GMO INTERNET

見抜く力を！データを見て対策を考える (権威サーバ)

Internet Week 2016

2016/12/01

GMOインターネット株式会社

永井祐弥

GMO INTERNET

本日のアジェンダ

- 自己紹介
- データとは？
- データの取り方
- データを見てますか？
- データを見て対策を考える
- まとめ
- おまけ

自己紹介

名前

永井　祐弥（ながい　ゆうや）

所属

GMOインターネット株式会社

システム本部 インフラサービス開発部

担当

2012年にGMOインターネットへ入社。お名前.com、ConoHa、Z.comのDNSや、GMOインターネットグループ会社でレジストリシステムのDNSなど、DNS関連サービスの開発、運用を担当

GMOインターネットって？

このようなサービスを提供しています
- ドメイン名事業「お名前.com」「Z.com Domain」
- サーバ事業「ConoHa」「Z.com Cloud」など

DNSサービスの種類も多数
- 権威DNSサーバ
  - レンタルDNS（85万ゾーン、760万レコード）
  - セカンダリDNS（7千ゾーン）
  - ドメインパーキング
- キャッシュDNSサーバ
  - VPS向け（6万サーバ）

データとは？

- データの主な意味（辞書から引用）
  - データ、資料、(観察や実験による)事実、知識、情報
- データに含まれるもの
  - データログ
  - 統計情報
  - 分析レポート
- データから得られるもの
  - 稼働状況
  - 需要予測
  - 攻撃兆候

データを取得する その1

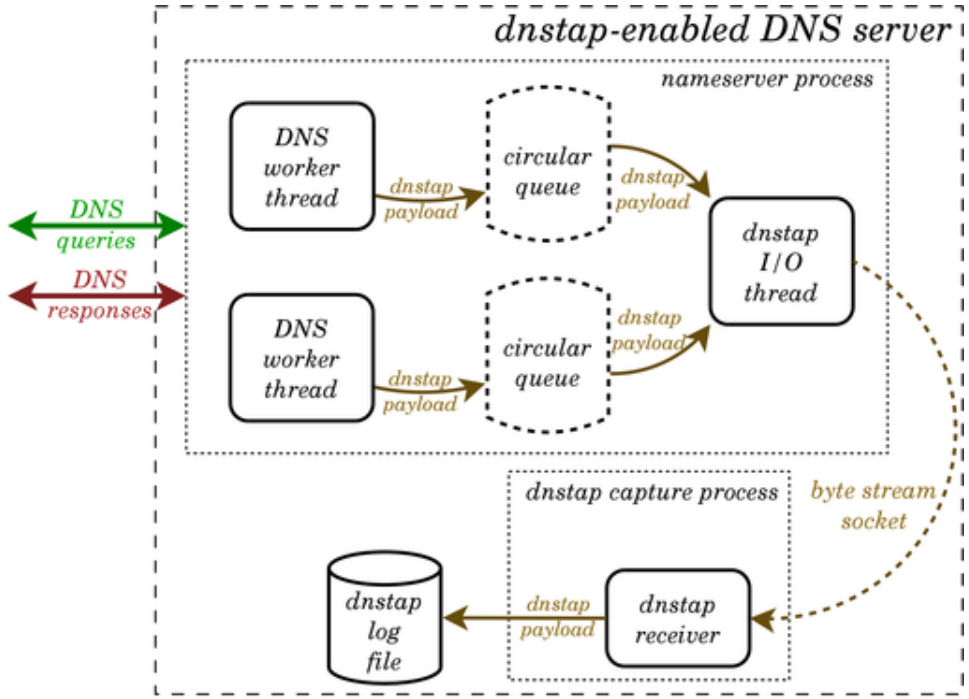
- ネームサーバのロギング機能
  - BIND 9.x系
    - クエリログあり（File、Syslog）
  - PowerDNS 3.x系
    - クエリログあり（Syslogのみ）
  - NSD
    - クエリログなし
  - KnotDNS
    - クエリログなし
- 監視においても重要な役割
- 但しクエリログはパフォーマンスに影響する

