DNSDAY
DNSQC-TF活動報告(1)

2003年12月2日

小島育夫　kojima@nic.ad.jp
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

DNSの現状

一見「うまく動いている」ように見える

- しかし、実際には、DNSの運用上正しく　ない設定が行われている場合も多い
  - DNS運用の健全化を行おう
  - 各ホストで動いているネームサーバのエラーログを確認してみよう

正しくない設定により惹き起こされる事項

- DNSの不安定な動作
  - 本来不必要なDNSパケットの再送
  - 不必要なDNSタイムアウト待ち
  - 情報の取得が不安定

  ⇒インターネット上の各種サービスに影響を及ぼす
- DNSパケットストーム(2002年2月)
  - 特定のDNSサーバへの過大なDNSトラフィックが発生
  - 特定のBIND (8.3.0)の実装の問題

    +Lame delegation

DNSの適切な設定の必要性

- DNSを基盤としたインターネットの安定運用
  - DNSへの不必要なパケットの転送を排除
  - DNSの負荷の低減
  - インターネットの見かけの不安定さを低減
- DNSの負荷を低減
  - ルートサーバやTLDのネームサーバ等の基幹となるサーバ群への不必要な問い合わせを低減
  - 現在のDNSシステムで安定的な運用を継続的に維持する

DNSの運用健全化に向けて

- 必要な活動
  - 現在のDNSの状況を観測、分析する
  - 分析した結果を公開し改善を求める
  - 自らのDNSの設定をチェックする手段を提供する
- 必要な要件
  - 商業ベースで実施することは困難
  - 国内や場合によっては海外にあるDNSサーバに対する網羅的な調査が必要
  - DNSに関する技術スキルが必要
  - DNS管理組織との連携が必要

ARINでは

- LameDelegationに対する処理方針を公開
- http://www.arin.net/registration/lame_delegations/index.html
  - LAMEを発見したら
    - ゾーンの連絡先(POC)にメールする
    - そのアドレスが属するASの連絡先(POC)にメールする
    - 両連絡先に電話する
    - 30日以内に対応するよう関連する連絡先に郵便で通知
  - DNSのdelegationを解除する
    - 30日以上経過しても改善されない場合

