Internet Week 2012 DNS DAY - DNS実装ダイバーシティの話
NSD

滝澤 隆史
株式会社ハートビーツ MSP事業部所属
http://heartbeats.jp/
日本Unboundユーザー会
http://unbound.jp/

アジェンダ

- NSDの概要
- NSD3の管理運用／仕様上の注意点
- 次期バージョンNSD4

NSDの概要

NSDとは

- Name Server Daemon
  - DNSのアナグラム？
- 権威ネームサーバ
  - 権威ネームサーバのみの機能を提供
- オープンソース ソフトウェア

NSDの開発元

- NLnet LabsとRIPE NCCの共同チームによる開発
  - NLnet Labs
    - オランダにある研究開発機関
    - 主にDNSとDNSSECについての調査研究およびソフトウェア開発をしている
    - NSD, Unbound, drill, ldns, OpenDNSSEC
  - RIPE NCC
    - 欧州・中近東地域のRIR

NSDのリリース

- NLnet Labsからリリース
  - http://www.nlnetlabs.nl/projects/nsd/
- 最新版はNSD 3.2.14
- 次期バージョンNSD4を開発中
  - http://www.nlnetlabs.nl/svn/nsd/trunk/

NSDとルートサーバ

- ルートサーバの遺伝的多様性
  - BINDに対するゼロ デイ アタックへの対策
- 2003年2月、RIPE NCCが運用しているルートサーバk.root-servers.netがBINDからNSDに切り替え
- 現在、H, K, LがNSDで運用している

```
$ dig @h.root-servers.net. version.server. CH TXT +norec
  (中略)
;; ANSWER SECTION:
version.server.          0       CH      TXT     "NSD 3.2.14"
```

NSDの設計目標

- "NSD3 an Authoritative Nameserver: Technical Design"より抜粋
  - Olaf Kolkman, 04 April 2006
  - http://www.nlnetlabs.nl/downloads/presentations/NSD_DenicTechnical.pdf

NSDの設計目標

- DNS関連のRFCへの適合
  - 曖昧なところを文書で説明
- 他の実装に対するコードの多様性
  - 新たに書き起こしている
- 権威サーバのみ
  - 再帰検索機能を持たない
- BIND 8/9に対する回帰試験
  - 違いを理解する
- 高負荷への耐性
  - DoS攻撃への対処

NSDの設計目標

- オープンソース
  - 最初の公開から
- ドキュメンテーション
  - 操作方法と内部コード
- レビューされたコード
  - 内部チェックとテスト
- 単純さ
  - Simple == Secure
- 移植性
  - UNIX系OS(FreeBSD, Linux, Solaris, etc)

NSD3の脆弱性

- 全くないわけではないが少ない
- 2006年5月～現在（2012年11月）の6年半
  - 2012年7月 CVE-2012-2979
  - 2012年7月 CVE-2012-2978
  - 2009年5月 CVE-2009-1755

性能

- Performance tests results on BIND9/NSD/UNBOUND
  - IEPG Meeting – November 2010 @ IETF 79
    - http://iepg.org/2010-11-ietf79/
  - Orange LabsのDaniel Migault氏の発表
- Alternaive DNS Servers
  - Jan-Piet Mens氏の書籍
    - http://jpmens.net/2010/10/29/alternative-dns-servers-the-book-as-pdf/

NSD3の
管理運用・仕様上の注意点

BIND 9と違う！

- コマンドもアーキテクチャも異なることを意識すること
- BIND 9と同じようには使えない

機能 (REQUIREMENTSより)

