Internet Week 2019 DNS DAY

DNS flag day

2019振り返りと2020に向けて

株式会社XACK
技術部　矢島　崇史

DNS flag dayとは

DNSソフトウェアやサービス提供者たちが共同で

- 特定の日付以降
- 運用上またはセキュリティ上の問題に対して
- 相互運用性を持続させ、性能に影響を与える問題を解消するために
- 何らかの動作を変更する日

公式サイト

https://dnsflagday.net/

DNS flag day 2019とは

DNSソフトウェアやサービス提供者たちが共同で

- 2019/02/01から
- EDNS0に正しく対応していない権威サーバーに対して
- 名前解決の再送回数低減および時間短縮を目的として
- EDNS0なしへの再送する回避策を止めた日

(当時は2019は付与されておらず、継続的に行うことは決定していなかったと思われる)

DNS flag day 2019でどうなるか

- 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

DNS flag day 2019でどうなったか

- 公式に「DNS Flag Day 2019は成功裏に終わりました。」と高らかに宣言されている
  - 高遅延のドメインが全ドメイン中5.68%減少

    ⇒名前解決できないドメインに

- 私自身は開発者で直接運用しているわけでないので実数を観測できないが、実施後特に問い合わせもなく、うまくいったのでは

DNS flag day 2020とは

DNSソフトウェアやサービス提供者たちが共同で

- 時期未定
- IPフラグメンテーションに対して
- 転送の失敗原因やメッセージの一部偽装を回避するために
- UDPで送信するDNSメッセージをフラグメンテーションしないようなサイズに制限する日

サイズを制限するとどうなる

- フラグメントしなくなるのでフラグメント由来の脆弱性から解放される(第一フラグメント便乗攻撃など)
- フラグメントパケットの欠損や、UDPパケットのフラグメントを許容しないNW機器の破棄などによる、後続パケット待ちタイムアウトから解放される
- TCの増加により、TCPのクエリーが増えるかも
- TCPのクエリーに応答しない権威サーバーの管理するドメインが引けなくなるかもしれない

どうすればいい？

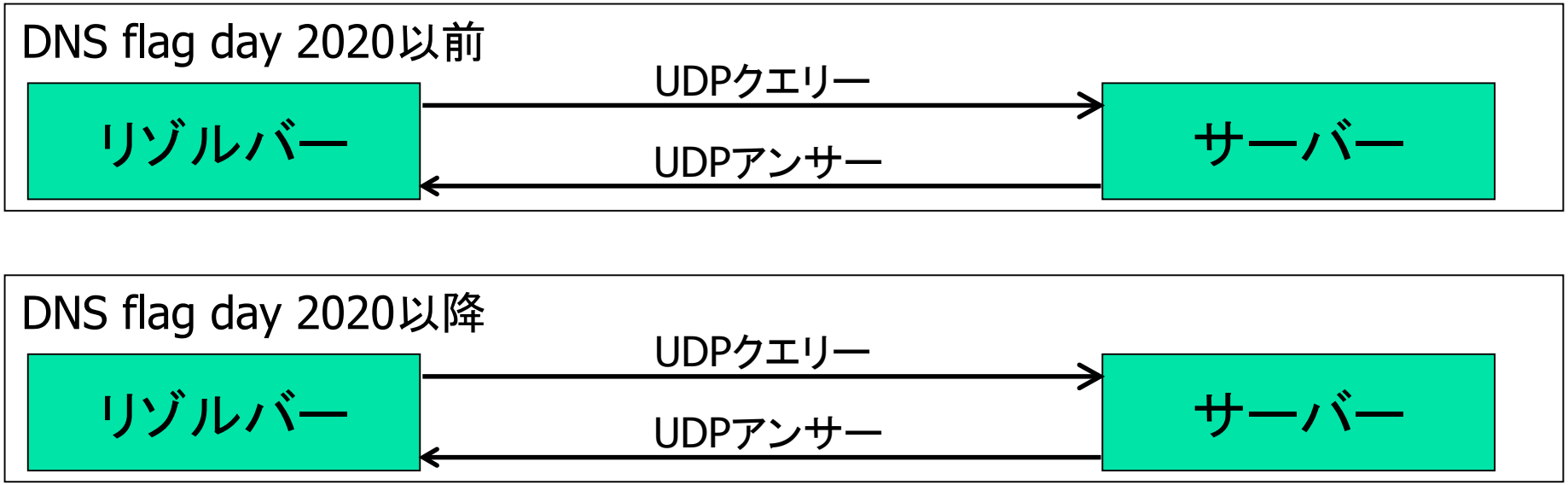
- サーバーがTCPのクエリーに応答するか確認
- リゾルバーがTC応答に対し、TCPにフォールバックするか確認
- トラフィックモデルが変わることが想定されるので必要に応じて検証、チューニングを検討

