Internet Week 2018 DNS DAY

DNS flag day関連

株式会社XACK

技術部　矢島　崇史

DNS flag dayとは

DNSサーバーソフトウェア(※)からEDNS0が正しく実装されていないサーバー向けの回避策を削除する日(2019/2/1)

※DNSソフトウェアのベンターおよび大規模なパブリックDNSプロバイダーが対象。OSS4製品から拡張になりました

公式サイト

https://dnsflagday.net/

回避策を削除するとどうなる

- 一部または全部の権威サーバーがタイムアウトするようなドメインの名前解決にかかる時間が短くなることが期待される

- EDNS0に正しく対応していない権威サーバーの管理するドメイン名が名前解決できなくなるかもしれない

※EDNS0はRFC 6891で規定されるDNSの拡張機構

どうすればいい？

- EDNS0に正しく対応しているか確認

- 正しく対応していなければ対応
(EDNS0をサポートしないことも含む)

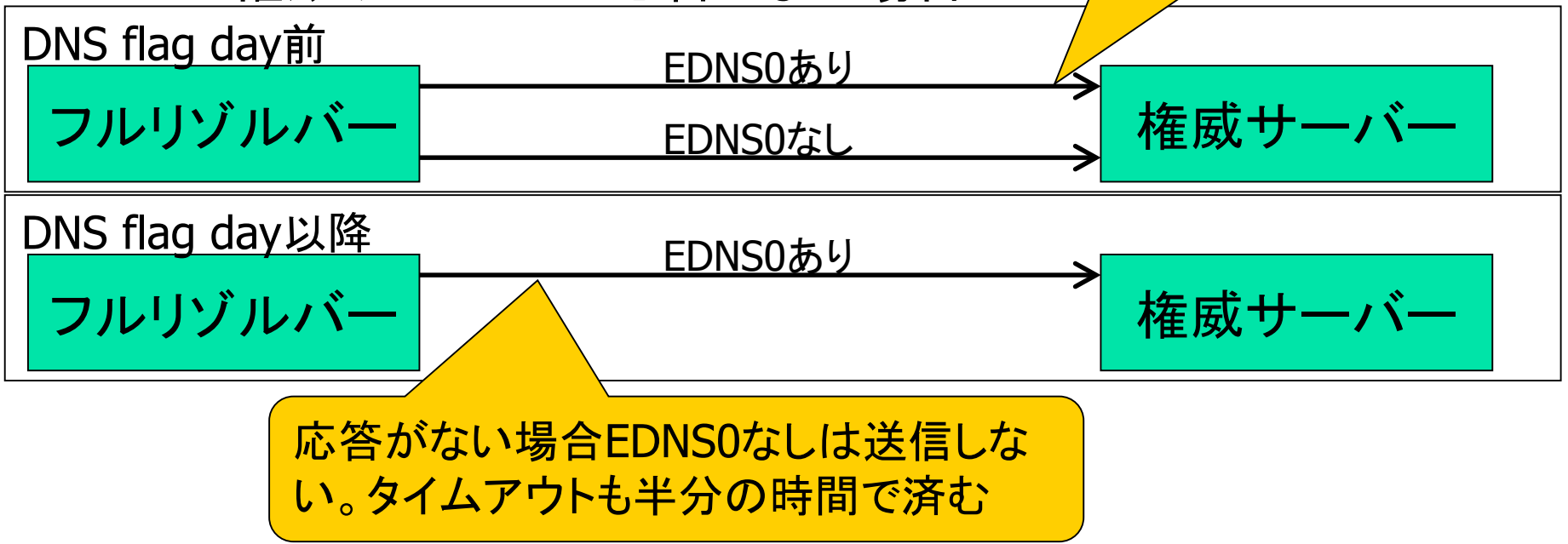
- トラフィックモデルが変わることが想定されるので必要に応じて検証、チューニングを検討

どうなるのかもう少し具体的に

- いつから
  - 2019/2/1以降、ベンダーが回避策を削除したモジュールをリリースし、自身あるいは対向がそのモジュールを適用したら(2/1一斉にではない)
- 何が
  - 主にフルリゾルバー(キャッシュサーバー)
  - 権威サーバーも対象となることがあると思われる
  - スタブリゾルバー(クライアント)はこのタイミング(あるいは将来的にも？)では対応しないと思われるが……

