Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

IPv6/IPv4トランスレータ環境下における DNSsecの実装と評価

渋谷卓磨† 佐々木良一†

IPv4 アドレスの枯渇時期が近づく中，その対策として IPv6 アドレスが使用され始めており IPv4 ネットワークと IPv6 ネットワークが共存しはじめている．これらを実現する方法の１つに IPv6/IPv4 トランスレータがある．一方，DNS のキャッシュポイズニング攻撃対策として考案された DNSsec が普及しつつある．しかし，IPv6/IPv4 トランスレータ環境下において DNSsec が近い将来使われるのは明らかでありながら，機能的・性能的に問題なく動くかどうかの検証は著者らの知る限り行われてこなかった．そこで，著者らは実験環境を構築し，IPv6/IPv4 トランスレータと DNSsec の同時使用が可能かどうかの確認と，通信時間に与える影響の測定と評価をしたので報告する．

Implementation and evaluation of DNSsec in the IPv6/IPv4 translator environment

Takuma Shibuya† and Ryoichi Sasaki†

An IPv6 address begins to be used as the measures, and an IPv6 network begins to coexist with an IPv4 network while the drying up time of the IPv4 address is reaching. An IPv6/IPv4 translator is one of the methods to realize such coexisting environment. On the other hand, DNSsec devised as an anti-cache poisoning attack measure of the DNS is spreading. However, though DNSsec in IPv6/IPv4 translator environment will be clearly used in near future, there are no researches to confirm the function and/or the performance. Therefore the authors built experiment environment and confirmed the weather IPv6/IPv4 translator environment can be used at the same time or not, and measured the transmission time. This paper reports the confirmed, measured and evaluated results.

1. はじめに

近年インターネットの普及に伴うIPv4アドレスの枯渇問題が懸念されている．IPv4アドレスの枯渇する時期が２０１１年内と言われており（図１），既にIPv6アドレスが導入され始めている．IPv6アドレスの導入に伴い，現在使用されているIPv4アドレスと新しく導入されているIPv6アドレスが共存するネットワークが存在し，その相互接続技術の一つとしてIPv6/IPv4トランスレータ（以下トランスレータ）[1] が提案され利用されてきた．一方，DNSのキャッシュポイズニング攻撃対策として考案されたDNSsec[2]の利用も増え始めている．

トランスレータに関する研究[3]～[5]，DNSsecに関する研究[6]～[8]は個別に存在するが，IPv6/IPv4トランスレータ環境下においてDNSsecが近い将来使われるのは明らかでありながら，機能的・性能的に問題なく動くかどうかの検証は著者らの知る限り行われてこなかった．

本稿では，同時使用が出来なくなる原因を予想し対策を立てした上で実験環境を構築し，IPv6/IPv4トランスレータとDNSsecの同時使用が可能かどうかの確認と，同時使用時の通信時間に与える影響の測定を行い各技術の単独使用時とデータ比較を行い評価したので報告する．なお，同時使用における問題は互いの動作が影響しているため，トランスレータとDNSsecを順々に説明した後に同時使用の説明をする．

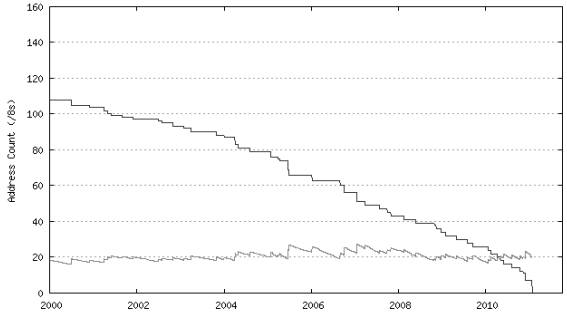

図 1 IPv4アドレスの在庫枯渇予想グラフ[9]

† 東京電機大学
Tokyo Denki University

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

2. IPv6/IPv4 トランスレータ

2.1 IPv4 アドレスと IPv6 アドレス

IPv4アドレスとIPv6アドレスは直接的な互換性がないため，互いのインターネットプロトコル（以下IP）を越えて通信することが出来ない．これは，IPv4とIPv6ではいくつかの仕様が異なるためである．大きな違いは以下の二つである．

（１） アドレス空間に利用できるビット数
（２） IPヘッダのフォーマット

アドレス空間に利用できるビット数はIPv4の場合は32ビットでIPv6は128ビットである．IPv6アドレスはIPv4アドレスの４倍のビット数を確保しているのでその差を補完または圧縮することが必要になる．また，IPヘッダの変換をする必要もある．

この２つの違いを変換し通信を可能にする技術は現在のところ次の３つにわけられる[10].

