日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

Unboundの紹介

日本Unboundユーザ会
株式会社サードウェア
滝澤 隆史

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

Unbound とは

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDの代替を目指したDNSキャッシュサーバ

BSDライセンス

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

Verisign labs，Nominet，Kirei，EP.netによってプロトタイプをJavaで開発した

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

NLnet Labsが
Cで実装し直した

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

NLnet Labsが開発・保守

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDの代替？

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDが圧倒的なシェアを持っている

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDに深刻な問題があるとインターネット全体の問題になる

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

Dan Kaminsky氏の新しい攻撃方法

多様性が必要

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSコンテンツサーバではNSDがあるよね

（NSDはルートサーバH，K，L）

では、BINDを置き換えられる機能を持ったDNSキャッシュサーバは？

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

フルスペックの
オープンソースの
DNSキャッシュサーバは
BIND以外は無いよね

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

そこで
2008年5月20日
Unbound登場！

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSSEC対応、IPv6対応のフルスペックのDNSキャッシュサーバ

バージョン

2008-05-20 1.0.0 最初のバージョン
2008-06-16 1.0.1 バグ修正
2008-08-07 1.0.2 バグ修正
2008-11-18 1.1.0 DLVサポート、他
2008-11-20 1.1.1 バグ修正

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

Unboundの特徴

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

- フルスペックのDNSキャッシュサーバ
- 限定的なDNSコンテンツサーバ
- DNSSEC対応
- DNSキャッシュ汚染に対する高い耐性
- 高い処理性能、スケーラブル
- IPv4/IPv6デュアルスタック
- 設定の容易さ

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

フルスペックのDNSキャッシュサーバ

- 再帰クエリー
- キャッシュ
- スタブ
- フォワード

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

stub-zone

特定のゾーンに対するDNSコンテンツサーバへのクエリ

stub-zoneの設定例

```
stub-zone:
  name: "example.org"
  stub-addr: 192.168.0.8
stub-zone:
  name: "0.168.192.in-addr.arpa"
  stub-addr: 192.168.0.8
```

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

forward-zone

特定のゾーンに対する DNSキャッシュサーバへの 再帰クエリー

forward-zoneの設定例

```
forward-zone:
        name: "example.com"
        forward-addr: 192.0.2.68
        forward-addr: 192.0.2.73@5355
```

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSラウンドロビンに非対応

Unboundは
キャッシュした内容を
そのままの順番で返す

DNSラウンドロビンを運用しているサイトではTTLを短めに設定している。

影響はそれほど無い？

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

限定的なDNSコンテンツサーバ

（フル実装は目指していない）

ループバックアドレス
localhost
127.0.0.1
::1
名前解決は暗黙で設定

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

ループバックアドレスの正引きと逆引きのゾーンファイルを書く必要はない

localhost
127.in-addr.arpa.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.ip6.arpa.

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

192.168.0.0/16などのプライベートアドレスやリンクローカルアドレスの逆引きのクエリーは迷惑（AS112）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

unboundは
プライベートアドレスなどの
不要な逆引きの
問い合わせを行わない
（NXDOMAINを返す）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

デフォルトの設定で安全に運用できる

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

local-data
権威を持ったレコードを登録可能
（LAN内のホスト登録）

local-dataの設定例

```
local-zone: "example.org." static
local-data: "www.example.org.  3600 IN A 192.168.0.1"
local-data-ptr: "192.168.0.1  3600 www.example.org."
```

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSSEC対応

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSSECの署名の検証をサポート

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DLV対応 (DNSSEC Lookaside Validation) （バージョン1.1.0から）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSキャッシュ汚染対策の本命はDNSSECですよね

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSSECは実用レベルなの？

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSSEC抜きでのDNSキャッシュ汚染対策が必要

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSキャッシュ汚染に対する高い耐性

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

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
アクセスを許可する

```
interface: 0.0.0.0
access-control: 192.168.0.0/24 allow
```

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

オープンリゾルバにはならない

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

クエリーの回答に対するサニタイジング

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

暗号学的に強いランダム性を持つクエリーIDの利用

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

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

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

ランダムな
デスティネーション
IPアドレスの利用

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

ランダムな
ソースIPアドレスの
利用

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

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

16 bits ID
16 bits port
  2 bits destination address (平均).

