DNSSECツールの状況

IIJ 山口崇徳

アジェンダ

- DNSサーバ
- DNSSEC運用管理ツール
- ちょっと便利な小物ツール

- オープンソースのみ
- ソフトウェアのバージョンその他の状況は4月25日現在のもの

DNSサーバ

BIND 9.7

- 最新は9.7.5
- DNSSECを運用するのであれば9.7以降を
  - いちおう9.6.2以降なら何とかならなくもないですが…
- スマート署名
  - 所定の場所に鍵を放り込んでおくと、署名時に日付情報を見て適切に取り込んでくれる
- 全自動ゾーン署名
  - 加えて再署名も適切なタイミングで自動でおこなう
- 詳細はぐぐってください
  - 話すと長くなるので…:-)

BIND 9.8

- 最新は9.8.2
- DNSSECに関していえば9.7系とほとんど変わらず
  - GOSTアルゴリズム(RFC5933) 対応
  - ルートのトラストアンカーが内蔵された
  - …ぐらい
- DNSSEC以外ではRPZなどいろいろ

BIND 9.9 (1)

- 最新は9.9.0
- インライン署名
  - 9.7からの全自動ゾーン署名は、元ゾーンファイルにnamedが署名を追加して上書きしてしまう
    - ゾーンの履歴管理がめんどくさい
    - 署名レコードが邪魔でゾーンファイルが見づらい
  - 元のゾーンファイルはいじらず、署名済みゾーンを別ファイルに出力できるようになった
    - DNSSECを気にせずにゾーンファイルを編集できる
  - 例: https://deepthought.isc.org/article/AA-00626

BIND 9.9 (2)

- dnssec-signzone
  - 署名レコードだけを出力したり、不要になった署名を削除できるようになったり
- dig
  - デフォルトが dig +adflag +edns=0 に
  - dig +rrcomments
    - DNSKEYレコードに鍵ID、アルゴリズム、KSK/ZSKを表示

NSD

- NLNet Labsによる権威DNS
- 最新版は3.2.10
  - ここ最近はDNSSECまわりの新機能はない
- 次リリースでECDSA(RFC6605)、DANE(draft-ietf-dane-protocol)をサポートするらしい?
- 大きなサイズの応答でauthority sectionやadditional sectionを付加しなくなった(3.2.9)
  - DNSSECのような大きな応答がtruncateされにくくなる
  - BINDのminimal-responses yes;は常にauthority/additional sectionを削るが、NSDではパケットが一定サイズを越える場合のみauth/addが削られる

Unbound

- NLNet LabsによるキャッシュDNS
- 最新版は1.4.16
  - ここ最近はDNSSECまわりの新機能はない
- 1.4.17でECDSA(RFC6605)対応予定
  - DNSSEC以外では待望のラウンドロビン機能も！
- DNS over SSL (1.4.14)
  - DNSSECと直接関係はないですが、「毒入れを防いで正しい名前解決」という意味ではアリかも
  - まあ、対応してる権威DNSが存在しないんですけどね
  - unboundからunboundに対してforwardするときに使える程度か

PowerDNS

- バックエンドにRDBMSなどを使える権威DNS
- 3.0 (2011/6)からDNSSECをサポート
  - ただしDoS穴あり(CVE-2012-0206)
  - 最新版の3.0.1を使いましょう
- DNSSEC対応からわずか半年後の今年1月の時点で、.seの全署名済みドメインの97%がPowerDNS
  - 未署名ドメインまで含めると.seの10%、実数では16.5万
  - http://mailman.powerdns.com/pipermail/pdns-users/2012-January/008439.html
- 姉妹品のPowerDNS Recursor(キャッシュDNS)はいまだDNSSEC非対応

新顔

- Knot DNS
  - http://www.knot-dns.cz/
  - CZ NIC (チェコ)によるDNSSEC対応権威DNS
  - 今年2/29に1.0.0が出たばかり / 最新は1.0.3
  - DNS実装の多様性の欠如に危機感を抱いたのが開発の動機らしい
- YADIFA
  - http://www.yadifa.eu/
  - EURid (.euのレジストリ)によるDNSSEC対応権威DNS
  - 現在1.0.0RC2
  - BINDやNSDよりもパフォーマンスがいいらしい

DNSSEC運用管理ツール

OpenDNSSEC

- DNSSEC運用管理ツール
  - 鍵・署名管理の自動化
- HSM(hardware security module)の使用が前提
  - 堅牢な鍵管理
  - SoftHSM(ソフトウェア実装したHSM)も提供
- 最新版1.3.7
  - 細かい修正はあるものの、ここ最近目立った新機能はない模様
  - 2012Q3のバージョン2.0ではパフォーマンス改善やアルゴリズムロールオーバーなどが予定されている