データを取得する その2

- ネットワークパケットキャプチャ
  - DNS statistics collector (DSC)
  - Men & Mice DNS Traffic Monitor
  - momentum DNS viewer
- アプリケーションの種類に依存しない
  - クエリログが取れないNSDやKnotDNSでも動作
  - パフォーマンスに影響しない
  - データ取得環境をネームサーバと分けて用意出来る
- フラグメントパケットや、キャプチャを設置する箇所によっては拾いきれない場合あり

データを取得する その3

- dnstap
  - high speed DNS logging without packet capture
- 対応済みアプリケーション
  - BIND 9.11
  - Unbound 1.5
  - KnotDNS 2.x
- 対応計画中
  - NSD
  - PowerDNS



データを取得する その4

- Nagios、Munin、Cactiなどリソース監視を目的としたツール類
  - ネットワークの帯域、サーバのCPU、メモリ、ディスクI/Oが不足していると、期待しているパフォーマンスが十分に発揮しない場合がある
- 外部モニタリングサービス
  - 外部ネットワークから到達性や遅延などを監視
  - SLAを保証するDNSサービスでは必須

データを見てますか？

- そもそもログを取っていない…
  - ログの存在を知らなかった
  - ログの取り方がわからない
  - ログを取りたいけど取れない
  - ログなんて必要ない！（キリッ
- ログは取ってるけど…
  - 見方がわからない
  - 見る頻度が少ない
  - 見たいけど見れない
  - 見る必要なんてない！（キリッ

データを見てますか？続き

- 余程の事がない限りDNSサーバは動き続ける
  - 異常が発生しないと気がつかない
- 異常のしきい値は一定ではない
  - 監視ツールで全てをカバーするのは難しい
- 日頃からクエリの傾向を掴んでおくことが大切
  - 「いつもと違う」を感じられるようになること

データを見てますか？続き

- 見るべきポイント
  - ピーク時のデータ
    - クエリ数がキャパシティを超えそうになっていませんか？
    - リソース（CPU/メモリ/帯域/…）は足りていますか？
  - 応答ステータス（RCODE）
    - SERVFAIL/REFUSEDなど増えていませんか？
    - NOERRORでもANYレコードばかり来ていませんか？
  - ログ
    - エラーメッセージが記録されていませんか？

データを見て対策を考える

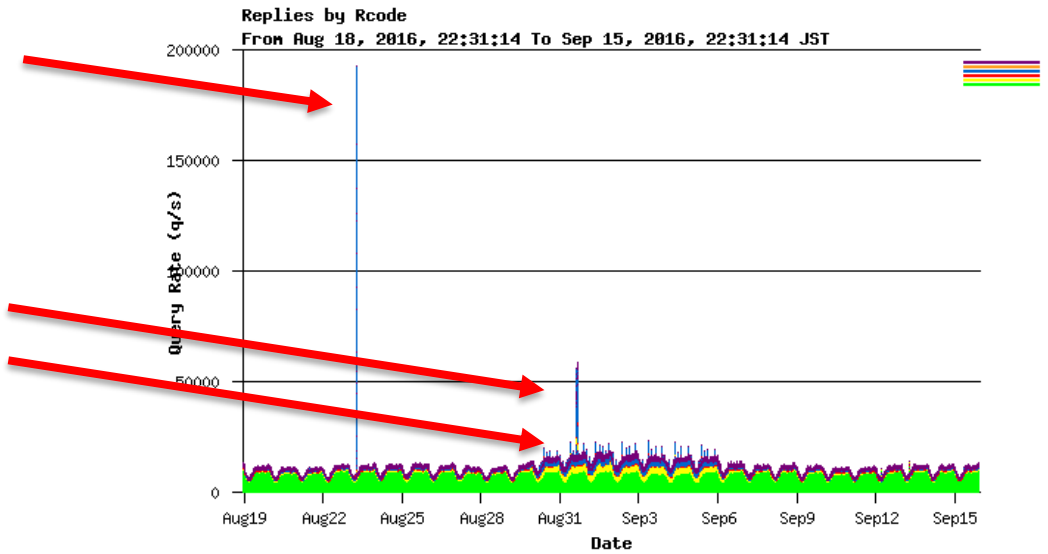
事象発生	データを見て事象を認識する
原因調査	事象が発生した理由や原因を調査する
対策実施	異常がある場合は対策を行う
監視（検知）	事象が発生した事を検知する