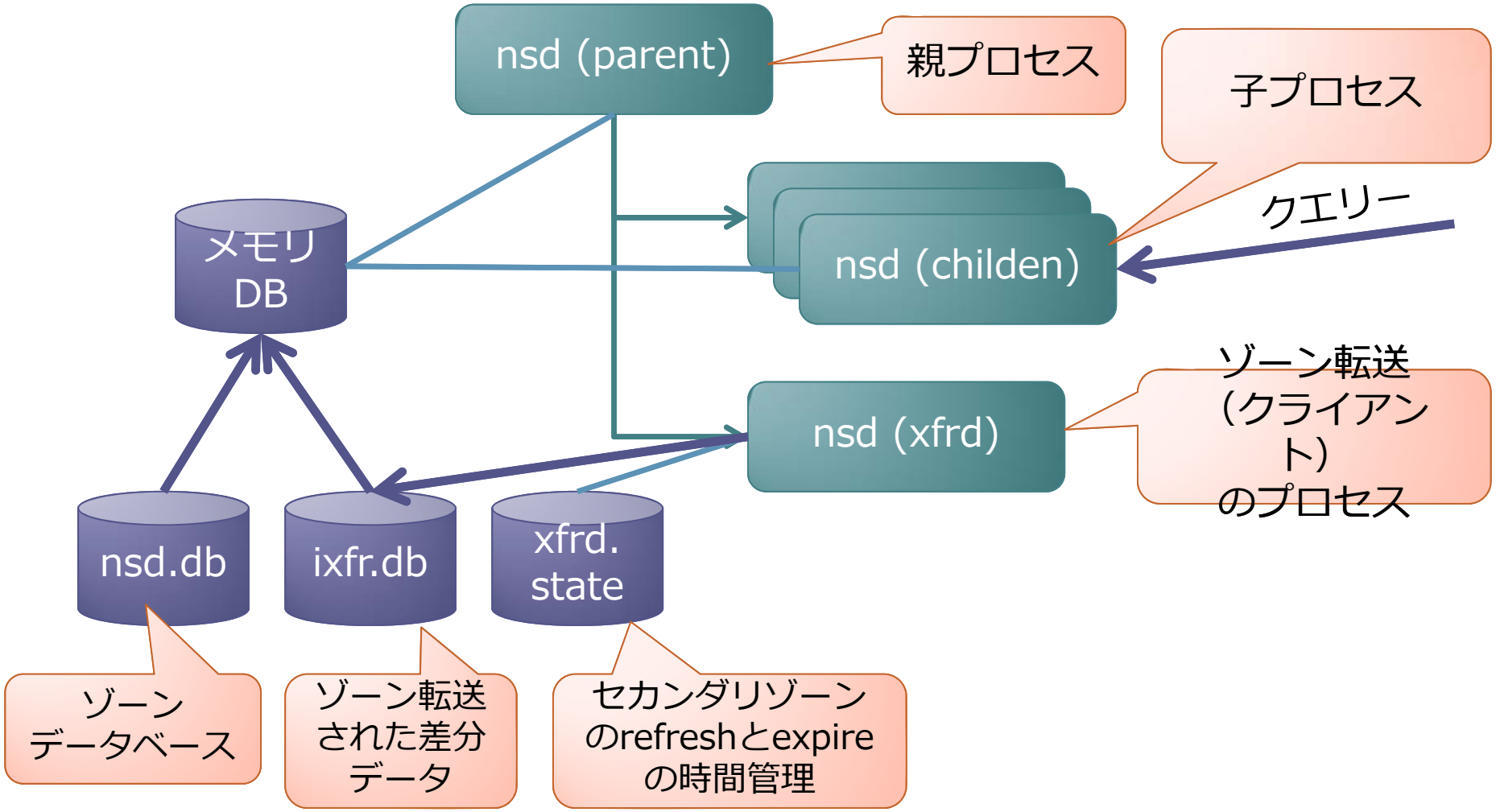
- サポートしている機能
  - RFC 1995 (IXFR) （スレーブ側のみ）
  - RFC 1996 (NOTIFY)
  - RFC 2845 (TSIG)
  - RFC 2672 (DNAME)
  - RFC 4509 (SHA-256 DS)
  - RFC 4635 (HMAC SHA TSIG)
  - RFC 5001 (NSID)
  - RFC 5155 (NSEC3)
  - RFC 5702 (SHA-2)
  - RFC 5936 (AXFR)
  - RFC 6605 (ECDSA)
  - draft-ietf-dane-protocol (DANE)
- サポートしてない機能
  - RFC 2136 (Dynamic update)