（ａ）デュアルスタックと呼ばれる方法：通信に関わる全ての機器が両方のIPを使用可能にする．これの問題点は全ての機器を両方のIPが使用可能にしなければならないので実現に時間が掛かることである．

（ｂ）トンネリングと呼ばれる方法：これは一方のIPネットワークを挟んで通信する場合に，パケットをカプセル化してもう一方のIPだというように見せて通信しネットワークの出口で元のIPに戻す方法である．

（ｃ）トランスレータと呼ばれる方法：これはIPパケットを変換して通信を可能にする方法である．

この３つの方法のうち直近の問題でかつセキュリティの分野に影響があると考えられたトランスレータに関し，DNSsecとの同時使用における問題を取り上げることにした．

2.2 トランスレータの概要

トランスレータは内部と外部ネットワークのIPが異なる場合に使用する変換器である．IPv6/IPv4変換用DNSプロキシ（以下DNSプロキシ）によって作成，変換されたIPアドレスを使用しパケットのIPヘッダとIPアドレスを変換することで通信を可能にする．

2.3 トランスレータの動作

今回使用したトランスレータの動作を時系列で説明する（図２）．説明を簡略化するために先ずDNSの動作用語を説明する. IPアドレスの問い合わせはDNS queryである．さらにDNS queryには２種類存在し，IPv4アドレスを問い合わせる場合はDNS query(A)とし，IPv6アドレスを問い合わせる場合はDNS query(AAAA)とする．ただ単にDNS queryと記されている場合はどちらでもよいことにする. また, DNS queryに対してDNSサーバがする応答はDNS responseである．

ここでは，IPv6ネットワークにつながっているユーザが，IPv4ネットワークにつながっているwebサーバにアクセスする場合を用いて説明する．

（１）ユーザがドメイン名からIPアドレスを検索するために内部ネットワーク内にあるDNSプロキシにDNS query(AAAA)を送信する．

（２）内部ネットワークと外部ネットワークでIPが異なるのでDNSプロキシはDNS query(A)に変換し，DNSサーバに送信する．

（３）DNS query(A)を受け取ったDNSサーバはDNS query(A)に対しての応答としてIPアドレス情報が入ったDNS responseをDNSプロキシに送信する

