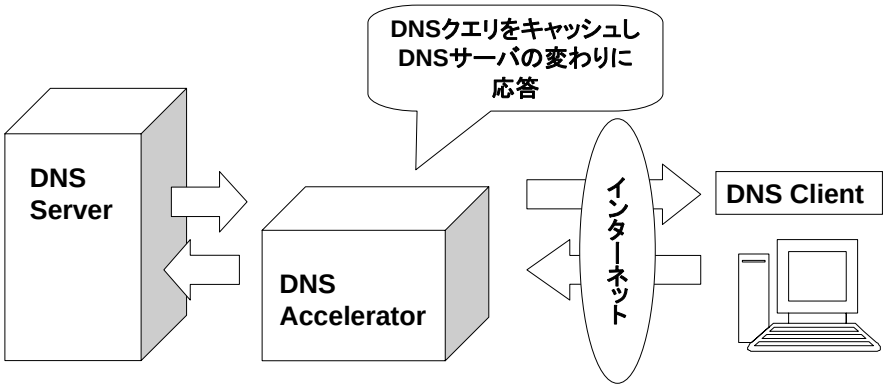
DNSの応答速度を改善する新しいキャッシュシステム2

50万qpsを超えるDNS応答の測定方法について

DNS Accelerator

DNS Acceleratorとは、
DNSサーバの応答を手助けするシステム



BINDの応答速度

BIND9(.4.0)の応答速度を測定

送信：**queryperf**にて、**45,000qps**を送信
結果：**BIND9**より、**45,000qps**を応答

送信：**自作ツール**にて、**240,000qps**を送信
結果： **BIND9**より、**34,000qps**を応答

マシンスペック
CPU: Intel Xeon 1.86GHz

DNS Acceleratorの応答速度

DNS Accelerator使用時の応答速度を測定

測定条件

・DNSサーバは、前回の**BIND9**を使用
・キャッシュはすでに保存済みとする
・キャッシュされているデータは**50,000**とする

送信：**自作ツール**にて、**360,000qps**を送信
結果： **Accelerator**より、**360,000qps**を応答

DNS Acceleratorの応答速度2

DNS Accelerator使用時の応答速度を測定

送信：**自作ツール**にて、**700,000qps**を送信
結果：**Accelerator**より、**530,000qps**を応答

BIND9との比較

- **BIND9**: **34,000qps** (**47.1Mbps**)
- **Accelerator**: **530,000qps** (**733.5Mbps**)

（約**15～16**倍の速度）

※ ただし、あくまでも、あらかじめ
全データがキャッシュされた状態での速度

キャッシュ量による性能の低下

- 保存クエリ数が 1 の場合
  - 毎秒70万の要求クエリに対して、約60万の応答
- 保存クエリ数が 50,000 の場合
  - 毎秒70万の要求クエリに対して、約53万の応答

※ キャッシュしているデータ量により
5万～10万程度の性能低下がみられる

前回からの改善点

- 応答速度の改善
- キャッシュ汚染によるメモリリークを防止
- DoS（DDoS）攻撃を検知する機能を追加
- 特定の条件下にて、サーバへ送るパケット量を制限する機能を追加

※ このような機能を加えることで、DoS（DDoS）攻撃に対して、ある程度の対処ができる

DoS（DDoS）攻撃以外には効果なし

- DNS amplification attack（DNS amp）
- DNS Spoofing（Cache poisoning）
- DNS Rebinding Attack

このようなDNSに対するセキュリティ上の問題には、対処できない。

有用なテスト方法の考察

- 要求クエリや応答クエリが双方に届かずに、「応答なし」と判断されている可能性はないか？
- CPU以外の機器（NICやスイッチなど）がボトルネックになっていないか？

- ハッキングされる可能性はないか？
- 運用できるレベルの安定性を持っているか？
- 他に必要なテストはないか？

ご協力頂ける方を探しています

よろしくお願い致しますm(_ _)m

Email:
kenji@netagent.co.jp

ご清聴 ありがとうございました