DNSソフトウェア最新動向

2022年11月29日

Internet Week 2022 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）

自己紹介

- 名前: 阿波連　良尚 （あはれん　よしたか）
- 勤務先: （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
  - サーバー証明書関連の情報収集
  - 事業用・社内ネットワークの運用　など

本資料の内容

- 広く利用されているDNSサーバー実装の最近の変更点
  ～OARC 38（2022年7月）での各ベンダーの発表を基に～
  - BIND 9 (ISC)
  - NSD / Unbound (NLnet Labs)
  - Knot DNS / Knot Resolver (CZ.NIC)
  - PowerDNS Authoritative Server / PowerDNS Recursor (PowerDNS.COM)
- 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
  - XDP・Catalog Zones
  - 新しい脆弱性「Phoenix Domain」の概要についても簡単に説明

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

各ソフトウェアの概要と最近の変更

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
- 最新の安定版は9.18.xシリーズ
  - 長期サポートの安定版（ESV）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の最近の変更点

- 内部データ構造を赤黒木からqp-trieに変更
  - これまで赤黒木（red-black tree）を使ってデータを管理していたのを、Tony Fitch氏が考案したqp-trieに置き換え中
  - 赤黒木と比べてゾーン読み込みは30％高速化、メモリ使用量は4割に削減
  - まだマージされておらず、マルチスレッド対応は作業中
- 9.18での機能追加や改善
  - フルリゾルバーの性能改善
  - jemallocを採用してメモリ使用量の削減・フラグメントの削減
  - DoH・DoT・XFR over TLS対応
- テストの追加
  - respdiffを利用した他のフルリゾルバーとの応答比較

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（4.6.1）
- 特徴: 権威DNSサーバーとして機能する
- 特徴: クエリに答える機能にフォーカス
  - ~~IXFRによる差分転送の送信はできない（受信は可能）~~
  - IXFRによる差分ゾーン転送（送信）が可能に（4.5.0～）
  - DNSSECゾーン署名機能は提供されていないのでOpenDNSSECなどを使う

NSDの最近の変更点

- ゾーン転送の送信側としてNSDを使うための機能追加
  - これまではクエリーに答えるための機能に特化していた
  - IXFRでの差分ゾーン転送（送信）：
    NSD自身ではゾーンファイルから差分を生成できず、受け取った差分を蓄積しておく
  - セカンダリーとして動作する他の権威DNSサーバーにゾーン転送する用途で
    NSDを使いやすくなる
- そのほか最近の機能追加
  - Extended DNS Errors （EDE）
  - SVCB/HTTPSレコード
  - 相互運用性の高いDNS Cookiesの生成アルゴリズム
  - XFR over TLS

Unboundの概要

- https://nlnetlabs.nl/projects/unbound/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（1.17.0）
- 特徴: フルリゾルバーとして機能する

Unboundの最近の変更点

- エンタープライズ向け機能の追加
  - Response Policy Zone（RPZ）：
    フィルタリングなど応答の書き換えポリシーをDNSゾーンの形で記述
  - インタフェース単位でのビューやACL
- そのほか最近の機能追加
  - ZONEMDレコードによるゾーンの検証
  - SVCB/HTTPSレコード （クエリ処理）
  - ストリーム接続（TCP・TLS）の再利用
  - Extended DNS Errors（EDE）
  - DNS over QUIC（DoQ）（予定）
  - 反復検索でのDNS Cookies対応（予定）

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3.2.xシリーズ
  - Linuxディストリビューションのパッケージではなく、CZ.NICがビルドしたパッケージを使うことが推奨されている
- 特徴: 権威DNSサーバーとして機能する
- 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の最近の変更点

- XDPを使ったパケット処理機能の改善
  - 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
- 多数のゾーンをホストするサーバーでのゾーン転送の改善
  - NOTIFYをリトライ
  - TCP接続の再利用
  - 設定の単純化 （ACLの自動適用、リモート設定のグループ化）
- Catalog Zones機能の改善
  - Hackathonなどで他ベンダーと協力して相互運用性を確認

