DNS運用健全化タスクフォース

2002年12月19日　DNS Day

DNSQC-TF
石田慶樹
yoshiki@mex.ad.jp

DNSの現状

- 全体的には、一見「概ねうまく動いている」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が多く見られる
  - レジストリやプロバイダへの問い合わせ
  - 各ホストで動いているネームサーバのエラーログ
  - JP DNSへの問い合わせパケットの到達状況
  - これまでのIETF, NANOG等各種ミーティングにおける調査報告、議論(CAIDA等)

DNSの現状(続き)

- サーバのログによる(2002年12月9日)
  - カスタマ以外の再帰的なqueryを拒否するネームサーバへの問い合わせ
  - 一日に約1.9万件の不正な(再帰的)問い合わせ
  - 問い合わせを行うホスト(IPアドレス)数は約2,100ホスト
  - 上位3位のホストから計約1.1万件の不正な問いあわせ
  - 上位4位から10位のホストで計約1,300件
  - 問い合わせするアドレスブロックには偏り

⇒問題のある設定

  - 誤った設定の局在
  - 誤った設定の広がり
  - 誤った設定の修正の困難性

よくある間違い

- **設定の誤り、不適切な設定**
  - **いわゆる**Lame delegation(RFC1912)
  - NS、MX**で指定された名前が**CNAME(RFC1912, 2181)
  - SOA**の値が不適切**(RFC1912)
  - “.”**のつけ忘れ**
  - **プライベートアドレスを外部に問い合わせ**(RFC1918)
  - **プライベートアドレスの登録**
- **問題のある**BIND**の使用**
  - 8.3.0(DNS**パケットストームを惹き起こす**)
  - **セキュリティホールのあるバージョンの使用**

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
  - BIND ネームサーバの更新に関するお願い(JPNIC)
    - http://www.nic.ad.jp/ja/topics/2002/20020207-01.html

DNSが不安定な原因

- 自組織DNSの動作異常は発見しにくい
  - ネームサーバのログの監視
  - 設定としては文法的に正しいが外部からは問題となる設定
  - 上位や他のDNSとの不整合による問題の発生
- 外部からの連絡で異常が発覚する場合が多い

⇒このような状況をどう改善するべきか

DNSの運用健全化の必要性

- 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(特にJPで)の連携が必要

DNS運用健全化タスクフォース (DNSQC-TF)

- DNSサーバに対する網羅的な調査
  ⇒中立的な公益法人(JPNIC内)に設置
- DNSに関する技術スキル
  ⇒WIDE Projectが技術サポート
- JP DNS管理組織との連携
  ⇒JPRS / JP DNS managersと連携
- 「DNS運用健全化タスクフォース(DNSQC-TF)」
  - JPNIC内に設立
  - 2002年5月に活動を開始
  - JPNIC, WIDE Project, JPRSという3組織の共同運用

DNSQC-TFの活動

- 2002年度の活動内容
  - 基本的な技術(チェックツール等)の開発
  - 現状の分析
  - 判明した問題点のコミュニティへの発信
  - 自らの設定のチェック手段の提供
  - 実運用ベースでのサービス化の検討
  - 実運用に伴う個別通知に向けた環境作り

活動スケジュール

- 2002年5月
  - **設立**
- 2002年7月
  - **活動開始報告**(JANOG10 meeting)
- 2002年12月
  - **中間報告**(Internet Week2002 / DNS Day)***←今日はここ***
  - **中間報告**(Internet Week 2002 / IP meeting)
- 2003年1月
  - **進捗報告**(JANOG11 meeting)
- 2003年3月
  - **最終報告**

DNSQC-TFに関連した調査

- [第0段階] 予備調査
  - 2002年6月
  - 加藤朗氏による第0次調査
  - IETF/JANOG-10における発表
- [第1段階] 試行調査
  - 2002年11月
  - 開発中のツールのデバッグも兼ねて
  - 本報告他で発表
- [第2段階] 本格調査
  - 2003年1月～3月に調査予定
  - 管理者へのフィードバックも検討

