Vol.2009-IOT-7 No.9
2009/10/9

IPv6 および DNSSEC 普及時における DNS トラフィックの動向分析と予測

豊野 剛[†] 石橋 圭介[†] 三宅 延久[†]

インターネットにおける重要インフラストラクチャである DNS は IPv4/IPv6 を同一システム上で扱う．このため IPv6 インターネットへの移行期には IPv4/IPv6 双方の名前解決を行うことになり DNS トラフィックの増加が予測される．また導入が急速に普及しつつある DNSSEC により DNS のセキュリティは向上するが DNS トラフィックは増加する．本稿ではキャッシングサーバにおいて実トラフィックを分析し，上記要因でユーザクエリが 46%，サーバクエリが 20%増加し応答パケットサイズは 3.34 倍に達すると予測した．

An Analysis and Projection of DNS Traffic Based on the Research of IPv6 and DNSSEC

Tsuyoshi Toyono[†], Keisuke Ishibashi[†] and Nobuhisa Miyake[†]

The DNS (Domain Name System) domain names to be used in the Internet transactions instead of IP addresses. We analyzed user DNS queries and responses on caching servers in a large scale network. These measurements show users' queries increase by 46% due to the IPv6 support and servers' queries increase by 20% due to their DNSSEC support. It's mean we have to reconsider DNS server farms in our networks.

1. はじめに

DNS（Domain Name System）はインターネット上においてドメイン名（Domain Name）と IP アドレスなど情報を相互変換する機能を有する分散データベースシステムである．インターネット上のノードは一意な IP アドレスを持ち，これを識別子として用いている．しかし一般的にネットワークサービスの利用者は IP アドレスではなくドメイン名によってアクセス先のノードを指定する．このためこの変換を担う DNS は今日のインターネットのインフラストラクチャとして重要な役割を担っている．

DNS はインターネット初期からほぼプロトコルが変更されること無く運用され続けてきているが[1][2]，今後 2-3 年で DNS を取り巻く環境は大きく変わると考えられる．一つ目の変化要因は IPv4 枯渇における IPv6 への移行である．DNS では IPv4 アドレスも IPv6 アドレスも同一システム上で扱われる．このため IPv6 インターネットへの移行期には DNS は IPv4 アドレスと IPv6 アドレスの双方の名前解決を同時に担うことになる．二つ目の変化要因は DNSSEC の導入である．ドメイン名詐称へのセキュリティ対策として DNSSEC が急速に整備されつつある．DNSSEC の導入は DNS の実装だけなく DNS の通信内容にも多くの変更を伴う．

上記に挙げたような利用形態の変化が生じても DNS の正常な運用を維持することがインターネット全体にとって重要と言える．本稿では DNS のキャッシングサーバに注目した．キャッシングサーバでは権威サーバおよびクライアント端末双方のトラフィックを分析することができる．本稿ではまず現状の DNS トラフィックの動向を分析し，その上で上記に挙げたような環境の変化に伴って DNS トラフィックがどのように変化するかを予測し，ネットワークや DNS のサーバ，クライアントに与える影響を考察した．

2. DNS の仕組みとトラフィック増加要因

2.1 DNS の仕組み

DNS はスタブレゾルバ（クライアント端末），キャッシングサーバ，権威サーバの三種類から構成される．クライアント端末はキャッシングサーバに対して DNS 問合せを行い，キャッシングサーバがこれに応答する．キャッシングサーバはクライアント端末からの問合せと権威サーバの応答を仲介する．権威サーバは資源レコード（Resource Record, RR)と呼ばれるデータを保持し応答する権限を持つ．DNS では同一のドメイン名（ラベル）に対して RR を複数持つことができ，例えば IPv4 アドレス，IPv6 アドレスなどといった複数の回答内容を同時に付与できる．キャッシングサーバはクライアント端末からの問合せ（再帰クエリ）を受けると，代理として権威サーバ

[†] NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

への問合せ（反復クエリ）を順次行い，最終的に得られた回答をユーザへ応答する．同時に得られた回答内容をキャッシュとして権威サーバから指定された TTL（Time To Live）期間だけ保持し，他のユーザから同じ問合せがあった場合にはキャッシュから応答する．これにより権威サーバへの問合せの氾濫を抑制し，またクライアント端末からの問合せに対する応答時間を短縮している．

