

キャッシュDNSサーバーとして BINDのみを使用している現場で Unboundを使い始めるまで

日本Unboundユーザー会

山森 夏葉

この中でDNSサーバーの管理者の人は
どのぐらいいらっしゃるでしょうか？
(当てないので安心してください)

＼はい／



このセッションではこんな方をターゲットにお話します！

- ✓ **DNSサーバの管理者だ**
- ✓ **BINDの脆弱性対応に工数が取られている**
- ✓ **BIND以外のソフトを検討・導入を考えている**

- 名前：山森夏葉（やまもりかよう）
- 富山から来ました
- 地元の高専卒業後北陸のIT企業に勤めています（6年目）
- 数万人規模のISPのインターネット系サーバの運用をしています（メール、web、DNSなど）
- Twitter（@infragirl755）

- 1. BINDからの卒業を決意するまで**
- 2. どうやってUnboundに決めたの？**
- 3. どうやってUnboundによる運用を定着させたの？**
- 4. 今後はどうするの？**

- 普段からBINDの脆弱性対応に**工数を取られていた**
- 「**どうしてこんな脆弱性の多い物を使うのか**」と疑問に思っていた
- 脆弱性が多い = **脆弱性対応の工数が増加、サービスの可用性の低下のリスク**
- その年開催のDNS Summer Day 2016のテーマが「**BINDからの卒業**」だと知り参加した

その時のプログラムはこんな感じ

- **BINDからの卒業** (株)インターネットイニシアティブ 島村さん
- **実装紹介：Unbound** (株)インターネットイニシアティブ 島村さん
- **実装紹介：PowerDNS** (株)デージーネット OSS研究室 大野さん
- **実装紹介：NSD** (株)インターネットイニシアティブ 山口さん
- **BINDを辞められない理由 Q&A**

dnsops.jp のDNS Summer Day 2016
のサイトで資料公開されています

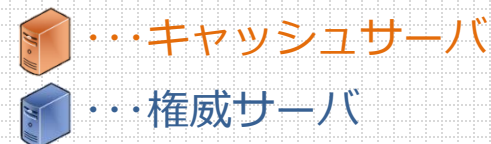
聞いているうちに「うちの現場でBINDに
こだわる理由特にないな」という気持ちに



**BINDからの卒業を
決意して帰社**

当時の現場の環境

- 数千QPS程度
- ACLによるアクセス制限
- view未使用
- 児童ポルノブロッキング実施



外部への反復的な問い合わせも行う

このDNSサーバの運用範囲

冗長構成



反復的な問い合わせ



外部の権威サーバ

再帰検索要求



ユーザ

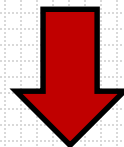
ゾーン転送

外部に公開されている
権威サーバ

当時の現場担当者レベル

DNSサーバを構築するなら…

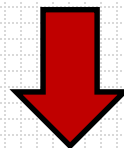
Linux系はBIND一択



古い習慣が残ったままだった

興味本位で調べる人はいるものの、

Linux系ではBIND以外の運用実績はなかった



Linux系のDNSサーバでBIND以外を取り入れる際には
教育コストも考える必要があった

- どのサーバからBINDを卒業しようか？
- キャッシュ or 権威
- 権威は面倒くさそう（レコード更新などの手順書変更が必要）
- キャッシュは楽そう（手順書変更がない）



キャッシュ3台のうち1台をBIND以外に置き換えれば、
マルチベンダ構成により可用性がアップできる！

まずはキャッシュから！

どれにしようかな？

- **PowerDNS Recursor**
- **Unbound**
- **djbdns** ※ググっていたら出てきた

- djbdnsは早々に候補から外れた
(DebianやRHELの安定版でパッケージ採用なし、そもそも動かし方が分からなかった・・・)

- ~~PowerDNS Recursor~~
- Unbound
- ~~djbdns~~

以下の点からUnboundを採用

- ・ **日本語情報の充実**

→日本Unboundユーザー会、素晴らしいスライドの数々

「DNSキャッシュサーバチューニングの勘所」東さん

「Unboundの紹介とその運用」

(株)インターネットイニシアティブ 島村さん

※最近ではpowerDNSも素晴らしい資料がいっぱいあるのよ

- ・ **児童ポルノブロッキングの具体的な設定例があった**

→powerDNS Recursorでも出来るかもしれないが、当時はそのような情報が見つけれなかった・・・

「BINDオンリーのデメリット」

「Unboundがこわくないこと」を知って貰う



BINDオンリーのデメリットを分かって貰うために…

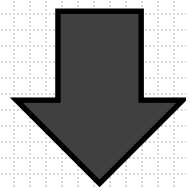
- ・ DNS Summer Day 2016の資料を回覧したり自分の卓上に置き皆さんの目に留めるようにした

Unboundがこわくないことを分かって貰うために…

- ・ Unboundが動くところを見せる
- ・ 大手プロバイダの利用実績があることを見せる
- ・ BINDとの機能およびコマンドの対比表を作る
(現行利用機能は全て備わっているよとか、named-checkconfはunbound-checkconfだよとか)
- ・ 児童ポルノブロッキングのレコード更新はスクリプトで自動化されていた。
スクリプト側でUnboundとBINDの違いを吸収し人間系への負担をかけない
- ・ zabbixによる監視方法を考えて提案

→導入による教育コストを極力減らす努力をした

- 先輩がとても良い意味で厳しくレビューしてくれた
- 上司も「マルチベンダ構成ならば」と承諾してくれた



**理解のある先輩や上司に恵まれたことも
大きかった**

導入してからは・・・

- ・ 2016年9月よりUnbound稼働開始
- ・ 今のところ大きな問題なく動作中！

今後は・・・

- ・ BINDとUnboundのマルチベンダ構成を続ける
→今後の動向を見てBINDからの完全卒業を視野に
- ・ 権威もBINDからの卒業を検討していく

1. BINDからの卒業を決意するまで

→きっかけは**DNS Summer Day 2016**

2. どうやってUnboundに決めたの？

→まずは**キャッシュ**から**マルチベンダ構成**で導入する

→日本語情報の充実

→現場の要件に合っていた（児童ポルノブロッキング）

3. どうやってUnboundによる運用を定着させたの？

→BINDオンリーのデメリット & Unboundこわくないよと布教

→**導入による教育コストを減らす**ための努力

→理解のある先輩や上司にも助けられたよ

4. 今後はどうするの？

→2016年9月から今まで問題なく稼働中

→マルチベンダ構成を続ける

→権威もBINDからの卒業を検討していく