権威DNSの監視

2014年11月20日（木）

Internet Week 2014 DNS DAY

株式会社日本レジストリサービス（JPRS）

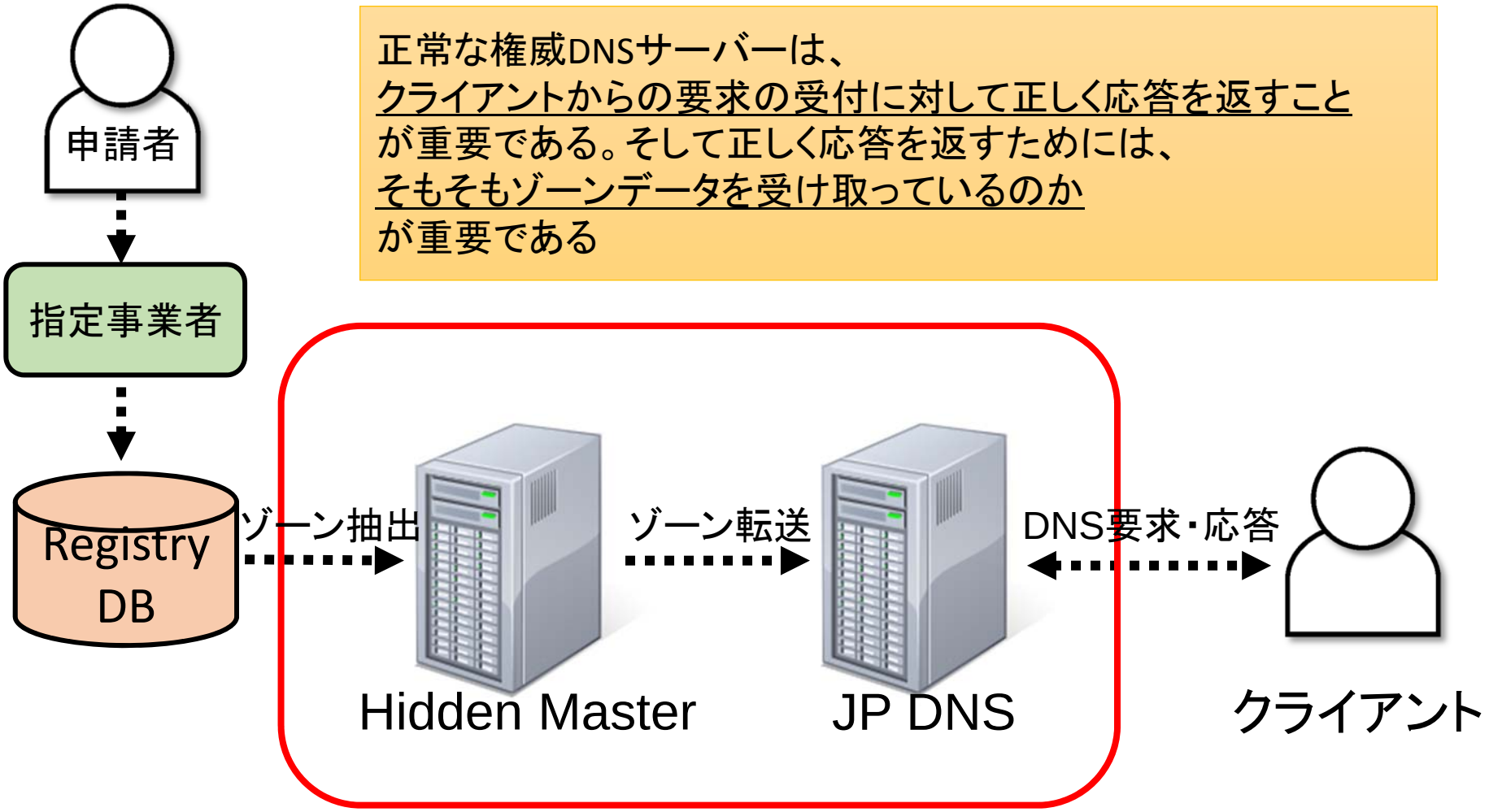
坂口　智哉（Tomoya Sakaguchi）

はじめに

■ 権威DNSサーバーの監視について
- ここでは権威DNSサーバーならではの監視について取り上げます
- サーバーのリソース監視や死活監視など一般的な監視は説明対象外としています

