

# DNS設定 勤所をしっかりと押さえる

## 駆け込み寺 第5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の運用は難しく、管理者もなかなか苦労しているところがあると思う。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 DNSを使用してサーバへの負荷を分散させたい

Webサーバの負荷が増大したのでWebサーバを複数台配置し、DNSを使用してクライアントからのアクセスを分散させたい。

### A BINDのラウンドロビン機能を利用する

BINDでは、同じ名前に対して複数のAレコードを記述することによって、サーバへの負荷を分散することができる。同じ名前に対して複数のAレコードを記述した場合は、クライアントからの名前解決要求に対してすべてのAレコードが返却されるが、BINDでは、回答に含まれるレコードの順番を名前解決を行うたびに変更するようにしている。クライアントリゾルバでは、同じ名前に対して複数のレコードが返却された場合は、回答に含ま

れる先頭のレコードから優先的に使用するので、この性質を利用して負荷分散を実現することができる。

例えば、図1のように「www.example.com」というWebサーバを3台設置し、クライアントからのアクセスの負荷を分散させたい場合は、リスト1のようにexample.comゾーンのゾーンデータファイルを記述する。このように、そ

www	IN	A	192.168.0.30
	IN	A	192.168.0.31
	IN	A	192.168.0.32

リスト1 ● 「www.example.com」に対して複数のAレコードを記述する

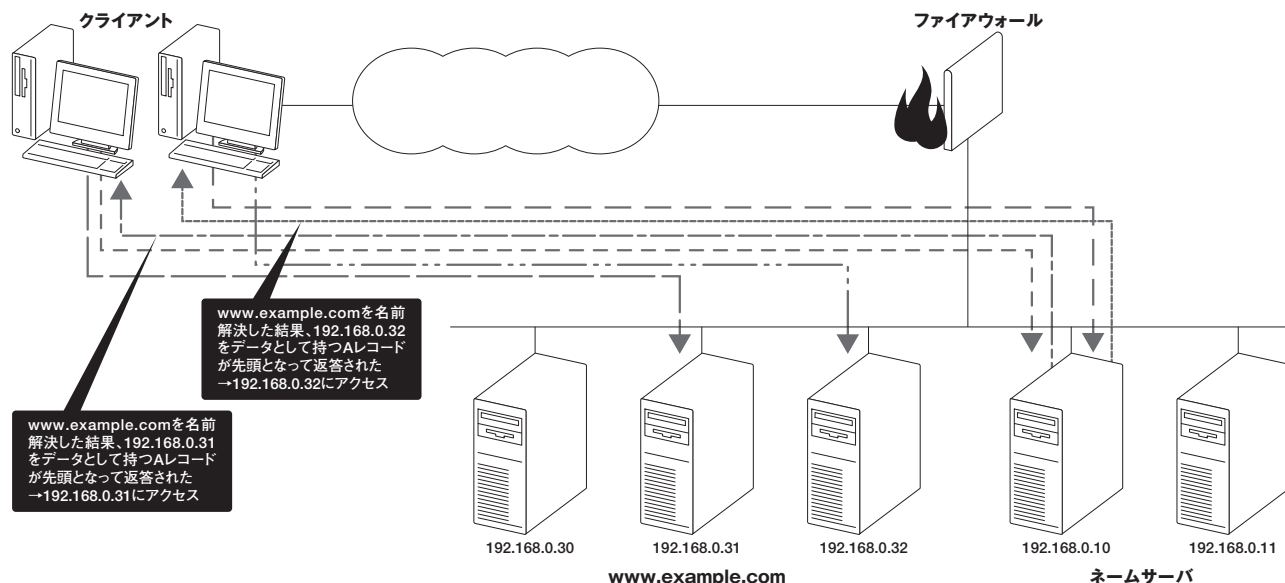


図1 ● DNSを使用してWebサーバへの負荷を分散させる

```

$ dig @192.168.0.10 www.example.com
; <<>> DiG 9.2.1 <<>> @192.168.0.10 www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34223
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.example.com.          IN      A

;; ANSWER SECTION:
www.example.com.          86400  IN      A       192.168.0.31
www.example.com.          86400  IN      A       192.168.0.32
www.example.com.          86400  IN      A       192.168.0.30

;; AUTHORITY SECTION:
example.com.              86400  IN      NS      ns1.example.com.
example.com.              86400  IN      NS      ns2.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.          86400  IN      A       192.168.0.10
ns2.example.com.          86400  IN      A       192.168.0.11

;; Query time: 2 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Fri Oct 10 00:21:53 2003
;; MSG SIZE rcvd: 129

