DNS設定駆け込み寺

勘所をしっかり押さえる

第2回

馬場達也

DNSは、インターネットでアプリケーションを使用する場合になくてはならない重要なシステムである。しかし、DNSの運用は難しいため、取り扱いに苦労している管理者も多いことだろう。ここでは、実際にネームサーバ(DNSサーバ)を運用する際に生じるさまざまな疑問に答え、管理者がスムーズにDNSを運用するためのテクニックを紹介する。

Q11 クライアントからの問い合わせをほかのネームサーバに回送したい

ファイアウォールの内側に設置された複数のローカルネームサーバから直接外部に通信することができない場合に、ファイアウォールを通過できる上位のネームサーバに問い合わせを回送したい。

A BINDの回送機能を使用する

問い合わせ分散と安全性を両立するBINDの回送機能

大規模な組織のネットワークでは、負荷分散や管理の分散などのために、部署ごとにローカルネームサーバを設置したいという要求がある。しかし、それぞれのローカルネームサーバから外部のネームサーバに問い合わせを発行できるようにするためには、ファイアウォールでそれぞれのローカルネームサーバからの問い合わせを通すように設定しなければならない。これは、ファイアウォールの設定が複雑になるだけでなく、セキュリティ的にも好ましくない。BINDの回送機能を利用すれば、図1のように、ローカルネームサーバが保持していないレコードの問い合わせを、外部のネームサーバと通信できるように設定された上位のネームサーバに回送するように設定することができる。

問い合わせの回送は、BINDの設定ファイルである「named.conf」ファイルのoptionsステートメント内で、次のように「forwarders」サブステートメントを記述することにより実現できる。

```
options {
        directory "/var/named/";
        forwarders { 163.135.0.10; };
        forward only;
};
```

forwardersサブステートメントでは、回送先の上位のネームサーバのIPアドレスを指定する。IPアドレスを複数記述した場合は、応答時間の短いものを選択して回送する。ただし、forwardersサブステートメントのみを記述した場合は、回送先のネームサーバから応答がないときに自力で名前解決を行おうとして、ルートネームサーバから反復問い合わせを行ってしまう。ファイアウォールで外部のネームサーバとの通信が許可されていない場合には、反復問い合わせをしても失敗してしまうだけであるため、「forward only」という行を追加することによって、回送先のネームサーバからの応答がなかった場合でも反復問い合わせを始めないように設定することができる。

このように、forwardersサブステートメントを設定することによって、自身でデータを保持していない問い合わせを上位のネームサーバに回送することが可能になる。しかし、図2のように、デフォルトでは上位のネームサーバに回送するが、自組織のドメイン名に対する問い合わせは回送せずに、ファイアウォール内のあるネームサーバを起点として組織内のネームサーバに対して反復問い合わせをしたい場合があるだろう。このように自力で名前解決を行うには、そのドメイン名に対するzoneステートメントを次のように設定することにより実現できる。