34ビットのランダム性

いろいろ工夫すると

16 bits ID
16 bits port
  2 bits destination address (平均)
  2 bits source address (平均)
  8 bits capitalisation (平均)

44ビットのランダム性

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（パッチなしBIND9）
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の範囲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）

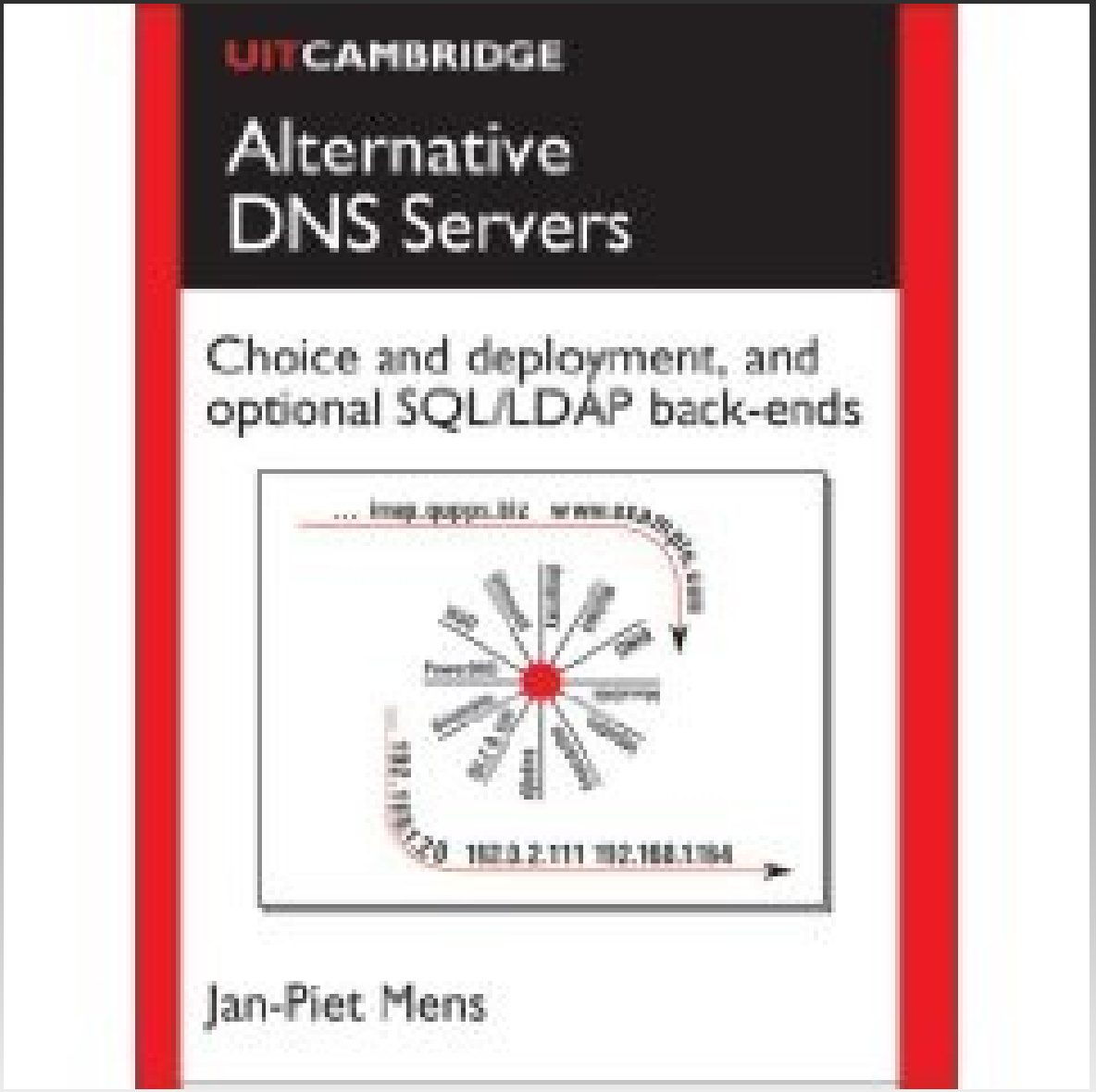
日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

