

# ■ DNS flag dayの概要・影響と対応状況の確認方法

(最終更新:2019年1月28日)

## ▼DNS flag day の概要

2019年2月1日は主要なDNSソフトウェアベンダーとパブリックDNSサービス事業者が参加する「DNS flag day」の開始日です。DNS flag dayは、その日(2019年2月1日)以降にリリースするDNSソフトウェア・サービスからEDNS0に関するワークアラウンド処理を削除することで、DNSの品質・パフォーマンスの向上と、新機能の導入・拡張機能の推進を図るためのイベントです。

DNS flag dayの対象は、2019年2月1日以降に参加組織からリリースされるDNSソフトウェアとパブリックDNSサービスです。運用中のDNSソフトウェアの動作は、2019年2月1日以降も変わりません。

## ▽EDNS0の概要

EDNS0は、RFC 6891で定義されるDNSの機能拡張方式です。DNSSECやDNSのIPv6対応をはじめとするさまざまな機能拡張に対応するため、512バイトを超えるDNSメッセージを通信コストの低いUDPで扱えるようにし、フラグや応答コードを拡張・追加します。

最近の主なフルリゾルバー(キャッシュDNSサーバー)はEDNS0に標準で対応しており、EDNS0機能を有効にした問い合わせを権威DNSサーバーに送信します(図1)。

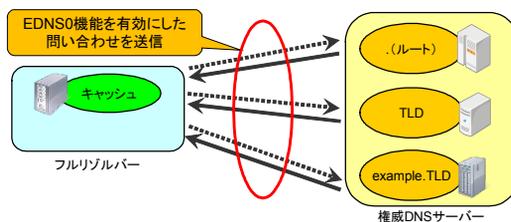


図1 EDNS0機能を有効にした問い合わせを送信

EDNS0では、フルリゾルバーと権威DNSサーバーの双方がEDNS0に対応する必要があります。また、通信途中のネットワーク機器がEDNS0機能を有効にした問い合わせ/応答を、適切に中継する必要があります。

## ▽ワークアラウンド処理

送信先の権威DNSサーバーや通信途中のネットワーク機器がEDNS0に対応していないことで、応答が得られない場合があります。主要なDNSソフトウェアでは応答が得られなかった場合、EDNS0機能を無効にして再問い合わせする「ワークアラウンド処理」が実行されています(図2)。

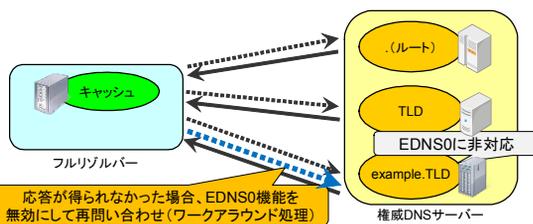


図2 EDNS0機能を無効にして再問い合わせ

この処理が、2019年2月1日以降にリリースされる主要なDNSソフトウェアから削除されます。

## ▽DNS flag dayの背景/理由

DNS flag dayの実施に至った背景/理由として、以下の二つが挙げられます。

### ① DNSソフトウェア/サービスの品質とパフォーマンスの向上

ワークアラウンド処理は例外処理であり、バグや脆弱性の要因となります。また、再送処理によりパフォーマンスも低下します。こうした処理を減らして、DNSの安定性と効率向上を図る狙いがあります。

### ② DNSにおける新機能の導入・機能拡張の推進

ワークアラウンド処理は短期的な問題解決手段としては有効ですが、EDNS0を用いた新機能の導入や機能拡張を図る上での障害となります。ワークアラウンド処理を取りやめることでEDNS0への対応を進め、新機能の導入・機能拡張の推進を図る狙いがあります。