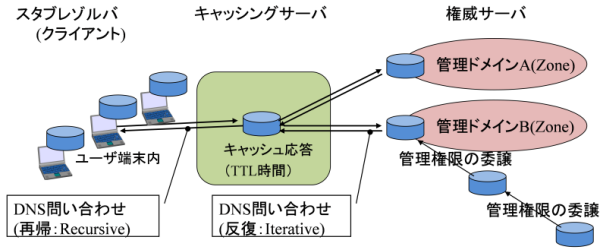

図 1 DNS 概要

2.2 DNS トラフィックの増加要因

2.2.1 IPv4 枯渇に伴う IPv6 移行

近年のインターネット利用状況から演繹すると，IPv4 アドレスは 2011 年から 2012 年には枯渇すると予測されている[3]．これに伴い今後新しく提供されるサービスや新規ユーザから徐々に IPv6 インターネットへの移行が進むと考えられる．IPv4 インターネットと IPv6 インターネットは独立した別個のネットワークであり，直接の相互疎通性がない．IPv6 インターネットへの移行過渡期においてユーザは当面の間 IPv4・IPv6 ネットワーク双方への疎通性を備えたデュアルスタック環境を利用する必要がある．ユーザが IPv4・IPv6 の両サービスを透過的に利用できるようにするために DNS の果たす役割は重要である．IPv6 移行過渡期のユーザは DNS に対して IPv4 アドレス問合せだけでなく IPv6 アドレス問合せも同時に行う必要が生じる．ユーザは DNS の応答によってそのサービスが IPv4 上のサービスなのか，IPv6 上のサービスなのか，またその両方で提供されているのかを判断してからアクセスすることになる[a]．このように IPv6 移行過渡期においてはドメイン名に対する IP アドレス問合せが IPv4 アドレス・IPv6 アドレスの両方に対して行われることになり，DNS トラフィックの増大が懸念される．

2.2.2 キャッシュ汚染攻撃と DNSSEC の普及推進

キャッシュ汚染攻撃とはキャッシングサーバに対して不正規な情報を注入し，キャッシュ内容を書き換えることによりクライアント端末からの問合せに対して不正規な情報を応答させ，クライアント端末のアクセスをコントロールする攻撃のことである．キャッシュ汚染攻撃は従来から知られていたが，2008 年 7 月に Kaminsky により発見された新たなキャッシュ汚染攻撃手法（Kaminsky 型攻撃）[4]は攻撃成功確率および所用時間が飛躍的に短縮されたもので，実際に著名ドメイン名に対する複数の被害事例も報告された．本攻撃手法は DNS のプロトコル自体の脆弱性に基づいており，現状普及している対策手法は攻撃成功確率を低減するだけの暫定的な対策に過ぎない．

DNS では得られた応答が正しい権利者からの応答であるかどうかの正当性検証を行う仕組みが存在せずセキュリティ的に脆弱であることは古くから指摘されており，既に 1997 年には DNSSEC（DNS Security Extensions）と呼ばれるセキュリティ拡張が標準化されている[5]．DNSSEC は公開鍵暗号技術を用い DNS の登録データに署名を施すことで第三者による改ざんや偽造を検証できるようにする技術である．DNSSEC が普及すればキャッシュ汚染攻撃は完全に無効化できる．2008 年の Kaminsky 型攻撃の発見で DNS 全体が危殆化したことにより，標準化は完了[6][7][8]していたものの実装や普及が遅れていた DNSSEC の導入が本格化した．DNSSEC の普及にはサーバ側の実装・運用の対応と検証端末（Validator）側の実装・運用の対応の両方が必要となる．サーバ側に関しては既に幾つかの ccTLD や gTLD[b]が対応を開始しており，インターネットの DNS の根幹を担うルートサーバも 2009 年中に DNSSEC による認証署名を開始する見込みとなった[9]．また日本の ccTLD である JP ドメインの管理団体 JPRS も 2010 年度中に DNSSEC に対応することを表明している[10]．DNSSEC の導入に当たっては幾つかの課題が残っていると考えられているが，その一つに DNS トラフィックの増大が挙げられる．DNS プロトコル上で公開鍵を通信する DNSSEC の仕組みから，普及に伴い DNS トラフィックが大幅に増大することが懸念される[11]．

