トラフィック計測を用いた、DNS サービス方式変更によるトラフィック変化の予測手法

代表研究者　　石　原　知　洋　　東京大学　大学院　総合文化研究科　特任助教

1 はじめに

Domain Name System(DNS) は，インターネットで広く一般的に利用されている名前解決システムであり，インターネット上におけるアプリケーションの利用に先立ち，ドメイン名から IP アドレスへの変換を行っている。そのため DNS はインターネット上でサービスをする上で欠かせない重要なシステムとなっている。

以上のように DNS は重要なシステムであるが、基本的な設計については 20 年以上前のプロトコル制定時から変化はしていない。しかし、現状の DNS はいくつかの問題点を抱えていることが知られており、例えばその安全性については以前より脆弱性が指摘されてきた。脆弱性により、悪意ある攻撃者が DNS の応答を偽ることで通信を不正に誘導することができてしまう。これを利用して、攻撃者はさまざまな情報を不正に取得することが可能となる。

そのため、それらの問題を解決するための DNSSEC という公開鍵暗号を利用したデータ署名を利用する方式が考えられた。しかし、これによってデータの安全性は確保できるようになったが、その署名のため扱うデータの量や種類が増えることになった。

新しい方式を実際の運用上で使うためには、その通信負荷の変化を正しく見積もる必要がある。もし予測をせずに運用に導入したとすれば、最悪の場合、サービスが停止する恐れもある。DNS はあらゆる通信に先立って行われるサービスのため DNS の停止はあらゆるサービスの停止と等しい。

上記の理由から、DNS の拡張は数多く提案されているが、実ネットワーク上への普及には長い時間がかかっているというのが現状である。そこで本研究では DNS 拡張の普及のため、DNS のサービス方式を変更した場合の負荷予測について、トラフィック計測およびそれを基にしたシミュレーションによって求める方法について研究をおこなった。具体的には、DNS のキャッシュ TTL を変化させた場合に発生するトラフィックの変化を、サーバ上で取得できる情報をもとに推測する方法の提案および評価をおこなった。

本研究によって DNS 運用者に対して安全に DNS のサービス方式を変更するための指標を提供することが可能となり、DNS 拡張技術の速やかな普及に寄与できる。

2 DNS のプロトコル概要

DNS はホスト名と IP アドレスの変換を行うシステムである。ホスト名は木構造を持つドメイン名空間にマップされており、その名前の一意性が確保されている。ドメイン名空間は、木構造の各ノードにおいて、そのノード以下の部分木をサブドメインとして分離しており、それぞれのサブドメインの管理は別々のサーバに委譲されている。

この木構造の節点および末端がインターネット上での名前を示している。名前は、root を右端として、枝をおりるごとに左にピリオドで区切ってそのゾーン名を付け加えていく。これにより、木構造の各点を一意な名前で表わすことができる。

自分自身でゾーンを所有している名前サーバのことを、そのゾーンの権威サーバという。権威サーバは自分のゾーンに含まれるすべてのデータと、自分のすぐ下のゾーンを所有している権威サーバについての情報を所有している。

DNS によるホスト名から IP アドレスへの変換は名前解決と呼ばれるが、これはドメイン名空間を根本から辿ることによって実現している。キャッシュサーバは、クライアントからのドメイン名変換の問い合わせを受け、ドメイン名空間の木構造をたどって目的のホスト名を管理している権威サーバを特定し、その権威サーバに問い合わせを行うことでホスト名から IP アドレスへの変換を行う。

2-1 DNS のキャッシュ機構

名前解決を行うキャッシュサーバはキャッシュ機能を持っており、名前解決を行った際に、問い合わせ結

果を一定時間保持し、クライアントから再度の問い合わせがあった場合には、その保持内容を応答し、権威サーバへの問い合わせを行わない。

キャッシュサーバがキャッシュを保持する時間は、個々の DNS レコードの TTL パラメータで指定されている。TTL パラメータは元のデータを管理している権威サーバ上で設定する。権威サーバは TTL パラメータを変更することで、問い合わせを行うキャッシュサーバにどれだけの期間キャッシュを保持させるかを調整することができる。

キャッシュ TTL の設定は整合性と負荷のトレードオフであり、長い TTL を設定した場合には DNS の問い合わせ数が減少することが期待できるが、一方で DNS のレコード変更時には古いデータがキャッシュ上に長く滞留することとなる。例えば DNS による負荷分散など、クライアントに対して教えるレコードを変えることで分散を確保している場合は、その時々でトラフィックが発生する IP アドレスを変えたい要求があるため、キャッシュサーバのキャッシュ保持期間は短いほうが望ましい場合もある。