DNSSEC-Tools

- http://www.dnssec-tools.org/
- DNSSECの運用全般に役立つツール群
  - 権威DNS: 鍵の管理、署名、ロールオーバーなど
  - キャッシュDNS: トラストアンカー自動更新など
  - その他: 各種エラーチェック、統計ツール、監視プラグイン(Nagios、Zabbix)、DNSSEC対応アプリ開発用ライブラリなど
- 1.12.1が最新
- 単体で使えるツールが多いので、すべてをこれに任せるのではなく、一部だけに利用することも可能

AtomiaDNS

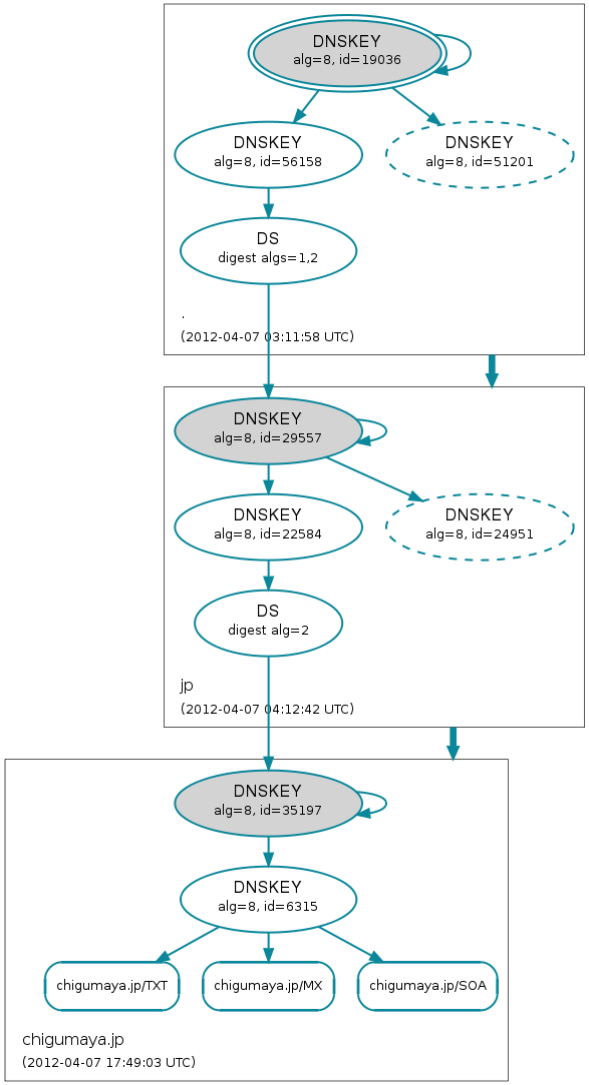
- http://atomiadns.com/
- 大規模ホスティング向けDNS管理システム
  - DNS管理が主で、DNSSECはその中の1機能
  - SOAPインターフェースによるプログラミングAPI
- 主にPowerDNS用
  - BINDも使えるが no longer recommend だそうな
- 開発元のAtomia社はスウェーデン、セルビアを拠点とする大手ホスティングプロバイダ
  - .seでPowerDNSが使われまくってるのはだいたいこいつのせい

ちょっと便利な小物ツール

…というか、署名済みゾーンの検証ツール

DNSViz

- http://dnsviz.net/
- DNSSECの信頼の連鎖を可視化してくれるWebサービス
  - うまく動いているかの確認に便利
- が、ここでDNSSEC検証に失敗と判定されてるときはすでに手遅れ
  - キャッシュの状態にもよりますが、validationしている世界中のサイトからあなたのドメインが見えません
  - ゾーンに署名した後すぐに公開するのではなく、それが問題ないことをテストしてから公開するフローにしましょう



署名済みゾーンの検証

- ロールオーバー手順が間違っていたり、間違った引数で署名コマンドを実行すると署名の検証に失敗する
  - 間違ってないのにツールのバグを踏んでトラブルになったTLDの事例もあり
- 署名したらまず検証して、問題ないことを確認してから公開するのが重要
- dnssec-signzone -a
  - 生成した署名を検証してくれる
  - でも、署名と検証で同じコードを共有しているプログラムの検証結果を信頼していいのかどうか？
- ということで、いろいろツールを調査しました

YAZVS

(Yet Another Zone Validation Script)