Knot Resolverの概要

- https://www.knot-resolver.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
- 最新版は5.5.3
  - Linuxディストリビューションのパッケージではなく、
    CZ.NICがビルドしたパッケージを使うことが推奨されている
- 特徴: フルリゾルバーとして機能する
- 特徴: Lua言語などでモジュールを書いて柔軟に機能拡張できる

Knot Resolverの最近の変更点

- 反復検索の問い合わせ先権威DNSサーバー選択の改善
  - ゾーンの権威DNSサーバーが複数個ある時、一番良いものを選択したい
  - すぐにIPアドレスが分かるサーバーを選ぶ
  - 選択アルゴリズムを改善して、レイテンシーを短縮・問い合わせパケット数を削減
- Assertion failureからの回復
  - プログラムを書く時のミスを検知するため、「この条件が成立したら異常」というチェックを仕掛けることがある（assertion）
  - 引っかかった場合、デバッグのためにコアダンプ（メモリ内容を保存）してプログラムを異常終了させるが、サービスは止まってしまう
  - fork(2)した子プロセスでコアダンプを出力し、親プロセスでサービスの再開処理を進めることで、後の調査と修正のための情報取得とダウンタイムの最小化を両立
- ログ出力内容の改善

PowerDNS Authoritative Serverの概要

- https://www.powerdns.com/auth.html
- PowerDNS.COM（オランダの会社）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
- 最新版は4.7.2
- 特徴: 権威DNSサーバーとして機能する
- 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ができる
- 特徴: 独特の機能がある
  - RDBMSをゾーンデータベースのバックエンドとして使える
  - DNSSECのオンライン署名（クエリを受け取ったときに署名を生成）ができる
  - 耐量子暗号（PQC）の1つであるFALCON-512を使ったゾーン署名に対応

PowerDNS Authoritative Serverの最近の変更点

- バージョン4.6 （2022年1月）
  - DNS Cookiesに対応
  - NSEC3パラメーターのデフォルト設定値を改善
- バージョン4.7 （2022年10月）
  - Catalog Zonesに対応

PowerDNS Recursorの概要

- https://www.powerdns.com/recursor.html
- PowerDNS.COM（オランダの会社）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
- 特徴: フルリゾルバーとして機能する
- 最新版は4.7.2