■ 目次
- 本日お話しする範囲
- ゾーン抽出の監視
- ゾーン転送の監視
- JP DNS監視
- まとめ

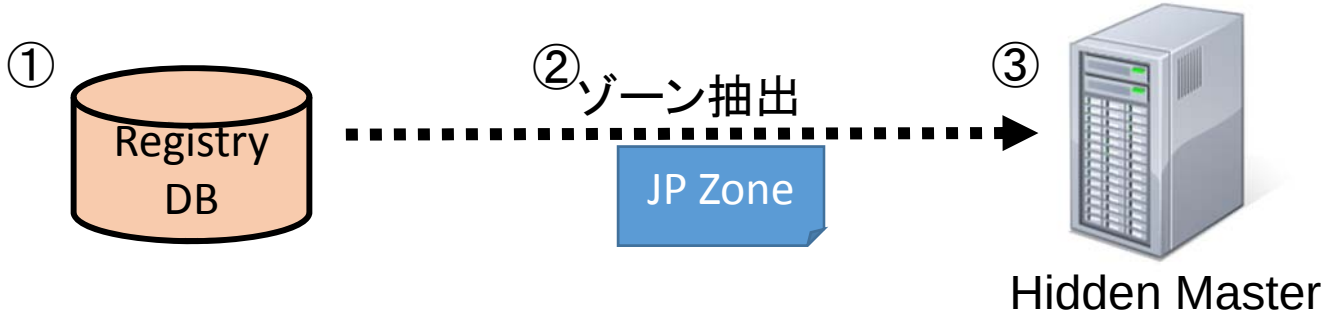
本日お話しする範囲



正常な権威DNSサーバーは、
クライアントからの要求の受付に対して正しく応答を返すこと
が重要である。そして正しく応答を返すためには、
そもそもゾーンデータを受け取っているのか
が重要である

ゾーンの抽出～DNS要求・応答までの間で
JPRS が行っている監視についてご紹介

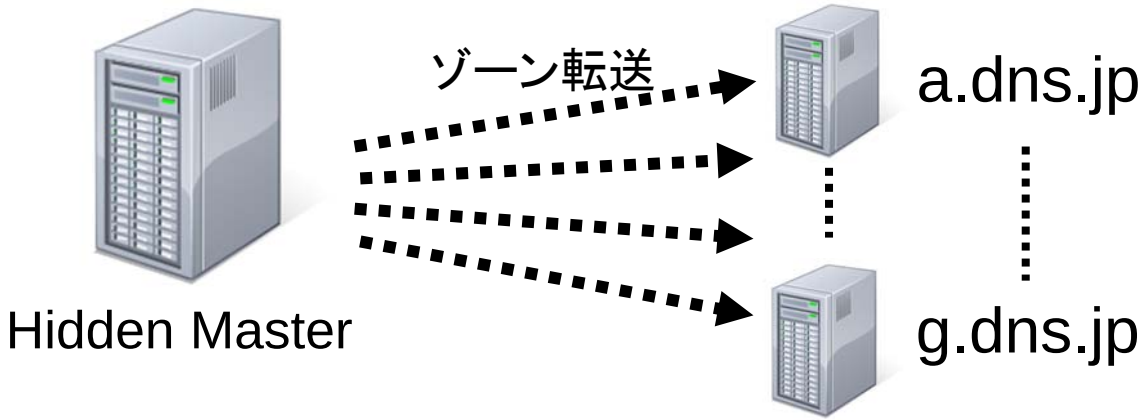
ゾーン抽出の監視



- ゾーン抽出の監視：ゾーンデータ変化量の監視
  - 前回と今回のゾーンデータ比較を行い、変化量が一定の閾値を超えたら異常とする
  - ①～③のいずれかで何らか異常が発生した場合、生成されるゾーンデータに変化があるはずである
- ゾーンデータ変化量の監視におけるアクション
  - 監視で異常を検知した場合は Hidden MasterのDNSサーバープロセスを強制停止することにより、不適切なデータの転送を確実に防ぐようにする