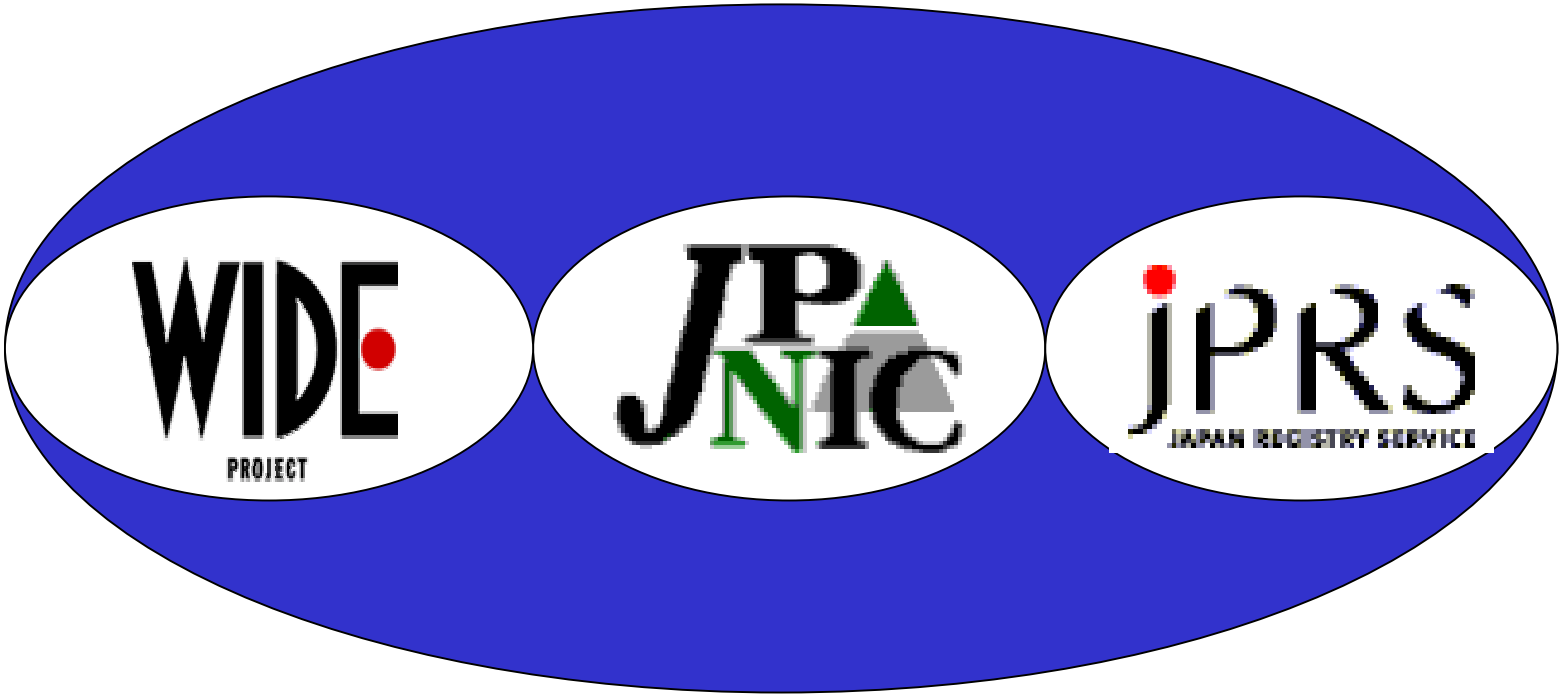
RIPEでは

- RFC1912に基づく検証を実施
- 逆引きゾーンの調査結果を公開
- http://www.ripe.net/ripencc/pub-services/stats/revdns/zcheck/quality-report.html#method

APNICでは

- 第16回APNIC会議でLameDelegationCleanupの方針が提案され承認された(2003/8/20)
- http://www.apnic.net/meetings/16/programme/minutes/dns.html#3
- 処理手順
  - Lameの状態が15日以上になると通知開始
  - ゾーンの管理者にメール、FAX、電話で通知
  - 45日間の通知期間を経過しても改善されない場合DNSのdelegationを解除

DNS運用健全化タスクフォース (DNSQC-TF)



2002年5月、WIDE・JPRS・JPNICの共同プロジェクトとしてDNSQC-TFを設置

活動概要

- 2002年5月：設立
- 2002年度：JPゾーンの正引きに関する調査を実施
  (調査項目の検討、調査ツールの開発を含む)
- 2003年度：JPNICが管理するin-addr.arpaゾーンの
  逆引きに関する調査を実施

役割分担

WIDE:調査項目のレビュー、技術支援

JPRS:正引きの調査

JPNIC:逆引きの調査

調査の対象

- 調査実施日(2003年10月22日)の登録データ
- JPNICが管理運用する逆引きDNSのゾーン
  - http://www.nic.ad.jp/ja/dns/jp-addr-block.html
  - /8のゾーン:1
    - → NSが登録される/16のゾーンが、256
    - →割当済みのアドレス(ゾーン)が、234
    - →DNS登録済みのゾーンが、171(73.0%)
  - /16のゾーン:338
    - → NSが登録される/24のゾーンが、86,528
    - →割当済みのアドレス(ゾーン)が、75,212
    - →DNS登録済みのゾーンが、71,009(94.4%)

調査項目

- 不完全委譲(LameDelegation)

  上位ゾーン(JPNIC)へ登録されたネームサーバが信頼ある応答（authoritative answer）を返すネームサーバかどうか
- SOAのシリアル番号が一致しているか
- 各ゾーンのNSの数は適切か
- NSがCNAMEでないか
- NSがMXでないか
- NSがプライベートアドレスでないか

Lame Delegation とは

- 不完全委譲(Lame Delegation)のネームサーバとは、上位ゾーンに　登録されているネームサーバが、実際にはそのゾーンの信頼ある　(Authoritative)ネームサーバでない場合をいう。

