科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１２６０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００８０

研究課題名（和文）ＤＮＳＳＥＣに対応した広域分散ＤＮＳサービス環境シミュレータの設計と実装

研究課題名（英文）The design and implementation of the simulator for distributed DNS services with DNS SEC enabled

研究代表者
関谷　勇司（SEKIYA, Yuji）

東京大学・情報基盤センター・准教授

研究者番号：３０３６１６８７

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：本研究では、DNSSECの普及を促進し、信頼できるインターネットを実現するための一助となるべく、DNSSECシミュレータの設計と実装を行った。DNSSECは、DNSを信頼できるシステムにするための重要な技術であるが、導入後のDNSサーバの負荷やトラフィックの変化などを適切に予想する手法が存在しない。そこで本研究では、DNS管理者が自組織のDNS環境をそのままDNSSECに対応させた場合の、DNSサーバの負荷やネットワークトラフィックの変化、ユーザに与える影響を的確にシミュレーションするためのソフトウェアを設計・実装した。なお、本研究の成果物はフリーソフトウェアとして公開した。

研究成果の概要（英文）：In this research, we designed and implemented a DNSSEC simulator to encourage deployment of DNSSEC and achieve the trusted Internet. DNSSEC is an important technology to validate the origin of DNS data, however, there was no method to evaluate the load of DNS servers, the changes of network traffic, and the changes of response time when DNSSEC enabled. The DNSSEC simulator implemented in this research can evaluate them beforehand, and it is published as open source software.

研究分野：　情報学

科研費の分科・細目：　計算機システム・ネットワーク

キーワード：　DNS　DNSSEC　NS-3　シミュレーション　DCE　CreateZones

１．研究開始当初の背景

DNSSEC は、DNS の信頼性を向上させる技術として、近年注目を浴びている。

DNSSEC 自体は古くから標準化が進められている技術であるが、その導入は全くと言っていいほど進んでおらず、誰も使わないまま標準化だけが行われていた。しかし、2008 年に図 1 に示す「カミンスキー攻撃」が公表されると、DNSSEC の必要性が再認識された。これによって、DNS 管理者はやむなく DNSSEC 導入を迫られる結果となり、特に TLD などの公共性の高いドメイン名において、DNSSEC の導入が急速に進行している。

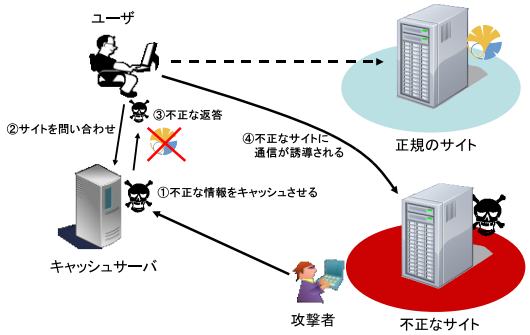


図 1：カミンスキー攻撃の概要

２．研究の目的

本研究の目的は、DNSSEC の普及によって大きな変化を迎えている DNS を、DNSSEC を含めた DNS のシステム全体としてシミュレーションする手法を確立し、その手法を利用したシミュレータを設計・実装することである。

DNSSEC を利用することで、DNS 応答のなりすましや改ざんを防ぐことが可能となる。その一方で、DNSSEC 導入による DNS 通信パケットサイズの増大や、DNS メッセージ交換回数の増加、ならびにユーザに対する DNS 応答時間の増加といった問題が発生している。これらの変化は、今までの DNS に対する経験や知識からでは予測が難しいものであり、DNSSEC 対応によって DNS サーバやユーザに及ぼされる影響を、広範囲にわたってシミュレーションする手法が必要とされている。そこで本研究では、DNSSEC を導入した際に、DNS サーバに与える負荷やトラフィックの変化、ユーザへの応答速度の変化をシミュレーションすることのできる手法とソフトウェアを研究開発することを目的とする。

本研究の成果によって、DNSSEC 導入が組織の DNS 全体に与える影響を事前に分析し、DNSSEC 導入前に起こりうる問題を発見することが可能となる。

３．研究の方法

(1) シミュレーションアルゴリズム確立のための基礎データの収集と解析

まず、既存研究［2］の、DNS サーバ応答性能データを元にした Root DNS サーバ、gTLD DNS サーバ、ccTLD DNS サーバへのネットワーク到達性能、ならびに世界各地からそれぞれの DNS サーバへの応答性能を分析した研究成果である［1, 2, 3, 4, 5］を用いて、シミュレーション手法を確立するための基礎データを収集する。実際に収集するデータは次の 3 つである。

