

ECS(改めRFC7871)ってどうよ? その後

日本ネットワークイネイブラー株式会社 / DNSOPS.JP

石田慶樹

問題意識

JANOG38 (2016年7月)からの進捗はどのような状況か

当時と比べてCDNへの依存はさらに大きくなっている

- ISPにとってはGSLBとエッジキャッシュでトラフィック・コストを削減したい

Public DNSも利用が拡大している

- ISPやエンドユーザの意思に関わらずPublic DNSを利用する局面が増加する可能性

現在の状況についての共有と議論が必要ではないか

本セッションの進行

- ECSの概要と動向 石田
- DNS運用者の立場から 山口
- ISPの立場から 末松
- ディスカッション

ECSの概要と動向

RFC7871

- Client Subnet in DNS Queries
 - Author:
 - C. Contavalli(Google)
 - W. van der Gaast(Google)
 - D. Lawrence(Akamai Technologies)
 - W. Kumari (Google)
 - Category: Informational
 - ISSN: 2070-1721
 - EDNS-client-subnetを以下では ECS と略す。

RFC7871

Table of Contents		
1. Introduction	4	
2. Privacy Note	5	
3. Requirements Notation	5	
4. Terminology	6	
5. Overview	7	
6. Option Format	8	
7. Protocol Description	9	
7.1. Originating the Option	9	
7.1.1. Recursive Resolvers	9	
7.1.2. Stub Resolvers	10	
7.1.3. Forwarding Resolvers	11	
7.2. Generating a Response	11	
7.2.1. Authoritative Nameserver	11	
7.2.2. Intermediate Nameserver	13	
7.3. Handling ECS Responses and Caching	14	
7.3.1. Caching the Response	15	
7.3.2. Answering from Cache	16	
7.4. Delegations and Negative Answers	17	
7.5. Transitivity	18	
8. IANA Considerations	18	
9. DNSSEC Considerations	19	
10. NAT Considerations	19	
11. Security Considerations	20	
11.1. Privacy	20	
11.2. Birthday Attacks	21	
11.3. Cache Pollution	22	
12. Sending the Option	23	
12.1. Probing	23	
12.2. Whitelist	24	
13. Example	24	
14. References	26	
14.1. Normative References	26	
14.2. Informative References	27	
Acknowledgements	28	
Contributors	29	
Authors' Addresses	30	

RFC7871

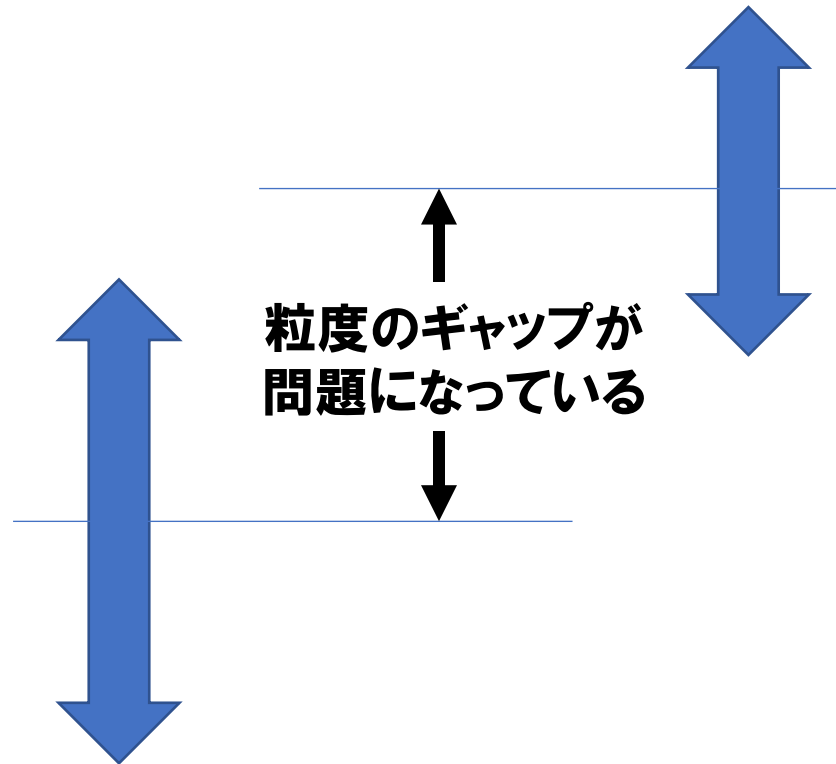
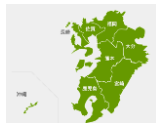
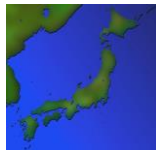
- 登場人物
 - Public DNS Recursive Resolver(Public DNS)
 - Global Server Load Balance (GSLB)
- GSLBの機能
 - 最寄りのコンテンツキャッシュサーバからエンドユーザにコンテンツを配信
- Public DNSの機能
 - フルリゾルバ機能を提供
 - スタブリゾルバからのDNS Queryに応答
 - (多くの場合)Any Castを利用
 - DNSSEC, DoH, DoTなどの付加機能も提供