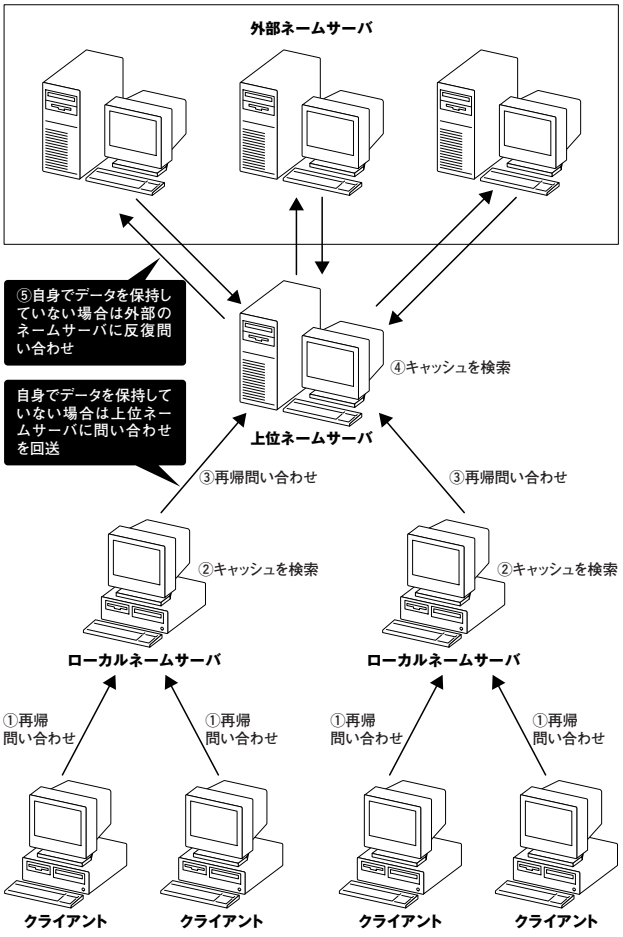

図1● 自身でデータを保持していない場合には、クライアントからの問い合わせを上位のネームサーバに回送する

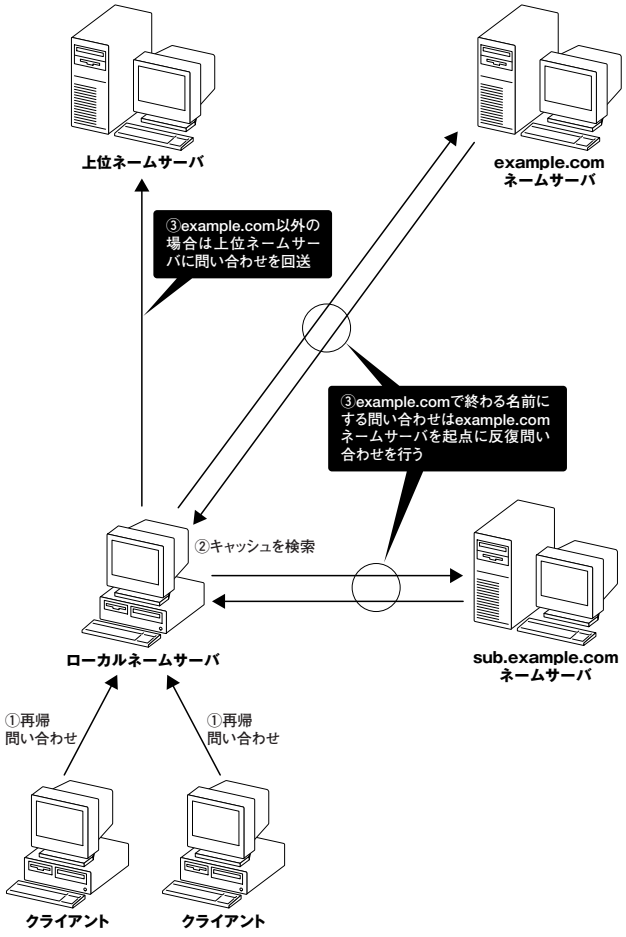

図2● ファイアウォール内のほかのネームサーバが管理しているゾーンに対しては、回送せずに反復問い合わせを行う

```
zone "example.com" {
    type stub;
      └ スタブゾーンとして設定
    masters { 192.168.0.3; };
      └ 反復問い合わせの起点となるネームサーバを指定
    file "stub.example.com.zone";
    forwarders {};
      └ このドメインで終わる名前に対する
        問い合わせは回送しないように設定
};
```

zoneステートメントのtypeサブステートメントでは「stub」（スタブゾーン）として設定し、そのゾーンを管理するネームサーバのIPアドレスをmastersサブステートメントで記述する。「stub」は「slave」と似ているが、slaveの場合と違って、ゾーン転送を行わずに、そのゾーンのSOAレコードとNSレコードのみを取得して保持する。つまり、このゾーンのデータ自身は持っておらず、このゾーンに対して問い合わせを受けた場合には、mastersサブステートメントで記述したネームサーバに対して問い合わせを発行する。スタブゾーンは、ゾーン転送を行う必要がないので、相手がゾーン転送を許可していない場合でも設定することが可能である。

そして、このドメイン名で終わる名前に対する問い合わせを、optionsステートメントのforwardersサブステートメントで設定したネームサーバに回送させないように、このzoneステートメントの中で「forwarders {};」と記述する。こうすることによって、optionsステートメントで記述したforwardersサブステートメントの設定が、このゾーンに対して解除され、このドメイン名で終わる名前に対する問い合わせを受けた場合は、上位のネームサーバに回送せずに指定したネームサーバ（この場合はexample.comネームサーバ）を起点として反復問い合わせを行うようになる。

Q12 問い合わせ元のクライアントに応じて異なる内容を回答したい

内部のホストからの問い合わせにはすべてのホストの情報を回答したいが、外部のホストからの問い合わせに対しては、外部からのアクセスを許可している一部のホストの情報のみを回答したい。