- DNS サーバの配置によるネットワーク基本性能
- DNS サーバの種別やソフトウェアの差異による基本応答性能
- エニーキャスト等の運用形態の差異や役割の差異による基本応答性能

これによって、DNS サーバの配置や運用形態による、応答性能のある程度のつかみ、シミュレーション手法の基礎となるデータとして利用する。なお、DNS サーバは、その役割から二種類のサーバに分類できる。図 2 に示す通り、それぞれの役割とその動作は全く異なるものであるため、DNS サーバ（Auth）と DNS サーバ（Cache）と分類して 基礎データの分析と作成を行う。

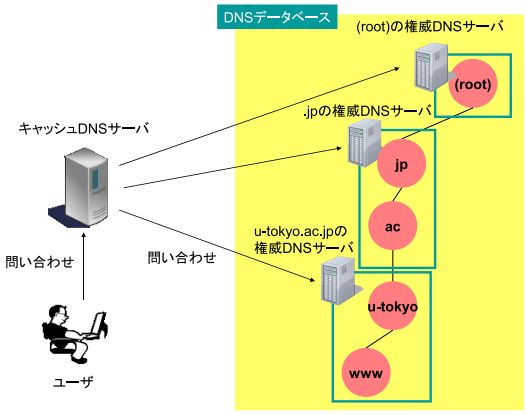


図 2 ： 役割による DNS サーバの分類

本項目は平成 23 年度前半期において行い、既存研究の研究成果を最大限に利用して、シミュレータ作成の基礎となる実験データを収集ならびに分析する。

(2) シミュレーションへの入力/出力パラメータの定義

本研究では、シミュレーションに用いる入力パラメータを以下の通り定義する。

- DNS サーバのネットワーク性能
- Root DNS サーバならびに gTLD DNS、ccTLD DNS サーバからのネットワーク距離
- DNS サーバの役割とユーザ問い合わせの頻度

また、シミュレーション結果として出力されるパラメータを以下の通り定義する。

- DNS サーバ単体の負荷
- DNSSEC のために行われる DNS サーバ間のインタラクションによる負荷
- 署名検証によるユーザに対する応答速度の変化

さらに、シミュレーションで発生するイベントを以下の通り定義する。

- あるゾーンもしくはある権威 DNS サーバ

に DNSSEC を導入した場合
- あるキャッシュサーバを DNSSEC 対応にした場合
- あるゾーンを担当する権威 DNS サーバを追加もしくはエニーキャスト運用した場合

これらの定義を用いて、本研究では DNSSEC の導入ならびに DNS サーバの設定変更が DNS 全体に与える影響をシミュレーションできる仕組みを提供する。

(3) シミュレータの設計・実装・検証

基礎データ、シミュレーションパラメータ、シミュレーションアルゴリズムを定義した後に、シミュ レータの設計と実装を行う。シミュレータは C 言語にて作成し、DNS サーバやユーザといった要素を、モジュールとしてシミュレータ内部で動作させることができるよう作成する。一つのシミュレータ内部でモジュールとして扱えるようにする要素を、以下の通り定義する。
- 複数の DNSSEC ゾーン
- 複数の権威 DNS サーバ
- 複数のキャッシュサーバ
- 複数のユーザ

なお、本研究にて作成したシミュレータは、その開発段階から積極的に公開を行ない、オープンソースソフトウェアとして公開しながら開発を進める。

[1]“Availability and Effectiveness of Root DNS servers: A long term study”, Bu-Sung Lee, Yu Shyang Tan, Yuji Sekiya, Atsushi Narishige, Susumu Date, Proceedings of the 12th IEEE/IFIP Network Operations and Management Symposium (NOMS 2010), pp.862-865, Osaka, Japan, April 2010.
[2]“Gulliver Project - status update in 2009”,Yuji Sekiya, ISMA 2010 AIMS-2 Workshop on Active Internet Measurements, San Diego, U.S.A., February 2010.
[3]“Behavior Analysis of DNS Anycast in 2008”, Yuji Sekiya, The 2nd CAIDA/WIDE/CASFI Workshop, Seoul, Korea, April 2009.
[4]“Trends of DNS Reachability in 2008”, Yuji Sekiya, The 7th JST/CNRS Workshop, Toulouse, France, March 2009.
[5] Gulliver Project Summary on 2007”, Yuji Sekiya, 9th CAIDA/WIDE Workshop, Honolulu, Hawaii, U.S.A., January 2008.