- http://yazvs.verisignlabs.com/
- Verisign Labsによるゾーン検証スクリプト
- 実際にルートとarpaゾーンは署名後このスクリプトを使って検証されてから公開されているらしい
- KSKと上位ゾーンに登録されたDSが正しく対応しているかの確認も可能
- 現在公開されているゾーンとこれから公開しようとする新ゾーンの差分をチェックできる

ldns-verify-zone

- http://www.nlnetlabs.nl/projects/ldns/
- NSDやUnboundの開発元NLNet Labs製のDNSライブラリldnsにサンプルプログラムとして含まれるツール
  - サンプルプログラムだけどちゃんと使える
  - これ以外にも鍵作成、署名など、DNSSEC運用に必要なツールはひととおり含まれている
- DNSKEYとRRSIGの対応は正しいか、NSEC(3)が適切か
- ldns-1.6.13で機能がかなり強化されるらしい(もうすぐリリースされる?)

validns

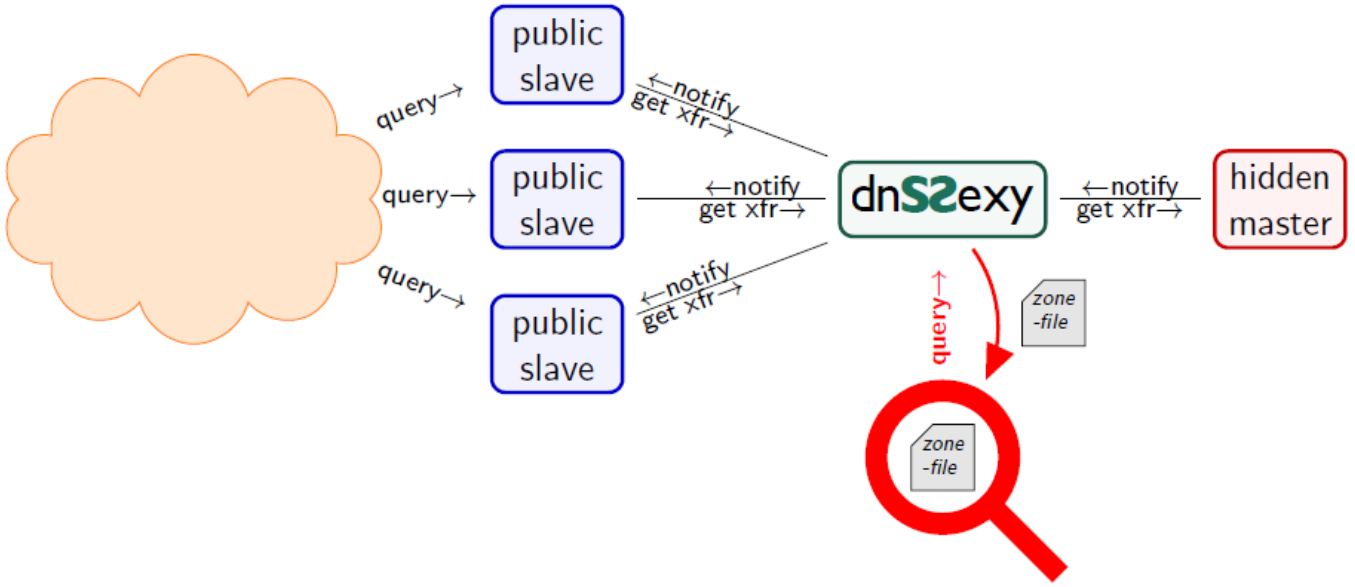
- http://www.validns.net/
- 最新版は0.4
  - 絶賛開発中
  - まだまだバグも多いが、レポートするとあっというまに修正してくれる
- DNSSEC署名済みゾーンだけでなく、未署名ゾーンの検査も可能
  - named-checkzoneにDNSSEC検証機能がついたツールと考えるとよい

donuts

- 前述のDNSSEC-Toolsに含まれる検証ツール
  - これ単体での利用が可能
  - https://www.dnssec-tools.org/wiki/index.php/Donuts
- プラグイン方式になっていて、どんなルールを用いて検証するかを自由に選択できる
  - 大半はDNSSEC関連のルールだが、DNSSEC以外の検証項目もあり
  - ルールの自作も可能(perl)
- GUIあり
- donutsd: donutsをデーモン化して定期実行

DNSSexy

- DNSSEc proXY
- 署名済みゾーンをmasterサーバから受け取り、検証できたものだけをslaveサーバに転送
- NLNet LabsがNSDをベースに現在開発進行中
  - まだサイトはなさげ; dnssexy.net は無関係



まとめ

- DNSSECの運用はめんどくさいものですが…
  - とくに権威DNS
- 運用を助けてくれる便利なツールもだいぶ充実してきました
- うまく使いこなして手間を省きながら事故のないDNSSEC運用を