Internet インターネット 10分講座

DNSルートサーバ

インターネットを支えるDNS。その起点たるDNSルートサーバの現状をお伝えします。

1. ルートサーバの概要

DNSルートサーバは、インターネットで利用されるDNSにおいて、ツリー構造の起点となるサーバです。ちなみにDNSは、ドメイン名とそれに関する情報を持つ分散データベースです。

ルートサーバはルートゾーンと呼ばれる情報を保持し、インターネット上のDNSクライアントからの問い合わせに対して、この中から必要な情報を取りだしてクライアントに回答する役目を負っています。

```
. NS A.ROOT-SERVERS.NET.
. NS H.ROOT-SERVERS.NET.
. NS C.ROOT-SERVERS.NET.
. NS G.ROOT-SERVERS.NET.
. NS F.ROOT-SERVERS.NET.
. NS B.ROOT-SERVERS.NET.
. NS J.ROOT-SERVERS.NET.
. NS K.ROOT-SERVERS.NET.
. NS L.ROOT-SERVERS.NET.
. NS M.ROOT-SERVERS.NET.
. NS I.ROOT-SERVERS.NET.
. NS E.ROOT-SERVERS.NET.
. NS D.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. A 198.41.0.4
A.ROOT-SERVERS.NET. AAAA 2001:503:BA3E:0:0:0:2:30
H.ROOT-SERVERS.NET. A 128.63.2.53
H.ROOT-SERVERS.NET. AAAA 2001:500:1:0:0:0:803F:235
C.ROOT-SERVERS.NET. A 192.33.4.12
G.ROOT-SERVERS.NET. A 192.112.36.4
F.ROOT-SERVERS.NET. A 192.5.5.241
F.ROOT-SERVERS.NET. AAAA 2001:500:2F:0:0:0:0:F
B.ROOT-SERVERS.NET. A 192.228.79.201
J.ROOT-SERVERS.NET. A 192.58.128.30
J.ROOT-SERVERS.NET. AAAA 2001:503:C27:0:0:0:2:30
K.ROOT-SERVERS.NET. A 193.0.14.129
K.ROOT-SERVERS.NET. AAAA 2001:7FD:0:0:0:0:0:1
L.ROOT-SERVERS.NET. A 199.7.83.42
L.ROOT-SERVERS.NET. AAAA 2001:500:3:0:0:0:0:42
M.ROOT-SERVERS.NET. AAAA 2001:DC3:0:0:0:0:0:35
M.ROOT-SERVERS.NET. A 202.12.27.33
I.ROOT-SERVERS.NET. A 192.36.148.17
E.ROOT-SERVERS.NET. A 192.203.230.10
D.ROOT-SERVERS.NET. A 128.8.10.90

(中略)

COM. NS A.GTLD-SERVERS.NET.
COM. NS G.GTLD-SERVERS.NET.
COM. NS H.GTLD-SERVERS.NET.
COM. NS C.GTLD-SERVERS.NET.
COM. NS I.GTLD-SERVERS.NET.
COM. NS B.GTLD-SERVERS.NET.
COM. NS D.GTLD-SERVERS.NET.
COM. NS L.GTLD-SERVERS.NET.
COM. NS F.GTLD-SERVERS.NET.
COM. NS J.GTLD-SERVERS.NET.
COM. NS K.GTLD-SERVERS.NET.
COM. NS E.GTLD-SERVERS.NET.
COM. NS M.GTLD-SERVERS.NET.

(後略)
```

図1　DNSルートゾーンに含まれるデータの一部

ルートゾーンには、com、org、jp、arpaなどのトップレベルドメイン（TLD）の参照情報が書かれており、具体的にそれぞれのTLDを受け持つDNSサーバがどんな名前であるか、どのようなIPアドレスを持っているか、といった情報が記載されています。DNSクライアントはその情報を元にして、次に問い合わせるべきDNSサーバを把握します※1。

2010年5月現在、ルートゾーンには約280個のTLDとそれぞれのDNSサーバ約1,600個の情報が登録されています（試験用のドメインを含む）※2。

DNSは、ドメイン名（ホスト名）からIPアドレスを求める、メールの送信先サーバを調べるなど、インターネットの通信やサービスに頻繁に利用されるデータベースです。そのため、検索の起点となるルートサーバは非常に重要なものになっています。