４．研究成果

(1) 平成 23 年度研究成果

平成 23 年度は、DNSSEC に対応した DNS シミュレータを作成するための前提となる、基礎データの収集とパラメータ決定を行った。また、シミュレーションソフトウェアを作成するにあたっての、基盤となるソフトウェアの決定を行った。まず、基礎データの収集として、現在インターネットにて稼働している DNS サーバの状況とゾーン数に関する調査を行った。その結果、DNS 全体のサービスを支えるために重要と役割を担っている Root DNS サーバと TLD DNS サーバは、約 1000 台の個体にて構成されていることがわかった。これにより、1000 台程度の DNS サーバの動作をシミュレーションすることができれば、あるゾーンを DNSSEC 対応にした場合の、Root DNS から始まる DNS 全体の挙動をシミュレーションできることが判明した。この DNS サーバ個体数をもとに、それぞれの DNS サーバ個体が有している平均ゾーン数を調査し、シミュレーション全体として有すべきゾーン数を算出した。また、実際のユーザがキャッシュ DNS サーバに出す問い合わせクエリを分析し、シミュレーションソフトウェアが実現すべき次の規模性を抽出した。
- DNS サーバ個体数
- 全体としてのゾーン数
- ユーザの個体数と問い合わせクエリ数

また、実際の権威サーバとキャッシュサーバに問い合わせられたクエリを分析し、ひとつゾーンを有する一つの組織におけるサンプルクエリデータを作成した。

さらに、DNSSEC シミュレーションソフトウェアを作成するにあたっての基盤となるシミュレーション環境を選定した。この時点で開発が活発に進められていた ns-3 を選択し、さらに本研究の当初の目的である、モジュール化された DNS サーバやユーザを実現するために、ns-3 の拡張である DCE(Direct Code Execution)機能を採用することを決定した。

(2) 平成 24 年度研究成果

平成 24 年度は、前年度の基礎データ収集結果やシミュレーション規模の結果を経て、シミュレータの設計と実装を進めた。シミュレータを設計するにあたって、実現すべきシナリオをより具現化し、DNS 管理者や運用者により役立つシミュレータを目指した。具体的には、自組織の DNS サーバやゾーンを DNSSEC 対応にした場合の、DNS サーバの負荷や特性、ネットワークに与える影響をより忠実にシミュレーションできるような設計を目指した。そのため、以下の点を実現できるよう、DNSSEC シミュレータを設計した。
- 自組織で用いている DNS サーバ実装の特性をそのまま再現できる
- 実際にユーザからの問い合わせを記録し、その記録を用いてシミュレーションができる
- 自組織内部の DNS サーバやゾーンに限らず、DNSSEC 対応時の影響を調べるために必要となる DNS サーバやゾーンも用いてシミュレーションができる

これらのシミュレーションシナリオ要件を実現するために、図 3 に示す通りシミュレータを設計した。

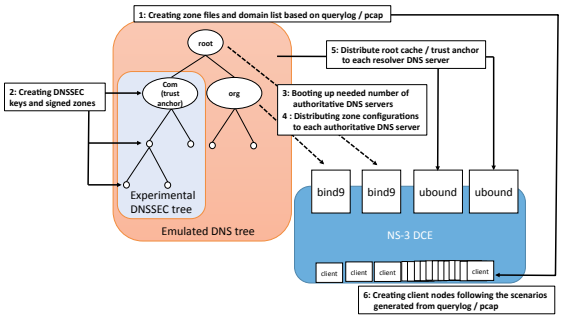


図 3 ： DNSSEC シミュレータ設計概要

(3) 平成 25 年度研究成果

平成 25 年度は、前年度に行った DNSSEC シミュレータの設計に基づき、実装と評価を行った。シミュレータの実装にあたっては、NS-3 の DCE (Direct Code Execution)という拡張機能を利用し、実際の DNS サーバ実装をそのままシミュレータ上にて動作させる方式を採用した。これによって、実際に組織内にて運用に用いられている DNS サーバ実装を、バージョンや設定まで同様な状態でシミュレーションを行うことを可能とした。DCE を用いた DNSSEC シミュレータの実装概要を、図 4 に示す。

