NextDNSを運用してみた
― NISOC編 ―

新潟インターネット研究会
神保道夫

NextDNSとは？

- Cloudflareの「1.1.1.1」や、Googleの「Google Public DNS」と同じような、Public DNSサービスに近い位置付け
- サービスラインナップとして「Free」「Pro」「Business」「Education」があります。
- 個人で本格的に利用するためには、250円/月 もしくは2,500円/1年の費用を払う必要がある(Proの場合)
- 無料(Free)でも利用できるが、300,000クエリ/月の制限があり、この制限に引っかかると、利用制限がかかる
- では、NextDNSを利用するメリットはどこにあるのでしょうか？

NextDNSで利用できる主な機能(1)

- 通常のDNSクエリに加えて、DoH(DNS over HTTPS) や、DoT(DNS over TLS)といった、DNSクエリの暗号化にも対応しています。
- DNSのクエリに対してのログを取る事ができます(クライアントIP、ドメインなど、最大2年のログを保存できる様だ)。
ログの保存先は、アメリカ及びヨーロッパ圏内で選択可能。
- ログをサーバーサイドで分析する事が可能。
- 任意のドメインのDNS応答を変更可能

NextDNSで利用できる主な機能(2)

- ブロック機能の充実
  - ・トップレベルドメインレベル
  - ・任意のドメイン名での応答拒否
  - ・DNSやアプリ、ゲーム単位
  - ・カテゴリ別(ポルノ、ギャンブル・出会い系サイト等)

その他、多数のレベルでの機能が充実しています。

これらの機能を利用する事により、ネットを安全に利用する事ができます。

NextDNSを利用する方法

- 利用する方法として、大きく分けて
  「ブラウザレベル」・・・簡単
  「OSレベル」・・・条件が厳しいかも？
  「リゾルバを変更する」
  という方法が考えられます。
- 次からは、具体的な利用例を説明します。

ブラウザレベルでの設定(1)

- Firefoxを使用している場合、「ツール」→「オプション」→「一般」→「ネットワーク設定」→「接続設定」を開くと、「DNS over HTTPSを有効にする」という項目があり、この中の「NextDNS」の項目があります。
- この項目はあくまで「DoH」を有効にするだけのため、前述の機能を使用する場合は「URLを指定」を選び、my NextDNSで指示されるURLを記載します。
- アドレスバーに「about:config」を入力し、「network.trr.mode」の設定値を3に変更します。

ブラウザレベルでの設定(2)

- Google ChromeやMicrosoft Edgeでは「設定」→「プライバシーとセキュリティ」→「セキュリティ」→「詳細」→「セキュアDNSを使用する」を有効にし、「次を使用」を選択後、「カスタム」を選び、指示されたNextDNSのURLを入力します。
- Microsoft Edgeでも「設定」→「プライバシー、検索、サービス」→セキュリティ」→「セキュアDNSを使用する」を有効にし、「サービスプロバイダを選択」後、NextDNSのURLを入力します。

OSレベルでの設定

- Windows10 Insider Preview Build 19628以降で、DNS over HTTPS機能に対応しました。
- 現在のビルド(2020/11/24現在では、Build 20261)では、コマンドプロンプトを利用して、WindowsにNextDNSのURLを登録する事により、DoHを利用したDNSクエリを出す事ができる様になります。

  netsh dns add encryption server=<your-server's-IP-address> dohtemplate=<your-server's-DoH-URI-template>

リゾルバを変更する

- 自前のリゾルバを使用する事ができる場合、次の様な手順でNextDNSを利用する事が可能です。
- 私の環境では、FreeBSD 12.2-RELEASEに「unbound」をインストールし、unbound.confのforwarderとしてNextDNSを利用する様に変更し、常時NextDNSを利用しています。
- 「nginx」をpkgでインストール＋設定後、「ports/dns/doh-proxy」を自前でmakeすることにより、DoH機能を利用

といった事を実現しています。DoH機能に関しては、リソース的制約から、現状はDoTによる運用をしています。

NextDNSの応答速度について

- IPv4のRTTは、国内にサーバーがある様に見えるため、そんなに遅くない(さくらインターネットから1.2ms位)
- IPv6のRTTは、USあたりまでいってしまう様だ(さくらインターネットから150ms以上)
- ForwarderにIPv6アドレスを書いてしまうと、応答が悪くなる様ですね･･･。
- とはいえ、あまり体感上の遅さは感じません。
  自宅内のリゾルバでクエリーをキャッシュしているので、自分一人で使用する分には、気にする必要はなさそうです。

NextDNSの副作用

- フィルタによって、本来見る事のできるはずのサイトが見れなくなってしまう。
  例1）障害）　Tverで、視聴前に表示されるアンケートに答えないといけないが、画面が表示されない。動画自体が再生されない。
  解決法）googleadmanager.com を許可リストに設定しないとダメ？
  例2）障害）　iPhoneのiOSアップデートができない
  解決法）*.apple.com.akadns.netを許可リストに設定しないとダメ？
- よくわからないトラブルが出た際は、ブロックされたクエリを元にサイトを特定し、許可リストに加える必要がある様だ。

まとめ

- NextDNSを利用すると、お手軽に広告サービスの遮断やドメイン単位のブロックを行う事が可能です。
- 運用してみると、遮断した事による副作用もあり、お手軽に運用する事は難しいかもしれない、という印象です。

参考URL

- Windows10でのDNS over HTTPSの設定方法
  https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282
- FreeBSDでのDoHの利用イメージ
  https://wordpress.metro.cx/2019/07/10/running-a-dns-over-https-endpoint-on-freebsd-doh/
- NextDNS
  https://nextdns.io/
- My NextDNS
  https://my.nextdns.io/