djbdns

2001年12月7日
InternetWeek2001/DNS meeting

(株)日本レジストリサービス(JPRS)
森下 泰宏
<yasuhiro@jprs.jp>

djbdnsとは

- qmail等の優秀なソフトウェアツールの作者として有名なD. J. Bernstein氏(以下DJB)によって作成されたDNSの実装の1つ
- **現在の最新版**: djbdns-1.05
- **フリーソフトウェアとして、** http://cr.yp.to/djbdns.html **から入手可能**

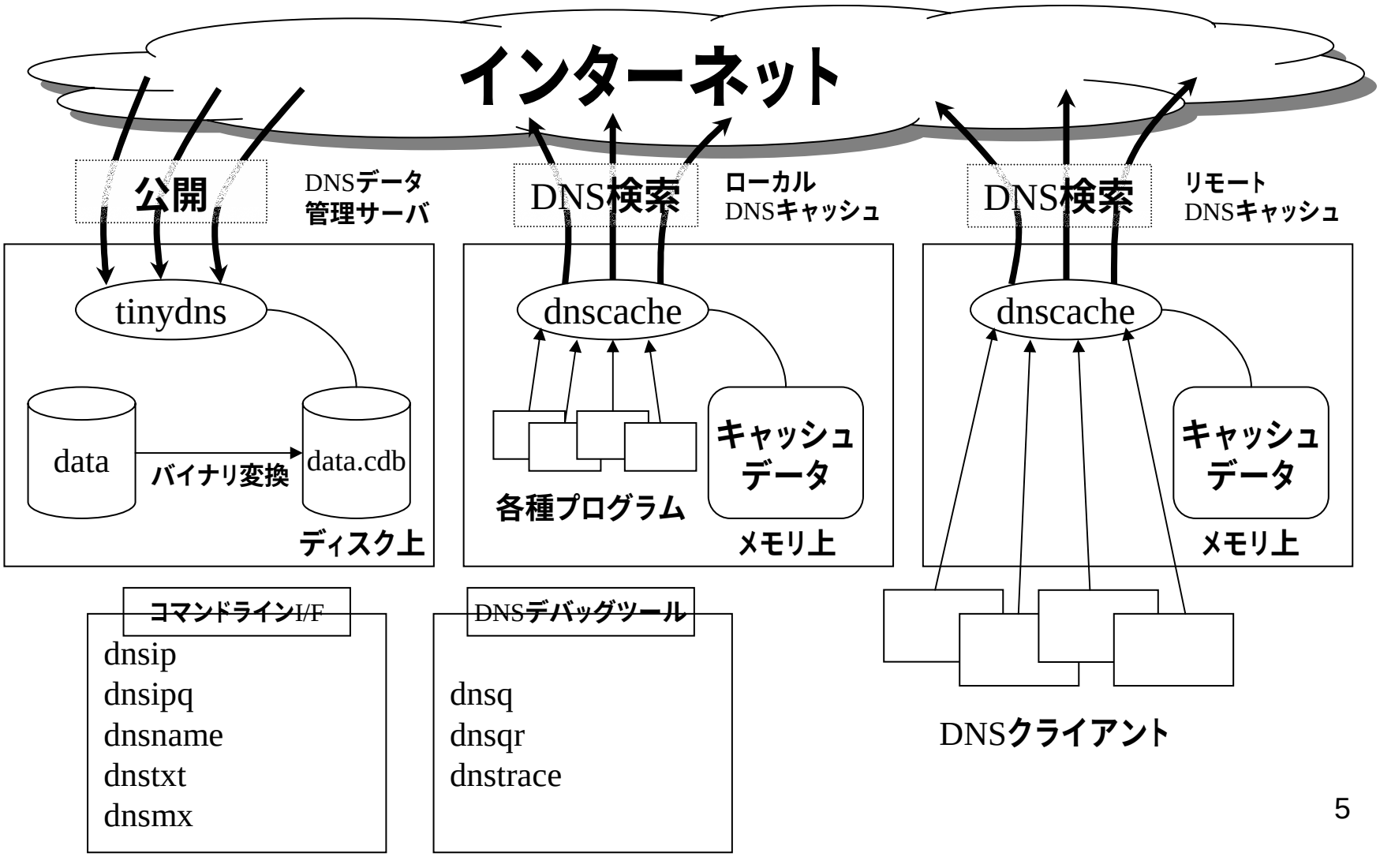
djbdnsの特徴

- 他のDJBのプログラム/ツールと同様、DJBのソフトウェアに対する哲学が色濃く反映されている
  - 機能ごとに分割された「小さな」プログラム群
  - セキュリティ保全に対する高度な配慮
  - 簡潔かつ必要十分な機能
  - 簡潔な設定ファイル

djbdnsの主な構成

- DNSキャッシュサーバ(ローカル、リモート)
  - dnscache
- DNSデータ管理サーバ
  - tinydns
- DNSに対するコマンドラインインタフェース
  - dnsip, dnsipq, dnsname, dnstxt, dnsmx
- DNSデバッグツール
  - dnsq, dnsqr, dnstrace

djbdnsの構成図


インターネット
公開
DNSデータ
管理サーバ
DNS検索
ローカル
DNSキャッシュ
DNS検索
リモート
DNSキャッシュ
tinydns
dnscache
dnscache
data
バイナリ変換
data.cdb
ディスク上
各種プログラム
キャッシュ
データ
メモリ上
キャッシュ
データ
メモリ上
コマンドラインI/F
dnsip
dnsipq
dnsname
dnstxt
dnsmx
DNSデバッグツール
dnsq
dnsqr
dnstrace
DNSクライアント

djbdnsのセキュリティ

- 各種サーバプログラムはすべて専用の非root UIDのもと、chroot()された環境で実行される
- リモートDNSキャッシュサーバは明示的に指定されたIPアドレス以外からのアクセス(利用)は受け付けない