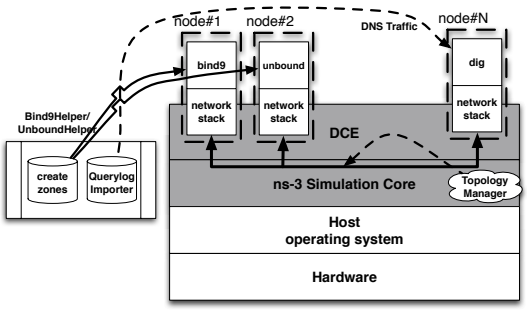
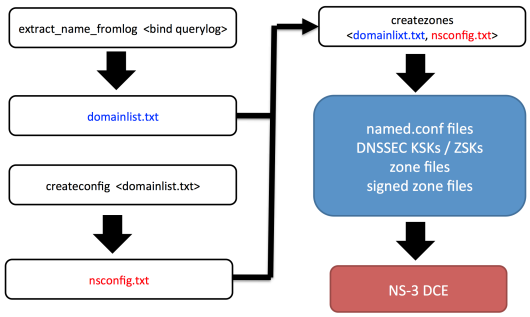


図 4 ： DNSSEC シミュレータ実装概要

さらに、シミュレーションのための DNS サーバ設定やゾーンの設定、シナリオ作成、ならびにユーザが実際にキャッシュ DNS サーバに問い合わせたログを利用してシミュレーションを行うための、CreateZone ツールを作成した。CreateZone ツールによる、DNSSEC シミュレーションシナリオ作成の概要を、図 5 に示す。

図 5 ： CreateZone によるシナリオ作成



これらのソフトウェア実装はすべてオープンソースとしてプロジェクトサイト[1]にて公開しており、誰でも入手して利用することが可能となっている。冒頭でも述べた通り、これは DNSSEC の普及に対する大きな貢献である。DNSSEC の普及を促すことは、信頼して利用できるインターネットを実現するための大きな貢献につながる。DNSSEC を利用することで、なりすましや意図的な詐称情報の注入といった、脅威からユーザを守ることができるため、結果として信頼できるインターネットを実現できるためである。

本研究にて作成したシミュレータを評価するため、ある DNS サーバを DNSSEC 対応にした場合のシミュレーションを行った結果を示す。ユーザが用いるキャッシュサーバ、ユーザが実際に問い合わせたドメイン名、ならびにそのドメイン名を保持する DNS サーバが全て DNSSEC 対応になった場合に、ユーザが名前解決結果を受け取るまでの時間がどの程度変化するかをシミュレーションした結果である。シミュレーションの手順としては、実際の運用環境においてユーザが問い合わせた名前を bind9 の querylog 機能にて記録し、その結果をもとに名前解決を実現するために必要となる DNS サーバをシミュレーションソフトウェア内部にて起動して、そのゾーンならびに DNS サーバを DNSSEC 対応にすることでシミュレーションを行った。例えば mal.example.org という名前をユーザが問い合わせ、それを解決するにあたって関わった DNS サーバとゾーンの例を、図 6 に示す。

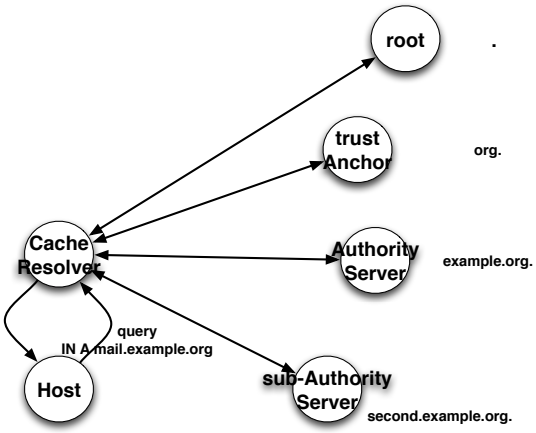


図 6 ： mail.example.org の問い合わせ

この場合、4 台の権威 DNS サーバならびに 1 台のキャッシュ DNS サーバをシミュレーションソフトウェア内部にて起動し、それぞれの権威 DNS サーバが持つゾーンを DNSSEC 対応にして DNSSEC によるレコードの署名検証機能を有効にして問い合わせる、ユーザに最終的な応答結果が返るまでの時間を計測した。さらに、同様に DNSSEC を用いない環境をシミュレータにて再現し、同様な問い合わせを行った場合の応答時間を計測した結果を、図 7 に示す。