（４）DNSプロキシがDNS responseのIPアドレスを変換し，ユーザに送信する．

これで，ユーザはIPアドレスを取得することが出来る．次にユーザがwebサイトと通信する手順を説明する．

（５）IPアドレスを受け取ったユーザは変換されたIPアドレスに向けてデータを送信する．

（６）変換されたIPアドレスの上位32ビットはトランスレータのネットワークアドレスなので，送信されたデータはトランスレータへ届く．

（７）トランスレータはIPヘッダとアドレスを元に戻し，webサーバに送信する．

（８）webサーバから送られてくるデータに対してトランスレータがIPヘッダとIPアドレス変換を行い，ユーザに送る．

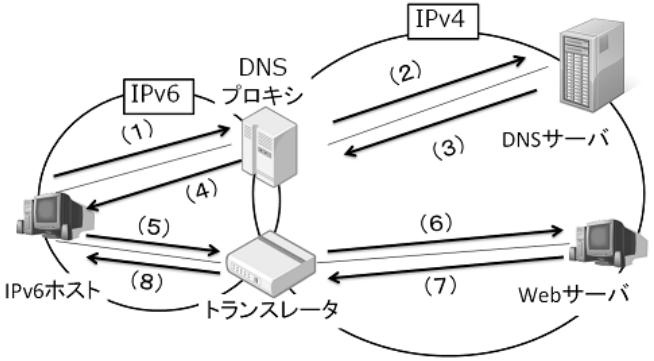

図 2 トランスレータの動作環境

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

2.4 IP アドレス変換

次に，変換用DNSプロキシの機能であるIPアドレス変換の仕組みを説明する．今回の研究ではIPv4アドレスをIPv6アドレスに変換した．変換するために使った技術はIPv4アドレスをマッピングする方法である(図３). マッピングの仕組みはIPv6のネットワークを指定する64ビットのプレフィックスを用意し，下位32ビットはIPv4アドレスで残りの部分に0を挿入する．このようにしてIPv4アドレス情報が含まれたIPv6アドレスが作成される．

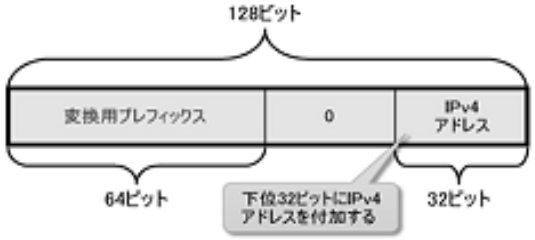

図 3　変換用プレフィックスを用いたIPv6アドレス[1]

3. DNSsec

3.1 DNSsec の概要

DNSキャッシュポイズニングといったDNS応答の成りすまし攻撃が存在する．DNSキャッシュポイズニングはDNSのキャッシュ機能を利用し，一時的にホスト名とは別のIPアドレスを登録し，本来登録されていたサイトの情報とは別のサイトの情報に書き換える攻撃のことである．この攻撃を受けることにより，ユーザが通信しようとしているwebサイトとは違う偽のWebサイトに誘導されてしまう．この攻撃を防ぐのがDNSsecである． DNSsecはDNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するためのセキュリティ拡張機能である．

3.2 DNSsec の仕組み

DNSsecは公開鍵暗号方式を利用した電子署名を転送データに付与することでDNSのセキュリティを拡張する技術である．公開鍵暗号方式は公開鍵と秘密鍵と呼ばれる２つの鍵を用いて暗号化と復号をする方式である．また，電子署名とは公開鍵暗号方式とハッシュ値と呼ばれる値を用いて本人確認やデータの改ざんを防止するものである．

DNSsecはDNSサーバから送られてくるDNS responseが正規のDNSサーバからの応答であることを証明してくれる．DNSサーバは階層構造になっておりIPアドレスを問い合わせる際には，複数のDNSサーバに問い合わせをすることになる．DNSsecはDNSサーバからの応答が正しいものであるかを判定するため，複数のサーバに問い合わせを行う場合はその回数分DNSsecの署名を検証する必要がある．なお，DNSの最上位に位置するルートDNSサーバについては通信の前にルートDNSサーバの公開鍵を登録しておくことで正規であることを確認できる．

次に，DNSsecの動作について説明する（図４）． DNSsecは通信における名前解決の工程で使用される．

（１） ユーザがDNSサーバにDNSsec付きDNS queryを送信する．DNSsecをつけることでユーザ側がDNSsecの対応が出来ていることを知らせている．
（２） DNS queryを受け取ったDNSサーバはドメイン名とホスト情報を関連付けたデータであるリソースレコードの中から該当するデータを探し出す．
（３） （２）で該当したリソースレコードに対してハッシュ関数を用いてハッシュ値を求める．
（４） ハッシュ値を公開鍵暗号の秘密鍵を用いて暗号化して署名とする．
（５） 該当したリソースレコードと署名をDNS responseとしてユーザへ送る．
（６） 署名を公開鍵を用いて復号し，送られてきたリソースレコードのハッシュ値と同じかどうかを検証することにより署名を確認することで，正規DNSサーバから送られてきたDNS responseであり，かつ改ざんされていないことが証明できる．