NSD3のプログラム

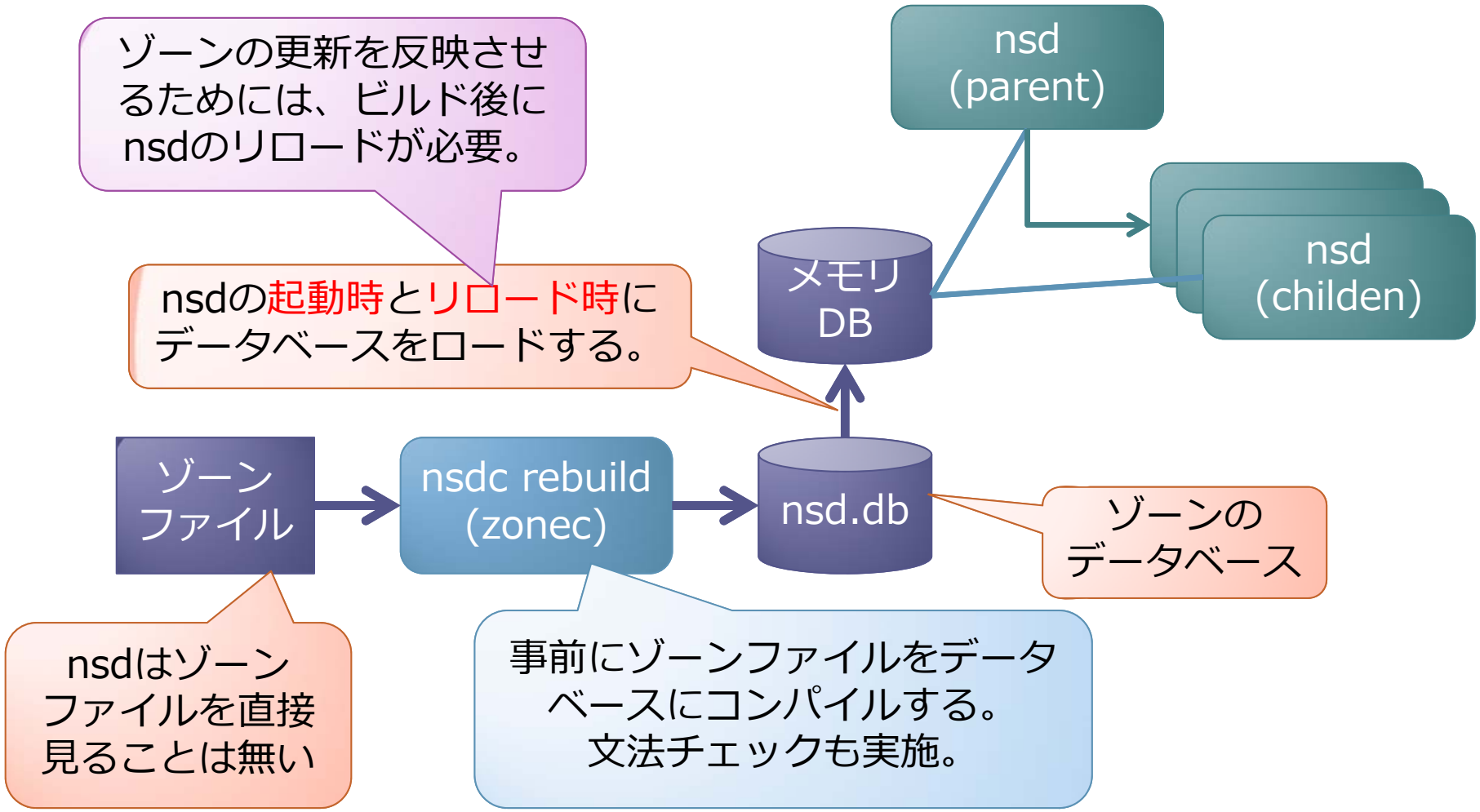
プログラム	説明
nsd	デーモン
nsd-checkconf	nsd.confをチェックするプログラム
nsdc	デーモンを制御するシェルスクリプト。 下記プログラムのフロントエンドでもある。
zonec	ゾーン コンパイラ
nsd-patch	ゾーン転送による変更をゾーンファイルに書き戻すプログラム
nsd-notify	NOTIFYを送信するプログラム
nsd-xfer	コマンドラインからAXFRを使って、マスタ サーバからゾーンを受け取るプログラム

