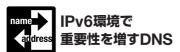
日の性組みと主義制

第8回 DNSをIPv6に対応させる

馬場達也

前回は、DNSメッセージの送信元の認証と通信路上でのメッセージの改ざんの検出を行う、TSIGおよびSIG(0)について解説した。今回は、IPv6ネットワークを構築する際に必要不可欠となる、DNSのIPv6対応について解説する。



現在のIPv4で使用されているアドレスの長さは32ビットであるが、IPv6では、その4倍の128ビットの長さのアドレスを使用する。このIPv6アドレスは、次のように、128ビットのアドレスを16ビットずつ8つのフィールドに分け、その間を「:」で区切り、16進数で表記する。

fec0:0000:0000:0002:0206:5bff:fec7:b6a5

ただし、各フィールド内の最初の「0」は省略することができる。また、0だけから成るフィールドが連続している場合は、1回だけ「::」で置き換えることができる。このルールを適用すると、上記のIPv6アドレスは以下のように簡潔に表現できる。

fec0::2:206:5bff:fec7:b6a5

しかし、実際にIPv6アドレスを手で入力してアクセスするのは、IPv4の場合以上に困難である。このため、IPv6環境ではDNSの役割がさらに重要となってくる。

IPv6環境では、DNSに2つの機能が要求される。1つは、名前解決要求に対して、ネームサーバがIPv6アドレスを返却できることである。この機能は、DNSのリソースレコードの1つである「AAAA(「クワッドエー」と読む)レコード」を使用することによって可能となる。クライアントは、DNSに対して従来のIPv4アドレス用のAレコードの代わりにAAAAレコードを問い合わせることで、アクセス先ホストのIPv6アドレスを得ることができるのである。

もう1つは、IPv6を使用したDNS問い合わせに対

して、ネームサーバがIPv6を使用してこたえられることである。DNSにAAAAレコードを問い合わせる際には、クライアントはネームサーバに対してIPv4を使用して問い合わせてもかまわないため、必ずしもネームサーバ自身がIPv6に対応している必要はない。しかし、IPv6環境に本格的に移行するのであれば、DNSの問い合わせでもIPv6を使用する必要性が出てくるため、ネームサーバがIPv6を使用したDNS問い合わせを処理できるようにする必要がある。



IPv6アドレスを記述する AAAAリソースレコード

AAAAレコードは、ホスト名に対応するIPv6アドレスを記述するためのリソースレコードであり、RFC 1886で定義されている。AAAAレコードは、従来のIPv4アドレスを記述するためのAレコードと比較して、IPv4アドレスの代わりにIPv6アドレスを記述する点だけが異なる。「AAAA」というレコードの名称は、128ビットのIPv6アドレスが32ビットのIPv4アドレスの4倍の長さであることから、従来のIPv4アドレスを記述するAレコードの「A」を4つ並べたものからきている。AAAAレコードの書式は以下のようになっている。

<owner> <ttl> <class> AAAA <IPv6address>

<owner>には、ホスト名(正規名)を記述し、<ttl>には、このリソースレコードのキャッシュの有効期間を秒単位で記述する。<ttl>が省略された場合には、直前の\$TTLでセットされたデフォルトの有効期間がセットされる。<class>には、ネットワーククラスを記述する。インターネットでは「IN」と記述し、実際にはこれ以外には使用されていない。<class>が

省略された場合には、自動的に「IN」がセットされ る。<IPv6address>には、そのホストのIPv6アドレ スを記述する。

例えば、「sykes.example.com」というホストのIPv6 アドレスが、「fec0::2:206:5bff:fec7:b6a5」である場合 には、以下のように記述する。

sykes.example.com. IN AAAA fec0::2:206:5bff:fec7:b6a5

IPv4とIPv6の両方に対応したクライアントは、最初 にDNSに対してアクセス先ホストのAAAAレコード を問い合わせる。もし、AAAAレコードが存在し、 IPv6アドレスが返却された場合は、クライアントはア クセス先ホストがIPv6に対応していると判断し、IPv6 を使用してアクセスを行う(図1)。もし、AAAAレコ ードが存在せずエラーが返却された場合は、クライア ントは次にアクセス先ホストのAレコードを問い合わ せてIPv4アドレスを取得し、IPv4を使用してアクセス を行う(図2)。このように、IPv4とIPv6の両方に対応 しているクライアントは、DNSからの回答によって、 IPv4とIPv6のどちらでアクセスするのかを判断する。

