対訳(参照用)

■スライド 1

BIND 9.11 新機能

Mukund Sivaraman

Internet Systems Consortium

■スライド 2

BIND 9.11 での新しいこと

- データ供給
  - Catalog Zones
  - DynDB
  - rnd showzone, modzone と NZD バックエンド
- DNSSEC
  - ネガティブトラストアンカー(NTA)
  - 子 CDS/CDNSKEY 自動生成
  - DNSSEC 鍵マネージャ
- その他
  - dnstap ロギング
  - EDNS クライアントサブネット(ECS)(権威側)
  - 性能改善

■スライド 3

データ供給

- Catalog Zones 以前は、スレーブサーバ運用者はマスターサーバの新ゾーン追加に自動追従する仕組みを持たなかった。スレーブサーバの設定を変更し reconfig するのみであった。
- 運用者はスレーブを更新する特製のスクリプトや仕組みを必要としない標準的なデータ供給手段を望んでいた。
- ある運用者は共有データベースバックエンドからゾーンデータを供給する機能を望んでいた。
- BIND 管理者はゾーン数が多いと NZF 設定ファイル(rdnc delzone)を使ったゾーン削除が遅いことに気づいた。

■スライド 4

Catalog Zones

- DNS カタログとはゾーンのリストのこと。
- Catalog zone は通常の RR と同様な表記でゾーンのリストを含む通常の DNS ゾーンのこと。
- スレーブはこのゾーンをマスターから転送し、カタログ中のゾーンリストを提供するよう自動的に reconfig する。
- ゾーン名がマスターの catalog zone に追加されると、catalog zone 更新はスレーブに転送される。スレーブは自動的に設定へ新しいゾーンを追加し、それから新しいゾーンの内容をマスターから転送する。
- ISC はこの仕組みを draft-muks-dnsop-dns-catalog-zones-01 で標準化提案している

■スライド 5

Catalog Zone の例

```
cat.isc.org. IN SOA . . 2016022901 900 600 86400 1
cat.isc.org. IN NS nsexample.
version.cat.isc.org. IN TXT "1"
5960775b5c.zones.cat.isc.org. IN PTR domain1.com.
0e2ffd0d66.zones.cat.isc.org. IN PTR domain2.net.
ab89bcd650.zones.cat.isc.org. IN PTR domain3.org.
```

■スライド 6

DynDB - 動的 DB インターフェース

- dns_db は C 言語の API で、named がゾーンデータを格納したり DNS クエリへの応答のためにゾーンデータへアクセスする際に使われる。
- RBTDB は dns_db にデフォルトで静的リンクされた named 内の実装で、ゾーンデータをメモリに格納するのに使われる。
- DynDB は、SQL データベースのような別のバックエンド提供や特製の応答生成のため、動的に読み込み可能な.so モジュールとして、管理者が別の dns_db 実装をインストールできるようにする。このモジュールはドライバと呼ばれる。
- 現在のところ、BIND 9.11 にドライバは含まれていない。ISC はオープンソースの SQL データベース用ドライバが提供されることを期待している。

■スライド 7

ネガティブトラストアンカー(NTA)

- rdnc nta コマンドは一時的かつ特定期間中に特定のドメイン名の DNSSEC 検証を無効にするため使われる。
- この機能は、リゾルバ運用者が、著名なドメイン名が一時的な DNSSEC 検証失敗状態によりそのゾーンの名前解決が失敗するとユーザから苦情を受けたときに役立つ。
- named は定期的に NTA 配下のデータが検証可能になったかを確認する。
- NTA は指定した時間が経過すると期限切れとなる。

■スライド 8

子 CDS/CDNSKEY 自動生成

- BIND は KSK に署名された CDS と CDNSKEY を自動生成するようになった。
- 委任の親側は子ゾーンの CDS と CDNSKEY をポーリングし自動的に親ゾーンの DS を更新することができる。
- この機能は、手作業による親ゾーンの DS 更新を必要とせずに KSK 更新を可能とする。
- 現在のところ BIND は親側が DS を自動更新する機能は実装していないことにご注意。

■スライド 9

dnssec-keymgr - DNSSEC 鍵マネージャ

- BIND が適用する、ゾーンの鍵更新プロセスを補助する Python ラッパーツール。BIND ユーティリティと呼ばれる。
- ポリシー定義ファイル(デフォルトは/etc/dnssec.policy)ファイルを読み込み、ゾーンの鍵がそのゾーンのポリシーに適合するよう DNSSEC 鍵を生成もしくは更新する。
- 新しい鍵は必要に応じて生成される。
- 既存の鍵のタイミングメタデータは正しい鍵更新の必要などに応じて調整される。
- ポリシーに変更があると、関連するすべての鍵は訂正される。
- このツールは自動的かつ補助なし(たとえば cron を使うなど)で使われることが想定されている。

■スライド 10

EDNS クライアントサブネット(ECS)

- BIND 9.11 に権威サーバ用 ECS の基本的な実験実装が追加された。
- BIND 9.11 開発サイクル中に、リゾルバ用 ECS サポートを実装する予定である。こちらは、完全なものでかつすぐにサービス運用可能なものとする。残念ながら、現在は契約的理由でリリースできていない。まずは BIND サブスクリプションユーザに提供を開始する予定だが、一般リリースは 2018 年中となるだろう。

■スライド 11
BIND 開発プロセスへの変更
- 性能ラボ
- ファジングテスト

■スライド 12
性能ラボ - 継続的なベンチマーク
(図省略)

■スライド 13
性能ラボ - テストのリスト
(図省略)

■スライド 14
性能ラボ - QPS 変化の通知
(図省略)

■スライド 15
ファジングと CVE アナウンス
- ISC は能動的に欠陥を見つけ出すため BIND のファジングテストを実施している。
- 昨年から、ファジングとコードレビューにより内部的に発見したバグに対して CVE が発行されている。
- パッチは常に CVS アナウンスとともに提供される。JPRS がリリースアナウンスの日本語訳を提供してくれている。https://jprs.jp/tech/
- OS ディストリビューションにはパッチの適用されたパッケージを用意するため事前に連絡をしており、アナウンス日にはアップグレードが用意される。
- CVE バグ(クラッシュを起こすもの)のほとんどは数年前に入り込んだものである。コードの品質はバグの修正とコードのリファクタリングによって向上している。

■スライド 16
さいごに
- 日本のコミュニティーからのフィードバックを歓迎します。私たちは Twitter 上で多くの問題が日本語で議論されているのを知っています。
- bind-users メーリングリストで問題を議論してください。https://lists.isc.org/mailman/listinfo/bind-users