3. 関連研究

IPv4 枯渇に伴う IPv6 移行に関しては，前述した IPv4 アドレス枯渇時期の見極めなどを受け DNS 分野でも対応が進んだ．DNS ルートサーバに 2008 年 2 月に IPv6 アドレスが付与され[12]IPv6 ネットワーク上においても問合せが行えるようになり，これに前後して多くの ccTLD，gTLD が IPv6 に対応した．また逆に DNS トラフィック分析を用いて IPv6 インターネットの普及度を計測する研究も行われている[13]．

DNSSEC に関しても幾つかの先行研究が見受けられる．一つ目は権威サーバの応答数および応答パケット長の増加に関する文献である．NIST[14]では権威サーバへの問合せのうち 50%が DNSSEC に対応した場合トラフィック量は 3.3-3.6 倍になると指摘している．同じく Kolkman[15]は権威サーバのトラフィック量は 2-3 倍と指摘している．Ager[16]，力武[11]らはさらに DNSSEC の導入により UDP パケットサイズが増加する

a このため DNS では IPv4・IPv6 ネットワークどちらのトランスポート上においても，IPv4・IPv6 両方のアドレス問合せに応答できる必要がある．

b ここでは ccTLD（country code Top Level Domain），gTLD（generic Top Level Domain）の管理団体を指す．

ことで IP パケットフラグメントの問題が発生すると指摘している．Ager によれば権威サーバからのエラーでない応答のうち 72-77%の応答が 1480 バイト以上に，力武らによれば 30%の応答が 1232 バイト以上になり，それぞれ IPv4 および IPv6 フラグメントに抵触するとしている．二つ目は権威サーバで署名を施す際のデータ増大および処理性能の劣化に関する文献である．Gieben[17]は ccTLD CA ドメインの署名を例示し，ゾーンデータは 1024bit 鍵長で 3.7 倍，1584bit 鍵長でおよそ 4.7 倍になったとした．三つ目は署名検証による処理性能の劣化に関する文献である．Schlyter[18]は DNS サーバをキャッシングサーバ兼 Validator として署名検証させると 2-36%の性能劣化が生じるとした．また若杉[19]はキャッシングサーバ兼 Validator における性能劣化の主な要因は署名鍵長には依存せず，権威サーバとのトランザクション数に比例すると指摘した．また Kolkman，Rozendaal[20]，Ager らはサーバ性能の検証を行っており，Ager は Validator の CPU 利用率は 2.3 倍の増加に留まるがメモリ効率は約 1/4 まで劣化するとしている．これらの先行研究から UDP パケットサイズの増加がネットワークに与える影響，およびトランザクション数の増加がサーバに与える影響が大きいことが分かる．

4. 現状のトラフィック動向分析と増加予測

前節で示したように，IPv6 移行ならびに DNSSEC の利用が普及するとサービスやユーザの利用変化に伴い今後数年で DNS トラフィック，DNS サーバ負荷ともに増大していく．トラフィックや負荷がどの程度増大するのか，またその場合に各ネットワークにおいて DNS 設備が十分かどうかを早急に検討しておくことが DNS の正常な運用ひいてはインターネットの正常な運用の維持のために重要といえる．本稿では特にキャッシングサーバのトラフィックに着目する．キャッシングサーバはクライアント端末と権威サーバを仲介し応答性能に影響する他，今後 DNSSEC の普及時には Validator として署名検証を行い認証の終端となると考えられるからである．

本稿ではインターネット上での実際の DNS 問合せ･応答の振る舞いを正確に把握するために多数のユーザに利用されている大規模ネットワークの DNS キャッシングサーバおけるトラフィックデータを取得した．

表 1 分析データ

Data set	Date	Time frame
data06	2006 Nov. 3 (Fri)	0:00-1:00 (60 min.)
data07	2007 Nov. 2 (Fri)	0:00-1:00 (60 min.)
data08	2008 Nov. 14 (Fri)	0:00-1:00 (60 min.)
data09	2009 Feb. 3 (Tue)	0:00-1:00 (60 min.)