どうなるのかもう少し具体的に

- どこが変更されるのか
- リゾルバーのEDNS0に含まれるUDPペイロードサイズが変更される
- 推奨値である1232オクテットになると思われる
  - IPv6必須MTU-(IPv6+UDPヘッダー)=1280-48=1232
- 多くの実装で4096オクテットがデフォルト値になっており、縮小になる
  - 以降は現状UDPペイロードサイズが4096オクテットで動作している前提

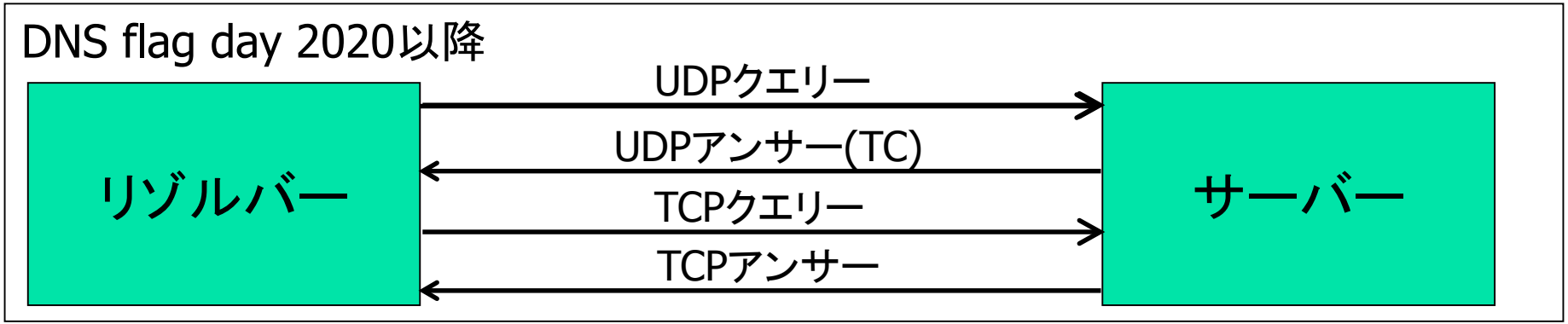
どうなるのかもう少し具体的に

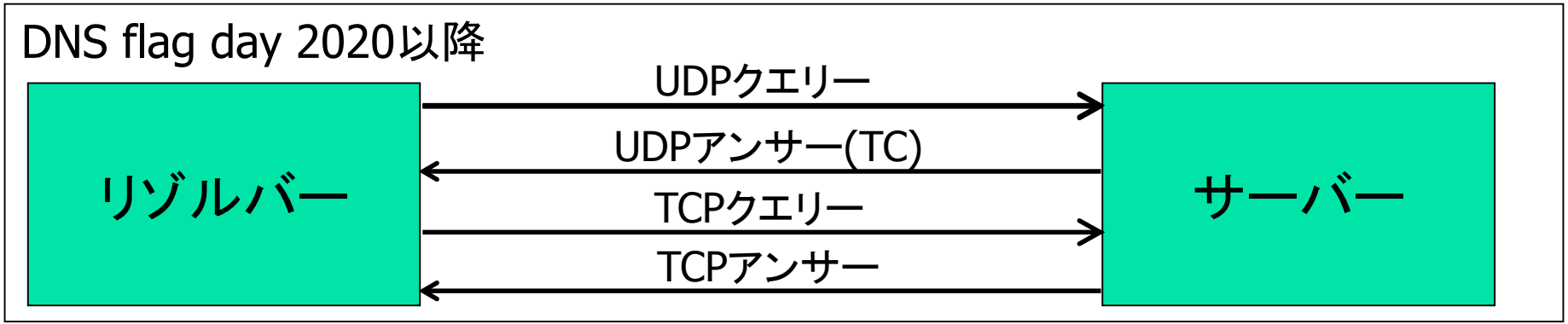
- どうなる(1232オクテット以下の応答)⇒変更なし