A BINDのビュー機能を使用する

外部向けと内部向けのビューを設定する

BIND 9には、問い合わせ元のクライアントに応じて、異なるゾーンデータを見せるための「ビュー」を設定できる。例えば、内部のホストからの問い合わせには、全ホストの情報を回答したいが、外部のホストからの問い合わせには、Webサーバやメールサーバなどの一部のホストの情報しか回答したくないような場合に利用できる。

```
options {
        directory "/var/named";
};

acl "internal" {
        10.0.0.0/8;
        163.135.0.0/16;
};

view "internal" {
        match-clients { internal; };      ← 内部アドレスで問い合わせてきた場合は、このビューを適用
        recursion yes;                    ← 内部からは再帰問い合わせを受け付ける
        zone "example.com" {
                type master;
                file "example.com.internal.zone";   ← 内部向けゾーンデータファイルを指定
        };
};

view "external" {
        match-clients { any; };           ← 内部アドレスにマッチしなかったアドレスで問い合わせてきた場合は、このビューを適用
        recursion no;                     ← 外部からは再帰問い合わせを受け付けない
        zone "example.com" {
                type master;
                file "example.com.external.zone";   ← 外部に公開するゾーンデータファイルを指定
        };
};
```

リスト1● 内部向けビューと外部向けビューの設定例

この「ビュー」の機能は、BINDの設定ファイルである「named.conf」ファイルで、「view」ステートメントを記述することで利用できる。viewステートメントの基本的な書式は次のようになっている。

```
view <view_name> {
    match-clients { <address_match_list> } ;
    match-destinations { <address_match_list> } ;
    ...
    <zoneステートメント>
};
```

<view_name>には、このビューに付与する名称を記述する。問い合わせの送信元IPアドレスによってビューを切り替える場合には、このビューを適用する送信元IPアドレスのリストを「match-clients」サブステートメントに記述する。そして、問い合わせの宛先IPアドレスによってビューを切り替える場合には、「match-destinations」サブステートメントで宛先IPアドレスを記述する。「match-destinations」サブステートメントは、ネームサーバが複数のIPアドレスを使用している場合に利用できる。また、viewステートメント内には、optionsステートメントで記述するrecursionサブステートメントや、zoneステートメントを記述することもできる。

例えば、example.comゾーンへの問い合わせに対して、内部のホストからの問い合わせには存在するすべてのホストの情報を回答し、外部のホストからの問い合わせには外部に公開する一部のホストの情報のみを回答したい場合を考えてみよう。

```
options {
        directory "/var/named";
};

acl "internal" {
        ! 163.135.0.12;
        10.0.0.0/8;
        163.135.0.0/16;
};

view "internal" {
        match-clients { internal; };
        recursion yes;
        zone "example.com" {
                type master;
                file "example.com.internal.zone";
                allow-transfer { 163.135.0.11; };
        };
};

view "external" {
        match-clients { any; };
        recursion no;
        zone "example.com" {
                type master;
                file "example.com.external.zone";
                allow-transfer { 163.135.0.12; };
        };
};
```

163.135.0.12は外部アドレスとして認識される

163.135.0.11は内部アドレスとして認識される

163.135.0.11からのゾーン転送要求にのみ答える

163.135.0.12からのゾーン転送要求にのみ答える

リスト2● ビューを定義したプライマリネームサーバ（163.135.0.10）での設定例

この場合には、最初に、存在するすべてのホストを記述した内部向けのゾーンデータファイルと、外部に公開するホストのみの情報を記述した外部向けのゾーンデータファイルの2種類のファイルを用意しておく。そして、リスト1のように、viewステートメントで内部向けのビュー（ここでは“internal”というビュー名を付与）と外部向けのビュー（ここでは“external”というビュー名を付与）を定義する。

内部向けのビューでは、「match-clients」サブステートメントを使用して、問い合わせの送信元IPアドレスが内部アドレスであった場合にこのビューが適用されるように設定する。aclステートメントを使用して、内部のホストが使用しているIPアドレスに対して“internal”というACL名を付与し、そのACL名を使用して「match-clients { internal; };」と設定することにより、このビューが内部のホストからの問い合わせに適用されるように設定している。また、内部のホストからの再帰問い合わせを許可する場合は、このビューの内部で「recursion yes;」と設定する。そして、zoneステートメントを記述し、内部向けに作成したゾーンデータファイルを指定する。

外部向けのビューも同様に設定する。外部向けのビューでは、先に記述した内部向けのビューにマッチしなかったすべてのホストからの問い合わせに対して、このビューが適用されるように、「match-clients { any; };」と設定する。そして、外部のホストからの再帰問い合わせを拒否するように、「recursion no;」と設定する。そして、zoneステートメントを記述し、そこで、外部向けに作成したゾーンデータファイルを指定する。

ビューを設定したセカンダリネームサーバを設定する

ここまでは、内部向けと外部向けの2種類のゾーンを管理するプライマリネームサーバを設定する方法について紹介した。それでは、同じように、内部向けと外部向けの2種類のゾーンを管理するセカンダリネームサーバを設定する場合はどうすればよいだろう。