取得するデータは DNS サーバを送信元あるいは宛先とする UDP/TCP port 53 の DNS トラフィックのみを対象とした．今回は 2006 年から 2009 年までの 4 年間のトラフィックデータを対象とし各々1 時間分のデータを分析した（表 1）．なお，キャッシングサーバには秒間 10,000 回以上の問合せを定常的に繰り返す超ヘビーユーザが存在する[21]．本稿では分析の偏りを防ぐため，秒間 10,000 回以上の問合せを行ったユーザのデータはあらかじめ分析から除外した．

4.1 現状のトラフィック動向分析

はじめに現状のトラフィック動向を俯瞰する．図 1 図 2 は DNS 応答の UDP パケットサイズの補累積度数分布を示したものである．主軸は応答パケットのサイズを，縦軸は累積分布を示す．これによればユーザへの応答は 512 バイト付近で大きく落ち込んでいる．DNS のパケットサイズはプロトコル上 512 バイト以内に制限されている．パケットサイズ制限を緩和する拡張プロトコル EDNS0 が標準化[22]されているが，EDNS0 に対応したユーザ端末はそれほど普及・利用されていないことが伺える．それに比して権威サーバからの応答は 512 バイトより大きいパケットも問題なく応答されている．これは観測しているキャッシングサーバが EDNS0 に対応していることを示すとともに，問合せ先であるインターネットの権威サーバの大部分も既に EDNS0 を利用してサイズの大きな DNS 応答を返すことを示している．

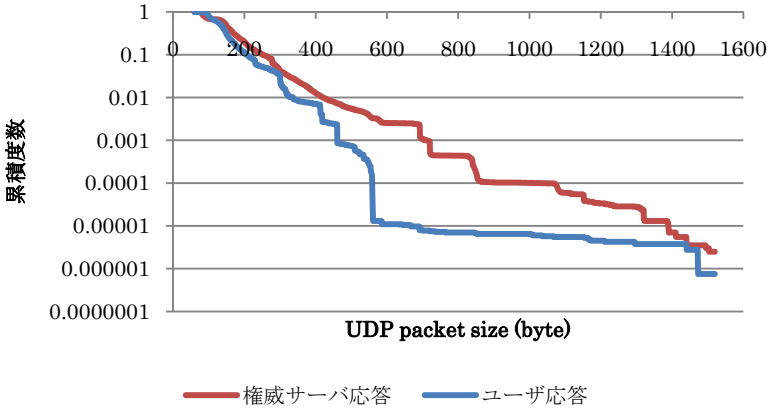

図 2 応答サイズ補累積度数分布

表 2 はユーザからの問合せのうち EDNS0 対応の問合せと TCP による問合せを割合で示したものである．これによればユーザの EDNS0 対応率はおよそ 0.3%前後に過ぎず，大多数のユーザは 512 バイトのパケットサイズ制限のまま DNS 問合せを行っていることが分かる．これは図 2 の観察を裏付けている．なお図 2 の 512 バイト超の応答比率と合致していないのは EDNS0 対応の問合せを受けても応答が必ずしも 512 バイトを超えるとは限らないためである．

表 2 ユーザ問合せの EDNS0 対応および TCP 比率(%)

	対応問合せ比率	対応ユーザ数比率	TCP 問合せ比率 (参考)
2006/11	1.230%	0.391%	0.001%
2007/11	0.876%	0.265%	0.001%
2008/11	0.559%	0.295%	0.001%
2009/2	0.768%	0.322%	0.007%

4.2 IPv6 移行時におけるトラフィック予測

次にユーザの IPv4・IPv6 デュアルスタック対応時における DNS 問合せの増加数を予測する．DNS ではクエリタイプ（Qtype）によって問合せ内容が異なり，IPv4 アドレス問合せは A クエリ，IPv6 アドレス問合せは AAAA クエリとなる．