アーキテクチャ

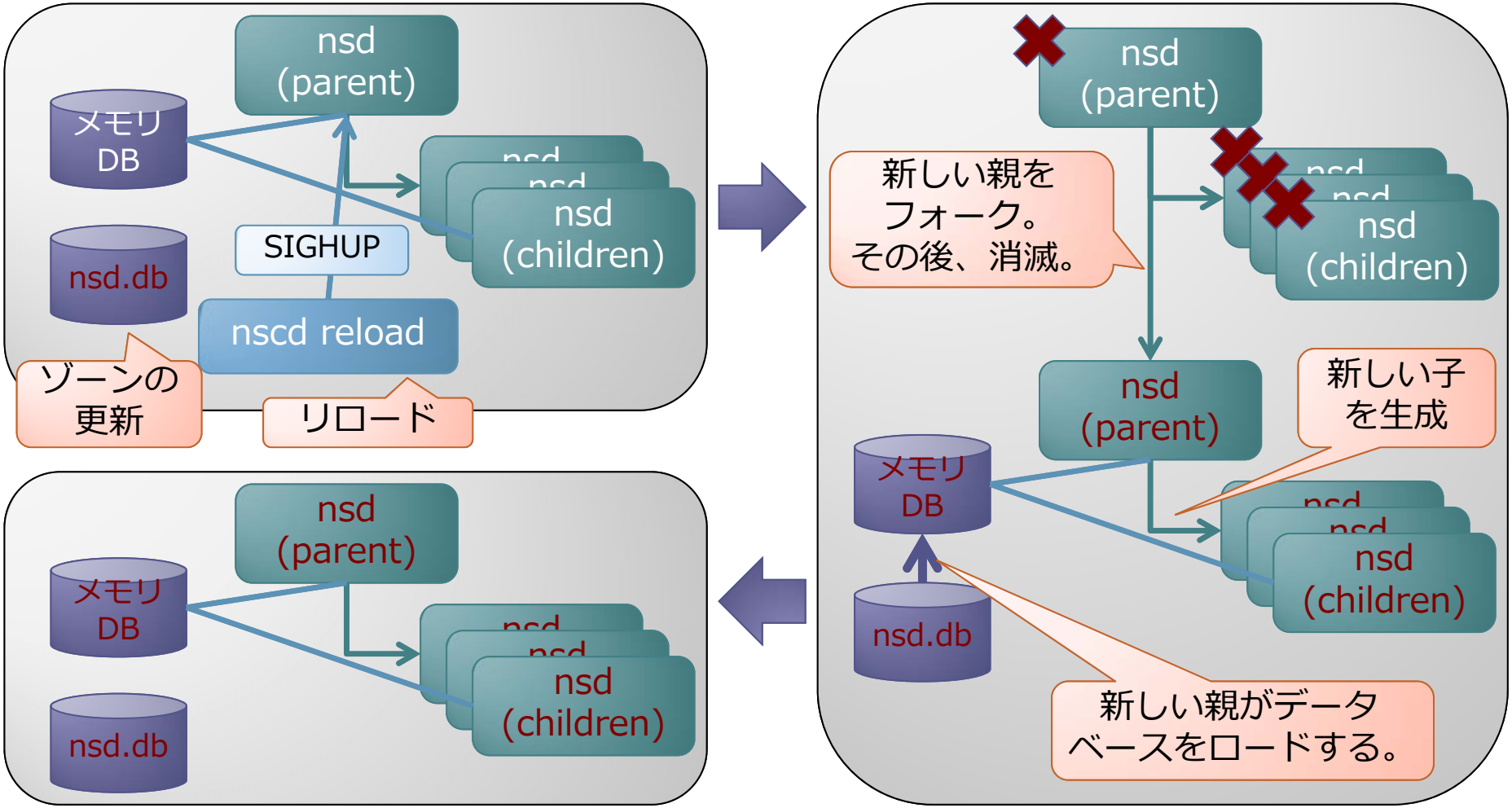
```
$ ps axf
  PID TTY STAT TIME COMMAND
24219 ?   Ss   0:00 /usr/sbin/nsd -c /etc/nsd3/nsd.conf
24220 ?   S    0:00  ¥_ /usr/sbin/nsd -c /etc/nsd3/nsd.conf
24221 ?   S    0:00  ¥_ /usr/sbin/nsd -c /etc/nsd3/nsd.conf
24222 ?   S    0:00  ¥_ /usr/sbin/nsd -c /etc/nsd3/nsd.conf
```