セカンダリネームサーバのIPアドレスが、プライマリネームサーバのnamed.confファイル中で内部アドレスとして設定されていれば、プライマリネームサーバに対してゾーン転送のリクエストをすると、セカンダリネームサーバには内部向けのゾーンが転送される。逆に、セカンダリネームサーバのIPアドレスがプライマリネームサーバで外部アドレスとして設定されていれば、セカンダリネームサーバには、外部向けのゾーンが転送される。つまり、内部向けと外部向けの両方のゾーンを同時に転送することはできない。

そこで、セカンダリネームサーバに両方のゾーンが転送されるようにするために、セカンダリネームサーバに

```
options {
        directory "/var/named";
};

acl "internal" {
        ! 163.135.10.12;
        10.0.0.0/8;
        163.135.0.0/16;
};

view "internal" {
        match-clients { internal; };
        recursion yes;
        zone "example.com" {
                type slave;
                masters { 163.135.0.10; };
                file "example.com.internal.zone.bak";
                allow-transfer { none; };
                transfer-source 163.135.10.11; ―― 163.135.10.11からゾーン転送要求を行う
        };
};

view "external" {
        match-clients { any; };
        recursion no;
        zone "example.com" {
                type slave;
                masters { 163.135.0.10; };
                file "example.com.external.zone.bak";
                allow-transfer { none; };
                transfer-source 163.135.10.12; ―― 163.135.10.12からゾーン転送要求を行う
        };
};
```

リスト3● ビューを定義したセカンダリネームサーバ（163.135.0.11/163.135.0.12）での設定例

内部アドレスと外部アドレスの2つのアドレスを持つように設定する。例えば、セカンダリネームサーバに「163.135.0.11」と「163.135.0.12」という2つのアドレスを設定し、プライマリネームサーバでは片方のアドレス（163.135.0.11）を内部アドレスとして設定し、もう片方のアドレス（163.135.0.12）を外部アドレスとして設定する。これで、「163.135.0.11」のアドレスを使用してゾーン転送のリクエストを行った場合には内部向けのゾーンが転送され、「163.135.0.12」のアドレスを使用してゾーン転送のリクエストを行った場合には外部向けのゾーンが転送されるようになる。セカンダリネームサーバがゾーン転送の際に使用する送信元IPアドレスは、named.confファイルのzoneステートメント内の「transfer-source」サブステートメントで指定する。リスト2にプライマリネームサーバでの設定例を、リスト3にセカンダリネームサーバでの設定例を示す。

しかし、この方法では、セカンダリネームサーバに2つのIPアドレスを付与しなければならない。そこで、内部向けのゾーンを管理するプライマリネームサーバと外部向けのゾーンを管理するプライマリネームサーバを別のネームサーバとして用意し、お互いに相手のゾーンのセカンダリネームサーバとする方法がある（リスト4およびリスト5）。この方法では、内部向けと外部向けのゾーンを1台のネームサーバで管理することはできないが、付与するIPアドレスは1つずつで済む。

NTTデータ　馬場達也

```
options {
        directory "/var/named";
};

acl "internal" {
        10.0.0.0/8;
        163.135.0.0/16;
};

view "internal" {
        match-clients { internal; };
        recursion yes;
        zone "example.com" {
                type master;
                file "example.com.internal.zone";
                allow-transfer { 163.135.0.11; };
        };
};

view "external" {
        match-clients { any; };
        recursion no;
        zone "example.com" {
                type slave;
                masters { 163.135.0.11; };
                file "example.com.external.zone.bak";
                allow-transfer { none; };
        };
};
```

163.135.0.11からは内部向けビューが見える

163.135.0.11からのゾーン転送要求にのみ答える

外部向けゾーンのセカンダリネームサーバとして設定

リスト4●　内部向けプライマリネームサーバ（163.135.0.10）の設定例

```
options {
        directory "/var/named";
};

acl "internal" {
        ! 163.135.0.10;
        10.0.0.0/8;
        163.135.0.0/16;
};

view "internal" {
        match-clients { internal; };
        recursion yes;
        zone "example.com" {
                type slave;
                masters { 163.135.0.10; };
                file "example.com.internal.zone.bak";
                allow-transfer { none; };
        };
};

view "external" {
        match-clients { any; };
        recursion no;
        zone "example.com" {
                type master;
                file "example.com.external.zone";
                allow-transfer { 163.135.0.10; };
        };
};
```

163.135.0.10からは外部向けビューが見える

内部向けゾーンのセカンダリネームサーバとして設定

163.135.0.10からのゾーン転送要求にのみ答える

リスト5●　外部向けプライマリネームサーバ（163.135.0.11）の設定例