

（続報）DNSソフトウェアダイバーシティの確保

■ JP DNSのさらなる安定運用に向けた複数ソフトウェアの導入が完了しました
- ご協力いただいたセカンダリ組織の皆さま、ありがとうございました！



JP DNS Updateより再掲

（続報）DNSソフトウェアダイバーシティの確保

■ 導入までのスケジュールはざっくり下記の通り

- 2023年03月～2023年07月　環境準備
- 2023年08月～2024年05月　応答内容/性能比較、ソフトウェアの機能評価、ゾーン転送評価
- 2023年12月～2024年06月　運用手順準備
- 2024年07月　導入判断
- 2024年07月～08月　NSD・Knot DNS導入

■ 導入時の評価観点例

#	評価項目	確認方法	評価ポイント
1	ソフトウェア機能評価	JP DNSに求められる機能を有しているか確認する	社内で定めている機能評価項目の一覧表を用いて確認し、問題点がないこと
2	ゾーン転送評価	JPゾーンをロードしたBIND 9, NSD, Knot DNSを準備し、ゾーン転送時間を測定する	社内で定めているゾーン転送のサービスレベル目標を満たすこと
3	クエリ応答内容評価	BIND 9, NSD, Knot DNSの応答内容を比較・評価する	JPドメイン名の名前解決の支障とならない応答を返すこと
4	クエリ応答性能評価	性能評価ツールで測定	BIND 9と同等以上の応答性能を有すること
5	運用手順への影響	NSDとKnot DNSを想定した運用手順を作成し、運用可能かを評価する	バージョンアップなどの運用上必要な作業が円滑に実施できること

導入時の評価結果の一覧

#	評価項目	確認方法	評価ポイント	NSDの結果	KnotDNSの結果
1	ソフトウェア機能評価	JP DNSに求められる機能を有しているか確認する	社内で定めている機能評価項目の一覧表を用いて確認し、問題点がないこと	○	○ ゾーン転送用の鍵名がログに出力されなかったため、開発元に依頼し修正してもらった
2	ゾーン転送評価	JPゾーンをロードしたBIND 9, NSD, Knot DNSを準備し、ゾーン転送時間を測定する	社内で定めているゾーン転送のサービスレベル目標を満たすこと	○	○
3	クエリ応答内容評価	BIND 9, NSD, Knot DNSの応答内容を比較・評価する	JPドメイン名の名前解決の支障とならない応答を返すこと	○	○
4	クエリ応答性能評価	性能評価ツールで測定※	BIND 9と同等以上の応答性能を有すること	○ BIND 9の約4倍の性能を有することを確認	○ BIND 9の約4倍の性能を有することを確認
5	運用手順への影響	定型業務の手順やドキュメントを準備し、実際にオペレーションを実施する	ソフトウェアのバージョンアップ手順等を準備し、問題なく動作すること	○	○

※ DNS Summer Day 2024で当社の阿部が発表しておりますのでそちらもご参照ください
DNSソフトウェアのパフォーマンステストをしてみた(https://www.dnsops.jp/event/20240621/20240621_abe.pdf)

クエリ応答比較の詳細

当日投影のみ

3種類のソフトウェアを同時運用することで変わったこと

■ 可用性が向上した
- NSD/Knot DNS導入後にBIND 9の脆弱性情報が公開されたが、これまでよりも落ち着いて対応ができた
  ➔従来：脆弱性が出た！？　影響は！？　いつ一般公開！？ etc…
- ゼロデイ攻撃でサーバーが全滅しないという安心感はとても大きい

■ その一方、実装を多様化したことで運用のコストはある程度上昇した
- 実装の置き換えに伴い、クエリログの取得方法をファイルからdnstapに変更
  ➔出力される情報の違いにより、ログ取得・保存に必要なディスク容量が変化
- 実装ごとに運用・設定・監視・情報収集などのマニュアルを整備する必要がある
  ➔BIND 9の脆弱性対応にかかるコストを考えると、それほどでもないかも？

活動全体の所感

■ 改善の活動はどうしても後手に回りがち
- 最悪、導入日を遅らせて(= 優先度を下げて)対応することになる
- 稼働を集中的に確保できれば、半年ぐらいのプロジェクトか？

➔個人的に、2024年上半期の必須案件の稼動に影響

- プロジェクトの進行中、数回にわたりBIND 9の脆弱性対応が必要になった

➔導入したソフトウェア側でもトラブルに見舞われる…

まとめ

- 事前検証に手間はかかったがNSD/Knot DNSともにある程度の利用実績を持つソフトウェアであることなこともあり、JP DNSへの導入について、途中で断念することはなかった
  - 改善にはそれなりの苦労があった

- BIND 9がベースになっていた分、3種類のソフトウェアを導入することで運用における負荷の集中は避けられるようになったと感じている
  - 情報収集など、平常時の運用負荷は上昇→自動化により運用負荷を軽減
  - 3種類のソフトウェアによる運用は始まったばかりで、改善すべき点はまだ残っている