

# Unboundの紹介

日本Unboundユーザ会 滝澤隆史

2011-03-04

日本Unboundユーザ会 OSC 2011 Tokyo/Spring発表資料

# 日本Unboundユ-ザ会の紹介

# 日本Unboundユーザ会

- 何となくノリで作った
- なぜか公式 (NLnet Labs) 公認
- ユーザ会と名乗っている割にはコミュニティとして体をなしていない
- ときどき協力してくださる方がいるので助かっている
- Googleグループに議論や連絡の場所を作った。
  - <http://groups.google.com/group/unbound-jp>

# ユーザ会の主な活動

- ウェブサイトの公開
  - <http://unbound.jp/>
- マニュアル等の翻訳
- Unboundだけでなく、IdnsとNSDについてもマニュアルを翻訳して公開している
- 技術検証はほとんどできていない

# Unboundとは

# BINDの代替を目指したキャッシュサーバ

- 設定の容易さ
- フルスペックのキャッシュサーバ
- 機能を限定した権威サーバ
- キャッシュ汚染への高い耐性
- 高い処理性能
- リモート制御ツール
- DNSSEC対応

## NLnet Labsが開発・保守

- Verisign labs, Nominet, Kirei, EP.netがプロトタイプをJavaで開発した
- NLnet LabsがCで実装し直した
- NLnet Labsはレートサーバでも利用されている権威DNSサーバのNSDの開発元でもある
- BSDライセンス

# 動作環境

- UNIX系OS (Linux, \*BSD, MacOS X, Solaris)
- Windows

# 動作環境/依存ライブラリ

- 依存するライブラリ
  - OpenSSL
    - GOSTに対応していない場合 (0.9.8以前) はunboundのconfigure時に--disable-gostを付ける必要がある。
  - libexpat
    - Unbound 1.4.7以降で必要となる
  - Idns
    - unboundのビルド時に同梱のIdnsを組み込むこともできる

# 動作環境/パッケージ (Linux系)

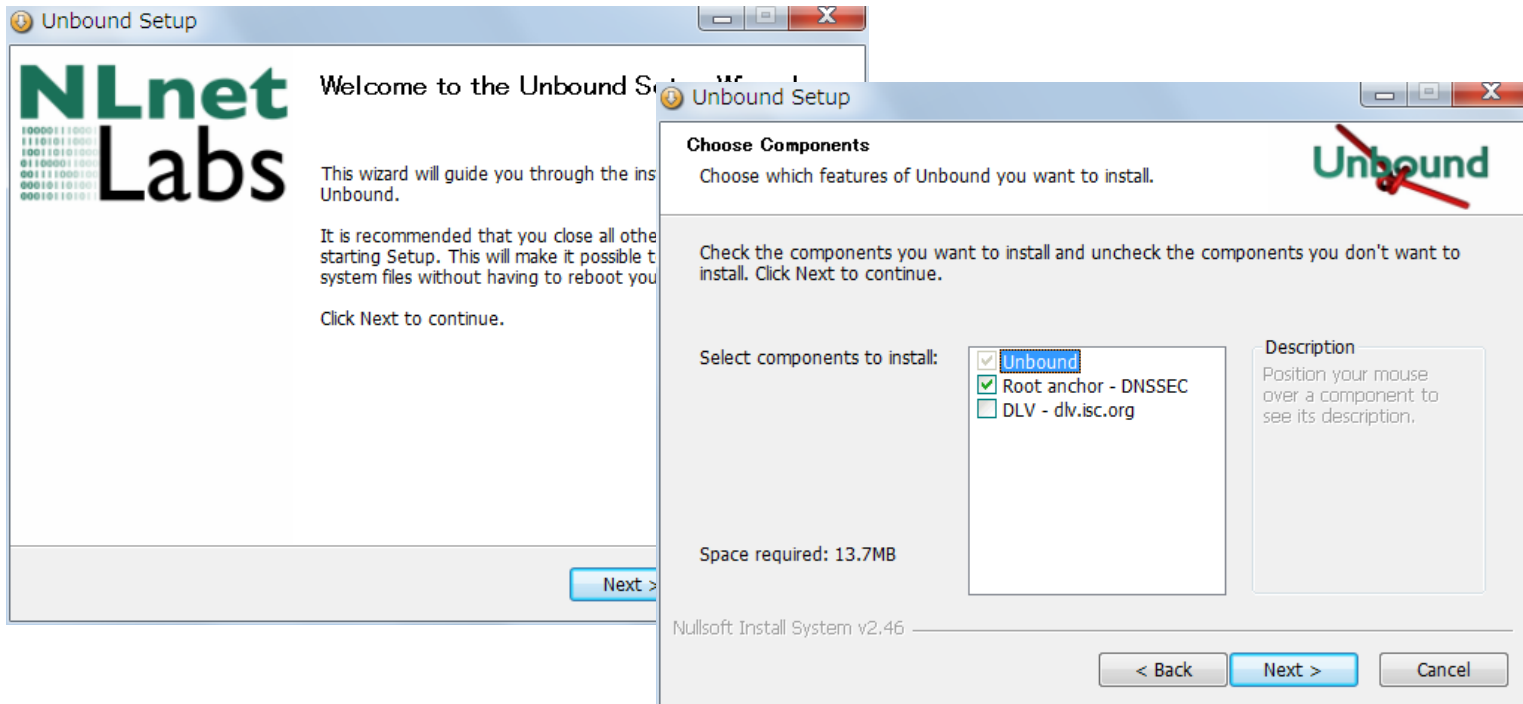
Linuxディストロ	Unbound	Idns	備考
Debian GNU/Linux squeeze	1.4.6	1.6.6	
Debian GNU/Linux wheezy	1.4.8	1.6.9	
Ubuntu 10.04 LTS	1.4.1	1.6.1	
Ubuntu 10.10	1.4.5	1.6.4	
Fedora 14	1.4.5 (1.4.8)	1.6.6 (1.6.8)	括弧内はupdates
RHEL 5/CentOS 5	(1.4.4)	(1.6.4)	標準パッケージなし。 Fedora EPEL 5より
RHEL 6	(1.4.4)	(1.6.4)	標準パッケージなし。 Fedora EPEL 6より
openSUSE 11.3	-	1.5.1	パッケージなし
Momonga Linux 7	1.4.6	1.6.5	
Gentoo Linux	1.4.3 (1.4.9)	1.6.4 (1.6.9)	括弧内はunstable