- いわゆるDNS cache poisoningに対して耐性がある
- DNSデータ管理サーバは情報をキャッシュしない
- DNSデータ管理サーバは再帰検索を行わない(本来不必要)

DNSキャッシュサーバ - dnscache

- 「容量に上限のある」キャッシュにDNS検索情報を保持(オンメモリ)
  - 上限のデフォルトは1MB(変更可能)
  - BIND(8まで)のキャッシュ容量は制限なし
- localhostに対する正引きと127.0.0.1に対する逆引きはdnscacheの内部で独自に処理される
  - サーバ側で明示的に設定する必要なし

dnscache(続き)

- ローカルdnscacheとリモートdnscache
  - ローカルdnscache
    - 127.0.0.1のポート53にbind()
    - ローカルホストに対するDNSキャッシュサーバとして動作
  - リモートdnscache
    - インタフェースにつけられたIPアドレスのポート53にbind()
    - リモートホストに対するDNSキャッシュサーバとして動作
- ある(サブ)ドメインツリー以下を、指定したDNSサーバに問い合わせるようにする設定が簡単にできる
  - split DNS機能
  - イントラネット/ファイアウォール内部用のDNSキャッシュサーバを簡単に構築できる

DNSデータ管理サーバ - tinydns

- 指定されたゾーンのDNSデータを管理し、DNSサーバとして公開する機能をもつ
- DNSデータ管理および公開に特化
  - データをキャッシュしない
  - 再帰検索を行わない
- データファイルは簡潔なテキストファイルで記述する(後述)

tinydns(続き)

- データファイルはcdbというバイナリ形式でディスク上に保存され、参照される
  - オンメモリでデータを持たない(BINDと異なる)
- データファイルの更新の際は、テキスト形式からcdbに変換された上でアトミックに置換される
  - データ更新の際に不安定な状態が起らない
- データファイルにエラーがあった場合にはcdbの更新は行われず、古いデータで継続して動作する
  - BINDと比較して、データ更新の際の不慮の事故が起りにくい構造となっている