データを見る前の注意事項

- これから紹介する内容は架空のネームサーバの出来事です
- 実在するDNSサービスやネームサーバとは一切関係ありません
- グラフはDSCのデータを元に話を進めます

データを見る（ケース1）

- 権威DNSサーバがRCODEを
  SERVFAIL/REFUSEDで返すケース



データを見る（ケース1）

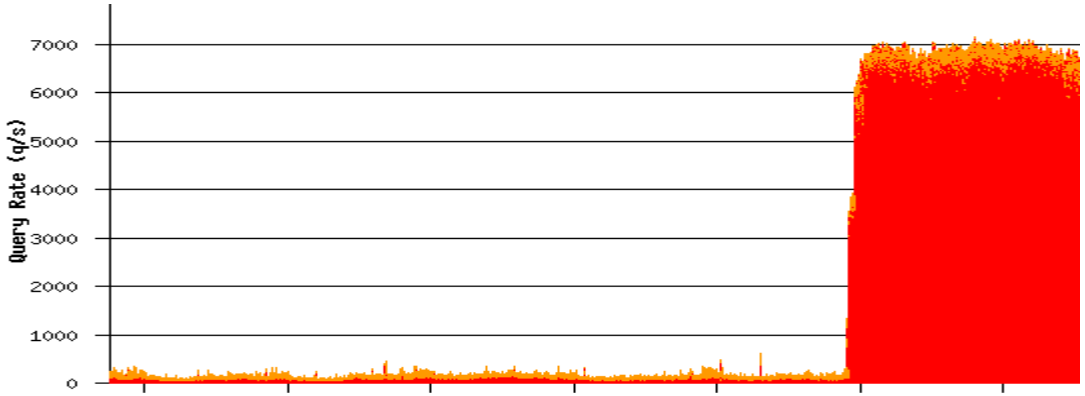
- 原因
  - Lame Delegation
  - 理由は様々だがこの権威DNSサーバからゾーンが削除された
  - 消えたレコードを求めてクエリが増加
- 傾向
  - メールサービス関係は特に注意が必要
  - 退蔵されるドメイン名に多い傾向がある

データを見る（ケース1）

- 対策
  - ネームサーバ情報を変更、あるいは削除
  - ゾーンを設定する（ネガティブキャッシュさせる）
    - SOAレコード、NSレコードがあればよい
    - プライベートネットワークで使われていることもあるので注意
- 検知
  - 統計情報を出してREFUSED/SERVFAILのカウント値を計測する
  - DSCならRcodesのグラフを参照する

データを見る（ケース2）

- 権威DNSサーバがRCODEをNXDOMAINで返すケース
- ランダムサブドメイン名で大量のクエリ




```
queries: info: client X.X.X.X#XXX (409a276749a266d6b15c30ff39a0a012.example.test): query: 409a276749a266d6b15c30ff39a0a012.example.test IN
queries: info: client X.X.X.X#XXX (08062f9b15991bc7ce59232b2fa6367d.example.test): query: 08062f9b15991bc7ce59232b2fa6367d.example.test IN
queries: info: client X.X.X.X#XXX (3f8f6e5263e47eaecb7289c64738e4ed.example.test): query: 3f8f6e5263e47eaecb7289c64738e4ed.example.test IN
queries: info: client X.X.X.X#XXX (4ecaba219f7fcd8a95996d59fb70a461.example.test): query: 4ecaba219f7fcd8a95996d59fb70a461.example.test IN
queries: info: client X.X.X.X#XXX (2c778f8576f86d77f5d43e84c79d42c2.example.test): query: 2c778f8576f86d77f5d43e84c79d42c2.example.test IN
queries: info: client X.X.X.X#XXX (ab493b28ba7cc159123fc342e9333cf0.example.test): query: ab493b28ba7cc159123fc342e9333cf0.example.test IN
queries: info: client X.X.X.X#XXX (2537da1010d0eb2b28c68a27b61ba8b2.example.test): query: 2537da1010d0eb2b28c68a27b61ba8b2.example.test IN
queries: info: client X.X.X.X#XXX (04abba3aad66bc35088fb861a2b5594e.example.test): query: 04abba3aad66bc35088fb861a2b5594e.example.test IN
queries: info: client X.X.X.X#XXX (d2e6f300cfd337115f66cc4bbc416e51.example.test): query: d2e6f300cfd337115f66cc4bbc416e51.example.test IN
queries: info: client X.X.X.X#XXX (18d94981e1f4be7f59a511c9d08cae84.example.test): query: 18d94981e1f4be7f59a511c9d08cae84.example.test IN
```