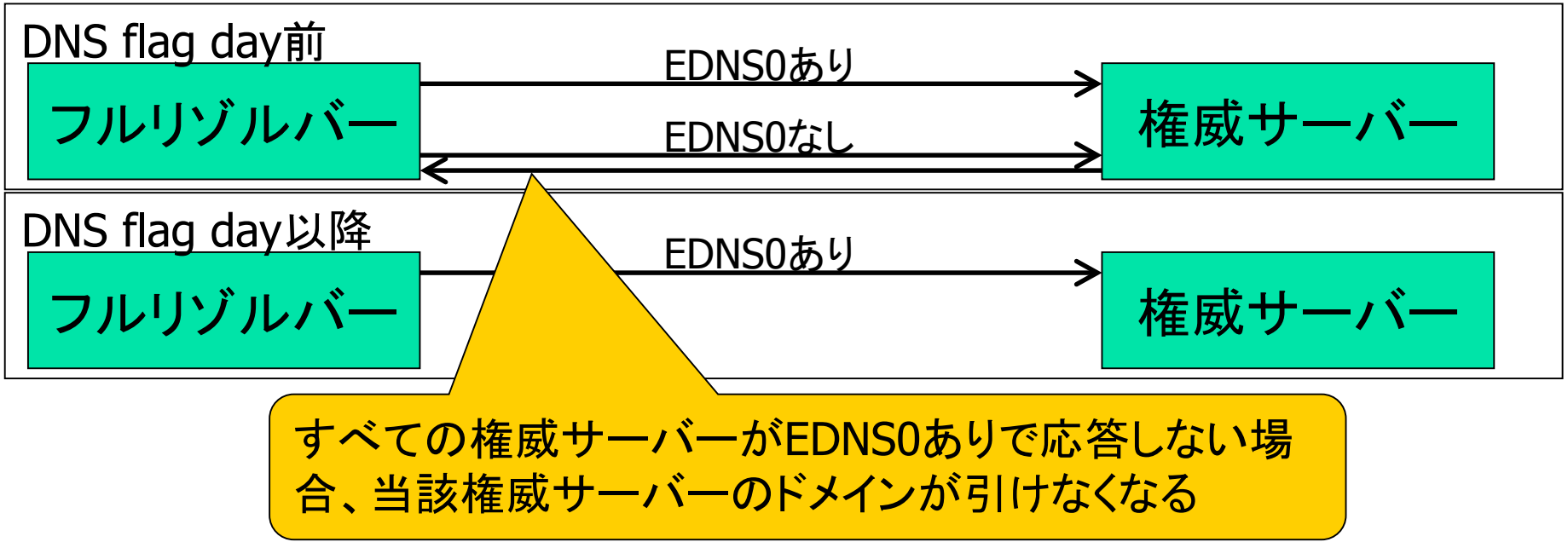
どうなるのかもう少し具体的に

- どうなる(フルリゾルバー)
  - 権威サーバーが応答しない場合



どうなるのかもう少し具体的に

- どうなる(フルリゾルバー)
  - 権威サーバーがEDNS0なしに応答する場合



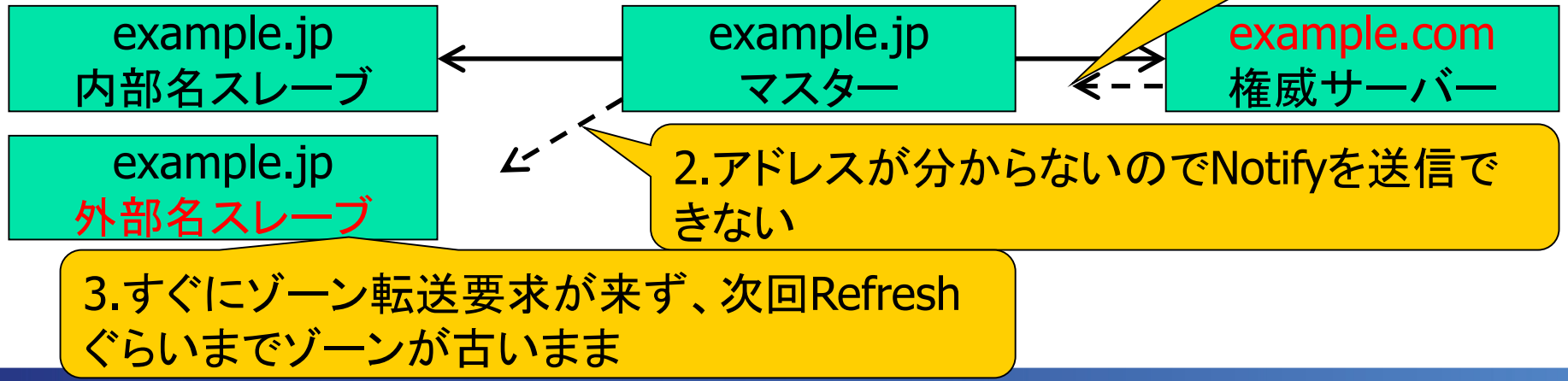
どうなるのかもう少し具体的に

- どうなる(マスター権威サーバー)
  - ソフトウェアによっては、マスター権威サーバーでも自身が反復問い合わせをするケースがある
    - BINDの外部名NS向けにNotifyを送信する際など
  - 外部名の名前解決時に対向の権威サーバーがEDNS0に正しく対応していないと、フルリゾルバーと同様の動作となる
  - 結果、一部権威サーバーに即座にゾーン更新が反映されなくなる

どうなるのかもう少し具体的に

■ どうなる(マスター権威サーバー)

```