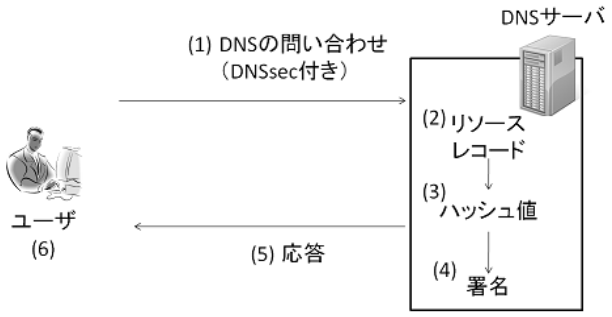

図 4　DNSsec の動作

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

4. 同時利用の問題

4.1 問題点

トランスレータとDNSsecを同時使用するとDNSsecの認証が正常に動作しない可能性があるという報告がある[1]．しかし，具体的な説明が記述されていないのでなぜ通信が出来なくなるのかを考える必要あった．トランスレータとDNSsecを使用する場合，動作の時点で重なる部分があり，その部分は名前解決の部分である．トランスレータはDNSサーバに送るDNS query(A)をDNS query(AAAA)に変換する．変換された問い合わせはDNSサーバへ届き，DNSサーバからDNS responseが応答として送信される．その応答をまた変換してユーザに届ける．この工程の中でDNSsecを使用する場合はトランスレータ自体に影響を与えることはない．それよりもトランスレータのために使用するDNSプロキシと動作部分が重なるのでここが動作できない問題だと思われる．このDNSプロキシが変換するものは二つあり，IPアドレスの問い合わせとDNSサーバの応答内容である．この内のDNSサーバの応答を変換する過程がDNSsecの認証する過程と重なるためにDNSsecの検証時に「改ざん」と判断してしまうのである．

4.2 従来方式の動作

その結果にいたる動作を詳しく説明する（図５）．

（１） ユーザがDNS queryを送信する．
（２） DNSキャッシュサーバがDNS queryにDNSsecを付加する．
（３） DNSsec付きDNS queryを変換してDNSサーバに送信する．
（４） DNSサーバがDNS queryの応答として署名付きDNS responseを送信する．
ここでIPアドレスを元にハッシュ値を取る
（５） DNSプロキシはDNSサーバから送られてきたDNS responseを変換する．このときにDNSサーバからの応答内容であるIPアドレスを変換する．
（６） DNSキャッシュサーバで送られてきたIPアドレスのハッシュ値を得て署名を検証すると改ざん判定が出る．

上記のような通信手順ではDNSsecの署名を検証する段階で問題が起こると予想される．これはDNSsecの検証がハッシュ値の比較をすることで行うためである．ハッシュ値はIPアドレスを元に作成される．ハッシュ値を得るためにDNSサーバで使用したIPアドレスとDNSキャッシュサーバで使用したIPアドレスが異なるので「改ざん」の判定を出してしまい安全な応答ではないものとされてしまう．このようにしてDNSsecでは間違った判断をしてしまうのだと予想できる．

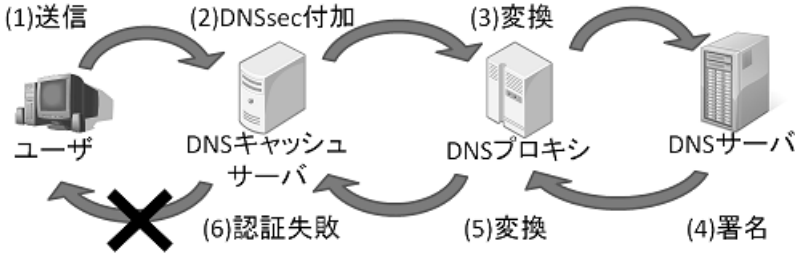

図 5　通信できない場合

4.3 影響

DNSsecが改ざんの判定を出すと通信することが出来なくなる．また現在の仕様ではDNSsecが改ざんの判定を出したことが通信が出来ない原因だとユーザが受動的に知ることが出来ず，コマンドプロンプトなどで原因を追究しなければならない．ユーザはただ単にDNSサーバとの名前解決に問題が生じたことしか知ることができないので一般的なユーザは原因を探すことが難しくなる．このため早急に対処することが求められる．

4.4 改良方式

これは認証と変換の順序が間違った順序であるために起こるものだと思われる．そこで改良方式を導入し，DNSプロキシとDNSキャッシュサーバが逆の順序で配置されていれば通信は可能だと推測できる．その理由を説明する（図６）．実験環境はDNSプロキシのあとにDNSキャッシュサーバを設置する環境に変更する．

