

DNS正引きの実態
--- DNSQC report ---

JANOG11

Fujiwara, Kazunori

JPRS

fujiwara@jprs.co.jp

DNSQC

- DNS Quality Check Task Force
- started since Apr, 2002
- Joint work of JPNIC, WIDE, JPRS
 - JPNIC: for public benefit
 - WIDE: technical support
 - JPRS: on behalf of JP domain registry
- JPドメインの各サイトの設定状況を調査する

チェックするエラー

- 直接委譲しているドメイン名(JPRSが知っているところ)しかチェックできない
- SOA メールアドレスの間違い(例:アドレスに @)
- SOAの中に使ってはいけない文字(例: ホスト名に ‘_’)
- ゾーンのNSレコードのホスト名に ‘_’
- MXレコードのホスト名がCNAME
 - mailが届かない可能性がある(多くの場合届くが)
 - DNSそのものの問題ではなくアプリケーションの問題
- NSレコードのホスト名がCNAME
 - RFC違反であり 名前解決ができない可能性
- 親とゾーンのNSリストが不一致(後述)
- Lame delegation(後述)
- NS, MXレコードのアドレスにprivate address
- 到達できないネームサーバ
 - 一時的な可能性がある 何度かチェック
- ゾーンのすべてのネームサーバへ到達できなかったとき
- NSレコードのアドレスが解決できない

Lame Delegationについて

- 指定されたネームサーバにゾーンの情報を発見できないとき
- Lameの理由
 - ネームサーバにゾーンが定義されていないとき
 - 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
 - マスターサーバがLameだとスレーブサーバもLame
- Lameにより困ること
 - ゾーンの名前がひけない
 - 検索のたびに、そのゾーンのネームサーバすべてに毎回問い合わせがいく
 - 一部のネームサーバだけがLameな場合でも、Lameにあたると再問い合わせが発生するので無駄な問い合わせが発生する

親に登録されたNSリストと、ゾーンに登録されたNSリストが異なる場合

- 問題が少ないケース:
 - 親のNSリスト 子のNSリスト
 - 子のNSがすべて正しく設定されている場合
 - 例
 - ネームサーバ置き換えのときなど
 - 親がAAAAを書いてくれないけど、子ではAAAAを書きたいとき (com,org,net, rootなど)
- 問題があるケース:
 - 親のNSのリスト 子のNSのリスト
 - 子のNSにLame がある
 - 子のNSの内容が不一致
 - むだなトラフィックが発生する
 - 検索結果に一貫性がないことがある

現在のチェックプログラムと環境

- written by sohgo@wide
- 2400 line perl program.
- Queryを出すのにdigを使用
 - NET::DNSやselectを使って書き直します
- 現在の測定環境
 - P3-1260*2, 4GB memory
 - NSPIXP2まで6Mbps, 6to4
 - 二日間, 47万ドメイン(20並列)

2003 Jan 19 スキャン結果 ドメイン名種別ごとのエラードメインの割合

	総数	co	or	ne	ad	gr	ac	goLGed	地域	汎用	日本語
エラー率%	37.9	30.2	30.9	43.4	37.0	37.4	41.7	40.1	39.5	50.2	88.4
badns%	24.6	21.6	25.4	30.8	30.1	26.9	35.7	31.3	32.0	29.9	10.3
LAMEns%	17.8	11.9	10.5	19.8	11.4	16.2	13.7	18.4	14.0	26.7	79.0
nsnone%	11.1	5.9	2.8	11.1	4.5	7.7	1.7	3.3	3.4	19.3	79.1
cnamens%	0.5	0.4	0.6	0.7	0.5	0.6	0.8	2.0	0.7	0.8	0.0
cnamemx%	3.6	3.8	3.6	3.5	2.2	4.4	3.2	2.9	3.8	3.5	0.2
badsoa%	0.3	0.3	0.2	0.3	0.0	0.3	0.3	0.8	0.2	0.3	0.0
private%	0.0	0.0	0.0	0.0	0.2	0.0	0.1	0.0	0.1	0.0	0.0