1 http://dnssec.sekiya-lab.info/

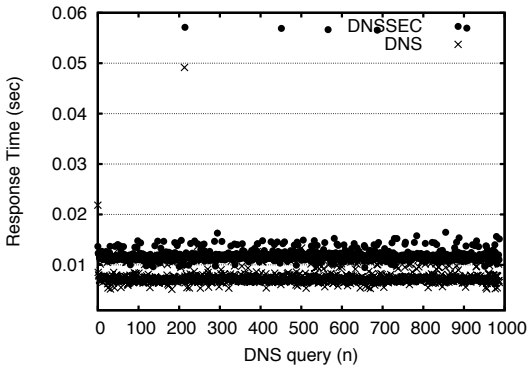


図 7 ： 応答時間の比較結果

この図より、DNSSEC に対応した場合のユーザへの応答時間の増加がシミュレーションできていることがわかる。

本研究にて設計・実装した DNSSEC シミュレータはまだまだ初歩的なものであり、大規模かつ正確なシミュレーションを行うためには、さらなる改良が必要となる。しかし、DNS 管理者が、自組織の DNS を DNSSEC 対応にした場合の影響を事前に把握することのできる、現時点での唯一かつ有用なシミュレーションソフトウェアであり、本研究の成果は、DNSSEC の普及ならびに信頼できるインターネットの実現に向けた大きな貢献である。

５．主な発表論文等

〔雑誌論文〕（計６件）

- 石原 知洋, 関谷 勇司, 村井 純 : “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・ソフトウェア, Vol.28, No.4, pp.92-107, 2011 年 11 月
- 鈴木 茂哉, 石原 知洋, Bill Manning, 村井 純 : “DNSSEC リソースレコードを用いたアドホックネットワークノード間公開鍵認証方式”, 査読あり, 情報処理学会論文誌, Vol.53, No.1, pp.385-402, 2012 年 1 月, http://ci.nii.ac.jp/naid/110008736794
- Tomohiro Ishihara, Hajime Tazaki, and Yuji Sekiya :“Design and Implementation of DNSSEC Simulator using Unmodified Real Implementations”,査読無し, IEICE Tech. Report, Vol.133, No.240, IA2013-27, pp.7-12, October 2013, http://ci.nii.ac.jp/naid/40019867426
- 石原 知洋, 櫨山 寛章, 関谷 勇司 :” 失効したルート鍵を持つ DNSSEC 検証サーバの挙動調査と対策についての一考察”, 査読無し, 情報処理学会, 研究報告インターネットと運用技術(IOT), Vol. 2013-IOT-23, No. 5, pp. 1-4, 2013 年 9 月, http://ci.nii.ac.jp/naid/110009610275
- Hajime Tazaki, Frédéric Uarbani, Emilio Mancini, Mathieu Lacage, Daniel Camara, Thierry Turletti, Walid Dabbous, “Direct code execution: revisiting library OS architecture for reproducible network experiments”, 査読あり, In Proceedings of ACM CoNEXT ’13, pp. 217-228, December 2013, DOI:10.1145/2535372.2535374
- Camara, D.; Tazaki, H.; Mancini, E.; Turletti, T.; Dabbous, W.; Lacage, M., “DCE : Test the real code of your protocols and applications over simulated networks”, 査読あり, Communications Magazine, IEEE, Vol.52, No.3, pp.104-110, March 2014, DOI:10.1109/MCOM.2014.6766093

〔学会発表〕（計３件）

- 石原 知洋 :“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, 第 29 回大会, 2012 年 8 月 22 日, 法政大学
- Tomohiro Ishihara, “Design and Implementation of DNSSEC Simulator using Unmodified Real Implementations”, IEICE IA Workshop, October 10th, 2013, Konkuk University, Seoul, Korea
- Hajime Tazaki,” Direct code execution: revising library OS architecture for reproducible network experiments”, ACM CoNEXT ’13,December 11th, 2013, Fess Parker Double Tree Resort, Santa Barbara, California, U.S.A.

〔その他〕

ホームページ等

- DNSSEC シミュレータプロジェクト http://dnssec.sekiya-lab.info/
- DNSSEC シミュレータソフトウェア配布 https://github.com/shored/createzones/
- Example Simulation : DNSSEC Re-Keying https://www.youtube.com/watch?v=GUUurmUNdds

６．研究組織

(1)研究代表者

関谷 勇司（SEKIYA, Yuji）

東京大学 情報基盤センター 准教授

研究者番号：30361687

(2)研究分担者

石原 知洋（ISHIHARA, Tomohiro）

東京大学 大学院総合文化研究科 特任助教

研究者番号：60588242

(3)連携研究者

田崎 創（TAZAKI, Hajime）
東京大学 情報基盤センター 特任講師
研究者番号：10611303