どうなるのかもう少し具体的に

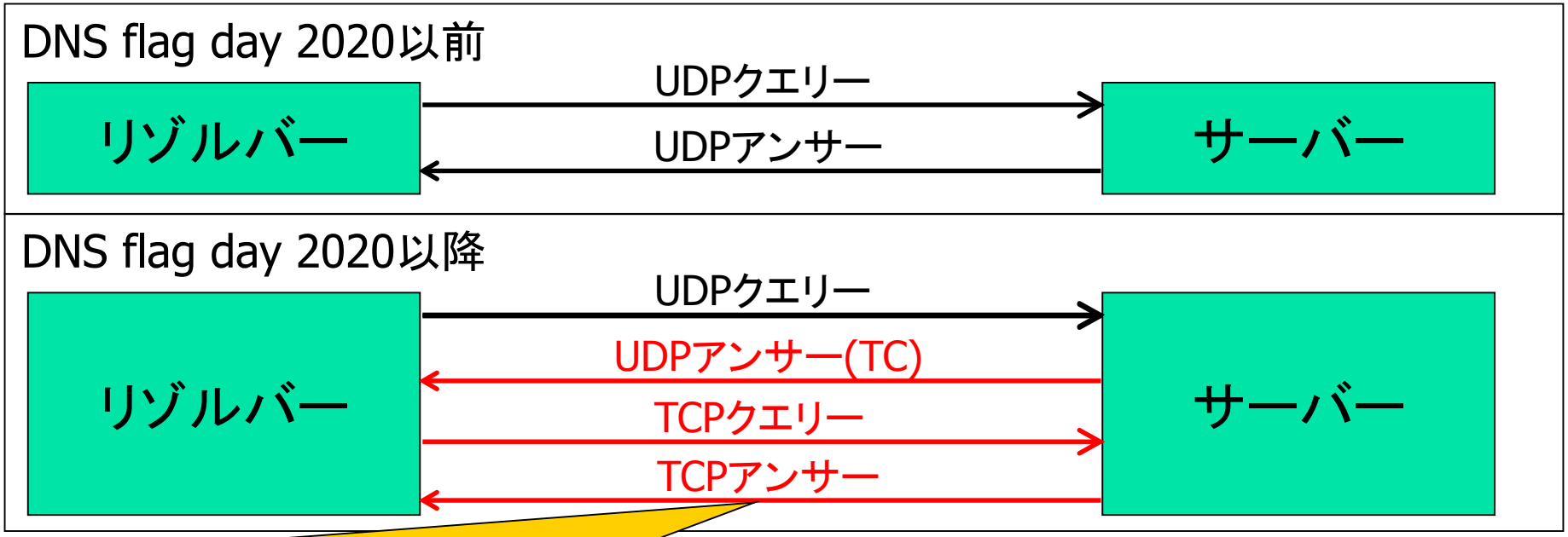
- どうなる(4096オクテット超の応答) ⇒変更なし





どうなるのかもう少し具体的に

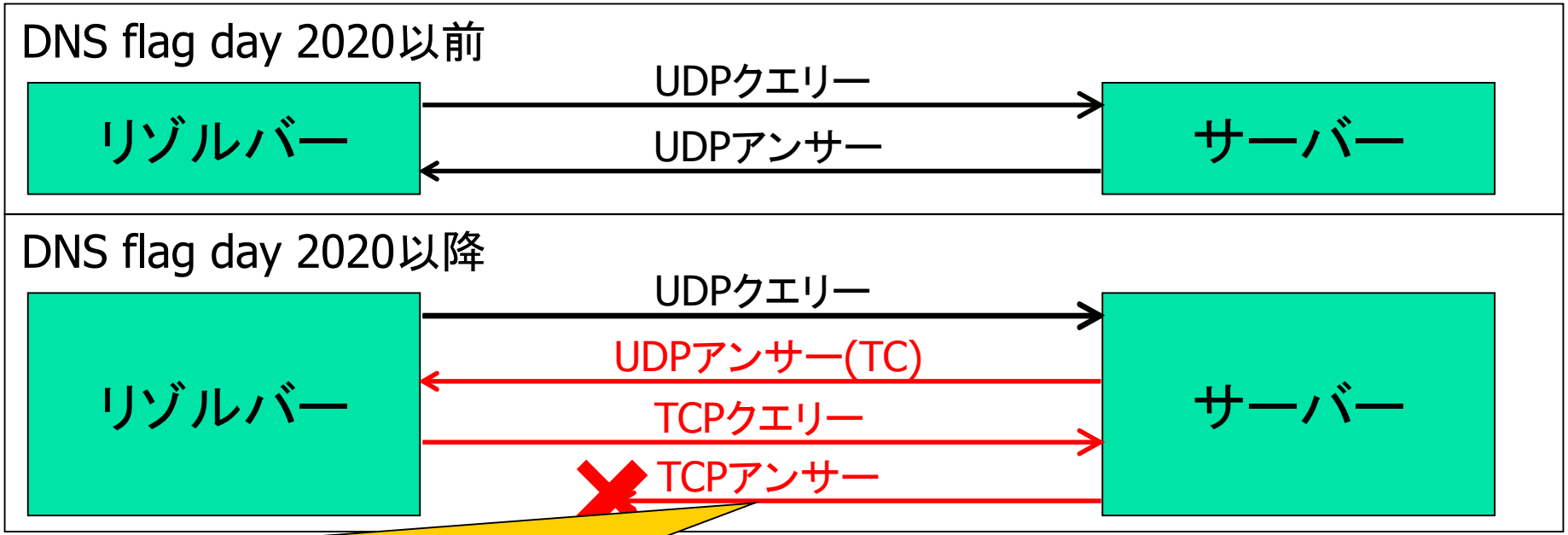
- どうなる(1232～4096オクテットの応答)
  - TCPに応答するサーバーの場合



UDPで名前解決できていたのが、TC応答により、TCPにフォールバックする。

どうなるのかもう少し具体的に

- どうなる(1233～4096オクテットの応答)
  - TCPに応答しないサーバーの場合



TCPにフォールバックする上、名前解決できなくなる。

