権威DNSサーバ 脱自前運用のススメ

IIJ
Internet Initiative Japan

株式会社　インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

disclaimer

- 私の立ち位置について
  - IIJの人間です
  - 「DNSは趣味です」と、普段言っていますが
    - IIJではDNSサービスを販売しています。
    - 多少はDNSサービスに関わっています
  - IIJのサービスを特別扱いはしていないつもりですが、サービス提供者側であるということはお伝えしておきます。

今日、お話を聞いてもらい方

- 公開権威DNSサーバを運用管理していて、
  - 疲れている方
  - 困りごと・悩み事を抱えている方
  - もっと他のことに時間を使いたい方

過去の発表

- DNS Summer day 2016
  - BINDからの卒業
- DNS Summer day 2017
  - BIND卒業できました？

DNSサーバソフトのダイバシティを奨めてきていました。今年はもう一歩進んで。

権威DNSサーバーの運用、楽したくありませんか？

権威DNSサーバの自前運用、大変じゃないですか？

- BIND祭
- ソフトウェアダイバーシティの確保
  - 複数実装のドキュメント整備、教育、運用 etc…
- ネットワーク冗長性の確保
  - ラック、DC、国内、国外、AS、NSのTLDの分散…
- 水責め攻撃への対策
  - 日本では権威DNSは狙われていない？
- DDoS攻撃への対策
  - Janog39 Dynへの攻撃の顛末

Internet Initiative Japan Inc.

何が起こったか？

Dynの権威DNSサーバに対する、(超)大規模なDDoS攻撃 (1.2Tbps)

世界中の著名サイトが6時間ほどダウン

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- FiveThirtyEight[14]
- Fox News[20]
- *The Guardian*[20]
- GitHub[12][17]
- Grubhub[21]
- HBO[14]
- Heroku[22]
- HostGator[14]
- iHeartRadio[13][23]
- Imgur[24]
- Indiegogo[13]
- Mashable[25]
- National Hockey League[14]
- Netflix[14][20]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[26]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[22]
- Seamless[24]
- *Second Life*[27]
- Shopify[12]
- Slack[24]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][23]
- Storify[16]
- Swedish Civil Contingencies Agency[28]
- Swedish Government[28]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[29]
- Vox Media[30]
- Walgreens[14]
- *The Wall Street Journal*[20]
- Wikia[13]
- *Wired*[16]
- Wix.com[31]
- WWE Network[32]
- Xbox Live[33]
- Yammer[24]
- Yelp[14]
- Zillow[14]

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack#Affected_services

100%のSLAを持つサービスは存在しない

Dyn Statement on 10/21/2016 DDoS Attack
- https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Global DNS outage hits Microsoft Azure customers
- http://www.zdnet.com/article/global-dns-outage-hits-microsoft-azure-customers/

AWS Route53 DNS Outage – Impacts Last Almost a Full Day
- https://mwork.io/2017/03/14/aws-route53-dns-outage-impacts-last-almost-a-full-day/

Internet Week 2017 DNSOPS.jp BoF

権威DNSサービスのダイバーシティ 高嶋さん

複数の権威DNSサービスの利用

候補

- オンプレ
- 外部DNSサービス
  - クラウド事業者のDNSサービス
  - 専業のDNSサービスプロバイダ
  - ISPのDNSサービス

Internet Week 2017 DNSOPS.jp BoF

権威DNSサービスのダイバーシティ 高嶋さん

権威DNSサーバの運用、アウトソースしませんか？

メリット

- 諸々の理由のサーバソフトversion upからの開放
  - 脆弱性対応
  - サーバーソフトEoL対応
  - 新RR type対応

  - 設備リプレース
  - OS EoL対応

メリット

- 運用・教育コストの削減 (サーバのお守り以外で)
  - ダイバシティーのために色々な種類のサーバソフトウェアのことを考えなくて良い
    - APIのあるサービスならwrapperを作成すれば、サービスが変わってもレコード編集の方法は何も変わらないで済む
      - もっとも、APIを作るのが面倒…という場合も多々

メリット

- DDoS対策
  - anycastしていたり、DDoS対策装置が入っていたり、uplink帯域が太かったり、Backboneが太かったり
    - サービス提供側も、お客さんが少ないとコストが重くのしかかるので、大規模なところでないと難しい
    - 大規模なところもいっぱいお客さんに契約してもらって、コストメリットを出したい