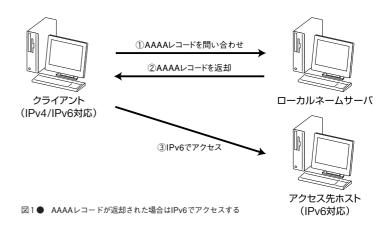
なお、IPv6アドレスを記述するためのリソースレコ ードとして、AAAAレコードのほかに、A6レコード がRFC 2874として提案されていた。しかし、A6レコ ードは、AAAAレコードと比較して便利な点はある が、複雑すぎるという理由で現在は利用しないことに なっている。

IPv6アドレスの逆引きは IPv4同様PTRレコードに記述

IPv6アドレスの逆引き用レコードは、IPv4と同じ ように、PTR (Pointer) レコードを使用して記述する。 例えば、PTRレコードでは「192.168.2.10 | というIPv4 アドレスは、「10.2.168.192.in-addr.arpa」のようにIP アドレス部分を左右逆にして記述する。IPv6において も、IPアドレス部分を左右逆に記述する点は同じであ る。しかし、IPv4では、逆引き用ドメインとして「inaddr.arpa」ドメインを使用していたのに対し、IPv6で は「ip6.arpa」ドメインを使用する。例えば「fec0::2: 206:5bff:fec7:b6a5 というアドレスであれば、PTRレ

コードでは「5.a.6.b.7.c.e.f.f.f.b.5.6.0.2.0.2.0.0.0.0.0.0.0.0.0. 0.0.0.c.e.f.ip6.arpa」のように、IPv6アドレスの省略表 記を元に戻してから1文字ずつ(4ビットずつ)逆に し、それぞれをドットで区切り、最後に「ip6.arpa」 を付加して表記する (リスト1)。

ip6.arpaドメインはICANN (The Internet Corpora tion for Assigned Names and Numbers) が管理し ており、あるアドレスブロックが割り当てられている 組織に、その部分の逆引きゾーンの管理を委任してい る。例えば、IPv6アドレスのブロック「2001:200::/24 | は地域インターネットレジストリであるAPNIC(Asia Pacific Network Information Centre) に割り当てら れているが、ICANNは、このアドレスに対する逆引 きゾーンである「2.0.1.0.0.2.ip6.arpaゾーン」の管理を



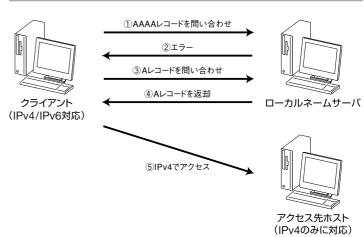


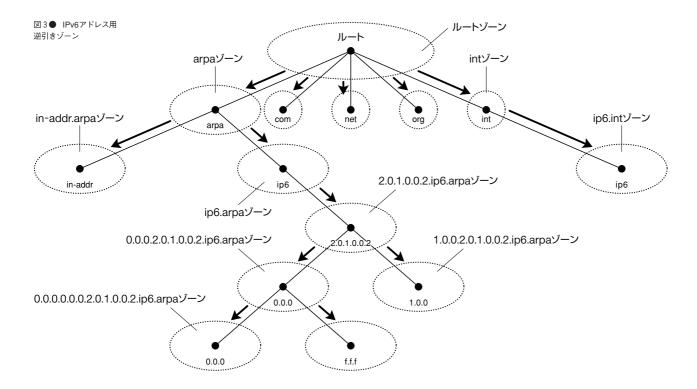
図2● IPv4のみに対応したホストのAAAAレコードは存在しない

リスト1● 逆引きレコード でのIPv6アドレスの記述例

5.a.6.b.7.c.e.f.f.f.b.5.6.0.2.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa

IPv6アドレスをドットで区切って逆に記述

「ip6.arpa」を最後に付加



APNICに委任している(図3)。そして、APNICは IPv6アドレスのブロック「2001:200::/35」をWIDEプロジェクトに割り当てているが、APNICは、同時にこのアドレスに対する逆引きゾーンである「0.0.0.2.0.1. 0.0.2.ip6.arpaゾーン」および「1.0.0.2.0.1.0.0.2.ip6.arpaゾーン」の管理をWIDEプロジェクトに委任している。さらにWIDEプロジェクトは、ほかの組織にIPv6アドレスのブロックを割り当てており、そのアドレスに対する逆引きゾーンの管理をその組織に委任している。

