動かしてみましたDNSSEC 権威DNSサーバ編

民田雅人
株式会社日本レジストリサービス
2010-07-08 JANOG26@恵比寿

権威DNSサーバの DNSSEC化による負荷の変化の調査

- DNSサーバハードウェアを2種類
  - 松: Xeon E5540(2.53GHz)x 2 CentOS 5.5
  - 梅: Pentium III 1.26GHz FreeBSD 8.0
- テストするゾーンデータを用意
  - 小規模ネットワークのDNSゾーン
- DNSサーバ(BIND 9.7系)を起動
- LAN接続の別サーバからdnsperfで負荷をかけ応答性能を計測
  - DNSSEC無し、DNSSEC有り(NSECとNSEC3)

計測に利用したデータ

- 計測対象のゾーンデータ
  - 手元で実運用している小規模ドメイン名のゾーンデータを、ほぼそのまま利用(総リソースレコード数 244)
- dnsperfで使うクエリデータ
  - 上記ゾーンのDNSサーバへのクエリログより生成
    ⇒ 実際に発生しているクエリを利用
- DNSSECパラメータ
  - 暗号化アルゴリズム　RSASHA256
  - KSK / ZSKの鍵長　2048bit / 1024bit

DNSサーバの DNSSEC化による負荷の変化

DNSSEC化による計算量の変化　(●:増加)

			権威	キャッシュ
通常応答		署名の検証	N/A	●
不在応答	NSEC	署名の検証	N/A	●
	NSEC3	署名の検証	N/A	●
		ハッシュ計算	●	●

(JANOG25「そこが知りたいDNSSEC」より再掲)

NSEC3でDNSSEC化した権威DNSサーバは、
不在応答時に負荷が増える

参考:NSEC3のハッシュ計算方法 (RFC 5155 セクション5)

- 問合せドメイン名、ソルト(Salt)、繰返し回数(Iterations)の3つのパラメータから計算
  - ドメイン名: 小文字に正規化したFQDNのワイヤフォーマット
  - ソルト: 任意のバイナリ文字列
  - ハッシュアルゴリズム: 現時点の規格はSHA1のみ
  1. ドメイン名とソルトを文字列的に結合しハッシュ計算
  2. 結果にソルトを結合してハッシュ計算
  3. 2をIterationsで指定した回数繰り返す
- Iterationsを増やすとドメイン名の秘匿性が高まる
  ⇒ Iterationsを増やすと計算量も増加

結果1: 各方式の応答性能比較

	方式	梅 (P-3)		松 (E5540)	
		存在	不在	存在	不在
DNSSEC無	N/A	9345	8855	58423	58248
DNSSEC有	NSEC	8352	7433	57279	56642
	NSEC3	7309	3364	57122	41437

存在：クエリログから存在するドメイン名のみ抽出　(単位: qps)
不在：存在から生成した不存在レコード　NSEC3のIterationsは5

- 計測中の松のCPU使用率は30～45%程度であり、最大能力は更に高い可能性あり
  - dnsperfがシングルスレッドのため負荷をかけきれない(?)
  - 梅はいずれの計測においてもCPU使用率100%

結果2: 各方式の平均DNS応答サイズ

	方式	通常	存在	不在
DNSSEC無	N/A	115	115	112
DNSSEC有	NSEC	602	598	648
	NSEC3	637	604	884

通常: クエリログをほぼそのまま適用(不在率 約8%)
存在: クエリログから存在するドメイン名のみ抽出
不在: 存在から生成した不存在レコード

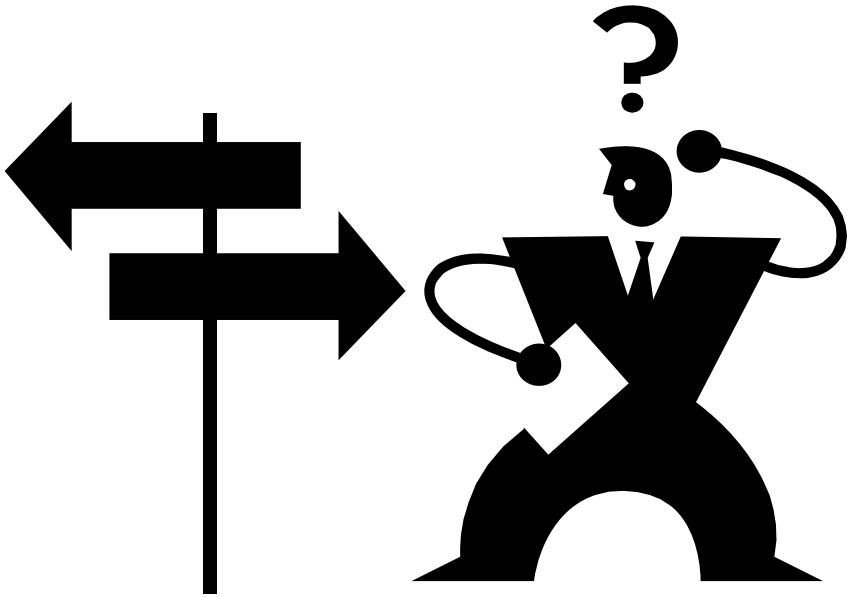
- DNS問合せサイズは平均45バイト

本実験範囲でのまとめ

- DNSSEC化により、権威DNSサーバの応答性能はある程度低下する
  - 存在する名前の応答で10～20%程度の低下
  - 特にNSEC3の不在応答は、サーバによっては50%以上の処理能力の低下を招く
- DNSSEC化により、権威DNSサーバからのDNS応答パケットは5～8倍程度に増加する