メリット

- DNSSEC対応
  - 面倒な鍵管理・ロールオーバーなどを代行
  - ただし、複数サービスの併用では難しい
    - サービス間での鍵のやりとりが実質無理
    - プライマリで一括管理し、セカンダリサービスを利用する場合を除く
  - サービスを乗り換えるときに一旦DNSSECをOFFにする必要がある場合がほとんど
    - offし忘れて引っ越ししたらDNSSEC validation failに

そうは言っても…

- セキュリティーポリシー的にNG
  - これが一番大きい理由でしょうか
- 統計情報・クエリログが不十分/無い

過去に発生した問題

- 共用DNSサーバにおけるサブドメインハイジャックの脆弱性

  example.jpの権威DNSサーバにwww.example.jpを、別の契約者が契約できるとき、多くのサーバ実装でexample.jpにNSレコードを書かなくても権威が移譲されてしまい、ハイジャックが可能となる

  サービス運用上の問題に起因するドメイン名ハイジャックの危険性について

  https://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html

デメリット

- 直接的なキャッシュアウトが発生する
- 同じサービスに収容されている、他のお客さんへの攻撃の巻き添えを食らう場合がある

  ⇛ 複数サービスの組み合わせ
- 脆弱性対応ポリシーが不明・遅い場合がある

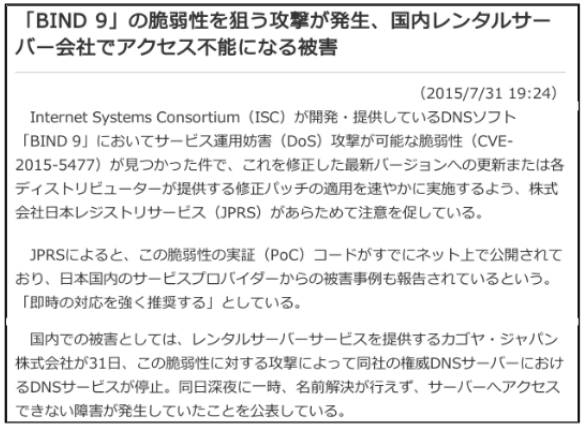
Internet Initiative Japan Inc.

実際の攻撃

- 攻撃ってそんなにすぐ来ないよね?(つぶらな瞳)

来 ま す

- CVE-2015-5477: Bind TKEY Query Assertion Failure



「BIND 9」の脆弱性を狙う攻撃が発生、国内レンタルサーバー会社でアクセス不能になる被害

(2015/7/31 19:24)

Internet Systems Consortium（ISC）が開発・提供しているDNSソフト「BIND 9」においてサービス運用妨害（DoS）攻撃が可能な脆弱性（CVE-2015-5477）が見つかった件で、これを修正した最新バージョンへの更新または各ディストリビューターが提供する修正パッチの適用を速やかに実施するよう、株式会社日本レジストリサービス（JPRS）があらためて注意を促している。

JPRSによると、この脆弱性の実証（PoC）コードがすでにネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されているという。「即時の対応を強く推奨する」としている。

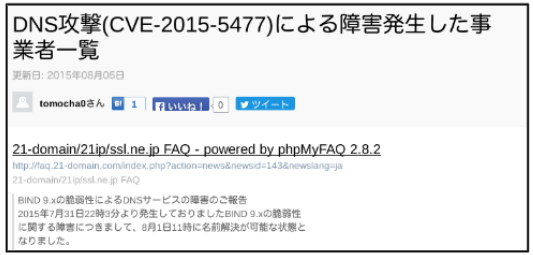
国内での被害としては、レンタルサーバーサービスを提供するカゴヤ・ジャパン株式会社が31日、この脆弱性に対する攻撃によって同社の権威DNSサーバーにおけるDNSサービスが停止。同日深夜に一時、名前解決が行えず、サーバーへアクセスできない障害が発生していたことを公表している。

