

逆引きDNSの lame delegationへの対策

2008年4月23日

JPNIC技術部 小山祐司



社団法人 日本ネットワークインフォメーションセンター

Copyright © 2008 Japan Network Information Center

スケジュール

- 4月22日 指定事業者の皆様にあナウンス
- 4月23日 指定事業者連絡会
- 5月22日 技術連絡担当者の皆様にあナウンス
- 7月1日 lameチェック開始

指定事業者の皆様へのお願い

- lame delegationはDNSに悪影響が出るため、改善取り組みにご協力をお願いします。
- 逆引きDNSの設定見直しをお願いします。
- whoisの連絡先メールアドレスの確認をお願いします。
- 5月22日に技術連絡担当者宛にアナウンスメールを送信します。

解説webページ

The screenshot shows a web browser window displaying the JPNIC website. The browser's address bar shows the URL "http://www.jpnictoken.jp". The website header includes the JPNIC logo and the text "日本ネットワークインフォメーションセンター Japan Network Information Center". There are navigation links for "TOP", "ENGLISH", "SITMAP", and "RSS". A search box is present with the text "サイト内検索:" and a "検索" button. Below the header, there are several green buttons for navigation: "JPNICとは", "インターネットガバナンス", "インターネットの技術", "ドメイン名", "インターネットの歴史・統計", "IPアドレス", "インターネットの教育", "JPNIC協議会", "JPNICライブラリ", and "トピックス". A horizontal menu contains links such as "IPアドレス・AS番号とは", "IPアドレスの管理", "IPアドレス・AS番号が欲しい時は", "JPIRR", "お知らせ", "統計・各種リスト", "IPアドレストピックス", "IPアドレス関連のミーティング", "各種申請手続について", and "IPv4アドレスの在庫枯渇に関して". A "印刷用ページの表示" button is located in the top right corner of the content area.

適切に設定されていない逆引きネームサーバによる 影響改善のための取り組みについて

インターネットの安定した運用のためには、逆引きゾーンに関するDNSの問い合わせに対して正しくない応答が返ることや問い合わせ元のタイムアウト待ち、ネームサーバ間で無駄なDNSトラフィックの発生を防ぐ必要があります。

JPNICではインターネットの安定した運用を実現するための取り組みの一環として、JPNICの管理するIPアドレスの逆引きゾーンにおいて適切に設定されていない (lame delegationの)状態の有無を調査し、一定期間設定されていない状態が継続する場合には、JPNICはそのネームサーバへの逆引きゾーンの委任を停止します。

lame delegationとは

lame delegationとは、ドメインの一部分(ゾーン)の管理を別のサーバへまかせる (ゾーンを委任する、delegationする)方法で階層的な管理を行う DNSにおいて、上位のゾーンから下位のゾーンへの委任が正しく行われていない状態を指します。

上位のゾーンに下位ゾーンの権威ネームサーバが正しく登録されていない場合や、下位のネームサーバが委任されたゾーンの権威ネームサーバとして動作していない場合にはゾーンへの委任が正しく行われず、lame delegationの状態となります。

逆引きDNSの適切な動作に向けて

悪影響のある逆引きDNSの
lame delegationを減らす

JPNICに登録されたネームサーバが
lameの場合、委任を停止

この取り組みの実施対象

- 指定事業者に割り振られたアドレス
- 特殊用途用PIアドレス
- 歴史的PIアドレス(割り当て先組織にID/パスワードを発行したもの)

/24より大きい逆引きゾーンが対象

/25より小さい逆引きは対象外

この取り組みでの判定基準

UDPによるSOAレコードの問い合わせに対して
AAビット付きの応答を返すこと

digの例

```
% dig @dns.example.jp 2.0.192.in-addr.arpa. -t SOA +norec
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28757
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
...
...
```

委任停止までの流れ (1/2)

調査対象のネームサーバに対し、定期的に(一日一回) lameかどうか調査

1. 15日間連続してlameと判定した場合

ネットワーク情報の技術連絡担当者(割り当て先・上位割り振り先)へメール通知



委任停止までの流れ (2/2)

- 以降lame継続の間、週一回メールを送信
- 最初のメール通知から30日経過しても解消しない場合、該当逆引きゾーンの委任を停止
 - 逆引きゾーンからlameの NSレコードを削除
 - whoisにlameである旨表示
- ✓ 途中でlameでなくなったら日数はリセット
- ✓ 委任が停止していたときは委任再開



通知メールの例

JPNIC

ご担当者様


貴組織に割り当てられたIPアドレスのネットワーク情報に登録されているネームサーバのうち、適切に設定されていない(lame delegationである)と判定されたものについて、以下のとおりお知らせいたします。