データを見る（ケース2）

- 原因
  - 水責め攻撃
  - キャッシュDNSサーバも辛いけど、権威DNSサーバも辛い
  - 権威DNSサーバは異常なクエリをIPアドレスでフィルタしてはいけない
    - キャッシュDNSサーバからの正常なクエリも落としてしまう
- 傾向
  - 不定（ある日、突然）
  - SNSに犯行声明が投稿される場合もある

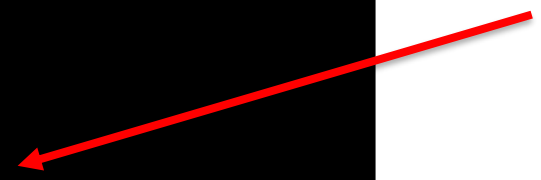
データを見る（ケース2）

- 対策
  - 退避用の権威DNSサーバを用意して、水責め攻撃を受けているドメイン名をそちらに誘導する
    - DNSサーバ引っ越しの原理を応用
  - ネームサーバの変更/削除を行う
    - 権威DNSサーバがどう頑張っても耐えられない場合の緊急手段
    - 元に戻すことを考えると合理的ではない
- 検知
  - qps（query per second）の増加を検知する
  - DSCなら以下のグラフを参照する
    - By nodes
    - 2nd Level Domains / 3rd Level Domains

データを見る（ケース3）

- 事象
  - Slaveのネームサーバ（BIND 9）が起動するまでに時間がかかる
  - あるいはゾーン転送を始めるまでに時間がかかる
  - rndcコマンドで状態を見てみると…

```
root@server:~# rndc status
version: 9.9.x
number of zones: 12345
debug level: 0
xfers running: 100
xfers deferred: 0
soa queries in progress: 4321
recursive clients: 0/0/1000
```