http://internet.watch.impress.co.jp/docs/news/714526.html

dais
@hdais
Following

で、インドのNICの人がCVE-2015-5477 の攻撃に遭って助けを求めてる lists.isc.org/pipermail/bind …

View translation



DNS攻撃(CVE-2015-5477)による障害発生した事業者一覧

更新日: 2015年08月05日

tomocha0さん 1 いいね! 0 ツイート

21-domain/21ip/ssl.ne.jp FAQ - powered by phpMyFAQ 2.8.2

http://faq.21-domain.com/index.php?action=news&newsid=143&newslang=ja

21-domain/21ip/ssl.ne.jp FAQ

BIND 9.xの脆弱性によるDNSサービスの障害のご報告

2015年7月31日22時3分より発生しておりましたBIND 9.xの脆弱性に関する障害につきまして、8月1日11時に名前解決が可能な状態となりました。

2015/07/29早朝(日本時間)公開→ 7/29 AM11時「重複」→ 7/31障害

幸い、この時は7/28,29(現地時刻)にRHELのupdateがでている

デメリット

- 使いたいRR Typeを書けない場合がある
  - 最近ではなさそうだけど、AAAA書けないとか
- 新RR typeなどへの対応が遅い場合がある
  - BINDでCAAをサポートしたのは9.9.6(2014年9月)
  - Route 53 2017年8月、さくら 2017年9月、Azure 2017年11月、お名前.com, IIJ 2018年6月…
    - セカンダリサービスなら特に対応不要(なはず)

天秤

- ドキュメント・教育コストはサービスごとにかかるし、乗り換えたら再作成＆再教育が必要
  - APIで…
    - APIを作るのに工数かかるじゃん？
      - 自前プライマリ＋セカンダリサービス とか
- DDoS攻撃
  - うちのドメインにはこないよ
  - そんなにお金かけられるほどのドメインではないよ

求められそうな機能

- 普通の権威DNSサーバの機能は一通り
  - とはいえ先述の通り、RR typeの対応状況には差異がある。対応される予定のないRR typeも。
  - ワイルドカードが使えなかったりする場合も
- DNSSEC
  - 意外と対応していないサービスが多い
    - × Azure, Route 53, さくら
    - ○ Google, お名前.com, IIJ

求められそうな機能

- 権限分割、権限委譲
- 操作・変更履歴
- API
- 統計情報
- クエリログ

求められそうな機能

- 負荷分散関連
  - GSLB
  - 重み付きround robin
  - レイテンシベースルーティング
- zone APEXにCNAME(もどき)
  - ALIAS/ANAME

求められそうな機能

- セカンダリ関連機能
  - 他にゾーン転送をする (サービスがプライマリ)
  - 他からゾーン転送を受ける (〃　がセカンダリ)

アンケート結果

アンケートご協力ありがとうございます

m(_ _)m

- 回答人数: 95名
  - 昨年の「ご利用のサーバーはなんですか？」と比べて、約3倍

設問内容

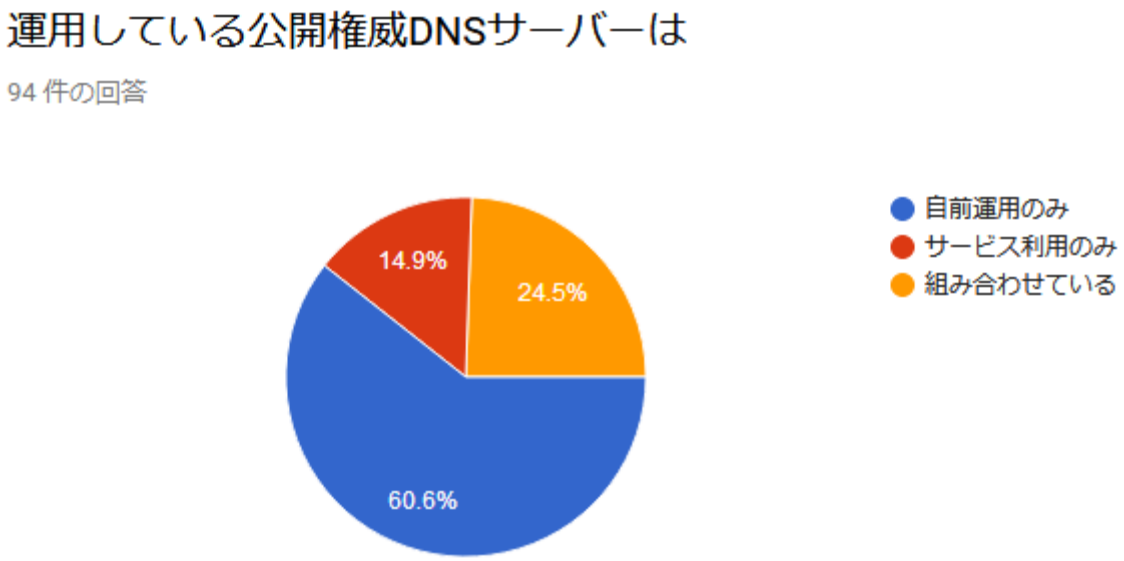
- 運用している公開権威DNSサーバーは？
  - 自前運用のみ/サービス利用のみ/組み合わせ