キャッシュの効果については Jung らの論文[7]で、大学およびルートネームサーバに寄せられるトラフィック解析をもとに、そのキャッシュの有効性について論じている。

上記のように、キャッシュの有効性については検証がなされており、キャッシュによってトラフィックの発生を抑制していることにより、DNS は規模性が確保されていることは明らかである。しかし現状の DNS 運用において、キャッシュの TTL についての適切な指標があるとは言いがたい。整合性に対する要求から極端に低いキャッシュの TTL が決定され、その結果増えたトラフィックを処理することが難しくなる場合もある。

本研究では、適切なキャッシュ TTL を設定する上の指標の一つとして、権威サーバに寄せられるトラフィックのパターンから、キャッシュサーバ上に寄せられる、キャッシュによって減少する前の DNS のトラフィックパターンを推測し、その推測結果を利用することで、TTL 変更後のトラフィック量の見積りを行う方法について提案する。

3 関連研究

DNS のサービス形式変化によるトラフィックやパフォーマンスの変化については、いくつか研究がなされている。

力武らは実トラフィックでのサンプルを元に、IPv6 導入時における DNS パケットペイロードの変化[1]および DNSSEC 導入時のパケットペイロードの変化[2]について述べている。また、Guillard らの論文[3]では、DNSSEC 導入時の DNS サーバの負荷や、鍵の生成、ゾーンの署名などのパフォーマンスについて言及されている。Ager らの研究[4]では、実ネットワーク環境で記録された DNS トラフィックを元に、そのトラフィックの問い合わせおよび応答を DNSSEC のものに変換し、テストベッド上で再生するアプローチで、DNSSEC 導入時の変化についての解析を行なっている。

また、DNSSEC 導入によるキャッシュサーバ側への影響については、副島・若杉ら[5][6]が特定のシナリオの元で、キャッシューサーバでの署名検証に起因する性能変化について検証をおこなっている。

4 設計

キャッシュサーバは、保持しているキャッシュが有効な間は権威サーバに問い合わせることなくクライアントに応答する。そのため、実際には断続的にキャッシュサーバに問い合わせが送られている場合でも、権威サーバからそのトラフィックは見えない。

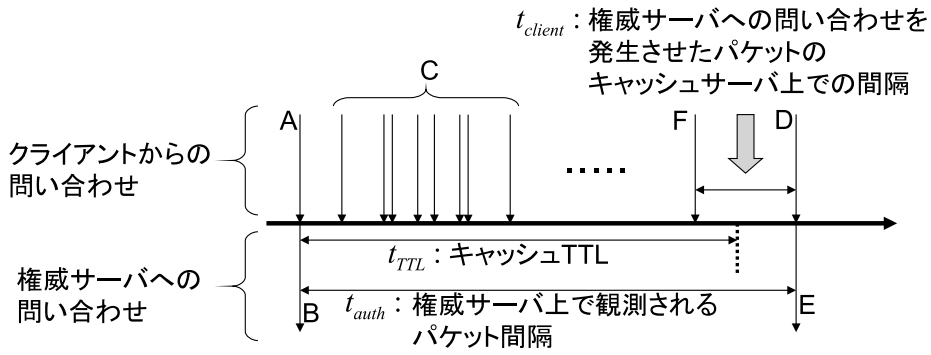

図 1　キャッシュサーバの動作モデル

図 1は、キャッシュサーバの動作を示したものである。キャッシュサーバは、当該レコードのキャッシュを保持していない状態でクライアントからの問い合わせが寄せられると(A)、権威サーバへ問い合わせを出し(B)、その結果をクライアントに応答し、その際にキャッシュを保持する。

キャッシュ TTL が切れるまで、クライアントからの問い合わせ(C)に対してはキャッシュから応答し、権威サーバへ問い合わせを行わない。キャッシュ TTL の期間が過ぎるとキャッシュが破棄され、キャッシュ破棄後にクライアントからの問い合わせがあった際(D)に、再び権威サーバに対して問い合わせを行う(E)。

この時、キャッシュ有効期間内での最後の問い合わせ(F)と、キャッシュ破棄後の最初の問い合わせ(D)の間隔t_{client}は、権威サーバで観測された２つの問い合わせの間隔をt_{auth}、キャッシュの TTL をt_{TTL}とし、クライアントからの問合せが発生する確率を独立とすれば、t_{client}期間内のどの時点でキャッシュが破棄されるかは、元のレコードの TTL を超えない範囲で一様な確率となる。

