DNSソフトウェア最新動向（権威DNSサーバー編）

2021年11月19日

Internet Week 2021 DNS DAY

（株）日本レジストリサービス

阿波連　良尚（あはれん　よしたか）

本資料の内容

- 広く利用されているOSSの権威DNSサーバー実装の最近の変更
  - BIND 9
  - NSD
  - Knot DNS
- ここ数年で追加された仕様や機能に関する各実装の対応

参考情報として個人的な見解を含んでいます
所属組織や開発元の意見を代表するものではありません

自己紹介

- 名前: 阿波連　良尚 （あはれん　よしたか）
- 所属: （株）日本レジストリサービス　システム部
- 業務内容
  - JP DNSサーバーの運用
  - 事業用・社内ネットワークの運用　など

各ソフトウェアの概要

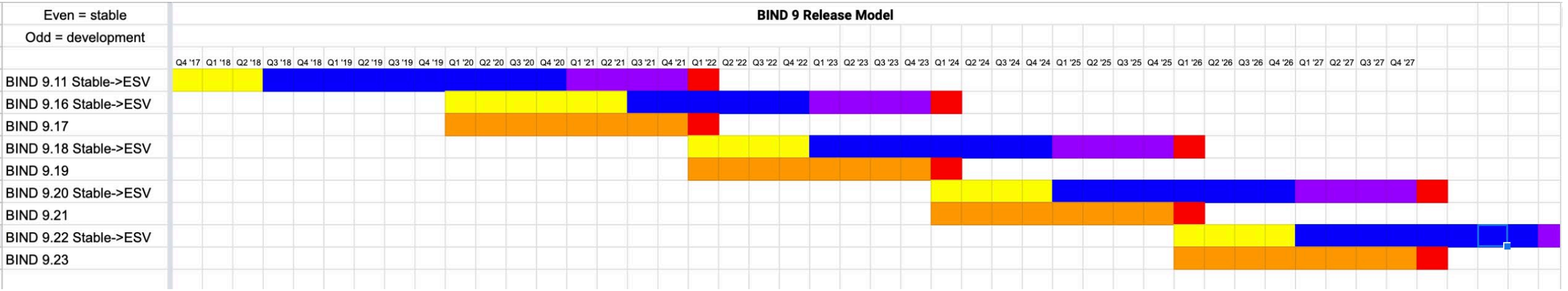
BIND 9の概要

- https://www.isc.org/bind/
- Internet Systems Consortium（アメリカの非営利法人）が開発
- オープンソースソフトウェアだが有償サポートあり
- 最新の安定版（Extended Support Version）は9.16.xシリーズ
- 特徴: 権威DNSサーバーとフルリゾルバーのハイブリッド
- 特徴: ゾーンのプライマリーとしての機能も持つ
  - IXFRによる差分転送の送信やDynamic Updateの処理ができる
  - ZSKのロールオーバーを含めたDNSSEC自動署名ができる

BIND 9の最近の変更

- 9.16がExtended Support Version（ESV: 延長サポート版）に
  - 9.16のサポート期限は2023年末まで
  - 現在ESVである9.11は2021年末までサポート

https://kb.isc.org/docs/aa-00896 から引用



- ネットワーク関連のコードが大幅に書き直された
  - 非同期I/Oライブラリであるlibuvを採用した（必要な外部ライブラリが増えた）

NSDの概要

- https://www.nlnetlabs.nl/projects/nsd/about/
- NLnet Labs（オランダの非営利法人）が開発
- オープンソースソフトウェアだが有償サポートあり
- 安定版と開発版の区別はなく、最新リリースが安定版
- 特徴: 権威DNSサーバー機能に特化
- 特徴: クエリに答える機能に特化
  - IXFRによる差分転送の送信はできない（受信は可能）
  - DNSSEC署名機能は別ソフトウェア（ldns）で提供されている

NSDの最近の変更

- 待ち受けるアドレスをインタフェース名で指定可能に（4.3.3）
  - IPアドレスを設定ファイルにハードコードしなくてよくなった
- ACLがゾーン単位で適用可能に（4.3.6）
  - RPZやCatalog Zones（後述）のようなクエリに応答することを意図していないゾーンについて、 ACLで制限することが可能になった
- answer-cookieのデフォルト設定値がnoに（4.3.8）
  - 複数の実装を混在させた場合に問題があったので変更した

Knot DNSの概要

- https://www.knot-dns.cz/
- CZ.NIC（チェコのccTLD）が開発
- オープンソースソフトウェアだが有償サポートあり
- 最新の安定版は3.1.xシリーズ
- 特徴: 権威DNSサーバー機能に特化
- 特徴: ゾーンのプライマリーとしての機能も持つ
  - IXFRによる差分転送の送信やDynamic Updateの処理ができる
  - ZSKのロールオーバーを含めたDNSSEC自動署名ができる

Knot DNSの最近の変更

- XDPを使ったパケット処理
  - Express Data Path（XDP）は、Linuxカーネル内の処理としてeBPFという特殊なプログラムを実行してパケット処理を行う仕組み
  - Linuxカーネルの提供するプロトコルスタックを飛ばして直接ユーザーランドに渡すことで、処理の高速化を期待できる
  - UDPは3.0.0から、TCPは3.1.0から対応