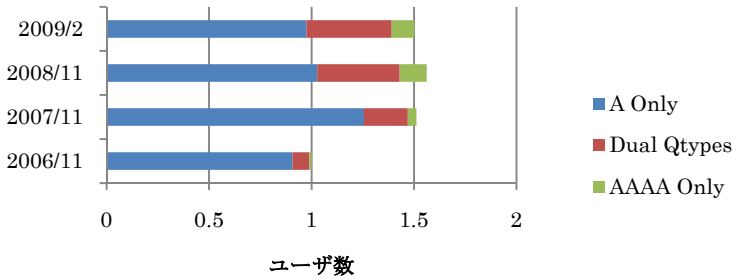

図 3 A クエリ・AAAA クエリ送信ユーザ数

図 3 は IPv4 アドレスのみを問合せるユーザと，IPv4 と IPv6 アドレスの両方もしくは IPv6 アドレスを問合せるユーザの割合を示したものである．なお図中の主軸・ユーザ数は 2006 年時点を 1 単位として正規化している．これは以降の図で同様とする．これによれば 2006 年には IPv6 アドレスを問合せているユーザ（Dual Qtypes と AAAA Only の合計）が全体の 7.54%であったものが，2009 年には全体の 33.66%を占めるまでになっている．なお，ユーザシェアの大部分を占める Windows OS の現行バージョン Windows Vista および今年 10 月 22 日に発売される次期バージョン Windows 7 はデュアルスタックネットワークに対応しており，DNS 問合せ時に A クエリと AAAA クエリの双方を送出する．この問合せは IPv6 ネットワークの疎通性に限らず送出される[c]．なお Windows Vista のユーザシェアは 21%という調査もあり[23]，これは AAAA クエリの増加と合致している．

IPv6 移行過渡期にユーザがデュアルスタック環境に対応した場合，現状では IPv4 アドレスの問合せしか行っていないユーザからも IPv6 アドレスの問合せが行われるようになると仮定できる．図 3 の 2009 年時点において，A クエリのみ送信ユーザと両クエリ（Dual Qtypes）送信ユーザのクエリ傾向分布を調べたところ，分布傾向はほぼ同様となり標準偏差，変動係数とも差が見られなかった．そして A クエリのみ送信ユーザの平均クエリレートは 1 時間当たり 59.96 クエリ(Queries/hour, qph)であり，両クエリ送信ユーザの平均クエリレートは 111.44qph であった．後者は前者のほぼ 2 倍となる．従ってデュアルスタック環境に移行したユーザは IPv4 アドレス問合せと同数程度の IPv6 アドレス問合せ行っていると推定できる．

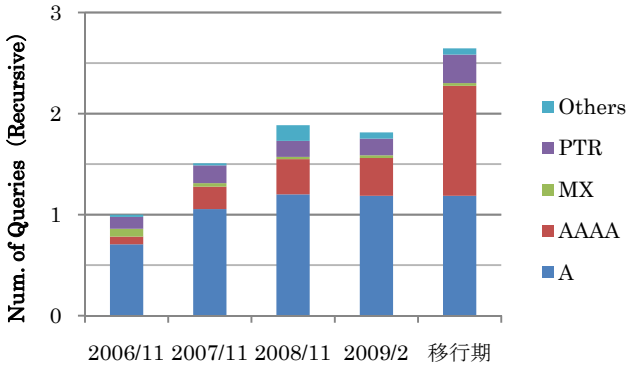

図 4 ユーザクエリ QTYPE 割合と増加予測

図 3 で示した現状の IPv4 および IPv6 アドレス問合せのユーザ数比率を元に，IPv6 移行過渡期におけるサーバへの問合せ数の増加を予測した（図 4）．図中に示した移行期の予測クエリ数は，現状では IPv4 アドレス問合せ（A クエリ）のみを行っているユーザからも同数の IPv6 アドレス問合せ（AAAA クエリ）が発出されるようになった場合，およびそれに伴って IP アドレスからドメイン名を検索するクエリタイプ PTR の問合せ（逆引き）が同じ割合だけ増加した場合を試算したものである．ここでは IPv6 移行期におけるユーザからキャッシングサーバへの問合せ数は 2009 年時点のおよそ 1.46 倍に増加するという予測結果が得られた．