[第2段階]試行調査

- 2002年11月1日～11日に実施
- JP配下のトップレベルのドメイン
  - 属性型･地域型ドメイン
  - 汎用ドメイン
- 逆引きは未調査
- 約38万ドメインを対象

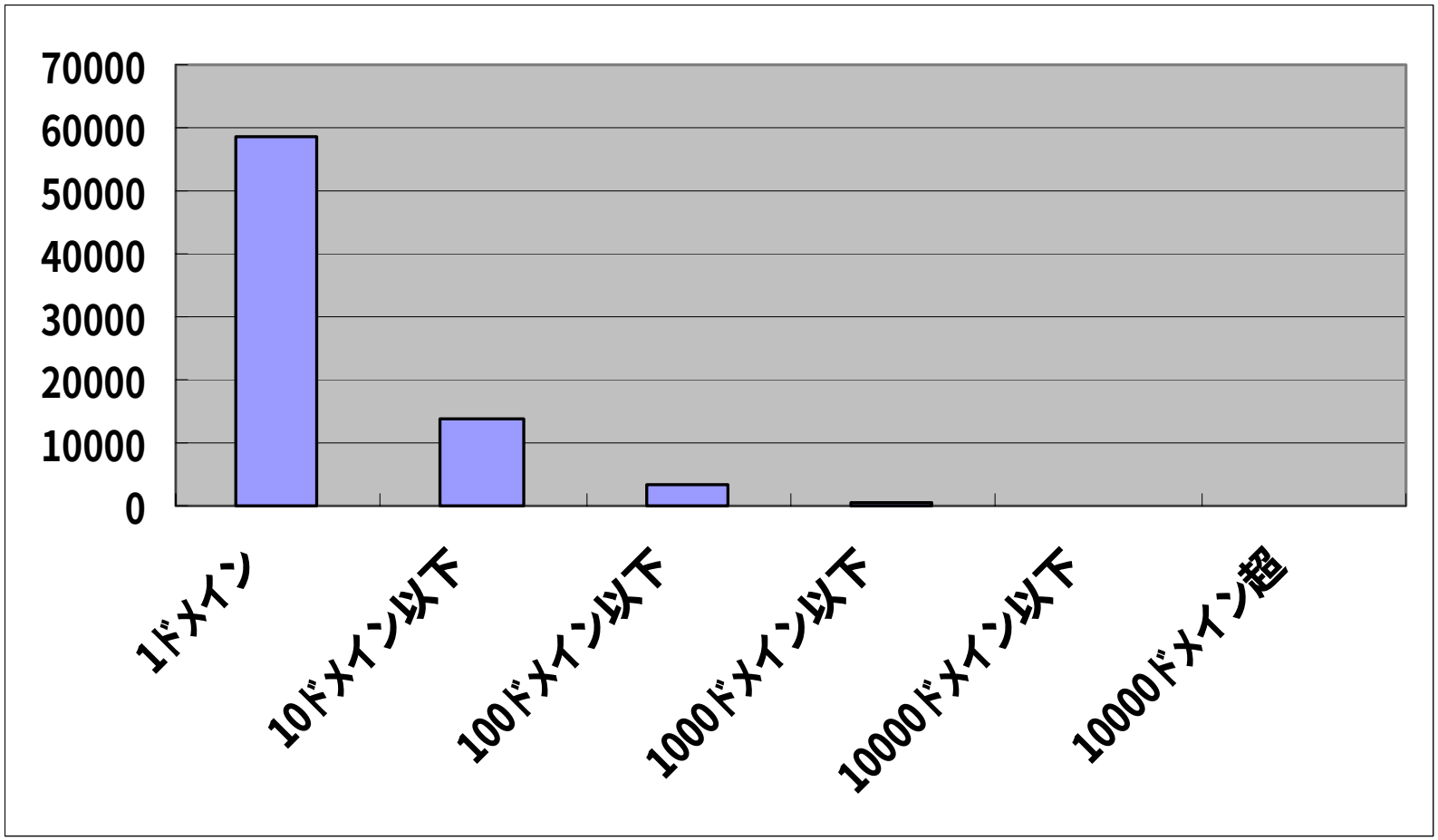
試行調査結果のまとめ(1)