ちなみに、RFC 1886では、逆引き用ドメインとして「ip6.int」ドメインを使用するように記述されていたが、RFC 3152で「ip6.arpa」ドメインを使用するように変更された。このため、RFC 1886の仕様を修正する作業が現在進められている。

なお、IPv6アドレスの逆引き用に、RFC 2672およびRFC 2673でDNAMEレコードとバイナリラベルの仕様が提案されたが、こちらも複雑すぎるという理由で現在では利用しないことになっている。



これまでに説明した、AAAAレコードとip6.arpaドメインを使用したPTRレコードの問い合わせにより、IPv6アドレスの正引きと逆引きができるようになる。そこで、次にIPv6を使用したDNSの問い合わせについ

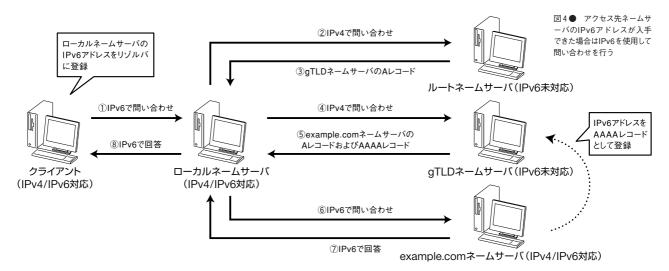
て説明する。基本的に、IPv6に対応したホストはアクセス先ホストのIPv6アドレスをDNSで問い合わせ、IPv6アドレスが入手できれば、そのホストはIPv6に対応していると判断し、IPv6を使用してアクセスを行おうとする。ネームサーバのIPv6アドレスが入手できれば、そのネームサーバはIPv6に対応していると判断し、IPv6を使用してDNSの問い合わせを行おうとする。

それでは、クライアントがexample.comゾーンのレコードを問い合わせる場合を例に、IPv6を使用したDNS問い合わせを説明しよう。まず、クライアントからローカルネームサーバに対してIPv6を使用して問い合わせを行うには、クライアントとローカルネームサーバの両方がIPv6に対応しており、さらに、クライアントのリゾルバにローカルネームサーバのIPv6アドレスを登録しておく必要がある。例えば、IPv6に対応したUnix系OSの場合は、リスト2のように「/etc/resolv.conf」ファイルにローカルネームサーバのIPv6アドレスを設定しておくことで、ローカルネームサーバに対して、IPv6を使用してDNS問い合わせを行うようになる(図4-①)。

クライアントから問い合わせを受けたIPv6対応ローカルネームサーバは、自身で問い合わせ対象のレコードをキャッシュとして保持していなければ、次にルートネームサーバに対して問い合わせを行う。しかし、現在13台あるルートネームサーバのいずれもIPv6を使用

\$ cat /etc/resolv.conf
search example.com
domain example.com
nameserver fec0:0:0:2::10 + 最初に問い合わせるローカルネームサーバのIPv6アドレス
nameserver fec0:0:0:2::11 + 次に問い合わせるローカルネームサーバのIPv6アドレス

リスト2● 「/etc/resolv.co nf」ファイルの記述例



した問い合わせには対応しておらず、ローカルネーム サーバの持つルートキャッシュファイルには、各ルー トネームサーバのIPv4アドレスしか記述されていない。 そこで、ローカルネームサーバはルートネームサー バに対してIPv4で問い合わせを行う(図4-②)。すると、 ルートネームサーバは、comゾーンを管理するgTLD (generic Top Level Domain) ネームサーバのAレコ ードを返却する(図4-③)。ローカルネームサーバは、 gTLDネームサーバのIPv4アドレスしか入手できなか ったので、gTLDサーバのうちの1台に対してIPv4を 使用して問い合わせを行う(図4-④)。ここで、もし example.comゾーンを管理するネームサーバがIPv6 を使用したDNS問い合わせに対応しており、そのIPv6 アドレスをAAAAレコードとしてgTLDネームサー バが管理するcomゾーンに登録していた場合には、 gTLDネームサーバは、ローカルネームサーバに対し てexample.comネームサーバのAレコードとAAAA レコードの両方を返却する(図4-⑤)。ローカルネーム サーバは、example.comネームサーバのIPv4アドレ スとIPv6アドレスの両方を入手できたので、次に、IPv6 を使用してexample.comネームサーバに問い合わせを 行う(図4-⑥)。すると、example.comネームサーバ は、IPv6を使用して目的のレコードを返却するので (図4-⑦)、ローカルネームサーバは、クライアントに その結果をIPv6を使用して返却する(図4-®)。