プロトコル関連の最近の変更

EDNSバッファサイズ

- UDPで応答するメッセージの最大長
  - メッセージがこのサイズに収まりきらない場合、収まる分だけレコードを含めたうえでTCビットをオンにしたメッセージを返す
- DNS Flag Day 2020で、1232バイトがデフォルトの推奨とされた
  - IPフラグメントを避けるため、一般的な環境でフラグメントしないサイズを選定した
  - デフォルト値の変更なので、運用者の判断で別の値を選択することも可能
  - DNSソフトウェアの開発元が足並みを揃えてデフォルト値の変更に追従している

https://dnsflagday.net/2020/index-ja.html

BIND 9	NSD	Knot DNS
• 9.16.8で変更（1232）	• 4.3.3で変更（1232）	• 2.9.0で変更（1232）

IP_PMTUDISC_OMIT

- インタフェースMTUを超えた場合だけIPフラグメントを行う
  - Linuxカーネル3.15で追加されたソケットオプション
  - ICMP packet-too-bigを無視する: 詐称してフラグメントさせる攻撃を防げる
  - SAD DNS（2021年の新型）の対策として有効
- IPフラグメントを禁止（IP_DONTFRAG・IPV6_DONTFRAGをオンに設定）しているわけではない
  - BIND 9・NSDの最新版では明示的にこれらのオプションをオフにしている
  - JPRSの藤原がdraft-ietf-dnsop-avoid-fragmentationとして、UDPではIPフラグメントを避けることを提案中

BIND 9	NSD	Knot DNS
• 9.12.0で追加（v4） 9.16.20で追加（v6）	• 4.1.27で追加	• 2.8.2で追加

HTTPSレコード

- HTTPS通信に必要な情報をDNSで提供するレコードタイプ
  - RFCは近日発行予定（IESGにてレビュー中）　詳しくは次のセッションにて
  - Safari（Mac・iOS）などが対応していて、すでにクエリを送っている
  - エイリアス機能が存在し、CNAMEレコードと違ってゾーン頂点にも書くこともできる
  - 優先度・ターゲット名・key-value型のパラメーターからなる複雑なRDATAになっている
- タイプやRDATAを読みやすい形で書くにはサーバーの対応が必要
  - 対応していなくてもレコードを追加できるが、RDATAをバイナリ表現で書くことになる
  - key-value型のパラメーターについて、未定義のkeyはチェックでエラーになる

BIND 9	NSD	Knot DNS
• 9.16.21で対応 • keyのチェックあり	• 1.13.2で対応 • keyのチェックあり	• 3.1.0で対応 • keyのチェックあり

DNS Cookies（改訂版）

- DNSメッセージのやりとりに軽量なセキュリティを実装する
  - 送信元を偽装したDNS Amp攻撃やキャッシュポイズニング攻撃を防ぐことができる
  - サーバーとクライアント双方の対応が必要
- ロードバランサーやAnycast等で複数の実装を混在させると問題
  - RFC 9018（2021年4月発行）で、実装間で互換性のあるアルゴリズムが標準化された
  - サーバークッキーの生成に使うsecretも共有する必要がある

BIND 9	NSD	Knot DNS
• 9.16.0でRFC 9018対応 • デフォルトでは有効（Cookieを返す）	• 4.3.7でRFC 9018対応 • デフォルトでは無効（Cookieを返さない）	• 2.9.0でRFC 9018対応 • デフォルトでは無効（Cookieを返さない）

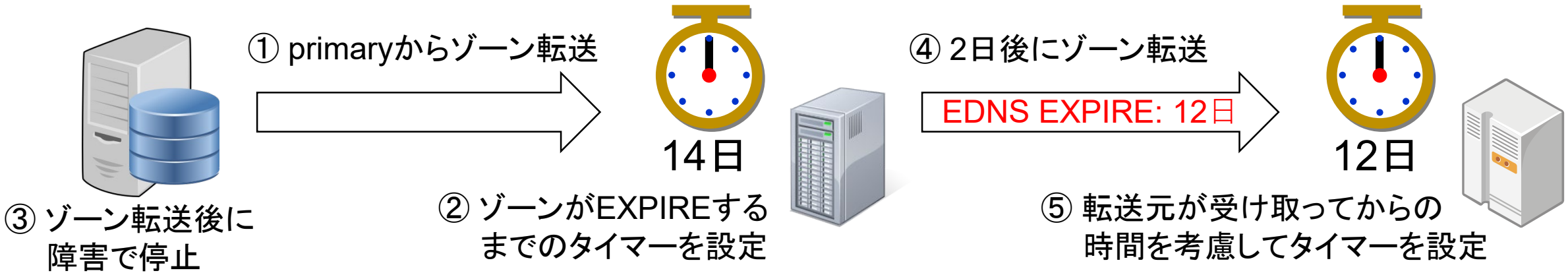
EDNS Extended DNS Error Code

- クライアントに追加のエラー情報を伝えるEDNS拡張
  - rcodeとしてServFailやRefusedを返す状況は複数ありうることに対して、追加のエラー情報を伝えることができるようにする
  - たとえば、権威DNSサーバーが問い合わせを受けたゾーンを持っていない場合、rcodeとしてServFailやRefusedを返すのに加えて「Not Authoritative」（コード20）を返せる
  - フルリゾルバーからの応答に含まれていると、lame delegationになっているのかDNSSEC検証に失敗したのかなど判断できる: トラブルシューティングに便利