- 自前運用の人:
  - 自前運用のみの理由
  - サービスに望むこと
  - どのような課金体系が望ましいか

設問内容

- サービス利用のみ/組み合わせ の人:
  - サービスを利用している理由
  - 選定の際のポイント
  - サービスに望むこと
  - どのような課金体系が望ましいか

運用している公開権威DNSサーバーは



自前運用のみの理由 (複数回答)

- サービス提供者だから (30)
- 特に困っていない・必要性を感じない (24)
- 技術水準維持のため (17)
- 費用感が合わない (13)
- メンテナンスタイミングを好きにできる (12)
- 趣味 (11)
- トラブルシュートがしづらい (10)
- ゾーン情報の変更がしづらい (9)
- 統計情報・ログが不十分 (6)
- BINDの独自機能を使いたい (5)
- ゾーン追加の際のスピード感があわない (5)
- セキュリティーポリシー (4)
- 対応していないRR typeがある (2)
- セキュリティ対応が遅い (2)
- 検討したいけど人手が足りない・手が回っていない (3)

自前運用のみの理由 (複数回答) (cont.)

- 運用ツールをBINDに作り込んでしまっているから
- 機器更新時に移行先サービスを認識していなかった

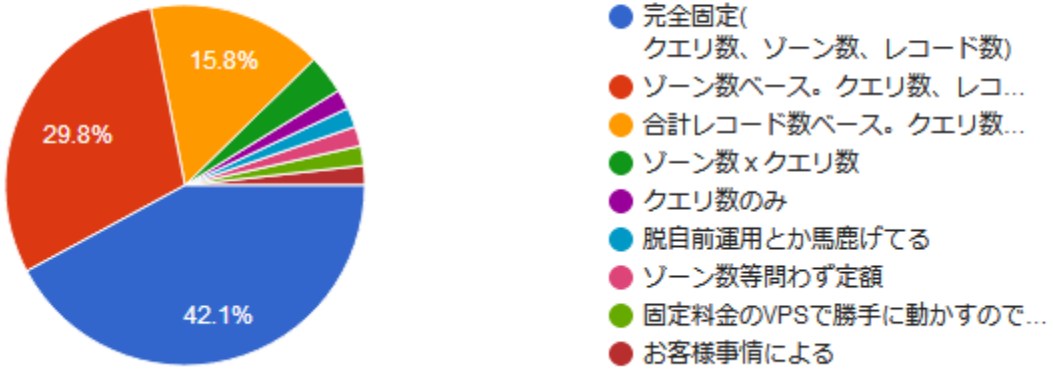
サービスに望むことは (自前運用) (複数回答)

- 素敵な統計情報 (23)
- クエリログ (22)
- 特になし (21)
- 定額課金 (20)
- SLA (16)
- UI/APIがメンテナンスで止まらない (15)
- 専有権威DNSサーバ(11)
- 費用の安さ (2)
- hidden master対応
- スレーブとして機能
- 逆引き対応
- サービスにないことを求めているのではない
- 権威DNSのIPアドレスの固定 (NSレコードを自社ドメインにしたい、AWS route53のホワイトラベルネームサーバのようなものを想定)

課金体系について（自前運用）

どのような課金体系が望ましいですか？

57 件の回答



サービスを利用している理由は (複数回答)

- セキュリティ対応が不要 (20)
- トータルコストが安い (19)
- DDoS耐性 (14)
- ダイバーシティ確保 (9)
- 別サービスのオマケ(無料) (8)
- DNSSEC対応が自前では大変 (4)
- 素敵な統計情報画面
- 楽
- BCP
- 各サービス責任者の判断
- 直接の担当ではないので不明

サービス選定の際のポイントは (複数回答)