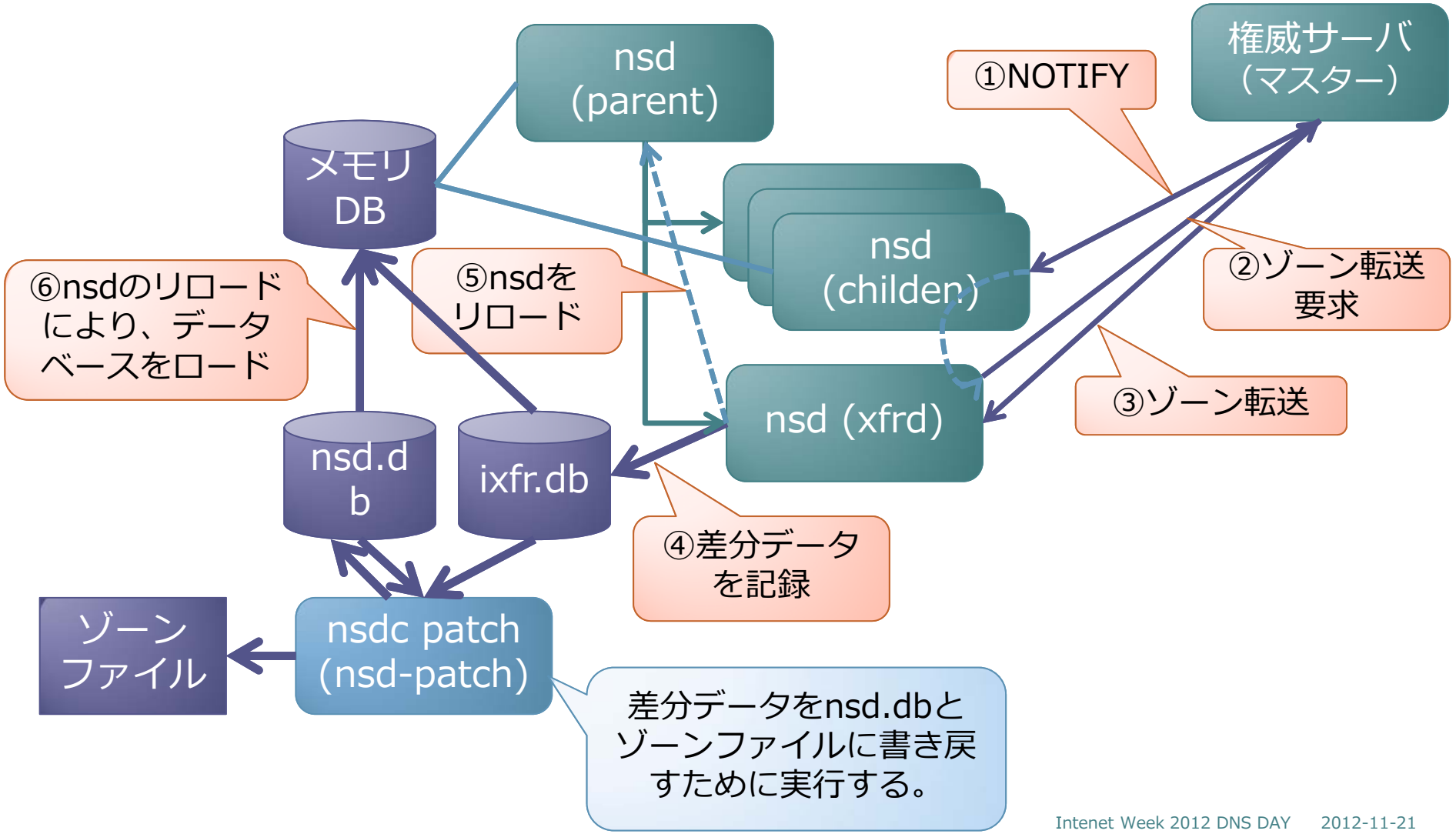
ゾーンファイルとデータベース



ゾーンの更新とnsdのリロード



ゾーン転送（スレーブ側の動作）



ゾーンの更新

- 更新手順
  - ゾーンファイルの更新
  - ゾーンファイルのビルド
    - nsdc rebuild
  - ゾーン データベースのリロード
    - nsdc reload
- マスター側
  - nsdのプロセスが起動し直しになる。
- スレーブ側
  - ゾーン転送後にnsdが自動的にリロードされ、nsdのプロセスが起動し直しになる。