  - 指定されたNSにそのゾーンの情報が発見できない

    原因:

    (1) そのNSにそのゾーンが定義されていないとき

    (2) ゾーンファイルに構文エラーがあり正しく設定されていないとき

    (3) プライマリが Lame のとき

Lame Delegation による影響

発生する問題

- そのゾーンの名前が引けない.
- 検索のたびに，そのNSのネームサーバ(プライマリ，セカンダリ)に毎回問い合わせがいく
- ネガティブキャッシュが登録されないので．普通の検索でも，Lameにあたると，再問い合わせが発生する.
- むだなトラフィックが発生する

調査結果(1)
/8ゾーン

	NS数	率	ゾーン数	率
総数	437		171	
応答なし	36	8.237986	28	16.37427
REFUSED	3	0.686499	1	0.584795
SERVFAIL	36	8.237986	22	12.8655
NOERROR&aaビットなし	27	6.17849	21	12.2807
NOERROR&aaビットあり	335	76.65904	143	83.62573
aaを返さないNSがあるゾーン	160	36.61327	58	33.91813
ゾーン内の全NSがaaビットあり	277	63.38673	113	66.08187

調査結果(2)
/8ゾーン

	NS数	率	ゾーン数	率
総数	277		113	
シリアル不一致	5	1.805054	2	1.769912
シリアル一致	272	98.19495	111	98.23009
	NS数	率	ゾーン数	率
総数	437		171	
LAME	160	36.61327	58	33.91813
シリアル不一致	5	1.144165	2	1.169591
正しい委任	272	62.24256	111	64.91228

調査結果(3)
/16ゾーン

	NS数	率	ゾーン数	率
総数	165880		71009	
応答なし	5487	3.307813	3871	5.451422
REFUSED	252	0.151917	183	0.257714
SERVFAIL	8034	4.84326	4171	5.873903
NXDOMAIN	538	0.324331	261	0.367559
NOERROR&aaビットなし	4352	2.623583	2949	4.152995
NOERROR&aaビットあり	147217	88.7491	64371	90.65189
aaを返さないNSがあるゾーン	23520	14.17892	9875	13.90669
ゾーン内の全NSがaaビットあり	142360	85.82108	61134	86.09331

調査結果(4)
/16ゾーン

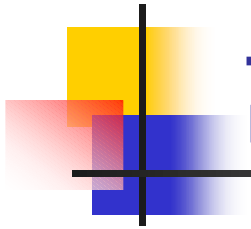
	NS数	率	ゾーン数	率
総数	142360		61134	
シリアル不一致	2609	1.832678	818	1.338044
シリアル一致	139751	98.16732	60316	98.66196
	NS数	率	ゾーン数	率
総数	165880		71009	
LAME	23520	14.17892	9875	13.90669
シリアル不一致	2609	1.572824	818	1.151967
正しい委任	139751	84.24825	60316	84.94135

調査結果(5)
ゾーン毎のNS数：/8ゾーン

NSレコードの数	ゾーンの数	率
0	63	26.9%
1	3	1.3%
2	95	40.6%
3	53	22.6%
4	16	6.8%
5	2	0.9%
6	2	0.9%
7	0	0.0%
8	0	0.0%
9	0	0.0%
10	0	0.0%

調査結果(6)
ゾーン毎のNS数：/16ゾーン

NSレコードの数	ゾーン数	率
0	4203	5.6%
1	1130	1.5%
2	53219	70.8%
3	10835	14.4%
4	3533	4.7%
5	2148	2.9%
6	111	0.1%
7	16	0.0%
8	1	0.0%
9	0	0.0%
10	16	0.0%



調査結果(7)

	NS数	率
総数	6931	
CNAME	119	1.716924
MX	0	0
private address	2	0.028856

調査結果から

- /8ゾーンでは36.6%、/16ゾーンでは14.2%(23,500以上)のネームサーバが不完全委譲の状態にあることがわかった

電子メールの配送など、インターネットのサービスが正しく機能していないかもしれない

DNSの設定再確認と、
「正しい設定を行おう」という意識改革を！