# 動作環境/パッケージ (BSD系)

OS	Unbound	Idns	備考
FreeBSD	1.4.9	1.6.9	Ports
NetBSD	1.4.9	1.6.9	Packages Collection
OpenBSD	1.4.9	1.6.9	Ports
Mac OS X (MacPorts)	1.4.9	1.6.8	MacPorts

# 動作環境/Windows

- 公式サイトにWindows版が公開されている
- インストーラー付き



## 動作環境/Windows

- インストール後に参照する「DNSサーバー」を「127.0.0.1」に変更するだけ
- ルートのトランスアンカーが自動で取得され、DNSSECの検証が有効になる。

# バージョンの履歴

- 1.0.0 (2008年05月)
  - 正式リリース
- 1.1.0 (2008年11月)
  - DLV対応
- 1.2.0 (2009年1月)
  - unbound-controlコマンド
- 1.3.0 (2009年6月)
  - Windows版、Python対応

# バージョンの履歴

- 1.4.0 (2009年11月)
  - トラストアンカーの自動更新機能
  - RSASHA256とRSASHA512サポート  
(デフォルト有効)
- 1.4.7 (2010年11月)
  - unbound-anchorコマンド  
(ルートゾーンのDNSKEYの取得)
- 1.4.9 (2011年3月)
  - 最新版

# 利用すべきバージョン

- 少なくとも1.4.0以降を利用すべき
  - トラストアンカーの自動更新
  - RSASHA256とRSASHA512のサポート
- 1.4.7以降を推奨
  - unbound-anchorコマンドが新規導入には便利

# 設定の容易さ

# 設定ファイル

- 設定ファイルは一つ
  - unbound.conf
- 形式
  - パラメータ名: 設定値
- 設定例
  - server:
    - verbosity: 1
    - interface: 0.0.0.0
    - access-control: 192.0.2.0/24 allow

# ゾーンファイルの記述不要

- ループバックアドレスに対する正引きおよび逆引きのゾーンなどのお決まりのゾーン
  - 組み込まれている
  - BINDのようにゾーンファイルを用意する必要はない

# ホスト自身のリゾルバ

- デフォルトの設定で動作可能
  - ローカルホストにバインド
  - アクセス制御はローカルホストのみ許可

# 他のホストに対するフルリゾルバ

- "interface"でバインドするインターフェイスの指定
- "access-control"でアクセス制御を指定
- 設定例
  - server:
    - interface: 0.0.0.0 ←バインドするインターフェイス(IPv4)
    - interface: ::0 ←バインドするインターフェイス(IPv6)
    - access-control: 192.0.2.0/24 allow ←アクセス制御
    - access-control: 2001:DB8:BEEF::/48 allow ←アクセス制御

# フルスペックのキャッシュサーバ

# フルスペックのキャッシュサーバ

- 再帰問い合わせ
- キャッシュ
- DNSSECの検証
  - 別資料「UnboundとDNSSEC」参照
- スタブ
- フォワード

# スタブ

- 指定したゾーンに対して指定した権威サーバへ問い合わせを行う
- "stub-zone"を設定する
- 設定例
  - stub-zone:

```
name: "example.org"  
stub-addr: 192.0.2.1
```
  - stub-zone:

```
name: "2.0.192.in-addr.arpa"  
stub-addr: 192.0.2.1
```

# フォワード

- 指定したゾーンに対して指定したキャッシュサーバへ再帰問い合わせを行う
- "forward-zone"を設定する
- 設定例
  - forward-zone:  
name: "example.com"  
forward-addr: 192.0.2.68  
forward-addr: 192.0.2.73@5355

