

Version 6/28

DMM.com Labo

JANOG38@沖縄

**RFC7871ってどうよ
～コンテンツ屋サイドから～**

2016年7月8日

株式会社DMM.comラボ

高嶋隆一

RFC7871: Client Subnet in DNS Queries

以下、
ECS="EDNS Client Subnet"
と省略

Why ECS?

Tailored Response

DNSのA/AAAA等の応答をクライアントのIPアドレスに応じて変更することがある

= “Tailored Response” @RFC7871

Tailored Response (cont.)

例

DNS LB

Akamaiに代表される様なコンテンツ分散に利用されるケース。
IPアドレスと地理情報を結びつけて、近いWebサーバのアドレスを返す等。

内部参照用
サーバ

組織内部からのアクセスと外部からのアクセスで、繋ぎ先を変えたい様なケース。

その他

DoS/DDoSが来たら特定の国からのアクセスを捻じ曲げたい等・・・実際の所の有効性は疑問。

Why ECS?

Tailored ResponseはキャッシュDNSサーバのIPアドレスを元に生成

8.8.8.8に代表される様な広範囲で利用されるキャッシュDNSサーバでは権威DNSサーバ側は区別がつかなくなる

EDNS0 Option で実際のクライアントのアドレスを付加したクエリを送付
=ECS

権威DNSサーバにおけるECS対応状況

UNIX上で動作
するもの

BIND9.11.0以降, PowerDNS
Authoritative Server 3.0以降対応済み。
(KnotDNS, NSDは2016/6時点で未)

アプライアンス

Infoblox対応済み。
F5,A10:L7ルールで対応可能。

DNSサービス

Route53対応済み。(未調査多数)

CDN

Akamai, CloudFront, Azure CDN対応済
み。(未調査多数)

**実際の所、コンテンツ屋は
ECSを使いたいか？**

DMM.comの場合

オンプレの場合

コンテンツ

国別レギュレーションもある為、IPアドレスと国の紐付けによる返す**コンテンツ**をWebサーバが変更。
クライアントは90%が国内。

配信基盤

オンプレは基本的には一地方にのみ配置

オンプレの配信基盤に関してはそもそも Tailored Response 自体を利用していない

DMM.comの場合

CDN利用の場合

コンテンツ

国別レギュレーションもある為、IPアドレスと国の紐付けによる返す**コンテンツ**をWebサーバが変更。
クライアントは90%が国内。

配信基盤

複数のCDN事業者を利用。
CDN側の機能でTailored Responseはもちろん行われている

ECSは関係あるが、顧客が国外には少ない為、DDoSの局所化以外には寄与しなさそう

その他のコンテンツ事業者さんの場合

ECSが欲しいケース

- ✓ コンテンツの利用者が世界中に存在
- ✓ 自社の配信基盤が世界の複数地点に存在
- ✓ 8.8.8.8の用なパブリックDNSの利用者のクライアントに占める割合が高い

のAND条件を持つコンテンツ屋が当てはまるとおもわれる

**殆どの日本のコンテンツ屋だと
オンプレ環境では
ECSは関係ない気がしてきた**

**どうなんでしょう？
CDN事業者さん、
ISPさん、
他のコンテンツ屋さん。。。。**