（１） ユーザがDNS queryを送信する．
（２） DNSプロキシがDNS queryを変換しDNSキャッシュサーへ送信する
（３） 変換されたDNS queryに対してDNSsecを付加してDNSサーバに送信する．
（４） DNS queryを受け取ったDNSサーバはDNSsecの署名を付けて送信する．
（５） 署名を検証して正規サーバからの情報と判断し，その後DNSプロキシに送信する．
（６） DNSプロキシは変換してユーザにIPアドレスの情報を送信する．

先ほどと違うのはDNSsecの認証の工程の間にDNSプロキシの変換する工程が入っていない点である．この通信環境であればDNSsecの署名を変換することはないと考えられる．

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

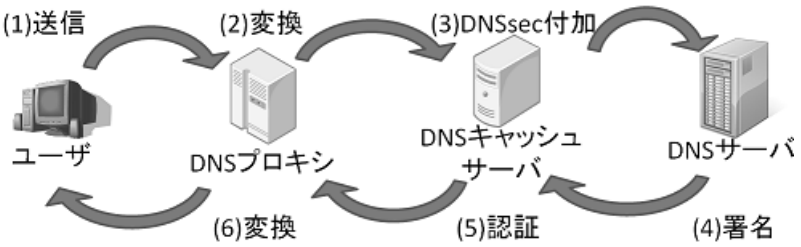

図 6　通信可能の場合

そこで，改良方式を導入し機能・性能的に問題ないか実験してみることにした．

5. 実装と評価

5.1 実験目標

トランスレータとDNSsecの同時使用時の双方の正常な動作を確認することが最大の目標である．ついでにDNSsecの認証が適切に行われているのか，トランスレータの変換により計算が合わず改ざんの判定をするかを確認する．またトランスレータの変換内容がDNSsecの有無で違いがないかを比較検証する．さらに，トランスレータとDNSsecの各技術が与える遅延時間が通信にどの程度の影響を与えるものなのかを実験から得たデータをもとに考察にまとめる．また，実験で得た結果をもとにトランスレータとDNSsecの改良方法や問題点を見つける．２つの技術を同時使用することでさらに遅延時間が増大したりしないかなど通信できるが悪い影響があった場合なども見つけるようにする．

5.2 実験手法

トランスレータとDNSsecを同時使用しその併用を確認するためにトランスレータとDNSsecを有効にした実験環境を用意する．この実験環境で通信を行い通信が確認できたら同時利用しても通信することが証明される．このときに通信内容も確認してDNSsecの署名を適切に行えているかも確認する．さらに同時使用の遅延時間を測定して通信にどの程度の影響を与えるのかを調べ，２つの技術が普及した場合に正常に使える範囲の影響度なのかを判定する．

また，トランスレータのみを使用する環境を構築しトランスレータの遅延時間を測定する．これと同様にDNSsecのみを有効にした環境を構築しDNSsecの遅延時間を測定する．最後にデータを比較するためにトランスレータとDNSsecを無効にした環境で通信時間を測定する．これら４種の環境で得られたデータを比較して，同時利用をすると他の通信環境と比較してどれだけの影響を与えるものなのかを調査することができる．

5.3 実験環境

同時使用の弊害の有無を確認，及びトランスレータとDNSsecの通信時間に与える影響を測定比較するために4種の実験環境を構築した．使用したソフトウェアを表１に記述し，実験環境の比較を表２に記述する．表２における○と×は実験環境における機能の有無を示している．

表 1　使用したソフトウェア

機能	ソフトウェア
DNSプロキシ	totd 1.4
トランスレータ	ptrtd 0.5.2
DNSキャッシュサーバ	bind 9.7.2-P2

表 2　実験環境比較表

	（1）	（2）	（3）	（4）
トランスレータ	×	×	○	○
DNSsec	×	○	×	○

次にトランスレータを使用する実験環境の構築方法を説明する．この実験環境を構築するには二つの条件が必要である．それは内部ネットワークと外部ネットワークを異なるプロトコルにすることとDNSプロキシを使用することである．まず内部，外部ネットワークを異なるプロトコルにするためにIPv6ルータであるradvdを使用した．このルータを使用することでIPv6ホストにローカルIPv6アドレスを設定することができる．このようにすることでIPv6のPC間で通信が可能となるので内部IPv6ネットワーク