JPレジストリシステムでは、汎用JPと、属性型JPについてはラベル単位で監視
これまでこの仕組みが動いた実績は何度かあり、いずれも問題ないものであった
→ お客様が一気に登録情報を書き換えた場合などに検知することがある

ゾーン転送の監視



■ ゾーン転送の監視：SOAシリアル値の監視

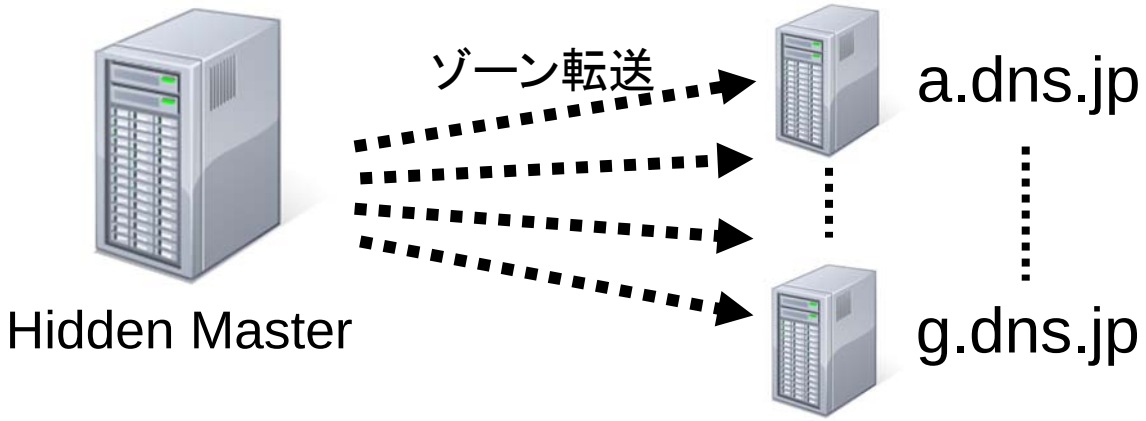
- 各JP DNSがゾーンを更新できているかどうかをJPゾーンのSOAシリアル値がHidden Masterとそろっているかどうかで定期的に確認
- Hidden MasterからJP DNSへのゾーン転送で何らかの異常が発生した場合ゾーン情報が更新されず、古い情報を応答するはずである

■ JP DNSで実施しているSOAシリアル値の監視

- JP DNSの場合、海外拠点のサーバーもいくつか存在し、それぞれRTTが異なる
- そのためSOAシリアル値の監視も遅延の閾値パラメータを各サーバーごとにフレキシブルに設定できるよう工夫

異常を検知した場合はアラートを出すのみで復旧はオペレータが手動で実施
監視ツールは自作。残念ながら今のところ公開の予定はありません

ゾーン転送の監視



■ ゾーン転送の監視：ゾーンデータの整合性の監視

- 各サーバーのゾーンデータが正しいかどうかを定期的に確認
- ゾーン転送やサーバーに異常があった場合、ゾーンデータに異常が生じる
- JPドメイン名は2014年11月現在約138万件、ゾーンデータサイズがそれなりに大きいため、平常時は差分転送(IXFR)を採用

■ JP DNSで実施しているゾーンデータの整合性の監視

- 監視サーバーから各JP DNSに対してゾーン転送要求（AXFR)を行い、Hidden Masterと同一であるかどうかを確認
- SOAシリアル値監視と同様、各サーバーごとに遅延閾値パラメータを設定