高い処理性能

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

12月発売予定 "Alternative DNS Servers”の著者Jan-Piet Mens

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料



Unboundのプレスリリースにて
“It is great code, very versatile, and it is the fastest caching server we tested."
「優れたコードで、多目的に使える。私たちが試験をした中で最も速いキャッシュサーバだ」

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

スケーラブル

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

マルチスレッド対応
（今どき珍しくもないが）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

チューニング
パラメータ多数

メモリ削減のチューニング例 unbound.conf(5)

```
server:
        num-threads: 1
        outgoing-num-tcp: 1     # TCPサービスを制限し、バッファを少なくします。
         incoming-num-tcp: 1
        outgoing-range: 16      # メモリを減らします。しかし、性能も落ちます。
         msg-buffer-size: 8192   # サービスを制限します。
         msg-cache-size: 100k
        msg-cache-slabs: 1
        rrset-cache-size: 100k
        rrset-cache-slabs: 1
        infra-cache-numhosts: 200
        infra-cache-slabs: 1
        infra-cache-lame-size: 1k
        key-cache-size: 100k
        key-cache-slabs: 1
        neg-cache-size: 10k
        num-queries-per-thread: 30
        target-fetch-policy: "2 1 0 0 0 0"
        harden-large-queries: "yes"
        harden-short-bufsize: "yes"
```

メモリの最適化の方法

http://unbound.net/documentation/howto_optimise.html

```
# some optimisation options.
server:
        # use all CPUs
        num-threads: <number of cores>
        # power of 2 close to num-threads
        msg-cache-slabs: <same>
        rrset-cache-slabs: <same>
        infra-cache-slabs: <same>
        key-cache-slabs: <same>
        # more cache memory, rrset=msg*2
        rrset-cache-size: 100m
        msg-cache-size: 50m
        # more outgoing connections
        # depends on number of cores: 1024/cores - 50
        outgoing-range: 950
```

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

libeventを使うと同時処理クエリー数を増やすことができる

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

IPv4/IPv6 デュアルスタック

IPv6対応

- IPv6トランスポート
- IPv6リソースレコード
（AAAA, DNAMEなど）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

設定ファイルでIPv4/IPv6の利用の有無を設定可能


```
server:
    do-ip4: yes
    do-ip6: yes
```

設定の容易さ

設定ファイルは一つ
unbound.conf

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

設定ファイルの形式
パラメータ名: 設定値

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDのように
セミコロン“;”を付け忘れたり
{}の対応を間違えたりして
怒られることはない

最小限の設定（これだけで動く）

```
server:
        interface: 0.0.0.0
        access-control: 192.168.0.0/24 allow
        do-ip6: no
```

←IPv6トランスポートが出来ないとき

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

BINDより設定が簡単

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

リモート制御ツール
（BINDのrndcのようなツール）

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

unbound-control
（バージョン1.1.0から）

サーバには
SSL/TLS経由で接続
(秘密鍵や証明書が必要)
ポート番号はTCP953

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

- 起動・停止・リロード
- 統計情報の出力
- 饒舌さ（verbosity）の変更

- キャッシュのダンプ
- キャッシュのロード
- キャッシュのフラッシュ
- ローカルゾーンの操作
- ローカルデータの操作

まとめ

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

DNSキャッシュサーバとしてBINDを置き換えられる機能や性能を持っている

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

気になるのは
DNSラウンドロビン
非対応くらいかな。

日本Unboundユーザ会
Internet Week 2008 DNSOPS BoF 発表資料

デフォルトが安全側に倒れているため、簡単な設定で安心して利用できる

おわり