データを見る（ケース3）

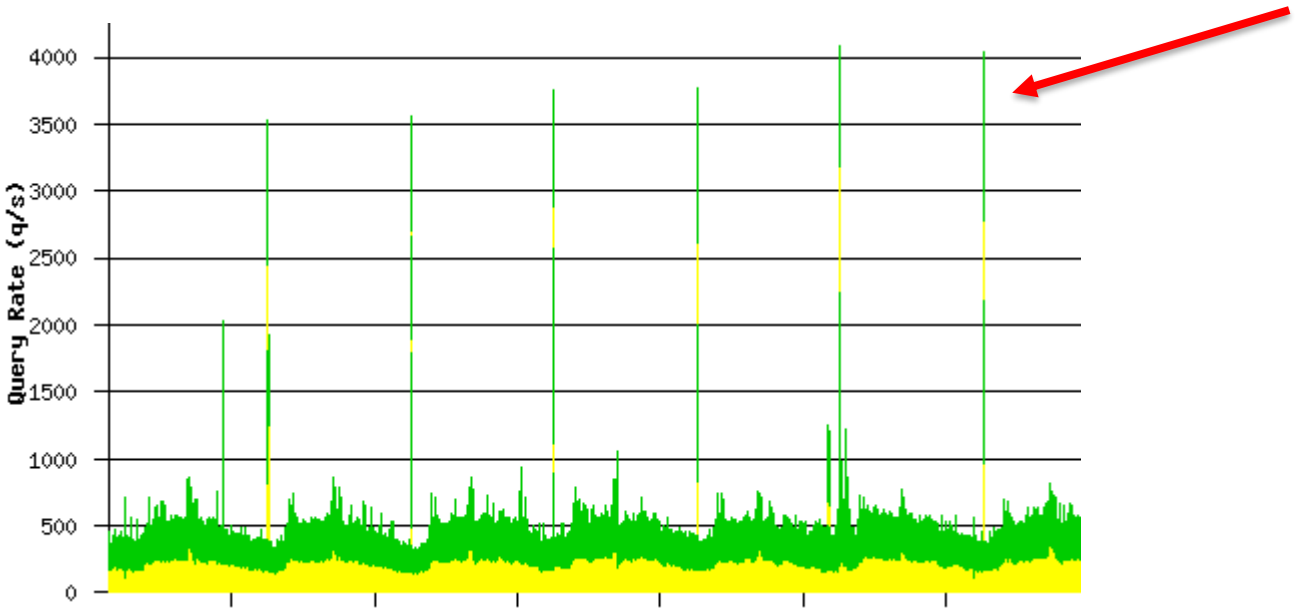
- 原因
  - ゾーン転送処理中のキューがMasterのネームサーバが応答しない等の理由でタイムアウトを待っている
  - タイムアウトが解消されないと次のゾーン転送処理が開始されない
- 傾向
  - 多数のMasterや、ゾーンが登録されるような環境で発生しやすい

データを見る（ケース3）

- 対策
  - 不要なゾーンを設定ファイルから定期的に削除する
  - チューニングを行う
    - タイムアウトを短くする
      - max-transfer-time-in、max-transfer-idle-in
    - 同時ゾーン転送数を大きくする
      - transfers-in、transfers-per-ns、tcp-clients
    - ゾーンの更新頻度を下げる
      - min-refresh-time, min-retry-time
- 検知
  - rndc status
    - soa queries in progressが増えすぎていないか

データを見る（ケース4）

- 事象
  - 毎日決まった時間に大量のクエリが届く
  - クエリログを見るとリスト検索しているような形跡



データを見る（ケース4）

- 原因
  - クローラからの名前解決
    - ドメイン名の不正利用の監視
    - リソースレコードの監視
    - WEBサービス（検索エンジン/アフェリエイト/…）
- 傾向
  - 大量のドメイン名を保有するネームサーバで発生しやすい
  - ドメイン名のネームサーバを大量に設定した直後は特に発生しやすい（新gTLD系）

データを見る（ケース4）

- 対策
  - パフォーマンスに影響するようなら権威DNSサーバを増強
    - DNS的には正規のクエリ
    - 相手がクローラとはいえ攻撃ではないのでフィルタは厳しい
  - 接続元管理者に問い合わせ
    - クローリングをやめてもらう
    - 頻度を減らしてもらう
- 検知
  - qpsの増加を検知する
  - DSCならBy Nodesのグラフを参照する

まとめ

- データを取ろう！
  - 日々のデータの積み重ねが大事
  - データの管理も忘れずに
- データを見よう！
  - 異常はデータに現れる
  - 「いつもと違う」を感じられるようになろう
- 対策を考えよう！
  - データから異常を検知しよう
  - 検知した後の手順や対応方法を決めておこう
  - 取得するデータや、監視のしきい値を定期的に見直そう

おまけ

- DSCのススメ
  - お手軽、簡単
  - 見たいものが最初から揃っている
  - 説明資料にグラフの画像が使える
  - 収集したデータはXMLファイルやJSONファイルに保存されるので、自作ツールでアレコレやり放題
    - 1分毎にファイルが作成される
    - 記録されるのは1分間の累計値（count）
    - 秒間の値は累計値から60で割る

```
<ClientAddr val="X.X.X.X" count="123456"/>
<SecondLD val="example.test" count="1234"/>
<ThirdLD val="sub.example.test" count="1234"/>
```

すべての人にインターネット

GMO