DNSサービス提供者としての権威DNS

IIJ
Internet Initiative Japan

InternetWeek 2016 DNS DAY
株式会社インターネットイニシアティブ
山口崇徳

Ongoing Innovation

はじめに

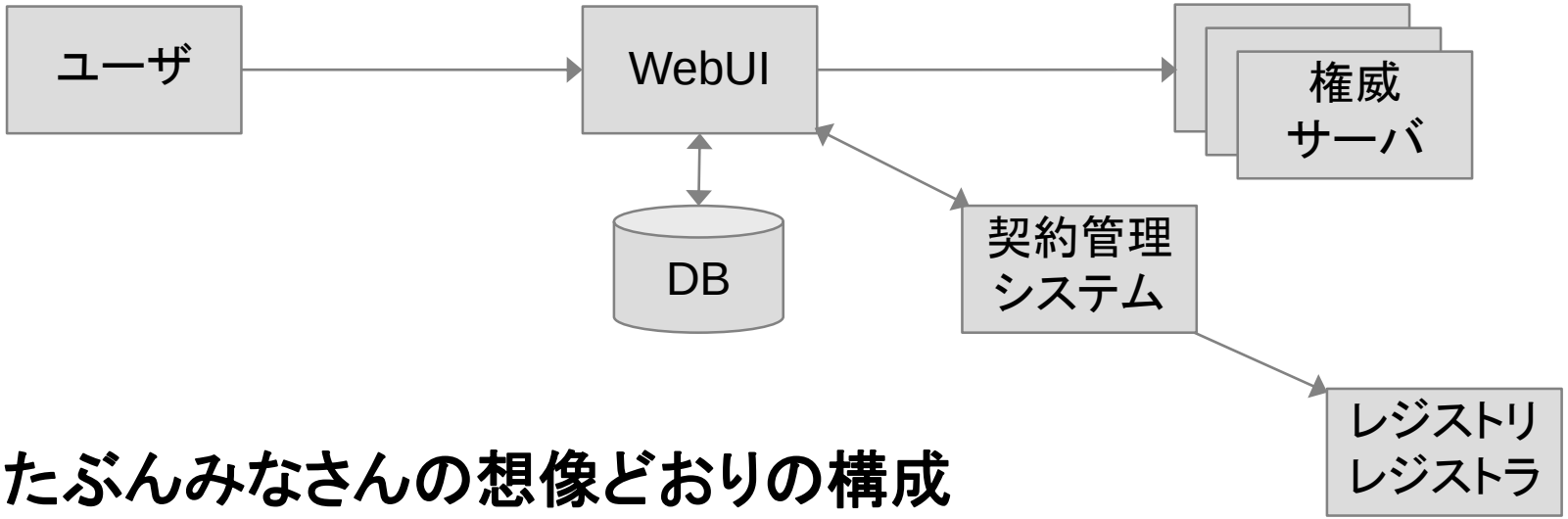
- こんにちは、IIJ の DNS サービスの中の人です
  - 開発とか運用とかじゃなくてサポートとかやってます

- 宣伝になってもつまんないので、IIJ の内側の話はそこそこにして、DNS 屋さん一般の話を多めに

DNS ホスティング事業者の特徴

- **共用ホスティング**
  - 所有者の異なるゾーンが同じサーバに収容される
  - 専用ホスティングが不可能なわけではない
    - が、実際にそのような事業者が存在すると聞いたことはない
- **収容ゾーン数が多い**
  - 数千～
  - ゾーンの追加/削除が頻繁
  - 1ゾーンあたりのレコード数はそれほど多くない

ホスティング屋の裏側(1)



- **たぶんみなさんの想像どおりの構成**
- **一般的なプライマリ/セカンダリ構成ではない**
  - それぞれの権威サーバの関係は対等であり、主従関係はない
  - 権威サーバ間の依存性を排して耐障害性を上げる

ホスティング屋の裏側(2)

- **セカンダリ専用サービスの構成**
- **顧客プライマリと AXFR/NOTIFY のやりとりをするサーバは、NS レコードに載せる権威サーバとは別**
  - 権威サーバを増強して数が増えたり IP アドレスが変わったりしても、ユーザが設定変更する必要はない