注意：あくまでも本実験範囲での結果であり、他の条件での結果を保障するものでは無い

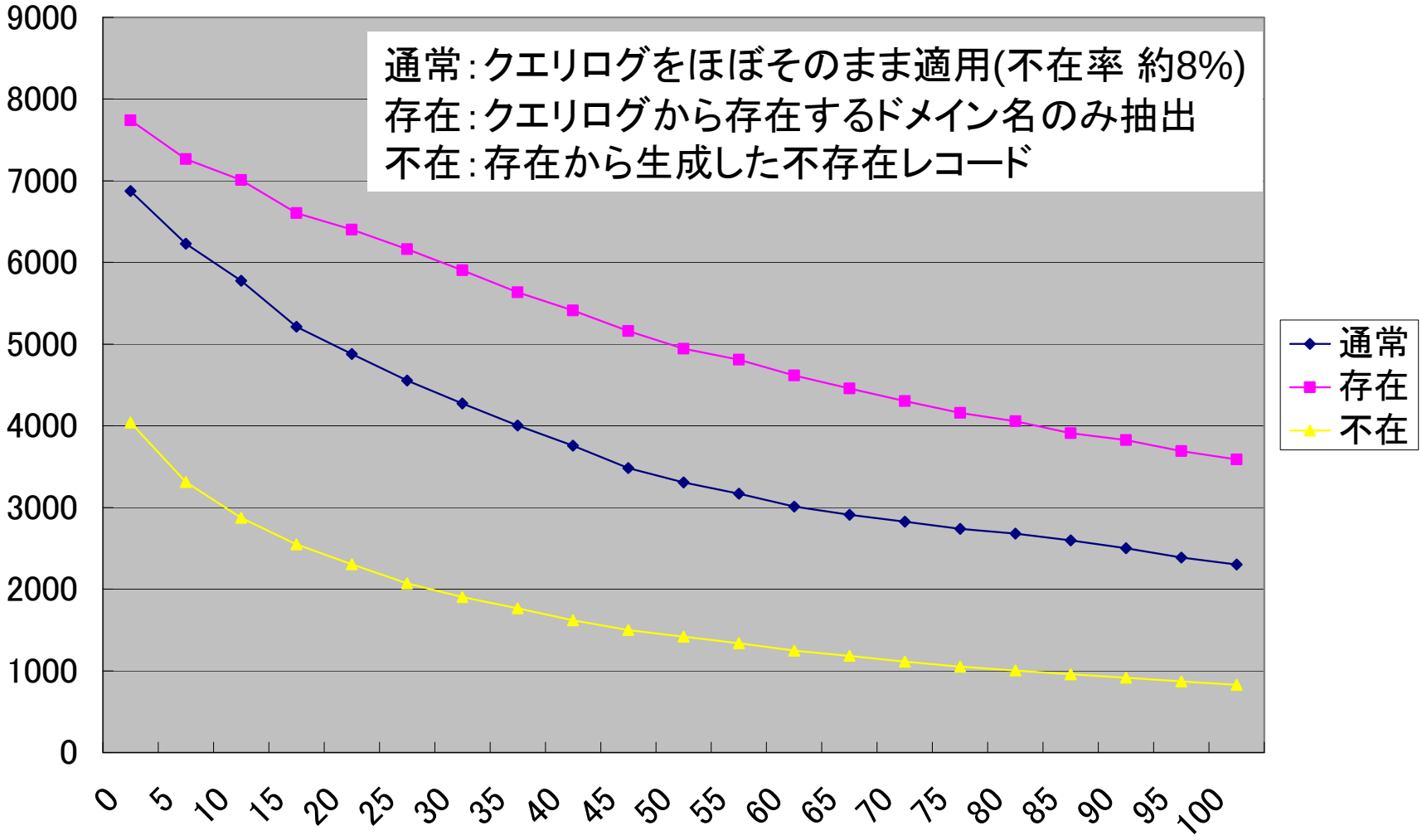
JAPAN REGISTRY SERVICES



参考 : Iterationsと応答性能

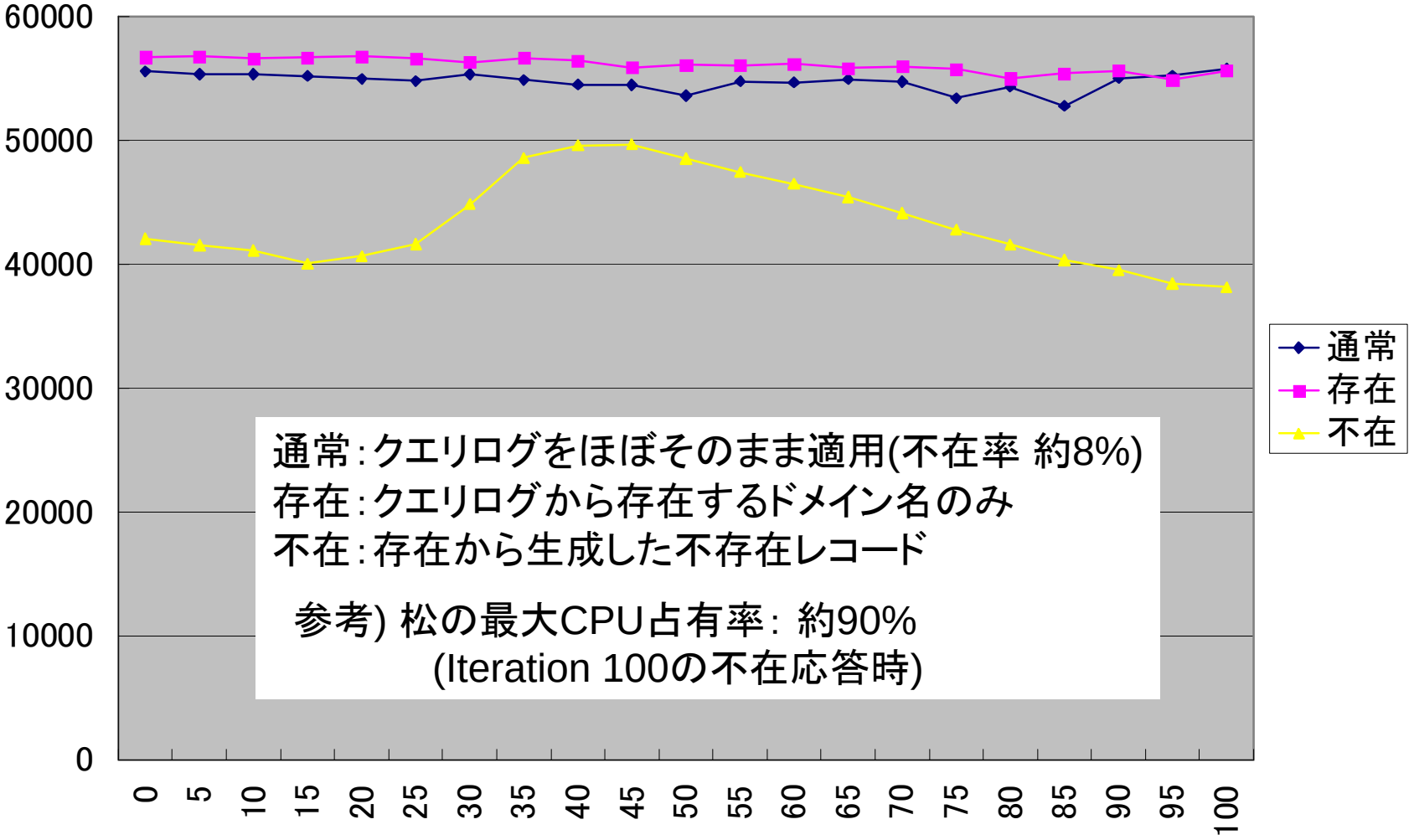
参考1: Iterationsと応答性能 梅

x軸：Iterations　y軸:応答性能(qps)



参考2: Iterationsと応答性能 松

x軸:Iterations　y軸:応答性能(qps)



Iterationsと応答性能

- Iterationsを極端に大きな数字にするのは、応答性能に悪影響があるため、あまり大きくしない
  - 10程度であれば実用上問題無い

- 計測結果から
  - 松(E5540)でのIterationsの変化に対する不在応答の性能変化が不自然
    ⇒ 複数回計測しても同様の結果となる
  - 梅(Pentium III)での存在応答の性能が、Iterations増加に伴って悪化している
    ⇒ 存在応答でもNSEC3ハッシュを計算している(?)

  ⇒ 今後要調査

さいごに

- 将来的にDNSSEC対応を考えているなら、キャッシュDNSサーバでの対応は早めに行うほうが得策である
  - DNSSEC普及の初期段階では、DNSSEC対応の組織は少ないためキャッシュDNSサーバへの負荷の影響まだ小さい
  - 反対に、充分DNSSECが普及してから導入するとDNSSEC無しとの差が大きくなり導入への敷居が高くなる

JAPAN REGISTRY SERVICES