4.3 DNSSEC 導入時におけるトラフィック予測

2009 年中に DNS ルートサーバが DNSSEC の署名を開始するとされていることから，

c ただし現在の実装ではグローバル IPv4 アドレスが付与されない場合 Teredo（RFC4380）が動作し IPv6 問合せは行わない．

DNSSEC の普及は加速すると考えられる．DNSSEC では認証に用いる鍵情報を DNS プロトコル上で通信することからトラフィック量，パケットサイズ共に増大することになる．DNS の署名検証を行うためには，検証を行う Validator 内に DNS ルートサーバの鍵を定期的に設定する必要があるが，インターネット上の全ユーザ端末でこれを更新することは実行運用上困難が伴う．このことから実質的に署名検証を行うのはキャッシングサーバになると考えられている．よってここでは DNSSEC の導入によってキャッシングサーバが Validator としても動作すると仮定する．認証の終端がキャッシングサーバになることにより，ここではユーザ問合せの増加は考慮しないとする．

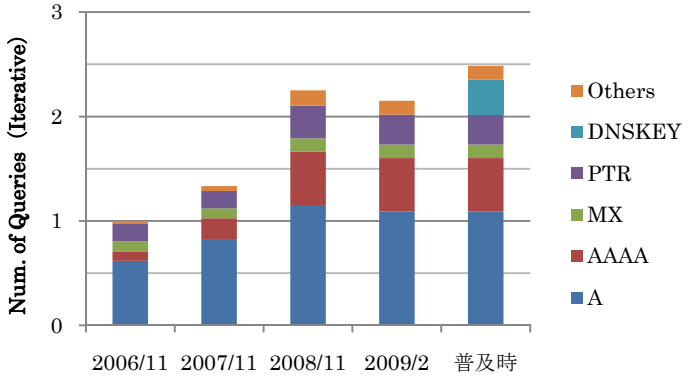

図 5 権威サーバクエリ QTYPE 割合と増加予測

図 5 は権威サーバクエリの時系列変化を示すと共に DNSSEC 普及時におけるクエリ数の増加を示している．増加量に関しては以下のように計算した．

DNSSEC ではゾーンと呼ばれる応答権限範囲毎に対して公開鍵を取得する必要があり，キャッシングサーバはこれをクエリタイプ DNSKEY によって問合せる．キャッシングサーバから権威サーバ宛ての問合せは，ユーザからの問合せのうちキャッシュされていない RR であると考えられることから，DNSSEC 普及時には問合せ先の全てのゾーンの DNSKEY RR を問合せる必要が生じる．そして問合せ頻度は権威サーバ側で設定された TTL に依存する．従って総権威ゾーン数を Z とすると単位時間当たりの DNSKEY の問合せ回数 Q は単純に$Q = Z/TTL$となる．計算の簡易化のためここでは DNSKEY の TTL として一律に全 NS RR の平均 TTL を用いた．また権威ゾーン数 Z は NS セクションのユニークラベル数とした．

2009 年時点のデータにおいて，仮に全ての権威ゾーンで署名が実施されたとした場合，DNSKEY の問合せ回数は図 5 に示す通りである．ここでは DNSKEY による問合せ数の増加は普及前のおよそ 1.20 倍という結果になった．これは問合せられるドメイン名数や反復頻度に対して観測された応答ゾーン数が少なかったためである．ただしこの問合せ数は DNSKEY RR の TTL 設定や権威サーバ側が保有するゾーン数などによって大きく変動する可能性がある．