サーバの粒度(Granularity)の問題

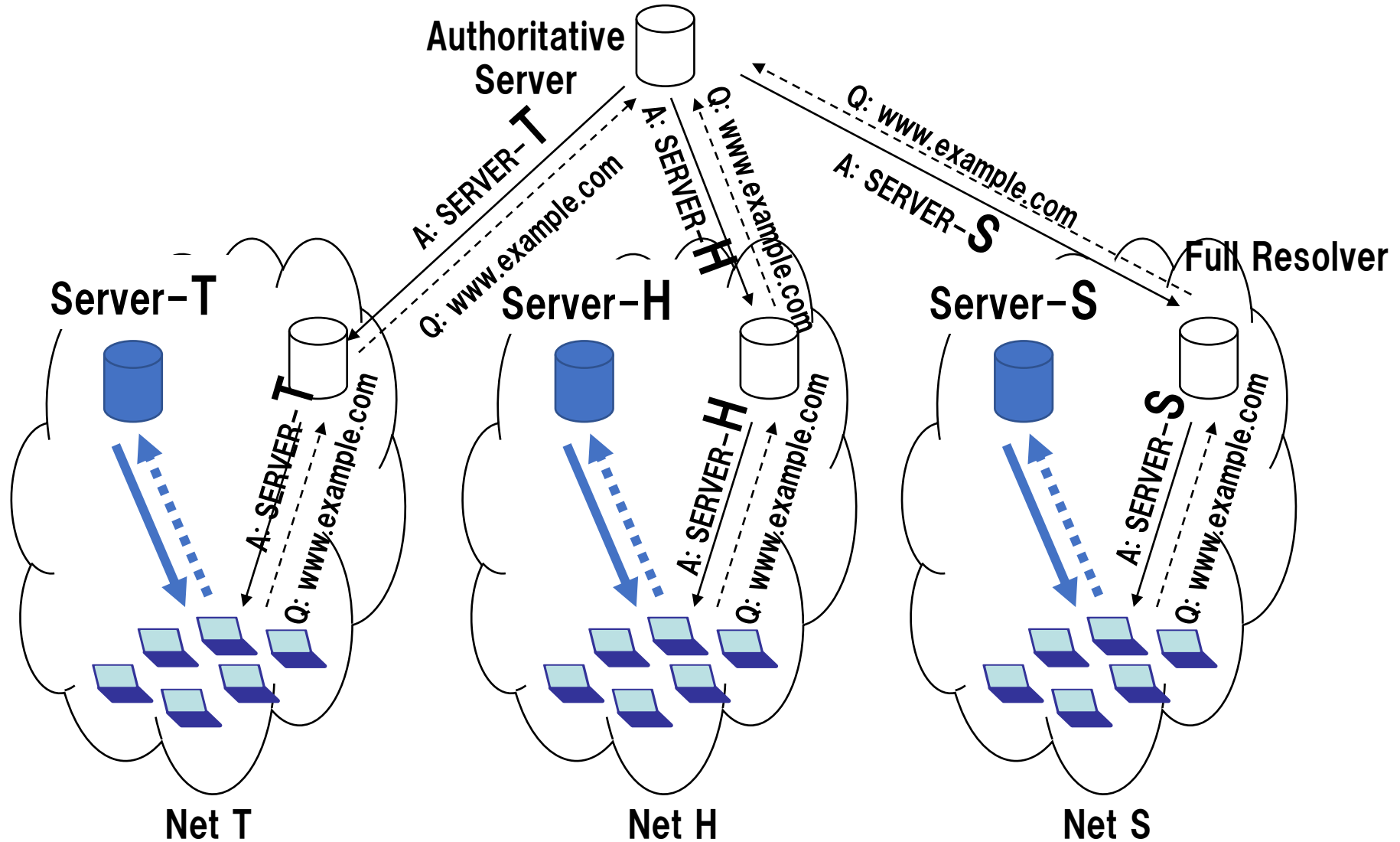
GSLB側
コンテンツキャッシュ
サーバ

Public DNS
(フルリゾルバ)