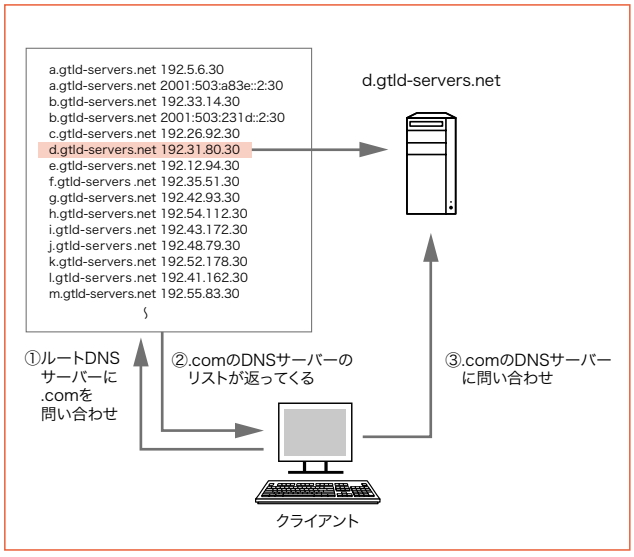
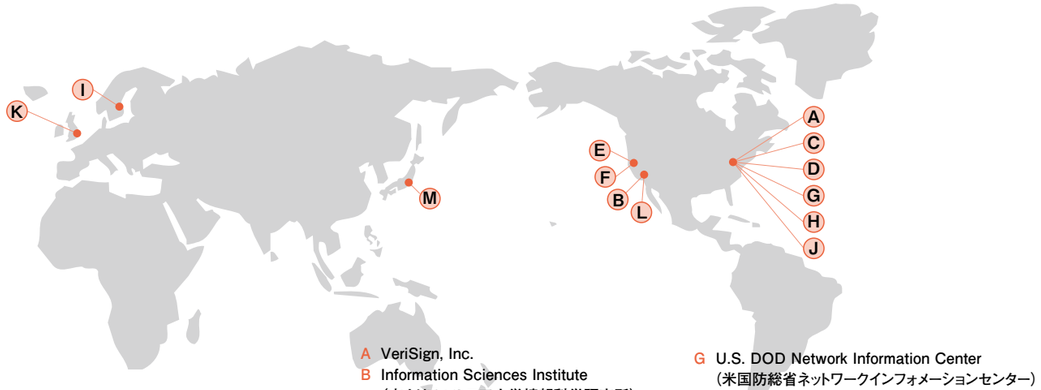


図2　DNSルートサーバは、下位のDNSサーバへの情報を回答する

※1 インターネット10分講座●DNS
http://www.nic.ad.jp/ja/newsletter/No22/080.html
※2 Root Zone Database
http://www.iana.org/domains/root/db/



A VeriSign, Inc.
B Information Sciences Institute
（南カリフォルニア大学情報科学研究所）
C Cogent Communications
D University of Maryland（メリーランド大学）
E NASA Ames Research Center
（米航空宇宙局エイムズ研究所）
F Internet Systems Consortium, Inc.
G U.S. DOD Network Information Center
（米国防総省ネットワークインフォメーションセンター）
H U.S. Army Research Lab（米陸軍研究所）
I Autonomica
J VeriSign, Inc.
K RIPE NCC
L ICANN
M WIDEプロジェクト

図3　各ルートサーバの運用組織と所在地

2. ルートサーバの運用組織

ルートサーバを運用している組織は世界中で12組織あり、VeriSign社が二つのサーバを運用しているため、全部で13のサーバがルートサーバとしてDNSに登録されています。（図3）

ここでルートサーバの数が13となっている理由は、まずDNSプロトコル（RFC 1035[※3]）で規定されたUDPの最大パケットサイズが512オクテットとなっていることが一点。次に、起点となるDNSサーバを問い合わせると、回答の中に、回答自身に責任を持つ権威サーバのホスト名とIPアドレスも含まれます。このセットを512オクテットの中に格納できるのが最大で13エントリという、複合した理由に基づいています。

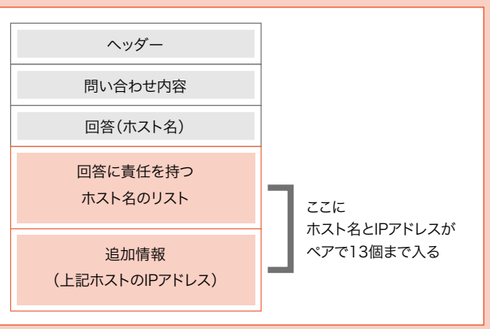


図4　SOAを問い合わせたときの回答パケット概念図

また、これらのAからMまでの英字で区別される13のサーバは、DNS上にルートサーバとして登録されたエントリであり、実際の物理的なサーバの数が13台ということではありません。