DNSSEC ではパケット数だけでなくパケットサイズの増加も問題になる．DNSSEC 導入時のパケットサイズの増加を，以下の試算によって求めた．

- 署名鍵長は DNSKEY・RRSIG とも一律 1024bit（128byte）と仮定する．
- エラーでなく（NoError）回答セクションが有りかつ回答が CNAME で無い場合，回答 RR 数と同数の RRSIG が付与されるとする．
- エラーでなく権威応答である場合，NS セクションに 1 つの RRSIG が付与されるとする．
- エラーでなく権威応答でかつ初見のゾーンからの応答だった場合，更に DNSKEY 問合せが発生するとする．
  - DNSKEY 応答では 2 つの DNSKEY RR および同数の RRSIG が付与されるとする．
  - DNSKEY 問合せの際には 追加セクションで NS RR 数と同数の RRSIG が付与されるとする．
- エラーでなく応答が NXDomain（存在しないことをしめす応答コード）である場合，NSEC3 応答として 2 つの RRSIG が付与されるとする．
- その他の応答およびエラー応答（ServFail，FormError など）は現状の応答サイズのままとする．

図 5 は 2009 年時点のデータを元に現状の権威サーバからの応答パケットサイズと DNSSEC 導入時のパケットサイズの分布の比較を示したものである．ここで示されている現状の応答パケットサイズ分布は図 2 で示したものと同一である．これによれば DNSSEC 導入時にはパケットサイズは現状と比べ大幅に増加する．現状のパケットサイズは平均で 167.3 バイトであるが，上記計算によれば DNSSEC 時のパケットサイズの平均は 559.83 バイトに増加し，これは現状の 3.24 倍である．また EDNS0 での標準的な回答サイズである 4096 バイトを超過するものも全体の 0.17%に達した．特にドメインが存在しないことを示す NXDomain 応答時に，非存在証明を行う NSEC3 で署名が付与されることで現状に比べパケットサイズ分布全体が増加傾向にシフトした．

本試算では単純化のため幾つかの要因を考慮していない．まず DS RR の付与を考慮していない．DS RR を正しく計算した場合パケットサイズは更に増大する．また鍵長を一律 1024bit としているが，実際にはより強固な鍵長の長い鍵を登録することも考えられる．同じく DNSKEY は一律 2 つ応答するとしたが鍵更新期などを考えるとこれも再考する必要がある．これらは更なるパケットサイズの増大要因である．逆に減少要因としては，回答セクションに付与される RRSIG の個数などが挙げられる．今回の試算で大幅にサイズが増大したものの中には，具体例として 170 の回答セクション，

3 の NS セクション，4 の追加セクションを持つ現状で 1152 バイトの MX 応答などが含まれ，こういった応答には必ずしもそのまま署名が付与されるとは限らないと思われる．これらの要因を加味し今後更に精査が必要である．