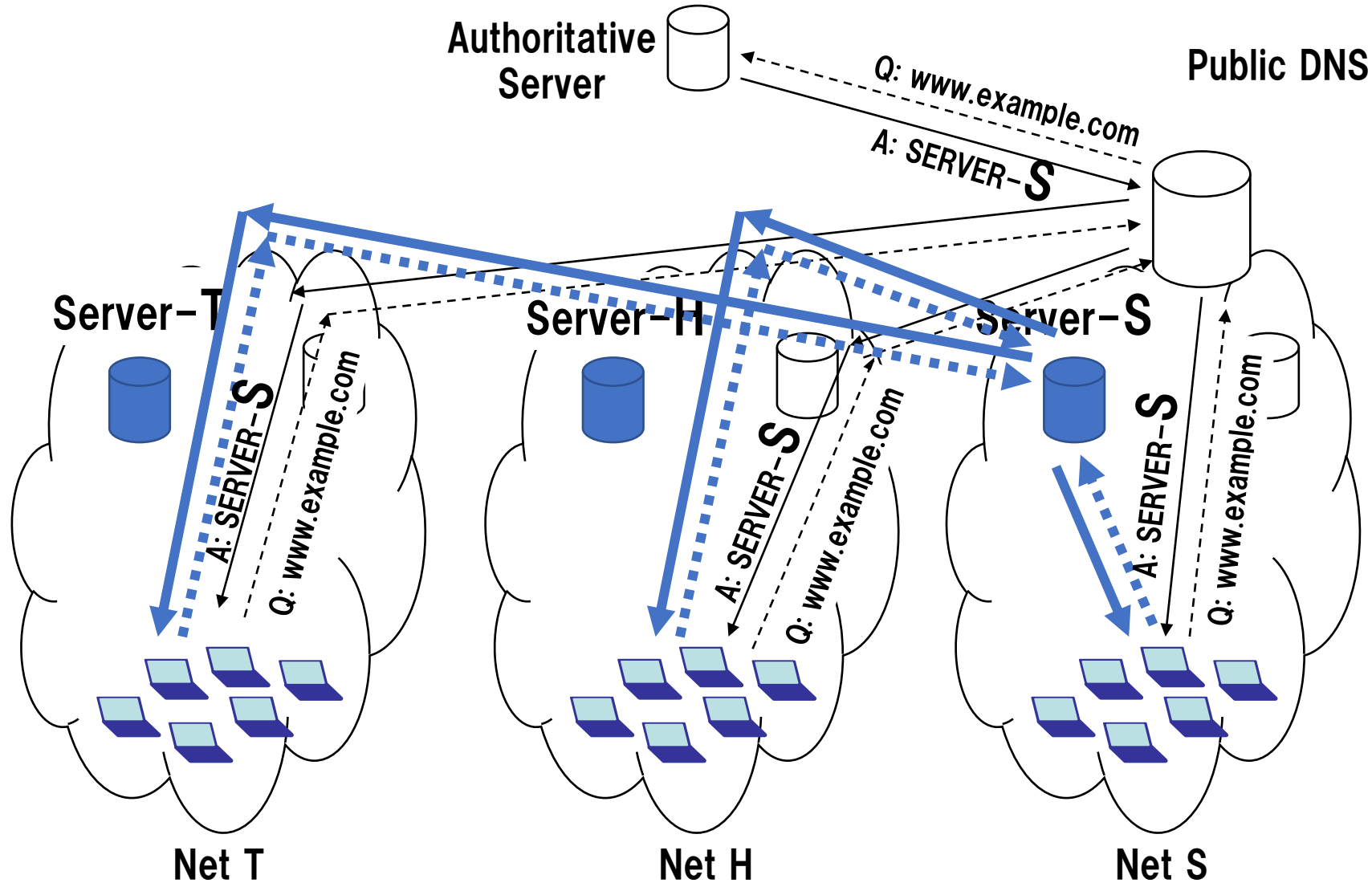
- Global
- Regional
- National
- Local



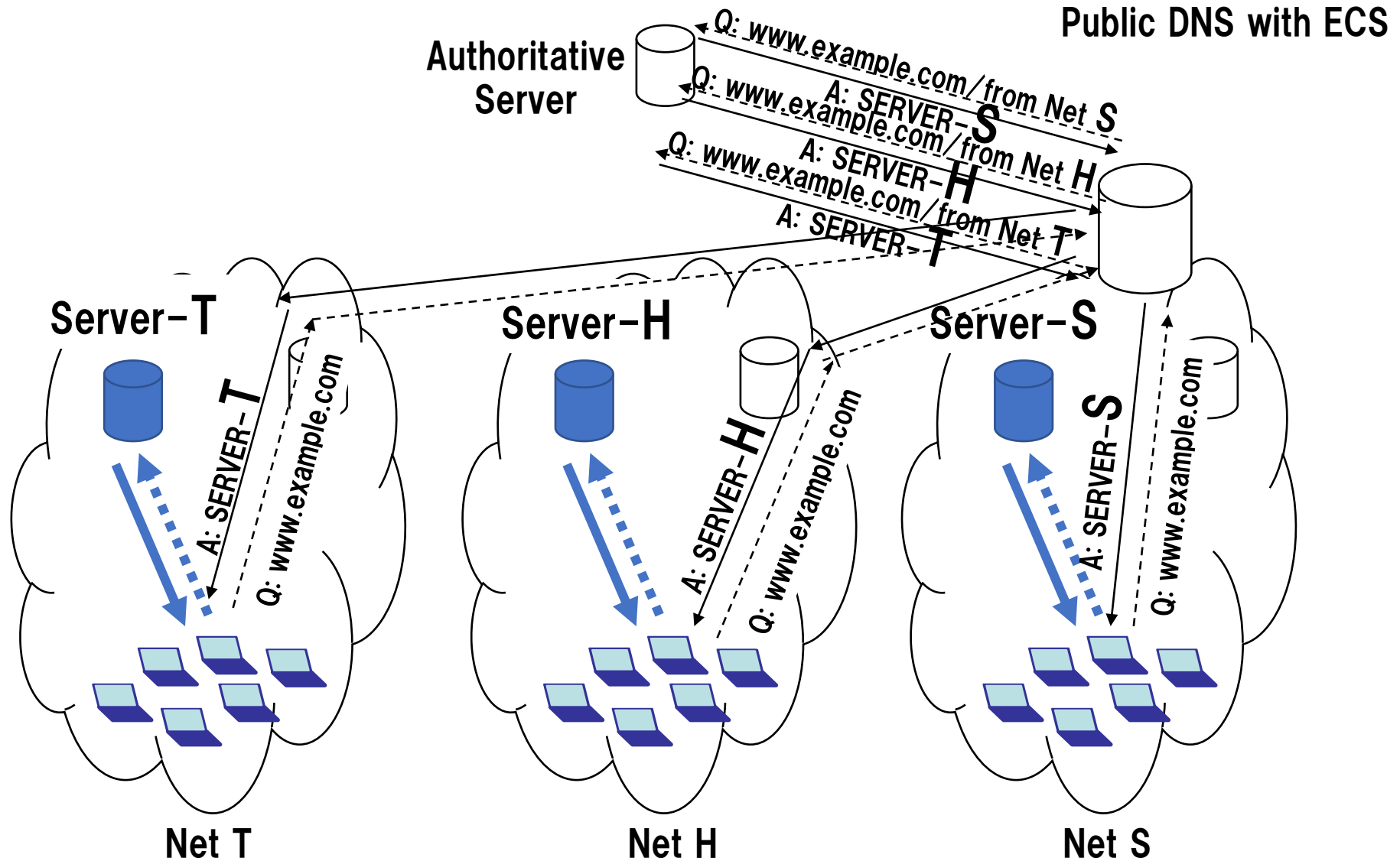
GSLBの仕組みとフルリゾルバの関係



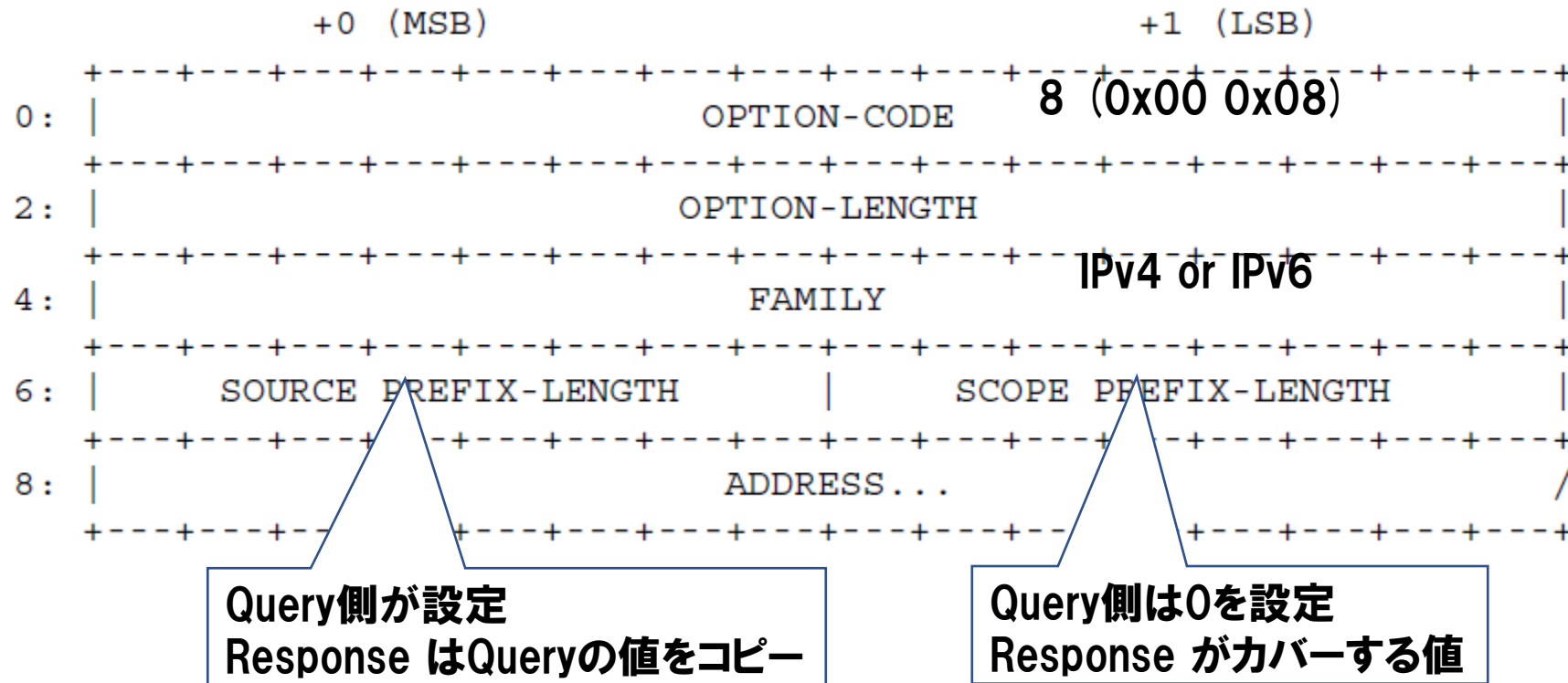
GSLBの仕組みとフルリゾルバの関係



GSLBの仕組みとフルリゾルバの関係



RFC7871 Packet Format



RFC7871への対応

- 権威サーバ側
 - ECSに対してTailored Responseを送信できる機能
- リカーシブリゾルバ側
 - ECSを付加して権威サーバにQueryを送信
 - IPアドレス空間毎にキャッシュする機能

JANOG38以降の状況変化

CDN事業者の増加

- GSLBではなくコンテンツをAnycast化することによりCDNを行っている事業者が大半
- GSLBによるCDNやISPに対してエッジキャッシュを提供している事業者はごく少数

ECSって必要？

Public DNSの増加

- 様々な目的でPublic DNSを提供する事業者が増加
- GoogleとCloudflareが大手だがそれ以外のPublic DNSも使われている
- エッジキャッシュを有するGSLBからのトラフィックが巨大

ECSって必要！

CDN事業者のリスト(Wikipediaより)