IIJ の DNS サービスの裏側

- **権威サーバ2系統**
  - 国内外複数拠点で Anycast
  - DDoS 対策装置導入の非 Anycast
  - 各ノード内は完全冗長構成
- **BIND と NSD を併用**
- **くわしくは → http://techlog.iij.ad.jp/archives/2135**

- **DNS クエリを受けない WebUI や DB などのサーバも国内2拠点に設置して災害対策**

DNS ホスティングならではの機能(1)

- **WebUI によるゾーン編集**
  - テキストエディタでゼロから書かなくてよい
  - DNS サーバに読みこませてみたら文法エラーが出たー、とかシリアル番号上げ忘れたー、とかいうことがない
  - ただし履歴管理は弱い
- **API によるゾーン編集**
  - REST など
  - デプロイの自動化や、監視失敗したホストを自動的にゾーンから削除する、などの用途に
  - Amazon Route53、Dozens、IIJ など

DNS ホスティングならではの機能(2)

- **DNSSEC**
  - 死ぬほどめんどくさい DNSSEC の鍵ロールオーバーと定期再署名を全自動で
  - WebUI からチェックボックスを有効にするだけ!
  - という風景が一般的になるかなー、と思ったんですけどぜんぜんそうなってないですね……
  - SANNET、Cloudflare、IIJ など

DNS ホスティングならではの機能(3)

```
@ IN CNAME www.example.com.
```

- **ゾーン頂点の CNAME は禁止**
  - かならず SOA と NS が存在するので同居できない
  - が、外部のクラウドサービスを利用する際には CNAME で向けてくれ、と案内されることが多い
- **名前で記述しておくと、内部で名前解決して A/AAAA レコードに置き換える機能がある DNS 屋さんがいくつか**
  - ALIAS(Route53) とか ANAME(DNSimple、DNSMadeEasy) とか CNAME Flattening(CloudFlare) とか APEX(IIJ) などと呼ばれる

DNS ホスティングならではの機能(4)

- **GeoIP**
  - 問い合わせ元の所在地域により応答する IP アドレスを動的に変える
  - どちらかというと DNS 専業の事業者ではなく、Akamai など CDN 屋さんの DNS サービスに多い機能
- **GSLB**
  - Global Server Load Balancing (広域負荷分散)
  - ゾーンファイルに記載されている IP アドレスに対して ping や HTTP などのヘルスチェック
    - 応答がないサーバを自動的にゾーンから削除
    - 復活したら自動的にゾーンに戻す
  - Route53、さくら、IIJ など

DNS ホスティングでできないこと(1)

- **キャッシュ DNS**
  - そういうサービスではありません
  - ISP であればキャッシュ DNS も持ってるはずだが、もちろん同一サーバで動いているわけではない
- **イントラ用権威 DNS**
  - インターネット上のサービスなので、イントラ向けはイントラ内に自前で構築してください
  - クラウドホスティング事業者の提供する DNS では可能なところもあり(Amazonとか)

DNS ホスティングでできないこと(2)

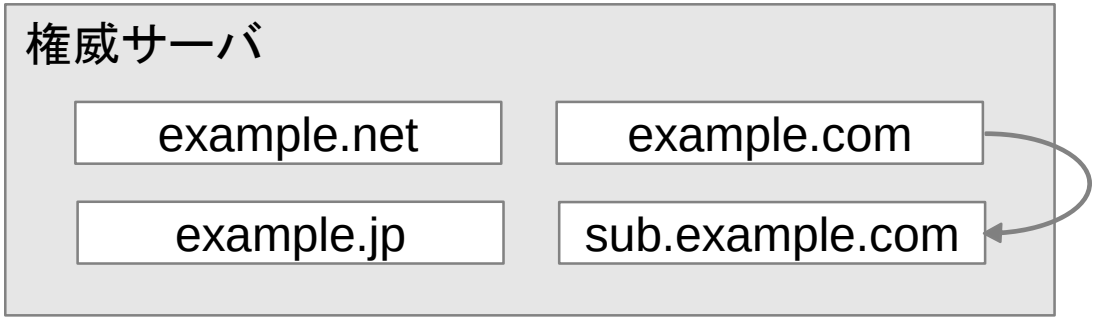
- **特殊な RRType**
  - SOA、NS、MX、A、AAAA、CNAME、TXT、SRV、PTR ぐらいしか書けない
    - SRV は Office365 で必要になるので急速に対応が進んだ
  - それ以外の RRType はまず対応してないと思っていい
  - WebUI が対応していない
    - ゾーン編集機能のないセカンダリ専用サービスならたいてい大丈夫