どうなるのかもう少し具体的に

- 応答サイズが1233～4096オクテットのクエリーがTC応答するようになる
  - TCPにフォールバックするのでTCPのクエリーが増加する
- TCPに応答しないサーバーは名前解決できなくなる
  - とはいえ現状でも4096オクテット超の場合にはすでに名前解決できない状態であるはず
- ゾーン転送はほぼ影響がないはず
  - AXFRは始めからTCP、IXFRはUDPの実装が多分ない
  - SOAは署名付きだと1232を超えるかも、Notifyは……

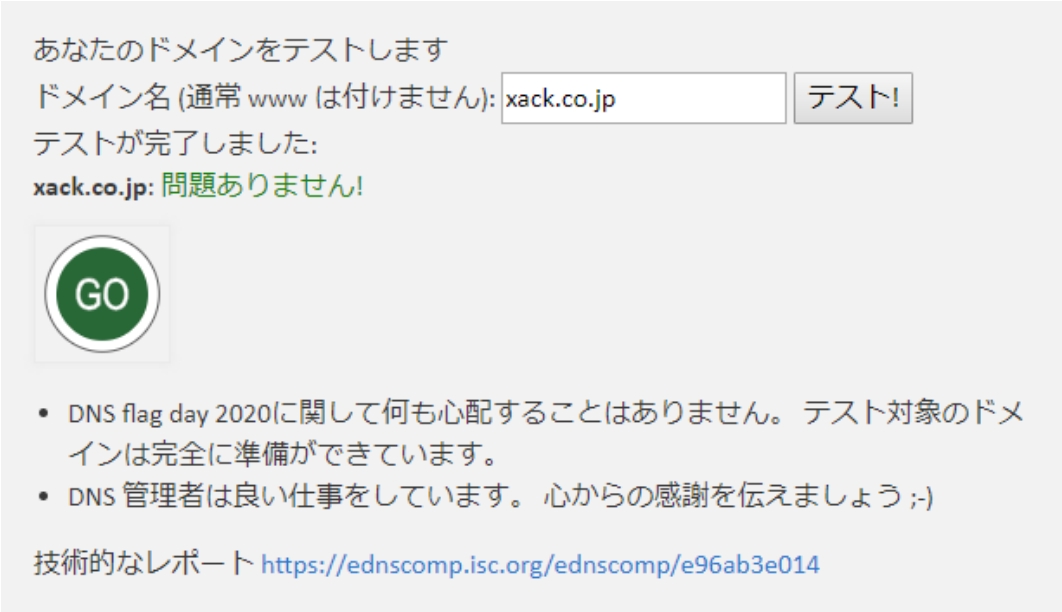
どうすればいいかもう少し具体的に

DNSサーバー運用者(権威サーバー)