なぜなら上記のうち、いくつかの組織は、信頼性や応答性能の向上、ハードウェア障害への対策などの理由から、IPエニーキャスト[※4]技術などを利用して地理的分散や冗長化を行い、同じルートサーバ名（IPアドレス）で複数のサーバを運用しているからです。2010年5月現在、世界中の200以上のサイトでルートサーバが運用されています[※5]。アジア太平洋地域ではF、I、J、K、Mルートサーバが40サイトで稼働しています[※6]。

※3 RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
http://www.ietf.org/rfc/rfc1035.txt
※4 RFC 3258
Distributing Authoritative Name Servers via Shared Unicast Addresses
http://www.ietf.org/rfc/rfc3258.txt
※5 Root Server Technical Operations Assn
http://www.root-servers.org/
※6 APNIC Root server map
http://www.apnic.net/community/support/root-servers/root-server-map

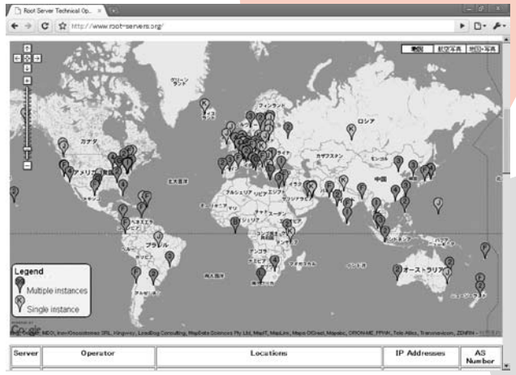


図5　Root Server Technical Operations Assnに表示された、DNSルートサーバの配置図

図6　APNIC Root server mapにある、アジア太平洋地域のDNSルートサーバ配置図

3. IPv6アドレスの追加とDNSパケットサイズ

2008年2月4日、正式にA、F、H、J、K、Mの各ルートサーバにIPv6アドレスが追加されました[※7]。IPv6トランスポートでDNSをサービスしているTLDサーバは以前から存在していたのですが、ルートサーバにはこのとき初めて追加されました[※8]。

ルートサーバへIPv6アドレスを追加することで問題が発生するかもしれないという懸念があったため、その作業は慎重に行われました。

その理由は、IPv6アドレスがルートサーバに追加されるとルートサーバに関する回答のUDPパケットが大きくなり、前述の512オクテット制限を超える可能性があるからです。

例えばルートサーバに関する最新情報を問い合わせた[※9]ときの回答パケットサイズを見てみると、ルートサーバの情報としてIPv4アドレス13個とIPv6アドレスを三つ以上含んだ回答のパケットサイズは、最大サイズの512オクテットを超えてしまいます。

さらに13のルートサーバすべてにIPv6アドレスが付加された場合、IPv4およびIPv6アドレス13個ずつすべて含めて回答されたときのDNSパケットは、サイズが811オクテットになります。

しかしこの懸念については、通常時はIPv4アドレス13個と、ランダムに選択したIPv6アドレス2個の回答を返すようにして512オクテットを超えないようにして対応することが可能です。もちろん、DNSの拡張プロトコルであるEDNS0をサポートし十分に大きなパケットの受信が可能なクライアントに限っては、IPv4およびIPv6アドレスをすべて含んだ回答を返すようにすることでDNSプロトコル上の問題を回避しています。

IPv6アドレス追加による問題発生の懸念としては、ほかに、ルートサーバとDNSクライアントの通信経路間に、古いルータやファイアウォールがあった場合、DNSがうまく利用できなくなることが心配されていました。しかしこの問題は、ベンダー等の協力により解決に向かいました。

※7 IPv6 Addresses for the Root Servers
http://www.iana.org/reports/2008/root-aaaa-announcement.html
JPNIC News letter No.39「ルートサーバ IPv6対応への道」
http://www.nic.ad.jp/ja/newsletter/No39/0320.html
※8 DNSクライアントの持つヒントファイルとルートサーバの持つルートゾーンにそれぞれIPv6アドレスの情報が追加されることを指します。ルートサーバそのものにIPv6アドレスを割り当てることは、実験的に以前から行われていました。
※9 priming response等を指します。SOA問い合わせの制限からDNSルートサーバは13セットですが、priming responseだと13個分のホスト名とIPアドレスを入れても、多少の余裕があるのでIPv6アドレス2個を追加して収納できます。

4. DNSSEC

DNSSECとは、公開鍵暗号方式の技術を用いてDNSの情報に電子署名を施すことができるようにする、DNSの拡張プロトコルです。DNSSECを用いれば、DNSサーバから受け取った情報が正しいものかどうか確認できるようになります。