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

を構築することが出来る．次に外部ネットワークと通信を可能にするためにDNSプロキシとトランスレータを用意する．DNSプロキシとトランスレータの設置場所はIPv4ネットワークとIPv6ネットワークの両方に接続することが出来る場所にする必要がある．これは，どちらも変換をするので異なるネットワーク間に設置する必要があるからである．

まず，DNSプロキシを用意する．DNSプロキシには変換するプレフィックスと次のDNSキャッシュサーバを設定する．DNSプロキシを用意できたらトランスレータの設定をする．このときトランスレータに設定するプレフィックスをDNSプロキシで設定したプレフィックスと同じアドレスにすることで，ユーザがトランスレータに通信データを送信することが出来る．

今実験ではDNSsecと同時使用するためにトランスレータを使用できる環境を構築した上でDNSsecを用意する必要がある．DNSsecを使用するためにDNSsec対応をしているDNSキャッシュサーバを用意した（図７）．

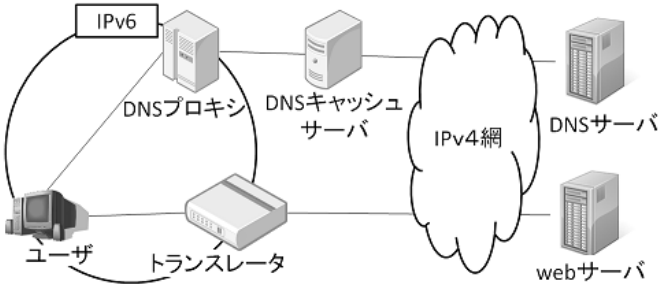

図 7　IPv6実験環境

また，通信データの比較をするためにトランスレータを使用しない環境が必要になる．これはトランスレータを使用しないので外部と内部のネットワークを同じプロトコルにする必要がある．このため，先ほどの環境構築で使用したIPv6ルータを使用せず，はじめから設定してあったIPv4ルータを使用した．また，DNSsecを有効にする場合はDNSキャッシュサーバであるbindのDNSsecを有効に設定することでDNSsecだけを有効にした環境を構築した（図８）．

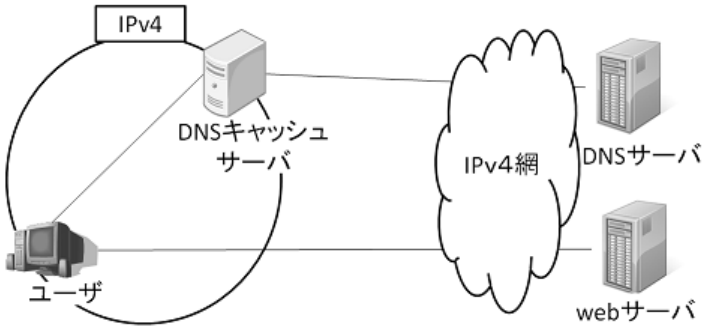

図 8　IPv4実験環境

今回の実験では図７の環境でトランスレータとDNSsecの同時使用が可能であるか確認を行う．また，４種類の環境で通信時間を測定，比較しトランスレータとDNSsecが通信時間に与える影響と２つの機能の相性を検討する．

5.4 実験手順

各通信環境を用意して同じwebサイト（www.isc.org）に対しての通信動作の確認，及び通信時間の測定をした．なお，このwebサイトを使用したのはDNSsecに対応しているDNSサーバを使っているサイトだからである．DNSsecの対応をしているサイトは国内を検索したが，現段階で私が調べた限りでは存在しておらず外国にあるサイトを実験のサイトにするしかなかった．また，このサイトはInternet Software Consortiumというインターネットにおける実装の標準となるような，質の高いオープンソースのソフトウェアを作ることを目標とする非営利団体であり，今回使用したソフトウェアの１つであるBindを作成した会社である．今回の実験でBindはDNSsecの実装に使っておりDNSsecの認証に関わる実験をするのにあたり適切なサイトであると考えられる．実験の方法は以下の３つの手順を踏んだ．