```

リスト2 ● digコマンドによる問い合わせの結果。指定した順にAコードが表示され、「192.168.0.31」が先頭になっている

それぞれのIPアドレスに対するAレコードを同じホスト名に対して設定する。

そして、digを使用して「www.example.com」のAレコードを問い合わせると、リスト2のような回答が返却される。リスト1では「192.168.0.30」を含むAレコードを先頭に記述したが、digの結果では「192.168.0.31」が先頭になっていることに気づくだろう。実は、BINDでは、同じ名前に対して複数のAレコードが存在した場合、最初にAレコードをIPアドレス順にソートして保持する。そして、クライアントから問い合わせがあった場合には、その中から先頭にして返却するレコードをランダムに選び出し、順にメッセージの回答部に入れていくのである。

以前は、この負荷分散の機能をリスト3のようにCNAMEレコードを複数記述することで実現している場合も

www	IN	CNAME	www1
		CNAME	www2
		CNAME	www3
www1	IN	A	192.168.0.30
www2	IN	A	192.168.0.31
www3	IN	A	192.168.0.32

リスト3 ● 同じ名前に対して複数のCNAMEレコードを記述することは仕様で許可されていない

あった。しかし、同じ名前に対してCNAMEレコードを複数記述することは仕様で許可されていない。BIND 8では、named.confファイルのoptionsステートメントにおいて、「multiple-cnames yes;」と設定することによってCNAMEレコードを複数設定できるようになっていた。しかし、BIND 9.1.0以降では複数のCNAMEレコードを記述することは許可されていないので注意してほしい。

# Q12

## クライアントに最寄りのサーバのIPアドレスを返却したい

NTPサーバへのアクセスの負荷を分散させるために、同じ名前のNTPサーバを分散配置したい。そして、クライアントには、最寄りのNTPサーバを使用させたい。

### A BINDのsortlist機能を使用する

Q1で紹介したとおり、同じ名前に対してAレコードを複数記述した場合には、クライアントからの問い合わせに応じる際に先頭にして返却するAレコードはランダムに選び出される。もし、クライアントに返却するAレコードの順序を指定したい場合には、BIND 9.1.0以降でサポートされている「sortlist」サブステートメントを使用すればよい。sortlistサブステートメントを使用すれば、クライアントのIPアドレスに応じて最寄りのサーバが先頭になるようにAレコードの順序を指定できるため、ク

ライアントはわざわざ遠いサーバにアクセスしなくても済むようになる。

sortlistサブステートメントはoptionsステートメント中に記述し、その書式はリスト4のようになっている。

「送信元アドレス」には問い合わせ元となるクライアントのIPアドレスを記述する。ここにはホストアドレスも記述できるが、通常はネットワークアドレスを記述する。そして、「ソートリスト」には、そのアドレスからの問い合わせに対して返答するIPアドレスの順序を記述する。「ソートリスト」を省略した場合には、「送信元アドレス」で記述したアドレスの範囲に合致するAレコードが先頭となって返されるようになる。

例えば、図2のようにNTPサーバを異なるセグメント上に分散配置させ、クライアントに最寄りのNTPサーバを使用させたい場合には、example.comゾーンのゾーンデータファイルに、「ntp.example.com」に対するAレコードをリスト5のように記述し、named.confファイルのoptionsステートメントにおいてsortlistサブステートメントをリスト6のように記述すればよい。こうすることで、例えば「192.168.3.0/24」のセグメントに存在するクライアントからの問い合わせに対しては、リスト7のように「192.168.3.12」のアドレスを持つAレコードを先頭に、「192.168.2.11」「192.168.1.10」の順番で回答するようになり、クライアントから