[ネットワークアドレス]	255.3.3.0-255.3.5.255
[ネームサーバ名]	ns1.example.ad.jp
[エラー内容]	A/AAAAレコードが引けません (query timed out)
[逆引きゾーンの委任停止予定日]	2008/05/19

今回は、1回目のお知らせとなります。
適切に設定されていない状態が続く場合には、上記の委任停止予定日の翌日以降、記載のネームサーバへの逆引きゾーンの委任を停止します。

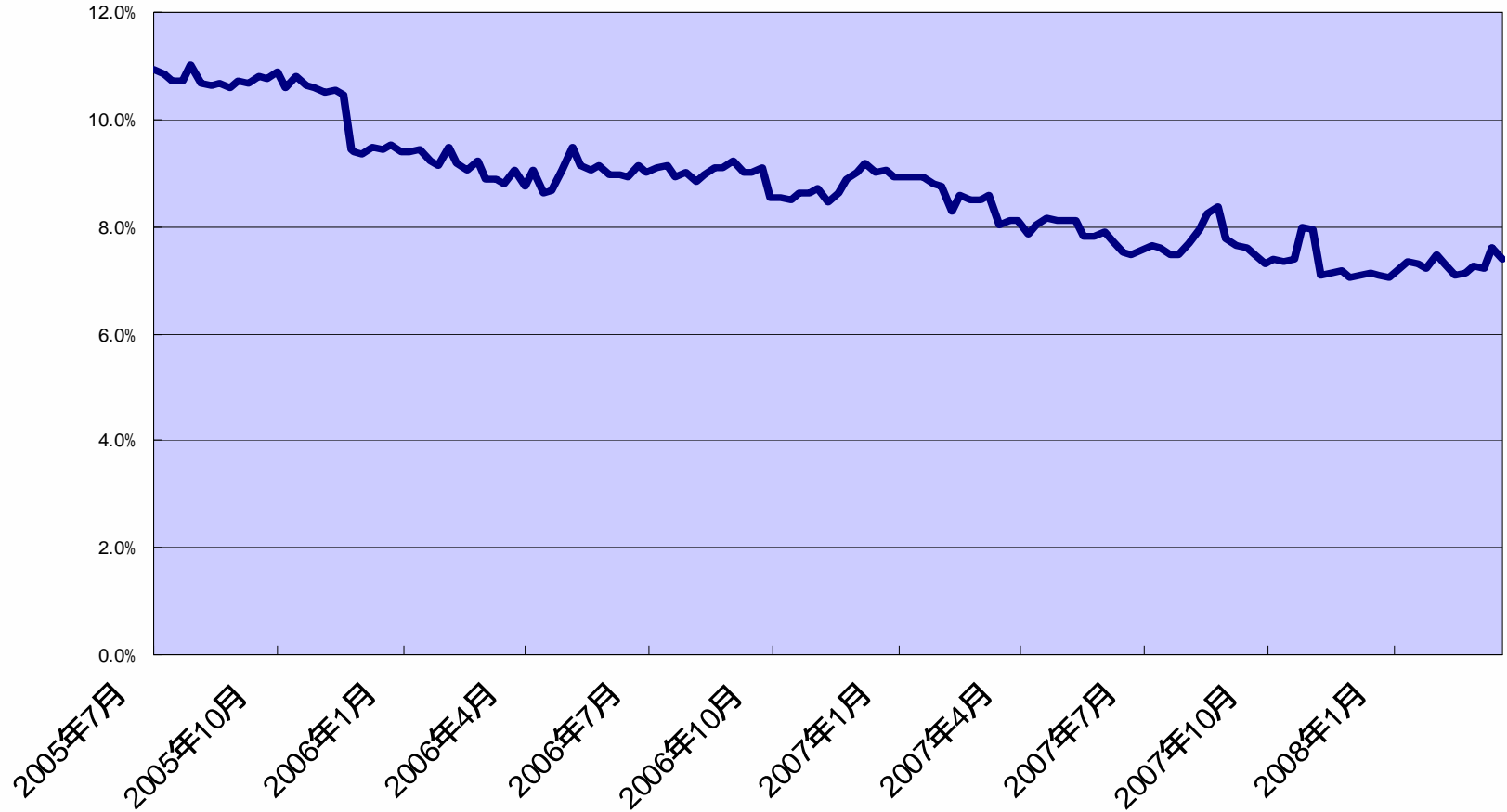
whoisの例

```
Network Information: [ネットワーク情報]
a. [IPネットワークアドレス] 192.0.2.0/24
   :
   :
p. [ネームサーバ]      ***LAME***_example1.nic.ad.jp_2008/04/23
p. [ネームサーバ]      example2.nic.ad.jp
```



参考: lame NSレコードの割合

JPNICの逆引きゾーンに占める lameのNSレコードの割合



ありがとうございました