仮に、IPv4にしか対応していないローカルネームサーバが次に問い合わせを行うネームサーバのAレコードとAAAAレコードの両方を取得した場合には、AAAAレコードの内容を無視して、Aレコードに記述されたIPv4アドレスを使用してアクセスを行う。

name BIND 9を IPv6対応ネームサーバに

それでは、BIND 9をIPv6に対応させるための設定 を紹介しよう。BIND 9でIPv6を使用したDNS問い合 わせを受信できるようにするためには、まず、ネームサ ーバとなるマシンがあらかじめIPv6に対応している必 要がある。そして、BINDの設定ファイルである「/etc /named.conf」のoptionsステートメントで「listenon-v6 { any; };」と記述しておく(リスト3-①)。ま た、IPv6アドレスの逆引きができるように、各セグメ ントに対するIPv6アドレス用の逆引きゾーン(リスト 3-②、③) と、IPv6ループバックアドレス用の逆引 きゾーン(リスト3-④、⑤)の設定を追加する。ここ で、リスト3では、逆引きゾーンとして「ip6.arpa」の ほかに「ip6.int」も登録している。これは、最近まで は、IPv6の逆引き用ドメインとして、「ip6.arpa」では なく「ip6.int」を使用していたという経緯があるため、 アプリケーションの中には、「ip6.int」を使用して逆引

```
$ cat /etc/named.conf
//オプション設定
options {
      directory "/var/named/";
      listen-on-v6 { any; }; ← ①この行を追加する
};
/ /ルートネームサーバの設定
zone "." {
   type hint;
     file "named.ca";
};
//正引きゾーンの設定
zone "example.com" {
     type master;
      file "example.com.zone";
};
//IPv4アドレス用逆引きゾーンの設定
zone "2.168.192.in-addr.arpa" {
     type master;
     file "2.168.192.in-addr.arpa.zone";
};
//IPv6アドレス用逆引きゾーンの設定(ip6.arpa) ← ②
zone "2.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa" {
     type master;
      file "2.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa.zone";
//IPv6アドレス用逆引きゾーンの設定(ip6.int) ← ③
zone "2.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.int" {
      type master;
      file "2.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.int.zone";
};
/ /ループバック用正引きゾーンの設定
zone "localhost" {
     type master;
      file "localhost.zone";
//IPv4ループバックアドレス用逆引きゾーンの設定
zone "0.0.127.in-addr.arpa" {
      type master;
      file "0.0.127.in-addr.arpa.zone";
};
//IPv6ループバックアドレス用逆引きゾーンの設定(ip6.arpa) ← ④
type master;
```

リスト3のつづき

```
← ⑤
//IPv6ループバックアドレス用逆引きゾーンの設定(ip6.int)
type master;
 };
```

```
$TTL 86400
              SOA
                     ns1.example.com. hostmaster.example.com. (
                             2003011801 ; シリアル番号
                             28800
                                     ; リフレッシュ間隔(秒)
                             7200
                                      ; リトライ間隔(秒)
                             604800
                                       ; ゾーンの有効期間(秒)
                             3600
                                      ; ネガティブキャッシュの有効期間(秒)
       IN
              NS
                     ns1.example.com.
       IN
              NS
                     ns2.example.com.
                     192.168.2.10
ns1
       IN
              A
                     fec0:0:0:2::10
       IN
             AAAA
                                                IPv6に対応している場合はAAAAレコードを追加
             A
                     192.168.2.11
ns2
       IN
             AAAA
                     fec0:0:0:2::11
       IN
                                                IPv6に対応している場合はAAAAレコードを追加
winger IN
              Α
                     192.168.2.50
                                                 IPv4のみに対応している場合はAレコードのみを登録
sykes
       IN
                     192.168.2.51
       IN
             AAAA
                     fec0::2:206:5bff:fec7:b6a5 ← IPv6に対応している場合はAAAAレコードを追加
```