## ▼DNS flag day への参加・支持を表明している主な組織・ソフトウェア・サービス

2018年12月27日現在、表1に示すDNSソフトウェアベンダーとパブリックDNSサービス事業者が、DNS flag day への参加・支持を表明しています。

DNSソフトウェアベンダー (DNSソフトウェア名)	CZ.NIC (Knot DNS/Knot Resolver), Internet Systems Consortium (BIND), NLnet Labs (NSD/Unbound), PowerDNS.COM (PowerDNS Authoritative Server/PowerDNS Recursor)
パブリックDNSサービス事業者 (パブリックDNSサービス名)	Cisco Systems (OpenDNS), Cleanbrowsing (Cleanbrowsing DNS), CleanerDNS (Quad9 DNS), Cloudflare/APNIC (1.1.1.1), Google (Google Public DNS)

表1 DNS flag day への参加・支持を表明している主な組織・事業者(組織名のアルファベット順)

## ▼DNS flag day の影響

ワークアラウンド処理が削除されるため、EDNS0に対応していない権威DNSサーバーからの応答が得られなくなる可能性があります(図3)。その結果、特定のドメイン名の名前解決エラーや、名前解決の遅延が発生する可能性があります。

また、通信途中にEDNS0に対応していないネットワーク機器がある場合にも、名前解決エラーや名前解決の遅延が発生する可能性があります(図4)。

該当する機器の例として、EDNS0機能を有効にしたパケットがドロップされる場合や、IPフラグメンテーションにより断片化されたパケットの処理が適切でない場合などが挙げられます。

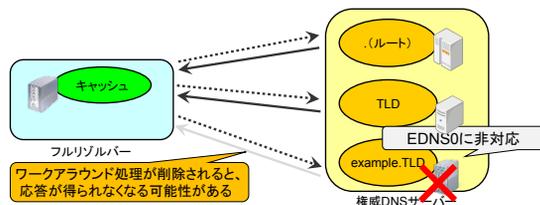


図3 DNS flag day の影響(1)

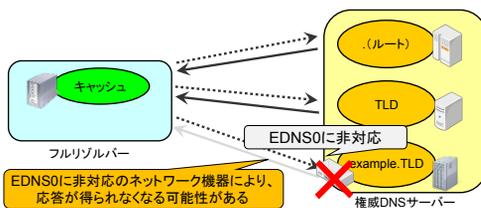


図4 DNS flag day の影響(2)

## ▼対応状況の確認方法

DNS flag dayの公式サイトで、管理対象のドメイン名がDNS flag dayの影響を受ける可能性があるかを確認できます。結果は、「GO」「!」「SLOW」「STOP」の4種類のアイコンで表示されます(図5)。

「SLOW」「STOP」アイコンが表示された場合、そのドメイン名を管理する権威DNSサーバーや、その権威DNSサーバーが接続されているネットワーク機器において、確認・対応作業が必要になります。

	「GO」アイコン: DNS flag dayの影響を受けない
	「!」アイコン: DNS flag dayの影響を受けないが、最新のDNS標準をサポートしていない
	「SLOW」アイコン:(対応作業が必要) DNS flag dayの影響で、名前解決の遅延が発生する可能性がある
	「STOP」アイコン:(対応作業が必要) DNS flag dayの影響で、名前解決エラーが発生する可能性がある

※エラーにより評価できなかった場合、アイコンは表示されません。

図5 公式サイトにおける確認結果とその意味

## ▼参考リンク

- DNS flag day公式サイト  
<<https://dnsflagday.net>>
- DNSソフトウェアベンダー4社(CZ.NIC、ISC、NLnet Labs、PowerDNS.COM)からのアナウンス
  - Together for better stability, speed and further extensibility of the DNS ecosystem | The CZ.NIC Staff Blog  
<<https://en.blog.nic.cz/2018/03/14/together-for-better-stability-speed-and-further-extensibility-of-the-dns-ecosystem/>>
  - End to Band-aids for Broken EDNS | Internet Systems Consortium  
<<https://www.isc.org/blogs/end-to-band-aids/>>
  - NLnet Labs - News - Putting an End to Workarounds for Broken Software  
<<https://www.nlnetlabs.nl/news/2018/Jun/07/putting-an-end-to-workarounds-for-broken-software/>>
  - Removing EDNS Workarounds | PowerDNS Blog  
<<https://blog.powerdns.com/2018/03/22/removing-edns-workarounds/>>