ゾーンの追加・削除

- 手順
  - nsd.confの更新
  - ゾーンファイルのリビルド
    - ・nsdc rebuild
  - nsdの再起動
    - ・nsdc restart
- 説明
  - nsd.confを更新しているため、設定を反映するためにはnsdの再起動が必要。
    - ・nsdには設定ファイルのリロード機能は無い！
  - 再起動に伴い、サービスの瞬断が発生。

設定ファイルの形式

- 設定ファイル
  - /etc/nsd/nsd.conf
- 形式
  - 属性名: 値

設定例（マスター）

```
server:
    ip-address: 192.0.2.1
key:
    name: tsig.example.jp
    algorithm: hmac-sha1
    secret: "ICzS3R+oAZJp607jZ36eKw=="
zone:
    name: example.jp.
    zonefile: example.jp.zone
    notify: 192.0.2.2 NOKEY
    provide-xfr: 192.0.2.2 tsig.example.jp
```

NOTIFYによる通知先。
スレーブのIPアドレスを明示的に指定。

ゾーン転送要求に対するアクセス制御。
デフォルト拒否。
スレーブのIPアドレスを明示的に指定。

設定例（スレーブ）

```
server:
    ip-address: 192.0.2.2
key:
    name: tsig.example.jp
    algorithm: hmac-sha1
    secret: "lCzS3R+oAZJp607jZ36eKw=="
zone:
    name: example.jp.
    zonefile: example.jp.zone
    allow-notify: 192.0.2.1 NOKEY
    allow-notify: 127.0.0.1 NOKEY
    request-xfr: AXFR 192.0.2.1 tsig.example.jp
```

NOTIFYの受信のアクセス制御。
マスターのIPアドレスを明示的に指定。

nsdc update用

ゾーン転送の要求先。
マスターのIPアドレスを明示的に指定。

ゾーン転送とNOTIFY

- マスターやスレーブであることを宣言する設定はない
- 役割に応じて、ゾーン転送とNOTIFYの設定を行う。
  - ゾーン転送を受け付ける(provide-xfr)、要求する(request-xfr)
  - NOTIFYを受け付ける(allow-notify)、送信する(notify)
- NOTIFYの暗黙の設定がない。
  - ゾーンのRRにより動作が変わることはない。
    - リゾルバ機能がないため、そもそもSOA MNAMEやNSで指定したホストの名前の解決ができない。
  - 明示的に設定する必要がある。
  - 参考：BINDの場合
    - NOTIFYの通知先（マスター側）
      - （SOA MNAMEを除いた）NSレコードのサーバに通知する。
    - NOTIFYの許可（スレーブ側）
      - マスターからのNOTIFYを許可する。

リゾルバ機能無し

- ヒントファイルを持たない。
- 権威を持たないゾーンへのクエリーに対してSERVFAILを返す。
  - ヒントを持たないし、再帰検索もしないのでreferralを返しようがない。
- NOTIFYの通知先やアクセス制御にゾーンのSOAやNSを参照しない。

NSD3の注意点のまとめ

- BINDとアーキテクチャやコマンドが異なるので同じようには運用できない（当たり前ですが）。
  - ゾーンファイルとデータベース
  - 設定ファイルの形式や内容
- 権威サーバとしての機能や挙動の違いがある
  - Response Differences between NSD and other DNS Servers
    - http://www.nlnetlabs.nl/downloads/nsd/differences.pdf

NSD3の注意点のまとめ

- 何か変更をするたびに、プロセスが再起動あるいはリロード（プロセスの起動し直し）する
  - 設定ファイルの変更 → 再起動
  - ゾーンの追加や削除 → 再起動
  - ゾーンの更新 → リロード
  - スレーブ側のゾーン転送後 →リロード

NSD3が適した用途

- ゾーンの変更の頻度が多くない場合
- 用途
  - ルートサーバ
  - 企業・団体の権威ネームサーバ

NSD3が適さない用途

- ゾーンの変更の頻度が多い場合
  - ゾーンのRRを変更するたびにプロセス再起動とか、
  - ゾーンを追加するたびにnsdを再起動とか、
  - 頻繁にあったらいやですよね。
- 用途
  - xSP
    - 使うとしたら、何らかの工夫が必要と思われる。