リスト4 ● 正引きゾーンファイルの記述例(example.comゾーン)

```
$TTL 86400
     IN
              SOA
                    ns1.example.com. hostmaster.example.com. (
                            2003011801 ; シリアル番号
                                    ; リフレッシュ間隔(秒)
                            28800
                            7200
                                     ; リトライ間隔(秒)
                            604800
                                     ; ゾーンの有効期間(秒)
                            3600
                                     ; ネガティブキャッシュの有効期間(秒)
                            )
      IN
             NS
                   ns1.example.com.
                    ns2.example.com.
5.a.6.b.7.c.e.f.f.b.5.6.0.2.0 IN PTR sykes.example.com. ← IPv6逆引き用PTRレコード
```

リスト5● IPv6アドレス用逆引きゾーンファイルの記述例(2.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpaゾーン)

きをしようとするものがあるからである。当分はこの ようにして、「ip6.arpa」と「ip6.int」のどちらでも逆 引きができるように設定しておくのがよいだろう。

正引き用ゾーンの設定ファイルは、IPv4とIPv6と

で共通である。リスト4のように、IPv6に対応したホ ストに対してAAAAレコードを追加し、IPv6アドレ スを記述する。IPv6に対応していないホストについて は、従来どおりAレコードのみを記述する。

```
$TTL 86400
              SOA
      IN
                     localhost. root.localhost. (
                            2003011801 ; シリアル番号
                            28800
                                     ; リフレッシュ間隔(秒)
                            7200
                                      ; リトライ間隔(秒)
                                     ; ゾーンの有効期間(秒)
                            604800
                            3600
                                     ; ネガティブキャッシュの有効期間(秒)
                     localhost.
       TN
              NS
                     127.0.0.1
                                ← ループバック用のIPv4アドレス
       IN
              A
                                 ← ループバック用のIPv6アドレスを追加
       TN
              AAAA
                    ::1
```

リスト6 ● ループバック用正引きゾーンファイルの記述例(localhostゾーン)

```
$TTL 86400
              SOA
                     localhost. root.localhost. (
                            2003011801 ; シリアル番号
                            28800
                                  ; リフレッシュ間隔(秒)
                            7200
                                     ; リトライ間隔(秒)
                            604800
                                     ; ゾーンの有効期間(秒)
                            3600
                                      ; ネガティブキャッシュの有効期間(秒)
                     localhost.
      IN
             NS
      TN
              РTR
                     localhost. ← IPv6ループバックアドレス用の逆引きレコードを追加
```

そして、逆引き用ゾーンファイルはリスト5のよう に記述する。PTRレコードの左辺は途中までしか書か れていないが、このうしろに「/etc/named.conf」ファ イルで設定したゾーンの名前(リスト5の例では「2.0.0. 0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa」)が補完され、正式な名 称(FQDN: Fully Qualified Domain Name)となる。

また、IPv6ループバックアドレス用に、ループバッ ク用正引きゾーンファイルをリスト6のように設定す る。IPv6用のループバックアドレスは「::1」と表記する。

そして、ループバック用IPv6アドレスは、逆引き用 0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa」と表記する。このため、 6.arpa」というゾーン用の逆引きゾーンファイルを作 成し、リスト7のように設定する。

これで、IPv6に対応したDNSが動作するようにな る。しかし、手作業でIPv6アドレスをDNSに登録する のは非常に手間がかかるため、実際の運用では、第6回 で説明したDNSダイナミックアップデートと第7回で 説明したTSIGを使用して、IPv6アドレスを自動的に登 録するようにしたほうがよいだろう。次回は、リソー スレコードごとに署名を付加することでゾーンデータ の改ざんを防ぐことを可能とする、DNSSEC (DNS Security Extensions)の仕組みについて説明する。

NTTデータ 馬場達也

●今回の内容に関連するRFC

```
RFC 1886 "DNS Extensions to support IP version 6"
```

RFC 2672 "Non-Terminal DNS Name Redirection"

RFC 2673 "Binary Labels in the Domain Name System"

RFC 2874 "DNS Extensions to Support IPv6 Address Aggregation and Renumbering"

RFC 3152 "Delegation of IP6.ARPA"