■ ひとまず影響ありかは公式ツールでチェック可能

https://ednscomp.isc.org/ednscomp

https://dnsflagday.net/



どうすればいいかもう少し具体的に

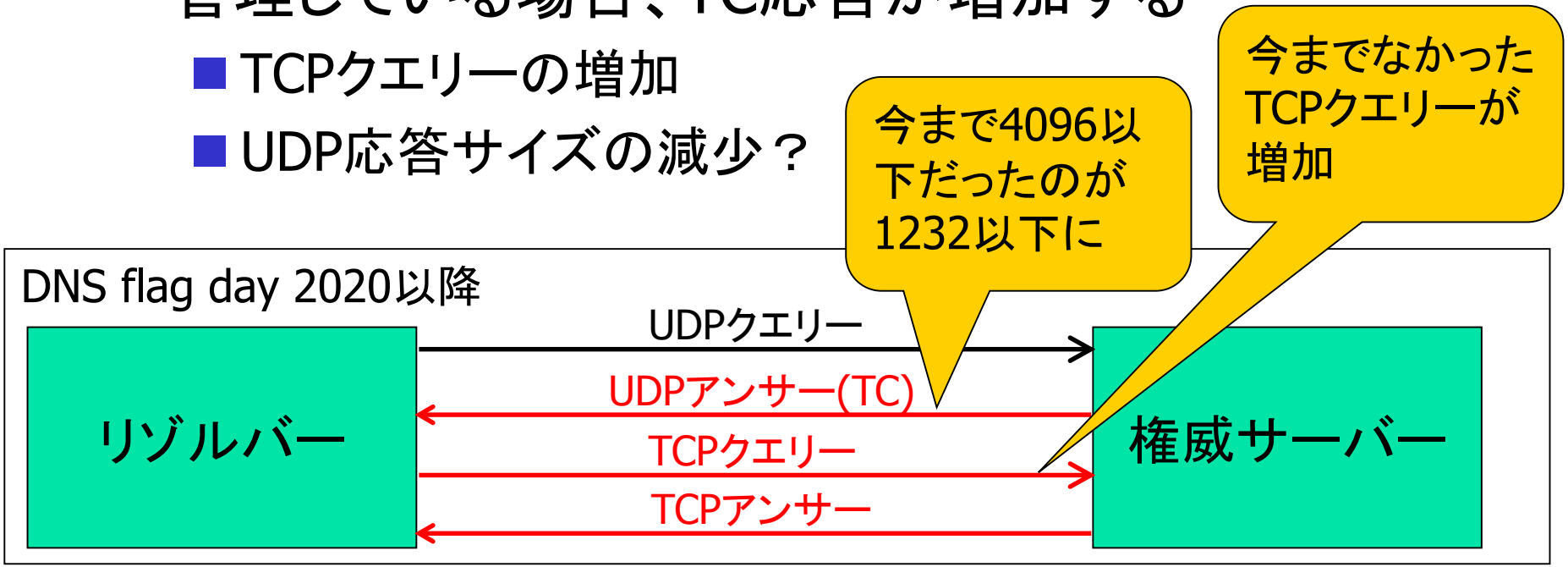
DNSサーバー運用者(権威サーバー)

- TCP/53で応答することを確認する
  - dig +tcp @auth_IP yourdomain.example
  - ブロックするFWもあるので忘れずに
- MTUが1280以上であることを確認する
  - 1280未満だとフラグメントしなくなる、という効果を享受できないかも
- (EDNS0のUDPペイロードサイズを1232に変更する)

どうすればいいかもう少し具体的に

DNSサーバー運用者(権威サーバー)

