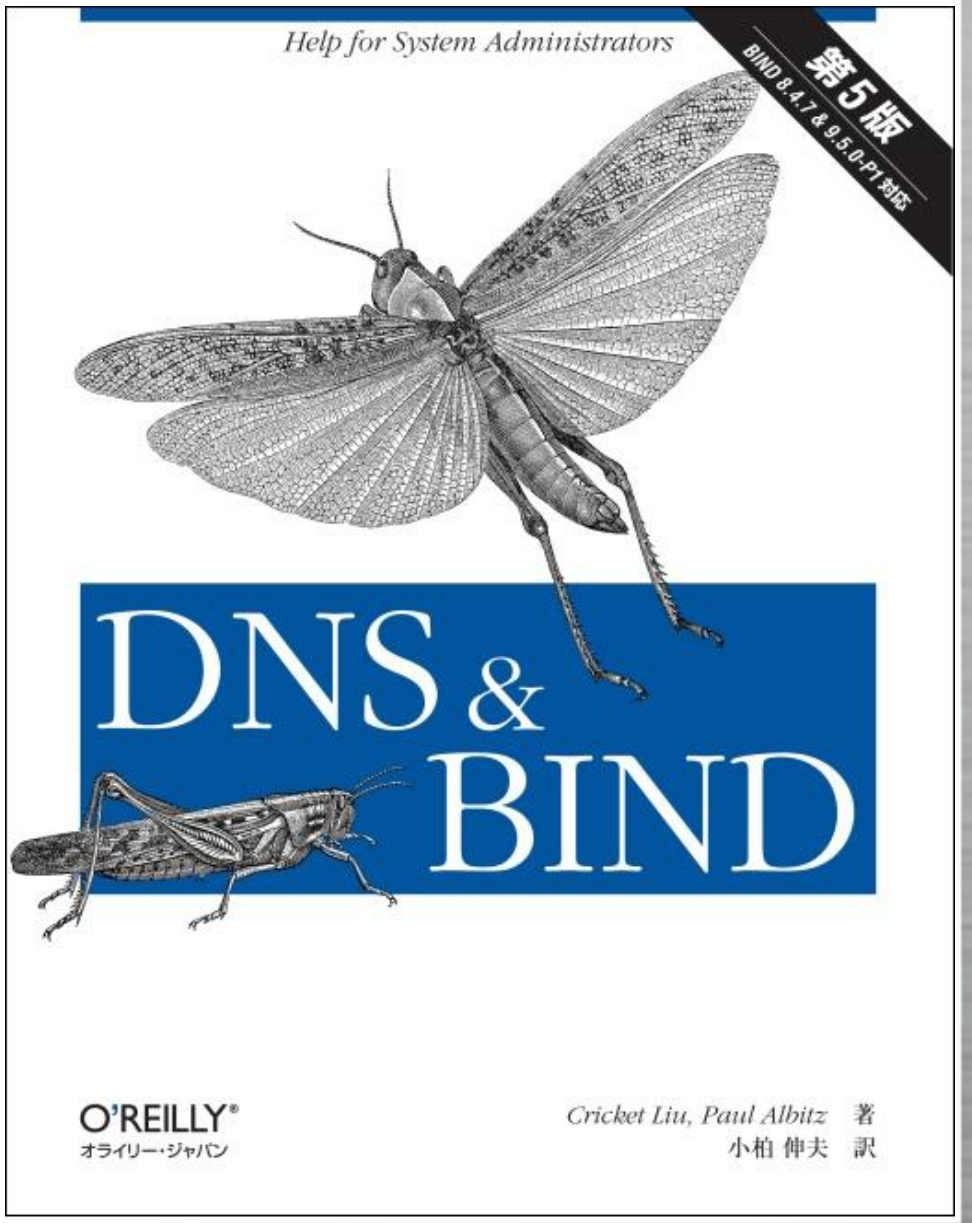
DNSに関する常識の変化
～これからの常識編～

山口崇徳（インターネットイニシアティブ）

DNS の常識といえば

- DNS = BIND でした



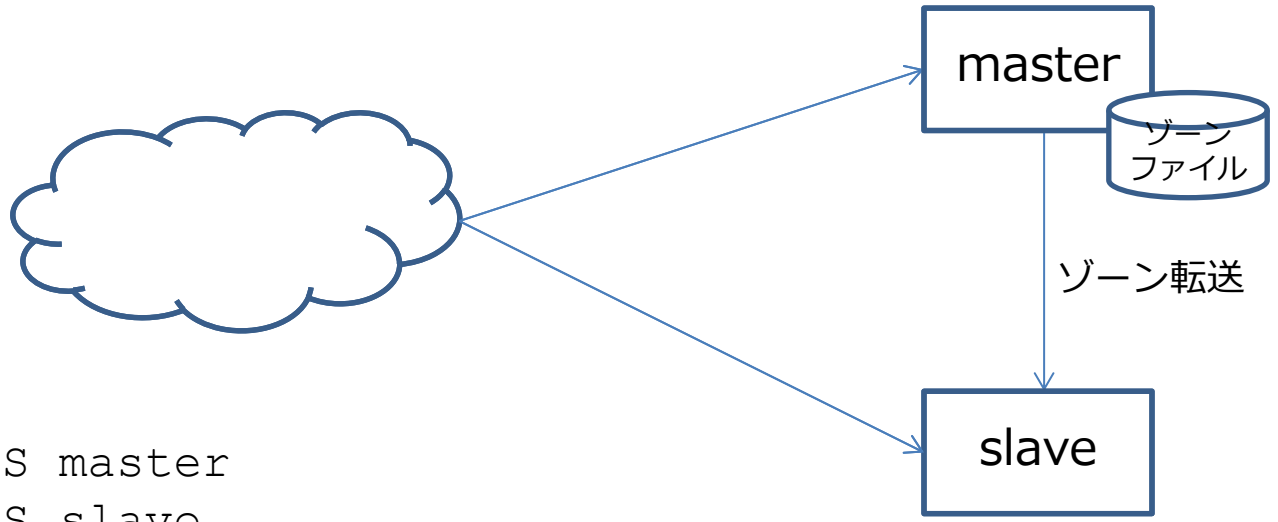
脱 BIND

- BIND は脆弱性が多い
  - ここ数年は年5~10件ほど
  - プロセス停止する穴が多い

- こんな信頼できないものにいつまでしがみついてるんですか
  - …というのが最近の dnsops.jp の見解
    - https://dnsops.jp/event20160624.html
    - https://dnsops.jp/event20170628.html

権威 DNS サーバの構成(古墳時代)

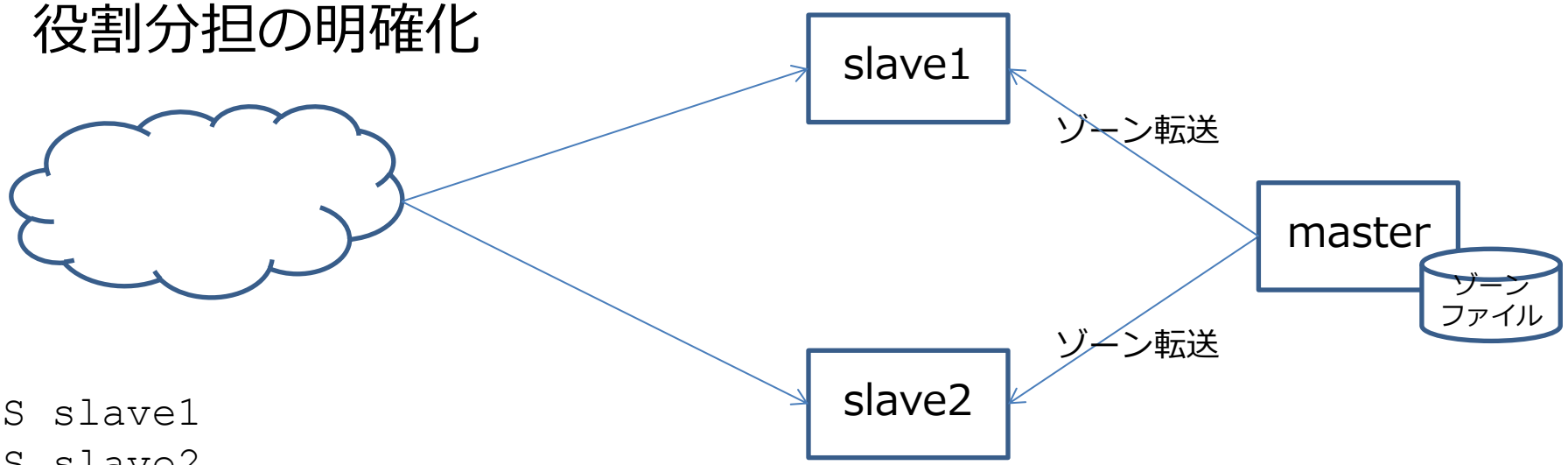
- マスター/スレーブ（あるいはプライマリ/セカンダリ)構成




```
@ IN NS master
@ IN NS slave
```

権威 DNS サーバの構成(最近)

- hidden master 構成
  - 外からの DNS 問い合わせに答えるのは slave だけ
  - master は内部でゾーンの管理だけ
  - 役割分担の明確化




```
@ IN NS slave1
@ IN NS slave2
```

2016 Dyn cyberattack

- 2016/10/21 DNS ホスティングサービス最大手の一角、Dyn が Mirai botnet による大規模な DDoS のためサービス障害
- ほかにも DNS amp、水責め攻撃など、DNS に対する DDoS はいまや日常茶飯事
- これまでの構成では攻撃に耐えられない