DNS ホスティングでできないこと(3)

- **クエリログ**
  - ログ取得が不可能なわけではないが、提供しないところがほとんど
  - Amazon Route53 はクエリ数に応じた従量課金なんだから、エビデンスとしてのログ提供はあってもいいとは思う……
- **ゾーン転送**
  - セカンダリ専用サービスであれば転送受けはもちろん可能
  - ゾーン編集した結果を顧客セカンダリに対して転送することはできない

親子同居問題

- たくさんのゾーンが同じサーバに収容される
- 親子関係になってるゾーンも



- NS で明示的に親ゾーンから子に権威を委譲しなくても、権威サーバは子ゾーンに対する問い合わせに権威応答を返す
  - そうすべきというルールはないはずだが、既存の権威 DNS サーバ実装はどれもみなそのように動作するようだ

サブドメインハイジャック

- **example.com ゾーン内の www.example.com**
- **www.example.com ゾーン内の www.example.com**
- **親子同居しているとき、優先されるのは後者**
- **親ゾーンと子ゾーンの管理者が別だったら……？**
  - 悪意ある人物が www.example.com ゾーンを契約することで、親ドメイン内の www.example.com を乗っ取れる

ドメインハイジャック

- **サブドメインが特定の名前の場合、親ドメイン乗っ取りも可能**
  - 内部名で指定されている NS、MX、SRV
  - wpad.example.com (プロクシ自動設定)
  - isatap.example.com (ISATAPルータ自動発見)
  - _domainkey, _dmarc (メール送信ドメイン認証)
  - _tcp, _udp (SRV)
  - _acme-challenge (SSL証明書発行)
- **2012年に注意喚起が出ている**
  - https://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html

ドメインハイジャック対策

- **そもそも親子ゾーンで管理者が異なるような契約は拒否しちゃえばいいんじゃないの？**
  - 同じ組織だけどあえて別契約にしたい、というケースもある
    - 本社と地方拠点とか、サブドメインの運用を SIer に委託する、とか
  - 顧客の利便を考えると、一概に断るのは難しい
- **IIJ の場合、親ゾーンの管理者と異なる人が子ゾーンを契約しようとした場合、親の契約者に確認を取る**
- **Amazon Route53 の場合、サブドメインはかならず(?)親ドメインと異なるサーバに収容される模様**
  - そもそも親子同居しないので問題が起きない

ネームサーバは内部名で

```
example.com. IN NS ns.example.com.
```

- って、JPRS さんが言ってました
  - https://jprs.jp/tech/material/IW2004-DNS-DAY-internal-hostname-in-nameserver-minda.pdf
  - http://www.janog.gr.jp/meeting/janog15/data/12-dns-fujiwara.pdf

ネームサーバは内部名で

```
example.com.  IN  NS  ns.example.com.
```

- って、JPRS さんが言った
  - https://jprs.jp/tech/materials-2004-DNS-DAY-internal-hostname-in-nameserver-jprs.pdf
  - http://www.janog.gr.jp/meeting/janog15/data/12-dns-fujiwara.pdf

内部名が推奨された理由

JPRS JAPAN REGISTRY SERVICE

Japan Registry Service

BINDキャッシュサーバの動作

- グルーがない参照が2段続くとBIND 8.2キャッシュサーバからは検索不能
  - www.bad2.co.dnslab.jp の A の検索
    isp.ne.dnslab.jp, isp.ad.dnslab.jpを使い上記を再現
- BIND 8.3で修正され、引けるようになったが、時間がかかる
  - ネームサーバのアドレスがキャッシュに入ると速い
  - 二度目のクリックで読めるようなこともある
- BIND 9では問題なし、時間も短い
- 検索できたりできなかったりする名前がある場合、ネームサーバの設定を確認しましょう