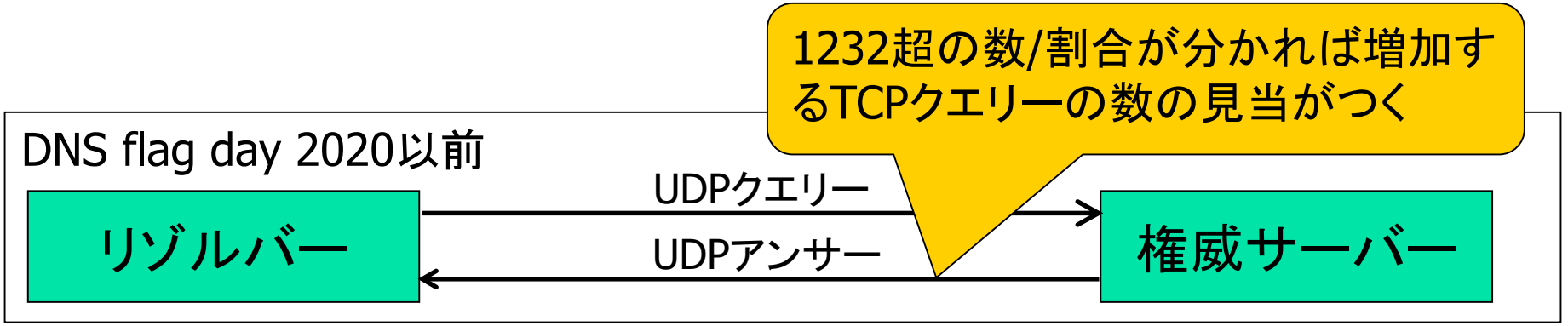
- 応答サイズが1232オクテットを超えるようなゾーンを管理している場合、TC応答が増加する
  - TCPクエリーの増加
  - UDP応答サイズの減少？



どうすればいいかもう少し具体的に

DNSサーバー運用者(権威サーバー)

- 現状のトラフィックを把握すると、DNS flag day 2020前後の変化がある程度予測できるのでは
  - ソケット数やFWのセッション数などチューニング
  - minimal-responseで応答サイズを小さくするのもありかも



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)

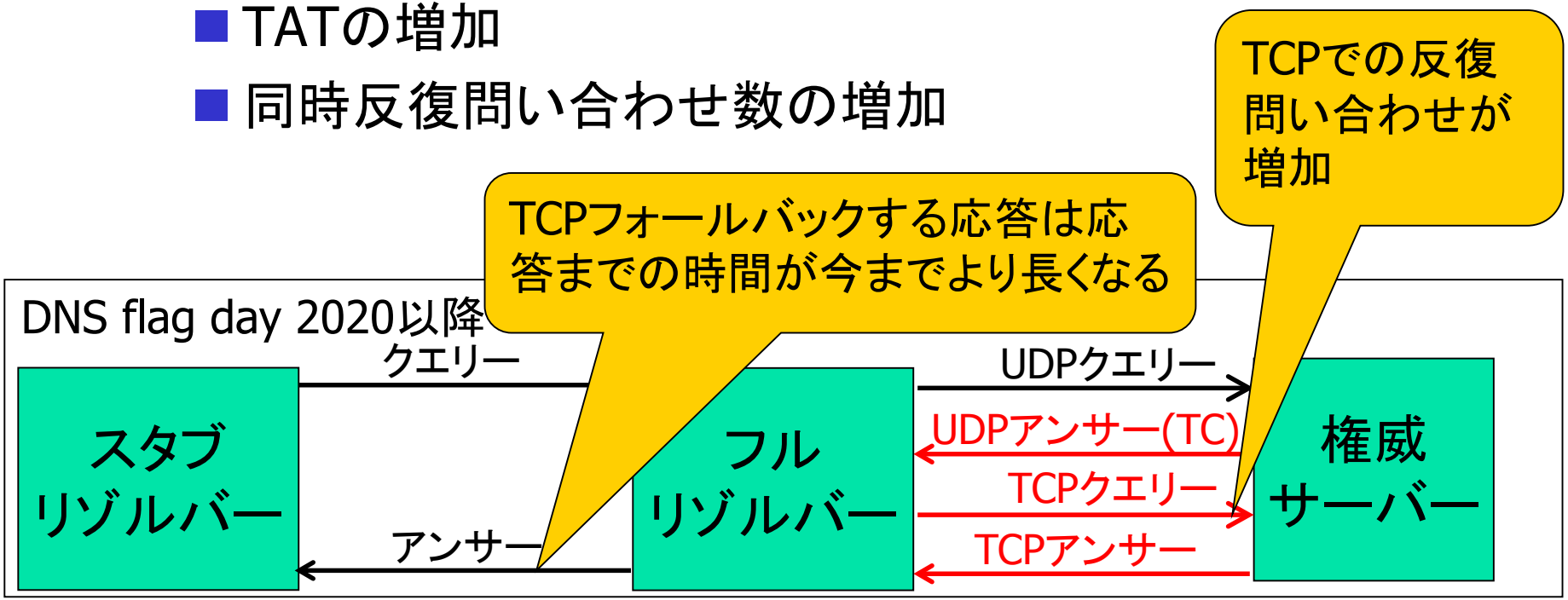
- 基本的には権威サーバーと同じ
  - TCP/53、MTU、UDPペイロードサイズ

