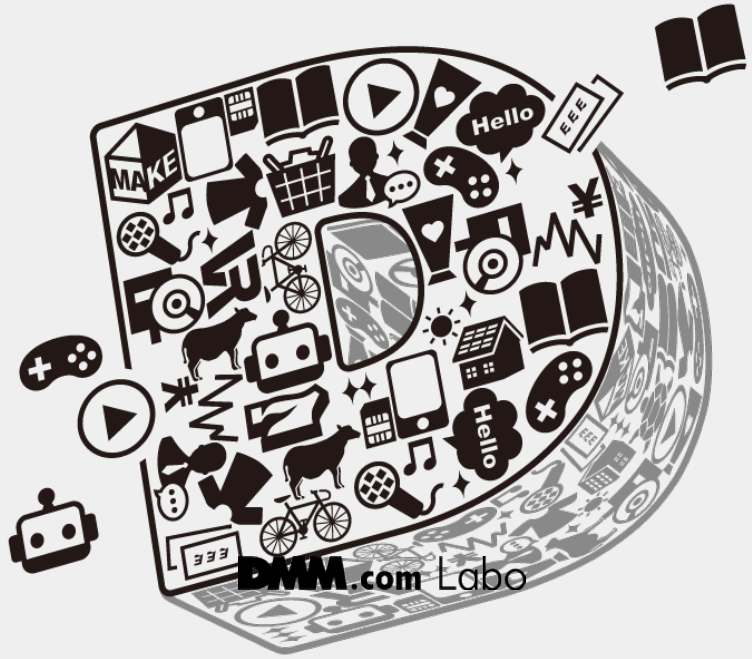

権威DNSサービスのダイバーシティ

DMM.com Labo 高嶋隆一

背景

コンテンツプロバイダは

- サーバロードバランシングを用いたサーバ冗長
- GSLBを利用したサイト間冗長
- パブリッククラウドやCDNを用いた個別コンテンツ分散

等様々な冗長化技術を使ってリスク分散をしているが、

その**親ゾーンの権威DNSサーバ**が参照できなくなればおしまい

事業担当部門からのリクエスト

事業担当部門からも、対DDoS耐性を含む権威DNSサーバへの可用性向上のリクエストが発生。事業によってはそもそもの必要条件となっているものもあり。

(例) DMM.com 証券

この要件、どう解決するか

https://commons.wikimedia.org/wiki/Sport_wrestling_(Mundja)#/media/File:WrestlingUSAF_Flag.jpg Public Domain

オンプレミスの強化

- 対DDoS防御ネットワーク装置の導入
- サーバロードバランシングや網内Anycastによるスケールアウト

等の対策が考えられるが、いずれの対策も高コストな上、
データセンタ内外のネットワーク障害、上位ISPの障害等には無力

外部DNSサービスの導入

- DDoS対策サービスを用意しているものを選定する
- 十分なキャパシティを用意しているサービスを選定する

事は可能だが、どんなにメジャーなサービスも止まる時は止まる

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/

単一でダメなら
組み合わせれば
いいじゃない
= ダイバーシティ

http://www.hq.nasa.gov/office/pao/History/alsj/a15/ap15-S71-42217HR.jpg Public Domain

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

オンプレ

可能な限りがんばる

- サーバロードバランシング
- 台数を増やしたスケールアウト
- 複数ネットワーク、拠点への分散配置
- DDoS防御装置の導入(できれば)

しかし、投資、維持運用コストもそれなりにかかるので、
複数の外部DNSサービスを利用できるのであれば
「使わない」というオプションもある。

外部サービス

要件

- BGP Anycast、異国間地域分散、キャパシティ等DDoS対策が十分取れている事
- 複数サービスを利用する為、専用の方法以外で外部のDNSサービスと連携が取れる事

クラウド事業者のDNSサービス

性能、DDoS対策の観点では申し分ないのだが、やはり提供事業者のクラウド内での利用を想定したものとなっている。

- ○ DDoS対策、キャパシティ
- × 全てのRRがサポートされているわけではない
- × ゾーン転送はサポートされていない。
  他サービスとの併用を考える時にはAPIを使った同期ツールを作成し、APIの更新に合わせて保守する必要がある

専業のDNSサービスプロバイダ

条件さえ盛り込めば、可用性、データ同期共に可能なDNSサービスプロバイダが存在する

- ○ DDoS対策、キャパシティについては、それを売り物にした複数のサービス(*)が存在
- ○ データの同期についても複数のDNSサービスプロバイダがAXFR/IXFR等の標準ベースの同期をサポート
- ? DDoS対策、キャパシティを鑑みればコストは安いが会社によっては?

(*)条件を満たすDNSサービスプロバイダの例
https://dyn.com/
https://www.akamai.com/jp/ja/products/cloud-security/fast-dns.jsp
https://www.neustar.biz/security/dns-services

ISPの権威DNSサービス

回線の付加サービスとなっているケースが多くピンキリだが、
たまにアタリが・・・

? DDoS対策、キャパシティについては素晴らしい設備があるプロバイダから物理サーバ1台しかないところまでピンキリ
◯ データの同期については、殆どのAXFR/IXFR等の標準ベースの同期をサポート
◯ 付加サービス扱いの為、妙に安い時がある
× 付加サービス扱いの為、回線を買っていないと買えない時がある
× 付加サービス扱いの為、ダッシュボードとかなくて申込書がいったりする時がある

というわけで・・・

これが

2017年5月以前：権威DNSサーバはオンプレミスにのみ存在

```
$ dig ns dmm.com @8.8.8.8

~~snip~~
;; ANSWER SECTION:
dmm.com.                899     IN      NS      ns1.dmm.com.
dmm.com.                899     IN      NS      ns2.dmm.com.
dmm.com.                899     IN      NS      ns4.dmm.com.
~~snip~~
```

こうじゃ

オンプレと複数のDNSサービスプロバイダへ権威DNSサーバを分散配置

```
$ dig ns dmm.com @8.8.8.8

~~snip~~
;; ANSWER SECTION:
dmm.com.        899     IN      NS      ns1.dmm.com.
dmm.com.        899     IN      NS      ns2.dmm.com.
dmm.com.        899     IN      NS      ns4.dmm.com.
dmm.com.        899     IN      NS      dns-a.iij.ad.jp.
dmm.com.        899     IN      NS      a9-67.akam.net.
dmm.com.        899     IN      NS      a1-198.akam.net.
dmm.com.        899     IN      NS      a13-64.akam.net.
dmm.com.        899     IN      NS      a12-67.akam.net.
dmm.com.        899     IN      NS      a14-65.akam.net.
dmm.com.        899     IN      NS      a18-66.akam.net.
~~snip~~
```

→ オンプレ

→ DNSサービスその1

→ DNSサービスその2

ポイント

- オンプレ含む複数のDNSサービスを利用して全落ちは避ける
- DDoS対策も取れたDNSサービスプロバイダを選んで全落ちは避ける
- データ同期はAXFR/IXFRを利用したレガシーなスタイルで保守コストと将来のサービス変更を容易に

結論

複数の権威DNSサービスを使って、
自社のサービスを守ろう！

Thank you !