- エラー率 下記いずれかのエラーのあるドメインの割合(パーセント)
- badns% レジストりに登録したネームサーバと、ゾーンに書いたものが違う(パーセント)
 - LAMEns% レジストりに登録したネームサーバがゾーンのデータをもっていない(パーセント)
 - nsnone% 測定時に全くデータを引けなかったゾーン(パーセント)
 - cnamens% ゾーンに登録してあるネームサーバがCNAMEであるもの(パーセント)
 - cnamemx% ドメイン名のMXレコードに書かれているホストがCNAMEなもの(パーセント)
 - badsoa% ゾーンのSOAに間違いがあるもの(パーセント)
 - private% NS, MXレコードのアドレスにprivate addressが混じっているもの(パーセント)

エラー率に関する考察

- JP ドメイン名におけるネームサーバ設定関連のエラーについては、次の2つのものの割合が高い。
 - badns
レジストりに登録したネームサーバと、ゾーンに書いたものが違う
 - LAME
レジストりに登録したネームサーバがゾーンのデータをもっていない

badnsについて

- badns は、JPRS に登録されているネームサーバと、実際に各ゾーンで定義されているネームサーバのリストが不一致なものを検出対象としている。このエラー率が高い理由は以下のようなものであると考えられる。
 - ドメイン名を登録し、そのためのネームサーバもJPRSに登録したが、運用の中でネームサーバを変更した。
 1. この際、JPRS への登録は変更したが、ゾーン中の定義を変更し忘れている。
 2. この際、ゾーン中の定義は変更したが、JPRS への登録を変更し忘れている。

LAMEについて

- LAMEは、JPRS に登録されているネームサーバが、実際にはゾーンに関する情報を持っておらず、ネームサーバとして動作していない状態のものを検出対象としている。このエラー率が高い理由は以下のようなものであると考えられる。
 - JP ドメイン名では、かつてネームサーバが登録されていないドメイン名は利用されていないものとして登録削除対象となっていたため、事業者や登録者が、運用していないドメイン名に対しても（ドメイン名のネームサーバとしては動作しない）ネームサーバを登録していたケースが多々あり、その名残で当時のままの業務運用が行われているものがある。
 - gTLD などドメイン名の登録にあたってネームサーバの登録も必須となっているものがあり、事業者や登録者がJP ドメイン名でも同様の業務運用を行っているものがある。

日本語JPドメインについて

- 特に日本語 JP ドメイン名には以下の傾向がある
 - LAME 率が高い(79%)
 - LAME率とnsnone(まったくゾーンのデータを引けなかったもの)の割合がほぼ一致
 - 一部の設定間違いではない
 - badnsは比較的少ない(10.3%)
- これはドメイン名の運用稼働率がまだ低いために、DNS登録だけして使っていないという傾向が他よりも高い数値となって表れているものと考えられる。そのため、他のドメインよりもLAME以外のエラー率は少ない。

改善に向けて

- 連絡をとる
 - mailで連絡？ whois？ SOA？
 - 電話で連絡？ (レジストリデータベースより)
 - JPNIC/JPRS指定事業者？
- ある意見として、駄目なところはdelegationしない
- ユーザによるチェック
 - チェック環境をつくってユーザに調べてもらう
 - Web interfaceが必要
 - どうも、他人に自分のところを調べてもらいたくない人が多いらしい
 - ドメイン名がわかればdigでもわかることだが
 - JPNICがチェックページを公開した場合、駄目なゾーンはJPNICが駄目と認定したことになる？
 - DNSQC-TFでは仕様を決めて、善意の第三者が作る？

議論

- どこかにチェックページがあったとして、他人のサイトを調べるのは？
 - いいこと？ 悪いこと？
 - 他人に指摘されるとうれしい？
 - 2chにだめなドメイン名公開されたり？
- ドメイン名さえわかれば、ふつうにDNS Queryするだけ
- どうやって指摘すると直してもらえるか