そのため、t_{client} の平均は以下で表すことができる。

$$t_{client} = \left(t_{auth} - t_{TTL}\right) \times 2 \quad \left(t_{client} < t_{TTL}\right)$$

$$t_{client} = t_{auth} - \frac{t_{TTL}}{2} \quad \left(t_{client} \geq t_{TTL}\right)$$

上式より、特定レコードに対するキャッシュサーバからの問い合わせの間隔t_{auth} と、当該レコードのキャッシュ TTL であるt_{TTL}から、クライアントからキャッシュサーバに送られている問い合わせについて、その間隔のサンプルを推定することができる。

また、ある間隔t_{client}が、キャッシュ破棄後に観測される確率は、t_{client}の長さに比例する。そこで、本研究で提案する方式では、権威サーバ上での観測から推定されたt_{client}のサンプル一つにつき、その間隔でt_{TTL} / t_{client}個のクエリがキャッシュサーバに送られていると推定する。

以上をまとめると、本方式で提案するクライアントからの問い合わせの推定方法は以下のようになる。

1. あるキャッシュサーバから送られてくる、特定のレコードに対する問い合わせのパケット間隔を DNS 問い合わせのログか、パケットダンプ等から取得する
2. 取得したパケット間隔t_{auth}および DNS レコードの TTL(t_{TTL})より、当該キャッシュサーバにクライアントから送られている問い合わせの間隔t_{client}を推定する
3. 個々の推定されたt_{client}とキャッシュの TTL(t_{TTL})から、その間隔で送られているパケット数を推定す

る。

上記の方法で作成した場合、実際に個々のクライアントから行われた問い合わせの時系列は不明だが、そのパケット間隔の分布は推定できる。時系列が不明であっても、問い合わせ間隔の分布が推定できれば、問い合わせの発生する確率分布は導き出せるため、キャッシュの効果の推定に利用するためには十分な内容であるといえる。

5 評価

本研究で提案した方式の評価のため、実際のネットワーク環境にて行われた DNS のトラフィックをもとにシミュレーションを行い、その有効性を確かめた。

シミュレーションに利用したデータは、慶応義塾大学に設置してあるキャッシュサーバ上にて、2012 年 1 月 22 日 8:00(JST)から 2012 年 3 月 11 日 8:00(JST)までの 49 日間に寄せられた問い合わせの DNS のトラフィックを利用した。

評価に利用したキャッシュサーバのシミュレータは、入力した時系列での DNS トラフィックについて、図 1に従った動作を行い、キャッシュ期限切れによって権威サーバに問い合わせをおこなった際に、その時間を記録する。キャッシュの TTL はシミュレータのパラメータとして指定できるようにし、キャッシュ TTL を変えた場合に、権威サーバへの問い合わせがどのように変化するかを測定した。

シミュレータに対する入力には、測定を行ったキャッシュサーバ上に寄せられたトラフィックから、最も問い合わせが多かった DNS レコードについて抽出したものを利用した。

評価は以下の手順で行った。

1. 実トラフィックのデータを特定の TTL でシミュレータにかけ、権威サーバに問い合わせが送られた時間を記録
2. 得られた時系列データから、本研究で提案した推定方式で元のトラフィックの分布を推定する
3. 得られた分布を異なる TTL でシミュレータにかける
4. 実トラフィックのデータをその TTL でシミュレータにかけ、両者の結果を比較する

キャッシュの TTL は、60 秒、300 秒、3600 秒を使い、それぞれの TTL で得られたキャッシュサーバのシミュレーション結果を元に、本研究で提案した方式による推測結果と、実トラフィックから割り出される結果を比較した。