- 価格 (31)
- DDoS対策 (18)
- ゾーン情報の編集のしやすいUI (16)
- ゾーンの追加・削除がオンラインでできる (15)
- ゾーン転送(受信側)対応 (12)
- ゾーン情報の編集がAPIでできる (10)
- サポートへの質問に対する回答が早い (7)
- DNSSECに対応している (5)
- 素敵な統計情報・ログ (2)

サービスに望むことは (サービス利用) (複数回答)

- 素敵な統計情報 (14)
- クエリログ (13)
- UI/APIがメンテナンスで止まらない (12)
- SLA (10)
- 定額課金 (10)
- 特になし (6)
- 専有権威DNSサーバ (5)
- 素早い画面レスポンス
- 無料sandbox
- 安定運用
- 自前運用と共存するためのより複雑な権限管理機能
- DNSSEC対応(鍵管理含む)
- 手軽な内部サーバ名前解決向けサービス。速度が出ないかなぁ。unboundとかのwebサービス。荒唐無稽すぎるか。

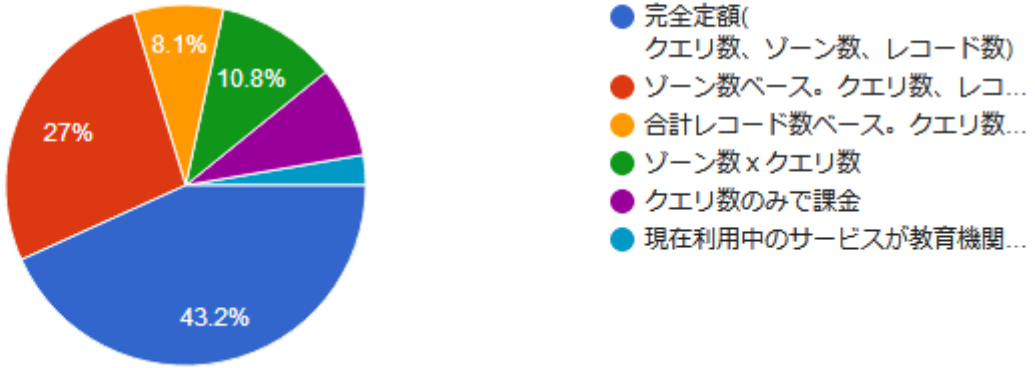
サービスに望むことは (自前運用) (複数回答)

- 素敵な統計情報 (23)
- クエリログ (22)
- 特になし (21)
- 定額課金 (20)
- SLA (16)
- UI/APIがメンテナンスで止まらない (15)
- 専有権威DNSサーバ(11)
- 費用の安さ (2)
- hidden master対応
- スレーブとして機能
- 逆引き対応
- サービスにないことを求めているのではない
- 権威DNSのIPアドレスの固定 (NSレコードを自社ドメインにしたい、AWS route53のホワイトラベルネームサーバのようなものを想定)

課金体系について (サービス利用)

どのような課金体系が望ましいですか？

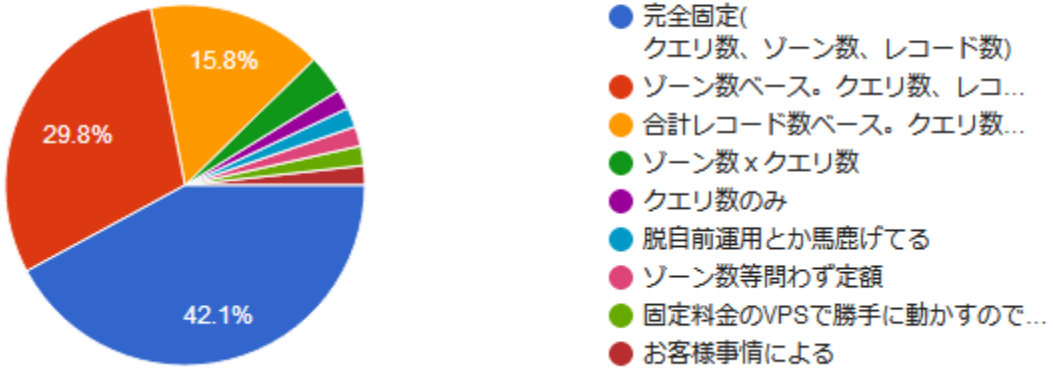
37 件の回答



課金体系について (自前運用)

どのような課金体系が望ましいですか？

57 件の回答



Any Questions?