Internet Initiative Japan

DNSアワー
権威DNSと可用性

InternetWeek 2016プログラム委員
株式会社インターネットイニシアティブ
其田　学

Ongoing Innovation

権威DNSと可用性

おさらい編

権威DNSと可用性

権威DNSとは

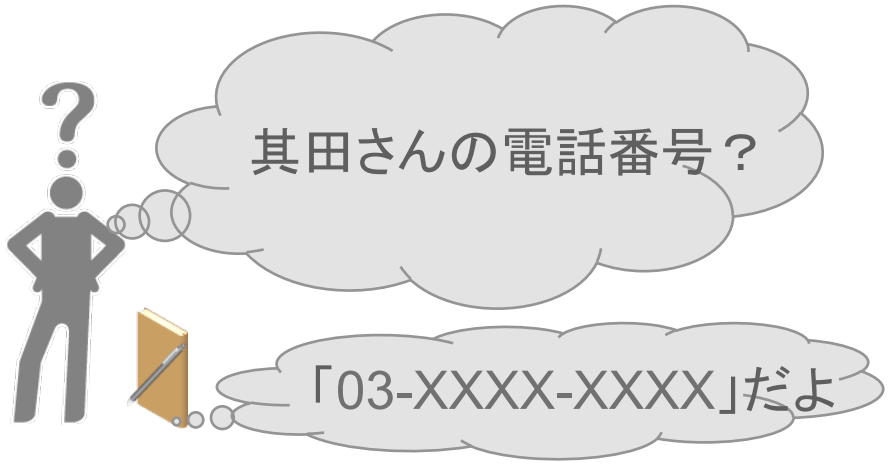
- 権威DNSは、ドメイン名と結びつく資源情報を提供するサーバです
- よくアドレス帳に例えられています

アドレス帳

名前： 其田 学
電話番号： 03-XXXX-XXXX
email: manabu@example.jp

権威DNS

ドメイン名： example.jp.
IPアドレス： 203.0.113.1
メール送信先： mail.example.jp.



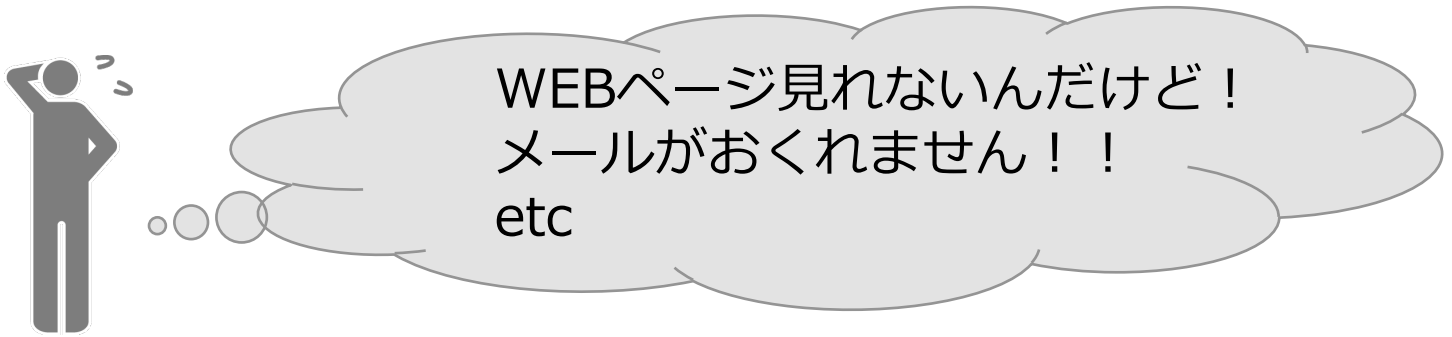
権威DNSと可用性

可用性とは

- システムが使用できる状態を維持し続ける能力

権威DNSは不特定多数のクライアントから、
不特定なタイミングでリクエストを受けるため、
高い可用性が求められます。

リクエストに答えられないと。。。



可用性とは

- **使えなくなると、大変なことになる為、権威DNSは可用性を高めるため複数の系を使って冗長化しています。**

弊社の例（iij.ad.jpの権威DNSサーバは、dns0とdns1の２系統）

```
iij.ad.jp. 3600IN    NS    dns0.iij.ad.jp.
iij.ad.jp. 3600IN    NS    dns1.iij.ad.jp.
```