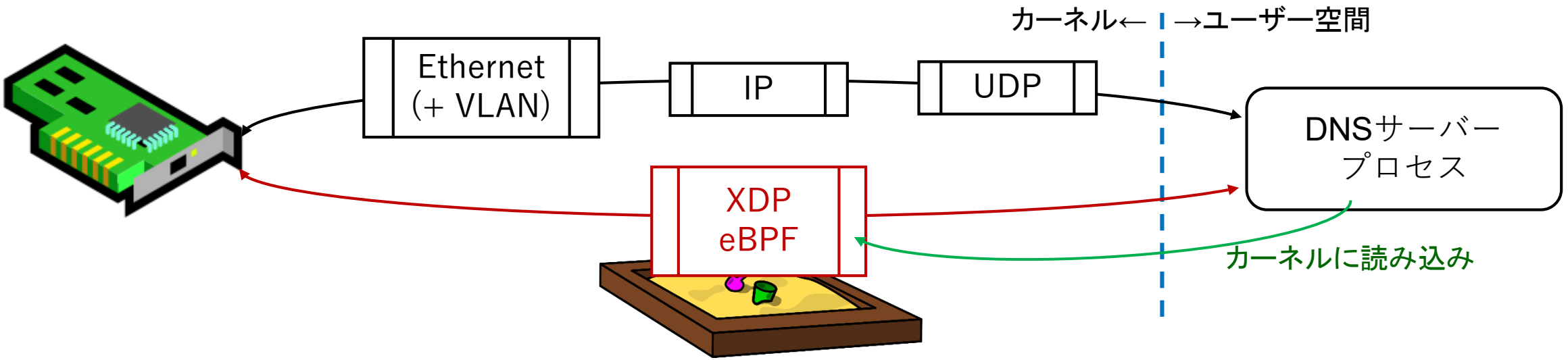
PowerDNS Recursorの最近の変更点

- バージョン4.6 （2021年12月）
  - DNS NOTIFYを使ってキャッシュをクリアする機能の追加
  - 反復検索でのDNS over TLS（DoT）対応
  - ストリーム接続（TCP・TLS）の再利用
  - zone-to-cache: フルリゾルバーのキャッシュにゾーンを読み込む
    （利用例: ルートゾーンの内容を持っておくことで性能向上させる）
- バージョン4.7 （2022年10月）
  - QNAME minimizationに関する更新
  - 権威DNSサーバーがDoTをサポートしているか自動検出
  - ZONEMDレコードによるzone-to-cacheゾーンの検証

Express Data Path (XDP)

XDPとは

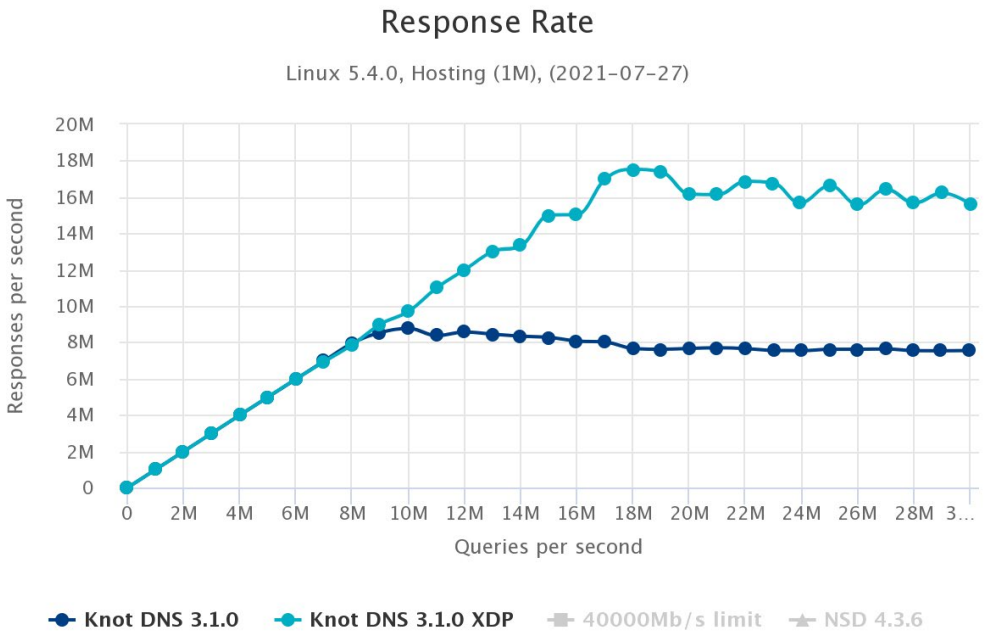
- Linuxカーネルに実装されているパケット処理の仕組み
  - イーサネット→ネットワーク層（IPv4/IPv6）→トランスポート層（TCP/UDP）やiptables/nftables等を通さずに処理することで、オーバーヘッドを極限まで減らす
  - ネットワークカードからパケットを読み取って処理する小さなプログラム（eBPF）をカーネルに読み込ませてサンドボックス環境で処理させる
  - DNS RRLやDNS Cookiesの処理をeBPFで書くことで、カーネル内でドロップさせてDNSサーバープロセスの負荷を減らせる → DDoS攻撃に強くなる



各ソフトウェアでのXDP対応

- 複数のサーバーソフトウェアがXDPに対応しつつある

NSD	Knot DNS	Knot Resolver
• 2022～2023年の開発ロードマップに掲載	• UDP・TCP対応済 • QUIC対応済（初期実装）	• 実験的サポート