Notable content delivery service providers [edit]			
Free CDNs [edit]			
<ul style="list-style-type: none">• cdnjs^{[42][43]}• BootstrapCDN	<ul style="list-style-type: none">• Cloudflare• JSDelivr	<ul style="list-style-type: none">• PageCDN^{[44][45]}• Coral Content Distribution Network (Defunct)	
Traditional commercial CDNs [edit]			
<ul style="list-style-type: none">• Akamai Technologies^[46]• Amazon CloudFront^[46]• Aryaka• Azure CDN• CacheFly• CDNetworks^[46]• CenterServ^[46]• ChinaCache	<ul style="list-style-type: none">• Cloudflare^[47]• Cotendo• EdgeCast Networks• Fastly• Google Cloud CDN• Highwinds Network Group• HP Cloud Services• Incapsula	<ul style="list-style-type: none">• Instart• Internap• LeaseWeb• Level 3 Communications• Limelight Networks• MetaCDN• NACEVI• OnApp	<ul style="list-style-type: none">• Godaddy• OVH• Rackspace Cloud Files• Speedera Networks• StreamZilla• Wangsu Science & Technology• Yottaa
Telco CDNs [edit]			
<ul style="list-style-type: none">• AT&T Inc.• Bharti Airtel• Bell Canada• BT Group• CenturyLink• China Telecom• Chunghwa Telecom• Deutsche Telekom	<ul style="list-style-type: none">• KT• KPN• Level 3 Communications• Megafon• NTT• Pacnet• PCCW• Qualitynet	<ul style="list-style-type: none">• Singtel• SK Broadband• Tata Communications• Telecom Argentina• Telecom Italia• Spark New Zealand• Telefonica• Telenor	<ul style="list-style-type: none">• TeliaSonera• Telin• Telstra• Telus• Turk Telekom• Verizon
Commercial CDNs using P2P for delivery [edit]			
<ul style="list-style-type: none">• BitTorrent, Inc.	<ul style="list-style-type: none">• Internap	<ul style="list-style-type: none">• Pando Networks	<ul style="list-style-type: none">• Rawflow
Multi CDN [edit]			
<ul style="list-style-type: none">• MetaCDN	<ul style="list-style-type: none">• WarpCache^{[48][49]}		
In-house CDN [edit]			
<ul style="list-style-type: none">• Netflix^[50]			

https://en.wikipedia.org/wiki/Content_delivery_network

Public DNSのリスト(Wikipediaより)

https://en.wikipedia.org/wiki/Public_recursive_name_server

Provider						
AdGuard	176.103.130.130	176.103.130.131	176.103.130.132	176.103.130.134	176.103.130.136	176.103.130.137
	2a00:5a60::ad1:0ff	2a00:5a60::ad2:0ff	2a00:5a60::bad1:0ff	2a00:5a60::bad2:0ff	2a00:5a60::01:ff	2a00:5a60::02:ff
CleanBrowsing	185.228.168.168	185.228.169.168	185.228.168.10	185.228.169.11	185.228.168.9	185.228.169.9
	2a0d:2a00:1::	2a0d:2a00:2::	2a0d:2a00:1::1	2a0d:2a00:2::1	2a0d:2a00:1::2	2a0d:2a00:2::2
Cloudflare	1.1.1.1	1.0.0.1	—	—	1.1.1.2	1.0.0.2
	2606:4700:4700::1111	2606:4700:4700::1001	2606:4700:4700::64	2606:4700:4700::6400	2606:4700:4700::1112	2606:4700:4700::1002
Comodo	8.26.56.26	8.20.247.20				
Dyn	216.146.35.35	216.146.36.36				
Google	8.8.8.8	8.8.4.4	—	—		
	2001:4860:4860::8888	2001:4860:4860::8844	2001:4860:4860::6464	2001:4860:4860::64		
Neustar	156.154.70.1	156.154.71.1	156.154.70.2	156.154.71.2	156.154.70.3	156.154.71.3
	2610:a1:1018::1	2610:a1:1019::1	2610:a1:1018::2	2610:a1:1019::2	2610:a1:1018::3	2610:a1:1019::3
OpenDNS	208.67.222.222	208.67.220.220	208.67.222.123	208.67.220.123	208.67.222.2	208.67.220.2
	2620:119:35::35	2620:119:53::53	2620:119:35::123	2620:119:53::123	2620:0:ccc::2	2620:0:ccd::2
OpenNIC	185.121.177.177	169.239.202.202				
	2a05:dfc7:5::53	2a05:dfc7:5::5353				
Quad9	9.9.9.9	149.112.112.112	9.9.9.10	149.112.112.10		
	2620:fe::fe	2620:fe::9	2620:fe::10	2620:fe::fe:10		
Verisign	64.6.64.6	64.6.65.6				
	2620:74:1b::1:1	2620:74:1c::2:2				
Yandex	77.88.8.1	77.88.8.8	77.88.8.2	77.88.8.88	77.88.8.3	77.88.8.7
	2a02:6b8::feed:0ff	2a02:6b8:0:1::feed:0ff	2a02:6b8::feed:bad	2a02:6b8:0:1::feed:bad	2a02:6b8::feed:a11	2a02:6b8:0:1::feed:a11