通常は２系統ー３系統ぐらいの系統で冗長化

大規模な権威DNSになると沢山
例）JPの権威DNSは、a.dns.jp. からh.dns.jp.の８系統
　　COMの権威DNSは１３系統

権威DNSの可用性を脅かす脅威

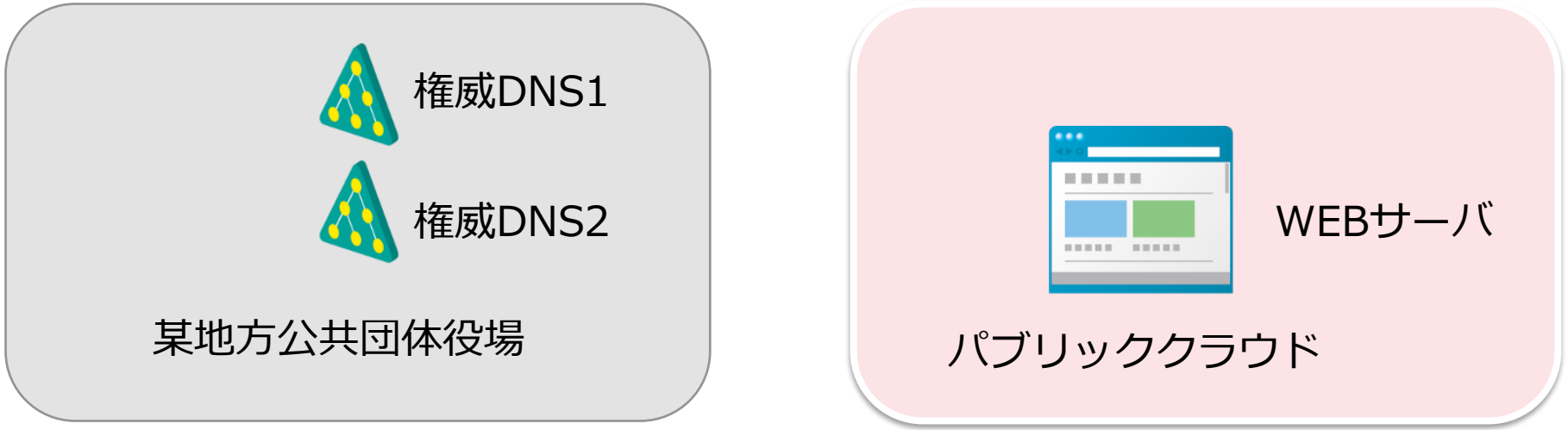
権威DNSの可用性を脅かす脅威

- 物理的な脅威
- ネットワーク的な脅威
- ソフトウェアに対する脅威

物理的な脅威

物理的な脅威

- 例えば地震、台風などの天災
- 実際にあった例



WEBはパブリッククラウド上で冗長化されていたが、
権威DNSは役場に集中していた。
結果として、台風で役場が停電、WEBサーバのIPアドレスが引けなくなり、
災害時の情報発信に支障をきたしました。