DNSSECでは、電子署名に関するデータが新たにルートゾーンに追加されることになります。そのデータの大きさはこれまでのルートゾーンの持つデータと比較してかなり大きくなることが予想されており（2010年5月現在、鍵一つに付きデータが数KB、回答パケットが200オクテットほど増加）、サイズの増大による影響がIPv6アドレス追加の時以上に懸念されています。

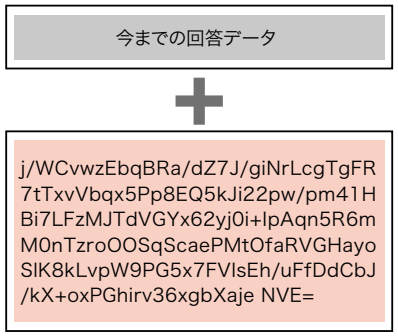


図7　DNSSECによって追加されるデータの例

ルートゾーンへの電子署名については2010年5月現在、ダミーの署名をルートゾーンに行うDeliberately-Unvalidatable RootZone（意図的に検証不能にしたルートゾーン:DURZ）と呼ばれる措置がなされており、ルートゾーンにDNSSECを導入した場合に問題が出るかどうかの確認が行われています。問題ないことが確認できれば、2010年7月15日に正式な電子署名がルートゾーンに対して行われることになっています※10。

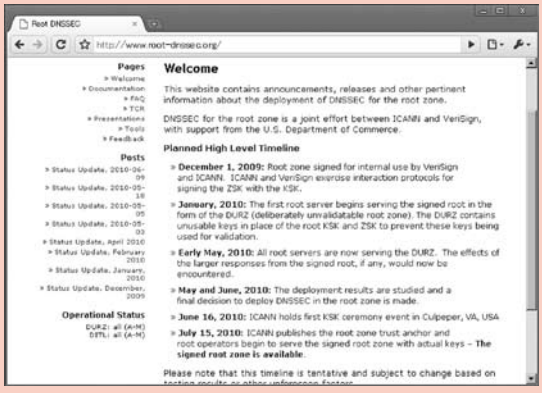


図8　Root DNSSECのWebページに掲載されているDNSSEC電子署名導入スケジュール（2010年6月14日時点）

DNSSECは、子ゾーンの電子署名が正しいことを親ゾーンが保証し、またその親ゾーンの電子署名もさらにその親ゾーンによって保証することで信頼性が成り立っています。DNSの最も上の親となるのはルートゾーンであり、ルートゾーンに電子署名が行われることによってDNS全体でのDNSSEC導入が可能となります。2010年7月以降には、さまざまなTLDにDNSSEC導入がなされることが予想されます。

5. ルートゾーンスケーリング

これまで述べた通り、ルートゾーンへIPv6アドレスが追加され、DNSSECも追加目前です。さらにルートゾーンへのデータ追加要因として、新gTLDおよびIDN TLDがあります。これらの要因による、ルートゾーンのデータ量および更新頻度の増加、さらにその対策について（ルートゾーンスケーリング※11）、ICANNは専門家に調査・予測を依頼した上で2009年9月に報告書を発行しました※12。

同報告書では、サーバの負荷などはさほど問題とされていません。また回線容量は、ゾーンデータ配布の際に途上国などで接続回線の容量が限られているところでは問題になるかもしれないとしています。しかし一番の制約事項は、オペレーターの作業負荷であるとしています。中でもDNSSEC導入によるルートサーバ運用への負荷が大きいため、DNSSECとそれ以外の要素（IPv6、IDN TLD、新gTLD）とを分け、DNSSECを先に導入することを勧告しています。

なお、同報告書の内容や調査実施の経緯、調査における問題点などについては、P.20からの「ICANNによるルートゾーンスケーリング調査について」で取り上げていますので、そちらもぜひご覧ください。

しかし実際は勧告に先んじて、まずIPv6アドレスから導入されました。その後はIDN TLD、新gTLDに先駆けてルートゾーンへDNSSECが導入される予定です。DNS全体への悪影響なしにスムーズな導入となることを期待します。

（JPNIC 技術部 小山祐司/JPNIC インターネット推進部 山崎信）

※10 Root DNSSEC
http://www.root-dnssec.org/
※11 ルートゾーンスケーリングとは
http://www.nic.ad.jp/ja/basics/terms/rootzone-scaling.html
※12 Scaling the Root
http://www.icann.org/en/committees/dns-root/root-scaling-study-report-31aug09-en.pdf