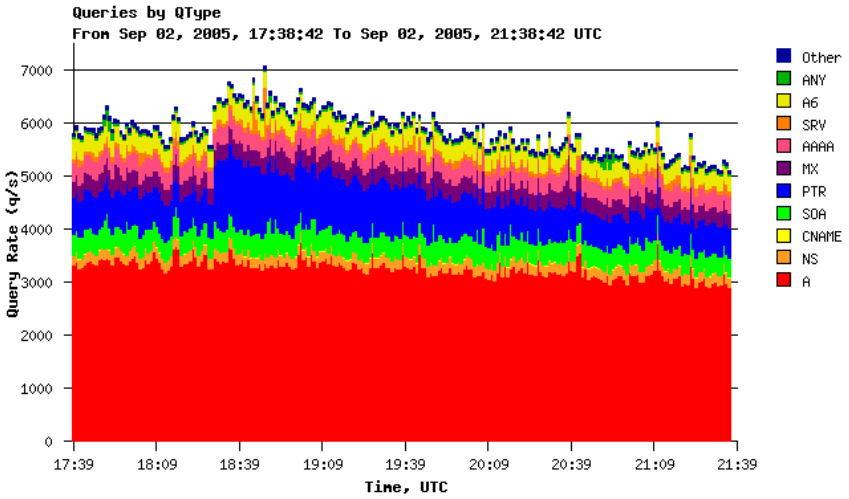
発生することはまれであるため、アラートが出た場合はオペレータが手動で復旧

JP DNS監視（1）

今風のWeb UIの Hedgehogというツールもある
(L-Rootで使われている)
https://github.com/dns-stats/hedgehog

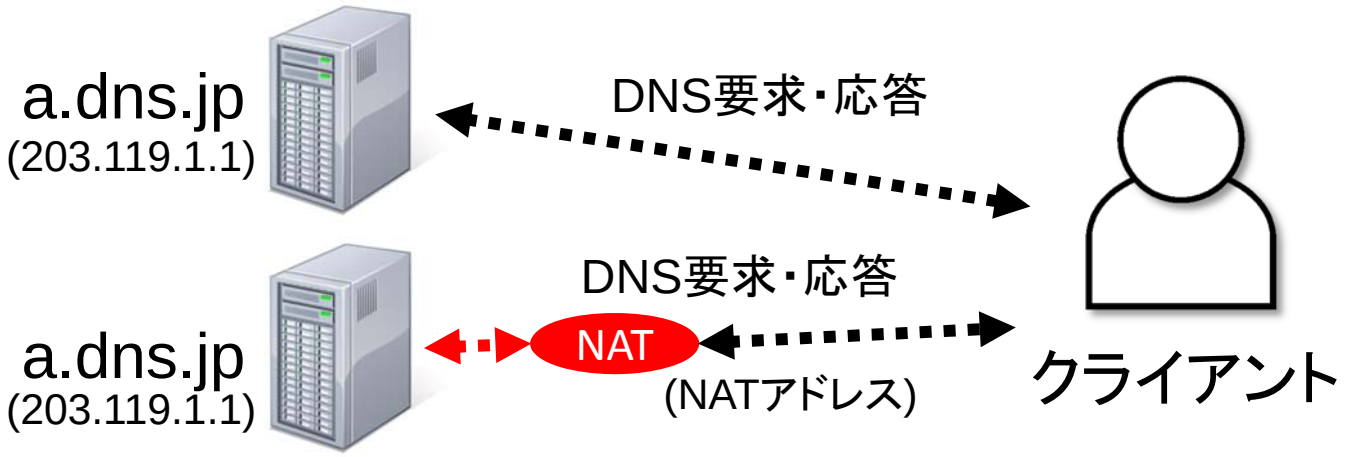
■ JP DNS監視：クエリ監視

- JP DNSでは DSC (DNS Statistics Collector) を利用している
- http://dns.measurement-factory.com/tools/dsc/
- 大量のクエリ、異常なパターンのクエリがきた場合にどのようなクエリがきているか、問題があるかを確認