ソフトウェアに対する脅威

ソフトウェア的な脅威

権威DNSにとてもよく使われているソフトウェア

BIND9

可用性に対する致命的な脆弱性がたまによく発見されます
JPRSさんが緊急でアナウンスしている数

- 2014年　　3件
- 2015年　　5件
- 2016年　　6件
- 2017年現在までに 4件

脆弱性の発見数は年々右肩上がり！！

ソフトウェア的な脅威 -

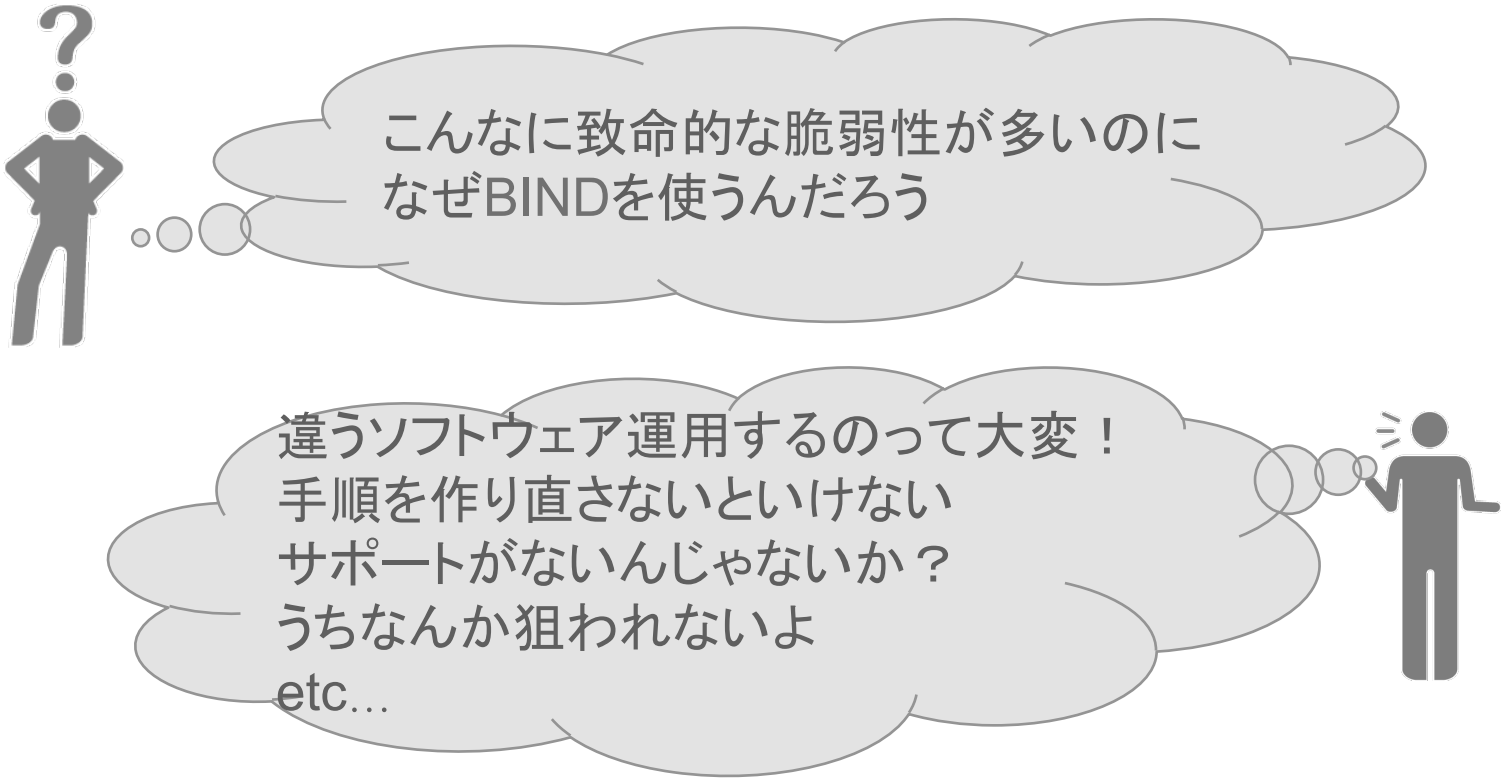
BIND9の可用性に対する脆弱性が多い理由

- BIND8の頃、リモートコード実行の脆弱性が多かったため、BIND9では変な入力があると、処理を止めて、プロセスを落とす設計
- 権威DNSとリゾルバ両方の機能を持つ複雑な設計
- 新機能の実装が続いており、新機能が原因の脆弱性が多い。
- すでに１７年選手でコードの保守が困難。

近年の脆弱性発見のプロセスの変化

- 以前は人が脆弱性を踏んで発見することが多かった
- 脆弱性検査ソフトの発達で、機械的に発見できるようになった

ソフトウェア的な脅威 – 実際の脅威



と言っている間に。。
既に、何度か国内のメジャーな権威DNSサービスもパッチ適用が遅れて落とされています

ソフトウェア的な脅威 – 対策

対策

- **BIND9の開発元とサポート契約を行い、事前に脆弱性情報を手にいれる。**
  - 利点
    - 脆弱性情報の公開前に脆弱性を防ぐパッチが手にはいる
  - 欠点
    - 費用がかかる
    - ゼロデイ攻撃には対応できない
- **別の商用ソフトウェアを使って運用する**
  - 利点
    - BINDの脆弱性からは逃れられる。
  - 欠点
    - 費用がかかる
    - ゼロデイ攻撃には対応できない
      - ただし、ソース公開してない場合がほとんどなので、BINDよりは少ない

ソフトウェア的な脅威

- **BIND9のみの運用をやめて、別のソフトウェアと混ぜて使う**
  - 権威DNSは複数の系を作れる
  - BIND9じゃない系を作れば、BIND9由来の脆弱性で全滅はしない

ソフトウェア的な脅威

注意

- 全ての系をBIND以外の１つの実装にしてしまうと、
  結局その実装の脆弱性が出た時に全滅する恐れがある。

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。

Ongoing Innovation