これ以外にもTWNIC(Quad101), Baidu, Alibaba等も

ECSに関する状況

- Google Public DNS と Akamai 間には実装済み
- DNSソフトウェアでの実装はあまり進まず
 - 権威サーバ・フルリゾルバとも必要としているサーバは少数
- ユーザ・プライバシーに関する議論
 - ⇒JANOG45 「Public DNSとプライバシー」

ECSの今後

- 想定以外のリンクにトラフィックが流れる事象

JANOG45

「SoftBank インターネット&バックボーンネットワークの進化」(會田 英孝)

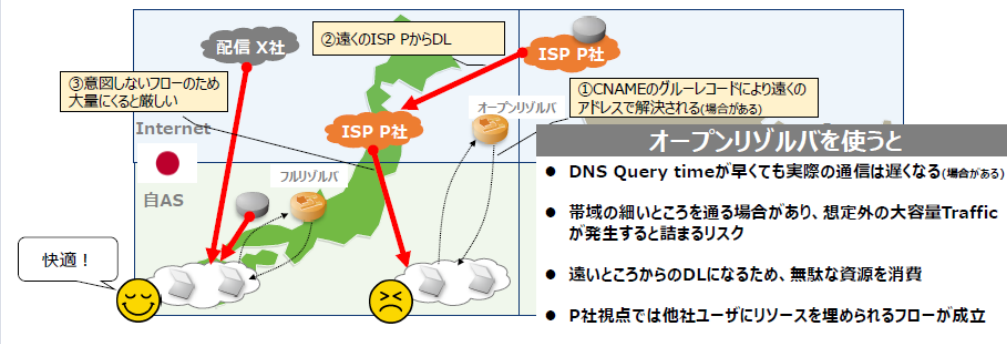
- MECの展開における期待

JANOG45

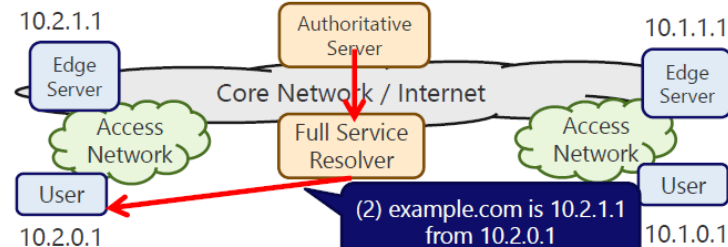
「MEC : Multi-access Edge Computing(こついで)」(宮坂 拓也)

2-4 Internet Trafficフロー

- DNSにまつわる大容量ゲームDL Trafficフロー
 - フルリゾルバ(ISP指定のDNS)を利用 : そのISPにとっての最適な名前解決
 - オープンリゾルバを利用 : 速くの配信元に誘導される場合がある
- ⇒ ECS(EDNS Client Subnet)未対応のオープンリゾルバを使用すると遠回りフローが成立



DNSによるエッジサーバー選択



どのようにして送信元IPアドレス情報を得る?

- EDNS-Client-Subnetにより、送信元IPアドレスブロックを通知
- もしくは、エッジサーバーを設置する単位毎にISPがフルサービスリゾルバを設置し、フルサービスリゾルバの送信元IPアドレスで選択する

ECSの今後

- Public DNSの動向
 - エンドユーザーによる設定
 - 8.8.8.8や1.1.1.1(等)でネットが早くなるという都市伝説
 - 小規模接続事業者によるPublic DNSのデフォルト提供
 - アプリ/ブラウザ/OSによるPublic DNSの埋め込み(DoH/DoT)
- CDNの動向
 - GSLBとエッジキャッシュの展開(バラマキ)
 - vs.
 - Anycastによる提供

本セッションの進行

- ECSの概要と動向 石田
- DNS運用者の立場から 山口
- ISPの立場から 末松
- ディスカッション