Knot DNS 3.1.0での比較で、

- XDPなし: 約900万リクエスト／秒で頭打ち
- **XDPあり**: 約1,700万リクエスト／秒がピーク

（100万ゾーンを読み込んだサーバーの例）

https://www.knot-dns.cz/benchmark/

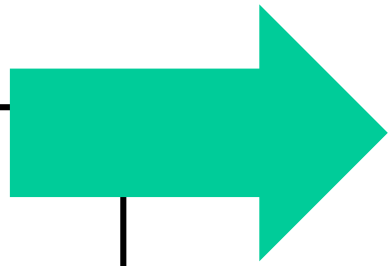
Catalog Zones

Catalog Zonesとは

- 権威DNSサーバーのゾーン設定をDNSゾーンの形で記述する
  - セカンダリーとして動作する際のゾーンの名前・ゾーン転送元などを記載できる
  - サーバーソフトウェアごとに異なる文法の設定ファイルの代わりに、統一された書き方で設定できる
  - ゾーン転送できる: セカンダリーゾーンの追加・削除を多数のサーバーに展開できる

```
zone ”example.jp” {
    type secondary;
    file ”zonefile.zone”;
};
```

```
zone:
    name: example3.or.jp
    zonefile: ”zonefile.zone”
    request-xfr: 2001:db8::feed:53
```



```
$ORIGIN catalog-zone.example.
@             IN  SOA   . . 42 900 600 86400 1
              IN  NS    invalid.
version       IN  TXT   ”1”
masters       IN  AAAA  2001:db8:feed::53
1..0.zones    IN  PTR   example.jp.
a..9.zones    IN  PTR   example3.or.jp.
```

各ソフトウェアでの対応

- Catalog ZonesはまだIETFにて標準化作業中
  - 最初に実装したBIND 9の仕様から変更されスキーマバージョン2となった
  - IETF Hackathonなどで各開発者が相互運用性のテストを実施
  - dnsop WGでの議論を終え、IETF Last Callに向けて作業中
- 多くのサーバーソフトウェアで対応されつつある

BIND 9	NSD	Knot DNS	PowerDNS
• 最初に実装 • スキーマバージョン1と2に対応	• 2022～2023年の開発ロードマップに掲載	• スキーマバージョン2に対応	• スキーマバージョン1と2に対応