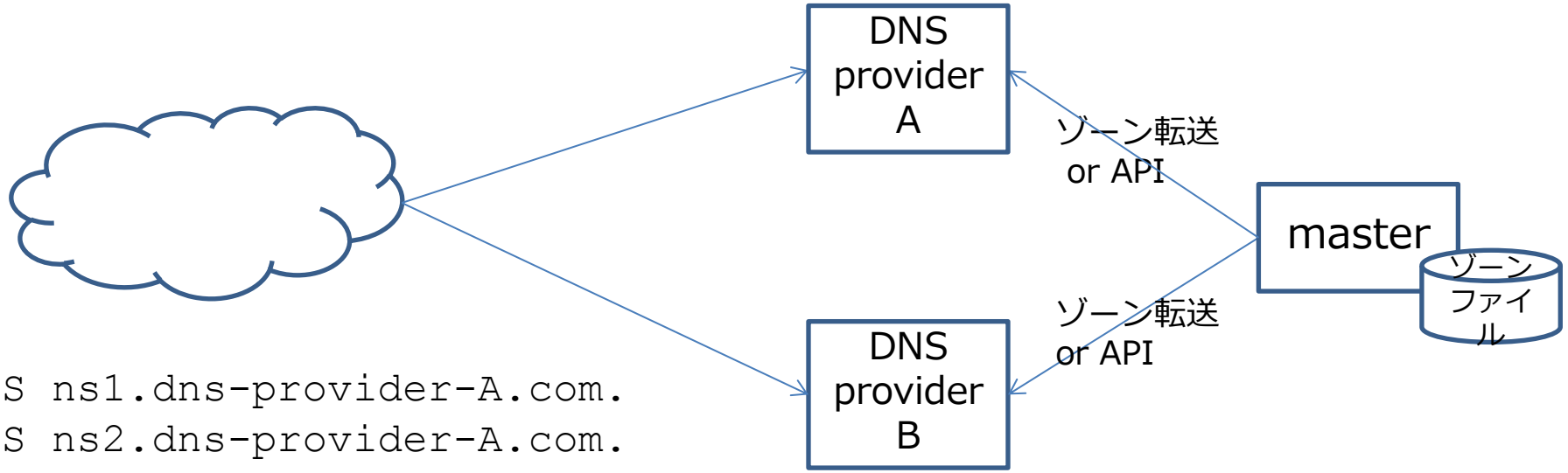
- DNS が CPU もメモリも帯域もほとんど使わないサービスだったのは昔話
- いまは潤沢に用意しないと DDoS にやられる

DDoS 対策としての DNS

- DNS が落ちると Web、メールその他あらゆるサービスが使えない
  - 攻撃者にとってかっこうのターゲット
  - Web サーバを強化するだけでなく、そこにアクセスを誘導するための DNS も強化しなければ意味がない
- いまや自前ネットワーク内に権威 DNS を置くこと自体がリスク
  - 脆弱性がなくても帯域を埋められたら負け
  - BIND を捨てたから安心ということにはならない
- じゃあどうすればいいのか?

権威 DNS サーバの構成(最新)

- 事業者ダイバーシティ
  - 複数の DNS ホスティングサービスを併用し、一方のサービスが障害になっても名前解決が止まらないようにする




```
@ IN NS ns1.dns-provider-A.com.
@ IN NS ns2.dns-provider-A.com.
@ IN NS ns1.dns-provider-B.net.
@ IN NS ns2.dns-provider-B.net.
```

事業者ダイバーシティの実例

- DMM

```
dmm.com.        900     IN      NS      ns1.dmm.com.
dmm.com.        900     IN      NS      ns2.dmm.com.
dmm.com.        900     IN      NS      ns4.dmm.com.
dmm.com.        900     IN      NS      a1-198.akam.net.
dmm.com.        900     IN      NS      a12-67.akam.net.
dmm.com.        900     IN      NS      a13-64.akam.net.
dmm.com.        900     IN      NS      a14-65.akam.net.
dmm.com.        900     IN      NS      a18-66.akam.net.
dmm.com.        900     IN      NS      a9-67.akam.net.
dmm.com.        900     IN      NS      dns-a.iij.ad.jp.
```

DMM 自社運用

Akamai FastDNS

IIJ DNS セカンダリサービス

- その他 twitter、amazon、github、paypal など大手サイト
  多数が複数サービス(+自社運用)を組み合わせ

権威 DNS サーバの新常識

× DNS といったら BIND だろう

△ もう BIND はやめて他の実装を使おう

○ サービスを買おう、できれば複数事業者を

- 外に晒す DNS を自前で運用する時代は終わりました
  - Web だけ CDN に任せて DNS が自前なのは片手落ちと言わざるを得ない
  - 外部からのアクセスが来ない hidden master やキャッシュサーバはこれからも自前で
- 自前運用を続けるなら相当な覚悟(と設備投資)を