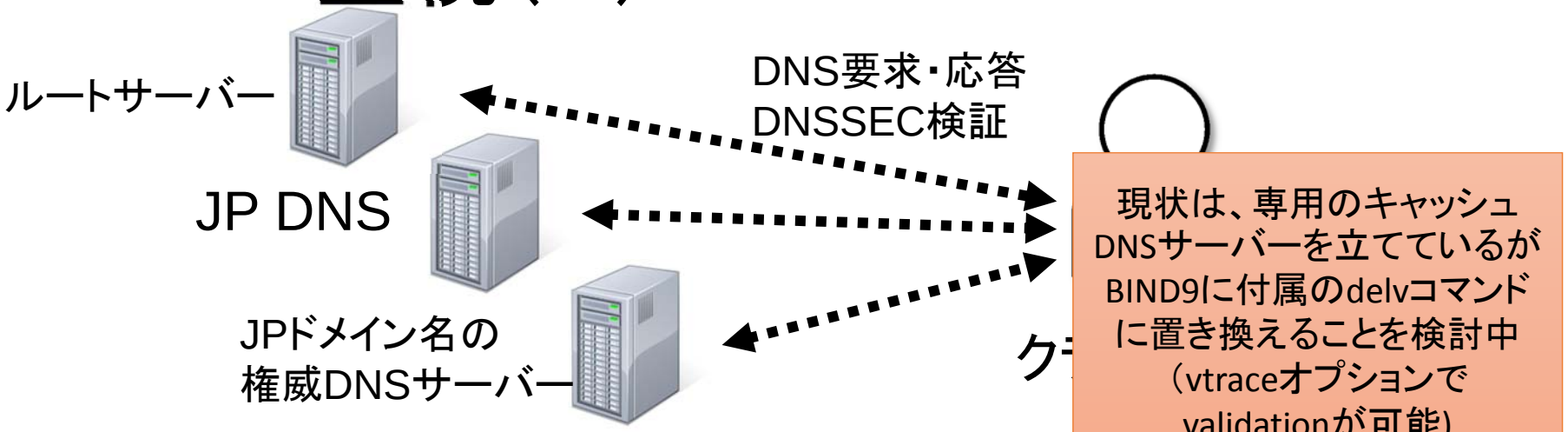
単純なトラフィック異常については機械的に監視しているが、
それ以外は、現状、定期的にオペレータが監視

JP DNS監視（2）



- JP DNSにおける監視：Anycastの各ノードの監視
  - JP DNSは IP Anycast 技術を使い、複数の拠点にサーバーを配置している
  - それぞれのサーバーノードが正常に稼働しているか確認する必要があるが、Anycastの場合、サービス用のIPアドレスが同一であるためそれぞれのサーバーノードを監視することが難しい
- JP DNSで実施している監視手法
  - 各Anycast拠点においてNAT箱を用意し、Anycastのサービスアドレスを NAT変換し、NATアドレスに対して応答確認を行う
  - JP DNSに特殊な設定を入れることなく監視が可能

JP DNS監視（3）



■ JP DNSの監視：DNSSEC信頼の連鎖の監視

- 信頼の連鎖が途切れていないかどうかを定期的にチェック
- ルートゾーン～JPドメイン名の権威DNSサーバーにおいて何らかの異常が発生するとDNSSEC信頼の連鎖が途切れる可能性

■ DNSSEC信頼の連鎖の監視におけるアクション

- JPRSでは現状のところアラートを出すのみに留まっている
- 発生した場合は致命的なパターン
- 最悪のケースではIANAへ緊急連絡を入れてルートゾーンからDSレコードを削除する可能性も想定

今のところ、この監視が活躍した場面はない

監視で重要なこと

- 一面のみの監視ではなく、複数の要素を対象とした多面的な監視が重要
  - 権威DNSサーバーおいてはクライアントからの要求・応答、サーバーのリソース監視以外にゾーンデータ（コンテンツ）の完全性も気にする必要がある

- 想定内の状況しか監視はできない
  - 想定しえない異常は監視をしていても検知できない場合があることに留意が必要
  - 想定しえない異常が発生した場合、次回以降は想定されるものとしてより良い監視に役立てるという姿勢が重要（経験・ノウハウの蓄積）