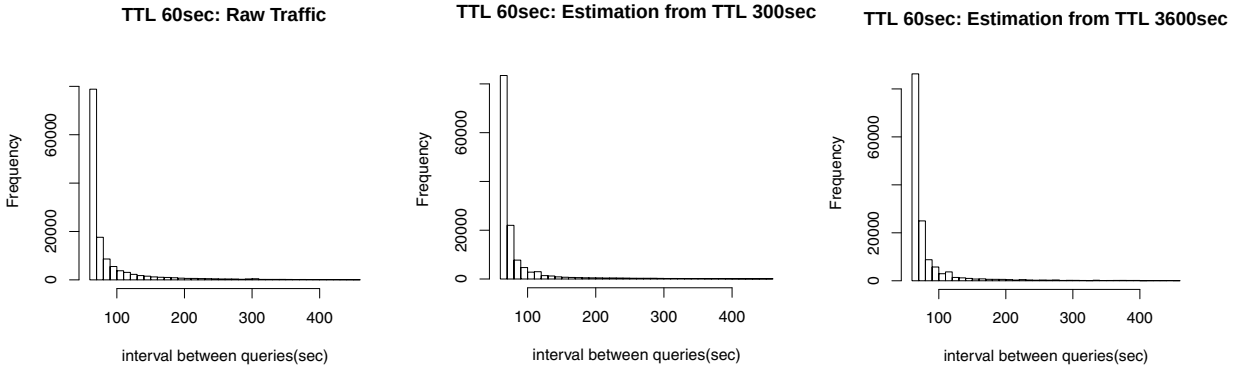

図 2 TTL60 秒における、権威サーバへの問い合わせ間隔の分布

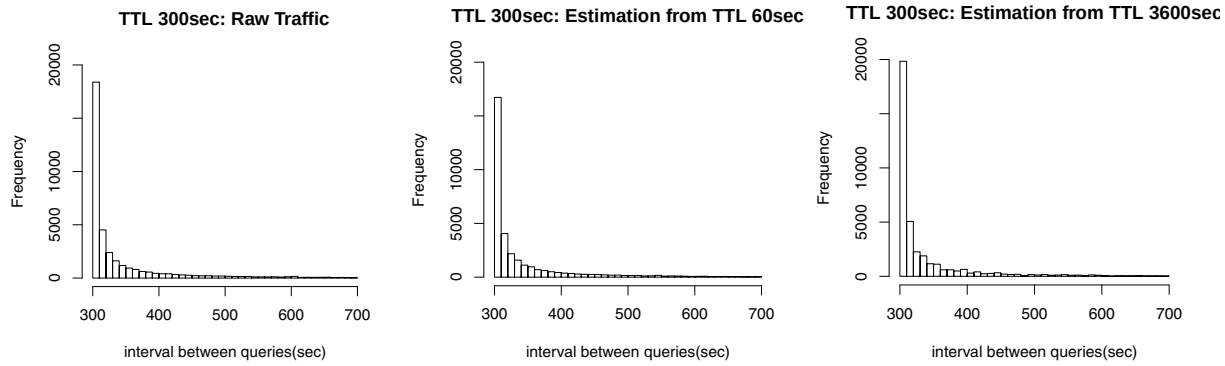

図 3 TTL300 秒における、権威サーバへの問い合わせ間隔の分布

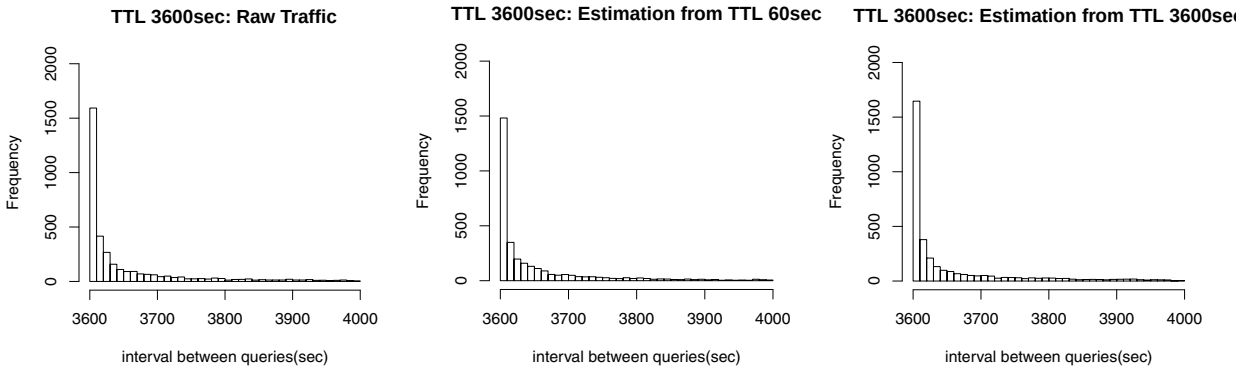

図 4 TTL 3600 秒における、権威サーバへの問い合わせ間隔の分布

推定を行う対象のキャッシュ TTL [sec]	元トラフィックから算出された平均クエリ間隔[sec]	推定元データにおけるキャッシュ TTL					
		60[sec]		300[sec]		3600[sec]	
		推定平均クエリ間隔[sec]	誤差率	推定平均クエリ間隔[sec]	誤差率	推定平均クエリ間隔[sec]	誤差率
60[sec]	102	−	−	97	−4.9%	96	−5.9%
300[sec]	374	376	0.5%	−	−	364	−2.7%
3600[sec]	3737	3742	0.1%	3729	0.2%	−	−