@ NS master.example.jp ; マスター
  NS slave.example.jp  ; 内部名スレーブ
  NS slave.example.com ; 外部名スレーブ
slave.example.jp A    192.0.2.1
slave.example.jp AAAA 2001:db8::1
```



どうなるのかもう少し具体的に

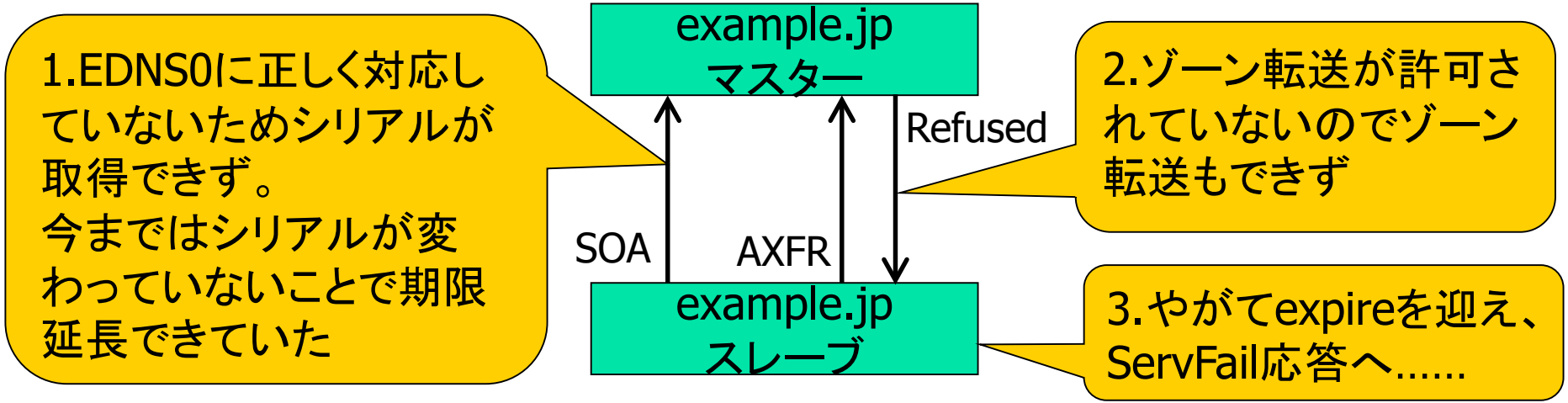
- どうなる(スレーブ権威サーバー)
  - ゾーン転送要求時に大抵SOAを問い合わせる
  - シリアルが更新なしだとゾーン転送処理をしない
  - マスター権威サーバーがEDNS0に正しく対応していないとシリアルが取得できない
  - その後、ゾーン転送要求をするが、ゾーン転送応答が返ってこないとやがて期限切れとなる(例えばスレーブIPが変わったけれどマスター側で対応していないようなゾーン)
  - 結果、当該ゾーンを応答できなくなる