- ドメイン数は381,000ドメイン
  - 何らかのエラーのあるドメイン数：155,000
  - エラー率：40.7%
- エラーの種別
  - プライベートアドレスが登録:103(0.02%)
  - SOAが不適切：1,350(0.35%)
  - NSレコード不一致：84,100(22.1%)
  - Lame Delegation: 61,100(16.0%)
  - NSレコードにCNAME：2,360(0.62%)
  - MXレコードにCNAME:17,000(4.46%)

試行調査結果のまとめ(2)

- ネームサーバに着目
- JPドメインをサーブするネームサーバ数は76,600サーバ
  - JPに属さないサーバ数は7,660サーバ
  - 1サーバあたり平均5ドメインをサーブ
    - 1万ドメイン以上を登録しているサーバ数：7台
    - 1ドメインしか登録してないサーバ数：58,800台(76.7%)

試行調査結果のまとめ(3)



試行調査結果のまとめ(4)

- サーバ毎のエラー状況
  - 何らかのエラーがあるサーバ：43,700サーバ
  - エラー率
    - 全サーバに対して：57.1%
  - 登録されている全ドメインで何らかのエラーがあるサーバ数:34,500サーバ
  - エラー率
    - 全サーバに対して：45.0%
    - エラーを有するサーバに対して：78.8%

試行調査結果のまとめ(5)

- 1ドメインのみのサーバに注目
  - エラーがあるサーバ：29,500サーバ
  - エラー率
    - 全サーバに対して：38.5%
    - エラーを有するサーバに対して：67.1%
    - 1ドメインのみのサーバに対して：49.9%

⇒多数のサーバ(管理者)に対して対象に注意を促す必要がある

エラーとして検出する例

- SOAのメイルアドレスに root.jprs.jp. -> root@jprs.jp など, (軽微)
- SOAの中に使ってはいけない文字がある, ホスト名に下線がある (軽微)
- NSレコードのNSホスト名に下線がある (軽微)
- MXにCNAME (軽微だとおもおう, 規定違反)
- NSにCNAME (規定違反)
- NSリストの不一致 (良くない場合と, 軽微な場合)
- Lame Delegation (良くない)
- NS, MXレコードにプライベートアドレスが設定(子どもが) (良くない)
- unreachable な NS (良くない, 一次的な状況も)
- アドレスが解決できない NS (だめ)
- (違うドメイン名のNS, jpとcomの混在 (セキュリティリスクが大きく))
  - 最後の項はチェックしていない. 微妙な問題.

改善すべきエラー(1)

- Lame Delegation
  - **指定されたNSにそのゾーンの情報が発見できない**
    発生する原因:
    (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**

⇒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**

改善すべきエラー(2)

- **親に登録されたNSのリストと，そのゾーンに登録されたNSの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
  - **親のNSのリスト⊃子のNSのリスト <--- 問題**
  - **子のNSにLame がある　　<--- 問題**
  - **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

今後の展開

- **セルフチェックの機構**
  - Webページを介したチェック
  - 2003年1月中には開始の予定
  - http://www.nic.ad.jp/ja/dnsqc/index.html
- **利用のためのインタフェース**
  - メイイルアドレスを登録
  - 特定のドメインのチェックを指定されたメイルアドレスに返信

今後の展開(続き)

- DNSQC-TFとして本格調査
  - 2003年3月中までには実施予定
  - わかりやすいような形式で実施
    - 試行するホストのドメイン名
    - 試行するホストの逆引きドメイン名
    - 情報提供ためのWebページの容易
  - 最終報告書としてまとめ
- 継続的かつ定期的にチェックを行う機構
  - JPRS/JPNICが主体として展開
  - ドメイン登録時，変更時，あるいは定期的なチェックを行う
  - 現在様々な検討を行っている段階