次期バージョンNSD4

2012年11月時点での情報です。
11月5日に開発リポジトリからcheckoutしたもので評価を行っています。このときのバージョンは4.0.0_imp_6です。
将来、仕様や実装が変わる可能性がありますのでご了承ください。

NSD4のプログラム(4.0.0_imp_6)

プログラム	説明
nsd	デーモン
nsd-checkconf	nsd.confをチェックするプログラム
nsd-control	デーモンを制御するプログラム
nsd-control-setup	nsd-control用のプライベート鍵と公開鍵証明書を作成するスクリプト

nsdc, zonec,
nsd-notify, nsd-patch,
nsd-xferコマンドの廃止

参考: Unboundの場合
unbound
unbound-checkconf
unbound-control
unbound-control-setup
unbound-host
unbound-anchor

ゾーン コンパイラー

- nsdにゾーンコンパイラーの機能が統合された
  - 手動でゾーンファイルをコンパイルする必要はなくなった
  - ゾーンの更新を反映させるためのプロセスの再起動は必要なくなるはず（動作未確認）

高負荷への耐性

- libevent対応によるイベント駆動
  - 元々それなりに処理が速かったが、
  - もっと速くなる
  - ベンチマーク
    - http://www.nlnetlabs.nl/downloads/presentations/NSD_Update_OARC_2011SF.pdf
- 内部データベースの変更
- Response Rate Limiting (RRL)対応
  - NSD3でも対応予定らしい

nsd-controlによる制御

- unbound-controlのNSD版
  - TCP 8952番ポート
  - TLSによる通信の暗号化
  - nsd-control-setup.shスクリプトによるプライベート鍵と公開鍵証明書の作成

nsd-controlのコマンド

```
Usage:      nsd-control [options] command
Commands:
  start                                start server; runs nsd(8)
  stop                                 stops the server
  reload [<zone>]                      reload modified zonefiles from disk
  repattern                            reload tsig keys, patterns from config file
  log_reopen                           reopen logfile (for log rotate)
  status                               display status of server
  stats                                print statistics
  stats_noreset                        peek at statistics
  addzone <name> <pattern>             add a new zone
  delzone <name>                       remove a zone
  write [<zone>]                       write changed zonefiles to disk
  notify [<zone>]                      send NOTIFY messages to slave servers
  transfer [<zone>]                    try to update slave zones to newer serial
  force_transfer [<zone>]              update slave zones with AXFR, no serial check
  zonestatus [<zone>]                  print state, serial, activity
  verbosity <number>                   change logging detail
```

パターン

- パターンを使った動的なゾーンの追加・削除
  - 再起動無しにゾーンの追加・削除が可能
  - 設定例

```
pattern:
        name: "masterzone"
        zonefile: "zones/%s.zone"
        notify: 192.0.2.1 NOKEY
        provide-xfr: 192.0.2.1 tsig.masterzone
```

ゾーンファイルの配置
（マクロ%sを使える）

  - コマンド例
    - nsd-control addzone example.jp masterzone
      nsd-control delzone example.jp
- パターンの定義そのもののリロードも可能

NSD4のまとめ

- 特徴
  - nsd-controlによる制御
  - パターンで動的にゾーンの追加・削除
  - 再起動無しに設定やゾーンの更新が可能
  - ⇒ ゾーンの更新頻度が高いxSPでも利用できるレベルになるはず
- NSD 4.0.0_imp_6の状況
  - まだ動かない機能が多い。
    - 話者の環境・使い方の問題なのか、まだ実装されていないのか。

参考文書

- 公式サイト
  - http://www.nlnetlabs.nl/projects/nsd/
- ドキュメントの邦訳（日本Unboundユーザー会）
  - http://unbound.jp/nsd/
- NSD3 an Authoritative Nameserver: Technical
  - http://www.nlnetlabs.nl/downloads/presentations/NSD_DenicTechnical.pdf
- Response Differences between NSD and other DNS Servers
  - http://www.nlnetlabs.nl/downloads/nsd/differences.pdf
- NSD Evolution of a name server
  - http://www.nlnetlabs.nl/downloads/presentations/NSD_Update_OARC_2011SF.pdf
- nlnetlabs.nl :: Blog :: NSD4 Features
  - http://www.nlnetlabs.nl/blog/2012/09/14/nsd4-features/
- nlnetlabs.nl :: Blog :: NSD Response Rate Limiting
  - http://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/