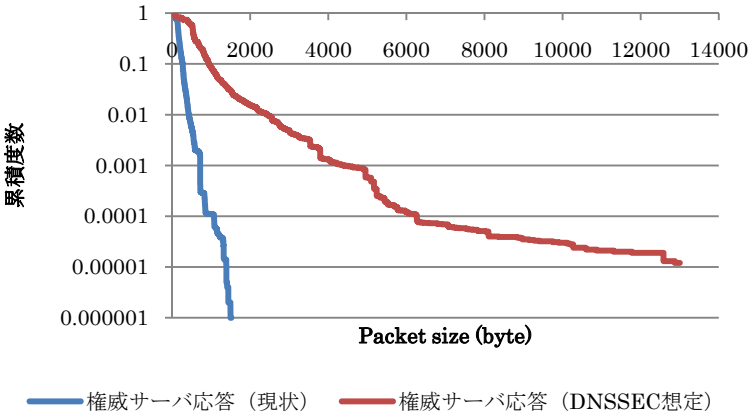

図 6 DNSSEC 普及時のパケットサイズ予測

5. まとめ

DNS はインターネット初期からほぼプロトコルが変更されること無く運用され続けてきているが，近年では DNS をとりまく状況が変わりつつある．特に今後 2-3 年で DNS を取り巻く環境は大きく変わると考えられている．変化要因の一つは IPv4 枯渇における IPv6 への移行である．もう一つは DNSSEC の導入が世界的に本格化していることである．上記に挙げたような利用形態の変化が生じても DNS の正常な運用を維持することがインターネット全体の健全な運用にとって重要と言える．本稿ではキャッシングサーバの実トラフィックに基づいて現状の DNS トラフィックの動向を分析した．また，この分析結果からキャッシングサーバにおいてはユーザクエリが約 1.46 倍，権威サーバクエリが約 1.2 倍に増加し，また権威サーバからの応答パケットサイズは平均で現状の 3.34 倍に達するという予測が導かれた．これらの数値は移行状況や実際の運用上の設定値によっても変動するため今後とも引き続き精査が必要であるが，ネットワークの運用者は実際のサービスに影響が出ないよう，あらかじめ各ネットワークにおいて今後の DNS トラフィック増加を予測し設備・設計が十分かどうかを早期に検討しておくことが重要と言えるだろう．

参考文献

1) P. V. Mockapetris, “Domain names - concepts and facilities,” RFC 1034, November 1987.
2) P. V. Mockapetris, “Domain names - implementation and specification,” RFC 1035, November 1987.
3) G. Huston, “IPv4 Address Space Report,” http://www.potaroo.net/tools/ipv4/.
4) US CERT/CC, “Multiple DNS implementations vulnerable to cache poisoning,” http://www.kb.cert.org/vuls/id/800113, July 2008.
5) D. Eastlake, 3rd, C. Kaufman, “Domain Name System Security Extensions,” RFC2065, January 1997.
6) R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, “DNS Security Introduction and Requirements,” RFC4033, March 2005.
7) R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, “Resource Records for the DNS Security Extensions,” RFC4034, March 2005.
8) R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, “Protocol Modifications for the DNS Security Extensions,” RFC4035, March 2005.
9) ICANN, “ICANN to Work with United States Government and VeriSign on Interim Solution to Core Internet Security Issue,” ICANN Announcements, June 2009.
10) JPRS, “JP ドメイン名サービスへの DNSSEC の導入予定について,” http://jprs.jp/info/notice/20090709-dnssec.html, June 2009.
11) K. Rikitake, H. Nogawa, T. Tanaka, K. Nakao and S. Shimojo, “An Analysis of DNSSEC Transport Overhead Increase,” IPSJ SIG Technical Reports 2005-CSEC-28, Vol. 2005, No. 33, pp. 345-350, March 2005.
12) IANA, “IPv6 Addresses for the Root Servers,” http://www.iana.org/reports/2008/root-aaaa-announcement.html, IANA Reports, January 2008.
13) Internet Association Japan, “Measurement of IPv6 readiness,” http://v6metric.jp/
14) http://snad.ncsl.nist.gov/dnssec/bandwidth.html
15) O. Kolkman, “Measuring the resource requirements of DNSSEC.” http://www.ripe.net/ripe/docs/ripe-352.html, RIPE-352, September 2005.
16) B. Ager, H. Dreger and A. Feldmann, “Predicting the DNSSEC overhead using DNS traces,” Information Sciences and Systems, 2006 40th Annual Conference, pp.1484-1489, March 2006.
17) R. Gieben “.ca Signing Metrics.,” http://www.nlnetlabs.nl/downloads/publications/ca-reg.pdf, NLnet Labs document 2006-001, May 2006.
18) J. Schlyter, “DNSSEC Validation Performance Testing,” http://www.ietf.org/old/2009/proceedings/06mar/slides/dnsop-0.pdf, 65th IETF dnsop WG, March 2006.
19) 若杉泰輔, 副島裕司, 島村祐一, 岡英一, “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,” 信学技報, Vol. 109, No. 119, IN2009-35, pp. 61-66, June 2009.
20) E. Rozendaal, “Modifying NSD for DNSSEC: Design, Implementation, Performance,” January 2004.
21) 豊野剛, 石橋圭介, 西田晴彦, 三宅延久, “DNS キャッシングサーバにおける異常クエリ分析,” 情報処理学会研究報告, Vol. 2008, No. 23, pp. 19-24, March 2008.
22) P. Vixie, “Extension Mechanisms for DNS (EDNS0),” RFC2671, August 1999.
23) OneStat.com, “Microsoft's Windows Vista global usage share is 21.16 percent on the web according to OneStat.com,” http://www.onestat.com/, December 2008.