WebサーバのDNSへの登録方法が変わるよ

山口崇徳@IIJ

JANOG48 LT

こんなふうに変わるよ

```
https://example.com/
```

- これまで

```
example.com.        IN A      192.0.2.1            ; アクセスされるIPアドレスを設定
                    IN AAAA   2001:db8::1
```

- これから

```
example.com.        IN HTTPS  1 svr.example.com.  ; アクセスされるホスト名を設定
svr.example.com.    IN A      192.0.2.1            ; そのホスト名のIPアドレスを設定
                    IN AAAA   2001:db8::1
```

new!

HTTPSレコードってのができるよ

- draft-ietf-dnsop-svcb-https
  - SVCB(汎用版)とHTTPS(HTTP専用)の2つのリソースレコードを定義
  - dnsop WGでの議論はすでに終了し、正式にRFCになるのを待つばかり
- まだ正式なRFCにはなってないが、すでに使われている
  - Safari (iOS、macOS)はデフォルトで使いまくってる
  - Firefox、Chromeはデフォルトではないが実装済み
  - CloudflareにホスティングされているサイトはHTTPSレコードが登録されている
  - 観測されているクエリ数はすでにA、AAAAについで3番目の量

HTTPSレコードの機能

- ゾーン頂点(ゾーン名自身)でも使える別名
  - CNAMEは制限があってゾーン頂点では使えなかった
- MXやSRVのような優先度によるサーバ選択
- Webサーバに接続する前に知っておくべき情報をDNSで事前通知
  - 対応しているHTTPバージョン
  - Encrypted Client Helloの公開鍵
    - TLSハンドシェイク初期にこれまで平文でやりとりされていた情報を暗号化するTLS1.3拡張
- …など

典型的な利用例

https://example.com/

```
; ドメインオーナーはWebサイトの別名をCDNサービスに向ける
example.com.      IN HTTPS 0  cdn.example.net.
```

優先度0はエイリアスモード(ゾーン頂点でも使える別名)

優先度0以外はサービスモード(優先度にしたがったサーバ選択)

サービスパラメータ(key=value形式のリスト)

```
; CDNサービスは具体的な構成情報を記載
cdn.example.net. IN HTTPS 10 sv1.example.net. alpn=h3,h2 ech=abc…
                 IN HTTPS 20 sv2.example.net. alpn=h3,h2 ech=xyz…
sv1.example.net. IN A     192.0.2.1
sv2.example.net. IN A     192.0.2.2
```

対応HTTPバージョン

ECH公開鍵

ファイアウォール設定の見直しを

- HTTPSレコードの問い合わせパケットを「未知のリソースレコードは怪しい」として捨ててしまうファイアウォールが存在する模様
- HTTPSレコードの仕様では、「中間者攻撃を検知した場合、ダウングレードを避けるためにアクセスをやめるべし(SHOULD)」と規定されている
  - A/AAAAの名前解決ができたとしても、そのサイトにアクセスしなくなる
- 中間者攻撃として認識されなくても、A/AAAAが使われるのはドロップされたHTTPSレコードの名前解決がタイムアウトしてから
- SVCB/HTTPSレコード(Type64/65)はドロップせず通過させるようファイアウォールの設定を変更してください

まとめ

- WebサーバのDNSへの登録方法が変わる
  - まもなくRFCになるHTTPSレコードを利用
  - すでに実用フェイズに入っている
    - 現時点ではSafariがデフォルトで利用
    - Chrome、Firefoxがデフォルトになるまでは、従来のA/AAAAによる登録の方が無難
- とくにファイアウォールでドロップしてないかは今すぐ確認を
- もっと詳しい話はDNS Summer Day 2021の資料を参照
  - https://dnsops.jp/event/20210625/11-yamaguchi.pdf