表 1　推定された問い合わせ間隔の平均および誤差率

図２、図３、図４はそれぞれのキャッシュ TTL において、元トラフィックによるシミュレーションによって計算されたクエリ間隔の分布と、本研究で提案した推定方式から割り出した分布からシミュレーションをした場合のクエリ間隔の分布の比較である。

表は、元トラフィックから計算されたクエリ間隔の平均値、およびそれぞれの推定されたクエリ間隔の平均値と、推定値の誤差を示している。

表１から、推定元データの TTL が大きく、かつ推定先の TTL が小さいほうが誤差が多いことがわかる。これは、推定元データの TTL が大きいほうがキャッシュによって問い合わせの回答が行われる回数が増加し、結果として権威サーバから隠蔽されるデータが増加することと、推定先データの TTL が小さいほうが、推定トラフィックの分布の違いによる影響を強く受けるからである。

全体として見た場合､実際に元のトラフィックをシミュレーションすることで得られる平均クエリ間隔と、推定によって算出される平均クエリ間隔の誤差は±6%以下であることがわかる。また、図２，図３，図４のパケット間隔のヒストグラムから、各階級の分布についても大きな違いが出ていないことがわかる。以上か

ら、本研究で提案した推定方式は、TTL 変更時のキャッシュ効果を高い精度で推定できることがわかった。

まとめ

本研究では、権威サーバに寄せられるトラフィックの情報から、キャッシュサーバに対して出されている問い合わせの分布を推定する方法についての提案を行った。また、実際のネットワーク上で取得された DNS のトラフィックを利用して、本研究が提案する推定方法の評価を行い、その有効性を確かめた。

本研究の成果により、DNS 権威サーバの運用において生じる TTL の要求に対し、TTL 変化後のトラフィックの推移を予測することができ、適切な運用上の計画を立てることが可能となる。

今後は本推定手法をさまざまな実環境に対して適用し、その有効性をより深く検証するとともに、さまざまな運用シナリオに対して対応できる形に改良していく予定である。

【参考文献】

[1] Kenji Rikitake, Hiroki Nogawa, Toshiaki Tanaka, Koji Nakao, Shinji Shimojo, "An Analysis of DNS Payload Length Increase during Transition to IPv6",IEICE Trans. Commun. (Japanese Edition), vol. J87-B, No. 10, pp.1552-1563(2004)

[2] Kenji Rikitake, Hiroki Nogawa, Toshiaki Tanaka, Koji Nakao, Shinji Shimojo, "An Analysis of DNSSEC Transport Overhead Increase", IPSJ SIG Notes, , pp345-350(2005)

[3] Alexis Guillard, "DNSSEC Operational Impact and Performance",Proceedings of the International Multi-Conference on Computing in the GlobalInformation Technology(ICGI'06) (2006)

[4] Bernhard Ager, Holger Dreger, Anja Feldmann, "Predicting the DNSSEC overhead using DNS traces", nformation Sciences and Systems, 2006 40th Annual Conference, pp1484-1489(2006)

[5] 副島裕司, 若杉泰輔, 島村祐一, 平野衡, 岡栄一, "DNS キャッシュサーバにおける DNSSEC 性能評価", 電子情報通信学会, 信学技法 情報ネットワーク, Vol. 108(426), 37-42pp, 2009-01-29

[6] 若杉泰輔, 副島裕司, 島村祐一, 岡栄一, "署名パターンに着目した DNS キャッシュサーバの DNSSEC 性能評価", 電子情報通信学会, 信学技法 情報ネットワーク Vol. 109(119), 61-66pp, 2009-07-02

[7] Jaeyeon Jung, Emil Sit, Hari Balakrishnan, and Robert Morris,"DNS performance and the efectiveness of caching", in Proceedings of the ACM SIGCOMM internet measurement workshop '01, San Francisco, California, USA, ACM, November 2001

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
ＤＮＳにおける認証情報管理手法の提案	日本ソフトウェア科学会 コンピューターソフトウェア	2011 年 11 月
トラフィック計測を用いた、DNS サービス方式変更によるトラフィック変化の予測手法	日本ソフトウェア科学会／インターネットテクノロジー研究会	2012 年 8 月（発表予定）