- 加えてTC応答に対して、TCPフォールバックするか確認する
  - dig @resolver_IP test.knot-resolver.cz. TXT

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)

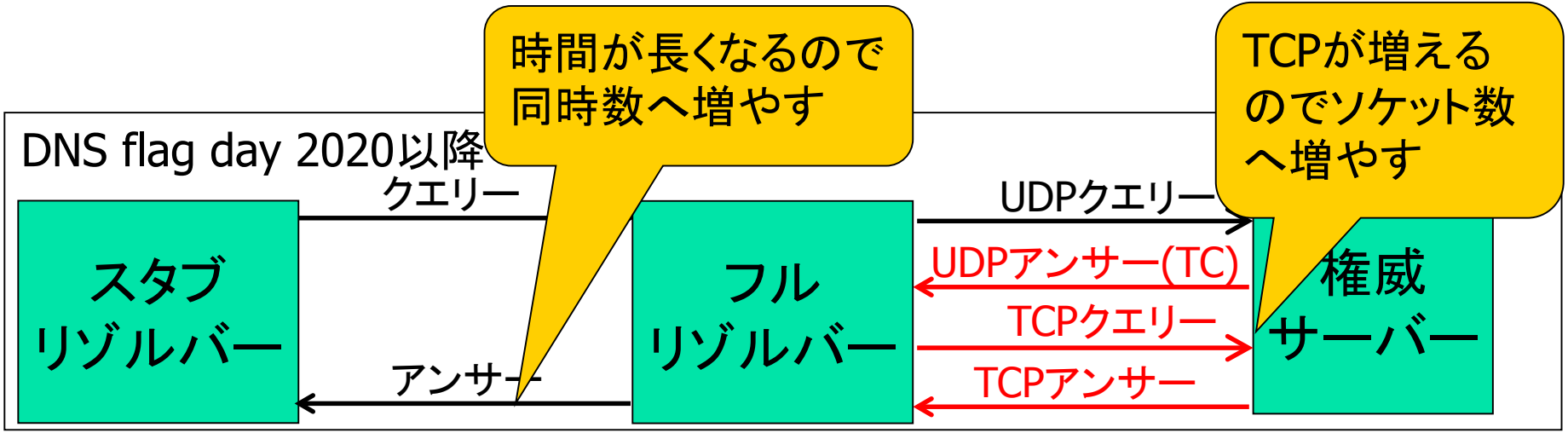
- TCPによる反復問い合わせが増えるはず
  - TATの増加
  - 同時反復問い合わせ数の増加



どうすればいいかもう少し具体的に

DNSサーバー管理者(フルリゾルバー)

- 場合によってはチューニングが必要
  - BINDならrecursive-clients、reserved-sockets
  - Unboundならnum-queries-per-thread、outgoing-num-tcp



どうすればいいかもう少し具体的に

DNSソフトウェア製品ベンダー

- 標準規格に準拠しましょう
  - RFC7766
  - RFC6891
  - 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 2020に賛同するなら、UDPペイロードサイズのデフォルト値を1232に、ただし設定可能とすることも重要

まとめ

- 時期未定ですが、そのうちEDNS0のUDPペイロードサイズのデフォルト値が1232オクテットに変更されます
- 基本的によい方向に修正されるはずですが、一部名前解決ができなくなることが懸念されています
- 事前に検証、対応できることはしておきましょう

https://xack.co.jp