BIND 9	NSD	Knot DNS
• 未対応: 次期安定版で実装予定（9.18？） • digコマンドは対応済	• 4.3.6で対応	• 3.1.0で対応

EDNS EXPIRE（実験的）

- ゾーンがexpireするまでの時間を伝えるEDNS拡張
- 多段でゾーン転送を行う際に便利
  - expireまでのタイマー値を引き継いでゾーン転送できる



BIND 9	NSD	Knot DNS
• ゾーン送り側: 有効 • ゾーン受け側: デフォルトでオン	• 未対応	• 未対応

EDNS tcp-keepailve

- TCP接続のタイムアウト時間をクライアントに伝えるEDNS拡張
  - TCP Pipelining（RFC 7766）で、1本のTCP接続で複数のリクエストを処理できるようになったが、アイドル状態の接続は切断すべき（SHOULD）とされている
- このEDNS拡張で、アイドル状態の接続をキープできる
  - クライアントから送ることで、TCP接続をアイドル状態でキープしたいことを伝える
  - サーバーから送ることで、接続をキープしてよい時間を伝える
  - BIND 9は対応しているが、デフォルトはEDNS拡張の有無に関わらず同じタイムアウト

BIND 9	NSD	Knot DNS
• 9.16.21から動作 • デフォルトでは30秒でタイムアウト	• 未対応	• 未対応

XFR-over-TLS（XoT）

- TLSでゾーン転送を行う規格
  - 現在のAXFR・IXFRによるゾーン転送は平文で行われる
  - TSIG等の仕組みでメッセージ認証を行えるが、通信路を覗き見ることでゾーンの内容を見ることは可能であった
  - TLSを使うことで、通信内容の暗号化も行える
  - ゾーン転送の相手は限られるので、証明書の管理は比較的容易と思われる

BIND 9	NSD	Knot DNS
• 未対応: 次期安定版で実装予定（9.18？）	• 4.3.7で対応	• 未対応

Catalog Zones（標準化中）

- ゾーン設定をDNSゾーンの形で展開できる
  - 多数のゾーンをサービスする権威DNSサーバーを複数台展開する際、ゾーンを追加・削除する際にはサーバー設定ファイルの変更も必要だった
  - Catalog Zonesという専用のゾーンを用意し、このゾーンを編集するだけで権威DNSサーバーにゾーンを追加・削除することができる
  - 普通のゾーンと同じなのでゾーン転送の仕組みで更新でき、適用が楽になる
- ソフトウェア実装によらずゾーン設定を統一できる
  - IETFにて標準化が進められており、インターネットドラフトは複数のソフトウェア実装の開発者が著者となっている

BIND 9	NSD	Knot DNS
• 9.11から対応	• 未対応（作業中）	• 3.0.0で対応

ZONEMD

- ゾーンのハッシュ値を書ける新しいレコードタイプ
  - ゾーンのprimaryとなるサーバーで計算してゾーンに含める
  - ハッシュ値を計算して突き合わせることで、正しいゾーンであることを確認できる
  - ゾーンがDNSSEC署名されている場合、 ZONEMDレコードを検証することで、ゾーン全体の内容が署名時点から変更されていないことを検証できる
  - フルリゾルバーがルートゾーンをローカルに持つときに便利
- 現時点では、Knot DNSを除いてハッシュの検証は未対応

BIND 9	NSD	Knot DNS
• ZONEMDレコード: 対応（9.16.16） • ZONEMDハッシュの検証: 未対応	• ZONEMDレコード: 対応（4.3.4） • ZONEMDハッシュの検証: 未対応	• ZONEMDレコード: 対応（2.8.0） • ZONEMDハッシュの検証: 対応（3.1.0）

ANYクエリへの応答を小さくする

- DNS Amp攻撃としてANYクエリが使われてきた
  - ANYクエリへの応答は、存在するすべてのレコードタイプを返すため大きくなりがち
  - UDPでは送信元の偽装が容易であるため、攻撃先を送信元として偽ったANYクエリをインターネットにある権威DNSサーバーに送ることで、DDoS攻撃を行える
- UDPでのANYクエリへの応答を小さくすることで緩和する
  - どれか1つのタイプと対応するRRSIGレコードだけ含めてTCビットをオンにする
  - TCPでクエリを送られた場合には制限しない

BIND 9	NSD	Knot DNS
• 9.11で対応 （デフォルトは無効）	• 4.1.22で対応 （デフォルトは無効）	• 3.0で完全に対応 （常に有効）