① DNSキャッシュサーバのキャッシュを初期化
② ブラウザにあるwebページキャッシュ機能の無効
③ ユーザのブラウザでwebサイトの表示

１つの環境につき上記の手順を２０回繰り返し通信時間を８０回分測定した．測定したデータを実験環境ごとに分け，各環境ごとの平均通信時間を算出した．

Vol.2011-DPS-146 No.6
Vol.2011-CSEC-52 No.6
2011/3/10

5.5 実験結果

実験結果は表３の通りである．

表 3　実験結果

	（1）	（2）	（3）	（4）
トランスレータ	×	×	○	○
DNSsec	×	○	×	○
通信時間(秒)	5.18	6.92	5.69	6.98
遅延時間（秒）	0	+1.74	+0.51	+1.80

6. 考察

6.1 機能の考察

今回の実験ではトランスレータとDNSsecの配置を適切な状態にして同時使用した場合，正しく動作することを確認できた．これは問題原因を考察するときに推測した通りトランスレータが応答を変換する前にDNSsecが署名の検証をしていたためだと考えられる．

6.2 性能の考察

今回の実験により，DNSsecとトランスレータを併用することによる通信時間の増加は1.8秒と十分小さいことが明らかになった．なお，実験ではDNSsecのためのデータ通信をしていることは確認出来たので，認証が正しくできていると考えているが，内容を具体的に確認する方法が見つからず，今後の研究で明確にしていきたい．また，規模を拡大しての実験も今後の課題である．

7. まとめ

今回の実験によりトランスレータの変換より先にDNSsec認証の検証が出来るような通信環境にすれば，トランスレータとDNSsecの同時使用は条件を満たせば可能であることが明らかになった．

また，DNSsecとトランスレータを併用することによる通信時間の増加は十分小さいことが明らかになった．しかし，今回の性能評価の実験は最小の規模で行ったものであり，規模を拡大して実験を実施していきたいと考えている．

謝辞　IPv6 に関する種々の知識をご教授いただいき，研究の方向づけに関しご議論いただいた株式会社インターネットイニシアティブの歌代和正氏，島 慶一氏，山本和彦氏に感謝申し上げる．

参考文献

[1]　トランスレータの動作概要
http://itpro.nikkeibp.co.jp/article/COLUMN/20100125/343740/?ST=neteng&P=3
(2011年1月24日)
[2]　DNSsecとは
http://itpro.nikkeibp.co.jp/article/Keyword/20090721/334154/
(2011年1月24日)
[3]　藤崎 智宏，松本 存史，新延 史郎：IPv6/IPv4プロトコルトランスレータの評価(試作・評価・実用化,サービス管理,ビジネス管理,料金管理,及び一般)，電子情報通信学会技術研究報告，2008.5
[4]　山本 和彦，角川 宗近，島 慶一：Pv4とIPv6のトランスレータに関する考察，情報処理学会研究報告，1997.6
[5]　竹内 敬亮，武田 幸子，井内 秀則，立川 敦：IPv4/IPv6トランスレータ連携DNS Proxyサーバの開発，電子情報通信学会技術研究報告，2003.3
[6]　副島 裕司，若杉 泰輔，島村 祐一，平野 衡，岡 英一：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，2009.2
[7]　力武 健次，野川 裕記，田中 俊昭，中尾 康二，下條 真司：DNSSECトランスポートオーバヘッド増加に関する解析，情報処理学会研究報告，2005.3
[8]　辻野 大輔，飯田 勝吉，山口 英：DNSSEC導入のためのCPU負荷解析と大規模Authoritativeサーバの実現手法，電子情報通信学会技術研究報告，2002.3
[9]　IPv4 address report
http://ipv4.potaroo.net/
(2011月1月24日)
[10]　トランスレータの役割
http://itpro.nikkeibp.co.jp/article/COLUMN/20090924/337702/?ST=neteng
(2011年1月24日)