

ネームサーバは内部名で

民田雅人
(株) 日本レジストリサービス

2004年6月のJP DNSの変更

- ゾーン外グルーの削除
 - ドメイン名の問い合わせにおいて、ネームサーバの名前のみを返し、不要なグルーは返さない
- 親ドメインの無いホストの削除
 - JP DNSに、過去の不要な情報を抱え続けることになり、ネームサーバ中に占める量が無視できなくなる。
 - 残っているとセキュリティ的にも問題となる

グルーレコードについておさらい

- グルーレコードは、ネームサーバをアクセスするために必要なIPアドレスのレコード
 - RFC1912の2.3より、xx.ゾーンの設定例

podunk.xx.	in	ns	ns1.podunk.xx.
		in	ns2.podunk.xx.
ns1.podunk.xx.	in	a	1.2.3.4
ns2.podunk.xx.	in	a	1.2.3.5
 - ここでのA RRがグルーレコード
 - 現在ではAAAA RRも含む
- 以下単に「グルー」と表記する

ゾーン外グルー

- 例えば“co.jp”ゾーンのドメインのネームサーバに、“co.jp”以外のホストが設定してある場合、それらのネームサーバのIPアドレス

example.co.jp.	IN	NS	ns1.example.ne.jp.
		NS	ns2.example.ne.jp.
ns1.example.ne.jp.		A	192.168.123.234
ns2.example.ne.jp.		A	10.12.34.56
- 赤字の部分がゾーン外グルー
- ゾーン外グルーは不要(RFC 1034, 1912)
 - “ns1.example.co.jp”であればゾーン内グルー

親ドメインの無いホストとは

- ネームサーバに設定してあったホストが、ドメイン名の廃止またはNS設定の解除によって、ホスト名のみ上位ドメインに残ってしまうもの

```
example.co.jp.      IN  NS   ns.example.co.jp.  
                   NS   ns.example2.co.jp.  
ns.example.co.jp.  A   10.79.123.4  
ns.example2.co.jp. A   192.168.1.1
```

- example2.co.jpドメインを廃止すると、ns.example2.co.jpはグルーではなく、“co.jp”ゾーンのホストとなる

JP DNSの変更

- 技術的に極めて正しい処理を行ったのだが、環境によって、一部のドメイン名が正常に検索できなくなるトラブルが発生した
 - <http://www.example.jp/> に繋がらない！
- JP DNSでのグルーの扱いの変更の影響

JP DNSのグルーの扱い 1 JP DNSからグルーが得られる場合

- グルーが確実にJP DNSから得られる場合
example.co.jp. IN NS ns.example.co.jp.
ns.example.co.jp. A 10.10.10.10
 - www.example.co.jpのA RRをJP DNSに問い合わせると、ネームサーバ名としてns.example.co.jpと、そのグルーとして10.10.10.10を得ることができる。
- ネームサーバが、当該ドメインに所属している
 - 「ネームサーバが内部名に設定してある」
→外部名

JP DNSのグルーの扱い 2 JP DNSからグルーが得られない場合

- ドメインとネームサーバのドメインが別ゾーン
example.CO.jp. IN NS ns.example.NE.jp.
- 同じゾーン内であっても、他ドメイン所属のホスト
example-xx.co.jp. IN NS xx.example-yy.co.jp.
example-yy.co.jp. NS yy.example-yy.co.jp.
yy.example-yy.co.jp. A 10.12.34.56
- 以前は、上記例でもグルーを返していた

BIND 8キャッシュサーバの不具合

- BIND 8.2.7までのBIND 8キャッシュサーバ
 - あるドメイン名の検索中に、グルー無しが2段以上続く場合(JP DNSに対して3回以上アクセスが必要)、BIND 8.2系のキャッシュサーバでは当該ドメインの検索が不能となる。
 - BIND 4.9.11、4.9.10なども同じ
- BIND 8.3.0以降のBIND 8キャッシュサーバ
 - グルーが得られないと、クライアントからの再送に頼るため、結果として、検索に時間がかかる
 - 但し通常の運用では、キャッシュの関係で気づきにくい

他のキャッシュサーバの挙動

- 主なキャッシュサーバの実装
 - BIND 9系
 - djbdnsのdnscache
 - Windows 2000 ServerのDNSサービス
- 直接グルーが得られなくても問題無いが、グルーが無いことによる別の問題もある

グルーが得られないキャッシュサーバの挙動 example.jpのネームサーバがjp.example.net

1. ルートネームサーバに www.example.jp のIPアドレスを問い合わせ、JP DNSの名前とグルーの返答を受け取る
2. JP DNSにwww.example.jpのIPアドレスを問い合わせ、example.jpのネームサーバの名前、つまりjp.example.netを受け取る
ここではグルーは得られない
3. ルートネームサーバにjp.example.netのIPアドレスを問い合わせ、NETのネームサーバの名前(ns.example.net)とグルーを受け取る
4. NETのネームサーバにns.example.netのネームサーバのIPアドレスを問い合わせ、example.netドメインのネームサーバであるns.example.netとそのグルーとして IPアドレスを受け取る
5. ns.example.netに、jp.example.netのIPアドレスを問い合わせ結果を受け取る
6. jp.example.jpにwww.example.jpのIPアドレスを問い合わせ結果を得る

グルーが無い場合の問題点

- グルーが得られない場合、多くのネームサーバへのアクセスが必要となり、ドメインの検索に時間がかかる
- 依存するネームサーバの数が不必要に多くなり、ドメイン運用の安定性という観点からも、信頼性が低下している
- 2段以上続けてグルーが得られないと、BIND 8.2.xまでのキャッシュサーバでは、ドメイン検索ができなくなる

JPドメインの現状

グループを得るまでのJP DNSへの問い合わせ回数	JP DNSのBIND	
	BIND 8	BIND 9
1	76.43%	54.62%
2	23.52%	38.50%
3	0.05%	6.85%
4	0.00%	0.02%

- JPドメインのうち、JP DNSがBIND 8だと0.05%のドメインが、BIND 9だと6.88%のドメインが、BIND 8.2.x以前のキャッシュサーバからは検索できない。
- 古いBIND(BIND 8.2.7以前)はまだまだ利用されている！

確実なドメインアクセスのために

- ネームサーバを内部名として設定する

```
example.co.jp.    IN NS ns.example.co.jp.
ns.example.co.jp. A 10.10.10.10
```
- 複数のネームサーバがある場合、少なくとも一つは内部名にする
 - 理想は全部内部名

```
example.CO.jp.   IN NS ns.example.CO.jp.
                  NS ns.example.NE.jp.
ns.example.CO.jp. A 10.10.10.10
```