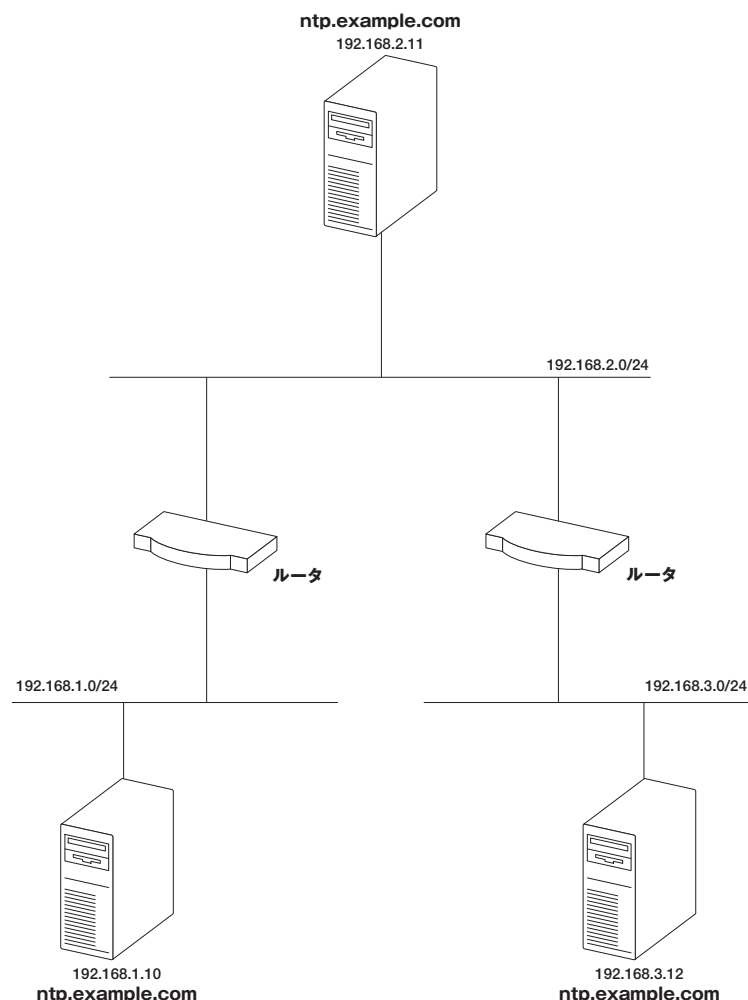


図2● NTPサーバが異なるセグメント上に分散配置されているネットワークの例

```
options {  
  
    sortlist {  
        { 送信元アドレス; {ソートリスト}; };  
        { 送信元アドレス; {ソートリスト}; };  
        ...  
    };  
  
};
```

リスト4● optionsステートメント中に記述するsortlistサブステートメント

最も近いNTPサーバのアドレスが先頭になって返却されるようになる。

```
ntp          IN      A       192.168.1.10
            IN      A       192.168.2.11
            IN      A       192.168.3.12
```

馬場達也 (NTTデータ)

リスト5● 「ntp.example.com」に対して複数のAレコードを記述する

```
options {
    directory "/var/named/";
    sortlist {
        { 192.168.1/24; { 192.168.1/24; 192.168.2/24; 192.168.3/24; } } ;
        { 192.168.2/24; { 192.168.2/24; 192.168.1/24; 192.168.3/24; } } ;
        { 192.168.3/24; { 192.168.3/24; 192.168.2/24; 192.168.1/24; } } ;
    } ;
};
```

sortlistでIPアドレスの順序を記述

リスト6● sortlistサブステートメントの記述例。IPアドレスを3つ指定している

```
$ dig @192.168.0.10 ntp.example.com
; <<>> DiG 9.2.1 <<>> @192.168.0.10 ntp.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44956
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;ntp.example.com.          IN      A

;; ANSWER SECTION:
ntp.example.com.         86400  IN      A       192.168.3.12
ntp.example.com.         86400  IN      A       192.168.2.11
ntp.example.com.         86400  IN      A       192.168.1.10

;; AUTHORITY SECTION:
example.com.             86400  IN      NS      ns1.example.com.
example.com.             86400  IN      NS      ns2.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        86400  IN      A       192.168.0.10
ns2.example.com.        86400  IN      A       192.168.0.11

;; Query time: 2 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Fri Oct 10 12:25:52 2003
;; MSG SIZE rcvd: 129
```

digコマンド

192.168.3.12が最初に返される

リスト7● 192.168.3.0/24から「ntp.example.com」のAレコードを問い合わせた場合の回答。「192.168.3.12」が最初に返される