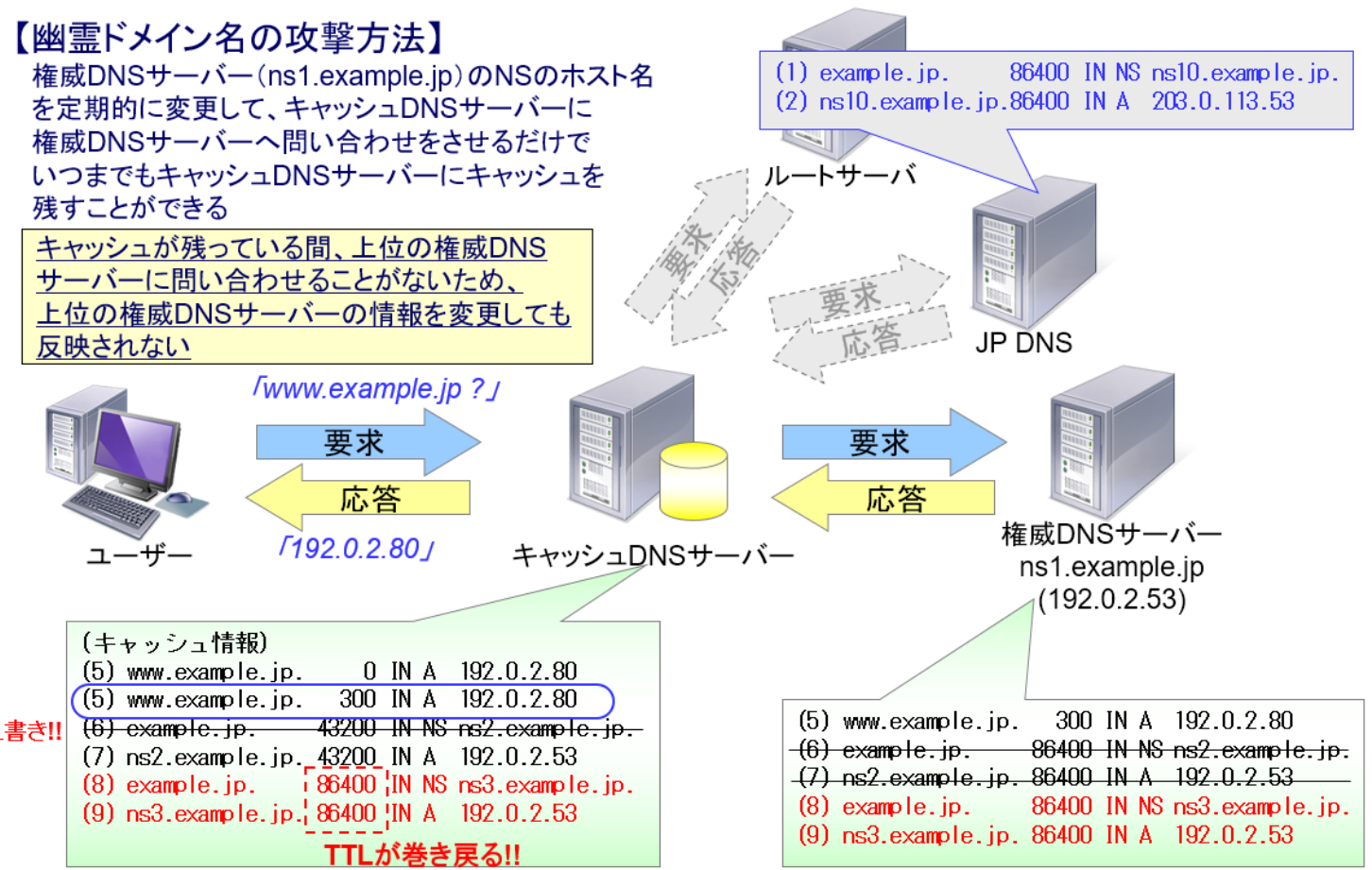
Phoenix Domain

Ghost Domain Names（2012年）

幽霊ドメイン名の動作原理(5)

【幽霊ドメイン名の攻撃方法】
権威DNSサーバー(ns1.example.jp)のNSのホスト名を定期的に変更して、キャッシュDNSサーバーに権威DNSサーバーへ問い合わせをさせるだけでいつまでもキャッシュDNSサーバーにキャッシュを残すことができる

キャッシュが残っている間、上位の権威DNSサーバーに問い合わせることがないため、上位の権威DNSサーバーの情報を変更しても反映されない



13

Interop Tokyo 2012のJPRSブースで投影したスライドを再掲☜

- 委任情報が消されたドメイン名を、名前解決できる状態に残せる
- 2012年に論文が発表された
- 取りうる対策
  - 不具合のないDNSサーバーにバージョンアップする
  - DNSSEC検証を行う
  - 定期的にキャッシュをクリアする

Ghost Domain Reloaded

Webサイト: https://phoenixdomain.net/

- Phoenix Domain: Ghost Domain Namesから10年後……
  - OARC 39（2022年10月）・ICANN DNS Symposium（2022年11月）で発表があった
  - 論文が2023年2月に公開される予定
- 多くのフルリゾルバーが影響を受けるとされている
  - パブリックDNSサービスも含む
  - Unbound・Knot Resolver・PowerDNS等についてはCVE IDが発行されている
- 今後の情報に注意が必要

参考資料

- OARC 38（2022年7月）での各ベンダーの発表
  - セッションのページ
    https://indico.dns-oarc.net/event/43/contributions/927/
  - 発表資料
    https://indico.dns-oarc.net/event/43/contributions/927/attachments/899/1649/DNS-OARC38-vendorpanel.pdf