# 制限事項

- DNSラウンドロビン非対応
  - キャッシュした内容をそのままの順番で回答する

# 機能を限定した権威サーバ

# 限定的な機能の権威サーバ

- フル実装は目指していない
- 別の権威サーバに問い合わせるまでもないリソースレコードについて回答する



# 不要な逆引きの問い合わせへの回答

- 不要な逆引きの問い合わせにはNXDOMAINを返す（AS112的な対応）
  - プライベート
  - リンクローカル
  - テストネット
  - ブロードキャスト
  - 例示

# リソースレコードの登録

- local-data
  - リソースレコードを登録できる
    - local-data: 'a.example.jp. IN A 192.0.2.1'
    - local-data: '1.2.0.192.in-addr.arpa. IN PTR a.example.jp.'
- local-data-ptr
  - PTRの簡略記法
    - local-data-ptr: '192.0.2.1 a.example.jp.'
- local-data, local-data-ptrはLAN内のホストの名前解決用に利用すると便利

# プライベートアドレスの注意事項

- forward-zoneやstub-zoneでプライベートアドレスの逆引き用にキャッシュサーバや権威サーバを指定する場合
  - stub-zone:  
name: "0.168.192.in-addr.arpa"  
stub-addr: 192.0.2.1
- このときAS112対策でNXDOMAINが返される
  - 対策としてlocal-zoneでtransparentを指定
  - local-zone: "0.168.192.in-addr.arpa." transparent

# キヤツシユ汚染への高い耐性

"Unbound 1.0.2 Patch Announcement"のまとめ

[http://unbound.net/documentation/patch\\_announce102.html](http://unbound.net/documentation/patch_announce102.html)

# オープンリゾルバにならないための アクセス制御

- デフォルトではlocalhostからのみアクセス可能
- 必要に応じてアクセスを許可
  - interface: 0.0.0.0
  - access-control: 192.0.2.0/24 allow

# キャッシュ汚染への高い耐性

- 回答に対するサニタイジング
- 暗号学的に強いランダム性を持つクエリーIDの利用
- 暗号学的に強いランダム性を持つソースポート番号の利用
- ランダムなデスティネーションIPアドレスの利用
- ランダムなソースIPアドレスの利用
- dns-0x20 (クエリーの際に大文字・小文字をランダムに混ぜる)

# デフォルトのランダム性

クエリーID	16 ビット
ポート番号	16 ビット
デスティネーションIPアドレス (平均)	2 ビット
<b>ランダム性の合計</b>	<b>34 ビット</b>

# さらに工夫した場合のランダム性

クエリーID	16ビット
ポート番号	16ビット
デスティネーションIPアドレス (平均)	2ビット
ソースIPアドレス (平均)	2ビット
dns-0x20 (平均)	8ビット
<b>ランダム性の合計</b>	<b>44ビット</b>

# 攻撃に対する耐性

ビット	50%機会	5%機会	
16	10秒	1秒	ランダムなクエリーIDのみ
26	2.8時間	17分	ランダムなクエリーIDとソースポートのランダムな範囲1024ポート
34	28日	2.8日	Unboundデフォルト
44	28444日	2844.4日	Unbound (dns-0x20とソースアドレス)

# 高い処理性能

## 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
- BINDの2～3倍のキャッシュ処理性能

## Alternative DNS Servers: the book as PDF

- Jan-Piet Mens著" Alternative DNS Servers "
  - <http://blog.fupps.com/2010/10/29/alternative-dns-servers-the-book-as-pdf/>

	MaraDNS	BIND	dnscache	PowerDNS Recursor	Unbound
Queries /sec	13,846	16,066	14,957	10,796	25,072
Queries /sec (LAN)	13,308	26,656	13,114	21,218	30,569
Queries /sec (10 clients)	3,068	3,003	2,928	2,074	8,276
RSS size	1,336	40,916	1,712	14,336	16,828
VSZ size	168,408	195,380	6,044	26,500	180,648

# リモート制御ツール

# unbound-control

- リモート制御ツール
- BINDのrndcのようなもの

# Unboundへの接続

- ポート番号はTCP953
- サーバにはSSL/TLS経由で接続
  - 秘密鍵や証明書が必要
  - 秘密鍵と自己署名証明書を作成する  
unbound-control-setupというスクリプトあり

# 主な機能

- 起動、停止、リロード、状態の出力
- 饒舌さ (verbosity) の変更
- 統計情報の出力
- ローカルゾーンの操作 (追加、削除)
- ローカルデータの操作 (追加、削除)
- キャッシュのダンプ、ロード、削除
- 設定オプションの設定および取得
- 利用中のスタブゾーン、フォワードゾーン、ローカルゾーン、ローカルデータの一覧の出力

# DNSSEC

# DNSSEC

- 別資料「UnboundとDNSSEC」を参照

# 終わり