どうなるのかもう少し具体的に

■ どうなる(スレーブ権威サーバー)

```
@ SOA example.jp master postmaster (
  2001010101; はるか昔から更新されてない
  ...)
```

```
allow-transfer { 192.0.2.2; }; 太古に捨て去ったマスター
```



どうなるのかもう少し具体的に

- 回避策がどの通信に適用されなくなるかは明言されていない
- ソフトウェアによって例示の通信自体がないケースも(Unboundのゾーン転送時SOAなど)
- 例示のケース以外にもありそうな気がする(フォワーダーなど)
- 管理しているサーバーがどんな通信をしているか把握しよう！

どうすればいいかもう少し具体的に

- ゾーン管理者

なにはともあれ公式ツールでチェック

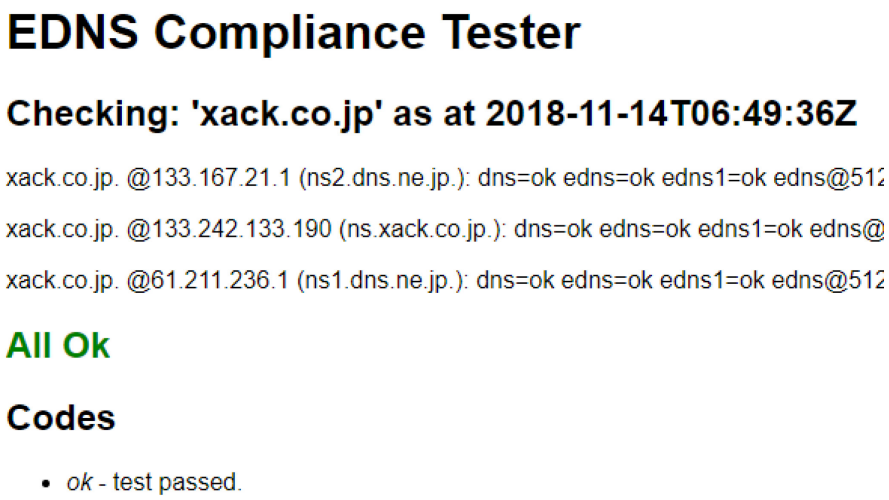
https://dnsflagday.net/

どうすればいいかもう少し具体的に

- DNSサーバー管理者

なにはともあれ公式(に紹介されている)ツールでチェック

https://ednscomp.isc.org/ednscomp/



EDNS Compliance Tester

Checking: 'xack.co.jp' as at 2018-11-14T06:49:36Z

xack.co.jp. @133.167.21.1 (ns2.dns.ne.jp.): dns=ok edns=ok edns1=ok edns@512

xack.co.jp. @133.242.133.190 (ns.xack.co.jp.): dns=ok edns=ok edns1=ok edns@

xack.co.jp. @61.211.236.1 (ns1.dns.ne.jp.): dns=ok edns=ok edns1=ok edns@512

All Ok

Codes

- *ok* - test passed.

どうすればいいかもう少し具体的に

- DNSサーバー管理者

チェックに引っ掛かったら

- 典型的にはソフトウェアかFWの問題らしい
- バージョンアップや設定の見直しを
- FWはEDNS0を理由にDNSパケットを破棄すべきではありません

どうすればいいかもう少し具体的に

- DNSサーバー管理者(フルリゾルバー)

チェックに引っ掛からなくても

  - バージョンアップ時には検証しましょう
  - 同時反復問い合わせ数が少なくなるはず
  - タイムアウト時間が短くなる=TATが短くなるので、スタブリゾルバーからの再送間隔も短くなるかもしれない(QPSの増加)

どうすればいいかもう少し具体的に

- DNSサーバー管理者(権威サーバー)

チェックに引っ掛からなくても

  - バージョンアップ時には検証しましょう

  - 対向がおおよそ想定できると思われるので、あらかじめ挙動を確認しておきましょう

どうすればいいかもう少し具体的に

- DNSソフトウェア開発者

なにはともあれ(ry

https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing

  - RFC 6891に従って実装しましょう
  - EDNS0の対応が必須なわけではありません。対応していなければOPTレコードなしのFormErrを応答すればよいです
  - DNS flag dayに賛同しソフトウェアから回避策を削除するなら、どの場合に削除されるかを明確に

http://www.xack.co.jp