Copyright © 2005 株式会社日本レジストリサービス

.JP

http://www.janog.gr.jp/meeting/janog15/data/12-dns-fujiwara.pdf より

ネームサーバは外部名で

```
example.com. IN NS ns.example.net.
```

- **設備都合による IP アドレス変更がありうるので、ホスティング事業者が指定する外部名で!!**
  - 外部名: DNS 屋さんが A レコードを変えるだけ
  - 内部名: すべてのお客さんがそれぞれの A レコードを変更 + レジストラに glue 変更申請 → 困難
- **できるだけアドレス変更せずに済むように運用しているが、常に可能とはかぎらない**
  - いざ必要になったときに不可能では困る
- **勝手に内部名で登録してるお客さん、マジ困る…**

権威 DNS への最近の攻撃

- **2014/初頭～2016/夏 水責め攻撃の流行**
  - 国内ではキャッシュサーバが多く影響を受けたが、真の狙いは権威サーバだったと思われる
- **2015/11/30 ルートサーバに DDoS**
- **2016/08/末 国内複数サービスに DDoS**
  - さくらインターネットの権威 DNS が障害
- **2016/10/21 米 Dyn に DDoS**
  - Twitter、Paypal、GitHub その他多数に影響

なぜ DNS が狙われるのか?

- 実際に IIJ にホスティングされたサイトが攻撃された事例

- 某政治家さんが失言 → 炎上
- その人がトップを務める役所の Web サイトに攻撃
- Web が落ちないので標的が DNS に向く

- 攻撃者の狙いの多くは Web 閲覧不能
  - Web サイトを落としても DNS を落としても目的を達せられる

DDoS 攻撃に耐える構成

- **帯域増強**
- **DDoS 対策装置**
- **Anycast**
  - Dyn は anycast してても全世界的に障害になりましたが…
- **サーバよりも、その手前のネットワーク構成を強化**
  - 回線帯域が埋まるので、サーバのパフォーマンスを上げてもあまり意味がない
  - ネットワーク内部での輻輳を避けるため、できるだけボーダールータに近いところに配置

DDoS 対策のコスト

- **設備コスト、運用コストともハンパない**
  - プライマリ/セカンダリ各1台 + 100Mbps で済む時代ではない
  - 1企業が自前で対策するのはかなり無理がある
- **権威サーバを自前で持つ時代は終わりました**
- **……DNS 屋さんならそのコストをかけられるの？**

DNS ホスティングの位置づけ

- **無料または安価な「おまけ」サービス**
  - ドメインを買ってくれたお客さんにおまけ
  - Webホスティングを買ってくれたお客さんにおまけ
  - 回線接続を買ってくれたお客さんにおまけ
- **安いおまけが競合なので、DNS 単体サービスも高い料金では客がつかない**
- **DNS は金にならない**
- **攻撃がなかった時代ならそれでも採算取れたんですけどね**

国内事業者の現状

- **残念ながら、大規模な DDoS に耐えられる構成になっている事業者は国内ではかなり少なそうに見える**
- **DDoS 対策には莫大な設備投資が必要だが、現状の売り上げでは投資しても回収できる見込みが立たない**
- **現状が続けば、顧客は対策完了している海外大手に流出するだろう**
  - すでに多くの客がRoute53 や Akamai などに奪われている
- **DDoS 対策しないわけにはいかない**
  - いざ狙われて回線が埋まると DNS 以外のサービスにも影響が及ぶ

まとめ

- **DNS 屋さんの裏側を紹介してみました**
  - 設備構成とか
  - お便利機能とか
  - 共有ホスティング特有の問題とか
- **DDoS ヤバい**
  - DNS は狙われてます
  - 対策にはお金がかかる
  - 設備強化がんばるぞ