tinydnsデータファイルの記述例

```
# This line is comment
# SOA/NS/A of example.jp and 123.168.192.in-addr.arpa
.example.jp:192.168.123.250:a
.example.jp:10.0.0.1:b
.123.168.192.in-addr.arpa::a.ns.example.jp
.123.168.192.in-addr.arpa::b.ns.example.jp
# MX/A of example.jp
@example.jp:192.168.123.251:a
@example.jp::host.example.com:10
# A/PTR of example.jp
=host1.example.jp:192.168.123.1
=host2.example.jp:192.168.123.2
=router.example.jp:192.168.123.254
# A of example.jp
+www.example.jp:192.168.123.1
+ftp.example.jp:192.168.123.1
# NS/A of example.jp (for delegation)
&sub1.example.jp:10.0.1.1:a
&sub1.example.jp:10.0.1.2:b
&sub2.example.jp:10.0.2.1:ns1.sub2.example.jp
&sub2.example.jp:10.0.2.2:ns2.sub2.example.jp
&sub3.example.jp::ns1.example.com
&sub3.example.jp::ns2.example.com
```

tinydnsデータファイルの記述例

- `.fqdn:ip:x[:ttl]`
  - fqdnドメインのネームサーバ
  - NS、SOA、(必要なら)Aレコードを生成
- `@fqdn:ip:x[:dist:ttl]`
  - fqdnドメインのMXの指定
  - MX、(必要なら)Aレコードを生成
- `=fqdn:ip[:ttl]`
  - fqdnホストの指定(正引き、逆引き両方)
  - A、PTRレコードを生成
- `+fqdn:ip[:ttl]`
  - fqdnホストの指定(正引きのみ)
  - Aレコードを生成(www.fqdnやftp.fqdnの指定に使う)
- `&fqdn:ip:x[:ttl]`
  - サブドメインfqdnの指定
  - NS、(必要なら)Aレコードを生成
- `#comment`
  - コメント行

BINDとの比較(運用管理面)

- **サーバ間のデータの同期**
  - **ゾーン転送ではなく**ssh+rsync**で行うことが推奨されている**
  - BIND**流のゾーン転送で行う仕組みも提供されているが、推奨されていない**
- **データファイルは**1**行単位で構成**
  - SOA**のシリアルの上げ忘れ、ドットの付け忘れ、逆引きレコードの書き忘れ等の事故が未然に防止されている**

BINDとの比較 (機能ごとに分割されたサーバ)

- DNSデータ管理サーバとDNSキャッシュサーバの分離
  - 本来別の機能であるものはそれぞれ別のサーバで実現すべき、というDJBの設計思想を反映
  - ifconfig alias(相当)の機能を使用すれば、1台のホストで双方の機能を実現可能
- 上記を同一IPアドレスで兼用している環境から移行する場合、これを分離する必要がある
  - BIND環境でもキャッシュ等によるトラブルを防ぐため、本来分離すべき

djbdnsにおけるIPv6サポート

- オリジナルのdjbdnsでもIPv6 AAAAレコードを保持、管理すること自体は可能
  - ただしAAAAレコードの記述は若干面倒
- IPv6対応patchがhttp://www.fefe.de/dns/で公開されている
  - IPv6 AAAAレコードの取り扱いの向上
  - 周辺ツールのIPv6 AAAAレコードの取り扱いの向上
- 最近上記URLにてIPv6データリンクのサポートのテストパッチも公開されはじめた
- A6, DNAMEはdjbdnsではサポートされていない
  - DJBは「サポートしない」と自身のWebページで明言
  - 理由はDJBのページに書かれている

有用なサイト、リンク

- DJBのページ(オリジナル)
  - http://cr.yp.to/djbdns/
  - まずはここをきちんと読むとよい
- 東工大の前野氏のページ(日本語)
  - http://djbdns.jp.qmail.org/djbdns/
  - DJBのページの和訳をはじめとする有用な情報あり
- Life with djbdns
  - http://www.lifewithdjbdns.org/
  - Henning Brauer氏のページ、djbdnsを使うにあたり有用な情報あり
- djbdns home page
  - http://www.djbdns.org/
  - Russell Nelson氏のdjbdns home page
- FAQTs にあるdjbdnsのFAQ
  - http://djbdns.faqts.com/